ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ

ΑΝΕΣΤΗ Α. ΦΥΡΑΡΙΔΗ

Επίκουρου Καθηγητή Τμήματος Μαθηματικών

ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

ΙΩΑΝΝΙΝΑ 2000

ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ

ΑΝΕΣΤΗ Α. ΦΥΡΑΡΙΔΗ

Επίκουρου Καθηγητή Τμήματος Μαθηματικών

ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

ΙΩΑΝΝΙΝΑ 2000

Κάθε γνήσιο αντίτυπο φέρει την υπογραφή του συγγραφέα

Στα παιδιά μου

Σταύρο και Κωνσταντίνο.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ IV Ισοτιμίες

ΚΕΦΑΛΑΙΟ V Συστήματα γραμμικών ισοτιμιών

ΚΕΦΑΛΑΙΟ VI Πολυωνυμικές ισοτιμίες

ΚΕΦΑΛΑΙΟ VII Αρχικές ρίζες, Δείκτες, m-αδικά υπόλοιπα

ΚΕΦΑΛΑΙΟ VIII Τετραγωνικά υπόλοιπα

ΠΡΟΛΟΓΟΣ

"Είναι πάντως αξιοπερίεργο ότι όλοι εκείνοι που μελετούν σοβαρά την Επιστήμη της θεωρίας Αριθμών κυριεύονται από ένα είδος πάθους γι' αυτή."

C.F Gauss

Η θεωρία Αριθμών έχει σαν κύριο αντικείμενο μελέτης, τουλάχιστον στη στοιχειώδη της μορφή, τις ιδιότητες του συνόλου $\mathbb{Z}=\{0,\pm1,\pm2,\dots\}$ των ακεραίων, και ιδιαίτερα του συνόλου $\mathbb{N}=\{1,2,\dots\}$ των φυσικών αριθμών. Είναι ένας από τους πιο σπουδαίους κλάδους της Μαθηματικής Επιστήμης και ιδιαίτερα της Άλγεβρας και μάλιστα ο πιο παλιός, αφού μερικά από τα αποτελέσματά της ήταν γνωστά στους Αρχαίους Έλληνες της Κλασικής περιόδου (800 π.χ - 1500 μ.χ) π.χ στον **Πυθαγόρα** (569 - 500 π.χ), **Ευκλείδη** (~ 350 π.χ), **Ερατοσθένη** (276 - 196 π.χ) και στον **Διόφαντο** (~ 250 μ.χ)

Η μοντέρνα περίοδος της θεωρίας Αριθμών αρχίζει τυπικά το 1500 μ.χ με τον **Claude Bacher** (1581-1638) και συνεχίζεται με τις περίφημες έρευνες των **Pierre Fermat** (1601-1665) και **Leonard Euler** (1707-1783). Ουσιαστικά όμως αρχίζει με την δημοσίευση το 1801 του περίφημου συγγράμματος "Disquisitiones arithmeticae" του **Carl Friedrich Gauss** (1777 - 1855). Σ' αυτό το έργο ο Gauss συστηματοποίησε όλες τις μέχρι τότε γνώσεις για την Αριθμοθεωρία παρουσιάζοντας και πολλές νέες ιδέες του.

Από το 1800 και μετά πολλά από τα κλασσικά προβλήματα της θεωρίας αριθμών λύθηκαν, αλλά το πιο σημαντικό είναι ότι η μελέτη τους οδήγησε στη δημιουργία νέων θεωριών που αποδείχτηκαν χρήσιμες και σ' άλλους κλάδους των Μαθηματικών. Προσφατα, το 1994 ο A Wiles απέδειξε

το περίφημο Τελευταίο Θεώρημα του Fermat "Η διοφαντική εξίσωση $x^n+y^n=z^n$ δεν έχει ακέραια λύση (x,y,z) με $xyz\neq 0$ για $n\geq 3$" Στηρίχθηκε η απόδειξη αυτή σε μια εργασία των Frey, Serre και Rider το 1985-86 οι οποίοι απέδειξαν ότι το τελευταίο θεώρημα του Fermat είναι συνέπεια μιας πρότασης της Αριθμητικής Γεωμετρίας.

Η Θεωρία Αριθμών βρίσκει σήμερα εφαρμογές και σ' άλλους σύγχρονους κλάδους, όπως π.χ της Θεωρίας Αυτομάτων, της Θεωρίας Κωδίκων, της Κρυπτογραφίας κλπ. Η κατοχή του περιεχομένου του βιβλίου αυτού αποτελεί ένα στέρεο θεμέλιο για τους σύγχρονους αυτούς κλάδους αλλά και για την αφηρημένη άλγεβρα και βοηθά πολύ σε οποιαδήποτε μεγαλύτερη εξειδίκευση στην Άλγεβρα.

Σκοπός του βιβλίου αυτού είναι να δώσει μια Εισαγωγή στην Στοιχειώδη Θεωρία Αριθμών που να περιέχει όσο πιο πολλά γίνεται για ένα εισαγωγικό μάθημα θεωρίας Αριθμών, χρονικής διάρκειας ενός εξαμήνου. Έγινε προσπάθεια για την απλούστερη και πληρέστερη παρουσίαση και κατανόηση της ύλης. Οι διευκρινίσεις και οι αποδείξεις είναι λεπτομερείς και συνοδεύονται από ένα πλήθος παραδειγμάτων.

Η Θεωρία Αριθμών πάντως έχει μια εσωτερική ομορφιά που ξεπερνά και την πιο λαμπρή εικόνα που θα μπορούσε να περιέχει το κείμενο.

Ανέστης Α. Φυραφίδης

Ιωάννινα Μάιος του 1998.

ΚΕΦΑΛΑΙΟ Ι

ΘΕΜΕΛΙΩΔΕΙΣ ΕΝΝΟΙΕΣ και ΘΕΩΡΗΜΑΤΑ

1. Ακέραιοι

Σκοπός μας δεν είναι εδώ να παρουσιάσουμε μία αξιωματική θεμελίωση των ακεραίων αριθμών. Θεωρούμε ότι ο αναγνώστης γνωρίζει με ακρίβεια το σύνολο

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

των **ακεραίων**, το σύνολο

$$\mathbb{N} = \{1, 2, \ldots\}$$

των **φυσικών** αριθμών και τις στοιχειώδεις ιδιότητες της πρόσθεσης, του πολλαπλασιασμού και της διάταξης.

Ιδιαίτερα, για κάθε $a, b, c \in \mathbb{Z}$:

(1) $(a+b)+c = a+(b+c)$ και $(ab)c = a(bc)$ (Προσεταιριστικοί νόμοι)

(2) $a+b = b+a$ και $ab = ba$ (Αντιμεταθετικοί νόμοι)

(3) $a(b+c) = ab+ac$ και $(a+b)c = ac+bc$ (Επιμεριστικοί νόμοι)

(4) $a+0 = a$ και $a1 = a$ (Ουδέτερα στοιχεία)

(5) Για κάθε $a \in \mathbb{Z}$ υπάρχει ο $-a \in \mathbb{Z}$ έτσι ώστε

$$a + (-a) = 0$$ (Προσθετικό αντίστροφο)

(Γράφουμε $a-b$ για το $a+(-b)$)

(6) $ab = 0 \iff a = 0$ ή $b = 0$

(7) $a < b \longrightarrow a+c < b+c$ για κάθε $c \in \mathbb{Z}$

(8) $a < b \longrightarrow ad < bd$ για κάθε $d \in \mathbb{N}$.

Γράφουμε $a<b$ ή ισοδύναμα $b>a$ και

$$a \leq b \quad \text{αν} \quad a<b \ \text{ή} \ a=b.$$

Η απόλυτη τιμή $|a|$ για κάθε $a \in \mathbb{Z}$ ορίζεται ως εξής:

$$|a| = \begin{cases} a & \text{αν } a \geq 0 \\ -a & \text{αν } a<0 \end{cases}.$$

Αλγεβρικά, το σύνολο $\mathbb{Z}$ των ακεραίων, εφοδιασμένο με τις πράξεις πρόσθεσης και πολλαπλασιασμού, αποτελεί ένα πεδίο ακεραιότητας το σώμα κλασμάτων του οποίου είναι το σώμα $\mathbb{Q}$ των ρητών αριθμών. Έτσι κάθε ρητός αριθμός είναι της μορφής $\frac{a}{b}$, όπου $a, b \in \mathbb{Z}$ και $b \neq 0$.

Το σύνολο των μη-αρνητικών ακεραίων θα το παριστάνουμε

$$\mathbb{N}_0 = \{0, 1, 2, \ldots\}$$

και στο εξής θα χρησιμοποιούμε τους συμβολισμούς $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{N}_0$, χωρίς να επαναλαμβάνουμε κάθε φορά τη σημασία τους.

Τέλος, υποθέτουμε σαν βασικό αξίωμα την

<u>Αρχή της καλής διάταξης</u>: Κάθε μη κενό υποσύνολο S του $\mathbb{N}_0$ έχει ελάχιστο στοιχείο, δηλ υπάρχει $b \in S$ τέτοιο ώστε $b \leq c$, $\forall c \in S$.

2. <u>Μαθηματική επαγωγή</u>.

Χρησιμοποιώντας την Αρχή της καλής διάταξης είναι εύκολο να πάρουμε την Αρχή της Μαθηματικής επαγωγής ή Αρχή της Πεπερασμένης επαγωγής. Αυτή αποτελεί την βάση για μια αποδεικτική μέθοδο στα Μα-

θεώρημα που καλείται "Μαθηματική επαγωγή".

Θεώρημα 2.1 (Αρχή Μαθηματικής Επαγωγής)

Έστω S ένα υποσύνολο του συνόλου $\mathbb{N}$ των φυσικών αριθμών τέτοιο ώστε $1 \in S$ και

i) Για κάθε φυσικό $n \in S \Rightarrow n+1 \in S$

ή

ii) Για κάθε φυσικό $n > 1$ τέτοιο ώστε $m \in S$ για κάθε m με $1 \leq m < n \Rightarrow n \in S$,

τότε $S = \mathbb{N}$.

Απόδειξη.

Υποθέτουμε ότι $\mathbb{N} - S \neq \phi$. Σύμφωνα με την αρχή της καλής διάταξης το σύνολο $\mathbb{N} - S$ έχει ελάχιστο στοιχείο, ας είναι αυτό το l. Αφού $1 \in S$ το $l > 1$.

i) Είναι $1 \leq l-1 < l$ οπότε $l-1 \in S$, αφού το l είναι το ελάχιστο στοιχείο του $\mathbb{N} - S$. Από την υπόθεσή μας όμως παίρνουμε

$$(l-1)+1 = l \in S$$

άτοπο, αφού το $l \notin S$. Έτσι $\mathbb{N} - S = \phi$ δηλ. $S = \mathbb{N}$.

ii) Αφού το l είναι το ελάχιστο στοιχείο του $\mathbb{N} - S$ θα έχουμε $1, 2, \ldots, l-1 \in S$. Από την υποθεσή μας τώρα παίρνουμε ότι $l \in S$, άτοπο αφού $l \notin S$. Έτσι $\mathbb{N} - S = \phi$, δηλ. $S = \mathbb{N}$. ∎

Η Αρχή της Μαθηματικής Επαγωγής χρησιμοποιείται για να αποδειχθούμε προτάσεις που εξαρτώνται από φυσικό αριθμό n. Πιο συγκεκριμένα:

Θεώρημα 2.2

Έστω $P(n)$ μια πρόταση που εξαρτιέται από το φυσικό αριθμό n, τέτοια ώστε η $P(1)$ να είναι αληθής και

i) Για κάθε φυσικό η με $P(\eta)$ αληθή $\Rightarrow$ $P(\eta+1)$ αληθής

ή

ii) Για κάθε φυσικό $\eta>1$ τέτοιο ώστε η $P(m)$ αληθής για κάθε m με $1\leq m<\eta \Rightarrow P(\eta)$ αληθής,

τότε η $P(\eta)$ είναι αληθής για κάθε $\eta\in\mathbb{N}$.

Απόδειξη.

Αν $S=\{\eta\in\mathbb{N} / P(\eta) \text{ αληθής}\}$, τότε, από το θεώρημα 2.1, συμπεραίνουμε εύκολα ότι $S=\mathbb{N}$ και για το i) και για το ii). ■

Στο εξής, σε αποδείξεις προτάσεων με μαθηματική επαγωγή, θα χρησιμοποιούμε το σύνολο S των φυσικών αριθμών για τους οποίους αληθεύουν.

Παράδειγμα 2.1

Θα δείξουμε ότι

$$1+2+\cdots+\eta=\frac{\eta(\eta+1)}{2}\ ,\ \forall \eta\in\mathbb{N}.$$

Θεωρούμε την πρόταση $P(\eta)$: $1+2+\cdots+\eta=\frac{\eta(\eta+1)}{2}$

Η $P(1)$ αληθεύει, αφού $1=\frac{1(1+1)}{2}$.

Υποθέτουμε ότι η $P(\eta)$ αληθεύει. Θα δείξουμε ότι και η $P(\eta+1)$ αληθεύει δηλ ότι

$$1+2+\cdots+\eta+(\eta+1)=\frac{(\eta+1)(\eta+2)}{2}$$

Πραγματικά,

$$1+2+\cdots+\eta+(\eta+1)=\frac{\eta(\eta+1)}{2}+(\eta+1)=\frac{(\eta+1)(\eta+2)}{2}$$

Η $P(\eta)$ λοιπόν αληθεύει για κάθε $\eta\in\mathbb{N}$.

Όμοια εργαζόμενοι επαγωγικά, μπορούμε να δείξουμε ότι:

α) $1+3+5+\cdots+(2n-1)=n^2$, $\forall n\in\mathbb{N}$

β) $1\cdot2+2\cdot3+3\cdot4+\cdots+n(n+1)=\frac{n(n+1)(n+2)}{3}$, $\forall n\in\mathbb{N}$.

Η μορφή της μαθηματικής επαγωγής που διατυπώσαμε αρχίζει με $n=1$. Η μορφή αυτή μπορεί να γενικευτεί με τρόπο ώστε να αρχίζουμε την επαγωγή με $n=n_0>1$. Πραγματικά,

Θεώρημα 2.3

Έστω $n_0\in\mathbb{N}$ $(n_0>1)$ και $P(n)$ μια πρόταση που εξαρτιέται από τον φυσικό αριθμό $n\geq n_0$. Αν

i) Η $P(n_0)$ είναι αληθής και

ii) Για κάθε φυσικό $n>n_0$ τέτοιο ώστε η $P(n)$ αληθής $\Rightarrow P(n+1)$ αληθής.

τότε η $P(n)$ είναι αληθής, $\forall n\geq n_0$.

Απόδειξη.

Ας είναι $M=\{n\in\mathbb{N} / n>n_0$ και $P(n)$ ψευδής$\}$.

Υποθέτουμε ότι $M\neq\emptyset$. Το M σύμφωνα με την αρχή της καλής διάταξης θα έχει ελάχιστο στοιχείο (>1) και ας είναι αυτό το $l+1$. Έτσι το $l+1>n_0$, οπότε $l\geq n_0$. επιπλέον το $l<l+1$, που, σε συνδυασμό με το ότι το $l+1$ είναι το ελάχιστο στοιχείο του M, μάς δίνουν ότι η $P(l)$ είναι αληθής. Από το ii) όμως παίρνουμε ότι η $P(l+1)$ είναι αληθής, που σημαίνει ότι $l+1\notin M$, πράγμα άτοπο. Έτσι $M=\emptyset$, δηλ η πρόταση $P(n)$ αληθεύει $\forall n\geq n_0$. ∎

Παράδειγμα 2.2

Αν $0<x<1$ τότε

$$(1-x)^n>1-nx$$ για κάθε φυσικό $n\geq2$.

(Ανισότητα του Bernoulli)

Έστω $P(n)$ η πρόταση: $(1-x)^n > 1-nx$

Η $P(2)$ αληθεύει, γιατί

$$(1-x)^2 = 1-2x+x^2 > 1-2x$$

Υποθέτουμε ότι η $P(n)$ αληθεύει για τον φυσικό αριθμό $n>2$, οπότε

$$(1-x)^n > 1-nx. \qquad (9)$$

Θα δείξουμε ότι και η $P(n+1)$ αληθεύει δηλαδή ότι

$$(1-x)^{n+1} > 1-(n+1)x.$$

Πραγματικά: $x<1 \Rightarrow 1-x>0$, οπότε, πολλ/ντας και τα δυό μέλη της (9) με $1-x$, παίρνουμε

$$(1-x)^{n+1} > (1-nx)(1-x) = 1-(n+1)x+nx^2$$

και, επειδή $nx^2>0$, τελικά έχουμε

$$(1-x)^{n+1} > 1-(n+1)x.$$

Η $P(n)$ τοιπόν αληθεύει για κάθε φυσικό $n \geq 2$. ■

Θεωρούμε την ακολουθία του Fibonacci

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

στην οποία, κάθε στοιχείο μετά το δεύτερο είναι ίσο με το άθροισμα των δύο προηγούμενων στοιχείων του. Αν F_n παριστάνει τον n-στο όρο της ακολουθίας, τότε:

$$F_1 = 1$$
$$F_2 = 1$$
$$F_{n+1} = F_n + F_{n-1} \quad \text{για όλα τα } n \geq 2.$$

<u>Παράδειγμα 2.3</u>

Για την ακολουθία $(F_n)_{n\in\mathbb{N}}$ του Fibonacci ισχύει

$$F_n < 2^n, \text{ για κάθε } n \geq 1.$$

Η ανισότητα αληθεύει για $n=1$ και $n=2$.

Από τον ορισμό τώρα είναι φανερό ότι κάθε F_n $n \geq 3$ είναι μεγαλύτερο από το αμέσως προηγούμενο.

Θα δείξουμε ότι $F_n < 2^n$, για κάθε $n \geq 2$.

Πραγματικά, αν $n > 2$ και $F_n < 2^n$, τότε

$$F_{n+1} = F_n + F_{n-1} < F_n + F_n < 2 \cdot 2^n = 2^{n+1}$$

Έτσι, σύμφωνα με το θεώρημα 2.3, $F_n < 2^n$, για κάθε $n \geq 2$ και τελικά $F_n < 2^n$, για κάθε $n \geq 1$. ■

Θα παρατηρήσουμε εδώ ότι η ισχυρότερη πρόταση

$$F_n < (7/4)^n, \quad \text{για κάθε } n \geq 1$$

είναι όμοια αληθής, αλλά δε μπορεί να αποδειχτεί ακριβώς με τον ίδιο τρόπο, γιατί η προηγούμενη διαδικασία μας δίνει μόνο

$$F_{n+1} < 2F_n < 2(7/4)^n \quad \text{και ατυχώς } 2(7/4)^n > (7/4)^{n+1}.$$

Εδώ η υπόθεση επαγωγής είναι πάρα πολύ ασθενής για να μάς δώσει το επιθυμητό αποτέλεσμα $F_{n+1} < (7/4)^{n+1}$.

Στην περίπτωση αυτή η δυσκόλεια μπορεί να αρθεί, αν χωρίζουμε ότι η ανισότητα αυτή αληθεύει για δυο διαδοχικές τιμές του n, ώστε να αποκαταστήσουμε την αρχή της για την επομένη τιμή.

Έχουμε έτσι την επόμενη μορφή μαθηματικής επαγωγής.

Θεώρημα 2.4

Έστω $n_0 \in \mathbb{N}$ $(n_0 > 1)$ και $P(n)$ μια πρόταση που εξαρτιέται από τον φυσικό $n \geq n_0$. Αν

i) Η $P(n_0)$ είναι αληθής, και

ii) Για κάθε φυσικό $n > n_0$ τέτοιο ώστε η $P(m)$ είναι αληθής για κάθε m με $n_0 \leq m < n \Rightarrow$ η $P(n)$ είναι αληθής,

τότε η $P(n)$ είναι αληθής $\forall\, n \geq n_0$.

Απόδειξη

Έστω $Q(n)$ η πρόταση " Η $P(m)$ είναι αληθής, για κάθε m, $n_0 \leq m \leq n$ ".

Για να δείξουμε ότι η $P(n)$ είναι αληθής για κάθε φυσικό $n \geq n_0$, αρκεί να δείξουμε ότι η $Q(n)$ είναι αληθής για κάθε φυσικό $n \geq n_0$. Αρκεί τοιπόν να δείξουμε (βλέπε θεωρ. 2.3)

a) Η $Q(n_0)$ είναι αληθής και

b) Για κάθε φυσικό $n > n_0$, αν η $Q(n-1)$ είναι αληθής $\Rightarrow$ η $Q(n)$ είναι αληθής.

Η a) είναι η ίδια με την i), επομένως ισχύει.

Για την b) υποθέτουμε ότι η $Q(n-1)$ είναι αληθής, δηλ. ότι η $P(m)$ είναι αληθής για κάθε φυσικό m, $n_0 \leq m \leq n-1$. Από την ii) όμως συμπεραίνουμε ότι η $P(n)$ είναι αληθής. Έτσι η $P(m)$ είναι αληθής για κάθε φυσικό $n_0 \leq m \leq n$, που σημαίνει ότι η $Q(n)$ είναι αληθής, πράγμα που επιδιώκαμε. ■

Παράδειγμα 2.4

Για την ακολουθία $(F_n)_{n \in \mathbb{N}}$ του Fibonacci ισχύει

$$F_n < (7/4)^n \quad \text{για κάθε } n \geq 1.$$

Η ανισότητα ισχύει για $n=1$, και $n=2$.

Για κάθε φυσικό $n > 2$, υποθέτουμε ότι η ανισότητα αληθεύει για όλους τους φυσικούς m, $2 \leq m < n$. Τότε ιδιαίτερα

$$F_{n-1} < (7/4)^{n-1} \quad \text{και} \quad F_{n-2} < (7/4)^{n-2}$$

Έτσι

$$F_n = F_{n-1} + F_{n-2} < (7/4)^{n-1} + (7/4)^{n-2} = (7/4)^{n-2}(7/4 + 1) =$$

$= (7/4)^{n-2}(11/4) < (7/4)^{n-2}(7/4)^2 = (7/4)^n$.

Έτσι, σύμφωνα με την πρόταση 2.3, για κάθε $n \geq 2$, $F_n < (7/4)^n$ και τελικά $F_n < (7/4)^n$ για κάθε φυσικό $n \geq 1$. ∎

Στα επόμενα κεφάλαια θα δώσουμε αποδείξεις προτάσεων με μαθηματική επαγωγή και ιδιαίτερα της μορφής που περιγράφει το θεώρημα 2.4.

3. Διώνυμο του Νεύτωνα.

Η παρακάτω πρόταση είναι πολύ χρήσιμη στους υπολογισμούς μας.

Υπενθυμίζουμε ότι για ακεραίους n, k με $0 \leq k \leq n$ έχουμε

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

(όπου $0! = 1 = 1!$ και $n! = 1 \cdot 2 \cdots (n-1)n$ για κάθε φυσικό $n > 1$) ενώ ο $\binom{n}{k}$ είναι πάντα ένας ακέραιος αριθμός.

Πρόταση 3.1

Αν x, y είναι τυχόντες αριθμοί (πραγματικοί ή μιγαδικοί) τότε, για κάθε φυσικό αριθμό n, έχουμε

$$\boxed{(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{k}x^{n-k}y^k + \cdots + \binom{n}{n}y^n} \quad (*)$$

Απόδειξη

Θα αποδείξουμε την πρόταση επαγωγικά.

Για $n = 1$ η πρόταση ισχύει. Πραγματικά

$$(x+y)^1 = x + y = \binom{1}{0}x + \binom{1}{1}y .$$

Υποθέτουμε ότι η πρόταση ισχύει για τον φυσικό αριθμό n.

Θα έχουμε,

$$(x+y)^{n+1} = (x+y)^n(x+y) = \left\{\binom{n}{0}x^n + \cdots + \binom{n}{k}x^{n-k}y^k + \cdots + \binom{n}{n}y^n\right\}(x+y) =$$

$$= \binom{n}{0}x^{n+1} + \left\{\binom{n}{0}+\binom{n}{1}\right\}x^n y^1 + \cdots + \left\{\binom{n}{k-1}+\binom{n}{k}\right\}x^{(n+1)-k}y^k +$$

$$+ \cdots + \binom{n}{n}y^{n+1}$$

Αλλά $\binom{n}{0} = 1 = \binom{n+1}{0}$, $\binom{n}{n} = 1 = \binom{n+1}{n+1}$

και

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1} \qquad \text{για } k < n.$$

Επομένως

$$(x+y)^{n+1} = \binom{n+1}{0}x^{n+1} + \cdots + \binom{n+1}{k}x^{(n+1)-k}y^k + \cdots + \binom{n+1}{k+1}y^{n+1}$$

Η πρόταση λοιπόν ισχύει και για τον φυσικό $n+1$, ισχύει επομένως για κάθε φυσικό $n \geq 1$. ■

Ο τύπος (*) ονομάζεται <u>διώνυμο του Νεύτωνα</u> ή <u>τύπος του διωνύμου</u>. ■

ΚΕΦΑΛΑΙΟ ΙΙ

ΘΕΩΡΙΑ ΔΙΑΙΡΕΤΟΤΗΤΑΣ ΤΩΝ ΑΚΕΡΑΙΩΝ.

1. Ευκλείδια διαίρεση.

Λήμμα 1.1

Για κάθε ζεύγος ακεραίων a, b με $b \neq 0$ υπάρχει ακέραιος x, έτσι ώστε $a - bx > 0$.

Απόδειξη

Αν $b > 0$, τότε, για τον ακέραιο $x = -(1+|a|)$, παίρνουμε

$$a - bx = a + b(1+|a|) \geqslant a + (1+|a|) \geqslant 1$$

Αν $b < 0$, τότε, για τον ακέραιο $x = (1+|a|)$, έχουμε

$$a - bx = a - b(1+|a|) = a + (-b)(1+|a|) \geqslant a + (1+|a|) \geqslant 1.$$

■

Θεώρημα 1.1 (Ευκλείδια διαίρεση)

Για κάθε ζεύγος ακεραίων a, b με $b \neq 0$ υπάρχει μοναδικό ζεύγος ακεραίων q, r, έτσι ώστε

$$a = bq + r \quad \text{και} \quad 0 \leqslant r < |b| \qquad (1)$$

Απόδειξη.

Αρχικά θα δείξουμε ότι υπάρχει ένα τουλάχιστον τέτοιο ζεύγος ακεραίων q, r. Θεωρούμε το σύνολο

$$S = \{a - bx \,/\, x \in \mathbb{Z},\ a - bx \geqslant 0\}.$$

Από το λήμμα 1 έχουμε $S \neq \phi$. Είναι $S \subseteq \mathbb{N}_0$ σύμφωνα λοιπόν με την αρχή της καλής διάταξης, το S θα έχει ελάχιστο στοιχείο, και αν είναι αυτό το $r = a - bq$.

Ο $r \geq 0$, αφού $r \in S$. Μένει να δείξουμε ότι $r < |b|$.

Παρατηρούμε ότι

i) $r - |b| = a - bq - |b|$.

Αν $b > 0$, τότε $r - |b| = a - bq - b = a - b(q+1)$

Αν $b < 0$, τότε $|b| = -b$ και $r - |b| = a - bq + b = a - b(q-1)$

Ο $r - |b|$ είναι δηλαδή ένας αριθμός της μορφής $a - bx$.

ii) $r - |b| \notin S$, γιατί $r - |b| < r$, αφού $b \neq 0$.

Ο $r - |b|$ είναι αριθμός της μορφής $a - bx$ και δεν ανήκει στο S, θα είναι λοιπόν $r - |b| < 0$ δηλ. $r < |b|$.

Για να δείξουμε ότι το ζεύγος q, r είναι μοναδικό, υποθέτουμε ότι υπάρχει ζεύγος ακεραίων q', r', έτσι ώστε

$$a = bq' + r' \quad \text{και} \quad 0 \leq r' < |b|. \qquad (2)$$

Από τις (1) και (2) παίρνουμε

$$r' - r = bq - bq' = b(q - q') \Rightarrow |r' - r| = |b||q - q'|$$

Από τις ανισότητες τώρα $-|b| < -r \leq 0$ και $0 \leq r' < |b|$ παίρνουμε

$$-|b| < r' - r < |b| \quad \text{ή} \quad |r' - r| < |b|$$

επομένως

$$|b||q - q'| < |b| \quad \text{δηλ.} \quad |q - q'| < 1.$$

Επειδή $0 \leq |q - q'| < 1$, θα είναι υποχρεωτικά $|q - q'| = 0$, δηλ. $q = q'$. τότε όμως $r = a - bq = a - bq' = r'$, πράγμα που επιδιώκαμε. ■

Η σχέση (1) καλείται ταυτότητα διαίρεσης του a διά του b. Ο μη-αρνητικός ακέραιος r ονομάζεται υπόλοιπο της διαίρεσης του a δια του b και ο ακέραιος q πηλίκο της διαίρεσης αυτής.

Για παράδειγμα, αν $b=-9$, τότε, ενλέγοντας τον $a=1, 23, -29, -87$. παίρνουμε

$$1=(-9)0+1$$
$$23=(-9)(-2)+5$$
$$-29=(-9)4+7$$
$$-87=(-9)10+3.$$

Εξαιρετικό ενδιαφέρον παρουσιάζει η διαίρεση ενός ακέραιου a δια του 2. στην περίπτωση αυτή θα έχουμε

$$a=2q+r \qquad 0\le r<2.$$

Έτσι τα δυνατά υπόλοιπα είναι $r=0$ και $r=1$.

Όταν $r=0$, ο ακέραιος a έχει τη μορφή

$$a=2q \quad , \quad q\in\mathbb{Z}$$

και λέγεται **άρτιος**.

Όταν ο $r=1$, ο ακέραιος a έχει την μορφή

$$a=2q+1 \quad , q\in\mathbb{Z}.$$

και καλείται **περιττός**

Είναι εύκολο να δούμε ότι για το λογισμό με άρτιους και περιττούς ακέραιους ισχύουν:

i) άρτιος ± άρτιο = άρτιος
ii) περιττός ± περιττό = άρτιος
iii) άρτιος ± περιττό = περιττος
iv) άρτιος · άρτιο = άρτιος
v) άρτιος · περιττό = άρτιος
vi) περιττός · περιττό = περιττός

Γενικά τώρα, αν $m\in\mathbb{N}$, τότε κάθε ακέραιος a έχει μια από τις παρακάτω μορφές

$$a=mq \;,\; a=mq+1, \;\dots,\; a=mq+(m-1)$$

Η ανταγωγή στα υπόλοιπα, όπως θα δούμε και στο παρακάτω παράδειγμα, είναι πολύ χρήσιμη στην πράξη.

Παράδειγμα 1.1

Το τετράγωνο κάθε περιττού ακέραιου είναι της μορφής

$$8k+1.$$

Πραγματικά, κάθε ακέραιος διαιρούμενος με τον 4 θα έχει μια από τις επόμενες μορφές

$$4q,\quad 4q+1,\quad 4q+2,\quad 4q+3$$

Ένας περιττός ακέραιος επομένως, θα είναι της μορφής

$$4q+1 \quad \text{ή} \quad 4q+3.$$

Αφού $(4q+1)^2 = 8(2q^2+q)+1 = 8k+1$

και όμοια

$$(4q+3)^2 = 8(2q^2+3q+1)+1 = 8k+1$$

πράγμα που επιδιωκόσαμε.

2. Διαιρετότητα

Ορισμός.

Θα λέμε ότι ο ακέραιος αριθμός a **διαιρεί** τον ακέραιο αριθμό b και θα το συμβολίζουμε $a|b$, αν υπάρχει ακέραιος αριθμός c έτσι ώστε

$$b = ac.$$

Θα γράφουμε $a \nmid b$ για να δηλώνουμε ότι ο ακέραιος a **δεν** διαιρεί τον b.

Για να εκφράσουμε τη σχέση διαιρετότητας $a|b$ πολλές φορές χρησιμοποιούμε και τις ισοδύναμες εκφράσεις "ο b διαιρείται από τον a" ή "ο b είναι ένα πολλαπλάσιο του a".

Για παράδειγμα, ο 4 διαιρεί τον -20, αφού $(-20) = 4(-5)$

ενώ ο 15 δε διαιρεί τον 10, αφού δεν υπάρχει ακέραιος c έτσι ώστε $10 = 15c$.

Οι παρακάτω ιδιότητες της διαιρετότητας είναι άμεσες συνέπειες του ορισμού.

i) $a|0$ για κάθε $a \in \mathbb{Z}$

ii) Αν $0|b$ τότε $b=0$

iii) $a|b \leftrightarrow -a|b \Leftrightarrow a|-b \leftrightarrow -a|-b \Leftrightarrow |a||b|$.

Απ' αυτές συμπεραίνουμε ότι είναι δυνατό, σε ότι αφορά τη διαιρετότητα ακεραίων, να περιοριστούμε στους φυσικούς αριθμούς και στους φυσικούς διαιρέτες τους.

Στην πρόταση που ακολουθεί δίνονται ορισμένες επιπλέον ιδιότητες της διαιρετότητας.

Πρόταση 2.1

Η διαιρετότητα έχει τις επόμενες ιδιότητες:

1) $a|a \quad \forall a \in \mathbb{Z}$

2) Αν $a|b$ και $b|c$ τότε $a|c$

3) Αν $a|b$ και $a|c$ τότε $a|bx+cy$, για κάθε $x,y \in \mathbb{Z}$.

4) Αν $a|b$ και $c|d$ τότε $ac|bd$

5) Αν $a|b$ τότε $ax|bx$, για κάθε $x \in \mathbb{Z}$

6) Αν $a|b$ και $b \neq 0$ τότε $|a| \leq |b|$

7) Αν $a|b$ και $b|a$ τότε $|a| = |b|$

Απόδειξη.

Θα αποδείξουμε μόνο την 3) · οι υπόλοιπες αφήνονται σαν άσκηση.

$$\left.\begin{array}{l} a|b \Leftrightarrow b = ak_1 \rightarrow bx = ak_1 x \\ a|c \Leftrightarrow c = ak_2 \rightarrow by = ak_2 y \end{array}\right\} \Rightarrow$$

$bx+cy = a(k_1x+k_2)y \iff a \mid bx+cy$. ∎

Παράδειγμα 2.1

Αν οι a, b είναι περιττοί ακέραιοι, τότε $8 \mid a^2-b^2$.

Πραγματικά, για τους a, b θα έχουμε

$$a^2 = 8k+1 \quad \text{και} \quad b^2 = 8k'+1,$$

σύμφωνα με το παράδειγμα 1.1. Έτσι

$$a^2-b^2 = (8k+1)-(8k'+1) = 8(k-k') \longrightarrow 8 \mid a^2-b^2.$$

Παράδειγμα 2.2

$$4 \nmid (n^2+2) \quad \text{για κάθε } n \in \mathbb{Z}.$$

Ας υποθέσουμε ότι υπάρχει $n \in \mathbb{Z}$ έτσι ώστε $4 \mid (n^2+2)$.

i) Αν ο n είναι άρτιος, τότε $n = 2k$, συνεπώς

$n^2+2 = 4k^2+2 = 2(2k^2+1)$. Επειδή $4 \mid 2(2k^2+1)$ θα έχουμε $2 \mid (2k^2+1)$ άτοπο, αφού ο $2k^2+1$ είναι περιττός.

ii) Αν ο n είναι περιττός, τότε $n = 2k+1$, επομένως

$n^2+2 = 4(k^2+k+1)-1$. Έτσι $4 \mid 4(k^2+k+1)-1 \Rightarrow$ $4 \mid 1$ άτοπο.

Επομένως, $4 \nmid (n^2+2)$ για κάθε $n \in \mathbb{Z}$.

3. Πρώτοι αριθμοί.

Ορισμός

Ένας φυσικός αριθμός $p > 1$ καλείται πρώτος αριθμός, αν οι μοναδικοί φυσικοί διαιρέτες του είναι ο 1 και ο p.

Συνήθως τους πρώτους αριθμούς τους παριστάνουμε με τα γράμματα p, q, εφοδιασμένα αν χρειάζεται με τόνους και δείκτες, εκτός αν αναφέρουμε και διαφορετικά.

Τους διαιρέτες ενός ακέραιου α που είναι πρώτοι αριθμοί θα τους λέμε <u>πρώτους διαιρέτες του α</u>.

Κάθε φυσικός αριθμός που δεν είναι πρώτος λέγεται <u>σύνθετος</u>. Αν λοιπόν ο φυσικός α είναι σύνθετος τότε $\alpha > 1$ και θα υπάρχει ανάλυση

$$\alpha = bb' \quad \text{με} \quad 1 < b < \alpha \quad \text{και} \quad 1 < b' < \alpha .$$

Έτσι οι φυσικοί $4, 10, 15, 20$ είναι σύνθετοι, ενώ οι $2, 3, 5, 7, 11, 13$ είναι πρώτοι.

<u>Θεώρημα 3.1</u>

Κάθε φυσικός αριθμός $\alpha > 1$ έχει ένα τουλάχιστον πρώτο διαιρέτη

Απόδειξη.

Θεωρούμε το σύνολο $S = \{ m / \, m \in \mathbb{N}, \, m | \alpha \text{ και } m > 1 \}$.

Το $S \neq \emptyset$ αφού $\alpha \in S$. Θα έχει επομένως ελάχιστο στοιχείο και ας είναι αυτό το p. Θα δείξουμε ότι ο p είναι πρώτος.

Ο $p > 1$ και ας υποθέσουμε ότι είναι σύνθετος, δηλ.

$$p = rs \quad , \quad 1 < r < p \quad \text{και} \quad 1 < s < p.$$

Έχουμε $r | p$ και $p | \alpha$, επομένως $r | \alpha$ με $1 < r < p$, πράγμα άτοπο από την εκλογή του p. Ο p είναι λοιπόν πρώτος αριθμός. ∎

Θεώρημα 3.2 (Ευκλείδη)

Το πλήθος των πρώτων αριθμών είναι άπειρο.

Απόδειξη

Υποθέτουμε ότι το πλήθος των πρώτων αριθμών είναι πεπερασμένο και ας είναι $p_1, \dots, p_\nu$ όλοι οι πρώτοι αριθμοί.

Θεωρούμε τον φυσικό αριθμό

$$a = p_1 \cdot p_2 \cdots p_\nu + 1$$

Σύμφωνα με το θεώρημα 3.1 ο a θα έχει ένα πρώτο διαιρέτη p. Ο $p = p_\kappa$ για κάποιο κ, $1 \le \kappa \le \nu$.

Είναι

$$p \mid a \quad \text{και} \quad p \mid p_1 \cdots p_\nu$$

επομένως

$$p \mid a - p_1 \cdots p_\nu \quad \text{δηλ} \quad p \mid 1, \text{ οπότε } p = 1 \text{ άτοπο.}$$

Το πλήθος λοιπόν των πρώτων αριθμών είναι άπειρο. ∎

Πρόταση 3.1

Αν p_η παριστάνει τον η-στο πρώτο αριθμό στη φυσική τους διάταξη, τότε

$$p_\eta \le 2^{2^{\eta-1}}$$

Απόδειξη

Θα εργαστούμε επαγωγικά. Για $\eta = 1$ η πρόταση αληθεύει, αφού $p_1 = 2$ και $2 \le 2^{2^0} = 2$.

Για κάθε φυσικό $\eta > 1$ υποθέτουμε ότι η πρόταση αληθεύει για κάθε m, $1 \le m < \eta$. Θα δείξουμε ότι ισχύει και για το φυσικό η.

Αρχικά θα δείξουμε ότι $p_\eta \le p_1 p_2 \cdots p_{\eta-1} + 1$.

Θεωρούμε το φυσικό αριθμό $a = p_1 \cdots p_{\eta-1} + 1$ και έστω p ένας πρώτος διαιρέτης του, δηλ $p \mid a$. Ο p είναι διά-

φορος από τους $p_1, \dots, p_{n-1}$ γιατί διαφορετικά $p|1$.

Αν ο $p=p_k$ (p_k ο κ-στος πρώτος αριθμός) τότε $k>n-1$ οπότε $k \geq n$. Έτσι $p_n \leq p_k$ και επειδή $p_k|\alpha$ θα έχουμε $p_k \leq \alpha$. Τελικά

$$p_n \leq p_k \leq p_1 \cdots p_{n-1} + 1 .$$

Από την υπόθεση επαγωγής παίρνουμε τώρα.

$$p_n \leq p_1 \cdots p_{n-1} + 1 \leq 2 \cdot 2^2 \cdots 2^{2^{n-2}} + 1 =$$

$$= 2^{1+2+\cdots+2^{n-2}} + 1 .$$

Υπενθυμίζουμε ότι

$$1+2+\cdots+2^{n-2} = 2^{n-1} - 1$$

οπότε

$$p_n \leq 2^{2^{n-1}-1} + 1 .$$

Αλλά $1 \leq 2^{2^{n-1}-1}$ για κάθε $n \in \mathbb{N}$, επομένως

$$p_n \leq 2^{2^{n-1}-1} + 2^{2^{n-1}-1} = 2 \cdot 2^{2^{n-1}-1} = 2^{2^{n-1}}$$

πράγμα που επιδιώκαμε. ∎

Πρόταση 3.2

Για κάθε φυσικό αριθμό n, οι n σε πλήθος διαδοχικοί φυσικοί αριθμοί

$$(n+1)!+2 , (n+1)!+3 , \dots , (n+1)!+(n+1) \quad (3)$$

είναι σύνθετοι αριθμοί.

Απόδειξη

Παρατηρούμε ότι για κάθε $k=2,3,\dots,(n+1)$ έχουμε

i) $1 < k < (n+1)! + k$

ii) $k \mid (n+1)! + k$

Οι σχέσεις i) και ii) μας βεβαιώνουν ότι οι φυσικοί αριθμοί της λίστας (3) είναι σύνθετοι αριθμοί.

Παρατήρηση.

Η παραπάνω πρόταση μάς βεβαιώνει ότι υπάρχουν διαστήματα διαδοχικών φυσικών αριθμών όσο θέλουμε μεγάλα, που δεν περιέχουν πρώτους αριθμούς. Απ' την άλλη μεριά, υπάρχουν ζεύγη πρώτων αριθμών της μορφής $(p, p+2)$ π.χ $(11, 11+2)$. Τα παραπάνω φανερώνουν ότι η κατανομή των πρώτων στους φυσικούς αριθμούς είναι πολύ ανώμαλη.

Η συνάρτηση $\pi : \mathbb{R}^+ \longrightarrow \mathbb{N}$, $x \longmapsto \pi(x)$

($\mathbb{R}^+$ παριστάνει τους θετικούς πραγματικούς αριθμούς και $\pi(x)$ το πλήθος των πρώτων αριθμών $\leq x$)

παίζει βασικό ρόλο στη μελέτη της κατανομής των πρώτων αριθμών. Το 1896 οι Μαθηματικοί J. Hadamard και De Vallee Poussin χρησιμοποιώντας μέσα της μιγαδικής ανάλυσης απέδειξαν ότι:

$$\lim_{x \to \infty} \pi(x) \frac{\log x}{x} = 1$$

δηλ. αν ο x είναι μεγάλος, τότε ο $\pi(x)$ είναι κατά προσέγγιση $\frac{x}{\log x}$.

Αυτό είναι γνωστό σαν <u>θεώρημα των πρώτων αριθμών</u> που το 1948 οι Μαθηματικοί P. Erdös και A. Selberg απέδειξαν στοιχειωδώς, χωρίς δηλ. τα μέσα της μιγαδικής ανάλυσης.

Θεώρημα 3.3

Κάθε σύνθετος φυσικός αριθμός $a>1$ έχει ένα τουλάχιστον πρώτο διαιρέτη $p \leq \sqrt{a}$.

Απόδειξη.

Ο a σαν σύνθετος γράφεται

$$a = bc \quad \text{όπου} \quad 1<b<a \quad \text{και} \quad 1<c<a.$$

Υποθέτουμε ότι $c \leq b$, έτσι $c^2 \leq bc = a$ και επομένως $c \leq \sqrt{a}$. Αφού ο $c>1$, θα έχει ένα πρώτο διαιρέτη p. Έτσι $p \leq c \leq \sqrt{a}$ και, επειδή $p|c$ και $c|a$, παίρνουμε $p|a$. ■

Πόρισμα. 3.1

Αν έναs φυσικος αριθμός $a>1$ δε διαιρείται από κανένα πρώτο αριθμο $p \leq \sqrt{a}$, τότε ο a είναι πρώτος αριθμός.

Το παραπάνω θεώρημα και το πόρισμα που ακολουθεί είναι πολύ βασικά για την πράξη, αφού μας δίνουν οικονομικότερο τρόπο για να διαπιστώσουμε αν έναs φυσικός αριθμός $a>1$ είναι πρώτος ή σύνθετος αριθμός.

Έτσι, έχουμε το επόμενο κριτήριο.

> Δοθέντος φυσικού αριθμού $a>1$, έχουμε.
>
> A) Αν ο a <u>δε</u> διαιρείται από κανένα πρώτο αριθμό $p \leq \sqrt{a}$, τότε ο a είναι πρώτος αριθμός
>
> B) Αν ο a διαιρείται από ένα τουλάχιστο πρώτο αριθμό $p \leq \sqrt{a}$ τότε ο a είναι σύνθετος αριθμός.

Για να ξεκαθαρίσουμε περισσότερο τα πράγματα ας πάρουμε τους φυσικούς αριθμούς $a = 643$ και $b = 583$

1) $25 < \sqrt{643} < 26$, χρειαζόμαστε μόνο τους πρώτους που είναι ≤ 25, δηλ. τους

$$2, 3, 5, 7, 11, 13, 17, 19, 23.$$

Διαιρώντας τον 643 με καθένα από αυτούς, βρίσκουμε ότι κανένας από αυτούς δεν τον διαιρεί. Ο 643 είναι λοιπόν πρώτος αριθμός.

2) Αφού $24 < \sqrt{583} < 25$, χρειαζόμαστε μόνο τους πρώτους που είναι ≤ 24, δηλ. τούς

$$2, 3, 5, 7, 11, 13, 17, 19, 23.$$

Διαιρώντας τον 583 βρίσκουμε ότι ο 11 είναι διαιρέτης του, αφού $583 = 11 \cdot 53$. Ο 583 είναι λοιπόν σύνθετος. ■

4. Κόσκινο του Ερατοσθένη

Είδαμε ότι αν ένας ακέραιος $a > 1$ δε διαιρείται από κανένα πρώτο αριθμό $p \leq \sqrt{a}$, τότε ο a είναι πρώτος αριθμός.

Ο Ερατοσθένης χρησιμοποίησε το αποτέλεσμα αυτό σαν βάση για μια <u>απλή μέθοδο</u> που καλείται "<u>Κόσκινο του Ερατοσθένη</u>" για την εύρεση όλων των πρώτων p που είναι μικρότεροι ή ίσοι με ένα δοθέντα ακέραιο $a > 1$.

<u>Γενικά η μέθοδος αυτή περιγράφεται ως εξής:</u>

Γράφουμε τούς αριθμούς

$$2, 3, \ldots a \qquad (*)$$

στη φυσική τους σειρά και απορρίπτουμε από αυτούς όλους τους σύνθετους διαγράφοντας τα γνήσια πολλάπλα

$$2p, 3p, \ldots$$

όλων των πρώτων $p \leq \sqrt{a}$.

Από την παραπάνω διαγραφή, οι φυσικοί που απομένουν στη λίστα (*) (δηλ. αυτοί που δεν διαπερνούν το κόσκινο) είναι πρώτοι αριθμοί.

Πιο αναλυτικά:

Γνωρίζουμε ότι ο 2 είναι πρώτος αριθμός. Αρχίζουμε διαγράφοντας από την λίστα (*) όλα τα πολλαπλάσια του 2 εκτός από τον 2. Ο 1ος από τους απομένοντες φυσικούς είναι ο 3, που είναι πρώτος αριθμός. Κρατάμε τον 3 και διαγράφουμε όλα τα μεγαλύτερα πολλαπλάσιά του, δηλ. τους 9, 15, 21, ... (Τα άρτια πολλαπλάσια του 3 έχουν διαγραφεί κατά το προηγούμενο βήμα).

Ο μεγαλύτερος ακέραιος μετά τον 3, που δεν έχει ακόμη διαγραφτεί, είναι ο 5. Αυτός δε διαιρείται από τον 2 ούτε από τον 3 (διαφορετικά θα είχε διαγραφτεί), επομένως είναι πρώτος αριθμός. Διαγράφουμε όλα τα πολλαπλάσια του 5 εκτός από τον ίδιο τον 5.

Συνεχίζοντας την πορεία αυτή αποκτούμε όλο και περισσότερους διαφορετικούς πρώτους αριθμούς.

Παρατηρούμε ότι, αν έχουμε διαγράψει με τη μέθοδο αυτή όλους τους φυσικούς πού είναι πολλαπλάσια πρώτων αριθμών μικρότερων του πρώτου p, τότε όλοι οι ακέραιοι που δεν έχουν διαγραφτεί και είναι μικρότεροι του p^2, είναι πρώτοι αριθμοί.

Πραγματικά, κάθε σύνθετος φυσικός $m < p^2$ $(\sqrt{m} < p)$ έχει διαγραφτεί από την λίστα (*), αφού είναι πολλαπλάσιο του ελάχιστου πρώτου διαιρέτη q του m, πον είναι $q \leq \sqrt{m} < p$.

Έτσι

i) Διαγράφοντας τα πολλαπλάσια ενός πρώτου p, αρχίζουμε από τον p^2.

ii) Ο πίνακας των πρώτων των $\leq a$ συμπληρώνεται, αφού

διαγράφουμε όλα τα πολλαπλάσια

$2p, 3p, \ldots$

για όλους τους πρώτους $p \leq \sqrt{a}$. ■

Για να δούμε πώς δουλεύει η μέθοδος αυτή, θα βρούμε όλους τους πρώτους αριθμούς που είναι ≤ 100.

Ο πίνακας των πρώτων εδώ ευμενηρόνεται αφού διαγράφουμε όλα τα γνήσια πολλαπλάσια των πρώτων

$2, 3, 5$ και 7

που είναι $\leq \sqrt{100} = 10$.

Διαγράφουμε τα γνήσια πολλαπλάσια του 2 με το σύμβολο "\", τα γνήσια πολλαπλάσια του 3 με "/", τα γνήσια πολλαπλάσια του 5 με "−", και τα γνήσια πολλαπλάσια του 7 με "v". Παίρνουμε τον παρακάτω πίνακα:

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	34	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	52	53	~~54~~	~~55~~	~~56~~	~~57~~	58	59	~~60~~
~~61~~	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Οι πρώτοι αριθμοί χωρίς που είναι ≤ 100 είναι οι

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53$

$59, 61, 67, 71, 73, 79, 83, 89$ και ο 97.

5. Θεμελιώδες Θεώρημα της Αριθμητικής.

Θεώρημα 5.1

Κάθε φυσικός αριθμός $\alpha > 1$ μπορεί να γραφεί σαν γινόμενο πεπερασμένου πλήθους πρώτων αριθμών, όχι κατ' ανάγκη διαφόρων μεταξύ τους.

Απόδειξη

Θα εργαστούμε επαγωγικά. Το θεώρημα αληθεύει για $\alpha = 2$.

Για κάθε φυσικό $\alpha > 2$, υποθέτουμε ότι, το θεώρημα αληθεύει για όλους τους φυσικούς m με $2 \leq m < \alpha$. Θα δείξουμε ότι αληθεύει και για τον φυσικό α. Αν α είναι πρώτος, το θεώρημα αληθεύει. Αν ο α είναι σύνθετος, θα έχουμε

$$\alpha = rs \quad \text{με} \quad 1 < r < \alpha \quad \text{και} \quad 1 < s < \alpha.$$

και από την υπόθεσή μας, θα υπάρχουν πρώτοι αριθμοί $p_1, \dots, p_\nu, q_1, \dots, q_\mu$, όχι κατ' ανάγκη διάφοροι μεταξύ τους έτσι ώστε

$$r = p_1 \cdots p_\nu \quad \text{και} \quad s = q_1 \cdots q_\mu.$$

Επομένως

$$\alpha = rs = p_1 \cdots p_\nu q_1 \cdots q_\mu . \ \blacksquare$$

Σκοπός μας στη συνέχεια, είναι να δείξουμε ότι μια τέτοια ανάλυση ενός φυσικού $\alpha > 1$ είναι μοναδική αν δε λάβουμε υπόψη μας τη σειρά των πρώτων παραγόντων.

Θεώρημα 5.2

Εάν ο p είναι πρώτος και $p|ab$, τότε $p|a$ ή $p|b$.

Απόδειξη

Το θεώρημα αληθεύει για $a=0$ ή $b=0$. Για να δείξουμε ότι το θεώρημα αληθεύει για μη-μηδενικούς ακεραίους a, b, αρκεί να δείξουμε ότι αυτό αληθεύει για φυσικούς αριθμούς a, b, αφού $p|c \iff p||c|$.

Υποθέτουμε ότι το θεώρημα δεν ισχύει για όλους τους πρώτους και ας είναι p ο μικρότερος πρώτος για τον οποίο υπάρχουν φυσικοί a, b έτσι ώστε:

$$p|ab \ , \ p\nmid a \text{ και } p\nmid b .$$

Θα καταλήξουμε σε άτοπο. Αφού $p\nmid a$ και $p\nmid b$ θα έχουμε:

$$a = pq_1 + r_1 \quad , \quad 0 < r_1 < p$$

$$b = pq_2 + r_2 \quad , \quad 0 < r_2 < p$$

Από τις παραπάνω σχέσεις παίρνουμε

$$r_1 r_2 = ab + p(pq_1q_2 - bq_1 - aq_2)$$

και, επειδή ο $p|ab$, θα έχουμε $p|r_1 r_2$, δηλ

$$r_1 r_2 = pc$$

Από τις ανισότητες $0<r_1<p$ και $0<r_2<p$, παίρνουμε

$$0 < c < p .$$

Αν τώρα q είναι ένας πρώτος αριθμός τέτοιος ώστε $q|c$ τότε $q<p$ και, επειδή $q|r_1 r_2$, θα έχουμε $q|r_1$ ή $q|r_2$.

Επειδή κάθε πρώτος διαιρέτης του c θα διαιρεί και τα δυο μέλη της εξίσωσης $r_1 r_2 = pc$, παίρνουμε τελικά

$$r_1' r_2' = p \ , \text{ όπου } r_1'|r_1 \text{ και } r_2'|r_2 .$$

Από τον ορισμό τώρα του πρώτου αριθμού συμπεραίνουμε ότι ένας από τούς x_1' ή x_2' θα είναι ίσος με 1 και ο άλλος ίσος με p. Ας υποθέσουμε ότι $x_1' = p$ Τότε $p | x_1$ οπότε $p | a$ άτοπο, πράγμα που επιδιώξαμε. ■

Το προηγούμενο θεώρημα επεκτείνεται και σε γινόμενα με περισσότερους από δυο παράγοντες

Πόρισμα 5.1

Αν ο p είναι πρώτος και $p | a_1 a_2 \dots a_n$, τότε ο $p | a_k$ για κάποιο k, $1 \le k \le n$.

Απόδειξη.

Θα εργαστούμε επαγωγικά πάνω στο πλήθος n των παραγόντων του γινόμενου.

Για $n = 1$ δεν έχουμε να δείξουμε τίποτα. Για $n = 2$ επαληθεύεται σύμφωνα με το προηγούμενο θεώρημα.

Για κάθε φυσικό $n > 2$, υποθέτουμε ότι η πρόταση αληθεύει για κάθε m $2 \le m < n$. Έστω

$$p | a_1 \dots a_m .$$

Έχουμε $p | (a_1 \dots a_{n-1}) a_n$, επομένως $p | a_n$ ή $p | a_1 \dots a_{n-1}$, σύμφωνα με την υπόθεση επαγωγής.

Αν $p | a_n$, η απόδειξή μας τελειώνει. Αν όχι, τότε $p | a_1 \dots a_{n-1}$, και από την υπόθεση επαγωγής $p | a_i$, για κάποιο i, $1 \le i \le n-1$.

Σε κάθε περίπτωση, λοιπόν, ο p θα διαιρεί έναν από τους $a_1 \dots a_n$. ■

Πόρισμα 5.2.

Αν $p, p_1, \dots, p_n$ είναι πρώτοι αριθμοί και $p \mid p_1 \cdots p_n$, τότε $p = p_k$, για κάποιο k, $1 \le k \le n$.

Απόδειξη

Από το πόρισμα 5.1 γνωρίζουμε ότι $p \mid p_k$ για κάποιο k, $1 \le k \le n$. Αφού ο p_k είναι πρώτος ο p θα είναι ίσος με 1 ή p_k. Επειδή $p > 1$, θα είναι $p = p_k$. ■

Είμαστε σε θέση τώρα να αποδείξουμε το θεμελιώδες θεώρημα της Αριθμητικής.

Θεώρημα 5.3 (θεμελιώδες θεώρημα της Αριθμητικής)

Η παράσταση ενός ακεραίου $a > 1$ σε γινόμενο πρώτων αριθμών είναι **μοναδική** αν δε λάβουμε υπόψη μας την τάξη των παραγόντων.

Απόδειξη.

Έστω ότι

$$a = p_1 \cdots p_\mu = q_1 \cdots q_\nu$$

με τους p_i, q_j πρώτους αριθμούς τέτοιους ώστε

$$p_1 \le p_2 \le \cdots \le p_\mu \quad \text{και} \quad q_1 \le q_2 \le \cdots \le q_\nu .$$

Θα εργαστούμε επαγωγικά. Για $a = 2$, το θεώρημα αληθεύει, αφού $\mu = \nu = 1$ και $p_1 = q_1 = 2$.

Για κάθε φυσικό $a > 2$ υποθέτουμε ότι το θεώρημα ισχύει για κάθε φυσικό $2 \le m < a$.

Αν ο a είναι πρώτος, τότε $\mu = \nu = 1$ και $p_1 = q_1 = a$, και το θεώρημα αληθεύει.

Αν ο a είναι σύνθετος, τότε $\mu > 1$ και $\nu > 1$.

Επειδή $p_1 \mid q_1 \cdots q_\nu$ και $q_1 \mid p_1 \cdots p_\mu$.

σύμφωνα με το Πόρισμα 5.2, θα είναι

$$p_1 = q_r \ , \ q_1 = p_s \qquad 1 \le r \le \nu \ , \ 1 \le s \le \mu .$$

Αλλά $p_1 \le p_s = q_1 \le q_r = p_1 \Rightarrow p_1 = q_1$

Είναι $1 < p_1 < \alpha$ και $p_1 | \alpha$, επομένως για τον ακέραιο

$$\frac{\alpha}{p_1} = p_2 \cdots p_\mu = q_2 \cdots q_\nu$$

έχουμε $1 < \frac{\alpha}{p_1} < \alpha$ και σύμφωνα με την υπόθεση επαγωγής $\mu - 1 = \nu - 1$, δηλ $\mu = \nu$ και $p_i = q_i$ $i = 2, \ldots, \mu$. Τελικά, $\mu = \nu$ και $p_i = q_i$, για κάθε $i = 1, \ldots, \mu$. ■

Στην ανάλυση του φυσικού αριθμού $\alpha > 1$ σε γινόμενο $\alpha = p_1 \cdot p_2 \cdots p_r$ πρώτων, είναι δυνατόν οι παράγοντες p_i να ταυτίζονται κατά ομάδες. Αν τους παράγοντες που ταυτίζονται, τους συμπτύξουμε, θα βρούμε την επόμενη έκφραση

$$\alpha = p_1^{\alpha_1} \cdots p_\kappa^{\alpha_\kappa} \qquad (*)$$

όπου ο φυσικός $\kappa \ge 1$, $\alpha_i \ge 1$ για κάθε $i \in \{1, \ldots, \kappa\}$ και $p_i \ne p_j$ για $i \ne j$.

Με το νόημα αυτό, την παράσταση (*) θα την καλούμε <u>πρωτογενή ανάλυση του α</u>.

<u>Συμφωνία:</u> Στο εξής, όταν θα γράφουμε $\alpha = p_1^{\alpha_1} \cdots p_\kappa^{\alpha_\kappa}$ χωρίς να αναφέρουμε συνθήκες για τους πρώτους p_i και για τους φυσικούς α_i, θα εννοούμε την πρωτογενή ανάλυση του α.

Υπάρχει ένας πρακτικώς τρόπος για να βρίσκουμε την πρωτογενή ανάλυση ενός φυσικού $a>1$, που στηρίζεται στο κριτήριο που δώσαμε στην παράγραφο 3 για να διαπιστώνουμε αν ένας φυσικός $a>1$ είναι πρώτος ή σύνθετος.

Ας βρούμε για παράδειγμα, την πρωτογενή ανάλυση του φυσικού αριθμού $a=1985$

Επειδή $44 < \sqrt{1985} < 45$, αρκεί να δοκιμάσουμε αν ο 1985 διαιρείται με κάποιο πρώτο $p \leq 44$, δηλ. με κάποιον από τους

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43.

Με δοκιμή, ο 1ος απ' αυτούς που διαιρεί τον 1985, είναι ο 5 και

$$1985 = 5 \cdot 397 \qquad (**)$$

Όσον αφορά τον 397 (σημειώνουμε $19 < \sqrt{397} < 20$.) οι μόνοι πρώτοι αριθμοί οι ≤ 19 είναι οι

2, 3, 5, 7, 11, 13, 17, 19.

Δοκιμάζοντας βλέπουμε ότι κανένας απ' αυτούς δεν τον διαιρεί· ο 397 είναι λοιπόν πρώτος αριθμός.

Έτσι η πρωτογενής ανάλυση του 1985 είναι η (**)

Παρατηρήσεις

1) Ας είναι

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_\nu^{\alpha_\nu} \qquad (1)$$

$$b = (p'_1)^{\beta_1} \cdot (p'_2)^{\beta_2} \cdots (p'_\mu)^{\beta_\mu} \qquad (2)$$

οι πρωτογενείς αναλύσεις των φυσικών αριθμών a και b.

Είναι δυνατόν να επιτύχουμε γραφή των a και b υπό

μορφή γινομένων στα οποία να περιέχονται οι ίδιοι πρώτοι αριθμοί, δηλαδή

$$a = p_1^{\alpha_1} \cdots p_m^{\alpha_m} \qquad (3)$$

$$b = p_1^{\beta_1} \cdots p_m^{\beta_m} \qquad (4)$$

αν θεωρήσουμε ότι οι πρώτοι αριθμοί που περιέχονται στην πρωτογενή ανάλυση (1) του a και δεν περιέχονται στην πρωτογενή ανάλυση (2) του b, τοποθετούνται στην (4) με μηδενισμένους εκθέτες, δηλαδή

$\forall p_i \in \{p_1, \ldots, p_\nu\}$ με $p_i \nmid b$, θα είναι $p_i \in \{p_1, \ldots, p_m\}$ με $\beta_i = 0$, οπότε $p_i^{\beta_i} = 1$.

Αν θεωρήσουμε το αντίστοιχο για το b, καταλήγουμε στις (3) και (4), όπου θέσαμε $m = \max\{\nu, \mu\}$.

2. Γενικότερα, για κάθε φυσικό a, μπορούμε να συμπεριλάβουμε στην πρωτογενή ανάλυσή του όλους τους πρώτους αριθμούς με την προϋπόθεση ότι οι πρώτοι αριθμοί που δεν διαιρούν τον a θα έχουν εκθέτη το μηδέν:

$$a = \prod_{i=1}^{\infty} p_i^{\alpha_i} \quad , \alpha_i \geq 0$$

Οι α_i προσδιορίζονται μονοσήμαντα για κάθε φυσικό a

3. Κάθε ακέραιος $a \neq 0$ μπορεί να γραφτεί κατά μοναδικό τρόπο σε γινόμενο

$$a = \varepsilon a', \text{ όπου } \varepsilon = \pm 1 \text{ και } a' \in \mathbb{N}.$$

Έτσι κάθε ακέραιος $a \neq 0$ μπορεί να γραφτεί κατά μοναδικό τρόπο σε γινόμενο πρώτων παραγόντων ($|a| > 1$),

$$a = \varepsilon p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_\nu^{\alpha_\nu} .$$

Το επόμενο θεώρημα είναι πολύ χρήσιμο στην πράξη, αφού μας δίνει όλους τους φυσικούς διαιρέτες ενός φυσικού $\alpha>1$ με μορφή γινομένου πρώτων αριθμών.

Θεώρημα 5.4.

Έστω $\alpha=p_1^{\alpha_1}\cdots p_\nu^{\alpha_\nu}$ η πρωτογενής ανάλυση ενός φυσικού $\alpha>1$. Ο φυσικός αριθμός d είναι διαιρέτης του α, δηλ $d|\alpha$ τότε και μόνο εάν ο d είναι της μορφής

$$d=p_1^{\beta_1}\cdots p_\nu^{\beta_\nu} \quad \text{με} \quad 0\le\beta_i\le\alpha_i \qquad (5)$$

Απόδειξη.

Αν $d=1$ τότε $d=p_1^0\cdots p_\nu^0$.

Αν $d>1$ και p είναι ένας πρώτος διαιρέτης του, δηλ. $p|d$, τότε $p|d$ και $d|\alpha \rightarrow p|\alpha$

που σημαίνει ότι ο p θα είναι ίσος κάποιος από τους $p_1,\dots,p_\nu$.

Έτσι, η πρωτογενής ανάλυση του d, θα εμπεριέχει τους πρώτους από την πρωτογενή ανάλυση του α, δηλ ο d θα είναι της μορφής $d=p_1^{\beta_1}\cdots p_\nu^{\beta_\nu}$ με $0\le\beta_i$.

Αφού ο $d|\alpha$, θα είναι $\alpha=d\alpha'$ και ο α' επίσης μπορεί να γραφτεί όπως και παραπάνω με τη μορφή $\alpha'=p_1^{\gamma_1}\cdots p_\nu^{\gamma_\nu}$ με $0\le\gamma_i$.

Τελικά θα είναι

$$p_1^{\alpha_1}\cdots p_\nu^{\alpha_\nu}=p_1^{\beta_1}\cdots p_\nu^{\beta_\nu}\cdot p_1^{\gamma_1}\cdots p_\nu^{\gamma_\nu}=p_1^{\beta_1+\gamma_1}\cdots p_\nu^{\beta_\nu+\gamma_\nu}$$

επομένως $\alpha_i=\beta_i+\gamma_i$ και έτσι $\beta_i\le\alpha_i$

Ο d έχει τελικά την μορφή

$$d=p_1^{\beta_1}\cdots p_\nu^{\beta_\nu} \quad \text{με} \quad 0\le\beta_i\le\alpha_i.$$

Αντίστροφα, αν ο d έχει την μορφή (5), τότε

$$a=(p_1^{b_1}\cdots p_v^{b_v})(p_1^{a_1-b_1}\cdots p_v^{a_v-b_v})$$

που σημαίνει ότι ο $d|a$. ■

Παράδειγμα 5.1

Οι φυσικοί διαιρέτες του φυσικού $720=2^4\cdot 3^2\cdot 5$ είναι όλοι οι φυσικοί της μορφής

$2^{b_1}\cdot 3^{b_2}\cdot 5^{b_3}$ όπου $0\le b_1\le 4$, $0\le b_2\le 2$, $0\le b_3\le 1$.

Αν τώρα αφήσουμε τα b_1, b_2, b_3 να διατρέξουν, ανεξάρτητα το ένα από το άλλο τις τιμές

$b_1=0,1,2,3,4$, $b_2=0,1,2$, $b_3=0,1$

παίρνουμε τους φυσικούς διαιρέτες του 720, που είναι οι:

1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144, 5, 10, 20, 40, 80, 15, 30, 60, 120, 240, 45, 90, 180, 360 και 720.

Παρατήρηση.

Αν $\Delta=\{d \,/\, d\in\mathbb{N} \,,\, d|a\}$ και

$$A=\{(b_1,\dots,b_v) \,/\, 0\le b_i\le a_i \quad i=1,\dots,v\}$$

τότε εύκολα διαπιστώνουμε ότι η σχέση (5) ορίζει μια αμφιέση (ένα προς ένα και επί απεικόνιση)

$$f:\Delta\longrightarrow A \quad , \quad d=p_1^{b_1}\cdots p_v^{b_v}\longmapsto(b_1,\dots,b_v)\ .\ \blacksquare$$

Στα επόμενα θα δούμε και άλλα ενδιαφέροντα θέματα σχετικά με πρώτους αριθμούς, που θα ισχυροποιήσουν τη θέση ότι "οι πρώτοι αριθμοί είναι ένα από τα πιο ισχυρά εργαλεία της Θεωρίας Αριθμών".

6. Μέγιστος Κοινός Διαιρέτης (Μ.Κ.Δ)

Ορισμός

Ο ακέραιος αριθμός δ καλείται κοινός διαιρέτης των ακεραίων αριθμών $\alpha_1, \alpha_2, \ldots, \alpha_\nu$ αν

$$\delta|\alpha_1\ ,\ \delta|\alpha_2\ ,\ \ldots\ ,\ \delta|\alpha_\nu\ .$$

Επειδή ο 1 είναι κοινός διαιρέτης των $\alpha_1,\ldots,\alpha_\nu$, το σύνολο των κοινών διαιρετών τους είναι $\neq\phi$.

Αν $\alpha_1=\alpha_2=\cdots=\alpha_\nu=0$, τότε κάθε ακέραιος είναι κοινός διαιρέτης των $\alpha_1,\ldots\alpha_\nu$, αφού κάθε ακέραιος διαιρεί τον 0. Στην περίπτωση αυτή, το σύνολο των **φυσικών** κοινών διαιρετών των $\alpha_1,\alpha_2,\ldots,\alpha_\nu$ είναι άπειρο.

Στην περίπτωση, όμως, που ένας τουλάχιστον των $\alpha_1,\ldots,\alpha_\nu$ είναι διάφορος του μηδενός, π.χ $\alpha_\kappa\neq 0$, τότε το σύνολο D των **φυσικών** κοινών διαιρετών των $\alpha_1,\ldots,\alpha_\nu$ είναι **πεπερασμένο**, αφού τα στοιχεία του θα διαιρούν τον α_κ. Το σύνολο D, λοιπόν, θα έχει **μέγιστο στοιχείο** που το καλούμε **μέγιστο κοινό διαιρέτη** (μ.κ.δ) των $\alpha_1,\alpha_2,\ldots,\alpha_\nu$ και το συμβολίζουμε

$$(\alpha_1,\alpha_2,\ldots,\alpha_\nu)$$

Στο εξής, όταν θα μιλάμε για τον μ.κ.δ ακεραίων αριθμών, θα υποθέτουμε σιωπηρά ότι αυτός υπάρχει, δηλ. ότι ένας τουλάχιστον απ' αυτούς είναι $\neq 0$.

Μπορούμε, λοιπόν, να δώσουμε τον επόμενο ορισμό για τον μ.κ.δ.

Ορισμός.

Έστω $a_1, \ldots, a_n$ δοθέντες ακέραιοι, από τους οποίους ένας τουλάχιστον είναι $\neq 0$. Ο **μέγιστος κοινός διαιρέτης** των $a_1, \ldots, a_n$ είναι ένας φυσικός αριθμός d τέτοιος ώστε

i) $d|a_1$, $d|a_2, \ldots, d|a_n$

ii) Αν $\delta|a_1, \delta|a_2, \ldots, \delta|a_n$, τότε $\delta \leq d$.

Θεώρημα 6.1

Αν $d=(a_1, \ldots, a_n)$ τότε υπάρχουν ακέραιοι $k_1, k_2, \ldots, k_n$ έτσι ώστε να είναι

$$d = a_1k_1 + a_2k_2 + \cdots + a_nk_n .$$

Απόδειξη.

Θεωρούμε το σύνολο $S=\{a_1x_1 + \cdots + a_nx_n \;/\; x_i \in \mathbb{Z}\}$

Οι ακέραιοι $a_1, \ldots, a_n \in S$, αφού για κάθε i , $1 \leq i \leq n$ έχουμε

$$a_i = a_i 0 + \cdots + a_{i-1}\cdot 0 + a_i \cdot 1 + a_{i+1}\cdot 0 + \cdots + a_n 0 .$$

Το S περιέχει και φυσικούς αριθμούς. Πραγματικά, αν $a_k \neq 0$, τότε και το $-a_k \in S$, αφού

$$-a_k = a_1 \cdot 0 + \cdots + a_{k-1}\cdot 0 + a_k(-1) + a_{k+1}\cdot 0 + \cdots + a_n 0 .$$

Αφού είναι d ο ελάχιστος φυσικός που ανήκει στο σύνολο S. Θα υπάρχουν, λοιπόν, ακέραιοι $k_1, \ldots, k_n$ έτσι ώστε

$$d = a_1k_1 + \cdots + a_nk_n \qquad (6)$$

Θα δείξουμε ότι $d=(a_1, \ldots, a_n)$.

Αρχικά θα δείξουμε ότι $d|a_1, d|a_2, \ldots, d|a_n$.

Αν $m \in S$, τότε $m = a_1\xi_1 + \cdots + a_n\xi_n$, $\xi_i \in \mathbb{Z}$, επομένως από την Ευκλείδια διαίρεση παίρνουμε

$$m = dq + r \qquad 0 \leq r < d .$$

Είναι $r = m - dq = a_1(\xi_1 - k_1 q) + \dots + a_n(\xi_n - k_n q)$, δηλ $r \in S$.
Από τον ορισμό τώρα του d, και επειδή $0 \le r < d$, συμπεραίνουμε ότι $r = 0$. Έτσι $m = dq$, δηλ $d|m$ για κάθε $m \in S$, που σημαίνει ότι: $S \subseteq \{dq / q \in \mathbb{Z}\}$. Φανερά όμως $\{dq / q \in \mathbb{Z}\} \subseteq S$, οπότε, $S = \{dq / q \in \mathbb{Z}\}$.

Επειδή $a_1, \dots, a_n \in S$, παίρνουμε ότι $d|a_1, \dots, d|a_n$.
Απομένει να δείξουμε ότι, αν $\delta|a_1, \dots, \delta|a_n$, τότε $\delta \le d$.
Πραγματικά

$$\left.\begin{matrix} \delta|a_1 \\ \vdots \\ \delta|a_n \end{matrix}\right\} \Rightarrow \left.\begin{matrix} \delta|a_1k_1 \\ \vdots \\ \delta|a_nk_n \end{matrix}\right\} \Rightarrow \delta \Big| a_1k_1 + \dots + a_nk_n \quad \text{δηλ } \delta|d$$

και επειδή $d \in \mathbb{N}$, θα είναι $\delta \le d$, πράγμα που επιδιώκαμε. ∎

Παρατήρηση.
Το θεώρημα 6.1 μας εξασφαλίζει την ύπαρξη n-άδας ακεραίων $(k_1, \dots, k_n)$ έτσι ώστε $d = a_1k_1 + \dots + a_nk_n$, όχι όμως και την μοναδικότητά της. Όπως θα δούμε στα επόμενα (στις διοφαντικές εξισώσεις) η n-άδα $(k_1, \dots, k_n)$ δεν είναι μοναδική.

Πόρισμα 6.1

Έστω $a_1, \dots, a_n$ δοθέντες ακέραιοι όχι όλοι ίσοι με μηδέν.
Ο φυσικός αριθμός d είναι ο μ.κ.δ των $a_1, \dots, a_n$ δηλ. $d = (a_1, \dots, a_n)$, αν και μόνο αν:

1) $d|a_1, \dots, d|a_n$

2) Αν $\delta|a_1, \dots, \delta|a_n$ τότε $\delta|d$.

Απόδειξη.
Αν $d = (a_1, \dots, a_n)$ τότε αρκεί να δείξουμε μόνο την 2)
Σύμφωνα με το θεώρημα 6.1, $d = a_1k_1 + \dots + a_nk_n$, $k_i \in \mathbb{Z}$.
Έχουμε

$$\left.\begin{matrix} \delta|a_1 \\ \vdots \\ \delta|a_n \end{matrix}\right\} \Rightarrow \left.\begin{matrix} \delta|a_1k_1 \\ \vdots \\ \delta|a_nk_n \end{matrix}\right\} \Rightarrow \delta|a_1k_1 + \dots + a_nk_n \text{ δηλ. } \delta|d.$$

Για το αντίστροφο παρατηρούμε ότι, αν $\delta|d$ και $d\in\mathbb{N} \Rightarrow \delta\le d$. ■

Πόρισμα 6.2

Αν $a_1,\dots,a_n$ είναι ακέραιοι όχι όλοι ίσοι με μηδέν και υπάρχει φυσικός αριθμός d τέτοιος ώστε

i) Υπάρχουν ακέραιοι $k_1,\dots,k_n$: $d=a_1k_1+\dots+a_nk_n$

ii) $d|a_1,\dots,d|a_n$,

τότε $d=(a_1,\dots,a_n)$

Απόδειξη.

Αρκεί να δείξουμε ότι, αν $\delta|a_1,\dots,\delta|a_n$, τότε $\delta|d$.

Έχουμε

$$\left.\begin{matrix}\delta|a_1\\ \vdots\\ \delta|a_n\end{matrix}\right\}\Rightarrow\left.\begin{matrix}\delta|a_1k_1\\ \vdots\\ \delta|a_nk_n\end{matrix}\right\}\Rightarrow \delta|a_1k_1+\dots+a_nk_n \text{ δηλ } \delta|d. \blacksquare$$

Ορισμός

Οι ακέραιοι αριθμοί $a_1,\dots,a_n$ καλούνται <u>πρώτοι μεταξύ τους</u>, αν

$$(a_1,\dots,a_n)=1.$$

Θα παρατηρήσουμε εδώ, ότι αν δυό τουλάχιστον από τους ακεραίους $a_1,a_2,\dots,a_n$ είναι πρώτοι μεταξύ τους τότε $(a_1,\dots,a_n)=1$, που ισχύει φυσικά, και στην περίπτωση που οι $a_1,\dots,a_n$ είναι <u>πρώτοι μεταξύ τους ανά δύο</u> δηλ. όταν

$(a_i,a_j)=1$ για κάθε $i,j\in\{1,2,\dots,n\}$ με $i\neq j$.

Είναι δυνατό όμως να έχουμε $(a_1,\dots,a_n)=1$ και οι ακέραιοι $a_1,\dots,a_n$ να μην είναι πρώτοι μεταξύ τους ανά δύο, π.χ. $(6,14,21)=1$ ενώ $(6,14)=2$, $(6,21)=3$ και $(14,21)=7$.

Αν, όμως, έστω και δυο από τους $a_1,\dots,a_n$ είναι πρώτοι μεταξύ τους, τότε $(a_1,\dots,a_n)=1$ π.χ αν $(a_1,a_2)=1$, τότε $(a_1,\dots,a_n)=((a_1,a_2),a_3,\dots,a_n)=(1,a_3,\dots,a_n)=1$.

Πόρισμα 6.3

Οι ακέραιοι $a_1,\dots,a_n$ είναι πρώτοι μεταξύ τους, δηλ $(a_1,\dots,a_n)=1$, εάν και μόνο εάν υπάρχουν ακέραιοι $k_1,k_2,\dots,k_n$, τέτοιοι ώστε

$$1=a_1k_1+\dots+a_nk_n$$

Απόδειξη.

Αν $(a_1,\dots,a_n)=1$, τότε, σύμφωνα με το θεώρημα 6.1, υπάρχουν ακέραιοι $k_1,\dots,k_n$, έτσι ώστε $1=a_1k_1+\dots+a_nk_n$.

Αντίστροφα, σύμφωνα με το πόρισμα 6.2, αφού

i) υπάρχουν ακέραιοι $k_1,\dots,k_n$: $1=a_1k_1+\dots+a_nk_n$

ii) $1/a_1,\dots,1/a_n$

συμπεραίνουμε ότι $(a_1,\dots,a_n)=1$. ■

Παράδειγμα 6.1

$$(2k+1,\ 9k+4)=1 \quad \text{για κάθε } k\in\mathbb{Z}$$

Πραγματικά υπάρχουν ακέραιοι οι 9 και -2, έτσι ώστε

$$9(2k+1)-2(9k+4)=18k+9-18k-8=1$$

συνεπώς $(2k+1,9k+4)=1$.

Θεώρημα 6.2

Έστω $a_1,\dots,a_n$ ακέραιοι όχι όλοι ίσοι με μηδέν. Ισχύουν

1) $(a_1,\dots,a_n)=(|a_1|,\dots,|a_n|)$

μ' άλλα λόγια ο μ.κ.δ είναι ανεξάρτητος από τα πρόσημα

2) Αν $\lambda\neq 0$, τότε $(\lambda a_1,\dots,\lambda a_n)=|\lambda|(a_1,\dots,a_n)$

3) Αν $y = a_1x_1 + \cdots + a_nx_n$, $x_i \in \mathbb{Z}$, τότε

$$(a_1, \ldots, a_n, y) = (a_1, \ldots, a_n)$$

4) Αν $(a_1, \ldots, a_n) = d$, τότε $\left(\frac{a_1}{d}, \ldots, \frac{a_n}{d}\right) = 1$.

Απόδειξη.

1) Έστω $d = (a_1, \ldots, a_n)$ και $d' = (|a_1|, \ldots, |a_n|)$.

Είναι $\left.\begin{matrix} d|a_1 \\ \vdots \\ d|a_n \end{matrix}\right\} \Rightarrow \left.\begin{matrix} d||a_1| \\ \vdots \\ d||a_n| \end{matrix}\right\} \Rightarrow d \,|\, (|a_1|, \ldots |a_n|)$, δηλ $d|d'$

Όμοια παίρνουμε ότι και ο $d'|d$. Αφού $d, d' \in \mathbb{N}$ και $d|d'$ και $d'|d$ συμπεραίνουμε ότι $d = d'$

2) Αν $d = (a_1, \ldots, a_n)$ τότε $d|a_1, \ldots, d|a_n$. Επειδή επιπλέον $\lambda|\lambda$, θα έχουμε $\pm\lambda d|\lambda a_1, \ldots, \pm\lambda d|\lambda a_n$ και τελικά $|\lambda|d|\lambda a_1, \ldots, |\lambda|d|\lambda a_n$.

Σύμφωνα τώρα με το πόρισμα 6.2 για να είναι $(\lambda a_1, \ldots, \lambda a_n) = |\lambda|d$ αρκεί να δείξουμε ότι υπάρχουν ακέραιοι $x_1, \ldots, x_n$, έτσι ώστε $|\lambda|d = (\lambda a_1)x_1 + \cdots + (\lambda a_n)x_n$.

Πραγματικά, αφού $d = (a_1, \ldots, a_n)$, υπάρχουν ακέραιοι $k_1, \ldots, k_n$, έτσι ώστε $d = a_1k_1 + \cdots + a_nk_n$.

Έτσι $|\lambda|d = |\lambda|(a_1k_1 + \cdots + a_nk_n)$, επομένως

i) Αν $\lambda > 0$, τότε $|\lambda|d = (\lambda a_1)k_1 + \cdots + (\lambda a_n)k_n$

ii) Αν $\lambda < 0$, τότε $|\lambda|d = (\lambda a_1)(-k_1) + \cdots + (\lambda a_n)(-k_n)$,

πράγμα που επιδιώκαμε.

3) Αν $d = (a_1, \ldots, a_n)$ και $d' = (a_1, \ldots, a_n, y)$, τότε εύκολα διαπιστώνουμε ότι $d|d'$ και $d'|d$, οπότε $d = d'$.

4) Είναι $d = (a_1, \ldots, a_n) = \left(d \cdot \frac{a_1}{d}, \ldots, d \cdot \frac{a_n}{d}\right) =$

$$= d\left(\frac{a_1}{d}, \ldots, \frac{a_n}{d}\right)$$

Επειδή $d \neq 0$, παίρνουμε $\left(\frac{a_1}{d}, \ldots, \frac{a_n}{d}\right) = 1$. ■

Για παράδειγμα έχουμε

α) $(7, -21, -35) = (7, 21, 35) = (-7, 21, 35)$

β) $(20, 35, 60) = (5\cdot 4, 5\cdot 7, 5\cdot 12) = 5\,(4, 7, 12)$

γ) $(20, 35, 90) = (20, 35, 20 + 2\cdot 35) = (20, 35)$

δ) Είναι $(6, 10) = 2$ οπότε $\left(\frac{6}{2}, \frac{10}{2}\right) = (3, 5) = 1$.

Θεώρημα 6.3

Ο μ.κ.δ ακεραίων αριθμών $a_1, \ldots, a_n$, $(n > 2)$ δεν μεταβάλλεται αν μερικοί απ' αυτούς αντικατασταθούν με τον μ.κ.δ τους, π.χ για κάθε k , $1 \leq k \leq n-2$, ισχύει.

$$(a_1, \ldots, a_n) = (a_1, \ldots, a_k, (a_{k+1}, \ldots, a_n)) .$$

Απόδειξη.

Παρατηρούμε ότι, για κάθε μετάθεση $i_1, \ldots, i_n$ των $1, 2 \ldots, n$, έχουμε $(a_1, \ldots, a_n) = (a_{i_1}, \ldots, a_{i_n})$. Για να αποδείξουμε, λοιπόν το θεώρημα αρκεί να δείξουμε ότι, για κάθε k $1 \leq k \leq n-2$, ισχύει

$$(a_1, \ldots, a_n) = (a_1, \ldots, a_k, (a_{k+1}, \ldots, a_n)) .$$

Έστω $d = (a_1, \ldots, a_n)$, $\delta = (a_{k+1}, \ldots, a_n)$ και $d' = (a_1, \ldots, a_k, \delta)$.

Έχουμε

$$d \mid a_1, \ldots, d \mid a_k, d \mid a_{k+1}, \ldots, d \mid a_n \Rightarrow d \mid a_1, \ldots, d \mid a_k, d \mid \delta,$$

οπότε $d \mid d'$. Όμοια δείχνουμε ότι $d' \mid d$, συνεπώς $d = d'$. ■

Για παράδειγμα $(7, 21, 40, 155) = (7, 155, 40, 21) =$

$= \big((7, 155), 40, 21\big) = \big(7, (155, 40), 21\big) = \ldots$

Θεώρημα 6.4

Αν για τους φυσικούς αριθμούς a, b έχουμε

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_\kappa^{\alpha_\kappa} \quad \alpha_i \geq 0 \quad \text{και} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_\kappa^{\beta_\kappa} \quad \beta_i \geq 0$$

τότε

$$(a, b) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_\kappa^{\gamma_\kappa} \quad \text{με} \quad \gamma_i = \min\{\alpha_i, \beta_i\} \quad , i = 1, 2, \ldots, \kappa.$$

Απόδειξη.

Παρατηρούμε ότι για το φυσικό αριθμό

$$d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_\kappa^{\gamma_\kappa} \quad \text{με } \gamma_i = \min\{a_i, b_i\} \quad i = 1, \ldots, \kappa$$

σύμφωνα με το θεώρημα 5.4, έχουμε

$d|a$ και $d|b$, αφού $\min\{a_i, b_i\} \leq a_i$ και $\min\{a_i, b_i\} \leq b_i$, για κάθε i, $1 \leq i \leq \kappa$.

Απομένει να δείξουμε ότι, αν $\delta \in \mathbb{N}$, με $\delta|a$ και $\delta|b$, τότε $\delta|d$. Πραγματικά, ο $\delta = p_1^{\lambda_1} \cdots p_\kappa^{\lambda_\kappa}$, με $\lambda_i \geq 0$. Είναι

$$\left.\begin{array}{l} \delta|a \Leftrightarrow \lambda_i \leq a_i \text{ για κάθε } i, 1 \leq i \leq \kappa \\ \delta|b \Leftrightarrow \lambda_i \leq b_i \text{ για κάθε } i, 1 \leq i \leq \kappa \end{array}\right\} \Leftrightarrow \lambda_i \leq \min\{a_i, b_i\} \text{ για κάθε } i, 1 \leq i \leq \kappa$$

$\Leftrightarrow \delta|d$. ■

Γενικότερα ισχύει:

Θεώρημα 6.5

Για φυσικούς αριθμούς $a_1, \ldots, a_\kappa$ $(\kappa > 2)$, αν

$$a_j = \prod_{i=1}^{\tau} p_i^{\alpha_{ji}} \quad , \alpha_{ji} \geq 0 \quad (j = 1, 2, \ldots, \kappa)$$

τότε

$$(a_1, a_2, \ldots, a_\kappa) = \prod_{i=1}^{\tau} p_i^{b_i}$$

με $b_i = \min\{\alpha_{1i}, \ldots, \alpha_{\kappa i}\}$, $(i = 1, 2, \ldots, \tau)$

Απόδειξη.

Η απόδειξη γίνεται με ίδιο τρόπο, όπως και στο θεώρημα 6.4.

Πόρισμα 6.4

Αν $a, b \in \mathbb{Z}-\{0\}$, τότε, για κάθε φυσικό αριθμό n, ισχύει

$$(a^n, b^n) = (a, b)^n$$

Απόδειξη.

Για $a=1$ ή $b=1$ ισχύει. Υποθέτουμε ότι $a>1$ και $b>1$ και έστω

$$a = p_1^{\alpha_1} \cdots p_\kappa^{\alpha_\kappa}, \quad \alpha_i \geq 0 \quad \text{και} \quad b = p_1^{\beta_1} \cdots p_\kappa^{\beta_\kappa} \quad \beta_i \geq 0.$$

Αν

$\delta = (a, b)$ τότε $\delta = p_1^{\gamma_1} \cdots p_\kappa^{\gamma_\kappa}$ όπου $\gamma_i = \min\{\alpha_i, \beta_i\}$, $i = 1, \ldots, \kappa$.

Για κάθε φυσικό αριθμό n έχουμε,

$$a^n = p_1^{n\alpha_1} \cdots p_\kappa^{n\alpha_\kappa} \quad \text{και} \quad b^n = p_1^{n\beta_1} \cdots p_\kappa^{n\beta_\kappa},$$

και αν $d = (a^n, b^n)$, τότε

$d = p_1^{\lambda_1} \cdots p_\kappa^{\lambda_\kappa}$, όπου $\lambda_i = \min\{n\alpha_i, n\beta_i\}$ $i = 1, \ldots, \kappa$.

Έτσι $\lambda_i = \min\{n\alpha_i, n\beta_i\} = n \cdot \min\{\alpha_i, \beta_i\} = n \cdot \gamma_i$

επομένως

$d = p_1^{\lambda_1} \cdots p_\kappa^{\lambda_\kappa} = p_1^{n\gamma_1} \cdots p_\kappa^{n\gamma_\kappa} = (p_1^{\gamma_1} \cdots p_\kappa^{\gamma_\kappa})^n = \delta^n$, όπως επιδιώκουμε.

Αφού ο μ.κ.δ είναι ανεξάρτητος από τα πρόσημα των ακεραίων, το πόρισμα ισχύει για $a, b \in \mathbb{Z}-\{0\}$. ■

Θεώρημα 6.6.

Για ακεραίους $a, b_1, \ldots, b_n$ ισχύει.

$$(a, b_1 \cdot b_2 \cdots b_n) = (a, (a, b_1) \cdot (a, b_2) \cdots (a, b_n)).$$

Απόδειξη

Αρχικά θα δείξουμε ότι, για κάθε κ, $1 \leq \kappa \leq n$ ισχύει.

$$(a, b_1 b_2 \cdots b_n) = (a, b_1 \cdots b_{\kappa-1} (a, b_\kappa) b_{\kappa+1} \cdots b_n)$$

Πραγματικά

$$(a, b_1 \cdots b_n) = (a, b_1 \cdots b_n, b_1 \cdots b_{\kappa-1} b_{\kappa+1} \cdots b_n \, a) \quad \text{(Θεωρ. 6.2)}$$

$$= (a, (b_1 \cdots b_n, b_1 \cdots b_{\kappa-1} b_{\kappa+1} \cdots a)) \quad \text{(Θεωρ. 6.3)}$$

$$= (a, |b_1 \cdots b_{\kappa-1} b_{\kappa+1} \cdots b_n| (a, b_\kappa)) \quad \text{(Θεωρ. 6.2)}$$

$= (a, b_1 \cdots b_{k-1}(a,b_k) b_{k+1} \cdots b_n)$ (θεωρ. 6.2)

Έτσι

$(a, b_1 b_2 \cdots b_n) = (a, (a,b_1) b_2 \cdots b_n)$

$= (a, (a,b_1)(a,b_2) \cdots b_n)$

. . . . . -

$= (a, (a,b_1)(a,b_2) \cdots (a,b_n))$ - ■

Πόρισμα 6.5

Αν οι $a, b_1, \ldots, b_n$ είναι ακέραιοι τέτοιοι ώστε $(a, b_i) = 1$, για κάθε i, $1 \le i \le n$, τότε $(a, b_1 \cdot b_2 \cdots b_n) = 1$.

Απόδειξη.

Σύμφωνα με το θεώρημα 6.6

$(a, b_1 \cdots b_n) = (a, (a,b_1) \cdots (a,b_n)) = (a, 1 \cdot 1 \cdots 1) =$

$= (a, 1) = 1$. ■

Πόρισμα 6.6.

i) Αν $(a,b) = 1$, τότε $(a^\mu, b^\nu) = 1$, για κάθε $\mu, \nu \in \mathbb{N}$

ii) Αν $\mu, \nu \in \mathbb{N}$ και $(a^\mu, b^\nu) = 1$, τότε $(a,b) = 1$.

Απόδειξη.

i) Αρχικά παρατηρούμε ότι για κάθε φυσικό μ, έχουμε $(a^\mu, b) = 1$. Πραγματικά,

$(a^\mu, b) = (\underbrace{a \cdot a \cdots a}_{\mu\text{-φορές}}, b) =$ (θεωρ. 6.6)

$= (\underbrace{(a,b) \cdots (a,b)}_{\mu\text{-φορές}}, b) =$

$= ((a,b)^\mu, b) = (1, b) = 1$.

Έτσι

$(a^\mu, b^\nu) = (a^\mu, b \cdots b) = (a^\mu, \underbrace{(a^\mu, b) \cdots (a^\mu, b)}_{\nu\text{-φορές}})$

$= (a^\mu, 1^\nu) = (a^\mu, 1) = 1$.

ii) $(a,b) = (a,b,a^\mu)$ (θεωρ. 6.2, 3))

$= (a,b,a^\mu,b^\nu)$ >>

$= (a,b,(a^\mu,b^\nu))$ (θεωρ. 6.3)

$= (a,b,1) = 1$. ■

Θεώρημα 6.7 (Λήμμα του Ευκλείδη)

Αν $a|bc$ και $(a,b)=1$, τότε $a|c$.

Απόδειξη 1η.

Αφού $(a,b)=1$, και $a|bc$, υπάρχουν ακέραιοι x,y,k έτσι ώστε $1=ax+by$ και $bc=ak$.

Έχουμε

$$c = c\cdot 1 = c(ax+by) = cax+cby = cax+aky = a(cx+ky)$$

δηλ $a|c$.

Απόδειξη 2η

Αφού $a|bc$, θα έχουμε $(a,bc)=|a|$.

Αλλά $(a,bc) = (a,(a,b)c) = (a,1\cdot c) = (a,c)$,

οπότε $(a,c) = |a| \Rightarrow a|c$. ■

Θα παρατηρήσουμε εδώ ότι είναι δυνατόν $a|bc$ και όμως $a\nmid b$, $a\nmid c$. Για παράδειγμα, $15|5\cdot 9$ και $15\nmid 5$, $15\nmid 9$.

Το επόμενο πόρισμα είναι το γνωστό μας θεώρημα 5.2, που εδώ θα το αποδείξουμε με τη χρήση της θεωρίας μ.κ.δ.

Πόρισμα 6.7

Για κάθε πρώτο αριθμό p,

$$p|bc \text{ και } p\nmid b \Rightarrow p|c.$$

Απόδειξη

Αν ο p είναι πρώτος και $p \nmid b$, τότε είναι φανερό ότι $(p,b)=1$. Από το θεώρημα 6.7 παίρνουμε τώρα ότι $p \mid c$. ■

Θεώρημα 6.8

Αν $(b,c)=1$ τότε $(a,bc)=(a,b)(a,c)$

Απόδειξη.

$$\begin{aligned}
(a,bc) &= (a^2, a, bc) && (\text{θεωρ. } 6.2,\ 3)\\
&= (a^2, a(b,c), bc) && \text{αφού } (b,c)=1\\
&= (a^2, (ab,ac), bc) && (\text{θεωρ } 6.2,\ 2)\\
&= (a^2, ab, ac, bc) && (\text{θεωρ. } 6.3)\\
&= \big((a^2,ab), (ac,bc)\big) && \gg\\
&= \big(a(a,b), c(a,b)\big) && (\text{θεωρ. } 6.2,\ 2)\\
&= (a,b)(a,c) && \gg \text{ για } \lambda=(a,b). \blacksquare
\end{aligned}$$

Πόρισμα 6.8

Αν $b \mid a$ και $c \mid a$, με $(b,c)=1$, τότε $bc \mid a$.

Απόδειξη.

Παρατηρούμε ότι $(a,b)=|b|$, $(a,c)=|c|$, αφού $b \mid a$ και $c \mid a$, αντίστοιχα. Από το θεώρημα 6.8 έχουμε $(a,bc)=(a,b)(a,b)=|b||c|=|bc|$, οπότε $|bc| \mid a$ και επομένως $bc \mid a$. ■

Είναι δυνατόν $b \mid a$, $c \mid a$ και όμως $bc \nmid a$. Για παράδειγμα, $10 \mid 20$ και $5 \mid 20$ και $5 \cdot 10 \nmid 20$.

Πόρισμα 6.9

Αν $(b,c)=1$, τότε για κάθε φυσικό αριθμό a με $a|bc$, ισχύει

$$a=(a,b)(a,c)$$

δηλ. ο a αναφέρεται σε γινόμενο $(a,b)\cdot(a,c)$ φυσικών διαιρετών των b,c, αντίστοιχα.

Απόδειξη.

Αφού $a\in\mathbb{N}$ και $a|bc$ θα είναι $(a,bc)=a$.

Από το θεώρημα 6.8 τώρα παίρνουμε $a=(a,b)(a,c)$. ∎

Όπως θα δείξουμε στη συνέχεια (στη γενική περίπτωση), μια τέτοια ανάλυση του a είναι μοναδική.

Το θεώρημα 6.8, γενικότερα, διατυπώνεται ως εξής:

Θεώρημα 6.9.

Αν οι ακέραιοι $b_1,\dots,b_n$ είναι πρώτοι μεταξύ τους ανά δύο, τότε

$$(a,b_1b_2\cdots b_n)=(a,b_1)(a,b_2)\cdots(a,b_n).$$

Απόδειξη.

Αρχικά θα δείξουμε ότι $(b_i,b_{i+1}\cdots b_n)=1 \quad \forall i,\ 1\le i\le n-1$.

Σύμφωνα με το Θεώρημα 6.6, έχουμε

$$(b_i,b_{i+1}\cdots b_n)=\big(b_i,(b_i,b_{i+1})\cdots(b_i,b_n)\big)=$$
$$=(b_i,1\cdots1)=(b_i,1)=1.$$

Από το θεώρημα 6.8, τώρα, διαδοχικά παίρνουμε

$$(a,b_1\cdot b_2\cdots b_n)=(a,b_1)(a,b_2\cdots b_n)=$$
$$=(a,b_1)(a,b_2)(a,b_3\cdots b_n)$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$=(a,b_1)(a,b_2)\cdots(a,b_n). \ ∎$$

Πόρισμα 6.10

Αν οι $a_1, \ldots, a_\nu$ είναι πρώτοι μεταξύ τους ανά δύο και, όμοια, αν οι $b_1, \ldots, b_\mu$ είναι πρώτοι μεταξύ τους ανά δύο, τότε

$$(a_1 \cdots a_\nu , b_1 \cdots b_\mu) = \prod_{i=1}^{\nu} \prod_{j=1}^{\mu} (a_i, b_j)$$

Απόδειξη.

Αν συμβολίσουμε $a = a_1 \cdots a_\nu$ και $b = b_1 \cdots b_\mu$, έχουμε

$$(a,b) = (a_1 \cdots a_\nu, b) = \prod_{i=1}^{\nu} (a_i, b) \qquad (\text{Θεωρ. } 6.9)$$

$$= \prod_{i=1}^{\nu} (a_i, b_1 \quad b_\mu) = \qquad (\text{Θεωρ. } 6.9)$$

$$= \prod_{i=1}^{\nu} \prod_{j=1}^{\mu} (a_i, b_j) \; . \; \blacksquare$$

Οι αποδείξεις των επόμενων δύο παρισμάτων είναι όμοιες με εκείνες των Πορισμάτων 6.8 και 6.9, αντίστοιχα.

Πόρισμα 6.11

Αν οι ακέραιοι $b_1, \ldots, b_n$ είναι πρώτοι μεταξύ τους ανά δύο και $b_1 | a , \ldots b_n | a$, τότε $b_1 \cdots b_n | a$.

Πόρισμα 6.12

Αν οι ακέραιοι $b_1, \ldots, b_n$ είναι πρώτοι μεταξύ τους ανά δύο, τότε, για κάθε φυσικό αριθμό a με $a | b_1 \cdots b_n$, ισχύει

$$a = (a, b_1) \cdots (a, b_n) \; . \; \square$$

δηλ. ο a αναλύεται σε γινόμενο $(a, b_1) \cdots (a, b_n)$ φυσικών διαιρετών των $b_1, \ldots, b_n$, αντίστοιχα .

Στη συνέχεια, θα δείξουμε ότι κάθε τέτοια ανάλυση είναι μοναδική. Γι' αυτόν τον σκοπό δίνουμε τα επόμενα δυο λήμματα.

Λήμμα 6.1

Για ακεραίους $a_1, \ldots, a_n$ και για κάθε n-άδα $s_1, \ldots, s_n$ διαιρετών $s_1 | a_1, \ldots, s_n | a_n$, ισχύουν.

i) Αν $(a_1, \ldots, a_n) = 1 \Rightarrow (s_1, \ldots s_n) = 1$

ii) Αν οι $a_1, \ldots, a_n$ είναι πρώτοι μεταξύ τους ανά δύο, τότε και οι $s_1, \ldots, s_n$ είναι πρώτοι μεταξύ τους ανά δύο.

Απόδειξη.

i) Έστω $\delta = (s_1, \ldots, s_n)$. Είναι

$$\left.\begin{array}{ll} \delta | s_1 & \text{και } s_1 | a_1 \\ \vdots & \vdots \\ \delta | s_n & s_n | a_n \end{array}\right\} \Rightarrow \left.\begin{array}{l} \delta | a_1 \\ \vdots \\ \delta | a_n \end{array}\right\} \Rightarrow \delta | (a_1, \ldots, a_n) \text{ δηλ. } \delta | 1$$

επομένως $\delta = 1$.

ii) Αν $\delta = (s_i, s_j)$, $i \neq j$, $i, j \in \{1, \ldots, n\}$ τότε

$$\left.\begin{array}{l} \delta | s_i \text{ και } s_i | a_i \\ \delta | s_j \text{ και } s_j | a_j \end{array}\right\} \Rightarrow \left.\begin{array}{l} \delta | a_i \\ \delta | a_j \end{array}\right\} \Rightarrow \delta | (a_i, a_j) \text{ δηλ. } \delta | 1$$

οπότε $\delta = 1$. ■

Λήμμα 6.2

Θεωρούμε τους ακέραιους $a_1, \ldots, a_n$, που είναι πρώτοι μεταξύ τους ανά δύο και δύο n-άδες $s_1, \ldots, s_n$ και $t_1, \ldots, t_n$ φυσικών διαιρετών $s_1 | a_1, \ldots, s_n | a_n$ και $t_1 | a_1, \ldots, t_n | a_n$.

i) $(s_1 \cdots s_n, t_1 \cdots t_n) = (s_1, t_1) \cdots (s_n, t_n)$

ii) Αν $s_1 \cdots s_n = t_1 \cdots t_n$ τότε $s_1 = t_1, \ldots, s_n = t_n$.

Απόδειξη.

i) Σύμφωνα με το λήμμα 6.1, έχουμε

$$(s_i, s_j) = (t_i, t_j) = 1 \quad \text{για } i \neq j.$$

Επιπλέον $(s_i, t_j) = 1$, για $i \neq j$. Πραγματικά, αν $\delta = (s_i, t_j)$, τότε $\left.\begin{array}{l} \delta | s_i \text{ και } s_i | a_i \\ \delta | t_j \text{ και } t_j | a_j \end{array}\right\} \Rightarrow \left.\begin{array}{l} \delta | a_i \\ \delta | a_j \end{array}\right\} \Rightarrow \delta | (a_i, a_j)$,

δηλ. $\delta \mid 1$, οπότε $\delta = 1$.

Σύμφωνα με το πόρισμα 6.10, θα είναι

$$(s_1 \cdots s_n, t_1 \cdots t_n) = \prod_{i=1}^{n} \prod_{j=1}^{n} (s_i, t_j) = (s_1, t_1) \cdots (s_n, t_n).$$

ii) Έχουμε $s_1 \cdots s_n = (s_1 \cdots s_n, t_1 \cdots t_n) = t_1 \cdots t_n$

και από το i) θα είναι

$$s_1 \cdots s_n = (s_1, t_1) \cdots (s_n, t_n) = t_1 \cdots t_n.$$

με $(s_i, t_i) \leq s_i$ και $(s_i, t_i) \leq t_i$, $i = 1, \ldots, n$.

Ταυτόχρονα, λοιπόν, θα είναι

$$s_i = (s_i, t_i) = t_i \qquad i = 1, \ldots, n,$$

οπότε $s_i = t_i \qquad i = 1, \ldots, n$. ■

Θεώρημα 6.10.

Αν οι ακέραιοι $b_1, \ldots, b_n$ είναι πρώτοι προς ανάγωγους ανά δύο, τότε, για κάθε φυσικό διαιρέτη $a \mid b_1 \cdots b_n$ του γινομένου των, είναι

$$a = (a, b_1) \cdots (a, b_n)$$

και η ανάλυση αυτή του a σε γινόμενο φυσικών διαιρετών των $b_1, \ldots, b_n$, αντίστοιχα, είναι μοναδική.

Απόδειξη.

Η υπαρξη εξασφαλίζεται από το πόρισμα 6.12, και η μοναδικότητα από το λήμμα 6.2. ■

7. Στην εύρεση του μ.κ.δ. - Ευκλείδιος Αλγόριθμος

Λήμμα 7.1

Για κάθε ζεύγος ακεραίων a, b, με $b \neq 0$, και για το μοναδικό (σύμφωνα με την Ευκλείδια διαίρεση) ζεύγος ακεραίων q, r, με $a = bq + r$, $0 \leq r < |b|$ ισχύει

$$(a, b) = (b, r)$$

Απόδειξη

Έστω $d = (a, b)$ και $\delta = (b, r)$. Είναι

$$\left.\begin{matrix} d|a \\ d|b \end{matrix}\right\} \Rightarrow \left.\begin{matrix} d|a \\ d|bq \end{matrix}\right\} \Rightarrow d|a - bq, \text{ δηλ } d|r.$$

Έτσι $d|b$ και $d|r \Rightarrow d|(b, r)$, δηλ $d|\delta$.

Από την άλλη μεριά

$$\left.\begin{matrix} \delta|b \\ \delta|r \end{matrix}\right\} \Rightarrow \left.\begin{matrix} \delta|bq \\ \delta|r \end{matrix}\right\} \Rightarrow \delta|bq + r, \text{ δηλ } \delta|a$$

Έτσι $\delta|b$ και $\delta|a \Rightarrow \delta|(a, b)$, δηλ $\delta|d$.

Επειδή $d|\delta$, $\delta|d$ και $\delta, d \in \mathbb{N}$, παίρνουμε $\delta = d$. ■

Τον μ.κ.δ δυο ακεραίων μπορούμε να τον βρούμε αν γράψουμε τους φυσικούς κοινούς τους διαιρέτες και πάρουμε το μεγαλύτερο. Για μεγάλους, όμως, ακέραιους η εργασία αυτή είναι επίπονη.

Υπάρχει, όμως, μια πιο κατάλληλη συστηματική διαδικασία για την εύρεση του μ.κ.δ, που στηρίζεται στην επαναληπτική εφαρμογή της Ευκλείδιας διαίρεσης και είναι γνωστή σαν <u>Αλγόριθμος του Ευκλείδη</u> ή Αλγόριθμος εύρεσης του μ.κδ και περιγράφεται ως εξής:

Ας υποθέσουμε ότι θέλουμε να βρούμε τον μ.κ.δ δυο ακεραίων α_0, α_1, με $\alpha_1 \neq 0$. Επειδή $(\alpha_0, \alpha_1) = (|\alpha_0|, |\alpha_1|)$ δε χάνουμε τίποτα αν υποθέσουμε $\alpha_0 \geq \alpha_1 > 0$.

Έστω, ότι, μετά από ν σε πλήθος διαδοχικές εφαρμογές της Ευκλείδιας διαίρεσης είναι:

$$(I)\begin{cases} \alpha_0 = \alpha_1 q_1 + r_2 & , \quad 0 \leq r_2 < \alpha_1 \\ \alpha_1 = r_2 q_2 + r_3 & , \quad 0 \leq r_3 < r_2 \\ \vdots & \qquad \vdots \\ r_{\nu-2} = r_{\nu-1} q_{\nu-1} + r_\nu & , \quad 0 \leq r_\nu < r_{\nu-1} \\ r_{\nu-1} = r_\nu q_\nu + r_{\nu+1} & , \quad 0 \leq r_{\nu+1} < r_\nu \end{cases}$$

όπου $0 \leq r_{\nu+1} < r_\nu < r_{\nu-1} < \cdots < r_2 < \alpha_1$.

Αν, λοιπόν, για κάθε φυσικό αριθμό ν, με τον παραπάνω τρόπο, προέκυπτε ένα υπόλοιπο $r_{\nu+1} > 0$, θα υπήρχαν μεταξύ των αριθμών α_1 και 0, άπειροι άνισοι φυσικοί αριθμοί $r_2, r_3, \ldots$, πράγμα άτοπο, αφού το σύνολό τους οφείλει να έχει ελάχιστο στοιχείο.

Επομένως, για κάποιο φυσικό αριθμό ν, μοναδικά ορισμένο για το ζεύγος των ακεραίων α_0, α_1, θα είναι $r_{\nu+1} = 0$ οπότε $r_{\nu-1} = r_\nu q_\nu$.

Εφαρμόζοντας, τώρα, το λήμμα 7.1 στις εξισώσεις του συστήματος (I), παίρνουμε

$$(\alpha_0, \alpha_1) = (\alpha_1, r_2) = (r_2, r_3) = \cdots = (r_{\nu-1}, r_\nu) = r_\nu ,$$

αφού $r_\nu \mid r_{\nu-1}$.

Η αποκατάσταση του συστήματος (I) μέχρι του φυσικού αριθμού ν, για τον οποίο $r_{\nu+1} = 0$, και αυτό το ίδιο το σύστημα (I) καλείται **Ευκλείδιος αλγόριθμος** για το δοθέν ζεύγος α_0, α_1.

Επομένως, <u>ο μ.κ.δ δυό ακεραίων α, b είναι το τελευταίο μη-μηδενικό υπόλοιπο στον Ευκλείδιο αλγόριθμο για τα βήματα των ακεραίων |a|, |b|</u>.

Το θεώρημα, τώρα 6.1, μας βεβαιώνει ότι ο μ.κ.δ των ακεραίων a_0, a_1 μπορεί να γραφεί με την μορφή a_0x+a_1y, η απόδειξη τους, όμως, δεν μας παρέχει τρόπο για να βρίσκουμε τέτοιους ακεραίους x, y.

<u>Τον τρόπο αυτό μας τον δίνει ο Ευκλείδιος Αλγόριθμος</u> ως εξής:

Από την προτελευταία εξίσωση του συστήματος (τ) παίρνουμε

$$r_n = r_{n-2} - r_{n-1}q_{n-1} \qquad (7)$$

και από την προηγούμενή της

$$r_{n-1} = r_{n-3} - r_{n-2}q_{n-2} \qquad (8)$$

Αντικαθιστώντας το r_{n-1}, από την (8) στην (7) παίρνουμε

$$r_n = (1+q_{n-1}q_{n-2})r_{n-2} + (-q_{n-1})r_{n-3}, \qquad (9)$$

δηλ. τον ακέραιο $r_n = (a_0, a_1)$ σαν γραμμικό συνδυασμό των r_{n-2} και r_{n-3}.

Συνεχίζοντας μ' αυτό τον τρόπο και με την τελευταία αντικατάσταση του υπόλοιπου $r_1 = a_0 - a_1q_1$, θα πάρουμε τον r_n σαν γραμμικό συνδυασμό των a_0 και a_1.

Για να ξεκαθαρίσουμε περισσότερο τα πράγματα δίνουμε το επόμενο παράδειγμα.

Παράδειγμα 7.1

Θα βρούμε τον (1985, 132).

Από τον Ευκλείδιο αλγόριθμο έχουμε

$$1985 = 132 \cdot 15 + 5$$
$$132 = 5 \cdot 26 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 1 \cdot 2 + 0$$

Έτσι $(1985, 132) = 1$.

Για να βρούμε τώρα ακεραίους x, y έτσι ώστε

$$1 = 1985x + 132y$$

εργαζόμαστε ως εξής:

$$1 = 5 - 2\cdot 2 = 5 - 2(132 - 5\cdot 26) = 5\cdot 53 - 132\cdot 2$$

$$= (1985 - 15\cdot 132)\cdot 53 - 132\cdot 2$$

$$= 1985\cdot(53) + 132(-797)$$

Έτσι $x = 53$ και $y = -797$. ∎

Θα παρατηρήσουμε, εδώ ότι το ζεύγος των ακεραίων $x = 53$ $y = -797$ έτσι ώστε $1 = 1985x + 132y$, δεν είναι μοναδικό. Όπως θα δούμε στις Γραμμικές Διοφαντικές εξισώσεις πιο κάτω, και οι ακέραιοι

$$x = 53 + 132t \quad , \quad y = -797 - 1985t \quad , t \in \mathbb{Z}$$

πληρούν την εξίσωση

$$1 = 1985x + 132y$$

π.χ αν $t = -1$, τότε, για τους ακέραιους $x = 53 - 132 = -79$ και $y = -797 + 1985 = 1.188$, έχουμε

$$1985(-79) + 132\cdot(1188) = 1 .$$

Παράδειγμα 7.2

Για την ακολουθία F_n του Fibonacci

$$F_1 = F_2 = 1 \quad \text{και} \quad F_{n+1} = F_n + F_{n-1} \quad , \forall n \geq 2$$

έχουμε:

$$(F_{n+2}, F_{n+1}) = 1 \quad , \quad \text{για κάθε } n \geq 1 .$$

Πραγματικά, από τον Ευκλείδιο Αλγόριθμο παίρνουμε

$$\begin{cases} F_{n+2} = 1\cdot F_{n+1} + F_n \\ F_{n+1} = 1\cdot F_n + F_{n-1} \\ \vdots \\ F_4 = 1\cdot F_3 + F_2 \\ F_3 = 2\cdot F_2 + 0 \end{cases}$$

οπότε $(F_{n+2}, F_{n+1}) = F_2 = 1 \quad , \forall n \geq 1.$

Το πλήθος των βημάτων που απαιτούνται στον παραπάνω Ευκλείδιο αλγόριθμο είναι **ακριβώς** n.

Επιπλέον αν χάσουμε υπόψη μας ότι $(F_1, F_2) = 1$, θα έχουμε

$$(F_n, F_{n+1}) = 1 \quad , \forall n \geq 1.$$

Παρατηρήσεις

1) Για κάθε φυσικό αριθμό n υπάρχουν ακέραιοι a, b έτσι ώστε, για τον υπολογισμό του (a,b), το πλήθος των βημάτων στον Ευκλείδιο Αλγόριθμο να είναι ακριβώς n.
Πραγματικά, για κάθε φυσικό n υπάρχουν οι ακέραιοι $a = F_{n+2}$ και $b = F_{n+1}$ όπως στο παράδειγμα 7.2, για τους οποίους το πλήθος των βημάτων στον Ευκλείδιο Αλγόριθμο είναι ακριβώς n.

2) Ο Γάλλος μαθηματικός Gabriel Lamé (1795-1870) απέδειξε ότι ο αριθμός n των βημάτων στον Ευκλείδιο Αλγόριθμο είναι $\leq$ του αριθμού 5 επί το πλήθος των ψηφίων του μικρότερου ακεραίου.
Έτσι, στο παράδειγμα 7.1, το πλήθος των βημάτων είναι $n = 4$, που είναι μικρότερο του $5 \cdot 3 = 15$. ■

Η εύρεση τώρα του μ.κ.δ n σε πλήθος ($n > 2$) ακεραίων $a_1, a_2, \ldots, a_n$ είναι υπόθεση ρουτίνας.
Αν συμβολίσουμε

$$d_1 = (a_1, a_2) \ , d_2 = (d_1, a_3), \ldots, d_{n-1} = (d_{n-2}, a_n)$$

τότε

$$(a_1, a_2, \ldots, a_n) = d_{n-1} .$$

Πραγματικά, σύμφωνα με το θεώρημα 6.3 είναι

$$\begin{aligned}(a_1, a_2, \ldots, a_n) &= \big((a_1, a_2), a_3, \ldots, a_n\big) \\ &= (d_1, a_3, \ldots, a_n) \\ &= \big((d_1, a_3), \ldots, a_n\big) \\ &= (d_2, a_4, \ldots, a_n) \\ &\vdots \\ &= (d_{n-2}, a_n) = d_{n-1}\,.\end{aligned}$$

Παράδειγμα 7.3

Θα υπολογίσουμε τον $d=(112,96,24)$ και θα βρούμε ακεραίους x,y,z τέτοιους ώστε $d=112x+96y+24z$.

Είναι

$$\left.\begin{aligned}112 &= 96\cdot 1 + 16 \\ 96 &= 16\cdot 6 + 0\end{aligned}\right\},\ \text{οπότε } (112,96)=16 \text{ και } 16 = 112 + 96(-1)$$

και

$$\left.\begin{aligned}24 &= 16\cdot 1 + 8 \\ 16 &= 8\cdot 2 + 0\end{aligned}\right\},\ \text{οπότε } (16,24)=8 \text{ και } 8 = 24 + 16(-1)$$

Έτσι $(112,96,24) = \big((112,96),24\big) = (16,24) = 8$

και

$$8 = 24 + 16(-1) = 24 - (112 + 96(-1)) = 112(-1) + 96\cdot 1 + 24\cdot 1\,.$$

Υπάρχουν, προφανώς, οι ακέραιοι $x=-1$ και $y=z=1$, έτσι ώστε

$$8 = 112x + 96y + 24z\,. \blacksquare$$

8. Ελάχιστο κοινό πολλαπλάσιο (Ε.Κ.Π)

Ορισμός

Ο ακέραιος αριθμός ℓ καλείται **κοινό πολλαπλάσιο** των ακεραίων αριθμών $a_1, a_2, \ldots, a_n$, αν

$$a_1 \mid \ell\,,\ a_2 \mid \ell\,,\ \ldots,\ a_n \mid \ell\,.$$

Στην περίπτωση που ένας τουλάχιστον από τους ακεραίους $a_1, a_2, \ldots, a_n$ είναι ίσος με μηδέν, τότε όλα τον τα πολ/σια είναι ίσα με μηδέν, επομένως ο 0 είναι το μόνο κοινό πολ/πλο των $a_1, \ldots, a_n$ και τον δεχόμαστε σαν το ελάχιστο κοινό τους πολ/σιο.

Στην περίπτωση, όμως, που οι ακέραιοι $a_1, \ldots, a_n$ είναι διάφοροι του μηδενός, το σύνολο των κοινών πολ/σίων τους περιέχει και φυσικούς αριθμούς (αφού ο ακέραιος $|a_1 a_2 \cdots a_n|$ είναι κοινό τους πολ/σιο). Το σύνολο, λοιπόν, των φυσικών κοινών πολ/σίων τους, σύμφωνα με την αρχή της Καλής Διάταξης, θα έχει ελάχιστο στοιχείο, που το καλούμε "**ελάχιστο κοινό πολ/σιο**" των $a_1, \ldots, a_n$ και θα το συμβολίζουμε

$$m = [a_1, \ldots, a_n]$$

Μπορούμε να δώσουμε τώρα τον επόμενο ορισμό για το ε.κ.π μη-μηδενικών ακεραίων.

Ορισμός

Το ελάχιστο κοινό πολλαπλάσιο των μη-μηδενικών ακεραίων $a_1, \ldots, a_n$ είναι ένας φυσικός αριθμός m τέτοιος ώστε

i) $a_1 | m, a_2 | m, \ldots, a_n | m$

ii) Αν $a_1 | l, a_2 | l, \ldots, a_n | l$ και $l \in \mathbb{N}$, τότε $m \leq l$.

Θεώρημα 8.1

Έστω $a_1, a_2, \ldots, a_n$ δοθέντες μη-μηδενικοί ακέραιοι. Ο φυσικός αριθμός m είναι το ε.κ.π των $a_1, \ldots a_n$, δηλ. $m = [a_1, \ldots, a_n]$, εάν και μόνο εάν

1) $a_1 | m, \ldots, a_n | m$

2) Αν $a_1 | l, \ldots, a_n | l$, τότε $m | l$.

Απόδειξη.

Αν $m=[a_1,\dots,a_n]$, τότε αρκεί να δείξουμε μόνο το 2). Από την ευκλείδια διαίρεση παίρνουμε

$$l = mq + r \quad , \quad 0 \le r < m.$$

Αφού $a_1|m, \dots, a_n|m$, θα είναι $a_1|mq, \dots, a_n|mq$ και επειδή $a_1|l, \dots, a_n|l$, θα έχουμε

$a_1|l-mq, \dots, a_n|l-mq$, δηλ $a_1|r, \dots, a_n|r$.

Ο $r=0$ αφού $m=[a_1,\dots,a_n]$. Έτσι $l=mq$, δηλ $m|l$.

Για το αντίστροφο παρατηρούμε ότι, αν $m|l$ και $l \in \mathbb{N}$, τότε $m \le l$. ∎

Θεώρημα 8.2

Για ακεραίους $a_1,\dots,a_n$, λ ισχύουν:

1) $[a_1,\dots,a_n] = [|a_1|,\dots,|a_n|]$

2) $[\lambda a_1,\dots,\lambda a_n] = |\lambda|\,[a_1,\dots,a_n]$

3) Αν $[a_1,\dots,a_n]=m\neq 0$ τότε $\left(\frac{m}{a_1},\dots,\frac{m}{a_n}\right)=1$.

Απόδειξη.

1) Αν κάποιος από τους $a_1,\dots,a_n$ είναι μηδέν, τότε

$[a_1,\dots,a_n]=0=[|a_1|,\dots,|a_n|]$.

Αν όλοι είναι διάφοροι του μηδενός και παίρνουμε $m=[a_1,\dots,a_n]$ και $m'=[|a_1|,\dots,|a_n|]$, τότε εύκολα συμπεραίνουμε ότι $m|m'$ και $m'|m$, συνεπώς $m=m'$.

2) Αν $\lambda=0$ τότε και τα δυο μέρη της αποδεικτέας ισότητας μηδενίζονται. Όμοια συμβαίνει και αν κάποιος από τους $a_1,\dots,a_n$ είναι μηδενικός. Υποθέτουμε ότι οι ακέραιοι $a_1,\dots,a_n,\lambda$ είναι διάφοροι του μηδενός. Παρατηρούμε ότι, αν ο A είναι ένα κοινό πολλαπλάσιο των $\lambda a_1,\dots,\lambda a_n$, δηλ, αν

α) $A=(\lambda a_1)\mu_1 = \dots = (\lambda a_n)\mu_n$, τότε

$A=\lambda A'$, όπου

β) $A'=a_1\mu_1 = \dots = a_n\mu_n$

δηλ το A είναι λ-πλάσιο ενός κοινού πολλαπλασίου A' των $a_1,\dots,a_n$ και αντίστροφα, αν έχουμε τη β), δηλ. ένα κοινό πολλαπλάσιο A' των $a_1,\dots,a_n$, τότε κάθε λ-πλάσιο του $A=\lambda A'$ είναι ένα κοινό πολλαπλάσιο των $\lambda a_1,\dots,\lambda a_n$ από την α).

Έτσι, το σύνολο των κοινών πολλαπλασίων των $\lambda a_1,\dots,\lambda a_n$ ταυτίζεται με το σύνολο των λ-πλασίων των κοινών πολλαπλασίων των $a_1,\dots a_n$, και, επειδή τα σύνολα αυτά ταυτίζονται αντίστοιχα με τα σύνολα των αντιθέτων των στοιχείων τους, ο ελάχιστος φυσικός $m=[\lambda a_1,\dots,\lambda a_n]$ του πρώτου συνόλου είναι το $|\lambda|$-πλάσιο του ελαχίστου φυσικού $m'=[a_1,\dots,a_n]$ του δεύτερου.

3). Αν $d=\left(\frac{m}{a_1},\dots,\frac{m}{a_n}\right)$ τότε $d\left|\frac{m}{a_1},\dots,d\right|\frac{m}{a_n}$.

Αν λοιπόν $\frac{m}{a_1}=dc_1,\dots,\frac{m}{a_n}=dc_n$ $\quad c_1,\dots,c_n\in\mathbb{Z}$,

τότε

$m=da_1c_1=\dots=da_nc_n$, δηλ $da_1|m,\dots,da_n|m$

Επομένως

$[da_1,\dots,da_n]\,|\,m$, δηλ $d\,m\,|\,m$, οπότε $dm\in m$.

Έτσι $d\in 1$ και, επειδή $d\in\mathbb{N}$, αναγκαστικά $d=1$. ∎

Έτσι για παράδειγμα

1) $[-13,-39,-154]=[13,39,154]$

2) $[10\cdot3,\ 10\cdot27,\ 10\cdot62]=10\,[3,27,62]$

3) $[12,30,40]=120$, οπότε $\left(\frac{120}{12},\frac{120}{30},\frac{120}{40}\right)=(10,4,3)=1$.

Θεώρημα 8.3

Για αμεραίους $a_1,\dots,a_n$, $(n>2)$ ισχύει

$$[a_1,\dots,a_n]=[a_1,\dots,a_k,[a_{k+1},\dots,a_n]]$$

για κάθε k $1\le k\le n-2$.

Απόδειξη

Αν κάποιος από τους $a_1,\dots,a_n$ είναι μηδενικός και τα δυο μέλη της αποδεικτέας ισότητας μηδενίζονται.

Αν οι $a_1,\dots,a_n$ είναι διάφοροι του μηδενός και υποθέσουμε $m=[a_1,\dots,a_n]$ και $m'=[a_1,\dots,a_k,[a_{k+1},\dots,a_n]]$, τότε εύκολα δείχνουμε ότι $m\mid m'$ και $m'\mid m$, οπότε $m=m'$. ■

Από το προηγούμενο θεώρημα συμπεραίνουμε <u>ότι το ε.κ.π των ακέραιων αριθμών $a_1,\dots,a_n$ δεν μεταβάλλεται, αν ορισμένοι απ'αυτούς αντικατασταθούν με το ε.κ.π τους</u>. Έτσι

$$[12,54,108,45]=[[12,54],108,45]=[12,54,[108,45]].$$

Θεώρημα 8.4

Αν οι ακέραιοι αριθμοί $a_1,\dots,a_n$ είναι πρώτοι μεταξύ τους ανά δύο, τότε

$$[a_1,\dots,a_n]=|a_1\cdots a_n|$$

Απόδειξη

Αν ένας τουλάχιστον από τους $a_1,\dots,a_n$ είναι μηδενικός, τότε $[a_1,\dots,a_n]=0=|a_1\cdots a_n|$.

Αν όλοι τους είναι διάφοροι του μηδενός, τότε

$$\left.\begin{array}{l} a_1\mid|a_1\cdots a_n| \\ \vdots \\ a_n\mid|a_1\cdots a_n| \end{array}\right\}\Rightarrow [a_1,\dots,a_n]\,\Big|\,|a_1\cdots a_n| \qquad (\text{θεωρ. 8.1})$$

Απ'την άλλη μεριά, αφού οι $a_1,\dots,a_n$ είναι πρώτοι μεταξύ τους ανά δύο, και $a_1\mid m,\dots,a_n\mid m$ (όπου $m=[a_1,\dots,a_n]$) από το Πόρισμα 6.11, παίρνουμε ότι $a_1\cdots a_n\mid m$, επομένως $|a_1\cdots a_n|\,\big|\,[a_1,\dots,a_n]$

Τελικά, λοιπόν, $[a_1,\dots,a_n]=|a_1\cdots a_n|$. ■

Έτσι για δυο ακέραιους a, b ισχύει

$$(a,b)=1 \Rightarrow [a,b]=|ab|.$$

Δεν υπάρχει αλγόριθμος για την εύρεση του ε.κ.π δυο ακεραίων, αντίστοιχος με τον Ευκλείδιο αλγόριθμο για την εύρεση του μ.κ.δ, αλλά μια σχέση μεταξύ τους που μάς επιτρέπει άνετα να υπολογίζουμε το ε.κ.π.

Θεώρημα 8.5

Για μή-μηδενικούς ακεραίους a, b ισχύει

$$[a,b]\cdot(a,b)=|ab|.$$

Απόδειξη.

Αν $d=(a,b)$, τότε $d|a$ και $d|b$ οπότε $d||ab|$. Θα δείξουμε ότι ο φυσικός αριθμός

$$m=\frac{|ab|}{(a,b)}$$

είναι το $[a,b]$.

Σύμφωνα με το θεώρημα 8.1 αρκεί να δείξουμε

1) $a\left|\frac{|ab|}{d}\right.$, $b\left|\frac{|ab|}{d}\right.$

2) Αν $a|\ell$, $b|\ell$, τότε $\frac{|ab|}{d}\left|\ell\right.$.

Αφού $d||a|$ και $d||b|$ οι αριθμοί $\frac{|a|}{d}$ και $\frac{|b|}{d}$ είναι ακέραιοι. Επομένως

$$a\left||a|\cdot\frac{|b|}{d}\right. \quad \text{και} \quad b\left||b|\frac{|a|}{d}\right. ,$$

Μένει να δείξουμε το 2). Αρκεί να δείξουμε ότι ο αριθμός

$$\frac{\ell}{\frac{|ab|}{d}}=\frac{\ell d}{|ab|}$$ είναι ακέραιος. Υπάρχουν ακέραιοι τώρα x, y έτσι ώστε $d=ax+by$. επομένως αρκεί να δείξουμε ότι ο αριθμός $\frac{\ell(ax+by)}{|ab|}=\frac{\ell ax}{|ab|}+\frac{\ell by}{|ab|}$ είναι ακέραιος.

Επειδή $|a|\,|a$ και $|b|\,|l \Rightarrow |ab|\,|al$ και επομένως $|ab|\,|alx$.
Ο αριθμός δηλαδή $\frac{alx}{|ab|}$ είναι ακέραιος. Όμοια δείχνουμε
ότι και ο αριθμός $\frac{bly}{|ab|}$ είναι ακέραιος. Συνεπώς, ο $\frac{ld}{|ab|}$ σαν
άθροισμα ακεραίων είναι ακέραιος, έτσι $[a,b](a,b)=|ab|$. ■

Για παράδειγμα $[12,30]=\frac{360}{(12,30)}=\frac{360}{3}=120$.

Πόρισμα 8.1

Αν για τους φυσικούς αριθμούς a,b έχουμε

$$a=p_1^{\alpha_1}\cdots p_\kappa^{\alpha_\kappa},\ \alpha_i\geq 0 \text{ και } b=p_1^{\beta_1}\cdots p_\kappa^{\beta_\kappa},\ \beta_i\geq 0,$$

τότε

$$[a,b]=p_1^{\delta_1}\cdots p_\kappa^{\delta_\kappa}, \text{ με } \delta_i=\max\{\alpha_i,\beta_i\},\ i=1,\dots,\kappa.$$

Απόδειξη.

Είναι $[a,b]\cdot(a,b)=ab$, επομένως $[a,b]=\frac{ab}{(a,b)}$.

Έτσι

$$[a,b]=\frac{p_1^{\alpha_1+\beta_1}\cdots p_\kappa^{\alpha_\kappa+\beta_\kappa}}{p_1^{\gamma_1}\cdots p_\kappa^{\gamma_\kappa}},\quad \text{όπου } \gamma_i=\min\{\alpha_i,\beta_i\}$$

και επειδή $\alpha_i+\beta_i=\min\{\alpha_i,\beta_i\}+\max\{\alpha_i,\beta_i\}$ $i=1,\dots,\kappa$

θα είναι

$$[a,b]=p_1^{\delta_1}\cdots p_\kappa^{\delta_\kappa},\ \text{όπου}\ \delta_i=\max\{\alpha_i,\beta_i\},\ i=1,\dots,\kappa.$$

■

Για παράδειγμα,

$$[2\cdot 3^4\cdot 11^{22},\ 2^9\cdot 3^5\cdot 11^7]=2\cdot 3^5\cdot 11^{22}.$$

Γενικότερα έχουμε.

Θεώρημα 8.6

Για φυσικούς αριθμούς $a_1, \ldots, a_\kappa$, $(\kappa > 2)$ αν

$$a_j = \prod_{i=1}^{r} p_i^{\alpha_{ji}} \quad , \ \alpha_{ji} \geq 0 \qquad (j = 1, 2, \ldots, \kappa)$$

τότε

$$[a_1, \ldots, a_\kappa] = \prod_{i=1}^{r} p_i^{\delta_i}$$

με $\delta_i = \max(\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{\kappa i})$, $(i = 1, 2, \ldots, r)$

Απόδειξη.

Έχουμε $a_1 = p_1^{\alpha_{11}} \ldots p_r^{\alpha_{1r}}$

$a_2 = p_1^{\alpha_{21}} \ldots p_r^{\alpha_{2r}}$

$\vdots$

$a_\kappa = p_1^{\alpha_{\kappa 1}} \ldots p_r^{\alpha_{\kappa r}}$

Παρατηρούμε ότι ο φυσικός $m = p_1^{\delta_1} \cdots p_r^{\delta_r}$, με

$$\left.\begin{aligned} \delta_1 &= \max\{\alpha_{11}, \alpha_{21}, \ldots, \alpha_{\kappa 1}\} \\ \delta_2 &= \max\{\alpha_{12}, \alpha_{22}, \ldots, \alpha_{\kappa 2}\} \\ &\vdots \\ \delta_r &= \max\{\alpha_{1r}, \alpha_{2r}, \ldots, \alpha_{\kappa r}\} \end{aligned}\right\} \qquad (10)$$

είναι κοινό πολλαπλάσιο των $a_1, \ldots, a_\kappa$ δηλ. $a_1 | m, \ldots, a_\kappa | m$,

αφού από την (10) έχουμε

$\alpha_{j1} \leq \delta_1, \ \ldots, \ \alpha_{jr} \leq \delta_r \qquad (j = 1, \ldots, \kappa)$,

δηλ. $0 \leq \alpha_{ji} \leq \delta_i \qquad (i = 1, \ldots, r, \ j = 1, \ldots, \kappa)$.

Μένει να δείξουμε ότι, αν $l \in \mathbb{N}$ και $a_1 | l, \ldots, a_\kappa | l$, τότε $m \leq l$. Πραγματικά, αν

$$l = p_1^{\lambda_1} \cdot p_2^{\lambda_2} \ldots p_r^{\lambda_r} \cdot p_{r+1}^{\lambda_{r+1}} \ldots p_\mu^{\lambda_\mu} ,$$

έχουμε

$a_1 | l \Rightarrow \alpha_{11} \leq \lambda_1, \ \ldots, \ \alpha_{1r} \leq \lambda_r$

$\vdots$

$a_\kappa | l \Rightarrow \alpha_{\kappa 1} \leq \lambda_1, \ \ldots, \ \alpha_{\kappa r} \leq \lambda_r$,

δηλ. $0 \le \delta_1 = \max\{\alpha_{11}, \dots, \alpha_{k1}\} \le \lambda_1$

$\vdots$

$0 \le \delta_r = \max\{\alpha_{1r}, \dots, \alpha_{kr}\} \le \lambda_r$,

συνεπώς $m \mid \ell$, δηλ $m \le \ell$, πράγμα που επιδιώκουμε. ■

Για παράδειγμα,

$[2^1 \cdot 3^3 5^4,\ 2^0 \cdot 3^5 \cdot 5^2,\ 2^3 \cdot 3^2 \cdot 5] = 2^3 \cdot 3^6 \cdot 5^4$.

Από το προηγούμενο θεώρημα και το θεώρημα 6.5 συμπεραίνουμε ότι για περισσότερους από δύο ακεραίους, δεν ισχύει γενικά, ανάλογη σχέση με την $[a,b](a,b) = |ab|$, δηλ. γενικά $[a_1, \dots, a_n](a_1, \dots, a_n) \ne |a_1 \cdots a_n|$.

Ας δούμε, όμως, ποια σχέση έχουμε στην περίπτωση που οι ακέραιοι είναι περισσότεροι από δύο.

Θεώρημα 8.7

Αν $\lambda_1 a_1 = \lambda_2 a_2 = \dots = \lambda_n a_n = \ell \ne 0$, δηλ αν ο ℓ είναι ένα μη-μηδενικό κοινό πολλαπλάσιο των ακεραίων $a_1, \dots, a_n$, τότε

$$|\ell| = (\lambda_1, \dots, \lambda_n)\,[a_1, \dots, a_n] .$$

Απόδειξη.

Αν $m = [a_1, \dots, a_n]$, τότε

$m = \mu_1 a_1 = \mu_2 a_2 = \dots = \mu_n a_n$, με $(\mu_1, \dots, \mu_n) = 1$,
σύμφωνα με το θεώρημα 8.2, 3).

Αφού, όμως, $a_1 \mid \ell, \dots, a_n \mid \ell$, θα έχουμε $m \mid \ell$, και έστω ότι

$$\ell = k \cdot m , \quad \text{οπότε} \quad |\ell| = |k| m .$$

Μένει να δείξουμε ότι $|k| = (\lambda_1, \dots, \lambda_n)$.

Είναι $\ell = km = k\mu_1 a_1 = \dots = k\mu_n a_n$ και από την υπόθεσή μας $\ell = \lambda_1 a_1 = \dots = \lambda_n a_n$.

Επειδή οι $a_1,\dots,a_n$ είναι μη-μηδενικοί, διαφορετικά $\ell=0$, παίρνουμε

$\lambda_1=k\mu_1,\ \dots,\ \lambda_n=k\mu_n$. Έτσι

$(\lambda_1,\dots,\lambda_n)=(k\mu_1,\dots,k\mu_n)=|k|\,(\mu_1,\dots,\mu_n)=|k|\cdot 1=|k|$

πράγμα που επιδιώκουμε. ■

Πόρισμα 8.2.

Αν $\lambda_1 a_1=\lambda_2 a_2=\dots=\lambda_n a_n=\ell\neq 0$ και $(\lambda_1,\dots,\lambda_n)=1$, τότε

$$[a_1,\dots,a_n]=|\ell|\ .\ \blacksquare$$

Θεωρούμε τους μη-μηδενικούς ακεραίους, $a_1,\dots,a_n$. Το σύνολο S_k των ανά κ γινομένων τους, περιέχει $\binom{n}{k}$ σε πλήθος στοιχεία. Αν συμβολίσουμε (S_k) και $[S_k]$ τον μ.κ.δ και το ε.κ.π των στοιχείων του συνόλου S_k, αντίστοιχα, και με τη συμφωνία ότι $(S_0)=1=[S_0]$, έχουμε το παρακάτω πόρισμα.

Πόρισμα 8.2

Για μη-μηδενικούς ακεραίους $a_1,\dots,a_n$ ισχύει

$$(S_k)\cdot[S_{n-k}]=|a_1a_2\cdots a_n|\ ,\ (k=0,1,\dots,n)$$

Απόδειξη.

Σε κάθε ανά κ γινόμενο π.χ $a_1\cdots a_k=\lambda$ αντιστοιχεί ένα συμπληρωματικό ανά η-κ γινόμενο $a_{k+1}\cdots a_n=b$, με $\lambda b=a_1\cdots a_n$. Είναι εύκολο να δούμε ότι η αντιστοιχία αυτή είναι μια αμφίεση του συνόλου S_k στο σύνολο S_{n-k}, έτσι ώστε, αν $\binom{n}{k}=v$ και $S_k=\{\lambda_1,\dots,\lambda_v\}$, $S_{n-k}=\{b_1,\dots,b_v\}$, να έχουμε

$\lambda_1 b_1=\dots=\lambda_v b_v=a_1\cdots a_n\neq 0$, οπότε, σύμφωνα με το θεώρημα 8.7,

$(\lambda_1, \dots, \lambda_v)\,[b_1, \dots, b_v] = |a_1 \cdots a_n|$, δηλ

$$(S_k)\,[S_{n-k}] = |a_1 \cdots a_n| \quad \blacksquare$$

Για παράδειγμα, αν $a, b, c \in \mathbb{Z} - \{0\}$ τότε έχουμε

i) $(a, b, c)\,[ab, ac, bc] = |abc|$

ii) $(ab, ac, bc)\,[a, b, c] = |abc|$.

Και εδώ η εύρεση του ε.κ.π των ακεραίων $a_1, \dots, a_n$, $(n > 2)$ είναι υπόθεση ρουτίνας. Έτσι, αν συμβολίσουμε

$$m_1 = [a_1, a_2]\,,\ m_2 = [m_1, a_3]\,,\ \dots,\ m_{n-1} = [m_{n-2}, a_n]$$

έχουμε

$$[a_1, a_2, \dots, a_n] = m_{n-1}\,.$$

Πραγματικά, σύμφωνα με το θεώρημα 8.3, έχουμε

$$[a_1, a_2, \dots, a_n] = [[a_1, a_2], a_3, \dots, a_n] = [m_1, a_3, \dots, a_n]$$

$$= [[m_1, a_3], \dots, a_n] = [m_2, \dots a_n]$$

$$\vdots$$

$$= [m_{n-2}, a_n] = m_{n-1}\,.$$

Για παράδειγμα.

$$[12, 30, 40, 240] = [[12, 30], 40, 240] = [60, 40, 240] =$$

$$= [[60, 40], 240] = [120, 240] = 240\,.$$

9. Η Διοφαντική εξίσωση $ax + by = c$.

Η ονομασία Διοφαντική ανάλυση είναι εκείνο το μέρος της θεωρίας Αριθμών που ασχολείται με εξισώσεις που έχουν ακέραιους συντελεστές και μπορούν να επιλυθούν μέσα στο σύνολο $\mathbb{Z}$ των ακεραίων. Τέτοιες εξισώσεις ονομάζονται Διοφαντικές εξισώσεις και η ονομασία τους

προέρχεται από το όνομα του Διόφαντου

Αν και παρα πολλοί ερευνητές μέχρι και σήμερα ασχολήθηκαν και ασχολούνται με τη Διοφαντική Ανάλυση, πολλά ερωτήματα σχετικά με τις Διοφαντικές εξισώσεις, παραμένουν ακόμη ανοικτά και αφορούν

i) Την ύπαρξη μιας τουλάχιστον ακέραιας λύσης της εξίσωσης

ii) Το πλήθος των ακέραιων λύσεων (πεπερασμένο ή άπειρο) της εξίσωσης

iii) Την εύρεση όλων των ακέραιων λύσεων της εξίσωσης.

Γεωμετρικά το σύνολο των ακέραιων λύσεων μιας Διοφαντικής εξίσωσης, π.χ της $f(x,y)=0$, είναι το σύνολο όλων εκείνων των σημείων (x,y) της καμπύλης $f(x,y)=0$ για τα οποία $x,y\in\mathbb{Z}$.

Για παράδειγμα, η εξίσωση $x^3+y^3+z^3=4$ δεν έχει ακέραιες λύσεις, ενώ η εξίσωση $x^3+y^3+z^3=2$ έχει άπειρες σε πλήθος ακέραιες λύσεις, π.χ τις $(x,y,z)=(1+6\eta^3,\ 1-6\eta^3,\ -6\eta^2)$ $\eta\in\mathbb{N}$.
αυτά δεν είναι γνωστό, αν αυτές είναι όλες οι ακέραιες λύσεις της.

Εδώ θα ασχοληθούμε με την <u>γραμμική Διοφαντική εξίσωση με δυό αγνώστους</u>

$$ax+by=c \quad , \quad a,b,c\in\mathbb{Z}.$$

Το ζεύγος των ακεραίων (x_0,y_0) λέγεται **λύση** της, αν

$$ax_0+by_0=c.$$

Το πρόβλημά μας είναι η εύρεση όλων των ακεραίων λύσεών της (αν υπάρχουν) που γεωμετρικά αντιστοιχεί στην εύρεση όλων των σημείων (x,y) επί της ευθείας γραμμής $ax+by=c$, για τα οποία $x,y\in\mathbb{Z}$.

Θεώρημα 9.1

Η γραμμική Διοφαντική εξίσωση

$$ax+by=c \qquad a,b,c\in\mathbb{Z} \qquad (*)$$

έχει μία τουλάχιστον λύση, εάν και μόνο εάν $d|c$, όπου $d=(a,b)$. Αν (x_0,y_0) είναι μια τυχούσα λύση της, τότε όλες οι λύσεις της δίνονται από τις σχέσεις,

$$x=x_0+\frac{b}{d}t \ , \ y=y_0-\frac{a}{d}t \quad , \ t\in\mathbb{Z}.$$

Απόδειξη.

Αν το ζεύγος των ακεραίων (x_0, y_0) είναι λύση της (*), τότε $ax_0+by_0=c$.
Αφού $d=(a,b)$ θα έχουμε $a=da'$ και $b=db'$, οπότε
$c=ax_0+by_0=d(a'x_0+b'y_0)$, δηλ $d|c$.
Αντίστροφα, υποθέτουμε ότι $d|c$ οπότε $c=dc'$. Αφού $d=(a,b)$, θα υπάρχουν ακέραιοι x_0, y_0, έτσι ώστε $d=ax_0+by_0$. Επομένως,
$c=dc'=(ax_0+by_0)c'=a(x_0c')+b(y_0c')$ που σημαίνει ότι η (*) έχει την ακέραια λύση $x=x_0c'$, $y=y_0c'$.

Αν τώρα (x', y') είναι μια τυχούσα ακέραια λύση της (*), τότε

$$ax_0+by_0=c=ax'+by',$$

συνεπώς

$$a(x'-x_0)=b(y_0-y') \qquad (11)$$

Αφού $d=(a,b)$, θα έχουμε $a=da'$ κ $b=db'$, όπου $(a',b')=1$ και με αντικατάσταση στην (11) παίρνουμε

$$a'(x'-x_0)=b'(y_0-y') \qquad (12)$$

Από την (12) έχουμε $a' \mid b'(y_0-y')$ και επειδή $(a',b')=1$, θα είναι $a' \mid y_0-y'$, σύμφωνα με το θεώρημα 6.7.
Έτσι $y_0-y'=a't$, για κάποιο ακέραιο t, δηλ

$$y'=y_0-a't=y_0-\frac{a}{d}t$$

και αντικαθιστώντας στην (12), παίρνουμε $x'-x_0=b't$, δηλ

$$x'=x_0+\frac{b}{d}t.$$

Η απόδειξή μας τελειώνει αν δείξουμε ότι, για κάθε $t\in\mathbb{Z}$, οι ακέραιοι $x=x_0+\frac{b}{d}t$ και $y=y_0-\frac{a}{d}t$ είναι λύσεις της (*). Πραγματικά,

$$ax+by=a\left(x_0+\frac{b}{d}t\right)+b\left(y_0-\frac{a}{d}t\right)=$$

$$=ax_0+by_0+\left(\frac{ab}{d}t-\frac{ab}{d}t\right)$$

$$=ax_0+by_0=c. \quad \blacksquare$$

Πόρισμα 9.1.

Αν $(a,b)=1$ και οι ακέραιοι x_0, y_0 είναι μια λύση της γραμμικής Διοφαντικής εξίσωσης $ax+by=c$, $a,b,c \in \mathbb{Z}$, τότε όλες οι λύσεις της δίνονται από τις σχέσεις

$$x=x_0+bt \quad , \quad y=y_0-at \quad , \quad t\in\mathbb{Z} . \blacksquare$$

Αν η εξίσωση (*) έχει λύσεις, τότε μια τυχούσα λύση της βρίσκεται από τον Αλγόριθμο του Ευκλείδη, για την εύρεση του $d=(a,b)$. Βρίσκουμε έτσι ζεύγος ακεραίων (x_0,y_0) τέτοιο ώστε $d=ax_0+by_0$.

Αφού $d|c$, θα είναι $c=dc'$, οπότε το ζεύγος των ακεραίων $x'=x_0c'$, $y'=y_0c'$ είναι μια λύση της (*)

Παράδειγμα 9.1

Θα βρούμε τις ακέραιες λύσεις της Γραμμικής Διοφαντικής Εξίσωσης

$$1985x+132y=5 .$$

Από το παράδειγμα 7.1, έχουμε $(1985, 132)=1$, επομένως η εξίσωση έχει λύση. Επειδή

$$1=1985\cdot(53)+132(-797)$$

θα είναι $5\cdot 1=1985\cdot(265)+132(-3985)$

Έτσι μια λύση της είναι η $x_0=265$, $y_0=-3985$.

Όλες οι λύσεις της επομένως, δίνονται από τις σχέσεις,

$$x'=265+132t \quad , \quad y'=-3985-1985t \quad , \quad t\in\mathbb{Z}.$$

Πόρισμα 9.2

Αν οι φυσικοί αριθμοί a, b είναι πρώτοι μεταξύ τους, δηλ $(a,b)=1$ τότε υπάρχουν φυσικοί αριθμοί u και v έτσι ώστε

$$au-bv=1 .$$

Απόδειξη.

Αφού $(a,b)=1$, υπάρχουν ακέραιοι x_0, y_0, έτσι ώστε $ax_0+by_0=1$. Όλες οι λύσεις της διοφ. εξίσωσης $ax+by=1$ δίνονται από τις σχέσεις $x=x_0+bt$, $y=y_0-at$, $t\in\mathbb{Z}$. Επιλέγοντας ακέραιο t_0 μ[illegible] $t_0>-\frac{x_0}{b}$, $t_0>\frac{y_0}{a}$, οι ακέραιοι $u=x_0+bt_0>0$, $v=-(y_0-at_0)>0$ είναι τέτοιοι ώστε $au-bv=ax_0+by_0=1$. $\blacksquare$

ΚΕΦΑΛΑΙΟ ΙΙΙ

ΑΡΙΘΜΗΤΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ

1. Το μονοειδές $\mathcal{A}$ των αριθμητικών συναρτήσεων

Ορισμός

Μια αριθμητική (ή αριθμοθεωρητική) συνάρτηση είναι μια συνάρτηση

$$a : \mathbb{N} \longrightarrow \mathbb{C}$$

με πεδίο ορισμού το σύνολο $\mathbb{N}$ των φυσικών αριθμών και πεδίο τιμών το σύνολο $\mathbb{C}$ των μιγαδικών αριθμών.

Για παράδειγμα, οι παρακάτω συναρτήσεις

α) $f(n) = e^{in}$, για κάθε $n \in \mathbb{N}$

β) Αν $\kappa \in \mathbb{Z}$, $g(n) = n^{\kappa}$, για κάθε $n \in \mathbb{N}$

γ) $h(n) = n!$ για κάθε $n \in \mathbb{N}$

είναι αριθμητικές.

Γενικά δεν μας δίνουν όλες οι αριθμητικές συναρτήσεις ενδιαφέροντα αποτελέσματα στη Θεωρία Αριθμών. Αυτές οι πιο σημαντικές, όπως θα διαπιστώσουμε στα επόμενα, είναι οι παρακάτω:

1. Η συνάρτηση $\tau : \mathbb{N} \longrightarrow \mathbb{N}$, $n \longmapsto \tau(n)$

   όπου $\tau(n)$ παριστάνει το πλήθος των φυσικών διαιρετών του φυσικού αριθμού n.

2. Η συνάρτηση $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$, $n \longmapsto \sigma(n)$

   όπου $\sigma(n)$ παριστάνει το άθροισμα των φυσικών διαιρετών του φυσικού αριθμού n.

3. Η συνάρτηση του Euler, $\varphi : \mathbb{N} \to \mathbb{N}$, $n \mapsto \varphi(n)$
όπου $\varphi(n)$ παριστάνει το πλήθος των φυσικών αριθμών που είναι μικρότεροι ή ίσοι με τον n και πρώτοι με τον n. (το $\varphi(n)$ είναι δηλ. το πλήθος των φυσικών αριθμών k με $1 \le k \le n$ και $(k,n)=1$).

4. Η συνάρτηση του Möbius $\mu : \mathbb{N} \to \{0,1,-1\}$ που ορίζεται ως εξής:

$$\mu(n) = \begin{cases} 1 & \text{αν } n=1 \\ 0 & \text{αν } \exists \text{ πρώτος } p \text{ , με } p^2 \mid n \\ (-1)^k & \text{αν } n = p_1 \cdots p_k \text{ και οι πρώτοι } p_1, \ldots, p_k \text{ είναι διαφορετικοί. (άνισοι ανά δύο).} \end{cases}$$

Με άλλα λόγια, αν $n>1$ και $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ είναι η πρωτογενής μορφή του, τότε $\mu(n)=0$ αν ένας τουλάχιστον από τους εκθέτες $\alpha_i \ge 2$ και $\mu(n)=(-1)^k$ αν $n = p_1 \cdots p_k$.

Για παράδειγμα, αν $n=12$, τότε οι φυσικοί που διαιρέτες είναι οι $1,2,3,4,6,12$, συνεπώς

$$\tau(12)=6 \quad \text{και} \quad \sigma(12)=1+2+3+4+6+12=28.$$

Παρατηρούμε ότι οι φυσικοί αριθμοί k, $1 \le k \le 12$ με $(k,12)=1$ είναι οι $1,5,7,11$, οπότε $\varphi(12)=4$.
Τέλος η πρωτογενής μορφή του 12 είναι η $12 = 2^2 \cdot 3$ επομένως $\mu(12)=0$.

5. Η συνάρτηση $\gamma : \mathbb{N} \to \mathbb{N}$, $n \mapsto \gamma(n)$
όπου $\gamma(n)$ παριστάνει το γινόμενο των φυσικών διαιρετών του φυσικού αριθμού n.

Για παράδειγμα $\gamma(12) = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 \cdot 12 = 1728$.

Θεώρημα 1.1

Το γινόμενο $\gamma(n)$ των φυσικών διαιρετών του φυσικού αριθμού n εκφράζεται από τον τύπο.

$$\gamma(n) = n^{\tau(n)/2}$$

Απόδειξη.

Παρατηρούμε ότι $d|n \iff \frac{n}{d}|n$. Έτσι δυο διαφορετικοί διαιρέτες d_1, d_2 του n ορίζουν δυο διαφορετικούς διαιρέτες $\frac{n}{d_1}, \frac{n}{d_2}$ του n.

Αν λοιπόν $d_1, d_2, \dots, d_{\tau(n)}$ είναι όλοι οι φυσικοί διαιρέτες του n, τότε και οι

$$\frac{n}{d_1}, \frac{n}{d_2}, \dots, \frac{n}{d_{\tau(n)}}$$

είναι όλοι οι φυσικοί διαιρέτες του n. Συνεπώς

$$\gamma(n) = d_1 \cdot d_2 \cdots d_{\tau(n)} = \frac{n}{d_1} \cdot \frac{n}{d_2} \cdots \frac{n}{d_{\tau(n)}} = \frac{n^{\tau(n)}}{\gamma(n)}$$

δηλ.

$$\gamma(n)^2 = n^{\tau(n)}, \quad \text{οπότε} \quad \gamma(n) = n^{\tau(n)/2}. \blacksquare$$

Για παράδειγμα $\gamma(12) = 12^{\tau(12)/2} = 12^{6/2} = 12^3 = 1728$.

Ας είναι τώρα $f: \mathbb{N} \longrightarrow \mathbb{C}$ μια αριθμητική συνάρτηση. Στο εξής θα συμβολίζουμε με

$$\sum_{d|n} f(d)$$

το άθροισμα όλων των τιμών $f(d)$ που παίρνονται όταν ο d διατρέχει όλους τους φυσικούς διαιρέτες του n.

Αν λοιπόν $d_1, d_2, \dots, d_{\tau(n)}$ είναι όλοι οι φυσικοί διαιρέτες του n, τότε

$$\sum_{d|n} f(d) = f(d_1) + f(d_2) + \cdots + f(d_{\tau(n)}).$$

Επειδή όμως και οι $\frac{n}{d_1}, \frac{n}{d_2}, \ldots, \frac{n}{d_{\tau(n)}}$ είναι όλοι οι φυσικοί διαιρέτες του n, θα έχουμε

$$\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right) \qquad (1)$$

Πραγματικά,

$$\sum_{d|n} f\left(\frac{n}{d}\right) = f\left(\frac{n}{d_1}\right) + \cdots + f\left(\frac{n}{d_{\tau(n)}}\right) = f(d_1) + \cdots + f(d_{\tau(n)}) =$$

$$= \sum_{d|n} f(d) .$$

Για παράδειγμα, οι φυσικοί διαιρέτες του 18 είναι οι

$$1, 2, 3, 6, 9, 18 .$$

Αλλά τότε και οι

$$\frac{18}{1}=18, \ \frac{18}{2}=9, \ \frac{18}{3}=6, \ \frac{18}{6}=3, \ \frac{18}{9}=2, \ \frac{18}{18}=1$$

είναι όλοι οι φυσικοί διαιρέτες του 18. Έτσι

$$\sum_{d|18} \sigma(d) = \sigma(1)+\sigma(2)+\sigma(3)+\sigma(9)+\sigma(18)$$

$$= \sigma\left(\tfrac{18}{1}\right)+\sigma\left(\tfrac{18}{2}\right)+\sigma\left(\tfrac{18}{3}\right)+\sigma\left(\tfrac{18}{6}\right)+\sigma\left(\tfrac{18}{9}\right)+\sigma\left(\tfrac{18}{18}\right)$$

$$= \sum_{d|18} \sigma\left(\frac{18}{d}\right) .$$

Από την σχέση (1) λοιπόν, ορίζεται μια νέα αριθμητική συνάρτηση

$$F : \mathbb{N} \longrightarrow \mathbb{C}$$

όπου, για κάθε $n \in \mathbb{N}$ είναι $F(n) = \sum_{d|n} f(d)$.

Έτσι $F(1) = \sum_{d|1} f(d) = f(1)$

$F(2) = \sum_{d|2} f(d) = f(1)+f(2)$

$F(3) = \sum_{d|3} f(d) = f(1)+f(3)$

$F(4) = \sum_{d|4} f(d) = f(1)+f(2)+f(4)$

$F(5) = \sum_{d|5} f(d) = f(1)+f(5)$

$\vdots$

Στο εξής θα συμβολίζουμε με $\mathcal{A}$ το σύνολο όλων των αριθμητικών συναρτήσεων.

Ορισμός

Αν f και $g \in \mathcal{A}$, καλούμε <u>ενελικτικό γινόμενο</u> (ή γινόμενο Dirichlet) των f και g και το παριστάνουμε $f*g$, την αριθμητική συνάρτηση

$$f*g : \mathbb{N} \longrightarrow \mathbb{C}$$

που ορίζεται για κάθε $n \in \mathbb{N}$, από τη σχέση:

$$\boxed{(f*g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right)} \qquad (2)$$

όπου το άθροισμα εκτείνεται σε όλους τους φυσικούς διαιρέτες του n.

Πιο αναλυτικά θα έχουμε

$$(f*g)(1) = f(1)g(1)$$
$$(f*g)(2) = f(1)g(2) + f(2)g(1)$$
$$(f*g)(3) = f(1)g(3) + f(3)g(1)$$
$$(f*g)(4) = f(1)g(4) + f(2)g(2) + f(4)g(1)$$
$$(f*g)(5) = f(1)g(5) + f(5)g(1)$$
$$(f*g)(6) = f(1)g(6) + f(2)g(3) + f(3)g(2) + f(6)g(1)$$
$$\vdots$$

Αν τώρα $d_1, \ldots, d_{\tau(n)}$ είναι όλοι οι φυσικοί διαιρέτες του n, τότε και οι $\frac{n}{d_1}, \ldots, \frac{n}{d_{\tau(n)}}$ είναι όλοι οι φυσικοί διαιρέτες του n, συνεπώς

$$(f*g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d) \qquad (3).$$

Είναι σκόπιμο να δώσουμε και την εφόμενη ισοδύναμη μορφή για το ενελικτικό γινόμενο $f*g$, για κάθε $n \in \mathbb{N}$ ισχύει

$$\boxed{(f*g)(n) = \sum_{st=n} f(s)\, g(t)} \qquad (4)$$

όπου το άθροισμα εκτείνεται πάνω σ' όλα τα διατεταγμένα ζεύγη s,t φυσικών αριθμών με γινόμενο $st=\eta$.

Πραγματικά, γνωρίζουμε ότι $d|\eta \iff \frac{\eta}{d}|\eta$. Έτσι, όταν ο d διαιρέσει όλους τους φυσικούς διαιρέτες του η, τα διατεταγμένα ζεύγη $d, \frac{\eta}{d}$ διαιρέσουν όλα τα διαλεταγμένα ζεύγη φυσικών αριθμών με γινόμενο η.

Ορίζεται έτσι μια δυαδική πράξη πάνω στο σύνολο $\mathcal{A}$

$$\cdot : \mathcal{A}\times\mathcal{A} \longrightarrow \mathcal{A} \quad , \quad (f,g) \longmapsto f\cdot g .$$

Στη συνέχεια, θα δείξουμε ότι το σύνολο $\mathcal{A}$ εφοδιασμένο με την παραπάνω πράξη "$\cdot$" δομείται σε αντιμεταθετικό μονοειδές.[1]

Θεώρημα 1.2

Το ενελικτικό γινόμενο αριθμητικών συναρτήσεων είναι προσεταιριστικό, δηλ για κάθε $f,g,h \in \mathcal{A}$ ισχύει

$$f\cdot(g\cdot h) = (f\cdot g)\cdot h$$

Απόδειξη.

Αρκεί να δείξουμε ότι $\big(f\cdot(g\cdot h)\big)(n) = \big((f\cdot g)\cdot h\big)(n)$ για κάθε $n\in\mathbb{N}$.

Πραγματικά,

$$\big(f\cdot(g\cdot h)\big)(n) = \sum_{st=n} f(s)(g\cdot h)(t) = \sum_{st=n} f(s)\Big(\sum_{rp=t} g(r)h(p)\Big)$$

$$= \sum_{srp=n} f(s)g(r)h(p)$$

$$= \sum_{kp=n}\Big(\sum_{sr=k} f(s)g(r)\Big)h(p)$$

---

1) Υπενθυμίζουμε ότι ένα σύνολο M εφοδιασμένο με μια δυαδική πράξη $*: M\times M \longrightarrow M$ τέτοια ώστε

i) $a*(b*c) = (a*b)*c \quad , \forall a,b,c\in M$

ii) $a*b = b*a \quad , \forall a,b\in M$

iii) Υπάρχει συγκεκριμένο στοιχείο $e\in M$ για την πράξη "$*$", δηλ

$$a*e = a = e*a$$

καλείται αντιμεταθετικό μονοειδές.

$$= \sum_{kp=\eta} \big((f\cdot g)(k)\big)\, h(p)$$

$$= \big((f\cdot g)\cdot h\big)(\eta) \quad . \blacksquare$$

Θεώρημα 1.3

Το ενεργητικό γινόμενο αριθμητικών συναρτήσεων είναι αντιμεταθετική πράξη, δηλ., για κάθε $f, g \in \mathcal{A}$, ισχύει

$$f\cdot g = g\cdot f$$

Απόδειξη.

Αρκεί να δείξουμε ότι $(f\cdot g)(n) = (g\cdot f)(n)$ για κάθε $n\in\mathbb{N}$.

Πραγματικά,

$$(f\cdot g)(n) = \sum_{sx=\eta} f(s)g(x) = \sum_{xs=\eta} g(x)f(s) = (g\cdot f)(n) \quad . \blacksquare$$

Το <u>ερώτημα</u> που γεννάται τώρα είναι το εξής:

Υπάρχει αριθμητική συνάρτηση $\varepsilon : \mathbb{N} \longrightarrow \mathbb{C}$ τέτοια ώστε

$$\varepsilon\cdot f = f = f\cdot\varepsilon \quad , \text{ για κάθε } f\in\mathcal{A}$$

ή ισοδύναμα,

$$\varepsilon\cdot f = f \quad , \text{ για κάθε } f\in\mathcal{A};$$

(αφού το ενεργητικό γινόμενο είναι αντιμεταθετική πράξη)

Η απάντηση είναι ναι· και για να την εντοπίσουμε εργαζόμαστε ως εξής: Υποθέτουμε ότι μια τέτοια αριθμητική συνάρτηση ε υπάρχει και βρίσκουμε τις ιδιότητες που πρέπει να έχει.

Για κάθε $f\in\mathcal{A}$ ισχύει:

$$(\varepsilon\cdot f)(n) = f(n) \quad , \text{ για κάθε } n\in\mathbb{N}.$$

Για $n=1$ παίρνουμε $(\varepsilon\cdot f)(1) = f(1)$, δηλ. $\varepsilon(1)f(1) = f(1)$.

Επειδή αυτή η σχέση πιστοποιείται για κάθε $f\in\mathcal{A}$, θα πιστοποιείται ιδιαίτερα όταν $f(1)\neq 0$ (συναρτήσεις $f\in\mathcal{A}$ με $f(1)\neq 0$ υπάρχουν), οπότε

$$\varepsilon(1) = 1 .$$

Για $n=2$ παίρνουμε $(\varepsilon\cdot f)(2)=f(2)$, δηλ

$$\varepsilon(1)f(2)+\varepsilon(2)f(1)=f(2)$$

Επειδή $\varepsilon(1)=1$, η παραπάνω ισότητα ανάγεται στην

$$\varepsilon(2)f(1)=0$$

και επειδή αυτή, με την σειρά της ικανοποιείται για κάθε $f\in\mathcal{A}$ και ιδιαίτερα μ' εκείνες για τις οποίες $f(1)\neq 0$, παίρνουμε

$$\varepsilon(2)=0$$

Συνεχίζουμε τώρα επαγωγικά.

Για κάθε φυσικό $n>2$, υποθέτουμε ότι $\varepsilon(m)=0$ για κάθε m, $2\leq m<n$. Θα δείξουμε ότι και

$$\varepsilon(n)=0.$$

Πραγματικά, έχουμε $(\varepsilon\cdot f)(n)=f(n)$, δηλ.

$$f(n)=\sum_{d|n}\varepsilon(d)f\left(\frac{n}{d}\right)=\varepsilon(1)f(n)+\sum_{\substack{d|n\\ 1<d<n}}\varepsilon(d)f\left(\frac{n}{d}\right)+\varepsilon(n)f(1)$$

και σύμφωνα με την υπόθεση είναι

$$f(n)=\varepsilon(1)f(n)+\varepsilon(n)f(1),\ \text{οπότε}\ \ \varepsilon(n)f(1)=0.$$

Επειδή η παραπάνω σχέση οφείλει να πληρούται για κάθε $f\in\mathcal{A}$, θα έχουμε

$$\varepsilon(n)=0.$$

Έτσι αν η αριθμητική συνάρτηση $\varepsilon:\mathbb{N}\to\mathbb{C}$ είναι ουδέτερο στοιχείο για το ενεργητικό γινόμενο, τότε

$$\varepsilon(n)=\begin{cases}1 & \text{αν } n=1\\ 0 & \text{αν } n>1\end{cases}.$$

Αλλά και αντίστροφα, η παραπάνω αριθμητική συνάρτηση ε παίζει τον ρόλο του ουδέτερου στοιχείου για το ενεργητικό γινόμενο, δηλ για κάθε $f\in\mathcal{A}$ ισχύει

$$\varepsilon\cdot f=f \quad \text{ή ισοδύναμα} \quad (\varepsilon\cdot f)(n)=f(n),\ \text{για κάθε } n\in\mathbb{N}.$$

Πραγματικά

$$(\varepsilon * f)(n) = \sum_{d|n} \varepsilon(d)\, f\left(\frac{n}{d}\right) = \varepsilon(1) f(n) + \sum_{\substack{d|n \\ d>1}} \varepsilon(d)\, f\left(\frac{n}{d}\right) = \text{(}\varepsilon(d)\to 0\text{)}$$

$$= \varepsilon(1) f(n) = f(n) .$$

Δείξαμε, λοιπόν, μ' αυτό τον τρόπο, το επόμενο θεώρημα.

Θεώρημα 1.4.

Το σύνολο $\mathcal{A}$ των αριθμητικών συναρτήσεων εφοδιασμένο με την πράξη ενελικτικό γινόμενο, δομείται σε αντιμεταθετικό μονοειδές, με ουδέτερο στοιχείο την αριθμητική συνάρτηση ε, που ορίζεται ως εξής:

$$\varepsilon(n) = \begin{cases} 1, & \text{αν } n=1 \\ 0, & \text{αν } n>1 . \end{cases} \quad \blacksquare$$

2. Η ομάδα $\mathcal{U}$ των αντιστρέψιμων στοιχείων του μονοειδούς $\mathcal{A}$

Ορισμός

Μία αριθμητική συνάρτηση f καλείται <u>ενελικτικά αντιστρεπτή</u>, όταν υπάρχει αριθμητική συνάρτηση f' τέτοια ώστε

$$f * f' = \varepsilon = f' * f \qquad (5)$$

Η σχέση (5) είναι ισοδύναμη με την

$$f * f' = \varepsilon \qquad (6)$$

αφού το ενελικτικό γινόμενο είναι αντιμεταθετική πράξη.

Τέτοια αριθμητική συνάρτηση f', όταν υπάρχει, είναι <u>μοναδική</u> για την f· θα την καλούμε <u>ενελικτική αντίστροφο</u> της f και θα την συμβολίζουμε f^{-1}

Πραγματικά, αν f'' είναι μια αριθμητική συνάρτηση τέτοια

ώστε $f'\cdot f = \varepsilon = f\cdot f''$ τότε

$$f' = f'\cdot\varepsilon = f'\cdot(f\cdot f'') = (f'\cdot f)\cdot f'' = \varepsilon\cdot f'' = f''\,.$$

Ατυχώς, όμως, δεν είναι όλα τα στοιχεία του μονοειδούς $(\mathcal{A},\cdot)$ αντιστρεπτά. Για παράδειγμα, η <u>μηδενική συνάρτηση</u>

$$0: \mathbb{N} \longrightarrow \mathbb{C}$$

που ορίζεται ως εξής: $0(n)=0$ για κάθε $n\in\mathbb{N}$, δεν είναι ενεχωτικά αντιστρεπτή.

Πραγματικά, αν υπήρχε αριθμητική συνάρτηση $0'$ τέτοια ώστε $0\cdot 0' = \varepsilon$, τότε θα είχαμε

$$1 = \varepsilon(1) = 0(1)\,0'(1) = 0\,0'(1) = 0$$

που είναι άτοπο.

Θα σημειώσουμε εδώ ότι μια αριθμητική συνάρτηση f είναι <u>μη-μηδενική</u>, όταν

$$f(n)\neq 0\,,\ \text{για ένα τουλάχιστον } n\in\mathbb{N}\,.$$

Δεν είναι, λοιπόν, όλες οι αριθμητικές συναρτήσεις ενεχωτικά αντιστρέψιμες. Το παρακάτω θεώρημα μας δίνει την ικανή και αναγκαία συνθήκη για να είναι μία αριθμητική συνάρτηση ενεχωτικά αντιστρεπτή.

Θεώρημα 2.1.

Έστω f μια αριθμητική συνάρτηση. Η ενεχωτικά αντίστροφη της f^{-1} υπάρχει, εάν και μόνο εάν

$$f(1)\neq 0\,.$$

Απόδειξη.

Υποθέτουμε ότι η f^{-1} υπάρχει. Τότε $f\cdot f^{-1}=\varepsilon$, οπότε

$$(f\cdot f^{-1})(1) = \varepsilon(1) \quad \text{δηλ.} \quad f(1)\,f^{-1}(1) = 1$$

επομένως $f(1)\neq 0$.

Αντίστροφα, υποθέτουμε ότι $f(1) \neq 0$ και θεωρούμε την αριθμητική συνάρτηση $g : \mathbb{N} \longrightarrow \mathbb{C}$, που ορίζεται επαγωγικά από

$$\begin{cases} g(1) = \dfrac{1}{f(1)} \\ \\ g(n) = \dfrac{-1}{f(1)} \displaystyle\sum_{\substack{cd=n \\ c>1}} f(c)g(d) \qquad , \qquad n > 1 \end{cases}$$

θα δείξουμε ότι $f \cdot g = \varepsilon$, οπότε $g = f^{-1}$.

Αρκεί να δείξουμε ότι για κάθε $n \in \mathbb{N}$, είναι $(f \cdot g)(n) = \varepsilon(n)$.

Εργαζόμαστε επαγωγικά.

Για $n=1$ είναι $(f \cdot g)(1) = f(1)g(1) = f(1)\dfrac{1}{f(1)} = 1 = \varepsilon(1)$.

Για $n=2$, έχουμε

$$\begin{aligned} (f \cdot g)(2) &= f(1)g(2) + f(2)g(1) = \\ &= f(1)\left[\frac{-1}{f(1)} f(2)g(1)\right] + f(2)g(1) \\ &= -f(2)g(1) + f(2)g(1) = 0 = \varepsilon(2). \end{aligned}$$

Για $n \geq 3$, υποθέτουμε ότι, για κάθε k, $2 \leq k < n$ ισχύει $(f \cdot g)(k) = \varepsilon(k) = 0$.

Τότε

$$(f \cdot g)(n) = \sum_{ab=n} f(a)g(b) = f(n)g(1) + \sum_{\substack{ab=n \\ b>1}} f(a)g(b) =$$

$$= f(n)g(1) + \sum_{\substack{ab=n \\ b>1}} f(a)\left\{-\frac{1}{f(1)} \sum_{\substack{cd=b \\ c>1}} f(c)g(d)\right\}$$

$$= f(n)g(1) - \frac{1}{f(1)} \sum_{\substack{ab=n \\ b>1}} f(a)\left\{\sum_{cd=b} f(c)g(d) - f(1)g(b)\right\}$$

$$= f(n)g(1) - \frac{1}{f(1)} \sum_{\substack{ab=n \\ b>1}} f(a)\left\{(f \cdot g)(b) - f(1)g(b)\right\}$$

$$= f(n)g(1) - \frac{1}{f(1)} \sum_{\substack{ab=n \\ b>1}} f(a)(f\cdot g)(b) + \sum_{\substack{ab=n \\ b>1}} f(a)g(b)$$

Από την υπόθεση επαγωγής, όμως, ο μοναδικώς μη-μηδενικώς όρος στο πρώτο παραπάνω άθροισμα συναντάται για $b=n$ έτσι

$$(f\cdot g)(n) = f(n)g(1) - \frac{1}{f(1)} f(1)(f\cdot g)(n) + \sum_{\substack{ab=n \\ b>1}} f(a)g(b) =$$

$$= -(f\cdot g)(n) + (f\cdot g)(n) = 0 = \varepsilon(n)$$

Έτσι $(f\cdot g)(n) = \varepsilon(n)$, για κάθε $n\in\mathbb{N}$, πράγμα που επιθυμούσαμε. ∎

Παράδειγμα 2.1

Η αριθμητική συνάρτηση Λ του Mangoldt ορίζεται ως εξής

$$\Lambda(n) = \begin{cases} \log p, & \text{αν } n = p^m, \ p \text{ πρώτος και } m \geq 1 \\ 0 & \text{οπουδήποτε αλλού.} \end{cases}$$

Έτσι $\Lambda(1)=0$, $\Lambda(2)=\log 2$, $\Lambda(3)=\log 3$, $\Lambda(4)=\log 2$,

$\Lambda(5)=\log 5$, $\Lambda(6)=0$, $\Lambda(7)=\log 7$, $\Lambda(8)=\log 2$

$\Lambda(9)=\log 3$, $\Lambda(10)=0$.

Η συνάρτηση Λ δεν είναι αντιστρέψιμη, αφού $\Lambda(1)=0$.

Παρατήρηση.

Αν $f\in\mathcal{A}$ και $f(1)\neq 0$, τότε η f^{-1} υπάρχει και ορίζεται επαγωγικά ως εξής:

$$\begin{cases} f^{-1}(1) = \dfrac{1}{f(1)} \\ f^{-1}(n) = \dfrac{-1}{f(1)} \displaystyle\sum_{\substack{cd=n \\ c>1}} f(c) f^{-1}(d), & n>1. \end{cases}$$

Στο εξής θα συμβολίζουμε με $\mathcal{U}$ το σύνολο όλων των αριθμητικών συναρτήσεων που είναι ενεργητικά αντιστρεπτές δηλ

$$\mathcal{U} = \{f / f \in \mathcal{A},\ f(1) \neq 0\}.$$

Θα παρατηρήσουμε εδώ ότι το σύνολο $\mathcal{U} \neq \phi$, αφού, για παράδειγμα, οι συναρτήσεις $\varepsilon, \varphi, \tau, \sigma$ ανήκουν σ' αυτό. Επιπλέον, το $\mathcal{U}$ είναι γνήσιο υποσύνολο του $\mathcal{A}$ δηλ.

$$\mathcal{U} \subset \mathcal{A}$$

αφού η μηδενική συνάρτηση $0 \notin \mathcal{U}$.

Τέλος, παρατηρούμε ότι το $\mathcal{U}$ είναι κλειστό ως προς την πράξη ενεργητικό γινόμενο. Μ' άλλα λόγια, αν $f, g \in \mathcal{U}$, τότε και η συνάρτηση $f \cdot g \in \mathcal{U}$.

Πραγματικά, $(f \cdot g)(1) = f(1)g(1) \neq 0$, αφού $f(1) \neq 0$ και $g(1) \neq 0$.

Στην περίπτωση αυτή, η ενεργητικά αντίστροφη της $f \cdot g$ είναι η αριθμητική συνάρτηση $g^{-1} \cdot f^{-1}$, αφού

$$(f \cdot g) \cdot (g^{-1} \cdot f^{-1}) = f \cdot (g \cdot g^{-1}) \cdot f^{-1} = f \cdot \varepsilon \cdot f^{-1}$$
$$= f \cdot f^{-1} = \varepsilon.$$

Θεώρημα 2.2.

Το σύνολο $\mathcal{U}$ των ενεργητικά αντιστρεπτών αριθμητικών συναρτήσεων, εφοδιασμένο με την πράξη ενεργητικό γινόμενο, δομείται σε αντιμεταθετική ομάδα.[11]

Απόδειξη.

Το σύνολο $\mathcal{U}$ εφοδιασμένο με την πράξη ενεργητικό γινόμενο δομείται σε αντιμεταθετικό μονοειδές, αφού

i) $f\cdot(g\cdot h)=(f\cdot g)\cdot h$, για κάθε $f,g,h\in\mathcal{U}$

ii) $f\cdot g=g\cdot h$, για κάθε $f,g\in\mathcal{U}$

iii) Υπάρχει $\varepsilon\in\mathcal{U}$, τέτοια ώστε

$$f\cdot\varepsilon=f=\varepsilon\cdot f\ ,\quad \text{για κάθε } f\in\mathcal{U}.$$

Επισημαίνουμε ότι αν $f\in\mathcal{U}$ τότε και η $f^{-1}\in\mathcal{U}$ (αφού $f^{-1}(1)=\frac{1}{f(1)}\neq 0$), οπότε $f^{-1}\cdot f=\varepsilon=f\cdot f^{-1}$.

Το σύνολο $\mathcal{U}$, λοιπόν, δομείται σε αντιμεταθετική ομάδα. ■

3. Η υποομάδα $\mathcal{M}$ των πολλαπλασιαστικών συναρτήσεων.

Ορισμός

Μια μη-μηδενική αριθμητική συνάρτηση f καλείται πολλαπλασιαστική, όταν ικανοποιεί την εξής ιδιότητα.

O_1) Για οποιουσδήποτε φυσικούς αριθμούς m,n, με $(m,n)=1$, ισχύει

$$f(mn)=f(m)f(n)\ .$$

Παράδειγμα 3.1.

Η συνάρτηση $\varepsilon(n)=\begin{cases}1 & \text{αν } n=1\\ 0 & \text{αν } n>1\end{cases}$

είναι πολλαπλασιαστική. Πραγματικά, αν $m,n\in\mathbb{N}$, με $(m,n)=1$, τότε:

1) Αν $m=1$ και $n=1$, $\varepsilon(1\cdot 1)=1=1\cdot 1=\varepsilon(1)\,\varepsilon(1)$

2) Αν $m=1$ και $n>1$, $\varepsilon(1\cdot n)=0=1\cdot 0=\varepsilon(1)\,\varepsilon(n)$

3) Αν $m>1$ και $n=1$, $\varepsilon(m1)=0=0\cdot 1=\varepsilon(m)\cdot\varepsilon(1)$

4) Αν $m>1$ και $n>1$, $\varepsilon(mn)=0=0\cdot 0=\varepsilon(m)\cdot\varepsilon(n)$.

++ Ένα αντιμεταθετικό μονοειδές $(M,*)$, για το οποίο ισχύει

iv) Για κάθε $a\in M$ υπάρχει $a'\in M$ έτσι ώστε

$$a*a'=e=a'*a$$

καλείται αντιμεταθετική ομάδα.

Παράδειγμα 3.2.

Η συνάρτηση $\nu: \mathbb{N} \longrightarrow \mathbb{N}$, που ορίζεται ως εξής,

$$\nu(n) = 1 \ , \quad \text{για κάθε } n \in \mathbb{N} \qquad (7)$$

είναι πολλαπλασιαστική. Πραγματικά, για $m, n \in \mathbb{N}$, με $(m,n)=1$, έχουμε

$$\nu(mn) = 1 = 1 \cdot 1 = \nu(m) \cdot \nu(n) \ .$$

Παράδειγμα 3.3

Η συνάρτηση $\iota : \mathbb{N} \longrightarrow \mathbb{N}$, που ορίζεται ως εξής:

$$\iota(n) = n \ , \quad \text{για κάθε } n \in \mathbb{N} \qquad (8)$$

είναι πολλαπλασιαστική. Πραγματικά, αν $m, n \in \mathbb{N}$, με $(m,n)=1$, τότε $\iota(mn) = mn = \iota(m)\iota(n)$.

Παράδειγμα 3.4

Η αριθμητική συνάρτηση λ του Liouville, που ορίζεται ως εξής

$$\lambda(n) = \begin{cases} 1 & \text{αν } n=1 \\ (-1)^{k_1+\cdots+k_r} & \text{αν } n = p_1^{k_1}\cdots p_r^{k_r} \end{cases}$$

είναι πολλαπλασιαστική συνάρτηση.

Αν $m, n \in \mathbb{N}$, με $(m,n)=1$, θα δείξουμε ότι $\lambda(mn)=\lambda(m)\lambda(n)$. Αν ένας τουλάχιστον των m, n είναι ίσος με 1, τότε, φανερά, ισχύει. Έστω $m>1$, $n>1$ και

$$m = q_1^{\beta_1}\cdots q_v^{\beta_v} \ , \quad n = p_1^{\alpha_1}\cdots p_u^{\alpha_u}$$

οι πρωτογενείς μορφές τους. Φανερά, $p_i \neq q_j$ αφού $(m,n)=1$. Έτσι η πρωτογενής μορφή του γινομένου mn είναι

$$mn = q_1^{\beta_1}\cdots q_v^{\beta_v} \cdot p_1^{\alpha_1}\cdots p_u^{\alpha_u}$$

οπότε

$$\lambda(mn) = (-1)^{\beta_1+\cdots+\beta_v+\alpha_1+\cdots+\alpha_u} = (-1)^{\beta_1+\cdots+\beta_v} \cdot (-1)^{\alpha_1+\cdots+\alpha_u} =$$

$$= \lambda(m)\lambda(n) \ .$$

Παράδειγμα 3.5

Οι συναρτήσεις τ και σ είναι πολλαπλασιαστικές.

Πραγματικά, αν $m, n \in \mathbb{N}$, με $(m,n)=1$, τότε, σύμφωνα με το θεώρημα 6.10 Κεφ. II, έχουμε ότι, κάθε διαιρέτης $d|mn$ αναλύεται σε γινόμενο $d=s\cdot t$, με $s|m$ και $t|n$ (και η ανάλυση αυτή είναι μοναδική) και αντίστροφα.

Έτσι, αν $d_1, \dots, d_{\tau(m)}$ είναι όλοι οι φυσικοί διαιρέτες του m και $\delta_1, \dots, \delta_{\tau(n)}$ όλοι οι φυσικοί διαιρέτες του n, τότε οι

$$d_1\delta_1, \dots, d_{\tau(m)}\delta_1, \dots, d_1\delta_{\tau(n)}, \dots, d_{\tau(m)}\delta_{\tau(n)}$$

είναι όλοι οι φυσικοί διαιρέτες του mn, που είναι σε πλήθος $\tau(m)\tau(n)$. Έτσι

$$\tau(mn)=\tau(m)\tau(n),$$

και

$$\sigma(mn)=d_1\delta_1+\dots+d_{\tau(m)}\delta_1+\dots+d_1\delta_{\tau(n)}+\dots+d_{\tau(m)}\delta_{\tau(n)}=$$

$$=\left(d_1+\dots+d_{\tau(m)}\right)\left(\delta_1+\dots+\delta_{\tau(n)}\right)=\sigma(m)\sigma(n).$$

Όμοια μπορούμε να δείξουμε ότι και οι συναρτήσεις φ και μ είναι πολλαπλασιαστικές. (Άσκηση).

Στα επόμενα θα δείξουμε, με πιο κομψό τρόπο, ότι οι συναρτήσεις $\varphi, \mu, \tau, \sigma$ είναι πολλαπλασιαστικές.

Θεώρημα 3.1

Αν f είναι μια πολλαπλασιαστική συνάρτηση και $m_1, \dots, m_k$ είναι φυσικοί αριθμοί πρώτοι μεταξύ τους ανά δύο, τότε

$$f(m_1 \cdots m_k)=f(m_1)\cdots f(m_k)$$

Απόδειξη.

Παρατηρούμε ότι $(m_i, m_{i+1}\cdots m_k)=1$, για $i=1,2,\dots,k-1$.

Πραγματικά, σύμφωνα με το θεώρημα 6.9 Κεφ II, έχουμε

$$(m_i, m_{i+1} \cdots m_k) = (m_i, m_{i+1}) \cdots (m_i, m_k) = 1 \cdots 1 = 1$$

Συνεπώς, αφού η f είναι πολλαπλασιαστική, θα έχουμε

$$f(m_1 m_2 \cdots m_k) = f(m_1) f(m_2 \cdots m_k) =$$

$$= f(m_1) f(m_2) f(m_3 \cdots m_k)$$

$$\vdots$$

$$= f(m_1) f(m_2) \cdots f(m_k) . \blacksquare$$

Πόρισμα 3.1

Αν f είναι μια πολλαπλασιαστική συνάρτηση, τότε, για κάθε φυσικό αριθμό $n > 1$ με πρωτογενή ανάλυση

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} ,$$

ισχύει $$f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k}) .$$

Απόδειξη

Παρατηρούμε ότι, για $i \neq j$, είναι $(p_i, p_j) = 1$, επομένως $(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$. Οι φυσικοί αριθμοί, λοιπόν, $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$, είναι πρώτοι μεταξύ τους ανά δύο, επομένως

$$f(n) = f(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k}),$$

σύμφωνα με το προηγούμενο θεώρημα. $\blacksquare$

Το παραπάνω πόρισμα μας βεβαιώνει ότι κάθε πολλαπλασιαστική συνάρτηση καθορίζεται πλήρως από τις τιμές της πάνω στους φυσικούς αριθμούς p^{α}, για κάθε πρώτο p και για κάθε φυσικό αριθμό α.

Πόρισμα 3.2

Αν f και g είναι δύο πολλαπλασιαστικές συναρτήσεις τέτοιες ώστε

$$f(p^{\alpha}) = g(p^{\alpha}) ,$$

για κάθε πρώτο p και για κάθε φυσικό αριθμό α, τότε

$$f = g.$$

Απόδειξη.

Αρκεί να δείξουμε ότι, για κάθε φυσικό αριθμό n, ισχύει

$$f(n) = g(n).$$

Πραγματικά, για $n=1$, έχουμε $f(1) = 1 = g(1)$, σύμφωνα με το θεώρημα 3.3 πιο κάτω.

Αν $n>1$ και $n = p_1^{\alpha_1} \cdots p_\kappa^{\alpha_\kappa}$

η πρωτογενής μορφή του, τότε, σύμφωνα με το πόρισμα 3.1 και την υποθεσή μας, έχουμε

$$\begin{aligned} f(n) &= f(p_1^{\alpha_1}) \cdots f(p_\kappa^{\alpha_\kappa}) \\ &= g(p_1^{\alpha_1}) \cdots g(p_\kappa^{\alpha_\kappa}) \\ &= g(n) \quad . \blacksquare \end{aligned}$$

Πόρισμα 3.3

Αν $m, n \in \mathbb{N}$, τότε, για κάθε πολλαπλασιαστική συνάρτηση f, ισχύει

$$f((m,n))\, f([m,n]) = f(m)\, f(n).$$

Απόδειξη.

Έστω $m = p_1^{\alpha_1} \cdots p_\nu^{\alpha_\nu}$ και $n = p_1^{\beta_1} \cdots p_\nu^{\beta_\nu}$ με $\alpha_i \geq 0$ και $\beta_i \geq 0$.

Τότε $f(m) = f(p_1^{\alpha_1}) \cdots f(p_\nu^{\alpha_\nu})$ και $f(n) = f(p_1^{\beta_1}) \cdots f(p_\nu^{\beta_\nu})$

και (βλέπε Κεφ. II, Θεωρ. 6.4 και Πορ. 8.1)

$$f((m,n)) = f(p_1^{\min\{\alpha_1,\beta_1\}}) \cdots f(p_\nu^{\min\{\alpha_\nu,\beta_\nu\}})$$

$$f([m,n]) = f(p_1^{\max\{\alpha_1,\beta_1\}}) \cdots f(p_\nu^{\max\{\alpha_\nu,\beta_\nu\}}).$$

Η απόδειξή μας τελειώνει παρατηρώντας ότι

$$f(p^\alpha)\, f(p^\beta) = f(p^{\min\{\alpha,\beta\}}) \cdot f(p^{\max\{\alpha,\beta\}}).$$

Θεώρημα 3.2

Αν f και g είναι πολλαπλασιαστικές συναρτήσεις, τότε

i) Και το συνηθισμένο τους γινόμενο, δηλ η αριθμητική συνάρτηση $\Gamma : \mathbb{N} \to \mathbb{C}$, που ορίζεται ως εξής

$$\Gamma(n) = f(n)g(n), \quad \text{για κάθε } n \in \mathbb{N}$$

είναι επίσης πολλαπλασιαστική

ii) Αν $g(n) \neq 0$, για κάθε $n \in \mathbb{N}$, τότε και η αριθμητική συνάρτηση $G : \mathbb{N} \to \mathbb{C}$, που ορίζεται ως εξής

$$G(n) = \frac{f(n)}{g(n)} \quad \text{για κάθε } n \in \mathbb{N}$$

είναι επίσης πολλαπλασιαστική.

Απόδειξη

i) Η Γ είναι μη-μηδενική συνάρτηση, αφού $\Gamma(1) = f(1)g(1) = 1 \neq 0$.

Αν $m, n \in \mathbb{N}$, με $(m,n) = 1$, τότε

$$\begin{aligned}\Gamma(mn) &= f(mn)g(mn) = f(m)f(n)\,g(m)g(n) \\ &= \big(f(m)g(m)\big)\big(f(n)g(n)\big) \\ &= \Gamma(m)\,\Gamma(n)\end{aligned}$$

ii) Η G είναι μη-μηδενική συνάρτηση, αφού

$$G(1) = \frac{f(1)}{g(1)} = \frac{1}{1} = 1 \neq 0.$$

Αν τώρα $m, n \in \mathbb{N}$, με $(m,n) = 1$ τότε

$$G(mn) = \frac{f(mn)}{g(mn)} = \frac{f(m)f(n)}{g(m)g(n)} = \frac{f(m)}{g(m)} \cdot \frac{f(n)}{g(n)}$$

$$= G(m) \cdot G(n) \;. \blacksquare$$

Θεώρημα 3.3

Για κάθε πολλαπλασιαστική συνάρτηση f, ισχύει

$$f(1)=1.$$

Απόδειξη.

Η f είναι μη-μηδενική συνάρτηση. επομένως, για κάποιο φυσικό αριθμό n, θα είναι $f(n)\neq 0$. Επειδή $(1,n)=1$ και η f είναι πολλ/μή, θα έχουμε

$$f(n)=f(n\cdot 1)=f(n)f(1), \text{ επομένως } f(1)=1. \blacksquare$$

Στο εξής, θα συμβολίζουμε με $\mathcal{M}$ το σύνολο των πολλαπλασιαστικών συναρτήσεων, δηλ

$$\mathcal{M}=\{f / f\in\mathcal{A}, f \text{ πολλαπλασιαστική}\}.$$

Φανερά, $\mathcal{M}\neq\phi$.

Πόρισμα 3.4

Αν $f\in\mathcal{M}$, τότε η f είναι ενελικτικά αντιστρεπτή.

Απόδειξη.

Αφού $f\in\mathcal{M}$, θα είναι $f(1)=1\neq 0$, και, σύμφωνα με το θεώρημα 2.1, η f είναι ενελικτικά αντιστρεπτή. $\blacksquare$

Έτσι $\mathcal{M}\subseteq\mathcal{U}$ και, όπως θα δούμε παρακάτω, το σύνολο $\mathcal{M}$ είναι γνήσιο υποσύνολο του $\mathcal{U}$, δηλαδή

$$\mathcal{M}\subset\mathcal{U}.$$

Μ' άλλα λόγια, υπάρχουν ενελικτικά αντιστρεπτές συναρτήσεις που δεν είναι πολλ/κές. Για παράδειγμα, η συνάρτηση

$$\gamma:\mathbb{N}\to\mathbb{N}, \qquad n\longmapsto\gamma(n)$$

($\gamma(n)$ = το γινόμενο των φυσικών διαιρετών του n)

είναι ενελικτικά αντιστρεπτή, δηλ $\gamma\in\mathcal{U}$, αφού $\gamma(1)=1\neq 0$ αλλά δεν είναι πολλ/κή. Πραγματικά,

$(2,3)=1$ και $\gamma(2\cdot3)=\gamma(6)=36$, $\gamma(2)=2$, $\gamma(3)=3$

αλλά $\gamma(2\cdot3)\neq\gamma(2)\gamma(3)$, έτσι $\gamma\notin\mathcal{M}$.

Τελικά λοιπόν, έχουμε

$$\mathcal{M}\subset\mathcal{U}\subset\mathcal{A} \qquad (9)$$

Έχουμε δείξει ότι το ζεύγος $(\mathcal{U},\cdot)$ είναι μια αντιμεταθετική ομάδα. Στη συνέχεια θα δείξουμε ότι το $\mathcal{M}$ είναι μια υποομάδα της, μ'άλλα λόγια ότι το σύνολο $\mathcal{M}$ εφοδιασμένο με την πράξη ενεργητικό γινόμενο, δομείται και αυτό σε αντιμεταθετική ομάδα.

Θεώρημα 3.4

Το ενεργητικό γινόμενο πολλαπλασιαστικών αναρτήσεων είναι επίσης πολλαπλασιαστική συνάρτηση. Μ'άλλα λόγια αν $f,g\in\mathcal{M}$, τότε και $f\cdot g\in\mathcal{M}$.

Απόδειξη.

Έστω $\alpha=f\cdot g$. Η συνάρτηση α είναι μη-μηδενική. Πράγμα-τι $\alpha(1)=(f\cdot g)(1)=f(1)\,g(1)=1\cdot1=1\neq0$.

Μένει να δείξουμε ότι, αν $m,n\in\mathbb{N}$ με $(m,n)=1$, τότε

$$\alpha(mn)=\alpha(m)\,\alpha(n)\ .$$

Υπενθυμίζουμε ότι, αν $(m,n)=1$, τότε

1ον) Για οποιουσδήποτε διαιρέτες $s\mid m$, $t\mid n$ είναι επίσης $(s,t)=1$. (Κεφ. II, Λημμα 6.1)

2ον) Κάθε φυσικός διαιρέτης $d\mid mn$ αναλύεται σε γινόμενο $d=st$ φυσικών διαιρετών $s\mid m$ και $t\mid n$ κατά μοναδικό τρόπο. (Κεφ. II, Θεώρημα 6.10).

Έτσι

$$\alpha(mn)=(f\cdot g)(mn)=\sum_{d\mid mn}f(d)\,g\left(\frac{mn}{d}\right)=$$

$$=\sum_{s\mid m}\sum_{t\mid n}f(st)\,g\left(\frac{mn}{st}\right)$$

$$= \sum_{s|m} \sum_{t|n} f(s) f(t) g\left(\frac{m}{s}\right) g\left(\frac{n}{t}\right) \qquad \left(\frac{m}{s}, \frac{n}{t}\right) = 1$$

$$= \left(\sum_{s|m} f(s) g\left(\frac{m}{s}\right)\right)\left(\sum_{t|n} f(t) g\left(\frac{n}{t}\right)\right)$$

$$= (f \cdot g)(m) \cdot (f \cdot g)(n) = a(m)\, a(n) \; . \; \blacksquare$$

Πόρισμα 3.5

Αν η συνάρτηση f είναι πολλαπλασιαστική και

$$F(n) = \sum_{d|n} f(d)$$

τότε και η συνάρτηση F είναι πολλαπλασιαστική.

Απόδειξη.

Η συνάρτηση $v(n) = 1$, για κάθε $n \in \mathbb{N}$, είναι πολ|κή. Είναι

$$F(n) = \sum_{d|n} f(d) = \sum_{d|n} f(d)\, v\left(\frac{n}{d}\right) = (f \cdot v)(n), \text{ δηλ.}$$

$F = f \cdot v$. Σύμφωνα τώρα με το θεώρημα 3.4 και η συνάρτηση F είναι πολ|κή. $\blacksquare$

Παράδειγμα 3.6

Για την πολλαπλασιαστική συνάρτηση λ του Liouville (βλ. παραδ. 3.4) ισχύει

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{αν } n = m^2, \text{ για κάποιο ακέραιο } m \\ 0 & \text{οπουδήποτε αλλού} \end{cases}$$

Για $n = 1 = 1^2$ έχουμε $\sum_{d|1} \lambda(d) = \lambda(1) = 1$.

Έστω $n > 1$ και $n = p_1^{\alpha_1} \cdots p_\kappa^{\alpha_\kappa}$ η πρωτογενής μορφή του.

Η συνάρτηση

$$F(n) = \sum_{d|n} \lambda(d)$$

είναι πολ|κή, επομένως $F(n) = F(p_1^{\alpha_1}) \cdots F(p_\kappa^{\alpha_\kappa})$, (βλέπ. Πόρισμα 3.1)

Για $i = 1, 2, \ldots, \kappa$ έχουμε

$$F(p_i^{\alpha_i}) = \sum_{d|p_i^{\alpha_i}} \lambda(d) = \lambda(1) + \lambda(p_i) + \cdots + \lambda(p_i^{\alpha_i}) =$$

$$= 1 + (-1)^1 + (-1)^2 + \cdots + (-1)^{\alpha_i} = \begin{cases} 1, & \text{αν ο } \alpha_i \text{ είναι άρτιος} \\ 0, & \text{αν ο } \alpha_i \text{ είναι περιττός} \end{cases}$$

Αν ένας τουλάχιστον από τους εκθέτες α_i είναι περιττός, τότε $F(p_i^{\alpha_i}) = 0$ και επομένως $F(n) = 0$. Αν όλοι οι εκθέτες α_i είναι άρτιοι, τότε $F(p_i^{\alpha_i}) = 1$ και επομένως $F(n) = 1$, πράγμα που επιδιώξαμε.

Για τον καθορισμό της συνάρτησης $F(n) = \sum_{d|n} f(d)$, στην περίπτωση που η συνάρτηση f δεν είναι πολλαπλή, τα πράγματα δυσκολεύουν

Παράδειγμα 3.7

Για την συνάρτηση Λ του Mangoldt (βλεπ. παραδ. 2.1), ισχύει

$$\log n = \sum_{d|n} \Lambda(d) \qquad \text{για κάθε } n \in \mathbb{N}.$$

Η συνάρτηση Λ **δεν** είναι πολλαπλή, αφού $\Lambda(1) = 0$. Δεν μπορούμε λοιπόν να εργαστούμε όπως στο προηγούμενο παράδειγμα.

Για $n = 1$ ισχύει, αφού $\log 1 = 0$ και $\sum_{d|1} \Lambda(d) = \Lambda(1) = 0$.

Έστω $n > 1$ και $n = p_1^{\alpha_1} \cdots p_\nu^{\alpha_\nu}$ η πρωτογενής μορφή του και d ένας διαιρέτης του n.

Αν $d = 1$, τότε $\Lambda(1) = 0$.

Αν η πρωτογενής μορφή του d περιέχει περισσότερους από έναν πρώτους της πρωτογενούς ανάλυσης του n, τότε $\Lambda(d) = 0$, ενώ, αν περιέχει ακριβώς έναν πρώτο, δηλ. αν

$$d = p_i^{\beta_i} \qquad i = 1, \ldots, \nu \quad \text{και} \quad 1 \le \beta_i \le \alpha_i,$$

τότε $\Lambda(d) \neq 0$. Έτσι

$$\sum_{d|n} \Lambda(d) = \left(\Lambda(p_1) + \cdots + \Lambda(p_1^{\alpha_1})\right) + \cdots + \left(\Lambda(p_\nu) + \cdots + \Lambda(p_\nu^{\alpha_\nu})\right)$$

$$= \underbrace{(\log p_1 + \cdots + \log p_1)}_{\alpha_1 \text{-φορές}} + \cdots + \underbrace{(\log p_\nu + \cdots + \log p_\nu)}_{\alpha_\nu \text{-φορές}}$$

$$= \alpha_1 \log p_1 + \dots + \alpha_v \log p_v$$
$$= \log(p_1^{\alpha_1}) + \dots + \log(p_v^{\alpha_v})$$
$$= \log(p_1^{\alpha_1} \dots p_v^{\alpha_v}) = \log \eta \quad . \blacksquare$$

Θεώρημα 3.5

Η ενελικτική αντίστροφη πολλαπλασιαστικής συνάρτησης f υπάρχει και είναι επίσης πολλαπλασιαστική.

Απόδειξη.

Το πόρισμα 3.4 μας εξασφαλίζει την ύπαρξη της f^{-1}. Για να δείξουμε ότι η f^{-1} είναι πολλ/κή, θα εργαστούμε επαγωγικά.

Από τον ορισμό της f^{-1} έχουμε $f^{-1}(1) = \frac{1}{f(1)} = 1$

και επομένως

$$f^{-1}(st) = f^{-1}(s) f^{-1}(t), \quad \text{για } st = 1.$$

Έστω $K > 1$ και ας υποθέσουμε ότι

$$f^{-1}(st) = f^{-1}(s) f^{-1}(t)$$

για κάθε ζεύγος φυσικών s, t, με $1 \leq st < K$ και $(s,t) = 1$.

Έστω m, n τυχόν ζεύγος φυσικών αριθμών με $mn = K$ και $(m,n) = 1$.

Παρατηρούμε ότι, επειδή

$$f^{-1} \cdot f = \varepsilon$$

και η συνάρτηση ε είναι πολλ/κή, θα έχουμε

$$\varepsilon(mn) = \varepsilon(m)\varepsilon(n)$$

η ισοδύναμα

$$(f^{-1} \cdot f)(mn) = (f^{-1} \cdot f)(m) \cdot (f^{-1} \cdot f)(n) \qquad (10)$$

Αφού $(m,n) = 1$ η σχέση (10) γράφεται

$$\sum_{d|mn} f^{-1}(d)\, f\left(\frac{mn}{d}\right) = \left(\sum_{d|m} f^{-1}(d)\, f\left(\frac{m}{d}\right)\right)\left(\sum_{d|n} f^{-1}(d)\, f\left(\frac{n}{d}\right)\right).$$

Η παραπάνω ισότητα, σύμφωνα με όσα αναφέραμε και στην απόδειξη του θεωρήματος 3.4, γράφεται

$$\sum_{s|m}\sum_{t|n} f^{-1}(st) f\left(\frac{mn}{st}\right) = \left(\sum_{s|m} f^{-1}(s) f\left(\frac{m}{s}\right)\right)\left(\sum_{t|n} f^{-1}(t) f\left(\frac{n}{t}\right)\right) =$$

$$= \sum_{s|m}\sum_{t|n} f^{-1}(s) f^{-1}(t) f\left(\frac{m}{s}\right) f\left(\frac{n}{t}\right)$$

$$= \sum_{s|m}\sum_{t|n} f^{-1}(s) f^{-1}(t)\, f\left(\frac{mn}{st}\right)$$

αφού $\left(\frac{m}{s}, \frac{n}{t}\right) = 1$ και η f πολλαπλασιαστική. Επομένως, με μεταφορά στο πρώτο μέλος παίρνουμε

$$\sum_{s|m}\sum_{t|n} \left\{ f^{-1}(st) - f^{-1}(s) f^{-1}(t) \right\} f\left(\frac{mn}{st}\right) = 0$$

Εδώ όμως, από την υπόθεση επαγωγής, οι διαφορές $f^{-1}(st) - f^{-1}(s) f^{-1}(t)$, για $st < mn$, μηδενίζονται, ενώ $st = mn$ αριθμώ και μόνον όταν $s = m$ και $t = n$ (βλ. Κεφ II. λήμμα 6.2).

Έτσι

$$\left\{ f^{-1}(mn) - f^{-1}(m) f^{-1}(n) \right\} f\left(\frac{mn}{mn}\right) = 0$$

δηλαδή, αφού $f(1) = 1$

$$f^{-1}(mn) - f^{-1}(m) f^{-1}(n) = 0$$

πράγμα που επιθυμούσαμε. ■

Τα θεωρήματα 3.4 και 3.5 και το γεγονός ότι το ενεργητικό γινόμενο αριθμητικών συναρτήσεων είναι προσεταιριστικό και αντιμεταθετικό μας αποδεικνύουν το επόμενο θεώρημα

Θεώρημα 3.6

Το σύνολο $\mathcal{M}$ των πολλαπλασιαστικών συναρτήσεων, εφοδιασμένο με την πράξη ενελικτικό γινόμενο, δομείται σε αντιμεταθετική ομάδα. ■

Ας δούμε όμως τώρα, τα σπουδαιότερα αποτελέσματα που παίρνουμε εφαρμόζοντας την θεωρία που μέχρις εδώ παρουσιάσαμε, στις πιο βασικές Αριθμοθεωρητικές συναρτήσεις μ, φ, τ και σ.

4. Η συνάρτηση μ του Möbius και ο τύπος αντιστροφής του Möbius.

Θα ξεκινήσουμε δίνοντας μια φυσική ερμηνεία για τον τόσο παραξενο τρόπο ορισμού της συνάρτησης μ του Mobius, όπως αυτή ορίστηκε στην αρχή του κεφαλαίου αυτού.

Αρχικά παρατηρούμε και πάλι ότι η συναρτηση

$$V : \mathbb{N} \longrightarrow \mathbb{C} \ , \quad V(n) = 1 \quad \text{για κάθε } n \in \mathbb{N}$$

είναι πολλαπλασιαστική (Παραδ. 3.2) και επομένως ενελικτικά αντιστρεπτή (Πόρισμα 3.1). Υπάρχει, λοιπόν, η ενελικτική αντίστροφη της V^{-1} και ας τη συμβολίσουμε με

$$V^{-1} = \mu$$

Ισχύει λοιπόν

$$\mu \bullet V = \varepsilon = V \bullet \mu$$

Από το θεώρημα 3.5 συμπεραίνουμε ότι η συνάρτηση μ είναι πολλαπλασιαστική σαν ενελικτική αντίστροφος της πολλαπλασιαστικής συνάρτησης V. Η μ, λοιπόν

είναι πλήρως ορισμένη από τις τιμές της $\mu(p^\alpha)$, για κάθε πρώτο p και για κάθε φυσικό αριθμό α.

Έστω p ένας σταθερός πρώτος αριθμός. Θα εργαστούμε επαγωγικά πάνω στο φυσικό αριθμό α.

Για $\alpha=1$, έχουμε

$$(\mu\cdot\nu)(p)=\varepsilon(p)=0 \quad \text{δηλ}$$

$$0=\sum_{d|p}\mu(d)\nu\left(\frac{p}{d}\right)=\mu(1)\nu(p)+\mu(p)\nu(1)=$$

$$=1\cdot 1+\mu(p)\cdot 1=1+\mu(p)$$

(επειδή $\mu(1)=1$, αφού η μ είναι πολλαπλή) επομένως,

$$\mu(p)=-1$$

Για $\alpha=2$, έχουμε $(\mu\cdot\nu)(p^2)=\varepsilon(p^2)=0$, δηλ.

$$0=\sum_{d|p^2}\mu(d)\nu\left(\frac{p^2}{d}\right)=\mu(1)\nu(p^2)+\mu(p)\nu(p)+\mu(p^2)\nu(1)=$$

$$=1\cdot 1+\mu(p)1+\mu(p^2)\cdot 1=$$

$$=1-1+\mu(p^2)$$

επομένως

$$\mu(p^2)=0$$

Άν ο φυσικός $\eta>2$, υποθέτουμε ότι

$$\mu(p^\alpha)=0, \text{ για κάθε } \alpha, \quad 2\le\alpha<\eta.$$

Θα είναι $(\mu\cdot\nu)(p^\eta)=\varepsilon(p^\eta)=0$, δηλ

$$0=\sum_{d|p^\eta}\mu(d)\nu\left(\frac{p^\eta}{d}\right)=\mu(1)\nu(p^\eta)+\mu(p)\nu(p^{\eta-1})+\cdots+\mu(p^\eta)\nu(1)=$$

$$=\mu(1)+\mu(p)+\mu(p^2)+\cdots+\mu(p^\eta)=$$

$$=1-1+0+\cdots+0+\mu(p^\eta)=\mu(p^\eta)$$

δηλ

$$\mu(p^\eta)=0$$

Τελικά, για κάθε πρώτο p είναι

$\mu(p) = -1$ και $\mu(p^\alpha) = 0$, για κάθε φυσικό $\alpha \geq 2$.

Επομένως, αν ο φυσικός $n>1$ και $n = p_1^{\alpha_1} \cdots p_\kappa^{\alpha_\kappa}$ είναι η πρωτογενής μορφή του, τότε, επειδή η μ είναι πολλαπλή θα έχουμε

$$\mu(n) = \mu(p_1^{\alpha_1}) \cdots \mu(p_\kappa^{\alpha_\kappa}),$$

σύμφωνα με το Πόρισμα 3.3.

Αν ένας τουλάχιστον των $\alpha_i \geq 2$, τότε $\mu(n) = 0$, ενώ, αν $n = p_1 \cdot p_2 \cdots p_\kappa$, τότε

$$\mu(n) = \underbrace{(-1)\cdots(-1)}_{\kappa\text{-φορές}} = (-1)^\kappa .$$

Άρα η συνάρτηση $\mu : \mathbb{N} \longrightarrow \mathbb{C}$ ορίζεται ως εξής:

$$\mu(n) = \begin{cases} 1 & \text{αν } n = 1 \\ 0 & \text{αν } \exists \text{ πρώτος } p \text{ με } p^2 \mid n \\ (-1)^\kappa & \text{αν } n = p_1 \cdots p_\kappa \text{ και οι πρώτοι } p_1, \ldots, p_\kappa \text{ είναι διαιωρισμένοι (άνισοι ανά δύο).} \end{cases}$$

Η συνάρτηση μ καλείται συνάρτηση του Möbius, είναι πολλαπλασιαστική σαν ενεργητική αντίστροφος της συνάρτησης V και πληροί τη σχέση

$$\mu * V = \varepsilon \qquad (11)$$

Θεώρημα 4.1

Για την συνάρτηση μ του Möbius ισχύει

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{άν } n = 1 \\ 0 & \text{άν } n > 1 \end{cases}$$

Απόδειξη.

Ισχύει $\mu * \nu = \varepsilon$, δηλ $(\mu * \nu)(n) = \varepsilon(n)$, για κάθε $n \in \mathbb{N}$

Επομένως

$$\sum_{d|n} \mu(d)\, \nu\left(\frac{n}{d}\right) = \varepsilon(n), \quad \text{δηλ} \quad \left(\text{αφού } \nu\left(\frac{n}{d}\right) = 1\right)$$

$$\sum_{d|n} \mu(d) = \varepsilon(n) = \begin{cases} 1 & \text{αν } n = 1 \\ 0 & \text{αν } n > 1 \end{cases} \quad . \blacksquare$$

Παρατήρηση.

Το παραπάνω θεώρημα μπορούμε να το αποδείξουμε και κομπινατορικά, χωρίς δηλ να χάσουμε υπόψη μας ότι η συνάρτηση μ είναι πολλαπλ. Μια άλλη απόδειξη προκύπτει απ' ευθείας από το πόρισμα 3.5, αν χάσουμε εαν γνωστό ότι η συνάρτηση μ είναι πολλαπλ.

Για παράδειγμα, $\sum_{d|18} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(6) + \mu(9) + \mu(18) =$

$$= 1 + (-1) + (-1) + (-1)^2 + 0 + 0 = 0$$

αφού $\mu(6) = \mu(2 \cdot 3) = (-1)^2$, $\mu(9) = \mu(3^2) = 0$, $\mu(18) = (2 \cdot 3^2) = 0$.

Η σπουδαιότητα της συνάρτησης μ του Möbius φαίνεται από το παρακάτω θεώρημα.

Θεώρημα 4.2 (Τύπος αντιστροφής του Möbius)

Αν f και g είναι αριθμητικές συναρτήσεις, τότε

$$g(n) = \sum_{d|n} f(d), \text{ για κάθε } n \in \mathbb{N} \iff f(n) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) \text{ για κάθε } n \in \mathbb{N}$$

Απόδειξη.

Αν $g(n) = \sum_{d|n} f(d)$, για κάθε $n \in \mathbb{N}$, τότε

$$g(n)=\sum_{d|n} f(d)\,\nu\left(\frac{n}{d}\right)=(f\cdot\nu)(n),\ \text{για κάθε } n\in\mathbb{N},$$

δηλ

$$g=f\cdot\nu=\nu\cdot f \qquad (12)$$

Επειδή η $\nu^{-1}=\mu$ υπάρχει, από την σχέση(12) παίρνουμε

$$\mu\cdot g=\mu\cdot(\nu\cdot f)=(\mu\cdot\nu)\cdot f=\varepsilon\cdot f=f,$$

δηλ. για κάθε $n\in\mathbb{N}$ ισχύει

$$f(n)=(\mu\cdot g)(n)=\sum_{d|n}\mu(d)\,g\left(\frac{n}{d}\right) \qquad (13)$$

Αντίστροφα, αν ισχύει η (13), δηλ αν $f=\mu\cdot g$, τότε

$$f\cdot\nu=\nu\cdot f=\nu\cdot(\mu\cdot g)=(\nu\cdot\mu)\cdot g=\varepsilon\cdot g=g$$

ισχύει δηλ η (12), επομένως

$$g(n)=\sum_{d|n} f(d)\,\nu\left(\frac{n}{d}\right)=\sum_{d|n} f(d),\ \text{για κάθε } n\in\mathbb{N}.\ \blacksquare$$

<u>Παράδειγμα 4.1</u>

Για την συνάρτηση Λ του Mangoldt ισχύει

$$\Lambda(n)=\sum_{d|n}\mu(d)\log\frac{n}{d}=-\sum_{d|n}\mu(d)\log d$$

για κάθε $n\in\mathbb{N}$.

Στο παράδειγμα 3.7 δείξαμε ότι

$$\log n=\sum_{d|n}\Lambda(d),\ \text{για κάθε } n\in\mathbb{N}.$$

συνεπώς από τον τύπο αντιστροφής του Möbius έχουμε.

$$\Lambda(n)=\sum_{d|n}\mu(d)\log\frac{n}{d},\ \text{για κάθε } n\in\mathbb{N}$$

Αλλά $\log\frac{n}{d}=\log n-\log d$, απομένως

$$\Lambda(n)=\sum_{d|n}\mu(d)(\log n-\log d)=\sum_{d|n}\mu(d)\log n-\sum_{d|n}\mu(d)\log d=$$

$$=\log n\sum_{d|n}\mu(d)-\sum_{d|n}\mu(d)\log d.$$

Αλλά για $n=1$ είναι $\log 1 = 0$ και για $n>1$ $\sum_{d|n} \mu(d) = 0$,

οπότε $\log n \sum_{d|n} \mu(d) = 0$, για κάθε $n \in \mathbb{N}$.

Έτσι $$\Lambda(n) = -\sum_{d|n} \mu(d) \log d .$$

Πόρισμα 4.1

Αν f και g είναι αριθμητικές συναρτήσεις τέτοιες ώστε

$$g(n) = \sum_{d|n} f(d) \quad , \text{ για κάθε } n \in \mathbb{N}$$

τότε $$(f \text{ πολλαπλασιαστική}) \Longleftrightarrow (g \text{ πολλαπλασιαστική})$$

Απόδειξη.

Από τον τύπο αντιστροφής του Möbius παίρνουμε

$$f(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) , \text{ δηλ. } f = \mu * g$$

Αν η g είναι πολλ/κή, τότε, αφού και η μ είναι πολλ/κή, θα είναι και το εσωτερικό τους γινόμενο $f = \mu * g$ πολλ/κή συνάρτηση (βλέπ. Θεωρ. 3.2).

Το αντίστροφο είναι αμφιβόλου το Πόρισμα 3.5 . ■

Θεώρημα 4.3

Αν ο φυσικός $n>1$ και $n = p_1^{\alpha_1} \dots p_\kappa^{\alpha_\kappa}$ είναι η πρωτογενής μορφή του, τότε, για κάθε πολλαπλασιαστική συνάρτηση f, είναι

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_\kappa))$$

Απόδειξη.

Η συνάρτηση $\Gamma(n) = \mu(n) f(n)$ είναι πολλ/κή, σύμφωνα με το Θεωρ. 3.6.

Όμοια και η συνάρτηση

$$F(n) = \sum_{d|n} \Gamma(d) = \sum_{d|n} \mu(d) f(d)$$

είναι πολ/μή, σύμφωνα με το προηγούμενο πόρισμα.
Θα έχουμε λοιπόν, σύμφωνα με το πόρισμα 3.3,

$$F(n) = F(p_1^{\alpha_1}) \cdots F(p_\kappa^{\alpha_\kappa}) = \Big(\sum_{d|p_1^{\alpha_1}} \mu(d) f(d)\Big) \cdots \Big(\sum_{d|p_\kappa^{\alpha_\kappa}} \mu(d) f(d)\Big).$$

Αλλά για $i=1,\dots,\kappa$ είναι

$$\sum_{d|p_i^{\alpha_i}} \mu(d) f(d) = \mu(1) f(1) + \mu(p_i) f(p_i) + \mu(p_i^2) f(p_i^2) + \cdots + \mu(p_i^{\alpha_i}) f(p_i^{\alpha_i})$$
$$= 1 + \mu(p_i) f(p_i) = 1 - f(p_i)$$

Έτσι

$$F(n) = (1 - f(p_1)) \cdots (1 - f(p_\kappa)) \cdot \blacksquare$$

Παράδειγμα 4.2

Αν ο φυσικός $n > 1$ και $n = p_1^{\alpha_1} \cdots p_\kappa^{\alpha_\kappa}$ είναι η πρωτογενής μορφή του, τότε, για την συνάρτηση λ του Liouville, ισχύει

$$\sum_{d|n} \mu(d) \lambda(d) = 2^\kappa .$$

Είναι σύμφωνα με το θεώρ. 4.3

$$\sum_{d|n} \mu(d) \lambda(d) = (1 - \lambda(p_1))(1 - \lambda(p_2)) \cdots (1 - \lambda(p_\kappa)) .$$
$$= (1 - (-1))(1 - (-1)) \cdots (1 - (-1))$$
$$= \underbrace{2 \cdot 2 \cdots 2}_{\kappa\text{-φορές}} = 2^\kappa$$

αφού για $i = 1, \dots, \kappa$ είναι $\lambda(p_i) = -1$. $\blacksquare$

5. Η συνάρτηση φ του Euler

Υπενθυμίζουμε ότι, για κάθε φυσικό αριθμό n, αν παραστήσουμε με $\varphi(n)$ το πλήθος των φυσικών αριθμών που είναι $\leq n$ και πρώτοι με το n, τότε ορίζεται μια αριθμητική συνάρτηση

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N} \quad , \quad n \longmapsto \varphi(n)$$

που την καλούμε <u>συνάρτηση του Euler</u>.

Στη συνέχεια θα δούμε ορισμένα βασικά αποτελέσματα, που αφορούν τη συνάρτηση φ.

Θεώρημα 5.1 (Gauss)

Για κάθε φυσικό αριθμό n ισχύει

$$n = \sum_{d|n} \varphi(d)$$

Απόδειξη.

Αν είναι $S = \{1, 2, \ldots, n\}$ και d ένας φυσικός διαιρέτης του n.

Ορίζουμε το σύνολο

$$S_d = \{t / t \in S,\ (t,n) = d\} .$$

Παρατηρούμε ότι, για όλους τους φυσικούς διαιρέτες d του n, η συλλογή (S_d), των πεπερασμένων υποσυνόλων του S αποτελεί έναν διαμερισμό του S. Πραγματικά,

α) Για κάθε d, $1 \le d \in n$, με $d|n$, είναι $S_d \neq \phi$, αφού $d \in S_d$.

β) Αν $t \in S$, τότε, αν $(t,n) = d$, θα έχουμε $t \in S_d$, επομένως

$$S = \bigcup_{d|n} S_d$$

γ) Αν d, d_1 είναι δυο φυσικοί διαιρέτες του n, με $d \neq d_1$, τότε

$$S_d \cap S_{d_1} = \phi .$$

Πραγματικά, αν $t \in S_d \cap S_{d_1}$, τοτε $d_1 = (t,n) = d$ άτοπο.

Θα έχουμε λοιπόν

$$|S| = \sum_{d|n} |S_d| \quad \text{δηλ} \quad n = \sum_{d|n} |S_d| \qquad (14)$$

όπου το άθροισμα εκτείνεται σ' όλους τους φυσικούς διαιρέτες d του n και $|S|, |S_d|$ παριστάνουν τους πληθικούς αριθμούς των συνόλων S και S_d, αντίστοιχα.

Για να τελειώσουμε την απόδειξη σημειώνουμε ότι, αν $1 \le d \le n$ και $d|n$, τα σύνολα S_d και

$$A_d = \{b / 1 \le b \le n/d,\ (b, \tfrac{n}{d}) = 1\}$$

έχουν το ίδιο πλήθος στοιχείων.

Πραγματικά, αν $t \in S_d$, τότε $(t,n) = d$, οπότε

$\left(\frac{t}{d}, \frac{n}{d}\right) = 1$ με $1 \le \frac{t}{d} \le \frac{n}{d}$ δηλ $\frac{t}{d} \in A_d$.

Η απεικόνιση $S_d \longrightarrow A_d$, $t \longmapsto \frac{t}{d}$

είναι μιά αμφιέση, επομένως

$$|S_d| = |A_d| = \varphi\left(\frac{n}{d}\right).$$

Η σχέση (14) γράφεται τώρα

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d) \; . \; \blacksquare$$

Για παράδειγμα

$$\sum_{d|10} \varphi(d) = \varphi(1)+\varphi(2)+\varphi(5)+\varphi(10) = 1+1+4+4 = 10 .$$

Για κάθε φυσικό αριθμό n έχουμε

$$\iota(n) = \sum_{d|n} \varphi(d)$$

και από τον τύπο αντιστροφής του Mobius παίρνουμε

$$\varphi(n) = \sum_{d|n} \mu(d)\, \iota\left(\frac{n}{d}\right) \quad \text{δηλ} \quad \varphi(n) = (\mu \cdot \iota)(n),$$

οπότε

$$\varphi = \mu \cdot \iota = \iota \cdot \mu \qquad (15)$$

Πόρισμα 5.1

Για κάθε φυσικό αριθμό n ισχύει

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = \sum_{d|n} d\,\mu\left(\frac{n}{d}\right)$$

Απόδειξη.

Η σχέση 15 μας δίνει τη ζητούμενη ισότητα. $\blacksquare$

Για παράδειγμα,

$$\varphi(10) = \sum_{d|10} d\,\mu\left(\frac{n}{d}\right) = 1\cdot\mu(10)+2\mu(5)+5\mu(2)+10\mu(1)$$
$$= 1\cdot 1 + 2(-1)+5(-1)+10 = 4 .$$

Πόρισμα 5.2.
Η συνάρτηση φ του Euler είναι πολλαπλασιαστική.

Απόδειξη
Δείξαμε ότι $\varphi = \mu * \iota$ οπότε, σαν ενελικτικό γινόμενο πολλών συναρτήσεων, είναι πολλική συνάρτηση. ■

Λήμμα 5.1
Αν p είναι ένας πρώτος αριθμός και $\alpha \in \mathbb{N}$ τότε

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$$

Απόδειξη
Θεωρούμε το σύνολο $S = \{1, 2, \ldots, p^\alpha\}$ που περιέχει p^α σε πλήθος φυσικούς αριθμούς. Το $\varphi(p^\alpha)$ είναι ίσον με το πλήθος των φυσικών $n \in S$, με $(n, p^\alpha) = 1$.
Είναι φανερό ότι: $(n, p^\alpha) = 1$, εάν και μόνο εάν $p \nmid n$.
Παρατηρούμε ίσον ότι υπάρχουν $p^{\alpha-1}$ σε πλήθος φυσικοί αριθμοί από το σύνολο S οι

$$p, 2p, 3p, \ldots, p^{\alpha-1}p$$

που διαιρούνται από τον p, άρα δεν είναι πρώτοι με τον p^α.
Οι υπόλοιποι φυσικοί του S δε διαιρούνται από τον p και επομένως είναι πρώτοι με τον p^α, δηλ το S περιέχει $p^\alpha - p^{\alpha-1}$ φυσικούς πρώτους προς τον p^α. Έτσι

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right). \blacksquare$$

Έτσι αν ο p είναι πρώτος, τότε $\varphi(p) = p - 1$.
Όμοια $\varphi(9) = \varphi(3^2) = 3^2 - 3 = 6$ και
$\varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$.

Θεώρημα 5.2

Αν ο φυσικός $n>1$ έχει πρωτογενή μορφή $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_\Sigma^{\alpha_\Sigma}$, τότε

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_\Sigma}\right).$$

Απόδειξη.

Η συνάρτηση φ είναι πολλαπλή, επομένως

$$\varphi(n)=\varphi(p_1^{\alpha_1})\cdots\varphi(p_\Sigma^{\alpha_\Sigma}).$$

Από το Λήμμα 5.1 παίρνουμε

$$\varphi(n)=p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\cdots p_\Sigma^{\alpha_\Sigma}\left(1-\frac{1}{p_\Sigma}\right)=$$

$$=p_1^{\alpha_1}\cdots p_\Sigma^{\alpha_\Sigma}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_\Sigma}\right)$$

$$=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_\Sigma}\right).\ \blacksquare$$

Για παράδειγμα $1985=5\cdot 397$, οπότε

$$\varphi(1985)=1985\left(1-\frac{1}{5}\right)\left(1-\frac{1}{397}\right)=1985\cdot\frac{4}{5}\,\frac{396}{397}=4\cdot 396=1584.$$

Πόρισμα 5.3

Για κάθε φυσικό $n>2$, ο $\varphi(n)$ είναι άρτιος αριθμός.

Απόδειξη.

Αν ο n είναι δύναμη του 2, δηλ $n=2^k$, με $k\geq 2$ θα έχουμε

$$\varphi(n)=\varphi(2^k)=2^k\left(1-\frac{1}{2}\right)=2^{k-1}$$

που είναι άρτιος αριθμός.

Αν ο n δεν είναι δύναμη του 2, τότε ο n θα διαιρείται από ένα περιττό πρώτο p και επομένως

$$n=p^k m \quad \text{όπου } k\geq 1 \text{ και } (p^k,m)=1.$$

Έτσι $\varphi(n)=\varphi(p^k m)=\varphi(p^k)\varphi(m)=p^{k-1}(p-1)\varphi(m)$

που είναι άρτιος αριθμός, αφού $2\mid p-1$. $\blacksquare$

Παράδειγμα 5.1

Αν ο φυσικός $n>1$ και $n=p_1^{\alpha_1}\cdots p_\kappa^{\alpha_\kappa}$ είναι η πρωτογενής μορφή του, τότε

1) $\sum_{d|n} d\varphi(d) = \left(\frac{p_1^{2\alpha_1+1}+1}{p_1+1}\right)\cdots\left(\frac{p_\kappa^{2\alpha_\kappa+1}+1}{p_\kappa+1}\right)$

2) $\sum_{d|n} \frac{\varphi(d)}{d} = \left(1+\alpha_1\frac{(p_1-1)}{p_1}\right)\cdots\left(1+\alpha_\kappa\frac{(p_\kappa-1)}{p_\kappa}\right)$

3) $\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\varphi(n)}$.

Πραγματικά.

1) Παρατηρούμε ότι η συνάρτηση $f(n)=n\varphi(n)$ είναι πολλ/μή, επομένως και η συνάρτηση $F(n)=\sum_{d|n} d\varphi(d)$ είναι πολλ/μή. Έτσι

$$F(n)=F(p_1^{\alpha_1})\cdots F(p_\kappa^{\alpha_\kappa}) = \left(\sum_{d|p_1^{\alpha_1}} d\varphi(d)\right)\cdots\left(\sum_{d|p_\kappa^{\alpha_\kappa}} d\varphi(d)\right).$$

Η απόδειξη τελειώνει, παρατηρώντας ότι, αν p είναι πρώτος αριθμός και $\alpha\in\mathbb{N}$, τότε

$$\begin{aligned}\sum_{d|p^\alpha} d\varphi(d) &= 1\varphi(1)+p\varphi(p)+p^2\varphi(p^2)+\cdots+p^\alpha\varphi(p^\alpha)=\\ &= 1+p(p-1)+p^2(p^2-p)+\cdots+p^\alpha(p^\alpha-p^{\alpha-1})\\ &= 1-p+p^2-p^3+\cdots+(-1)^{2\alpha-1}p^{2\alpha-1}+p^{2\alpha}\\ &= \frac{p^{2\alpha+1}+1}{p+1}.\end{aligned}$$

2) Η συνάρτηση $\frac{\varphi(n)}{n}$ είναι πολλ/μή και επομένως και η $F(n)=\sum_{d|n}\frac{\varphi(d)}{d}$ είναι πολλ/μή. Έτσι

$$F(n)=F(p_1^{\alpha_1})\cdots F(p_\kappa^{\alpha_\kappa})=\left(\sum_{d|p_1^{\alpha_1}}\frac{\varphi(d)}{d}\right)\cdots\left(\sum_{d|p_\kappa^{\alpha_\kappa}}\frac{\varphi(d)}{d}\right).$$

Η απόδειξη τελειώνει παρατηρώντας ότι, αν ο p είναι πρώτος και $\alpha\in\mathbb{N}$, τότε

$$\begin{aligned}\sum_{d|p^\alpha}\frac{\varphi(d)}{d} &= \frac{\varphi(1)}{1}+\frac{\varphi(p)}{p}+\frac{\varphi(p^2)}{p^2}+\cdots+\frac{\varphi(p^\alpha)}{p^\alpha}=\\ &= 1+\frac{p-1}{p}+\frac{p^2-p}{p^2}+\frac{p^3-p^2}{p^3}+\cdots+\frac{p^\alpha-p^{\alpha-1}}{p^\alpha}=\end{aligned}$$

$$= 1 + \underbrace{\frac{p-1}{p} + \cdots + \frac{p-1}{p}}_{\alpha\text{-φορές}} = 1 + \alpha\frac{p-1}{p}.$$

3) Η συνάρτηση $f(n) = \dfrac{\mu(n)\,\mu(n)}{\varphi(n)} = \dfrac{\mu^2(n)}{\varphi(n)}$ είναι πολλ/κή, επομένως πολλ/κή είναι και η συνάρτηση

$$F(n) = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)}$$

Έτσι

$$F(n) = F(p_1^{\alpha_1}) \cdots F(p_\Sigma^{\alpha_\Sigma}) = \left(\sum_{d|p_1^{\alpha_1}} \frac{\mu^2(d)}{\varphi(d)}\right) \cdots \left(\sum_{d|p_\Sigma^{\alpha_\Sigma}} \frac{\mu^2(d)}{\varphi(d)}\right).$$

Και εδώ η απόδειξη τελειώνει παρατηρώντας ότι, αν p είναι πρώτος και $\alpha \in \mathbb{N}$, τότε

$$\sum_{d|p^\alpha} \frac{\mu^2(d)}{\varphi(d)} = \frac{\mu^2(1)}{\varphi(1)} + \frac{\mu^2(p)}{\varphi(p)} + \frac{\mu^2(p^2)}{\varphi(p^2)}^{\nearrow 0} + \cdots + \frac{\mu^2(p^\alpha)}{\varphi(p^\alpha)}^{\nearrow 0} =$$

$$= 1 + \frac{\mu^2(p)}{\varphi(p)} = 1 + \frac{(-1)^2}{p-1} = \frac{p}{p-1}$$

οπότε

$$F(n) = \frac{p_1}{p_1-1} \cdots \frac{p_\Sigma}{p_\Sigma-1} = \frac{p_1 \cdots p_\Sigma}{(p_1-1)\cdots(p_\Sigma-1)} = \frac{p_1^{\alpha_1} \cdots p_\Sigma^{\alpha_\Sigma}}{p_1^{\alpha_1-1} \cdots p_\Sigma^{\alpha_\Sigma-1}(p_1-1)\cdots(p_\Sigma-1)} =$$

$$= \frac{n}{\varphi(n)}.$$

Θεώρημα 5.3

Αν ο φυσικός $n > 1$ τότε το άθροισμα των φυσικών, που είναι μικρότεροι του n και πρώτοι με τον n, είναι ίσο με $\frac{1}{2} n\,\varphi(n)$, δηλ

$$\frac{1}{2} n \cdot \varphi(n) = \sum_{\substack{(k,n)=1 \\ 1 \le k < n}} k$$

Απόδειξη.

Έστω $t_1, \ldots, t_{\varphi(n)}$ οι φυσικοί οι μικρότεροι του n και πρώτοι προς τον n. Επειδή $(t, n) = 1$, εάν και μόνο εάν $(n-t, n) = 1$, θα έχουμε

$$t_1+\cdots+t_{\varphi(n)} = (n-t_1)+\cdots+(n-t_{\varphi(n)}) =$$

$$=\underbrace{(n+\cdots+n)}_{\varphi(n)\text{-φορές}} - (t_1+\cdots+t_{\varphi(n)}) =$$

$$= n\varphi(n) - (t_1+\cdots+t_{\varphi(n)}) .$$

Επομένως

$$2(t_1+\cdots+t_{\varphi(n)}) = n\varphi(n) \Rightarrow t_1+\cdots+t_{\varphi(n)} = \frac{1}{2}n\varphi(n),$$

πράγμα που επιθυμούσαμε. ■

6. Οι συναρτήσεις τ, σ και σ_k.

Έχουμε δείξει στο παράδειγμα 3.5 ότι οι συναρτήσεις τ και σ είναι πολλ/μές. Υπενθυμίζουμε ότι, αν $n\in\mathbb{N}$, τότε

$\tau(n)$ = πλήθος των φυσικών διαιρετών του n

$\sigma(n)$ = το άθροισμα των φυσικών διαιρετών του n.

Αλλά και διαφορετικά. αφού οι συναρτήσεις V και i είναι πολλ/μές, όμοια και οι συναρτήσεις

$$\sum_{d|n} V(i) = \underbrace{1+\cdots+1}_{\tau(n)} = \tau(n)$$

$$\sum_{d|n} i(d) = \sum_{d|n} d = \sigma(n)$$

είναι πολλ/μές. Έτσι δείξαμε το επόμενο θεώρημα

Θεώρημα 6.1

Οι συναρτήσεις τ και σ είναι πολλαπλασιαστικές. ■

Θεωρούμε τώρα για κάθε $k\in\mathbb{N}$, τη συνάρτηση

$$\sigma_k : \mathbb{N} \longrightarrow \mathbb{N} \quad , \quad n \longmapsto \sigma_k(n)$$

όπου $\sigma_k(n)$ είναι το άθροισμα των k-στων δυνάμεων των φυσικών διαιρετών του n.

Για $k=1$ είναι $\sigma_1 = \sigma$, ενώ για $k=2$ έχουμε
$\sigma_2(10) = 1^2+2^2+5^2+10^2$.

Και η συνάρτηση σ_k είναι πολλαπλασιαστική.

Πραγματικά η συνάρτηση $g(n)=n^k$ είναι φανερά πολ|μή, επομένως και η συνάρτηση

$$\sigma_k(n) = \sum_{d|n} g(d) = \sum_{d|n} d^k$$

είναι πολ|μή.

Θεώρημα 6.2

Αν ο φυσικός $n>1$ και $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ είναι η πρωτογενής μορφή του, τότε

1) $\tau(n) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)$

2) $\sigma(n) = \prod_{i=1}^{r}(1+p_i+\cdots+p_i^{\alpha_i}) = \prod_{i=1}^{r}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$

3) $\sigma_k(n) = \prod_{i=1}^{r}(1+p_i^{k}+\cdots+p_i^{\alpha_i k}) = \prod_{i=1}^{r}\frac{p_i^{k(\alpha_i+1)}-1}{p_i^k-1}$

Απόδειξη.

Αν ο p είναι ένας πρώτος και $\alpha\in\mathbb{N}$ τότε οι φυσικοί διαιρέτες του p^α είναι οι $1, p, p^2, \ldots, p^\alpha$. Επομένως,

$$\left.\begin{aligned}\tau(p^\alpha) &= \alpha+1\\ \sigma(p^\alpha) &= 1+p+p^2+\cdots+p^\alpha\\ \sigma_k(p^\alpha) &= 1+p^k+p^{2k}+\cdots+p^{\alpha k}.\end{aligned}\right\} \quad (*)$$

Αφού οι συναρτήσεις τ, σ, σ_k είναι πολ|μες, θα είναι

$$\tau(n) = \tau(p_1^{\alpha_1})\cdots\tau(p_r^{\alpha_r})$$
$$\sigma(n) = \sigma(p_1^{\alpha_1})\cdots\sigma(p_r^{\alpha_r})$$
$$\sigma_k(n) = \sigma_k(p_1^{\alpha_1})\cdots\sigma_k(p_r^{\alpha_r})$$

και αν λάβουμε υπόψη μας τις σχέσεις (*), παίρνουμε τα 1), 2), και 3). ■

Για παράδειγμα $1985 = 5 \cdot 397$, επομένως

$\tau(1985) = (1+1)(1+1) = 4$

Οι φυσικοί διαιρέτες του 1985 είναι πραγματικά τέσσερις, οι $1, 5, 397, 1985$.

Όμοια

$$\sigma(1985) = \frac{5^{1+1}-1}{5-1} \cdot \frac{397^{1+1}-1}{397-1} = \frac{24}{4} \cdot \frac{157.608}{396} =$$

$$= 2388$$

Πραγματικά $\sigma(1985) = 2388 = 1+5+397+1985$.

Παράδειγμα 6.1

Αν ο φυσικός $n>1$ και $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ είναι η πρωτογενής μορφή του, τότε

1) $\sum_{d|n} \mu(d)\tau(d) = (-1)^r$

2) $\sum_{d|n} \mu(d)\sigma(d) = (-1)^r p_1 p_2 \cdots p_r$.

Πραγματικά, σύμφωνα με θεώρημα 4.3, είναι

1) $\sum_{d|n} \mu(d)\tau(d) = (1-\tau(p_1))(1-\tau(p_2)) \cdots (1-\tau(p_r)) =$

$$= \underbrace{(1-2) \cdots (1-2)}_{r\text{-φορές}} = (-1)^r$$

και

2) $\sum_{d|n} \mu(d)\sigma(d) = (1-\sigma(p_1)) \cdots (1-\sigma(p_r))$

$$= (1-(p_1+1)) \cdots (1-(p_r+1)) =$$

$$= (-p_1) \cdots (-p_r) = (-1)^r p_1 \cdots p_r .$$

Παράδειγμα 6.2.

Για κάθε φυσικό αριθμό n έχουμε

1) $\sum_{d|n} \sigma(d) = \sum_{d|n} \frac{n}{d}\tau(d)$

2) $\sum_{d|n} \frac{n}{d}\sigma(d) = \sum_{d|n} d\cdot\tau(d)$.

Πραγματικά,

1) Η συνάρτηση $F(n) = \sum_{d|n}\sigma(d)$ είναι πολλ/μή, αφού η σ είναι πολλ/μή, σύμφωνα με το πόρισμα 4.1. Αλλά και η συνάρτηση $G(n) = \sum_{d|n}\tau(d)\frac{n}{d} = (\tau * \iota)(n)$, δηλ η συνάρτηση $G = \tau * \iota$ είναι πολλ/μή, αφού οι συναρτήσεις τ και ι είναι πολλ/μές, σύμφωνα με το θεώρημα 3.2.

Για να δείξω ότι $F = G$, αρκεί να δείξω ότι, για κάθε πρώτο p και για κάθε φυσικό αριθμό α, ισχύει

$$F(p^\alpha) = G(p^\alpha)$$

σύμφωνα με το πόρισμα 3.4.

Έτσι $F(p^\alpha) = \sum_{d|p^\alpha} = \sigma(1)+\sigma(p)+\sigma(p^2)+\cdots+\sigma(p^\alpha)$

$$= 1 + (p+1) + (1+p+p^2) + \cdots + (1+p+p^2+\cdots+p^\alpha)$$

$$= (\alpha+1) + \alpha p + (\alpha-1)p^2 + \cdots + 2p^{\alpha-1} + p^\alpha$$

και από την άλλη μεριά,

$$G(p^\alpha) = \sum_{d|p^\alpha} \frac{p^\alpha}{d}\tau(d) = \frac{p^\alpha}{1}\tau(1) + \frac{p^\alpha}{p}\tau(p) + \cdots + \frac{p^\alpha}{p^\alpha}\tau(p^\alpha) =$$

$$= p^\alpha + 2p^{\alpha-1} + \cdots + (\alpha+1)$$

πράγμα που επιδιώκαμε.

2) Η συνάρτηση $f(n) = n\tau(n)$ είναι πολλ/μή, επομένως πολλ/μή είναι και η συνάρτηση $F(n) = \sum_{d|n} d\tau(d)$.

Αλλά και η συνάρτηση

$$G(n) = \sum_{d|n}\sigma(d)\frac{n}{d} = (\sigma * \iota)(n)$$

είναι πολλ/μή, αφού το ενεργητικό γινόμενο πολλ/μων συναρτήσεων είναι επίσης πολλ/μή συνάρτηση.

Για να είναι $F = G$ αρκεί να δείξουμε ότι, για κάθε πρώτο p και κάθε φυσικό αριθμό α, ισχύει

$$F(p^\alpha) = G(p^\alpha).$$

Είναι

$$F(p^\alpha) = \sum_{d|p^\alpha} d\tau(d) = 1\cdot\tau(1) + p\,\tau(p) + \cdots + p^\alpha \tau(p^\alpha) =$$

$$= 1 + 2p + 3p^2 + \cdots + (\alpha+1)p^\alpha.$$

Από την άλλη μεριά

$$G(p^\alpha) = \sum_{d|p^\alpha} \frac{p^\alpha}{d}\sigma(d) = \frac{p^\alpha}{1}\sigma(1) + \frac{p^\alpha}{p}\sigma(p) + \cdots + \frac{p^\alpha}{p^{\alpha-1}}\sigma(p^{\alpha-1}) + \frac{p^\alpha}{p^\alpha}\sigma(p^\alpha) =$$

$$= p^\alpha + p^{\alpha-1}\sigma(p) + \cdots + p\cdot\sigma(p^{\alpha-1}) + \sigma(p^\alpha) =$$

$$= p^\alpha + p^{\alpha-1}(1+p) + \cdots + p(1+p+p^2+\cdots+p^{\alpha-1}) + (1+p+\cdots+p^\alpha) =$$

$$= (\alpha+1)p^\alpha + \alpha p^{\alpha-1} + \cdots + 2p + 1.$$

πράγμα που επιδιώκαμε. ■

Παράδειγμα 6.3

Αν ο φυσικός η είναι ελεύθερος τετραγώνου ($\nexists t\in\mathbb{N}$, $t>1$ ώστε $t^2|\eta$), τότε, για κάθε φυσικό $\kappa\geq 2$, ισχύει

$$\sum_{d|\eta} \sigma(d^{\kappa-1})\varphi(d) = \eta^\kappa$$

Πραγματικά, η συνάρτηση $g(n) = \sigma(n^{\kappa-1})$ είναι πολλ/μή, επομένως και η συνάρτηση $G(n) = g(n)\varphi(n)$ είναι πολλ/μή. Τελικά και η συνάρτηση $F(n) = \sum_{d|\eta} G(n) = \sum_{d|\eta} \sigma(d^{\kappa-1})\varphi(d)$ είναι πολλ/μή.

Αφού ο η είναι ελεύθερος τετραγώνου, η κανονική μορφή του είναι $\eta = p_1\cdot p_2\cdots p_\Sigma$. Έτσι $F(\eta) = F(p_1)\cdots F(p_\Sigma)$. Αλλά, αν ο p είναι ένας πρώτος, τότε

$$\sum_{d|p} \sigma(d^{\kappa-1})\varphi(d) = \sigma(1)\varphi(1) + \sigma(p^{\kappa-1})\varphi(p) = 1 + \frac{p^{(\kappa-1)+1}-1}{(p-1)}(p-1) = p^\kappa$$

Επομένως,

$$F(n) = \sum_{d|\eta} \sigma(d^{\kappa-1})\varphi(d) = p_1^\kappa\cdot p_2^\kappa\cdots p_\Sigma^\kappa = (p_1\cdots p_\Sigma)^\kappa = \eta^\kappa. \blacksquare$$

7. Τέλειοι αριθμοί & Αριθμοί του Mersenne

Υπάρχουν άπειροι φυσικοί αριθμοί η τέτοιοι ώστε το άθροισμα των φυσικών διαιρετών τους εκτός του η να είναι μικρότερο του η δηλ τέτοιοι ώστε

$$\sigma(\eta) - \eta < \eta .$$

Για παράδειγμα, τέτοιοι είναι όλοι οι πρώτοι αριθμοί και οι φυσικές τους δυνάμεις. (Για κάθε πρώτο p και για κάθε φυσικό κ έχουμε $\sigma(p^\kappa) - p^\kappa = 1 + p + \dots + p^{\kappa-1} = \frac{p^\kappa - 1}{p-1} < p^\kappa$).

Όμοια, υπάρχουν άπειροι φυσικοί αριθμοί η, τέτοιοι ώστε

$$\sigma(\eta) - \eta > \eta .$$

Για παράδειγμα τέτοιοι είναι όλοι οι φυσικοί αριθμοί $\eta = 2^\kappa \cdot 3$, $\kappa > 1$
(Πραγματικά $\sigma(\eta) - \eta = \sigma(2^\kappa 3) - 2^\kappa 3 = \sigma(2^\kappa)\sigma(3) - 2^\kappa 3 =$
$= (2^{\kappa+1} - 1)\, 4 - 2^\kappa 3 > 2^\kappa 3$).

Είναι φυσικό ζητήσουν, να παρουσιάζουν ενδιαφέρον οι φυσικοί αριθμοί, για τους οποίους ισχύει

$$\sigma(\eta) - \eta = \eta .$$

Ορισμός

Ένας φυσικός αριθμός καλείται **τέλειος αριθμός** (perfect number), αν είναι ίσος με το άθροισμα των φυσικών διαιρετών του εκτός του η, δηλ αν είναι λύση της εξίσωσης

$$\sigma(\eta) = 2\eta .$$

Για παράδειγμα, οι φυσικοί αριθμοί 6 και 28 είναι τέλειοι αριθμοί, αφού

$$\sigma(6) = 1 + 2 + 3 + 6 = 2 \cdot 6$$
$$\sigma(28) = 1 + 2 + 4 + 7 + 28 = 2 \cdot 28 .$$

Δεν γνωρίζουμε ακόμη αν υπάρχουν άπειροι τέλειοι αριθμοί

Πραγματικά, οι τέλειοι αριθμοί είναι πολύ σπάνιοι. Μέχρι

και το 1981 μόνο 27 τέλειοι αριθμοί είναι γνωστοί και, όπως θα δούμε πιο κάτω, όλοι τους είναι <u>άρτιοι αριθμοί</u>.

Περιττοί τέλειοι αριθμοί δεν είναι γνωστοί μέχρι τώρα και δεν είναι γνωστό αν θα μπορούν. Ένα από τα μεγάλα άλυτα προβλήματα της θεωρίας αριθμών αφορά την ύπαρξη περιττών τέλειων αριθμών.

Εκείνο, όμως, που έχει αποδειχθεί, είναι ότι, αν τέτοιοι τέλειοι αριθμοί υπάρχουν, αυτοί οφείλουν να είναι πολύ μεγάλοι. Πραγματικά, ο A. Τuscanini το 1908 απέδειξε ότι οι περιττοί τέλειοι αριθμοί οφείλουν να είναι μεγαλύτεροι του $2 \cdot 10^6$ και να έχουν τουλάχιστον πέντε διαφορετικούς πρώτους παράγοντες, ενώ ο J. Kanold το 1955 απέδειξε ότι πρέπει να είναι μεγαλύτεροι του 10^{20} και να έχουν τουλάχιστον έξη διαφορετικούς πρώτους παράγοντες. Τέλος, το 1973 ο P. Hagis απέδειξε ότι αυτοί οφείλουν να είναι μεγαλύτεροι του 10^{50} και, με την χρήση ηλεκτρονικών υπολογιστών, τελευταία, αποδείχτηκε ότι αυτοί οφείλουν να είναι μεγαλύτεροι του 10^{100}.

Ενώ όλα αυτά μας κάνουν να υποστηρίζουμε ότι δεν υπάρχουν περιττοί τέλειοι αριθμοί, μόνο μια απόδειξη για την μη-ύπαρξή τους θα μπορούσε να το συμπεράνει.

Εκείνο, όμως, που γνωρίζουμε είναι ποιοι άρτιοι φυσικοί είναι τέλειοι αριθμοί. Από τον καιρό του Ευκλείδη ήταν γνωστό ότι όλοι οι φυσικοί αριθμοί της μορφής

$$\eta = 2^{\kappa-1}(2^{\kappa}-1),$$

με τον $2^{\kappa}-1$ πρώτο αριθμό ($\kappa > 1$), είναι τέλειοι αριθμοί, ενώ 2.000 χρόνια μετά ο Euler απέδειξε και το αντίστροφο, δηλ. ότι κάθε άρτιος τέλειος αριθμός είναι της παραπάνω μορφής.

Θεώρημα 7.1.

Αν ο $2^κ-1$ είναι πρώτος αριθμός ($κ>1$), τότε ο φυσικός αριθμός

$$η=2^{κ-1}(2^κ-1) \qquad (*)$$

είναι τέλειος αριθμός και κάθε άρτιος τέλειος αριθμός είναι της μορφής (*).

Απόδειξη

Ας υποθέσουμε ότι $η=2^{κ-1}(2^κ-1)$. Επειδή $(2^{κ-1}, 2^κ-1)=1$ και η συνάρτηση $σ$ είναι πολλαπλασιαστική, θα είναι

$$σ(η)=σ\left(2^{κ-1}(2^κ-1)\right)=σ(2^{κ-1})\cdot σ(2^κ-1).$$

Αλλά

$$σ(2^{κ-1})=\frac{2^{(κ-1)+1}-1}{2-1}=2^κ-1 \quad \text{και}$$

$$σ(2^κ-1)=(2^κ-1)+1=2^κ,$$

αφού ο $2^κ-1$ είναι πρώτος αριθμός. Έτσι,

$$σ(η)=(2^κ-1)\cdot 2^κ=2\cdot η$$

που σημαίνει ότι ο $η$ είναι τέλειος αριθμός.

Από την άλλη μεριά, υποθέτουμε ότι ο $η$ είναι ένας άρτιος τέλειος αριθμός, δηλ.

$$η=2^{κ-1}m \quad , \text{ όπου } κ\geq 2 \text{ και ο } m \text{ περιττός φυσικός.}$$

Επειδή $(2^{κ-1}, m)=1$, θα είναι

$$σ(η)=σ(2^{κ-1}m)=σ(2^{κ-1})σ(m)=(2^κ-1)σ(m). \qquad (16)$$

Αλλά ο $η$ είναι τέλειος αριθμός, οπότε

$$σ(η)=2η=2\cdot 2^{κ-1}m=2^κm. \qquad (17)$$

Από τις σχέσεις (16) και (17) παίρνουμε

$$2^κm=(2^κ-1)σ(m). \qquad (18)$$

προκύπτει $2^κ-1 \mid 2^κ\cdot m$.

Επειδή $2^κ-1 \mid 2^κ\cdot m$ και $(2^κ-1, 2^κ)=1$, θα έχουμε,

σύμφωνα με το Λήμμα του Ευκλείδη (θεωρ. 6.7 Κεφ II),

$$2^k-1 \mid m$$

οπότε

$$m = (2^k-1)\,m' \quad , \quad m' \in \mathbb{N}.$$

Η σχέση (18) γράφεται τώρα

$$(2^k-1)\sigma(m) = 2^k(2^k-1)m', \text{ οπότε } \sigma(m) = 2^k m'.$$

Επειδή οι m, m' είναι διαιρέτες του m (με $m' < m$) και έχουμε επιπλέον ότι

$$m + m' = (2^k-1)m' + m' = 2^k m' = \sigma(m)$$

οι m και m' είναι οι μόνοι διαιρέτες του m, επομένως $m' = 1$ και ο $m = 2^k - 1$ είναι πρώτος αριθμός.
Έτσι $n = 2^{k-1}(2^k-1)$, πράγμα που επιθυμούσαμε. ∎

Βασικό ρόλο λοιπόν παίζουν οι φυσικοί αριθμοί

$$M_k = 2^k - 1 \qquad (k \geq 1)$$

που καλούνται <u>αριθμοί του Mersenne</u>, σε μνήμη του Γάλλου μαθηματικού Μάριν Mersenne (1588 - 1648).

Αριθμούς του Mersenne, που είναι πρώτοι αριθμοί, θα τους καλούμε <u>πρώτους του Mersenne</u>

Θα παρατηρήσουμε εδώ ότι, αν ο

$$M_p = 2^p - 1 \quad , \quad p \geq 2$$

είναι ένας πρώτος του Mersenne, τότε ο p είναι πρώτος αριθμός.

Πραγματικά, αν ο p ήταν σύνθετος, τότε $p = r \cdot s$ με $r > 1$ και $s > 1$. Αλλά τότε

$$2^p - 1 = (2^r)^s - 1 = (2^r-1)\left(2^{r(s-1)} + 2^{r(s-2)} + \dots + 2^r + 1\right)$$

και οι παράγοντες στο δεύτερο μέλος είναι μεγαλύτεροι του 1.
Ο 2^p-1 είναι επομένως σύνθετος, πράγμα άτοπο. Ο p είναι λοιπόν πρώτος αριθμός.

Έτσι ένας πρώτος του Mersenne είναι ένας πρώτος αριθμός της μορφής

$$M_p = 2^p - 1$$

με τον p πρώτο αριθμό.

Θα παρατηρήσουμε εδώ ότι υπάρχουν πρώτοι αριθμοί p, για τους οποίους ο 2^p-1 είναι σύνθετος, π.χ., αν $p=11$, τότε ο $2^{11}-1 = 23 \cdot 89$ είναι σύνθετος.

Το παραπάνω πόρισμα μας χαρακτηρίζει πλήρως τους άρτιους τέλειους αριθμούς.

Πόρισμα 7.1

Μια ικανή και αναγκαία συνθήκη για να είναι ο φυσικός αριθμός η ένας άρτιος τέλειος αριθμός είναι η

$$\eta = 2^{p-1}(2^p-1)$$

όπου ο 2^p-1 είναι ένας πρώτος του Mersenne.

Υπάρχει φυσικά μια αμφίεση μεταξύ των πρώτων του Mersenne και των τέλειων αριθμών. Το πρόβλημα, επομένως, της εύρεσης όλων των τέλειων αριθμών ανάγεται στην εύρεση όλων των πρώτων του Mersenne.

Για να τους βρούμε, παίρνουμε όλους τους πρώτους αριθμούς p ξεκινώντας από τον 2 και παρατηρούμε αν ο αριθμός 2^p-1 είναι πρώτος ή όχι.

Μέχρι το 1986 ήταν γνωστοί μόνο 30 πρώτοι του Mersenne και επομένως 30 άρτιοι τέλειοι αριθμοί που αντιστοιχούν στους 30 πρώτους αριθμούς της πρώτης στήλης στον παρακάτω πίνακα. ($2^{19.936}(2^{19937}-1)$ έχει 12.003 ψηφία στο δεκαδικό σύστημα αρίθμησης) Αν υπάρχουν άπειροι τέλειοι αριθμοί, είναι ένα άλλο δύσκολο, άλυτο μέχρι σήμερα πρόβλημα της θεωρίας αριθμών.

Πρώτοι αριθμοί	Πρώτοι του Mersenne	Άρτιοι τέλειοι αριθμοί
2	2^2-1	$2(2^2-1)$
3	2^3-1	$2^2(2^3-1)$
5	2^5-1	$2^4(2^5-1)$
7	2^7-1	$2^6(2^7-1)$
13	$2^{13}-1$	$2^{12}(2^{13}-1)$
17	$2^{17}-1$	$2^{16}(2^{17}-1)$
19	$2^{19}-1$	$2^{18}(2^{19}-1)$
31	$2^{31}-1$	$2^{30}(2^{31}-1)$
61	$2^{61}-1$	$2^{60}(2^{61}-1)$
89	$2^{89}-1$	$2^{88}(2^{89}-1)$
107	$2^{107}-1$	$2^{106}(2^{107}-1)$
127	$2^{127}-1$	$2^{126}(2^{127}-1)$
521	$2^{521}-1$	$2^{520}(2^{521}-1)$
607	$2^{607}-1$	$2^{606}(2^{607}-1)$
1279	$2^{1279}-1$	$2^{1278}(2^{1279}-1)$
2203	$2^{2203}-1$	$2^{2202}(2^{2203}-1)$
2281	$2^{2281}-1$	$2^{2280}(2^{2281}-1)$
3217	$2^{3217}-1$	$2^{3216}(2^{3217}-1)$
4253	$2^{4253}-1$	$2^{4252}(2^{4253}-1)$
4423	$2^{4423}-1$	$2^{4422}(2^{4423}-1)$
9689	$2^{9689}-1$	$2^{9688}(2^{9689}-1)$
9941	$2^{9941}-1$	$2^{9940}(2^{9941}-1)$
11213	$2^{11213}-1$	$2^{11212}(2^{11213}-1)$
19937	$2^{19937}-1$	$2^{19936}(2^{19937}-1)$
21701	$2^{21701}-1$	$2^{21700}(2^{21701}-1)$
23209	$2^{23209}-1$	$2^{23208}(2^{23209}-1)$
44497	$2^{44497}-1$	$2^{44496}(2^{44496}-1)$
86243	$2^{86243}-1$	$2^{86242}(2^{86243}-1)$
132.049	$2^{132.049}-1$	$2^{132048}(2^{132.049}-1)$
216 091	$2^{216\,091}-1$	$2^{216\,090}(2^{216.091}-1)$

Παράδειγμα 7.1

Αν ο n είναι ένας άρτιος τέλειος αριθμός, δηλ. αν $n = 2^{p-1}(2^p-1)$ με τον 2^p-1 πρώτο αριθμό, τότε

1) $\gamma(n) = \prod_{d|n} d = n^p$

2) $n = 1+2+\cdots+(2^p-1)$

3) $\varphi(n) = 2^{p-1}(2^{p-1}-1)$

Πραγματικά.

1) Σύμφωνα με το θεώρημα 1.1, είναι $\gamma(n) = n^{\tau(n)/2}$.
Αλλά $\tau(n) = (p-1+1)\cdot(1+1) = 2p$, οπότε $\gamma(n) = n^p$.

2) $1+\cdots+(2^p-1) = \frac{(2^p-1)(2^p-1+1)}{2} = 2^{p-1}(2^p-1) = n$.

3) Παρατηρούμε ότι

α) $\varphi(2^{p-1}) = 2^{p-2}$

β) $\varphi(2^p-1) = 2^p-1-1 = 2^p-2$, αφού 2^p-1 είναι πρώτος

επομένως

$$\varphi(n) = \varphi\left(2^{p-1}(2^p-1)\right) = \varphi(2^{p-1})\,\varphi(2^p-1) = 2^{p-2}(2^p-2) =$$
$$= 2^{p-1}(2^{p-1}-1). \blacksquare$$

Παράδειγμα 7.2.

Αν ο n είναι άρτιος τέλειος αριθμός, τότε $\sum_{d|n} \frac{1}{d} = 2$.

Πραγματικά ο $n = 2^{p-1}(2^p-1)$ με τον 2^p-1 πρώτο αριθμό.
Η συνάρτηση $F(n) = \sum_{d|n} \frac{1}{d}$ είναι σταθμική, επομένως
$F(n) = F(2^{p-1})\cdot F(2^p-1)$. Αλλά

$$F(2^{p-1}) = \sum_{d|2^{p-1}} \frac{1}{d} = 1+\frac{1}{2}+\cdots+\frac{1}{2^{p-1}} = \frac{2^{p-1}+\cdots+2+1}{2^{p-1}} = \frac{2^p-1}{2^{p-1}} \quad \text{και}$$

$$F(2^p-1) = \sum_{d|2^p-1} \frac{1}{d} = 1+\frac{1}{2^p-1} = \frac{2^p}{2^p-1}.$$

Έτσι $F(n) = \frac{2^p-1}{2^{p-1}}\cdot\frac{2^p}{2^p-1} = 2$. $\blacksquare$

ΚΕΦΑΛΑΙΟ IV

ΙΣΟΤΙΜΙΕΣ

1. Η έννοια της ισοτιμίας - βασικές ιδιότητες.

Ορισμός

Έστω n ένας σταθερός φυσικός αριθμός. Δυο ακέραιοι a, b καλούνται **ισότιμοι modulo n** (ισότιμοι κατά μέτρο n) και γράφουμε $a \equiv b \pmod{n}$, αν και μόνο αν η διαφορά $a-b$ είναι διαιρετή από τον n, δηλαδή

$$a \equiv b \pmod{n} \iff n \mid a-b.$$

Αν $n \nmid a-b$, θα γράφουμε $a \not\equiv b \pmod{n}$ και θα λέμε ότι ο a είναι ανισότιμος με τον b modulo n.

Για παράδειγμα, έχουμε

$$5 \equiv 15 \pmod{5}, \quad 27 \equiv 7 \pmod{4}, \quad 25 \not\equiv 12 \pmod{7}$$

αφού $5 \mid 5-15$, $4 \mid 27-7$, $7 \nmid 25-12$, αντίστοιχα.

Επίσης

i) Ο ακέραιος a είναι άρτιος $\iff a \equiv 0 \pmod{2}$

ii) Ο ακέραιος a είναι περιττός $\iff a \equiv 1 \pmod{2}$.

iii) Για κάθε ζεύγος ακεραίων a, b ισχύει $a \equiv b \pmod{1}$.

Θεώρημα 1.1

Δυο τυχόντες ακέραιοι a, b είναι ισότιμοι modulo n, δηλ $a \equiv b \pmod{n}$, εάν και μόνο εάν διαιρούμενοι με τον n δίνουν το ίδιο μη-αρνητικό υπόλοιπο.

Απόδειξη

Ας υποθέσουμε ότι $a=q_1\eta+r$ και $b=q_2\eta+r$ με $0\le r<\eta$.
Θα είναι τότε $a-b=(q_1-q_2)\eta$, δηλ $\eta|a-b$, επομένως $a\equiv b(\mathrm{mod}\eta)$
Αντίστροφα. αν $a\equiv b(\mathrm{mod}\eta)$, θα έχουμε $\eta|a-b$ δηλ
$a-b=\eta q$, $q\in\mathbb{Z}$, οπότε

$$a=b+\eta q \qquad (1)$$

Διαιρώντας τώρα τον b με τον η, παίρνουμε

$$b=k\eta+r \qquad 0\le r<\eta \qquad (2)$$

επομένως η (1) γράφεται

$$a=k\eta+\eta q+r=(k+q)\eta+r \quad \text{με} \quad 0\le r<\eta \qquad (3)$$

Οι σχέσεις τώρα (2) και (3) μάς δίνουν το αποτέλεσμα που επιθυμούσαμε. ■

Θα παρατηρήσουμε εδώ ότι η ισοτιμία mod η ορίζει μια σχέση "$\equiv$" στο σύνολο $\mathbb{Z}$ (δηλ ένα υποσύνολο $\equiv$ του $\mathbb{Z}\times\mathbb{Z}$) ως εξής:

$(a,b)\in\equiv$, εάν και μόνο εάν $a\equiv b(\mathrm{mod}\eta)$.

Η σχέση αυτή, όπως θα δούμε αμέσως παρακάτω, είναι μια σχέση ισοδυναμίας.

Θεώρημα 1.2.

Η σχέση ισοτιμίας mod η είναι μια σχέση ισοδυναμίας στο σύνολο $\mathbb{Z}$, δηλ. είναι

i) ανακλαστική: $a\equiv a(\mathrm{mod}\eta)$, για κάθε $a\in\mathbb{Z}$.

ii) συμμετρική: Αν $a\equiv b(\mathrm{mod}\eta)$, τότε $b\equiv a(\mathrm{mod}\eta)$

iii) μεταβατική: Αν $a\equiv b(\mathrm{mod}\eta)$ και $b\equiv c(\mathrm{mod}\eta)$, τότε $a\equiv c(\mathrm{mod}\eta)$.

Απόδειξη.

i) Για κάθε $a\in\mathbb{Z}$ έχουμε $\eta|a-a$, επομένως $a\equiv a(\mathrm{mod}\eta)$

ii) Αν $a\equiv b(\mathrm{mod}\eta)$, τότε $\eta|a-b$, επομένως $\eta|-(a-b)$, δηλ $\eta|b-a$, οπότε $b\equiv a(\mathrm{mod}\eta)$

iii) Αν $\left.\begin{matrix}a\equiv b(\mathrm{mod}\eta)\\ b\equiv c(\mathrm{mod}\eta)\end{matrix}\right\}\Rightarrow\left.\begin{matrix}\eta|a-b\\ \eta|b-c\end{matrix}\right\}\Rightarrow\eta|(a-b)+(b-c)$ δηλ $\eta|a-c$

που σημαίνει ότι $a\equiv c(\mathrm{mod}\eta)$. ■

Στη συνέχεια θα διατυπώσουμε ορισμένα απόμη χρήσιμα θεωρήματα για ισοτιμίες mod η.

Θεώρημα 1.3.

Αν η είναι ένας σταθερός φυσικός αριθμός και a, b, c, d τυχόντες ακέραιοι τότε ισχύουν

i) Αν $a \equiv b \pmod{\eta}$ και $c \equiv d \pmod{\eta}$, τότε

$$a+c \equiv b+d \pmod{\eta} \quad \text{και} \quad ac \equiv bd \pmod{\eta}$$

ii) Αν $a \equiv b \pmod{\eta}$, τότε

$$a+c \equiv b+c \pmod{\eta} \quad \text{και} \quad ac \equiv bc \pmod{\eta}$$

iii) Αν $a \equiv b \pmod{\eta}$, τότε

$$a^\kappa \equiv b^\kappa \pmod{\eta}, \text{ για κάθε } \kappa \in \mathbb{N}$$

iv) Αν $f(x) = c_0 + c_1 x + \cdots + c_\kappa x^\kappa$ είναι μια πολυωνυμική συνάρτηση με ακέραιους συντελεστές και $a \equiv b \pmod{\eta}$ τότε

$$f(a) \equiv f(b) \pmod{\eta}.$$

Απόδειξη

i) Αν $a \equiv b \pmod{\eta}$ και $c \equiv d \pmod{\eta}$, θα έχουμε αντίστοιχα,

$$a-b = k_1\eta \quad \text{και} \quad c-d = k_2\eta \text{ , για κάποιους ακεραίους } k_1, k_2.$$

Έτσι

$(a+c)-(b+d) = (a-b)+(c-d) = (k_1+k_2)\eta$, επομένως $a+c \equiv b+d \pmod{\eta}$

όμοια

$ac = (b+k_1\eta)(d+k_2\eta) = bd + (bk_2 + dk_1 + k_1k_2\eta)\eta$, επομένως

$\eta \mid ac-bd$ άρα $ac \equiv bd \pmod{\eta}$

ii) Με την παρατήρηση ότι $c \equiv c \pmod{\eta}$, το ζητούμενο προκύπτει άμεσως από το i)

iii) Εργαζόμαστε με επαγωγή. Για $\kappa = 1$ ισχύει. Υποθέτουμε ότι ισχύει για τον φυσικό $\kappa > 1$, δηλ $a^\kappa \equiv b^\kappa \pmod{\eta}$.

Αλλά $\left.\begin{matrix} a \equiv b \pmod{\eta} \\ a^\kappa \equiv b^\kappa \pmod{\eta} \end{matrix}\right\} \xrightarrow{i)} a^{\kappa+1} \equiv b^{\kappa+1} \pmod{\eta}$

ισχύει τοτέ και για τον φυσικό $\kappa+1$, πράγμα που επιδιώκαμε.

iv) Αφού $a \equiv b \pmod{n}$, θα είναι $a^2 \equiv b^2 \pmod{n}, \ldots, a^k \equiv b^k \pmod{n}$.
Επομένως, σύμφωνα με την ii), θα έχουμε
$c_1 a \equiv c_1 b \pmod{n}$, $c_2 a^2 \equiv c_2 b^2 \pmod{n}, \ldots, c_k a^k \equiv c_k b^k \pmod{n}$
και αν χάσουμε υπόψη μας ότι $c_0 \equiv c_0 \pmod{n}$, παίρνουμε
$c_0 + c_1 a + c_2 a^2 + \cdots + c_k a^k \equiv c_0 + c_1 b + c_2 b^2 + \cdots + c_k b^k \pmod{n}$,
σύμφωνα με την i). Έτσι $f(a) \equiv f(b) \pmod{n}$. ■

Παράδειγμα 1.1

Θα δείξουμε ότι

α) $41^{65} \equiv 6 \pmod{7}$

β) $1! + 2! + 3! + 4! + \cdots + 99! + 100! \equiv 9 \pmod{12}$

γ) $1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5 \equiv 0 \pmod{4}$

Πραγματικά

α) Παρατηρούμε ότι $41 \equiv -1 \pmod{7}$, οπότε $41^{65} \equiv (-1)^{65} \pmod{7}$,
δηλ $41^{65} \equiv -1 \pmod{7}$. Αλλά $-1 \equiv 6 \pmod{7}$ επομένως
$41^{65} \equiv 6 \pmod{7}$, που σημαίνει ότι το κύριο υπόλοιπο της
διαίρεσης του 41^{65} με τον 7 είναι 6.

β) Παρατηρούμε ότι
$1! + 2! + 3! \equiv 9 \pmod{12}$ και $4! \equiv 24 \equiv 0 \pmod{12}$
ενώ για κάθε φυσικό αριθμό $k > 4$ έχουμε
$k! \equiv 4! \cdot 5 \cdot 6 \cdots k \equiv 0 \cdot 5 \cdot 6 \cdots k \equiv 0 \pmod{12}$.
Έτσι $1! + 2! + 3! + 4! + \cdots + 99! + 100! \equiv 9 + 0 + \cdots + 0 \equiv 9 \pmod{12}$.

γ) Παρατηρούμε αρχικά ότι $2^5 + 4^5 + 6^5 + \cdots + 100^5 \equiv 0 \pmod{4}$
αφού για κάθε άρτιο φυσικό $\eta = 2a$ ισχύει
$\eta^5 = (2a)^5 = 2^2(2^3 a^5) = 4(2^3 a^5)$, δηλ. $\eta^5 \equiv 0 \pmod{4}$.
Επιπλέον έχουμε
$1 \equiv 1 \pmod{4}$, $3 \equiv -1 \pmod{4}$, $5 \equiv 1 \pmod{4}, \ldots, 99 \equiv -1 \pmod{4}$,
οπότε
$1^5 \equiv 1^5 \pmod{4}$, $3^5 \equiv -1 \pmod{4}$, $5^5 \equiv 1 \pmod{4}, \ldots, 99^5 \equiv -1 \pmod{4}$
επομένως $1^5 + 3^5 + \cdots + 99^5 \equiv 1 + (-1) + \cdots + (-1) \equiv 0 \pmod{4}$.
Έτσι $1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5 \equiv 0 + 0 \equiv 0 \pmod{4}$.

Παράδειγμα 1.2

Αν $m,n \in \mathbb{N}$, τότε $(m+n-1)! \equiv (-1)^n n!\,(m-1)! \pmod{m+n}$.

Παρατηρούμε ότι

$$(m+n-1)! = (m+n-1)\dots(m+n-n)(m-1)!$$

Άλλά

$$\big((m+n)-1\big)\dots\big((m+n)-n\big) = A(m+n) + (-1)^n n! \quad , A \in \mathbb{N}.$$

επομένως

$$(m+n-1)\dots(m+n-n) \equiv (-1)^n n! \pmod{m+n}.$$

Αν χάσουμε υπ' όψη μας ότι $(m-1)! \equiv (m-1)! \pmod{m+n}$

παίρνουμε

$$(m+n-1)\dots(m+n-n)(m-1)! \equiv (-1)^n n!\,(m-1)! \pmod{m+n}.$$

Θεώρημα 1.4

Αν ο ακέραιος $c \neq 0$ τότε

$$a \equiv b \pmod{n} \text{ εάν και μόνο εάν } ca \equiv cb \pmod{nc}$$

Απόδειξη.

Παρατηρούμε ότι

$$n \mid a-b \text{ εάν και μόνο εάν } nc \mid c(a-b)$$

δηλ $a \equiv b \pmod{n}$ εάν και μόνο εάν $ca \equiv cb \pmod{nc}$. ∎

Είδαμε στα προηγούμενα ότι, αν $a \equiv b \pmod{n}$, τότε $ca \equiv cb \pmod{n}$ για κάθε ακέραιο c. Το αντίστροφο δεν ισχύει. Πράγματι λ.χ., παρατηρούμε ότι $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$, ενώ $4 \not\equiv 1 \pmod{6}$.

Ισχύει όμως το εξής:

Θεώρημα 1.5

Αν $d = (c,n)$, τότε

$$ca \equiv cb \pmod{n} \text{ εάν και μόνο εάν } a \equiv b \pmod{\tfrac{n}{d}}$$

Απόδειξη.

Αν $a \equiv b \pmod{\frac{n}{d}}$, τότε, αφού $d \neq 0$ θα έχουμε, σύμφωνα με το

θεωρ. 1.4 $da \equiv db \pmod{n}$. Αλλά $d|c$, οπότε $c = dc_1$

Έτσι
$c_1 da \equiv c_1 db \pmod{n}$ δηλ $ca \equiv cb \pmod{n}$.

Αντίστροφα, αν $ca \equiv cb \pmod{n}$, τότε $n | c(a-b)$ και επομένως $\frac{n}{d} \Big| \frac{c}{d}(a-b)$. Αλλά $\left(\frac{n}{d}, \frac{c}{d}\right) = 1$, οπότε σύμφωνα με το λήμμα του Ευκλείδη $\frac{n}{d} \Big| (a-b)$ δηλ $a \equiv b \pmod{\frac{n}{d}}$. ■

Πόρισμα 1.1

Αν $ca \equiv cb \pmod{n}$ και $(c, n) = 1$, τότε $a \equiv b \pmod{n}$ ■

Πόρισμα 1.2

Αν $ca \equiv cb \pmod{p}$ με τον p πρώτο αριθμό τέτοιο ώστε $p \nmid c$, τότε $a \equiv b \pmod{p}$.

Απόδειξη.
Αφού $p \nmid c$ και ο p είναι πρώτος, θα έχουμε $(p, c) = 1$.
Το ζητούμενο τώρα συμπεραίνεται από το πόρισμα 1.1.

Θεώρημα 1.6

Αν $d = (a, n)$, τότε, για κάθε ακέραιο x με $x \equiv a \pmod{n}$, είναι $d = (x, n)$.

Απόδειξη
Έστω $\delta = (x, n)$. Αφού $\delta | n$ και $n | x-a$, θα έχουμε $\delta | x-a$. Αλλά $\delta | x$, οπότε $\delta | \{x-(x-a)\}$, δηλ $\delta | a$.
Είναι $\delta | a$ και $\delta | n$, οπότε $\delta | (a, n)$, δηλ $\delta | d$.
Από την άλλη μεριά, αφού $d | n$ και $n | x-a$, παίρνουμε $d | x-a$. Αλλά $d | a$, οπότε $d | \{(x-a)+a\}$, δηλ $d | x$. Έτσι αφού $d | x$ και $d | n$, έχουμε $d | (x, n)$, δηλ $d | \delta$. Τέλος τοιούτον $\delta = d$. ■

Το προηγούμενο θεώρημα μας βεβαιώνει ότι ισότιμοι ακέραιοι modη έχουν τον ίδιο μ.κ.δ με τον η.

2. Κριτήρια διαιρετότητας

Θεώρημα 2.1

Έστω $\eta = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$

η παράσταση του φυσικού αριθμού στο δεκαδικό σύστημα

$0 \le a_k < 10 \quad k = 0, 1, \cdots, m$, και

$S(\eta) = a_m + a_{m-1} + \cdots + a_1 + a_0$

$T(\eta) = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$.

Τότε

i) $9 | \eta$ εάν και μόνο εάν $9 | S(\eta)$

ii) $3 | \eta$ εάν και μόνο εάν $3 | S(\eta)$

iii) $11 | \eta$ εάν και μόνο εάν $11 | T(\eta)$.

Απόδειξη.

Θεωρούμε το πολυώνυμο $f(x) = a_0 + a_1 x + \cdots + a_m x^m$.

i) Αφού $10 \equiv 1 \pmod 9$, θα είναι $f(10) \equiv f(1) \pmod 9$.

Αλλά $f(10) = \eta$ και $f(1) = S(\eta)$, έτσι

$$\eta \equiv S(\eta) \pmod 9$$

Επομένως, $9 | \eta$ δηλ $\eta \equiv 0 \pmod 9$ εάν και μόνο εάν $S(\eta) \equiv 0 \pmod 9$ δηλ $9 | S(\eta)$.

ii) Όμοια εργαζόμαστε και εδώ, παρατηρώντας ότι $10 \equiv 1 \pmod 3$.

iii) Παρατηρούμε ότι $10 \equiv (-1) \pmod{11}$. Έτσι $f(10) \equiv f(-1) \pmod{11}$

Αλλά $f(10) = \eta$ και $f(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m = T(\eta)$,

έτσι $\eta \equiv T(\eta) \pmod{11}$.

Επομένως $11 | \eta$, δηλ $\eta \equiv 0 \pmod{11}$, εάν και μόνο εάν $T(\eta) \equiv 0 \pmod{11}$, δηλ $11 | T(\eta)$. ■

Για παράδειγμα, ο φυσικός $\eta = 7.893$, με παράσταση $\eta = 7\cdot 10^3 + 8\cdot 10^2 + 9\cdot 10 + 3$, διαιρείται από το 3 και τον 9, αφού $S(\eta) = 7+8+9+3 = 27$ και $3|27$, $9|27$. Δε διαιρείται από τον 11, αφού $T(\eta) = 3-9+8-7 = -5$ και $11 \nmid -5$. Αντίθετα, ο φυσικός $\eta = 4917$, με παράσταση $\eta = 4\cdot 10^3 + 9\cdot 10^2 + 1\cdot 10 + 7$ διαιρείται από τον 11 αφού $T(\eta) = 7-1+9-4 = 11$ και $11 | T(\eta)$.

Θεώρημα 2.2

Αν ο φυσικός αριθμός η γράφεται με την μορφή

$$\eta = 10a_1 + a_0$$

όπου $0 \le a_0 < 10$, τότε

i) $2|\eta \iff 2|a_0$,
δηλ. ο $2|\eta$, αν και μόνο αν $a_0 = 0,2,4,6,8$.

ii) $5|\eta \iff 5|a_0$,
δηλ. ο $5|\eta$ αν και μόνο αν $a_0 = 0,5$

iii) $7|\eta \iff 7|a_1 - 2a_0$

Απόδειξη.

i) Παρατηρούμε ότι $10 \equiv 0 \pmod 2$, επομένως $10a_1 \equiv 0 \pmod 2$
Έτσι $2|\eta$, δηλ. $\eta \equiv 0 \pmod 2 \iff a_0 \equiv 0 \pmod 2$, δηλ αν $2|a_0$.

ii) Όμοια $10a_1 \equiv 0 \pmod 5$, έτσι $5|\eta$ δηλ $\eta \equiv 0 \pmod 5$ εάν και μόνο εάν $a_0 \equiv 0 \pmod 5$, δηλ αν $5|a_0$.

iii) Παρατηρούμε ότι $7|\eta \iff 7|2\eta$. Αλλά $20 \equiv -1 \pmod 7$, επομένως $20a_1 \equiv -a_1 \pmod 7$. Έτσι

$$2\eta \equiv 20a_1 + 2a_0 \equiv -(a_1 - 2a_0) \pmod 7.$$

Έτσι $2\eta \equiv 0 \pmod 7 \iff a_1 - 2a_0 \equiv 0 \pmod 7$. Τελικά $7|\eta \iff 7|a_1 - 2a_0$.

Για παράδειγμα $2|4628$ και $5|5730$, ενώ $7|3542$ αφού $3542 = 354 \cdot 10 + 2$ και $7 | 354 - 2 \cdot 2$.

3. Ο δακτύλιος $\mathbb{Z}_\eta$.

Ας είναι $\eta > 1$, ένας σταθερός φυσικός αριθμός.

Είδαμε στα προηγούμενα ότι στο σύνολο $\mathbb{Z}$ των ακεραίων ορίζεται μια σχέση ισοδυναμίας "$\equiv$, από

$$a \equiv b \pmod{\eta} \iff \eta | a-b.$$

Στο εξής, για κάθε $a \in \mathbb{Z}$ θα συμβολίζουμε με $[a]_\eta$ ή αν δεν υπάρχει αμφιβολία για το μέτρο η, με $\bar{a}$, την **κλάση ισοδυναμίας** του ακεραίου a, δηλαδή

$$\bar{a} = \{x \in \mathbb{Z} \,/\, x \equiv a \pmod{\eta}\},$$

δηλαδή

$$\bar{a} = \{a + \eta q \mid q \in \mathbb{Z}\}.$$

Υπενθυμίζουμε ότι, για ακεραίους a, b, ισχύει

$$\boxed{\bar{a} = \bar{b} \iff a \equiv b \pmod{\eta}.}$$

Το σύνολο $\mathbb{Z}$ λοιπόν διαμερίζεται σε κλάσεις ισοδυναμίας mod η (η κλάσεις ισοτιμίας mod η) και το σύνολο πηλίκο $\mathbb{Z}/\equiv$ δηλ. το σύνολο όλων των διαμεριμένων κλάσεων ισοτιμίας mod η θα το συμβολίζουμε στο εξής $\mathbb{Z}_\eta$.

Για να προσδιορίσουμε τώρα τις διαμεριμένες κλάσεις ισοτιμίας mod η, δηλ τα στοιχεία του συνόλου $\mathbb{Z}_\eta$, παρατηρούμε ότι:

Για κάθε ακέραιο a η κλάση $\bar{a}$ ταυτίζεται με την κλάση $\bar{r}$, όπου r το υπόλοιπο της διαίρεσης του a με τον η δηλ

$$\bar{a} = \bar{r}, \qquad a = \eta q + r \qquad 0 \le r < \eta.$$

Πραγματικά, από τη σχέση $a = \eta q + r$ παίρνουμε $a - r = \eta q$, οπότε $a \equiv r \pmod{\eta}$, δηλ $\bar{a} = \bar{r}$.

Οι διαφορετικές, λοιπόν, τάξεις ισοτιμίας mod η είναι οι τάξεις

$$\bar{0}, \bar{1}, \ldots, \overline{\eta-1}$$

που αντιστοιχούν σε όλα τα δυνατά υπόλοιπα της διαίρεσης ενός ακεραίου a με τον η.

Έτσι

$$\mathbb{Z}_\eta = \{\bar{0}, \bar{1}, \ldots, \overline{\eta-1}\}$$

είναι δηλ. το $\mathbb{Z}_\eta$ ένα πεπερασμένο σύνολο με η στοιχεία τις τάξεις

$$\bar{0} = \{k\eta \,/\, k \in \mathbb{Z}\}$$
$$\bar{1} = \{k\eta + 1 \,/\, k \in \mathbb{Z}\}$$
$$\vdots$$
$$\overline{\eta-1} = \{k\eta + (\eta-1) \,/\, k \in \mathbb{Z}\}.$$

Έχουμε λοιπόν.

$$\mathbb{Z}_1 = \{\bar{0}\}, \quad \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}, \quad \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}, \ldots$$

Θα σημειώσουμε εδώ ότι κάθε ακέραιος x ανήκει σε μία και μόνο τάξη από τις $\bar{0}, \bar{1}, \ldots, \overline{\eta-1}$, δηλ κάθε ακέραιος x είναι ισότιμος mod η με ακριβώς ένα από τους αριθμούς $0, 1, \ldots, \eta-1$.

Στη συνέχεια παρατηρούμε ότι στο σύνολο $\mathbb{Z}$ των ακεραίων, η σχέση ισοτιμίας mod η είναι συμβιβαστή και με την πρόσθεση και τον πολλαπλασιασμό του $\mathbb{Z}$ (βλ. Θεωρ 1.3 i).

Μπορούμε λοιπόν στο σύνολο $\mathbb{Z}_\eta$ να ορίσουμε δυο πράξεις πρόσθεσης και πολλαπλασιασμού (που επάγονται από τις αντίστοιχες πράξεις στο συνολο $\mathbb{Z}$)

$$+ : \mathbb{Z}_\eta \times \mathbb{Z}_\eta \longrightarrow \mathbb{Z}_\eta \quad , \quad \cdot : \mathbb{Z}_\eta \times \mathbb{Z}_\eta \longrightarrow \mathbb{Z}_\eta ,$$

ως εξής: Για κάθε $\bar{a}, \bar{b} \in \mathbb{Z}_n$

$$\bar{a}+\bar{b} = \overline{a+b} \qquad (*)$$
$$\bar{a}\cdot\bar{b} = \overline{a\cdot b}$$

Αυτές είναι καλά ορισμένες, με την έννοια ότι τα αξιόμενα των πράξεων $\bar{a}+\bar{b}$ και $\bar{a}\cdot\bar{b}$ δεν εξαρτώνται από τους αντιπροσώπους a, b των κλάσεων, αλλά από τις κλάσεις $\bar{a}$ και $\bar{b}$, δηλ. αν $\bar{a}=\bar{x}$ και $\bar{b}=\bar{y}$, τότε $\bar{a}+\bar{b}=\bar{x}+\bar{y}$ και $\bar{a}\cdot\bar{b}=\bar{x}\cdot\bar{y}$.

Πραγματικά, έχουμε

$a \equiv x \pmod n$ και $b \equiv y \pmod n$, οπότε

$a+b \equiv x+y \pmod n$ και $a\cdot b \equiv x\cdot y \pmod n$

δηλ $\overline{a+b} = \overline{x+y}$ και $\overline{ab} = \overline{xy}$, επομένως

$\bar{a}+\bar{b} = \bar{x}+\bar{y}$ και $\bar{a}\,\bar{b} = \bar{x}\,\bar{y}$.

Για παράδειγμα, στο $\mathbb{Z}_{12}$ έχουμε

$$\overline{224} = \overline{18\cdot 12+8} = \overline{18}\cdot\overline{12}+\overline{8} = \overline{18}\cdot\bar{0}+\overline{8} = \bar{0}+\overline{8} = \overline{8} \quad \text{και}$$

$$\overline{345} = \overline{28\cdot 12+9} = \overline{28}\cdot\overline{12}+\overline{9} = \overline{28}\cdot\bar{0}+\overline{9} = \bar{0}+\overline{9} = \overline{9},$$

οπότε

$$\overline{224}+\overline{345} = \overline{8}+\overline{9} = \overline{17} = \overline{12+5} = \overline{12}+\overline{5} = \bar{0}+\overline{5} = \overline{5}.$$

Πρακτικά, βρίσκουμε το άθροισμα και το γινόμενο δύο κλάσεων προσθέτοντας ή πολλαπλασιάζοντας δύο αριθμούς αυτών των κλάσεων (κατά προτίμηση τα υπόλοιπα της διαίρεσης με το n) και κατόπιν αντικαθιστούμε το αποτέλεσμα με το υπόλοιπο της διαίρεσής του από τον n.

Έτσι έχουμε, για παράδειγμα, τους επόμενους πίνακες πρόσθεσης και πολλαπλασιασμού για το σύνολο

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}.$$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

όπου το $\bar{4}+\bar{2}$ π.χ, βρίσκεται στην τομή της γραμμής του $\bar{4}$ και της στήλης του $\bar{2}$ · το $\bar{3}\cdot\bar{5}$ βρίσκεται στην τομή της γραμμής του $\bar{3}$ και της στήλης του $\bar{5}$, κτ λ.

Είναι εύκολο τώρα να διαπιστώσουμε ότι, για τις παραπάνω πράξεις πρόσθεσης και πολλαπλασιασμού κλάσεων στο $\mathbb{Z}_\eta$, έχουμε:

1) Για κάθε $\bar{a},\bar{b},\bar{c}\in\mathbb{Z}_\eta$ ισχύουν

$$\bar{a}+(\bar{b}+\bar{c})=(\bar{a}+\bar{b})+\bar{c}$$
$$\bar{a}\cdot(\bar{b}\cdot\bar{c})=(\bar{a}\cdot\bar{b})\bar{c}$$

(προσεταιριστικές)

2) Για κάθε $\bar{a},\bar{b}\in\mathbb{Z}_\eta$ ισχύουν

$$\bar{a}+\bar{b}=\bar{b}+\bar{a}$$
$$\bar{a}\,\bar{b}=\bar{b}\cdot\bar{a}$$

(αντιμεταθετικές)

3) Υπάρχουν, συγκεκριμένα στοιχεία για την πρόσθεση και τον πολλαπλασιασμό, οι κλάσεις $\bar{0}$ και $\bar{1}$ αντίστοιχα, δηλ, για κάθε $\bar{a}\in\mathbb{Z}_\eta$, ισχύει

$$\bar{a}+\bar{0}=\bar{a}=\bar{0}+\bar{a}$$
$$\bar{a}\cdot\bar{1}=\bar{a}=\bar{1}\cdot\bar{a}$$

4) Για κάθε $\bar{a}\in\mathbb{Z}_\eta$ υπάρχει το αντίθετό του, που είναι η κλάση $\overline{-a}$, αφού

$$\bar{a}+\overline{-a}=\bar{0}=\overline{-a}+\bar{a}.$$

5) Για κάθε $\bar{a},\bar{b},\bar{c}\in\mathbb{Z}_\eta$ ισχύουν

$$\bar{a}(\bar{b}+\bar{c})=\bar{a}\bar{b}+\bar{a}\bar{c}$$
$$(\bar{a}+\bar{b})\bar{c}=\bar{a}\bar{c}+\bar{b}\bar{c}$$

(επιμεριστικοί νόμοι).

Τα παραπάνω αποδεικνύουν το επόμενο θεώρημα.

Θεώρημα 3.1

Το σύνολο $\mathbb{Z}_n$ των τάξεων ισοτιμίας mod n, εφοδιασμένο με τις πράξεις (*), δομείται σε αντιμεταθετικό δακτύλιο με μονάδα. ■

Τον δακτύλιο $\mathbb{Z}_n$ τον καλούμε **δακτύλιο των mod n κλάσεων ισοτιμίας**.

Παρατηρούμε τώρα ότι στον δακτύλιο $\mathbb{Z}_6$ οι τάξεις $\bar{1}, \bar{5}$ έχουν αντίστροφο αφού $\bar{1}\,\bar{1}=\bar{1}$ και $\bar{5}\,\bar{5}=\bar{1}$, ενώ οι τάξεις $\bar{0}, \bar{2}, \bar{3}, \bar{4}$ δεν έχουν. Επιπλέον υπάρχουν διαιρέτες του μηδενός δηλ υπάρχουν τάξεις $\bar{a}, \bar{b} \neq \bar{0}$ τέτοιες ώστε $\bar{a}\cdot\bar{b}=\bar{0}$. π.χ, για τις τάξεις $\bar{2}$ και $\bar{3}$ έχουμε $\bar{2}\cdot\bar{3}=\bar{6}=\bar{0}$.

Το επόμενο θεώρημα μας χαρακτηρίζει ποιες τάξεις του $\mathbb{Z}_n$ έχουν αντίστροφο.

Θεώρημα 3.2.

Ένα μη-μηδενικό στοιχείο $\bar{a} \in \mathbb{Z}_n$ είναι αντιστρέψιμο στο δακτύλιο $\mathbb{Z}_n$, εάν και μόνο εάν $(a,n)=1$.

Απόδειξη.

Αν $(a,n)=1$, υπάρχουν ακέραιοι x, y τέτοιοι ώστε $ax+ny=1$.
Αυτό δίνει

$$\bar{1} = \overline{ax+ny} = \overline{ax}+\overline{ny} = \overline{ax}+\bar{0} = \bar{a}\cdot\bar{x}$$

οπότε η τάξη $\bar{x}$ είναι η αντίστροφη της $\bar{a}$.
Αντίστροφα, αν η τάξη $\bar{b}$ είναι η αντίστροφη της $\bar{a}$, τότε

$$\bar{a}\,\bar{b} = \bar{1} = \bar{b}\,\bar{a}$$

Έτσι, $\boxed{\bar{a}\cdot\bar{b}=\bar{1} \iff ab \equiv 1 \pmod n}$, επομένως
$ab-1=kn \quad k\in\mathbb{Z}$, δηλ $ab+n(-k)=1$, οπότε $(a,n)=1$. ■

Παράδειγμα 3.1

Για να βρούμε το αντίστροφο της τάξης $\overline{1985}$ στο δακτύλιο $\mathbb{Z}_{132}$ (αν υπάρχει), εργαζόμαστε ως εξής:

Από τον Ευκλείδιο αλγόριθμο βρίσκουμε ότι

$$(1985, 132) = 1$$

και $\quad 1 = 1985 \cdot 53 + 132(-797) \quad$ (βλέπε Παρ. 7.1 Κεφ II)

Υπάρχει το αντίστροφο της τάξης $\overline{1985}$ και είναι η τάξη $\overline{53}$, αφού

$$\overline{1} = \overline{1985} \cdot \overline{53} + \overline{132}\ \overline{-797} = \overline{1985} \cdot \overline{53} + \overline{0} = \overline{1985} \cdot \overline{53}.$$

Θα παρατηρήσουμε εδώ ότι, αν $\bar{a} \in \mathbb{Z}_n$ και $(a,n) = d$, τότε, για κάθε κλέρασμα $x \in \bar{a}$, θα έχουμε $(x,n) = d$, δηλ. όλα τα στοιχεία της τάξης του $\bar{a}$ έχουν τον ίδιο μέγιστο κοινό διαιρέτη με τον n.

Πραγματικά, αφού $x \in \bar{a}$, θα είναι $x \equiv a \pmod n$, οπότε, σύμφωνα με το θεώρημα 1.6, θα έχουμε

$$(x,n) = (a,n) = d.$$

Αυτό μας κατοχυρώνει τον εξής ορισμό.

Ορισμός

Αν $\bar{a} \in \mathbb{Z}_n$, καλούμε διαιρέτη της $(\bmod n)$ κλάσης $\bar{a}$ τον ανεξάρτητο του αντιπροσώπου αριθμό

$$d = (a,n).$$

Θεώρημα 3.3

Ο δακτύλιος $\mathbb{Z}_p$ των $\bmod p$ τάξεων ισοτιμίας είναι σώμα, εάν και μόνο εάν ο p είναι πρώτος αριθμός.

Απόδειξη.

Αν ο p είναι πρώτος αριθμός, τότε, για κάθε $\bar{a} \in \mathbb{Z}_p - \{\bar{0}\}$

θα είναι $(a,p)=1$, αφού ο a θα είναι ισότιμος (mod n) με ένα αριθμό από τους αμέσους $1, 2, \ldots, p-1$, που έχουν με τον p μ.κ.δ τη μονάδα. Επομένως, σύμφωνα με το θεώρημα 3.2, η τάξη $\bar{a}$ είναι αντιστρέψιμη.

Αντίστροφα, αν ο δακτύλιος $\mathbb{Z}_p$ είναι σώμα, τότε κάθε τάξη $\bar{a} \in \mathbb{Z}_p - \{\bar{0}\}$ θα είναι αντιστρέψιμη. επομένως $(a,p)=1$; σύμφωνα με το θεώρημα 3.2. Αλλά, επειδή κάθε τάξη $\bar{a} \in \mathbb{Z}_p - \{\bar{0}\}$ ταυτίζεται με μία αριθμό από τις τάξεις $\bar{1}, \bar{2}, \ldots, \overline{p-1}$, θα έχουμε για κάθε x, $1 \le x \le p-1$ ότι $(x,p)=1$, που σημαίνει ότι ο p είναι πρώτος αριθμός. ■

Για παράδειγμα, οι δακτύλιοι $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$, και $\mathbb{Z}_{11}$ είναι σώματα, αφού οι φυσικοί 2, 3, 5, 7, 11 είναι πρώτοι αριθμοί.

Ορισμός.

Αν $\bar{a} \in \mathbb{Z}_n$ και ο διαιρέτης της τάξης $\bar{a}$ είναι ο 1, δηλ, αν $(a,n)=1$, τότε λέμε την τάξη $\bar{a}$ πρωτογενή ή στοιχειώδη.

Κάθε πρωτογενής τάξη $\bar{a} \in \mathbb{Z}_n$ είναι αντιστρέψιμη στο δακτύλιο $\mathbb{Z}_n$, σύμφωνα με το θεωρ. 3.2.

Στο εξής, θα παριστάνουμε με H_n το σύνολο των πρωτογενών τάξεων του $\mathbb{Z}_n$. Το H_n, λοιπόν, δεν είναι παρά το σύνολο όλων των αντιστρέψιμων στοιχείων του δακτύλιου $\mathbb{Z}_n$, δηλαδή

Ένας αντιμεταθετικός δακτύλιος R με μονάδα $1 \neq 0$ λέγεται σώμα, αν κάθε μη-μηδενικό στοιχείο του είναι αντιστρέψιμο.

$$H_n = \{\bar{a} \in \mathbb{Z}_n \;/\; (a,n)=1\}$$

Το H_n είναι ένα πεπερασμένο σύνολο με $\varphi(n)$ σε πλήθος στοιχεία, όπου φ η συνάρτηση του Euler.

Πραγματικά, υπάρχουν τόσες σε πλήθος πρωτογενείς τάξεις (mod n) όσοι είναι και οι φυσικοί αριθμοί a με $1 \le a \le n$ και $(a,n)=1$, που είναι $\varphi(n)$ σε πλήθος, σύμφωνα με τον ορισμό της συνάρτησης του Euler. Έτσι $|H_n| = \varphi(n)$.

Θεώρημα 3.4

Το σύνολο H_n των (mod n) πρωτογενών τάξεων εφοδιασμένο με την πράξη του πολλαπλασιασμού τάξεων, δομείται σε αντιμεταθετική ομάδα.

Απόδειξη

Το σύνολο H_n είναι κλειστό ως προς τον πολλαπλασιασμό δηλ.

για κάθε $\bar{a}, \bar{b} \in H_n \Rightarrow \bar{a}\,\bar{b} \in H_n$.

Πραγματικά, αφού $\bar{a}, \bar{b} \in H_n$, θα είναι $(a,n)=(b,n)=1$, οπότε $(ab,n) = (n,(a,n)(b,n)) = (n,1) = 1$, που σημαίνει ότι $\overline{ab} = \bar{a}\,\bar{b} \in H_n$.

Επιπλέον παρατηρούμε ότι ο πολλαπλασιασμός είναι προσεταιριστικός και αντιμεταθετικός, ενώ η τάξη $\bar{1} \in H_n$ είναι το ουδέτερο στοιχείο.

Μένει να δείξουμε ότι, για κάθε $\bar{a} \in H_n$, υπάρχει τάξη $\bar{b} \in H_n$, τέτοια ώστε $\bar{a}\,\bar{b} = \bar{1}$.

Πραγματικά, η τάξη $\bar{a}$ είναι αντιστρέψιμη αφού $\bar{a} \in H_n$, επομένως υπάρχει $\bar{b} \in \mathbb{Z}_n$, τέτοια ώστε $\bar{a}\,\bar{b} = \bar{1}$.

Θα δείξουμε ότι $\bar{b} \in H_n$, δηλ. ότι $(b,n)=1$.

Αφού $\overline{ab} = \bar{1}$, θα είναι $ab \equiv 1 \pmod n$, οπότε $(ab,n) = (1,n) = 1$. Έτσι

$$(b,n) = (b,ab,n) = (b,(ab,n)) = (b,1) = 1. \blacksquare$$

Για $n=5$ η ομάδα H_5 περιέχει $\varphi(5) = 5-1 = 4$ τάξεις τις $\bar{1}, \bar{2}, \bar{3}, \bar{4}$, δηλ. $H_5 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.

Όμοια $H_6=\{\bar{1},\bar{5}\}$, $H_7=\{\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}\}$ και $H_8=\{\bar{1},\bar{3},\bar{5},\bar{7}\}$.

Οι δακτύλιοι $\mathbb{Z}_n$ πρωτοεμφανίστηκαν ουσιαστικά το 1801 στο περίφημο έργο "Disquitiones Arithmeticae" του F. Gauss. Οι δακτύλιοι $\mathbb{Z}_n$ αποτελούν ένα σημαντικό εργαλείο για τη μελέτη των διοφαντικών εξισώσεων και γενικά των ιδιοτήτων των ακεραίων, όπως θα δούμε στα επόμενα.

4. Τα θεωρήματα των Euler και Fermat

Ορισμός

Καλούμε πλήρες σύστημα υπολοίπων (mod n) ένα σύνολο από n σε πλήθος ακέραιους

$$\{a_1,\dots,a_n\}$$

τέτοιο ώστε

$$a_i \not\equiv a_j \pmod n \quad , i\neq j .$$

Αν χρησιμοποιούμε $\mathbb{Z}_n=\{\bar{x}_1,\bar{x}_2,\dots,\bar{x}_n\}$, τότε παίρνοντας από κάθε κλάση ισοτιμίας (mod n) $\bar{x}_1,\dots,\bar{x}_n$ ένα ακέραιο, έχουμε ένα πλήρες σύστημα υπολοίπων (mod n)

$$\{a_1,\dots,a_n\}$$

όπου $a_i\in\bar{x}_i$ $\quad i=1,\dots,n$.

Στην περίπτωση αυτή, κάθε ακέραιος y είναι ισότιμος με ένα και μόνο ένα στοιχείο του συνόλου $\{a_1,\dots,a_n\}$, δηλ., για κάθε $y\in\mathbb{Z}$, υπάρχει μοναδικό $i\in\{1,\dots,n\}$ έτσι ώστε $y\equiv a_i \pmod n$.

Διακρίνουμε ειδικά τα εξής πλήρη συστήματα υπολοίπων (mod n):

1) Ελάχιστο μη-αρνητικό πλήρες σύστημα υπολοίπων (mod n)

$$\{0,1,\dots,n-1\}.$$

2) Ελάχιστο θετικό πλήρες σύστημα υπολοίπων (mod n)
$\{1, 2, \dots, n\}$

3) Πλήρες σύστημα των απόλυτα ελαχίστων υπολοίπων (mod n)

i) Για η περιττό $\left\{-\frac{n-1}{2}, \dots, -1, 0, 1, \dots, \frac{n-1}{2}\right\}$.

ii) Για η άρτιο $\left\{-\left(\frac{n}{2}-1\right), \dots, -1, 0, 1, \dots \frac{n}{2}\right\}$.

Για παράδειγμα, αν $n=6$, το πλήρες σύστημα των απόλυτα ελαχίστων υπολοίπων (mod 6) είναι το $\{0,1,2,3,-2,-1\}$. Αν $n=7$, αυτό είναι το $\{-3,-2,-1,0,1,2,3\}$.

Παράδειγμα 1.1

Αν η είναι ένας περιττός φυσικός $n>1$ και $\{x_1, \dots, x_n\}$ ένα πλήρες σύστημα υπολοίπων (mod n), τότε

$$\sum_{i=1}^{n} x_i \equiv 0 \pmod{n}$$

Πραγματικά, αφού τα σύνολα $\{x_1, \dots, x_n\}$ και $\{1, 2, \dots, n\}$ είναι δύο πλήρη συστήματα υπολοίπων (mod n), κάθε αριθμός x_i, $i=1, \dots, n$ θα είναι ισότιμος με ένα ακριβώς $\lambda \in \{1, \dots, n\}$, δηλαδή, υπάρχει μετάθεση $(\lambda_1 \lambda_2 \dots \lambda_n)$ του συνόλου $\{1, \dots, n\}$ τέτοια ώστε

$$x_i \equiv \lambda_i \pmod{n} \qquad i = 1, \dots, n.$$

Έτσι $\sum_{i=1}^{n} x_i \equiv \sum_{i=1}^{n} \lambda_i \pmod{n}$.

Αλλά $\sum_{i=1}^{n} \lambda_i = 1 + 2 + \dots + n = \frac{n(n+1)}{2} \equiv 0 \pmod{n}$,

γιατί ο $\frac{n+1}{2}$ είναι ακέραιος, αφού ο η είναι περιττός.

Τελικά, $\sum_{i=1}^{n} x_i \equiv 0 \pmod{n}$. ■

Θεώρημα 4.1

Αν το σύνολο $\{x_1, x_2, \ldots, x_n\}$ είναι ένα πλήρες σύστημα υπολοίπων $(\mathrm{mod} n)$ και $(a,n)=1$, τότε και το σύνολο

$$\{ax_1, \ldots, ax_n\}$$

είναι ένα πλήρες σύστημα υπολοίπων $(\mathrm{mod} n)$.

Απόδειξη

Αρκεί να δείξουμε ότι $ax_i \not\equiv ax_j \ (\mathrm{mod} n)$ με $i \neq j$. Υποθέτουμε ότι υπάρχουν i, j, με $i \neq j$, έτσι ώστε $ax_i \equiv ax_j \ (\mathrm{mod} n)$. Αλλά $(a,n)=1$ επομένως, σύμφωνα με το πόρισμα 1.1, θα είναι $x_i \equiv x_j \ (\mathrm{mod} n)$, $i \neq j$, πράγμα άτοπο. ■

Ορισμός

Θα λέμε ένα σύνολο από $\varphi(n)$ σε πλήθος ακέραιους

$$\{a_1, \ldots, a_{\varphi(n)}\}$$

ανάγμενο (ή περιορισμένο) σύστημα υπολοίπων $(\mathrm{mod} n)$, όταν

1) $a_i \not\equiv a_j \ (\mathrm{mod} n)$, $i \neq j$

2) $(a_i, n) = 1$, για κάθε $i \in \{1, 2, \ldots, \varphi(n)\}$

Αν λοιπόν $H_n = \{\bar{x}_1, \ldots, \bar{x}_{\varphi(n)}\}$, τότε, παίρνοντας από κάθε πρωτογενή κλάση ισοτιμίας $(\mathrm{mod} n)$ $\bar{x}_1, \ldots, \bar{x}_{\varphi(n)}$ ένα ακέραιο, έχουμε ένα ανάγμενο σύστημα υπολοίπων $(\mathrm{mod} n)$

$$\{a_1, \ldots, a_{\varphi(n)}\},$$

όπου $a_i \in \bar{x}_i$, $i = 1, \ldots, \varphi(n)$.

Στην περίπτωση αυτή, κάθε ακέραιος y με $(y,n) = 1$ είναι ισότιμος με ένα και μόνο ένα στοιχείο του συνόλου $\{a_1, \ldots, a_{\varphi(n)}\}$, δηλ. για κάθε $y \in \mathbb{Z}$ με $(y,n)=1$ υπάρχει μοναδικό $i \in \{1, \ldots, \varphi(n)\}$, έτσι ώστε $y \equiv a_i \ (\mathrm{mod} n)$.

Ειδικά το ανάγμενο σύστημα ελάχιστων θετικών υπολοίπων $(\mathrm{mod} n)$ αποτελείται από εκείνους τους ακέραιους του συνόλου $\{1, \ldots, n\}$, που είναι πρώτοι με τον n.

Για παράδειγμα, για κάθε πρώτο p το σύνολο $\{1, 2, \dots, p-1\}$ είναι ένα αναγμένο σύστημα υπολοίπων mod p.

Λήμμα 4.1.

Αν το σύνολο $\{x_1, \dots, x_{\varphi(n)}\}$ είναι ένα αναγμένο σύστημα υπολοίπων (mod n) και $(a, n) = 1$, τότε και το σύνολο

$$\{ax_1, \dots, ax_{\varphi(n)}\}$$

είναι όμοια ένα αναγμένο σύστημα υπολοίπων (mod n)

Απόδειξη.

Για τους $\varphi(n)$ σε πλήθος ακεραίους $ax_1, \dots, ax_{\varphi(n)}$ έχουμε:

1) $(ax_i, n) = (n, (a, n)(x_i, n)) = (n, 1) = 1$, για κάθε $i \in \{1, \dots, \varphi(n)\}$.

2) $ax_i \not\equiv ax_j \pmod n$, με $i \neq j$.

Πραγματικά αν υποθέσουμε ότι για κάποια i, j με $i \neq j$ είναι $ax_i \equiv ax_j \pmod n$, τότε, επειδή $(a, n) = 1$, θα έχουμε $x_i \equiv x_j \pmod n$, για κάποια i, j με $i \neq j$ πράγμα άτοπο. ∎

Στη συνέχεια, θα αποδείξουμε τρία βασικά θεωρήματα της αριθμοθεωρίας.

Θεώρημα 4.2 (Euler)

Αν ο n είναι φυσικός αριθμός και $(a, n) = 1$ τότε

$$a^{\varphi(n)} \equiv 1 \pmod n$$

Απόδειξη.

Για $n = 1$ φανερά ισχύει. Έστω $n > 1$ και

$$\{a_1, a_2, \dots, a_{\varphi(n)}\} \qquad (I)$$

ένα αναγμένο σύστημα υπολοίπων (mod n).

Σύμφωνα με το λήμμα 4.1, αφού $(a, n) = 1$, και το σύνολο

$$\{aa_1, aa_2, \dots, aa_{\varphi(n)}\} \qquad (II)$$

είναι ένα αναγμένο σύστημα υπολοίπων (mod n).
Κάθε ακέραιος μοιπόν της (II) είναι ισότιμος (mod n) με ένα και μόνο ένα ακέραιο του (I) και έστω

$$\begin{aligned} a a_1 &\equiv a_1' \pmod n \\ a a_2 &\equiv a_2' \pmod n \\ &\vdots \\ a a_{\varphi(n)} &\equiv a_{\varphi(n)}' \pmod n \end{aligned}$$

όπου οι ακέραιοι $a_1', a_2', \dots, a_{\varphi(n)}'$ είναι οι $a_1, a_2, \dots, a_{\varphi(n)}$ με κάποια τάξη.

Παίρνοντας το γινόμενο των $\varphi(n)$ σε μηδός ισοτιμιών, έχουμε

$$\begin{aligned} (a a_1) \cdots (a a_{\varphi(n)}) &\equiv a_1' \cdots a_{\varphi(n)}' \pmod n \\ &\equiv a_1 \cdots a_{\varphi(n)} \pmod n \end{aligned}$$

επομένως

$$a^{\varphi(n)} (a_1 \cdots a_{\varphi(n)}) \equiv a_1 \cdots a_{\varphi(n)} \pmod n$$

Αλλά $(a_1 \cdots a_{\varphi(n)}, n) = 1$, αφού $(a_i, n) = 1$, για κάθε $i \in \{1, \dots, \varphi(n)\}$ μπορούμε μοιπόν να απλοποιήσουμε, σύμφωνα με το πόρισμα 1.1 και έχουμε

$$a^{\varphi(n)} \equiv 1 \pmod n \ . \ \blacksquare$$

Το θεώρημα του Euler, με άλλα λόγια, μας βεβαιώνει ότι, αν $\bar{a}$ είναι ένα στοιχείου του $\mathbb{Z}_n$ που είναι αντιστρέψιμο, δηλ αν $\bar{a}$ είναι ένα στοιχείο της πολλαπλής ομάδας H_n των πρωτογενών κλάσεων (mod n) τότε

$$\bar{a}^{\varphi(n)} = \bar{1} \ .$$

Πραγματικά, αφού $a^{\varphi(n)} \equiv 1 \pmod n$, περνώντας στις κλάσεις έχουμε την επόμενη ισότητα

$$\underbrace{\bar{a} \cdots \bar{a}}_{\varphi(n) \text{ φορές}} = \bar{1} \qquad \text{δηλ} \quad \bar{a}^{\varphi(n)} = \bar{1} \ .$$

Παρατήρηση.

Μπορούμε να πάρουμε μια άλλη απόδειξη του θεωρήματος του Euler χρησιμοποιώντας θεωρία ομάδων. Υπενθυμίζουμε ότι: τάξη ενός στοιχείου x μιας πολλ/της ομάδας G καλούμε τον ελάχιστο φυσικό αριθμό s (αν υπάρχει) έτσι ώστε $x^s=1$. Είναι φανερό ότι, αν η ομάδα G είναι πεπερασμένη, τότε τα στοιχεία της έχουν πεπερασμένη τάξη· ενώ από το θεώρημα του Lagrange έχουμε ότι οι τάξεις των στοιχείων μιας πεπερασμένης ομάδας διαιρούν την τάξη της ομάδας.

Στην ενημερωμένη περίπτωση η τάξη της ομάδας H_n είναι $\varphi(n)$ και, αν η κλάση $\bar{a}\in H_n$ έχει τάξη s, τότε

$$\bar{a}^s=\bar{1} \quad \text{και} \quad s\mid\varphi(n).$$

Έτσι $\varphi(n)=sk$, οπότε $(\bar{a}^s)^k=\bar{1}^k=\bar{1}$, δηλ $\bar{a}^{\varphi(n)}=\bar{1}$, επομένως $a^{\varphi(n)}\equiv 1 \pmod n$, όταν $(a,n)=1$, αφού $\bar{a}\in H_n$. ■

Για παράδειγμα, $3^{40}\equiv 1 \pmod{100}$, αφού

$$\varphi(100)=\varphi(2^2\cdot 5^2)=100\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{5}\right)=40.$$

Θεώρημα 4.3 (Fermat)

Αν ο p είναι πρώτος αριθμός και $p\nmid a$ τότε

$$a^{p-1}\equiv 1 \pmod p.$$

Απόδειξη.

Αφού ο p είναι πρώτος και $p\nmid a$ θα είναι $(a,p)=1$. Από το θεώρημα του Euler τώρα παίρνουμε ότι $a^{\varphi(p)}\equiv 1 \pmod p$ και επειδή $\varphi(p)=p-1$, έχουμε

$$a^{p-1}\equiv 1 \pmod p. \ ■$$

Μία ανεξάρτητη απόδειξη του θεωρήματος του Fermat μπορούμε να πάρουμε, αν εργαστούμε όπως και στο θεώρημα του Euler.

Για παράδειγμα, έχουμε $5^{16} \equiv 1 \pmod{17}$, αφού ο 17 είναι πρώτος αριθμός και $17 \nmid 5$.

Πόρισμα 4.1

Αν ο p είναι πρώτος αριθμός, τότε, για κάθε $a \in \mathbb{Z}$, ισχύει

$$a^p \equiv a \pmod{p}$$

Απόδειξη.

Αν $p \mid a$, δηλ αν $a \equiv 0 \pmod{p}$, τότε $a^p \equiv 0 \pmod{p}$, οπότε $a^p \equiv a \pmod{p}$.

Αν $p \nmid a$, τότε, από το θεώρημα του Fermat έχουμε $a^{p-1} \equiv 1 \pmod{p}$, οπότε $a^p \equiv a \pmod{p}$. ■

Πόρισμα 4.2

Αν οι p, q είναι διαφορετικοί πρώτοι αριθμοί και

$$a^p \equiv a \pmod{q} \quad , \quad a^q \equiv a \pmod{p}$$

τότε

$$a^{pq} \equiv a \pmod{pq}$$

Απόδειξη.

Σύμφωνα με το πόρισμα 4.1, έχουμε $a^p \equiv a \pmod{p}$, οπότε $(a^p)^q \equiv a^q \pmod{p}$. Αλλά $a^q \equiv a \pmod{p}$, από την υπόθεσή μας, επομένως

$$a^{pq} \equiv a \pmod{p}, \text{ δηλ } p \mid a^{pq} - a \qquad (4)$$

Όμοια έχουμε,

$a^q \equiv a \pmod{q}$, οπότε $(a^q)^p \equiv a^p \pmod{q}$

Αλλά $a^p \equiv a \pmod{q}$, επομένως $a^{pq} \equiv a \pmod{q}$, δηλ

$$q \mid a^{pq} - a \qquad (5)$$

Από τις σχέσεις (4) και (5) και το γεγονός ότι $(p, q) = 1$, παίρνουμε (βλ. Πόρισμα 6.8, Κεφ. II)

$$pq \mid a^{pq} - a, \text{ δηλ. } a^{pq} \equiv a \pmod{pq}. \blacksquare$$

Παράδειγμα 4.2

Θα δείξουμε ότι $2^{340} \equiv 1 \pmod{341}$.

Παρατηρούμε ότι $341 = 11 \cdot 31$ με τους 11 και 31 πρώτους αριθμούς και ότι $2^5 \equiv 1 \pmod{31}$ και $2^{10} \equiv 1 \pmod{11}$. Έτσι

$$2^{11} \equiv 2 \pmod{31} \quad \text{και} \quad 2^{31} \equiv 2 \pmod{11},$$

οπότε το πόρισμα 4.2 μας δίνει

$$2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31},$$

δηλαδή

$$2^{341} \equiv 2 \pmod{341}$$

Επειδή όμως $(2, 341) = 1$, εφαρμόζοντας σύμφωνα με το πόρισμα 1.1 παίρνουμε:

$$2^{340} \equiv 1 \pmod{341}. \blacksquare$$

Το αντίστροφο ακριβώς του θεωρήματος Fermat δεν ισχύει, με άλλα λόγια, αν $a^{n-1} \equiv 1 \pmod{n}$, για κάποιο ακέραιο a, τότε ο n δεν είναι αναγκαία πρώτος αριθμός. Πραγματικά, στο παράδειγμα 4.2 δείξαμε ότι για $n = 341$ ισχύει, $2^{341-1} \equiv 1 \pmod{341}$ με τον $n = 341 = 11 \cdot 31$ σύνθετο. Το θεώρημα 6.1 πιο κάτω, μας δίνει ένα κριτήριο για πρώτο αριθμό.

Παράδειγμα 4.3

Θα δείξουμε ότι $5^{38} \equiv 2 \pmod{17}$

Πραγματικά, είναι $5^{16} \equiv 1 \pmod{17}$, όπως είδαμε προηγούμενα. Επιπλέον έχουμε

$$5^{38} = 5^{16 \cdot 2 + 6} = (5^{16})^2 (5^6) = (5^{16})^2 \cdot (5^3)^2$$

Αλλά $(5^{16})^2 \equiv 1 \pmod{17}$ και

$5^3 = 125 \equiv 6 \pmod{17}$, οπότε $(5^3)^2 \equiv 6^2 \equiv 2 \pmod{17}$

Έτσι $5^{38} = (5^{16})^2 (5^3)^2 \equiv 2 \pmod{17}$.

Παράδειγμα 4.4

Αν ο p είναι ένας περιττός πρώτος αριθμός, τότε

1) $1^{p-1}+2^{p-1}+3^{p-1}+\cdots+(p-1)^{p-1}\equiv(-1)\pmod p$

2) $1^{p}+2^{p}+\cdots+(p-1)^{p}\equiv 0\pmod p$.

Πραγματικά,

1) Για κάθε φυσικό κ, $1\le\kappa\le p-1$, αφού $p\nmid\kappa$, θα έχουμε από

$$\kappa^{p-1}\equiv 1\pmod p$$

Έτσι, για $\kappa=1,2,\ldots,p-1$ παίρνουμε

$$\begin{aligned}1^{p-1}&\equiv 1\pmod p\\ 2^{p-1}&\equiv 1\pmod p\\ &\vdots\\ (p-1)^{p-1}&\equiv 1\pmod p\end{aligned}$$

Προσθέτοντας τις παραπάνω ισοτιμίες έχουμε

$$1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}\equiv \underbrace{1+\cdots+1}_{(p-1)\text{ φορές}}\pmod p \quad \text{δηλ.}$$

$$1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}\equiv(p-1)\pmod p.$$

Αλλά $p-1\equiv(-1)\pmod p$ οπότε $1^{p-1}+\cdots+(p-1)^{p-1}\equiv(-1)\pmod p$.

2) Από το πόρισμα 4.1 παίρνουμε

$$\begin{aligned}1^{p}&\equiv 1\pmod p\\ 2^{p}&\equiv 2\pmod p\\ &\vdots\\ (p-1)^{p}&\equiv(p-1)\pmod p\end{aligned}$$

Προσθέτοντας τις παραπάνω ισοτιμίες έχουμε

$$1^{p}+2^{p}+\cdots+(p-1)^{p}\equiv 1+2+\cdots+(p-1)\pmod p$$

Αλλά $1+2+\cdots+(p-1)=\dfrac{p(p-1)}{2}$ και επειδή p είναι περιττός

$2\mid p-1$, οπότε $1+2+\cdots+(p-1)\equiv 0\pmod p$. Έτσι

$$1^{p}+2^{p}+\cdots+(p-1)^{p}\equiv 0\pmod p.\ \blacksquare$$

5. Γραμμικές ισοτιμίες

Καλούμε γραμμική ισοτιμία ή ισοτιμία πρώτου βαθμού κάθε "ισοτιμία" της μορφής

$$ax \equiv b \pmod{n} \qquad (I)$$

όπου $n \in \mathbb{N}$ και $a, b \in \mathbb{Z}$.

Θα παρατηρήσουμε εδώ ότι η ισοτιμία (I) είναι μια "υπογήσια ισοτιμία" στον δακτύλιο $\mathbb{Z}$ των ακεραίων. Δηλ αναζητούμε τις ακέραιες τιμές του x που καθιστούν τα δυο μέλη της (I) αριθμούς ισότιμους $(\bmod n)$.

Θα λέμε ότι ο ακέραιος x_0 "επαληθεύει" την (I), αν

$$ax_0 \equiv b \pmod{n}$$

Αν για κάθε $u \in \mathbb{Z}$ είναι $au \not\equiv b \pmod{n}$, θα λέμε ότι η (I) δεν έχει λύση.

Για παράδειγμα η ισοτιμία $2x \equiv 3 \pmod 4$ δεν έχει λύση, αφού, για κάθε $u \in \mathbb{Z}$, ο $2u-3$ είναι περιττός και $4 \nmid 2u-3$.

Αν ο ακέραιος x_0 επαληθεύει την (I), δηλ $ax_0 \equiv b \pmod n$, τότε και κάθε ακέραιος x', $x' \equiv x_0 \pmod n$ επαληθεύει την (I), δηλ $ax' \equiv b \pmod n$.

Πραγματικά, αν $x' \equiv x_0 \pmod n$, τότε και $ax' \equiv ax_0 \pmod n$, οπότε $ax' \equiv b \pmod n$.

Αυτό μας οδηγεί στον επόμενο ορισμό

Ορισμός

Μια **λύση** της γραμμικής ισοτιμίας (I) θα λέμε ένα ακέραιο x_0 που την επαληθεύει δηλ. $ax_0 \equiv b \pmod n$, μαζί με όλους τους ισότιμους $(\bmod n)$ με τον x_0 ακεραίους.

Στην περίπτωση αυτή θα λέμε ότι η ισοτιμία (I) έχει μια ρίζα, την

$$x \equiv x_0 \pmod n \quad \text{ή} \quad x_0 \pmod n.$$

Δυο ρίζες χοιηόν $x_1, x_2 \pmod n$ της (I) θα είναι διαφορετικές, αν $x_1 \not\equiv x_2 \pmod n$

Για παράδειγμα, οι ακέραιοι 3 και -9 πληρούν τη γραμμική ισοτιμία $3x \equiv 9 \pmod{12}$ και $3 \equiv -9 \pmod{12}$. Οι ρίζες επομένως $x \equiv 3 \pmod{12}$ και $x \equiv -9 \pmod{12}$ δεν είναι διαφορετικές. Αντίθετα, οι ακέραιοι 3 και 7 την πληρούν και $3 \not\equiv 7 \pmod{12}$, επομένως οι ρίζες $x \equiv 3 \pmod{12}$ και $x \equiv 7 \pmod{12}$ είναι διαφορετικές.

Σαν ρίζες χοιηόν της γραμμικής ισοτιμίας (I) δουρούνται κλάσεις ισοδυναμίας $(\bmod n)$, πράγμα φυσικό, αφού η λύση της γραμμικής ισοτιμίας

$$ax \equiv b \pmod n$$

είναι ισοδύναμη με την λύση της εξίσωσης

$$\bar{a}\bar{x} = \bar{b}$$

στο δακτύλιο $\mathbb{Z}_n$.

Αν λοιπόν $\{x_1, \ldots, x_n\}$ είναι ένα πλήρες σύστημα υποδοίπων $(\bmod n)$ δοκιμάζοντας διαδοχικά όλους τους ακέραιους r_i στην (I), βρίσκουμε ποιοι από αυτούς την πληρούν, βρίσκοντας έτσι όλες τις ρίζες (αν υπάρχουν) της (I). Αυτό φαίνεται χαρακτηριστικά στο επόμενο παράδειγμα.

Παράδειγμα 5.1.

Θα βρούμε τις ρίζες της ισοτιμίας

$$3x \equiv 9 \pmod{12}$$

Το σύνολο $\{0, 1, 2, \ldots, 11\}$ είναι ένα πλήρες σύστημα υποδοίπων $(\bmod 12)$. Δοκιμάζοντας αυτούς, βρίσκουμε

οι αιέραιοι 3, 7 και 11 την επαληθεύουν αφού

$3 \cdot 3 \equiv 9 \pmod{12}$, $3 \cdot 7 \equiv 9 \pmod{12}$, $3 \cdot 11 \equiv 9 \pmod{12}$

Η ισοτιμία έχει τοιπόν μόνο τρεις λύσεις, τις

$x \equiv 3 \pmod{12}$, $x \equiv 7 \pmod{12}$, $x \equiv 11 \pmod{12}$

ή, πιο σύντομα, τις $x \equiv 3, 7, 11 \pmod{12}$.

Ο τρόπος αυτός εφαρμόζεται για μικρούς αιέραιους n. Για μεγάλα n η εργασία είναι αρκετά επίπονη.

Θεώρημα 5.1

Η ικανή και αναγκαία συνθήκη για να δέχεται η γραμμική ισοτιμία

$$ax \equiv b \pmod{n} \qquad (I)$$

λύση είναι η $\delta = (a, n) \mid b$.

Στην περίπτωση που $\delta \mid b$ υπάρχουν ακριβώς δ το πλήθος λύσεις $\pmod{n}$, οι

$$x_0 \ , \ x_0 + \frac{n}{\delta} \ , \ x_0 + 2\frac{n}{\delta} \ , \ \ldots \ , \ x_0 + (\delta - 1)\frac{n}{\delta} \qquad (6)$$

όπου x_0 είναι μια λύση $\pmod{n}$ της (I)

Απόδειξη.

Αν $x \equiv x_0 \pmod{n}$ είναι μια λύση της (I), τότε $ax_0 \equiv b \pmod{n}$ οπότε $n \mid ax_0 - b$ Αλλά $\delta \mid n$, επομένως $\delta \mid ax_0 - b$ και, επειδή $\delta \mid a$, θα έχουμε $\delta \mid ax_0 - (ax_0 - b)$, δηλ $\delta \mid b$.

Αντίστροφα, αν $\delta \mid b$, θα είναι $b = \delta b'$. Αφού $\delta = (a, n)$, θα έχουμε $a = \delta a'$ και $n = \delta n'$, με $(a', n') = 1$. Θα υπάρχουν ακέραιοι τοιπόν x_0, y_0 έτσι ώστε

$$1 = a'x_0 + n'y_0 \ ,$$

οπότε

$$b = a'x_0 b + n'y_0 b = a'x_0 \delta b' + n'y_0 \delta b' = a(x_0 b') + n(y_0 b'),$$

δηλ.

$a(x_0 b') \equiv b \pmod{n}$, επομένως η (I) δέχεται τη λύση

$x \equiv x_0 b' \pmod{n}$.

Θα αποδείξουμε τώρα ότι οι ακέραιοι (6) ικανοποιούν την (I).

Πραγματικά, για κάθε k, $0 \le k \le \delta - 1$, έχουμε

$$a\left(x_0 + k\frac{n}{\delta}\right) = ax_0 + \frac{akn}{\delta} = ax_0 + \frac{a'\delta kn}{\delta} = ax_0 + (a'k)n \equiv b \pmod{n}$$

Επιπλέον οι ακέραιοι (6) είναι ανά δύο ανισότιμοι $(\bmod n)$.

Αν $0 \le k, \lambda \le \delta - 1$ και $k \neq \lambda$, τότε

$$\left|\left(x_0 + k\frac{n}{\delta}\right) - \left(x_0 + \lambda\frac{n}{\delta}\right)\right| = |k-\lambda|\frac{n}{\delta} < n \quad (\text{γιατί } |k-\lambda| < n)$$

Επομένως

$$n \nmid \left\{\left(x_0 + k\frac{n}{\delta}\right) - \left(x_0 + \lambda\frac{n}{\delta}\right)\right\} \quad \text{οπότε}$$

$$x_0 + k\frac{n}{\delta} \not\equiv x_0 + \lambda\frac{n}{\delta} \pmod{n}.$$

Μένει να δείξουμε ότι κάθε τάξη $x_1 \pmod{n}$ της (I) ταυτίζεται με μία από τις τάξεις (6).

Θα είναι $ax_1 \equiv b \pmod{n}$. Αλλά και $ax_0 \equiv b \pmod{n}$ επομένως

$$ax_1 \equiv ax_0 \pmod{n}, \text{ δηλ } n \mid a(x_1 - x_0)$$

Θα έχουμε λοιπόν

$n'\delta \mid a'\delta(x_1 - x_0)$, οπότε $n' \mid a'(x_1 - x_0)$ και επειδή $(n', a') = 1$, θα είναι $n' \mid x_1 - x_0$, δηλ

$$x_1 - x_0 = kn' \quad , \quad k \in \mathbb{Z}. \qquad (7)$$

Διαιρώντας τον k με τον δ, έχουμε

$$k = \delta q + r \quad , \quad 0 \le r \le \delta - 1.$$

και από την (7) παίρνουμε

$$x_1 - x_0 = (\delta q + r)n' = \delta n' q + rn' = nq + rn' \equiv rn' \pmod{n}$$

δηλ $x_1 \equiv x_0 + r\frac{n}{\delta}$ με $0 \le r \le \delta - 1$. ■

Πόρισμα 5.1

Αν $(a,n)=1$, η γραμμική ισοτιμία $ax \equiv b \pmod n$ έχει μοναδική λύση $(\mathrm{mod}\, n)$. ■

Πόρισμα 5.2

Η γραμμική ισοτιμία $ax \equiv 1 \pmod n$ έχει λύση εάν και μόνο εάν $(a,n)=1$. ■

Στην εύρεση μιας λύσης $(\mathrm{mod}\, n)$ της γραμμικής ισοτιμίας $ax \equiv b \pmod n$ όταν $\delta \mid b$, όπου $\delta=(a,n)$.

Αφού $\delta=(a,n)$, θα υπάρχουν ακέραιοι x_0, y_0 τέτοιοι ώστε

$$\delta = ax_0 + ny_0 \quad , \qquad (8)$$

(Τα x_0, y_0 τα υπολογίζουμε από τον Αλγόριθμο του Ευκλείδη.)

Αφού $\delta \mid b$, θα είναι $b=\delta b'$, και από τη σχέση (8) παίρνουμε

$$\delta b' = b = ax_0 b' + ny_0 b', \text{ δηλ. } ab'x_0 - b = (-b'y_0)n$$

επομένως

$$a(b'x_0) \equiv b \pmod n$$

Μία λύση, λοιπόν, της γραμμικής ισοτιμίας $ax \equiv b \pmod n$ είναι η

$$x \equiv b'x_0 \pmod n .$$

Παράδειγμα 5.2

Θα λύσουμε τη γραμμική ισοτιμία

$$540x \equiv 18 \pmod{462} \qquad (9)$$

Από τον Αλγόριθμο του Ευκλείδη βρίσκουμε ότι:

(i) $540 = 462 + 78$

(ii) $462 = 5 \cdot 78 + 72$

(iii) $78 = 72 + 6$

(iv) $72 = 12 \cdot 6 + 0$,

οπότε $\delta=(540,462)=6$.

Αλλά $6|18$, επομένως η γραμμική ισοτιμία (9) έχει 6 σε πλήθος ρίζες (mod 462). Για να τις προσδιορίσουμε βρίσκουμε μέ μια ρίζα (mod 462) της (9) ως εξής:

$$6 \overset{(iii)}{=\!=} 78-72 \overset{(ii)}{=\!=} 78-(462-5\cdot 78) = -462+6\cdot 78 =$$

$$\overset{(i)}{=\!=} -462+6(540-462) = 6\cdot 540+(-7)\cdot 462, \text{ άρα}$$

$6 = 540x_0 + 462y_0$ μέ $x_0=6$ και $y_0=-7$

Μια ρίζα της (9) (mod 462) είναι η

$$x \equiv 3\cdot 6 \pmod{462}, \text{ δηλ } x \equiv 18 \pmod{462}$$

Επομένως οι 6 ρίζες (mod 462) της (9) είναι οι

$$18,\ 18+\frac{462}{6},\ 18+2\frac{462}{6},\ 18+3\frac{462}{6},\ 18+4\frac{462}{6},\ 18+5\frac{462}{6}.$$

δηλ οι

$$18,\ 95,\ 172,\ 249,\ 326,\ 403.$$

Με άλλη έκφραση, η γραμμική ισοτιμία (9) έχει τις ρίζες

$$x \equiv 18, 95, 172, 249, 326, 403 \pmod{462}.$$

<u>Ορισμός</u>

Δυό γραμμικές ισοτιμίες

$$ax \equiv b \pmod{n}, \quad a'x \equiv b' \pmod{n'}$$

καλούνται <u>ισοδύναμες</u>, αν πληρούνται από τις ίδιες ακέραιες τιμές του x, δηλ. για ένα ακέραιο u

$au \equiv b \pmod{n}$, εάν και μόνο εάν $a'u \equiv b' \pmod{n'}$.

<u>Θεώρημα 5.2</u>

Αν $\delta=(a,n)$ και $\delta|b$, τότε η γραμμική ισοτιμία

$$ax \equiv b \pmod{n}$$

είναι ισοδύναμη με την

$$\left(\frac{a}{\delta}\right)x \equiv \left(\frac{b}{\delta}\right) \pmod{\frac{n}{\delta}} \quad \text{με} \quad \left(\frac{a}{\delta}, \frac{n}{\delta}\right) = 1. \qquad (II)$$

Απόδειξη.

Έστω $a=\delta a_1$, $n=\delta n_1$ και $b=\delta b_1$ με $(a_1, n_1)=1$.

Για ένα ακέραιο u έχουμε

$$au \equiv b \pmod{n} \iff \delta a_1 u \equiv \delta b_1 \pmod{\delta n_1}$$
$$\iff a_1 u \equiv b_1 \pmod{n_1} \quad , \delta \neq 0$$
$$\iff \left(\frac{a}{\delta}\right)u \equiv \left(\frac{b}{\delta}\right) \pmod{\frac{n}{\delta}} . \blacksquare$$

Θα παρατηρήσουμε εδώ, ότι, σύμφωνα με το θεώρημα 5.2, η εύρεση μιας ρίζας $x_0 \pmod{n}$ της (I) (όταν υπάρχει) ανάγεται στην εύρεση της μοναδικής ρίζας $x_0 \pmod{\frac{n}{\delta}}$ της γραμμικής ισοτιμίας (II).

Στην περίπτωση αυτή οι δ σε πλήθος ρίζες $(\mathrm{mod}\, n)$ της (I) είναι οι

$$x_0, \; x_0 + \frac{n}{\delta}, \; \ldots, \; x_0 + (\delta - 1)\frac{n}{\delta}.$$

Παράδειγμα 5.3

Θα λύσουμε τη γραμμική ισοτιμία (βλ. παραδ. 5.1)

$$540x \equiv 18 \pmod{462}$$

Από το παράδειγμα 5.1 γνωρίζουμε ότι $(540, 462)=6$, και ο $6 \mid 18$. Είναι λοιπόν αυτή ισοδύναμη με τη γραμμική ισοτιμία

$$\frac{540}{6}x \equiv \frac{18}{6} \pmod{\frac{462}{6}}$$

δηλ. την

$$90x \equiv 3 \pmod{77} \qquad \text{με } (90, 77)=1.$$

Βρίσκουμε τη μοναδική λύση της $(\mathrm{mod}\, 77)$. Είναι

(i) $90 = 77 + 13$
(ii) $77 = 5 \cdot 13 + 12$
(iii) $13 = 1 \cdot 12 + 1$
(iv) $12 = 12 \cdot 1 + 0$.

Έτσι $1 \overset{(iii)}{=\!=} 13-12 \overset{(ii)}{=\!=} 13-(77-5\cdot 13) = 6\cdot 13 - 77$

$\overset{(i)}{=\!=} 6(90-77)-77 = 6\cdot 90 + (-7)\,77$,

οπότε $1 = 90x_0 + 77y_0$ με $x_0 = 6$, $y_0 = -7$.

Η μοναδική λύση είναι λοιπόν η

$$x \equiv 6\cdot 3 \pmod{77} \quad \text{δηλ} \quad x \equiv 18 \pmod{77}$$

Επομένως, οι 6 λύσεις της γραμμικής ισοτιμίας (mod 462) είναι οι

$$x \equiv 18, 95, 172, 249, 326, 403 \pmod{462}$$

όπως τις υπολογίσαμε και στο παράδειγμα 5.1.

Για να βρούμε τη μοναδική λύση (mod n) της ισοτιμίας

$$ax \equiv b \pmod{n} \quad , \quad (a,n) = 1$$

υπάρχει και ένας απευθείας τρόπος, όπως φαίνεται στο επόμενο θεώρημα.

Θεώρημα 5.3

Αν $(a,n)=1$, η μοναδική λύση (mod n) της γραμμικής ισοτιμίας

$$ax \equiv b \pmod{n}$$

είναι η

$$x \equiv b\,a^{\varphi(n)-1} \pmod{n}.$$

Απόδειξη.

Από το θεώρημα του Euler έχουμε ότι

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

οπότε

$$ba^{\varphi(n)} \equiv b \pmod{n}.$$

Ο αριθμός $ba^{\varphi(n)-1}$ την πληροί αφού

$$a\,ba^{\varphi(n)-1} = ba^{\varphi(n)} \equiv b \pmod{n}$$

Η μοναδική λύση της είναι η

$$x \equiv ba^{\varphi(n)-1} \pmod{n}. \blacksquare$$

Για παράδειγμα, η γραμμική ισοτιμία

$$5x \equiv 3 \pmod{24}$$

έχει μοναδική λύση $\pmod{24}$, αφού $(5,24)=1$ την

$$x \equiv 3 \cdot 5^{\varphi(24)-1} \equiv 3 \cdot 5^7 \pmod{24},$$

αφού $\varphi(24) = \varphi(2^3 \cdot 3) = 24\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 8$.

Αλλά $5^2 \equiv 1 \pmod{24}$, οπότε $5^6 \equiv 1 \pmod{24}$ και τέλος, $5^7 \equiv 5 \pmod{24}$ Έτσι η μοναδική λύση είναι η

$$x \equiv 3 \cdot 5^7 \equiv 15 \pmod{24}.$$

Το θεώρημα 5.3 το χρησιμοποιούμε στην περίπτωση που οι αμίγαιοι α και η είναι μικροί.

6. Θεώρημα του Wilson

Θεώρημα 6.1

Αν ο p είναι πρώτος αριθμός τότε

$$(p-1)! \equiv -1 \pmod{p}$$

Απόδειξη

Για τους πρώτους 2 και 3 ισχύει. Έστω p πρώτος >3.

Ας είναι α ένας από τους $p-1$ σε πηλίκος φυσικούς

$$1, 2, \ldots, p-1$$

και ας θεωρήσουμε τη γραμμική ισοτιμία

$$\alpha x \equiv 1 \pmod{p}.$$

Αφού $(\alpha,p)=1$, η παραπάνω ισοτιμία έχει μοναδική λύση $\pmod{p}$, επομένως υπάρχει μοναδικός αμίγαιος α', με $1 \leq \alpha' \leq p-1$, τέτοιος ώστε

$$\alpha \cdot \alpha' \equiv 1 \pmod{p}.$$

Αφού ο p είναι πρώτος, ισχύει

$a = a'$ εάν και μόνο εάν $a=1$ ή $a=p-1$.

Πραγματικά, η ισοτιμία $a^2 \equiv 1 \pmod p$ είναι ισοδύναμη με την $(a-1)(a+1) \equiv 0 \pmod p$ και επομένως

$p \mid a-1$ ή $p \mid a+1$, δηλ.

$a-1 \equiv 0 \pmod p$ ή $a+1 \equiv 0 \pmod p$

Έτσι $a=1$ ή $a=p-1$, αν χάσουμε υπόψη μας ότι $1 \le a \le p-1$ και $1 \le a' \le p-1$.

Διαγράφοντας λοιπόν τους 1 και $p-1$ από τους φυσικούς $1, 2, \dots, p-1$, χωρίζουμε τους απομένοντες φυσικούς

$$2, 3, \dots, p-2$$

(που είναι σε πλήθος $p-3$) σε ζεύγη a, a', έτσι ώστε

$$a \neq a' \quad \text{και} \quad aa' \equiv 1 \pmod p, \qquad (10)$$

δηλ. παίρνουμε $\frac{p-3}{2}$ σε πλήθος ζεύγη a, a' έτσι ώστε να ισχύει η (10).

Αν πολλαπλασιάσουμε αυτές κατά μέλη παίρνουμε

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod p$$

οπότε $(p-1)! \equiv (p-1) \pmod p$.

Αλλά $p-1 \equiv -1 \pmod p$, επομένως

$$(p-1)! \equiv -1 \pmod p. \quad \blacksquare$$

Ισχύει όμως και το αντίστροφο του θεωρήματος του Wilson.

Θεώρημα 6.2

Αν για το φυσικό $n>1$ ισχύει $(n-1)! \equiv -1 \pmod n$, τότε ο n είναι πρώτος αριθμός.

Απόδειξη.

Υποθέτουμε ότι ο n είναι σύνθετος, θα υπάρχει τότε $d \mid n$, με $1 < d < n$, επομένως ο d θα είναι ένας παράγοντας

του $(n-1)!$, δηλ. $d|(n-1)!$. Επειδή $d|n$ ή $n|(n-1)!+1$, θα έχουμε $d|(n-1)!+1$, επομένως $d|1$, πράγμα άτοπο, αφού $d>1$. Ο η είναι λοιπόν πρώτος. ■

Παράδειγμα 6.1

Αν ο p είναι πρώτος αριθμός της μορφής $4k+1$, τότε

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1) \pmod p$$

Πραγματικά, έχουμε $\frac{p-1}{2} = 2k$, επομένως

$$\left(\frac{p-1}{2}\right)! = 1\cdot 2 \cdots \frac{p-1}{2} = (-1)(-2)\cdots\left(-\frac{p-1}{2}\right)$$

Παρατηρούμε ότι.

$$-1 \equiv p-1 \pmod p$$
$$-2 \equiv p-2 \pmod p$$
$$\vdots$$
$$-\frac{p-1}{2} \equiv \frac{p+1}{2} \pmod p,$$

οπότε πολ/ζοντας κατά μέλη, παίρνουμε

$$(-1)(-2)\cdots\left(-\frac{p-1}{2}\right) \equiv (p-1)(p-2)\cdots\frac{p+1}{2} \pmod p,$$

δηλ.

$$\left(\frac{p-1}{2}\right)! \equiv (p-1)(p-2)\cdots\frac{p+1}{2} \pmod p \qquad (11)$$

Αλλά

$$\left(\frac{p-1}{2}\right)! \equiv 1\cdot 2\cdots\frac{p-1}{2} \pmod p \qquad (12).$$

Πολ/ζοντας τις (11) και (12) κατά μέλη και αν λάβουμε υπόψη μας ότι ο p είναι της μορφής $4k+1$, έχουμε

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1\cdot 2\cdots\frac{p-1}{2}\cdot\frac{p+1}{2}\cdots(p-1) \equiv (p-1)! \pmod p$$

Από το θεώρημα του Wilson, όμως, $(p-1)! \equiv -1 \pmod p$, επομένως

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p.$$

Θεώρημα 6.3

Έστω p ένας περιττός πρώτος. Υπάρχει ακέραιος a έτσι ώστε

$$a^2 \equiv -1 \pmod{p}$$

εάν και μόνο εάν $p \equiv 1 \pmod{4}$.

Απόδειξη.

Αν $p \equiv 1 \pmod{4}$, τότε ο p θα είναι της μορφής $p = 4k+1$. Από το παράδειγμα 6.1 όμως έχουμε ότι

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p},$$

δηλ υπάρχει ο ακέραιος $a = \left(\frac{p-1}{2}\right)!$ έτσι ώστε $a^2 \equiv -1 \pmod{p}$.

Αντίστροφα, υποθέτουμε ότι υπάρχει ακέραιος a έτσι ώστε $a^2 \equiv -1 \pmod{p}$. Παρατηρούμε ότι $p \nmid a$. Πραγματικά, αν $p \mid a$, τότε $p \mid a^2$, δηλ $a^2 \equiv 0 \pmod{p}$, επομένως $-1 \equiv 0 \pmod{p}$, πράγμα άτοπο.

Αφού $p \nmid a$, σύμφωνα με το θεώρημα του Fermat,

$$1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

Διαιρώντας τώρα τον p με τον 4, τα δυνατά υπόλοιπα θα είναι 1 ή 3, αφού ο p είναι περιττός, δηλ ο p θα είναι της μορφής $4k+1$ ή $4k+3$.

Ο p δε μπορεί να είναι της μορφής $4k+3$ γιατί τότε

$$(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$$

οπότε $1 \equiv -1 \pmod{p}$, δηλ $p \mid 2$, πράγμα άτοπο.

Επομένως $p = 4k+1$, δηλ $p \equiv 1 \pmod{4}$, όπως επιθυμούσαμε. ∎

Για παράδειγμα, η ισοτιμία $x^2 \equiv -1 \pmod{29}$ έχει μία λύση, τον ακέραιο $\left(\frac{29-1}{2}\right)! = 14!$, αφού ο πρώτος 29 ικανοποιεί $29 \equiv 1 \pmod{4}$.

Παράδειγμα 6.2.

Αν ο p είναι περιττός πρώτος αριθμός, τότε

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

Πραγματικά, ο p θα είναι της μορφής $2\lambda+1$, οπότε ο $\frac{p-1}{2}$ θα είναι φυσικός αριθμός. Παρατηρούμε ότι, για κάθε αυτόν κ ισχύει $-\kappa \equiv (p-\kappa) \pmod p$

επομένως

$$-2 \equiv p-2 \pmod p$$
$$-4 \equiv p-4 \pmod p$$
$$\vdots$$
$$-(p-5) \equiv 5 \pmod p$$
$$-(p-3) \equiv 3 \pmod p$$
$$-(p-1) \equiv 1 \pmod p$$

Πολλαπλασιάζοντας κατά μέλη, παίρνουμε

$$(-1)^{\frac{p-1}{2}} \cdot 2 \cdot 4 \cdots (p-1) \equiv 1 \cdot 3 \cdot 5 \cdots (p-2) \pmod p$$

και επομένως

$$(-1)^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots (p-2)(p-1) \equiv 1^2 3^2 \cdots (p-2)^2 \pmod p,$$

δηλ.

$$(-1)^{\frac{p-1}{2}} \cdot (p-1)! \equiv 1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \pmod p$$

Από το θεώρημα του Wilson έχουμε $(p-1)! \equiv -1 \pmod p$

οπότε

$$(-1)^{\frac{p-1}{2}} (p-1)! \equiv (-1)^{\frac{p-1}{2}} \cdot (-1) \pmod p,$$

δηλ.

$$(-1)^{\frac{p-1}{2}} (p-1)! \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

Έτσι

$$1^2 \cdot 3^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p \;.$$

7. Η αριθμητική συνάρτηση $\lambda(n)$

Για την συνάρτηση φ του Euler γνωρίζουμε ότι το $\varphi(n)$ είναι ένας καθολικός εκθέτης για τον n, με την έννοια ότι για κάθε ακέραιο a με $(a,n)=1$ ισχύει $a^{\varphi(n)} \equiv 1 \pmod n$.

Πρώτος ο R. Carmichael συμβόλισε με $\lambda(n)$ τον ελάχιστο καθολικό εκθέτη για τον n, με την έννοια ότι το $\lambda(n)$ είναι ο ελάχιστος εκθέτης τέτοιος ώστε, για κάθε ακέραιο a με $(a,n)=1$ να είναι $a^{\lambda(n)} \equiv 1 \pmod n$.

Ορίζεται μ' αυτόν τον τρόπο μια αριθμητική συνάρτηση λ την οποία ο E. Lucas όρισε ως εξής:

$$\lambda(n) = \begin{cases} \varphi(n) & \text{αν } n = 1, 2, 4, p^b, 2p^b, \ p \text{ περιττός πρώτος και } b \geq 1 \\ \frac{1}{2}\varphi(n) & \text{αν } n = 2^b, \ b \geq 3 \\ [\lambda(2^b), \varphi(p_1^{b_1}), \ldots, \varphi(p_r^{b_r})] & \text{αν } n = 2^b \prod_{i=1}^{r} p_i^{b_i} \end{cases}$$

p_i περιττοί πρώτοι

Την συνάρτηση αυτή δεν πρέπει να την ταυτίζουμε με την συνάρτηση του Liouville που ορίσαμε στο Παράδειγμα 3.4 του Κεφ. II.

Οι επόμενες παρατηρήσεις θα μας βοηθήσουν να κατανοήσουμε πλήρως τον τρόπο με τον οποίο ορίζεται η συνάρτηση $\lambda(n)$ και θα μας δώσουν την δυνατότητα να βγάλουμε χρήσιμα συμπεράσματα που αφορούν αρχικές ρίζες $\pmod n$ που θα δούμε στο κεφάλαιο VI

Παρατήρηση 1

1α) Αν φυσικός n δεν είναι της μορφής $1, 2, 4, p^b, 2p^b$, p περιττός πρώτος <u>ούτε</u> της μορφής 2^b, $b \geq 3$ τότε στην παραγοντοποίηση

$$n = 2^b \prod_{i=1}^{r} p_i^{b_i}$$

αν $r=1$ τότε $b \geq 2$, (αφού ο n δεν είναι της μορφής p^b ή $2p^b$, p περιττός πρώτος) άρα

$$n = 2^b \cdot p_1^{b_1}, \quad b \geq 2, \ p_1 \text{ περιττός πρώτος}, \ b_1 \geq 1.$$

Αν $r \geq 2$ τότε

$$n = 2^b \cdot p_1^{b_1} \cdots p_r^{b_r}, \quad p_i \text{ περιττοί πρώτοι}, \ b \geq 0, \ b_i \geq 1.$$

1b) Ο φυσικός n δεν είναι της μορφής $1, 2, 4, p^b, 2p^b$, p περιττός πρώτος ούτε της μορφής 2^b, $b \geq 3$ αν και μόνο αν

$$n = k \cdot l \quad \text{με } (k,l) = 1 \text{ και } k > 2, \ l > 2.$$

1c) Ο φυσικός n δεν είναι της μορφής $1, 2, 4, p^b, 2p^b$, p περιττος πρώτος αν και μόνο αν ο n είναι πολλαπλάσιο ενός φυσικού αριθμού του τύπου

(a) $4p$, p περιττός πρώτος

(b) $p \cdot q$, $p \neq q$, p, q περιττοί πρώτοι

(c) 8.

1d) Αν ο φυσικός n δεν είναι της μορφής $1, 2, 4, p^b, 2p^b$, p περιττός πρώτος τότε

$$\lambda(n) \mid \tfrac{1}{2}\varphi(n)$$

και επομένως

$$\lambda(n) < \varphi(n).$$

Πραγματικά, αν $n = 2^b$, $b \geq 3$ τότε $\lambda(n) = \frac{1}{2}\varphi(n)$.

Αν $n = 2^b \cdot p_1^{b_1} \cdots p_r^{b_r}$ τότε $\lambda(n) = \left[\lambda(2^b), \varphi(p_1^{b_1}), \ldots, \varphi(p_r^{b_r})\right]$

Από τον ορισμό του $\lambda(2^b)$, τις ιδιότητες του Ε.Κ.Π, το γεγονός ότι η συνάρτηση $\varphi(n)$ του Euler είναι πολλαπλασιαστική και το γεγονός ότι οι $\varphi(p_i^{b_i})$ είναι άρτιοι φυσικοί, και το γεγονός ότι

$$\lambda(n) \mid \lambda(2^b)\varphi(p_1^{b_1}) \cdots \varphi(p_r^{b_r})$$

παίρνουμε ότι

$$\lambda(n) \mid \tfrac{1}{2}\varphi(n),$$

και επομένως $\lambda(n) \leq \frac{1}{2}\varphi(n) < \varphi(n)$.

1ε) Για κάθε φυσικό n ισχύει $1 \le \lambda(n) \le \varphi(n)$.

Θεώρημα 7.1

Έστω η φυσικός. Για κάθε ακέραιο a με $(a,n)=1$ ισχύει

$$a^{\lambda(n)} \equiv 1 \pmod{n}.$$

Απόδειξη.

Αν $n = 1, 2, 4, p^\beta, 2p^\beta$ όπου p περιττός πρώτος, τότε $\lambda(n)=\varphi(n)$ και το αποτέλεσμα προκύπτει αμέσως από το θεώρημα του Euler.

Έστω $n = 2^\beta$, $\beta \ge 3$, τότε $\lambda(n) = \frac{1}{2}\varphi(n)$.

Αν $(a, 2^\beta) = 1$ τότε ο a είναι περιττός αριθμός, και έστω $a = 2b+1$, $b \in \mathbb{Z}$. Τότε $a^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 4b(b+1) + 1$.

Επειδή, $2 \mid b(b+1)$ έχουμε $8 \mid a^2 - 1$, δηλαδή $a^2 \equiv 1 \pmod 8$

Για $\beta = 3$ είναι $\lambda(2^3) = \frac{1}{2}\varphi(2^3) = 2$, επομένως $a^{\lambda(2^3)} \equiv 1 \pmod{2^3}$.

Θα εργασθούμε επαγωγικά. Υποθέτουμε ότι για $\beta - 1 \ge 3$ ισχύει:

Αν $(a, 2^{\beta-1}) = 1$ τότε $a^{\lambda(2^{\beta-1})} \equiv 1 \pmod{2^{\beta-1}}$.

Θα υπάρχει επομένως $k \in \mathbb{Z}$ ώστε $a^{\lambda(2^{\beta-1})} = 1 + k2^{\beta-1}$.

Υψώνοντας στο τετράγωνο και τα δύο μέλη της παίρνουμε

$$a^{2\cdot\lambda(2^{\beta-1})} = 1 + k\cdot 2^\beta + k^2 \cdot 2^{2\beta-2}, \text{ δηλαδή}$$

$$a^{2\lambda(2^{\beta-1})} \equiv 1 \pmod{2^\beta}.$$

Αλλά $\lambda(2^\beta) = \frac{1}{2}\varphi(2^\beta) = \frac{1}{2}2^{\beta-1} = 2^{\beta-2} = 2\lambda(2^{\beta-1})$

και $(a, 2^\beta) = (a, 2^{\beta-1}) = 1$, επομένως για κάθε ακέραιο a με $(a, 2^\beta) = 1$ ισχύει $a^{\lambda(2^\beta)} \equiv 1 \pmod{2^\beta}$.

Τέλος, έστω $n = 2^\beta \cdot \prod_{i=1}^{r} p_i^{\beta_i}$, p_i περιττοί πρώτοι.

Τότε $\lambda(n) = [\lambda(2^\beta), \varphi(p_1^{\beta_1}), \dots, \varphi(p_r^{\beta_r})] = [\lambda(2^\beta), \lambda(p_1^{\beta_1}), \dots, \lambda(p_r^{\beta_r})]$.

Αν $(a,n) = 1$ δηλαδή $(a, 2^\beta p_1^{\beta_1} \dots p_r^{\beta_r}) = 1$, οπότε

$(a, 2^\beta) = (a, p_1^{\beta_1}) = \dots = (a, p_r^{\beta_r}) = 1$

σύμφωνα με το θεώρημα 6.9 του κεφ. II.
Έχουμε όμως αποδείξει ότι

$$\alpha^{\lambda(2^\beta)} \equiv 1 \pmod{2^\beta}$$
$$\alpha^{\lambda(p_1^{\beta_1})} \equiv 1 \pmod{p_1^{\beta_1}}$$
$$\vdots$$
$$\alpha^{\lambda(p_\kappa^{\beta_\kappa})} \equiv 1 \pmod{p_\kappa^{\beta_\kappa}}$$

Αλλά $\lambda(2^\beta) \mid \lambda(n)$ και $\lambda(p_i^{\beta_i}) \mid \lambda(n)$ $\quad i=1,\dots,\kappa$
οπότε

$$\alpha^{\lambda(n)} \equiv 1 \pmod{2^\beta}$$
$$\alpha^{\lambda(n)} \equiv 1 \pmod{p_1^{\beta_1}}$$
$$\vdots$$
$$\alpha^{\lambda(n)} \equiv 1 \pmod{p_\kappa^{\beta_\kappa}}$$

Οι φυσικοί αριθμοί $2^\beta, p_1^{\beta_1}, \dots, p_\kappa^{\beta_\kappa}$ είναι πρώτοι μεταξύ τους ανα δύο και καθένας απ' αυτούς διαιρεί τον $\alpha^{\lambda(n)}-1$, οπότε

$$2^\beta \cdot p_1^{\beta_1} \dots p_\kappa^{\beta_\kappa} \mid \alpha^{\lambda(n)}-1$$

σύμφωνα με το πόρισμα 6.11 του κεφ II, δηλαδή αν $(\alpha,n)=1$ τότε $\alpha^{\lambda(n)} \equiv 1 \pmod n$. ■

Πόρισμα 7.1

Αν ο φυσικός η δεν είναι της μορφής $1, 2, 4, p^\beta, 2p^\beta$, p περιττός πρώτος, τότε για κάθε ακέραιο α με $(\alpha,n)=1$ ισχύει

$$\alpha^{\frac{\varphi(n)}{2}} \equiv 1 \pmod n$$

Απόδειξη
Αν ο η δεν είναι της μορφής $1, 2, 4, p^\beta, 2p^\beta$, p περιττός πρώτος τότε όπως είδαμε στην παρατήρηση 1δ $\lambda(n) \mid \frac{1}{2}\varphi(n)$.
Από το θεώρημα 7.1 έχουμε: αν $(\alpha,n)=1$ τότε $\alpha^{\lambda(n)} \equiv 1 \pmod n$ και επομένως $\alpha^{\varphi(n)/2} \equiv 1 \pmod n$. ■

Παράδειγμα 7.1

Έστω $\eta = 2800 = 2^4 \cdot 5^2 \cdot 7$.

Είναι $\varphi(2800)=\varphi(2^4)\cdot\varphi(5^2)\cdot\varphi(7)=960$ και

$$\lambda(2800)=\lambda(2^4\cdot 5^2\cdot 7)=[\lambda(2^4),\varphi(5^2),\varphi(7)]$$

$$=\left[\tfrac{1}{2}\varphi(2^4),\ \varphi(5^2),\ \varphi(7)\right]=[4,20,6]=60.$$

Αν $(a,2800)=1$ τότε $a^{\lambda(2800)}\equiv 1 \pmod{2800}$ δηλαδή

$a^{60}\equiv 1 \pmod{2800}$.

Το θεώρημα 7.1 είναι χρήσιμο και στην εύρεση του υπολοίπου της διαίρεσης με τον φυσικό η δύναμης a^k ενός ακεραίου a με $(a,n)=1$, οποτεδήποτε ο εκθέτης k είναι $\lambda(n)\le k\le\varphi(n)$.

Παράδειγμα 7.2

Να βρεθεί το υπόλοιπο της διαίρεσης του 31^{122} με τον 2800.

Είναι $(31,2800)=1$ και $\lambda(2800)=60$ σύμφωνα με το παράδειγμα 7.1. Άρα $31^{60}\equiv 1 \pmod{2800}$. Έτσι

$$31^{120}\equiv 1 \pmod{2800}$$

και

$$31^{122}\equiv 31^2\equiv 961 \pmod{2800}.$$

Άρα το ζητούμενο υπόλοιπο είναι 961.

8. Η τάξη ενός ακεραίου mod n

Έστω φυσικός $n>1$ και a ακέραιος με $(a,n)=1$. Από το θεώρημα του Euler έχουμε $a^{\varphi(n)}\equiv 1 \pmod n$. Πολύ συχνά όμως για τον ακέραιο αυτό a υπάρχει φυσικός $s<\varphi(n)$ έτσι ώστε $a^s\equiv 1 \pmod n$.

Για παράδειγμα, αν ο η δεν είναι της μορφής $1, 2, 4, p^\beta, 2p^\beta$, p περιττός πρώτος, τότε όπως είδαμε στην παράγραφο 7, υπάρχει ο $\lambda(n)<\varphi(n)$, και για ακέραιο a με $(a,n)=1$ ισχύει $a^{\lambda(n)}\equiv 1 \pmod n$.

Αλλά και όταν ο η είναι της μορφής $2, 4, p^b, 2p^b$, p περιττός πρώτος για παράδειγμα αν $\eta = 2 \cdot 5^2 = 50$, τότε $\varphi(50) = 20$.
Για τον ακέραιο 7 με $(7, 50) = 1$ είναι $7^4 \equiv 1 \pmod{50}$ με $4 < 20$ ενώ για τον ακέραιο 3 με $(3, 50) = 1$ είναι $7^{20} \equiv 1 \pmod{50}$ και δεν υπάρχει $s < 20$ ώστε $a^s \equiv 1 \pmod{50}$, δηλαδή ο 3 είναι μια αρχική ρίζα $(\mathrm{mod}\, 50)$ όπως θα δούμε στα επόμενα κεφάλαια.

Οδηγούμεθα λοιπόν στον επόμενο ορισμό.

Ορισμός

Έστω η φυσικός > 1 και a ακέραιος με $(a, \eta) = 1$.
Ονομάζουμε <u>τάξη του a $(\mathrm{mod}\, \eta)$</u> και το συμβολίζουμε $\mathrm{ord}_\eta(a)$ τον ελάχιστο φυσικό s τέτοιο ώστε

$$a^s \equiv 1 \pmod{\eta}.$$

ord είναι η σύντμηση της λέξης order (= τάξη).

Έτσι, αν $(a, \eta) = 1$ τότε

$\mathrm{ord}_\eta(a) = s \iff$ ο s είναι ο ελάχιστος φυσικός έτσι ώστε: $a^s \equiv 1 \pmod{\eta}$

Αν λοιπόν $\mathrm{ord}_\eta(a) = s > 1$ τότε $a^s \equiv 1 \pmod{\eta}$ και $a^k \not\equiv 1 \pmod{\eta}$ για κάθε k με $1 \le k < s$.

Θα τονίσουμε ιδιαίτερα ότι ο ορισμός της τάξης $(\mathrm{mod}\, \eta)$ <u>έχει νόημα μόνο για ακεραίους a με $(a, \eta) = 1$.</u>

Πραγματικά, αν $(a, \eta) > 1$ τότε η γραμμική ισοτιμία $ax \equiv 1 \pmod{\eta}$ δεν έχει λύση, σύμφωνα με το θεώρημα 5.1.
Αν λοιπόν υπήρχε φυσικός $k \ge 1$ τέτοιος ώστε $a^k \equiv 1 \pmod{\eta}$ τότε ο ακέραιος $x = a^{k-1}$ θα ήταν μια λύση της, πράγμα άτοπο.
Οποιαδήποτε λοιπόν αναφορά στην $\mathrm{ord}_\eta(a)$ προϋποθέτει ότι $(a, \eta) = 1$.

Από τον ορισμό της $ord_n(a)$, το θεώρημα του Euler και το θεώρημα 7.1 έχουμε: $1 \leq ord_n(a) \leq \lambda(n) \leq \varphi(n)$.

Παράδειγμα 8.1

Θα υπολογίσουμε την $ord_{55}(12)$.

Είναι $(12,55)=1$ και $12^1 \equiv 12 \pmod{55}$, $12^2 \equiv 34 \pmod{55}$, $12^3 \equiv 23 \pmod{55}$ και $12^4 \equiv 1 \pmod{55}$, άρα $ord_{55}(12)=4$.

Παράδειγμα 8.2

Θα δείξουμε ότι $ord_{15}(7)=4$

Πραγματικά, $(7,55)=1$ και $7^1 \equiv 7 \pmod{15}$, $7^2 \equiv 49 \equiv 4 \pmod{15}$

$7^3 \equiv 7 \cdot 7^2 \equiv 28 \equiv 13 \pmod{15}$, $7^4 \equiv 7^2 \cdot 7^2 \equiv 16 \equiv 1 \pmod{15}$.

Παράδειγμα 8.3

Θα υπολογίσουμε την τάξη του 5 (mod 7)

Είναι $5^1 \equiv 5 \pmod 7$, $5^2 \equiv 25 \equiv 4 \pmod 7$, $5^3 \equiv 5 \cdot 5^2 \equiv 20 \equiv -1 \pmod 7$

$5^4 \equiv 5 \cdot 5^3 \equiv -5 \equiv 2 \pmod 7$, $5^5 \equiv 5^3 \cdot 5^2 \equiv -4 \equiv 3 \pmod 7$ και

$5^6 \equiv 5^3 5^3 \equiv (-1)^2 \equiv 1 \pmod 7$, άρα $ord_5(7)=6=\varphi(7)$, που σημαίνει όπως θα δούμε στα επόμενα ότι ο 5 είναι αρχική ρίζα (mod 7).

Πρόταση 8.1

Αν n φυσικός >1 και a, b ακέραιοι, με $(a,n)=1$, τότε

$$a \equiv b \pmod n \Longrightarrow ord_n(a) = ord_n(b).$$

Απόδειξη

Έστω $a \equiv b \pmod n$. Τότε $(b,n)=(a,n)=1$ σύμφωνα με το θεώρημα 1.6 και επιπλέον $a^k \equiv b^k$, $\forall k \in \mathbb{N}$ σύμφωνα με το θεώρημα 1.3

Αν $ord_n(a)=s$, τότε ο s είναι ο ελάχιστος φυσικός με $a^s \equiv 1 \pmod n$, επομένως $b^s \equiv a^s \equiv 1 \pmod n$ και εύκολα διαπιστώνουμε ότι ο s είναι ο ελάχιστος φυσικός με $b^s \equiv 1 \pmod n$. Άρα $ord_n(b)=s$. ■

Θα παρατηρήσουμε εδώ ότι για ακεραίους a, b μπορεί να είναι $ord_n(a)=ord_n(b)$ και όμως $a \not\equiv b \pmod n$. Για παράδειγμα

$ord_7(2) = ord_7(4) = 3$ και $2 \not\equiv 4 \pmod 7$.

Η πρόταση 8.1 διευκολύνει τη διαδικασία της εύρεσης της τάξης(mod n) ενός ακεραίου a, που είναι μεγαλύτερος από το modulo n και $(a,n)=1$. Στην περίπτωση αυτή διαιρώντας τον a με τον n, παίρνουμε $a = nq + r$ με $0 < r < n$. Έτσι $a \equiv r \pmod n$ και επομένως $ord_n(a) = ord_n(r)$.

Παράδειγμα 8.4

Θα βρούμε την $ord_{55}(72\,227)$

Είναι $72\,227 = 55 \cdot 1313 + 12$ και $(72.227, 55) = (12, 55) = 1$

οπότε $ord_{55}(72.227) = ord_{55}(12)$.

Αλλά $ord_{55}(12) = 4$ σύμφωνα με το παράδειγμα 8.1, άρα

$ord_{55}(72.227) = 4$.

Για να βρούμε λοιπόν τις $ord_n(x)$ όλων των ακεραίων x με $(x,n)=1$ περιοριζόμαστε στην εύρεση όλων των τάξεων των ακεραίων ενός αναγμένου συστήματος υπολοίπων (mod n) $\{a_1, \ldots, a_{\varphi(n)}\}$.

Πραγματικά, κάθε ακέραιος x με $(x,n)=1$ είναι ισότιμος (mod n) μ' ένα ακριβώς ακέραιο του συνόλου $\{a_1, \ldots, a_{\varphi(n)}\}$ και επομένως θα έχει την ίδια τάξη (mod n) μ' αυτόν.

Παράδειγμα 8.5

Θα βρούμε $ord_{12}(x)$ όλων των ακεραίων x με $(x,12)=1$.

Θεωρούμε το αναγμένο σύστημα υπολοίπων (mod 12) $\{1, 5, 7, 11\}$ και βρίσκουμε $ord_{12}(1) = 1$, $ord_{12}(5) = ord_{12}(7) = ord_{12}(11) = 2$. Κάθε ακέραιος x με $(x,12)=1$ είναι ισότιμος (mod 12) μ' ένα ακριβώς από τους 1, 5, 7, και 11 και επομένως η τάξη του (mod 12) θα είναι 1 ή 2.

Ας είναι H_n το σύνολο των πρωτογενών μονάδων (mod n)
Αν $\bar{a} \in H_n$, τότε όλοι οι ακέραιοι της μονάδας $\bar{a}$ έχουν την ίδια τάξη (mod n) σύμφωνα με την πρόταση 8.1. Η κοινή αυτή τάξη ονομάζεται τάξη της κλάσης $\bar{a}$ και συμβολίζεται $ord_n(\bar{a})$. Έτσι

Αν $\bar{a} \in H_n$, τότε $ord_n(\bar{a}) = s \iff ord_n(a) = s$.

Μ' άλλα λόγια, αν $\bar{a} \in H_n$, τότε

$ord_n(\bar{a}) = s \iff$ ο s είναι ο ελάχιστος φυσικός : $\bar{a}^s = \bar{1}$.

Γνωρίζουμε ότι το H_n είναι μια πολλαπλασιαστική ομάδα. Η τάξη μιας μονάδας $\bar{a} \in H_n$ συμπίπτει με την τάξη $\bar{a}$ σαν στοιχείου της H_n όπως την ορίσαμε στην παρατήρηση μετά το θεώρημα του Euler.

Κάθε αναφορά στην $ord_n(\bar{a})$ προυποθέτει ότι $\bar{a} \in H_n$. Από τις μονάδες λοιπόν του $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ τάξη έχουν μόνο οι πρωτογενείς μονάδες του H_n. Για παράδειγμα, αν $n = 12$ τότε από τις μονάδες του $\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \ldots, \overline{11}\}$ τάξη έχουν μόνο οι πρωτογενείς μονάδες του $H_{12} = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$ και μάλιστα

$ord_{12}(\bar{1}) = 1$, ενώ $ord_{12}(\bar{5}) = ord_{12}(\bar{7}) = ord_{12}(\overline{11}) = 2$

όπως είδαμε στο παράδειγμα 8.5

Πρόταση 8.2

Ας είναι $a, n \in \mathbb{Z}$, με $n > 1$ και $(a, n) = 1$. Αν $ord_n(a) = s$, τότε

i) $a^h \equiv a^k \pmod n \iff h \equiv k \pmod s$

ii) $a^h \equiv 1 \pmod n \iff s \mid h$

iii) Οι ακέραιοι $1, a, a^2, \ldots a^{s-1}$ είναι ανά δύο ανισότιμοι (mod n)

Απόδειξη.

Αφού $ord_n(a) = s$ θα είναι $a^s \equiv 1 \pmod n$

i) Υποθέτουμε ότι $h \geq k$. Διαιρώντας το $h - k$ με τον s έχουμε

$$h - k = sq + r \quad \text{με} \quad 0 \leq r < s.$$

Είναι $a^s \equiv 1 \pmod n$ οπότε $a^{sq} \equiv 1 \pmod n$ και τέλος $a^{sq+r} \equiv a^r \pmod n$.

Έχουμε.

$$a^h \equiv a^k \pmod n \Rightarrow n \mid a^h - a^k \Rightarrow n \mid a^k(a^{h-k}-1) \xrightarrow{(n,a^k)=1}$$

$$n \mid a^{h-k}-1 \rightarrow a^{h-k} \equiv 1 \pmod n \Rightarrow a^{sq+r} \equiv 1 \pmod n$$

δηλαδή $a^r \equiv 1 \pmod n$

Καθώς όμως $0 \le r < s$ και $ord_n(a) = s$ η τελευταία ισοτιμία αληθεύει όταν $r=0$ δηλαδή όταν $h-k = sq$ άρα $h \equiv k \pmod s$.

Αντίστροφα, αν $h \equiv k \pmod s$, τότε $h-k = sq$, οπότε $a^{h-k} = a^{sq} = (a^s)^q \equiv 1 \pmod n$. Επομένως $a^h \equiv a^k \pmod n$.

ii) Αν στην i) θέσουμε $k=0$ παίρνουμε αμέσως την ii).

iii) Οι ακέραιοι $0, 1, \ldots, s-1$ είναι ανά δύο ανισότιμοι $(\bmod s)$, η i) συνεπάγεται ότι οι αιέραιοι $a^0=1, a^1=a, \ldots, a^{s-1}$ είναι ανα δύο ανισότιμοι $(\bmod n)$. ■

Πόρισμα 8.1

Αν είναι η φυσικός >1 και a ακέραιος με $(a,n)=1$ τότε

$$ord_n(a) \mid \varphi(n).$$

Απόδειξη

Απο το θεώρημα του Euler έχουμε $a^{\varphi(n)} \equiv 1 \pmod n$, και απο την Πρόταση 8.2 ii) είναι $ord_n(a) \mid \varphi(n)$.

Το Πόρισμα 8.1 είναι χρήσιμο στον υπολογισμό της $ord_n(a)$, γιατί δεν υπολογίζουμε όλες τις δυνάμεις a^k με $k \le \varphi(n)$ αλλά περιορίζόμαστε μόνο σ' εκείνες για τις οποίες $s \mid \varphi(n)$.

Παράδειγμα 8.6

Θα υπολογίσουμε την $ord_{36}(5)$.

Απο το πόρισμα 8.1 θα είναι $\text{ord}_{36}(5) \mid \varphi(36)$. Αλλά $\varphi(36) = \varphi(2^2 \cdot 3^2) = 12$, άρα ο φυσικός $\text{ord}_{36}(5)$ θα είναι κάποιος απο τους $1, 2, 3, 4, 6, 12$. Είναι, $5^1 \equiv 5 \pmod{36}$, $5^2 \equiv 25 \pmod{36}$, $5^3 \equiv 17 \pmod{36}$, $5^4 \equiv 13 \pmod{36}$ και $5^6 \equiv 5^4 \cdot 5^2 \equiv 1 \pmod{36}$
Επομένως $\text{ord}_{36}(5) = 6$.

Πόρισμα 8.2

Ας είναι η φυσικός >1 και a ακέραιος με $(a,n)=1$. Τότε

$$\text{ord}_n(a) \mid \lambda(n)$$

Απόδειξη
Απο το θεώρημα 7.1 είναι $a^{\lambda(n)} \equiv 1 \pmod{n}$. Απο την Πρόταση 8.2 ii) έχουμε $\text{ord}_n(a) \mid \lambda(n)$. ■

Αν $(a,n)=1$ τότε $\text{ord}_n(a) \leq \lambda(n) \leq \varphi(n)$.

Το πόρισμα 8.2 είναι χρήσιμο στον υπολογισμό της $\text{ord}_n(a)$, στην περίπτωση που ο n <u>δεν</u> είναι της μορφής $2, 4, p^k, 2p^k$, p περιττός πρώτος, γιατί τότε

$$\text{ord}_n(a) \leq \lambda(n) < \varphi(n).$$

Δεν υπολογίζουμε όλες τις δυνάμεις a^k με $k \leq \lambda(n)$, αλλά περιοριζόμαστε μόνο σ' εκείνες για τις οποίες $k \mid \lambda(n)$.

Παράδειγμα 8.7

Αν $n = 2800$ τότε απο το παράδειγμα 7.1 έχουμε $\varphi(2800) = 960$ και $\lambda(2800) = 60$.
Αν λοιπόν $(a, 2800) = 1$, η $\text{ord}_{2800}(a) \mid 60$ δηλαδή θα είναι ένας απο τους φυσικούς $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$.

Πρόταση 8.3

Αν $\text{ord}_n(a) = s$ και $\text{ord}_n(b) = t$ και $(s,t) = 1$, τότε

$$\text{ord}_n(ab) = s \cdot t.$$

Απόδειξη.

Είναι $a^s \equiv 1 \pmod n$ και $b^t \equiv 1 \pmod n$. Έστω $\text{ord}_n(ab) = \delta$

Τότε, $(ab)^{st} \equiv (a^s)^t \cdot (b^t)^s \equiv 1 \pmod n$, οπότε $\delta | st$.

Θα δείξουμε τώρα ότι $st | \delta$.

Είναι $(ab)^{\delta s} \equiv 1 \pmod n$ και $(ab)^{\delta s} \equiv (a^s)^\delta \cdot b^{\delta s} \equiv b^{\delta s} \pmod n$

επομένως $b^{\delta s} \equiv 1 \pmod n$, άρα $t | \delta s \xrightarrow{(t,s)=1} t | \delta$.

Όμοια, $(ab)^{\delta t} \equiv 1 \pmod n$ και $(ab)^{\delta t} \equiv a^{\delta t} (b^t)^\delta \equiv a^{\delta t} \pmod n$.

επομένως $a^{\delta t} \equiv 1 \pmod n$, άρα $s | \delta t \xrightarrow{(s,t)=1} s | \delta$.

Τελικά έχουμε, $s | \delta$, $t | \delta$ και $(s,t) = 1 \Rightarrow st | \delta$.

Είναι $s, t, \delta \in \mathbb{N}$, $st | \delta$ και $\delta | st$ οπότε $\delta = st$. ■

Παράδειγμα 8.8.

Θα υπολογίσουμε $\text{ord}_{11}(30)$.

Αν γράψουμε $30 = 3 \cdot 10$, τότε $\text{ord}_{11}(3) = 5$ και $\text{ord}_{11}(10) = 2$ και επειδή $(5,2) = 1$, σύμφωνα με την πρόταση 8.3 θα είναι $\text{ord}_{11}(30) = 5 \cdot 2 = 10$.

Αν όμως γράψουμε $30 = 6 \cdot 5$, τότε $\text{ord}_{11}(6) = 10$ και $\text{ord}_{11}(5) = 5$, αλλά $(5, 10) = 5 \neq 1$, άρα δεν εφαρμόζεται η πρόταση 8.3 στην γραφή $30 = 6 \cdot 5$.

Πρόταση 8.4

Αν $\text{ord}_n(a) = s$ και h φυσικός, τότε

$$\text{ord}_n(a^h) = \frac{s}{(s,h)}$$

Απόδειξη

Είναι $a^s \equiv 1 \pmod n$. Έστω $d = (s,h)$, οπότε $s = s_1 d$, $h = h_1 \cdot d$ και $(s_1, h_1) = 1$.

Έστω $\text{ord}_n(a^h) = r$, οπότε $(a^h)^r \equiv 1 \pmod n$.

Θα δείξουμε ότι $r = s_1$.

Φανερά, $(\alpha^h)^{s_1} = (\alpha^{h_1 \cdot d})^{\frac{s}{d}} = (\alpha^s)^{h_1} \equiv 1 \pmod n$ οπότε $r | s_1$

Απ' την άλλη μεριά

$\alpha^{hr} \equiv (\alpha^h)^r \equiv 1 \pmod n$, οπότε $s | h \cdot r$ δηλαδή

$s_1 \cdot d | h_1 d \cdot r$, άρα $s_1 | h_1 r$ και επομένως $s_1 | r$ αφού

$(s_1, h_1) = 1$.

Τελικά, $r, s_1 \in \mathbb{N}$ με $r | s_1$ και $s_1 | r$ άρα

$$r = s_1 = \frac{s}{d} = \frac{s}{(s,h)} . \blacksquare$$

Πόρισμα 8.3

Αν $ord_n(\alpha) = s$ και h φυσικός τότε,

$$ord_n(\alpha^h) = s \iff (s,h) = 1.$$

Απόδειξη.

$$ord_n(\alpha^h) = s \iff \frac{s}{(s,h)} = s \iff (s,h) = 1 . \blacksquare$$

Πόρισμα 8.4

Αν $ord_n(\alpha) = st$ τότε $ord_n(\alpha^s) = t$.

Απόδειξη

$$ord_n(\alpha^s) = \frac{st}{(s,st)} = \frac{st}{s} = t . \blacksquare$$

Παράδειγμα 8.9

Θα υπολογίσουμε την $ord_{11}(8^{1998})$

Είναι $ord_{11}(8) = 10$, επομένως

$$ord_{11}(8^{1998}) = \frac{10}{(10,1998)} = \frac{10}{2} = 5 .$$

Πρόταση 8.5

Αν $\text{ord}_{m_1}(a)=t_1$ και $\text{ord}_{m_2}(a)=t_2$ τότε

$$\text{ord}_{[m_1,m_2]}(a) = [t_1,t_2] .$$

Απόδειξη.

Έστω $\text{ord}_{[m_1,m_2]}(a) = s$ και $L=[t_1,t_2]$.

Είναι $a^s \equiv 1 \pmod{[m_1,m_2]}$ και επειδή $m_1 \mid [m_1,m_2]$ και $m_2 \mid [m_1,m_2]$ θα είναι $a^s \equiv 1 \pmod{m_1}$ και $a^s \equiv 1 \pmod{m_2}$.

Αφού $\text{ord}_{m_1}(a)=t_1$ και $a^s \equiv 1 \pmod{m_1}$ θα είναι $t_1 \mid s$.

Όμοια και $t_2 \mid s$. Επομένως $[m_1,m_2] \mid s$ δηλαδή $L \mid s$.

Απ' την άλλη μεριά, αν $L = t_1 \cdot \lambda_1$, $L = t_2 \lambda_2$ τότε

$$a^L = a^{t_1\lambda_1} = (a^{t_1})^{\lambda_1} \equiv 1 \pmod{m_1} \quad \text{και}$$

$$a^L = a^{t_2\lambda_2} = (a^{t_2})^{\lambda_2} \equiv 1 \pmod{m_2} .$$

άρα $a^L \equiv 1 \pmod{[m_1,m_2]}$ και επειδή $\text{ord}_{[m_1,m_2]}(a) = s$ θα είναι $s \mid L$. Τελικά $L=s$ όπως επιθυμούσαμε. ∎

Πόρισμα 8.5

Αν $\text{ord}_{m_1}(a)=t_1$, $\text{ord}_{m_2}(a)=t_2$ και $(m_1,m_2)=1$ τότε

$$\text{ord}_{m_1m_2}(a) = [t_1,t_2] .$$

Παράδειγμα 8.10

Θα υπολογίσουμε την $\text{ord}_{143}(18)$

Είναι $143 = 11 \cdot 13$ με $(11,13)=1$. Επιπλέον, $18 \equiv 7 \pmod{11}$ άρα $\text{ord}_{11}(18) = \text{ord}_{11}(7) = 10$ και $18 \equiv 5 \pmod{13}$ άρα $\text{ord}_{13}(18) = \text{ord}_{13}(5) = 4$ άρα $\text{ord}_{143}(18) = [10,4] = 20$.

Μετά το Παράδειγμα 4.2 είδαμε ότι το αντίστροφο ακριβώς του θεωρήματος του Fermat δεν είναι αλήθες. Απ' όλα τα προηγούμενα, μπορούμε να πάρουμε <u>ένα κριτήριο για πρώτο αριθμό</u>.

Το επόμενο θεώρημα αποδείχθηκε πρώτα από τον E. Lucas το 1876 και απ' αυτό προέκυψαν ισχυρές μέθοδοι για να κρίνουμε αν φυσικοί αριθμοί που έχουν κάποιες μορφές είναι πρώτοι αριθμοί.

<u>Θεώρημα 8.1</u>

Ας είναι $a, n \in \mathbb{Z}$ με $n > 1$. Αν

$a^{n-1} \equiv 1 \pmod{n}$ και $a^d \not\equiv 1 \pmod{n}$ για κάθε φυσικό διαιρέτη d του $n-1$ με $d < n-1$, τότε ο n είναι πρώτος αριθμός.

Απόδειξη.

Αφού $a^{n-1} \equiv 1 \pmod{n}$, θα είναι $(a^{n-1}, n) = (1, n) = 1$, οπότε και $(a, n) = 1$.

Έστω $\text{ord}_n(a) = s$. Τότε $a^s \equiv 1 \pmod{n}$ και επομένως $s \mid n-1$ σύμφωνα με την πρόταση 8.2 ii). Από την υπόθεσή μας όμως υποχρεωτικά θα είναι $s = n-1$. Από το πόρισμα 8.1 θα είναι $n-1 \mid \varphi(n)$, άρα $\varphi(n) \geq n-1$.

Ας υποθέσουμε τώρα ότι ο n είναι σύνθετος, θα υπάρχει επομένως φυσικός διαιρέτης $d \mid n$ με $d < n$, οπότε $\varphi(n) < n-1$ που είναι άτοπο. Άρα ο n είναι πρώτος. ■

<u>Παράδειγμα 8.11</u>

Θα δείξουμε ότι ο 47 είναι πρώτος αριθμός.

Παρατηρούμε ότι,

$\text{ord}_{47}(2) = 23$ και $\text{ord}_{47}(46) = 2$

Επειδή $(23, 2) = 1$ θα έχουμε $\text{ord}_{47}(2 \cdot 46) = 23 \cdot 2 = 46$

Αλλά $2 \cdot 46 = 92 \equiv 45 \pmod{47}$ και επομένως

$\text{ord}_{47}(2 \cdot 46) = \text{ord}_{47}(45) = 46$ δηλαδή $45^{46} \equiv 1 \pmod{47}$.

Είναι λοιπόν $45^{47-1} \equiv 1 \pmod{47}$.

Οι διαιρέτες $d \mid 46$ με $d < 46$ είναι οι $1, 2, 23$.

Γι' αυτούς έχουμε

$$45^1 \equiv 45 \not\equiv 1 \pmod{47},$$

$$45^2 \equiv 4 \not\equiv 1 \pmod{47},$$

$$45^{23} \equiv (47-2)^{23} \equiv (-2)^{23} \equiv -1 \not\equiv 1 \pmod{47}.$$

Άρα ο 47 είναι πρώτος αριθμός.

Πρόταση 8.6

1. Για κάθε περιττό ακέραιο ισχύει

$$a^{2^{\beta-2}} \equiv 1 \pmod{2^\beta}, \quad \beta \geq 3.$$

2. $\text{ord}_{2^\beta}(5) = 2^{\beta-2}$, $\beta \geq 3$.

3. Οι ακέραιοι, $\pm 5, \pm 5^2, \ldots, 5^{2^{\beta-2}}$ αποτελούν ένα αναγμένο σύστημα υπολοίπων $(\text{mod } 2^\beta)$ όπου $\beta \geq 3$.

Απόδειξη.

1. Αν $\eta = 2^\beta$, $\beta \geq 3$ τότε έχουμε $\lambda(n) = \frac{1}{2}\varphi(n)$ από τον ορισμό της συνάρτησης $\lambda(n)$. Αλλά

$$\lambda(2^\beta) = \frac{1}{2}\varphi(2^\beta) = \frac{1}{2}2^{\beta-1} = 2^{\beta-2}.$$

Σύμφωνα με το θεώρημα 7.1 ή Πόρισμα 7.1 αφού $(a, 2^\beta) = 1$ θα είναι

$$a^{2^{\beta-2}} \equiv 1 \pmod{2^\beta}.$$

2. Έστω $\text{ord}_{2^\beta}(5)=t$.

Αφού $(5,2^\beta)=1$, σύμφωνα με το 1, θα είναι $5^{2^{\beta-2}} \equiv 1 \pmod{2^\beta}$, άρα $t \mid 2^{\beta-2}$, από την Πρόταση 8.2 ii).

Υποθέτουμε ότι $t \neq 2^{\beta-2}$, θα καταλήξουμε σε άτοπο. Είναι $t \mid 2^{\beta-2}$ και $t < 2^{\beta-2}$, επομένως $t \mid 2^{\beta-3}$. Σύμφωνα με την Πρόταση 8.2 ii) θα είναι

$$5^{2^{\beta-3}} \equiv 1 \pmod{2^\beta}. \qquad (1)$$

Με επαγωγή μπορούμε να δείξουμε ότι για $\beta \geq 3$ ισχύει

$$5^{2^{\beta-3}} = 1 + 2^{\beta-1} + 2^\beta \cdot A \qquad (*)$$

όπου A ακέραιος.

Για $\beta=3$, φανερά ισχύει.

Υποθέτουμε ότι ισχύει για τον φυσικό $\beta>3$, και ας είναι

$$5^{2^{\beta-3}} = 1 + 2^{\beta-1} + 2^\beta T \quad , \; T \text{ ακέραιος}.$$

Θα δείξουμε ότι ισχύει και για τον φυσικό $\beta+1$.

Υψώνοντας στο τετράγωνο και τα δύο μέλη της παραπάνω ισότητας, έχουμε

$$5^{2^{\beta-2}} = 1 + 2^\beta + 2^{\beta+1}\left(T + 2^{\beta-3} + 2^{\beta-1}T + 2^{\beta-1}T^2\right)$$

$$= 1 + 2^\beta + 2^{\beta+1} \cdot A \quad , \; A \text{ ακέραιος}$$

πράγμα που συμπληρώνει την επαγωγή.

Από τις (1) και (*) θα είχαμε $1 + 2^{\beta-1} \equiv 1 \pmod{2^\beta}$, άρα, $2^{\beta-1} \equiv 0 \pmod{2^\beta}$, δηλαδή $2^\beta \mid 2^{\beta-1}$ πράγμα άτοπο. Άρα $t = 2^{\beta-2}$, πράγμα που επιδιώξαμε.

3. Αφού $\text{ord}_{2^\beta}(5) = 2^{\beta-2}$, σύμφωνα με την πρόταση 8.2 οι $2^{\beta-2}$ σε πλήθος ακέραιοι

$$5, 5^2, \ldots, 5^{2^{\beta-2}} \qquad (i)$$

είναι ανισότιμοι ανα δύο $(\mathrm{mod}\ 2^\beta)$.

Επομένως και οι ακέραιοι

$$-5, -5^2, \ldots, -5^{2^{\beta-2}} \qquad (ii)$$

είναι ανισότιμοι ανα δύο $(\mathrm{mod}\ 2^\beta)$.

Έκαστος όμως των (i) είναι $\equiv 1 \ (\mathrm{mod}\ 4)$, ενώ έκαστος των (ii) είναι $\equiv -1 \ (\mathrm{mod}\ 4)$. Επομένως έκαστος των (i) είναι ανισότιμος $(\mathrm{mod}\ 2^\beta)$ προς έκαστον των (ii). γιατί αν $5^k \equiv -5^\lambda \ (\mathrm{mod}\ 2^\beta)$, $1 \le k, \lambda \le 2^{\beta-2}$ θα ήταν $5^k \equiv -5^\lambda \ (\mathrm{mod}\ 4)$ αφού $\beta \ge 3$, και επομένως $1 \equiv -1 \ (\mathrm{mod}\ 4)$ δηλαδή $4 \mid 2$ πράγμα άτοπο.

Έτσι οι, $2^{\beta-2} + 2^{\beta-2} = 2^{\beta-1} = \varphi(2^\beta)$ σε πλήθος ακέραιοι

$$\pm 5, \pm 5^2, \ldots, \pm 5^{2^{\beta-2}}$$

αποτελούν ένα αναγμένο σύστημα υπολοίπων $(\mathrm{mod}\ 2^\beta)$. ■

ΚΕΦΑΛΑΙΟ V

ΣΥΣΤΗΜΑΤΑ ΓΡΑΜΜΙΚΩΝ ΙΣΟΤΙΜΙΩΝ

Θεωρούμε το επόμενο σύστημα γραμμικών ισοτιμιών

$$(I)\quad \begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_n x \equiv b_n \pmod{m_n} \end{cases}$$

Θα λέμε ότι ο ακέραιος αριθμός x_0 "πληροί ή ικανοποιεί, ή ότι είναι μία κοινή λύση του συστήματος (I) αν πληροί κάθε μία από τις γραμμικές ισοτιμίες του (I) δηλαδή αν

$$a_i x_0 \equiv b_i \pmod{m_i}, \quad i = 1, \dots, n.$$

Ορισμός

Δυό συστήματα γραμμικών ισοτιμιών καλούνται ισοδύναμα, όταν έχουν το ίδιο σύνολο κοινών λύσεων.

Στην συνέχεια θα ασχοληθούμε με την εύρεση του συνόλου όλων των κοινών λύσεων του συστήματος (I). Εάν το σύστημα (I) δεν έχει καμμιά κοινή λύση, θα λέμε ότι το σύστημα δεν έχει λύση. Αυτό συμβαίνει όταν π.χ μία τουλάχιστον απο τις γραμμικές ισοτιμίες του συστήματος (I) δέν έχει λύση. Αλλά ενδεχομένως να μην έχει το σύστημα λύση ακόμη κι' αν κάθε ισοτιμία έχει λύση, π.χ το σύστημα

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 0 \pmod{4} \end{cases}$$

Θα μελετήσουμε και αρχήν ορισμένες μορφές γραμμικών συστημάτων, από τις οποίες τελικά θα οδηγηθούμε στη λύση (όταν υπάρχει) του συστήματος (Ι).

Το πρόβλημα της εύρεσης ενός ακεραίου, ο οποίος μας δίνει ορισμένα υπόλοιπα όταν διαιρείται από δοθέντες ακεραίους, ήταν γνωστό στους αρχαίους Κινέζους, από τον πρώτο αιώνα μ.Χ. Έτσι η εύρεση ενός ακεραίου, ο οποίος δίνει υπόλοιπα 2, 3, 2 όταν διαιρείται από τους ακεραίους 3, 5, 7 αντιστοίχα, ισοδυναμεί με την εύρεση μιας κοινής λύσης του συστήματος

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Θεώρημα 1 (Κινεζικό θεώρημα των υπολοίπων)

Έστω οι φυσικοί αριθμοί $m_1, \dots, m_r$ πρώτοι μεταξύ τους ανά δύο, δηλαδή $(m_i, m_j) = 1$ όταν $i \neq j$.

Τότε το σύστημα των γραμμικών ισοτιμιών

$$(I_1) \quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

έχει μοναδική λύση $\bmod m_1 \cdot m_2 \cdots m_r$.

(Εννοούμε ότι το σύστημα (I_1) έχει μία κοινή λύση x_0, έτσι ώστε το σύνολο των λύσεων του (I_1) να είναι το σύνολο όλων των ακεραίων x ώστε $x \equiv x_0 \pmod{m_1 \cdot m_2 \cdots m_r}$. Θα λέμε επομένως ότι η μοναδική λύση του συστήματος (I_1) είναι η $x \equiv x_0 \pmod{m_1 \cdots m_r}$).

Απόδειξη

Έστω $M = m_1 \cdot m_2 \cdots m_r$ θεωρούμε τους φυσικούς αριθμούς

$$M_i = \frac{M}{m_i} \qquad i = 1, 2, \dots, r$$

για τους οποίους έχουμε, σύμφωνα με την υπόθεση

$$(M_i, m_i) = 1 \quad , \quad i = 1, \dots, r.$$

Έτσι η γραμμική ισοτιμία

$$M_i x \equiv 1 \pmod{m_i}$$

έχει μοναδική λύση, έστω την $b_i \pmod{m_i}$ δηλαδή

$$M_i b_i \equiv 1 \pmod{m_i} \qquad (1)$$

Θα δείξουμε τώρα ότι ο ακέραιος αριθμός

$$\boxed{x_0 = \sum_{i=1}^{r} M_i b_i a_i = M_1 b_1 a_1 + \cdots + M_r b_r a_r} \qquad (2)$$

είναι μια κοινή λύση του συστήματος (I_1).

Πραγματικά για $j \neq i$, $m_j \mid M_i$ δηλαδή $M_i \equiv 0 \pmod{m_j}$ και επομένως

$$M_i b_i a_i \equiv 0 \pmod{m_j}.$$

Άρα $x_0 = \sum_{i=1}^{r} M_i b_i a_i = M_j b_j a_j \overset{(1)}{\equiv} a_j \pmod{m_j}$

δηλαδή ο x_0 πληροί καθε μία από τις ισοτιμίες του συστήματος (I_1).

Αν τώρα x' είναι μια άλλη κοινή λύση του συστήματος (I_1) δηλαδή

$$x' \equiv a_i \pmod{m_i}, \quad i = 1, \ldots, r$$

τότε

$$x' \equiv x_0 \pmod{m_i}, \quad i = 1, \ldots, r$$

Επομένως

$$m_i \mid x' - x_0, \quad i = 1, \ldots, r$$

και επειδή $(m_i, m_j) = 1$ για $i \neq j$ έχουμε ότι

$$m_1 \cdot m_2 \cdots m_r \mid x' - x_0 \Rightarrow x' \equiv x_0 \pmod{m_1 \cdots m_r}.$$

Αντίστροφα, για καθε ακέραιο x με

$$x \equiv x_0 \pmod{m_1 \cdots m_r} \Rightarrow x \equiv x_0 \pmod{m_i}, \ \forall i \in \{1, \ldots, r\}$$

και αφού $x_0 \equiv a_i \pmod{m_i}$ έχουμε $x \equiv a_i \pmod{m_i}$

δηλαδή ο x είναι κοινή λύση του συστήματος (I_1).

Άρα η μοναδική λύση είναι η

$$x \equiv x_0 \pmod{m_1 \cdots m_r} \quad \blacksquare$$

Παράδειγμα 1

Να λύσετε το επόμενο σύστημα γραμμικών ισοτιμιών

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Λύση: Επειδή οι φυσικοί αριθμοί 3, 5, 7 είναι πρώτοι μεταξύ τους ανά δύο, το σύστημα έχει σύμφωνα με το Κινεζικό Θεώρημα μοναδική λύση (mod 105) όπου $105 = 3 \cdot 5 \cdot 7$

Έστω $M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$, $M_3 = \frac{105}{7} = 15$

Οι γραμμικές ισοτιμίες.

$35x \equiv 1 \pmod 3$, $21x \equiv 1 \pmod 5$, $15x \equiv 1 \pmod 7$

έχουν μοναδικές λύσεις αντίστοιχα τις

$x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv 1 \pmod 7$.

Μια κοινή λύση του συστήματος είναι ο ακέραιος

$$x_0 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233.$$

Η μοναδική λύση του συστήματος (mod 105) είναι η

$$x = 233 \equiv 23 \pmod{105}.$$

Όταν οι φυσικοί $m_1, \ldots, m_k$ δεν είναι πρώτοι μεταξύ τους ανά δύο, τότε το πρόβλημα της λύσης (όταν υπάρχει) του συστήματος (I_1) είναι πιό πολύπλοκο. Τα δύο επόμενα θεωρήματα απαντούν στο παραπάνω πρόβλημα.

Θεώρημα 2

Το σύστημα των γραμμικών ισοτιμιών

$$(I_2) \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

έχει τότε και μόνο τότε κοινή λύση όταν

$d \mid a_1 - a_2$ όπου $d = (m_1, m_2)$.

Εάν x_0 είναι μία κοινή λύση του συστήματος (I_2) τότε αυτό έχει μοναδική λύση $(\mathrm{mod}\, L)$ όπου $L=[m_1,m_2]$ την

$$x \equiv x_0 \ (\mathrm{mod}\, L)$$

(Δηλαδή το σύνολο των κοινών λύσεων του συστήματος (I_2) είναι όλοι οι ακέραιοι της μορφής x_0+Lt, $t\in\mathbb{Z}$).

Απόδειξη

Έστω x_0 μια κοινή λύση του συστήματος. Τότε

$$\left.\begin{array}{l} x_0\equiv a_1 \ (\mathrm{mod}\, m_1) \Rightarrow m_1 \mid x_0-a_1 \Rightarrow d\mid x_0-a_1 \\ x_0\equiv a_2 \ (\mathrm{mod}\, m_2) \Rightarrow m_2 \mid x_0-a_2 \Rightarrow d\mid x_0-a_2 \end{array}\right\} \Rightarrow d\mid a_1-a_2 .$$

Αντίστροφα: Έστω $d\mid a_1-a_2$ θα δείξουμε ότι υπάρχει μία κοινή λύση του συστήματος. Οι ακέραιοι που περιέχουν την πρώτη ισοτιμία είναι της μορφής $x=a_1+m_1y$, $y\in\mathbb{Z}$.

Προκειμένου να βρούμε τις κοινές λύσεις του συστήματος, αρκεί να βρούμε εκείνα τα y για τα οποία

$$a_1+m_1y\equiv a_2 \ (\mathrm{mod}\, m_2).$$

ή ισοδύναμα

$$m_1y\equiv a_2-a_1 \ (\mathrm{mod}\, m_2). \qquad (3)$$

Επειδή $d\mid a_2-a_1$ η γραμμική ισοτιμία (3) έχει λύση και επομένως υπάρχει έναν ακέραιος y_0 που την περιέχει. Ο ακέραιος λοιπόν $x_0=a_1+m_1y_0$ είναι μία κοινή λύση του συστήματος.

Έστω τώρα x_0 μια κοινή λύση του συστήματος. Αν x_1 είναι μία άλλη λύση του συστήματος τότε

$$\left.\begin{array}{l} x_1\equiv x_0 \ (\mathrm{mod}\, m_1) \Rightarrow m_1\mid x_1-x_0 \\ x_1\equiv x_0 \ (\mathrm{mod}\, m_2) \Rightarrow m_2\mid x_1-x_0 \end{array}\right\} \Rightarrow L\mid x_1-x_0$$

δηλαδή

$$x_1\equiv x_0 \ (\mathrm{mod}\, L).$$

Αντίστροφα, κάθε ακέραιος της μορφής x_0+Lt, $t\in\mathbb{Z}$ είναι λύση του συστήματος, αφού

$$Lt\equiv 0 \ (\mathrm{mod}\, m_i), \quad i=1,2. \ \blacksquare$$

Παράδειγμα 2

Να λύσετε το σύστημα

$$\begin{cases} x \equiv 3 \pmod 8 \\ x \equiv 7 \pmod{12} \end{cases}$$

Λύση

Είναι $(8,12)=4$ και $[8,12]=24$. Αφού $4 \mid 7-3$ υπάρχει μία μοναδική λύση του συστήματος. Θέτουμε στην 2η γραμμική $x=3+8y$ και παίρνουμε

$$3+8y \equiv 7 \pmod{12} \iff 8y \equiv 4 \pmod{12}$$

η οποία είναι ισοδύναμη με την $2y \equiv 1 \pmod 3$. Αυτή έχει μοναδική λύση την $y \equiv 2 \pmod 3$, άρα ο ακέραιος $x_0 = 3+8\cdot 2 = 19$ είναι μία κοινή λύση του συστήματος. Άρα η μοναδική λύση του συστήματος είναι η $x \equiv 19 \pmod{24}$.

Το επόμενο θεώρημα είναι γενίκευση του θεωρήματος 2.

Θεώρημα 3

Το σύστημα των γραμμικών ισοτιμιών $(n \geq 2)$

$$(I_3) \quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

έχει τότε και μόνον τότε κοινή λύση όταν

$$d_{ij} \mid a_i - a_j \quad , \forall i,j \in \{1,\dots,n\} \text{ με } i \neq j$$

όπου $d_{ij} = d_{ji} = (m_i, m_j)$.

Αν x_0 είναι μία κοινή λύση του συστήματος (I_3) τότε αυτό έχει μοναδική λύση $(\mathrm{mod}\, L)$ όπου $L = [m_1,\dots,m_n]$ την $x \equiv x_0 \pmod L$. (Δηλαδή το σύνολο των κοινών λύσεων του συστήματος (I_3) είναι όλοι οι ακέραιοι της μορφής $x_0 + Lt$, $t \in \mathbb{Z}$).

Απόδειξη

Με επαγωγή πάνω στο πλήθος των γραμμικών ισοτιμιών της

Γενικευμένη μορφή

Για $k=2$ είναι αληθές. Θεώρημα 2.

Υποθέτουμε ότι το θεώρημα είναι αληθές για κάθε σύστημα $k-1$ γραμμικών ισοτιμιών στη θεωρούμενη μορφή.

Έστω τώρα ένα σύστημα k-γραμμικών ισοτιμιών της θεωρούμενης μορφής, τό

$$(*)\quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

και έστω X μια κοινή λύση του. Ο X είναι κοινή λύση του συστήματος των $k-1$ πρώτων γραμμικών ισοτιμιών του $(*)$ και από την υπόθεση επαγωγής

$$d_{ij} = d_{ji} = (m_i, m_j) \mid a_i - a_j \quad \text{για } i,j = 1,\dots,k-1 \text{ και } i \neq j.$$

Αλλά $\begin{cases} X \equiv a_i \pmod{m_i} & i = 1,2,\dots,k-1 \\ X \equiv a_k \pmod{m_k} \end{cases}$

από τις οποίες παίρνουμε.

$$\begin{cases} X \equiv a_i \pmod{d_{ik}} & i = 1,2,\dots,k-1 \\ X \equiv a_k \pmod{d_{ik}} \end{cases}$$

και τελικά

$$a_i \equiv a_k \pmod{d_{ik}} \qquad i = 1,2,\dots,k-1.$$

Επομένως, $d_{ij} \mid a_i - a_j$ για $i,j = 1,2,\dots,k$ και $i \neq j$.

Αντίστροφα: Έστω ότι

$$d_{ij} \mid a_i - a_j \quad \text{για } i,j = 1,\dots,k \text{ και } i \neq j.$$

Σύμφωνα με την υπόθεση επαγωγής, υπάρχει μια κοινή λύση X_0 του συστήματος των $k-1$ πρώτων γραμμικών ισοτιμιών, έτσι ώστε όλες οι κοινές λύσεις αυτού να είναι της μορφής

$$X_0 + L_{k-1} t, \quad t \in \mathbb{Z}$$

όπου $L_{k-1} = [m_1, \dots, m_{k-1}]$.

Είναι δυνατό τώρα να βρούμε μια τιμή του t τέτοια ώστε

ο αριθμός $X_0 + L_{k-1}t$ να ικανοποιεί την γραμμική ισοτιμία

$$x \equiv a_k \pmod{m_k}$$

Για να δείξουμε αυτό, θεωρούμε την γραμμική ισοτιμία

$$X_0 + L_{k-1}t \equiv a_k \pmod{m_k}$$

ή ισοδύναμα την

$$L_{k-1}t \equiv a_k - X_0 \pmod{m_k} \qquad (4)$$

Μπορούμε να δείξουμε ότι η (4) έχει τουλάχιστον μία λύση $t \equiv t_0 \pmod{m_k}$ αν δείξουμε ότι $(L_{k-1}, m_k) \mid a_k - X_0$

Πράγματι, έστω p ένας πρώτος παράγοντας των m_i και m_i' ο εκθέτης της μεγαλύτερης δύναμης αυτού του πρώτου στην πρωτογενή μορφή των m_i. Η μεγαλύτερη δύναμη του p στην πρωτογενή μορφή του L_{k-1}, είναι η μεγαλύτερη δύναμη του p στις πρωτογενείς μορφές των $m_1, \dots, m_{k-1}$. Ας υποθέσουμε ότι είναι η $p^{m_r'}$ δηλαδή η δύναμη του p στην πρωτογενή μορφή του m_r, $1 \le r \le k-1$

Ο εκθέτης τώρα της μεγαλύτερης δύναμης του p στην πρωτογενή μορφή του $D = (L_{k-1}, m_k)$ είναι ο $\min(m_r', m_k') = m_s'$ $(s = k$ ή $s = r)$ Αλλά

$$X_0 - a_r \equiv 0 \pmod{m_r} \Rightarrow X_0 - a_r \equiv 0 \pmod{p^{m_r'}} \Rightarrow$$

$$X_0 - a_r \equiv 0 \pmod{p^{m_s'}} \qquad (5)$$

Ο $d_{kr} \mid a_k - a_r$ και επειδή $p^{\min(m_r', m_k')} \mid d_{kr} \Rightarrow$

$$p^{m_s'} \mid a_k - a_r \quad \text{δηλαδή} \quad a_k - a_r \equiv 0 \pmod{p^{m_s'}} \qquad (6)$$

Από τις ισοτιμίες (5) και (6) συνάγουμε ότι

$$X_0 - a_k \equiv 0 \pmod{p^{m_s'}} \Rightarrow p^{m_s'} \mid X_0 - a_k \qquad (7)$$

Επειδή η σχέση (7) αληθεύει για κάθε πρώτο παράγοντα του $D = (L_{k-1}, m_k)$ και το γινόμενο των δυνάμεων αυτών όλων των πρώτων παραγόντων θα διαιρεί τον $X_0 - a_k$, δηλαδή

$$D \mid X_0 - a_k$$

Επομένως η (4) έχει τουλάχιστον μια λύση $t \equiv t_0 \pmod{m_k}$ έτσι ώστε ο αριθμός $x_0 = X_0 + L_{k-1} t$ να είναι κοινή λύση του συστήματος (*).

Αν τώρα x_0 είναι μία κοινή λύση του συστήματος (*) όλοι οι αριθμοί της μορφής

$$x_0 + L_k t \,, \quad t \in \mathbb{Z} \quad \text{όπου } L_k = [m_1, \dots, m_k]$$

είναι κοινές λύσεις του (*) αφού $L_k t \equiv 0 \pmod{m_i}$

Αντίστροφα, αν x_1 είναι μία άλλη κοινή λύση του (*) οι x_0, x_1 είναι κοινές λύσεις των $k-1$ πρώτων γραμμικών ισοτιμιών του (*) και από την υπόθεση έχουμε

$$\left.\begin{aligned} x_0 &\equiv x_1 \pmod{L_{k-1}} \\ x_0 &\equiv x_1 \pmod{m_k} \end{aligned}\right\} \Rightarrow x_0 \equiv x_1 \pmod{[L_{k-1}, m_k]}$$

δηλαδή

$$x_0 \equiv x_1 \pmod{L_k}$$

αφού $[L_{k-1}, m_k] = [[m_1, \dots, m_{k-1}], m_k] = L_k$.

Το θεώρημα λοιπόν ισχύει για κάθε σύστημα n-γραμμικών ισοτιμιών $(n \geq 2)$. ∎

Παρατήρηση:

Το Κινεζικό θεώρημα των υπολοίπων είναι μία ιδιαίτερη περίπτωση του θεωρήματος 3. Πραγματικά αν $(m_i, m_j) = 1$ με $i \neq j$ τότε $[m_1, \dots, m_k] = m_1 \cdots m_k$. Στην περίπτωση αυτή το σύστημα έχει πάντα λύση μοναδική mod $m_1 \cdots m_k$.

Παράδειγμα 3

Να λύσετε το σύστημα των γραμμικών ισοτιμιών

$$\begin{cases} x \equiv 7 \pmod{18} \\ x \equiv 10 \pmod{15} \\ x \equiv 1 \pmod{14} \end{cases}$$

Λύση

Έστω $d_1=(18,15)=3$, $d_2=(18,14)=2$, $d_3=(15,14)=1$

Επειδή $d_1 \mid x-10$, $d_2 \mid x-1$, $d_3 \mid 10-1$, το σύστημα έχει κοινή λύση που είναι μοναδική mod 630 όπου $630=[18,15,14]$.

Εργαζόμαστε ως εξής:

Παίρνουμε το σύστημα των δύο πρώτων γραμμικών ισοτιμιών

$$(i)\begin{cases} x\equiv 7 \pmod{18} \\ x\equiv 10 \pmod{15} \end{cases}$$

και δουλεύοντας όπως στο παράδειγμα 2 βρίσκουμε τη μοναδική λύση mod 90 όπου $90=[18,15]$. Είναι αυτή η

$$x\equiv 25 \pmod{90}$$

Στην συνέχεια παίρνουμε το σύστημα

$$\begin{cases} x\equiv 25 \pmod{90} \\ x\equiv 1 \pmod{14} \end{cases}$$

και όμοια βρίσκουμε ότι η $x\equiv 295 \pmod{630}$ είναι η μοναδική λύση, όπου $630=[90,14]=[18,15,14]$.

Η $x\equiv 295 \pmod{630}$ είναι η μοναδική λύση του αρχικού μας συστήματος.

Παράδειγμα 4

Να λύσετε το σύστημα των γραμμικών ισοτιμιών

$$\begin{cases} x\equiv 11 \pmod{21} \\ x\equiv 4 \pmod{10} \\ x\equiv 2 \pmod{12} \end{cases}$$

Λύση

Είναι $d_1=(21,10)=1$, $d_2=(21,12)=3$, $d_3=(10,12)=2$, και αφού $d_1 \mid 11-4$, $d_2 \mid 11-2$, $d_3 \mid 4-2$ το σύστημα έχει μοναδική λύση mod 420 όπου $420=[21,10,12]$. Πράγματι το σύστημα

$$\begin{cases} x\equiv 11 \pmod{21} \\ x\equiv 4 \pmod{10} \end{cases}$$

έχει σύμφωνα με το κινεζικό θεώρημα μοναδική λύση

mod 210 όπου $210=[21,10]$ την $x\equiv\mp4 \pmod{210}$

Στην συνέχεια παίρνουμε το σύστημα

$$\begin{cases} x\equiv\mp4 \pmod{210} \\ x\equiv 2 \pmod{12} \end{cases}$$

Το οποίο έχει μοναδική λύση σύμφωνα με το θεώρημα 2 την $x\equiv\mp4 \pmod{420}$

όπου: $420=[210,12]=[21,10,12]$

Έτσι το αρχικό σύστημα έχει μοναδική λύση την

$x\equiv\mp4 \pmod{420}$. ∎

Ας επιστρέψουμε πίσω στο αρχικό σύστημα

$$(I)\quad \begin{cases} a_1x\equiv b_1 \pmod{m_1} \\ a_2x\equiv b_2 \pmod{m_2} \\ \vdots \\ a_nx\equiv b_n \pmod{m_n} \end{cases}$$

Για να έχει κοινή λύση είναι αναγκαία προφανώς καθεμία από τις γραμμικές ισοτιμίες του (I) να έχει λύση, δηλαδή πρέπει να έχουμε:

$$d_k \mid b_k \quad k=1,\dots,n \text{ , όπου } d_k=(a_k,m_k).$$

Αν αυτό ισχύει, έστω

$$b_k=d_k b_k' \text{ , } m_k=d_k m_k' \text{ , } a_k=d_k a_k' \text{ , } k=1,\dots,n.$$

Τότε η ισοτιμία $a_kx\equiv b_k \pmod{m_k}$ είναι ισοδύναμη με την $a_k'x\equiv b_k' \pmod{m_k'}$ $k=1,\dots,n$

και το σύστημα

$$(I')\quad \begin{cases} a_1'x\equiv b_1' \pmod{m_1'} \\ a_2'x\equiv b_2' \pmod{m_2'} \\ \vdots \\ a_n'x\equiv b_n' \pmod{m_n'} \end{cases} \quad , (a_k',m_k')=1$$

είναι ισοδύναμο με το σύστημα (I).

Επειδή $(a'_k, m'_k) = 1$, η γραμμική ισοτιμία $a'_k x \equiv b'_k \pmod{m'_k}$ έχει μοναδική λύση $x \equiv c_k \pmod{m'_k}$, $k = 1, \dots, n$

Κατα ακόλουθο το σύστημα

$$(I'') \begin{cases} x \equiv c_1 \pmod{m'_1} \\ x \equiv c_2 \pmod{m'_2} \\ \vdots \\ x \equiv c_n \pmod{m'_n} \end{cases}$$

είναι ισοδύναμο με το (I'), επομένως και με το (I).

Η λύση (όταν υπάρχει) του συστήματος (I'') σύμφωνα με το θεώρημα 3 είναι μοναδική $(\bmod L')$ όπου

$$L' = [m'_1, \dots, m'_n]$$

η οποία είναι η μοναδική λύση $(\bmod L')$ του (I)

Παράδειγμα.

Να λύσετε το σύστημα

$$2x \equiv 4 \pmod{12}$$
$$2x \equiv 8 \pmod{20}$$

Λύση

Εστω $d_1 = (2,12) = 2$, $d_2 = (2,20) = 2$ Επειδή $d_1 | 4$ και $d_2 | 8$ το σύστημα πιθανόν να έχει λύση. Αυτό είναι ισοδύναμο με το σύστημα

$$x \equiv 2 \pmod{6}$$
$$x \equiv 4 \pmod{10}$$

Είναι $(6,10) = 2$ και $2 | 4-2$, επομένως το σύστημα έχει μοναδική λύση $\bmod 30$ όπου $30 = [6,10]$.

Από την πρώτη έχουμε $x = 2 + 6y$ οπότε $2 + 6y \equiv 4 \pmod{10}$, έτσι $6y \equiv 2 \pmod{10}$. Ο ακέραιος $y = 2$ είναι λύση της, επομένως ο ακέραιος $2 + 6 \cdot 2 = 14$ είναι μία κοινή λύση του συστήματος. Έτσι η μοναδική λύση του είναι η

$$x \equiv 14 \pmod{30}.$$

Παράδειγμα 6

Να λύσετε το σύστημα των γραμμικών ισοτιμιών

$$\begin{cases} 5x \equiv 6 \pmod 8 \\ 8x \equiv 10 \pmod{14} \\ 10x \equiv 5 \pmod{15} \end{cases}$$

Λύση

Είναι $d_1=(5,8)=1$, $d_2=(8,14)=3$, $d_3=(10,15)=5$. Επειδή $d_1|6$, $d_2|10$, $d_3|5$ το σύστημα είναι ισοδύναμο με το σύστημα

$$\begin{cases} 5x \equiv 6 \pmod 8 \\ 4x \equiv 5 \pmod 7 \\ 2x \equiv 1 \pmod 3 \end{cases}$$

Αυτό είναι ισοδύναμο με το σύστημα

$$\begin{cases} x \equiv 6 \pmod 8 \\ x \equiv 3 \pmod 7 \\ x \equiv 2 \pmod 3 \end{cases}$$

αφού $(5,8)=1$, $(4,7)=1$, $(2,3)=1$.

Από το Κινεζικό θεώρημα, αυτό έχει μοναδική λύση την $x \equiv 38 \pmod{168}$ όπου $168=8\cdot 7\cdot 3$, η οποία είναι και η μοναδική λύση mod 168 του αρχικού συστήματος.

Παράδειγμα 7

Να λύσετε το σύστημα των γραμμικών ισοτιμιών

$$\begin{cases} 2x \equiv 4 \pmod 8 \\ 3x \equiv 12 \pmod 9 \\ x \equiv 34 \pmod{12} \end{cases}$$

Λύση

Έστω $d_1=(2,8)=2$, $d_2=(3,9)=3$, $d_3=(1,12)=1$. Επειδή $d_1|4$, $d_2|12$, $d_3|34$, το σύστημα πιθανόν να έχει λύση. Είναι ισοδύναμο με το

$$\begin{cases} x \equiv 2 \pmod 4 \\ x \equiv 4 \pmod 3 \\ x \equiv 34 \pmod{12} \end{cases}$$

Σύμφωνα με το θεώρημα 3, το σύστημα αυτό έχει μοναδική λύση την $x \equiv 10 \pmod{12}$ όπου $12=[4,3,12]$. Αυτή είναι και η μοναδική λύση του αρχικού συστήματος.

ΑΣΚΗΣΕΙΣ

1

Αν $a+b \neq 0$, $(a,b)=1$ και p ένας περιττός πρώτος αριθμός τότε

$$\left(a+b,\ \frac{a^p+b^p}{a+b}\right)=1 \text{ ή } p.$$

Λύση

Γράφουμε $a^p=(a+b-b)^p=\binom{p}{0}(a+b)^p-\binom{p}{1}(a+b)^{p-1}b+\cdots+\binom{p}{p-1}(a+b)b^{p-1}-b^p$

αφού ο p είναι περιττός πρώτος, οπότε

$$a^p+b^p=(a+b)^p-\binom{p}{1}(a+b)^{p-1}b+\cdots+\binom{p}{p-1}(a+b)b^{p-1}$$

Έτσι

$$\frac{a^p+b^p}{a+b}=(a+b)^{p-1}-\binom{p}{1}(a+b)^{p-2}b+\cdots+pb^{p-1}=$$

$$=k(a+b)+pb^{p-1}.$$

Άρα

$$\delta=\left(a+b,\ \frac{a^p+b^p}{a+b}\right)=\left(a+b,\ k(a+b)+pb^{p-1}\right)=\left(a+b,\ pb^{p-1}\right)$$

$$=(a+b,\ p\underbrace{b\cdots b}_{(p-1)\text{ φορές}})$$

$$=(a+b,\ p\cdot(a+b,b)^{p-1})$$

$$=(a+b,\ p\cdot(a,b)^{p-1})$$

$$=(a+b,\ p).$$

Έτσι $\delta \mid p \Rightarrow \delta=1$ ή p. ∎

2

Για κάθε ζεύγος διαιρεμμένων αμεραίων a,b και για κάθε φυσικό αριθμό $n\geq 1$ ισχύει

$$\left(\frac{a^n-b^n}{a-b},\ a-b\right)=\left(n(a,b)^{n-1},\ a-b\right)$$

Τι συμβαίνει όταν ο n είναι πρώτος αριθμός και $(a,b)=1$.

Λύση

Είναι $A=\dfrac{a^n-b^n}{a-b}=a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1}$

Έτσι

$$A = A - (n-1)a^{n-1} + (n-1)b^{n-1} = (a^{n-1} - b^{n-1}) + (a^{n-2}b - b^{n-1}) + \dots + (ab^{n-2} - b^{n-1}) + nb^{n-1}$$

$$= (a^{n-1} - b^{n-1}) - (a^{n-2} - b^{n-2})b + \dots + (a-b)b^{n-2} + nb^{n-1}$$

$$= (a-b)P(a,b) + nb^{n-1} \qquad (1)$$

όπου $P(a,b)$ είναι ένα πολυώνυμο των a και b με ακέραιους συντελεστές.

Όμοια λόγω συμμετρίας έχουμε

$$\frac{a^n - b^n}{a-b} = (a-b)Q(a,b) + na^{n-1} \qquad (2)$$

όπου $Q(a,b)$ ένα πολυώνυμο των a και b με ακέραιους συντελεστές.

Έστω $d = \left(\frac{a^n - b^n}{a-b}, a-b\right)$ και $\delta = (n(a,b)^{n-1}, a-b)$

Είναι,

$$\left.\begin{matrix} d \mid \frac{a^n-b^n}{a-b} \\ d \mid a-b \end{matrix}\right\} \xrightarrow{(1)} d \mid nb^{n-1}. \text{ Όμοια } \left.\begin{matrix} d \mid \frac{a^n-b^n}{a-b} \\ d \mid a-b \end{matrix}\right\} \xrightarrow{(2)} d \mid na^{n-1}$$

Επομένως,

$$d \mid (nb^{n-1}, na^{n-1}) = n(a,b)^{n-1}. \qquad (3)$$

Από την (3) και επειδή $d \mid a-b \Rightarrow d \mid \delta$.

Από την άλλη μεριά, $\delta \mid n(a,b)^{n-1} = (na^{n-1}, nb^{n-1})$, επομένως $\delta \mid na^{n-1}$ και $\delta \mid nb^{n-1}$. Από τις (1) και (2) και επειδή $\delta \mid a-b$ έχουμε $\delta \mid \frac{a^n-b^n}{a-b}$.

Έτσι

$$\left.\begin{matrix} \delta \mid \frac{a^n-b^n}{a-b} \\ \delta \mid a-b \end{matrix}\right\} \Longrightarrow \delta \mid \left(\frac{a^n-b^n}{a-b}, a-b\right) = d.$$

Άρα $\delta = d$, πράγμα που επιδιώξαμε.

Αν ο n είναι πρώτος αριθμός και $(a,b) = 1$ τότε

$$d = \left(\frac{a^n-b^n}{a-b}, a-b\right) = (n, a-b) = 1 \text{ ή } n. \quad \blacksquare$$

3

Αν $(a,b)=1$ τότε για φυσιακούς αριθμούς m και n ισχύει

$$(a^m-b^m,\ a^n-b^n)=a^{(m,n)}-b^{(m,n)}$$

Λύση

Έστω $d=(m,n)$, $e=a^d-b^d$ και $\delta=(a^m-b^m,\ a^n-b^n)$.

Θα δείξουμε ότι $\delta=e$.

Έχουμε $\left.\begin{array}{l} d|m \Rightarrow e|a^m-b^m \\ d|n \Rightarrow e|a^n-b^n \end{array}\right\} \Rightarrow e|\delta \qquad (1)$

Θα αποδείξουμε τώρα ότι $\delta|e$. Επιλέγουμε ακεραίους $x>0$ και $y>0$ τέτοιους ώστε (Κεφ. II, Πόρισμα 9.2)

$$mx-ny=d.$$

Είναι $$a^{mx}=a^{ny+d}=a^{ny}a^d=a^{ny}(b^d+e)$$

οπότε $$a^{mx}-b^{nx}=a^{ny}(b^d+e)-b^{ny+d}=b^d(a^{ny}-b^{ny})+ea^{ny} \qquad (2)$$

Αλλά

$$\left.\begin{array}{l} \delta|a^m-b^m \Rightarrow \delta|a^{mx}-b^{nx} \\ \delta|a^n-b^n \Rightarrow \delta|a^{ny}-b^{ny} \end{array}\right\} \overset{(2)}{\Longrightarrow} \delta|ea^{ny} \qquad (3)$$

Παρατηρούμε ότι $\delta'=(\delta,a)=1$. Πραγματικά,

$$\left.\begin{array}{l} \delta'|a \Rightarrow \delta'|a^m \\ \delta'|\delta \Rightarrow \delta'|a^m-b^m \end{array}\right\} \Rightarrow \delta'|b^m.$$ Έτσι $\delta'|(a^m,b^m)=(a,b)^m=1$.

Από την (3) αφού $(\delta,a^{ny})=(\delta,(\delta,a)^{ny})=(\delta,1)=1$

έχουμε $\delta|e \qquad (4)$

Από τις (1) και (4) έχουμε $\delta=e$. ∎

4

Αν $A=\underbrace{22\cdots2}_{n\ \text{ψηφία}}$ και $B=\underbrace{88\cdots8}_{m\ \text{ψηφία}}$ τότε

$$(A,B)=\frac{2}{9}(10^d-1) \quad \text{όπου } d=(n,m)$$

Λύση

Για τους φυσιακούς αριθμούς A και B έχουμε

$A = 2\cdot\frac{10^n-1}{9}$ και $B = 8\,\frac{10^m-1}{9}$. Έτσι

$$(A,B) = \frac{2}{9}\left(10^n-1,\ 4(10^m-1)\right) = \frac{2}{9}\left(10^n-1,\ (10^n-1,4)(10^m-1)\right)$$

$$= \frac{2}{9}\left(10^n-1,\ 10^m-1\right) \quad \text{αφού } (10^n-1,4)=1.$$

Σύμφωνα με την άσκηση 3, $(10^n-1,\ 10^m-1) = 10^{(m,n)}-1$

οπότε $$(A,B) = \frac{2}{9}\left(10^d-1\right) \quad \text{όπου } d=(n,m). \blacksquare$$

5

Υποθέτουμε ότι $(m,n)=1$. Δείξτε ότι

$$(mx+ny,\ mn)=1 \iff (x,n)=(y,m)=1.$$

Λύση

Επειδή $(m,n)=1$ έχουμε

$$(mx+ny,\ mn) = (mx+ny,\ m)\cdot(mx+ny,\ n) = (ny,m)\cdot(mx,n).$$

Αν $(mx+ny,\ mn)=1$ τότε $(ny,m)=1$ και $(mx,n)=1$. Άρα

$$1=(m,ny)=(m,(n,n)y)=(m,y) \quad \text{και}$$

$$1=(n,mx)=(n,(n,m)x)=(n,x)$$

πράγμα που επιδιωκόσαμε.

Αντίστροφα, αν

$$1=(x,n)=((m,n)x,\ n)=(mx,\ nx,\ n)=(mx,n)$$

και $$1=(y,m)=((m,n)y,\ m)=(my,\ ny,\ m)=(ny,m)$$

οπότε $$(mx+ny,\ mn)=(ny,m)(mx,n)=1\cdot 1=1. \blacksquare$$

6

Θεωρούμε την αριθμητική συνάρτηση

$$g(n)=\begin{cases} 1 & \text{όταν } n=1 \\ (1-p_1)\cdots(1-p_k) & \text{όταν } n>1 \text{ με } n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}. \end{cases}$$

Αν φ είναι η συνάρτηση του Euler τότε

$$\sum_{d|n} \varphi(d) g\left(\frac{n}{d}\right) = \begin{cases} 1 & \text{όταν } n=1 \\ 0 & \text{όταν } n>1 \end{cases}$$

Λύση

Η συνάρτηση g είναι πολλ/νή. Πραγματικά αν $m,n \in \mathbb{N}$ και είναι συνλάχιστον αλλήλους είναι ίσος με 1 τότε $(m,n)=1$ και $g(mn)=g(m)g(n)$. Αν $(m,n)=1$ και $m>1$, $n>1$ τότε αν

$$n = p_1^{a_1} \cdots p_\kappa^{a_\kappa}$$
$$m = q_1^{b_1} \cdots q_\lambda^{b_\lambda} \quad \text{με } p_i \neq q_i$$

θα είναι

$$nm = p_1^{a_1} \cdots p_\kappa^{a_\kappa} q_1^{b_1} \cdots q_\lambda^{b_\lambda}$$

και

$$g(nm) = (1-p_1)\cdots(1-p_\kappa)(1-q_1)\cdots(1-q_\lambda) = g(n)g(m)$$

Αφού και η συνάρτηση φ είναι πολλ/νή, πολλ/νή θα είναι και η συνάρτηση

$$F(n) = \sum_{d|n} \varphi(d) g\left(\frac{n}{d}\right)$$

θα είναι πολλ/νή

Αν $n=1$ τότε $F(1) = \sum_{d|1} \varphi(d) g\left(\frac{1}{d}\right) = \varphi(1)g(1) = 1$

Αν $n>1$ και $n = p_1^{a_1} \cdots p_\kappa^{a_\kappa}$ τότε

$$F(n) = F\left(p_1^{a_1}\right) \cdots F\left(p_\kappa^{a_\kappa}\right). \qquad (1)$$

Για πρώτο αριθμό p και $a \in \mathbb{N}$ έχουμε

$$F(p^a) = \sum_{d|p^a} \varphi(d) g\left(\frac{p^a}{d}\right) = \varphi(1)g(p^a) + \varphi(p)g(p^{a-1}) + \cdots + \varphi(p^{a-1})g(p) + \varphi(p^a)g(1)$$
$$= (1-p) + (p-1)(1-p) + p(p-1)(1-p) + \cdots + p^{a-2}(p-1)(1-p) + p^{a-1}(p-1)1$$
$$= (1-p)\left[1 + p - 1 + p(p-1) + \cdots + p^{a-2}(p-1)\right] + p^a - p^{a-1}$$
$$= (1-p)p^{a-1} + p^a - p^{a-1} = p^{a-1} - p^a + p^a - p^{a-1} = 0$$

Έτσι από την (1) έχουμε

$$F(n) = 0 \cdot 0 \cdots 0 = 0 \qquad \blacksquare$$

7

Για την αριθμητική συνάρτηση $f: \mathbb{N} \to \mathbb{C}$ που ορίζεται ως εξής

$$f(n) = \frac{1}{n} \sum_{\substack{1 \le k \le n \\ (k,n)=1}} k$$

δείξτε ότι

$$\sum_{d|n} f(d) = \frac{1}{2}(n+1)$$

Λύση

Από το θεώρημα 5.3 του κεφ. III γνωρίζουμε ότι, για $n>1$

$$\sum_{\substack{1 \le k \le n \\ (k,n)=1}} k = \frac{1}{2} n \varphi(n) .$$

Έτσι για $n>1$ είναι $f(n) = \frac{1}{2}\varphi(n)$.

Έχουμε

$$\sum_{d|n} f(d) = f(1) + \sum_{\substack{d|n \\ d>1}} f(d) = 1 + \sum_{\substack{d|n \\ d>1}} f(d) = 1 + \frac{1}{2} \sum_{\substack{d|n \\ d>1}} \varphi(d)$$

$$= 1 + \frac{1}{2}\left[\sum_{d|n} \varphi(d) - \varphi(1)\right] = 1 + \frac{1}{2}\left[\sum_{d|n} \varphi(d) - 1\right]$$

$$= 1 - \frac{1}{2} + \frac{1}{2} \sum_{d|n} \varphi(d) \qquad \text{(Θεωρ 5.1 κεφ III)}$$

$$= 1 - \frac{1}{2} + \frac{1}{2} n = \frac{1}{2}(n+1) . \blacksquare$$

8

Αν $\tau(n)$ συμβολίζει το πλήθος των φυσικών διαιρετών του φυσικού n, τότε:

Οι αριθμητικές συναρτήσεις

$$F(n) = \sum_{d|n} \tau^3(d) \qquad \text{και} \qquad \Phi(n) = \left(\sum_{d|n} \tau(d)\right)^2$$

είναι πολλαπλασιαστικές, και μάλιστα

$$F(n) = \Phi(n) \quad , \forall n \in \mathbb{N}.$$

Λύση

Η συνάρτηση τ είναι πολλ/μή (θεωρ. 6.1 Κεφ III), άρα η συνάρτηση τ^3 είναι πολλ/μή (θεωρ. 3.2 i), Κεφ III) συνεπώς και η αριθμητική συνάρτηση $F(n) = \sum_{d|n} \tau^3(d)$ είναι πολλ/μή (Πορ. 3.5)

Όμοια η συνάρτηση

$$\sum_{d|n} \tau(d)$$

είναι πολλ/μή και επομένως και η $\Phi(n)$ είναι πολλ/μή.

Για να δείξουμε ότι $F = \Phi$ αρκεί να δείξουμε (Πορ. 3.2) ότι

$$F(p^a) = \Phi(p^a)$$

για κάθε πρώτο αριθμό p και $a \in \mathbb{N}$.

Πραγματικά,

$$F(p^a) = \sum_{d|p^a} \tau^3(d) = \tau^3(1) + \tau^3(p) + \cdots + \tau^3(p^a) =$$

$$= 1^3 + 2^3 + \cdots + (a+1)^3 = \frac{1}{4}(a+1)^2(a+2)^2 \quad (1)$$

$$\Phi(p^a) = \left(\sum_{d|p^a} \tau(d)\right)^2 = \left(\tau(1) + \tau(p) + \cdots + \tau(p^a)\right)^2$$

$$= \left(1 + 2 + \cdots + (a+1)\right)^2 = \left(\frac{1}{2}(a+1)(a+2)\right)^2$$

$$= \frac{1}{4}(a+1)^2(a+2)^2 \quad (2)$$

Από τις (1) και (2) έχουμε ότι $\Phi = F$. ∎

9

Αν είναι $q \in \mathbb{C}$ και W μια αριθμητική συνάρτηση, έτσι ώστε

$$q^n = \sum_{d|n} d \cdot W(d) \qquad n \in \mathbb{N}$$

α) Βρείτε το $W(24)$ συναρτήσει του q.

β) Αν $q \in \mathbb{Z}$, δείξτε ότι $W(24) \in \mathbb{Z}$.

Λύση

Θεωρούμε τις αριθμητικές συναρτήσεις $g, f : \mathbb{N} \to \mathbb{C}$

που ορίζονται ως εξής:

$g(n) = q^n \quad \forall n \in \mathbb{N}$ και $f(n) = n \cdot W(n), \ \forall n \in \mathbb{N}$

Είναι από την υπόθεση

$$g(n) = \sum_{d|n} f(d)$$

και από το θεώρημα Αντιστροφής του Möbius,

$$f(n) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right)$$

δηλαδή

$$n\, W(n) = \sum_{d|n} \mu(d)\, q^{\frac{n}{d}} \qquad (1)$$

α) Αν $n=24$ τότε από την (1) έχουμε

$$24 \cdot W(24) = \sum_{d|24} \mu(d)\, q^{\frac{24}{d}}$$

Έτσι, $24 \cdot W(24) = \mu(1)q^{24} + \mu(2)q^{12} + \mu(3)q^8 + \mu(4)q^6 +$

$+\mu(6)q^4 + \mu(8)q^3 + \mu(12)q^2 + \mu(24)q =$

$= q^{24} - q^{12} - q^8 + q^4.$

Άρα

$$W(24) = \frac{1}{24}\left(q^{24} - q^{12} - q^8 + q^4\right) \qquad (2)$$

β) Αν $q \in \mathbb{Z}$ τότε ο $B = q^4 - q^8 - q^{12} + q^{24} \in \mathbb{Z}$.

Για να είναι $W(24) = \frac{B}{24} \in \mathbb{Z}$ πρέπει $24 \mid B$ δηλαδή

$3 \cdot 8 \mid B$. Αφού $(3,8) = 1$ αρκεί να δείξω ότι

$$3 \mid B \quad \text{και} \quad 8 \mid B.$$

β_1) Θα δείξουμε ότι $3 \mid B$.

Για τον $q \in \mathbb{Z}$ έχουμε $3 \mid q$ ή $3 \nmid q$.

Αν $3 \mid q \Rightarrow 3 \mid B$.

Αν $3 \nmid q$ τότε $q \equiv 1 \pmod 3$ ή $q \equiv 2 \pmod 3$

οπότε $q^2 \equiv 1 \pmod 3$ ή $q^2 \equiv 4 \pmod 3 \equiv 1 \pmod 3$.

Έτσι $q^2 \equiv 1 \pmod 3$ και $q^{2k} \equiv 1 \pmod 3$

Άρα $B \equiv 1 - 1 - 1 + 1 \pmod 3$ δηλ $B \equiv 0 \pmod 3$

Άρα πάντα 3|B

b_2) Θα δείξουμε ότι 8|B.

Για τον $q \in \mathbb{Z}$ έχουμε 2|q ή 2∤q

Αν 2|q ⇒ $2^4 | q^4$ δηλαδή 16|q^4 άρα 8|q^4 Έτσι

$q^4 \equiv 0 \pmod 8$, $q^8 \equiv 0 \pmod 8$, $q^{12} \equiv 0 \pmod 8$, $q^{24} \equiv 0 \pmod 8$

Άρα $B \equiv 0 \pmod 8$ δηλαδή 8|B.

Αν 2∤q τότε $q = 2k+1$ και $q^2 = 4k^2+4k+1$ δηλαδή

$q^2 - 1 = 4k(k+1)$. Αλλά 2|k(k+1) οπότε $q^2 - 1 = 8\lambda$

για κάποιο λ, δηλαδή $q^2 \equiv 1 \pmod 8$.

Έτσι $q^4 \equiv 1 \pmod 8$, $q^8 \equiv 1 \pmod 8$, $q^{12} \equiv 1 \pmod 8$

και $q^{24} \equiv 1 \pmod 8$. Άρα

$B = 1 - 1 - 1 + 1 \pmod 8$ δηλαδή $B \equiv 0 \pmod 8$. ∎

10

Να δείξετε ότι $11 \cdot 31 \cdot 61 \mid 20^{15} - 1$.

Λύση

Αφού οι φυσικοί αριθμοί 11, 31, 61 είναι πρώτοι μεταξύ τους ανά δύο, αρκεί να δείξουμε ότι (Πόρισμα 6.11, Κεφ II)

$11 \mid 20^{15} - 1$, $31 \mid 20^{15} - 1$, $61 \mid 20^{15} - 1$

α) Ο 11 είναι πρώτος αριθμός και 11∤20, επομένως από Θεώρημα Fermat, $2^{10} \equiv 1 \pmod{11}$ (1)

Επίσης, $20^5 = (2 \cdot 10^5) = 2^5 \cdot 10^5$ και

$2^5 = 32 \equiv -1 \pmod{11}$, $10 \equiv -1 \pmod{11}$ άρα $10^5 \equiv -1 \pmod{11}$.

Έτσι $20^5 = 2^5 \cdot 10^5 \equiv 1 \pmod{11}$ (2)

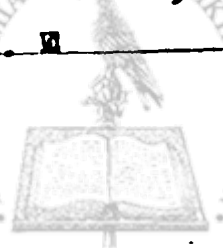
Από τις (1) και (2) έχουμε ότι $20^{15} \equiv 1 \pmod{11}$

β) $\left.\begin{array}{l} 20 \equiv -11 \pmod{31} \\ 20^2 \equiv 400 \equiv -3 \pmod{31} \end{array}\right\} \Rightarrow 20^3 \equiv 33 \equiv 2 \pmod{11}$ ...

Άρα $(20^3)^5 \equiv 2^5 \equiv 32 \equiv 1 \pmod{31}$

γ) $20 \equiv 81 \pmod{61}$ δηλαδή $20 \equiv 3^4 \pmod{61}$. Άρα $20^{15} \equiv 3^{60} \pmod{61}$

Από Θ. Fermat $3^{60} \equiv 1 \pmod{61}$ άρα $20^{15} \equiv 1 \pmod{61}$. ∎



11

Να βρεθεί το υπόλοιπο της διαίρεσης του αριθμού

$$A = 11^{11} + 11^{11^2} + \cdots + 11^{11^{11}}$$

με τον αριθμό 7.

Λύση

Αρκεί να βρούμε φυσικό k, $0 \le k \le 6$ έτσι ώστε $A \equiv k \pmod 7$.

Είναι
$$\left.\begin{aligned} 11 &\equiv 4 \pmod 7 \\ 11^{11} &\equiv 4^{11} \pmod 7 \\ &\vdots \\ 11^{11^{11}} &\equiv 4^{11^{11}} \pmod 7 \end{aligned}\right\} \Rightarrow A \equiv 4^{11} + 4^{11^2} + \cdots + 4^{11^{11}} \pmod 7.$$

Θα υποβιβάσουμε τους εκθέτες. Παρατηρούμε ότι

$4^2 \equiv 2 \pmod 7$ και $4^3 \equiv 8 \equiv 1 \pmod 7$

Θα βρούμε λοιπόν τα υπόλοιπα των εκθετών $11, 11^2, \ldots, 11^{11}$ διαιρούμενων με τον 3, αφού $4^3 \equiv 1 \pmod 7$.

$11 \equiv 2 \pmod 3 \Rightarrow 11^{2k} \equiv 2^{2k} \equiv 4^k \equiv 1 \pmod 3$

Δηλαδή $11^{2k} = 1 \pmod 3$ (1)

Επίσης $11^{2k+1} \equiv 11 = 2 \pmod 3$ (2)

Έτσι από την (1) $11^{2k} = 3\lambda + 1$, $\lambda \in \mathbb{Z}$

και από την (2) $11^{2k+1} = 3\rho + 2$, $\rho \in \mathbb{Z}$.

Άρα
$$\left.\begin{aligned} 4^{11^{2k}} &= 4^{3\lambda+1} = 4^{3\lambda} \cdot 4 \equiv 4 \pmod 7 \\ \text{και } 4^{11^{2k+1}} &= 4^{3\rho+2} = 4^{3\rho} \cdot 4^2 \equiv 4^2 \equiv 2 \pmod 7 \end{aligned}\right\} \text{(3)}$$

Επομένως, από την (3) έχουμε

$$A \equiv 2+4+2+4+2+4+2+4+2+4+2 \pmod 7$$

δηλ. $A \equiv 32 \pmod 7 \Rightarrow A \equiv 4 \pmod 7$.

Το ζητούμενο υπόλοιπο λοιπόν είναι 4. ∎

12

Να δείξετε ότι $9^{9^9} \equiv 89 \pmod{100}$

Λύση

Παρατηρούμε ότι

$$9^2 \equiv 81 \pmod{10}$$
$$9^4 \equiv 81^2 \equiv 61 \pmod{100}$$
$$9^8 \equiv 61^2 \equiv 21 \pmod{100}$$
$$9^{10} \equiv 21 \cdot 9 \equiv 89 \pmod{100}$$
$$9^{20} \equiv 89 \cdot 9 \equiv 1 \pmod{100}$$

Αφού $9^{10} \equiv 1 \pmod{100}$, μας διευκολύνει να βρούμε το υπόλοιπο του 9^9 διαιρούμενο με τον 10. Είναι

$9^2 \equiv 1 \pmod{10} \Rightarrow 9^8 \equiv 1 \pmod{10}$. Άρα $9^9 \equiv 9 \pmod{10}$

δηλαδή $9^9 = 10k + 9$, $k \in \mathbb{Z}$. Επομένως

$$9^{9^9} \equiv 9^{10k+9} \equiv 9^{10k} \, 9^9 \pmod{100}$$
$$\equiv 1 \cdot 89 \pmod{100} \equiv 89 \pmod{100}. \blacksquare$$

13

Δείξτε ότι $19 \mid 2^{2^{6k+2}} + 3$, $k = 0, 1, 2, \ldots$

Λύση

Θα δείξουμε ότι $2^{2^{6k+2}} + 3 \equiv 0 \pmod{19}$ ή ισοδύναμα

$$2^{2^{6k+2}} \equiv -3 \equiv 16 \pmod{19}.$$

Ο 19 είναι πρώτος, και $19 \nmid 2$ άρα από το θεώρημα Fermat

$$2^{18} \equiv 1 \pmod{19}.$$

Μας διευκολύνει να βρούμε το υπόλοιπο της διαίρεσης του αριθμού 2^{6k+2} με τον 18. Παρατηρούμε ότι

$2^6 \equiv 64 \equiv 1 \pmod{9}$ οπότε $2^{6k} \equiv 1 \pmod{9}$ και άρα

$2^{6k} \cdot 2 \equiv 2^2 \pmod{9}$ δηλαδή $9 \mid 2^{6k+2} - 4$.

Αλλά, $\left.\begin{matrix} 9 \mid 2^{6k+2} - 4 \\ 2 \mid 2^{6k+2} - 4 \end{matrix}\right\} \xrightarrow{(2,9)=1} 18 \mid 2^{6k+2} - 4$

δηλαδή

$$2^{6k+2} \equiv 4 \pmod{18} \rightsquigarrow 2^{6k+2} = 18t + 4, \quad t \in \mathbb{Z}$$

Άρα
$$2^{18t} \equiv 1 \pmod{19} \Rightarrow 2^{18t} \cdot 2^4 \equiv 2^4 \pmod{19}$$
δηλαδή
$$2^{18t+4} \equiv 16 \pmod{19} \Rightarrow 2^{2^{6k}+2} \equiv 16 \pmod{19}$$
πράγμα που επιδιωκόσαμε. ∎

14

Αν ο p είναι πρώτος αριθμός της μορφής $4k+3$ τότε
$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1 \pmod{p}$$

Λύση

Ο $\frac{p-1}{2} = \frac{4k+3-1}{2} = 2k+1$ είναι περιττός αριθμός.

Είναι
$$\left(\frac{p-1}{2}\right)! \equiv 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \pmod{p} \qquad (1)$$

Αλλά
$$\left.\begin{aligned} -1 &\equiv p-1 \pmod{p} \\ -2 &\equiv p-2 \pmod{p} \\ &\vdots \\ -\tfrac{p-1}{2} &\equiv \tfrac{p+1}{2} \pmod{p} \end{aligned}\right\} \Rightarrow -\left(1 \cdot 2 \cdots \frac{p-1}{2}\right) \equiv \frac{p+1}{2} \cdots (p-1) \pmod{p}$$
δηλαδή
$$\left(\frac{p-1}{2}\right)! \equiv -\left(\frac{p+1}{2} \cdots (p-1)\right) \pmod{p} \qquad (2)$$

Από τις (1) και (2)
$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -\left(1 \cdot 2 \cdots \frac{p-1}{2} \; \frac{p+1}{2} \cdots (p-1)\right) \pmod{p}$$
$$\equiv -(p-1)! \pmod{p}$$
$$\equiv 1 \pmod{p} \qquad (\text{θεωρ. Wilson}) \; . \; ∎$$

15

Να δείξετε ότι για κάθε φυσικό αριθμό ν
$$7 \mid 3^{2\nu+1} + 2^{\nu+2}$$

Λύση

Θα δείξουμε ότι $3^{2\nu+1} + 2^{\nu+2} \equiv 0 \pmod{7}$

Είναι $3^{2v+1} = 3 \cdot 3^{2v} = 3 \cdot (3^2)^v = 3 \cdot 9^v$ και

$2^{v+2} = 2^2 \cdot 2^v = 4 \cdot 2^v$

Θα δείξουμε δηλαδή ότι $3 \cdot 9^v + 4 \cdot 2^v \equiv 0 \pmod 7$, $\forall v \in \mathbb{N}$.

1ος τρόπος. $9 \equiv 2 \pmod 7 \Rightarrow 9^v \equiv 2^v \pmod 7$ οπότε

$3 \cdot 9^v \equiv 3 \cdot 2^v \pmod 7$

Έτσι

$$\left.\begin{array}{l} 4 \cdot 2^v \equiv 4 \cdot 2^v \pmod 7 \\ 3 \cdot 9^v \equiv 3 \cdot 2^v \pmod 7 \end{array}\right\} \Rightarrow 3 \cdot 9^v + 4 \cdot 2^v \equiv 7 \cdot 2^v \equiv 0 \pmod 7.$$

2ος τρόπος (Με επαγωγή)

Για $v=1$ $\quad 3 \cdot 9 + 4 \cdot 2 = 35 \equiv 0 \pmod 7$ ισχύει.

Υποθέτουμε $\quad 3 \cdot 9^v + 4 \cdot 2^v \equiv 0 \pmod 7 \qquad (1)$

Θα δείξουμε ότι $3 \cdot 9^{v+1} + 4 \cdot 2^{v+1} \equiv 0 \pmod 7$.

Από την (1) έχουμε $\quad 3 \cdot 9^v \equiv -4 \cdot 2^v \pmod 7$

και $\quad 3 \cdot 9^{v+1} \equiv -36 \cdot 2^v \pmod 7 \equiv -18 \cdot 2^{v+1} \pmod 7$

Αλλά $-18 \equiv -4 \pmod 7$ οπότε $-18 \cdot 2^{v+1} \equiv -4 \cdot 2^{v+1} \pmod 7$

Άρα $3 \cdot 9^{v+1} \equiv -4 \cdot 2^{v+1} \pmod 7 \Rightarrow 3 \cdot 9^{v+1} + 4 \cdot 2^{v+1} \equiv 0 \pmod 7$ ∎

16

Να δείξετε ότι

$$7 \mid 2222^{5555} + 5555^{2222}$$

Λύση

Παρατηρούμε ότι $2222 \equiv 3 \pmod 7 \Rightarrow 2222^{5555} \equiv 3^{5555} \pmod 7$

και $5555 \equiv -3 \pmod 7 \Rightarrow 5555^{2222} \equiv 3^{2222} \pmod 7$

Αρκεί να δείξουμε ότι:

$$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 3^{2222} \pmod 7$$
$$\equiv 3^{2222}(3^{3333} + 1) \pmod 7$$

Είναι, $3^{3333} + 1 = 3^{3(1111)} + 1$. Αλλά

$1111 \equiv 1 \pmod 6 \Rightarrow 1111 = 6t + 1$, $t \in \mathbb{Z}$.

και $3^6 \equiv 1 \pmod 7 \Rightarrow 3^{6t} \equiv 1 \pmod 7 \Rightarrow 3^{6t+1} \equiv 3 \pmod 7$

Έτσι $3^{1111} \equiv 3 \pmod 7 \Rightarrow 3^{3(1111)} \equiv 3^3 \pmod 7 \Rightarrow$

$3^{3(1111)}+1 \equiv 3^3+1 \equiv 28 \equiv 0 \pmod 7$. Επομένως

$3^{2222}(3^{3333}+1) \equiv 0 \pmod 7 \Rightarrow 3^{5555}+3^{2222} \equiv 0 \pmod 7$

πρόταση που επιδιωκόμασε. ∎

17

Δείξτε ότι όλοι οι αριθμοί της μορφής
$(2^{2n}+1)^2+2^2$ για $n=28k+1$, $k=1,2,\dots$
είναι σύνθετοι αριθμοί.

Λύση

Από το θεώρημα του Fermat, $2^{28} \equiv 1 \pmod{29}$ οπότε
$2^{2\cdot 28k} \equiv 1 \pmod{29}$, $k=1,2,\dots$.

Άρα
$$2^{2\cdot 28k+2} \equiv 2^2 \pmod{29} \Rightarrow$$
$$2^{2\cdot 28k+2}+1 \equiv 5 \pmod{29} \Rightarrow$$
$$(2^{2n}+1)^2 \equiv 25 \pmod{29} \Rightarrow$$
$$(2^{2n}+1)^2+2^2 \equiv 29 \equiv 0 \pmod{29} \Rightarrow$$
$$29 \mid (2^{2n}+1)^2+2^2, \quad n=28k+1, \quad k=1,2,\dots \quad (*)$$

Αλλά
$$(2^{2n}+1)^2+2^2 > 29 \qquad (**)$$

Από τις σχέσεις (*) και (**) έχουμε το ζητούμενο. ∎

18

Δείξτε ότι το άθροισμα των κύβων τριών διαδοχικών ακεραίων διαιρείται με το 9.

Λύση

Έστω $(a-1), a, a+1$ $, a \in \mathbb{Z}$ τρεις διαδοχικοί ακέραιοι. Είναι $A=(a-1)^3+a^3+(a+1)^3 = 3(a^3+2a)$

Για να δείξω ότι $9|A$ αρκεί να δείξω ότι $3|a^3+2a$.
Αν r είναι το υπόλοιπο της διαίρεσης του a με τον 3, τότε

$$a \equiv r \pmod 3.$$

Έτσι $a^3+2a \equiv r^3+2r \pmod 3$.

α) Αν $r=0$ τότε $a^3+2a \equiv 0 \pmod 3 \Rightarrow 3|a^3+2a$.

β) Αν $r=1$ τότε $a^3+2a = 3 \equiv 0 \pmod 3 \Rightarrow 3|a^3+2a$

γ) Αν $r=2$ τότε $a^3+2a \equiv 12 \equiv 0 \pmod 3 \Rightarrow 3|a^3+2a$. ∎

19

Έστω p ένας πρώτος αριθμός, $a \in \mathbb{N}$ και $p \nmid a$. Αν $k \in \mathbb{N}$ δείξτε ότι

$$a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k}$$

Λύση

Αφού $p \nmid a$ θά είναι $(a,p)=1$. Έτσι $(a,p^k)=1$.
Αν φ είναι η συνάρτηση του Euler θά έχουμε

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

Από το θεώρημα του Euler πάρα παίρνουμε

$$a^{\varphi(p^k)} \equiv 1 \pmod{p^k} \Rightarrow a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k}.$$ ∎

20

Αν ο p είναι πρώτος αριθμός τότε

$$(p-1)! \equiv p-1 \pmod{1+2+\cdots+(p-1)}$$

Λύση

Είναι $1+2+\cdots+(p-1) = \frac{p(p-1)}{2} = a \in \mathbb{N}$

Αρκεί λοιπόν να δείξουμε ότι

$$a \,|\, (p-1)! - (p-1).$$

Από το θεώρημα του Wilson έχουμε

$$(p-1)! \equiv -1 \pmod p \Rightarrow p \,|\, (p-1)! + 1.$$

Αλλά $p \mid p$ επομένως $p \mid (p-1)! + 1 - p$ δηλαδή

$$p \mid (p-1)! - (p-1) \qquad (1)$$

Είναι όμως $\quad p-1 \mid (p-1)! - (p-1) \qquad (2)$

αφού $(p-1)! - (p-1) = (p-1)\left[(p-2)! - 1\right]$.

Από τις (1) και (2) έχουμε εφ' όσον $(p, p-1) = 1$

ότι $\quad p(p-1) \mid (p-1)! - (p-1)$

δηλαδή $\quad (p-1)! - (p-1) = k\, p(p-1) \quad , \quad k \in \mathbb{Z}$

$$= k\, 2\alpha \, .$$

Άρα $\alpha \mid (p-1)! - (p-1)$. ∎

21

Αν ο p είναι περιττός πρώτος αριθμός, τότε

$$2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p .$$

Λύση

Παρατηρούμε ότι

$$\left.\begin{aligned} 2 &\equiv -(p-2) \pmod p \\ 4 &\equiv -(p-4) \pmod p \\ &\vdots \\ p-1 &\equiv -1 \pmod p \end{aligned}\right\} \Rightarrow 2 \cdot 4 \cdots (p-1) \equiv (-1)^{\frac{p-1}{2}} \cdot 1 \cdot 3 \cdots (p-2) \pmod p$$

$$\Rightarrow 2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \pmod p$$

$$\equiv (-1)^{\frac{p-1}{2}} (p-1)! \pmod p$$

Αλλά από το θεώρημα Wilson έχουμε $(p-1)! \equiv -1 \pmod p$

άρα $\quad (-1)^{\frac{p-1}{2}} \cdot (p-1)! \equiv (-1)^{\frac{p+1}{2}} \pmod p$

Έτσι $\quad 2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$. ∎

21

Αν ο p είναι περιττός πρώτος και $m \in \mathbb{N}$ έτσι ώστε $2^m \not\equiv 1 \pmod p$ δείξτε ότι

$$1^m + 2^m + \cdots + (p-1)^m \equiv 0 \pmod p$$

Λύση

Είναι $(2,p)=1$ και το $\{1,2,\ldots,p-1\}$ είναι ένα αναγμένο σύστημα υπολοίπων $(\mathrm{mod}\, p)$. Άρα και το $\{2\cdot 1, 2\cdot 2, \ldots, 2(p-1)\}$ δηλαδή το $\{2,4,6,\ldots,2(p-1)\}$ είναι ένα αναγμένο σύστημα υπολοίπων $(\mathrm{mod}\, p)$. Υπάρχει επομένως μετάθεση $\{k_1,\ldots,k_{p-1}\}$ των $\{1,2,\ldots,p-1\}$ έτσι ώστε

$$\left.\begin{array}{l} 2 \equiv k_1 \pmod p \\ \vdots \\ 2(p-1) \equiv k_{p-1} \pmod p \end{array}\right\} \Rightarrow \left.\begin{array}{l} 2^m \equiv k_1^m \pmod p \\ \vdots \\ [2(p-1)]^m \equiv k_{p-1}^m \pmod p \end{array}\right\} \Rightarrow$$

$$2^m + \cdots + [2(p-1)]^m \equiv k_1^m + \cdots + k_{p-1}^m \pmod p$$

$$\equiv 1^m + 2^m + \cdots + (p-1)^m \pmod p.$$

Άρα $\quad 2^m \sum_{i=1}^{p-1} i^m \equiv \sum_{i=1}^{p-1} i^m \pmod p$

και επομένως $\quad p \mid (2^m - 1) \sum_{i=1}^{p-1} i^m$. Αλλά $p \nmid 2^m - 1$,

άρα $(p, 2^m - 1) = 1$, οπότε

$$p \mid \sum_{i=1}^{p-1} i^m$$

δηλαδή $\quad 1^m + 2^m + \cdots + (p-1)^m \equiv 0 \pmod p$. ∎

ΚΕΦΑΛΑΙΟ VI

Πολυωνυμικές ισοτιμίες.

1. Ισοτιμίες στο δακτύλιο $\mathbb{Z}[x]$ - Ταυτοτικές ισοτιμίες.

Έστω $\mathbb{Z}[x]$ το σύνολο των πολυωνύμων με ακέραιους συντελεστές, δηλαδή των πολυωνύμων της μορφής

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \quad , \quad a_i \in \mathbb{Z} \ , \ n \in \mathbb{N}_0 .$$

Το $\mathbb{Z}[x]$ εφοδιασμένο με τις γνωστές πράξεις αθροίσματος και γινομένου πολυωνύμων δομείται ως γνωστόν σε αντιμεταθετικό δακτύλιο. Στον $\mathbb{Z}[x]$ ισχύει επιπλέον ο νόμος της απλοποίησης δηλαδή,

αν $f(x) \cdot g(x) = f(x) \cdot h(x)$ και $f(x) \neq 0$ τότε $g(x) = h(x)$, επομένως ο δακτύλιος $\mathbb{Z}[x]$ είναι πεδίο ακεραιότητας.

Θα λέμε ότι το μη-μηδενικό πολυώνυμο $h(x) \in \mathbb{Z}[x]$ διαιρεί το πολυώνυμο $f(x) \in \mathbb{Z}[x]$ και θα το συμβολίζουμε, $h(x) \mid f(x)$ αν υπάρχει $g(x) \in \mathbb{Z}[x]$ τέτοιο ώστε $f(x) = h(x) \cdot g(x)$.

Στην περίπτωση που δεν υπάρχει τέτοιο πολυώνυμο $g(x)$, θα λέμε ότι το $h(x)$ δεν διαιρεί το $f(x)$ και θα το συμβολίζουμε $h(x) \nmid f(x)$.

Έστω $h(x)$ τυχόν μη-μηδενικό πολυώνυμο του $\mathbb{Z}[x]$. Δύο πολυώνυμα $f(x), g(x)$ του $\mathbb{Z}[x]$ καλούνται ισότιμα modulo $h(x)$ και γράφουμε

$$f(x) \equiv g(x) \pmod{h(x)}$$

αν και μόνο αν

$$h(x) \mid (f(x) - g(x)) .$$

Αν $h(x) \nmid (f(x)-g(x))$ θα γράφουμε $f(x) \not\equiv g(x) \pmod{h(x)}$ και θα λέμε ότι το $f(x)$ είναι ανισότιμο με το $g(x)$ modulo $h(x)$.

Είναι εύκολο να δούμε ότι η σχέση ισοτιμίας $(\mathrm{mod}\, h(x))$ είναι μια σχέση ισοδυναμίας στο $\mathbb{Z}[x]$.

Ιδιαίτερο ενδιαφέρον παρουσιάζει η περίπτωση όπου το modulo $h(x)$ είναι ένα σταθερό πολυώνυμο m, m φυσικός αριθμός.

Ας δούμε όμως πιο αναλυτικά τι συμβαίνει στην περίπτωση αυτή.

<u>Ορισμός.</u> Δυο πολυώνυμα $f(x), g(x) \in \mathbb{Z}[x]$ θα λέγονται <u>ταυτοτικά ισότιμα</u> $(\mathrm{mod}\, m)$, m φυσικός αριθμός και θα γράφουμε

$$f(x) \equiv g(x) \pmod{m} \text{ : ταυτοτικά}$$

αν και μόνο αν στο $Z[x]$ είναι

$$f(x) \equiv g(x) \pmod{m}.$$

Έτσι,

$f(x) \equiv g(x) \pmod{m}$ ταυτοτικά $\iff m \mid (f(x)-g(x)) \iff$

$f(x)-g(x) = m \cdot r(x)$, $r(x) \in \mathbb{Z}[x]$.

Πρόταση 1.1

Για ακέραια πολυώνυμα

$f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $g(x) = b_0 + b_1 x + \cdots + b_n x^n$

ισχύει

$f(x) \equiv g(x) \pmod{m}$ ταυτοτικά $\iff a_i \equiv b_i \pmod{m}$, $i = 0, 1, \ldots, n$.

Απόδειξη

$f(x) \equiv g(x) \pmod{m}$ ταυτοτικά $\iff$ υπάρχει ακέραιο πολυώνυμο $r(x) = c_0 + c_1 x + \cdots + c_n x^n$ έτσι ώστε

$f(x) - g(x) = m \cdot r(x) \iff$

$$(a_0-b_0) + (a_1-b_1)x + \cdots + (a_n-b_n)x^n = mc_0 + mc_1 x + \cdots + mc_n x^n$$

$\iff a_i - b_i = m c_i \quad , i=0,1,\ldots,n$

$\iff a_i \equiv b_i \pmod m \quad , i=0,1,\ldots,n$. ■

Για παράδειγμα, έχουμε

$16x^4 - 2x^3 - 24x^2 + 4x \equiv -10x^3 - 12x + 8 \pmod 8$ ταυτοτικά

αφού

$16 \equiv 0 \pmod 8$, $-2 \equiv -10 \pmod 8$, $24 \equiv 0 \pmod 8$, $4 \equiv -12 \pmod 8$ και

$0 \equiv 8 \pmod 8$.,

ενώ $16x^4 - 2x^3 + 4x \not\equiv -10x^3 - 10x \pmod 8$ ταυτοτικά

αφού $4 \not\equiv -10 \pmod 8$.

Αν στην πρόταση 1.1 το $g(x)$ είναι το μηδενικό πολυώνυμο τότε έχουμε

Πόρισμα 1.1

Αν $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$, τότε

$f(x) \equiv 0 \pmod m$ ταυτοτικά $\iff a_i \equiv 0 \pmod m$, $i=0,1,\ldots,n$.

Για παράδειγμα, έχουμε

$14x^3 + 21x + 7 \equiv 0 \pmod 7$ ταυτοτικά

αφού $14 \equiv 0 \pmod 7$, $21 \equiv 0 \pmod 7$ και $7 \equiv 0 \pmod 7$

ενώ,

$14x^3 + 25x + 7 \not\equiv 0 \pmod 7$ ταυτοτικά

αφού $25 \not\equiv 0 \pmod 7$.

Είναι φανερό τώρα ότι

$f(x) \equiv g(x) \pmod m$ ταυτοτικά $\iff f(x) - g(x) \equiv 0 \pmod m$ ταυτοτικά.

Παρατήρηση.

Έστω $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ και m φυσικός αριθμός. Αν $\bar{a}_0, \bar{a}_1, \ldots, \bar{a}_n$ είναι οι κλάσεις ισοτιμίας $(\bmod m)$ των ακεραίων $a_0, a_1, \ldots, a_n$ αντίστοιχα, θα συμβολίζουμε

με $\bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_n x^n$

το αντίστοιχο πολυώνυμο με συντελεστές από τον δακτύλιο $\mathbb{Z}_m$.

Αν $f(x), g(x) \in \mathbb{Z}[x]$ τότε για τα πολυώνυμα $\bar{f}(x), \bar{g}(x)$ με συντελεστές από το $\mathbb{Z}_m$ έχουμε

$f(x) \equiv g(x) \pmod m$ ταυτοτικά $\iff \bar{f}(x) = \bar{g}(x)$.

Για παράδειγμα, αν

$f(x) = x^5 + 2x^2 + 1$, $g(x) = 4x^5 + 3x^4 + 9x^3 + 5x^2 + 7$

έχουμε $f(x) \equiv g(x) \pmod 3$.

και για τα αντίστοιχα πολυώνυμα $\bar{f}(x), \bar{g}(x)$ με συντελεστές από το $\mathbb{Z}_3$ έχουμε

$\bar{f}(x) = \bar{1}x^5 + \bar{2}x^2 + \bar{1}$

$\bar{g}(x) = \bar{4}x^5 + \bar{3}x^4 + \bar{9}x^3 + \bar{5}x^2 + \bar{7} = \bar{1}x^5 + \bar{0}x^4 + \bar{0}x^3 + \bar{2}x^2 + \bar{1}$

$= \bar{1}x^5 + \bar{2}x^2 + \bar{1}$

Δηλαδή $\bar{f}(x) = \bar{g}(x)$.

Εύκολα αποδεικνύεται ότι

α) Αν $h(x) = f(x) + g(x)$ τότε $\bar{h}(x) = \bar{f}(x) + \bar{g}(x)$

β) Αν $h(x) = f(x) \cdot g(x)$ τότε $\bar{h}(x) = \bar{f}(x) \cdot \bar{g}(x)$. ■

Θα τονίσουμε εδώ ότι η σχέση της ταυτοτικής ισοτιμίας $(\bmod m)$ είναι φανερά μια **σχέση ισοδυναμίας** στο σύνολο $\mathbb{Z}[x]$, επομένως για πολυώνυμα $f(x), g(x), h(x) \in \mathbb{Z}[x]$ ισχύουν

1) $f(x) \equiv f(x) \pmod m$ ταυτοτικά

2) Αν $f(x) \equiv g(x) \pmod m$ ταυτοτικά τότε και $g(x) \equiv f(x) \pmod m$ ταυτοτικά.

3) Αν $f(x) \equiv g(x) \pmod m$ ταυτοτικά και
$g(x) \equiv h(x) \pmod m$ ταυτοτικά. τότε και
$f(x) \equiv h(x) \pmod m$ ταυτοτικά.

Επιπλέον αν.
$f(x) \equiv f_1(x) \pmod m$ ταυτοτικά και $g(x) \equiv g_1(x) \pmod m$ ταυτοτικά τότε

4) $f(x) \pm g(x) \equiv f_1(x) \pm g_1(x) \pmod m$ ταυτοτικά

5) $f(x) \cdot g(x) \equiv f_1(x) \cdot g_1(x) \pmod m$ ταυτοτικά.

Άρα, αν $f(x) \equiv f_1(x) \pmod m$ ταυτοτικά, τότε για κάθε $h(x) \in \mathbb{Z}[x]$ έχουμε

6) $f(x) \pm h(x) \equiv f_1(x) \pm h(x) \pmod m$ ταυτοτικά

7) $f(x) \cdot h(x) \equiv f_1(x) \cdot h(x) \pmod m$ ταυτοτικά,

αφού $h(x) \equiv h(x) \pmod m$ ταυτοτικά.

Πρόταση 1.2

Ας είναι p πρώτος αριθμός και $f(x), g(x) \in \mathbb{Z}[x]$.
Αν $f(x) \cdot g(x) \equiv 0 \pmod p$ ταυτοτικά
και $f(x) \not\equiv 0 \pmod p$ ταυτοτικά
τότε $g(x) \equiv 0 \pmod p$ ταυτοτικά.

Απόδειξη.
Αφού $f(x) \not\equiv 0 \pmod p$ ταυτοτικά ένας τουλάχιστον από τους συντελεστές του $f(x)$ δεν διαιρείται από τον p. Αν από το $f(x)$ διαγράψουμε όλους τους όρους που οι συντελεστές του διαιρούνται από τον p, παίρνουμε ένα μη-μηδενικό πολυώνυμο $f_1(x)$ τέτοιο ώστε

$$f(x) \equiv f_1(x) \pmod p \text{ ταυτοτικά.}$$

Υποθέτουμε ότι $g(x) \not\equiv 0 \pmod p$ ταυτοτικά.
Με τον ίδιο τρόπο όπως και για το $f(x)$, θα έχουμε

$$g(x) \equiv g_1(x) \pmod p \text{ ταυτοτικά,}$$

όπου το $g_1(x)$ είναι μη-μηδενικό πολυώνυμο που οι συντελεστές του δεν διαιρούνται από τον p. Επομένως

$$f(x)\cdot g(x) \equiv f_1(x)\cdot g_1(x) \pmod p \text{ ταυτοτικά}$$

και από την υποθεσή μας θα είναι

$$f_1(x)\cdot g_1(x) \equiv 0 \pmod p \text{ ταυτοτικά}.$$

Αν λοιπόν a και b είναι οι συντελεστές των μεγιστοβαθμίων όρων του $f_1(x)$ και $g_1(x)$ αντίστοιχα τότε $p \mid a\cdot b$. Αλλά $p \nmid a$ και $p \nmid b$, οπότε $p \nmid ab$, πράγμα άτοπο. Άρα $g(x) \equiv 0 \pmod p$ ταυτοτικά. ■

Από την προηγούμενη πρόταση συμπεραίνουμε ότι:
Αν $f(x) \not\equiv 0 \pmod p$ ταυτοτικά και $g(x) \not\equiv 0 \pmod p$ ταυτοτικά τότε και

$$f(x)\cdot g(x) \not\equiv 0 \pmod p.$$

Ορισμός

Ένα πολυώνυμο $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $n \geq 1$ με ακέραιους συντελεστές ονομάζεται πρωταρχικό, αν

$$(a_0, a_1, \ldots, a_n) = 1.$$

Πόρισμα 1.2

Το γινόμενο δυο πρωταρχικών πολυωνύμων είναι πρωταρχικό πολυώνυμο.

Απόδειξη.

Έστω $f(x), g(x)$ δυο πρωταρχικά πολυώνυμα. Υποθέτουμε ότι το $f(x)\cdot g(x)$ δεν είναι πρωταρχικό πολυώνυμο. Αν d είναι ο Μ.Κ.Δ των συντελεστών του $f(x)\cdot g(x)$, θα είναι $d \neq 1$ οπότε υπάρχει πρώτος p με $p \mid d$. Άρα ο p διαιρεί όλους τους συντελεστές του $f(x)\cdot g(x)$, άρα

$$f(x)\cdot g(x) \equiv 0 \pmod p \text{ ταυτοτικά}.$$

Επειδή όμως τα $f(x), g(x)$ είναι πρωταρχικά πολυώνυμα θα είναι $f(x) \not\equiv 0 \pmod p$ ταυτοτικά
και $g(x) \not\equiv 0 \pmod p$ ταυτοτικά.

Άρα $f(x)\cdot g(x) \not\equiv 0 \pmod p$ ταυτοτικά
πράγμα άτοπο. Άρα το $f(x)g(x)$ είναι πρωταρχικό πολυώνυμο. ■

Πρόταση 1.3

Αν είναι $f(x), g(x) \in \mathbb{Z}[x]$ και $m \in \mathbb{N}$.

i) Αν $f(x) \equiv g(x) \pmod m$ ταυτοτικά, τότε $\forall u \in \mathbb{Z}$ ισχύει
$$f(u) \equiv g(u) \pmod m.$$

ii) Αν $f(x) \equiv 0 \pmod m$ ταυτοτικά, τότε $\forall u \in \mathbb{Z}$ ισχύει
$$f(u) \equiv 0 \pmod m.$$

Απόδειξη.

i) $f(x) \equiv g(x) \pmod m$ ταυτοτικά $\iff$ υπάρχει $h(x) \in \mathbb{Z}[x]$ τέτοιο ώστε $f(x) - g(x) = m \cdot h(x)$.

Για κάθε ακέραιο u, στο $\mathbb{Z}$ έχουμε
$$f(u) - g(u) = m \cdot h(u)$$
δηλαδή
$$f(u) \equiv g(u) \pmod m.$$

ii) Αν στο i) το $g(x)$ είναι το μηδενικό πολυώνυμο τότε, αν $f(x) \equiv 0 \pmod m$ ταυτοτικά, θα είναι
$$f(u) \equiv 0 \pmod m. \quad ■$$

Το αντίστροφο της παραπάνω πρότασης δεν ισχύει γενικά. Για παράδειγμα,

i') Έστω p πρώτος αριθμός και $f(x)=x^p$, $g(x)=x$.
Για κάθε ακέραιο u, έχουμε από το θεώρημα Fermat
$u^p \equiv u \pmod p$ δηλαδή $f(u) \equiv g(u) \pmod p$.
Αλλά, $x^p \not\equiv x \pmod p$ ταυτοτικά
αφού $p \neq 1$, άρα $f(x) \not\equiv g(x) \pmod p$ ταυτοτικά.

ii') Αν p πρώτος και $f(x)=x^p-x$, τότε $\forall u \in \mathbb{Z}$ έχουμε
$f(u)=u^p-u \equiv 0 \pmod p$ από θεώρημα Fermat.
ενώ $f(x)=x^p-x \not\equiv 0 \pmod p$ ταυτοτικά, αφού $p \neq 1$.
Το δεδομένο λοιπόν
$f(x) \equiv g(x) \pmod m$ ταυτοτικά
μας δίνει περισσότερες πληροφορίες από το δεδομένο.
$f(u) \equiv g(u) \pmod m$, $\forall u \in \mathbb{Z}$.

<u>Ορισμός</u>
Αν για τα πολυώνυμα $f(x), g(x), h(x)$ του $\mathbb{Z}[x]$ έχουμε
$f(x) \equiv g(x)h(x) \pmod m$ ταυτοτικά
τότε θα λέμε ότι,
Το $f(x)$ είναι ένα πολλαπλάσιο του $g(x)$ modulo m
ή
Το $g(x)$ είναι ένας διαιρέτης του $f(x)$ modulo m
ή
Το $f(x)$ διαιρείται από το $g(x)$ modulo m.

2. Πολυωνυμικές ισοτιμίες.

Έστω $f(x)=a_0+a_1x+\cdots+a_nx^n$ ένα πολυώνυμο με ακέραιους συντελεστές και m φυσικός αριθμός.

Μια "ισοτιμία" της μορφής

$$f(x)\equiv 0 \pmod m \qquad (I)$$

όπου x είναι ένας προσδιοριστέος ακέραιος, καλείται **πολυωνυμική ισοτιμία (mod m)**

Προσοχή, η (I) <u>δεν είναι</u> η ταυτοτική ισοτιμία

$$f(x)\equiv 0 \pmod m \text{ ταυτοσικά}$$

στο $\mathbb{Z}[x]$ που είδαμε στα προηγούμενα, αλλά <u>είναι</u> μια υποψήφια ισοτιμία στον δακτύλιο $\mathbb{Z}$, δηλαδή αναζητούνται οι ακέραιες τιμές του x που ικανοποιούν τα μέλη της (I) αριθμούς ισότιμους (mod m).

Οι γραμμικές ισοτιμίες είναι μια ειδική περίπτωση πολυωνυμικών ισοτιμιών.

Όπως και στις γραμμικές ισοτιμίες, ο ακέραιος x_0 **επαληθεύει** ή **πληρεί** την (I) αν

$$f(x_0)=a_0+a_1x_0+\cdots+a_nx_0^n\equiv 0 \pmod m.$$

Τώρα, για κάθε ακέραιο x_1 με $x_1\equiv x_0 \pmod m$ θα είναι

$$f(x_1)\equiv f(x_0) \pmod m \qquad \text{(κεφ IV. θεωρ 1.3)}$$

οπότε και

$$f(x_1)\equiv 0 \pmod m$$

δηλαδή και ο x_1 επαληθεύει την (I).

Θα καλούμε **λύση** της πολυωνυμικής ισοτιμίας (I) κάθε ακέραιο x_0 που την επαληθεύει μαζί με όλους τους ισότιμους με τον x_0 ακεραίους (mod m). Θα λέμε τότε ότι η (I) έχει μία λύση την $x\equiv x_0 \pmod m$ ή την $x_0 \pmod m$.

Δυο λύσεις, $x_1 \pmod m$ και $x_2 \pmod m$ της (I) θα είναι διαφορετικές αν είναι ανισότιμες $\pmod m$, δηλαδή αν

$$x_1 \not\equiv x_2 \pmod m .$$

Όταν μιλάμε για το πλήθος των λύσεων της πολυωνυμικής ισοτιμίας (I) εννοούμε το πλήθος των ανισότιμων $\pmod m$ ανά δύο λύσεων της, δηλαδή το πλήθος των ακεραίων που επαληθεύουν την (I) και ανήκουν στο σύνολο

$$\{0, 1, 2, \dots, m-1\}$$

ή σε οποιοδήποτε άλλο πλήρες σύστημα υπολοίπων $\pmod m$.

Επομένως, κάθε πολυωνυμική ισοτιμία (I) ή δεν έχει λύση ή έχει το πολύ m διαφορετικές λύσεις.

Παρατήρηση

Θεωρούμε την πολυωνυμική ισοτιμία (I) και το αντίστοιχο πολυώνυμο

$$\bar f(x) = \bar a_0 + \bar a_1 x + \dots + \bar a_n x^n$$

του δακτύλιου $\mathbb{Z}_m[x]$ των πολυωνύμων με συντελεστές από το $\mathbb{Z}_m$.

Τότε για ακέραιο u έχουμε

$$f(u) \equiv 0 \pmod m \iff \overline{f(u)} = \bar f(\bar u) = \bar 0 .$$

Δηλαδή, η κλάση $\bar u$ είναι λύση της (I) αν και μόνο αν η κλάση $\bar u$ είναι λύση της εξίσωσης

$$\bar f(x) = \bar 0$$

στον δακτύλιο $\mathbb{Z}_m[x]$.

Πραγματικά, $f(u) = a_0 + a_1 u + \dots + a_n u^n \equiv 0 \pmod m \iff$

$$\overline{f(u)} = \overline{a_0 + a_1 u + \dots + a_n u^n} = \bar a_0 + \bar a_1 \bar u + \dots + \bar a_n \bar u^n =$$

$$= \bar f(\bar u) = \bar 0 .$$

Το πρόβλημα λοιπόν της εύρεσης των λύσεων μιας πολυωνυμικής ισοτιμίας ανάγεται σε πρόβλημα εύρεσης των λύσεων μιας εξίσωσης στον δακτύλιο $\mathbb{Z}_m[x]$.

Μπορούμε λοιπόν να επιλύσουμε την (I) με **δοκιμή**, δηλαδή να δοκιμάσουμε τους ακεραίους απο ένα πλήρες σύστημα υπολοίπων (mod m) και να βρούμε εκείνους που την επαληθεύουν. Ας το δούμε αυτο στα επόμενα παραδείγματα.

Παράδειγμα 2.1

Θα επιλύσουμε με δοκιμή την πολυωνυμική ισοτιμία

$$f(x) = x^2 - 3x + 2 \equiv 0 \pmod 6.$$

Θεωρούμε ένα πλήρες σύστημα υπολοίπων (mod 6) για παράδειγμα το $\{0, \pm 1, \pm 2, 3\}$ και δοκιμάζουμε καθένα απο τους ακεραίους αυτού στην πολυωνυμική ισοτιμία. Έχουμε,

για $x=0$, $f(0) = 2 \not\equiv 0 \pmod 6$,
για $x=1$, $f(1) = 0 \equiv 0 \pmod 6$,
για $x=-1$, $f(-1) = 6 \equiv 0 \pmod 6$,
για $x=2$, $f(2) = 0 \equiv 0 \pmod 6$,
για $x=-2$, $f(-2) = 12 \equiv 0 \pmod 6$,
για $x=3$, $f(3) = 2 \not\equiv 0 \pmod 6$.

Έχει αυτή λοιπόν 4 λύσεις, τις

$x \equiv 1 \pmod 6$, $x \equiv -1 \pmod 6$, $x \equiv 2 \pmod 6$, $x \equiv -2 \pmod 6$.

Παράδειγμα 2.2

Θα επιλύσουμε με δοκιμή την πολυωνυμική ισοτιμία

$$x^2 + 2 \equiv 0 \pmod 5.$$

Θεωρούμε το πλήρες σύστημα υπολοίπων (mod 5) $\{0,1,2,3,4\}$ και με δοκιμή έχουμε

$$0^2 + 2 \not\equiv 0 \pmod 5$$
$$1^2 + 2 \not\equiv 0 \pmod 5$$
$$2^2 + 2 \not\equiv 0 \pmod 5$$
$$3^2 + 2 \not\equiv 0 \pmod 5$$
$$4^2 + 2 \not\equiv 0 \pmod 5$$

Άρα η πολυωνυμική ισοτιμία δεν έχει λύση.

Θα παρατηρήσουμε εδώ ότι, αν
$$f(x)\equiv 0 \pmod m \text{ ταυτοτικά},$$
ή γενικότερα, αν
$$f(u)\equiv 0 \pmod m \quad , \forall u\in\mathbb{Z},$$
τότε η πολυωνυμική ισοτιμία
$$f(x)\equiv 0 \pmod m$$
έχει ακριβώς m διαφορετικές λύσεις.

Πραγματικά, και στις δυο περιπτώσεις $\forall u\in\mathbb{Z}$ ισχύει (Προτ. 1.3)
$$f(u)\equiv 0 \pmod m.$$
Άρα όλοι οι ακέραιοι από το πλήρες σύστημα υπολοίπων $(\bmod m)$ $\{0,1,2,\ldots,m-1\}$ την επαληθεύουν, άρα έχει m ακριβώς λύσεις τις
$$x\equiv 0 \pmod m,\ x\equiv 1 \pmod m,\ \ldots,\ x\equiv m-1 \pmod m.$$
Θα το δούμε αυτό στα επόμενα δύο παραδείγματα.

Παράδειγμα 2.3

Η πολυωνυμική ισοτιμία $f(x)=16x^3+32x^2+8x+16\equiv 0 \pmod 8$ έχει ακριβώς 8 λύσεις τις
$$x\equiv 0 \pmod 8,\ x\equiv 1 \pmod 8,\ \ldots,\ x\equiv 7 \pmod 8.$$
Πραγματικά, αφού $16\equiv 0 \pmod 8$, $32\equiv 0 \pmod 8$, $8\equiv 8 \pmod 8$ και $16\equiv 0 \pmod 8$ θα είναι
$$f(x)\equiv 0 \pmod 8 \text{ ταυτοτικά}.$$
Άρα,
$$f(u)\equiv 0 \pmod 8,\ \forall u\in\mathbb{Z}.$$

Παράδειγμα 2.4

Θεωρούμε την πολυωνυμική ισοτιμία $f(x)=x^p-x\equiv 0 \pmod p$ όπου p πρώτος αριθμός.

Από το θεώρημα του Fermat έχουμε ότι
$$f(u)=u^p-u\equiv 0 \pmod p \qquad \forall u\in\mathbb{Z}.$$
Άρα αυτή έχει p ακριβώς λύσεις τις
$$x\equiv 0 \pmod p,\ x\equiv 1 \pmod p,\ \ldots,\ x\equiv p-1 \pmod p.$$

Η μέθοδος εύρεσης των λύσεων της (I) με δοκιμή γίνεται

αριθμητά επίπονος όταν το (modulo) m και ο βαθμός του πολυωνύμου η είναι αρκετά μεγάλοι αριθμοί. Γενικά, δεν υπάρχει μια απλή μέθοδος για την επίλυση πολυωνυμικών ισοτιμιών όπως στην περίπτωση των γραμμικών ισοτιμιών.

Στα επόμενα θα δούμε ορισμένα αποτελέσματα που απλουστεύουν την διαδικασία επίλυσης πολυωνυμικών ισοτιμιών.

Ορισμός.

Ονομάζουμε **βαθμό** της πολυωνυμικής ισοτιμίας

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \equiv 0 \pmod m$$

τον μεγαλύτερο θετικό ακέραιο k για τον οποίο

$$a_k \not\equiv 0 \pmod m.$$

Ειδικά, αν $a_n \not\equiv 0 \pmod m$ τότε η πολυωνυμική ισοτιμία έχει βαθμό n.

Αν η πολυωνυμική ισοτιμία έχει βαθμό $k < n$ τότε

$$a_k \not\equiv 0 \pmod m \quad \text{και} \quad a_{k+1} \equiv \cdots \equiv a_n \equiv 0 \pmod m.$$

Ο παραπάνω ορισμός έχει νόημα για όλα τα πολυώνυμα με ακέραιους συντελεστές πού ένας τουλάχιστον από τους συντελεστές του είναι $\not\equiv 0 \pmod m$.

Αν, $a_i \equiv 0 \pmod m$, $i = 0, 1, \ldots, n$

δηλαδή αν $f(x) \equiv 0 \pmod m$ ταυτοσικά

τότε η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod m$ **δεν** έχει βαθμό.

Ορισμός

Αν είναι $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ και m φυσικός αριθμός. Ονομάζουμε **βαθμό (mod m) του $f(x)$** τον βαθμό της πολυωνυμικής ισοτιμίας

$$f(x) \equiv 0 \pmod m.$$

Έτσι για τις παραπάτω πολυωνυμικές ισοτιμίες έχουμε,

i) $7+6x+9x^2+30x^3 \equiv 0 \pmod 3$ έχει βαθμό 0

ii) $8+5x+10x^2+20x^5 \equiv 0 \pmod 2$ » 1

iii) $7+6x+9x^2+30x^3 \equiv 0 \pmod 5$ » 2

iv) $1+3x^2+6x^3+10x^7 \equiv 0 \pmod 5$ » 3

v) $6+18x+36x^2+19x^8+24x^{15} \equiv 0 \pmod 6$ δεν έχει βαθμό.

Ο βαθμός μιας πολυωνυμικής ισοτιμίας $f(x) \equiv 0 \pmod m$ ή το ίδιο ο βαθμός $(\mathrm{mod}\, m)$ του $f(x)$ εξαρτάται απο το modulo και δεν έχει την ίδια έννοια με το γνωστό βαθμό του πολυωνύμου $f(x)$.

Για παράδειγμα, αν $f(x) = 30x^4 - 60x^3 + 12x^2 - 6x + 3$, τότε η πολυωνυμική ισοτιμία

$f(x) \equiv 0 \pmod 3$ δεν έχει βαθμό

» $f(x) \equiv 0 \pmod 6$ έχει βαθμό 0

» $f(x) \equiv 0 \pmod 5$ έχει βαθμό 2

» $f(x) \equiv 0 \pmod 7$ έχει βαθμό 4

» $f(x) \equiv 0 \pmod{12}$ έχει βαθμό 4,

ένω το πολυώνυμο $f(x)$ είναι 4ου βαθμού.

Αν η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod m$ δεν έχει βαθμό, δηλαδή αν $f(x) \equiv 0 \pmod m$ ταυτοτικά τότε όπως είδαμε έχει αυτή ακριβώς m λύσεις.

Το ενδιαφέρον μας στρέφεται λοιπόν σε πολυωνυμικές ισοτιμίες $f(x) \equiv 0 \pmod m$ που έχουν βαθμό, όταν δηλαδή ισχύει $f(x) \not\equiv 0 \pmod m$ ταυτοτικά.

<u>Παρατήρηση.</u>

Ο βαθμός μιας πολυωνυμικής ισοτιμίας

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \equiv 0 \pmod m \quad (I)$$

ή το ίδιο ο βαθμός $(\mathrm{mod}\, m)$ του πολυωνύμου $f(x)$ δεν είναι παρά ο βαθμός του πολυωνύμου $\bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_n x^n$

στον δακτύλιο $\mathbb{Z}_m[x]$.

Πραγματικά αν η (I) έχει βαθμό $k \leq n$ τότε $a_k \not\equiv 0 \pmod m$ και $a_{k+1} \equiv \dots \equiv a_n \equiv 0 \pmod m$, οπότε $\bar{a}_k \neq \bar{0}$ και $\bar{a}_{k+1} = \dots = \bar{a}_n = \bar{0}$. Επομένως

$$\bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \dots + \bar{a}_k x^k + \bar{a}_{k+1} x^{k+1} + \dots + \bar{a}_n x^n =$$

$$= \bar{a}_0 + \bar{a}_1 x + \dots + \bar{a}_k x^k, \quad \text{με } \bar{a}_k \neq \bar{0}$$

δηλαδή το $\bar{f}(x)$ έχει βαθμό k.

Αν η (I) δεν έχει βαθμό, όταν δηλαδή $a_0 \equiv \dots \equiv a_n \equiv 0 \pmod m$, τότε $\bar{a}_0 = \dots = \bar{a}_n = \bar{0}$ και επομένως $\bar{f}(x) = \bar{0}$ είναι δηλαδή το $\bar{f}(x)$ το μηδενικό πολυώνυμο που δεν έχει βαθμό. ■

Ορισμός

Θα λέμε ότι οι πολυωνυμικές ισοτιμίες

$$f(x) \equiv 0 \pmod m \quad \text{και} \quad g(x) \equiv 0 \pmod m$$

είναι **ισοδύναμες**, όταν επαληθεύονται από τις ίδιες ακέραιες τιμές του x, δηλαδή αν για ακέραιο u ισχύει

$$f(u) \equiv 0 \pmod m \iff g(u) \equiv 0 \pmod m.$$

Η διαφορετικά, είναι ισοδύναμες αν και μόνο αν έχουν τις ίδιες λύσεις (mod m).

Πρόταση 2.1

Αν $f(x) \equiv g(x) \pmod m$ ταυτοσικά

τότε οι πολυωνυμικές ισοτιμίες

i) $f(x) \equiv 0 \pmod m$ και ii) $g(x) \equiv 0 \pmod m$

είναι ισοδύναμες.

Απόδειξη.

Για καθεαυτό u έχουμε: $f(u) \equiv g(u) \pmod m$.

σύμφωνα με την πρόταση 1.3 και την υποθεσή μας
Αν λοιπόν η κλάση $a \pmod m$ είναι λύση της i) δηλαδή $f(a) \equiv 0 \pmod m$ τότε θα είναι και $g(a) \equiv 0 \pmod m$, δηλαδή η κλάση $a \pmod m$ είναι λύση και της ii). Όμοια εργαζόμαστε και για το αντίστροφο. ■

Το αντίστροφο της παραπάνω πρότασης **δεν ισχύει.** Για παράδειγμα, οι πολυωνυμικές ισοτιμίες

$$2x+3 \equiv 0 \pmod 5 \quad \text{και} \quad 4x+1 \equiv 0 \pmod 5$$

είναι ισοδύναμες, έχουν σαν λύση μόνο την $x \equiv 1 \pmod 5$ αλλά $2x+3 \not\equiv 4x+1 \pmod 5$ ταυτοτικά.

Η πρόταση 2.1 ισχύει και γενικώτερα.

Πρόταση 2.2

Αν για τα πολυώνυμα $f(x), g(x)$ με ακέραιους συντελεστές ισχύει

$$f(u) \equiv g(u) \pmod m \text{, για κάθε ακέραιο } u$$

τότε οι πολυωνυμικές ισοτιμίες

$$f(x) \equiv 0 \pmod m \quad \text{και} \quad g(x) \equiv 0 \pmod m$$

είναι ισοδύναμες. ■

Για να <u>απλοποιήσουμε</u> λοιπόν την επίλυση μιας πολυωνυμικής ισοτιμίας $f(x) \equiv 0 \pmod m$, συνήθως βρίσκουμε πολυώνυμο $g(x)$ απλούστερης μορφής απο αυτής του $f(x)$ και τέτοιο ώστε

$$f(x) \equiv g(x) \pmod m \text{ ταυτοτικά}$$

ή γενικώτερα

$$f(u) \equiv g(u) \pmod m \text{ για κάθε ακέραιο } u,$$

και επιλύουμε την απλούστερη αλλά ισοδύναμη πολυωνυμική ισοτιμία $g(x) \equiv 0 \pmod m$.

Έτσι έχουμε.

Πόρισμα 2.1

Κάθε πολυωνυμική ισοτιμία βαθμού $r<n$

$$f(x)=a_0+a_1x+\cdots+a_nx^n\equiv 0\ (\mathrm{mod}\, m)$$

είναι ισοδύναμη με την πολυωνυμική ισοτιμία βαθμού r

$$g(x)=a_0+a_1x+\cdots+a_rx^r\equiv 0\ (\mathrm{mod}\, m).$$

Απόδειξη.

Αφού ο βαθμός της είναι $r<n$ θα είναι

$$a_r\not\equiv 0\ (\mathrm{mod}\, m) \text{ και } a_{r+1}\equiv\cdots\equiv a_n\equiv 0\ (\mathrm{mod}\, m)$$

Έχουμε επόμενως την ταυτοτική ισοτιμία

$$f(x)\equiv g(x)\ (\mathrm{mod}\, m) \text{ ταυτοτικά,}$$

και σύμφωνα με την Πρόταση 2.1, οι πολυωνυμικές ισοτιμίες $f(x)\equiv 0\ (\mathrm{mod}\, m)$ και $g(x)\equiv 0\ (\mathrm{mod}\, m)$ είναι ισοδύναμες. ■

Για παράδειγμα η πολυωνυμική ισοτιμία

$$f(x)=7+12x+8x^2+13x^3+12x^4+24x^5\equiv 0\ (\mathrm{mod}\, 6)$$

έχει βαθμό 3 και είναι ισοδύναμη με την

$$g(x)=7+12x+8x^2+13x^3\equiv 0\ (\mathrm{mod}\, 6).$$

Όμοια μπορούμε να δείξουμε ότι.

Πόρισμα 2.2

Κάθε πολυωνυμική ισοτιμία $f(x)\equiv 0\ (\mathrm{mod}\, m)$ βαθμού r είναι ισοδύναμη με την πολυωνυμική ισοτιμία $g(x)\equiv 0\ (\mathrm{mod}\, m)$ βαθμού r. όπου $g(x)$ είναι το πολυώνυμο που προκύπτει από το $f(x)$ αν διαγράψουμε όλους τους όρους του $f(x)$ που οι

συντελεστές τους διαιρούνται απο τον m - όλοι οι συντελεστές του $g(x)$ είναι $\not\equiv 0 \pmod m$. ■

Για παράδειγμα, η πολυωνυμική ισοτιμία

$$f(x) = 5+8x+12x^2+16x^3+11x^4+32x^5 \equiv 0 \pmod 8$$

είναι ισοδύναμη με την

$$g(x) = 5+12x^2+11x^4 \equiv 0 \pmod 8.$$

Άμεση συνέπεια του Πορίσματος 2.2 και της παρατήρησης ότι, άν $a \not\equiv 0 \pmod m$ τότε $a = km + r$ όπου $1 \le r \le m-1$, δηλαδή $a \equiv r \pmod m$ με $1 \le r \le m-1$, είναι το παρακάτω πόρισμα.

Πόρισμα 2.3

Κάθε πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod m$ βαθμού r είναι ισοδύναμη με μια πολυωνυμική ισοτιμία $g(x) \equiv 0 \pmod m$ βαθμού r, όπου οι συντελεστές του πολυωνύμου $g(x)$ είναι $\geqslant 1$ και $\leq m-1$. ■

Για παράδειγμα, η πολυωνυμική ισοτιμία

$$f(x) = 5+9x+11x^2+17x^3+21x^4 \equiv 0 \pmod 8$$

είναι ισοδύναμη με την

$$g(x) = 5+x+3x^2+x^3+5x^4 \equiv 0 \pmod 8$$

αφού $9 \equiv 1 \pmod 8$, $11 \equiv 3 \pmod 8$, $17 \equiv 1 \pmod 8$ και $21 \equiv 5 \pmod 8$.

Πόρισμα 2.4

Η πολυωνυμική ισοτιμία βαθμού n

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod p$$

όπου $a_n \not\equiv 0 \pmod p$, p πρώτος, είναι ισοδύναμη με την πολυωνυμική ισοτιμία βαθμού n

$$g(x) = x^n + b(a_{n-1}x^{n-1} + \cdots + a_0) \equiv 0 \pmod p$$

όπου $b \pmod p$ η μοναδική λύση της γραμμικής ισοτιμίας

$$a_n x \equiv 1 \pmod p.$$

Απόδειξη.

Αφού $a_n \not\equiv 0 \pmod p$ θα είναι $(a_n, p) = 1$ και επομένως η γραμμική ισοτιμία $a_n x \equiv 1 \pmod p$ έχει μοναδική λύση έστω την $x \equiv b \pmod p$. Τότε $a_n b \equiv 1 \pmod p$ και όμοια $(b, p) = 1$.

Έχουμε τώρα

$$b \cdot f(x) = b a_n x^n + \cdots + b a_0 \equiv$$

$$\equiv x^n + b(a_{n-1}x^{n-1} + \cdots + a_0) \pmod p \quad \text{ταυτοσικά}$$

Συμβολίζουμε με $g(x) = x^n + b(a_{n-1}x^{n-1} + \cdots + a_0)$, οπότε

$$b f(x) \equiv g(x) \pmod p \quad \text{ταυτοσικά}.$$

Άρα, για κάθε ακέραιο u ισχύει

$$b f(u) \equiv g(u) \pmod p \qquad (*)$$

Θα δείξουμε τώρα ότι οι πολυωνυμικές ισοτιμίες

$$f(x) \equiv 0 \pmod p \quad \text{και} \quad g(x) \equiv 0 \pmod p$$

είναι ισοδύναμες.

Αν ο ακέραιος u επαληθεύει την $f(x) \equiv 0 \pmod p$ δηλαδή $f(u) \equiv 0 \pmod p$ τότε και $b f(u) \equiv 0 \pmod p$ οπότε από την σχέση $(*)$ έχουμε $g(u) \equiv 0 \pmod p$. Άρα ο u επαληθεύει και την $g(x) \equiv 0 \pmod p$.

Αντίστροφα, αν $g(u) \equiv 0 \pmod p$ τότε από την σχέση $(*)$ είναι $b f(u) \equiv 0 \pmod p$, και επειδή $p \nmid b$ θα είναι $f(u) \equiv 0 \pmod p$ πράγμα που επιδιώξαμε. ∎

Σχόλια. Είδαμε ότι η επίλυση μιας πολυωνυμικής ισοτιμίας $f(x) \equiv 0 \pmod m$ ανάγεται στην επίλυση της εξίσωσης $\overline{f}(x) = \overline{0}$ στον δακτύλιο $\mathbb{Z}_m[x]$. Ατυχώς όμως, όταν ο m είναι σύνθετος, ο δακτύλιος $\mathbb{Z}_m[x]$ δεν είναι πεδίο ακεραιότητας, αφού έχει διαιρέτες του μηδενός. Για παράδειγμα αν $m=6$ τότε τα μη-μηδενικά πολυώνυμα $\overline{2}x+\overline{2}$ και $\overline{3}x$ έχουν γινόμενο το μηδενικό πολυώνυμο

$$(\overline{2}x+\overline{2})\cdot\overline{3}x = \overline{6}x^2+\overline{6}x = \overline{0}.$$

Έτσι πολλά από τα γνωστά αποτελέσματα, για αλγεβρικές εξισώσεις στο πεδίο ακεραιότητας $F[x]$, όπου F σώμα, δεν ισχύουν στο δακτύλιο $\mathbb{Z}_m[x]$, m σύνθετος. Για παράδειγμα δεν υπάρχει σχέση μεταξύ του πλήθους των ριζών και του βαθμού πολυωνύμου, π.χ το μη-μηδενικό πολυώνυμο $x^2-\overline{3}x+\overline{2}$ στο $\mathbb{Z}_6[x]$ βαθμού 2 έχει 4-διαφορετικές ρίζες, τις $x=\overline{1}$, $x=\overline{2}$, $x=\overline{3}$, $x=\overline{5}$. (βλέπε Παραδ. 2.1) δηλαδή έχει περισσότερες ρίζες από τον βαθμό του.

Όταν όμως το modulo είναι πρώτος αριθμός p, τότε το $\mathbb{Z}_p$ είναι σώμα και το $\mathbb{Z}_p[x]$ πεδίο ακεραιότητας. Όλα τα γνωστά αποτελέσματα από την θεωρία πολυωνύμων στο $F[x]$ ισχύουν εδώ όπου $F=\mathbb{Z}_p$ και μέσω αυτών μπορούμε να πάρουμε αντίστοιχα αποτελέσματα για πολυωνυμικές ισοτιμίες $(\mathrm{mod}\, p)$. Δεν είναι στους σκοπούς μας κάτι τέτοιο, απλά στην επόμενη παράγραφο θα παρουσιασθούν απ'ευθείας οριζόμενα αποτελέσματα που αφορούν πολυωνυμικές ισοτιμίες $(\mathrm{mod}\, p)$, p πρώτος, και με παρατηρήσεις θα μεταφέρουμε στο $\mathbb{Z}_p[x]$ τα αντίστοιχα αποτελέσματα. ■

Βασικός μας στόχος είναι η επίλυση της πολυωνυμικής ισοτιμίας $f(x) \equiv 0 \pmod m$, όταν ο m είναι σύνθετος αριθμός.

3. Πολυωνυμικές ισοτιμίες με μέτρα πρώτους αριθμούς

Θεώρημα 3.1

Θεωρούμε την πολυωνυμική ισοτιμία βαθμού n

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \equiv 0 \pmod p$$

με $a_n \not\equiv 0 \pmod p$, p πρώτος και $n \geq p$.

Τότε ή το $f(x)$ είναι πολλαπλάσιο του $x^p - x \pmod p$ δηλαδή υπάρχει $q(x) \in \mathbb{Z}[x]$ έτσι ώστε

$$f(x) \equiv (x^p - x) q(x) \pmod p \text{ ταυτοτικά},$$

ή η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod p$ είναι **ισοδύναμη** με μια πολυωνυμική ισοτιμία $g(x) \equiv 0 \pmod p$ βαθμού $\leq p-1$.

Απόδειξη.

Διαιρώντας το $f(x)$ με το $x^p - x$ βρίσκουμε πολυώνυμα $q(x), r(x) \in \mathbb{Z}[x]$ έτσι ώστε:

$$f(x) = (x^p - x) q(x) + r(x) \qquad (1)$$

όπου $r(x) = 0$ ή $\deg r(x) < p$.

Για το υπόλοιπο $r(x)$ υπάρχουν 3 δυνατότητες:

i) $r(x) = 0$,

ή

ii) $\deg r(x) < p$ και $r(x) \equiv 0 \pmod p$ ταυτοτικά

ή

iii) $\deg r(x) < p$ και $r(x) \not\equiv 0 \pmod p$ ταυτοτικά.

Στις περιπτώσεις i) και ii) είναι πάντα $r(x) \equiv 0 \pmod p$ ταυτοτικά και επομένως από την (1) θα είναι

$$f(x) \equiv (x^p - x) q(x) \pmod p \text{ ταυτοτικά}.$$

Στην περίπτωση iii) ας υποθέσουμε ότι

$$r(x) = b_0 + b_1 x + \cdots + b_k x^k + \cdots + b_m x^m \quad , \quad b_m \neq 0$$

$m \leq p-1$, και έστω ότι η πολυωνυμική ισοτιμία $r(x) \equiv 0 \pmod p$ έχει βαθμό $k \leq m$, οπότε $b_k \not\equiv 0 \pmod p$ και $b_{k+1} \equiv \cdots \equiv b_m \equiv 0 \pmod p$.

Αν $g(x)=b_0+b_1x+\cdots+b_kx^k$ τότε

$$r(x)\equiv g(x)\ (\mathrm{mod}p)\ \text{ταυτοτικά}$$

και επομένως για κάθε ακέραιο u είναι

$$r(u)\equiv g(u)\ (\mathrm{mod}p). \qquad (2)$$

Από το θεώρημα Fermat έχουμε $u^p-u\equiv 0\ (\mathrm{mod}p)$, $\forall u\in\mathbb{Z}$, επομένως $\forall u\in\mathbb{Z}$ από την (1) θα έχουμε

$$f(u)=(u^p-u)q(u)+r(u)\equiv r(u)\ (\mathrm{mod}p) \qquad (3)$$

Από τις (2) και (3) έχουμε τελικά

$$f(u)\equiv g(u)\ (\mathrm{mod}p)\ ,\ \forall u\in\mathbb{Z}\ ,$$

Από την πρόταση 2.2 συμπεραίνουμε τώρα ότι η πολυωνυμική ισοτιμία $f(x)\equiv 0\ (\mathrm{mod}p)$ είναι ισοδύναμη με την πολυωνυμική ισοτιμία $g(x)\equiv 0\ (\mathrm{mod}p)$ που έχει βαθμό $k\le m\le p-1$. ∎

Παράδειγμα 3.1

Θεωρούμε την πολυωνυμική ισοτιμία βαθμού $7>3$

$$f(x)=x^7-3x^5+4x^3+3x^2+1\equiv 0\ (\mathrm{mod}3).$$

Διαιρώντας το $f(x)$ με το x^3-x έχουμε

$$f(x)=(x^3-x)(x^4-2x^2+2)+(3x^2+2x+1)$$

Για το υπόλοιπο έχουμε

$$3x^2+2x+1\equiv 2x+1\ (\mathrm{mod}3)\ \text{ταυτοτικά}$$

Έτσι η πολυωνυμική ισοτιμία $f(x)\equiv 0\ (\mathrm{mod}3)$ είναι ισοδύναμη με την $1+2x\equiv 0\ (\mathrm{mod}3)$ που έχει βαθμό $1<(3-1)$ και μοναδική λύση $x\equiv 1\ (\mathrm{mod}3)$ που είναι και η μοναδική λύση της $f(x)\equiv 0\ (\mathrm{mod}3)$.

Παράδειγμα 3.2

Θεωρούμε την πολυωνυμική ισοτιμία βαθμού 8

$$f(x)=x^8-2x^6-x^4+5x^3+12x^2+5\equiv 0\ (\mathrm{mod}5).$$

Διαιρώντας το $f(x)$ με το x^5-x έχουμε

$$f(x)=(x^5-x)(x^3-2x)+(5x^3+10x^2+5)$$

Αλλά $5x^3+10x^2+5 \equiv 0 \pmod 5$ ταυτοτικά

επομένως $f(x) \equiv (x^5-x)(x^3-2x) \pmod 5$ ταυτοτικά

Άρα $f(u) \equiv 0 \pmod 5$, $\forall u \in \mathbb{Z}$

και επομένως η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod 5$ έχει 5 διαφορετικές λύσεις (mod5) τις $x \equiv 0,1,2,3,4 \pmod 5$.

Παράδειγμα 3.3

Θεωρούμε την πολυωνυμική ισοτιμία

$$f(x) = 6\cdot x^{1998} + x^5 - 2x^3 + 6x^2 + x + 2 \equiv 0 \pmod 3.$$

Είναι

$$f(x) \equiv x^5 - 2x^3 + x + 2 \pmod 3$$ ταυτοτικά

και επομένως, σύμφωνα με το Πόρισμα 2.2 η αρχική πολυωνυμική ισοτιμία είναι ισοδύναμη με την

$$g(x) = x^5 - 2x^3 + x + 2 \equiv 0 \pmod 3$$

Διαιρούμε το $g(x)$ με το x^3-x και έχουμε

$$g(x) = (x^3-x)(x^2-1) + 2$$

Άρα η πολυωνυμική ισοτιμία $g(x) \equiv 0 \pmod 3$ είναι ισοδύναμη με την πολυωνυμική ισοτιμία βαθμού 0 , $2 \equiv 0 \pmod 3$ η οποία δεν έχει λύση Άρα η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod 3$ δεν έχει λύση.

Θεώρημα 3.2 (Lagrance)

Αν είναι p ένας πρώτος και

$$f(x) = a_n x^n + \cdots + a_0 \quad , \quad a_n \not\equiv 0 \pmod p$$

ένα πολυώνυμο με ακέραιους συντελεστές.

Τότε η πολυωνυμική ισοτιμία βαθμού n

$$f(x) \equiv 0 \pmod p$$

έχει το πολύ n διαφορετικές λύσεις.

Απόδειξη.

Θα χρησιμοποιήσουμε επαγωγή πάνω στο βαθμό της πολυωνυμικής ισοτιμίας $f(x)\equiv 0 \pmod p$.

Αν $n=0$ τότε η πολυωνυμική ισοτιμία βαθμού 0 $f(x)=a_0\equiv 0 \pmod p$ δεν έχει λύση, αφού $a_0\not\equiv 0 \pmod p$.

Αν $n=1$, τότε η $f(x)=a_1x+a_0\equiv 0 \pmod p$ με $a_1\not\equiv 0 \pmod p$ είναι γραμμική ισοτιμία και έχει μία ακριβώς λύση $\pmod p$ αφού $(a_1,p)=1$.

Υποθέτουμε ότι το θεώρημα αληθεύει για πολυωνυμικές ισοτιμίες βαθμού $<n$.

Θεωρούμε μια πολυωνυμική ισοτιμία βαθμού n

$$f(x)=a_nx^n+\cdots+a_0\equiv 0 \pmod p \quad , \quad a_n\not\equiv 0 \pmod p$$

και υποθέτουμε ότι το θεώρημα δεν αληθεύει γι' αυτή.

Θα έχει λοιπόν αυτή τουλάχιστον $n+1$ διαφορετικές λύσεις και ας είναι αυτές οι εξής:

$$c_0, c_1, \ldots, c_n \pmod p.$$

Άρα $$f(c_k)\equiv 0 \pmod p \quad , k=0,1,\ldots,n.$$

Θα καταλήξουμε σε άτοπο. Είναι

$$f(x)-f(c_0)=\sum_{r=1}^{n} a_r(x^r-c_0^r)=(x-c_0)q(x)$$

όπου

$$q(x)=a_nx^{n-1}+(a_nc_0+a_{n-1})x^{n-2}+\cdots+(a_nc_0^{n-1}+\ldots+a_1)$$

Έτσι για $k=1,\ldots,n$ έχουμε

$$f(c_k)-f(c_0)=(c_k-c_0)q(c_k)\equiv 0 \pmod p$$

αφού $f(c_k)\equiv f(c_0)\equiv 0 \pmod p \quad , k=1,\ldots,n$

Αλλά $c_k-c_0\not\equiv 0 \pmod p \quad , k=1,\ldots,n$

αφού οι λύσεις είναι ανισότιμες $\pmod p$

όπότε $$q(c_k)\equiv 0 \pmod p \quad , k=1,\ldots,n.$$

Δηλαδή η πολυωνυμική ισοτιμία βαθμού $n-1$

$$q(x) \equiv 0 \pmod p$$

έχει η ανισότιμες $(\mathrm{mod}\, p)$ λύσεις τις $c_1, c_2, \dots, c_n \pmod p$ πράγμα που αντιφάσκει στην επαγωγική μας υπόθεση. Άρα η πολυωνυμική ισοτιμία βαθμού η $f(x) \equiv 0 (\mathrm{mod}\, p)$ θα έχει το πολύ η διαφορετικές λύσεις. ■

Παρατήρηση.

Το θεώρημα του Lagrance αν το μεταφέρουμε στα πολυώνυμα με συντελεστές από το σώμα $\mathbb{Z}_p$, μας λέει ότι κάθε πολυώνυμο βαθμού η δεν μπορεί να έχει στο $\mathbb{Z}_p$ περισσότερες από η διαφορετικές ρίζες, ένα γνωστό μας αποτέλεσμα από την θεωρία πολυωνύμων με συντελεστές από ένα οποιοδήποτε σώμα F.

Πόρισμα 3.1

Αν η πολυωνυμική ισοτιμία

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \equiv 0 \pmod p \quad , p \text{ πρώτος}$$

έχει περισσότερες από η διαφορετικές λύσεις, τότε όλοι οι συντελεστές του πολυωνύμου $f(x)$ διαιρούνται από τον p δηλαδή

$$f(x) \equiv 0 \pmod p \text{ ταυτοτικά.}$$

Απόδειξη.

Ας υποθέσουμε ότι $f(x) \not\equiv 0 \pmod p$ ταυτοτικά.

Τότε η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod p$ έχει βαθμό και έστω ότι αυτός είναι r. Επομένως $0 \le r \le n$ και

$$a_r \not\equiv 0 \pmod p \quad , \quad a_{r+1} \equiv \dots \equiv a_n \equiv 0 \pmod p.$$

Αν $g(x) = a_0 + a_1 x + \dots + a_r x^r$ τότε

$$f(x) \equiv g(x) \pmod p \text{ ταυτοτικά} \qquad (\text{Πρότ. } 2.1)$$

Άρα οι πολυωνυμικές ισοτιμίες (πόρ. 2.1)

$$f(x) \equiv 0 \pmod p \quad \text{και} \quad g(x) \equiv 0 \pmod p$$

είναι ισοδύναμες. Έτσι η πολυωνυμική ισοτιμία $g(x) \equiv 0 \pmod p$ βαθμού $r \le n$ θα έχει περισσότερες από η διακεκριμένες λύσεις

δηλαδή έχει λύσεις περισσότερες από τον βαθμό της, πράγμα άτοπο σύμφωνα με το θεώρημα του Lagrange. Άρα

$$f(x) \equiv 0 \pmod p \text{ ταυτοσικά.}$$

Παρατήρηση

Το αποτέλεσμα αυτό αν το μεταφέρουμε στα πολυώνυμα του $\mathbb{Z}_p[x]$, μας λέει ότι κάθε πολυώνυμο του $\mathbb{Z}_p[x]$ που έχει περισσότερες διακεκριμένες ρίζες από τον βαθμό του είναι το μηδενικό πολυώνυμο.

Πόρισμα 3.2

Η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod p$, βαθμού $n \geq p$ έχει p διαφορετικές λύσεις $\pmod p$ αν και μόνο αν το $f(x)$ είναι πολλαπλάσιο του $x^p - x \pmod p$.

Απόδειξη.

Έστω ότι $f(x) \equiv (x^p - x) q(x) \pmod p$ ταυτοσικά, όπου $q(x) \in \mathbb{Z}[x]$.

Για κάθε ακέραιο u έχουμε (Πρότ. 1.3 και θεώρημα Fermat)

$$f(u) \equiv (u^p - u)\, q(u) \equiv 0 \pmod p.$$

Έτσι η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod p$ έχει p διακεκριμένες λύσεις τις $x \equiv 0, 1, \ldots, p-1 \pmod p$.

Αντίστροφα, ας υποθέσουμε ότι η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod p$ έχει p διαφορετικές λύσεις.

Διαιρώντας το $f(x)$ με το $x^p - x$ βρίσκουμε πολυώνυμα $q(x), r(x) \in \mathbb{Z}[x]$ τέτοια ώστε

$$f(x) = (x^p - x) q(x) + r(x), \quad r(x) = 0 \text{ ή } \deg r(x) < p.$$

Αν $r(x) = 0$ τότε φανερά

$$f(x) \equiv (x^p - x) q(x) \pmod p \text{ ταυτοσικά.}$$

Αν $\deg r(x) < p$ τότε για κάθε ακέραιο u έχουμε φανερά

$$f(u) \equiv r(u) \pmod p.$$

επομένως οι πολυωνυμικές ισοτιμίες (Πρότ. 2.2)

$$f(x) \equiv 0 \pmod p \quad \text{και} \quad r(x) \equiv 0 \pmod p$$

είναι ισοδύναμες. Έτσι η πολυωνυμική ισοτιμία $r(x) \equiv 0 \pmod p$ έχει p διαφορετικές λύσεις, ενώ ο βαθμός της $\leq \deg r(x) < p$ οπότε σύμφωνα με το Πόρισμα 3.1 θα είναι

$$r(x) \equiv 0 \pmod p \text{ ταυτοτικά.}$$

Έτσι $$f(x) \equiv (x^p - x)\, q(x) \pmod p \text{ ταυτοτικά.} \blacksquare$$

Παρατήρηση

Θεωρούμε την πολυωνυμική ισοτιμία

$$f(x) \equiv 0 \pmod p, \quad p \text{ πρώτος} \qquad (*)$$

Η (*), ή δεν έχει λύσεις ή για το πλήθος κ των διαφορετικών λύσεων έχουμε $1 \leq \kappa \leq p$. Ειδικότερα:

1) Αν η (*) <u>δεν έχει βαθμό</u>, δηλαδή αν

$$f(x) \equiv 0 \pmod p \text{ ταυτοτικά}$$

τότε η (*) έχει ακριβώς p διαφορετικές λύσεις.

2) Αν η (*) <u>έχει βαθμό η</u>, τότε.

α) Αν $\eta < p$ τότε η (*), ή δεν έχει λύση ή έχει κ διαφορετικές λύσεις, $1 \leq \kappa \leq \eta$.

β) Αν $\eta \geq p$ και

i) Το $f(x)$ <u>είναι πολλαπλάσιο</u> του $x^p - x \pmod p$, τότε η (*) έχει p ακριβώς διαφορετικές λύσεις.

ii) Το $f(x)$ <u>δεν είναι πολλαπλάσιο</u> του $x^p - x \pmod p$, τότε η (*) είναι ισοδύναμη με πολυωνυμική ισοδυναμία βαθμού $\ell < p$, και είμαστε στην περίπτωση α) δηλαδή η (*) ή δεν έχει λύση ή έχει κ διαφορετικές λύσεις $1 \leq \kappa \leq \ell$. $\blacksquare$

Η παραπάνω παρατήρηση συνοψίζει όλα όσα αναφέραμε μέχρι τώρα στην παράγραφο αυτή.

Θεώρημα 3.3.

Αν η πολυωνυμική ισοτιμία βαθμού n, p πρώτος

$$f(x)=a_0+a_1x+\cdots+a_nx^n\equiv 0\ (\mathrm{mod}\,p)$$

έχει k διαφορετικές λύσεις $c_1,\ldots,c_k\ (\mathrm{mod}\,p)$, $1\le k\le n$ τότε

$$f(x)\equiv(x-c_1)\cdots(x-c_k)\,g_k(x)\ (\mathrm{mod}\,p)\ \text{ταυτοτικά}$$

όπου $g_k(x)$ είναι ένα πολυώνυμο βαθμού $n-k$ με ακέραιους συντελεστές και συντελεστή του μεγιστοβαθμίου όρου το a_n. Ιδιαίτερα αν $k=n$ έχουμε $g_k(x)=a_n$.

Απόδειξη.

Θα χρησιμοποιήσουμε επαγωγή πάνω στο πλήθος k των διαφορετικών λύσεων Για $k=1$ έχουμε

$$f(x)-f(c_1)=\sum_{r=1}^{n}a_r\,(x^r-c_1^r)=(x-c_1)g_1(x)$$

όπου

$$g_1(x)=a_nx^{n-1}+(a_nc_1+a_{n-1})x^{n-2}+\cdots+(a_nc_1^{n-1}+\cdots+a_1)$$

Επειδή $f(c_1)\equiv 0\ (\mathrm{mod}\,p)$, έχουμε

$$f(x)\equiv(x-c_1)g_1(x)\ (\mathrm{mod}\,p)\ \text{ταυτοτικά.}$$

Υποθέτουμε ότι το θεώρημα είναι αληθές όταν το πλήθος των διαφορετικών λύσεων είναι $\le k-1$. Θα δείξουμε την αλήθεια του θεωρήματος όταν το πλήθος αυτό είναι k.

Απο την υπόθεση έχουμε

$$f(x)\equiv(x-c_1)\cdots(x-c_{k-1})\,g_{k-1}(x)\ (\mathrm{mod}\,p)\ \text{ταυτοτικά}\quad (i)$$

όπου το $g_{k-1}(x)$ είναι ένα πολυώνυμο του $\mathbb{Z}[x]$ βαθμού $n-(k-1)$ με συντελεστή του μεγιστοβαθμίου όρου το a_n.

Είναι όμως $f(c_k)\equiv 0\ (\mathrm{mod}\,p)$ οπότε

$$(c_k-c_1)\cdots(c_k-c_{k-1})\,g_{k-1}(c_k)\equiv 0\ (\mathrm{mod}\,p).$$

Επειδή οι $c_1,\ldots,c_k$ είναι διαφορετικές λύσεις $(\mathrm{mod}\,p)$

$p \nmid c_k - c_j$ $(j=1,\dots,k-1)$ θα έχουμε $g_{k-1}(c_k) \equiv 0 \pmod p$
επομένως

$$g_{k-1}(x) \equiv (x-c_k) g_k \pmod p \text{ ταυτοτικά.} \quad (ii)$$

όπου το $g_k(x)$ είναι ένα πολυώνυμο με ακέραιους συντελεστές βαθμού $(n-(k-1))-1 = n-k$ και συντελεστή του μεγιστοβαθμίου όρου το a_n.

Από τις (i) και (ii) έχουμε τελικά

$$f(x) \equiv (x-c_1)\cdots(x-c_k) g_k(x) \pmod p \text{ ταυτοτικά.}$$

Στην περίπτωση όπου $k=n$, το $g_n(x)$ έχει βαθμό 0 και είναι το σταθερό πολυώνυμο a_n, οπότε

$$f(x) \equiv a_n (x-c_1)\cdots(x-c_n) \pmod p \text{ ταυτοτικά.} \blacksquare$$

Από το θεώρημα 3.3 μπορούμε να πάρουμε σαν πόρισμα το θεώρημα Lagrange. Επιπλέον,

Το θεώρημα 3.3 δεν ισχύει αν το modulo είναι σύνθετος, για παράδειγμα οι $x \equiv 1, -1, 3, -3 \pmod{16}$ είναι κάποιες από τις λύσεις της πολυωνυμικής ισοτιμίας

$$x^4 - 1 \equiv 0 \pmod{16}$$

Αν ήταν $x^4-1 \equiv (x-1)(x+1)(x-3)(x+3) \pmod{16}$ ταυτοτικά θα έπρεπε $-1 \equiv 9 \pmod{16}$, πράγμα που δεν αληθεύει.

Πόρισμα 3.3

Για κάθε πρώτο p είναι

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod p \text{ ταυτοτικά}$$

Απόδειξη

Η πολυωνυμική ισοτιμία $f(x) = x^{p-1} - 1 \equiv 0 \pmod p$ σύμφωνα με το θεώρημα Fermat έχει $(p-1)$ διαφορετικές λύσεις $\pmod p$ τις

$$x \equiv 1 \pmod p, \dots, x \equiv p-1 \pmod p.$$

Απο το θεώρημα 3.3 θα έχουμε

$$x^{p-1} - 1 \equiv (x-1)\cdots(x-(p-1)) \pmod p \text{ ταυτοτικά.}$$ ■

Παρατήρηση. Μια απόδειξη του Πορίσματος 3.3 ανεξάρτητη απο το θεώρημα 3.3. είναι η ακόλουθη.

Για $p=2$ ισχύει. Έστω p περιττός πρώτος.

Θεωρούμε τα πολυώνυμα $g(x)=x^{p-1}-1$, $h(x)=(x-1)\cdots(x-(p-1))$ και $f(x)=g(x)-h(x)$.

Οι πολυωνυμικές ισοτιμίες $g(x)\equiv 0 \pmod p$ και $h(x)\equiv 0 \pmod p$ έχουν λύσεις τις $x \equiv 1,2,\ldots,(p-1) \pmod p$, οι οποίες είναι λύσεις και της πολυωνυμικής ισοτιμίας $f(x)\equiv 0 \pmod p$.

Ο βαθμός του πολυωνύμου $f(x)$ είναι $p-2$ και η πολυωνυμική ισοτιμία $f(x)\equiv 0 \pmod p$ έχει περισσότερες απο $p-2$ διαφορετικές λύσεις $\pmod p$ οπότε σύμφωνα με το Πόρισμα 3.1

$f(x)\equiv 0 \pmod p$ ταυτοτικά, δηλαδή

$$x^{p-1}-1 \equiv (x-1)\cdots(x-(p-1)) \pmod p \text{ ταυτοτικά.}$$ ■

Το επόμενο Πόρισμα είναι το γνωστό θεώρημα Wilson (θεωρ. 6.1 κεφ IV) με μια διαφορετική όμως απόδειξη.

Πόρισμα 3.4 (θεώρημα Wilson)

Για κάθε πρώτο p ισχύει

$$(p-1)! \equiv -1 \pmod p$$

Απόδειξη.

Για πρώτο p ισχύει (Πόρισμα 3.3)

$x^{p-1}-1 \equiv (x-1)\cdots(x-(p-1)) \pmod p$ ταυτοτικά.

Οι σταθεροί όροι των δύο μερών της ταυτοτικής ισοτιμίας θα είναι ακέραιοι ισότιμοι $\pmod p$, άρα

$$-1 \equiv (-1)^{p-1}\,(p-1)! \pmod p.$$

Είτε ο $p=2$, είτε ο p είναι περιττός πρώτος έχουμε

$$-1 \equiv (p-1)! \pmod p$$ ■

Παρατήρηση. Μια άλλη απόδειξη του θεωρήματος του Wilson προκύπτει αν στην ταυτοτική ισοτιμία

$x^{p-1}-1 \equiv (x-1)\cdots(x-(p-1)) \pmod p$ ταυτοτικά

θέσουμε $x=p$, οπότε έχουμε την ισοτιμία ακεραίων

$p^{p-1}-1 \equiv (p-1)\cdots 1 \pmod p$ δηλαδή $p^{p-1}-1 \equiv (p-1)! \pmod p$

Αλλά $p^{p-1} \equiv 0 \pmod p$, επομένως $-1 \equiv (p-1)! \pmod p$. ■

Πόρισμα 3.5

Αν ο p είναι περιττός πρώτος, $1 \le k < p-1$, και S_k είναι το άθροισμα των γινομένων των αριθμών $1,2,\ldots,p-1$ ανα k διαφορετικών κάθε φορά, τότε

$$S_k \equiv 0 \pmod p \qquad k=1,2,\ldots,p-2$$

Απόδειξη.

Έστω $g(x)=(x-1)(x-2)\cdots(x-(p-1))$

Οι αριθμοί $1,2,\ldots,p-1$ είναι οι ρίζες του πολυωνύμου $g(x)$ και το S_k είναι τώρα το άθροισμα των γινομένων των ριζών $1,2,\ldots,p-1$ ανα k διαφορετικών κάθε φορά. Επομένως

$$g(x)=x^{p-1}-S_1x^{p-2}+S_2x^{p-3}+\cdots+S_{p-3}x^2-S_{p-2}x+(p-1)!$$

Απο το πόρισμα 3.3 έχουμε

$x^{p-1}-1 \equiv x^{p-1}-S_1x^{p-2}+\cdots-S_{p-2}x+(p-1)! \pmod p$ ταυτοτικά

Οι συντελεστές λοιπόν των δυνάμεων $x^{p-2},\ldots,x^2,x$ και στα δύο μέρη της ταυτοτικής ισοτιμίας θα είναι ισότιμοι $\pmod p$, επομένως

$S_1 \equiv 0 \pmod p$, $S_2 \equiv 0 \pmod p$, $\ldots$, $S_{p-2} \equiv 0 \pmod p$

πράγμα που επιδιωκούσαμε. ■

Πρόβλημα.

Αν p είναι περιττός πρώτος τότε ο αριθμητής του κλάσματος

$$1+\frac{1}{2}+\cdots+\frac{1}{p-1}$$

διαιρείται από τον p.

Πραγματικά ο αριθμητής του κλάσματος είναι ο S_{p-2} δηλαδή το άθροισμα των γινομένων των αριθμών $1,2,\ldots,p-1$ όταν λαμβάνονται $p-2$ κάθε φορά, άρα σύμφωνα με το Πόρισμα 3.5 θα είναι $S_{p-2}\equiv 0 \pmod p$.

Πόρισμα 3.6 (Θεώρημα του Wolstenholme)

Για κάθε πρώτο $p\geq 5$ έχουμε

$$\sum_{k=1}^{p-1}\frac{(p-1)!}{k}\equiv 0 \pmod{p^2}$$

Απόδειξη.

Είναι

$$\sum_{k=1}^{p-1}\frac{(p-1)!}{k}=\frac{(p-1)!}{1}+\frac{(p-1)!}{2}+\cdots+\frac{(p-1)!}{p-1}=S_{p-2}$$

δηλαδή το εξεταζόμενο άθροισμα είναι το άθροισμα των γινομένων των αριθμών $1,2,\ldots,p-1$ όταν λαμβάνονται $p-2$ κάθε φορά.

Το άθροισμα αυτό είναι ο συντελεστής S_{p-2} του $-x$ στο πολυώνυμο

$$g(x)=(x-1)(x-2)\cdots(x-(p-1))=$$
$$=x^{p-1}-S_1x^{p-2}+S_2x^{p-3}+\cdots+S_{p-3}x^2-S_{p-2}x+(p-1)!$$

όπως είδαμε και στο Πόρισμα 3.5, επιπλέον

$$S_k\equiv 0 \pmod p \quad , \quad 1\leq k<p-1 .$$

Αλλά για $x=p$ έχουμε

$$g(p)=(p-1)\cdots 1=(p-1)!$$

$$g(p)=p^{p-1}-S_1p^{p-2}+S_2p^{p-3}+\cdots+S_{p-3}p^2-S_{p-2}p+(p-1)!$$

Άρα

$$(p-1)!=p^{p-1}-S_1p^{p-2}+\cdots+S_{p-3}p^2-S_{p-2}p+(p-1)!$$

οπότε, $p S_{p-2} = p^{p-1} - S_1 p^{p-2} + \cdots + S_{p-3} p^2$

Επειδή όμως $p \geq 5$ και $S_k \equiv 0 \pmod{p}$, $1 \leq k < p-1$ θα είναι $p S_{p-2} \equiv 0 \pmod{p^3}$

και επομένως $S_{p-2} \equiv 0 \pmod{p^2}$. ∎

Πρόβλημα

Αν p πρώτος $p \geq 5$ τότε ο αριθμητής του αθροίσματος

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$$

διαιρείται από τον p^2.

Πράγματι ο αριθμητής του αθροίσματος είναι ο S_{p-2} δηλαδή το άθροισμα των γινομένων των αριθμών $1, \ldots, p-1$ όταν λαμβάνονται $p-2$ κάθε φορά. Θα είναι $S_{p-2} \equiv 0 \pmod{p^2}$ σύμφωνα με το πόρισμα 3.6.

Πρόταση 3.1

Αν είναι p πρώτος και $f(x), g(x), h(x) \in \mathbb{Z}[x]$ τέτοια ώστε

$$f(x) \equiv g(x) h(x) \pmod{p} \text{ ταυτοτικά.}$$

Για τις πολυωνυμικές ισοτιμίες

i) $f(x) \equiv 0 \pmod{p}$

ii) $g(x) \equiv 0 \pmod{p}$

iii) $h(x) \equiv 0 \pmod{p}$

ισχύουν τα εξής:

1) Μια κλάση $a \pmod{p}$ είναι λύση της i) αν και μόνο αν είναι λύσης μιας από τις ii) και iii).

2) Αν η i) έχει βαθμό k και k διαφορετικές λύσεις $\pmod{p}$ τότε οι ii) και iii) θα έχουν τόσες διαφορετικές λύσεις όσες μονάδες έχουν οι βαθμοί τους.

Απόδειξη

1. Σύμφωνα με την πρόταση 2.1 η τάξη $a \pmod p$ είναι λύση της i) αν και μόνο αν η τάξη $a \pmod p$ είναι λύση της πολυωνυμικής ισοτιμίας $g(x)h(x) \equiv 0 \pmod p$.

Αν $g(a)\,h(a) \equiv 0 \pmod p$, θα έχουμε

$p \mid g(a)$ ή $p \mid h(a)$ δηλαδή

$g(a) \equiv 0 \pmod p$ ή $h(a) \equiv 0 \pmod p$.

Συνεπώς η τάξη $a \pmod p$ είναι λύση μιας εκ των ii) και iii). Το αντίστροφο είναι φανερό.

2. Αν είναι $g(x) = b_0 + b_1 x + \cdots + b_\mu x^\mu$ με $b_\mu \not\equiv 0 \pmod p$ και $h(x) = c_0 + c_1 x + \cdots + c_\nu x^\nu$ με $c_\nu \not\equiv 0 \pmod p$ Τότε η ii) έχει βαθμό μ και η iii) έχει βαθμό ν.

Έχουμε $g(x)h(x) = b_0 c_0 + \cdots + b_\mu c_\nu x^{\nu+\mu}$

με $b_\mu c_\nu \not\equiv 0 \pmod p$, οπότε η πολυωνυμική ισοτιμία $g(x)h(x) \equiv 0 \pmod p$ έχει βαθμό $\nu+\mu$.

Αφού $f(x) \equiv b_0 c_0 + \cdots + b_\mu c_\nu x^{\nu+\mu} \pmod{}$ ταυτοτικά εύκολα συμπεραίνουμε ότι $\kappa = \mu+\nu$.

Από την υπόθεση, το θεώρημα Lagrange και το μέρος 1) της πρότασης αυτής, έχουμε

Η i) έχει ακριβώς κ διαφορετικές λύσεις, έστω τις

$$a_1 \pmod p, \ldots, a_\kappa \pmod p.$$

η ii) έχει το πολύ μ λύσεις απ' αυτές της i)

η iii) έχει το πολύ ν λύσεις απ' αυτές της i).

Αν η ii) έχει λιγότερες από μ λύσεις και η iii) έχει λιγότερες από ν λύσεις τότε η i) θα έχει λιγότερες από $\mu+\nu$ λύσεις δηλαδή $\kappa < \mu+\nu$ αντίθετα με την υπόθεσή μας. Έτσι πρέπει να έχει, η ii) ακριβώς μ λύσεις και η iii) ακριβώς ν λύσεις. ∎

Η πρόταση ΔΕΝ ισχύει όταν το μέτρο είναι σύνθετος ακέραιος,

για παράδειγμα, $x^2 \equiv x^2 - 4 \equiv (x-2)(x+2) \pmod 4$ ταυτοτικά
Μία λύση της πολυωνυμικής ισοτιμίας $x^2 \equiv 0 \pmod 4$ είναι η $x \equiv 0 \pmod 4$, αλλά αυτή δεν είναι λύση ούτε της πολυωνυμικής ισοτιμίας $x-2 \equiv 0 \pmod 4$ ούτε της $x+2 \equiv 0 \pmod 4$.

Το επόμενα πόρισμα θα μας χρησιμεύσει στα επόμενα.

Πόρισμα 3.7

Ας είναι p πρώτος. Για κάθε φυσικό διαιρέτη d του $p-1$ η πολυωνυμική ισοτιμία

$$x^d - 1 \equiv 0 \pmod p$$

έχει ακριβώς d διαφορετικές λύσεις $\pmod p$.

Απόδειξη

Για $p=2$ είναι $d=1$ και η $x-1 \equiv 0 \pmod 2$ έχει μοναδική λύση.

Για περιττό πρώτο p έχουμε $d \mid p-1$ οπότε $p-1 = dk$, $k \in \mathbb{N}$.

Έτσι $$x^{p-1} - 1 = (x^d)^k - 1 = (x^d - 1)\, h(x)$$

όπου $h(x) = (x^d)^{k-1} + (x^d)^{k-2} + \dots + x^d + 1 =$

$$= x^{p-1-d} + x^{p-1-2d} + \dots + x^d + 1$$

δηλαδή

$$x^{p-1} - 1 \equiv (x^d - 1)\, h(x) \pmod p \text{ ταυτοτικά.}$$

Η πολυωνυμική ισοτιμία $x^{p-1} - 1 \equiv 0 \pmod p$ έχει βαθμό $p-1$ και $p-1$ λύσεις τις

$$x \equiv 1 \pmod p, \dots, x \equiv p-1 \pmod p.$$

Οι πολυωνυμικές ισοτιμίες $x^d - 1 \equiv 0 \pmod p$ και $h(x) \equiv 0 \pmod p$ έχουν βαθμούς d και $p-1-d$ αντίστοιχα. Σύμφωνα με την Πρόταση 3.1,2) η πολυωνυμική ισοτιμία $x^d - 1 \equiv 0 \pmod p$ έχει ακριβώς d διαφορετικές λύσεις $\pmod p$. ∎

Πόρισμα 3.8

Αν p περιττός πρώτος τότε κάθε μια απο τις πολυωνυμικές ισοτιμίες

i) $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$

και

ii) $x^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$

έχει ακριβώς $\frac{p-1}{2}$ διαφορετικές λύσεις $(\mathrm{mod}\, p)$.

Απόδειξη.

Για $p > 2$ έχουμε

$$x^{p-1} - 1 \equiv \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right) \pmod p .$$

Η πολυωνυμική ισοτιμία $x^{p-1} - 1 \equiv 0 \pmod p$ έχει βαθμό $p-1$ και έχει $p-1$ διαφορετικές λύσεις τις

$$x \equiv 1 \pmod p, \ldots, x \equiv p-1 \pmod p .$$

Η i) έχει βαθμό $\frac{p-1}{2}$ και η ii) όμοια έχει βαθμό $\frac{p-1}{2}$.

Σύμφωνα με την πρόταση 3.1 η i) και ii) έχουν καθεμιά $\frac{p-1}{2}$ διαφορετικές λύσεις $(\mathrm{mod}\, p)$. ■

Πρόταση 3.9

Η πολυωνυμική ισοτιμία βαθμού n

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \equiv 0 \pmod p$$

p πρώτος, $n < p$, έχει ακριβώς n διακεκριμένες λύσεις $(\mathrm{mod}\, p)$ αν και μόνο αν το $x^p - x$ είναι ένα πολλαπλάσιο του $f(x)$ $(\mathrm{mod}\, p)$.

Απόδειξη.

Αν το $x^p - x$ είναι πολλαπλάσιο του $f(x)$ $(\mathrm{mod}\, p)$, τότε

$$x^p - x \equiv f(x)\,q(x) \pmod p \quad \text{ταυτοτικά},$$

όπου $q(x) \in \mathbb{Z}[x]$.

Γνωρίζουμε ότι η πολυωνυμική ισοτιμία $x^p - x \equiv 0 \pmod p$

έχει βαθμό p και p διαφορετικές λύσεις (mod p).

Η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod p$ έχει βαθμό η και σύμφωνα με την πρόταση 3.1 θα έχει ακριβώς η διακεκριμένες λύσεις.

Αντίστροφα, έστω ότι η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod p$ έχει η διακεκριμένες λύσεις, $\eta < p$.

Διαιρώντας το $x^p - x$ με το $f(x)$ βρίσκουμε πολυώνυμα $q(x)$ και $r(x) \in \mathbb{Z}[x]$ έτσι ώστε

$$x^p - x = f(x)q(x) + r(x)$$

όπου $r(x) = 0$ ή $\deg r(x) < \eta$.

Παρατηρούμε ότι, κάθε λύση της πολυωνυμικής ισοτιμίας $f(x) \equiv 0 \pmod p$ είναι λύση και της $r(x) \equiv 0 \pmod p$. Πραγματικά αν για τον ακέραιο u είναι $f(u) \equiv 0 \pmod p$, τότε

$$0 \equiv u^p - u \equiv f(u)q(u) + r(u) \pmod p \quad \text{άρα}$$

$r(u) \equiv 0 \pmod p$.

Η πολυωνυμική ισοτιμία $r(x) \equiv 0 \pmod p$ θα έχει τουλάχιστον η διακεκριμένες λύσεις.

Αν $r(x) \neq 0$, τότε $\deg r(x) < \eta$, επομένως από το Πόρισμα 3.1 θα έχουμε $r(x) \equiv 0 \pmod p$ ταυτοτικά.

Έτσι πάντα $r(x) \equiv 0 \pmod p$ ταυτοτικά, οπότε

$$x^p - x \equiv f(x)q(x) \pmod p \text{ ταυτοτικά.} \blacksquare$$

Παρατήρηση.

Ο περιορισμός $a_\eta = 1$ στην παραπάνω πρόταση τέθηκε για να μπορέσουμε να εκτελέσουμε την διαίρεση του $x^p - x$ με το $f(x)$ και να πάρουμε τα $q(x), r(x)$ με ακέραιους συντελεστές, αφού δεν έχουμε αναφερθεί σε διαιρετότητα πολυωνύμων (mod p).

Η πρόταση 3.2 ισχύει και γενικότερα.

Πρόταση 3.3

Η πολυωνυμική ισοτιμία βαθμού η

$$f(x) = a_n x^n + \dots + a_0 \equiv 0 \pmod p \quad , \quad a_n \not\equiv 0 \pmod p$$

p πρώτος, $n < p$, έχει ακριβώς η διακεκριμένες λύσεις $\pmod p$ αν και μόνο αν το $x^p - x$ είναι ένα πολλαπλάσιο του $f(x)$.

Απόδειξη.

Θεωρούμε την γραμμική ισοτιμία $a_n x \equiv 1 \pmod p$ και ας είναι $b \pmod p$ η μοναδική της λύση. Τότε

$$b f(x) = b a_n x^n + \dots + b a_0 \equiv$$

$$\equiv x^n + b(a_{n-1} x^{n-1} + \dots + a_0) \pmod p \text{ ταυτοτικά.}$$

Αν $g(x) = x^n + b(a_{n-1} x^{n-1} + \dots + a_0)$ έχουμε

$$b f(x) \equiv g(x) \pmod p \text{ ταυτοτικά.}$$

Από το πόρισμα 2.4 έχουμε ότι οι πολυωνυμικές ισοτιμίες

i) $f(x) \equiv 0 \pmod p$ και ii) $g(x) \equiv 0 \pmod p$

είναι ισοδύναμες. Αν η i) έχει ακριβώς η διακεκριμένες λύσεις, τότε και η ii) θα έχει ακριβώς η διακεκριμένες λύσεις και επομένως σύμφωνα με την Πρόταση 3.2

$$x^p - x \equiv g(x) q(x) \pmod p \text{ ταυτοτικά}$$

Άρα $b \cdot f(x) q(x) \equiv g(x) q(x) \equiv x^p - x \pmod p$ ταυτοτικά

δηλαδή $x^p - x \equiv f(x) \cdot (b \cdot q(x)) \pmod p$ ταυτοτικά

όπως επιδιώκουμε.

Το αντίστροφο, όπως και στην πρόταση 3.2. ■

4. Πολυωνυμικές ισοτιμίες με μέτρο δύναμη πρώτου αριθμού

4.1 Σχηματική παράγωγος πολυωνύμου - Τύπος του Taylor

Ας είναι $f(x)=a_0+a_1x+\cdots+a_nx^n$, $n\geq 1$ ένα πολυώνυμο με πραγματικούς συντελεστές.

Ονομάζουμε **σχηματική (ή τυπική) παράγωγο** του $f(x)$, το πολυώνυμο

$$f'(x)=a_1+2a_2x+3a_3x^2+\cdots+na_nx^{n-1}$$

Στην περίπτωση που το $f(x)$ είναι μια σταθερά, δηλαδή αν $f(x)=a_0$, ορίζουμε $f'(x)=0$.

Είναι φανερό ότι η πολυωνυμική συνάρτηση που αντιστοιχεί στο $f'(x)$ είναι η παράγωγος (με την συνηθισμένη έννοια της Ανάλυσης) της πολυωνυμικής συνάρτησης που αντιστοιχεί στο $f(x)$. Η λέξη "σχηματική" δίνει έμφαση στο γεγονός ότι στον ορισμό του $f'(x)$ δεν γίνεται χρήση της έννοιας του ορίου.

Αν $f(x),g(x)\in\mathbb{R}[x]$ και $\lambda\in\mathbb{R}$ τότε ισχύουν τα εξής:

$$(\lambda f(x))'=\lambda\cdot f'(x)$$
$$(f(x)+g(x))'=f'(x)+g'(x)$$
$$(f(x)\cdot g(x))'=f'(x)\cdot g'(x)$$

Ορίζουμε επαγωγικά την (k)-τάξης σχηματική παράγωγο $f^{(k)}(x)$ του πολυωνύμου $f(x)$ ως εξής:

$$f^{(0)}(x)=f(x)\ ,\quad f^{(1)}(x)=f'(x)\ ,\ \ldots\ ,\quad f^{(k)}(x)=\left(f^{(k-1)}(x)\right)'.$$

Αν $u \in \mathbb{R}$, τότε απο τον γνωστό τύπο του Taylor για το $f(x)$ έχουμε

$$f(x+u) = f(u) + \frac{f'(u)}{1!}x + \frac{f^{(2)}(u)}{2!}x^2 + \cdots + \frac{f^{(n)}(u)}{n!}x^n = \sum_{k=0}^{n} \frac{f^{(k)}(u)}{k!}x^k.$$

Εύκολα διαπιστώνεται ότι

$$f^{(k)}(x) = \sum_{i=k}^{n} i(i-1)\cdots(i-k+1)\,a_i x^{i-k}$$

και επομένως

$$\frac{f^{(k)}(u)}{k!} = \sum_{i=k}^{n} \frac{i(i-1)\cdots(i-k+1)}{k!}a_i u^{i-k} = \sum_{i=k}^{n}\binom{i}{k}a_i u^{i-k}.$$

Αν τώρα το πολυώνυμο $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ βαθμού n και $u \in \mathbb{Z}$, τότε οι συντελεστές

$\frac{f^{(k)}(u)}{k!} \in \mathbb{Z}$ και επομένως το πολυώνυμο

$$f(x+u) = \sum_{k=0}^{n} \frac{f^{(k)}(u)}{k!}x^k \in \mathbb{Z}[x].$$

Άρα για ακεραίους x_0, u το

$f(x_0+u) = \sum_{k=0}^{n} \frac{f^{(k)}(u)}{k!}x_0^k$ είναι ακέραιος.

4.2 Επίλυση της $f(x) \equiv 0 \pmod{p^s}$.

Θεωρούμε την πολυωνυμική ισοτιμία

$$f(x) \equiv 0 \pmod{p^s} \qquad (1)$$

όπου $f(x)$ πολυώνυμο με ακέραιους συντελεστές, p πρώτος και s θετικός ακέραιος.

Παίρνουμε τώρα το $S \geq 2$ και ερευνούμε τη σχέση μεταξύ των λύσεων της (1) και της πολυωνυμικής ισοτιμίας

$$f(x) \equiv 0 \pmod{p^{S-1}} \qquad (2)$$

Αν η κλάση $a \pmod{p^S}$ είναι μια λύση της (1) τότε $f(a) \equiv 0 \pmod{p^S}$ απ' όπου $f(a) \equiv 0 \pmod{p^{S-1}}$. Επομένως η κλάση $a \pmod{p^{S-1}}$ είναι λύση της (2).

Το αντίστροφο δεν αληθεύει γενικά, αφού κάθε ακέραιος που επαληθεύει την (2) δεν επαληθεύει υποχρεωτικά και την (1). Αλλά αν η (2) δεν έχει λύσεις τότε και η (1) δεν έχει λύσεις.

Θα δείξουμε στα επόμενα ότι <u>αν γνωρίζουμε όλες τις λύσεις της (2) μπορούμε να υπολογίσουμε όλες τις λύσεις της (1)</u>

Ας είναι η κλάση $b \pmod{p^{S-1}}$ μια λύση της (2). Τότε όλοι οι ακέραιοι της μορφής $b + tp^{S-1}$ επαληθεύουν την (2).

Το ερώτημα είναι κάτω από ποιές συνθήκες ένας από τους ακέραιους $b + tp^{S-1}$ είναι λύση της (1). Θα βρούμε λοιπόν για ποιές τιμές του t, αν υπάρχουν, ο ακέραιος $b + tp^{S-1}$ επαληθεύει την πολυωνυμική ισοτιμία (1) δηλαδή είναι

$$f(b + tp^{S-1}) \equiv 0 \pmod{p^S}.$$

Απάντηση σ' αυτό δίνει το επόμενο λήμμα.

ΛΗΜΜΑ 4.1

Ας είναι $f(x) \in \mathbb{Z}[x]$ με $\deg f(x) = n$, p πρώτος, S φυσικός $S \geq 2$ και έστω $b \pmod{p^{S-1}}$ μια λύση της πολυωνυμικής ισοτιμίας

$$f(x) \equiv 0 \pmod{p^{S-1}} \qquad (2)$$

Η κλάση $b + tp^{S-1} \pmod{p^S}$ είναι λύση της πολυωνυμικής ισοτιμίας

$$f(x) \equiv 0 \pmod{p^S} \qquad (1)$$

αν και μόνο αν η κλάση $t \pmod p$ είναι λύση της γραμμικής ισοτιμίας

$$f'(b)\,t \equiv -\frac{f(b)}{p^{s-1}} \pmod p \qquad (3)$$

Απόδειξη.

Ας είναι η κλάση $b + tp^{s-1} \pmod{p^s}$ λύση της (1). Τότε

$$f(b+tp^{s-1}) \equiv 0 \pmod{p^s} \qquad (4)$$

Από τον τύπο του Taylor έχουμε

$$f(b+tp^{s-1}) = f(b) + f'(b)tp^{s-1} + \frac{f''(b)}{2!}(tp^{s-1})^2 + \cdots + \frac{f^{(n)}(b)}{n!}(tp^{s-1})^n$$

Αλλά για $s \geqslant 2$ είναι $2s-2 = s+(s-2) \geqslant s$, επομένως για κάθε $\kappa \geqslant 2$ έχουμε $p^{\kappa s-\kappa} \geqslant p^s$. Έτσι

$$f(b+tp^{s-1}) = f(b) + f'(b)tp^{s-1} + Ap^s \quad , \ A \text{ ακέραιος}$$

δηλαδή, $$f(b+tp^{s-1}) \equiv f(b) + f'(b)tp^{s-1} \pmod{p^s}$$

η οποία σε συνδιασμό με την (4) μας δίνει

$$f(b) + f'(b)tp^{s-1} \equiv 0 \pmod{p^s}.$$

Αλλά $f(b) \equiv 0 \pmod{p^{s-1}}$ δηλαδή $p^{s-1} \mid f(b)$, επομένως

$$p^{s-1}\left(\frac{f(b)}{p^{s-1}} + f'(b)\,t\right) \equiv 0 \pmod{p^s}$$

Άρα $$f'(b)t \equiv -\frac{f(b)}{p^{s-1}} \pmod p$$

δηλαδή η κλάση $t \pmod p$ είναι λύση της (3).

Αντίστροφα, αν $f(b) \equiv 0 \pmod{p^{s-1}}$ και η κλάση $t \pmod p$ είναι λύση της (3), τότε θα είναι

$$f'(b)t \equiv -\frac{f(b)}{p^{s-1}} \pmod p$$

Επομένως, $$f'(b)tp^{s-1} \equiv -\frac{f(b)}{p^{s-1}}p^{s-1} \pmod{p\cdot p^{s-1}}$$

δηλαδή $f(b) + f'(b)t p^{s-1} \equiv 0 \pmod{p^s}$.

Από τον τύπο του Taylor παίρνουμε τώρα ότι

$$f(b + tp^{s-1}) \equiv f(b) + f'(b)t p^{s-1} \equiv 0 \pmod{p^s}.$$

Ο ακέραιος $b + tp^{s-1}$ λοιπόν επαληθεύει την (1) δηλαδή η κλάση $b + tp^{s-1} \pmod{p^s}$ είναι λύση της (1). ∎

Ο επόμενος ορισμός θα διευκολύνει την παρουσίαση του κεντρικού θεωρήματος.

Ορισμός

Έστω $b \pmod{p^{s-1}}$ μια λύση της πολυωνυμικής ισοτιμίας

$$f(x) \equiv 0 \pmod{p^{s-1}} \qquad (2)$$

Μια λύση $a \pmod{p^s}$ της πολυωνυμικής ισοτιμίας

$$f(x) \equiv 0 \pmod{p^s} \qquad (1)$$

καλείται **αντίστοιχη** της $b \pmod{p^{s-1}}$ αν

$$a \equiv b \pmod{p^{s-1}}$$

δηλαδή αν $a = b + tp^{s-1}$ για κάποιο ακέραιο t.

Από το Λήμμα 4.1 έχουμε επομένως ότι υπάρχουν λύσεις της (1) αντίστοιχες της λύσης $b \pmod{p^{s-1}}$ της (2) αν και μόνο αν η γραμμική ισοτιμία (3) έχει λύσεις.

Από την άλλη μεριά παρατηρούμε ότι κάθε λύση $a \pmod{p^s}$ της (1) είναι αντίστοιχη της λύσης $a \pmod{p^{s-1}}$ της (2).

Πραγματικά, αν $f(a) \equiv 0 \pmod{p^s}$ τότε $f(a) \equiv 0 \pmod{p^{s-1}}$ και $a \equiv a \pmod{p^{s-1}}$.

Η σχέση μεταξύ των λύσεων των πολυωνυμικών ισοτιμιών (1) και (2) περιγράφεται στο επόμενο θεώρημα.

Θεώρημα 4.1

Έστω $f(x)$ ένα πολυώνυμο με ακέραιους συντελεστές, p πρώτος και s φυσικός, $s \geq 2$.

Αν $b \pmod{p^{s-1}}$ είναι μια λύση της πολυωνυμικής ισοτιμίας

$$f(x) \equiv 0 \pmod{p^{s-1}} \qquad (2)$$

τότε

i) Αν $f'(b) \not\equiv 0 \pmod{p}$,

τότε υπάρχει μοναδική λύση της πολυωνυμικής ισοτιμίας

$$f(x) \equiv 0 \pmod{p^s} \qquad (1)$$

που αντιστοιχεί στη λύση $b \pmod{p^{s-1}}$ η

$$a = b + t p^{s-1} \pmod{p^s}$$

όπου t ένας ακέραιος που επαληθεύει την γραμμική ισοτιμία

$$f'(b)t \equiv -\frac{f(b)}{p^{s-1}} \pmod{p}. \qquad (3)$$

ii) Αν $f'(b) \equiv 0 \pmod{p}$. Τότε

ii_1) Αν $f(b) \equiv 0 \pmod{p^s}$,
υπάρχουν p λύσεις της (1) που αντιστοιχούν στην $b \pmod{p^{s-1}}$ οι

$$a_t = b + t p^{s-1} \pmod{p^s}, \quad t = 0, 1, \dots, p-1.$$

ii_2) Αν $f(b) \not\equiv 0 \pmod{p^s}$,
δεν υπάρχει καμμία τέτοια λύση.

Απόδειξη.

i) Αφού $f'(b) \not\equiv 0 \pmod{p}$ θα είναι $(f'(b), p) = 1$. Επομένως η γραμμική ισοτιμία

$$f'(b)t \equiv -\frac{f(b)}{p^{s-1}} \pmod{p}$$

έχει μοναδική λύση $t \pmod{p}$. Από το λήμμα 4.1 έχουμε ότι υπάρχει μοναδική λύση της (1) η

$$b + t p^{s-1} \pmod{p^s}.$$

ii) Αφού $f'(b) \equiv 0 \pmod p$, θα είναι $(f'(b), p) = p$ και επομένως,

ii_2) Αν $f(b) \not\equiv 0 \pmod{p^s}$ τότε $p \nmid \frac{f(b)}{p^{s-1}}$, άρα η γραμμική ισοτιμία (3) δεν έχει λύση, με αποτέλεσμα να μην υπάρχει λύση της (1) που να αντιστοιχεί στην λύση $b \pmod{p^s}$ σύμφωνα με το λήμμα 4.1.

ii_1) Αν $f(b) \equiv 0 \pmod{p^s}$ τότε $p \mid \frac{f(b)}{p^{s-1}}$ και επομένως η γραμμική ισοτιμία (3) έχει p ανισότιμες $\pmod p$ λύσεις τις $0 \pmod p, 1 \pmod p, \dots, (p-1) \pmod p$. Σύμφωνα με το λήμμα 4.1 η (1) έχει τις επόμενες λύσεις που αντιστοιχούν στην $b \pmod{p^s}$

$$a_t \equiv b + t p^{s-1} \pmod{p^s}, \quad t = 0, 1, \dots, p-1.$$

Οι λύσεις αυτές είναι ανά δύο ανισότιμες $\pmod{p^s}$. Πραγματικά αν

$$a_\mu \equiv a_\nu \pmod{p^s} \quad \text{με } \mu \neq \nu$$

δηλαδή αν

$$b + \mu p^{s-1} \equiv b + \nu p^{s-1} \pmod{p^s}$$

τότε

$$\mu p^{s-1} \equiv \nu p^{s-1} \pmod{p^s}$$

άρα

$$\mu \equiv \nu \pmod p,$$

άτοπο, αφού $\mu, \nu \in \{0, 1, \dots, p-1\}$ και $\mu \neq \nu$.

Έτσι υπάρχουν ακριβώς p ανισότιμες ανά δύο λύσεις της (1) που αντιστοιχούν στην λύση $b \pmod{p^{s-1}}$. ■

Στην αναζήτηση των λύσεων

Γνωρίζουμε ότι κάθε λύση $a \pmod{p^s}$ της (1) είναι αντίστοιχη της λύσης $a \pmod{p^{s-1}}$ της (2).

Από την άλλη μεριά, σύμφωνα με το θεώρημα 4.1 από κάθε λύση $b \pmod{p^{s-1}}$ της (2) μπορούμε να έχουμε, καμμιά, ή μία ακριβώς ή p ακριβώς ανισότιμες $\pmod{p^s}$ λύσεις

της (1) που αντιστοιχούν στη λύση $b \pmod{p^{s-1}}$ της (2).

Επιπλέον, αν είναι $b \pmod{p^{s-1}}$ και $b' \pmod{p^{s-1}}$ δυο διαφορετικές λύσεις της (2) (δηλαδή $b \not\equiv b' \pmod{p^{s-1}}$) και

$$b + tp^{s-1} \pmod{p^s} \quad \text{και} \quad b' + t'p^{s-1} \pmod{p^s}$$

δυο τυχούσες λύσεις της (1) που αντιστοιχούν σ'αυτές, αντίστοιχα. Τότε και οι λύσεις αυτές είναι διαφορετικές, δηλαδή

$$b + tp^{s-1} \not\equiv b' + t'p^{s-1} \pmod{p^s}.$$

Πραγματικά, αν

$$b + tp^{s-1} \equiv b' + t'p^{s-1} \pmod{p^s} \quad \text{τότε}$$

$$b + tp^{s-1} \equiv b' + t'p^{s-1} \pmod{p^{s-1}}, \text{ δηλαδή}$$

$$b - b' \equiv (t' - t)p^{s-1} \pmod{p^{s-1}}.$$

Αλλά $(t - t')p^{s-1} \equiv 0 \pmod{p^{s-1}}$. άρα

$$b - b' \equiv 0 \pmod{p^{s-1}}, \text{ δηλαδή}$$

$$b \equiv b' \pmod{p^{s-1}} \quad \text{άτοπο.}$$

Επομένως, <u>αν γνωρίζουμε όλες τις λύσεις της πολυωνυμικής ισοτιμίας</u>

$$f(x) \equiv 0 \pmod{p^{s-1}}$$

<u>μπορούμε να υπολογίσουμε όλες τις λύσεις της πολυωνυμικής ισοτιμίας</u>

$$f(x) \equiv 0 \pmod{p^s}.$$

Με επαναληπτική εφαρμογή αυτής της μεθόδου η επίλυση της πολυωνυμικής ισοτιμίας

$$f(x) \equiv 0 \pmod{p^s} \qquad (1)$$

ανάγεται στην επίλυση της πολυωνυμικής ισοτιμίας

$$f(x) \equiv 0 \pmod{p} \qquad (4).$$

Αν η (4) δεν έχει λύσεις, τότε και η (1) δεν έχει λύσεις. Αν η (4) έχει λύσεις και καμμιά απ'αυτές δεν μας παρέ-

και αντίστοιχες λύσεις της

$$f(x) \equiv 0 \pmod{p^2} \qquad (5)$$

τότε η (5) δεν έχει λύσεις και επομένως και η (1) δεν έχει λύσεις.

Από τις λύσεις της (4) που μας δίνουν αντίστοιχες λύσεις της (5) βρίσκουμε όλες τις λύσεις της (5).

Για κάθε λύση της (5) χρησιμοποιούμε παρόμοια διαδικασία για να βρούμε τις λύσεις της

$$f(x) \equiv 0 \pmod{p^3}$$

και ούτω καθ' εξής, μέχρι να βρεθούν όλες οι λύσεις της (1).

Η διαδικασία αυτή γίνεται περισσότερο αντιληπτή μέσα από τα παραδείγματα που θα ακολουθήσουν, μετά από το επόμενο πόρισμα.

Πόρισμα 4.1

Για κάθε φυσικό s, η πολυωνυμική ισοτιμία

$$f(x) = x^{p-1} - 1 \equiv 0 \pmod{p^s}$$, p πρώτος

έχει ακριβώς $p-1$ διαφορετικές λύσεις $\pmod{p^s}$.

Απόδειξη

Θα εργασθούμε επαγωγικά. Για $s=1$ έχουμε την πολυωνυμική ισοτιμία $f(x) = x^{p-1} - 1 \equiv 0 \pmod{p}$ η οποία έχει $p-1$ διαφορετικές λύσεις $\pmod{p}$ τις $x \equiv 1 \pmod{p}, \ldots, x \equiv p-1 \pmod{p}$, σύμφωνα με το Θεώρημα Fermat.

Υποθέτουμε ότι η πολυωνυμική ισοτιμία

$$f(x) = x^{p-1} - 1 \equiv 0 \pmod{p^{s-1}}$$

έχει $p-1$ ακριβώς διαφορετικές λύσεις $\pmod{p^{s-1}}$.

Αν $b \pmod{p^{s-1}}$ είναι μία απ' αυτές θα έχουμε

$f(b) = b^{p-1} - 1 \equiv 0 \pmod{p^{s-1}}$ οπότε $b \not\equiv 0 \pmod{p^{s-1}}$

Είναι $f'(x) = (p-1)x^{p-2}$ άρα

$$f'(b) = (p-1)b^{p-2} \not\equiv 0 \pmod{p}$$

Σύμφωνα με το θεώρημα 4.1 υπάρχει μοναδική λύση της πολυωνυμικής ισοτιμίας $f(x) = x^{p-1} - 1 \equiv 0 \pmod{p^s}$ που αντιστοιχεί στη λύση $b \pmod{p^{s-1}}$. Επειδή σε διαφορετικές λύσεις της $f(x) = x^{p-1} - 1 \equiv 0 \pmod{p^{s-1}}$ αντιστοιχούν διαφορετικές λύσεις της $f(x) = x^{p-1} - 1 \equiv 0 \pmod{p^s}$, η τελευταία έχει ακριβώς $p-1$ διαφορετικές λύσεις $\pmod{p^s}$.

Η αρίθμηση των εξισώσεων στα παραδείγματα που ακολουθούν αφορούν τα συγκεκριμένα παραδείγματα και μόνον.

Παράδειγμα 4.1

Θα επιλύσουμε την πολυωνυμική ισοτιμία

$$f(x) = x^2 + x + 7 \equiv 0 \pmod{3^4}$$

Είναι $f'(x) = 2x + 1$

b_1) Εύκολα βρίσκουμε με δοκιμή ότι η πολυωνυμική ισοτιμία

$$f(x) = x^2 + x + 7 \equiv 0 \pmod{3} \qquad (1)$$

έχει μοναδική λύση την $x \equiv 1 \pmod{3}$.

b_2) Οι λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = x^2 + x + 7 \equiv 0 \pmod{3^2} \qquad (2)$$

είναι οι λύσεις της (2) που αντιστοιχούν στη λύση $x \equiv 1 \pmod{3}$ της (1). Αφού $f'(1) = 3 \equiv 0 \pmod{3}$ και $f(1) = 9 \equiv 0 \pmod{3^2}$ η (2) έχει τρεις λύσεις τις

$$1 + 3t \pmod{3^2}, \quad t = 0, 1, 2$$

δηλαδή τις $x \equiv 1 \pmod{3^2}$, $x \equiv 4 \pmod{3^2}$, $x \equiv 7 \pmod{3^2}$

b_3) Βρίσκουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = x^2 + x + 7 \equiv 0 \pmod{3^3} \qquad (3)$$

που αντιστοιχούν σε εις λύσεις της (2).

i) Αφού $f'(1) \equiv 0 \pmod{3}$ και $f(1) = 9 \not\equiv 0 \pmod{3^3}$ δεν υπάρχει λύση της (3) αντίστοιχη της λύσης $x \equiv 1 \pmod{3^2}$ της (2).

ii) Αφου $f'(4)=9\equiv 0 \pmod 3$ και $f(4)=27\equiv 0 \pmod{3^3}$
η (3) έχει τρεις λύσεις τις

$$4+3^2t \pmod{3^3}, \quad t=0,1,2$$

δηλαδή τις $x\equiv 4 \pmod{3^3}$, $x\equiv 13 \pmod{3^3}$, $x\equiv 22 \pmod{3^3}$
που αντιστοιχούν στη λύση $x\equiv 4 \pmod{3^2}$ της (2).
iii) Αφού $f'(7)=15\equiv 0 \pmod 3$ και $f(7)=63\not\equiv 0 \pmod{3^3}$
δεν υπάρχουν λύσεις της (3) αντίστοιχες της λύσης
$x\equiv 7 \pmod{3^2}$ της (2). Έτσι η (3) έχει τις λύσεις

$$x\equiv 4 \pmod{3^3}, \quad x\equiv 13 \pmod{3^3}, \quad x\equiv 22 \pmod{3^3}.$$

b_4) Βρίσκουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x)=x^2+x+7\equiv 0 \pmod{3^4} \qquad (4)$$

που αντιστοιχούν στις λύσεις τις (3).
Αφου $f'(4)=9\equiv 0 \pmod 3$, $f'(13)=27\equiv 0 \pmod 3$,
$f'(22)=45\equiv 0 \pmod 3$ και

$$f(4)=27\not\equiv 0 \pmod{3^4}, \quad f(13)=189\not\equiv 0 \pmod{3^4}$$
$$f(22)=513\not\equiv 0 \pmod{3^4}$$

η (4) δεν έχει λύσεις που αντιστοιχούν στις λύσεις της (3) επομένως η (4) δεν έχει λύσεις.

Παράδειγμα 4.2.

Θα επιλύσουμε την πολυωνυμική ισοτιμία

$$f(x)=2x^2-3x-1\equiv 0 \pmod{2^2}.$$

Είναι $f'(x)=4x-3$.
b_1) Η πολυωνυμική ισοτιμία

$$f(x)=2x^2-3x-1\equiv 0 \pmod 2 \qquad (1)$$

έχει μοναδική λύση την $x\equiv 1 \pmod 2$.
b_2) Οι λύσεις της πολυωνυμικής ισοτιμίας

$$f(x)=2x^2-3x-1\equiv 0 \pmod{2^2} \qquad (2)$$

είναι οι λύσεις της που αντιστοιχούν στη λύση $x \equiv 1 \pmod 2$ της (1).

Αφού $f'(1) = 1 \not\equiv 0 \pmod 2$ η (2) έχει μοναδική λύση

$$1 + t \cdot 2 \pmod{2^2}$$

όπου t ακέραιος που ικανοποιεί την γραμμική ισοτιμία

$$f'(1)\, t \equiv -\frac{f(1)}{2} \pmod 2$$

δηλαδή την

$$t \equiv 1 \pmod 2$$

Άρα η (2) έχει την μοναδική λύση $x \equiv 1 + 1 \cdot 2 = 3 \pmod{2^2}$.

Παράδειγμα 4.3

Να επιλυθεί η πολυωνυμική ισοτιμία

$$f(x) = 2x^2 - 3x - 1 \equiv 0 \pmod{19^2}.$$

Είναι $f'(x) = 4x - 3$.

b_1) Με δοκιμή διαπιστώνουμε ότι οι λύσεις της

$$f(x) = 2x^2 - 3x - 1 \equiv 0 \pmod{19} \qquad (1)$$

είναι οι $x \equiv 4 \pmod{19}$ και $x \equiv 7 \pmod{19}$.

b_2) Βρίσκουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = 2x^2 - 3x - 1 \equiv 0 \pmod{19^2} \qquad (2)$$

που αντιστοιχούν στις δύο λύσεις της (1).

i) Αφού $f'(4) = 13 \not\equiv 0 \pmod{19}$ η (2) έχει μοναδική λύση την

$$x \equiv 4 + 19 \cdot t \pmod{19^2}$$

που αντιστοιχεί στην λύση $x \equiv 4 \pmod{19}$ της (1) όπου t ακέραιος που επαληθεύει την γραμμική ισοτιμία

$$f'(4)\, t \equiv -\frac{f(4)}{19} \pmod{19}$$

δηλαδή την $13t \equiv -1 \pmod{19}$

που έχει μοναδική λύση την $t \equiv 16 \pmod{19}$

Άρα η ζητούμενη λύση είναι η

$$x \equiv 4 + 19 \cdot 16 = 308 \pmod{19^2}.$$

ii) Αφού $f'(7)=25\not\equiv 0 \pmod{19}$ η (2) έχει μοναδική λύση την $x\equiv 7+19t \pmod{19^2}$ όπου t ακέραιος που επαληθεύει την γραμμική ισοτιμία

$$f'(7)\,t \equiv -\frac{f(7)}{19} \pmod{19}$$

δηλαδή την $25t\equiv -4 \pmod{19}$
που έχει μοναδική λύση την $t\equiv 12 \pmod{19}$.
Άρα η ζητούμενη λύση είναι η

$$x\equiv 7+19\cdot 12 = 235 \pmod{19^2}.$$

Επομένως η (2) έχει δυό λύσεις, τις

$$x\equiv 308 \pmod{19^2} \quad \text{και} \quad x\equiv 235 \pmod{19^2}.$$

Παράδειγμα 4.4

Θα βρούμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x)=x^3+4x^2+3\equiv 0 \pmod{2^3}.$$

Είναι $f'(x)=3x^2+8x$

b_1) Η πολυωνυμική ισοτιμία

$$f(x)=x^3+4x^2+3\equiv 0 \pmod{2} \qquad (1)$$

έχει μοναδική λύση την $x\equiv 1 \pmod{2}$.

b_2) Βρίσκουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x)=x^3+4x^2+3\equiv 0 \pmod{2^2} \qquad (2)$$

που αντιστοιχούν στην λύση $x\equiv 1 \pmod{2}$ της (1).
Αφού $f'(1)=11\not\equiv 0 \pmod{2}$ η (2) έχει μοναδική λύση

$$1+2t \pmod{2^2}$$

που αντιστοιχεί στην λύση $x\equiv 1 \pmod{2}$ της (1), όπου t ακέραιος που επαληθεύει την γραμμική ισοτιμία

$$f'(1)\,t \equiv -\frac{f(1)}{2} \pmod{2}$$

δηλαδή την $11t\equiv -4 \pmod{2}$
που έχει μοναδική λύση την $t\equiv 0 \pmod{2}$.

Άρα η μοναδική λύση της (2) είναι η

$$x \equiv 1 + 2 \cdot 0 = 1 \pmod{2^2}.$$

β_3) Βρίσκουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = x^3 + 4x^2 + 3 \equiv 0 \pmod{2^3} \qquad (3)$$

που αντιστοιχούν στην λύση $x \equiv 1 \pmod{2^2}$ της (2)

Αφού $f'(1) = 11 \not\equiv 0 \pmod 2$ η (3) έχει μοναδική λύση

$$x \equiv 1 + t \cdot 2^2 \pmod{2^3}$$

όπου t ακέραιος που επαληθεύει την γραμμική ισοτιμία

$$f'(1)\, t \equiv -\frac{f(1)}{2^2} \pmod 2$$

δηλαδή την $11t \equiv -2 \pmod 2$,

που έχει μοναδική λύση την $t \equiv 0 \pmod 2$

Άρα η (3) έχει μοναδική λύση την

$$x \equiv 1 + 0 \cdot 2^2 = 1 \pmod{2^3}.$$

(Παρατήρηση. Επειδή το μέτρο $2^3 = 8$ είναι μικρό, μπορούμε και με δοκιμή να βρούμε ότι η (1) έχει μοναδική λύση την $x \equiv 1 \pmod{2^3}$.).

Παράδειγμα 4.5

Θα επιλύσουμε την πολυωνυμική ισοτιμία

$$f(x) = x^3 + 4x^2 + 3 \equiv 0 \pmod{3^4}.$$

Είναι $f'(x) = 3x^2 + 8x$

β_1) Η πολυωνυμική ισοτιμία

$$f(x) = x^3 + 4x^2 + 3 \equiv 0 \pmod 3 \qquad (1)$$

έχει δυο λύσεις τις $x \equiv 0 \pmod 3$ και $x \equiv 2 \pmod 3$.

β_2) Βρίσκουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = x^3 + 4x^2 + 3 \equiv 0 \pmod{3^2} \qquad (2)$$

που αντιστοιχούν στις δυο λύσεις της (1).

i) Αφού $f'(0) \equiv 0 \pmod 3$ και $f(0) = 3 \not\equiv 0 \pmod{3^2}$

δεν υπάρχει λύση της (2) αντίστοιχη της $x \equiv 0 \pmod 3$.

ii) Αφού $f'(2) = 28 \not\equiv 0 \pmod 3$ βρίσκουμε ότι η (2) έχει μοναδική λύση που αντιστοιχεί στην $x \equiv 2 \pmod 3$ της (1) την $x \equiv 2 \pmod{3^2}$.

β_3) Βρίσκουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = x^3 + 4x^2 + 3 \equiv 0 \pmod{3^3} \qquad (3)$$

που αντιστοιχούν στην λύση $x \equiv 2 \pmod{3^2}$ της (2).

Αφού $f'(2) = 28 \not\equiv 0 \pmod 3$ βρίσκουμε ότι η (3) έχει μοναδική λύση την $x \equiv 2 \pmod{3^3}$.

β_4) Βρίσκουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = x^3 + 4x^2 + 3 \equiv 0 \pmod{3^4} \qquad (4)$$

που αντιστοιχούν στην μοναδική λύση της (3).

Αφού $f'(2) = 28 \not\equiv 0 \pmod 3$ βρίσκουμε ότι η (4) έχει μοναδική λύση την $x \equiv 56 \pmod{3^4}$.

Παράδειγμα 4.6

Θα βρούμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = x^3 + 4x^2 + 3 \equiv 0 \pmod{11^2}.$$

Είναι $f'(x) = 3x^2 + 8x$

β_1) Με δοκιμή βρίσκουμε ότι η πολυωνυμική ισοτιμία

$$f(x) = x^3 + 4x^2 + 3 \equiv 0 \pmod{11} \qquad (1)$$

έχει τρεις λύσεις, τις

$$x \equiv 3 \pmod{11}, \quad x \equiv 6 \pmod{11}, \quad x \equiv 9 \pmod{11}$$

β_2) Όμοια εργαζόμενοι όπως και στα προηγούμενα παραδείγματα, βρίσκουμε ότι η δοθείσα πολυωνυμική ισοτιμία έχει τρεις λύσεις, τις

$$x \equiv 80 \pmod{11^2}, \quad x \equiv 6 \pmod{11^2}, \quad x \equiv 31 \pmod{11^2}.$$

Παράδειγμα 4.7

Θα επιλύσουμε την πολυωνυμική ισοτιμία

$$f(x) = x^3 + 2x - 3 \equiv 0 \pmod{5^3}.$$

Είναι $f'(x) = 3x^2 + 2$.

β_1) Οι λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = x^3 + 2x - 3 \equiv 0 \pmod 5 \qquad (1)$$

είναι $x \equiv 1 \pmod 5$ και $x \equiv 3 \pmod 5$.

β_2) Βρίσκουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = x^3 + 2x - 3 \equiv 0 \pmod{5^2} \qquad (2)$$

που αντιστοιχούν στις δυο λύσεις της (1).

i) Αφού $f'(1) = 5 \equiv 0 \pmod 5$ και $f(1) \equiv 0 \pmod{5^2}$. υπάρχουν πέντε λύσεις της (2), που αντιστοιχούν στην λύση $x \equiv 1 \pmod 5$ της (1), οι εξής:

$$a_t = 1 + t \cdot 5 \pmod{5^2}, \quad t = 0, 1, 2, 3, 4$$

δηλαδή οι

$x \equiv 1 \pmod{5^2}$, $x \equiv 6 \pmod{5^2}$, $x \equiv 11 \pmod{5^2}$

$x \equiv 16 \pmod{5^2}$ και $x \equiv 21 \pmod{5^2}$.

ii) Αφού $f'(3) = 29 \not\equiv 0 \pmod 5$ η (2) έχει μοναδική λύση την $x \equiv 3 + 5t \pmod{5^2}$

που αντιστοιχεί στην λύση $x \equiv 3 \pmod 5$ της (1), όπου t ακέραιος που επαληθεύει την γραμμική ισοτιμία

$$29t \equiv -6 \pmod 5$$

που έχει μοναδική λύση την $t \equiv 1 \pmod 5$. Άρα η ζητούμενη λύση είναι η $x \equiv 3 + 5 \cdot 1 \equiv 8 \pmod{5^2}$.

Οι λύσεις της (2) είναι λοιπόν οι

$$x \equiv 1, 6, 8, 11, 16, 21 \pmod{5^2}.$$

β_3) Βρίσκουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = x^3 + 2x - 3 \equiv 0 \pmod{5^2} \qquad (3)$$

που αντιστοιχούν στις λύσεις $x \equiv 1,6,8,11,16,21 \pmod{5^2}$ της (2).

α) Αφού

$f'(6) = 110 \equiv 0 \pmod 5$ και $f(6) = 285 \not\equiv 0 \pmod{5^3}$

$f'(11) = 365 \equiv 0 \pmod 5$ και $f(11) = 1350 \not\equiv 0 \pmod{5^3}$

$f'(21) = 1325 \equiv 0 \pmod 5$ και $f(21) = 9.300 \not\equiv 0 \pmod{5^3}$

δεν υπάρχουν λύσεις της (3) που να αντιστοιχούν στις λύσεις $x \equiv 6, 11, 21 \pmod{5^2}$ της (2).

b) Αφού $f'(1) = 5 \equiv 0 \pmod 5$ και $f(1) \equiv 0 \pmod{5^2}$

η (3) έχει πέντε λύσεις τις

$$x \equiv 1 + t\,5^2 \pmod{5^3} \quad , t = 0,1,2,3,4$$

δηλαδή τις

$$x \equiv 1, 26, 51, 76, 101 \pmod{5^3}.$$

που αντιστοιχούν στην λύση $x \equiv 1 \pmod{5^2}$ της (2).

c) Αφού $f'(16) = 770 \equiv 0 \pmod 5$ και $f(16) = 4.165 \equiv 0 \pmod{5^3}$

η (3) έχει πέντε λύσεις τις

$$x \equiv 16 + t \cdot 5^2 \pmod{5^3} \quad , \quad t = 0,1,2,3,4$$

δηλαδή τις

$$x \equiv 16, 41, 66, 91, 116 \pmod{5^3}.$$

που αντιστοιχούν στην λύση $x \equiv 16 \pmod{5^2}$ της (2).

d) Αφού $f'(8) = 194 \not\equiv 0 \pmod 5$ η (3) έχει μοναδική λύση την

$$x \equiv 8 + t \cdot 5^2 \pmod{5^3}$$

που αντιστοιχεί στην λύση $x \equiv 8 \pmod{5^2}$, όπου t ακέραιος που επαληθεύει την γραμμική ισοτιμία

$$194 \cdot t \equiv -21 \pmod 5$$

που έχει μοναδική λύση την $t \equiv 1 \pmod 5$

Άρα η $x \equiv 8 + 1 \cdot 5^2 = 33 \pmod{5^3}$ είναι η ζητούμενη

λύση της (3).

Η (3) έχει λοιπόν τις παρακάτω λύσεις

$x \equiv 1, 16, 26, 33, 41, 51, 66, 91, 101, 116 \pmod{5^3}$.

5. Πολυωνυμικές ισοτιμίες με μέτρα σύνθετους φυσικούς αριθμούς

Δεν υπάρχει μια γενική μέθοδος για το πρόβλημα της επίλυσης πολυωνυμικής ισοτιμίας με μέτρο σύνθετο φυσικό αριθμό. Στην παράγραφο αυτή θα δούμε ότι το πρόβλημα αυτό ανάγεται τελικά σε αντίστοιχα προβλήματα με μέτρα πρώτους αριθμούς και ενός συνόλου συστημάτων γραμμικών ισοτιμιών.

Σε ότι ακολουθεί θα συμβολίζουμε με $N(m)$ το πλήθος των διαφορετικών λύσεων της πολυωνυμικής ισοτιμίας $f(x) \equiv 0 \pmod{m}$.

Θεώρημα 51

Έστω $f(x) \in \mathbb{Z}[x]$ και m φυσικός με πρωτογενή ανάλυση $m = p_1^{a_1} \dots p_r^{a_r}$.

i) Η πολυωνυμική ισοτιμία

$$f(x) \equiv 0 \pmod{m} \qquad (1)$$

έχει λύση αν και μόνο αν κάθε μία από τις ισοτιμίες του συστήματος

$$\left.\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{a_1}} \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_r^{a_r}} \end{aligned}\right\} \qquad (I)$$

έχει λύση.

ii) Ισχύει $N(m) = N(p_1^{a_1}) \dots N(p_r^{a_r})$

Απόδειξη.

Έστω $c_1,\dots,c_r$ ακέραιοι τέτοιοι ώστε

$$f(c_1)\equiv 0 \pmod{p_1^{a_1}}$$
$$\vdots$$
$$f(c_r)\equiv 0 \pmod{p_r^{a_r}}$$

Η πολυωνυμική ισοτιμία $f(x)\equiv 0 \pmod{p_i^{a_i}}$ έχει την λύση $x\equiv c_i \pmod{p_i^{a_i}}$, $i=1,\dots,r$.

Το σύστημα των γραμμικών ισοτιμιών

$$\left.\begin{aligned} x&\equiv c_1 \pmod{p_1^{a_1}}\\ &\vdots\\ x&\equiv c_r \pmod{p_r^{a_r}}\end{aligned}\right\}$$

σύμφωνα με το κινεζικό θεώρημα των υπολοίπων, έχει μοναδική λύση $c \pmod m$, οπότε

$$c\equiv c_i \pmod{p_i^{a_i}} \qquad i=1,\dots,r.$$

Έτσι έχουμε

$$f(c)\equiv f(c_i) \pmod{p_i^{a_i}} \qquad i=1,\dots,r$$

Επειδή $f(c_i)\equiv 0 \pmod{p_i^{a_i}}$ $i=1,\dots,r$ θα είναι και

$$f(c)\equiv 0 \pmod{p_i^{a_i}} \qquad i=1,\dots,r.$$

Είναι λοιπόν

$$p_i^{a_i} \mid f(c) \qquad i=1,\dots,r$$

και επειδή $(p_i^{a_i}, p_j^{a_j})=1$ για $i\neq j$

θα έχουμε

$$p_1^{a_1}\cdots p_r^{a_r} \mid f(c)$$

δηλαδή

$$f(c)\equiv 0 \pmod m.$$

Η $x\equiv c \pmod m$ είναι λοιπόν λύση της (1).

Αντίστροφα, αν είναι η $x\equiv c \pmod m$ μια λύση της (1).

θα είναι $f(c)\equiv 0 \pmod m$, οπότε $m \mid f(c)$ δηλαδή $p_1^{a_1}\cdots p_r^{a_r} \mid f(c)$. Επειδή $(p_i^{a_i}, p_j^{a_j}) = 1$ για $i \neq j$, θα είναι $p_i^{a_i} \mid f(c)$, $i=1,\ldots,r$. δηλαδή

$$\left.\begin{aligned} f(c)&\equiv 0 \pmod{p_1^{a_1}} \\ &\vdots \\ f(c)&\equiv 0 \pmod{p_r^{a_r}} \end{aligned}\right\}$$

Επομένως κάθε μία απο τις πολυωνυμικές ισοτιμίες του συστήματος (I) έχει λύση αντίστοιχα την :

$$\begin{aligned} x &\equiv c \pmod{p_1^{a_1}} \\ &\vdots \\ x &\equiv c \pmod{p_r^{a_r}} \end{aligned}$$

και η απόδειξη του i) τελειώνει εδώ. Θα παρατηρήσουμε ότι το παραπάνω σύστημα γραμμικών ισοτιμιών έχει μοναδική λύση την $x \equiv c \pmod m$.

Συμπερασματικά λοιπόν δείξαμε ότι η κλάση $c \pmod m$ είναι λύση της πολυωνυμικής ισοτιμίας (1) αν και μόνο αν είναι η μοναδική λύση ενός συστήματος γραμμικών ισοτιμιών

$$\left.\begin{aligned} x &\equiv c_1 \pmod{p_1^{a_1}} \\ &\vdots \\ x &\equiv c_r \pmod{p_r^{a_r}} \end{aligned}\right\}$$

όπου ο ακέραιος c_i επαληθεύει την

$$f(x) \equiv 0 \pmod{p_i^{a_i}} \qquad i=1,\ldots,r .$$

ii) Αν μία τουλάχιστον απο τις πολυωνυμικές ισοτιμίες του συστήματος (I) δεν έχει λύση τότε και η (1) δεν έχει λύση Η ισότητα λοιπόν $N(m) = N(p_1^{a_1}) \cdots N(p_r^{a_r})$ ισχύει στην περίπτωση αυτή.

Ας υποθέσουμε ότι όλες οι πολυωνυμικές ισοτιμίες του συστήματος (I) έχουν λύση.

Συμβολίζουμε με A_i το σύνολο των λύσεων της πολυωνυμικής ισοτιμίας $f(x) \equiv 0 \pmod{p_i^{a_i}}$ $i=1,\dots,r$. και με A το σύνολο των λύσεων της πολυωνυμικής ισοτιμίας (1). Έτσι το πλήθος των στοιχείων του A_i είναι $N(p_i^{a_i})$ $i=1,\dots,r$ και του A είναι $N(m)$.

Σε κάθε διατεταγμένη r-άδα $(c_1,\dots,c_r)$ λύσεων των πολυωνυμικών ισοτιμιών του συστήματος (I) αντιστοιχούμε την λύση $c \pmod m$ της (1) όπως συμπερασματικά αναφέραμε στην απόδειξη του i) μέρους.

Ορίζουμε μ' αυτό τον τρόπο μια απεικόνιση

$$\Psi : A_1 \times \cdots \times A_r \longrightarrow A$$

$$(c_1, \dots c_r) \longmapsto c$$

η οποία είναι επί, σύμφωνα με την απόδειξη του i) μέρους. Επειδή τα σύνολα είναι πεπερασμένα, θα είναι η Ψ και 1-1. Επομένως τα σύνολα $A_1 \times \cdots \times A_r$ και A είναι ισοδύναμα, έχουν λοιπόν το ίδιο πλήθος στοιχείων. Το πλήθος όμως των στοιχείων του $A_1 \times \cdots \times A_r$ είναι $N(p_1^{a_1}) \cdots N(p_r^{a_r})$. άρα

$$N(m) = N(p_1^{a_1}) \cdots N(p_r^{a_r}) . \blacksquare$$

Παράδειγμα 5.1

Να επιλυθεί η πολυωνυμική ισοτιμία

$$f(x) = x^2 + x + 7 \equiv 0 \pmod{3^4 \cdot 7^2}.$$

Θεωρούμε το σύστημα των πολυωνυμικών

$$\left.\begin{aligned} f(x) = x^2 + x + 7 &\equiv 0 \pmod{3^4} \\ f(x) = x^2 + x + 7 &\equiv 0 \pmod{7^2} \end{aligned}\right\}$$

Η πρώτη όμως απ' αυτές, όπως είδαμε στο Παράδειγμα 4.1 δεν έχει λύση. Άρα και $f(x) \equiv 0 \pmod{3^4 \cdot 7^2}$ δεν έχει λύση.

Παράδειγμα 5.2

Θα βρούμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = 2x^2 - 3x - 1 \equiv 0 \pmod{2^2 \cdot 19^2}$$

Θεωρούμε το σύστημα των πολυωνυμικών ισοτιμιών

$$\left.\begin{aligned} f(x) = 2x^2 - 3x - 1 &\equiv 0 \pmod{2^2} \\ f(x) = 2x^2 - 3x - 1 &\equiv 0 \pmod{19^2} \end{aligned}\right\} \begin{matrix}(1)\\(2)\end{matrix}$$

και βρίσκουμε τις λύσεις των (1) και (2).

Η (1) από το παράδειγμα 4.2 έχει μοναδική λύση την

$$x \equiv 3 \pmod{2^2}.$$

Η (2) από το παράδειγμα 4.3 έχει δυο λύσεις τις

$$x \equiv 308 \pmod{19^2} \quad \text{και} \quad x \equiv 235 \pmod{19^2}.$$

Η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod{2^2 \cdot 19^2}$ έχει ακριβώς δύο λύσεις, που είναι οι λύσεις $\pmod{2^2 \cdot 19^2}$ των ακόλουθων συστημάτων γραμμικών ισοτιμιών

$$\left.\begin{aligned} x &\equiv 3 \pmod{2^2} \\ x &\equiv 308 \pmod{19^2} \end{aligned}\right\} (I_1) \qquad \text{και} \qquad \left.\begin{aligned} x &\equiv 3 \pmod{2^2} \\ x &\equiv 235 \pmod{19^2} \end{aligned}\right\} (I_2)$$

Από το Κινεζικό Θεώρημα των υπολοίπων βρίσκουμε ότι το (I_1) έχει την μοναδική λύση

$$x = 19^2 \cdot 3 \cdot 1 + 2^2 \cdot 308 \cdot 271 = 332.955 \equiv 835 \pmod{2^2 \cdot 19^2}$$

και το (I_2) την λύση

$$x = 19^2 \cdot 3 \cdot 1 + 2^2 \cdot 235 \cdot 271 = 255.823 \equiv 235 \pmod{2^2 \cdot 19^2}$$

Η δοθείσα πολυωνυμική ισοτιμία λοιπόν έχει τις λύσεις

$$x \equiv 235 \pmod{2^2 \cdot 19^2} \quad \text{και} \quad x \equiv 835 \pmod{2^2 \cdot 19^2}.$$

Παράδειγμα 5.3

Θα υπολογίσουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = x^3 + 4x^2 + 3 \equiv 0 \pmod{78408}.$$

Είναι $78.408 = 2^3 \cdot 3^4 \cdot 11^2$.

Θεωρούμε το σύστημα των πολυωνυμικών ισοτιμιών

$$\left.\begin{aligned} f(x) = x^3 + 4x^2 + 3 &\equiv 0 \pmod{2^3} \\ f(x) = x^3 + 4x^2 + 3 &\equiv 0 \pmod{3^4} \\ f(x) = x^3 + 4x^2 + 3 &\equiv 0 \pmod{11^2} \end{aligned}\right\} (1)$$

Η (1) από το Παράδειγμα 4.4 έχει μοναδική λύση την

$$x \equiv 1 \pmod{2^3}.$$

Η (2) από το παράδειγμα 4.5 έχει μοναδική λύση την

$$x \equiv 56 \pmod{3^4}$$

Η (3) από το παράδειγμα 4.6 έχει τις λύσεις

$x \equiv 8 \pmod{11^2}$, $x \equiv 6 \pmod{11^2}$, $x \equiv 31 \pmod{11^2}$.

Η πολυωνυμική ισοτιμία $f(x) \equiv 0 \pmod{2^3 \cdot 3^4 \cdot 11^2}$ έχει ακριβώς τρεις λύσεις, που είναι οι λύσεις $\pmod{2^3 \cdot 3^4 \cdot 11^2}$ των ακόλουθων συστημάτων γραμμικών ισοτιμιών.

$$\left.\begin{aligned} x &\equiv 1 \pmod{2^3} \\ x &\equiv 56 \pmod{3^4} \\ x &\equiv 80 \pmod{11^2} \end{aligned}\right\} (I_1) \quad , \quad \left.\begin{aligned} x &\equiv 1 \pmod{2^3} \\ x &\equiv 56 \pmod{3^4} \\ x &\equiv 6 \pmod{11^2} \end{aligned}\right\} (I_2)$$

και

$$\left.\begin{aligned} x &\equiv 1 \pmod{2^3} \\ x &\equiv 56 \pmod{3^4} \\ x &\equiv 31 \pmod{11^2} \end{aligned}\right\} (I_3).$$

Χρησιμοποιούμε το Κινεζικό Θεώρημα των υπολοίπων.

Οι γραμμικές ισοτιμίες,

$3^4 \cdot 11^2 x \equiv 1 \pmod{2^3}$, $2^3 \cdot 11^2 x \equiv 1 \pmod{3^4}$, $2^3 \cdot 3^4 \cdot x \equiv 1 \pmod{11^2}$

έχουν μοναδικές λύσεις αντίστοιχα τις

$x \equiv 1 \pmod{2^3}$, $x \equiv 20 \pmod{3^4}$, $x \equiv 76 \pmod{11^2}$.

Έτσι το (I_1) έχει την μοναδική λύση

$$X = 3^4 \cdot 11^2 \cdot 1 \cdot 1 + 2^3 \cdot 11^2 \cdot 56 \cdot 20 + 2^3 \cdot 3^4 \cdot 80 \cdot 76 = 5.033.801 \equiv$$
$$\equiv 15.689 \pmod{78.408}.$$

Το (I_2) έχει την λύση

$$X = 3^4 \cdot 11^2 \cdot 1 \cdot 1 + 2^3 \cdot 11^2 \cdot 56 \cdot 20 + 2^3 \cdot 3^4 \cdot 6 \cdot 76 = 1.389.449 \equiv$$
$$\equiv 56.513 \pmod{78408}.$$

Το (I_3) έχει την λύση

$$X = 3^4 \cdot 11^2 \cdot 11 + 2^3 \cdot 11^2 \cdot 56 \cdot 20 + 2^3 \cdot 3^4 \cdot 11 \cdot 76 = 2.620.649 \equiv$$
$$\equiv 33.185 \pmod{78408}.$$

Η δοθείσα πολυωνυμική ισοτιμία έχει τρεις λύσεις τις

$$x \equiv 15689,\ 56.513,\ 33.185 \pmod{78.408}. \blacksquare$$

ΚΕΦΑΛΑΙΟ VII

Αρχικές ρίζες. Δείκτες, π-αδικά υπόλοιπα.

1. Αρχικές ρίζες.

Έστω φυσικός $n>1$ και ακέραιος a με $(a,n)=1$. Από τον ορισμό της $ord_n(a)$ γνωρίζουμε ότι $ord_n(a) | \varphi(n)$.

Ορισμός

Έστω η φυσικός >1 και a ακέραιος με $(a,n)=1$. Ο a καλείται αρχική ρίζα (mod n) ή αρχική ρίζα του n, αν

$$ord_n(a) = \varphi(n).$$

Μ' άλλα λόγια ο a είναι αρχική ρίζα (mod n), αν $a^{\varphi(n)} \equiv 1 \pmod n$ και $a^k \not\equiv 1 \pmod n$ για κάθε φυσικό $k < \varphi(n)$.

Για παράδειγμα, αν $n=2$ τότε, ο 1 είναι αρχική ρίζα του 2, αφού $\varphi(2)=1$ και $1^1 \equiv 1 \pmod 2$. Όμοια αν $n=4$ τότε, ο 3 είναι αρχική ρίζα του 4, αφού $\varphi(4)=2$ και $3^1 \not\equiv 1 \pmod 4$ και $3^2 \equiv 1 \pmod 4$.

Σύμφωνα με τον παραπάνω ορισμό, θα λέμε ότι η τάξη $\bar{a} \in H_n$ είναι αρχική ρίζα της πολλαπλασιαστικής ομάδας H_n αν και μόνο αν $ord_n(\bar{a}) = \varphi(n)$.

Πρόταση 1.1

Έστω φυσικός $n>1$ και a ακέραιος με $(a,n)=1$. Ο ακέραιος a είναι μια αρχική ρίζα (mod n) αν και μόνο αν οι $\varphi(n)$ σε πλήθος ακέραιοι

$$1, a, a^2, \ldots, a^{\varphi(n)-1}$$

αποτελούν ένα αναγμένο σύστημα υπολοίπων (mod n).

Απόδειξη.

Αν ο α είναι αρχική ρίζα (mod n) τότε $ord_n(a)=\varphi(n)$ και επομένως σύμφωνα με την πρόταση 8.2 iii) του Κεφ IV, οι $\varphi(n)$ σε πλήθος ακέραιοι $1, a, \ldots, a^{\varphi(n)-1}$ είναι ανά δύο ανισότιμοι (mod n). Επιπλέον, $(a^k, n)=1$, $k=0,1,\ldots,\varphi(n)-1$. Αποτελούν οι ακέραιοι αυτοί ένα αναγμένο σύστημα υπολοίπων (mod n).

Αντίστροφα, αν οι ακέραιοι $1, a, \ldots, a^{\varphi(n)-1}$ αποτελούν ένα αναγμένο σύστημα υπολοίπων, τότε $a^k \not\equiv 1 \pmod n$ για κάθε φυσικό $k<\varphi(n)$ και $a^{\varphi(n)} \equiv 1 \pmod n$ από το θεώρημα του Euler, επομένως ο α είναι μια αρχική ρίζα (mod n). ∎

Πόρισμα 1.1

Έστω φυσικός $n>1$ και ακέραιος α με $(a,n)=1$. Ο ακέραιος α είναι μια αρχική ρίζα (mod n) αν και μόνο αν

$$H_n = \{\bar{1}, \bar{a}, \ldots, \bar{a}^{\varphi(n)-1}\}.$$

Απόδειξη.

Ο ακέραιος α είναι μια αρχική ρίζα (mod n) αν και μόνο αν οι ακέραιοι $1, a, \ldots, a^{\varphi(n)-1}$ αποτελούν ένα αναγμένο σύστημα υπολοίπων (mod n) αν και μόνο αν $H_n = \{\bar{1}, \bar{a}, \ldots, \bar{a}^{\varphi(n)-1}\}$. ∎

Η σημασία των αρχικών ριζών φαίνεται στο παραπάνω πόρισμα. Αν ο φυσικός η έχει αρχική ρίζα, τότε η πολλαπλασιαστική ομάδα H_n είναι κυκλική ομάδα.

Δυστυχώς όμως, δεν έχουν όλοι οι φυσικοί $n>1$, αρχικές ρίζες.

Για παράδειγμα, ο 12 δεν έχει αρχικές ρίζες, αφού για τους ακέραιους από το αναγμένο σύστημα υπολοίπων (mod 12) $\{1,5,7,11\}$ έχουμε $ord_{12}(1)=1$ και $ord_{12}(5)=ord_{12}(7)=ord_{12}(11)=2$ και $\varphi(12)=4$.

Άλλο παράδειγμα αποτελούν όλοι οι φυσικοί αριθμοί n για τους οποίους $\lambda(n) < \varphi(n)$, όπου $\lambda(n)$ η συνάρτηση ελάχιστος καθολικός εκθέτης που ορίσαμε στην παράγραφο 7 του Κεφ. IV, αφού για κάθε ακέραιο a με $(a,n)=1$ ισχύει $a^{\lambda(n)} \equiv 1 \pmod n$ σύμφωνα με το θεώρημα 7.1 του Κεφ. IV.

Το ερώτημα που φυσικά γεννάται είναι ποιοί φυσικοί $n>1$ έχουν αρχικές ρίζες. Στα επόμενα θ' ασχοληθούμε μ' αυτό το ερώτημα και θ' απαντήσουμε σ' αυτό, αποδεικνύοντας ότι:

Ο φυσικός $n>1$ έχει αρχικές ρίζες αν και μόνο αν $n = 2, 4, p^\beta, 2p^\beta$, p περιττός πρώτος, $\beta \geq 1$.

1α. Η ανυπαρξία αρχικών ριζών $(\bmod n)$ για $n \neq 1, 2, 4, p^\beta, 2p^\beta$, p περιττος πρώτος, $\beta \geq 1$.

Πρόταση 1.2

Έστω φυσικός $n>1$. Αν $n \neq 2, 4, p^\beta, 2p^\beta$, όπου p περιττός πρώτος, β φυσικός ≥ 1, τότε ο n δεν έχει αρχικές ρίζες.

Απόδειξη.

Αν $n \neq 1, 2, 4, p^\beta, 2p^\beta$, p περιττός πρώτος, $\beta \geq 1$, τότε, σύμφωνα με όσα αναφέραμε στην παράγραφο 7 του Κεφ IV, ο n θα έχει πρωτογενή ανάλυση της μορφής,

i) $n = 2^\beta$, $\beta \geq 3$

ii) $n = 2^\beta \cdot p_1^{\beta_1}$, p_1 περιττός πρώτος, $\beta \geq 2$, $\beta_1 \geq 1$.

iii) $n = 2^\beta \cdot p_1^{\beta_1} \cdots p_r^{\beta_r}$, p_i περιττοί πρώτοι, $r \geq 2$, $\beta_i \geq 1$, $\beta \geq 0$.

Αλλά τότε $\lambda(n) < \varphi(n)$, και επομένως ο n δεν έχει αρχικές ρίζες, αφού $a^{\lambda(n)} \equiv 1 \pmod n$ για κάθε ακέραιο a με $(a,n)=1$.

Αν λάβουμε υπόψη μας την παρατήρηση 1 της παραγράφου 7 του κεφ IV, έχουμε ισοδύναμα:

Πόρισμα 1.2

Ο φυσικός $n>1$ δεν έχει αρχικές ρίζες αν και μόνο αν ο n είναι της μορφής

i) $n = 2^\beta$, $\beta \geq 3$

ή της μορφής

ii) $n = k \cdot l$ με $(k,l)=1$, $k>2$, $l>2$. ■

Πόρισμα 1.3

Ο φυσικός $n>1$ δεν έχει αρχικές ρίζες, αν και μόνο αν είναι πολλαπλάσιο ενός αριθμού του τύπου

(i) $4p$, p περιττός πρώτος

ή

(ii) pq, $p \neq q$ περιττοί πρώτοι

ή

(iii) 8.

Παράδειγμα 1.1

Ο φυσικός $n = 1998 = 2 \cdot 3^3 \cdot 37$ δεν έχει αρχικές ρίζες αφού είναι πολλαπλάσιο του $3 \cdot 7$ με τους $3, 7$ περιττούς πρώτους, ή διαφορετικά, δεν είναι της μορφής $2, 4, p^\beta, 2p^\beta$ με p περιττό πρώτο και $\beta \geq 1$.

1β. Η ύπαρξη αρχικών ριζών $(\bmod n)$ όπου $n = 2, 4, p^\beta, 2p^\beta$, p περιττός πρώτος, $\beta \geq 1$.

1b$_1$. Η ύπαρξη αρχικών ριζών (mod p) όπου p πρώτος.

Πρόταση 1.3

Έστω η πολυωνυμική ισοτιμία

$$x^d - 1 \equiv 0 \pmod p \qquad (*)$$

όπου p πρώτος και d φυσικός με $d \mid p-1$.

Αν υπάρχει μια λύση αυτής τάξης d (mod p), τότε υπάρχουν $\varphi(d)$ λύσεις αυτής τάξης d (mod p).

Απόδειξη.

Έστω ότι υπάρχει μια λύση $\alpha \pmod p$ της (*) που έχει τάξη d (mod p).

Έχουμε λοιπόν $(\alpha, p)=1$, $\alpha^d \equiv 1 \pmod p$ και $\operatorname{ord}_p(\alpha)=d$.

Για τους ακεραίους $1, \alpha, \ldots, \alpha^{d-1}$ έχουμε τα εξής:

1) Είναι ανά δύο ανισοτιμοι (mod p) σύμφωνα με την Πρόταση 8.2 του Κεφ. IV

2) Είναι λύσεις της (*) αφού

$$(\alpha^i)^d = (\alpha^d)^i \equiv 1 \pmod p \qquad i=0,1,\ldots,d-1.$$

Η (*) έχει όμως ακριβώς d διαφορετικές λύσεις (mod p), σύμφωνα με το Πόρισμα 3.7 του Κεφ VI.

Αποτελούν λοιπόν οι d σε πλήθος κλάσεις

$$1 \pmod p,\ \alpha \pmod p,\ \ldots,\ \alpha^{d-1} \pmod p \qquad (**)$$

όλες τις λύσεις της (*).

Συνεπώς οι κλάσεις $c \pmod p$ που είναι λύσεις της (*) και έχουν τάξη d (mod p), δηλαδή $\operatorname{ord}_p(c)=d$, βρίσκονται μεταξύ των κλάσεων (**).

Είναι $\operatorname{ord}_p(c)=d$, επομένως, σύμφωνα με το Πόρισμα 8.3 του Κεφ IV,

$$\operatorname{ord}(\alpha^k)=d \iff (k,d)=1.$$

Άρα από τις κλάσεις (**), οι κλάσεις

$$\alpha^k \pmod p, \quad k \le d-1 \text{ και } (k,d)=1$$

είναι αυτές ακριβώς οι πρωτογενείς κλάσεις(modp) που είναι λύσεις της(*) και έχουν τάξη d. Το πλήθος τους είναι ίσο με το πλήθος των φυσικών $\kappa \le d-1$ και $(\kappa,d)=1$ δηλαδή ίσο με $\varphi(d)$.

Η επόμενη πρόταση μας εξασφαλίζει την **ύπαρξη** λύσεων της (*) που έχουν τάξη d (modp)

Πρόταση 1.4

Ας είναι p πρώτος και $d|p-1$, $d \in \mathbb{N}$.
Τότε η πολυωνυμική ισοτιμία

$$x^d - 1 \equiv 0 \pmod p \qquad (*)$$

έχει ακριβώς d διαφορετικές λύσεις και $\varphi(d)$ σε πλήθος απ' αυτές έχουν τάξη d (modp).

Απόδειξη

Η (*) έχει ακριβώς d διαφορετικές λύσεις (modp), σύμφωνα με το πόρισμα 3.7 του Κεφ VI.

Για κάθε φυσικό διαιρέτη d του p-1, το σύνολο των λύσεων της (*) που έχουν τάξη d, είναι ισοδύναμο με το σύνολο

$$A(d)=\{\kappa \,/\, 1 \le \kappa \le p-1 \text{ και } \mathrm{ord}_p(\kappa)=d\}.$$

Είναι φανερό ότι τα σύνολα A(d) για τους διάφορους διαιρέτες του p-1 είναι υποσύνολα του $\{1,2,\dots,p-1\}$ και μάλιστα ξένα μεταξύ τους. Απ' την άλλη μεριά κάθε φυσικός $\kappa \in \{1,2,\dots,p-1\}$ ανήκει σ' ένα και μόνο ένα απ' αυτά τα A(d), αφού $(\kappa,p)=1$ και, αν $\mathrm{ord}_p(\kappa)=d$ τότε $d|\varphi(p)=p-1$.

Αποτελούν λοιπόν τα σύνολα A(d) μια διαμέριση του συνόλου $\{1,2,\dots,p-1\}$.

Αν συμβολίσουμε λοιπόν με $\psi(d)$ το πλήθος των στοιχείων του A(d) τότε $\psi(d)=0$ ή $\psi(d)=\varphi(d)$ σύμφωνα με την Πρόταση 1.3, και

$$\sum_{d|p-1} \psi(d) = p-1 .$$

Από το θεώρημα 5.1 του Κεφ. III έχουμε όμως ότι

$$\sum_{d|p-1} \varphi(d) = p-1$$

Έτσι $\sum_{d|p-1} \psi(d) = \sum_{d|p-1} \varphi(d)$.

δηλαδή $\sum_{d|p-1} \{\varphi(d) - \psi(d)\} = 0$

Αλλά πάντα $\psi(d) \leq \varphi(d)$, και για να μηδενίζεται το προηγούμενο άθροισμα πρέπει $\psi(d) = \varphi(d)$ για κάθε $d|p-1$, $d \in \mathbb{N}$. Άρα για $d \in \mathbb{N}$, $d|p-1$, υπάρχουν $\varphi(d)$ λύσεις της (*) τάξης d. ■

Πόρισμα 1.4

Έστω p πρώτος και $d|p-1$, $d \in \mathbb{N}$.

Τότε υπάρχουν ακριβώς $\varphi(d)$ σε πλήθος ακέραιοι από το ανάγμενο σύστημα υπολοίπων $(\mathrm{mod}\, p)$

$$\{1, 2, \ldots, p-1\}$$

που η τάξη τους $(\mathrm{mod}\, p)$ ισούται με d. ■

Ισοδύναμα έχουμε

Πόρισμα 1.5

Έστω p πρώτος και $d|p-1$, $d \in \mathbb{N}$.

Τότε υπάρχουν ακριβώς $\varphi(d)$ σε πλήθος πρωτογενείς κλάσεις από το $H_p = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$

που η τάξη τους ισούται με d. ■

Αν $d = p-1$, έχουμε

Πόρισμα 1.6

Έστω p πρώτος. Υπάρχουν ακριβώς $\varphi(p-1)$ ακέραιοι από το αναγμένο σύστημα υπολοίπων (mod p)

$$\{1, 2, \ldots, p-1\}$$

που είναι αρχικές ρίζες (mod p).

Απόδειξη

Υπάρχουν $\varphi(p-1)$ ακέραιοι από το $\{1, 2, \ldots, p-1\}$ που έχουν τάξη $p-1 = \varphi(p)$, άρα υπάρχουν ακριβώς $\varphi(p-1)$ αρχικές ρίζες (mod p). ■

Παράδειγμα 1.2

Για τον πρώτο $p=7$. Είναι $\varphi(7)=6$. Οι φυσικοί διαιρέτες $d|6$ είναι οι 1, 2, 3, 6. Από το αναγμένο σύστημα υπολοίπων (mod 7)

$$\{1, 2, 3, 4, 5, 6\}$$

έχουμε,

1) $\varphi(1)=1$ Άρα μόνο ένας ακέραιος έχει τάξη 1 (mod 7) και είναι αυτός ο 1.

2) $\varphi(2)=1$ Άρα μόνο ένας ακέραιος έχει τάξη 2 (mod 7) και είναι αυτός ο 6.

3) $\varphi(3)=2$. Υπάρχουν ακριβώς 2 ακέραιοι που έχουν τάξη 3 (mod 7) και είναι αυτοί οι 2 και 4.

4) $\varphi(6)=2$. Δυο ακέραιοι ακριβώς έχουν τάξη 6 (mod 7) και είναι αυτοί υποχρεωτικά οι 3 και 5.

Ο 3 και ο 5 είναι λοιπόν αρχικές ρίζες (mod 7).

Τα σύνολα λοιπόν,

$\{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ και $\{5, 5^2, 5^3, 5^4, 5^5, 5^6\}$

είναι αναγμένα συστήματα υπολοίπων (mod 7), όπως και το $\{1, 2, 3, 4, 5, 6\}$. Ο ακέραιος 3^K $1 \le K \le 6$ είναι σσότιμος μέναν και μόνο έναν από τους ακεραίους του $\{1, 2, 3, 4, 5, 6\}$. Για παράδειγμα $3^4 \equiv 81 \equiv 4 \pmod 7$.

Όμοια και για τους αυέραιους 5^k, $1 \le k \le 6$. ■

Παράδειγμα 1.3

Αν ο $\varrho_n = 2^{2^n}+1$, $n>1$ είναι πρώτος, τότε ο 2 δεν είναι αρχική ρίζα $(\mathrm{mod}\,\varrho_n)$.

Επειδή $2^{2^{n+1}}-1 = (2^{2^n}+1)(2^{2^n}-1)$ έχουμε

$$2^{2^{n+1}} \equiv 1 \ (\mathrm{mod}\,\varrho_n)$$

Αν λοιπόν $\mathrm{ord}_{\varrho_n}(2) = r$ τότε $r \mid 2^{n+1}$, επομένως $r \le 2^{n+1}$

Αλλά $\varphi(\varrho_n) = \varrho_n - 1 = 2^{2^n}$

Επαγωγικά δείχνουμε ότι για κάθε φυσικό $n>1$ ισχύει $2^{n+1} < 2^{2^n}$. Έτσι $r \le 2^{n+1} < 2^{2^n}$ δηλαδή $\mathrm{ord}_{\varrho_n}(2) < \varphi(\varrho_n)$, άρα ο 2 δεν είναι αρχική ρίζα $(\mathrm{mod}\,\varrho_n)$.

1b₂. Η ύπαρξη αρχικών ριζών $(\mathrm{mod}\, n)$ $n = p^\beta, 2p^\beta$, p περιττός πρώτος, $\beta \ge 1$.

Λήμμα 1.1

Έστω p περιττός πρώτος.

Αν α είναι μια αρχική ρίζα $(\mathrm{mod}\,p^\beta)$, τότε για την τάξη του $\alpha (\mathrm{mod}\,p^{\beta+1})$ ένα εκ των δύο ισχύει:

ή $\mathrm{ord}_{p^{\beta+1}}(\alpha) = \varphi(p^\beta)$ ή ο α είναι αρχική ρίζα $(\mathrm{mod}\,p^{\beta+1})$.

Κάθε αρχική ρίζα του $p^{\beta+1}$ είναι μία αρχική ρίζα του p^β.

Απόδειξη.

Εύκολα φαίνεται ότι $\varphi(p^{\beta+1}) = p\varphi(p^\beta)$.

Έστω $\text{ord}_{p^{\beta+1}}(a)=t$, τότε $t \mid \varphi(p^{\beta+1})$ άρα $\varphi(p^{\beta+1})=t\lambda$, $\lambda\in\mathbb{N}$.
Αφού $a^t \equiv 1 \pmod{p^{\beta+1}}$ θα έχουμε $a^t \equiv 1 \pmod{p^\beta}$. Αλλά $a^{\varphi(p^\beta)} \equiv 1 \pmod{p^\beta}$ επειδή ο a είναι μία αρχική ρίζα $\pmod{p^\beta}$. Επομένως $\varphi(p^\beta) \mid t$ και επομένως $t = k\cdot\varphi(p^\beta)$, $k\in\mathbb{N}$.
Αν $k=1$ τότε $t=\varphi(p^\beta)$ και επομένως $\text{ord}_{p^{\beta+1}}(a)=\varphi(p^\beta)$.
Αν $k>1$ τότε έχουμε

$$p\cdot\varphi(p^\beta)=\varphi(p^{\beta+1})=t\cdot\lambda=k\lambda\,\varphi(p^\beta)$$

άρα $p=k\lambda$ και επειδή $k>1$ υποχρεωτικά $k=p$. Αλλά τότε
$t=p\cdot\varphi(p^\beta)=\varphi(p^{\beta+1})$ δηλαδή $\text{ord}_{p^{\beta+1}}(a)=\varphi(p^{\beta+1})$, άρα ο a είναι μία αρχική ρίζα $\pmod{p^{\beta+1}}$.

Στην συνέχεια ας είναι a μία αρχική ρίζα του $p^{\beta+1}$, δηλαδή $\text{ord}_{p^{\beta+1}}(a)=\varphi(p^{\beta+1})$ οπότε $a^{\varphi(p^{\beta+1})} \equiv 1 \pmod{p^{\beta+1}}$.

Έστω ότι $\text{ord}_{p^\beta}(a)=t$, τότε $t \mid \varphi(p^\beta)$ και $a^t \equiv 1 \pmod{p^\beta}$.
Θα δείξουμε ότι $t=\varphi(p^\beta)$ οπότε ο a είναι αρχική ρίζα του p^β.
Αφού $a^t \equiv 1 \pmod{p^\beta}$ έχουμε $a^t = 1 + k\cdot p^\beta$. Υψώνουμε και τα δύο μέρη της ισότητας αυτής στη p-στή δύναμη και έχουμε

$$a^{pt} = (1+kp^\beta)^p = 1 + pkp^\beta + \dots + k^p p^{\beta p} = 1 + p^{\beta+1}\cdot A \quad , A\in\mathbb{Z}$$

άρα $a^{pt} \equiv 1 \pmod{p^{\beta+1}}$. Επειδή $\text{ord}_{p^{\beta+1}}(a)=\varphi(p^{\beta+1})$ θα έχουμε $\varphi(p^{\beta+1}) \mid tp$ δηλαδή $p\varphi(p^\beta) \mid tp$ άρα $\varphi(p^\beta) \mid t$. Επειδή και $t \mid \varphi(p^\beta)$ θα είναι $t=\varphi(p^\beta)$ πράγμα που επιδιώκαμε. ∎

Πόρισμα 1.7

Έστω p περιττός πρώτος. Αν a είναι μία αρχική ρίζα $(\mathrm{mod}\, p)$ τότε ο a είναι επίσης αρχική ρίζα $(\mathrm{mod}\, p^2)$ αν και μόνο αν

$$a^{p-1} \not\equiv 1 \ (\mathrm{mod}\, p^2).$$

Απόδειξη.

Έστω ότι ο a είναι και αρχική ρίζα $(\mathrm{mod}\, p^2)$, τότε $\mathrm{ord}_{p^2}(a) = \varphi(p^2) = p\varphi(p)$ άρα $a^{\varphi(p)} \not\equiv 1 \ (\mathrm{mod}\, p^2)$ δηλαδή $a^{p-1} \not\equiv 1 \ (\mathrm{mod}\, p^2)$.

Αντίστροφα, αν $a^{p-1} \not\equiv 1 \ (\mathrm{mod}\, p^2)$ δηλαδή $a^{\varphi(p)} \not\equiv 1 \ (\mathrm{mod}\, p^2)$ οπότε $\mathrm{ord}_{p^2}(a) \neq \varphi(p)$. και επομένως σύμφωνα με το Λήμμα 1.1 ο a είναι αρχική ρίζα $(\mathrm{mod}\, p^2)$. ■

Παράδειγμα 1.3

Έστω $p = 7$. Γνωρίζουμε από το παράδειγμα 1.2 ότι οι 3 και 5 είναι αρχικές ρίζες $(\mathrm{mod}\, 7)$. Επειδή.

$$3^6 \equiv 43 \not\equiv 1 \ (\mathrm{mod}\, 7^2) \quad \text{και} \quad 5^6 \equiv 43 \not\equiv 1 \ (\mathrm{mod}\, 7^2)$$

ο 3 και ο 5 είναι αρχικές ρίζες $(\mathrm{mod}\, 7^2)$, δηλαδή

$$\mathrm{ord}_{7^2}(3) = \varphi(7^2) \quad \text{και} \quad \mathrm{ord}_{7^2}(5) = \varphi(7^2).$$

Επειδή $\varphi(7^2) = 42$ θα έχουμε

$$3^{42} \equiv 1 \ (\mathrm{mod}\, 7^2) \quad \text{και} \quad 5^{42} \equiv 1 \ (\mathrm{mod}\, 7^2).$$

Θεώρημα 1.1

Για κάθε φυσικό αριθμό b υπάρχει μία αρχική ρίζα $(\mathrm{mod}\, p^b)$, όπου p περιττός πρώτος.

Αν ο a είναι μία αρχική ρίζα $(\mathrm{mod}\, p)$, τότε ένας τουλάχιστον από τους a και $a+p$ είναι μία αρχική ρίζα $(\mathrm{mod}\, p^2)$.

Αν ο a είναι μία αρχική ρίζα $(\mathrm{mod}\, p^b)$, $b \geq 2$ τότε ο a είναι μία αρχική ρίζα $(\mathrm{mod}\, p^{b+1})$.

Επομένως, υπάρχει ακέραιος a (ανεξάρτητος από τον b) έτσι

ώστε ο α να είναι μια αρχική ρίζα $(\mathrm{mod} p^b)$ για κάθε φυσικό b.

Απόδειξη.

Σύμφωνα με το πόρισμα 1.6 υπάρχουν αρχικές ρίζες $(\mathrm{mod} p)$. Έστω α μια αρχική ρίζα $(\mathrm{mod} p)$. Επειδή $\alpha+p \equiv \alpha \ (\mathrm{mod} p)$ θα είναι $\mathrm{ord}_p(\alpha+p) = \mathrm{ord}_p(\alpha) = \varphi(p)$ σύμφωνα με την πρόταση 8.1 του κεφ. IV. Επομένως και ο $\alpha+p$ είναι αρχική ρίζα $(\mathrm{mod} p)$.

Αν ο α είναι αρχική ρίζα $(\mathrm{mod} p^2)$ έχει καλώς. Αν ο α δεν είναι αρχική ρίζα $(\mathrm{mod} p^2)$ θα δείξουμε ότι ο $\alpha+p$ είναι αρχική ρίζα $(\mathrm{mod} p^2)$. Σύμφωνα με το Πόρισμα 1.7 αρκεί να δείξουμε ότι $(\alpha+p)^{p-1} \not\equiv 1 \ (\mathrm{mod} p^2)$ δηλαδή ότι $(\alpha+p)^{\varphi(p)} \not\equiv 1 \ (\mathrm{mod} p^2)$.

Είναι,

$$(\alpha+p)^{\varphi(p)} = \alpha^{\varphi(p)} + (p-1)\alpha^{\varphi(p)-1} \cdot p + \cdots = \alpha^{\varphi(p)} - p\alpha^{\varphi(p)-1} + p^2 A$$

όπου $A \in \mathbb{Z}$. Άρα

$$(\alpha+p)^{\varphi(p)} \equiv \alpha^{\varphi(p)} - p\alpha^{\varphi(p)-1} \ (\mathrm{mod} p^2)$$

Σύμφωνα με το Λήμμα 1.1 αφού ο α δεν είναι αρχική ρίζα $(\mathrm{mod} p^2)$ υποχρεωτικά $\mathrm{ord}_{p^2}(\alpha) = \varphi(p)$, άρα

$\alpha^{\varphi(p)} \equiv 1 \ (\mathrm{mod} p^2)$. Έτσι η προηγούμενη ισοτιμία γίνεται

$$(\alpha+p)^{\varphi(p)} \equiv 1 - p\alpha^{\varphi(p)-1} \ (\mathrm{mod} p^2).$$

Αν υποθέσουμε ότι $(\alpha+p)^{\varphi(p)} \equiv 1 \ (\mathrm{mod} p^2)$, τότε

$1 \equiv 1 - p\alpha^{\varphi(p)-1} \ (\mathrm{mod} p^2)$ δηλαδη $-p\alpha^{\varphi(p)-1} \equiv 0 \ (\mathrm{mod} p^2)$

και επομένως $\alpha^{\varphi(p)-1} \equiv 0 \ (\mathrm{mod} p)$ πράγμα άτοπο, αφού $\mathrm{ord}_p(\alpha) = \varphi(p)$. Άρα $\alpha^{\varphi(p)} \not\equiv 1 \ (\mathrm{mod} p^2)$ πράγμα που επιθυμούσαμε.

Για το επόμενο θα εργασθούμε επαγωγικά.

Ας υποθέσουμε ότι ο α είναι μια αρχική ρίζα $(\mathrm{mod} p^x)$ για όλα τα $x = 1, 2, \ldots, b$, $b \geq 2$.

Θα δείξουμε ότι ο α είναι μια αρχική ρίζα $(\mathrm{mod}\, p^{\beta+1})$.
Σύμφωνα με το Λήμμα 1.1 αφού ο α είναι μία αρχική ρίζα $(\mathrm{mod}\, p^{\beta})$ ο α θα είναι και μία αρχική ρίζα $(\mathrm{mod}\, p^{\beta-1})$.
Επομένως, $\alpha^{\varphi(p^{\beta-1})} \equiv 1 \ (\mathrm{mod}\, p^{\beta-1})$, άρα

$$\alpha^{\varphi(p^{\beta-1})} = 1 + kp^{\beta-1}, \quad k \in \mathbb{Z}. \qquad (*)$$

Ο $p \nmid k$, γιατί αν $p \mid k$ τότε $k = p\lambda$, οπότε

$$\alpha^{\varphi(p^{\beta-1})} = 1 + \lambda p^{\beta} \quad \text{άρα} \quad \alpha^{\varphi(p^{\beta-1})} \equiv 1 \ (\mathrm{mod}\, p^{\beta})$$

και επομένως $\varphi(p^{\beta}) \mid \varphi(p^{\beta-1})$ αφού $\mathrm{ord}_{p^{\beta}}(\alpha) = \varphi(p^{\beta})$ πράγμα άτοπο αφού $\varphi(p^{\beta}) = p\,\varphi(p^{\beta-1}) > \varphi(p^{\beta-1})$.
Παίρνοντας τις p-στες δυνάμεις και των δύο μερών της $(*)$ έχουμε

$$\alpha^{p\cdot\varphi(p^{\beta-1})} = (1 + kp^{\beta-1})^{p} = 1 + pkp^{\beta-1} + p^{\beta+1}\cdot B, \quad B \in \mathbb{Z}.$$

Άρα $\alpha^{p\varphi(p^{\beta-1})} \equiv 1 + kp^{\beta} \ (\mathrm{mod}\, p^{\beta+1})$

Επειδή $p \nmid k$ είναι

$$\alpha^{p\varphi(p^{\beta-1})} = \alpha^{\varphi(p^{\beta})} \not\equiv 1 \ (\mathrm{mod}\, p^{\beta+1})$$

επομένως $\mathrm{ord}_{p^{\beta+1}}(\alpha) \neq \varphi(p^{\beta})$ και από το Λήμμα 1.1 υποχρεωτικά ο α είναι μια αρχική ρίζα $(\mathrm{mod}\, p^{\beta+1})$ πράγμα που επιδιώκουμε.

Για το τελευταίο παρατηρούμε ότι αν α είναι μια αρχική ρίζα $(\mathrm{mod}\, p)$ και,

i) Ο α είναι αρχική ρίζα $(\mathrm{mod}\, p^2)$ τότε ο α είναι αρχική ρίζα $(\mathrm{mod}\, p^{\beta})$ για κάθε φυσικό β.

ii) Ο α δεν είναι αρχική ρίζα $(\mathrm{mod}\, p^2)$ τότε ο $\alpha+p$ είναι αρχική ρίζα $(\mathrm{mod}\, p^{\beta})$ για κάθε φυσικό β. ∎

Πόρισμα 1.8

Υπάρχουν αρχικές ρίζες $(\mathrm{mod}\, 2p^\beta)$ όπου p περιττός πρώτος και $\beta \in \mathbb{N}$.

Απόδειξη.

Έστω α μια αρχική ρίζα $(\mathrm{mod}\, p^\beta)$. Η υπαρξή της εξασφαλίζεται από το θεώρημα 1.1.

Αν ο α είναι άρτιος, τότε $(\alpha, 2p^\beta) = 2 \neq 1$ και επομένως δεν ορίζεται η τάξη του α, άρα ο α δεν είναι αρχική ρίζα $(\mathrm{mod}\, 2p^\beta)$.

Ο $\alpha + p^\beta$ όμως, είναι περιττός αριθμός: Είναι

$$\alpha + p^\beta \equiv \alpha \ (\mathrm{mod}\, p^\beta) \quad \text{οπότε} \quad \varphi(p^\beta) = \mathrm{ord}_{p^\beta}(\alpha) = \mathrm{ord}_{p^\beta}(\alpha + p^\beta)$$

δηλαδή ο $\alpha + p^\beta$ είναι περιττή αρχική ρίζα $(\mathrm{mod}\, p^\beta)$.

Υποθέτουμε λοιπόν ότι ο α είναι μια περιττή αρχική ρίζα $(\mathrm{mod}\, p^\beta)$.

Επειδή ο α είναι περιττός θα είναι $\alpha \equiv 1 \ (\mathrm{mod}\, 2)$ οπότε

$$\mathrm{ord}_2(\alpha) = \mathrm{ord}_2(1) = \varphi(2) = 1$$

Επιπλέον, $\mathrm{ord}_{p^\beta}(\alpha) = \varphi(p^\beta)$.

Σύμφωνα με το πόρισμα 8.5 του Κεφ IV, αφού $(2, p^\beta) = 1$ θα είναι

$$\mathrm{ord}_{2p^\beta}(\alpha) = [1, \varphi(p^\beta)] = \varphi(p^\beta) = \varphi(2p^\beta)$$

Άρα ο α είναι μια αρχική ρίζα $(\mathrm{mod}\, 2p^\beta)$. ∎

Παράδειγμα 1.4

Θα βρούμε μια αρχική ρίζα $\mathrm{mod}\,(2 \cdot 7^4)$

Γνωρίζουμε από τα παραδείγματα 1.2 και 1.3 ότι ο περιττός φυσικός 3 είναι αρχική ρίζα $(\mathrm{mod}\, 7)$ και $(\mathrm{mod}\, 7^2)$. Επομένως σύμφωνα θεώρημα 1.1, ο 3 είναι αρχική ρίζα $(\mathrm{mod}\, 7^\beta)$ για κάθε φυσικό β, άρα ο 3 είναι αρχική ρίζα $(\mathrm{mod}\, 7^4)$

Αφού ο 3 είναι περιττός, και $(3, 2 \cdot 7^4) = 1$, ο 3 θα είναι

και μία αρχική ρίζα $(\mathrm{mod}\ 2\cdot 7^4)$, σύμφωνα με το Πόρισμα 1.8.

Παράδειγμα 1.5

Θα βρούμε μια αρχική ρίζα $(\mathrm{mod}\ 2\cdot 41^2)$

Ο 6 είναι μια αρχική ρίζα $(\mathrm{mod}\ 41)$ αφού,

$6^{\varphi(41)} = 6^{40} \equiv 1\ (\mathrm{mod}\ 41)$ και $6^k \not\equiv 1\ (\mathrm{mod}\ 41)$ για $1 \le k < 40$.

δηλαδή $\mathrm{ord}_{41}(6) = \varphi(41) = 40$.

Σύμφωνα με το Πόρισμα 1.7, επειδή

$$6^{40} \equiv 913 \not\equiv 1\ (\mathrm{mod}\ 41^2)$$

ο 6 είναι μια αρχική ρίζα $(\mathrm{mod}\ 41^2)$.

Ο 6 όμως είναι άρτιος, επομένως σύμφωνα με το Πόρισμα 1.8

ο περιττός $6 + 41^2 = 1687$ είναι μια αρχική ρίζα $(\mathrm{mod}\ 2\cdot 41^2)$.

Θεώρημα 1.9

Έστω φυσικός $n > 1$. Υπάρχουν αρχικές ρίζες $(\mathrm{mod}\ n)$ αν και μόνο αν ο n είναι της μορφής

$$n = 2, 4, p^\beta, 2p^\beta$$

όπου p περιττός πρώτος και β φυσικός.

Απόδειξη.

Ο 1 είναι μια αρχική ρίζα $(\mathrm{mod}\ 2)$ και ο 3 μια αρχική ρίζα $(\mathrm{mod}\ 4)$.

Το θεώρημα 1.1 και το πόρισμα 1.8 συμπληρώνουν την απόδειξη. ■

1c. Το πλήθος των αρχικών ριζών $(\mathrm{mod}\ n)$.

Έστω a μια αρχική ρίζα $(\mathrm{mod}\ n)$. Αν $b \equiv a\ (\mathrm{mod}\ n)$ τότε και ο b είναι μια αρχική ρίζα $(\mathrm{mod}\ n)$ αφού

$$\mathrm{ord}_n(b) = \mathrm{ord}_n(a) = \varphi(n).$$

Δυο αρχικές ρίζες $(\mathrm{mod}\, n)$ a και a' θα θεωρούνται διαφορετικές αν και μόνο αν $a \not\equiv a' \ (\mathrm{mod}\, n)$.

Πρόταση 1.5

Αν ο a είναι μια αρχική ρίζα $(\mathrm{mod}\, n)$, τότε ο n έχει ακριβώς $\varphi(\varphi(n))$ ανισότιμες $(\mathrm{mod}\, n)$ αρχικές ρίζες, και αυτές δίνονται από τους ακεραίους του συνόλου

$$S = \{a^k \ / \ 1 \le k \le \varphi(n) \quad \text{και} \quad (k, \varphi(n)) = 1\}.$$

Απόδειξη

Ας είναι a μια αρχική ρίζα $(\mathrm{mod}\, n)$, τότε σύμφωνα με την Πρόταση 1.1 οι ακέραιοι

$$a, a^2, \ldots, a^{\varphi(n)}$$

αποτελούν ένα αναγμένο σύστημα υπολοίπων $(\mathrm{mod}\, n)$.

Έτσι τα στοιχεία του συνόλου S, είναι ανά δύο ανισότιμα $(\mathrm{mod}\, n)$ και αν $a^k \in S$ τότε

$$\mathrm{ord}_n(a^k) = \frac{\mathrm{ord}_n(a)}{(k, \mathrm{ord}_n(a))} = \frac{\varphi(n)}{(k, \varphi(n))} = \frac{\varphi(n)}{1} = \varphi(n)$$

δηλαδή τα στοιχεία του S είναι αρχικές ρίζες $(\mathrm{mod}\, n)$ ανά δύο ανισότιμες $(\mathrm{mod}\, n)$.

Αντίστροφα, αν b είναι μια αρχική ρίζα $(\mathrm{mod}\, n)$, θα δείξουμε ότι ο b είναι ισότιμος $(\mathrm{mod}\, n)$ με ένα και μόνο ένα ακέραιο του συνόλου S. Πραγματικά, αφού $(b, n) = 1$, σύμφωνα με την πρόταση 1.1 θα υπάρχει ακέραιος k με $1 \le k \le \varphi(n)$ ώστε $b \equiv a^k \ (\mathrm{mod}\, n)$. Θα δείξουμε ότι $(k, \varphi(n)) = 1$ Θά είναι

$$\varphi(n) = \mathrm{ord}_n(b) = \mathrm{ord}_n(a^k) = \frac{\mathrm{ord}_n(a)}{(k, \mathrm{ord}_n(a))} = \frac{\varphi(n)}{(k, \varphi(n))}$$

επομένως $(k, \varphi(n)) = 1$.

Έτσι $b \equiv a^k \ (\mathrm{mod}\, n)$ και $a^k \in S$.

Οι ακέραιοι του συνόλου S, είναι όλες οι αρχικές ρίζες $(\mathrm{mod}\, n)$

και είναι σε τάξη $\varphi(\varphi(n))$ σύμφωνα με τον ορισμό της συνάρτησης φ του Euler. ■

Μολονότι αποδείξαμε την ύπαρξη αρχικών ριζών για οριομένα μέτρα δεν γνωρίζουμε μια απ' ευθείας μέθοδο για τον υπολογισμό αυτών των αρχικών ριζών γενικά. Η εύρεση τους, ιδίως για μεγάλα μέτρα απαιτεί πολλούς υπολογισμούς συχνά.

Παράδειγμα 1.6

Θα βρούμε όλες τις αρχικές ρίζες (mod 23).

Ο 23 είναι πρώτος και επομένως έχει αρχικές ρίζες.

Παρατηρούμε ότι $(5,23)=1$ και $\text{ord}_{23}(5)=22=\varphi(23)$, άρα ο 5 είναι μια αρχική ρίζα (mod 23).

Ο 23 έχει $\varphi(\varphi(23))=\varphi(22)=\varphi(2\cdot 11)=\varphi(2)\varphi(11)=10$ αρχικές ρίζες (mod 23)

Αυτές δίνονται από τις δυνάμεις

$$5^k \quad \text{με} \quad 1\le k\le 22\,, \quad (k,22)=1$$

δηλαδή από τις δυνάμεις

$$5,\ 5^3,\ 5^5,\ 5^7,\ 5^9,\ 5^{13},\ 5^{15},\ 5^{17},\ 5^{19},\ 5^{21}.$$

Αλλά (mod 23) έχουμε τις παρακάτω ισοτιμίες

$5\equiv 5$	$5^7\equiv 17$	$5^{15}\equiv 19$	$5^{21}\equiv 14$
$5^3\equiv 10$	$5^9\equiv 11$	$5^{17}\equiv 15$	
$5^5\equiv 20$	$5^{13}\equiv 21$	$5^{19}\equiv 7$	

Πιό απλά, οι 10 ακέραιοι

$$5,7,10,11,14,15,17,19,20,21$$

είναι όλες οι αρχικές ρίζες (mod 23) που φανερά είναι ανισότιμες ανά δύο (mod 23).

Παράδειγμα 1.7

Θα βρούμε όλες τις αρχικές ρίζες $(\text{mod } 2\cdot 7^2)$.

Ο 3 είναι σύμφωνα με το Παράδειγμα 1.4 μια αρχική ρίζα $(\mathrm{mod}\ 2\cdot 7^2)$.

Αφού $\varphi(2\cdot 7^2) = 6\cdot 7 = 42 = 2\cdot 3\cdot 7$ και

$\varphi(\varphi(2\cdot 7^2)) = \varphi(2\cdot 3\cdot 7) = 2\cdot 6 = 12$

υπάρχουν 12 αρχικές ρίζες $(\mathrm{mod}\ 2\cdot 7^2)$, και είναι αυτές οι

$$3, 3^5, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{25}, 3^{29}, 3^{31}, 3^{37}, 3^{41}$$

αφού οι 12 φυσικοί $1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41$ είναι όλοι οι φυσικοί k με $1 \le k \le 2\cdot 7^2$ και $(k, 2\cdot 7^2) = 1$.

Αλλά $(\mathrm{mod}\ 2\cdot 7^2)$ έχουμε τις παρακάτω ισοτιμίες

$3 \equiv 3$	$3^{17} \equiv 25$	$3^{29} \equiv 5$
$3^5 \equiv 47$	$3^{19} \equiv 87$	$3^{31} \equiv 45$
$3^{11} \equiv 53$	$3^{23} \equiv 89$	$3^{37} \equiv 73$
$3^{13} \equiv 85$	$3^{25} \equiv 17$	$3^{41} \equiv 33$

Πιο απλά, οι 12 φυσικοί

$$3, 5, 17, 25, 33, 45, 47, 53, 73, 85, 87, 89 \qquad (*)$$

είναι όλες οι αρχικές ρίζες $(\mathrm{mod}\ 2\cdot 7^2)$ που είναι φανερά ανισότιμες ανα δύο $(\mathrm{mod}\ 2\cdot 7^2)$.

Θα παρατηρήσουμε εδώ, ότι αν ξεκινήσει κανείς με μια άλλη αρχική ρίζα $(\mathrm{mod}\ 2\cdot 7^2)$ για παράδειγμα το 5 τότε όλες οι αρχικές ρίζες δίνονται από τις δυνάμεις

$$5, 5^5, 5^{11}, 5^{13}, 5^{17}, 5^{19}, 5^{23}, 5^{25}, 5^{29}, 5^{31}, 5^{37}, 5^{41}$$

οι οποίες $(\mathrm{mod}\ 2\cdot 7^2)$ μας οδηγούν και πάλι στις 12 αρχικές ρίζες $(*)$.

2. Δείκτες

Έστω n φυσικός >1 για τον οποίο υπάρχουν αρχικές ρίζες $(\mathrm{mod} n)$, δηλαδή της μορφής $n = 2, 4, p^\beta, 2p^\beta$, p περιττός πρώτος, $\beta \geq 1$.

Αν g είναι μια αρχική ρίζα $(\mathrm{mod} n)$ τότε οι φυσικοί αριθμοί

$$1, g, g^2, \cdots, g^{\varphi(n)-1} \qquad (*)$$

αποτελούν ένα αναγμένο σύστημα υπολοίπων $(\mathrm{mod} n)$, σύμφωνα με την πρόταση 1.1. Επομένως κάθε ακέραιος a με $(a,n)=1$ θα είναι ισότιμος με ένα και μόνο ένα από τους φυσικούς $(*)$.

Αν a είναι ένας ακέραιος με $(a,n)=1$, υπάρχει μοναδικός μη-αρνητικός ακέραιος k, $0 \leq k \leq \varphi(n)-1$ έτσι ώστε

$$a \equiv g^k \ (\mathrm{mod} n)$$

Αυτόν το μη-αρνητικό ακέραιο k, τον ονομάζουμε <u>δείκτη του a ως προς την βάση g</u> και τον <u>συμβολίζουμε</u> $\mathrm{ind}_g(a)$ ή απλά $\mathrm{ind}(a)$ όταν η βάση g υπονοείται.

Ind είναι η σύντμηση του Index (=δείκτης).

Έτσι, αν $(a,n)=1$ και g μια αρχική ρίζα $(\mathrm{mod} n)$, τότε

$$\boxed{\mathrm{ind}_g(a) = k \iff a \equiv g^k \ (\mathrm{mod} n), \quad 0 \leq k \leq \varphi(n)-1}$$

Είναι λοιπόν, $g^{\mathrm{ind}_g(a)} \equiv a \ (\mathrm{mod} n)$.

Αν s είναι μη-αρνητικός ακέραιος έτσι ώστε $g^s \equiv a \ (\mathrm{mod} n)$, τότε $g^s \equiv g^{\mathrm{ind}_g(a)} \ (\mathrm{mod} n)$, επομένως, σύμφωνα με την Πρόταση 8.2 του Κεφ IV, αφού $\mathrm{ord}_n(g) = \varphi(n)$, θα είναι

$$s \equiv \mathrm{ind}_g(a) \ (\mathrm{mod}\ \varphi(n))$$

δηλαδή

$$s = \mathrm{ind}_g(a) + \lambda \cdot \varphi(n), \quad \lambda \in \mathbb{N}_0.$$

Μπορούμε να δώσουμε τον επόμενο ορισμό για τον δείκτη.

Ορισμός

Έστω g μια αρχική ρίζα $(\mathrm{mod}\, n)$. Αν $(a,n)=1$ τότε ο ελάχιστος μη-αρνητικός ακέραιος k τέτοιος ώστε

$$a \equiv g^k \ (\mathrm{mod}\, n)$$

ονομάζεται δείκτης του a ως προς την βάση g και συμβολίζεται $\mathrm{ind}_g(a)$.

Φανερά θα είναι $0 \leq \mathrm{ind}_g(a) \leq \varphi(n)-1$.

Παρατήρηση.
Κάθε αναφορά στον $\mathrm{ind}_g(a)$ $(\mathrm{mod}\, n)$ προϋποθέτει ότι ο φυσικός η έχει αρχικές ρίζες, g είναι μία αρχική ρίζα $(\mathrm{mod}\, n)$ και $(a,n)=1$.

Πρόταση 2.1

Αν $(a,n)=1$, $(b,n)=1$ και g μια αρχική ρίζα $(\mathrm{mod}\, n)$, τότε

$$a \equiv b \ (\mathrm{mod}\, n) \iff \mathrm{ind}_g(a) = \mathrm{ind}_g(b).$$

Απόδειξη.
Έστω $\mathrm{ind}_g a = \mathrm{ind}_g b$, Είναι $g^{\mathrm{ind}_g a} \equiv a \ (\mathrm{mod}\, n)$ και $g^{\mathrm{ind}_g b} \equiv b \ (\mathrm{mod}\, n)$ και επειδή $g^{\mathrm{ind}_g a} = g^{\mathrm{ind}_g b}$ θα είναι $a \equiv b \ (\mathrm{mod}\, n)$.

Αντίστροφα, έστω $a \equiv b \ (\mathrm{mod}\, n)$. Τότε θα είναι και

$$g^{\mathrm{ind}_g a} \equiv g^{\mathrm{ind}_g b} \ (\mathrm{mod}\, n).$$

Σύμφωνα με την πρόταση 82 του Κεφ IV θα είναι

$$\mathrm{ind}_g a \equiv \mathrm{ind}_g b \ (\mathrm{mod}\, \varphi(n))$$

Επειδή όμως, $0 \leq \mathrm{ind}_g a \leq \varphi(n)-1$ και $0 \leq \mathrm{ind}_g b \leq \varphi(n)-1$ η παραπάνω ισοτιμία ισχύει μόνο όταν

$$\mathrm{ind}_g a = \mathrm{ind}_g b. \ \blacksquare$$

Παράδειγμα 2.1

Εστω $n=13$, που είναι πρώτος, έχει επομένως αρχικές ρίζες.
Ο 2 είναι μια αρχική ρίζα $(\mathrm{mod}\,13)$ αφού $\mathrm{ord}_{13}(2)=\varphi(13)=12$ όπως φαίνεται απο τις παρακάτω $(\mathrm{mod}\,13)$ ισοτιμίες.

$2^1\equiv 2$ $\quad 2^5\equiv 6$ $\quad 2^9\equiv 5$
$2^2\equiv 4$ $\quad 2^6\equiv 12$ $\quad 2^{10}\equiv 10$
$2^3\equiv 8$ $\quad 2^7\equiv 11$ $\quad 2^{11}\equiv 7$
$2^4\equiv 3$ $\quad 2^8\equiv 9$ $\quad 2^{12}\equiv 1$

Εχουμε λοιπόν τον επόμενο πίνακα για δείκτες

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_2 a$	12	1	4	2	9	5	11	3	8	10	7	6

Θα βρούμε τώρα $\mathrm{ind}_2(1998)$. Είναι $(1998,13)=1$.
Διαιρώντας τον 1998 με τον 13 έχουμε

$$1998=13\cdot 153+9$$

άρα $1998\equiv 9\ (\mathrm{mod}\,13)$ και επομένως $\mathrm{ind}_2(1998)=\mathrm{ind}_2(9)=8$.
Ας χρησιμοποιήσουμε τώρα σαν βάση άλλη αρχική ρίζα $(\mathrm{mod}\,13)$
Υπάρχουν $\varphi(\varphi(13))=\varphi(12)=4$ αρχικές ρίζες $(\mathrm{mod}\,13)$ και δίνονται απο τις δυνάμεις

$2\equiv 2\,(\mathrm{mod}\,13)$, $2^5\equiv 6\,(\mathrm{mod}\,13)$, $2^7\equiv 11\,(\mathrm{mod}\,13)$, $2^{11}\equiv 7\,(\mathrm{mod}\,13)$

Ο 7 είναι λοιπόν μια άλλη αρχική ρίζα $(\mathrm{mod}\,13)$ Εχουμε $(\mathrm{mod}\,13)$ τις επόμενες ισοτιμίες

$7^1\equiv 7$ $\quad 7^5\equiv 11$ $\quad 7^9\equiv 8$
$7^2\equiv 10$ $\quad 7^6\equiv 12$ $\quad 7^{10}\equiv 4$
$7^3\equiv 5$ $\quad 7^7\equiv 6$ $\quad 7^{11}\equiv 2$
$7^4\equiv 9$ $\quad 7^8\equiv 3$ $\quad 7^{12}\equiv 1$.

Εχουμε τώρα τον επόμενο πίνακα για δείκτες

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_7 a$	12	11	8	10	3	7	1	9	4	2	5	6

Έτσι $\text{ind}_7(1998) = \text{ind}_7(9) = 4$ που είναι διαφορετικό από τον $\text{ind}_2(1998) = 8$.

Το επόμενο θεώρημα δείχνει ότι ο λογισμός με τους δείκτες παρουσιάζει πλήρη αναλογία προς τον γνωστό λογισμό με τους <u>λογαριθμους</u> ως προς δοθείσα βάση.

<u>Θεώρημα 2.1</u>

Έστω g μια αρχική ρίζα $(\text{mod } n)$. Τότε ισχύουν τα ακόλουθα

i) $\text{ind}_g(ab) \equiv \text{ind}_g a + \text{ind}_g b \pmod{\varphi(n)}$

ii) $\text{ind}_g(a^s) \equiv s \cdot \text{ind}_g a \pmod{\varphi(n)}$, για κάθε φυσικό s.

iii) $\text{ind}_g 1 = 0$ και $\text{ind}_g g = 1$

iv) $\text{ind}_g a \equiv (\text{ind}_h a)(\text{ind}_g h) \pmod{\varphi(n)}$

όπου h μια άλλη αρχική ρίζα $(\text{mod } n)$.

Απόδειξη.

i) Έστω $\text{ind}_g a = k$ και $\text{ind}_g b = s$ τότε $g^k \equiv a \pmod n$ και $g^s \equiv b \pmod n$ άρα $ab \equiv g^{k+s} \pmod n$. Αν $\text{ind}_g(ab) = r$ τότε $ab \equiv g^r \pmod n$. Είναι λοιπόν $g^r \equiv g^{k+s} \pmod n$ και επομένως $r \equiv k+s \pmod{\varphi(n)}$ δηλαδή $\text{ind}_g(ab) \equiv (\text{ind}_g a)(\text{ind}_g b) \pmod{\varphi(n)}$.

ii) Αν $\text{ind}_g a = k$ τότε $g^k \equiv a \pmod n$ και επομένως $g^{ks} \equiv a^s \pmod n$

Αν $\text{ind}_g(a^s) = \lambda$ τότε $g^\lambda \equiv a^s \pmod n$, άρα $g^\lambda \equiv g^{ks} \pmod n$

συνεπώς $\lambda \equiv ks \pmod{\varphi(n)}$, δηλαδή,

$$\text{ind}_g(a^s) \equiv s \cdot \text{ind}_g a \pmod{\varphi(n)}$$

iii) Αν $\text{ind}_g 1 = k$ τότε $g^k \equiv 1 = g^0 \pmod n$, άρα $k \equiv 0 \pmod{\varphi(n)}$ και επειδή $0 \le k \le \varphi(n) - 1$ θα είναι $k = 0$. Άρα $\text{ind}_g 1 = 0$

Αν $ind_g g = k$ τότε $g^k \equiv g^1 \pmod n$ άρα $k \equiv 1 \pmod{\varphi(n)}$ και επειδή $0 \le k \le \varphi(n)-1$ θα είναι $k=1$.

iv) Αν $ind_h a = k$ και $ind_g h = \lambda$ τότε $h^k \equiv a \pmod n$ και $g^\lambda \equiv h \pmod n$, επομένως $g^{k\lambda} \equiv h^k \equiv a \pmod n$. Αν τώρα $ind_g a = s$ τότε $g^s \equiv a \pmod n$. Άρα $s \equiv k\lambda \pmod{\varphi(n)}$ δηλαδή

$$ind_g a \equiv (ind_h a)(ind_g h) \pmod{\varphi(n)}. \blacksquare$$

Παράδειγμα 2.2

Έστω $n=13$. Είναι $\varphi(13)=12$, και ο 2 και 7 είναι αρχικές ρίζες $(mod 13)$ όπως είδαμε στο παράδειγμα 2.1. Τότε

$$ind_2(35\cdot 11) \equiv ind_2(35) + ind_2(11) \pmod{12}.$$

Αλλά $ind_2(35) = ind_2(9) = 8$ αφού $35 \equiv 9 \pmod{13}$

και $ind_2(11) = 7$, όπως φαίνεται από τον πίνακα δεικτών του παραδείγματος 2.1 Έτσι

$$ind_2(35\cdot 11) \equiv 8+7 \pmod{12}$$ δηλαδή $ind_2(35\cdot 11) \equiv 15 \equiv 3 \pmod{12}$

και επειδή $0 \le ind_2(35\cdot 11) \le 12$ θα είναι $ind_2(35\cdot 11) = 3$.

Αυτό μπορούμε να το δούμε και διαφορετικά. Είναι

$35\cdot 11 = 385 = 13\cdot 29 + 8$ άρα $35\cdot 11 \equiv 8 \pmod{13}$ και επομένως $ind_2(35\cdot 11) = ind_2(8) = 3$.

Θα υπολογίσουμε τώρα τον $ind_2(35^4)$. Είναι

$$ind_2(35^4) \equiv 4\, ind_2(35) \equiv 4\cdot 8 = 32 \equiv 8 \pmod{12}$$

και επειδή $0 \le ind_2(35^4) \le 12$ είναι $ind_2(35^4) = 8$.

Επίσης επειδή $ord_2(9) = 8$, θα είναι $35^4 \equiv 9 \pmod{13}$.

Θα υπολογίσουμε τώρα τον $ind_7(1998)$. Είναι

$$ind_7(1998) \equiv ind_2(1998)\cdot ind_7(2) \pmod{12}$$

Αλλά $ind_2(1998) = 8$ και $ind_7(2) = 11$, από παράδειγμα 2.1.

Έτσι $\text{ind}_7(1998) \equiv 8 \cdot 11 = 88 \equiv 4 \pmod{12}$ και υποχρεωτικά $\text{ind}_7(1998) = 4$, ένα αποτέλεσμα που είδαμε και στο παράδειγμα 2.1.

Πρόταση 2.2

Έστω g μια αρχική ρίζα $(\text{mod } n)$. Αν $n > 2$ τότε

$$\text{ind}_g(-1) = \frac{\varphi(n)}{2}$$

Απόδειξη

Ο φυσικός $n > 2$, έχει αρχικές ρίζες, θα είναι επομένως της μορφής $n = 4, p^\beta, 2p^\beta$ όπου p περιττός πρώτος και $\beta \geq 1$.

Έστω $n = 4$. Ο 3 είναι η μοναδική αρχική ρίζα $(\text{mod } 4)$. Κάθε άλλη αρχική ρίζα g $(\text{mod } 4)$ θα είναι $g \equiv 3 \equiv -1 \pmod 4$. Επομένως

$$\text{ind}_g(-1) = \text{ind}_g g = 1 = \frac{\varphi(4)}{2}.$$

Έστω τώρα $n = p^\beta$ ή $2p^\beta$, όπου p περιττός πρώτος και $\beta \geq 1$.

Αν g είναι μια αρχική ρίζα $(\text{mod } n)$ τότε $g^{\varphi(n)} \equiv 1 \pmod n$, επομένως $\left(g^{\varphi(n)} - 1\right) \equiv 0 \pmod n$ δηλαδή $\left(g^{\frac{\varphi(n)}{2}} - 1\right)\left(g^{\frac{\varphi(n)}{2}} + 1\right) \equiv 0 \pmod n$

Υποχρεωτικά λοιπόν, είτε $n = p^\beta$ ή $2p^\beta$ θα έχουμε

$$p^\beta \mid \left(g^{\frac{\varphi(n)}{2}} - 1\right)\left(g^{\frac{\varphi(n)}{2}} + 1\right). \qquad (*)$$

Παρατηρούμε ότι, αν $p \mid g^{\frac{\varphi(n)}{2}} - 1$ και $p \mid g^{\frac{\varphi(n)}{2}} + 1$ τότε ο p θα διαιρεί και το αθροισμά τους, δηλαδή $p \mid 2$, πράγμα άτοπο, αφού $p > 2$. Λόγω της $(*)$ ο p θα διαιρεί ένα εκ των δύο, και επομένως μία ακριβώς από τις σχέσεις

$$p^\beta \mid g^{\frac{\varphi(n)}{2}} - 1 \quad \text{και} \quad p^\beta \mid g^{\frac{\varphi(n)}{2}} + 1$$

αληθεύει. Θέλουμε να δείξουμε ότι $p^\beta \mid g^{\frac{\varphi(n)}{2}} + 1$. Υποθέτουμε ότι $p^\beta \mid g^{\frac{\varphi(n)}{2}} - 1$, θα καταλήξουμε σε άτοπο.

Αν $n = p^\beta$, τότε είναι $n \mid g^{\frac{\varphi(n)}{2}} - 1$.

Αν $n = 2p^\beta$, τότε, επειδή για την αρχική ρίζα g $(\text{mod } 2p^\beta)$

είναι $(g, 2p^\beta)=1$, ο g είναι υποχρεωτικά περιττός αριθμός. Άρα ο $\left(g^{\frac{\varphi(n)}{2}}-1\right)$ είναι άρτιος, δηλαδή $2 \mid g^{\frac{\varphi(n)}{2}}-1$.

Επειδή $(2, p^\beta)=1$, θα είναι και $2p^\beta \mid g^{\frac{\varphi(n)}{2}}-1$ άρα $n \mid g^{\frac{\varphi(n)}{2}}-1$.

Επομένως είτε $n=p^\beta$ ή $2p^\beta$ θα έχουμε

$$g^{\frac{\varphi(n)}{2}} \equiv 1 \pmod n$$

πράγμα άτοπο, αφού ο g είναι αρχική ρίζα $(\mathrm{mod} n)$.

Άρα υποχρεωτικά

$$p^\beta \mid g^{\frac{\varphi(n)}{2}}+1.$$

Αν $n=p^\beta$ τότε είναι $n \mid g^{\frac{\varphi(n)}{2}}+1$

Αν $n=2p^\beta$ τότε όμοια, όπως και προηγουμένως, $2p^\beta \mid g^{\frac{\varphi(n)}{2}}+1$

όποτε $n \mid g^{\frac{\varphi(n)}{2}}+1$.

Επομένως είτε $n=p^\beta$ είτε $n=2p^\beta$, έχουμε

$$g^{\frac{\varphi(n)}{2}} \equiv -1 \pmod n$$

δηλαδή $\mathrm{ind}_g(-1) = \frac{\varphi(n)}{2}$. ■

Παράδειγμα 2.3

Αν $n=13$, τότε $-1 \equiv 12 \pmod{13}$. Σύμφωνα με το παράδειγμα 2.1 το 2 είναι αρχική ρίζα $(\mathrm{mod} 13)$ και επομένως

$$\mathrm{ind}_2(-1) = \mathrm{ind}_2(12) = 6 = \frac{\varphi(13)}{2}.$$

όπως φαίνεται από τον πίνακα δεικτών στο παράδειγμα 2.1.

Όμοια για την αρχική ρίζα $7 \pmod{13}$ είναι

$$-1 \equiv 12 \pmod{13}$$ οπότε

$$\mathrm{ind}_7(-1) = \mathrm{ind}_7(12) = 6 = \frac{\varphi(n)}{2}. ■$$

2α | Χρήση της θεωρίας δεικτών στην επίλυση ορισμένου τύπου ισοτιμιών (mod n), όταν υπάρχουν αρχικές ρίζες (mod n).

Υπενθυμίζουμε ότι ο φυσικός $n>1$ έχει αρχικές ρίζες αν και μόνο αν ο $n = 2, 4, p^\beta, 2p^\beta$ όπου p περιττός πρώτος και $\beta \geq 1$.

A) Γραμμικές ισοτιμίες.

Αν ο φυσικός $n>1$ έχει αρχικές ρίζες, τότε η γραμμική ισοτιμία

$$ax \equiv b \pmod n \qquad (I)$$

όπου $(a,n)=(b,n)=1$ μπορεί να επιλυθεί με την χρήση της θεωρίας δεικτών.

Στην περίπτωση αυτή η (I) έχει μοναδική λύση. Αν g είναι μια αρχική ρίζα (mod n), παίρνοντας τους δείκτες, ως προς την βάση g, των δύο μερών της (I), έχουμε

$$\operatorname{ind}_g(ax) = \operatorname{ind}_g b$$

και επειδή $\operatorname{ind}_g(ax) \equiv \operatorname{ind}_g a + \operatorname{ind}_g x \pmod{\varphi(n)}$

θα είναι $\operatorname{ind}_g a + \operatorname{ind}_g x \equiv \operatorname{ind}_g b \pmod{\varphi(n)}$

και επομένως, ο x είναι μοναδικά ορισμένος από την ισοτιμία

$$\operatorname{ind}_g x \equiv \operatorname{ind}_g b - \operatorname{ind}_g a \pmod{\varphi(n)}.$$

Παράδειγμα 2.4

Θα επιλύσουμε την γραμμική ισοτιμία

$$11x \equiv 51 \pmod{2\cdot 41}.$$

Είναι $(11, 2\cdot 41) = (51, 2\cdot 41) = 1$ και ο 47 είναι μια αρχική ρίζα (mod $2\cdot 41$) σύμφωνα με το πόρισμα 1.8 και το γεγονός ότι ο 6 είναι μια αρχική ρίζα (mod 41).

Υπολογίζοντας τις δυνάμεις του 47, έχουμε (mod $2\cdot 41$) τις ισοτιμίες

$47^1 \equiv 47$, $47^3 \equiv 11$, $47^5 \equiv 27$, $47^7 \equiv 29$
$47^2 \equiv 77$, $47^4 \equiv 25$, $47^6 \equiv 39$, $47^8 \equiv 51$, ...

Καταστενάζουμε πίνακα δεικτών με βάση τον 47

a	47	77	11	25	27	39	29	51	...
$\text{ind}_{47} a$	1	2	3	4	5	6	7	8	...

Παίρνοντας τους δείκτες ως προς την βάση 47, έχουμε

$$\text{ind}_{47} x \equiv \text{ind}_{47} 51 - \text{ind}_{47} 11 \pmod{\varphi(2.41)}$$

Άρα $$\text{ind}_{47} x \equiv 8 - 3 = 5 \pmod{40}$$

δηλαδή $$\text{ind}_{47} x \equiv \text{ind}_{47} 27 \pmod{40}$$

και υποχρεωτικά

$$\text{ind}_{47} x = \text{ind}_{47} 27 .$$

Επομένως, $x \equiv 27 \pmod{2.41}$ σύμφωνα με την πρόταση 2.1 που είναι η μοναδική λύση της γραμμικής ισοτιμίας. ■

Αν ο φυσικός n έχει αρχικές ρίζες και $(a, n) = 1$, τότε η εύρεση του υπολοίπου της διαίρεσης του a με τον n, δηλαδή η εύρεση μη-αρνητικού ακεραίου x , $0 \le x < 13$ έτσι ώστε

$$x \equiv a \pmod{n}$$

μπορεί να πραγματοποιηθεί με την χρήση θεωρίας δεικτών.

Παράδειγμα 2.8.

Να βρεθεί το υπόλοιπο της διαίρεσης του 7^{10^6} με τον 13.

Ο 2 είναι μία αρχική ρίζα (mod 13) και $(7^{10^6}, 13) = 1$.

Αναζητούμε x , $0 \le x < 13$ ώστε

$$x \equiv 7^{10^6} \pmod{13}.$$

Αυτή είναι ισοδύναμη με την $\text{ind}_2 x = \text{ind}_2 (7^{10^6})$

Άλλα, $\text{ind}_2 (7^{10^6}) \equiv 10^6 . \text{ind}_2 (7)$

και επειδή, $10^6 \equiv (-2)^6 \equiv 4 \pmod{12}$ και $\text{ind}_2 7 = 11$
θα είναι $\text{ind}_2 x \equiv 4 \cdot 11 \equiv 8 \pmod{12}$ και υποχρεωτικά
$\text{ind}_2 x = 8 = \text{ind}_2 9$, άρα $x \equiv 9 \pmod{13}$, και από τον περιορισμό που έχουμε για το x, θα είναι $x = 9$. ■

Β) Εκθετικές ισοτιμίες

Αν ο φυσικός $n > 1$ έχει αρχικές ρίζες, κάνοντας χρήση της θεωρίας δεικτών μπορούμε να επιλύσουμε μια εκθετική ισοτιμία

$$a^x \equiv b \pmod{n}$$

όπου $(a, n) = (b, n) = 1$.

Αν g είναι μια αρχική ρίζα $\pmod{n}$, τότε θα είναι

$$\text{ind}_g(a^x) = \text{ind}_g b$$

και επειδή

$$\text{ind}_g(a^x) \equiv x \cdot \text{ind}_g a \pmod{\varphi(n)}$$

θα έχουμε την γραμμική ισοτιμία

$$(\text{ind}_g a)\, x \equiv \text{ind}_g b \pmod{\varphi(n)}.$$

που είναι ισοδύναμη με την εκθετική ισοτιμία.

Αυτή η γραμμική ισοτιμία έχει λύση αν και μόνο αν ο $d = (\text{ind}_g a, \varphi(n))$ διαιρεί τον $\text{ind}_g b$. Στην περίπτωση αυτή έχει d αριθμώς λύσεις $\pmod{\varphi(n)}$.

Παράδειγμα 2.5

Θα βρούμε τις λύσεις της εκθετικής ισοτιμίας

$$5^x \equiv 25 \pmod{26}.$$

Ο $26 = 2 \cdot 13$ και επομένως έχει αρχικές ρίζες. Ο 7 είναι μια περιττή αρχική ρίζα $\pmod{13}$ άρα είναι και αρχική ρίζα $\pmod{2 \cdot 13}$.
Παίρνοντας τις δυνάμεις του 7, έχουμε $\pmod{26}$ τις ισοτιμίες

$$7^1 \equiv 7, \quad 7^3 \equiv 5, \quad 7^5 \equiv 9, \quad 7^{12} \equiv 1$$
$$7^2 \equiv 23, \quad 7^4 \equiv 9, \quad 7^6 \equiv 25 \equiv -1,$$

Η εκθετική ισοτιμία είναι ισοδύναμη με την γραμμική ισοτιμία

$$(\mathrm{ind}_7 5)\cdot x \equiv \mathrm{ind}_7 25 \pmod{\varphi(26)}$$

αφού $(5,26)=(25,26)=1$, δηλαδή με την $3x\equiv 6 \pmod{12}$.
Αφού $(3,12)=3$ και $3|6$, αυτή έχει 3 λύσεις (mod12) τις $x\equiv 2,6,10 \pmod{12}$. ■

Γ. Διωνυμικές ισοτιμίες

Οι πολυωνυμικές ισοτιμίες της μορφής

$$bx^m \equiv a \pmod{n}$$

ονομάζονται διωνυμικές ισοτιμίες.

Θα μας απασχολήσουν διωνυμικές ισοτιμίες όπου, $(b,n)=(a,n)=1$ και ο φυσικός $n>1$ έχει αρχικές ρίζες.

Πρόταση 2.3

Αν ο φυσικός $n>1$ έχει αρχικές ρίζες και a ακέραιος με $(a,n)=1$ τότε η διωνυμική ισοτιμία

$$x^m \equiv a \pmod{n} \qquad (I)$$

έχει μία λύση αν και μόνο αν $d \mid \mathrm{ind}a$, όπου $d=(m,\varphi(n))$.
Αν υπάρχει μία λύση της (I) τότε υπάρχουν ακριβώς d λύσεις (mod n) της (I). Διαφορετικά η (I) δεν έχει λύση.

Απόδειξη.

Αν εκλέξουμε μια αρχική ρίζα (mod n) και πάρουμε τους δείκτες των δύο μερών της (I) έχουμε $\mathrm{ind}(x^m)=\mathrm{ind}(a)$. Η (I) είναι λοιπόν ισοδύναμη με την γραμμική ισοτιμία

$$m\cdot \mathrm{ind}x \equiv \mathrm{ind}a \pmod{\varphi(n)} \qquad (II)$$

(ως προς τον άγνωστο indx).

Η (II) έχει λύση αν και μόνο αν $d \mid \mathrm{ind}a$.
Στην περίπτωση αυτή, υπάρχουν d διαφορετικές τιμές του $\mathrm{ind}a$ που ικανοποιούν την (II) και επομένως d λύσεις (mod n) της (I). Διαφορετικά, η (I) δεν έχει λύση. ■

Το επόμενο κριτήριο επιλυσιμότητας είναι πολύ χρήσιμο.

Θεώρημα 2.2

Αν ο φυσικός $n>1$ έχει αρχικές ρίζες και a ακέραιος με $(a,n)=1$, τότε η διωνυμική ισοτιμία

$$x^m \equiv a \pmod n \qquad (I)$$

έχει λύση αν και μόνο αν

$$a^{\varphi(n)/d} \equiv 1 \pmod n \qquad (III)$$

όπου $d=(m,\varphi(n))$.

Αν η (I) έχει μία λύση τότε αυτή έχει ακριβώς d λύσεις $(\mathrm{mod}\, n)$. Διαφορετικά η (I) δεν έχει λύση.

Απόδειξη.

Με την χρήση της θεωρίας δεικτών έχουμε

$$a^{\varphi(n)/d} \equiv 1 \pmod n \iff \mathrm{ind}(a^{\varphi(n)/d}) = \mathrm{ind}\, 1 = 0 \iff$$

$$\frac{\varphi(n)}{d}\cdot \mathrm{ind}\, a \equiv 0 \pmod{\varphi(n)}.$$

Η τελευταία ισοτιμία πληρούται αν και μόνο αν $d \mid \mathrm{ind}\, a$. Αυτό όμως, όπως είδαμε στην πρόταση 2.3 είναι η ικανή και αναγκαία συνθήκη για να έχει η (I) λύση. Διαφορετικά, αν $a^{\varphi(n)/d} \not\equiv 1 \pmod n$ τότε $d \nmid \mathrm{ind}\, a$ και επομένως η (I) δεν έχει λύση. ∎

Πόρισμα 2.1 (Euler).

Έστω p πρώτος και a ακέραιος με $(a,p)=1$. Η διωνυμική ισοτιμία

$$x^m \equiv a \pmod p$$

έχει λύση, αν και μόνο αν

$$a^{p-1/d} \equiv 1 \pmod p$$

όπου $d=(m,p-1)$. Αν έχει μία λύση τότε έχει ακριβώς d λύσεις $(\mathrm{mod}\, p)$. Διαφορετικά, αν $a^{p-1/d} \not\equiv 1 \pmod p$ τότε αυτή δεν έχει λύση. ∎

Παράδειγμα 2.6

Θα λύσουμε την διωνυμική ισοτιμία $x^9 \equiv 5 \pmod{13}$.

Ο 13 είναι πρώτος, έχει επομένως αρχικές ρίζες. Είναι $(5,13)=1$, ο $\varphi(13)=12$ και $d=(9,\varphi(13))=(9,12)=3$. Αφού

$$5^{12/3} = 5^4 \equiv 1 \pmod{13},$$

σύμφωνα με το θεώρημα 2.2 αυτή είναι επιλύσιμη.

Επιλέγουμε τώρα μια αρχική ρίζα(mod13). Ο 2 είναι μια αρχική ρίζα(mod13) από το παράδειγμα 2.1.

Η διωνυμική ισοτιμία είναι ισοδύναμη με την γραμμική ισοτιμία

$$9 \cdot \mathrm{ind}_2 x \equiv \mathrm{ind}_2 5 \pmod{\varphi(13)}$$

δηλαδή την $\quad 9 \cdot \mathrm{ind}_2 x \equiv 9 \pmod{12}$.

Επειδή $(9,12)=3$ διαιρεί το 9, αυτή έχει 3 λύσεις τις.

$\mathrm{ind}_2 x \equiv 1, 5, 9 \pmod{12}$ και επειδή $0 \le \mathrm{ind}_2 x \le 12$

αυτές είναι οι $\mathrm{ind}_2 x = 1, 5, 9$.

Αν $\mathrm{ind}_2 x = 1 = \mathrm{ind}_2 2$ τότε $x \equiv 2 \pmod{13}$

$\mathrm{ind}_2 x = 5 = \mathrm{ind}_2 6$ τότε $x \equiv 6 \pmod{13}$

$\mathrm{ind}_2 x = 9 = \mathrm{ind}_2 5$ τότε $x \equiv 5 \pmod{13}$.

Η διωνυμική ισοτιμία έχει 3 λύσεις τις $x \equiv 2, 5, 6 \pmod{13}$.

Παράδειγμα 2.7

Να επιλυθεί η διωνυμική ισοτιμία $x^9 \equiv 7 \pmod{13}$

Ο 13 έχει αρχικές ρίζες, $(7,13)=1$, $d=(9,\varphi(13))=(9,12)=3$

αλλά

$$7^{12/3} = 7^4 \equiv 9 \not\equiv 1 \pmod{13}$$

οπότε η διωνυμική ισοτιμία δεν έχει λύση.

Παρατήρηση.

Το κριτήριο επιλυσιμότητας του θεωρήματος 2.2 αφορά μέτρα $n>1$ που έχουν αρχικές ρίζες, δηλαδή που είναι της μορφής $n = 2, 4, p^\beta, 2p^\beta$, p περιττός πρώτος και β φυσικός ≥ 1.

Αν ο φυσικός $n>1$ έχει αρχικές ρίζες, τότε η διωνυμική ισοτιμία

$$bx^m \equiv a \pmod{n}, \quad (1)$$

όπου $(b,n)=(a,n)=1$, μπορεί να επιλυθεί με την χρήση της θεωρίας δεικτών.

Πραγματικά, αφού $(b,n)=1$ μπορούμε να βρούμε ακέραιο b' έτσι ώστε $b'b \equiv 1 \pmod{n}$, οπότε και $(b',n)=1$.

Άρα,

$$bx^m \equiv a \pmod{n} \iff b'bx^m \equiv b'a \pmod{n} \iff$$

$$x^m \equiv b'a \pmod{n}, \quad (2)$$

όπου $(b'a,n)=1$.

Η διωνυμική ισοτιμία (1) είναι ισοδύναμη με την διωνυμική ισοτιμία (2), την οποία όμως μπορούμε να επιλύσουμε με την χρήση της θεωρίας δεικτών, όπως είδαμε στα προηγούμενα.

Παράδειγμα 2.8

Θα επιλύσουμε την διωνυμική ισοτιμία

$$4x^9 \equiv 7 \pmod{13}$$

Ο 13 έχει αρχικές ρίζες. Είναι $(4,13)=(7,13)=1$.

Είναι $13=4\cdot 3+1$ άρα $4\cdot 3 \equiv -1 \pmod{13}$ και επομένως $(-3)4 \equiv 1 \pmod{13}$. Πολλαπλασιάζοντας και τα δύο μέλη της ισοτιμίας με (-3) έχουμε

$$(-12)x^9 \equiv -21 \pmod{13}$$

Αλλά $-12 \equiv 1 \pmod{13}$ και $-21 \equiv 5 \pmod{13}$.

Η διωνυμική ισοτιμία είναι ισοδύναμη με την

$$x^9 \equiv 5 \pmod{13}$$

που έχει λύσεις τις $x \equiv 2, 5, 6 \pmod{13}$ σύμφωνα με το παράδειγμα 2.6. ■

3. m-αδικα υπόλοιπα (mod n)

Ορισμός

Έστω φυσικός $n>1$. Ένας ακέραιος a με $(a,n)=1$, λεγεται m-αδικο υπόλοιπο (mod n), $m \in \mathbb{N}$, αν η διωνυμική ισοτιμία

$$x^m \equiv a \pmod n \qquad (*)$$

επιδέχεται μια τουλάχιστον λύση.

Αν η (*) δεν έχει λύση, θα λέμε ότι ο a είναι ένα m-αδικο μη-υπόλοιπο (mod n)

Στην βιβλιογραφία, τα m-αδικα υπόλοιπα (mod n) αναφέρονται και ως m-αδικα υπόλοιπα του η ή υπόλοιπα m-στης δύναμης (mod n).

Ιδιαίτερα για $m=2,3,4$ τα m-αδικά υπόλοιπα και μη-υπόλοιπα ονομάζονται τετραγωνικά, κυβικά, δις-τετραγωνικα αντίστοιχα.

Στο επόμενο κεφάλαιο θα ασχοληθούμε λεπτομερώς με τα τετραγωνικά υπόλοιπα.

Αν ο a είναι ένα m-αδικο υπόλοιπο (mod n) και $b \equiv a \pmod n$ τότε και ο b είναι ένα m-αδικο υπόλοιπο (mod n).

Διαφορετικά θεωρούνται δυό m-αδικά υπόλοιπα (mod n) a και b αν και μόνο αν $a \not\equiv b \pmod n$.

Αν λοιπόν a είναι ένα m-αδικο υπόλοιπο (mod n) και το

$$\{a_1, a_2, \ldots, a_{\varphi(n)}\}$$

είναι ένα αναγμένο σύστημα υπολοίπων (mod n), αφού $(a,n)=1$, ο a θα είναι ισότιμος (mod n) με έναναμφιβώς από τους ακεραίους $\{a_1, \ldots, a_{\varphi(n)}\}$, επομένως αν υπάρχουν m-αδικα υπόλοιπα (mod n), το πλήθος των διακεκριμένων m-αδικών υπολοίπων (mod n) είναι $\leq \varphi(n)$.

Για παράδειγμα, ο 1 είναι m-αδικό υπόλοιπο $(\mathrm{mod}\, n)$ για κάθε φυσικό m, αφού η διωνυμική ισοπμία $x^m \equiv 1 (\mathrm{mod}\, n)$ έχει πάντα λύση. Ο 39 είναι 6-αδικό υπόλοιπο $(\mathrm{mod}\, 82)$, αφού $(39, 68) = 1$ και $47^6 \equiv 39 (\mathrm{mod}\, 82)$.

Στην περίπτωση που ο φυσικός $n > 1$ <u>έχει αρχικές ρίζες, έχου-</u> με το επόμενο <u>κριτήριο</u> για να ελέγχουμε αν ένας ακέραιος είναι m-αδικό υπόλοιπο $(\mathrm{mod}\, n)$.

<u>Θεώρημα 3.1</u>

Έστω $n = 2, 4, p^k, 2p^k$, p περιττός πρώτος και $k \in \mathbb{N}$.
Αν $a \in \mathbb{Z}$ με $(a, n) = 1$ και $d = (m, \varphi(n))$, <u>τότε ο a είναι ένα m-αδικό υπόλοιπο $(\mathrm{mod}\, n)$ αν και μόνο αν,</u>

$$a^{\varphi(n)/d} \equiv 1 (\mathrm{mod}\, n).$$

Αν a είναι ένα m-αδικό υπόλοιπο $(\mathrm{mod}\, n)$ τότε αυτό είναι m-στη δύναμη ακριβώς d ακεραίων $(\mathrm{mod}\, n)$.

Απόδειξη

Η απόδειξη είναι άμεση συνέπεια του θεωρήματος 2.2. ■

Αν ο φυσικός $n > 1$ έχει αρχικές ρίζες, η επόμενη πρόταση μας καθορίζει τα διαφορετικά m-αδικά υπόλοιπα $(\mathrm{mod}\, n)$.

<u>Πρόταση 3.1</u>

Έστω $n = 2, 4, p^k, 2p^k$, p περιττός πρώτος, $k \geq 1$.
Αν $m \in \mathbb{N}$ και $d = (m, \varphi(n))$, τότε υπάρχουν $\frac{\varphi(n)}{d}$ σε πλήθος διακεκριμένα m-αδικά υπόλοιπα $(\mathrm{mod}\, n)$.
Αν g είναι μια αρχική ρίζα $(\mathrm{mod}\, n)$, τότε οι ακέραιοι

$$g^d, g^{2d}, \ldots, g^{\frac{\varphi(n)}{d} \cdot d}$$

είναι όλα τα διακεκριμένα m-αδικά υπόλοιπα.

Απόδειξη.

Ο ακέραιος a με $(a,n)=1$ είναι m-αδικό υπόλοιπο $(\mathrm{mod}\, n)$ αν και μόνο αν

$$a^{\varphi(n)/d} \equiv 1 \ (\mathrm{mod}\, n)$$

σύμφωνα με το θεώρημα 3.1.

Υπάρχουν λοιπόν τόσα διακεκριμένα m-αδικα υπόλοιπα $(\mathrm{mod}\, n)$ όσες είναι και οι διακεκριμένες λύσεις της διωνυμικής ισοτιμίας

$$x^{\varphi(n)/d} \equiv 1 \ (\mathrm{mod}\, n) \qquad (*)$$

Αφού $\left(\frac{\varphi(n)}{d}, \varphi(n)\right) = \frac{\varphi(n)}{d}$ και $1^{\varphi(n)/d} \equiv 1 \ (\mathrm{mod}\, n)$, σύμφωνα με το θεώρημα 2.2, η $(*)$ έχει ακριβώς $\frac{\varphi(n)}{d}$ λύσεις $(\mathrm{mod}\, n)$ άρα υπάρχουν $\frac{\varphi(n)}{d}$ διακεκριμένα m-αδικά υπόλοιπα $(\mathrm{mod}\, n)$.

Αν g είναι μια αρχική ρίζα $(\mathrm{mod}\, n)$ τότε οι $\frac{\varphi(n)}{d}$ σε πλήθος ακέραιοι,

$$g^d, g^{2d}, \ldots, g^{\frac{\varphi(n)}{d}\cdot d}$$

είναι ανισότιμοι ανα δύο $(\mathrm{mod}\, n)$ και ικανοποιούν την $(*)$ άρα είναι όλα τα m-αδικά υπόλοιπα $(\mathrm{mod}\, n)$. ■

Παράδειγμα 3.1

Θα προσδιορίσουμε όλα τα 7-αδικά υπόλοιπα $(\mathrm{mod}\, 2\cdot 7^2)$

Είναι $\varphi(2\cdot 7^2) = \varphi(98) = 42$ και $d=(7,42)=7$. Ο ακέραιος $2\cdot 7^2$ έχει αρχικές ρίζες και σύμφωνα με το Παράδειγμα 1.7 ο 3 είναι μια αρχική ρίζα $(\mathrm{mod}\, 2\cdot 7^2)$. Υπάρχουν επομένως

$\frac{\varphi(2\cdot 7^2)}{d} = \frac{42}{7} = 6$, 7-αδικα υπόλοιπα $(\mathrm{mod}\, 2\cdot 7^2)$

και είναι αυτά, οι $3^7, 3^{14}, 3^{21}, 3^{28}, 3^{35}, 3^{42}$.

Αλλά $3^7 \equiv 11 \ (\mathrm{mod}\, 98)$, $3^{14} \equiv 79 \ (\mathrm{mod}\, 98)$, $3^{21} \equiv 97 \ (\mathrm{mod}\, 98)$

$3^{28} \equiv 67 \ (\mathrm{mod}\, 98)$, $3^{35} \equiv 19 \ (\mathrm{mod}\, 98)$, $3^{42} \equiv 1 \ (\mathrm{mod}\, 98)$.

Άρα τα διακεκριμένα 7-αδικα υπόλοιπα $(\mathrm{mod}\, 98)$ είναι τα επόμενα, $1, 19, 31, 67, 79, 97 \ (\mathrm{mod}\, 98)$.

Ένας άλλος τρόπος εντοπισμού των 7-αδικών υπολοίπων (mod $2\cdot 7^2$) αρκεί επίσης είναι ο εξής: Τα 7-αδικά υπόλοιπα (mod $2\cdot 7^2$) είναι οι ακέραιοι a με $(a,98)=1$ και $a^{42/7}=a^6\equiv 1 \pmod{98}$.

Οι ακέραιοι K, με $1\le K\le 97$ και $(K,98)=1$ που είναι σε πλήθος $\varphi(98)=42$ αποτελούν ένα αναγμένο σύστημα υπολοίπων (mod 98). Υπολογίζοντας τις 6 δυνάμεις τους (mod 98) βρίσκουμε ότι μόνο οι ακέραιοι $1,19,31,67,79,97$ επαληθεύουν την ισοτιμία $a^6\equiv 1 \pmod{98}$.

Έτσι τα διακεκριμένα 7-αδικά υπόλοιπα (mod 98) είναι τα $1,19,31,67,79,97 \pmod{98}$. ■

Πρόταση 3.2

Έστω p περιττός πρώτος και β φυσικός ≥ 1.

Αν $a\in\mathbb{Z}$ με $p\nmid a$ και m φυσικός ≥ 2 με $p\nmid m$, τότε η διωνυμική ισοτιμία

$$x^m\equiv a \pmod{p^\beta} \qquad (I)$$

έχει λύση αν και μόνο η διωνυμική ισοτιμία

$$x^m\equiv a \pmod{p} \qquad (II)$$

έχει λύση

Απόδειξη.

Είναι φανερό ότι αν η (I) έχει λύση τότε και η (II) έχει λύση.

Αντίστροφα, ας υποθέσουμε ότι η (II) έχει λύση. Θα δείξουμε ότι για κάθε φυσικό β η (I) έχει λύση. Θα εργασθούμε επαγωγικά.

Για $\beta=1$ ισχύει. Υποθέτουμε ότι για τον φυσικό $\beta>1$ η διωνυμική ισοτιμία (I) έχει λύση. Θα δείξουμε ότι και η διωνυμική ισοτιμία

$$x^m\equiv a \pmod{p^{\beta+1}}$$

έχει λύση.

Αν $d=(m,\varphi(p^\beta))=(m,p^{\beta-1}(p-1))=(m,p-1)$ αφού $(m,p^{\beta-1})=1$.

Επομένως για κάθε φυσικό β είναι $d=(m,\varphi(p^\beta))=(m,p-1)$.

Απο το θεώρημα 3.1 θα είναι $a^{\frac{\varphi(p^b)}{d}} \equiv 1 \pmod{p^b}$, άρα

$$a^{\frac{\varphi(p^b)}{d}} = 1 + p^b \cdot t, \quad t \in \mathbb{Z}.$$

Υψώνοντας και τα δύο μέρη αυτής στην p-στή δύναμη, έχουμε

$$a^{p\frac{\varphi(p^b)}{d}} = a^{\frac{\varphi(p^{b+1})}{d}} = (1 + p^b \cdot t)^p =$$

$$= 1 + \binom{p}{1} p^b t + \binom{p}{2} p^{2b} t^2 + \cdots = 1 + p^{b+1} \cdot t_1$$

όπου t_1 ακέραιος, αφού $2b \geq b+1$.

Άρα $a^{\frac{\varphi(p^{b+1})}{d}} \equiv 1 \pmod{p^{b+1}}$,

όπου $d = (m, p-1) = (m, \varphi(p^{b+1}))$. Άρα, απο το θεώρημα 3.1 η διωνυμική ισοτιμία $x^m \equiv a \pmod{p^{b+1}}$ έχει λύση, πράγμα που επιθυμούσαμε.

Παράδειγμα 3.2

Θα εξετάσουμε αν οι αριθμοί 2 και 5 είναι 6-αδικά υπόλοιπα $(\mathrm{mod}\ 17^b)$, όπου b φυσικός ≥ 1, θα εξετάσουμε πρώτα την περίπτωση $b=1$. Είναι $d = (6, \varphi(17)) = (6,16) = 2$, και σύμφωνα με το θεώρημα 3.1 αφού

$$2^{\frac{\varphi(17)}{2}} = 2^{16/2} = 2^8 \equiv 1 \pmod{17} \quad \text{ενώ } 5^8 \equiv 16 \not\equiv 1 \pmod{17}$$

ο 2 είναι 6-αδικό υπόλοιπο $(\mathrm{mod}\ 17)$ ενώ ο 5 δεν είναι.

Από την πρόταση 3.2 συμπεραίνουμε ότι ο 2 είναι 6-αδικο υπόλοιπο $(\mathrm{mod}\ 17^b)$ για κάθε φυσικό $b \geq 1$, ενώ ο 5 δεν είναι.

Θα θεωρήσουμε στην συνέχεια την διωνυμική ισοτιμία

$$x^m \equiv a \pmod{2^b}$$

όπου a περιττός ακέραιος. Έχουμε το επόμενο θεώρημα.

Θεώρημα 3.2

1. Αν m και a είναι περιττοί, η διωνυμική ισοτιμία

$$x^m \equiv a \pmod{2^\beta} \qquad (*)$$

έχει ακριβώς μια λύση.

2. Αν ο a είναι περιττός ακέραιος, και $m = 2q$ όπου q περιττός ακέραιος. Έστω $\beta \geq 3$. Τότε η διωνυμική ισοτιμία

$$x^m \equiv a \pmod{2^\beta}$$

έχει λύση αν και μόνο αν $a \equiv 1 \pmod 8$. Σ'αυτή την περίπτωση η παραπάνω διωνυμική ισοτιμία έχει 4 διαφορετικές λύσεις $\pmod{2^\beta}$.

3. Έστω a περιττός ακέραιος και $m = 2q$ όπου q περιττος ακεραιος. Τότε, η διωνυμική ισοτιμία

$$x^m \equiv a \pmod 4$$

έχει λύση αν και μόνο αν $a \equiv 1 \pmod 4$. Σ'αυτή την περίπτωση η παραπάνω διωνυμική ισοτιμία έχει 2 διαφορετικές λύσεις $\pmod 4$.

Απόδειξη.

Έστω $\beta \geq 3$. Σύμφωνα με την Πρόταση 8.6 του Κεφ. IV, οι ακέραιοι $\pm 5, \pm 5^2, \ldots, \pm 5^{2^{\beta-2}}$ αποτελούν ένα αναγμένο σύστημα υπολοίπων $\pmod{2^\beta}$. Αφού $(a, 2^\beta) = (x, 2^\beta) = 1$ τότε

$$a \equiv (-1)^h \cdot 5^k \pmod{2^\beta} \qquad (1)$$

$$x \equiv (-1)^\mu \cdot 5^\nu \pmod{2^\beta} \qquad (2)$$

όπου h, k, μ, ν είναι ακέραιοι ≥ 0.

1. Έστω m περιττός ακέραιος. Θέτοντας τα a και x από (1) και (2) στην $(*)$, έχουμε

$$(-1)^\mu 5^{m\nu} \equiv (-1)^h 5^k \pmod{2^\beta}.$$

Επομένως $\mu \equiv h \pmod 2$, και από την πρόταση 8.2 i) του Κεφ IV είναι $m\nu \equiv k \pmod t$, όπου $t = \operatorname{ord}_{2^\beta}(5) = 2^{\beta-2}$

σύμφωνα με την πρόταση 8.6 του κεφ IV. Άρα

$$my \equiv k \pmod{2^{b-2}}.$$

Η γραμμική ως προς y ισοτιμία έχει μία λύση y και επομένως η (*) έχει ακριβώς μία λύση x.

Στην απόδειξη θεωρήσαμε ότι $b \geq 3$, αλλά το αποτέλεσμα ισχύει για $b=1$ και $b=2$.

Για $b=1$ έχουμε την $x^m \equiv a \pmod 2$.

Είναι $d=(m,2)=1$ και $\varphi(2)=1$. Σύμφωνα με το θεώρημα 2.2, είναι, $a^{\varphi(2)/d} = a \equiv 1 \pmod 2$, (αφού ο a είναι περιττός ακέραιος), άρα η $x^m \equiv a \pmod 2$ έχει μία ακριβώς μία λύση.

Για $b=2$, έχουμε την $x^m \equiv a \pmod 4$.

Είναι $d=(m,2)=1$ και $\varphi(4)=2$. Αν $a=2\lambda+1$, τότε

$$a^{\varphi(4)/d} = a^2 = (2\lambda+1)^2 \equiv 1 \pmod 4$$

και σύμφωνα με το θεώρημα 2.2 η $x^m \equiv a \pmod 4$, έχει ακριβώς μία λύση.

2. Έστω $m=2q$, q περιττός και $b \geq 3$, τότε θα είναι

$$5^{2qy} \equiv (-1)^h 5^k \pmod{2^b}$$

Άρα ο h είναι άρτιος, και επομένως, αφού $5 \equiv 1 \pmod 4$, θα είναι ο $a \equiv 1 \pmod 4$. Επομένως

$$2qy \equiv k \pmod{2^{b-2}}.$$

Άρα $k \equiv 0 \pmod 2$, δηλαδή ο k είναι άρτιος, και επειδή $5^2 \equiv 1 \pmod 8$ θα είναι $5^k \equiv 1 \pmod 8$, άρα $a \equiv 1 \pmod 8$.

Αν αυτή η συνθήκη ικανοποιείται, υπάρχουν δύο λύσεις της παραπάνω γραμμικής ισοτιμίας αφού $(2q, 2^{b-2}) = 2$ και επομένως υπάρχουν 4 λύσεις $x \pmod{2^b}$ της

$$x^m \equiv a \pmod{2^b}, \quad b \geq 3.$$

3. Είναι φανερό ότι η διωνυμική ισοτιμία

$$x^{29} \equiv a \pmod 4$$

έχει λύση αν και μόνο αν $a \equiv 1 \pmod 4$, σύμφωνα με το θεώρημα 2.2.

Όταν $a \equiv 1 \pmod 4$, αυτή έχει 2 λύσεις $\pmod 4$, αφού $d = (29, \varphi(4)) = (29, 2) = 2$, τις $x \equiv \pm 1 \pmod 4$. ■

Παρατήρηση

Το θεώρημα 3.2 μας βεβαιώνει ότι

1) Κάθε περιττός ακέραιος είναι m-αδικό υπόλοιπο $\pmod{2^\beta}$, $\beta \geq 1$ για κάθε περιττό φυσικό m.

2) Κάθε ακέραιος της μορφής $a = 8k+1$, $k \in \mathbb{Z}$, είναι 29-αδικό υπόλοιπο $\pmod{2^\beta}$, $\beta \geq 3$, για 9 περιττό φυσικό αριθμό.

3) Κάθε ακέραιος της μορφής $a = 4k+1$, $k \in \mathbb{Z}$ είναι 29-αδικό υπόλοιπο $\pmod 4$ για 9 περιττό φυσικό αριθμό.

Παράδειγμα 3.3

Η διωνυμική ισοτιμία $x^{29} \equiv 5 \pmod{2^6}$, έχει λύση αφού ο 29 και ο 5 είναι περιττοί αριθμοί.

Η διωνυμική ισοτιμία $x^{18} \equiv 9 \pmod{2^7}$ έχει λύση αφού $9 \equiv 1 \pmod 8$ ενώ η $x^{18} \equiv 11 \pmod{2^7}$ δεν έχει λύση αφού $11 \not\equiv 1 \pmod 8$.

Η διωνυμική ισοτιμία $x^{18} \equiv 5 \pmod 4$ έχει λύση αφού $5 \equiv 1 \pmod 4$ ενώ η $x^{18} \equiv 7 \pmod 4$ δεν έχει λύση αφού $7 \not\equiv 1 \pmod 4$. ■

Παράδειγμα 3.4

Θα επιλύσουμε την διωνυμική ισοτιμία

$$x^6 \equiv 9 \pmod{2^5}.$$

Είναι $6 = 2 \cdot 3$ με 3 περιττό. Αφού $9 \equiv 1 \pmod 8$

αυτή έχει 4 διαιρεμένες λύσεις $(\mathrm{mod}\, 2^5)$, σύμφωνα με το θεώρημα 3.2, 2).

Οι $\varphi(2^5)=2^4=16$ ακέραιοι $\pm 5, \pm 5^2, \pm 5^3, \pm 5^4, \pm 5^5, \pm 5^6, \pm 5^7, \pm 5^8$ αποτελούν ένα ανάγμενο σύστημα υπολοίπων $(\mathrm{mod}\, 2^5)$, σύμφωνα με την Πρόταση 8.6, 3) του Κεφ IV.

Έχουμε τις παρακάτω ισοτιμίες $(\mathrm{mod}\, 2^5)$

$5 \equiv 5$, $5^5 \equiv 21$, $-5 \equiv 27$, $-5^5 \equiv 11$

$5^2 \equiv 25$, $5^6 \equiv 9$, $-5^2 \equiv 7$, $-5^6 \equiv 23$

$5^3 \equiv 29$, $5^7 \equiv 13$, $-5^3 \equiv 3$, $-5^7 \equiv 19$

$5^4 \equiv 17$, $5^8 \equiv 1$, $-5^4 \equiv 15$, $-5^8 \equiv 31$.

Έτσι $9 \equiv 5^k \,(\mathrm{mod}\, 2^5)$ όπου $k=6$.

Η γραμμική ισοτιμία $6y \equiv k \,(\mathrm{mod}\, 2^3)$ δηλαδή η

$$6y \equiv 6 \,(\mathrm{mod}\, 2^3)$$

έχει δυο λύσεις, τις $y \equiv 1, 5 \,(\mathrm{mod}\, 2^3)$.

Η διωνυμική ισοτιμία έχει 4 λύσεις $(\mathrm{mod}\, 2^5)$, τις

$x_1 \equiv 5 \,(\mathrm{mod}\, 2^5)$, $x_2 \equiv -5 \,(\mathrm{mod}\, 2^5)$, $x_3 \equiv 5^5 \,(\mathrm{mod}\, 2^5)$,

και $x_4 \equiv -5^5 \,(\mathrm{mod}\, 2^5)$, δηλαδή τις

$x_1 \equiv 5 \,(\mathrm{mod}\, 2^5)$, $x_2 \equiv 27 \,(\mathrm{mod}\, 2^5)$, $x_3 \equiv 21 \,(\mathrm{mod}\, 2^5)$, $x_4 \equiv 11 \,(\mathrm{mod}\, 2^5)$.

Παράδειγμα 3.5

Θα επιλύσουμε την διωνυμική ισοτιμία $x^7 \equiv 11 \,(\mathrm{mod}\, 2^5)$.

Αφού ο 7 και ο 11 είναι περιττοί ακέραιοι, αυτή έχει μοναδική λύση $(\mathrm{mod}\, 2^5)$, σύμφωνα με το θεώρημα 3.2.1).

Όπως και στο παράδειγμα 3.4, είναι

$$11 \equiv -5^k \,(\mathrm{mod}\, 2^5) \quad \text{όπου } k=5.$$

Η γραμμική ισοτιμία $7y \equiv k \,(\mathrm{mod}\, 2^3)$ δηλαδή η

$$7y \equiv 5 \,(\mathrm{mod}\, 2^3)$$

έχει μοναδική λύση την $y \equiv 3 \,(\mathrm{mod}\, 2^3)$.

Αρα η διωνυμική ισοτιμία έχει την μοναδική λύση
$x \equiv -5^3 \pmod{2^5}$ δηλαδή την $x \equiv 3 \pmod{2^5}$.

Παράδειγμα 3.6

Θα επιλύσουμε την διωνυμική ισοτιμία $x^6 \equiv 17 \pmod 4$
Είναι $6 = 2 \cdot 3$ με 3 περιττό. Αφού $17 \equiv 1 \pmod 4$, σύμφωνα με το Θεώρημα 3.2.3), αύτη έχει 2 λύσεις, τις $x \equiv \pm 1 \pmod 4$ δηλαδή τις $x \equiv 1 \pmod 4$ και $x \equiv 3 \pmod 4$. ■

Η θεωρία των πολυωνυμικών ισοτιμιών που παρουσιάσαμε στο κεφάλαιο VI, και τα αποτελέσματα της παραγράφου αυτής μας βοηθούν, στην επίλυση της πολυωνυμικής ισοτιμίας (διωνυμικής ισοτιμίας)

$$f(x) = x^m - a \equiv 0 \pmod n \quad , \text{ όπου } (a,n)=1.$$

και στην εύρεση του πλήθους των λύσεών της.

Σ' αυτή την γενική περίπτωση (όπου δεν υπάρχουν άλλοι περιορισμοί για το μέτρο η και για τον εκθέτη m) όσον αφορά το πλήθος των λύσεων της, έχουμε.

Πρόταση 3.3

Έστω a ένας ακέραιος με $(a,n)=1$.

Αν ο a είναι ένα m-αδικο υπόλοιπο $(\bmod n)$ τότε οι διωνυμικές ισοτιμίες

$$x^m \equiv a \pmod n \quad \text{και} \quad x^m \equiv 1 \pmod n$$

έχουν το ίδιο πλήθος λύσεων.

Απόδειξη.

Έστω $U_1, \ldots, U_k \pmod n$ οι διακεκριμένες λύσεις της διωνυμικής ισοτιμίας $x^m \equiv 1 \pmod n$. Αφού ο a είναι m-αδικο υπόλοιπο $(\bmod n)$ θα υπάρχει ακέραιος c ώστε $c^m \equiv a \pmod n$.

Αφού $(a,n)=1$ θα είναι και $(c,n)=1$, οπότε οι ακέραιοι $cU_1, \ldots, cU_k$ είναι ανα δύο ανισότιμοι $(\bmod n)$. Αυτοί επίσης

επαληθεύουν την διωνυμική ισοτιμία $x^m \equiv a \pmod n$, αφού

$$(cU_i)^m = c^m \cdot U_i^m \equiv c^m \equiv a \pmod n \quad , \; i=1,2,\dots,\kappa.$$

Έστω τώρα $c_1 \in \mathbb{Z}$ με $c_1 \not\equiv c$ που επαληθεύει την $x^m \equiv a \pmod n$. Θα δείξουμε ότι η λύση c_1 είναι ισότιμη $\pmod n$ με μία από τις $cU_1, \dots, cU_\kappa$.

Πραγματικά, είναι $c_1^m \equiv a \equiv c^m \pmod n$.

Επειδή $(c,n)=1$, θα υπάρχει ακέραιος x_0 ώστε $cx_0 \equiv 1 \pmod n$.

Είναι, $(c_1 x_0)^m = c_1^m x_0^m \equiv c^m x_0^m = (cx_0)^m \equiv 1 \pmod n$

δηλαδή ο ακέραιος $U = c_1 x_0$ επαληθεύει την $x^m \equiv 1 \pmod n$

Θα υπάρχει λοιπόν δείκτης i με $U \equiv U_i \pmod n$ και επομένως $cU_i \equiv cU \equiv cc_1 x_0 \equiv c_1 c x_0 \equiv c_1 \pmod n$

πράγμα που επιδιώκαμε. ■

Πόρισμα 3.1

Έστω $a, b \in \mathbb{Z}$ με $(a,n)=(b,n)=1$. Αν οι ακέραιοι a, b είναι m-αδικά υπόλοιπα $\pmod n$ τότε οι διωνυμικές ισοτιμίες

$$x^m \equiv a \pmod n \quad \text{και} \quad x^m \equiv b \pmod n$$

έχουν το ίδιο πλήθος λύσεων. ■

Έστω και πάλι η διωνυμική ισοτιμία

$$x^m \equiv a \pmod n \;, \text{ με } (a,n)=1 \qquad (I)$$

Αν $n = 2^{\beta_0} \cdot p_1^{\beta_1} \dots p_r^{\beta_r}$, $\beta_0 \geq 0$, $\beta_i \geq 1 \dots$, τότε θα είναι

$(a, 2^{\beta_0}) = (a, p_1^{\beta_1}) = \dots = (a, p_r^{\beta_r}) = 1$.

Η (I) έχει λύση αν και μόνο αν καθεμιά από τις διωνυμικές ισοτιμίες (II)

$$(III) \quad \left\{ \begin{array}{l} x^m \equiv a \pmod{2^{\beta_0}} \\ x^m \equiv a \pmod{p_1^{\beta_1}} \\ \vdots \\ x^m \equiv a \pmod{p_r^{\beta_r}} \end{array} \right\} (II)$$

έχει λύση. Αν μία τουλάχιστον εκ των (II) δεν έχει λύση, τότε και η (I) δεν έχει λύση.

Για το πλήθος των λύσεων της (I) έχουμε, σύμφωνα με το Θεώρημα 5.1 του κεφ VI,

για $b=0$, $N(n) = N(p_1^{\beta_1}) \cdots N(p_\kappa^{\beta_\kappa})$

για $b \geq 1$, $N(n) = N(2^{b_0}) \cdot N(p_1^{\beta_1}) \cdots N(p_\kappa^{\beta_\kappa})$.

Το θεώρημα 2.2 μας βοηθά για να αποφανθούμε αν μία εκ των (III) έχει λύση. Στην περίπτωση αυτή, είναι

$$N(p_i^{\beta_i}) = d_i = \left(m, \varphi(p_i^{\beta_i})\right) \quad , i = 1, \ldots, \kappa.$$

Αν μία τουλάχιστον των (III) δεν έχει λύση, τότε και η (I) δεν έχει λύση.
Αν κάθε μία των (III) έχει λύση, τότε :

1) Αν $b_0 = 0$ και η (I) έχει λύση.
2) Αν $b_0 \geq 1$ τότε η (I) έχει λύση, αν και μόνο αν, η διοφαντική ισοτιμία, $x^m \equiv a \pmod{2^{b_0}}$, έχει λύση.

Το θεώρημα 3.2 βοηθά μερικώς προς την κατεύθυνση αυτή.

Επειδή, θα δώσουμε μεγαλύτερη έμφαση στα τετραγωνικά υπόλοιπα, που θα εξετάσουμε στο επόμενο κεφάλαιο, περισσότερα πάνω σ' αυτό το θέμα, θα δούμε εκεί.

ΚΕΦΑΛΑΙΟ VIII

Τετραγωνικά υπόλοιπα.

1. Η γενική τετραγωνική ισοτιμία.

Θεωρούμε την γενική τετραγωνική ισοτιμία

$$a_2x^2+a_1x+a_0\equiv 0 \pmod n \qquad (*)$$

όπου $a_2\not\equiv 0 \pmod n$. Είναι εύκολο να δούμε τώρα ότι η λύση της (*) ανάγεται στη λύση μιας διωνυμικής τετραγωνικής ισοτιμίας της μορφής

$$y^2\equiv b \pmod m.$$

Πραγματικά, αν πολλαπλασιάσουμε τα δύο μέρη και το μέτρο της (*) με $4a_2$ παίρνουμε την ισοδύναμη ισοτιμία

$$4a_2^2x^2+4a_2a_1x+4a_2a_0\equiv 0 \pmod{4a_2n}$$

οπότε $$(2a_2x+a_1)^2\equiv a_1^2-4a_2a_0 \pmod{4a_2n}.$$

Αν τώρα, θέσουμε

$$4a_2n=m$$
$$2a_2x+a_1\equiv y \pmod m$$
$$a_1^2-4a_2a_0\equiv b \pmod m$$

η ισοτιμία (*) ανάγεται στην ισοδύναμη διωνυμική τετραγωνική ισοτιμία

$$y^2\equiv b \pmod m.$$

Πρόταση 1.1

Έστω η διωνυμική τετραγωνική ισοτιμία

$$y^2\equiv b \pmod m \qquad (I)$$

Αν $(b,m)=d=e^2k$, όπου e^2 είναι το μεγαλύτερο τετράγωνο που περιέχεται στον d (ο k είναι ελεύθερος τετραγώνου) και $m=dm_0$, $b=db_0$, τότε η (I) είναι επιλύσιμη αν και

μόνο αν $(k, m_0) = 1$ και η διωνυμική τετραγωνική ισοτιμία

$$z^2 \equiv b_0 k \pmod{m_0} \qquad (II)$$

όπου $(b_0 k, m_0) = 1$, είναι επιλύσιμη.

Απόδειξη.

Έστω ότι η (I) είναι επιλύσιμη. Τότε $d | y^2$ δηλαδή $e^2 k | y^2$. και επομένως $ek | y$. Άς είναι,

$$y \equiv ekw \pmod{m}.$$

Η (I) παίρνει τώρα την μορφή

$$e^2 k^2 w^2 \equiv b \pmod{m}$$

και επομένως $$k w^2 \equiv b_0 \pmod{m_0}.$$

Αν $(k, m_0) = s$, τότε αυτή δεν έχει λύση, εκτός και αν $s | b_0$. Αν $s | b_0$, επειδή $s | m_0$ και $(b_0, m_0) = 1$ θα είναι $s | 1$ δηλαδή $s = 1$. Πολλαπλασιάζουμε και τα δύο μέρη της τελευταίας ισοτιμίας με k, έχουμε

$$k^2 w^2 \equiv b_0 k \pmod{m_0}.$$

Αν $z \equiv kw \pmod{m_0}$ τότε

$$z^2 \equiv b_0 k \pmod{m_0}$$

πράγμα που επιδιώκαμε.

Αντίστροφα, έστω ότι $(k, m_0) = 1$ και ότι υπάρχει ακέραιος z τέτοιος ώστε $z^2 \equiv b_0 k \pmod{m_0}$.

Ορίζουμε ακέραιο, w ώστε

$$kw \equiv z \pmod{m_0}.$$

Άρα, $k^2 w^2 \equiv z^2 \equiv b_0 k \pmod{m_0}$, και επειδή $(k, m_0) = 1$ θα είναι

$$kw^2 \equiv b_0 \pmod{m_0}.$$

Πολλαπλασιάζουμε, το μέτρο της και τα δύο μέρη της με $d = e^2 k$ και παίρνουμε

$$e^2 k^2 w^2 \equiv d b_0 \pmod{m_0 d}$$

δηλαδή

$$e^2 k^2 w^2 \equiv b \pmod{m}.$$

Θέτουμε $y \equiv ekw \pmod{m}$ και έχουμε

$$y^2 \equiv b \pmod{m}. \blacksquare$$

Παράδειγμα 1.1

Θα δείξουμε ότι η διωνυμική τετραγωνική ισοτιμία

$$y^2 \equiv 24 \pmod{60}$$

είναι επιλύσιμη, και στην συνέχεια θα βρούμε τις λύσεις της.

Είναι $(24,60) = 12 = 2^2 \cdot 3$. Επι πλέον $60 = 12 \cdot 5$ και $24 = 12 \cdot 2$

Έχουμε $(3,5) = 1$ και ότι η διωνυμική ισοτιμία

$$z^2 \equiv 2 \cdot 3 \pmod{5} \quad \text{όπου } (6,5) = 1$$

δηλαδή η $z^2 \equiv 1 \pmod{5}$,

είναι επιλύσιμη, με λύσεις τις $z \equiv 1, 4 \pmod{5}$. Σύμφωνα με την πρόταση 1.1 και η $y^2 \equiv 24 \pmod{60}$ είναι επιλύσιμη.

Θα βρούμε τώρα τις λύσεις της. Σύμφωνα με την πρόταση 1.1 θέτουμε $y \equiv 6w \pmod{60}$ και έχουμε $36w^2 \equiv 24 \pmod{60}$ δηλαδή την $3w^2 \equiv 2 \pmod{5}$. Αφού $(3,5) = 1$ πολλαπλασιάζουμε και τα δύο μέρη της με 3 και έχουμε

$$9w^2 \equiv 6 \pmod{5}.$$

Θέτουμε $z \equiv 3w \pmod{5}$ και έχουμε $z^2 \equiv 6 \pmod{5}$ ή $z^2 \equiv 1 \pmod{5}$. Άρα $z \equiv 1, 4 \pmod{5}$, και επομένως $w \equiv 3, 2 \pmod{5}$ και τελικά $y \equiv 18, 48, 12, 42 \pmod{60}$.

Παράδειγμα 1.2

Θα λύσουμε την διωνυμική ισοτιμία $y^2 \equiv 6 \pmod{15}$.

Είναι $(6,15) = 3$. Θέτουμε $y \equiv 3w \pmod{15}$ και έχουμε $9w^2 \equiv 6 \pmod{15}$. Επειδή $(3,5) = 1$ αυτή είναι ισοδύναμη με την $3w^2 \equiv 2 \pmod{5}$. Πολλαπλασιάζουμε με 3 και τα δύο μέρη της και έχουμε $9w^2 \equiv 6 \pmod{5}$. Θέτουμε $z \equiv 3w \pmod{5}$ και έχουμε $z^2 \equiv 6 \equiv 1 \pmod{5}$. Επομένως $z \equiv 1, 4 \pmod{5}$, και απ' αυτό έχουμε $w \equiv 3, 2 \pmod{5}$ και τελικά $y \equiv 6, 9 \pmod{5}$.

Από την Πρόταση 1.1 φαίνεται ότι το πρόβλημα της επίλυσης μιας γενικής τετραγωνικής ισοτιμίας, ανάγεται στην επίλυση μιας διωνυμικής ισοτιμίας και γραμμικών ισοτιμιών.

Πόρισμα 1.1

Μια επιλύσιμη τετραγωνική ισοτιμία

$$a_2x^2+a_1x+a_0 \equiv 0 \pmod m \quad , \quad a_2 \not\equiv 0 \pmod m$$

μπορεί να ανηχθεί στην μορφή

$$z^2 \equiv a \pmod m \quad , \text{ όπου } (a,m)=1. \blacksquare$$

Παράδειγμα 1.3

Θα εξετάσουμε την επιλυσιμότητα της γενικής τετραγωνικής ισοτιμίας

$$3x^2+6x+1 \equiv 0 \pmod 5$$

σύμφωνα με όσα είδαμε μέχρι εδώ.

Πολλαπλασιάζουμε τα δύο μέρη της και το μέτρο με $4 \cdot 3 = 12$ και παίρνουμε την ισοδύναμη ισοτιμία

$$36x^2+72x+12 \equiv 0 \pmod{60}$$

δηλαδή την $(6x+6)^2 \equiv 24 \pmod{60}$

Θέτουμε $y \equiv 6x+6 \pmod{60}$ και έχουμε ισοδύναμα την

$$y^2 \equiv 24 \pmod{60}$$

Σύμφωνα με το Παράδειγμα 1.1, η αρχική ισοτιμία ανάγεται στην $z^2 \equiv 1 \pmod 5$, όπου $(1,5)=1$.

Είναι $y \equiv 12, 48, 12, 48 \pmod{60}$ και $6x \equiv y-6 \pmod{60}$ και τελικά $x \equiv 1, 2 \pmod 5$. $\blacksquare$

Απ' όλα τα παραπάνω φαίνεται ότι είναι επαρκές να εξετάσουμε με λεπτομέρεια τις τετραγωνικές ισοτιμίες

$$x^2 \equiv a \pmod n \quad , \text{ όπου } (a,n)=1.$$

Στο κεφάλαιο VII μελετήσαμε με λεπτομέρεια τα π-διωνύμια υπόλοιπα. Για $n=2$, δηλαδή τα τετραγωνικά υπόλοιπα θα τα μελετήσουμε ιδιο κεφάλαιο αυτό.

Ας ξαναθυμηθούμε τον επόμενο ορισμό.

Ορισμός

Εστω φυσικός $n>1$. Ενας ακέραιος a με $(a,n)=1$ καλείται τετραγωνικό υπόλοιπο $(\mathrm{mod}\, n)$ ή τετραγωνικό υπόλοιπο του n αν η διωνυμική ισοτιμία

$$x^2 \equiv a \ (\mathrm{mod}\, n)$$

επιδέχεται μία τουλάχιστον λύση. Αν αυτή δεν έχει λύση, θα λέμε ότι ο a είναι τετραγωνικό μη-υπόλοιπο $(\mathrm{mod}\, n)$ ή τετραγωνικό μη-υπόλοιπο του n.

Στο κεφάλαιο VI διαπιστώσαμε ότι το πρόβλημα της επίλυσης μιας πολυωνυμικής ισοτιμίας $f(x) \equiv 0 \ (\mathrm{mod}\, n)$ με σύνθετο μέτρο, και για την περίπτωσή μας, της πολυωνυμικής ισοτιμίας

$$f(x) = x^2 - a \equiv 0 \ (\mathrm{mod}\, n) \quad , \text{ όπου } (a,n)=1,$$

μπορεί να ανάγεται σε πολυωνυμικές ισοτιμίες

$$f(x) = x^2 - a \equiv 0 \ (\mathrm{mod}\, p) \quad , \text{ όπου } p \nmid a$$

και ο p είναι πρώτος αριθμός, και σ' ένα σύνολο γραμμικών ισοτιμιών.

Αυτό θα το διαπραγματευθούμε στο τέλος του κεφαλαίου αυτού. Εκεί θα δούμε ότι η περίπτωση $p=2$ δεν παρουσιάζει εξαιρετικές δυσκολίες. Έτσι θα ξεκινήσουμε με την παρουσίαση της διωνυμικής ισοτιμίας

$$x^2 \equiv a \ (\mathrm{mod}\, p) \quad , \ p \nmid a,$$

και p περιττός πρώτος, δηλαδή με τα τετραγωνικά υπόλοιπα $(\mathrm{mod}\, p)$ όπου p περιττός πρώτος.

2. Τετραγωνικά υπόλοιπα (mod p)

Σ'αυτή την παράγραφο θα μελετήσουμε τα τετραγωνικά υπόλοιπα (mod p) όπου p περιττός πρώτος.

Δυο **βασικά προβλήματα** κυριαρχούν στην θεωρία των τετραγωνικών υπολοίπων

1ο Πρόβλημα. Μας δίνουν τον p και ζητούν να προσδιορίσουμε ποιοι ακέραιοι α, είναι τετραγωνικά υπόλοιπα (mod p) και ποιοι είναι τετραγωνικά μη-υπόλοιπα (mod p).

2ον Πρόβλημα. Μας δίνουν τον ακέραιο α και ζητούν να προσδιορίσουμε εκείνους τους περιττούς πρώτους p που έχουν τον α τετραγωνικό υπόλοιπο, με άλλα λόγια, τους περιττούς πρώτους p για τους οποίους η διωνυμική ισοτιμία $x^2 \equiv a \pmod p$ είναι επιλύσιμη.

Θα αρχίσουμε με μερικά αποτελέσματα για την επίλυση του 1ου προβλήματος.

Θεώρημα 2.1 (Κριτήριο του Euler)

Έστω p περιττός πρώτος και $a \in \mathbb{Z}$ με $(a,p)=1$.
Τότε, ο α είναι τετραγωνικό υπόλοιπο (mod p) αν και μόνο αν

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Απόδειξη.

Είναι $\varphi(p)=p-1$ και $d=(2,\varphi(p))=(2,p-1)=2$ αφού ο $p-1$ είναι άρτιος. Το θεώρημα προκύπτει τώρα σαν πόρισμα του θεωρήματος 3.1 του Κεφ VII. ∎

Πόρισμα 2.1

Έστω p περιττός πρώτος και $a \in \mathbb{Z}$ με $(a,p)=1$. Τότε, ο α είναι τετραγωνικό μη-υπόλοιπο (mod p) αν και μόνο αν

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Απόδειξη.

Από το θεώρημα του Fermat έχουμε $\alpha^{p-1} \equiv 1 \pmod p$. και επομένως $\left(\alpha^{\frac{p-1}{2}} - 1\right)\left(\alpha^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p$.

Αν ο α είναι τετραγωνικό μη-υπόλοιπο (mod p), θα είναι $\alpha^{p-1/2} - 1 \not\equiv 0 \pmod p$ σύμφωνα με το θεώρημα 2.1. Υποχρεωτικά λοιπόν $\alpha^{p-1/2} + 1 \equiv 0 \pmod p$, δηλαδή $\alpha^{p-1/2} \equiv -1 \pmod p$.

Αντίστροφα, ας είναι $\alpha^{p-1/2} \equiv -1 \pmod p$. Αν υποθέσουμε ότι ο α είναι τετραγωνικό υπόλοιπο (mod p) τότε $\alpha^{p-1/2} \equiv 1 \pmod p$ τότε θα είχαμε $1 \equiv -1 \pmod p$ δηλαδή $2 \mid p$ πράγμα άτοπο. Άρα ο α είναι τετραγωνικό μη-υπόλοιπο (mod p). ■

Παράδειγμα 2.1

Θα εξετάσουμε αν οι ακέραιοι 3 και 5 είναι τετραγωνικά υπόλοιπα (mod 31).

Είναι $\frac{31-1}{2} = 15$ και $5^{15} = (5^3)^5 \equiv (1)^5 \equiv 1 \pmod{31}$, άρα ο 5 είναι τετραγωνικό υπόλοιπο (mod 31).

Επίσης, $3^3 \equiv -4 \pmod{31}$ οπότε $3^6 \equiv 16 \pmod{31}$, άρα $3^{12} \equiv 16 \pmod{31}$ και τελικά $3^{15} \equiv -32 \equiv -1 \pmod{31}$, επομένως ο 3 είναι τετραγωνικό μη-υπόλοιπο (mod 31).

Το κριτήριο του Euler δεν προσφέρεται σαν ένας πρακτικός τρόπος ελέγχου για να καθορίσουμε πότε ένας ακέραιος είναι τετραγωνικό ή μη-τετραγωνικό υπόλοιπο, αφού οι υπολογισμοί είναι επίπονοι, εκτός και αν το μέτρο είναι μικρό. Είναι όμως ένα κριτήριο που χρησιμοποιείται περισσότερο για θεωρητικούς σκοπούς.

Μια περισσότερο αποφασιστική μέθοδος για τέτοιους υπολογισμούς περικλείεται στο Νόμο της τετραγωνικής αντιστροφής που θα δούμε στα επόμενα.

Για το πλήθος των τετραγωνικών υπολοίπων και μη-υπολοίπων και τον εντοπισμό τους έχουμε τα παρακάτω αποτελέσματα.

Πρόταση 2.1

Έστω p περιττός πρώτος. Τότε κάθε αναγμένο σύστημα υπολοίπων $(\mathrm{mod}\, p)$ περιέχει $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα $(\mathrm{mod}\, p)$ και $\frac{p-1}{2}$ τετραγωνικά μη-υπόλοιπα $(\mathrm{mod}\, p)$.

Απόδειξη

Έστω $\{a_1, \ldots, a_{p-1}\}$ ένα αναγμένο σύστημα υπολοίπων $(\mathrm{mod}\, p)$. Αφού $(2, \varphi(p)) = (2, p-1) = 2$, σύμφωνα με την πρόταση 3.1 του Κεφ VII υπάρχουν $\frac{\varphi(p)}{2} = \frac{p-1}{2}$ τετραγωνικά υπόλοιπα $(\mathrm{mod}\, p)$. Καθένα απο αυτά, είναι ισότιμο $(\mathrm{mod}\, p)$ με έναν και μόνο έναν απο τους αμεραίους του $\{a_1, \ldots, a_{p-1}\}$. Οι υπόλοιποι αμέραιοι του συστήματος $\{a_1, \ldots, a_{p-1}\}$ είναι φανερά τετραγωνικά μη-υπόλοιπα $(\mathrm{mod}\, p)$ και το πλήθος τους είναι $(p-1) - \left(\frac{p-1}{2}\right) = \frac{p-1}{2}$. ∎

Πόρισμα 2.2

Έστω p περιττός πρώτος. Υπάρχουν $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα $(\mathrm{mod}\, p)$ και $\frac{p-1}{2}$ τετραγωνικά μη-υπόλοιπα $(\mathrm{mod}\, p)$.

Πρόταση 2.2

Έστω p περιττός πρώτος. Τα $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα $(\mathrm{mod}\, p)$ συμπίπτουν με τους αμεραίους

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Απόδειξη.

Οι $\frac{p-1}{2}$ σε πλήθος αμέραιοι $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ είναι ανισότιμοι ανα δύο $(\mathrm{mod}\, p)$. Πραγματικά, έστω $a^2 \equiv b^2 \,(\mathrm{mod}\, p)$ με $a \neq b$ και $1 \leq a \leq \frac{p-1}{2}$ και $1 \leq b \leq \frac{p-1}{2}$.

Τότε θα είναι $(a-b)(a+b) \equiv 0 \,(\mathrm{mod}\, p)$.

Αλλά $1 < a+b < p$ οπότε $a-b \equiv 0 \pmod p$ πράγμα άτοπο αφού $0 < |a-b| < p$.

Επειδή $(p-a)^2 \equiv a^2 \pmod p$ οι ακέραιοι $1^2, \dots, \left(\frac{p-1}{2}\right)^2$ είναι τετραγωνικά υπόλοιπα (mod p).

Παρατήρηση

Καθένας από τους ακεραίους $1^2, \dots, \left(\frac{p-1}{2}\right)^2$ είναι ισότιμος με ένα και μόνο ένα από τους ακεραίους του αναμένου συστήματος υπολοίπων $\{1, 2, \dots, p-1\}$. Οι υπόλοιποι $\frac{p-1}{2}$ ακέραιοι από τους $\{1, 2, \dots, p-1\}$ είναι τα τετραγωνικά μή-υπόλοιπα (mod p).

Παράδειγμα 2.2.

Θα βρούμε τα τετραγωνικά υπόλοιπα και μη-υπόλοιπα (mod 17).

Τα τετραγωνικά υπόλοιπα (mod 17) συμπίπτουν με τους ακεραίους $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2$.

Τους ανάγουμε (mod 17) και έχουμε

$1^2 \equiv 1 \pmod{17}$, $5^2 \equiv 25 \equiv 8 \pmod{17}$

$2^2 \equiv 4 \pmod{17}$, $6^2 \equiv 36 \equiv 2 \pmod{17}$

$3^2 \equiv 9 \pmod{17}$, $7^2 \equiv 49 \equiv 15 \pmod{17}$

$4^2 \equiv 16 \pmod{17}$, $8^2 \equiv 64 \equiv 13 \pmod{17}$

Επομένως τα 8 τετραγωνικά υπόλοιπα (mod 17) συμπίπτουν με τους ακεραίους 1, 2, 4, 8, 9, 13, 15 και 16.

Οι υπόλοιποι 8 ακέραιοι από το αναμένο σύστημα υπολοίπων (mod 17) $\{1, 2, \dots, 16\}$, δηλαδή οι ακέραιοι

3, 5, 6, 7, 10, 11, 12 και 14

είναι όλα τα τετραγωνικά μη-υπόλοιπα (mod 17).

Πρόταση 2.3

Έστω p περιττός πρώτος και g μια αρχική ρίζα (mod 17). Τότε,

1) Τα $\frac{p-1}{2}$ σε πλήθος τετραγωνικά υπόλοιπα (mod p) συμπίπτουν με τις άρτιες δυνάμεις

$$g^2, g^4, \dots, g^{p-1}$$

της αρχικής ρίζας g.

2) Τα $\frac{p-1}{2}$ σε πλήθος τετραγωνικά μη-υπόλοιπα (mod p) συμπίπτουν με τις περιττές δυνάμεις

$$g, g^3, \dots, g^{p-2}$$

της αρχικής ρίζας g.

Απόδειξη.

1) Αφού $\varphi(p)=p-1$ και $d=(2,\varphi(p))=(2,p-1)=2$, σύμφωνα με την πρόταση 3.1 του Κεφ VII τα $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα (mod p) συμπίπτουν με τους ακεραίους

$$g^2, g^4, \dots, g^{p-1}.$$

2) Οι ακέραιοι $g, g^2, \dots, g^{p-1}$, αποτελούν ένα αναγμένο σύστημα υπολοίπων (mod p) σύμφωνα με την πρόταση 1.1 του Κεφ VII. Άρα τα $\frac{p-1}{2}$ τετραγωνικά μη-υπόλοιπα συμπίπτουν με τις περιττές δυνάμεις $g, g^3, \dots, g^{p-2}$ της αρχικής ρίζας g. ∎

Παράδειγμα 2.3

Γνωρίζουμε ότι ο 3 είναι μια αρχική ρίζα (mod 17) και έχουμε τον επόμενο πίνακα δεικτών

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Από τον πίνακα αυτό έχουμε για τις άρτιες δυνάμεις της αρχικής ρίζας 3,

$3^2 \equiv 9 \pmod{17}$, $3^4 \equiv 13 \pmod{17}$, $3^6 \equiv 15 \pmod{17}$, $3^8 \equiv 16 \pmod{17}$

$3^{10} \equiv 8 \pmod{17}$, $3^{12} \equiv 4 \pmod{17}$, $3^{14} \equiv 2 \pmod{17}$, $3^{16} \equiv 1 \pmod{17}$,

και επομένως τα 8 τετραγωνικά υπόλοιπα (mod17) είναι τα

1, 2, 4, 8, 9, 13, 15, 16

ενώ τα 8 τετραγωνικά μη-υπόλοιπα (mod17) συμπίπτουν με τις περιττές δυνάμεις της αρχικής ρίζας (mod17), είναι δηλαδή τα 3, 5, 6, 7, 10, 11, 12, 14.

όπως τα έχουμε βρει με διαφορετικό τρόπο στο παράδειγμα 2.2.

Παρατήρηση.

Αν γνωρίζουμε ένα πίνακα δεικτών (mod p) είναι καταλληλο να χρησιμοποιούμε τις άρτιες δυνάμεις της αρχικής ρίζας για να βρούμε τα τετραγωνικά υπόλοιπα (mod p).

Αν όμως πρέπει να υπολογίσουμε μια αρχική ρίζα, η μέθοδος που περιγράφεται στην Πρόταση 2.2 είναι περισσότερο πρόσφορος για την εύρεση των τετραγωνικών υπολοίπων.

Πόρισμα 2.3

Έστω p ένας περιττός πρώτος. Τότε, το γινόμενο δυο τετραγωνικών υπολοίπων (mod p) ή δυο μη-τετραγωνικών υπολοίπων (mod p) είναι τετραγωνικό υπόλοιπο (mod p), ενώ το γινόμενο ενός τετραγωνικού υπολοίπου (mod p) και ενός τετραγωνικού μη-υπολοίπου (mod p) είναι ένα τετραγωνικό μη-υπόλοιπο (mod p).

Απόδειξη.

Έστω g μια αρχική ρίζα (mod p). Είναι $g^{\mu} \cdot g^{\nu} = g^{\mu+\nu}$.

Αν αμφότεροι οι μ, ν είναι άρτιοι ή περιττοί ο μ+ν είναι άρτιος. Αν ο μ είναι άρτιος και ο ν περιττός τότε ο μ+ν είναι περιττός. Η απόδειξη ολοκληρώνεται χρησιμοποιώντας την πρόταση 2.3. ■

3. Το σύμβολο του Legendre.

Ορισμός.

Έστω p ένας περιττός πρώτος και $a \in \mathbb{Z}$ με $p \nmid a$.
Το σύμβολο του Legendre (a/p) ορίζεται από την εξέση.

$$(a/p) = \begin{cases} +1 & \text{αν ο } a \text{ είναι τετραγωνικό υπόλοιπο} (\text{mod} p) \\ -1 & \text{αν ο } a \text{ είναι τετραγωνικό μη-υπόλοιπο} (\text{mod} p) \end{cases}$$

και διαβάζεται "σύμβολο του a σε εξέση προς το p".

Ο a ονομάζεται **ονομαστής** και ο p **παρανομαστής** του συμβόλου (a/p). Άλλοι συμβολισμοί για το σύμβολο Legendre είναι $\left(\frac{a}{p}\right)$ ή $(a|p)$.

Κάθε αναφορά στο σύμβολο Legendre (a/p) προϋποθέτει ότι $p \nmid a$.

Παρατήρηση.

Για $p|a$ εμείς δεν ορίζουμε το σύμβολο Legendre. Μερικοί συγγραφείς βρίσκουν κατάλληλο να επεκτείνουν το σύμβολο Legendre και όταν $p|a$, ορίζοντας στην περίπτωση αυτή $(a/p) = 0$. Ένα πλεονέκτημα αυτής της θεώρησης είναι ότι ο αριθμός των λύσεων της ισοτιμίας $x^2 \equiv a (\text{mod} p)$ μπορεί τότε να δοθεί με τον απλό τύπο $1 + (a/p)$.

Πρόταση 3.1

Έστω p περιττός πρώτος και $a, b \in \mathbb{Z}$ με $(a,p) = (b,p) = 1$. Τότε το σύμβολο Legendre έχει τις επόμενες ιδιότητες.

1) Αν $a \equiv b (\text{mod} p)$ τότε $(a/p) = (b/p)$

2) $(a^2/p) = 1$

3) $(a/p) \equiv a^{\frac{p-1}{2}} (\text{mod} p)$

4) $(ab/p) = (a/p)(b/p)$

5) $(ab^2/p) = (a/p)$

6) $(1/p) = 1$ και $(-1/p) = (-1)^{p-1/2}$

Απόδειξη.

1) Αν $a \equiv b \pmod p$ τότε η ισοτιμία $x^2 \equiv a \pmod p$ έχει λύση αν και μόνο αν η ισοτιμία $x^2 \equiv b \pmod p$ έχει λύση. Έτσι οι ισοτιμίες αυτές ή έχουν αμφότερες λύση ή καμμία απ'αυτές δεν έχει λύση, που συμαίνει ότι $(a/p) = (b/p)$.

2) Ο ακέραιος a είναι μια λύση της ισοτιμίας $x^2 \equiv a^2 \pmod p$, άρα $(a^2/p) = 1$.

3) Αν ξαναδιατυπώσουμε το Θεώρημα 2.1 και το Πόρισμα 2.1, κάνοντας χρήση του συμβόλου Legendre, παίρνουμε $(a/p) \equiv a^{p-1/2} \pmod p$.

4) Είναι, $(ab/p) \equiv (ab)^{p-1/2} \equiv a^{p-1/2} \cdot b^{p-1/2} \equiv (a/p)(b/p) \pmod p$

Το σύμβολο Legendre παίρνει μόνο τις τιμές 1 και -1.

Αν $(ab/p) \neq (a/p)(b/p)$, τότε $1 \equiv -1 \pmod p$ δηλαδή $2 \equiv 0 \pmod p$ πράγμα άτοπο, αφού $p > 2$. Άρα $(ab/p) = (a/p)(b/p)$.

Μια διαφορετική απόδειξη προκύπτει από το πόρισμα 2.3 αν το ξαναδιατυπώσουμε κάνοντας χρήση του συμβόλου Legendre.

5) $(ab^2/p) = (a/p)(b^2/p) = (a/p) \cdot 1 = (a/p)$. Μ'άλλα λόγια αν στον ονομαστή του συμβόλου Legendre εμφανίζονται τετραγωνισμένοι παράγοντες, αυτοί δύνανται να παραληφθούν.

6) Η ισοτιμία $x^2 \equiv 1 \pmod p$ έχει μία λύση την $x \equiv 1 \pmod p$ άρα $(1/p) = 1$.

Από το 3) έχουμε $(-1/p) \equiv (-1)^{p-1/2} \pmod p$

Επειδή οι ποσότητες $(-1/p)$ και $(-1)^{p-1/2}$ παίρνουν μόνο τις τιμές 1 ή -1, αν $(-1/p) \neq (-1)^{p-1/2}$ τότε θα είχαμε $1 \equiv -1 \pmod p$ πράγμα άτοπο αφού $p > 2$. Άρα

$$(-1/p) = (-1)^{p-1/2}. \quad \blacksquare$$

Η παρακάτω πρόταση εμπίπτει στο 2ο βασικό ερώτημα της θεωρίας των τετραγωνικών υπολοίπων.

Πρόταση 3.2

Αν ο p είναι περιττος πρώτος, τότε

$$(-1/p) = \begin{cases} 1 & \text{αν } p \equiv 1 \pmod 4 \\ -1 & \text{αν } p \equiv 3 \pmod 4 \end{cases}$$

Απόδειξη

Διαιρώντας τον περιττό πρώτο p με τον 4 θα είναι $p = 4n+1$ ή $p = 4n+3$ δηλαδή $p \equiv 1 \pmod 4$ ή $p \equiv 3 \equiv -1 \pmod 4$.

Στην περίπτωση που $p = 4n+1$, είναι $\frac{p-1}{2} = 2n$ και επομένως $(-1/p) = (-1)^{p-1/2} = (-1)^{2n} = 1$.

Αν $p = 4n+3$, είναι $\frac{p-1}{2} = \frac{4n+2}{2} = 2n+1$ και επομένως $(-1/p) = (-1)^{p-1/2} = (-1)^{2n+1} = -1$. ∎

Πόρισμα 3.1

Ο ακέραιος -1 είναι τετραγωνικό υπόλοιπο για όλους τους πρώτους της μορφής $4n+1$ και είναι τετραγωνικό μη-υπόλοιπο για όλους τους πρώτους της μορφής $4n+3$.

Πόρισμα 3.2

Οι περιττοί πρώτοι παράγοντες p του ακεραίου x^2+1 όπου $x \in \mathbb{Z}$ είναι της μορφής $4n+1$.

Απόδειξη

Από την υπόθεση $p | x^2+1$ συμπεραίνουμε ότι η ισοτιμία $x^2 \equiv -1 \pmod p$ έχει λύση, άρα ο -1 είναι τετραγωνικό υπόλοιπο $(\mod p)$ και επομένως $p = 4n+1$ από το Πόρισμα 3.1.

Πόρισμα 3.3

Υπάρχουν άπειροι πρώτοι της μορφής $4n+1$.

Απόδειξη.

Υποθέτουμε ότι το πλήθος των πρώτων της μορφής $4n+1$ είναι πεπερασμένο, και ας είναι αυτοί οι $p_1, \dots, p_k$.

Θεωρούμε τον φυσικό

$$\alpha = 4p_1^2 \cdots p_k^2 + 1 .$$

Ο α είναι περιττός, επομένως θα υπάρχει περιττός πρώτος $p|\alpha$.

Αυτός θα είναι, σύμφωνα με το πόρισμα 3.2 της μορφής $4n+1$, θα είναι επομένως ο p κάποιος από τους $p_1, \dots, p_k$ και επομένως ο $p|1$, πράγμα άτοπο. Άρα υπάρχουν άπειροι πρώτοι της μορφής $4n+1$. ■

Πρόταση 3.3

Αν p είναι περιττός πρώτος, τότε

$$\sum_{a=1}^{p-1} (a/p) = 0 .$$

Απόδειξη.

Οι αμέραιοι $\{1, 2, \dots, p-1\}$ αποτελούν ένα ανάγμενο σύστημα υπολοίπων $(\mathrm{mod} p)$. Σύμφωνα με την πρόταση 2.1 $\frac{p-1}{2}$ σε πλήθος απ' αυτούς είναι τετραγωνικά υπόλοιπα $(\mathrm{mod} p)$ και επομένως έχουν σύμβολο Legendre $=1$ και οι υπόλοιποι $\frac{p-1}{2}$ σε πλήθος απ' αυτούς είναι τετραγωνικά μη-υπόλοιπα $(\mathrm{mod} p)$ και έχουν σύμβολο Legendre $=-1$. Έτσι

$$\sum_{a=1}^{p-1} (a/p) = (\underbrace{1 + \cdots + 1}_{\frac{p-1}{2} \text{ φορές}}) + (\underbrace{(-1) + \cdots + (-1)}_{\frac{p-1}{2} \text{ φορές}}) = 0. \quad ■$$

Παράδειγμα 3.1

Θα υπολογίσουμε το $(35/23)$

Καθώς $35 \equiv 12 \ (\mathrm{mod} 23)$, έχουμε $(35/23) = (12/23)$

Αλλά $12 = 2^2 \cdot 3$ οπότε $(12/23) = (2^2 3/23) = (2^2/23)(3/23)$

$= 1 \cdot (3/23)$. Επιπλέον $(3/23) \equiv 3^{\frac{23-1}{2}} \equiv 3^{11} \ (\mathrm{mod} 23)$.

Εύκολα βρίσκουμε ότι $3^{11} \equiv 1 \pmod{23}$, οπότε $\left(35/23\right) = 1$. ■

4. Το λήμμα του Gauss.

Όπως σημειώσαμε στα προηγούμενα, ο υπολογισμός του $\left(a/p\right) \equiv a^{p-1/2} \pmod{p}$ ιδίως όταν το μέτρο είναι μεγάλο είναι αρκετά επίπονος. Για παράδειγμα $\left(111/1999\right) \equiv 111^{999} \pmod{1999}$.

Ο Gauss βρήκε ένα άλλο κριτήριο, που περιλαμβάνει ηπιότερο υπολογισμό.

Θα χρειασθούμε στα επόμενα την συνάρτηση $[x]$ "ακέραιο μέρος του x".

Ορισμός

Για κάθε πραγματικό αριθμό x λαμβάνουμε <u>ακέραιο μέρος του x</u> και το συμβολίζουμε $[x]$, τον μέγιστο ακέραιο που είναι $\leq x$, δηλαδή

$$[x] = \{n / n \in \mathbb{Z},\ n \leq x\}.$$

Έτσι,

$$[x] \leq x < [x] + 1.$$

Ονομάζουμε <u>κλασματικό μέρος</u> του x, και το συμβολίζουμε $\{x\}$ την διαφορά $x - [x]$, δηλαδή είναι

$$\{x\} = x - [x].$$

Για παράδειγμα, είναι

$$\left[\tfrac{17}{2}\right] = 8 \quad \text{και} \quad \left\{\tfrac{17}{2}\right\} = \tfrac{1}{2}$$

$$\left[-\tfrac{17}{2}\right] = -9 \quad \text{και} \quad \left\{-\tfrac{17}{2}\right\} = \tfrac{1}{2}$$

$$\left[\tfrac{17}{3}\right] = 5 \quad \text{και} \quad \left\{-\tfrac{17}{3}\right\} = \tfrac{2}{3}$$

$$\left[-\tfrac{17}{3}\right] = -6 \quad \text{και} \quad \left\{-\tfrac{17}{3}\right\} = \tfrac{1}{3}.$$

Έχουμε πάντα $0 \le \{x\} < 1$.

Έτσι,

$$x = [x] + \{x\} \quad \text{με} \quad 0 \le \{x\} < 1 .$$

Θεώρημα 4.1 **Λήμμα του Gauss**

Έστω p περιττός πρώτος και $a \in \mathbb{Z}$ με $(a,p)=1$.
Θεωρούμε τα ελάχιστα θετικά υπόλοιπα $(\mathrm{mod} p)$ των ακεραίων

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a \qquad (*)$$

Συμβολίζουμε με m το πλήθος εκείνων από τα υπόλοιπα που υπερβαίνουν τον $p/2$, τότε,

$$(a/p) = (-1)^m$$

και

$$m \equiv \sum_{t=1}^{p\cdot 1/2} \left[\frac{ta}{p}\right] + (a-1)\frac{p^2-1}{8} \pmod 2 .$$

Απόδειξη

Οι ακέραιοι $(*)$ είναι ανά δύο ανισότιμοι $(\mathrm{mod} p)$. Παίρνουμε τα ελάχιστα θετικά υπόλοιπά τους $(\mathrm{mod} p)$ και τα καταν έμουμε σε δύο ξένα σύνολα A και B ανάλογα αν τα υπόλοιπα είναι $< \frac{p}{2}$ ή $> \frac{p}{2}$.

Είναι λοιπόν $A = \{a_1, \ldots, a_k\}$

όπου κάθε $a_i \equiv ta \pmod p$ για κάποιο $t \le \frac{p-1}{2}$ και

$0 < a_i < \frac{p}{2}$.

Επίσης, είναι $B = \{b_1, \ldots b_m\}$,

όπου κάθε $b_j \equiv sa \pmod p$ για κάποιο $s \le \frac{p-1}{2}$ και $\frac{p}{2} < b_j < p$.

Παρατηρούμε ότι $m+k = \frac{p-1}{2}$ αφού τα σύνολα A και B είναι ξένα μεταξύ τους.

Θεωρούμε τώρα το σύνολο C από m στοιχεία

$$C = \{c_1, \ldots, c_m\} \quad \text{όπου} \quad c_i = p - b_i \quad , i = 1, \ldots, m .$$

Είναι $0 < c_i < \frac{p}{2}$, δηλαδή τα στοιχεία του C βρίσκονται στο ίδιο διάστημα με τα στοιχεία του A. Θα δείξουμε ότι $C \cap A = \phi$.

Έστω ότι $C \cap A \neq \phi$ και ας είναι $c_i = a_j$ για κάποιο ζεύγος δεικτών i και j. Τότε $p - b_i = a_j$ ή $a_j + b_i \equiv 0 \pmod p$. Επομένως

$ta + sa = (t+s)a \equiv 0 \pmod p$ για κάποια t και s με $1 \leq t < \frac{p}{2}$ και $1 \leq s < \frac{p}{2}$. Αυτό όμως είναι άτοπο, γιατί $p \nmid a$ και $0 < (t+s) < p$. Άρα $C \cap A = \phi$ και η ένωσή τους $C \cup A$ περιέχει $m+k = \frac{p-1}{2}$ ακεραίους στο διάστημα $[1, \frac{p-1}{2}]$.

Άρα, $A \cup C = \{a_1, \ldots, a_k, c_1, \ldots, c_m\} = \{1, 2, \ldots, \frac{p-1}{2}\}$.

Παίρνοντας τώρα το γινόμενο όλων των στοιχείων της ένωσης $A \cup C$ έχουμε

$$a_1 \cdots a_k \cdot c_1 \cdots c_m = \left(\frac{p-1}{2}\right)!$$

Αφού $c_i = p - b_i$, έχουμε

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= a_1 \cdots a_k (p-b_1) \cdots (p-b_m) \\ &\equiv (-1)^m a_1 \cdots a_k \cdot b_1 \cdots b_m \pmod p \\ &\equiv (-1)^m a \cdot (2a) \cdots \left(\tfrac{p-1}{2} a\right) \pmod p \\ &\equiv (-1)^m a^{p-1/2} \cdot \left(\frac{p-1}{2}\right)! \pmod p\end{aligned}$$

Επειδή $p \nmid \left(\frac{p-1}{2}\right)!$ έχουμε

$$a^{p-1/2} \equiv (-1)^m \pmod p$$

και επομένως

$$(a/p) \equiv a^{p-1/2} \equiv (-1)^m \pmod p.$$

Αφού οι τιμές των (a/p) και $(-1)^m$ είναι 1 ή -1 και ο $p > 2$ έχουμε τελικά

$$(a/p) = (-1)^m.$$

πράγμα που επιδιώξαμε.

Παρατηρούμε ότι, για $t=1,\dots,\frac{p-1}{2}$ έχουμε

$$\frac{ta}{p}=\left[\frac{ta}{p}\right]+\left\{\frac{ta}{p}\right\} \quad \text{όπου} \quad 0<\left\{\frac{ta}{p}\right\}<1,$$

οπότε

$$ta=p\left[\frac{ta}{p}\right]+p\left\{\frac{ta}{p}\right\}=p\left[\frac{ta}{p}\right]+r_t \quad , \text{όπου} \quad 0<r_t<p.$$

Ο αριθμός $r_t=ta-p\left[\frac{ta}{p}\right]$ είναι λοιπόν το ελάχιστο θετικό υπόλοιπο του $ta \pmod p$. Έτσι

$$\left\{r_1,\dots,r_{\frac{p-1}{2}}\right\}=\left\{a_1,\dots,a_k,b_1,\dots,b_m\right\}$$

Υπολογίζουμε τα αθροίσματα των στοιχείων του συνόλου αυτού και του συνόλου $\left\{1,2,\dots,\frac{p-1}{2}\right\}=A\cup C$ και έχουμε τις παρακάτω δυο εξισώσεις

$$\sum_{t=1}^{p-1/2} r_t = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j \qquad (I)$$

$$\sum_{t=1}^{p-1/2} t = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} c_j = \sum_{i=1}^{k} a_i + mp - \sum_{j=1}^{m} b_j \qquad (II)$$

Αντικαθιστώντας τα r_i από τον ορισμό τους στην (I) έχουμε

$$\sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j = a\sum_{t=1}^{p-1/2} t - p\sum_{t=1}^{p-1/2}\left[\frac{ta}{p}\right]$$

Προσθέτοντας σ' αυτή την (II) έχουμε

$$mp - 2\sum_{i=1}^{k} a_i = (a+1)\sum_{t=1}^{p-1/2} t - p\sum_{t=1}^{p-1/2}\left[\frac{ta}{p}\right]$$

$$=(a+1)\frac{p^2-1}{8} - p\sum_{t=1}^{p-1/2}\left[\frac{ta}{p}\right]$$

Επειδή $a+1\equiv a-1 \pmod 2$ και $p\equiv 1 \pmod 2$ θα έχουμε

$$m\equiv (a-1)\frac{p^2-1}{8}+\sum_{t=1}^{p-1/2}\left[\frac{ta}{p}\right] \pmod 2 . \blacksquare$$

Πόρισμα 4.1

Έστω m ο αριθμός που ορίζεται στο Λήμμα του Gauss. Αν ο a είναι περιττός, τότε

$$m \equiv \sum_{t=1}^{p-1/2} \left[\frac{ta}{p}\right] \pmod 2$$

Απόδειξη

Αν ο a είναι περιττός τότε $a-1 \equiv 0 \pmod 2$, και επομένως

$$m \equiv \sum_{t=1}^{p-1/2} \left[\frac{ta}{p}\right] \pmod 2 . \blacksquare$$

Στον υπολογισμό του $(a/p) = (-1)^m$ δεν χρειαζόμαστε την ακριβή τιμή του m, αλλα κατα πόσο ο m είναι άρτιος ή περιττός.

Πόρισμα 4.2

Για κάθε περιττό πρώτο p, ισχύει

$$(2/p) = (-1)^{\frac{p^2-1}{8}}$$

Απόδειξη

Είναι $(2/p) = (-1)^m$ όπου $m \equiv \sum_{t=1}^{p-1/2} \left[\frac{2t}{p}\right] + (2-1)\frac{p^2-1}{8} \pmod 2$

Αλλά, $\sum_{t=1}^{p-1/2} \left[\frac{2t}{p}\right] = \left[\frac{2}{p}\right] + \cdots + \left[\frac{p-1}{p}\right] = 0$,

επομένως $$m \equiv \frac{p^2-1}{8} \pmod 2 .$$

Αρα $(-1)^m = (-1)^{\frac{p^2-1}{8}}$, οπότε $(2/p) = (-1)^{\frac{p^2-1}{8}} . \blacksquare$

Πόρισμα 4.3

Για κάθε περιττό πρώτο p, ισχύει

$$(2/p) = \begin{cases} 1 & \text{αν } p \equiv \pm 1 \pmod 8 \\ -1 & \text{αν } p \equiv \pm 3 \pmod 8 \end{cases} .$$

Απόδειξη.

Αν $p \equiv \pm 1 \pmod 8$ τότε $p = 8\eta \pm 1$, $\eta \in \mathbb{Z}$ και

$\frac{p^2-1}{8} = 8\eta^2 \pm 2\eta = 2(4\eta^2 \pm \eta)$ οπότε $(2/p) = 1$.

Αν $p \equiv \pm 3 \pmod 8$ τότε $p = 8\eta \pm 3$, $\eta \in \mathbb{Z}$ και

$\frac{p^2-1}{8} = 8\eta^2 \pm 6\eta + 1$ οπότε $(2/p) = -1$. ■

Το παρακάτω πόρισμα εμπίπτει στο 2ο βασικό ερώτημα της θεωρίας των τετραγωνικών υπολοίπων

Πόρισμα 4.4

Ο ακέραιος 2 είναι τετραγωνικό υπόλοιπο για όλους τους πρώτους της μορφής $8\eta \pm 1$ και είναι τετραγωνικό μη-υπόλοιπο για όλους τους πρώτους της μορφής $8\eta \pm 3$.

Παράδειγμα 4.1

Θα υπολογίσουμε τα $(2/23)$ και $(2/29)$.

Είναι $(2/23) = (-1)^{\frac{22 \cdot 24}{8}} = +1$, σύμφωνα με το πόρισμα 4.2

Διαφορετικά, αφού $23 \equiv -1 \pmod 8$ θα είναι $(2/23) = +1$ σύμφωνα με το πόρισμα 4.3.

Είναι $(2/29) = (-1)^{\frac{28 \cdot 30}{8}} = -1$ ή διαφορετικά αφού $29 \equiv -3 \pmod 8$ είναι $(2/29) = -1$.

Παράδειγμα 4.2

Θα υπολογίσουμε το $(5/13)$.

Αφού ο 5 είναι περιττός, θα είναι $(5/13) = (-1)^m$ όπου

$$m = \sum_{t=1}^{6} \left[\frac{t5}{13}\right] = \left[\frac{5}{13}\right] + \left[\frac{10}{13}\right] + \left[\frac{15}{13}\right] + \left[\frac{20}{13}\right] + \left[\frac{25}{13}\right] + \left[\frac{30}{13}\right] =$$

$$= 0 + 0 + 1 + 1 + 1 + 2 = 5$$

Άρα $(5/13) = (-1)^5 = -1$.

Πόρισμα 4.5

Για κάθε περιττό πρώτο p ισχύει

$$(-2/p) = \begin{cases} 1 & \text{αν } p \equiv 1,3 \pmod 8 \\ -1 & \text{αν } p \equiv 5,7 \pmod 8 \end{cases}$$

Απόδειξη

Είναι $(-2/p) = (-1/p)(2/p)$.

Από την Πρόταση 3.2 και το πόρισμα 4.3 έχουμε

$$(-1/p) = \begin{cases} 1 \text{ αν } p \equiv 1 \pmod 4 \\ -1 \text{ αν } p \equiv 3 \pmod 4 \end{cases} \quad \text{και} \quad (2/p) = \begin{cases} 1 \text{ αν } p \equiv \pm 1 \pmod 8 \\ -1 \text{ αν } p \equiv \pm 3 \pmod 8 \end{cases}.$$

Είναι $(-2/p) = 1$ αν $\left(p \equiv \pm 1 \pmod 8 \text{ και } p \equiv 1 \pmod 4 \right)$ ή $\left(p \equiv \pm 3 \pmod 8 \text{ και } p \equiv 3 \pmod 4 \right)$.

Άρα $(-2/p) = 1$ αν

1) $p \equiv 1 \pmod 8$ και $p \equiv 1 \pmod 4$

ή 2) $p \equiv -1 \pmod 8$ και $p \equiv 1 \pmod 4$

ή 3) $p \equiv 3 \pmod 8$ και $p \equiv 3 \pmod 4$

ή 4) $p \equiv -3 \pmod 8$ και $p \equiv 3 \pmod 4$.

Σύμφωνα με το Θεώρημα 2 του Κεφ. V τα συστήματα 2) και 4) δεν έχουν λύση, ενώ το σύστημα 1) έχει μοναδική λύση την $p \equiv 1 \pmod 8$ και το 3) έχει την μοναδική λύση $p \equiv 3 \pmod 8$.

Ομοια εργαζόμενοι βρίσκουμε ότι $(-2/p) = -1$ αν $p \equiv 5,7 \pmod 8$ ή διαφορετικά, τα δυνατά υπόλοιπα του περιττού πρώτου $p \pmod 8$ είναι $1, 3, 5$ και 7, επομένως $(-2/p) = -1$ στις περιπτώσεις που $p \equiv 5,7 \pmod 8$. ∎

Πόρισμα 4.6

Ο ακέραιος -2 είναι τετραγωνικό υπόλοιπο για όλους τους πρώτους της μορφής $8n+1$ ή της μορφής $8n+3$ και είναι τετραγωνικό

μη-υπόλοιπο για όλους τους πρώτους της μορφής $8n+5$ ή της μορφής $8n+7$.

Πόρισμα 4.7

Οι περιττοί πρώτοι παράγοντες του αμεραίου x^2+2 όπου $x \in \mathbb{Z}$ είναι της μορφής $8n+1$ ή της μορφής $8n+3$.

Απόδειξη.

Απο την υπόθεση $p \mid x^2+2$ συμπεραίνουμε ότι η ισοτιμία $x^2 \equiv -2 \pmod p$ έχει λύση, άρα ο -2 είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, p)$ και επομένως $p = 8n+1$ ή $p = 8n+3$. ∎

Εδώ είναι η κατάλληλη στιγμή για να δούμε τις αρχικές ρίζες απο μια άλλη σκοπιά. Όπως έχουμε δει, δεν υπάρχει μια γενική μέθοδος για να πάρουμε μια αρχική ρίζα $(\mathrm{mod}\, p)$, p περιττός πρώτος Η επόμενη πρόταση είναι αρκετά χρήσιμη προς αυτή την κατεύθυνση.

Πρόταση 4.1

1) Αν ο p και ο $2p+1$ είναι αμφότεροι περιττοί πρώτοι τότε ο αμέραιος

$$(-1)^{p-1/2} \cdot 2$$

είναι μια αρχική ρίζα του $2p+1$

2) Αν ο p και ο $4p+1$ είναι αμφότεροι περιττοί πρώτοι τότε ο 2 είναι αρχική ρίζα του $4p+1$.

Απόδειξη.

1. Θέτουμε $q = 2p+1$. Για τον p έχουμε δυο περιπτώσεις :

$p \equiv 1 \pmod 4$ και $p \equiv 3 \pmod 4$.

Αν $p \equiv 1 \pmod 4$, τότε $(-1)^{p-1/2} \cdot 2 = 2$. Επειδή $\varphi(q) = q-1 = 2p$ η $\mathrm{ord}_q 2 \mid 2p$ άρα $\mathrm{ord}_q 2$ θα είναι $1, 2, p$ ή $2p$.

Η $\mathrm{ord}_q 2$ δεν είναι 1 ούτε 2 ($2^2 \equiv 1 \pmod q$ συνεπάγεται $q \mid 3$ που είναι άτοπο). Θα δείξουμε ότι $\mathrm{ord}_q 2$ δεν είναι p.

Είναι $(2/q) \equiv 2^{q-1/2} = 2^p \pmod q$ απο Πρόταση 3.1, 3).

Όταν όμως $p \equiv 1 \pmod 4$ ο $q \equiv 3 \pmod 8$ και από το πόρισμα 4.3 το σύμβολο Legendre $(2/q) = -1$. Άρα

$$2^p \equiv -1 \pmod q$$

που σημαίνει ότι $ord_q 2 \neq p$. Επομένως $ord_q 2 = 2p = \varphi(q)$ άρα ο 2 είναι αρχική ρίζα του q.

Αν $p \equiv 3 \pmod 4$ τότε $(-1)^{p-1/2} \cdot 2 = -2$.

Στην περίπτωση αυτή ο $q \equiv 5 \pmod 8$ και από το Πόρισμα 4.5 είναι

$$(-2/q) = -1$$

Αλλά $(-2/q) \equiv (-2)^p \pmod q$ από Πρόταση 3.1 3)

επομένως $(-2)^p \equiv -1 \pmod q$ που σημαίνει ότι $ord_q(-2) \neq p$. Φανερά $ord_q(-2) \neq 1$, και 2 επομένως $ord_q(-2) = 2p = \varphi(q)$, άρα ο -2 είναι αρχική ρίζα του q.

2) Όμοια με την απόδειξη του 1). ■

5. Ο νόμος της τετραγωνικής αντιστροφής.

Ο νόμος της τετραγωνικής αντιστροφής είναι από τα διασημότερα θεωρήματα της Αριθμοθεωρίας. Η εικασία ότι ισχύει το θεώρημα αυτό είχε διατυπωθεί από τον Euler κατά την περίοδο 1744 - 1746, ενώ ο Legendre το 1785 έδωσε μια μερική απόδειξη.

Την πρώτη πλήρη απόδειξη έδωσε ο Gauss σε ηλικία 18 ετών το 1796 και περιέχεται στο μνημειώδες έργο του "Disquisitiones Arithmeticae" (1801).

Ο νόμος της τετραγωνικής αντιστροφής απαντά στο 2ο βασικό πρόβλημα των τετραγωνικών υπολοίπων που είναι κατά πολύ δυσκολότερο του 1ου προβλήματος, την επίλυσή του οποίου

παίρνουμε από το κριτήριο του Euler και το Λήμμα του Gauss με διαδικασίες που είναι μερικές φορές μακροσκελείς.

Υπολογίζεται ότι μέχρι σήμερα έχουν δοθεί πάνω από 150 ανεξάρτητες αποδείξεις του νόμου της τετραγωνικής αντιστροφής.

Η απόδειξη που θα δώσουμε είναι γεωμετρική χρησιμοποιούνται συνδεσμικά σημεία στο επίπεδο και οφείλεται στον μαθητή του Gauss Eisenstein.

Θεώρημα 5.1 (Νόμος της τετραγωνικής αντιστροφής)

Έστω p και q δυο διαφορετικοί περιττοί πρώτοι αριθμοί. Τότε,

$$(p/q)(q/p)=(-1)^{\frac{(p-1)(q-1)}{4}}$$

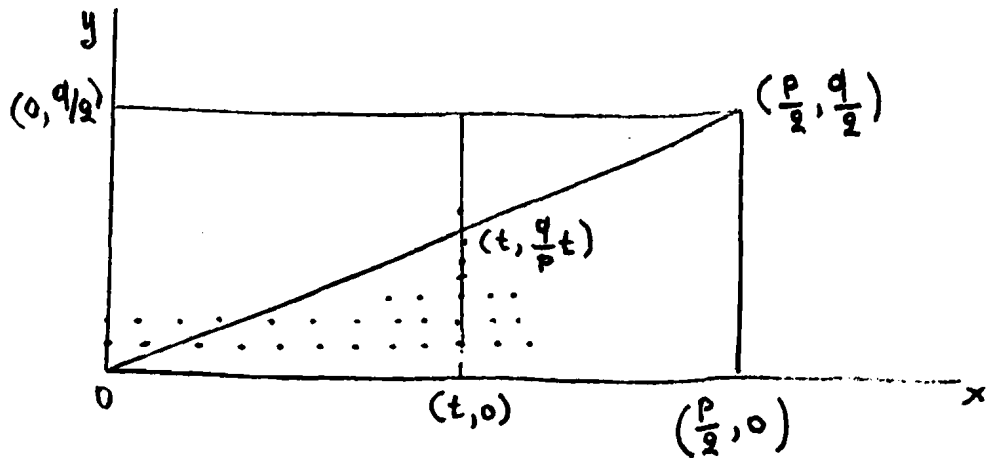
Απόδειξη

Σύμφωνα με το Λήμμα του Gauss, είναι

$$(q/p)=(-1)^m \quad \text{όπου} \quad m=\sum_{t=1}^{\frac{p-1}{2}}\left[\frac{tq}{p}\right]=\left[\frac{q}{p}\right]+\left[\frac{2q}{p}\right]+\cdots+\left[\frac{(p-1)q}{2p}\right]$$

$$(p/q)=(-1)^n \quad \text{όπου} \quad n=\sum_{t=1}^{\frac{q-1}{2}}\left[\frac{tp}{q}\right]=\left[\frac{p}{q}\right]+\left[\frac{2p}{q}\right]+\cdots+\left[\frac{(q-1)p}{2q}\right]$$

οπότε $(p/q)(q/p)=(-1)^n(-1)^m=(-1)^{m+n}$. Αρκεί να δείξουμε ότι $m+n=\frac{(p-1)(q-1)}{4}$. Πάνω στο επίπεδο xoy θεωρούμε



το ορθογώνιο παραλληλόγραμμο με κορυφές $(0,0), \left(\frac{p}{2},0\right), \left(0,\frac{q}{2}\right), \left(\frac{p}{2},\frac{q}{2}\right)$. Ένα συνδεσμικό σημείο (lattice point) σ' ένα καρτεσιανό επίπεδο, είναι ένα σημείο που έχει και τις δύο συντεταγμένες τους ακέραιους αριθμούς.

Το ορθογώνιο αυτό περικλείει στο εσωτερικό του

$\frac{p-1}{2} \cdot \frac{q-1}{2}$ σε πλήθος συνδεσμικά σημεία

(δεν υπολογίζονται όσα είναι στην περίμετρο) περιέχει δηλαδή όλα τα σημεία (x,y), $x,y \in \mathbb{Z}$ με $1 \leq x \leq \frac{p-1}{2}$ και $1 \leq y \leq \frac{q-1}{2}$.

Θεωρούμε την διαγώνιο του ορθογωνίου που διέρχεται από το $(0,0)$. Αυτή σαν ευθεία έχει καρτεσιανή εξίσωση $y = \frac{q}{p}x$. Πάνω στην διαγώνιο δεν υπάρχει κανένα από αυτά τα $\frac{p-1}{2} \cdot \frac{q-1}{2}$ συνδεσμικά σημεία. Πραγματικά, αν για κάποιο συνδεσμικό σημείο (x_1, y_1) με $1 \leq x_1 \leq \frac{p-1}{2}$ και $1 \leq y_1 \leq \frac{q-1}{2}$ είχαμε

$\frac{y_1}{x_1} = \frac{q}{p}$, τότε επειδή το κλάσμα $\frac{q}{p}$ είναι ανάγωγο θα είχαμε

$y_1 = q\mu$ και $x_1 = p\mu$, $\mu \in \mathbb{Z}$, άρα $q \mid y_1$ και $p \mid x_1$

πράγμα άτοπο $y_1 < q$ και $x_1 < p$.

Θα μετρήσουμε τώρα το πλήθος των συνδεσμικών σημείων (t,y) που υπάρχουν πάνω στο ευθύγραμμο τμήμα που είναι κάθετο στον άξονα των ox στο σημείο $(t,0)$ και στο κομμάτι που είναι κάτω από την διαγώνιο. Για $x=t$, το ανεξάρτητο y θα είναι $1 \leq y \leq t \cdot \frac{q}{p}$ και επειδή το y είναι ακέραιος θα έχουμε $1 \leq y \leq \left[\frac{tq}{p}\right]$. Επομένως το πλήθος των σημείων αυτών είναι $\left[\frac{tq}{p}\right]$.

Άρα το συνολικό πλήθος των συνδεσμικών σημείων που βρίσκονται στο κάτω ήμισυ του ορθογωνίου είναι

$$\left[\frac{q}{p}\right] + \cdots + \left[\frac{(p-1)q}{2p}\right] = \sum_{t=1}^{p-1/2} \left[\frac{tq}{p}\right] = m.$$

Με όμοιους συλλογισμούς βρίσκουμε ότι το πλήθος των συνδεσμικών σημείων που βρίσκονται στο πάνω ήμισυ του ορθογωνίου είναι

$$\sum_{t=1}^{q-1/2} \left[\frac{tp}{q}\right] = \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \cdots + \left[\frac{(q-1)p}{2q}\right] = \eta .$$

Αρα για το συνολικό πλήθος των θεωρούμενων σημείων ισχύει

$\frac{p-1}{2} \cdot \frac{q-1}{2} = m + \eta$ πράγμα που επιδιώξαμε. ■

Πόρισμα 5.1

Αν οι p και q είναι διαφορετικοί περιττοί πρώτοι, τότε

$$(p/q) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot (q/p)$$

Απόδειξη.

Από νόμο τετραγωνικής αντιστροφής έχουμε

$$(p/q)\cdot(q/p) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Πολλαπλασιάζουμε και τα δυο μέλη της με (q/p) και έχουμε

$$(p/q)(q/p)^2 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} (q/p)$$

και επειδή $(q/p)^2 = 1$, έχουμε το ζητούμενο. ■

Πόρισμα 5.2

Αν οι p και q είναι διαφορετικοί περιττοί πρώτοι, τότε

$$(p/q)(q/p) = \begin{cases} 1 & \text{αν } p \equiv 1 \pmod 4 \text{ ή } q \equiv 1 \pmod 4 \\ -1 & \text{αν } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Απόδειξη

Ο αριθμός $\frac{p-1}{2}\frac{q-1}{2}$ είναι άρτιος αν και μόνο αν ένας τουλάχιστον από τους p και q είναι της μορφής $4n+1$, αν και οι δύο είναι της μορφής $4n+3$ τότε ο $\frac{p-1}{2}\cdot\frac{q-1}{2}$ είναι περιττός. Από τον νόμο της τετραγωνικής αντιστροφής έχουμε το ζητούμενο. ■

Πόρισμα 5.3

Αν οι p και q είναι διαφορετικοί περιττοί πρώτοι, τότε

$$(p/q) = \begin{cases} (q/p) & \text{αν } p \equiv 1 \pmod 4 \text{ ή } q \equiv 1 \pmod 4 \\ -(q/p) & \text{αν } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Απόδειξη.

Η απόδειξη του προκύπτει από το Πόρισμα 5.1 και την απόδειξη του Πορίσματος 5.2. ■

5α. Εφαρμογές του νόμου τετραγωνικής αντιστροφής.

I) Στο 1ο πρόβλημα της θεωρίας των τετραγωνικών υπολοίπων.

Έστω p περιττός πρώτος και $a \in \mathbb{Z}$, $a \neq 1$ με $p \nmid a$.

Μας ζητούν να αποφανθούμε κατά πόσο ο a είναι τετραγωνικό υπόλοιπο ή μη-υπόλοιπο (mod p).

Υποθέτουμε ότι ο a έχει πρωτογενή ανάλυση

$$a = \pm 2^{\beta_0} \cdot p_1^{\beta_1} \cdots p_r^{\beta_r}, \quad p_i \neq 2 \quad i = 1, \ldots, r$$

Ο νόμος της τετραγωνικής αντιστροφής μαζί με την Πρόταση 3.1 και το Πόρισμα 4.2 καθιστούν τον υπολογισμό του (a/p) αρκετά απλό. Είναι

$$(a/p) = (\pm 1/p)(2/p)^{\beta_0} \cdot (p_1/p)^{\beta_1} \cdots (p_r/p)^{\beta_r}$$

Έτσι για να υπολογίσουμε το (a/p) αρκεί να υπολογίσουμε τα

$$(-1/p), (2/p), \text{ και } (p_i/p).$$

Τα $(-1/p)$ και $(2/p)$ τα έχουμε υπολογίσει, Πρόταση 3.1 και Πόρισμα 4.2. Μένουν τα σύμβολα (p_i/p) όπου p_i και p είναι διαφορετικοί περιττοί πρώτοι. Από τον νόμο της τετραγωνικής αντιστροφής μπορούμε πάντα να αντικαταστήσουμε

το (p_i/p) με ένα νέο σύμβολο Legendre που έχει μικρότερο παρονομαστή. Διαμέσου συνεχών αντιστροφών και διαιρέσεων ο υπολογισμός του (a/p) ανάγεται τελικά στις γνωστές ποσότητες

$$(-1/q),\ (1/q),\ (2/q)$$

όπου q περιττός πρώτος.

Ας δούμε αυτά μέσα από παραδείγματα.

Παράδειγμα 5.1

Είναι ο 210 τετραγωνικό υπόλοιπο του 1999;

Ο 1999 είναι πρώτος και $210 = 2\cdot 3\cdot 5\cdot 7$.

Έτσι $\left(\frac{210}{1999}\right) = \left(\frac{2}{1999}\right)\left(\frac{3}{1999}\right)\left(\frac{5}{1999}\right)\left(\frac{7}{1999}\right)$

Είναι $\left(\frac{2}{1999}\right) = (-1)^{\frac{1999^2-1}{8}} = 1$,

$$\left(\frac{3}{1999}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{1999-1}{2}}\left(\frac{1999}{3}\right) = \left(\frac{1999}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

αφού $1999 \equiv 1 \pmod 3$,

$$\left(\frac{5}{1999}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{1999-1}{2}}\left(\frac{1999}{5}\right) = \left(\frac{1999}{5}\right) = \left(\frac{2^2}{5}\right) = 1$$

αφού $1999 \equiv 4 \pmod 5$

και

$$\left(\frac{7}{1999}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{1999-1}{2}}\left(\frac{1999}{7}\right) = -\left(\frac{1999}{7}\right) = -\left(\frac{2^2}{7}\right) = -1$$

αφού $1999 \equiv 4 \pmod 7$

Άρα $\left(\frac{210}{1999}\right) = 1\,(-1)\,1\,(-1) = 1$, δηλαδή ο 210 είναι τετραγωνικό υπόλοιπο του 1999.

Παράδειγμα 5.2

Ο 1997 είναι πρώτος αριθμός, θα δείξουμε ότι κανείς αριθμός της μορφής $308 + 1997n$, $n \in \mathbb{Z}$, δεν μπορεί να είναι τετράγωνο ακεραίου.

Θα δείξουμε ότι δεν υπάρχουν ακέραιοι x ώστε $x^2 = 308 + 1997n$ δηλαδή ότι η ισοτιμία $x^2 \equiv 308 \pmod{1997}$ δεν έχει λύση.

Αρκεί να δείξουμε ότι $(308/1997) = -1$

Είναι $308 = 2^2 \cdot 7 \cdot 11$, οπότε

$$(308/1997) = (2^2/1997)(7/1997)(11/1997)$$

Είναι $(2^2/1997) = 1$,

$$(7/1997) = (-1)^{\frac{7-1}{2}\frac{1997-1}{2}} (1997/7) = (1997/7) = (2/7) = (-1)^{\frac{7^2-1}{8}} = 1$$

και $(11/1997) = (1997/11) = (6/11) = (2/11)(3/11)$

Αλλά $(2/11) = (-1)^{\frac{11^2-1}{8}} = -1$ και

$$(3/11) = (-1)^{\frac{3-1}{2}\cdot\frac{11-1}{2}} (11/3) = -(11/3) = -(2/3) = -(-1)^{\frac{9-1}{8}} =$$
$$= (-1)(-1) = 1$$

Άρα $(308/1997) = 1 \cdot 1 \cdot (-1) \cdot 1 = -1$.

Παράδειγμα 5.3

Είναι ο -540 τετραγωνικό υπόλοιπο του 7;

Επειδή $-540 \equiv -1 \pmod 7$ θα είναι

$$(-540/7) = (-1/7) = (-1)^{\frac{7-1}{2}} = -1.$$

Άρα ο -540 δεν είναι τετραγωνικό υπόλοιπο του 7.

Άλλος τρόπος. Είναι $-540 = -2^2 \cdot 3 \cdot 5$ οπότε

$(-540/7) = (-1/7)(2^2/7)(3/7)(5/7)$. Είναι

$(-1/7) = -1$, $(2^2/7) = 1$, $(3/7) = -1$ και $(5/7) = -1$

Έτσι $(-540/7) = (-1)1 \cdot (-1)(-1) = -1$ δηλαδή ο -540

δεν είναι τετραγωνικό υπόλοιπο του 7.

II) Στο 2ο πρόβλημα της θεωρίας των τετραγωνικών υπολοίπων.

Μας δίνεται ο ακέραιος a και αναζητούμε τους περιττούς πρώτους p με $p \nmid a$, που έχουν τον a τετραγωνικό υπόλοιπο ή μη-υπόλοιπο, δηλαδή, τα p για τα οποία $(a/p)=1$ ή $(a/p)=-1$.

Έστω $a=\pm k^2 \cdot b$, όπου k^2 είναι το μεγαλύτερο τετράγωνο που περιέχεται στον a και $b>0$, τότε

$$(a/p)=(\pm 1/p)(k^2/p)(b/p)=(\pm 1/p)(b/p).$$

Αν $b=q_1 \cdots q_r$ όπου q_i πρώτοι με $p \neq q_i$, $i=1,\dots,r$ τότε

$$(a/p)=(\pm 1/p)(q_1/p)\cdots(q_r/p).$$

Η αναζήτησή μας λοιπόν μπορεί να περαιωθεί από την μελέτη των συμβόλων

$$(\pm 1/p),\ (2/p),\ (q/p).$$

Είναι φανερό ότι $(1/p)=1$ για κάθε πρώτο p.
Από την Πρόταση 3.2 και το Πόρισμα 4.3 έχουμε

$$(-1/p)=\begin{cases} 1 & \text{αν } p\equiv 1 \pmod 4 \\ -1 & \text{αν } p\equiv 3 \pmod 4 \end{cases} \quad \text{και} \quad (2/p)=\begin{cases} 1 & \text{αν } p\equiv \pm 1 \pmod 8 \\ -1 & \text{αν } p\equiv 3 \pmod 8 \end{cases}$$

όπου p περιττός πρώτος.
Μένει λοιπόν το σύμβολο (q/p) όπου q περιττός πρώτος.
Αναζητούμε τους περιττούς πρώτους p, με $p \neq q$, για τους οποίους $(q/p)=1$ ή $(q/p)=-1$.

IIα) Αν ο q είναι της μορφής $4n+1$.

Αν $q\equiv 1 \pmod 4$ τότε από τον νόμο της τετραγωνικής αντιστροφής έχουμε

$$(q/p)=(p/q).$$

Αν $(q/p)=1$ τότε $(p/q)=1$ δηλαδή ο p οφείλει να είναι ένα περιττό τετραγωνικό υπόλοιπο του q, ενώ αν

$(q/p)=-1$ τότε και $(p/q)=-1$ δηλαδή ο p οφείλει να είναι ένα περιττό τετραγωνικό μη-υπόλοιπο του q.

Παράδειγμα 5.4.

Για $p\neq 5$ περιττό πρώτο, ισχύει

$$(5/p)=\begin{cases}1 & \text{αν } p\equiv\pm 1 \pmod{10}\\ -1 & \text{αν } p\equiv\pm 3 \pmod{10}\end{cases}.$$

Είναι $(5/p)=(-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}}(p/5)=(p/5)$

Ο p είναι περιττός πρώτος, επομένως $p\equiv 1 \pmod 2$.

Από το αναμένο σύστημα υπολοίπων (mod 5) $\{1,2,3,4\}$ βρίσκουμε ότι ο 1 και ο 4 είναι τετραγωνικά υπόλοιπα (mod 5), ενώ ο 2 και 3 είναι τετραγωνικά μη-υπόλοιπα (mod 5).

Έτσι $(5/p)=(p/5)=1$, αν

1) $p\equiv 1 \pmod 2$ και $p\equiv 1 \pmod 5$

ή 2) $p\equiv 1 \pmod 2$ και $p\equiv 4 \pmod 5$.

Από το σύστημα 1) έχουμε $p\equiv 1 \pmod{10}$ και από το 2) έχουμε $p\equiv 9\equiv -1 \pmod{10}$. Άρα $(5/p)=1$ αν $p\equiv\pm 1 \pmod{10}$.

Όμοια, $(5/p)=(p/5)=-1$, αν

3) $p\equiv 1 \pmod 2$ και $p\equiv 2 \pmod 5$

ή 4) $p\equiv 1 \pmod 2$ και $p\equiv 3 \pmod 5$

Από το σύστημα 3) έχουμε $p\equiv 7\equiv -3 \pmod{10}$ και από το 4) έχουμε $p\equiv 3 \pmod{10}$. Άρα $(5/p)=-1$ αν $p\equiv\pm 3 \pmod{10}$. ■

II$_6$) Αν ο q είναι της μορφής $4n+3$

Αν $q\equiv 3 \pmod 4$, τότε

$$(q/p)=(-1)^{\frac{p-1}{2}}(p/q)$$

Το $(q/p)=1$, αν

1) $p \equiv 1 \pmod 4$ και $(p/q) = 1$

ή 2) $p \equiv 3 \pmod 4$ και $(p/q) = -1$.

Το $(q/p) = -1$, αν

3) $p \equiv 3 \pmod 4$ και $(p/q) = 1$

ή 4) $p \equiv 1 \pmod 4$ και $(p/q) = -1$.

Παράδειγμα 5.5

Για $p \neq 3$ περιττό πρώτο, ισχύει

$$(3/p) = \begin{cases} 1 & \text{αν } p \equiv \pm 1 \pmod{12} \\ -1 & \text{αν } p \equiv \pm 5 \pmod{12} \end{cases}$$

Από τον νόμο της τετραγωνικής αντιστροφής έχουμε

$$(3/p) = (-1)^{\frac{p-1}{2}} \cdot (p/3)$$

Είναι όμως,

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{αν } p \equiv 1 \pmod 4 \\ -1 & \text{αν } p \equiv 3 \pmod 4 \end{cases} \quad \text{και} \quad (p/3) = \begin{cases} 1 & \text{αν } p \equiv 1 \pmod 3 \\ -1 & \text{αν } p \equiv 2 \pmod 3 \end{cases}$$

Από τα παραπάνω συμπεραίνουμε ότι

i) Το $(3/p) = 1$, αν

1) $p \equiv 1 \pmod 4$ και $p \equiv 1 \pmod 3$

ή 2) $p \equiv 3 \pmod 4$ και $p \equiv 2 \pmod 3$

και,

ii) Το $(3/p) = -1$, αν

3) $p \equiv 1 \pmod 4$ και $p \equiv 2 \pmod 3$

ή 4) $p \equiv 3 \pmod 4$ και $p \equiv 1 \pmod 3$.

Από το θεώρημα 2 του κεφ V έχουμε ότι, το σύστημα 1) έχει μοναδική λύση την $p \equiv 1 \pmod{12}$, το 2) την $p \equiv 11 \equiv -1 \pmod{12}$ το 3) την $p \equiv 5 \pmod{12}$ και το 4) την $p \equiv 7 \equiv -5 \pmod{12}$.

Παράδειγμα 5.6

Για $p \neq 7$ περιττό πρώτο ισχύει

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{αν } p \equiv \pm 1, \pm 3, \pm 9 \pmod{28} \\ -1 & \text{αν } p \equiv \pm 5, \pm 11, \pm 13 \pmod{28}. \end{cases}$$

Από το νόμο της τετραγωνικής αντιστροφής, έχουμε

$$\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{7}\right).$$

Είναι, $(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{αν } p \equiv 1 \pmod 4 \\ -1 & \text{αν } p \equiv 3 \pmod 4. \end{cases}$

Από το αναμένο σύστημα υπολοίπων $(\bmod 7)$, $\{1,2,3,4,5,6\}$ βρίσκουμε ότι οι ακέραιοι 1, 2, και 4 είναι τετραγωνικά υπόλοιπα $(\bmod 7)$ ενώ οι 3, 5 και 6 είναι τετραγωνικά μη-υπόλοιπα $(\bmod 7)$.

Έτσι $\left(\frac{p}{7}\right) = 1$ αν και μόνο αν $p \equiv 1, 2, 4 \pmod 7$

και $\left(\frac{p}{7}\right) = -1$ αν και μόνο αν $p \equiv 3, 5, 6 \pmod 7$

Είναι λοιπόν $\left(\frac{7}{p}\right) = 1$, αν

A) $p \equiv 1 \pmod 4$ και $p \equiv 1, 2, 4 \pmod 7$

ή B) $p \equiv 3 \pmod 4$ και $p \equiv 3, 5, 6 \pmod 7$

Από το A) έχουμε τα συστήματα

1) $p \equiv 1 \pmod 4$ και $p \equiv 1 \pmod 7$

2) $p \equiv 1 \pmod 4$ και $p \equiv 2 \pmod 7$

3) $p \equiv 1 \pmod 4$ και $p \equiv 4 \pmod 7$

με μοναδικές λύσεις αντίστοιχα τις $p \equiv 1 \pmod{28}$, $p \equiv 9 \pmod{28}$ και $p \equiv 25 \equiv -3 \pmod{28}$.

Από το B) έχουμε όμοια 3 συστήματα με μοναδικές λύσεις τις $p \equiv 3 \pmod{28}$, $p \equiv 19 \equiv -9 \pmod{28}$ και $p \equiv 27 \equiv -1 \pmod{28}$. Τελικά, είναι

$(7/p)=1$ αν $p\equiv\pm1,\pm3,\pm9 \pmod{28}$.

Όμοια $(7/p)=-1$, αν

Γ) $p\equiv1 \pmod4$ και $p\equiv3,5,6 \pmod7$

ή Δ) $p\equiv3 \pmod4$ και $p\equiv1,2,4 \pmod7$

Με τον ίδιο τρόπο βρίσκουμε ότι

$(7/p)=-1$ αν $p\equiv\pm5,\pm11,\pm13 \pmod{28}$. ■

Τα επόμενα παραδείγματα δείχνουν πως μπορούν να συνδιασθούν όλα τα προηγούμενα για την λύση του 2ου προβλήματος της θεωρίας των τετραγωνικών υπολοίπων.

Παράδειγμα 5.7

Θα βρούμε όλους τους περιττούς πρώτους p για τους οποίους ο 14 είναι τετραγωνικό υπόλοιπο.

Είναι $14=2\cdot7$ και $(14/p)=(2/p)(7/p)$.

Γνωρίζουμε όμως από πόρισμα 4.3 ότι,

$$(2/p)=\begin{cases}1 & \text{αν } p\equiv\pm1 \pmod8\\ -1 & \text{αν } p\equiv\pm3 \pmod8\end{cases}$$

και από παράδειγμα 5.6, ότι

$$(7/p)=\begin{cases}1 & \text{αν } p\equiv\pm1,\pm3,\pm9 \pmod{28}\\ -1 & \text{αν } p\equiv\pm5,\pm11,\pm13 \pmod{28}\end{cases}$$

Άρα $(14/p)=1$, αν

Α) $p\equiv\pm1 \pmod8$ και $p\equiv\pm1,\pm3,\pm9 \pmod{28}$

ή Β) $p\equiv\pm3 \pmod8$ και $p\equiv\pm5,\pm11,\pm13 \pmod{28}$.

Είναι $[8,28]=56$.

Από το Α) παίρνουμε 12 συστήματα. Τα 6 απ' αυτά δεν έχουν λύση, ενώ τα υπόλοιπα 6 μας δίνουν τις λύσεις

$$p \equiv 1, 9, 25, 31, 47, 55 \pmod{56}.$$

Όμοια από το Β) παίρνουμε 12 συστήματα που μας δίνουν τις λύσεις $p \equiv 5, 11, 13, 43, 45, 51 \pmod{56}$.

Τελικά $(14/p) = 1$ αν

$$p \equiv 1, 5, 9, 11, 13, 25, 31, 43, 45, 47, 51, 55 \pmod{56}. \blacksquare$$

Παράδειγμα 5.8

Θα βρούμε όλους τους περιττούς πρώτους p για τους οποίους ο 35 είναι τετραγωνικό υπόλοιπο.

Είναι $35 = 5 \cdot 7$ και $(35/p) = (5/p)(7/p)$.

Τα $(5/p)$ και $(7/p)$ τα γνωρίζουμε από τα παραδείγματα 5.4 και 5.6 αντίστοιχα.

Εργαζόμενοι όπως και στο παράδειγμα 5.7 βρίσκουμε ότι

$$p \equiv 1, 9, 13, 17, 19, 23, 29, 31, 33, 43, 59, 67, 73, 81, 87,$$
$$107, 109, 111, 117, 121, 123, 127, 131, 139, \pmod{140}$$

όπου $140 = [10, 28]$. $\blacksquare$

6. Το σύμβολο του Jacobi.

Το σύμβολο Legendre (a/p) ορίζεται μόνο για περιττό πρώτο p. Ο Jacobi εισήγαγε ένα πιο γενικότερο σύμβολο, το σύμβολο Jacobi (a/P) που ορίζεται για περιττούς φυσικούς P, με τον ακόλουθο τρόπο.

Ορισμός

Έστω P περιττός φυσικός και $P = p_1 \cdots p_r$, όπου p_i είναι περιττοί πρώτοι, όχι αναγκαία διαφορετικοί.

Αν $\alpha \in \mathbb{Z}$ και $(\alpha, P) = 1$, τότε το σύμβολο Jacobi (α/P) ορίζεται ως εξής:

$$(\alpha/P) = (\alpha/p_1) \cdots (\alpha/p_r)$$

όπου (α/p_i) είναι το σύμβολο του Legendre.

Τα σύμβολα Legendre (α/p_i), $i = 1, \ldots, r$ ορίζονται, γιατί όταν $(\alpha, P) = 1$ τότε θα είναι και $(\alpha, p_i) = 1$, $i = 1, \ldots, r$.
Έτσι αν η πρωτογενής ανάλυση του P είναι

$$P = p_1^{b_1} \cdots p_\nu^{b_\nu}, \quad p_i \text{ περιττοί πρώτοι, και } b_i \geq 1$$

τότε για το σύμβολο Jacobi (α/P) έχουμε

$$(\alpha/P) = (\alpha/p_1)^{b_1} \cdots (\alpha/p_\nu)^{b_\nu}.$$

Επειδή το σύμβολο Legendre (α/p_i) είναι είτε 1 είτε -1, για το σύμβολο Jacobi, έχουμε

$$(\alpha/P) = \pm 1.$$

Οι γνωστές ιδιότητες του συμβόλου του Legendre μας διευκολύνουν να αποδείξουμε παρόμοιες ιδιότητες για το σύμβολο του Jacobi.

Πρόταση 6.1

Έστω $P = p_1 \cdots p_r$ με τους p_i περιττούς πρώτους και $\alpha \in \mathbb{Z}$ με $(\alpha, P) = 1$. Αν ο α είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, P)$ τότε

$$(\alpha/P) = 1.$$

Απόδειξη.

Αν η διωνυμική ισοτιμία $x^2 \equiv \alpha \,(\mathrm{mod}\, P)$ έχει λύση, τότε για κάθε $i = 1, \ldots, r$ η διωνυμική ισοτιμία $x^2 \equiv \alpha \,(\mathrm{mod}\, p_i)$ είναι επίσης επιλύσιμη. Επομένως $(\alpha/p_i) = 1$ για $i = 1, \ldots, r$ και επομένως $(\alpha/P) = (\alpha/p_1) \cdots (\alpha/p_r) = 1$. ∎

Το αντίστροφο όμως δεν αληθεύει. Αν $P = p_1 \cdots p_r$, $r \geq 2$ και $(a/P) = 1$, δεν αληθεύει πάντα ότι ο a είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, P)$. Πραγματικά, αν στο δεξιό μέλος της σχέσης

$$(a/P) = (a/p_1) \cdots (a/p_r)$$

εμφανίζεται άρτιος αριθμός παραγόντων -1, τότε $(a/P) = 1$, αλλά η διωνυμική ισοτιμία $x^2 \equiv a \,(\mathrm{mod}\, P)$ δεν έχει λύση, δηλαδή το a δεν είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, P)$. Για παράδειγμα, $(2/9) = (2/3)(2/3) = 1$, αλλά η διωνυμική ισοτιμία $x^2 \equiv 2 \,(\mathrm{mod}\, 9)$ δεν έχει λύση.

Πρόταση 6.2

Έστω $P = p_1 \cdots p_r$ με τους p_i περιττούς πρώτους και $a \in \mathbb{Z}$ με $(a, P) = 1$.

Αν $(a/P) = -1$ τότε ο a είναι τετραγωνικό μη-υπόλοιπο $(\mathrm{mod}\, P)$.

Απόδειξη.

Αν $(a/P) = -1$, τότε στο δεξιό μέλος της σχέσης

$$(a/P) = (a/p_1) \cdots (a/p_r)$$

εμφανίζεται περιττός αριθμός παραγόντων -1, που σημαίνει ότι για κάποιο i, η διωνυμική ισοτιμία $x^2 \equiv a \,(\mathrm{mod}\, p_i)$ δεν έχει λύση, άρα και η $x^2 \equiv a \,(\mathrm{mod}\, P)$ δεν έχει λύση, δηλαδή ο a είναι τετραγωνικό μη-υπόλοιπο $(\mathrm{mod}\, P)$. ∎

Το αντίστροφο δεν αληθεύει.

Δηλαδή, αν $P = p_1 \cdots p_r$ με $r \geq 2$ και η διωνυμική ισοτιμία $x^2 \equiv a \,(\mathrm{mod}\, P)$ δεν έχει λύση, τότε δεν είναι αληθές ότι πάντα $(a/P) = -1$. Πραγματικά, μπορεί στο δεξιό μέλος της σχέσης $(a/P) = (a/p_1) \cdots (a/p_r)$ να εμφανίζεται άρτιος αριθμός παραγόντων -1 και συνεπώς $(a/P) = 1$.

Πρόταση 6.3

Έστω $P=p_1\cdots p_r$ όπου $p_1,\dots,p_r$ περιττοί πρώτοι και $a,b\in\mathbb{Z}$ με $(a,P)=1$ και $(b,P)=1$. Τότε ισχύουν τα εξής:

1) $(1/P)=1$

2) Αν $a\equiv b \pmod P$ τότε $(a/P)=(b/P)$.

3) $(ab/P)=(a/P)(b/P)$

4) $(ab^2/P)=(a/P)$.

Απόδειξη.

1) $(1/P)=(1/p_1)\cdots(1/p_r)=1\cdots 1=1$.

2) Αφού $a\equiv b \pmod P$ θα είναι και $a\equiv b \pmod{p_i}$, $i=1,\dots,r$ επομένως $(a/p_i)=(b/p_i)$, $i=1,\dots,r$.

Άρα $(a/P)=(a/p_1)\cdots(a/p_r)=(b/p_1)\cdots(b/p_r)=(b/P)$.

3) Αφού $(a,P)=(b,P)=1$ θα είναι και $(ab,P)=1$ και $(ab,p_i)=1$ $i=1,\dots,r$. Έτσι $(ab/p_i)=(a/p_i)(b/p_i)$ $i=1,\dots,r$.

Άρα, $(ab/P)=(ab/p_1)\cdots(ab/p_r)=(a/p_1)\cdots(a/p_r)(b/p_1)\cdots(b/p_r)$

$=(a/P)(b/P)$.

4) $(ab^2/P)=(a/P)(b^2/P)=(a/P)(b/P)^2=(a/P)$

αφού πάντα $(b/p)^2=1$. ■

Πρόταση 6.4

Αν $P=p_1\cdots p_r$ και $Q=q_1\cdots q_s$ όπου $p_1,\dots,p_r$ και $q_1,\dots,q_s$ είναι περιττοί πρώτοι και $(a,P)=(a,Q)=1$, τότε

$$(a/PQ)=(a/P)(a/Q).$$

Απόδειξη.

Είναι $(a/P) = (a/p_1)\cdots(a/p_r)$ και $(a/Q) = (a/q_1)\cdots(a/q_s)$

Επομένως,

$$(a/P)(a/Q) = (a/p_1)\cdots(a/p_r)(a/q_1)\cdots(a/q_s) =$$

$$= (a/p_1\cdots p_r q_1\cdots q_s) = (a/PQ) \cdot \blacksquare$$

Οι ειδικοί τύποι για τον υπολογισμό των συμβόλων Legendre $(-1/p)$ και $(2/p)$, ισχύουν επίσης και για το σύμβολο Jacobi.

Πρόταση 6.5

Αν $P = p_1\cdots p_r$ όπου $p_1,\dots,p_r$ είναι περιττοί πρώτοι, τότε

1) $(-1/P) = (-1)^{\frac{P-1}{2}}$

2) $(2/P) = (-1)^{\frac{P^2-1}{8}}$

Απόδειξη

1) Είναι $(-1/P) = (-1/p_1)\cdots(-1/p_r) = (-1)^{\frac{p_1-1}{2}}\cdots(-1)^{\frac{p_r-1}{2}} =$

$$= (-1)^{\sum_{i=1}^{r}\frac{p_i-1}{2}}$$

Αλλά, $P = p_1\cdots p_r = [1+(p_1-1)]\cdots[1+(p_r-1)] =$

$$= 1 + \sum_{i=1}^{r}(p_i-1) + \sum_{\substack{i,k=1\\ i<k}}^{r}(p_i-1)(p_k-1) + \cdots + \prod_{i=1}^{r}(p_i-1)$$

Κάθε παραγοντας $p-1$ είναι άρτιος, οπότε κάθε άθροισμα μετά το πρώτο είναι διαιρετό από τον 4. Επομένως,

$$P \equiv 1 + \sum_{i=1}^{r}(p_i-1) \pmod 4$$

άρα

$$\frac{P-1}{2} \equiv \sum_{i=1}^{r}\frac{p_i-1}{2} \pmod 2$$

Αρα $(-1)^{\frac{P-1}{2}} = (-1)^{\sum_{i=1}^{r} \frac{p_i-1}{2}}$, και επομένως

$$(-1/P) = (-1)^{\frac{P-1}{2}}.$$

2) Είναι $(2/P) = (2/p_1)\cdots(2/p_r) = (-1)^{\frac{p_1^2-1}{8}} \cdots (-1)^{\frac{p_r^2-1}{8}}$

$$= (-1)^{\sum_{i=1}^{r} \frac{p_i^2-1}{8}}$$ σύμφωνα με το Πόρισμα 4.2

Γράφουμε $P^2 = [1+(p_1^2-1)]\cdots[1+(p_r^2-1)] =$

$$= 1 + \sum_{i=1}^{r}(p_i^2-1) + \sum_{\substack{i,k=1 \\ i<k}}^{r}(p_i^2-1)(p_k^2-1) + \cdots + \prod_{i=1}^{r}(p_i^2-1)$$

Επειδή p_i περιττός, έχουμε $p_i^2 - 1 \equiv 0 \pmod 8$, οπότε κάθε άθροισμα μετά το πρώτο είναι διαιρετό από το 64, άρα

$$P^2 \equiv 1 + \sum_{i=1}^{r}(p_i^2-1) \pmod{64}$$

και επομένως

$$\frac{P^2-1}{8} \equiv \sum_{i=1}^{r} \frac{p_i^2-1}{8} \pmod 8$$

Αρα $(-1)^{\frac{P^2-1}{8}} = (-1)^{\sum_{i=1}^{r} \frac{p_i^2-1}{8}}$

και επομένως $(2/p) = (-1)^{\frac{p^2-1}{8}}$. ∎

Πρόταση 6.6 (Ο νόμος της τετραγωνικής αντιστροφής για τα σύμβολα Jacobi).

Αν $P = p_1 \cdots p_r$ και $Q = q_1 \cdots q_s$, όπου $p_1, \ldots, p_r$ και $q_1, \ldots, q_s$ είναι περιττοί πρώτοι και $(P,Q) = 1$, τότε

$$(P/Q)(Q/P) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

Απόδειξη.

$$(P/Q) = (P/q_1)\cdots(P/q_s) = \prod_{j=1}^{s}(P/q_j) = \prod_{j=1}^{s}\left(\prod_{i=1}^{r}(p_i/q_j)\right)$$

και

$$(Q/P) = (Q/p_1)\cdots(Q/p_r) = \prod_{i=1}^{r}(Q/p_i) = \prod_{i=1}^{r}\left(\prod_{j=1}^{s}(q_j/p_i)\right).$$

Αρα $$(P/Q)(Q/P) = \prod_{j=1}^{s}\left(\prod_{i=1}^{r}(p_i/q_j)\right)\prod_{i=1}^{r}\left(\prod_{j=1}^{s}(q_j/p_i)\right)$$

$$= \prod_{i=1}^{r}\prod_{j=1}^{s}(p_i/q_j)(q_j/p_i) = (-1)^m$$

όπου $$m = \frac{1}{4}\sum_{i=1}^{r}\sum_{j=1}^{s}(p_i-1)(q_j-1) = \frac{1}{4}\left(\sum_{i=1}^{r}(p_i-1)\right)\left(\sum_{j=1}^{s}(q_j-1)\right).$$

Απο την απόδειξη όμως της πρότασης 6.5 έχουμε

$$\frac{1}{2}\sum_{i=1}^{r}(p_i-1) \equiv \frac{P-1}{2} \pmod 2 \quad \text{και}$$

$$\frac{1}{2}\sum_{j=1}^{s}(q_j-1) \equiv \frac{Q-1}{2} \pmod 2$$

Αρα $$m \equiv \frac{P-1}{2}\,\frac{Q-1}{2} \pmod 2$$

και επομένως $$(-1)^m = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

πράγμα που επιδιώξαμε. ■

Πόρισμα 6.1

Αν $P = p_1\cdots p_r$ και $Q = q_1,\ldots,q_s$ όπου $p_1,\ldots,p_r$ και $q_1,\ldots,q_s$ είναι περιττοί πρώτοι και $(P,Q)=1$ τότε

$$(P/Q) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}(Q/P). \blacksquare$$

Το μεγάλο πλεονέκτημα του συμβόλου του Jacobi είναι ότι επιτρέπει υπολογισμούς με το σύμβολο Legendre χωρίς να αναλύουμε μεγάλους αριθμούς σε γινόμενα πρώτων

παραγόντων. Ας δούμε τώρα μερικά παραδείγματα, για να διευκρινίσουμε τις διαφορές των συμβόλων Jacobi και Legendre στην πράξη.

Παράδειγμα 6.1

Θα υπολογίσουμε το σύμβολο Jacobi $(210/1999)$.

Ο 1999 είναι περιττός, και μάλιστα περιττός πρώτος, και $(210, 1999) = 1$. Είναι $210 = 2 \cdot 105$ οπότε

$$\left(\frac{210}{1999}\right) = \left(\frac{2}{1999}\right)\left(\frac{105}{1999}\right).$$

Έχουμε $\left(\frac{2}{1999}\right) = (-1)^{\frac{1999^2-1}{8}} = 1$

και

$$\left(\frac{105}{1999}\right) = (-1)^{\frac{105-1}{2}\cdot\frac{1999-1}{2}}\left(\frac{1999}{105}\right) = \left(\frac{1999}{105}\right)$$

Αλλά $1999 \equiv 4 \pmod{105}$, οπότε $\left(\frac{1999}{105}\right) = \left(\frac{4}{105}\right)$

$$= \left(\frac{2^2}{105}\right) = \left(\frac{1}{105}\right) = 1.$$

Άρα $\left(\frac{210}{1999}\right) = 1$, όπως το είχαμε ξαναβρεί στο παράδειγμα 5.1 με σύμβολα Legendre.

Παράδειγμα 6.2

Θα υπολογίσουμε το σύμβολο Jacobi $(308/1997)$.

Στο παράδειγμα 5.2 υπολογίσαμε το σύμβολο Legendre $\left(\frac{308}{1997}\right) = -1$ αφού ο 1997 είναι περιττός πρώτος.

Ας το υπολογίσουμε με σύμβολα Jacobi.

$$\left(\frac{308}{1997}\right) = \left(\frac{2^2 \cdot 77}{1997}\right) = \left(\frac{2^2}{1997}\right)\left(\frac{77}{1997}\right) = 1 \cdot \left(\frac{77}{1997}\right)$$

$$= \left(\frac{77}{1997}\right)$$

Αλλά

$$\left(\frac{77}{1997}\right) = (-1)^{\frac{77-1}{2}\cdot\frac{1997-1}{2}}\left(\frac{1997}{77}\right) = \left(\frac{1997}{77}\right) = \left(\frac{72}{77}\right)$$

αφού $1997 \equiv 72 \pmod{77}$.

Αλλά $\left(\frac{72}{77}\right) = \left(\frac{2^3 \cdot 3^2}{77}\right) = \left(\frac{2}{77}\right)\left(\frac{2^2}{77}\right)\left(\frac{3^2}{77}\right) = \left(\frac{2}{77}\right)$

$= (-1)^{\frac{77^2-1}{8}} = -1.$

Έτσι και πάλι βρίσκουμε $\left(\frac{308}{1977}\right) = -1$, και σύμφωνα με την πρόταση 6.2 ο 308 είναι τετραγωνικό μη-υπόλοιπο (mod 1977).

Παράδειγμα 6.3

Θα επιλύσουμε την διωνυμική ισοτιμία $x^2 \equiv 21 \pmod{253}$.

Ο 253 δεν είναι πρώτος και $253 = 11 \cdot 23$.

Υπολογίζουμε το σύμβολο Jacobi $\left(\frac{21}{253}\right)$. Είναι

$$\left(\frac{21}{253}\right) = (-1)^{\frac{21-1}{2}\cdot\frac{253-1}{2}} \left(\frac{253}{21}\right) = \left(\frac{253}{21}\right) = \left(\frac{1}{21}\right) = 1.$$

αφού $253 \equiv 1 \pmod{21}$.

Επομένως $\left(\frac{21}{253}\right) = 1$, αλλά αυτό είναι ένα σύμβολο Jacobi και απ' αυτό δεν μπορούμε να συμπεράνουμε ότι η ισοτιμία $x^2 \equiv 21 \pmod{253}$ έχει λύση.

Είναι όμως,

$$\left(\frac{21}{253}\right) = \left(\frac{21}{11 \cdot 23}\right) = \left(\frac{21}{11}\right)\left(\frac{21}{23}\right)$$

και επειδή $21 \equiv -1 \pmod{11}$ θα είναι $\left(\frac{21}{11}\right) = \left(\frac{-1}{11}\right) = (-1)^{\frac{11-1}{2}} = -1$

που συμαίνει ότι η ισοτιμία $x^2 \equiv 21 \pmod{11}$ δεν έχει λύση και επομένως και η $x^2 \equiv 21 \pmod{253}$ δεν έχει λύση. ■

Παράδειγμα 6.4

Θα δείξουμε ότι ο 111 είναι τετραγωνικό μη-υπόλοιπο (mod 317).

Για το σύμβολο Jacobi $\left(\frac{111}{317}\right)$ έχουμε

$$\left(\frac{111}{317}\right) = \left(\frac{317}{111}\right) = \left(\frac{-16}{111}\right) = \left(\frac{-1}{111}\right) = -1$$

επομένως, σύμφωνα με την Πρόταση 6.2, έχουμε το ζητούμενο. ■

7. Τετραγωνικά υπόλοιπα $(\mathrm{mod} p^\beta)$ όπου p περιττός πρώτος.

Πρόταση 7.1

Έστω p περιττός πρώτος και β φυσικός ≥ 1. Αν $a \in \mathbb{Z}$, με $p \nmid a$, τότε η διωνυμική ισοτιμία $x^2 \equiv a \ (\mathrm{mod} p^\beta)$ έχει λύση αν και μόνο αν η διωνυμική ισοτιμία $x^2 \equiv a \ (\mathrm{mod} p)$ έχει λύση, δηλαδή $(a/p) = 1$.

Στην περίπτωση αυτή, η $x^2 \equiv a \ (\mathrm{mod} p^\beta)$ έχει ακριβώς δυο λύσεις.

Απόδειξη.

Αν στην πρόταση 3.2 του Κεφ VII θέσουμε $m = 2$, παίρνουμε το πρώτο μέρος της πρότασης. Στην περίπτωση που η $x^2 \equiv a \ (\mathrm{mod} p^\beta)$ έχει λύση, τότε αυτή, σύμφωνα με το θεώρημα 3.1 του Κεφ VII έχει d λύσεις, όπου $d = (2, \varphi(p^\beta)) = (2, p^{\beta-1}(p-1)) = (2, p-1) = 2$, αφού ο $p-1$ είναι άρτιος.

Πόρισμα 7.1

Έστω p περιττός πρώτος και β φυσικός ≥ 1. Αν $a \in \mathbb{Z}$ με $p \nmid a$, τότε ο a είναι τετραγωνικό υπόλοιπο $(\mathrm{mod} p^\beta)$ αν και μόνο αν ο a είναι τετραγωνικό υπόλοιπο $(\mathrm{mod} p)$ δηλαδή αν $(a/p) = 1$. ∎

Αν x_0 είναι μια λύση της ισοτιμίας $x^2 \equiv a \ (\mathrm{mod} p^\beta)$ τότε οι δύο λύσεις της είναι οι $x \equiv \pm x_0 \ (\mathrm{mod} p^\beta)$.

Παράδειγμα 7.1

Θα εξετάσουμε αν οι αριθμοί 3 και 5 είναι τετραγωνικά υπόλοιπα $(\mathrm{mod} 31^\beta)$ όπου β φυσικός ≥ 1.

Εξετάζουμε καταρχάς την περίπτωση $\beta = 1$.

Για τα σύμβολα Legendre $(3/31)$ και $(5/31)$ έχουμε.

$$(3/31) = (-1)^{\frac{3-1}{2} \cdot \frac{31-1}{2}} (31/3) = -(31/3) = -(1/3) = -1$$

και $\left(5/31\right)=(-1)^{\frac{5-1}{2}\cdot\frac{31-1}{2}}\left(31/5\right)=\left(31/5\right)=\left(1/5\right)=1$.

Επομένως ο 5 είναι τετραγωνικό υπόλοιπο (mod 31) και επομένως είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\ 31^b)$ για κάθε φυσικό $b\geq 1$, ενώ ο 3 είναι τετραγωνικό μη-υπόλοιπο $(\mathrm{mod}\ 31^b)$ για κάθε φυσικό $b\geq 1$.

Παράδειγμα 7.2

Θα δείξουμε ότι ο 2 είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\ 7^3)$ και θα βρούμε τις λύσεις της διωνυμικής ισοτιμίας

$$x^2\equiv 2\ (\mathrm{mod}\ 7^3) \qquad (*)$$

Είναι $(2/7)=(-1)^{\frac{7^2-1}{8}}=(-1)^6=1$, άρα ο 2 είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\ 7)$ και επομένως είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\ 7^3)$.

Αν γνωρίζαμε μια λύση της $(*)$, για παράδειγμα την $x\equiv 108\ (\mathrm{mod}\ 7^3)$ τότε η άλλη λύση της είναι η $x\equiv -108\equiv 235\ (\mathrm{mod}\ 7^3)$.

Θα βρούμε τώρα τις δυο λύσεις της $(*)$. Εργαζόμαστε όπως και στο Κεφ. VI. Θεωρούμε την πολυωνυμική ισοτιμία

$$f(x)=x^2-2\equiv 0\ (\mathrm{mod}\ 7) \qquad (1)$$

Είναι $f'(x)=2x$.

b_1) Η (1) έχει δυο λύσεις τις $x\equiv 3(\mathrm{mod}\ 7)$ και $x\equiv 4(\mathrm{mod}\ 7)$

b_2) Βρίσκουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x)=x^2-2\equiv 0\ (\mathrm{mod}\ 7^2) \qquad (2)$$

που αντιστοιχούν στις δύο λύσεις της (1).

i) Αφού $f'(3)=6\not\equiv 0\ (\mathrm{mod}\ 7)$ η (2) έχει μοναδική λύση την

$$x\equiv 3+7t\ (\mathrm{mod}\ 7^2)$$

που αντιστοιχεί στην λύση $x\equiv 3\ (\mathrm{mod}\ 7)$ της (1), όπου ο ακέραιος t επαληθεύει την γραμμική ισοτιμία

$$f'(3)\,t\equiv -\frac{f(3)}{7}\ (\mathrm{mod}\ 7)$$

δηλαδή, την $6t\equiv -1\ (\mathrm{mod}\ 7)$, που έχει μοναδική λύση την $t\equiv 1\ (\mathrm{mod}\ 7)$. Άρα η ζητούμενη λύση είναι η

$$x\equiv 3+7\equiv 10\ (\mathrm{mod}\ 7^2).$$

ii) Αφού $f'(4)=8\not\equiv 0\ (\mathrm{mod}\ 7)$, όμοια εργαζόμενοι, βρίσκουμε

ότι στην λύση $x \equiv 4 \pmod{7}$ αντιστοιχεί η λύση $x \equiv 39 \pmod{7^2}$.

β_3) Βρίσκουμε τις λύσεις της πολυωνυμικής ισοτιμίας

$$f(x) = x^2 - 2 \equiv 0 \pmod{7^3} \qquad (3)$$

που αντιστοιχούν στις δυο λύσεις $x \equiv 10 \pmod{7^2}$ και $x \equiv 39 \pmod{7^2}$ της (2).

Όμοια εργαζόμενοι βρίσκουμε ότι οι δυο λύσεις της (3) είναι οι

$x \equiv 108 \pmod{7^3}$ και $x \equiv -108 \equiv 235 \pmod{7^3}$. ■

8. Τετραγωνικά υπόλοιπα $\pmod{2^\beta}$.

Θα μελετήσουμε την διωνυμική ισοτιμία

$$x^2 \equiv a \pmod{2^\beta}$$

όπου a περιττός ακέραιος και β φυσικός ≥ 1.

Για $\beta = 1$ έχουμε την διωνυμική ισοτιμία

$$x^2 \equiv a \pmod{2}$$

που έχει μοναδική λύση την $x \equiv 1 \pmod{2}$

Για $\beta = 2$ έχουμε την διωνυμική ισοτιμία

$$x^2 \equiv a \pmod{4}$$

Αυτή έχει λύση αν και μόνο αν $a \equiv 1 \pmod{4}$ σύμφωνα με το θεώρημα 2.2 του Κεφ VII. Έχει τότε αυτή δυο λύσεις, τις $x \equiv 1 \pmod{4}$ και $x \equiv 3 \pmod{4}$. Πιο απλά, εδώ έχουμε τις ισοτιμίες $x^2 \equiv 1 \pmod{4}$ και $x^2 \equiv 3 \pmod{4}$. Οι λύσεις της πρώτης είναι $x \equiv 1, 3 \pmod{4}$, ενώ η δεύτερη δεν έχει λύσεις.

Για $\beta \geq 3$, έχουμε

Πρόταση 8.1

Έστω a περιττός ακέραιος και $\beta \geq 3$. Τότε η διωνυμική ισοτιμία

$$x^2 \equiv a \pmod{2^\beta}$$

έχει λύση αν και μόνο αν ο $a \equiv 1 \pmod{8}$. Στην περίπτωση αυτή, η διωνυμική ισοτιμία έχει 4 ακριβώς λύσεις.

Απόδειξη.

Το ζητούμενο προκύπτει αμέσως από το θεώρημα 3.2 του κεφ VII για $m=2$. ■

Αν η διωνυμική ισοτιμία $x^2 \equiv a \pmod{2^\beta}$, $\beta \geq 3$ έχει μια λύση $x_0 \pmod{2^\beta}$, τότε οι 4 λύσεις της είναι οι

$$x \equiv x_0,\ x_0+2^{\beta-1},\ -x_0,\ -x_0+2^{\beta-1} \pmod{2^\beta}.$$

Παράδειγμα 8.1

Θα επιλύσουμε την διωνυμική ισοτιμία

$$x^2 \equiv 17 \pmod{2^5}.$$

Αφού $17 \equiv 1 \pmod 8$, σύμφωνα με την πρόταση 8.1 ο 17 είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, 2^5)$. Αυτή έχει 4 λύσεις, τις οποίες και θα βρούμε.

1ος τρόπος. Παίρνουμε το αναγμένο σύστημα υπολοίπων $(\mathrm{mod}\, 2^5)$

$$\{1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31\}.$$

Υπάρχουν 4 αμέραιοι απ' αυτούς που ικανοποιούν την ισοτιμία $x^2 \equiv 17 \pmod{2^5}$. Δοκιμάζοντας βρίσκουμε τις λύσεις $x \equiv 7, 9, 23, 25 \pmod{2^5}$. Διαφορετικά, βρίσκουμε μια λύση για παράδειγμα την $x \equiv 7 \pmod{2^5}$ οπότε οι 4 λύσεις είναι οι $x \equiv 7 \pmod{2^5}$, $x \equiv -7 \equiv 25 \pmod{2^5}$, $x \equiv 7+2^4 = 23 \pmod{2^5}$ και $x \equiv -7+2^4 \equiv 9 \pmod{2^5}$.

2ος τρόπος

Είναι $\varphi(2^5) = 2^4 = 16$, και οι αμέραιοι

$$\pm 5, \pm 5^2, \pm 5^3, \pm 5^4, \pm 5^5, \pm 5^6, \pm 5^7, \pm 5^8$$

αποτελούν ένα αναγμένο σύστημα υπολοίπων $(\mathrm{mod}\, 2^5)$, σύμφωνα με την πρόταση 8.6 του κεφ IV. Έχουμε $(\mathrm{mod}\, 2^5)$ τις παρακάτω ισοτιμίες

$$\begin{array}{llll} 5 \equiv 5, & 5^5 \equiv 21, & -5 \equiv 27, & -5^5 \equiv 11 \\ 5^2 \equiv 25, & 5^6 \equiv 9, & -5^2 \equiv 7, & -5^6 \equiv 23 \\ 5^3 \equiv 29, & 5^7 \equiv 13, & -5^3 \equiv 3, & -5^7 \equiv 19 \\ 5^4 \equiv 17, & 5^8 \equiv 1, & -5^4 \equiv 15, & -5^8 \equiv 31 \end{array}$$

Από την απόδειξη του Θεωρήματος 3.2.2) του Κεφ VII, έχουμε $17 \equiv 5^k \pmod{2^5}$ όπου $k=4$. Η γραμμική ισοτιμία $2y \equiv k \pmod{2^3}$ δηλαδή η $2y \equiv 4 \pmod{2^3}$, έχει δυο λύσεις τις $y \equiv 2, 6 \pmod{2^3}$

Η διωνυμική ισοτιμία έχει 4 λύσεις $\pmod{2^5}$ τις

$x_1 \equiv 5^2 \equiv 25 \pmod{2^5}$, $x_2 \equiv -5^2 \equiv 7 \pmod{2^5}$,

$x_3 \equiv 5^6 \equiv 9 \pmod{2^5}$, $x_4 \equiv -5^6 \equiv 23 \pmod{2^5}$. ■

Παράδειγμα 8.2

Η διωνυμική ισοτιμία $x^2 \equiv a \pmod{2^4}$ έχει λύση αν και μόνο αν $a \equiv 1 \pmod 8$. Στην περίπτωση αυτή ο a μπορεί να έχει τις τιμές $a \equiv 1$ και $9 \pmod{2^4}$

Οι λύσεις της $x^2 \equiv 1 \pmod{2^4}$ είναι οι $x \equiv 1, 7, 9, 15 \pmod{2^4}$ ενώ οι λύσεις της $x^2 \equiv 9 \pmod{2^4}$ είναι οι $x \equiv 3, 5, 11, 13 \pmod{2^4}$.

9. Τετραγωνικά υπόλοιπα $(\mathrm{mod}\, n)$.

Θεώρημα 9.1

Έστω $n = 2^{b_0} p_1^{b_1} \dots p_r^{b_r}$ η πρωτογενής ανάλυση του φυσικού $n > 1$. Αν $a \in \mathbb{Z}$ με $(a, n) = 1$, τότε η διωνυμική ισοτιμία

$$x^2 \equiv a \pmod n \qquad (*)$$

έχει λύση αν και μόνο αν

(I) Όλες οι ισοτιμίες $x^2 \equiv a \pmod{p_i}$ $\quad i = 1, \dots, r$ έχουν λύση

(II) $a \equiv 1 \pmod 4$ αν $4 \mid n$ και $8 \nmid n$, και $a \equiv 1 \pmod 8$ αν $8 \mid n$.

Στην περίπτωση αυτή, αν $N(n)$ είναι το πλήθος των ανισοτίμων λύσεων της ισοτιμίας (*), τότε

$N(n) = 2^r$ για $b_0 = 0$ και $b_0 = 1$

$N(n) = 2^{r+1}$ για $b_0 = 2$

$N(n) = 2^{r+2}$ για $b_0 \geq 3$.

Απόδειξη.

Αν $(a,n) = 1$ τότε $(a, p_i) = 1$ για $i = 1, \ldots, r$ και $(a, 2) = 1$ αν $b_0 > 0$. Σύμφωνα με το θεώρημα 5.1 του κεφ. VI, η ισοτιμία (*) έχει λύση αν και μόνο αν οι ισοτιμίες

$$x^2 \equiv a \pmod{p_i^{b_i}} \quad i = 1, \ldots, r$$

$$x^2 \equiv a \pmod{2^{b_0}}$$

έχουν λύση, ή ισοδύναμα, σύμφωνα με την πρόταση 7.1, αν και μόνο αν οι ισοτιμίες

$$x^2 \equiv a \pmod{p_i} \quad i = 1, \ldots, r$$

$$x^2 \equiv a \pmod{2^{b_0}}$$

έχουν λύση. Για $b_0 = 0$ είναι φανερό. Για $b_0 = 1$ είναι και πάλι φανερό, αφού η ισοτιμία $x^2 \equiv a \pmod 2$ έχει μοναδική λύση την $x \equiv 1 \pmod 2$. Για $b_0 = 2$ η ισοτιμία $x^2 \equiv a \pmod 4$ έχει λύση αν και μόνο αν $a \equiv 1 \pmod 4$. Για $b_0 \geq 3$, σύμφωνα με την πρόταση 8.1 η $x^2 \equiv a \pmod{2^{b_0}}$ έχει λύση αν και μόνο αν $a \equiv 1 \pmod 8$.

Αν $n = p_1^{b_1} \cdots p_r^{b_r}$ τότε $N(n) = N(p_1^{b_1}) \cdots N(p_r^{b_r}) = \underbrace{2 \cdots 2}_{r\text{-φορές}} = 2^r$

Αν $n = 2 p_1^{b_1} \cdots p_r^{b_r}$ τότε $N(n) = N(2) N(p_1^{b_1}) \cdots N(p_r^{b_r}) = \underbrace{2 \cdots 2}_{(r+1)\text{-φορές}} = 2^{r+1}$

Αν $n = 2^{b_0} p_1^{b_1} \cdots p_r^{b_r}$ με $b_0 \geq 3$ τότε

$$N(n) = N(2^{b_0}) \cdot N(p_1^{b_1}) \cdots N(p_r^{b_r}) = 4 \cdot \underbrace{2 \cdots 2}_{r\text{-φορές}} = 2^{r+2}. \quad \square$$

Πόρισμα 9.1

Έστω $n = 2^{b_0} \cdot p_1^{b_1} \cdots p_r^{b_r}$ η πρωτογενής ανάλυση του φυσικού $n > 1$, όπου $b_0 \geq 0$, και $a \in \mathbb{Z}$ με $(a,n)=1$. Ο a είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, n)$ αν και μόνο αν

(I) Ο a είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, p_i)$, $i=1,\ldots,r$

(II) $a \equiv 1 \,(\mathrm{mod}\, 4)$ αν $4 \mid n$ και $8 \nmid n$. και

$a \equiv 1 \,(\mathrm{mod}\, 8)$ αν $8 \mid n$. ■

Παράδειγμα 9.1

Θα βρούμε το πλήθος των λύσεων της ισοτιμίας

$$x^2 \equiv 3 \,(\mathrm{mod}\, 11^2 \cdot 23^2).$$

Αυτή έχει λύση αν και μόνο αν οι ισοτιμίες

$$x^2 \equiv 3 \,(\mathrm{mod}\, 11)$$
$$x^2 \equiv 3 \,(\mathrm{mod}\, 23)$$

έχουν λύση. Είναι

$$\left(\frac{3}{11}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{3-1}{2}} \left(\frac{11}{3}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{3^2-1}{8}} = 1.$$

και

$$\left(\frac{3}{23}\right) = (-1)^{\frac{23-1}{2}\cdot\frac{3-1}{2}} \left(\frac{23}{3}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{-1}{3}\right) = -(-1)^{\frac{3-1}{2}} = 1.$$

Άρα ο 3 είναι τετραγωνικό υπόλοιπο $(\mathrm{mod}\, 11)$ και $(\mathrm{mod}\, 23)$. Αφού ο $11^2 \cdot 23^2$ περιέχει δυο περιττούς πρώτους στην αναλυσή του, το πλήθος των λύσεων της είναι $2^2 = 4$.

Παράδειγμα 9.2

Θα υπολογίσουμε το πλήθος των λύσεων της διωνυμικής ισοτιμίας

$$x^2 \equiv 17 \,(\mathrm{mod}\, 2^5 \cdot 13)$$

και στην συνέχεια θα βρούμε τις λύσεις της.

Ο $8 \mid 2^5 \cdot 13$ και $17 \equiv 1 \,(\mathrm{mod}\, 8)$, άρα η δοθείσα διωνυμική ισοτιμία έχει λύση αν και μόνο αν η διωνυμική ισοτιμία

$x^9 \equiv 17 \pmod{13}$ έχει λύση. Είναι

$$\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2^2}{13}\right) = \left(\frac{1}{13}\right) = 1.$$

άρα η διωνυμική ισοτιμία $x^2 \equiv 17 \pmod{13}$ έχει λύση

Η διωνυμική ισοτιμία $x^2 \equiv 17 \pmod{2^5 \cdot 13}$ λοιπόν έχει $2^{2+1} = 2^3 = 8$ λύσεις.

Η διωνυμική ισοτιμία $x^2 \equiv 17 \pmod{2^5 \cdot 13}$ έχει λύση αν και μόνο αν οι διωνυμικές ισοτιμίες

$$x^2 \equiv 17 \pmod{13}$$
$$x^2 \equiv 17 \pmod{2^5}$$

έχουν λύση. Η πρώτη απ'αυτές έχει δυο λύσεις τις $x \equiv 2 \pmod{13}$ και $x \equiv 11 \pmod{13}$ ενώ η δεύτερη έχει 4 λύσεις τις $x \equiv 7, 9, 23$ και $25 \pmod{2^5}$ που βρήκαμε στο παράδειγμα 8.1

Έχουμε έτσι, 8 συστήματα γραμμικών ισοτιμιών, τα

① $x \equiv 2 \pmod{13}$, $x \equiv 7 \pmod{2^5}$ ② $x \equiv 2 \pmod{13}$, $x \equiv 9 \pmod{2^5}$ ③ $x \equiv 2 \pmod{13}$, $x \equiv 23 \pmod{2^5}$

④ $x \equiv 2 \pmod{13}$, $x \equiv 25 \pmod{2^5}$ ⑤ $x \equiv 11 \pmod{13}$, $x \equiv 7 \pmod{2^5}$ ⑥ $x \equiv 11 \pmod{13}$, $x \equiv 9 \pmod{2^5}$

⑦ $x \equiv 11 \pmod{13}$, $x \equiv 23 \pmod{2^5}$ ⑧ $x \equiv 11 \pmod{13}$, $x \equiv 25 \pmod{2^5}$

που έχουν μοναδικές λύσεις, αντίστοιχα τις

$$x \equiv 327, 41, 119, 249, 167, 297, 374, 89 \pmod{2^5 \cdot 13}$$

Αυτές είναι οι ζητούμενες 8 λύσεις της δοθείσης διωνυμικής ισοτιμίας. ■

Στο θεώρημα 6.1 του Κεφ. IV αποδείξαμε ότι αν p είναι πρώτος, τότε $(p-1)! \equiv -1 \pmod{p}$. (Θεώρημα Wilson). Μια γενίκευση του θεωρήματος του Wilson θα δώσου-

με παρακάτω ως εφαρμογή του θεωρήματος 9.1.

Λήμμα 9.1

Έστω η φυσικός >2 και N το πλήθος των λύσεων της διωνυμικής ισοτιμίας

$$x^2 \equiv 1 \pmod{n}. \qquad (I)$$

Αν $\{a_1, \dots, a_{\varphi(n)}\}$ είναι ένα ανάγμενο σύστημα υπολοίπων $(\mathrm{mod}\, n)$ τότε

$$P = a_1 \cdots a_{\varphi(n)} \equiv (-1)^{N/2} \pmod{n}.$$

Απόδειξη.

Αν x_0 είναι μια λύση της (I) τότε ισχύει, $(x_0, n) = 1$ και ο $-x_0$ είναι μια λύση της και μάλιστα $-x_0 \not\equiv x_0 \pmod{n}$, γιατί αν $x_0 \equiv -x_0 \pmod{n}$ τότε $2x_0 \equiv 0 \pmod{n}$, δηλαδή $n \mid 2x_0$ και καθώς $(x_0, n) = 1$ θα είχαμε $n \mid 2$ πράγμα άτοπο αφού $n > 2$.

Το πλήθος N των λύσεων της (I) είναι άρτιος αριθμός σύμφωνα με το θεώρημα 9.1. Έστω

$$x_1, \dots, x_{N/2}, (-x_1), \dots, (-x_{N/2})$$

ένας αντιπρόσωπος από κάθε κλάση, που είναι λύση της (I). Τότε

$$x_1 \cdots x_{N/2} \cdot (-x_1) \cdots (-x_{N/2}) = (-1)^{N/2} x_1^2 \cdots x_{N/2}^2 \equiv (-1)^{N/2} \pmod{n}$$

Καθώς οι αυέραιοι $\{a_1, \dots, a_{\varphi(n)}\}$ είναι αντιπρόσωποι των πρωτογενών κλάσεων $(\mathrm{mod}\, n)$, για κάθε δείκτη i υπάρχει μοναδικός δείκτης $\sigma(i)$ ώστε $a_i \cdot a_{\sigma(i)} \equiv 1 \pmod{n}$

(Η γραμμική ισοτιμία $a_i x \equiv 1 \pmod{n}$ έχει μοναδική λύση).

Έχουμε $a_i = a_{\sigma(i)}$ αν και μόνο αν ο a_i είναι λύση της ισοτιμίας (I)

Ακριβώς N στοιχεία από τα $\{a_1, \dots, a_{\varphi(n)}\}$ έχουν αυτή την ιδιότητα. Ας υποθέσουμε ότι αυτά είναι τα $a_1, \dots, a_N$ και ότι τα υπόλοιπα είναι τα

$$a_{N+1}, a_{\sigma(N+1)}, \dots, a_K, a_{\sigma(K)}$$

όπου $K = \frac{\varphi(n)-N}{2}$.

Έχουμε λοιπόν, $a_1 \cdots a_N = x_1 \cdots x_{N/2}(-x_1)\cdots(-x_{N/2}) \equiv (-1)^{N/2} \pmod n$ και

$$a_{N+1}\cdot a_{\sigma(N+1)} \equiv 1 \pmod n, \ldots, a_K \cdot a_{\sigma(K)} \equiv 1 \pmod n$$

Τελικά, έχουμε

$$P = a_1 \cdots a_{\varphi(n)} = a_1 \cdots a_N \, a_{N+1} \, a_{\sigma(N+1)} \cdots a_K \, a_{\sigma(K)} \equiv (-1)^{N/2} \pmod n. \blacksquare$$

Θεώρημα 9.2 (Γενικευμένο θεώρημα του Wilson)

Έστω n ένας φυσικός >2 και $\{a_1, \ldots, a_{\varphi(n)}\}$ ένα αναγμένο σύστημα υπολοίπων $(\mathrm{mod}\, n)$. Τότε

$$a_1 \cdots a_{\varphi(n)} = \begin{cases} (-1) \pmod n & \text{αν } n = 4, p^\beta, 2p^\beta, \text{ όπου } p \text{ πρώτος} > 2 \text{ και } \beta \geq 1 \\ 1 \pmod n & \text{για κάθε άλλο } n. \end{cases}$$

Απόδειξη

Είναι $a_1 \cdots a_{\varphi(n)} \equiv (-1)^{N/2} \pmod n$ σύμφωνα με το λήμμα 9.1.

Από το θεώρημα 9.1 έχουμε τις τιμές για το N. Έστω $n = 2^{\beta_0} p_1^{\beta_1} \cdots p_r^{\beta_r}$ όπου $p_1, \ldots, p_r$ περιττοί πρώτοι, $\beta_0 \geq 0$ και $\beta_i \geq 1$, $i = 1, \ldots, r$.

Έχουμε τις εξής περιπτώσεις.

(1) Αν $\beta_0 = 0$ ή 1 τότε $N = 2^r$ και $N/2 = 2^{r-1}$. Άρα ο $N/2$ είναι περιττός μόνο για $r = 1$.

(2) Αν $\beta_0 = 2$ τότε $N = 2^{r+1}$ και $N/2 = 2^r$. Άρα ο $N/2$ είναι περιττός μόνο για $r = 0$.

(3) Αν $\beta_0 \geq 3$ τότε $N = 2^{r+2}$ και $N/2 = 2^{r+1}$. Άρα ο $N/2$ είναι πάντα άρτιος

Άρα αν $n = 4, p^\beta, 2p^\beta$, όπου p πρώτος > 2 και $\beta \geq 1$ έχουμε

$$a_1 \cdots a_{\varphi(n)} \equiv -1 \pmod n.$$

Σε κάθε άλλη περίπτωση, έχουμε

$$a_1 \cdots a_{\varphi(n)} \equiv 1 \pmod n. \blacksquare$$

ΒΙΒΛΙΟΓΡΑΦΙΑ

T. APOSTOL. Εισαγωγή στην αναλυτική θεωρία αριθμών, μετάφραση Α. Ζαχαρίου, Gutenberg, Αθήνα 1986.

E.P. ARMENDARIZ Elementary Number Theory, Macmillan Publishing Co. Inc New York 1980.

D.M. BURTON Elementary Number Theory, Allyn and Bacon Inc. Boston Mass 1980.

I.S. CHAHAL. Topics in Number Theory, Plenum Press, New York 1988.

G.H HARDY - E.M. WRIGHT. A introduction to the theory of numbers, πέμπτη έκδοση, Oxford Univ. Press london 1979.

J. HUNTER. Αριθμοθεωρία, μετάφραση Ν. Κριτικού, δεύτερη έκδοση, Αθήνα 1974

A HURWITZ. Μαθήματα Αριθμοθεωρίας, (επεξεργασμένα από τον Ν. Κριτικό) Έκδοση Γ.Α. Πνευματικού, Αθήνα 1981.

I. NIVEN - H.S ZUCKERMAN. An introduction to the theory of numbers, έβδομη έκδοση, Wiley Eastern Limited 1993

J. ROBERTS. Elementary Number Theory, A problem oriented approach. M.I.T press, Cambridge, Mass, 1977.

W. SIERPINSKI. Elementary Theory of Numbers, Panstwowe Wydawnictwo Naukowe, Warsaw, 1964

H STARK. An Introduction to Number Theory, Markham Publishing Company, Chicago 1970.

Γ. ΚΑΖΑΝΤΖΙΔΗ 'Θεωρία Αριθμών, Ιωάννινα 1976.

Τυπώθηκε στο Πανεπιστημιακό Τυπογραφείο
με δαπάνη του Πανεπιστημίου Ιωαννίνων.

ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ Τυπογραφείο

Διανέμεται Δωρεάν στους φοιτητές.

ΕΚΤΥΠΩΣΗ
Τυπογραφείο
ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΙΩΑΝΝΙΝΩΝ