ΘΠ08 Θεωρία Αριθμών

Σημειώσεις 2023-2024

Κωνσταντίνος Χούσος

Περίληψη

Αντικείμενο της θεωρίας αριθμών είναι η μελέτη των ακέραιων αριθμών.

1 Ιστορική αναδρομή

- Πυθαγόρας (600 π.Χ.)
  - Πυθαγόρεια τριάδα
  - Πρωτογενής Πυθαγόρεια τριάδα
  - Συνδεσμικό σημείο
  - Συνδεσμικό πολύγωνο
  - Πολύγωνοι αριθμοί
  - $\sqrt{2} \notin \mathbb{Q}$.
- Ευκλείδης (300 π.Χ.)
  - "Στοιχεία" του Ευκλείδη
  - Άπειροι πρώτοι αριθμοί
  - Αλγόριθμος για το Μ.Κ.Δ. δύο αριθμών
  - Ευκλείδιο θεώρημα
- Διόφαντος (250 μ.Χ.)
  - "Τα Αριθμητικά"
  - Διοφαντική Ανάλυση
- 16ο – 18ο αιώνα (κυρίως από τους: Fermat, Euler, Lagrange, Gauss και Dirichlet)

2 Διαιρετότητα

Ορισμός 2.1

Εστω οι ακέραιοι αριθμοί n, d. Θα λέμε ότι ο d διαιρεί τον n, και θα γράφουμε $d \mid n$, αν υπάρχει ακέραιος αριθμός k τέτοιος ώστε

$$n = dk.$$

Αν ο d δεν διαιρεί τον n, γράφουμε $d \nmid n$.

2.1 Ιδιότητες

Έστω $n, m, c, d \in \mathbb{Z}$.

1. $n \mid n$
2. $n \mid 0$

3. $1 \mid n$
4. Αν $d \mid n$ και $n \mid m$, τότε $d \mid m$.
5. Αν $d \mid n$ και $n \neq 0$, τότε $|d| \leq |n|$.
6. Αν $d \mid n$ και $n \mid d$, τότε $d = \pm n$.
7. Αν $cd \mid cn$ και $c \neq 0$, τότε $d \mid n$.
8. Αν $d \mid n$ και $d \mid m$, τότε $d \mid (an + bm)$.
9. Αν $c \mid n$ και $d \mid m$, τότε $cd \mid nm$.

2.2 Αλγόριθμος της διαίρεσης

Θεώρημα 2.1: Αλγόριθμος της διαίρεσης

Έστω a, b δύο ακέραιοι αριθμοί με $b \neq 0$. Τότε, υπάρχουν δύο μοναδικοί ακέραιοι q, r τέτοιοι ωστε

$$a = bq + r,\ \ 0 \leq r < |b|.$$

Ισχύει ότι $r = 0 \iff b \mid a$.
Ο ακέραιος αριθμός q λέγεται *πηλίκο* και ο r *υπόλοιπο* της διαίρεσης a δια b.

2.3 Μέγιστος Κοινός Διαιρέτης

Έστω οι ακέραιοι αριθμοί $a_1, a_2, \ldots, a_n$ που δεν είναι όλοι μηδέν. Κάθε ακέραιος που διαιρεί όλους τους ακέραιους $a_1, a_2, \ldots, a_n$ λέγεται *κοινός διαιρέτης* των $a_1, a_2, \ldots, a_n$. Ο μέγιστος ακέραιος που διαιρεί όλους τους $a_1, a_2, \ldots, a_n$ λέγεται **μέγιστος κοινός διαιρέτης** (Μ.Κ.Δ.) και συμβολίζεται με $(a_1, a_2, \ldots, a_n)$.

Ορισμός 2.2: Μέγιστος Κοινός Διαιρέτης (ΜΚΔ)

Ο φυσικός αριθμός d θα λέγεται Μ.Κ.Δ. των ακεραίων a_1 και a_2 , με $a_2 \neq 0$, αν και μόνο αν ισχύει:

$$d \mid a_1 \quad \text{και} \quad d \mid a_2$$

$$d_1 \mid a_1, d_1 \mid a_2 (d_1 \in \mathbb{Z}) \implies d_1 \mid d$$

Θεώρημα 2.2

Έστω $a, b \in \mathbb{Z}$ με $b \neq 0$. Τότε υπάρχει ο Μ.Κ.Δ. των a, b και ορίζεται μονοσήμαντα.

2.3.1 Μέθοδοι έυρεσης του ΜΚΔ

2.3.1.1 Αλγόριθμος του Ευκλείδη Η διαδοχική εφαρμογή του Αλγορίθμου της Διαίρεσης αποτελεί τον Αλγόριθμο του Ευκλείδη.

Στην ουσία, σε κάθε αναδρομή βάζουμε στο a το προηγούμενο b και στην θέση του διαιρέτη το πηλίκο r.

Σημείωση

Από τον αλγόριθμο του Ευκλείδη προκύπτει ότι: Αν $d = (a, b)$, τότε υπάρχουν ακέραιοι αριθμοί x, y τέτοιοι ώστε $d = (a, b) = ax + by$.

2.3.1.2 Ανθυφαίρεση Εναλλακτική του Αλγορίθμου του Ευκλείδη.

Ορισμός 2.3

Έστω δύο ακέραιοι αριθμοί a, b με $a > b$. Τότε,

$$(a, b) \sim (b, a - b) \sim (b, a - 2b) \sim \ldots$$

Η διαδικασία σταματάει όταν οι αριθμοί γίνονται ίσοι.

Αφαιρείς τον μικρότερο από τον μεγαλύτερο, και συνεχίζεις μέχρι να προκύψει ο ίδιος αριθμός.

Άρα είτε το κάνεις βήμα-βήμα, είτε αφαιρέσεις κατευθείαν το b όσες φορές χωράει, το ίδιο είναι. Βέβαια αυτό στην ουσία το κάνει ίδιο με τον Αλγόριθμο του Ευκλείδη.

Δεν έχει σημασία η σειρά. Δηλαδή, όταν το b γίνει μεγαλύτερο του a, τότε στην επόμενη επανάληψη απλά τους αλλάζεις σειρά, κι άρα αφαιρείς το $b - a$.

2.3.2 Ιδιότητες

Έστω $a, b \in \mathbb{Z}$ με έναν τουλάχιστον να είναι διάφορος του 0.

1. $(a, b) = (b, a)$
2. $(am, bm) = |m|(a, b)$
3. $(a, 1) = 1$
4. $(a, 0) = |a|, a \neq 0$

2.3.3 Εύρεση Μ.Κ.Δ. 3 ή περισσότερων αριθμών

Θεώρημα 2.3

Έστω οι ακέραιοι αριθμοί $a_1, a_2, \ldots, a_n$ με $n \geq 3$. Ισχύει ότι:

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

2.4 Διαιρετότητα και πρώτοι αριθμοί

Ορισμός 2.4

Εστω $a, b \in \mathbb{Z}$. Αν ο Μ.Κ.Δ. των a, b ισούται με 1, δηλαδή $(a, b) = 1$, τότε οι αριθμοί λέγονται *πρώτοι μεταξύ τους*.

Θεώρημα 2.4

Οι ακέραιοι αριθμοί a, b είναι πρώτοι μεταξύ τους αν και μόνο αν υπάρχουν ακέραιοι αριθμοί x, y τέτοιοι ώστε:

$$ax + by = 1.$$

Πρόταση 2.1

Έστω $a, b \in \mathbb{Z}$ με $(a, b) = d$. Τότε

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Θεώρημα 2.5

Έστω $a_1, a_2, \dots, a_n \in \mathbb{Z}$ με $(a_1, a_2, \dots, a_n) = d$. Τότε,

$$\left(\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d}\right) = 1.$$

Πρόταση 2.2

Έστω $a, b, c \in \mathbb{Z}$ με $(a, b) = 1$ και $c \mid a$. Τότε,

$$(b, c) = 1.$$

Πρόταση 2.3

Έστω $a, b, c \in \mathbb{Z}$ με $(a, b) = 1$ και $a \mid bc$. Τότε,

$$a \mid c.$$

Πρόταση 2.4

Έστω $a, b, c \in \mathbb{Z}$ με $(a, b) = 1$, $a \mid c$ και $b \mid c$. Τότε,

$$a \cdot b \mid c.$$

Θεώρημα 2.6

Έστω $a_1, a_2, \dots, a_n \in \mathbb{Z}$ με $n \geq 2$. Ισχύει ότι: $(a_i, a) = 1$, για κάθε $i = 1, 2, \dots, n$ *αν και μόνο αν* $(a_1 a_2 \dots a_n, a) = 1$.

Θεώρημα 2.7

Έστω p πρώτος αριθμός με $p \mid a_1 a_2 \dots a_n$ και $n \geq 2$. Τότε, ο p διαιρεί τουλάχιστον έναν από τους $a_i, i = 1, 2, \dots, n$.

3 Πρώτοι αριθμοί

Ορισμός 3.1: Πρώτος αριθμός

Ένας φυσικός αριθμός $n > 1$ λέγεται πρώτος αριθμός αν

$$a \nmid n, \forall a \in \mathbb{N},$$

με $2 \leq a \leq n-1$.

- Κάθε φυσικός αριθμός $n > 1$ είναι είτε πρώτος είτε γινόμενο πρώτων αριθμών.
- Υπάρχουν άπειροι πρώτοι αριθμοί (Ευκλείδης).

Ορισμός 3.2: Δίδυμοι πρώτοι αριθμοί

Οι διαδοχικοί πρώτοι αριθμοί, δηλαδή τα ζεύγη των πρώτων αριθμών που διαφέρουν κατά 2, λέγονται δίδυμοι πρώτοι αριθμοί.

- Αν ο n είναι φυσικός αριθμός, τότε υπάρχουν n διαδοχικοί φυσικοί αριθμοί που είναι σύνθετοι.
- Αν ο $n > 2$ είναι φυσικός αριθμός, τότε μεταξύ του n και του $n!$ υπάρχει τουλάχιστον ένας πρώτος αριθμός.

Θεώρημα 3.1: Εικασία του Goldbach

Κάθε άρτιος αριθμός > 2 είναι άθροισμα δύο πρώτων αριθμών.

Θεώρημα 3.2

Έστω $n \in \mathbb{N}$ ένας σύνθετος αριθμός. Τότε, υπάρχει διαιρέτης d του n με

$$1 < d \leq \left[\sqrt{n}\right].$$

3.1 Κόσκινο του Ερατοσθένη

Με το κόσκινο του Ερατοσθένη μπορούμε να βρούμε όλους τους πρώτους αριθμούς που δεν υπερβαίνουν έναν φυσικό αριθμό n. Η διαδικασία που ακολουθούμε είναι η εξής:

1. Γράφουμε όλους τους φυσικούς αριθμούς $2, 3, \ldots, n$.
2. Αφήνουμε το 2 και διαγράφουμε όλα τα πολλαπλάσια του 2.
3. Ο επόμενος αριθμός του 2 που δεν έχει διαγραφεί είναι πρώτος, εδώ το 3.
4. Αφήνουμε το 3 και διαγράφουμε όλα τα πολλαπλάσια του 3.
5. Ο επόμενος αριθμός του 3 που δεν έχει διαγραφεί είναι πρώτος, εδώ το 5. Η διαδικασία συνεχίζεται μέχρι ο επόμενος πρώτος αριθμός που δεν διαγράφεται είναι μικρότερος ή ίσος του $\left[\sqrt{n}\right]$.

3.2 Κριτήρια για πρώτους αριθμούς

1. Έστω ο φυσικός αριθμός $n > 3$. Τα ακόλουθα είναι ισοδύναμα.
   1. Ο n είναι πρώτος αριθμός.
   2. Για κάθε πρώτο αριθμό $p \leq \left[\sqrt{n}\right]$ ισχύει ότι $p \nmid n$, δηλαδή $(p, n) = 1$.
   3. Για κάθε φυσικό αριθμό $i \leq \left[\sqrt{n}\right]$ ισχύει $(i, n) = 1$.

2. Έστω ο φυσικός αριθμός $n > 3$ και $m = \left[\sqrt{n}\right]$. Τα ακόλουθα είναι ισοδύναμα.
    1. Ο n είναι πρώτος αριθμός.
    2. Ισχύει ότι $4\sum_{1\leq i<j\leq m}\left[\frac{ni}{j}\right] = (m-1)m(n-1)$.
3. **(Κριτήριο Wilson)** Έστω ο φυσικός αριθμός $n > 1$. Τα ακόλουθα είναι ισοδύναμα.
    1. Ο n είναι πρώτος αριθμός.
    2. Ισχύει ότι $n \mid (n-1)! + 1$.

3.3 Κριτήρια για σύνθετους αριθμούς

1. Έστω ο φυσικός αριθμός $n > 3$. Τα ακόλουθα είναι ισοδύναμα.
    1. Ο n είναι σύνθετος αριθμός.
    2. Υπάρχει πρώτος αριθμός p τέτοιος ώστε $p \leq \left[\sqrt{n}\right]$ και $p \mid n$.
    3. Υπάρχει φυσικός αριθμός j τέτοιος ώστε $j \leq \left[\sqrt{n}\right]$ και $j \mid n$.
2. Έστω ο φυσικός αριθμός $n > 3$ και $m = \left[\sqrt{n}\right]$. Τα ακόλουθα είναι ισοδύναμα.
    1. Ο n είναι σύνθετος αριθμός.
    2. Ισχύει ότι $4\sum_{1\leq i<j\leq m}\left[\frac{ni}{j}\right] > (m-1)m(n-1)$.

4 Θεμελιώδες Θεώρημα της Αριθμητικής

Θεώρημα 4.1: Θεμελιώδες Θεώρημα της Αριθμητικής

Έστω $n > 1$ ένας φυσικός αριθμός. Ο n γράφεται σαν γινόμενο πρώτων αριθμών κατά μοναδικό τρόπο, όχι κατ΄ ανάγκη διαφορετικοί μεταξύ τους.

4.1 Ανάλυση (Παραγοντοποίηση) σε γινόμενο δυνάμεων πρώτων παραγόντων

Έστω $n > 1$ ένας φυσικός αριθμός και $p_1, p_2, \ldots, p_k$ οι πρώτοι παράγοντες του n. Ο n γράφεται στη μορφή:

$$n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k},$$

όπου $a_i \in \mathbb{N}$.

Θεώρημα 4.2: Πλήθος διαιρετών

Έστω $n > 1$ ένας φυσικός αριθμός με ανάλυση σε γινόμενο δυνάμεων πρώτων παραγόντων

$$n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}.$$

Ο αριθμός των διαιρετών του n είναι

$$d(n) = (a_1+1)(a_2+1)\ldots(a_k+1).$$

Θεώρημα 4.3: Άθροισμα διαιρετών

Έστω $n > 1$ ένας φυσικός αριθμός με ανάλυση σε γινόμενο δυνάμεων πρώτων παραγόντων

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}.$$

Το άθροισμα των διαιρετών του n είναι

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \dots \frac{p_k^{a_k+1} - 1}{p_k - 1}.$$

5 Συναρτήσεις

5.1 Συνάρτηση ακέραιου μέρους

Ορισμός 5.1: Συνάρτηση ακέραιου μέρους

Έστω $x \in \mathbb{R}$. Η συνάρτηση ακέραιου μέρους x συμβολίζεται με $[x]$ και ορίζεται ως $[x]$ = ο μεγαλύτερος ακέραιος που είναι $\leq x$.

1. Για κάθε $x \in \mathbb{R}$ ισχύει ότι $x - 1 < [x] \leq x < [x] + 1$.
2. $[x] = x \iff x \in \mathbb{Z}$.
3. Ο φυσικός αριθμός $n > 2$ λέγεται πρώτος αν ισχύει

$$\left[\frac{n}{d}\right] \neq \frac{n}{d}, \quad \forall d = 2, 3, \dots, n - 1.$$

5.2 Συνάρτηση Möbius

Ορισμός 5.2: Συνάρτηση Möbius

Η συνάρτηση Möbius $\mu(n)$ ορίζεται ως

$$\mu(1) = 1.$$

Αν $n > 1$ και η ανάλυσή του σε γινόμενο πρώτων παραγόντων είναι

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}.$$

τότε

$$\mu(n) = \begin{cases} (-1)^k, & a_1 = a_2 = \cdots = a_k = 1 \\ 0, & \exists a_i > 1 (i = 1, 2, \dots, k) \end{cases}$$

Θεώρημα 5.1

Έστω $n \in N$. Ισχύει ότι

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}$$

5.3 Συνάρτηση Euler

Ορισμός 5.3: Συνάρτηση Euler

Η συνάρτηση Euler $\phi(n)$ ορίζεται ως το πλήθος των θετικών ακεραίων που είναι $\leq n$ και είναι πρώτοι προς τον n.

Η συνάρτηση Euler μπορεί να εκφραστεί με χρήση της συνάρτησης ακέραιου μέρους ως εξής:

$$\varphi(n) = \sum_{1 \leq k \leq n} \left[\frac{1}{(n,k)} \right].$$

Θεώρημα 5.2

Αν $n \in \mathbb{N}$, τότε ισχύει

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Θεώρημα 5.3

Αν $n \in \mathbb{N}$, τότε ισχύει

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

όπου ο p είναι πρώτος αριθμός.

Προσοχή

Η συνάρτηση Euler είναι πολλαπλασιαστική, αλλά όχι πλήρως πολλαπλασιαστική.

5.4 Αριθμητική συνάρτηση

Ορισμός 5.4: Αριθμητική συνάρτηση

Μια συνάρτηση ορισμένη στο σύνολο των θετικών ακεραίων και με τιμές πραγματικές ή μιγαδικές λέγεται αριθμητική συνάρτηση.

5.5 Πολλαπλασιαστική συνάρτηση

Ορισμός 5.5: Πολλαπλασιαστική συνάρτηση

Μία αριθμητική συνάρτηση f λέγεται πολλαπλασιαστική, αν ισχύουν τα ακόλουθα:

1. Η f δεν είναι η μηδενική συνάρτηση.
2. Αν $m, n \in \mathbb{N}$ με $(m, n) = 1$, τότε ισχύει

$$f(mn) = f(m)f(n).$$

Μία πολλαπλασιαστική συνάρτηση λέγεται πλήρως πολλαπλασιαστική αν ισχύει $f(mn) = f(m)f(n)$ για κάθε m, n.

5.6 Περιοδική συνάρτηση

Ορισμός 5.6: Περιοδική συνάρτηση

Έστω $k \in \mathbb{N}$ και f μία αριθμητική συνάρτηση. Η f λέγεται περιοδική με περίοδο k, αν ισχύει:

$$f(k+n) = f(n),$$

για κάθε $n \in \mathbb{Z}$.

6 Ισοδυναμίες (congruence)

Ορισμός 6.1

Έστω $m \in \mathbb{Z}$ και $a, b \in \mathbb{Z}$. Ορίζουμε στο σύνολο των ακέραιων αριθμών τη σχέση

$$a \equiv b \pmod{m} \iff m \mid (a-b).$$

Θα λέμε ότι ο a είναι ισοδύναμος με τον b modulo m. Ο φυσικός αριθμός m ονομάζεται *μέτρο* της ισοδυναμίας.

Αν $m \nmid (a-b)$, τότε γράφουμε $a \not\equiv b \pmod{m}$ και λέμε ότι ο a είναι *μη-ισοδύναμος* με τον b modulo m.

Εναλλακτικοί ορισμοί:

1. Οι αριθμοί a και b έχουν το ίδιο *υπόλοιπο* όταν διαιρούνται με το m.
2. $a = k \cdot m + b$

6.1 Ιδιότητες

1. **Αυτοπαθής** $a \equiv a \pmod{m}$ $\forall a \in \mathbb{Z}$.
2. **Συμμετρική** $a \equiv b \pmod{m} \implies b \equiv a$
3. **Μεταβατική** $a \equiv b \pmod{m}, b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$.

Θεώρημα 6.1

Έστω $a, b, c \in \mathbb{Z}$ και $m \in \mathbb{N}$. Αν $a \equiv b \pmod{m}$, τότε ισχύουν τα ακόλουθα:

1. $a \pm c \equiv b \pm c \pmod{m}$,
2. $ac \equiv bc \pmod{m}$.

Θεώρημα 6.2

Έστω $a, b, c, e \in \mathbb{Z}$ και $m \in \mathbb{N}$. Αν $a \equiv b \pmod{m}, c \equiv e \pmod{m}$, τότε ισχύουν τα ακόλουθα:

1. $ax + cy \equiv (bx + ey) \pmod{m}$, για κάθε $x, y \in \mathbb{Z}$
2. $ac \equiv be \pmod{m}$
3. $a^n \equiv b^n \pmod{m}$, για κάθε $n \in \mathbb{N}$
4. $f(a) \equiv f(b) \pmod{m}$, για κάθε πολυώνυμο f με ακέραιους συντελεστές.

Θεώρημα 6.3

Έστω $a, b, x \in \mathbb{Z}$ και $m \in \mathbb{N}$. Αν $d = (m, x)$ και $ax \equiv bx \pmod{m}$, τότε ισχύει:

$$a \equiv b \pmod{\frac{m}{d}}$$

Από το παραπάνω θεώρημα, προκύπτει το εξής πόρισμα: Έστω $a, b, x \in \mathbb{Z}$ και $m \in \mathbb{N}$. Αν $ax \equiv bx \pmod{m}$ και $(m, x) = 1$, τότε ισχύει:

$$a \equiv b \pmod{m}.$$

Θεώρημα 6.4

Έστω $a, b \in \mathbb{Z}$ και $m \in \mathbb{N}$. Ισχύει

$$a \equiv b \pmod{m}$$

αν και μόνο αν οι a, b διαιρούμενοι με τον m δίνουν το ίδιο υπόλοιπο.

6.2 Πλήρη - ανηγμένα συστήματα υπολοίπων

Ορισμός 6.2: Τάξη υπολοίπων

Έστω $m \in \mathbb{N}$. Το σύνολο των ακεραίων αριθμών x με την ιδιότητα

$$x \equiv a \pmod{m}$$

ονομάζεται *τάξη υπολοίπων* του $a \pmod{m}$ και συμβολίζεται με $\hat{a}$.

- $\hat{a} \equiv \hat{b} \iff a \equiv b \pmod{m}$
- Αν θεωρήσουμε $m = 2$, τότε

$$\hat{a} = \hat{0} \implies \text{άρτιοι}$$
$$\hat{b} = \hat{1} \implies \text{περιττοί}$$

- Δύο ακέραιοι αριθμοί x_1, x_2 ανήκουν στην ίδια τάξη υπολοίπων αν και μόνο αν $x_1 \equiv x_2 \pmod{m}$.

Ορισμός 6.3: Πλήρες σύστημα υπολοίπων

Ένα σύνολο από m αντιπροσώπους, έναν από καθεμιά από τις τάξεις υπολοίπων

$$\hat{0}, \hat{1}, \dots, \widehat{m-1},$$

ονομάζεται πλήρες σύστημα υπολοίπων $\mod m$.

Θεώρημα 6.5

Έστω $m \in \mathbb{N}$ και $\ell \in \mathbb{Z}$ με $(\ell, m) = 1$. Αν το σύνολο $\{a_1, a_2, \dots, a_m\}$ είναι πλήρες σύστημα υπολοίπων $\mod m$, τότε και το σύνολο

$$\{\ell a_1 + b, \ell a_2 + b, \dots, \ell a_m + b\}$$

είναι πλήρες σύστημα υπολοίπων $\mod m$.

Ορισμός 6.4: Ανηγμένο σύστημα υπολοίπων

Ανηγμένο σύστημα υπολοίπων $\mod m$ είναι κάθε σύνολο που αποτελείται από $\phi(m)$ ακεραίους, μη-ισοδύναμους modulo m που ο καθένας τους είναι πρώτος προς τον m.

Θεώρημα 6.6

Έστω $m \in \mathbb{N}$ και $\ell \in \mathbb{Z}$ με $(\ell, m) = 1$. Αν το σύνολο $\{a_1, a_2, \dots, a_{\phi(m)}\}$ είναι ανηγμένο σύστημα υπολοίπων $\mod m$, τότε και το σύνολο

$$\{\ell a_1, \ell a_2, \dots, \ell a_{\phi(m)}\}$$

είναι ανηγμένο σύστημα υπολοίπων $\mod m$.

6.3 Βασικά Θεωρήματα στις Ισοδυναμίες

Θεώρημα 6.7: Euler-Fermat

Έστω $a \in \mathbb{Z}$ και $m \in \mathbb{N}$ με $(a, m) = 1$. Ισχύει οτι

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Θεώρημα 6.8: Μικρό θεώρημα του Fermat

Έστω $a \in \mathbb{Z}$ και p ένας πρώτος αριθμός με $p \nmid a$. Ισχύει ότι

$$a^{p-1} \equiv 1 \pmod{p}.$$

Θεώρημα 6.9

Έστω $a \in \mathbb{Z}$ και p ένας πρώτος αριθμός. Ισχύει οτι

$$a^p \equiv a \pmod{p}.$$

Θεώρημα 6.10: Wilson

Αν ο p είναι πρώτος αριθμός, τότε

$$(p-1)! \equiv -1 \pmod{p}.$$

7 Γραμμικές ισοδυναμίες

Ορισμός 7.1: Γραμμική ισοδυναμία

Έστω $m \in \mathbb{N}$ και $a, b \in \mathbb{Z}$. Κάθε ισοδυναμία της μορφής

$$ax \equiv b \pmod{m}$$

λέγεται *γραμμική ισοδυναμία* $\pmod{m}$ ή *ισοδυναμία πρώτου βαθμού*.

1. Ο ακέραιος αριθμός y θα ονομάζεται λύση της γραμμικής ισοδυναμίας αν ισχύει:
$$ay \equiv b \pmod{m}$$
2. Αν y, z είναι λύσεις της γραμμικής ισοδυναμίας, θα θεωρούνται διαφορετικές αν ισχύει:
$$y \not\equiv z \pmod{m}.$$
3. Το πλήθος των λύσεων της γραμμικής ισοδυναμίας θα είναι το πλήθος των μη-ισοδύναμων λύσεών της.
4. Κάθε γραμμική ισοδυναμία $\mod m$ έχει το πολύ m λύσεις. Οι λύσεις αυτές βρίσκονται αν δώσουμε στο x τις τιμές $0, 1, 2, \ldots, m-1$.

7.1 Επίλυση γραμμικών ισοδυναμιών με έναν άγνωστο

Θεώρημα 7.1

Έστω $m \in \mathbb{N}$ και $a \in \mathbb{Z}$ με $(a, m) = d$. Η γραμμική ισοδυναμία

$$ax \equiv b \pmod{m}$$

έχει λύση αν και μόνο αν $d \mid b$.

Θεώρημα 7.2

Έστω $m \in \mathbb{N}$ και $a \in \mathbb{Z}$ με $(a, m) = 1$. Η γραμμική ισοδυναμία

$$ax \equiv b \pmod{m}$$

έχει μοναδική λύση η οποία δίνεται από τον τύπο

$$x \equiv ba^{\phi(m)-1} \pmod{m}.$$

Ένας άλλος τρόπος για τον προσδιορισμό της λύσης της γραμμικής ισοδυναμίας $ax \equiv b \pmod{m}$ με $(a, m) = 1$ βασίζεται στον αλγόριθμο του Ευκλείδη.

Θεώρημα 7.3

Έστω $m \in \mathbb{N}$ και $a \in \mathbb{Z}$ με $(a, m) = 1$. Υπάρχουν αριθμοί $\lambda, \mu \in \mathbb{Z}$ ώστε:

$$1 = \lambda a + \mu m.$$

Η μοναδική λύση της γραμμικής ισοδυναμίας

$$ax \equiv b \pmod{m}$$

είναι η

$$x = b\lambda \pmod{m}.$$

Θεώρημα 7.4

Έστω $m \in \mathbb{N}$ και $a, b \in \mathbb{Z}$ με $(a, m) = d$ και $d \mid b$. Η γραμμική ισοδυναμία

$$ax \equiv b \pmod{m}$$

έχει d λύσεις $\mod m$. Οι λύσεις αυτές είναι οι ακόλουθες:

$$x_0,\ x_0 + \frac{m}{d}, \dots,\ x_0 + (d-1)\frac{m}{d} \mod m,$$

όπου x_0 η μοναδική λύση $\mod \frac{m}{d}$ της γραμμικής ισοδυναμίας

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

7.2 Επίλυση γραμμικών ισοδυναμιών με περισσότερους από έναν αγνώστους

Έστω η γραμμική ισοδυναμία

$$a_1x_1 + a_2x_2 + \dots + a_kx_k \equiv b \pmod{m}, \tag{1}$$

όπου $k > 1, a_1, a_2, \dots, a_k, b \in \mathbb{Z}$ (με έναν τουλάχιστον από τους a_i να είναι διάφορος του μηδενός) και $m \in \mathbb{N}$.

Θεώρημα 7.5: Κριτήριο επιλυσιμότητας

Η γραμμική ισοδυναμία εξ. 1 έχει λύση αν και μόνο αν

$$(a_1, a_2, \dots, a_k, m) = d \mid b.$$

Θεώρημα 7.6: Πλήθος λύσεων

Έστω ότι η γραμμική ισοδυναμία εξ. 1 είναι επιλύσιμη. Το πλήθος των λύσεων της είναι

$$N_k = dm^{k-1},$$

όπου $d = (a_1, a_2, \dots, a_k, m)$.

Θεώρημα 7.7

Έστω ότι η γραμμική ισοδυναμία εξ. 1 είναι επιλύσιμη. Το σύνολο λύσεων του αγνώστου x_k συμπίπτει με τους $d\frac{m}{d_1}$ αριθμούς

$$y_{ij} = y_i + jd_1, \quad 1 \le i \le d,\ 1 \le j \le \frac{m}{d_1},$$

όπου $d = (a_1, a_2, \ldots, a_k, m), d_1 = (a_1, a_2, \ldots, a_{k-1}, m)$ και y_i είναι οι λύσεις $\mod d_1$ της γραμμικής ισοδυναμίας

$$a_k x_k = b \mod d_1.$$

7.2.1 Αλγόριθμος για την επίλυση της γραμμικής ισοδυναμίας 1

1. Ελέγχουμε αν είναι επιλύσιμη:

$$(a_1, a_2, \ldots, a_k, m) = d \mid b.$$

2. Βρίσκουμε το πλήθος των λύσεών της:

$$N_k = dm^{k-1},$$

3. Λύνουμε την ισοδυναμία για το x_k:

$$a_k x_k \equiv b \mod d_1, \tag{2}$$

όπου $d_1 = (a_1, a_2, \ldots, a_{k-1}, m)$. Έστω $y_{1i}(i = 1, 2, \ldots, d)$ οι λύσεις $\mod d_1$ της εξ. 2.

4. Κάθε λύση y_i επεκτείνεται σε $\frac{m}{d_1}$ τάξεις υπολοίπων $\mod m$ που αντιπροσωπεύονται από τους αριθμούς:

$$\begin{aligned} y_{i1} &= y_i + d_1 \\ y_{i2} &= y_i + 2\, d_1 \\ &\vdots \\ y_{i\frac{m}{d_1}} &= y_i + \frac{m}{d_1} d_1 \end{aligned}$$

5. Λύνουμε τις $\frac{dm}{d_1}$ ισοδυναμίες:

$$a_1 x_1 + a_2 x_2 + \cdots + a_{k-1} x_{k-1} \equiv (b - a_k y_{ij}) \pmod m,$$

με $k-1$ αγνώστους και συνεχίζουμε με τον ίδιο τρόπο.

8 Συστήματα γραμμικών ισοδυναμιών

Ορισμός 8.1: Αντίστροφος

Έστω $m \in \mathbb{N}$ και $a \in \mathbb{Z}$ με $(a, m) = 1$. Η μοναδική λύση της γραμμικής ισοδυναμίας

$$ax \equiv 1 \pmod m$$

λέγεται *αντίστροφος* του $a \mod m$ και συμβολίζεται με a'.

8.1 Μέτρα ισοδυναμίας που είναι πρώτοι αριθμοί ανά 2

Θεώρημα 8.1: Κινέζικο θεώρημα υπόλοιπων

Έστω το σύστημα ισοδυναμιών (Σ_1)

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_k \pmod{m_k}, \end{aligned}$$

όπου $b_1, b_2, \ldots, b_k \in \mathbb{Z}$ και $m_1, m_2, \ldots, m_k \in \mathbb{N}$ με

$$(m_i, m_j) = 1, i \neq j.$$

Το σύστημα έχει μοναδική λύση $\mod m_1 m_2 \ldots m_k$, η οποία προσδιορίζεται από τον τύπο:

$$x \equiv \sum_{i=1}^{k} b_i M_i \, M_i' \pmod{m_1 m_2 \cdots m_k},$$

όπου

$$M_i = \frac{m_1 m_2 \cdots m_k}{m_i}$$

και M_i' είναι ο αντίστροφος του $M_i \pmod{m_i}$ ή τον τύπο

$$x \equiv \sum_{i=1}^{k} b_i M_i^{\varphi(m_i)} \pmod{m_1 m_2 \cdots m_k}.$$

Θεώρημα 8.2

Το σύστημα ισοδυναμιών (Σ_1) είναι ισοδύναμο με την ισοδυναμία

$$\left(\sum_{i=1}^{k} M_i\right) x \equiv \sum_{i=1}^{k} M_i b_i \pmod{m_1 m_2 \cdots m_k}.$$

Θεώρημα 8.3

Έστω το σύστημα ισοδυναμιών (Σ_2)

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_kx &\equiv b_k \pmod{m_k}, \end{aligned}$$

όπου $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k \in \mathbb{Z}$ και $m_1, m_2, \dots, m_k \in \mathbb{N}$ με

$$\begin{aligned} (m_i, m_j) &= 1, \quad i \neq j, \\ (a_i, m_i) &= 1, \quad \forall i = 1, 2, \dots, k. \end{aligned}$$

Το σύστημα έχει μοναδική λύση $\mod m_1 m_2 \dots m_k$.

Θεώρημα 8.4

Το σύστημα ισοδυναμιών (Σ_2) είναι ισοδύναμο με την ισοδυναμία

$$\left(\sum_{i=1}^{k} a_i M_i\right) x \equiv \sum_{i=1}^{k} M_i b_i \pmod{m_1 m_2 \cdots m_k}.$$

Θεώρημα 8.5

Έστω το σύστημα ισοδυναμιών (Σ_3)

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_kx &\equiv b_k \pmod{m_k}, \end{aligned}$$

όπου $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k \in \mathbb{Z}$ και $m_1, m_2, \dots, m_k \in \mathbb{N}$ με

$$\begin{aligned} (m_i, m_j) &= 1, \quad i \neq j, \\ (a_i, m_i) &= d_i, \quad \forall i = 1, 2, \dots, k. \end{aligned}$$

Το σύστημα έχει λύση αν

$$d_i \mid b_i, \forall i = 1, 2, \dots, k$$

και το πλήθος των λύσεων είναι

$$d_1 d_2 \dots d_k.$$

Αν για κάποιο i ισχύει

$$d_i \nmid b_i$$

τότε το σύστημα δεν έχει λύση.

8.2 Μέτρα ισοδυναμίας που δεν είναι πρώτοι ανά 2

Θεώρημα 8.6

Έστω το σύστημα ισοδυναμιών (Σ_4)

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_k \pmod{m_k}, \end{aligned}$$

όπου $b_1, b_2, \dots, b_k \in \mathbb{Z}$ και $m_1, m_2, \dots, m_k \in \mathbb{N}$. Το σύστημα (Σ_4) έχει μοναδική λύση mod $[m_1, m_2, \dots, m_k]$ αν και μόνο αν

$$(m_i, m_j) \mid (b_i - b_j), \forall\, i, j = 1, 2, \dots, k.$$

9 Πολυωνυμικές ισοδυναμίες

9.1 Πολυωνυμικές ισοδυναμίες mod m

- Πολυωνυμικές ισοδυναμίες είναι ισοδυναμίες της μορφής

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \equiv 0 \pmod{m}, \tag{3}$$

όπου $a_1, a_2, \dots, a_n \in \mathbb{Z}$ και $m, n \in \mathbb{Z}$.
- Ο ακέραιος αριθμός y θα λέγεται λύση της πολυωνυμικής ισοδυναμίας εξ. 3 αν

$$f(y) \equiv 0 \pmod{m}.$$

- Αν y, z είναι λύσεις της πολυωνυμικής ισοδυναμίας εξ. 3, θα θεωρούνται διαφορετικές αν ισχύει

$$y \not\equiv z \pmod{m}.$$

- Όπως και στις γραμμικές ισοδυναμίες η πολυωνυμική ισοδυναμία εξ. 3 έχει το πολύ m λύσεις. Οι λύσεις αυτές μπορούν να βρεθούν δίνοντας στο x τις τιμές $0, 1, 2, \dots, m-1$.
- Όταν $n > 1$ και $m > 1$ το πλήθος των λύσεων της πολυωνυμικής ισοδυναμίας εξ. 3 δεν είναι γνωστό εκ των προτέρων.

Θεώρημα 9.1

Έστω f ένα πολυώνυμο με ακέραιους συντελεστές και $m \in \mathbb{N}$ με $m > 1$ ο οποίος αναλύεται σε γινόμενο πρώτων παραγόντων ως

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Η πολυωνυμική ισοδυναμία

$$f(x) \equiv 0 \pmod{m}$$

έχει λύση αν και μόνο αν καθεμιά από τις πολυωνυμικές ισοδυναμίες

$$f(x) \equiv 0 \pmod{p_i^{a_i}}, \tag{4}$$

έχει λύση. Επιπλέον, για το πλήθος N_m των λύσεων της πολυωνυμικής ισοδυναμίας ισχύει:

$$N_m = N_1 N_2 \cdots N_k,$$

όπου N_i είναι το πλήθος λύσεων της εξ. 4, $i = 1, 2, \dots, k$.

9.2 Πολυωνυμικές ισοδυναμίες $\mod p^a$

Θεωρούμε τις πολυωνυμικές ισοδυναμίες της μορφής:

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \equiv 0 \pmod{p^a}, \tag{5}$$

όπου $a_1, a_2, \dots, a_n \in \mathbb{Z}, m, a \in \mathbb{N}$ με $a \geq 2$ και p πρώτος αριθμός.

Ορισμός 9.1

Έστω r μία λύση της πολυωνυμικής ισοδυναμίας

$$f(x) \equiv 0 \pmod{p^{a-1}}, \tag{6}$$

με $0 \leq r < p^{a-1}$. Αν υπάρχει λύση y της πολυωνυμικής ισοδυναμίας

$$f(x) \equiv 0 \pmod{p^a},$$

με $0 \leq r < p^a$ και $y = kp^{a-1} + r$ $(k \in \mathbb{Z})$, τότε η λύση y λέγεται *αντίστοιχη* στη λύση r της πολυωνυμικής ισοδυναμίας 6.

Θεώρημα 9.2

Έστω $a \geq 2$ και r μία λύση της πολυωνυμικής ισοδυναμίας

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \equiv 0 \pmod{p^{a-1}},$$

με $0 \leq r < p^{a-1}$.

- Αν $f'(r) \not\equiv 0 \pmod{p}$, τότε υπάρχει μοναδική λύση y της πολυωνυμικής ισοδυναμίας 5 αντίστοιχη στη λύση r.
- Αν $f'(r) \equiv 0 \pmod{p}$ και επιπλέον:
  - $f(r) \equiv 0 \pmod{p^a}$, τότε θα υπάρχουν p λύσεις της πολυωνυμικής ισοδυναμίας 5 αντίστοιχες στη λύση r.
  - $f(r) \not\equiv 0 \pmod{p^a}$, τότε δεν υπάρχει καμία λύση.

10 Τετραγωνικά υπόλοιπα & Σύμβολο Legendre

10.1 Τετραγωνικά υπόλοιπα

Θεωρούμε τετραγωνικές ισοδυναμίες της μορφής:

$$x^2 \equiv n \pmod{p} \tag{7}$$

όπου ο p είναι περιττός πρώτος και $n \not\equiv 0 \pmod{p}$.

Πρόταση 10.1

Έστω $n \in \mathbb{Z}$ και p ένας περιττός πρώτος με $p \nmid n$. Η ισοδυναμία $x^2 \equiv n \pmod{p}$ έχει είτε δύο (μη-ισοδύναμες) λύσεις ή καμία λύση.

Ορισμός 10.1

- Αν η τετραγωνική ισοδυναμία $x^2 \equiv n \pmod{p}$ έχει λύση, τότε λέμε ότι ο n είναι τετραγωνικό υπόλοιπο $\bmod p$.
- Αν η τετραγωνική ισοδυναμία $x^2 \equiv n \pmod{p}$ δεν έχει λύση, τότε λέμε ότι ο n είναι τετραγωνικό μη-υπόλοιπο $\bmod p$.

Σημείωση

Για να υπολογίσουμε τα τετραγωνικά υπόλοιπα $\mod p$ αρκεί να πάρουμε μόνο τα τετράγωνα των αριθμών $1, 2, \ldots, \frac{p-1}{2}$, καθώς

$$\begin{aligned} p-1 &\equiv -1 \mod p \\ p-2 &\equiv -2 \mod p \\ &\vdots \\ p-\frac{p-1}{2} &\equiv -\left(\frac{p-1}{2}\right) \mod p \end{aligned}$$

δηλαδή

$$(p-x)^2 \equiv x^2 \mod p, \quad x = 1, 2, \ldots, \frac{p-1}{2}.$$

Θεώρημα 10.1

Έστω p ένας περιττός πρώτος. Κάθε ανηγμένο σύστημα υπολοίπων $\mod p$ περιέχει ακριβώς $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα και $\frac{p-1}{2}$ τετραγωνικά μη-υπόλοιπα. Τα τετραγωνικά υπόλοιπα ανήκουν στις τάξεις υπολοίπων που περιέχουν τους αριθμούς

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

10.2 Σύμβολο Legendre

Ορισμός 10.2: Σύμβολο Legendre

Το σύμβολο Legendre $\left(\frac{n}{p}\right)$ ορίζεται ως εξής:

$$\left(\frac{n}{p}\right) = \begin{cases} 1, & n \text{ τετραγωνικό υπόλοιπο} \mod p \\ -1, & n \text{ τετραγωνικό μη-υπόλοιπο} \mod p \end{cases}$$

όπου p είναι περιττός πρώτος και $n \not\equiv 0 \pmod p$. Ενώ, αν $n \equiv 0 \pmod p$, τότε

$$\left(\frac{n}{p}\right) = 0.$$

Θεώρημα 10.2: Κριτήριο Euler

Έστω $n \in \mathbb{N}$ και p ένας περιττός πρώτος αριθμός. Ισχύει ότι:

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod p.$$

Θεώρημα 10.3

Έστω $n_1, n_2 \in \mathbb{Z}$ και p ένας περιττός πρώτος αριθμός. Ισχύει ότι:

$$\left(\frac{n_1 n_2}{p}\right) = \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right).$$

Θεώρημα 10.4

Έστω $n_1, n_2 \in \mathbb{Z}$ και p ένας περιττός πρώτος αριθμός με $p \nmid n_1$ και $p \nmid n_2$. Ισχύει ότι:

1. $\left(\frac{1}{p}\right) = 1$
2. Αν $n_1 \equiv n_2 \pmod p$, τότε $\left(\frac{n_1}{p}\right) = \left(\frac{n_2}{p}\right)$
3. $\left(\frac{n_1^2}{p}\right) = 1$

Θεώρημα 10.5

Για κάθε περιττό πρώτο p ισχύει:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1 \\ \pmod 4, & \\ -1, & p \equiv 3 \\ \pmod 4). & \end{cases}$$

Θεώρημα 10.6

Για κάθε περιττό πρώτο p ισχύει:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8). \end{cases}$$

Θεώρημα 10.7: Τετραγωνικός Νόμος Αντιστροφής

Αν $p \neq q$ περιττοί πρώτοι, τότε

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

10.3 Σύμβολο Jacobi

Το σύμβολο Jacobi είναι γενίκευση του συμβόλου Legendre. Συγκεκριμένα, για το σύμβολο Legendre $\left(\frac{n}{p}\right)$ πρέπει ο αριθμός p να είναι περιττός πρώτος, ενώ στο σύμβολο Jacobi της μορφής $\left(\frac{n}{m}\right)$ ο αριθμός $1 < m \in \mathbb{N}$ είναι περιττός.

Ορισμός 10.3: Σύμβολο Jacobi

Το σύμβολο Jacobi $\left(\frac{n}{m}\right)$ ορίζεται ως εξής:

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)\left(\frac{n}{p_2}\right)\cdots\left(\frac{n}{p_k}\right),$$

όπου $\left(\frac{n}{p_i}\right), i = 1, 2, \dots, k$, είναι σύμβολα Lagrange. Αν $m = 1$, τότε

$$\left(\frac{n}{1}\right) = 1.$$

Ισχύουν τα παρακάτω:

1. Αν $(n, m) = 1$, τότε $\left(\frac{n}{m}\right) = \pm 1$.
2. Αν $(n, m) > 1$, τότε $\left(\frac{n}{m}\right) = 0$.
3. Ισχύει ότι $\left(\frac{1}{m}\right) = 1$.

Θεώρημα 10.8

Έστω $n \in \mathbb{Z}$ και $m > 1 \in \mathbb{N}$ ένας περιττός αριθμός με $(n, m) = 1$. Αν η ισοδυναμία

$$x^2 \equiv n \pmod{m}$$

έχει λύση, τότε ισχύει ότι:

$$\left(\frac{n}{m}\right) = 1.$$

Το αντίστροφο **δεν** ισχύει.

Θεώρημα 10.9

Έστω $n_1, n_2 \in \mathbb{Z}$ και $m \in \mathbb{N}$ ένας περιττός αριθμός. Αν ισχύει ότι:

$$n_1 \equiv n_2 \pmod{m},$$

τότε

$$\left(\frac{n_1}{m}\right) = \left(\frac{n_2}{m}\right).$$

Θεώρημα 10.10

Έστω $n_1, n_2 \in \mathbb{Z}$ και $m \in \mathbb{N}$ ένας περιττός αριθμός. Αν ισχύει ότι:

$$\left(\frac{n_1 n_2}{m}\right) = \left(\frac{n_1}{m}\right)\left(\frac{n_2}{m}\right).$$

Θεώρημα 10.11

Έστω $n \in \mathbb{Z}$ και $m \in \mathbb{N}$ ένας περιττός αριθμός με $(n,m) = 1$. Τότε ισχύει:

$$\left(\frac{n^2}{m}\right) = 1.$$

Θεώρημα 10.12

Έστω $m \in \mathbb{N}$ ένας περιττός αριθμός. Τότε, ισχύουν τα ακόλουθα.

1. $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$
2. $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$

Θεώρημα 10.13: Τετραγωνικός Νόμος Αντιστροφής για τα σύμβολα Jacobi

Αν $n, m \in \mathbb{N}$ περιττοί αριθμοί με $(n,m) = 1$, τότε

$$\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{m}{n}\right).$$

11 Διοφαντικές εξισώσεις

Διοφαντική εξίσωση ονομάζεται κάθε εξίσωση της μορφής

$$f(x_1, x_2, \dots, x_n) = 0,$$

όπου $f(x_1, x_2, \dots, x_n)$ είναι πολυώνυμο με ακέραιους συντελεστές και αναζητούμε λύσεις στους ακέραιους αριθμούς.

Μία Διοφαντική εξίσωση θεωρείται ότι έχει λυθεί, αν έχει δοθεί απάντηση στα παρακάτω ζητήματα:

1. Έχει μία τουλάχιστον ακέραια λύση;
2. Ο αριθμός των ακέραιων λύσεων είναι πεπερασμένος ή άπειρος;
3. Να βρεθούν όλες οι ακέραιες λύσεις.

Η Διοφαντική εξίσωση

$$x^n + y^n = z^n, \quad n \geq 3,$$

λέγεται *εξίσωση Fermat*. Υπήρχε η εικασία (εικασία του Fermat) ότι η παραπάνω εξίσωση δεν έχει ακέραιες λύσεις με την ιδιότητα $xyz \neq 0$. Η εικασία αυτή αποδείχθηκε τελικά.

11.1 Η εξίσωση $ax + by = c$

Θεώρημα 11.1

Έστω η Διοφαντική εξίσωση

$$ax + by = c \tag{8}$$

όπου $a, b, c \in \mathbb{Z}$, με έναν τουλάχιστον από τους $a, b \neq 0$, και $d = (a, b)$. Τα ακόλουθα είναι ισοδύναμα:

1. Η Διοφαντική εξίσωση εξ. 8 έχει ακέραια λύση.
2. Ισχύει ότι $d \mid c$.

Θεώρημα 11.2

Έστω η Διοφαντική εξίσωση

$$ax + by = c \tag{9}$$

όπου $a, b, c \in \mathbb{Z}$ και $d = (a, b) \mid c$. Τότε, όλες οι ακέραιες λύσεις της εξ. 9 δίνονται από τους τύπους:

$$x = x_0 + b_1 t, \quad y = y_0 - a_1 t,$$

όπου $t = 0, \pm 1, \pm 2, \dots, a_1 = \frac{a}{d}, b_1 = \frac{b}{d}$ και το ζεύγος (x_0, y_0) είναι μια ακέραια λύση της εξ. 9.

Θεώρημα 11.3: Γραμμική Διοφαντική εξίσωση με n μεταβλητές

Έστω η Διοφαντική εξίσωση

$$a_1 x_1 + a_2 x_2 + \cdots a_n x_n = c, \tag{10}$$

όπου $n > 1, a_1, a_2, \dots, a_n, c \in Z$, με έναν τουλάχιστον από τους $a_i, i = 1, 2, \dots, n$, να είναι διάφορος του μηδενός. Τα ακόλουθα είναι ισοδύναμα:

1. Η Διοφαντική εξίσωση εξ. 10 έχει ακέραια λύση.
2. Ισχύει ότι $(a_1, a_2, \dots, a_n) \mid c$.

11.2 Η εξίσωση $x^2 + y^2 = z^2$

Οι Πυθαγόρειοι συνδέανε τους αριθμούς με την Γεωμετρία. Μία τέτοια σύνδεση έχει προκύψει από το Πυθαγόρειο Θεώρημα.

Ορισμός 11.1: Πυθαγόρεια τριάδα

Η τριάδα (x, y, z) λέγεται *Πυθαγόρεια τριάδα*, αν $x, y, z \in \mathbb{N}$ με την ιδιότητα

$$x^2 + y^2 = z^2$$

Ορισμός 11.2

Μία Πυθαγόρεια τριάδα (x, y, z) λέγεται *πρωτογενής*, αν ισχύει

$$(x, y) = (x, z) = (y, z) = 1.$$

Θεώρημα 11.4

Όλες οι πρωτογενείς λύσεις της Διοφαντικής εξίσωσης

$$x^2 + y^2 = z^2,$$

δίνονται από τους εξής τύπους:

$$x = c^2 - h^2, \quad y = 2hc, \quad z = c^2 + h^2,$$

όπου $c, h \in \mathbb{N}$ αυθαίρετοι με $c > h, (c, h) = 1$ και ο ένας από τους c, h είναι περιττός και ο άλλος άρτιος.

Θεώρημα 11.5

Όλες οι ακέραιες (θετικές) λύσεις της Διοφαντικής εξίσωσης

$$x^2 + y^2 = z^2,$$

δίνονται από τους εξής τύπους:

$$x = (c^2 - h^2)t, \quad y = 2hct, \quad z = (c^2 + h^2)t,$$

όπου $t, c, h \in \mathbb{N}$ αυθαίρετοι με $c > h, (c, h) = 1$ και ο ένας από τους c, h είναι περιττός και ο άλλος άρτιος.

11.3 Η εξίσωση $xy = zt$

Θεώρημα 11.6

Έστω $x, y, z, t \in \mathbb{N}$. Όλες οι (ακέραιες) λύσεις της εξίσωσης

$$xy = zt,$$

δίνονται από τους τύπους:

$$x = ac, \quad y = bd, \quad z = ad, \quad t = bc,$$

όπου $a, b, c, d \in \mathbb{N}$ αυθαίρετοι.

11.3.1 Αλγόριθμος επίλυσης της Διοφαντικής εξίσωσης $xy = zt$

1. Θεωρούμε αυθαίρετους φυσικούς αριθμούς x, z.
2. Διαιρούμε την αρχική εξίσωση $xy = zt$ με (x, z), άρα

$$\frac{x}{(x,z)}y = \frac{z}{(x,z)}t.$$

οπότε

$$\frac{z}{(x,z)} \mid \frac{x}{(x,z)}y$$

κι αφού $\left(\frac{x}{(x,z)}, \frac{z}{(x,z)}\right) = 1$ προκύπτει ότι

$$\frac{z}{(x,z)} \mid y.$$

3. Οι λύσεις της Διοφαντικής εξίσωσης $xy = zt$ είναι:

$$y = u\frac{z}{(x,z)} \quad \text{κα} \quad t = u\frac{x}{(x,z)},$$

όπου $u \in \mathbb{N}$.

Αναφορές

[1] Ι. Αντωνιάδης και Α. Κοντογεώργης, *Θεωρία Αριθμών και εφαρμογές*, Θ. Θεοχάρη-Αποστολίδου, επιμελητής. Kallipos, Open Academic Editions, 10 Μάι. 2015, 250 **pagetotals**, ISBN: 978-618-82124-5-9. διεύθν.: http://hdl.handle.net/11419/107.