1 Ακέραιοι

Στην Ενότητα αυτή θα μελετήσουμε ιδιότητες του συνόλου των ακεραίων αριθμών, $\mathbb{Z}$. Ο σκοπός μας είναι διττός. Αφενός θα μελετήσουμε τις ιδιότητες του $\mathbb{Z}$ που θα χρησιμοποιήσουμε σε επόμενες Ενότητες και αφετέρου θα εισάγουμε μέσω του $\mathbb{Z}$ μερικές θεμελιώδεις έννοιες της Άλγεβρας. Έτσι, δίνεται η ευκαιρία στον αναγνώστη να μελετήσει αρκετές από τις έννοιες της Άλγεβρας, που εμφανίζονται παρακάτω, στην ειδική περίπτωση των ακεραίων. Σε καμιά περίπτωση η Ενότητα αυτή δεν αποτελεί εισαγωγή στον πλούσιο κλάδο της Θεωρίας Αριθμών.

Θα θεωρήσουμε γνωστές τις πλέον στοιχειώδεις ιδιότητες της πρόσθεσης και του πολλαπλασιασμού ακεραίων όπως και της διάταξης, $... < -1 < 0 < 1 < ...$, που υπάρχει στο $\mathbb{Z}$ με τις οποίες είμαστε εξοικειωμένοι από τα πρώτα μαθητικά μας χρόνια. Οι τεχνικές των αποδείξεων που θα δούμε εδώ είναι τυπικές για την Άλγεβρα, πράγμα που θα διαπιστώσουμε παρακάτω όταν μελετήσουμε δακτυλίους, σώματα και ομάδες.

Στο βιβλίο αυτό θα χρησιμοποιούμε τους παρακάτω συμβολισμούς.

$\mathbb{N} = \{0, 1, 2, \dots\}$ Το σύνολο των φυσικών αριθμών.
$\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$ Το σύνολο των ακεραίων αριθμών.
$\mathbb{Q}$ Το σύνολο των ρητών αριθμών.
$\mathbb{R}$ Το σύνολο των πραγματικών αριθμών.
$\mathbb{C}$ Το σύνολο των μιγαδικών αριθμών.
$\mathbb{Z}_{>0}$ Το σύνολο των θετικών ακεραίων.
$\mathbb{Q}_{>0}$ Το σύνολο των θετικών ρητών αριθμών.
$\mathbb{R}_{>0}$ Το σύνολο των θετικών πραγματικών αριθμών.

1.1 Μαθηματική Επαγωγή, Διωνυμικοί Συντελεστές

Στην Παράγραφο αυτή θα υπενθυμίσουμε τη μέθοδο απόδειξης που ονομαζεται Μαθηματική Επαγωγή. Επίσης θα ασχοληθούμε με τους διωνυμικούς συντελεστές. Η αφετηρία μας είναι το επόμενο αξίωμα.

1.1.1 Αξίωμα (*Αξίωμα Ελαχίστου*). *Κάθε μη κενό σύνολο φυσικών αριθμών περιέχει ελάχιστο στοιχείο.*

Σημειώνουμε ότι αντίστοιχη ιδιότητα δεν ισχύει στους πραγματικούς ή ρητούς αριθμούς. Για παράδειγμα, το σύνολο $\{1, 1/2, 1/3, 1/4, ...\}$ δεν περιέχει ελάχιστο στοιχείο αν και είναι υποσύνολο των θετικών ρητών αριθμών.

Από τη διάταξη που υπάρχει στο $\mathbb{Z}$, παρατηρούμε ότι κάθε μη κενό σύνολο φυσικών αριθμών περιέχει μοναδικό ελάχιστο στοιχείο.

1.1.2 Θεώρημα (*Μαθηματική Επαγωγή*). *Έστω ότι για κάθε φυσικό αριθμό n δίνεται μια πρόταση $P(n)$, που αφορά τον n, τέτοια ώστε*

1) η $P(0)$ αληθεύει, και

2) για κάθε n, αν η $P(n)$ αληθεύει, τότε η $P(n+1)$ αληθεύει.

Τότε η $P(n)$ αληθεύει για κάθε φυσικό αριθμό n.

Απόδειξη. Έστω A το υποσύνολο του $\mathbb{N}$ που αποτελείται από τους n για τους οποίους η πρόταση $P(n)$ δεν αληθεύει,

$$A = \{n \in \mathbb{N} | P(n) \text{ δεν αληθεύει}\}.$$

Θα δείξουμε ότι το A είναι κενό. Ας υποθέσουμε ότι $A \neq \emptyset$. Τότε από το Αξίωμα Ελαχίστου το A περιέχει ελάχιστο στοιχείο, έστω m. Από την υπόθεση 1) έχουμε $m > 0$. Από τον ορισμό του m έπεται ότι η πρόταση $P(m-1)$ αληθεύει. Τότε όμως η υπόθεση 2) δίνει ότι η $P(m)$ αληθεύει. Αυτό είναι άτοπο. ⊤

Είδαμε ότι το προηγούμενο Θεώρημα έπεται από το Αξίωμα Ελαχίστου. Μπορεί να αποδειχθεί ότι το Θεώρημα της Μαθηματικής Επαγωγής είναι ισοδύναμο με το Αξίωμα Ελαχίστου (Άσκηση 8). Η υπόθεση 1) στο προηγούμενο Θεώρημα συνήθως ονομάζεται "αρχικό βήμα της επαγωγής" ενώ η υπόθεση 2) "επαγωγικό βήμα." Πριν προχωρήσουμε σε παραδείγματα, αναφέρουμε μια παραλλαγή που διαφέρει στο αρχικό βήμα της επαγωγής.

1.1.3 Θεώρημα (*Μαθηματική Επαγωγή με αρχικό βήμα από το m*). *Έστω $m \in \mathbb{N}$. Έστω ότι για κάθε φυσικό αριθμό n με $n \geq m$ δίνεται μια πρόταση $P(n)$, που αφορά τον n, τέτοια ώστε*

1) *η* $P(m)$ *αληθεύει, και*

2) *για κάθε* $n \geq m$*, αν η* $P(n)$ *αληθεύει, τότε η* $P(n+1)$ *αληθεύει.*

Τότε η $P(n)$ *αληθεύει για κάθε* $n \in \mathbb{N}$ *με* $n \geq m$*.*

Απόδειξη. Η απόδειξη είναι παρόμοια με την προηγούμενη και αφήνεται σαν άσκηση. ⊤

1.1.4 Παραδείγματα.

1) $1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$ για κάθε θετικό ακέραιο n.
Χρησιμοποιούμε επαγωγή. *Αρχικό βήμα:* Για $n = 1$, η αποδεικτέα σχέση είναι $1 = \frac{1}{2}1(1+1)$, που ισχύει. *Επαγωγικό βήμα:* Έστω ότι ισχύει

$$1 + 2 + \cdots + n = \frac{1}{2}n(n+1). \qquad P(n)$$

Θα αποδείξουμε ότι ισχύει

$$1 + 2 + \cdots + (n+1) = \frac{1}{2}(n+1)(n+2). \qquad P(n+1)$$

Το αριστερό μέλος της $P(n+1)$ γράφεται με τη βοήθεια της $P(n)$

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

Το δεξιό μέλος της παραπάνω ισότητας είναι $\frac{1}{2}(n+1)(n+2)$, που είναι το ζητούμενο.

2) $2^n > n^2$ για κάθε ακέραιο $n \geq 5$.
Χρησιμοποιούμε επαγωγή. Για $n = 5$ η αποδεικτέα σχέση είναι η $2^5 > 5^2$, που ισχύει. Υποθέτουμε τώρα ότι ισχύει

$$2^n > n^2, \qquad P(n)$$

όπου $n \geq 5$, και θα αποδείξουμε ότι

$$2^{n+1} > (n+1)^2. \qquad P(n+1)$$

Από την $P(n)$ έχουμε ότι $2^{n+1} = 2 \cdot 2^n > 2n^2$. Επιπλέον ισχύει $2n^2 = n^2 + n \cdot n \geq n^2 + 3n$ (γιατί $n \geq 3$), και $n^2 + 3n \geq n^2 + 2n + 1 = (n+1)^2$. Από τις προηγούμενες σχέσεις προκύπτει το ζητούμενο.

3) Έστω A ένα πεπερασμένο σύνολο που έχει n στοιχεία. Τότε το πλήθος των υποσυνόλων του A είναι 2^n.
Χρησιμοποιούμε επαγωγή. Για $n = 0$, η πρόταση αληθεύει καθώς το κενό σύνολο έχει $2^0 = 1$ υποσύνολα. Υποθέτουμε τώρα ότι η πρόταση αληθεύει για κάθε σύνολο με $n \in \mathbb{N}$ στοιχεία. Έστω ότι το A έχει $n+1$ στοιχεία και $\alpha \in A$. Το σύνολο $B = A - \{\alpha\}$ έχει n στοιχεία και συνεπώς το πλήθος των υποσυνόλων του είναι 2^n. Θα μετρήσουμε το πλήθος των υποσυνόλων του A. Έστω $\Gamma \subseteq A$. Διακρίνουμε δύο περιπτώσεις. 1) Έστω $\alpha \notin \Gamma$. Τότε $\Gamma \subseteq B$ και συνεπώς το πλήθος των Γ είναι 2^n. 2) Έστω $\alpha \in \Gamma$. Τότε $\Gamma = \Delta \cup \{\alpha\}$ με $\Delta \subseteq B$, οπότε συμπεραίνουμε ότι το πλήθος των Γ είναι πάλι 2^n. Συνολικά, υπάρχουν $2^n + 2^n = 2^{n+1}$ υποσύνολα του A, που είναι το ζητούμενο.

4) **Θεώρημα de Moivre.** Έστω $\theta \in \mathbb{R}$. Τότε για τον μιγαδικό αριθμό $\sigma\upsilon\nu\theta + i\eta\mu\theta$ ισχύει $(\sigma\upsilon\nu\theta + i\eta\mu\theta)^n = \sigma\upsilon\nu(n\theta) + i\eta\mu(n\theta)$ για κάθε $n \in \mathbb{N}$.
Για $n = 0$ η αποδεικτέα σχέση είναι προφανής. Υποθέτουμε ότι αυτή ισχύει για n. Χρησιμοποιώντας τις γνωστές τριγωνομετρικές ταυτότητες $\sigma\upsilon\nu(\theta+\varphi) = \sigma\upsilon\nu\theta\sigma\upsilon\nu\varphi - \eta\mu\theta\eta\mu\varphi$ και $\eta\mu(\theta+\varphi) = \eta\mu\theta\sigma\upsilon\nu\varphi + \eta\mu\varphi\sigma\upsilon\nu\theta$, έχουμε

$$\begin{aligned}(\sigma\upsilon\nu\theta + i\eta\mu\theta)^{n+1} &= (\sigma\upsilon\nu\theta + i\eta\mu\theta)^n(\sigma\upsilon\nu\theta + i\eta\mu\theta)\\ &= (\sigma\upsilon\nu(n\theta) + i\eta\mu(n\theta))(\sigma\upsilon\nu\theta + i\eta\mu\theta)\\ &= \sigma\upsilon\nu(n\theta)\sigma\upsilon\nu\theta - \eta\mu(n\theta)\eta\mu\theta\\ &\quad + i(\sigma\upsilon\nu(n\theta)\eta\mu\theta + \eta\mu(n\theta)\sigma\upsilon\nu\theta)\\ &= \sigma\upsilon\nu(n\theta+\theta) + i\eta\mu(n\theta+\theta)\\ &= \sigma\upsilon\nu((n+1)\theta) + i\eta\mu((n+1)\theta).\end{aligned}$$

Υπάρχει μία άλλη μορφή της μαθηματικής επαγωγής που είναι χρήσιμη.

1.1.5 Θεώρημα (*Δεύτερη Μορφή της Μαθηματικής Επαγωγής*). *Έστω ότι για κάθε φυσικό αριθμό n δίνεται μια πρόταση $P(n)$, που αφορά τον n, τέτοια ώστε*

1) η $P(0)$ αληθεύει, και

2) για κάθε n, αν η $P(k)$ αληθεύει για κάθε φυσικό αριθμό k με $0 \leq k \leq n$, τότε η $P(n+1)$ αληθεύει.

Τότε η $P(n)$ αληθεύει για κάθε φυσικό αριθμό n.

Απόδειξη. Αρκεί να αποδειχθεί ότι το σύνολο $A = \{n \in \mathbb{N} | P(n) \text{ δεν αληθεύει}\}$ είναι κενό. Έστω ότι το A δεν είναι κενό. Τότε λόγω του Αξιώματος 1.1.1, το A περιέχει ελάχιστο στοιχείο, έστω m. Από την υπόθεση 1) έχουμε ότι $m \geq 1$. Από τον ορισμό του m προκύπτει ότι η πρόταση $P(k)$ αληθεύει για κάθε $k \leq m-1$. Από την υπόθεση 2) προκύπτει ότι η $P(m)$ αληθεύει, που είναι άτοπο. ⊤

Σημείωση. Στη Δεύτερη Μορφή της Μαθηματικής επαγωγής είναι δυνατόν το αρχικό βήμα να μην είναι το 0 αλλά οποιοσδήποτε $m \in \mathbb{N}$. Σύγκρινε με το Θεώρημα 1.1.3.

Διωνυμικοί συντελεστές

Στη συνέχεια θα ασχοληθούμε με το διωνυμικό ανάπτυγμα που θα χρησιμοποιηθεί στα επόμενα. Έστω $i \leq n$ φυσικοί αριθμοί. Με $\binom{n}{i}$ συμβολίζουμε τον συντελεστή του x^i στο ανάπτυγμα του διωνύμου $(1+x)^n$. Για παράδειγμα, έχουμε $\binom{2}{0} = 1$, $\binom{2}{1} = 2$, $\binom{2}{2} = 1$, αφού $(1+x)^2 = 1 + 2x + x^2$. Όμοια έχουμε $\binom{3}{0} = 1$, $\binom{3}{1} = 3$, $\binom{3}{3} = 1$, αφού $(1+x)^3 = 1 + 3x + 3x^2 + x^3$. Έτσι γράφουμε εξ ορισμού

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n.$$

Στην περίπτωση που έχουμε $i > n$ συμφωνούμε ότι $\binom{n}{i} = 0$. Αυτό επιτρέπει κάποια ομοιομορφία στις διατυπώσεις προτάσεων που αφορούν τους διωνυμικούς συντελεστές. (Βλ. την πρώτη σχέση της παρακάτω πρότασης για $i = n+1$.)

1.1.6 Πρόταση. *1) Έστω i, n φυσικοί αριθμοί με $1 \leq i \leq n+1$. Τότε*

$$\binom{n+1}{i} = \binom{n}{i-1} + \binom{n}{i}.$$

2) Έστω i, n φυσικοί αριθμοί με $i \leq n$. Τότε

$$\binom{n}{i} = \frac{n!}{i!(n-i)!} \tag{1}$$

όπου θέτουμε $0! = 1$ και για κάθε θετικό ακέραιο n, $n! = 1 \cdot 2 \cdot \cdots \cdot n$.

Απόδειξη. 1) Θεωρούμε την ταυτότητα πολυωνύμων

$$(1+x)^{n+1} = (1+x)^n(1+x) = (1+x)^n + (1+x)^n x$$

και συγκρίνουμε τους συντελεστές του x^i στο αριστερό και δεξιό μέλος. Στο αριστερό μέλος ο εν λόγω συντελεστής είναι $\binom{n+1}{i}$, ενώ στο δεξιό είναι $\binom{n}{i}+\binom{n}{i-1}$.
2) Χρησιμοποιούμε επαγωγή στο n. Για $n=0$, οπότε $i=0$, η αποδεικτέα σχέση είναι προφανής. Υποθέτοντας την (1) θα αποδείξουμε ότι

$$\binom{n+1}{i}=\frac{(n+1)!}{i!(n+1-i)!}. \tag{2}$$

Αν $i=0$, εύκολα επαληθεύεται η (2). Έστω λοιπόν $0<i\leq n+1$, οπότε από το 1) της πρότασης και την ισότητα (1) έχουμε

$$\begin{aligned}\binom{n+1}{i}=\binom{n}{i-1}+\binom{n}{i} &= \frac{n!}{(i-1)!(n-i+1)!}+\frac{n!}{i!(n-i)!}\\ &= \frac{n!}{(i-1)!(n-i)!}\left(\frac{1}{n-i+1}+\frac{1}{i}\right)\\ &= \frac{n!}{(i-1)!(n-i)!}\frac{n+1}{(n-i+1)i}\\ &= \frac{(n+1)!}{i!(n+1-i)!}.\end{aligned}$$

και άρα η (2) ισχύει. ⊤

1.1.7 Εφαρμογή.
Έστω A ένα πεπερασμένο σύνολο με n στοιχεία. Τότε το πλήθος των υποσυνόλων του A που έχουν i στοιχεία είναι ίσο με $\binom{n}{i}$ για κάθε i με $0\leq i\leq n$.
Εφαρμόζουμε επαγωγή στο n. Αν $n=0$, τότε $i=0$ και το ζητούμενο είναι προφανές, αφού το κενό σύνολο έχει ακριβώς $\binom{0}{0}=1$ υποσύνολο. Έστω ότι κάθε πεπερασμένο σύνολο με n στοιχεία, $n>0$, έχει $\binom{n}{i}$ υποσύνολα με i στοιχεία. Έστω ότι το A έχει $n+1$ στοιχεία. Θα μετρήσουμε τώρα το πλήθος των υποσυνόλων του A που έχουν i στοιχεία. Έστω $a\in A$ και $B=A-\{\alpha\}$. Έστω Γ ένα υποσύνολο του A που έχει i στοιχεία. Όπως στο Παράδειγμα 1.1.4 3), διακρίνουμε δύο περιπτώσεις. 1) Έστω $\alpha\notin\Gamma$. Τότε $\Gamma\subseteq B$. Από την υπόθεση της επαγωγής έπεται ότι το πλήθος των Γ είναι $\binom{n}{i}$. 2) Έστω $\alpha\in\Gamma$. Τότε $\Gamma-\{\alpha\}\subseteq B$. Από την υπόθεση της επαγωγής έπεται ότι το πλήθος των

$\Gamma - \{\alpha\}$ (και επομένως το πλήθος των Γ) είναι $\binom{n}{i-1}$. Συνολικά υπάρχουν $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$ υποσύνολα του A που έχουν i στοιχεία.

Ασκήσεις 1.1

1) Αποδείξτε ότι $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$ για κάθε θετικό ακέραιο n.

2) Αποδείξτε ότι $1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2 = (1+2+\cdots+n)^2$ για κάθε θετικό ακέραιο n.

3) Αποδείξτε ότι

   i) $3n < n^3$ για κάθε $n \in \mathbb{N}$, $n \geq 2$.

   ii) $mn < n^m$ για κάθε $m, n \in \mathbb{N}$ με $m \geq 3$ και $n \geq 2$.
   Υπόδειξη: επαγωγή στο m.

4) Αποδείξτε ότι για κάθε $k, m, n \in \mathbb{N}$ ισχύουν οι παρακάτω ταυτότητες.

   i) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n\binom{n}{n} = 0$,

   ii) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$,

   iii) $\binom{m+n}{k} = \binom{m}{0}\binom{n}{k} + \binom{m}{1}\binom{n}{k-1} + \cdots + \binom{m}{k}\binom{n}{0}$,

   iv) $\binom{2n}{n} = \binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2$

   v) $\forall\, n \in \mathbb{N}$ ισχύει $\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k} = \sum_{k=0}^{n}\binom{n}{k}^2 2^k$.

   Υπόδειξη: Για την πέμπτη συγκρίνετε τους συντελεστές στην ταυτότητα $(2+x)^n(1+x)^n = (1+(1+x))^n(1+x)^n$.

5) Έστω $f_0 = 0$, $f_1 = 1$ και $f_n = f_{n-1} + f_{n-2}$ για $n \geq 2$ (ακολουθία του Fibonacci).
   Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύουν:

   i) $f_0 + f_1 + \cdots + f_n = f_{n+2} - 1$.

ii) $f_{n+2}f_n - f_{n+1}^2 = (-1)^{n+1}$.

iii) $f_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$, όπου $\alpha = \frac{1+\sqrt{5}}{2}$ και $\beta = \frac{1-\sqrt{5}}{2}$ (οι α, β ικανοποιούν την εξίσωση $x^2 - x - 1 = 0$).

iv) $f_{2n} = \binom{n}{0}f_0 + \binom{n}{1}f_1 + \cdots + \binom{n}{n}f_n$.
Υπόδειξη: Χρησιμοποιήστε το iii).

6) Για κάθε $r, n \in \mathbb{N}$ με $r \leq n$ αποδείξτε ότι $\binom{r}{r} + \binom{r+1}{r} + \cdots + \binom{n}{r} = \binom{n+1}{r+1}$.

7) Έστω $\theta \in \mathbb{R}$. Τότε για τον μιγαδικό αριθμό $\sigma\upsilon\nu\theta + i\eta\mu\theta$ ισχύει $(\sigma\upsilon\nu\theta + i\eta\mu\theta)^n = \sigma\upsilon\nu(n\theta) + i\eta\mu(n\theta)$ για κάθε $n \in \mathbb{Z}$.

8) Αποδείξτε ότι τα ακόλουθα είναι ισοδύναμα.

i) Αξίωμα 1.1.1 (Αξίωμα Ελαχίστου).

ii) Θεώρημα 1.1.2 (Μαθηματική Επαγωγή)

iii) Θεώρημα 1.1.5 (Δεύτερη μορφή της Μαθηματικής Επαγωγής).

1.2 Διαιρετότητα

Στην Παράγραφο αυτή θα μελετήσουμε την έννοια της διαιρετότητας στο $\mathbb{Z}$. Αφού αποδείξουμε τον Αλγόριθμο Διαίρεσης, θα αναπτύξουμε την έννοια του μέγιστου κοινού διαιρέτη με τη βοήθεια του οποίου θα αποδείξουμε το Θεμελιώδες Θεώρημα της Αριθμητικής, σύμφωνα με το οποίο κάθε ακέραιος αριθμός διάφορος των 0 και ± 1 γράφεται ως γινόμενο πρώτων κατά τρόπο ουσιαστικά μοναδικό.

Διαιρετότητα και πρώτοι αριθμοί

Έστω $a, b \in \mathbb{Z}$. Θα λέμε ότι ο a ***διαιρεί*** τον b (ή ότι ο a είναι ***διαιρέτης*** του b ή ότι ο b είναι ***πολλαπλάσιο*** του a) αν υπάρχει $c \in \mathbb{Z}$ με $b = ac$. Θα γράφουμε τότε $a|b$. Παρατηρούμε ότι κάθε ακέραιος είναι διαιρέτης του 0 ενώ το 0 είναι διαιρέτης μόνο του εαυτού του.

Έστω a, b, c τρεις ακέραιοι αριθμοί. Εύκολα διαπιστώνουμε ότι ισχύουν οι παρακάτω ιδιότητες, τις οποίες θα χρησιμοποιούμε στη συνέχεια χωρίς ιδιαίτερη μνεία.

- Αν $a|b$ και $a|c$, τότε $a|bx + cy$ για κάθε $x, y \in \mathbb{Z}$. Ιδιαίτερα, $a|b \pm c$.
- Αν $a|b$ και $b|a$, τότε $a = \pm b$.
- Αν $a|b$ και $b|c$, τότε $a|c$
- Αν $a|b$ και οι a, b είναι θετικοί, τότε $a \leq b$.

Ενδεικτικά αποδεικνύουμε την πρώτη ιδιότητα: από την υπόθεση, υπάρχουν ακέραιοι e, f τέτοιοι ώστε $b = ae$ και $c = af$. Αντικαθιστώντας έχουμε ότι $bx + cy = aex + afy = a(ex + fy)$. Συνεπώς, $a|bx + cy$.

Ένας θετικός ακέραιος $p \neq 1$ λέγεται ***πρώτος*** αριθμός αν οι μόνοι διαιρέτες του είναι οι ± 1 και $\pm p$. Για παράδειγμα, από τους $1, 2, 3, 4, 5, 6, 7, 8$ και 9 οι πρώτοι αριθμοί είναι οι $2, 3, 5$ και 7. Ο κύριος σκοπός μας στην Παράγραφο αυτή είναι να αποδείξουμε ότι κάθε ακέραιος αριθμός διάφορος των $0, \pm 1$ γράφεται ως γινόμενο πρώτων κατά τρόπο ουσιαστικά μοναδικό (Θεμελιώδες Θεώρημα της Αριθμητικής). Αντίστοιχο αποτέλεσμα θα συναντήσουμε στην Ενότητα 2, όταν μελετήσουμε πολυώνυμα. Επίσης η ιδέα της μοναδικής παραγοντοποίησης αναπτύσσεται πιο γενικά στην Ενότητα 3.

Στην διατύπωση της ακόλουθης Πρότασης δεχόμαστε ότι κάθε πρώτος αριθμός είναι γινόμενο πρώτων αριθμών κατά τετριμμένο τρόπο.

1.2.1 Πρόταση. *Κάθε θετικός ακέραιος διάφορος του 1 είναι γινόμενο πρώτων αριθμών.*

Απόδειξη. Έστω ότι η πρόταση δεν ισχύει και έστω M το σύνολο των ακεραίων $n > 1$ οι οποίοι δεν είναι γινόμενα πρώτων αριθμών. Τότε $M \neq \emptyset$ και από

το Αξίωμα 1.1.1 υπάρχει ελάχιστο στοιχείο $m \in M$. Έχουμε $m > 1$ και ο m δεν είναι πρώτος (αφού κάθε πρώτος είναι κατά τετριμμένο τρόπο γινόμενο πρώτων). Συνεπώς $m = ab$ για κάποιους ακεραίους a, b όπου $1 < a < m$ και $1 < b < m$. Από τον ορισμό του m προκύπτει ότι $a \notin M$ και $b \notin M$, δηλαδή οι a, b είναι γινόμενα πρώτων αριθμών. Τότε όμως το ίδιο συμβαίνει για το γινόμενό τους $m = ab$, δηλαδή $m \notin M$. Αυτό είναι άτοπο. ⊤

Συνεπώς βλέπουμε ότι κάθε ακέραιος διάφορος των $0, \pm 1$ γράφεται στην μορφή $\pm p_1 \dots p_k$, όπου οι p_i είναι πρώτοι αριθμοί (όχι αναγκαστικά διακεκριμένοι).

1.2.2 Θεώρημα (*Ευκλείδης*).[1] *Υπάρχουν άπειροι πρώτοι αριθμοί.*

Απόδειξη. Έστω ότι το σύνολο των πρώτων αριθμών είναι πεπερασμένο και ότι είναι το $\{p_1, \dots, p_m\}$. Ο ακέραιος $p_1 p_2 \dots p_m + 1$ έχει έναν πρώτο διαιρέτη σύμφωνα με την Πρόταση 1.2.1, έστω p_i. Αφού $p_i | p_1 p_2 \dots p_m + 1$ και $p_i | p_1 p_2 \dots p_m$ συμπεραίνουμε ότι ο p_i διαιρεί τη διαφορά, δηλαδή $p_i | 1$. Αυτό είναι άτοπο. ⊤

Το επόμενο αποτέλεσμα περιγράφει μια από τις πιο σημαντικές ιδιότητες του $\mathbb{Z}$ και θα χρησιμοποιηθεί πολλές φορές στα παρακάτω.

1.2.3 Θεώρημα (*Αλγόριθμος Διαίρεσης ή Ευκλείδεια Διαίρεση*). *Έστω $a, b \in \mathbb{Z}$ με $a > 0$. Τότε υπάρχουν μοναδικοί $q, r \in \mathbb{Z}$ με τις ιδιότητες*

$$b = qa + r \quad \textit{και} \quad 0 \leq r < a.$$

Απόδειξη. 1) *Υπαρξη*: Θέτουμε $M = \{b - ta \geq 0 | t \in \mathbb{Z}\}$. Ισχύει $M \neq \emptyset$ (αρκεί να θεωρήσουμε $t < 0$ με $|t|$ αρκετά μεγάλο, όπου με $|t|$ συμβολίζουμε την απόλυτη τιμή του t), οπότε από το Αξίωμα 1.1.1 υπάρχει ελάχιστο στοιχείο $r \in M$. Έχουμε $r = b - qa$, για κάποιον ακέραιο q, και θα δείξουμε ότι $r < a$. Αν ίσχυε $r \geq a$, τότε αντικαθιστώντας θα είχαμε $b - (q+1)a \geq 0$, οπότε $b - (q+1)a \in M$. Αυτό είναι άτοπο από τον ορισμό του r, γιατί $r > r - a = b - (q+1)a$.
2) *Μοναδικότητα*: Έστω ότι είχαμε $b = qa + r$, $0 \leq r < a$, όπου $q, r \in \mathbb{Z}$ και $b = q'a + r'$, $0 \leq r' < a$, όπου $q', r' \in \mathbb{Z}$. Τότε λαμβάνουμε

$$(q - q')a = r' - r$$

και

$$-a < r' - r < a.$$

Άρα $-a < (q - q')a < a$ και συνεπώς (αφού $a > 0$) $-1 < q - q' < 1$. Επειδή $q - q \in \mathbb{Z}$, συμπεραίνουμε ότι $q - q' = 0$. Συνεπώς $r' - r = (q - q')a = 0$. ⊤

[1] Η απόδειξη αυτή, όπως και ο Ευκλείδειος Αλγόριθμος, περιέχονται στο έργο *Στοιχεία* του Ευκλείδη.

Σημειώσεις

1. Η απόδειξη της ύπαρξης των q και r στο προηγούμενο Θεώρημα συνίσταται στην αυστηρή διατύπωση της ακόλουθης απλής ιδέας. Ας υποθέσουμε για ευκολία ότι $b > 0$. Αφαιρούμε από τον b τα μη αρνητικά πολλαπλάσια του a, δηλαδή τα 0, a, $2a$, $3a, \ldots$, έτσι ώστε η διαφορά $b - ta$ να παραμένει μη αρνητική. Το τελευταίο τέτοιο πολλαπλάσιο είναι το qa και η διαφορά $b - qa$ είναι το r.

2. Αν παραλείψουμε το $a > 0$ από την υπόθεση του προηγούμενου Θεωρήματος και θεωρήσουμε $a \neq 0$, τότε το μόνο που αλλάζει είναι η ανισότητα του συμπεράσματος που πρέπει να είναι τώρα $0 \leq r < |a|$. (Η απόδειξη έπεται αμέσως από το Θεώρημα: αν ο a είναι αρνητικός, εφαρμόζουμε το Θεώρημα για $-a$ στη θέση του a).

3. Ο φυσικός αριθμός r του αλγορίθμου διαίρεσης ονομάζεται το ***υπόλοιπο*** της διαίρεσης του b με το a.

Μέγιστος κοινός διαιρέτης

Έστω $a, b \in \mathbb{Z}$ με τουλάχιστον έναν διάφορο του μηδενός. Ένας ***μέγιστος κοινός διαιρέτης*** των a και b (συμβολικά $\mu\kappa\delta(a, b)$ ή (a, b)) είναι ένας θετικός ακέραιος d που έχει τις ιδιότητες

1. $d|a$ και $d|b$

2. αν $c \in \mathbb{Z}$ με $c|a$ και $c|b$, τότε $c|d$.

Για παράδειγμα, έχουμε $\mu\kappa\delta(12, 30) = 6$. Παρατηρούμε ότι αν $d = \mu\kappa\delta(a, b)$, τότε κάθε άλλος κοινός διαιρέτης c των a και b είναι τέτοιος ώστε $c \leq d$ λόγω της συνθήκης 2 του ορισμού. Έτσι εξηγείται η ονομασία *μέγιστος* κοινός διαιρέτης.

Στο στάδιο αυτό δεν είναι τελείως σαφές ότι υπάρχει $\mu\kappa\delta$ για κάθε $a, b \in \mathbb{Z}$ με τουλάχιστον έναν διάφορο του μηδενός. Πέρα από την ύπαρξη, το παρακάτω αποτέλεσμα παρέχει μία σημαντική παράσταση του $\mu\kappa\delta$ που θα χρησιμοποιηθεί συχνά στα παρακάτω.

1.2.4 Θεώρημα. *Έστω $a, b \in \mathbb{Z}$ με τουλάχιστον έναν διάφορο του μηδενός. Τότε υπάρχει μοναδικός μέγιστος κοινός διαιρέτης των a και b. Επιπλέον υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $\mu\kappa\delta(a, b) = ax + by$.*

Απόδειξη. *Ύπαρξη*: Θέτουμε $M = \{ax + by | x, y \in \mathbb{Z} \text{ και } ax + by > 0\}$ και παρατηρούμε ότι $M \neq \emptyset$ (γιατί $a^2 + b^2 > 0$). Έστω d το ελάχιστο στοιχείο του M, το οποίο υπάρχει σύμφωνα με το Αξίωμα 1.1.1. Έχουμε $d = ax + by$ για κάποιους $x, y \in \mathbb{Z}$.

Θα αποδείξουμε ότι $d = \mu\kappa\delta(a, b)$. Για τον σκοπό αυτό, δείχνουμε πρώτα ότι $d|a$ και $d|b$. Από το Θεώρημα 1.2.3, υπάρχουν ακέραιοι q, r τέτοιοι ώστε $a = qd+r, 0 \leq r < d$. Έχουμε $r = a-qd = a-q(ax+by) = a(1-qx)+b(-qy)$. Αυτό σημαίνει ότι αν $r \neq 0$, τότε $r \in M$, που όμως είναι άτοπο λόγω του ελαχίστου του d. Άρα $r = 0$ και συνεπώς $d|a$. Όμοια αποδεικνύεται ότι $d|b$. Τώρα έστω $c|a$ και $c|b$. Επειδή έχουμε $d = ax + by$ συμπεραίνουμε ότι $c|d$. Άρα πράγματι ο d είναι ένας $\mu\kappa\delta$ των a και b.

Μοναδικότητα: Αν d και d' ήταν μέγιστοι κοινοί διαιρέτες των a, b, θα είχαμε $d|d'$ (γιατί ο d' είναι ένας $\mu\kappa\delta$ των a, b) και $d'|d$ (γιατί ο d είναι ένας $\mu\kappa\delta$ των a, b). Άρα $d = \pm d'$, και αφού $d, d' > 0$ παίρνουμε $d = d'$. ⊤

Η προηγούμενη απόδειξη παρέχει έναν τρόπο προσδιορισμού του $\mu\kappa\delta$ (ως το ελάχιστο του συνόλου M). Υπάρχει όμως ένας πιο πρακτικός τρόπος (Ευκλείδειος Αλγόριθμος) που περιγράφεται παρακάτω. Πριν από αυτό, όμως, θα αποδείξουμε το Θεμελιώδες Θεώρημα της Αριθμητικής. Για το σκοπό αυτό χρειαζόμαστε το ακόλουθο Λήμμα, που έπεται από το Θεώρημα 1.2.4.

1.2.5 Λήμμα. *Έστω $a, b, p \in \mathbb{Z}$ όπου ο p είναι πρώτος αριθμός. Αν ο p διαιρεί το γινόμενο ab, τότε ο p διαιρεί τουλάχιστον έναν από τους a και b.*

Απόδειξη. Έστω ότι ο p δεν διαιρεί τον a. Αφού ο p είναι πρώτος έχουμε $\mu\kappa\delta(a, p) = 1$. Σύμφωνα με το Θεώρημα 1.2.4 υπάρχουν ακέραιοι x και y τέτοιοι ώστε $1 = ax + py$. Άρα $b = abx + pyb$. Επειδή $p|abx$ και $p|pyb$ προκύπτει ότι $p|abx + pyb$, δηλαδή $p|b$. ⊤

1.2.6 Παρατηρήσεις.

1. Με επαγωγή μπορεί να γενικευθεί το προηγούμενο Λήμμα στην περίπτωση περισσοτέρων παραγόντων: Αν ο p είναι ένας πρώτος αριθμός που διαιρεί το γινόμενο $a_1 \dots a_m$, $(a_i \in \mathbb{Z})$, τότε θα διαιρεί τουλάχιστον έναν από τους a_i. Η απόδειξη αφήνεται σαν άσκηση.

2. Το Λήμμα 1.2.5 είναι ιδιαίτερα χρήσιμο. Μια τυπική εφαρμογή του είναι η απόδειξη ότι ο αριθμός $\sqrt{2}$ είναι άρρητος. Πράγματι, έστω ότι $\sqrt{2} = \frac{m}{n}$, όπου οι m, n είναι θετικοί ακέραιοι. Μπορούμε να υποθέσουμε ότι $\mu\kappa\delta(m, n) = 1$, γιατί διαφορετικά απλοποιούμε το κλάσμα. Έχουμε $m^2 = 2n^2$. Αν $n \neq 1$, τότε σύμφωνα με την Πρόταση 1.2.1 υπάρχει πρώτος p με $p|n$. Τότε $p|m^2$ και άρα $p|m$, από το Λήμμα 1.2.5. Συνεπώς $p|\mu\kappa\delta(m, n)$, δηλαδή $p|1$, που είναι άτοπο. Άρα $n = 1$. Αλλά τότε $\sqrt{2} = m \in \mathbb{Z}$, που είναι άτοπο. Με παρόμοιο τρόπο μπορεί να αποδειχθεί ότι για κάθε θετικό ακέραιο a που δεν είναι τετράγωνο ακεραίου ο αριθμός $\sqrt{a}$ είναι άρρητος (Άσκηση 15).

1.2.7 Θεώρημα (*Θεμελιώδες Θεώρημα της Αριθμητικής*). *Κάθε ακέραιος $a > 1$ γράφεται ως γινόμενο πρώτων αριθμών, $a = p_1 \dots p_m$, p_i πρώτος. Η παράσταση αυτή είναι μοναδική με την εξής έννοια: αν $a = p_1 \dots p_m = q_1 \dots q_n$ (p_i, q_j πρώτοι), τότε $m = n$ και, μετά ενδεχομένως από κάποια αναδιάταξη, έχουμε $p_1 = q_1, \dots, p_m = q_m$.*

Απόδειξη. Έστω $a > 1$ ένας ακέραιος αριθμός. Στην Πρόταση 1.2.1 δείξαμε ότι υπάρχουν πρώτοι αριθμοί $p_1, \dots, p_m$ που έχουν την ιδιότητα $a = p_1 \dots p_m$. Θα δείξουμε τώρα τη μοναδικότητα της παράστασης αυτής. Έστω ότι $a = p_1 \dots p_m = q_1 \dots q_n$, όπου οι p_i, q_j είναι πρώτοι αριθμοί. Μπορούμε να υποθέσουμε ότι $m \leq n$, οπότε εφαρμόζουμε επαγωγή στο m. Για $m = 1$ έχουμε $p_1 = q_1 \dots q_n$ οπότε ο p_1 θα διαιρεί κάποιον από τους q_j σύμφωνα με την Παρατήρηση 1.2.6, έστω τον q_1. Επειδή ο q_1 είναι πρώτος παίρνουμε $p_1 = q_1$. Έτσι $1 = q_2 \dots q_n$, πράγμα που σημαίνει ότι $n = 1$.

Έστω τώρα $m > 1$. Από την ισότητα $p_1 \dots p_m = q_1 \dots q_n$ παίρνουμε όπως πριν, μετά ενδεχομένως από μια αναδιάταξη των q_j, ότι $p_2 \dots p_m = q_2 \dots q_n$. Το ζητούμενο προκύπτει τώρα από την επαγωγική υπόθεση. ⊺

Σύμφωνα με το προηγούμενο Θεώρημα, κάθε ακέραιος $a \neq 0, \pm 1$ έχει μοναδική παράσταση (χωρίς να λαμβάνεται υπόψη η σειρά των παραγόντων) της μορφής $a = \pm p_1^{a_1} \dots p_n^{a_n}$, όπου οι p_i είναι ανά δύο διάφοροι πρώτοι αριθμοί και οι a_i είναι θετικοί ακέραιοι. Η παραγοντοποίηση αυτή καλείται ***ανάλυση του a σε γινόμενο πρώτων*** και οι πρώτοι αριθμοί $p_1, \dots, p_n$ ονομάζονται ***πρώτοι παράγοντες*** του a.

Δύο ακέραιοι a,b ονομάζονται ***σχετικά πρώτοι*** αν $\mu\kappa\delta(a, b) = 1$. Ισοδύναμα, δύο ακέραιοι είναι σχετικά πρώτοι αν δεν έχουν κοινό πρώτο παράγοντα.

Ευκλείδειος Αλγόριθμος

Περιγράφουμε τώρα μία πρακτική διαδικασία που υπολογίζει το $\mu\kappa\delta(a, b)$ και επιπλέον προσδιορίζει ακεραίους x, y έτσι ώστε να ισχύει $\mu\kappa\delta(a, b) = ax + by$ σύμφωνα με το Θεώρημα 1.2.4. Ονομάζεται δε ***Ευκλείδειος αλγόριθμος*** και στηρίζεται στην επαναλαμβανόμενη εφαρμογή της ακόλουθης απλής παρατήρησης:

$$b = aq + r \Rightarrow \mu\kappa\delta(a, b) = \mu\kappa\delta(r, a). \tag{1}$$

Πράγματι, από την ισότητα $b = aq + r$ έπεται ότι $\mu\kappa\delta(a, b) | r$. Έχουμε δηλαδή $\mu\kappa\delta(a, b) | r$ και $\mu\kappa\delta(a, b) | a$, οπότε από τον ορισμό του $\mu\kappa\delta$ παίρνουμε $\mu\kappa\delta(a, b) | \mu\kappa\delta(r, a)$. Με παρόμοιο τρόπο αποδεικνύεται ότι $\mu\kappa\delta(r, a) | \mu\kappa\delta(a, b)$. Επειδή ο $\mu\kappa\delta$ είναι θετικός ακέραιος, από τις δύο τελευταίες σχέσεις προκύπτει ότι $\mu\kappa\delta(a, b) = \mu\kappa\delta(r, a)$.

Παράδειγμα

Έστω $a = 50$ και $b = 240$. Από την ταυτότητα διαίρεσης λαμβάνουμε διαδοχικά

$$\begin{aligned} 240 &= 4 \cdot 50 + 40 \\ 50 &= 1 \cdot 40 + 10 \\ 40 &= 4 \cdot 10 + 0 \end{aligned}$$

Εφαρμόζοντας την (1) σε κάθε μια από τις τρεις ισότητες, έχουμε

$$\mu\kappa\delta(50, 240) = \mu\kappa\delta(40, 50) = \mu\kappa\delta(10, 40) = \mu\kappa\delta(0, 10) = 10.$$

Για να προσδιορίσουμε ακεραίους x, y τέτοιους ώστε $10 = 50x + 240y$ ξεκινάμε από την τελευταία ταυτότητα διαίρεσης που έχει μη μηδενικό υπόλοιπο (την $50 = 1 \cdot 40 + 10$) και εκτελούμε διαδοχικές αντικαταστάσεις "εργαζόμενοι προς τα πάνω". (Η διαδικασία αυτή ονομάζεται ανταναίρεση).

$$\begin{aligned} 10 &= 50 - 1 \cdot 40 = \\ &= 50 - 1 \cdot (240 - 4 \cdot 50) = \\ &= 50 \cdot 5 + 240 \cdot (-1), \end{aligned}$$

οπότε $x = 5$ και $y = -1$.

Από το προηγούμενο παράδειγμα βλέπουμε ότι ο $\mu\kappa\delta$ δύο ακεραίων a και $b (a \neq 0)$ ισούται με το τελευταίο μη μηδενικό υπόλοιπο (r_n) που συναντάμε στον αντίστοιχο Ευκλείδειο αλγόριθμο:

$$\begin{aligned} b &= aq + r, \quad 0 \leq r < a \\ a &= rq_1 + r_1, \quad 0 \leq r_1 < r \\ r &= r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2 \\ &\cdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 \leq r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} + 0. \end{aligned}$$

Πράγματι, εφαρμόζοντας διαδοχικά την (1) έχουμε

$$\mu\kappa\delta(a, b) = \mu\kappa\delta(r, a) = \mu\kappa\delta(r_1, r) = \mu\kappa\delta(r_2, r_1) = \cdots$$

$$= \mu\kappa\delta(r_n, r_{n-1}) = \mu\kappa\delta(0, r_n) = r_n.$$

Εδώ υπάρχει το ερώτημα αν η διαδικασία των διαδοχικών διαιρέσεων τερματίζεται μετά από πεπερασμένο αριθμό επαναλήψεων. Η απάντηση είναι θετική, γιατί τα υπόλοιπα σχηματίζουν μια αυστηρά φθίνουσα ακολουθία φυσικών αριθμών με αρχή το a, δηλαδή έχουμε $a > r > r_1 > \cdots > r_n$.

Για να γράψουμε τον $\mu\kappa\delta(a,b)$ στη μορφή $ax+by$ πρώτα επιλύουμε τις παραπάνω εξισώσεις ως προς τα υπόλοιπα λαμβάνοντας

$$\begin{aligned} r &= b - aq \\ r_1 &= a - rq_1 \\ r_2 &= r - r_1q_2 \\ r_3 &= r_1 - r_2q_3 \\ &\cdots \\ r_{n-2} &= r_{n-4} - r_{n-3}q_{n-2} \\ r_{n-1} &= r_{n-3} - r_{n-2}q_{n-1} \\ r_n &= r_{n-2} - r_{n-1}q_n. \end{aligned}$$

Στη συνέχεια αντικαθιστούμε στην τελευταία εξίσωση τον r_{n-1} από την προτελευταία

$$r_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = r_{n-2}(1 + q_{n-1}q_n) + r_{n-3}(-q_n).$$

Στη νέα εξίσωση αντικαθιστούμε την έκφραση που έχουμε για τον r_{n-2}.

$$r_n = r_{n-2}(1+q_{n-1}q_n)+r_{n-3}(-q_n) = (r_{n-4}-r_{n-3}q_{n-2})(1+q_{n-1}q_n)+r_{n-3}(-q_n).$$

Συνεχίζοντας κατά τον τρόπο αυτό φθάνουμε τελικά σε μια παράσταση της μορφής $r_n = ax + by$.

Παρατηρούμε ότι η παραπάνω μέθοδος παρέχει μια νέα απόδειξη της ύπαρξης του $\mu\kappa\delta(a,b)$ και της ύπαρξης $x, y \in \mathbb{Z}$ που έχουν την ιδιότητα $\mu\kappa\delta(a,b) = ax + by$.

Σημειώνουμε ότι οι x, y δεν είναι αναγκαστικά μοναδικοί , αφού $ax + by = a(x + b) + b(y - a)$. Ισχύει όμως $\mu\kappa\delta(x, y) = 1$ (Άσκηση 9).

Παρατηρήσεις στην ανάλυση ακεραίων σε γινόμενο πρώτων

1) Η ανάλυση ακεραίων σε γινόμενο πρώτων παρέχει έναν άλλο τρόπο υπολογισμού του $\mu\kappa\delta$. Έστω a, b θετικοί ακέραιοι και

$$a = p_1^{a_1} \cdots p_n^{a_n} \quad \text{και} \quad b = p_1^{b_1} \cdots p_n^{b_n} \tag{2}$$

όπου p_i είναι ανά δύο διάφοροι πρώτοι και $a_i, b_i \in \mathbb{N}$. (Και οι δύο παραγοντοποιήσεις περιέχουν τους ίδιους πρώτους $p_1, \ldots, p_n$ γιατί επιτρέπουμε εδώ μηδενικούς

εκθέτες). Παρατηρούμε ότι ισχύει

$$a|b \Leftrightarrow a_i \leq b_i \ \text{ για κάθε } \ i. \tag{3}$$

Πράγματι, η απόδειξη της κατεύθυνσης '$\Leftarrow$' είναι άμεση. Αντίστροφα, έστω $a|b$ και έστω ότι $a_1 > b_1$. Τότε από την (2) παίρνουμε ότι ο $p_1^{a_1-b_1}p_2^{a_2}\dots p_n^{a_n}$ διαιρεί τον $p_2^{b_2}\dots p_n^{b_n}$. Από την Παρατήρηση 1.2.6 1. βλέπουμε ότι $p_1|p_i$ για κάποιο $i \neq 1$. Αυτό είναι άτοπο.

Χρησιμοποιώντας την (3) και τον ορισμό του $\mu\kappa\delta$ μπορούμε να δούμε ότι

$$\mu\kappa\delta(a,b) = p_1^{d_1}\dots p_n^{d_n}, \ \ \text{όπου για κάθε } \ i \ \text{ είναι } \ d_i = \min\{a_i, b_i\}. \tag{4}$$

Για παράδειγμα, αν $a = 2^5 \cdot 3^4 \cdot 5^0$ και $b = 2 \cdot 3^6 \cdot 5^2$, τότε $\mu\kappa\delta(a,b) = 2 \cdot 3^4 \cdot 5^0$. Από την (4) μπορούμε να συνάγουμε χρήσιμες σχέσεις, όπως για παράδειγμα την

$$\mu\kappa\delta(ca, cb) = c \cdot \mu\kappa\delta(a,b). \tag{5}$$

Σημειώνουμε ότι ο τρόπος υπολογισμού του $\mu\kappa\delta$ που δίνεται στην (4) δεν είναι πολύ πρακτικός για μεγάλους αριθμούς γιατί προϋποθέτει τη γνώση αναλύσεων σε γινόμενα πρώτων. Γενικά η εύρεση της ανάλυσης ενός μεγάλου αριθμού σε γινόμενο πρώτων είναι ένας χρονοβόρος υπολογισμός που πολλές φορές καθίσταται πρακτικά αδύνατος, ακόμα και αν χρησιμοποιηθούν ισχυροί υπολογιστές. Σε αυτό ακριβώς το γεγονός στηρίζεται μια αξιόπιστη και διαδεδομένη μέθοδος κρυπτογράφησης μηνυμάτων, η RSA. Την μέθοδο αυτή παρουσιάζουμε συνοπτικά στην Παράγραφο 1.6 παρακάτω.

2) Έστω a, b ακέραιοι από τους οποίους τουλάχιστον ένας είναι μη μηδενικός. Ένα ***ελάχιστο κοινό πολλαπλάσιο*** ($\epsilon\kappa\pi$) των a, b είναι ένας θετικός ακέραιος e που έχει τις ιδιότητες

- $a|e$ και $b|e$
- αν ο $c \in \mathbb{Z}$ είναι τέτοιος ώστε $a|c$ και $b|c$, τότε $e|c$.

Είναι σαφές ότι αν υπάρχει $\epsilon\kappa\pi$ των a, b τότε αυτό είναι μοναδικό. Ας θεωρήσουμε τις παραγοντοποιήσεις των a, b σε γινόμενα πρώτων, $a = \pm p_1^{a_1}\dots p_n^{a_n}$ και $b = \pm p_1^{b_1}\dots p_n^{b_n}$. Για κάθε i θέτουμε $e_i = \max\{a_i, b_i\}$ και ορίζουμε τον θετικό ακέραιο $e = p_1^{e_1}\dots p_n^{e_n}$. Για παράδειγμα, αν $a = 2^5 \cdot 3^4 \cdot 5^0$ και $b = 2 \cdot 3^6 \cdot 5^2$, τότε $e = 2^5 \cdot 3^6 \cdot 5^2$. Χρησιμοποιώντας την (3), βλέπουμε ότι ο e ικανοποιεί τις δύο συνθήκες στον ορισμό του $\epsilon\kappa\pi$. Συνεπώς το $\epsilon\kappa\pi$ των a, b υπάρχει και είναι μοναδικό. Συμβολίζεται δε με $\epsilon\kappa\pi(a,b)$.

Από τη δεύτερη ιδιότητα στον ορισμό του $\epsilon\kappa\pi$ είναι σαφές ότι ανάμεσα στους θετικούς ακεραίους που είναι κοινά πολλαπλάσια των a και b το $\epsilon\kappa\pi(a,b)$ είναι ο ελάχιστος.

Χρησιμοποιώντας τη σχέση $\min\{a_i, b_i\} + \max\{a_i, b_i\} = a_i + b_i$, εύκολα αποδεικνύεται ότι

$$\mu\kappa\delta(a,b)\epsilon\kappa\pi(a,b) = |ab|. \tag{6}$$

1.2.8 Παραδείγματα.

1. Έστω $a, b, c \in \mathbb{Z}$ με $a|bc$. Αν ισχύει $\mu\kappa\delta(a,b) = 1$, τότε $a|c$. (Σύγκρινε με το Λήμμα 1.2.5).
   Επειδή ισχύει $\mu\kappa\delta(a,b) = 1$, υπάρχουν $x, y \in \mathbb{Z}$ με $1 = ax + by$ (Θεώρημα 1.2.4). Παίρνουμε $c = cax + cby$. Έχουμε $a|cax$ και από την υπόθεση έπεται ότι $a|cby$. Άρα ο a θα διαιρεί τον $cax + cby = c$. (Μια άλλη απόδειξη μπορεί να δοθεί χρησιμοποιώντας αναλύσεις σε γινόμενα πρώτων).

2. Έστω $a, m, n \in \mathbb{Z}$ με $m|a$ και $n|a$. Αν $\mu\kappa\delta(m,n) = 1$, τότε $mn|a$.
   Επειδή έχουμε $m|a$ και $n|a$, παίρνουμε $e|a$, όπου $e = \epsilon\kappa\pi(m,n)$. Αλλά από την (6) έχουμε $\epsilon\kappa\pi(m,n) = |mn|$, γιατί $\mu\kappa\delta(m,n) = 1$.

3. Αν $a, b \in \mathbb{Z}$ και $\mu\kappa\delta(a,b) = d$, τότε $\mu\kappa\delta(a/d, b/d) = 1$.
   Αν ο ακέραιος c διαιρεί και τον a/d και τον b/d, τότε ο cd διαιρεί και τον a και τον b. Άρα ο cd θα διαιρεί τον $\mu\kappa\delta(a,b) = d$ που σημαίνει ότι $c = \pm 1$.

4. Αν το γινόμενο δύο σχετικά πρώτων θετικών ακεραίων αριθμών a, b είναι τετράγωνο ακεραίου, τότε οι a, b είναι τετράγωνα ακεραίων.
   Έστω $ab = c^2$ και $a = p_1^{a_1} \dots p_r^{a_r}$, $b = p_1^{b_1} \dots p_r^{b_r}$, $c = p_1^{c_1} \dots p_r^{c_r}$ αναλύσεις σε γινόμενα πρώτων όπως στην (2). Επειδή $\mu\kappa\delta(a,b) = 1$, βλέπουμε ότι για κάθε i το πολύ ένας από τους a_i, b_i είναι μη μηδενικός. Από τη σχέση $(p_1^{a_1} \dots p_r^{a_r})(p_1^{b_1} \dots p_r^{b_r}) = p_1^{2c_1} \dots p_r^{2c_r}$ και τη μοναδικότητα της παραγοντοποίησης στο $\mathbb{Z}$ έχουμε ότι $a_i + b_i = 2c_i$ για κάθε i. Συνεπώς κάθε a_i (και b_i) είναι ίσο είτε με 0 είτε με $2c_i$. Επομένως ο a (και ο b) είναι τετράγωνο ακεραίου.

5. Να βρεθεί ο $\mu\kappa\delta(n^6 - 1, n^{10} - 1)$
   Από τις σχέσεις
   $$\begin{aligned} n^{10} - 1 &= n^4(n^6 - 1) + n^4 - 1, \\ n^6 - 1 &= n^2(n^4 - 1) + n^2 - 1, \\ n^4 - 1 &= (n^2 + 1)(n^2 - 1), \end{aligned}$$
   συνάγουμε ότι
   $$\mu\kappa\delta(n^{10} - 1, n^6 - 1) = \mu\kappa\delta(n^6 - 1, n^4 - 1) = \mu\kappa\delta(n^4 - 1, n^2 - 1) = n^2 - 1.$$
   Γενικά ισχύει $\mu\kappa\delta(n^a - 1, n^b - 1) = n^d - 1$, όπου $d = \mu\kappa\delta(a,b)$ (Άσκηση 17).

6. Έστω $\mu\kappa\delta(m,n)=1$. Να βρεθούν οι δυνατές τιμές για τον $\mu\kappa\delta(m+n, m-n)$.
Θα δείξουμε ότι η απάντηση είναι 1 ή 2. Έστω $d=\mu\kappa\delta(m+n,m-n)$. Επειδή $d|m+n$ και $d|m-n$, παίρνουμε $d|(m+n)+(m-n)$ και $d|(m+n)-(m-n)$, δηλαδή $d|2m$ και $d|2n$. Άρα $d|\mu\kappa\delta(2m,2n)$. Όμως $\mu\kappa\delta(2m,2n)=2\mu\kappa\delta(m,n)$ από την (5) και άρα $d|2$, δηλαδή $d=1$ ή 2. Αποδείξαμε ότι οι πιθανές τιμές του d είναι 1 και 2. Για $m=2$, $n=1$ έχουμε $d=1$, ενώ για $m=3$, $n=1$ έχουμε $d=2$. Συνεπώς οι δυνατές τιμές του d είναι 1 ή 2.

7. Έστω a,b,n θετικοί ακέραιοι. Τότε $a^n|b^n$ αν και μόνο αν $a|b$.
Έστω $a=p_1^{a_1}\dots p_r^{a_r}$ και $b=p_1^{b_1}\dots p_r^{b_r}$ όπου p_i είναι ανά δύο διάφοροι πρώτοι αριθμοί και $a_i,b_i\in\mathbb{N}$. Έχουμε
$$a^n=p_1^{na_1}\dots p_r^{na_r},\quad b^n=p_1^{nb_1}\dots p_r^{nb_r}.$$
Από τη σχέση (3) παίρνουμε
$$a^n|b^n \Leftrightarrow na_i\le nb_i \ \text{ για κάθε } \ i \Leftrightarrow a_i\le b_i \ \text{ για κάθε } \ i \Leftrightarrow a|b.$$

8. Να βρεθούν όλοι οι θετικοί ακέραιοι m, n τέτοιοι ώστε $m^n=n^m$.
Θα δείξουμε ότι τα ζητούμενα ζεύγη (m,n) είναι τα εξής: (2,4), (4,2) και (m,m) όπου m είναι θετικός ακέραος. Μπορούμε να υποθέσουμε ότι $m\ge n\ge 2$. Τότε $n^n|n^m$ δηλαδή $n^n|m^n$. Από την προηγούμενη Εφαρμογή παίρνουμε $n|m$. Έστω $m=an$. Τότε αντικαθιστώντας στην αρχική εξίσωση και λαμβάνοντας n-στες ρίζες παίρνουμε $an=n^a$. Όμως είναι εύκολο να δειχθεί με επαγωγή στο a ότι $an<n^a$ για κάθε $a\ge 3$ και $n\ge 2$ (Άσκηση 1.1.3). Συνεπώς $a=1$ ή 2. Για $a=1$ έχουμε $m=n$ και για $a=2$ έχουμε $2n=n^2$, οπότε $n=2$.

9) Έστω b ένας ακέραιος με $b>1$. Τότε κάθε θετικός ακέραιος n έχει μοναδική παράσταση της μορφής
$$n=a_kb^k+a_{k-1}b^{k-1}+\dots+a_1b+a_0,$$
όπου $k,a_j\in\mathbb{N}$ με $0\le a_j\le b-1$ για $j=0,1,\dots,k$ και $a_k\ne 0$.
Πράγματι, εφαρμόζοντας διαδοχικά τον Αλγόριθμο Διαίρεσης έχουμε
$$\begin{aligned}
n&=bq_0+a_0,\quad 0\le a_0\le b-1\\
q_0&=bq_1+a_1,\quad 0\le a_1\le b-1\\
&\vdots\\
q_{k-2}&=bq_{k-1}+a_{k-1},\quad 0\le a_{k-1}\le b-1\\
q_{k-1}&=b0+a_k,\quad 0<a_k\le b-1.
\end{aligned}$$

Έχουμε $q_0 > q_1 > \ldots$. Υποθέτουμε ότι q_k είναι το πρώτο πηλίκο που ισούται με 0. Στην πρώτη ισότητα $n = bq_0 + a_0$ αντικαθιστούμε το q_0 από τη δεύτερη, στη συνέχεια το q_1 από την τρίτη και ούτω καθ' εξής. Τελικά προκύπτει μία παράσταση της μορφής $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$, όπου $0 \leq a_j \leq b-1$ για $j = 0, 1, \ldots, k$ και $a_k \neq 0$. Για την απόδειξη της μοναδικότητας χρησιμοποιούμε τη δεύτερη μορφή της Μαθηματικής Επαγωγής. Το ζητούμενο είναι προφανές για $n = 1$. Έστω $n > 1$. Υποθέτουμε ότι η μοναδικότητα ισχύει για κάθε θετικό ακέραιο μικρότερο του n. Έστω ότι έχουμε και την παράσταση

$$n = c_l b^l + c_{l-1} b^{l-1} + \cdots + c_1 b + c_0,$$

όπου $l, c_j \in \mathbb{N}$ με $0 \leq c_j \leq b-1$ για $j = 0, 1, \ldots, l$ και $c_l \neq 0$. Έχουμε $a_0 = c_0$, γιατί καθένα από αυτά είναι το υπόλοιπο της διαίρεσης του n με τον b. Το ζητούμενο προκύπτει αν εφαρμοστεί η υπόθεση της επαγωγής στον ακέραιο $(n - a_0)/b$.

Η παραπάνω ισότητα που αποδείξαμε ονομάζεται η ***παράσταση του*** n ***ως προς τη βάση*** b. Για $b = 10$ έχουμε τη συνήθη ***δεκαδική παράσταση*** του n. Για $b = 2$ έχουμε τη ***δυαδική παράσταση*** του n. Επισημαίνουμε ότι η απόδειξη της ύπαρξης που δώσαμε παρέχει έναν αλγόριθμο με τον οποίο μπορούμε να βρούμε τα 'ψηφία' a_i στην παράσταση του n ως προς μια βάση b.

Ασκήσεις 1.2

1) Αν ο p είναι πρώτος αριθμός με $p|a^n$, αποδείξτε ότι $p^n|a^n$.
Υπόδειξη: Λήμμα 1.2.5

2) Αν ο p είναι πρώτος αριθμός με $p|a$ και $p|a^2 + b^2$, αποδείξτε ότι $p|b$.

3) Προσδιορίστε τον $\mu\kappa\delta(36, 210)$, όπως και ακεραίους x, y τέτοιους ώστε $\mu\kappa\delta(36, 210) = 36x + 210y$.

4) Να βρεθεί ο ακέραιος $a > 1$ αν $\mu\kappa\delta(a, a+3) = a$.

5) Αποδείξτε ότι $\mu\kappa\delta(m, n) = \mu\kappa\delta(m + kn, n)$ για κάθε $k \in \mathbb{N}$.

6) Αποδείξτε ότι $6|a$ αν και μόνο αν $\mu\kappa\delta(a, a+2) \neq 1$ και $\mu\kappa\delta(a, a+3) \neq 1$.

7) Αποδείξτε ότι $\mu\kappa\delta(m+n, mn) = 1$ αν $\mu\kappa\delta(m, n) = 1$.

8) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $\mu\kappa\delta(3n+1, 10n+3) = 1$.

9) Αν $d = \mu\kappa\delta(m,n)$ και $d = mx + ny$, αποδείξτε ότι $\mu\kappa\delta(x,y) = 1$.

10) Αποδείξτε τη σχέση (6).

11) Έστω $a, m \in \mathbb{Z}$ με $m > 0$ και $a \neq 1$. Αποδείξτε ότι
$\mu\kappa\delta\left(\dfrac{a^m-1}{a-1}, a-1\right) = \mu\kappa\delta(a-1, m)$.
Υπόδειξη: $\dfrac{a^m-1}{a-1} = (a^{m-1}-1) + (a^{m-2}-1) + \cdots + (a-1) + m$.

12) Αν $a_1, \ldots, a_n \in \mathbb{Z}$ (όχι όλοι μηδέν) ορίζουμε τον $\mu\kappa\delta(a_1, \ldots, a_n)$ ως έναν θετικό ακέραιο d που έχει τις ιδιότητες 1) $d|a_i$ για κάθε i, και 2) αν $c \in \mathbb{Z}$ με $c|a_i$ για κάθε i τότε $c|d$.

   i) Αποδείξτε ότι ο $\mu\kappa\delta(a_1, \ldots, a_n)$ υπάρχει, είναι μοναδικός και επιπλέον υπάρχουν $x_i \in \mathbb{Z}$ με $\mu\kappa\delta(a_1, \ldots, a_n) = a_1x_1 + \cdots + a_nx_n$.

   ii) Αποδείξτε ότι αν $a_i \neq 0$ για κάθε i και $n \geq 3$ τότε $\mu\kappa\delta(a_1, \ldots, a_n) = \mu\kappa\delta(a_1, \ldots, a_{n-2}, \mu\kappa\delta(a_{n-1}, a_n)) = \mu\kappa\delta(a_1, \mu\kappa\delta(a_2, \ldots, a_n))$.

   iii) Υπολογίστε τον $\mu\kappa\delta(135, 170, 205, 310)$.

   iv) Γενικεύστε τη σχέση (4).

13) Αν $a_1, \ldots, a_n \in \mathbb{Z}$ είναι μη μηδενικοί ακέραιοι, ορίζουμε το $\epsilon\kappa\pi(a_1, \ldots, a_n)$ ως έναν θετικό ακέραιο e που έχει τις ιδιότητες 1) $a_i|e$ για κάθε i, και 2) αν $c \in \mathbb{Z}$ με $a_i|c$ για κάθε i τότε $e|c$.

   i) Αποδείξτε ότι το $\epsilon\kappa\pi(a_1, \ldots, a_n)$ υπάρχει, είναι μοναδικό και ανάμεσα στα θετικά κοινά πολλαπλάσια των $a_1, \ldots, a_n$ είναι το ελάχιστο.

   ii) Αν τα a_i είναι μη μηδενικά και $n \geq 3$, αποδείξτε ότι $\epsilon\kappa\pi(a_1, \ldots, a_n) = \epsilon\kappa\pi(a_1, \ldots, a_{n-2}, \epsilon\kappa\pi(a_{n-1}, a_n)) = \epsilon\kappa\pi(a_1, \epsilon\kappa\pi(a_2, \ldots, a_n))$.

   iii) Αποδείξτε ότι $\epsilon\kappa\pi(a_1, a_2, a_3) = \dfrac{a_1a_2a_3\mu\kappa\delta(a_1, a_2, a_3)}{\mu\kappa\delta(a_1, a_2)\mu\kappa\delta(a_2, a_3)\mu\kappa\delta(a_1, a_3)}$
   Υπόδειξη: Για κάθε αριθμούς a, b, c ο $\max\{a, b, c\}$ είναι ίσος με

$$a + b + c - \min\{a, b\} - \min\{b, c\} - \min\{a, c\} + \min\{a, b, c\}.$$

14) Προσδιορίστε όλους τους θετικούς ακεραίους m, n ώστε $\epsilon\kappa\pi(m, n) = 100$.

15) Αποδείξτε ότι για κάθε θετικό ακέραιο a που δεν είναι τετράγωνο ακεραίου το $\sqrt{a}$ είναι άρρητος.

16) Ποιά είναι τα ελάχιστα στοιχεία των παρακάτω συνόλων;

i) $\{24a + 36b > 0 | a, b \in \mathbb{Z}\}$

ii) $\{24a + 36b + 8c > 0 | a, b, c \in \mathbb{Z}\}$

iii) $\{a > 0 | a$ είναι πολλαπλάσιο του 24 και του $36\}$.

17) Αποδείξτε ότι $\mu\kappa\delta(n^a - 1, n^b - 1) = n^d - 1$, όπου $d = \mu\kappa\delta(a, b)$, a, b, n είναι θετικοί ακέραιοι, $n > 1$.

18) Έστω $a, b \in \mathbb{Z}$, $a > 1$. Αποδείξτε ότι υπάρχουν μοναδικά $q, r \in \mathbb{Z}$ με $b = qa + r$ και $-a/2 \leq r < a/2$.

19) i) Αποδείξτε ότι κάθε πρώτος αριθμός διάφορος του 2 είναι της μορφής $4n + 1$ ή $4n + 3$, $n \in \mathbb{N}$.

ii) Αποδείξτε ότι κάθε φυσικός αριθμός της μορφής $4n + 3$ έχει έναν τουλάχιστον πρώτο διαιρέτη της μορφής $4n + 3$.

iii) Αποδείξτε ότι υπάρχουν άπειροι πρώτοι αριθμοί της μορφής $4n + 3$, όπου $n \in \mathbb{N}$.
Υπόδειξη: Τροποποιήστε κατάλληλα την απόδειξη του Ευκλείδη ότι υπάρχουν άπειροι πρώτοι αριθμοί θεωρώντας τον αριθμό $4a_1 \dots a_m + 3$, όπου $\{3, a_1, \dots, a_m\}$ είναι το σύνολο των πρώτων της μορφής $4n + 3$.
Σημείωση: Ένα φημισμένο και δύσκολο θεώρημα της Θεωρίας Αριθμών είναι αυτό του Dirichlet, που λέει ότι σε κάθε αριθμητική πρόοδο $an + b$, $n \in \mathbb{N}$, όπου $\mu\kappa\delta(a, b) = 1$, υπάρχουν άπειροι πρώτοι αριθμοί.

20) Αν a, n είναι θετικοί ακέραιοι, τέτοιοι ώστε $n > 1$ και ο $a^n - 1$ είναι πρώτος, αποδείξτε ότι $a = 2$ και ο n είναι πρώτος.

21) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ο ακέραιος $5^{2n+1} + 6^{2n+1}$ είναι πολλαπλάσιο του 11.

22) Να βρεθούν όλοι οι πρώτοι p ώστε ο $p + 5$ να είναι πρώτος.

23) Αποδείξτε ότι υπάρχει μοναδική τριάδα της μορφής $(p, p + 2, p + 4)$, όπου οι $p, p + 2, p + 4$ είναι πρώτοι αριθμοί.
Σημείωση. Παραμένει μέχρι σήμερα ανοικτό το ερώτημα αν υπάρχουν άπειρα ζεύγη της μορφής $(p, p + 2)$, όπου οι $p, p + 2$ είναι πρώτοι αριθμοί.

24) Η άσκηση αυτή δίνει ένα παράδειγμα υποσυνόλου του $\mathbb{N}$ όπου, ενώ κάθε στοιχείο γράφεται ως γινόμενο "πρώτων", η γραφή δεν είναι μοναδική, και έτσι δεν ισχύει σε αυτό το ανάλογο Θεμελιώδες Θεώρημα της Αριθμητικής. Έστω $2\mathbb{Z}$ το σύνολο των αρτίων ακεραίων. Ένα στοιχείο q του $2\mathbb{Z}$ ονομάζεται "πρώτο", αν δεν υπάρχουν $a, b \in 2\mathbb{Z}$ με $q = ab$. Για παράδειγμα, τα

$2, 6, 10, 30$ είναι πρώτα στοιχεία του $2\mathbb{Z}$. Αποδείξτε ότι κάθε μη μηδενικό στοιχείο του $2\mathbb{Z}$ γράφεται ως γινόμενο πρώτων στοιχείων. Παρατηρήστε ότι το $60 = 2 \cdot 30 = 6 \cdot 10$ γράφεται κατά δύο διαφορετικούς τρόπους ως γινόμενο πρώτων στοιχείων του $2\mathbb{Z}$.

25) Αν $\mu\kappa\delta(m, n) = 1$, ποιές είναι οι δυνατές τιμές για τον $\mu\kappa\delta(m^2+n^2, m+n)$;

26) Εξετάστε ποιές από τις παρακάτω συνεπαγωγές είναι σωστές.
Έστω $a, b \in \mathbb{Z}$ και $n \in \mathbb{N}$.

- $a|b^n \Rightarrow a|b$
- $a^n|b^n \Rightarrow a|b$
- $a^n|b \Rightarrow a|b$
- $a^3|b^2 \Rightarrow a|b$

27) Έστω a, m, n θετικοί ακέραιοι με $m < n$.

i) Αποδείξτε ότι $a^{2^m} + 1 | a^{2^n} - 1$.

ii) Αποδείξτε ότι $\mu\kappa\delta(a^{2^m} + 1, a^{2^n} + 1) = 1$ ή 2.

iii) Χρησιμοποιώντας το ii) αποδείξτε ότι υπάρχουν άπειροι πρώτοι.

28) i) Αποδείξτε ότι η εξίσωση $x^2 - y^2 = 2$ δεν έχει λύση με $x, y \in \mathbb{Z}$.

ii) Λύστε την εξίσωση $\dfrac{1}{x} + \dfrac{1}{y} = \dfrac{1}{7}$ όπου $x, y \in \mathbb{Z}$.

(*Υπόδειξη*: Παραγοντοποιήστε).

29) Δείξτε ότι για κάθε $n \in \mathbb{N}$ υπάρχει p πρώτος με $n < p \leq n! + 1$ και κατά συνέπεια υπάρχουν άπειροι πρώτοι.

30) Δείξτε ότι για για κάθε $n \in \mathbb{N}$, $n \geq 2$, δεν υπάρχει πρώτος αριθμός p με $n! + 2 \leq p \leq n! + n$.

31) Για την ακολουθία Fibonacci (Άσκηση 1.1.5) δείξτε ότι $\mu\kappa\delta(f_n, f_{n+1}) = 1$ για κάθε $n \in \mathbb{N}$.

32) Για την ακολουθία Fibonacci (Άσκηση 1.1.5) αποδείξτε ότι το f_n διαιρείται με το 3 αν και μόνο αν το n διαιρείται με το 4.

33) Έστω m, n δύο θετικοί ακέραιοι. Αποδείξτε ότι
$\mu\kappa\delta(m, n) = \mu\kappa\delta(m + n, \epsilon\kappa\pi(m, n))$.

34) Αποδείξετε ότι για κάθε ακέραιο $n > 1$, ο ρητός αριθμός $1 + 1/2 + 1/3 + \cdots + 1/n$ δεν είναι ακέραιος.
Υπόδειξη: Έστω ότι $1+1/2+1/3+\cdots+1/n = q \in \mathbb{N}$. Έστω 2^α η μέγιστη δύναμη του 2 που είναι μικρότερη ή ίση από το n. Έστω r το γινόμενο των μέγιστων δυνάμεων των περιττών πρώτων που είναι μικρότερες ή ίσες από το n. Πολλαπλασιάστε με $2^{\alpha-1}r$ για να φθάσετε σε άτοπο.

1.3 Ισοτιμίες

Συχνά συμβαίνει οι λύσεις προβλημάτων που αφορούν ακεραίους να εξαρτώνται μόνο από υπόλοιπα διαιρέσεων. Ας θεωρήσουμε ένα πολύ απλό παράδειγμα. Η απάντηση στο ερώτημα 'ποιά ημέρα της εβδομάδας θα είναι 7001 ημέρες από την επόμενη Κυριακή' φαίνεται αμέσως αν σκεφθούμε ότι οι ημέρες της εβδομάδας επαναλαμβάνονται με περίοδο 7 και ότι $7001 = 7 \cdot 1000 + 1$. Συνεπώς η απάντηση είναι Δευτέρα. Στην ίδια απάντηση θα φθάναμε αν στη θέση του 7001 είχαμε 8, 15 ή οποιονδήποτε φυσικό αριθμό της μορφής $7m + 1$.

1.3.1 Ορισμός. *Έστω m ένας ακέραιος. Δύο ακέραιοι a και b θα λέγονται* ***ισότιμοι*** *modulo m (ή* ***ισοϋπόλοιποι*** *modulo m) αν ο m διαιρεί τη διαφορά $a - b$. Στην περίπτωση αυτή γράφουμε $a \equiv b \mod m$, δηλαδή*[1]

$$a \equiv b \mod m \quad \Leftrightarrow \quad m|a - b.$$

Για παράδειγμα, έχουμε $7001 \equiv 1 \mod 7$ αφού ο 7 διαιρεί τον $7001 - 1 = 7000$. Επίσης $14 \equiv -2 \mod 8$ αφού ο 8 διαιρεί τον $14 - (-2) = 16$.

Επειδή ισχύει $m|a - b$ αν και μόνο αν $-m|a - b$, μπορούμε να θεωρήσουμε στον παραπάνω ορισμό ότι ο m είναι μη αρνητικός.

Παρατηρούμε ότι αν $m = 0$, τότε $a \equiv b \mod m$ αν και μόνο αν $0|a - b$, δηλαδή αν και μόνο αν $a = b$. Άρα δύο ακέραιοι είναι ισότιμοι modulo 0 αν και μόνο αν είναι ίσοι.

1.3.2 Πρόταση. *Έστω m ένας θετικός ακέραιος και a, b δύο ακέραιοι. Τότε:*

1) Ισχύει $a \equiv b \mod m$ αν και μόνο αν οι a και b αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν με το m.

2) Υπάρχει ακριβώς ένας ακέραιος r με $a \equiv r \mod m$ και $0 \leq r < m$.

Απόδειξη. 1) Από τον Αλγόριθμο Διαίρεσης έχουμε

$$a = mq_1 + r_1, \quad 0 \leq r_1 < m$$
$$b = mq_2 + r_2, \quad 0 \leq r_2 < m,$$

[1] Η έννοια της ισοτιμίας είναι εξαιρετικά χρήσιμη στη Θεωρία Αριθμών αλλά και στην Άλγεβρα όπου εμφανίζεται πιο γενικά υπό τη μορφή των δομών πηλίκο. Αναπτύχθηκε δε συστηματικά από τον Gauss στο έργο του *Disquitiones Arithmeticae* (1801). Εκεί εισήχθηκε ο συμβολισμός $a \equiv b \mod m$ ο οποίος επικράτησε από τότε. Είναι αξιοσημείωτο ότι, αν και έχουν περάσει περισσότερα από 200 χρόνια από την κυκλοφορία του *Disquitiones Arithmeticae*, το βιβλίο αυτό θεωρείται ' σύγχρονο ' και διαβάζεται με ευκολία.

όπου $q_1, q_2, r_1, r_2 \in \mathbb{Z}$. Τότε

$$a - b = m(q_1 - q_2) + r_1 - r_2$$

και από τις ανισότητες παίρνουμε

$$|r_1 - r_2| < m.$$

Επειδή $m|m(q_1 - q_2)$, η προηγούμενη ισότητα δίνει: $m|a - b$ αν και μόνο αν $m|r_1 - r_2$. Επειδή όμως $|r_1 - r_2| < m$, παίρνουμε: $m|r_1 - r_2$ αν και μόνο αν $r_1 - r_2 = 0$. Τελικά, $m|a - b$ αν και μόνο αν $r_1 - r_2 = 0$.
2) Ένας r που ικανοποιεί τις συνθήκες της πρότασης είναι το υπόλοιπο της διαίρεσης του a με τον m. Για τη μοναδικότητα παρατηρούμε ότι αν $a \equiv r \mod m$, $0 \leq r < m$ και $a \equiv s \mod m$, $0 \leq s < m$, τότε από το 1) και τη μοναδικότητα του υπολοίπου διαίρεσης με το m προκύπτει $r = s$. ⊤

1.3.3 Σημείωση. *Παρατηρούμε ότι ισχύουν οι παρακάτω ιδιότητες.*

1) $a \equiv a \mod m$ για κάθε $a \in \mathbb{Z}$, αφού $m|a - a$ για κάθε $a \in \mathbb{Z}$.

2) αν $a \equiv b \mod m$, τότε $b \equiv a \mod m$, αφού από $m|a - b$ έπεται ότι $m| - (a - b)$, δηλαδή $m|b - a$.

3) αν $a \equiv b \mod m$ και $b \equiv c \mod m$, τότε $a \equiv c \mod m$, αφού από τις σχέσεις $m|a - b$ και $m|b - c$ έπεται ότι $m|(a - b) + (b - c)$, δηλαδή $m|a - c$.

Δείχνουμε τώρα ότι οι ισοτιμίες ‘ συμπεριφέρονται καλά ’ σε σχέση με την πρόσθεση και τον πολλαπλασιασμό του $\mathbb{Z}$.

1.3.4 Πρόταση. *Αν $a \equiv b \mod m$ και $c \equiv d \mod m$, τότε*

$$a + c \equiv b + d \mod m \quad \textit{και} \quad ac \equiv bd \mod m$$

Απόδειξη. Από την υπόθεση έχουμε $m|a - b$ και $m|c - d$. Επομένως, $m|(a - b) + (c - d)$, δηλαδή $m|(a + c) - (b + d)$ που σημαίνει ότι $a + c \equiv b + d \mod m$.
Για την άλλη σχέση, παρατηρούμε ότι $ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d)$, που είναι πολλαπλάσιο του m αφού $m|a - b$ και $m|c - d$. Άρα $ac \equiv bd \mod m$. ⊤

1.3.5 Πόρισμα. *Αν $a \equiv b \mod m$, τότε*

$$a + c \equiv b + c \mod m, \quad ac \equiv bc \mod m \quad \textit{και} \quad a^n \equiv b^n \mod m$$

για κάθε φυσικό αριθμό n.

1.3.6 Σημείωση. Από τα προηγούμενα συνάγουμε ότι μπορούμε να χειριστούμε τις ισοτιμίες modulo m σαν ισότητες. Μπορούμε να πολλαπλασιάσουμε ή να προσθέσουμε κατά μέλη δύο ισοτιμίες. Επίσης μπορούμε να υψώσουμε τα μέλη μιας ισοτιμίας σε φυσική δύναμη. Όμως χρειάζεται προσοχή στη 'διαίρεση' όπως εξηγούμε αμέσως παρακάτω.

Νόμος Διαγραφής

Δεν αληθεύει γενικά ότι από $ac \equiv bc \mod m$ έπεται ότι $a = b \mod m$. Για πράδειγμα έχουμε $7 \cdot 2 \equiv 4 \cdot 2 \mod 6$, αλλά όχι $7 \equiv 4 \mod 6$. Αν όμως ισχύει $\mu\kappa\delta(c, m) = 1$, τότε από την ισοτιμία $ac \equiv bc \mod m$ συμπεραίνουμε ότι $a \equiv b \mod m$ σύμφωνα με το Παράδειγμα 1.2.8 1). Σχετικά ισχύει το εξής αποτέλεσμα.

1.3.7 Πρόταση.

1) Αν $ac \equiv bc \mod (cm)$, όπου c είναι διάφορος του μηδενός, τότε

$$a \equiv b \mod m.$$

2) Αν $ac \equiv bc \mod m$, όπου τουλάχιστον ένας από τους c, m είναι μη μηδενικός, τότε

$$a \equiv b \mod \frac{m}{d},$$

όπου $d = \mu\kappa\delta(c, m)$.

Απόδειξη. 1) Αν $ac - bc = ecm$ με $c \neq 0$, τότε $a - b = em$.
2) Από την υπόθεση έχουμε $m|c(a-b)$. Άρα $\frac{m}{d}\Big|\frac{c}{d}(a-b)$. Όμως $\mu\kappa\delta\left(\frac{m}{d}, \frac{c}{d}\right) = 1$ και άρα $\frac{m}{d}\Big|a - b$. ⊤

Είναι φανερό ότι ισχύουν τα αντίστροφα των 1) και 2) στην προηγούμενη Πρόταση, δηλαδή αν $a \equiv b \mod m$, τότε $ac \equiv bc \mod (cm)$, και αν $a \equiv b \mod \frac{m}{d}$, όπου $d = \mu\kappa\delta(c, m)$, τότε $ac \equiv bc \mod m$.

1.3.8 Εφαρμογές.

1. Θα αποδείξουμε ότι δεν υπάρχει ακέραιος της μορφής $4n + 3$ $(n \in \mathbb{N})$ που να είναι το άθροισμα δύο τετραγώνων ακεραίων.
   Έστω $a \in \mathbb{N}$ της μορφής $4n+3$ και έστω $x, y \in \mathbb{Z}$ με $a = x^2 + y^2$. Από τον Αλγόριθμο Διαίρεσης με το 4, έπεται ότι κάθε ακέραιος είναι της μορφής $4n + r$, όπου $r = 0, 1, 2, 3$. Επειδή $4n + r \equiv r \mod 4$, παίρνουμε $x \equiv 0$ ή 1 ή 2 ή $3 \mod 4$. Επομένως $x^2 \equiv 0$ ή 1 ή 4 ή $9 \mod 4$. Αλλά $4 \equiv 0 \mod 4$ και $9 \equiv 1 \mod 4$. Άρα $x^2 \equiv 0$ ή $1 \mod 4$. Όμοια έχουμε $y^2 \equiv 0$

ή 1 mod 4. Άρα έχουμε $x^2 + y^2 \equiv 0$ ή 1 ή 2 mod 4, δηλαδή $a \equiv 0$ ή 1 ή 2 mod 4. Αυτό όμως είναι άτοπο γιατί από την υπόθεση έχουμε $a \equiv 3$ mod 4.
Στην Παράγραφο 2.12 αποδεικνύεται ένα Θεώρημα που χαρακτηρίζει τους φυσικούς αριθμους που είναι άθροισμα δύο τετραγώνων ακεραίων.

2. Για κάθε $n \in \mathbb{N}$, ο ακέραιος $3^{3n} - 5^n$ είναι πολλαπλάσιος του 11.
Επειδή $3^3 = 27 \equiv 5 \mod 11$, έχουμε $3^{3n} = (3^3)^n = 27^n \equiv 5^n \mod 11$. Άρα $3^{3n} - 5^n \equiv 0 \mod 11$.

3. Θα αποδείξουμε ότι δεν υπάρχουν ακέραιοι x, y με $x^2 - 5y^2 = 13$.
Έστω ότι υπάρχουν τέτοιοι ακέραιοι. Τότε έχουμε $x^2 - 5y^2 \equiv 13 \mod 5$. Όμως $5y^2 \equiv 0 \mod 5$ και $13 \equiv 3 \mod 5$. Άρα $x^2 \equiv 3 \mod 5$. Αυτό όμως είναι άτοπο, αφού για κάθε ακέραιο x έχουμε $x \equiv 0, 1, 2, 3$ ή $4 \mod 5$ και κατά συνέπεια $x^2 \equiv 0, 1, 4, 9$ ή $16 \mod 5$, δηλαδή $x^2 \equiv 0, 1$ ή $4 \mod 5$.

4. Να βρεθούν όλοι οι πρώτοι p ώστε οι $p + 10$ και $p + 14$ να είναι πρώτοι.
Δοκιμάζοντας μερικούς μικρούς πρώτους αριθμούς, βλέπουμε ότι για $p = 3$ οι 13 και 17 είναι πρώτοι. Θα δείξουμε τώρα ότι δεν υπάρχει άλλος p. Έστω p πρώτος με $p > 3$. Τότε $p \equiv 1$ ή $2 \mod 3$. Αν $p \equiv 1 \mod 3$, τότε $p + 14 \equiv 15 \mod 3$, δηλαδή $p + 14 \equiv 0 \mod 3$, και επομένως ο $p + 14$ δεν είναι πρώτος αφού είναι πολλαπλάσιο του 3 και διάφορος του 3. Αν $p \equiv 2 \mod 3$, τότε $p + 10 \equiv 12 \mod 3$, δηλαδή $p + 10 \equiv 0 \mod 3$, και κατά συνέπεια ο $p + 10$ δεν είναι πρώτος.

5. Για κάθε περιττό $n \in \mathbb{N}$ ο $1^n + 2^n + \cdots + (n-1)^n$ είναι πολλαπλάσιος του n.
Παρατηρούμε ότι το άθροισμα μπορεί να γραφεί

$$1^n+2^n+\cdots+(n-1)^n = \sum_{k=1}^{k=\frac{n-1}{2}} k^n + \sum_{k=1}^{k=\frac{n-1}{2}} (n-k)^n = \sum_{k=1}^{k=\frac{n-1}{2}} (k^n+(n-k)^n).$$

Έχουμε $n - k \equiv -k \mod n$ και άρα $(n-k)^n \equiv (-k)^n \equiv (-1)^n k^n \equiv -k^n \mod n$, γιατί ο n είναι περιττός. Αρα $k^n + (n-k)^n \equiv 0 \mod n$, και κατά συνέπεια $1^n + 2^n + \cdots + (n-1)^n \equiv 0 \mod n$.

6. **Πυθαγόρειες τριάδες.** Χρησιμοποιώντας τη μοναδικότητα της ανάλυσης ακεραίων σε γινόμενα πρώτων αλλά και απλές ιδιότητες ισοτιμιών θα προσδιορίσουμε όλους τους ακεραίους x, y, z που έχουν την ιδιότητα $x^2 + y^2 = z^2$.

Αν η τριάδα (x, y, z) είναι μια λύση της εξίσωσης $x^2 + y^2 = z^2$, τότε και οι $(\pm x, \pm y, \pm z)$ είναι λύσεις και επομένως μπορούμε να υποθέσουμε ότι οι x, y, z είναι μη αρνητικοί. Παρατηρούμε ότι αν $d = \mu\kappa\delta(x, y, z)$ (Άσκηση 1.2.12), τότε $(x/d)^2 + (y/d)^2 = (z/d)^2$ και $\mu\kappa\delta(x/d, y/d, z/d) = 1$. Επομένως κάθε λύση της αρχικής εξίσωσης θα είναι της μορφής (dx_0, dy_0, dz_0), όπου d είναι θετικός ακέραιος και (x_0, y_0, z_0) είναι μια λύση με $\mu\kappa\delta(x_0, y_0, z_0) = 1$. Από τώρα και στο εξής υποθέτουμε ότι $\mu\kappa\delta(x, y, z) = 1$. Στην περίπτωση αυτή, οι x, y, z είναι ανά δύο σχετικά πρώτοι. Ιδιαίτερα, ακριβώς ένας από τους x, y, z είναι άρτιος.

Παρατηρούμε ότι ο z δεν είναι άρτιος. Πράγματι, αν ο z ήταν άρτιος, τότε οι x, y θα ήταν περιττοί. Αυτό είναι άτοπο αφού από τη μια μεριά έχουμε $z^2 \equiv 0 \mod 4$ και από την άλλη $z^2 = x^2 + y^2 \equiv 1 + 1 \equiv 2 \mod 4$.

Συνεπώς μπορούμε να υποθέσουμε ότι: x περιττός, y άρτιος και z περιττός.

Έχουμε

$$y^2 = z^2 - x^2 = (z - x)(z + x).$$

Ισχυριζόμαστε ότι $\mu\kappa\delta(z-x, z+x) = 2$. Πράγματι, αν $d = \mu\kappa\delta(z-x, z+x)$, τότε $d|(z - x) + (z + x) = 2z$ και $d|(z - x) - (z + x) = -2x$, οπότε $d|\mu\kappa\delta(2z, 2x) = 2\mu\kappa\delta(z, x) = 2$. Επειδή όμως οι $z - x, z + x$ είναι άρτιοι, παίρνουμε $d = 2$.

Θέτουμε $a = (z+x)/2$, $b = y/2$, $c = (z-x)/2$ (που είναι μη αρνητικοί ακέραιοι) οπότε $b^2 = ac$. Επειδή $\mu\kappa\delta(z - x, z + x) = 2$, έχουμε $\mu\kappa\delta(c, a) = 1$, οπότε, σύμφωνα με την Εφαρμογή 1.2.8 4), οι a, c είναι τετράγωνα ακεραίων, $a = u^2$, $c = v^2$. Άρα $z + x = 2u^2$, $z - x = 2v^2$, $y^2 = (2u^2)(2v^2)$ και επομένως

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2.$$

Επιπλέον ισχύει $u \geq v$, $\mu\kappa\delta(u, v) = 1$, αφού $\mu\kappa\delta(x, y, z) = 1$.

Αποδείξαμε ότι κάθε λύση της αρχικής εξίσωσης $x^2+y^2 = z^2$ με $x, y, z \in \mathbb{N}$ (χωρίς τον περιορισμό $\mu\kappa\delta(x, y, z) = 1$) είναι της μορφής

$$x = d(u^2 - v^2)+, \quad y = 2duv, \quad z = d(u^2 + v^2),$$

όπου $d, u, v \in \mathbb{N}$, $u \geq v$ και $\mu\kappa\delta(u, v) = 1$. Αντίστροφα, με έναν εύκολο υπολογισμό επαληθεύεται ότι οι παραπάνω ακέραιοι x, y, z είναι λύσεις.

Οι τριάδες ακεραίων της μορφής $(d(u^2 - v^2), 2duv, d(u^2 + v^2))$, όπου $\mu\kappa\delta(u, v) = 1$, ονομάζονται '***Πυθαγόρειες τριάδες***'.

7. **Θεώρημα του Fermat[2] για $n = 4$.** Με τη βοήθεια των Πυθαγορείων τριάδων θα αποδείξουμε εδώ ότι δεν υπάρχουν μη μηδενικοί ακέραιοι x, y, z που έχουν την ιδιότητα $x^4 + y^4 = z^4$.
Για τον σκοπό αυτό θα αποδείξουμε ότι η εξίσωση

$$x^4 + y^4 = z^2 \qquad (*)$$

δεν έχει θετικές ακέραιες λύσεις. Αυτό αρκεί γιατί αν (a, b, c) είναι λύση της $x^4 + y^4 = z^4$, τότε (a, b, c^2) είναι λύση της $x^4 + y^4 = z^2$.

Έστω ότι υπάρχει λύση (x, y, z) της (*) με $x, y, z > 0$ θετικοί ακέραιοι. Επιλέγουμε μια λύση με z ελάχιστο. Τότε $\mu\kappa\delta(x, y, z) = 1$ γιατί αν p είναι ένας πρώτος κοινός διαιρέτης των x, y, z ο p^4 διαιρεί τον $x^4 + y^4$ και άρα ο p^2 διαιρεί τον z. Αλλά τότε μία λύση της (*) είναι η $(x/p, y/p, z/p^2)$, πράγμα άτοπο αφού $z/p^2 < z$.

Γράφοντας $(x^2)^2 + (y^2)^2 = z^2$, από την προηγούμενη Εφαρμογή παίρνουμε

$$x^2 = u^2 - \nu^2, \quad y^2 = 2u\nu, \quad z = u^2 + \nu^2$$

όπου u, ν είναι θετικοί ακέραιοι και $\mu\kappa\delta(u, \nu) = 1$. Επειδή $y^2 = 2u\nu$ έχουμε $4|y^2$ και άρα τουλάχιστον ένας από τους u, ν είναι άρτιος. Αν ο u είναι άρτιος, ο ν είναι περιττός και κατά συνέπεια $x^2 = u^2 - \nu^2 \equiv -1 \mod 4$, που είναι άτοπο (βλ. Εφαρμογή 1). Επομένως ο u είναι περιττός και ο ν άρτιος, $\nu = 2\nu'$. Επειδή $y^2 = 4u\nu'$ και $\mu\kappa\delta(u, \nu') = 1$, οι u, ν' είναι τετράγωνα ακεραίων: $u = a^2$, $\nu' = b^2$ (Παράδειγμα 1.1.8 4). Εφαρμόζουμε πάλι τις Πυθαγόρειες τριάδες, αυτή τη φορά στην εξίσωση $x^2 + \nu^2 = u^2$. Παρατηρούμε ότι ο ν είναι άρτιος και οι x, u περιττοί και ότι $\mu\kappa\delta(x, \nu, u) = 1$. Επομένως υπάρχουν θετικοί ακέραιοι c, d με $\mu\kappa\delta(c, d) = 1$ τέτοιοι ώστε

$$x = c^2 - d^2, \quad \nu = 2cd, \quad u = c^2 + d^2.$$

Επειδή $b^2 = \nu' = cd$, συμπεραίνουμε ότι οι c, d είναι τετράγωνα ακεραίων, $c = e^2$, $d = f^2$. Έχουμε

$$e^4 + f^4 = a^2,$$

[2] Σύμφωνα με το 'Θεώρημα του Fermat' , η εξίσωση $x^n + y^n = z^n$ δεν έχει θετικές ακέραιες λύσεις όταν $n \geq 3$. Ο Fermat (περί το 1637) πίστευε ότι βρήκε μια απόδειξη, αλλά δεν άφησε κανένα σχετικό γραπτό έργο. Σήμερα επικρατεί η άποψη ότι ο Fermat έκανε λάθος. Η προσπάθεια απόδειξης του ισχυρισμού του Fermat οδήγησε στην ανάπτυξη νέων σημαντικών κλάδων των Μαθηματικών όπως είναι η Αλγεβρική Θεωρία Αριθμών και η Μεταθετική Άλγεβρα. Τελικά ο ισχυρισμός του Fermat αποδείχτηκε από τον A. Wiles (1995). Η απόδειξη είναι εξαιρετικά δύσκολη και για την εργασία αυτή απενεμήθη στον Wiles το Cole Prize, που είναι μια από τις ανώτατες διακρίσεις στα Μαθηματικά.

δηλαδή μια λύση της αρχικής εξίσωσης είναι η (e, f, a). Αλλά έχουμε $z = u^2 + \nu^2 = a^4 + 4b^4 > a^4 \geq a$, δηλαδή $z > a$. Αυτό είναι άτοπο από τον ορισμό του z. Η απόδειξη είναι πλήρης.

Η τεχνική που ακολουθήσαμε στην παραπάνω απόδειξη, σύμφωνα με την οποία κατασκευάσαμε μια λύση που είναι 'μικρότερη' από μια 'ελάχιστη', οφείλεται στον Fermat και ονομάζεται η '***μέθοδος της καθόδου***'.

8. **Οι κωδικοί ISBN.** Κάθε δημοσιευμένο βιβλίο περιέχει έναν κωδικό, ο οποίος αποτελείται από 9 ψηφία και έναν ακέραιο μεταξύ 0 και 10. Ο κωδικός αυτός ονομάζεται ISBN (International Standard Book Number). Τα πρώτα 9 ψηφία παρέχουν πληροφορίες για το βιβλίο, όπως τον τόπο και χρόνο έκδοσης. Το τελευταίο ψηφίο χρησιμεύει να εντοπίζονται λάθη. Αν ο κωδικός ISBN είναι $a_1 a_2 \dots a_{10}$, όπου $a_1, \dots, a_9 \in \{0, \dots, 9\}$ και $a_{10} \in \{0, \dots, 10\}$ τότε πρέπει να ισχύει

$$a_1 + 2a_2 + \cdots + 9a_9 \equiv a_{10} \mod 11.$$

9. **ΑΦΜ.** Σε κάθε Έλληνα φορολογούμενο πολίτη αντιστοιχεί ένας εννιαψήφιος Αριθμός Φορολογικού Μητρώου (ΑΦΜ). Όπως και στο προηγούμενο παράδειγμα, το τελευταίο ψηφίο υπάρχει για να αποφεύγονται λάθη ή και να εντοπίζονται πλαστοί ΑΦΜ. Συγκεκριμένα, αν $a_1 \dots a_9$ είναι ο ΑΦΜ τότε πρέπει να ισχύει

$$2^8 a_1 + 2^7 a_2 + \cdots + 2a_8 \equiv a_9 \mod 11,$$

όταν το αριστερό μέλος δεν είναι ισοδύναμο με το 10 mod 11. Διαφορετικά, πρέπει να ισχύει $a_9 = 0$.

Ασκήσεις 1.3

1) Αποδείξτε ότι αν $a \equiv b \mod m$ και $n|m$ τότε $a \equiv b \mod n$.

2) Εξετάστε αν ισχύουν τα παρακάτω ισοτιμίες

   i) $2004 \equiv 1003 \mod 11$

   ii) $(7 - a)^2 \equiv a^2 \mod 7$ για κάθε $a \in \mathbb{Z}$

   iii) $(1 - 2n)^2 \equiv (4n + 1)^{10} \mod 4n$ για κάθε $n \in \mathbb{Z}$

   iv) $(6n + 5)^2 \equiv 1 \mod 4$ για κάθε $n \in \mathbb{Z}$

3) Αποδείξτε ότι

i) $a \equiv b \mod 2 \Rightarrow a^2 \equiv b^2 \mod 4$

ii) $a \equiv b \mod 3 \Rightarrow a^3 \equiv b^3 \mod 9$

4) Αποδείξτε ότι $a \equiv b \mod m$ αν και μόνο αν $a^2 + b^2 \equiv 2ab \mod m^2$.
Υπόδειξη: Εφαρμογή 1.2.8 7).

5) Αποδείξτε ότι για κάθε περιττό ακέραιο a ισχύει $a^2 \equiv 1 \mod 8$.

6) Αποδείξτε ότι για κάθε $a \in \mathbb{Z}$ ισχύει $a^2 \equiv 0, 1$ ή $4 \mod 8$. Κατά συνέπεια ο αριθμός 200340067085 δεν είναι τετράγωνο ακεραίου.

7) Αποδείξτε ότι κανένας ακέραιος της μορφής $3^m + 3^n + 1$, όπου m, n θετικοί ακέραιοι, δεν είναι τετράγωνο ακεραίου.
Υπόδειξη: Εργαστείτε $\mod 8$.

8) Αποδείξτε ότι δεν υπάρχει ακέραιος της μορφής $4n + 2$, όπου $n \in \mathbb{Z}$, που είναι διαφορά δύο τετραγώνων ακεραίων.

9) Για κάθε $n \in \mathbb{N}$ αποδείξτε ότι $4^n \equiv 1 + 3n \mod 9$.

10) Να βρεθούν όλοι οι ακέραιοι $0 \leq x \leq 101$ που ικανοποιούν $x^2 \equiv 1 \mod 101$.

11) Έστω p πρώτος αριθμός. Αποδείξτε ότι αν για τον ακέραιο x ισχύει $x^2 \equiv x \mod p$, τότε $x \equiv 0$ ή $1 \mod p$.

12) Ποιό είναι το υπόλοιπο της διαίρεσης του 100^{100} με το 11;

13) Αποδείξετε ότι κάθε ημερολογιακό έτος (δίσεκτο ή μη) έχει μία τουλάχιστον "Τρίτη και 13".
Υπόδειξη: Μετρήστε modulo 7 αρχίζοντας από την 13η Ιανουαρίου.

14) Αποδείξτε ότι $\mu\kappa\delta(a, m) = \mu\kappa\delta(b, m)$ αν $a \equiv b \mod m$. Εξετάστε αν αληθεύει το αντίστροφο.

15) Ένας ακέραιος αριθμός (σε δεκαδική γραφή) διαιρείται με το 9 αν και μόνο αν το άθροισμα των ψηφίων του, $\sum_i a_i$, διαιρείται με το 9.

16) Ένας ακέραιος αριθμός $a_k \cdots a_1 a_0$ (σε δεκαδική γραφή) διαιρείται με το 11 αν και μόνο αν ο αριθμός $\sum_i (-1)^i a_i$ διαιρείται με το 11.

17) Ένας ακέραιος αριθμός $a_k \cdots a_1 a_0$ (σε δεκαδική γραφή) διαιρείται με το 5 αν και μόνο αν ο αριθμός a_0 διαιρείται με το 5.

18) i) Έστω $a \equiv b \mod m$ και $a \equiv b \mod n$. Αποδείξτε ότι $a \equiv b \mod e$, όπου $e = \epsilon\kappa\pi(m, n)$.

ii) Να βρεθούν όλοι οι ακέραιοι x που ικανοποιούν $x \equiv 7 \mod 8$ και $x \equiv 7 \mod 9$

19) Να βρεθούν όλες οι τριάδες $(p, p+4, p+8)$ όπου οι $p, p+4, p+8$ είναι πρώτοι αριθμοί.

20) Αποδείξτε ότι δεν υπάρχουν ακέραιοι x, y με $7x^2 - 15y^2 = 1$.

21) Αποδείξτε ότι δεν υπάρχουν μη μηδενικοί ακέραιοι x, y, z με $x^2 + y^2 = 3z^2$. *Υπόδειξη:*Μέθοδος της καθόδου: Έστω $(x, y, z) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ μια λύση με x θετικό και ελάχιστο. Από $x^2 + y^2 = 3z^2$, συμπεράνατε ότι καθένα από τα x, y, z είναι πολλαπλάσιο του 3. Απλοποιώντας λαμβάνουμε μια νέα λύση (x_0, y_0, z_0) με $0 < x_0 < x$. Αυτό είναι άτοπο.

22) Αν ο $x^2 + y^2 + z^2$ είναι πολλαπλάσιο του 5 (όπου $x, y, z \in \mathbb{Z}$) αποδείξτε ότι ένα τουλάχιστον από τους x, y, z είναι πολλαπλάσιο του 5.

23) Αποδείξτε ότι αν ο $m \in \mathbb{N}$ είναι τετράγωνο ακεραίου και κύβος ακεραίου, τότε είναι της μορφής $7k$ ή $7k + 1$.

24) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $11 | 3^{3n+1} + 2^{4n+3}$.

25) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $21 | 4^{n+2} + 5^{2n+1}$.

26) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει

i) $10^n + 3 \cdot 4^{n+2} \equiv 4 \mod 9$

ii) $(n+1)^{2n} + 4n^{2n+1}$ δεν είναι πολλαπλάσιο του 3.

27) Έστω $m, n \in \mathbb{N}$ με τον n περιττό. Τότε ο ακέραιος $i^n + (m-i)^n$ είναι πολλαπλάσιος του m για κάθε $i = 0, \ldots, m$.

28) Αποδείξτε ότι αν οι m, n είναι περιττοί τότε $1^m + 2^m + \cdots + (n-1)^m \equiv 0 \mod n$.

29) Έστω n περιττός φυσικός αριθμός. Αποδείξτε ότι κάθε ακέραιος είναι ισότιμος modulo n με ακριβώς έναν ακέραιο από τους $-\frac{n-1}{2}, -\frac{n-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{n-3}{2}, \frac{n-1}{2}$.

1.4 Οι Ακέραιοι modulo m

Στην προηγούμενη Παράγραφο διαπιστώσαμε ότι οι ισοτιμίες modulo m ικανοποιούν αριθμητικές ιδιότητες παρόμοιες με ιδιότητες των ακεραίων. Στην Παράγραφο αυτή θα κατασκευάσουμε ένα πεπερασμένο σύνολο $\mathbb{Z}_m$ και θα ορίσουμε κατά φυσικό τρόπο το άθροισμα και το γινόμενο δύο στοιχείων του. Θα δούμε ότι οι αριθμητική στο $\mathbb{Z}_m$ έχει άμεση σχέση με την αριθμητική ισοτιμιών modulo m. Το σύνολο $\mathbb{Z}_m$ με τις πράξεις αυτές παρουσιάζει ιδιαίτερο ενδιαφέρον, γιατί αφενός μεν οι υπολογισμοί σε αυτό επιτρέπουν συχνά την εξαγωγή με σύντομο και κομψό τρόπο χρήσιμων συμπερασμάτων που αφορούν ακεραίους, αφετέρου δε αυτό αποτελεί ένα σημαντικό παράδειγμα δύο γενικότερων εννοιών που θα μελετήσουμε στις επόμενες Ενότητες.

Σχέσεις ισοδυναμίας

Θα χρειαστούμε εδώ (αλλά και σε επόμενες Ενότητες) βασικά στοιχεία από τις ισοδυναμίες τα οποία θα υπενθυμίσουμε.

Μια ***σχέση*** σε ένα σύνολο A είναι ένα υποσύνολο του καρτεσιανού γινομένου $A \times A = \{(a, b) | a, b \in A\}$.

Έστω X μια σχέση στο A. Αντί να γράφουμε $(a, b) \in X$, συχνά χρησιμοποιούμε τον συμβολισμό $a \underset{X}{\sim} b$. Επίσης, πολλές φορές θα γράφουμε $a \sim b$, όταν είναι φανερό ποιο σύνολο X εννοούμε. Συνεπώς οι συμβολισμοί $(a, b) \in X$ και $a \sim b$ είναι ισοδύναμοι.

Μια σχέση στο μη κενό σύνολο A θα λέγεται ***σχέση ισοδυναμίας*** στο A αν ισχύουν οι παρακάτω ιδιότητες.

1) $a \sim a$ για κάθε $a \in A$ (ανακλαστική ιδιότητα)

2) αν $a \sim b$, τότε $b \sim a$ (συμμετρική ιδιότητα), και

3) αν $a \sim b$ και $b \sim c$, τότε $a \sim c$ (μεταβατική ιδιότητα).

1.4.1 Παραδείγματα.

1) Έστω A ένα μη κενό σύνολο. Θεωρούμε τη σχέση που ορίζεται ως εξής: $a \sim b$ αν και μόνο αν $a = b$. Τότε είναι σαφές ότι ορίζεται μια σχέση ισοδυναμίας στο A.

2) Έστω A το σύνολο των σημείων του πραγματικού επιπέδου. Θεωρούμε τη σχέση που ορίζεται ως εξής: $P \sim Q$ αν και μόνο αν τα σημεία P, Q ισαπέχουν από την αρχή των αξόνων. Τότε ορίζεται μια σχέση ισοδυναμίας στο A.

3) Έστω $A = \mathbb{R}$. Θεωρούμε τη σχέση στο $\mathbb{R}$ που ορίζεται ως εξής: $a \sim b$ αν και μόνο αν $a - b \in \mathbb{Z}$. Εύκολα διαπιστώνεται ότι ορίζεται μια σχέση ισοδυναμίας στο $\mathbb{R}$.

Έστω X μια σχέση ισοδυναμίας στο σύνολο A. Αν $a, b \in A$ με $a \sim b$, θα λέμε ότι το a είναι ***ισοδύναμο*** με το b (ή ότι τα a και b είναι ισοδύναμα, πράγμα που μπορούμε να πούμε λόγω της συμμετρικής ιδιότητας). Το σύνολο

$$[a] = \{x \in A | x \sim a\},$$

δηλαδή το σύνολο των στοιχείων του A που είναι ισοδύναμα με το a, ονομάζεται ***κλάση ισοδυναμίας*** του a. Προφανώς έχουμε $a \in [a]$ αφού $a \sim a$.

1.4.2 Παραδείγματα. (συνέχεια)
Η αρίθμηση εδώ αναφέρεται στα προηγούμενα παραδείγματα.

1) Για κάθε $a \in A$, ισχύει $[a] = \{a\}$,

2) Για κάθε σημείο P, η κλάση ισοδυναμίας $[P]$ είναι το σύνολο των σημείων του κύκλου που διέρχεται από το P και έχει κέντρο την αρχή των αξόνων.

3) Για κάθε $a \in \mathbb{R}$, ισχύει $[a] = \{a + m \in \mathbb{R} | m \in \mathbb{Z}\}$. Ειδικά έχουμε $[k] = \mathbb{Z}$ για κάθε $k \in \mathbb{Z}$.

Η επόμενη Πρόταση περιγράφει τις ιδιότητες των κλάσεων ισοδυναμίας που θα χρειαστούμε.

1.4.3 Πρόταση. *Έστω X μια σχέση ισοδυναμίας στο σύνολο A και $a, b \in A$. Τότε*

1. *$[a] = [b]$ αν και μόνο αν τα a, b είναι ισοδύναμα.*

2. *$[a] \cap [b] = \emptyset$ αν και μόνο τα a, b δεν είναι ισοδύναμα.*

3. *Το σύνολο A μπορεί να παρασταθεί ως ξένη ένωση κλάσεων ισοδυναμίας.*

Απόδειξη. 1. Έστω $[a] = [b]$. Τότε $a \in [a] = [b]$, οπότε $a \sim b$, από τον ορισμό της κλάσης ισοδυναμίας. Αντίστροφα, έστω $a \sim b$ και $x \in A$. Αν $x \in [a]$, τότε $x \sim a$. Επειδή $a \sim b$, η μεταβατική ιδιότητα δίνει $x \sim b$, οπότε έχουμε $x \in [b]$. Συνεπώς $[a] \subseteq [b]$. Με παρόμοιο τρόπο αποδεικνύεται ότι $[b] \subseteq [a]$. Άρα $[a] = [b]$.
2. Έστω ότι τα a και b δεν είναι ισοδύναμα και έστω $x \in [a] \cap [b]$. Από τη σχέση $x \in [a]$ συμπεραίνουμε ότι $a \sim x$. Όμοια, έχουμε ότι $x \sim \beta$. Επομένως έχουμε $a \sim b$, που είναι άτοπο. Τέλος αν τα a, b είναι ισοδύναμα, τότε $[a] = [b]$, όπως

είδαμε προηγουμένως, οπότε $[a] \cap [b] = [a] = [b] \neq \emptyset$.
3. Είναι φανερό ότι $A = \bigcup_{a \in A} [a]$. Η ένωση αυτή δεν είναι αναγκαστικά ξένη. Έστω ότι το σύνολο των διακεκριμένων κλάσεων ισοδυναμίας είναι το $\{[b] | b \in B\}$ για κάποιο $B \subseteq A$. Τότε έχουμε $A = \bigcup_{b \in B} [b]$ και επιπλέον από το 2 συμπεραίνουμε ότι $[b] \cap [b'] = \emptyset$, για κάθε $b, b' \in B$ με $b \neq b'$. ⊤

Έστω X μια σχέση ισοδυναμίας στο σύνολο A και $a \in A$. Κάθε στοιχείο της κλάσης ισοδυναμίας $[a]$ ονομάζεται ***αντιπρόσωπος*** της κλάσης $[a]$. Από την προηγούμενη Πρόταση έπεται ότι ένα $b \in A$ είναι αντιπρόσωπος της κλάσης $[a]$, αν και μόνο αν $[a] = [b]$, δηλαδή αν και μόνο αν $a \sim b$. Έστω ότι το σύνολο των διακεκριμένων κλάσεων ισοδυναμίας είναι το $\{[b] | b \in B\}$ για κάποιο $B \subseteq A$. Κάθε τέτοιο σύνολο B ονομάζεται ένα ***πλήρες σύστημα αντιπροσώπων*** της σχέσης ισοδυναμίας X.

Το σύνολο $\mathbb{Z}_m$

Θα εφαρμόσουμε τώρα τα παραπάνω σε μία ενδιαφέρουσα περίπτωση. Έστω m ένας φυσικός αριθμός. Στο σύνολο $\mathbb{Z}$ θεωρούμε τη σχέση που ορίζεται ως εξής

$$a \sim b \Leftrightarrow a \equiv b \mod m \tag{1}$$

Στη Σημείωση 1.3.3 είδαμε ότι η παραπάνω σχέση είναι μια σχέση ισοδυναμίας. Η κλάση ισοδυναμίας του $a \in \mathbb{Z}$ είναι

$$\begin{aligned} [a] &= \{x \in \mathbb{Z} | x \equiv a \mod m\} \\ &= \{x \in \mathbb{Z} | m \text{ διαιρεί τον } x - a\} \\ &= \{x \in \mathbb{Z} | x - a = km, \text{ για κάποιο } k \in \mathbb{Z}\} \\ &= \{a + km \in \mathbb{Z} | k \in \mathbb{Z}\}. \end{aligned} \tag{2}$$

Δηλαδή, τα στοιχεία του συνόλου $[a]$ είναι της μορφής $a + km$, $k \in \mathbb{Z}$. Για τον λόγο αυτό συνηθίζεται ο συμβολισμός $[a] = a + m\mathbb{Z}$. Όταν θέλουμε να δηλώσουμε την εξάρτηση του συνόλου $[a]$ από το m, συνήθως χρησιμοποιούμε τον συμβολισμό $[a]_m$, ή $a \mod m$.

Από την Πρόταση 1.4.3 έχουμε ότι

$$[a] = [b] \Leftrightarrow a \equiv b \mod m. \tag{3}$$

Το σύνολο των κλάσεων ισοδυναμίας που ορίζονται από την σχέση ισοδυναμίας (1) συμβολίζεται με $\mathbb{Z}_m$,

$$\mathbb{Z}_m = \{[a] \,|\, a \in \mathbb{Z}\}.$$

Για παράδειγμα, έστω $m = 2$. Τότε από τη (2) παίρνουμε $[0] = \{x \in \mathbb{Z} | x \text{ άρτιος}\}$ και $[1] = \{x \in \mathbb{Z} | x \text{ περιττός}\}$. Επειδή οι ακέραιοι $\ldots, -4, -2, 0, 2, 4,$

... είναι ισότιμοι $\mod 2$ έχουμε, λόγω της (3), ότι $\ldots = [-4] = [-2] = [0] = [2] = [4] = \ldots$. Επίσης, αφού οι ακέραιοι $\ldots, -3, -1, 1, 3, \ldots$ είναι ισότιμοι $\mod 2$, έχουμε $\ldots = [-3] = [-1] = [1] = [3] = \ldots$. Άρα $\mathbb{Z}_2 = \{[0], [1]\}$. Παρατηρούμε ότι $\mathbb{Z}_2 = \{[-4], [-3]\} = \{[-4], [1]\} = \ldots$ και γενικά

$$\mathbb{Z}_2 = \{[a_0], [a_1]\}, \quad \text{όπου} \quad a_i \equiv i \mod 2.$$

Έστω τώρα $m = 3$. Τότε από τη (2) παίρνουμε $[0] = \{x \in \mathbb{Z} | x = 3k, k \in \mathbb{Z}\}$, $[1] = \{x \in \mathbb{Z} | x = 3k + 1, k \in \mathbb{Z}\}$ και $[2] = \{x \in \mathbb{Z} | x = 3k + 2, k \in \mathbb{Z}\}$. Δηλαδή, $[0] = \{\ldots, -3, 0, 3, ...\}$, $[1] = \{\ldots, -2, 1, 4, \ldots\}$ και $[2] = \{\ldots, -1, 2, 5, \ldots\}$. Από τη σχέση (3) έχουμε ότι $\ldots = [-3] = [0] = [3] = \ldots$ όπως επίσης $\ldots = [-2] = [1] = [4] = \ldots$ και $\ldots = [-1] = [2] = [5] = \ldots$. Άρα $\mathbb{Z}_3 = \{[0], [1], [2]\}$. Παρατηρούμε ότι έχουμε $\mathbb{Z}_3 = \{[-3], [-2], [-1]\} = \{[-3], [1], [2]\} = \ldots$ και γενικά

$$\mathbb{Z}_3 = \{[a_0], [a_1], [a_2]\} \quad \text{όπου} \quad a_i \equiv i \mod 3.$$

1.4.4 Πρόταση. *Για κάθε θετικό ακέραιο m έχουμε $\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$. Πιο γενικά έχουμε $\mathbb{Z}_m = \{[a_0], [a_1], \ldots, [a_{m-1}]\}$, όπου οι a_i είναι ακέραιοι τέτοιοι ώστε $a_i \equiv i \mod m$ για κάθε i.*

Απόδειξη. Παρατηρούμε ότι οι κλάσεις ισοδυναμίας $[a_i]$, $i = 0, \ldots, m-1$ είναι διακεκριμένες. Πράγματι, αν $[a_i] = [a_j]$ με $0 \leq i, j \leq m-1$, τότε από την (3) έχουμε $i \equiv j \mod m$, οπότε από την Πρόταση 1.3.2 2) έχουμε $i = j$. Κάθε κλάση ισοδυναμίας $[a]$ ανήκει στο σύνολο $\{[a_0], [a_1], \ldots, [a_{m-1}]\}$. Πράγματι, από τον αλγόριθμο διαίρεσης έχουμε $\alpha = qm + r$, όπου $0 \leq r \leq m-1$, οπότε $a \equiv r \mod m$ και άρα $[a] = [r] = [a_r]$. Συνεπώς αποδείξαμε ότι $\mathbb{Z}_m \subseteq \{[a_0], [a_1], \ldots, [a_{m-1}]\}$. Επομένως $\mathbb{Z}_m = \{[a_0], [a_1], \ldots, [a_{m-1}]\}$. ⊤

Το $\mathbb{Z}_m$ ονομάζεται το σύνολο ***των ακεραίων*** modulo m και τα στοιχεία του ονομάζονται ***κλάσεις ισοτιμίας*** modulo m, ή ***κλάσεις υπολοίπων*** modulo m.

Παρατηρήσεις

1) Ένας διαισθητικός τρόπος να σκεφτόμαστε το σύνολο $\mathbb{Z}_m$ είναι ο εξής. Γύρω από έναν κύκλο με μήκος περιφέρειας m τυλίγουμε τον άξονα των πραγματικών αριθμών. Τότε τα σημεία $\ldots, -m, 0, m, 2m, \ldots$ του άξονα θα ταυτιστούν πάνω στον κύκλο. Ομοίως θα ταυτιστούν τα σημεία $\ldots, -m+1, 1, m+1, 2m+1, \ldots$.

2) Στην προηγούμενη Πρόταση είχαμε υποθέσει ότι ο m είναι θετικός. Αν $m = 0$, τότε από τη σχέση (1) έχουμε $a \sim b$ αν και μόνο αν $a = b$. Συνεπώς η κλάση ισοδυναμίας του a αποτελείται από ένα μόνο στοιχείο, $[a] = \{a\}$. Τότε, ταυτίζοντας το σύνολο $\{a\}$ με το στοιχείο a, μπορούμε να θεωρήσουμε ότι το σύνολο των κλάσεων υπολοίπων modulo 0 είναι το $\mathbb{Z}$.

3) Αν $m = 1$, τότε από τη σχέση (1) έχουμε $a \sim b$ για κάθε δύο ακεραίους a, b. Συνεπώς η κλάση ισοδυναμίας ενός ακεραίου a είναι όλο το σύνολο $\mathbb{Z}$ και άρα το σύνολο των κλάσεων υπολοίπων modulo 1 είναι ένα μονοσύνολο.

Η πρόσθεση και ο πολλαπλασιασμός στο $\mathbb{Z}_m$

Κατασκευάσαμε το σύνολο $\mathbb{Z}_m$ με τη βοήθεια μιας σχέσης ισοδυναμίας στο σύνολο $\mathbb{Z}$. Στο $\mathbb{Z}$, όμως, γνωρίζουμε πως να προσθέτουμε και να πολλαπλασιάζουμε στοιχεία. Συνεπώς είναι εύλογο το ερώτημα αν μπορούμε να προσθέτουμε και να πολλαπλασιάζουμε στοιχεία του $\mathbb{Z}_m$ με ανάλογο τρόπο.

Η πρόσθεση (αντίστοιχα, ο πολλαπλασιασμός) ακεραίων αντιστοιχεί σε *κάθε* ζεύγος (a, b) ακεραίων *μοναδικό* ακέραιο, τον $a+b$ (αντίστοιχα, τον ab). Δηλαδή έχουμε απεικονίσεις

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto a + b$$
$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto ab.$$

Με τη βοήθεια αυτών, ορίζουμε τις αντιστοιχίες,

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m, ([a], [b]) \mapsto [a + b]$$
$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m, ([a], [b]) \mapsto [ab].$$

Αποδεικνύουμε τώρα ότι οι αντιστοιχίες αυτές είναι απεικονίσεις. Πρέπει να δείξουμε ότι: αν $([a], [b]) = ([c], [d])$, δηλαδή αν $[a] = [c]$ και $[b] = [d]$, τότε έπεται ότι $[a + b] = [c + d]$ και $[ab] = [cd]$. Με άλλα λόγια, αν $a \equiv c \mod m$ και $b \equiv d \mod m$, τότε $a + b \equiv c + d \mod m$ και $ab \equiv cd \mod m$. Όμως αυτό ισχύει από την Πρόταση 1.3.4.

Για παράδειγμα, στο $\mathbb{Z}_3$ έχουμε $[4] + [2] = [6] = [0]$, $[2][2] = [4] = [1]$. Στο $\mathbb{Z}_{10}$ έχουμε $[4] + [7] = [11] = [1]$, $[4][7] = [28] = [8]$, $[5][6] = [30] = [0]$. Βλέπουμε ότι η πρόσθεση και ο πολλαπλασιασμός κλάσεων υπολοίπων ανάγονται στη πρόσθεση και στον πολλαπλασιασμό αντιπροσώπων τους, δηλαδή ακεραίων.

Για την πρόσθεση και τον πολλαπλασιασμό που ορίσαμε στο $\mathbb{Z}_m$ ισχύουν οι παρακάτω ιδιότητες που θυμίζουν γενικές ιδιότητες της Αριθμητικής. Για κάθε $[a], [b], [c] \in \mathbb{Z}_m$ έχουμε ότι:

1. $([a] + [b]) + [c] = [a] + ([b] + [c])$

2. $[a]+[0]=[0]+[a]$
3. $[a]+[-a]=[-a]+[a]=[0]$
4. $[a]+[b]=[b]+[a]$
5. $([a][b])[c]=[a]([b][c])$
6. $[a]([b]+[c])=[a][b]+[a][c]$
7. $([a]+[b])[c]=[a][c]+[b][c]$
8. $[a][b]=[b][a]$
9. $[a][1]=[1][a]=[a]$

Οι αποδείξεις είναι απλές και παραλείπονται.

Οι ιδιότητες 1-9 θα εφαρμόζονται στα παρακάτω χωρίς ιδιαίτερη μνεία.

Παρατήρηση Πρέπει να τονιστεί εδώ, ότι αν και η πρόσθεση και ο πολλαπλασιασμός στοιχείων του $\mathbb{Z}_m$ έχουν ιδιότητες που θυμίζουν την πρόσθεση και τον πολλαπλασιασμό ακεραίων, υπάρχουν σημαντικές διαφορές. Για παράδειγμα, στο $\mathbb{Z}$ το γινόμενο δύο μη μηδενικών στοιχείων είναι μη μηδενικό. Στο $\mathbb{Z}_6$, όμως, έχουμε $[2][3]=[0]$. Επίσης, αν οι ακέραιοι a,b,c είναι τέτοιοι ώστε $ac=bc$ και $c\neq 0$, τότε $a=b$. Στο $\mathbb{Z}_6$, όμως, έχουμε $[1][3]=[5][3]$ με $[3]\neq[0]$ και $[1]\neq[5]$.

Αντιστρέψιμα στοιχεία στο $\mathbb{Z}_m$

Στη μελέτη της Αριθμητικής του $\mathbb{Z}_m$ (δηλαδή των ιδιοτήτων της πρόσθεσης και του πολλαπλασιασμού του $\mathbb{Z}_m$) είναι φυσικό να θεωρήσουμε πολυωνυμικές εξισώσεις στο $\mathbb{Z}_m$, δηλαδή πολυωνυμικές εξισώσεις με συντελεστές στοιχεία του $\mathbb{Z}_m$. Μία από τις απλούστερες από αυτές τις εξισώσεις είναι η $[a][x]=[b]$. Στην περίπτωση που υπάρχει κλάση $[a']\in\mathbb{Z}_m$ με την ιδιότητα $[a'][a]=[1]$ μπορούμε εύκολα να λύσουμε την εξίσωση πολλαπλασιάζοντάς την με την $[a']$,

$$[a][x]=[b]\Rightarrow[a']([a][x])=[a'][b]\Rightarrow[x]=[a'b].$$

Όμως δεν υπάρχει πάντα τέτοια κλάση $[a']$. Για παράδειγμα, έστω $[2]\in\mathbb{Z}_6$. Αν υπήρχε $[a']\in\mathbb{Z}_6$ με $[2][a']=[1]$, τότε $[2a']=[1]$ και άρα $2a'\equiv 1 \mod 6$, δηλαδή $2a'=1+6n, n\in\mathbb{Z}$, που είναι άτοπο. Οδηγούμαστε έτσι στον επόμενο ορισμό.

Ένα στοιχείο $[a]\in\mathbb{Z}_m$ λέγεται ***αντιστρέψιμο*** αν υπάρχει $[a']\in\mathbb{Z}_m$ με την ιδιότητα $[a][a']=[1]$, δηλαδή αν υπάρχει ακέραιος a' τέτοιος ώστε $aa'\equiv 1 \mod m$. Στην περίπτωση αυτή, το στοιχείο $[a']$ ονομάζεται αντίστροφο του $[a]$. Επίσης θα λέμε ότι ένα ***αντίστροφο modulo m*** του ακεραίου a είναι ο ακέραιος

a'. Για παράδειγμα, στο $\mathbb{Z}_6$ το$[5]$ είναι αντιστρέψιμο αφού $[5][5] = [1]$, ενώ το $[2]$ δεν είναι, όπως είδαμε πριν. Μάλιστα, τα μόνα αντιστρέψιμα στοιχεία του $\mathbb{Z}_6$ είναι τα $[1], [5]$. Στο $\mathbb{Z}_7$ το$[2]$ είναι αντιστρέψιμο αφού $[2][4] = [1]$.

Το σύνολο των αντιστρέψιμων στοιχείων του $\mathbb{Z}_m$ συμβολίζεται με $U(\mathbb{Z}_m)$.

Έστω $[a]$ ένα αντιστρέψιμο στοιχείο του $\mathbb{Z}_m$. Τότε υπάρχει μοναδικό στοιχείο $[a'] \in \mathbb{Z}_m$ με την ιδιότητα $[a][a'] = [1]$. Πράγματι, αν είχαμε $[a][a'] = [1]$ και $[a][a''] = [1]$, τότε $[a'] = [a'][1] = [a']([a][a'']) = ([a'][a])[a''] = ([a'][a])[a''] = [1][a''] = [a'']$.

Στην επόμενη Πρόταση προσδιορίζοντα τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_m$.

1.4.5 Πρόταση. *Το στοιχείο $[a] \in \mathbb{Z}_m$ είναι αντιστρέψιμο αν και μόνο αν $\mu\kappa\delta(a, m) = 1$.*

Απόδειξη. Έστω ότι $[a][b] = 1$. Τότε $ab \equiv 1 \mod m$, δηλαδή $ab = mn + 1$ για κάποιο $n \in \mathbb{Z}$. Από την τελευταία σχέση προκύπτει ότι $\mu\kappa\delta(a, m) = 1$. Αντίστροφα, έστω $\mu\kappa\delta(a, m) = 1$. Τότε υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $ax + my = 1$ (Θεώρημα 1.2.4). Έχουμε

$$\begin{aligned}[ax + my] = [1] &\Rightarrow [ax] + [my] = [1] \\ &\Rightarrow [a][x] + [m][y] = [1] \\ &\Rightarrow [a][x] + [0][y] = [1] \\ &\Rightarrow [a][x] = [1],\end{aligned}$$

δηλαδή το $[a]$ είναι αντιστρέψιμο. ⊺

Σημείωση Η παραπάνω απόδειξη περιέχει έναν πρακτικό τρόπο υπολογισμού του αντιστρόφου (εφόσον αυτό υπάρχει)του $[a]$. Με το συμβολισμό της απόδειξης, το αντίστροφο του $[a]$ είναι το $[x]$. Ένας τέτοιος ακέραιος x μπορεί να βρεθεί χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο, όπως γνωρίζουμε από την Παράγραφο 1.2. Θα δούμε αμέσως παρακάτω ένα σχετικό παράδειγμα.

1.4.6 Εφαρμογή. Θα βρεθούν όλοι οι ακέραιοι x τέτοιοι ώστε $8x \equiv 11 \mod 15$. Εργαζόμενοι στο $\mathbb{Z}_{15}$ έχουμε $[8x] = [11]$, δηλαδή

$$[8][x] = [11]. \tag{1}$$

Επειδή $\mu\kappa\delta(8, 15) = 1$, το στοιχείο $[8]$ είναι αντιστρέψιμο στο $\mathbb{Z}_{15}$ σύμφωνα με την προηγούμενη Πρόταση. Έστω $[8][y] = [1]$. Πολλαπλασιάζοντας την (1) με $[y]$ παίρνουμε

$$[x] = [11y],$$

και συνεπώς αρκεί να προσδιορίσουμε έναν ακέραιο y. Χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο για το ζεύγος $(8, 15)$ έχουμε $15 = 1 \cdot 8 + 7, 8 = 1 \cdot 7 + 1$. Άρα

$1 = 8-1\cdot 7 = 8-1\cdot(15-1\cdot 8) = 8\cdot 2+15(-1)$. Συνεπώς $[1] = [8\cdot 2]+[15\cdot(-1)] = [8][2]$ και άρα μπορούμε να θέσουμε $y = 2$. Τελικά $[x] = [11\cdot 2] = [22] = [7]$, δηλαδή

$$x = 15n + 7, \quad n \in \mathbb{Z}.$$

Το σύνολο των αντιστρέψιμων στοιχείων του $\mathbb{Z}_m$ έχει ενδιαφέρουσες ιδιότητες ως προς τον πολλαπλασιασμό του $\mathbb{Z}_m$. Για παράδειγμα, ισχύει $[a]^k = [1]$ για κάθε $[a] \in U(\mathbb{Z}_m)$, όπου k είναι το πλήθος των στοιχείων του $U(\mathbb{Z}_m)$. Αυτό θα αποδειχθεί στην Παράγραφο 1.6. Εδώ θα αποδείξουμε την ειδική περίπτωση που ο $m = p$ είναι πρώτος. Στην περίπτωση αυτή, από την Πρόταση 1.4.4 και την Πρόταση 1.4.5 έχουμε ότι $k = p - 1$.

1.4.7 Θεώρημα (*Μικρό Θεώρημα του Fermat*). *Έστω $a \in \mathbb{Z}$ και p ένας πρώτος αριθμός. Τότε*

$$a^p \equiv a \mod p.$$

Αν επιπλέον ο p δεν διαιρεί τον a, τότε

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

Απόδειξη. Για να δείξουμε την πρώτη σχέση, θεωρούμε αρχικά την περίπτωση $a \in \mathbb{N}$ και χρησιμοποιούμε επαγωγή στον a. Για $a = 0$, η σχέση είναι προφανής. Υποθέτοντας ότι ισχύει η ισοτιμία για τον a, θα την αποδείξουμε για τον $a + 1$. Από το διωνυμικό ανάπτυγμα έχουμε

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1.$$

Ισχυριζόμαστε ότι οι ακέραιοι $\binom{p}{i} = \dfrac{(p-i+1)\cdots(p-1)p}{1.2\ldots i}$ είναι πολλαπλάσιοι του p όταν $i = 1, 2, \ldots, p-1$. Πράγματι, γράφοντας $(p-i+1)\ldots(p-1)p = \binom{p}{i}1\cdot 2\cdot\cdots\cdot i$ παρατηρούμε ότι ο p διαιρεί το αριστερό μέλος και άρα το δεξιό. Αφού ο p είναι πρώτος θα διαιρεί έναν τουλάχιστον παράγοντα λόγω της Παρατήρησης 1.2.6 1. Όμως ο p δεν διαιρεί κανένα από τους $1, 2, \ldots i$, οπότε διαιρεί τον $\binom{p}{i}$. Επομένως έχουμε ότι

$$(a+1)^p \equiv a^p + 1 \mod p.$$

Από την επαγωγική υπόθεση ισχύει $a^p \equiv a \mod p$ και συνεπώς $(a+1)^p \equiv a+1 \mod p$, που είναι το ζητούμενο.

Έχουμε αποδείξει την πρώτη σχέση για $a \in \mathbb{N}$. Έστω τώρα $a \in \mathbb{Z}$, $a < 0$. Αν ο p είναι περιττός έχουμε $a^p = -(-a)^p \equiv -(-a) \mod p$ από την περίπτωση

της ισοτιμίας που αποδείξαμε πριν. Άρα $a^p \equiv a \mod p$. Άν $p = 2$, τότε $a^2 = (-a)^2 \equiv -a \mod 2$. Αλλά $-a \equiv a \mod 2$ και κατά συνέπεια $a^2 \equiv a \mod 2$.

Θα αποδείξουμε τώρα τη δεύτερη σχέση. Επειδή έχουμε $\mu\kappa\delta(p, a) = 1$, το στοιχείο $[a]$ είναι αντιστρέψιμο στο $\mathbb{Z}_p$ (Πρόταση 1.4.5). Έστω $[b][a] = [1]$. Πολλαπλασιάζοντας τη σχέση $[a^p] = [a]$ με $[b]$ προκύπτει ότι $[a^{p-1}] = [1]$. ⊺

1.4.8 Παρατήρηση. Από τη δεύτερη ισοτιμία στο Μικρό Θεώρημα του Fermat έχουμε ότι αν ο p είναι πρώτος και ο $a \in \mathbb{Z}$ δεν διαιρείται με τον p, τότε το αντίστροφο του $[a]$ στο $\mathbb{Z}_p$ είναι το $[a^{p-2}]$.

1.4.9 Παραδείγματα.

1) Το Μικρό Θεώρημα του Fermat μας διευκολύνει να υπολογίσουμε υπόλοιπα διαιρέσεων μεγάλων αριθμών με πρώτους. Για παράδειγμα, ας υπολογίσουμε το υπόλοιπο της διαίρεσης του 222^{555} με το 7. Επειδή έχουμε $222 = 31 \cdot 7 + 5$ παίρνουμε $222 \equiv 5 \mod 7$. Άρα

$$222^{555} \equiv 5^{555} \mod 7.$$

Από τη σχέση $555 = 92 \cdot 6 + 3$ παίρνουμε $5^{555} = (5^6)^{92} \cdot 5^3$. Από το Μικρό Θεώρημα του Fermat έχουμε $5^6 \equiv 1 \mod 7$. Συνεπώς

$$5^{555} \equiv 5^3 \mod 7.$$

Αλλά $5^3 \equiv (-2)^3 \equiv -8 \equiv 6 \mod 7$. Το ζητούμενο υπόλοιπο είναι 6.

2) Έστω p ένας πρώτος αριθμός και $a, b \in \mathbb{Z}$ με $a^p \equiv b^p \mod p$. Τότε $a^p \equiv b^p \mod p^2$
Πράγματι, χρησιμοποιώντας το Μικρό Θεώρημα του Fermat, από την υπόθεση συμπεραίνουμε ότι $a \equiv b \mod p$. Συνεπώς $b = a + kp$, $k \in \mathbb{Z}$. Τότε χρησιμοποιώντας το διωνυμικό ανάπτυγμα έχουμε

$$\begin{aligned} b^p - a^p &= (a + kp)^p - a^p \\ &= \binom{p}{1} a^{p-1}(kp) + \binom{p}{2} a^{p-2}(kp)^2 + \cdots + \binom{p}{p} (kp)^p. \end{aligned}$$

Είναι προφανές ότι στο δεξιό μέλος κάθε προσθετέος διαιρείται με τον p^2.

3) Για κάθε $n \in \mathbb{N}$ ισχύει $42 | n^7 - n$.
Έχουμε $42 = 2 \cdot 3 \cdot 7$. Από το Παράδειγμα 1.2.8 2), αρκεί να αποδειχθεί ότι ισχύει κάθε μια από τις ισοτιμίες

$$\begin{aligned} n^7 &\equiv n \mod 7 \\ n^7 &\equiv n \mod 3 \\ n^7 &\equiv n \mod 2 \end{aligned}$$

Η πρώτη ισχύει από το Μικρό Θεώρημα του Fermat για $p = 7$. Για τη δεύτερη παρατηρούμε ότι εφαρμόζοντας δύο φορές το Μικρό Θεώρημα του Fermat για $p = 3$ έχουμε

$$n^7 = (n^3)^2 n \equiv n^2 n \equiv n \mod 3$$

Με παρόμοιο τρόπο (ή και άμεσα) αποδεικνύεται και η τρίτη ισοτιμία.

Ασκήσεις 1.4

1) Ποια είναι τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_{10}$; Για καθένα από αυτά υπολογίστε το αντίστροφο στοιχείο. Ποια από τα αντιστρέψιμα στοιχεία συμπίπτουν με το αντίστροφο τους;

2) Να βρεθούν όλοι οι ακέραιοι x τέτοιοι ώστε $12x \equiv 11 \mod 13$.

3) Να λυθεί στο $\mathbb{Z}_{127}$ η εξίσωση $[58][x] = [3]$.

4) Αληθεύει ότι η εξίσωση $[4][x] = [3]$ έχει λύση στο $\mathbb{Z}_6$;

5) Αποδείξτε ότι η εξίσωση $[a][x] = [b]$ έχει λύση στο $\mathbb{Z}_m$ αν και μόνο αν $\mu\kappa\delta(a, m)|b$.

6) Να λυθούν οι παρακάτω εξισώσεις

   - $[x]^2 = [1]$ στο $\mathbb{Z}_8$
   - $[x]^4 = [1]$ στο $\mathbb{Z}_5$
   - $[x]^3 = [1]$ στο $\mathbb{Z}_5$
   - $[x]^2 + [3][x] + [2] = [0]$ στο $\mathbb{Z}_6$
   - $[x] + [x] + [x] = [0]$ στο $\mathbb{Z}_3$.

7) Αποδείξτε ότι ο ακέραιος p είναι πρώτος αν και μόνο αν το πλήθος των αντιστρέψιμων στοιχείων του $\mathbb{Z}_p$ είναι $p - 1$.

8) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $n^5 \equiv n \mod 30$.

9) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $n^{49} \equiv n \mod 1547$.
   Υπόδειξη: $1547 = 7 \cdot 13 \cdot 17$.

10) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $(n + 1)^9 + 4n^5 \equiv 1 \mod 5$

11) Αποδείξτε ότι $n^{12} + 12^n \equiv 5 \mod 11$ αν και μόνο αν $n \equiv 2, 9 \mod 11$.

12) Ποιο είναι το υπόλοιπο της διαίρεσης του 100^{100} με το 13;

13) Ποια ημέρα της εβδομάδας θα είναι 333^{444} ημέρες από σήμερα;

14) Να βρεθεί ένα στοιχείο $[a]$ του $U(\mathbb{Z}_5)$ ώστε κάθε άλλο στοιχείο του $U(\mathbb{Z}_5)$ να είναι της μορφής $[a]^n$, $n \in \mathbb{N}$. Υπάρχει τέτοιο στοιχείο στο $U(\mathbb{Z}_8)$;

15) Έστω p πρώτος και $a \in \mathbb{Z}$ που δεν είναι πολλαπλάσιο του p. Αποδείξτε ότι ο ελάχιστος θετικός ακέραιος n για τον οποίο ισχύει στο $U(\mathbb{Z}_p)$ ότι $[a]^n = [1]$ είναι διαιρέτης του $p-1$.

16) Υπολογίστε το άθροισμα όλων των στοιχείων του $\mathbb{Z}_m$ όταν $m = 3, 4, 5, 6$. Αποδείξτε ότι αν ο m είναι περιττός, τότε το άθροισμα όλων των στοιχείων του $\mathbb{Z}_m$ είναι ίσο με $[0]$. Με τί ισούται το εν λόγω άθροισμα όταν ο m είναι άρτιος;

17) Έστω p πρώτος αριθμός με $p \equiv 3 \mod 4$. Αποδείξτε ότι δεν υπάρχει $[a] \in \mathbb{Z}_p$ με $[a]^2 = [-1]$.

18) Έστω $\mathbb{Z}_m = \{[a_1], \ldots [a_m]\}$ και $[a] \in \mathbb{Z}_m$. Αποδείξτε ότι τα στοιχεία $[a] + [a_i]$, όπου $i = 1, \ldots, m$, είναι διακεκριμένα και επομένως $\mathbb{Z}_m = \{[a + a_1], \ldots, [a + a_m]\}$. Έστω επιπλέον ότι $[a] \neq [0]$. Αληθεύει ότι τα στοιχεία $[a][a_i]$, $i = 1, \ldots, m$, είναι διακεκριμένα;

19) Εξετάστε αν αληθεύει ότι το άθροισμα δύο αντιστρέψιμων στοιχείων του $\mathbb{Z}_m$ είναι αντιστρέψιμο.

1.5 Διοφαντικές Εξισώσεις και Ισοτιμίες

Πολλά μαθηματικά προβλήματα που συναντάμε στην καθημερινή μας ζωή ανάγονται σε εξισώσεις στις οποίες επιζητούμε λύσεις που να είναι ακέραιοι αριθμοί. Οι εξισώσεις αυτής της μορφής παίζουν σημαντικό ρόλο στη Θεωρία Αριθμών και στην Άλγεβρα.

Μια εξίσωση της μορφής $f(x_1, \dots x_n) = 0$, όπου το $f(x_1, \dots x_n)$ είναι ένα πολυώνυμο των $x_1, \dots x_n$ με ακεραίους συντελεστές, ονομάζεται ***Διοφαντική*** όταν μας ενδιαφέρουν μόνο οι ακέραιες λύσεις της. Θα ασχοληθούμε εδώ με την πρώτη μη τετριμμένη Διοφαντική εξίσωση, $ax + by = c$, και θα περιγράψουμε πλήρως τις λύσεις της. Με τη χρήση αυτής θα λύσουμε την ισοτιμία $ax \equiv b \mod m$. Τέλος θα ασχοληθούμε με συστήματα ισοτιμιών (Κινεζικό Θεώρημα Υπολοίπων).

1.5.1 Θεώρημα. *Έστω $a, b, c \in \mathbb{Z}$ τέτοιοι ώστε τουλάχιστον ένας από τους a, b δεν είναι μηδέν. Θέτουμε $d = \mu\kappa\delta(a, b)$.*

1) *Αν ο d δεν διαιρεί τον c, τότε η Διοφαντική εξίσωση $ax + by = c$ δεν έχει λύσεις.*

2) *Αν ο d διαιρεί τον c, τότε η Διοφαντική εξίσωση έχει άπειρες λύσεις. Επιπλέον αν (x_0, y_0) είναι μία λύση, τότε κάθε άλλη λύση έχει τη μορφή*

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n, \quad n \in \mathbb{Z}. \tag{1}$$

Απόδειξη. 1) Υποθέτουμε ότι ο d δεν διαιρεί τον c. Έστω ότι υπάρχουν ακέραιοι x, y τέτοιοι ώστε $ax + by = c$. Αφού $d|a$ και $d|b$, παίρνουμε $d|c$, που είναι άτοπο.

2) Υποθέτουμε ότι ο d διαιρεί τον c. Επειδή $\mu\kappa\delta(a, b) = d$, υπάρχουν $s, t \in \mathbb{Z}$ με

$$d = as + bt \tag{2}$$

Αφού $d|c$, έχουμε $c = de$, όπου $e \in \mathbb{Z}$. Από την (2) παίρνουμε

$$c = de = a(se) + b(te),$$

που σημαίνει ότι μία λύση είναι η $x_0 = se$, $y_0 = te$.

Θα δείξουμε ότι η δοθείσα Διοφαντική εξίσωση έχει άπειρες λύσεις. Έστω $x = x_0 + \frac{b}{d}n$ και $y = y_0 - \frac{a}{d}n$, $n \in \mathbb{Z}$. Εύκολα επαληθεύεται με πράξεις ότι $ax + by = c$.

Τώρα θα δείξουμε ότι κάθε λύση είναι της μορφής (1). Έστω $x_0, y_0, x, y \in \mathbb{Z}$ με $ax + by = c$ και $ax_0 + by_0 = c$. Αφαιρώντας κατά μέλη παίρνουμε

$$a(x - x_0) = b(y_0 - y) \tag{3}$$

και άρα $\frac{a}{d}(x - x_0) = \frac{b}{d}(y - y_0)$. Αφού $\mu\kappa\delta\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, έχουμε ότι $\frac{a}{d} | y - y_0$. Άρα υπάρχει $n \in \mathbb{Z}$ με $y_0 - y = \frac{a}{d}n$, δηλαδή $y = y_0 - \frac{a}{d}n$.

Αν ο a δεν είναι μηδέν, τότε από την (3) παίρνουμε $x = x_0 + \frac{b}{d}n$. Η απόδειξη στην περίπτωση που ο b δεν είναι μηδέν είναι παρόμοια. ⊤

1.5.2 Παραδείγματα.

1) Η Διοφαντική εξίσωση $4x + 8y = 10$ δεν έχει λύσεις αφού $\mu\kappa\delta(4, 8) = 4$ που δεν διαιρεί τον 10.

2) Η Διοφαντική εξίσωση $21x + 14y = 70$ έχει άπειρες λύσεις αφού $\mu\kappa\delta(21, 14) = 7$ που διαιρεί το 70. Βρίσκουμε τις λύσεις ως εξής: Από τον Ευκλείδειο αλγόριθμο έχουμε $21 = 1 \cdot 14 + 7$, $14 = 2 \cdot 7 = 0$. Επομένως $7 = 1 \cdot 21 + (-1) \cdot 14$ και άρα $70 = 10 \cdot 21 + (-10) \cdot 14$. Έτσι μία λύση είναι η $x_0 = 10$, $y_0 = -10$. Επομένως κάθε λύση, σύμφωνα με το Θεώρημα 1.5.1, είναι της μορφής $x = 10 + 2n$ και $y = -10 - 3n$, όπου $n \in \mathbb{Z}$.

3) Θέλουμε να αγοράσουμε γραμματόσημα των 0.4 Ευρώ και 0.6 Ευρώ για μια επιστολή που κοστίζει 8 Ευρώ. Ποιος είναι ο ελάχιστος αριθμός γραμματοσήμων 0.4 Ευρώ που απαιτούνται;
Θα λύσουμε τη Διοφαντική εξίσωση $4x + 6y = 80$ και θα βρούμε τη λύση (x, y) όπου ο x είναι μη αρνητικός ακέραιος και ελάχιστος και $y \geq 0$. Αφού $\mu\kappa\delta(4, 6) = 2$ που διαιρεί το 80, υπάρχουν λύσεις. Από τον Ευκλείδειο Αλγόριθμο παίρνουμε $80 = (-40) \cdot 4 + 40 \cdot 6$ που σημαίνει ότι μία λύση είναι η $x_0 = -40$, $y_0 = 40$. Άρα κάθε λύση είναι της μορφής $x = -40 + 3n$, $y = 40 - 2n$. Επειδή $x \geq 0$ έχουμε $n \geq 14$. Άρα η ζητούμενη λύση προκύπτει για $n = 14$ και είναι η $x = 2$, $y = 12$.

Το προηγούμενο Θεώρημα μας βοηθά να μελετήσουμε ισοτιμίες.

1.5.3 Θεώρημα. *Έστω $a, b, m \in \mathbb{Z}$ με $m \neq 0$ και $d = \mu\kappa\delta(a, m)$. Για τις λύσεις της ισοτιμίας*

$$ax \equiv b \mod m$$

ισχύουν τα εξής:

1) αν $d \nmid b$, τότε δεν υπάρχουν λύσεις, και

2) αν $d|b$ τότε υπάρχουν ακριβώς d μη ισοδύναμες λύσεις modulo m.

Απόδειξη. Η ισοτιμία $ax \equiv b \mod m$ είναι ισοδύναμη με τη Διοφαντική εξίσωση $ax - my = b$. Οι λύσεις αυτής περιγράφονται από το Θεώρημα 1.5.1: αν $d \nmid b$ τότε δεν υπάρχουν λύσεις, ενώ αν $d|b$ τότε υπάρχουν άπειρες λύσεις που δίνονται από τις σχέσεις

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

όπου (x_0, y_0) είναι μια συγκεκριμένη λύση της εξίσωσης.

Έστω $t_1, t_2 \in \mathbb{Z}$ και

$$x_1 = x_0 - \frac{m}{d}t_1 \quad \text{και} \quad x_2 = x_0 - \frac{m}{d}t_2,$$

Θα αποδείξουμε τώρα ότι

$$x_1 \equiv x_2 \mod m \Leftrightarrow t_1 \equiv t_2 \mod d.$$

Πράγματι, αν $x_1 \equiv x_2 \mod m$, τότε $\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \mod m$. Από την Πρόταση 1.3.7 προκύπτει ότι $t_1 \equiv t_2 \mod d$. Αντίστροφα, αν $t_1 \equiv t_2 \mod d$, τότε $\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \mod m$ και άρα $x_1 \equiv x_2 \mod m$.

Άρα αποδείξαμε ότι υπάρχουν ακριβώς d μη ισοδύναμες λύσεις modulo m. Μία επιλογή d μη ισοδυνάμων λύσεων modulo m δίνεται από τη σχέση

$$x = x_0 - \frac{m}{d}t, \tag{4}$$

για $t = 0, 1, \ldots, d-1$. ⊤

Σημειώσεις

1) Αν $c \in \mathbb{Z}$ είναι μια λύση της ισοτιμίας $ax \equiv b \mod m$ τότε κάθε $c' \in \mathbb{Z}$ με $c' \equiv c \mod m$ θα είναι λύση της ισοτιμίας λόγω της Πρότασης 1.3.4. Συνεπώς, από τώρα και στο εξής όταν λέμε ***λύση*** μιας ισοτιμίας $ax \equiv b \mod m$ εννοούμε μια ***κλάση υπολοίπων modulo m***, τέτοια ώστε κάθε στοιχείο x της κλάσης ικανοποιεί την ισοτιμία. Έτσι στη δεύτερη περίπτωση του προηγούμενου Θεωρήματος, θα λέμε ότι η ισοτιμία $ax \equiv b \mod m$ έχει ακριβώς d λύσεις.

2) Επειδή η ισοτιμία $ax \equiv b \mod m$ είναι ισοδύναμη με την εξίσωση $[a][x] = [b]$ στο $\mathbb{Z}_m$, βλέπουμε ότι μια πρωτοβάθμια εξίσωση στο $\mathbb{Z}_m$ μπορεί να μην έχει λύσεις, να έχει ακριβώς μια λύση ή να έχει περισσότερες λύσεις.

1.5.4 Παραδείγματα.

1) Θα προσδιορίσουμε τους $x \in \mathbb{Z}$ που έχουν την ιδιότητα $9x \equiv 12 \mod 15$. Έχουμε $d = \mu\kappa\delta(9, 15) = 3$ και $3|12$. Άρα υπάρχουν ακριβώς 3 κλάσεις υπολοίπων $\mod 15$ που είναι λύσεις. Για να βρούμε μια λύση της αντίστοιχης Διοφαντικής εξίσωσης $9x - 15y = 12$ εφαρμόζουμε τον Ευκλείδειο αλγόριθμο

$$\begin{aligned} 15 &= 9 \cdot 1 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3. \end{aligned}$$

Άρα $3 = 9 - 6 \cdot 1 = 9 - (15 - 9 \cdot 1) = 9 \cdot 2 - 15 \cdot 1$ και πολλαπλασιάζοντας με 4 έχουμε $9 \cdot 8 - 15 \cdot 4 = 12$. Θέτουμε $(x_0, y_0) = (8, 4)$. Από την απόδειξη του Θεωρήματος 1.5.3, ισότητα (4), όλες οι λύσεις της αρχικής ισοτιμίας είναι

$$x \equiv 8 \mod 15, \quad x \equiv 3 \mod 15, \quad x \equiv 13 \mod 15.$$

2) Μπορούμε να λύσουμε την ισοτιμία $7x \equiv 22 \mod 10$ με την προηγούμενη μέθοδο ή εναλλακτικά να παρατηρήσουμε ότι αφού $\mu\kappa\delta(7, 10) = 1$, το 7 είναι αντιστρέψιμο modulo 10 (Πρόταση 1.4.5), έστω $7a \equiv 1 \mod 10$. Πολλαπλασιάζοντας την αρχική ισοτιμία με a παίρνουμε $x \equiv 22a \mod 10$. Με τον Ευκλείδειο αλγόριθμο (ή με όποιον άλλο τρόπο θέλουμε) βρίσκουμε το αντίστροφο του 7 modulo 10, $a \equiv 3 \mod 10$. Άρα $x \equiv 66 \equiv 6 \mod 10$ (δείτε και την Εφαρμογή μετά την Πρόταση 1.4.5).

Σημείωση Στο Παράδειγμα 1.5.4 1) μπορούμε να εργαστούμε και ως εξής. Η δοθείσα ισοτιμία είναι ισοδύναμη με την $3x \equiv 4 \mod 5$, που έχει ακριβώς μία λύση από το Θεώρημα 1.5.3, την $x \equiv 3 \mod 5$. Πώς σχετίζεται αυτή η λύση με τις τρεις λύσεις που βρήκαμε στο Παράδειγμα 1.5.4 1); Αν συμβολίσουμε την κλάση υπολοίπων $\mod m$ του a με $[a]_m$, τότε είναι εύκολο να δούμε ότι

$$[3]_5 = [3]_{15} \cup [8]_{15} \cup [13]_{15}.$$

Με άλλα λόγια βλέπουμε ότι έχουμε δύο περιγραφές του ιδίου συνόλου, δηλαδή του $\{x \in \mathbb{Z} | 9x \equiv 12 \mod 15\}$. Πιο γενικά, μπορεί να αποδειχθεί το εξής. Έστω d, m θετικοί ακέραιοι τέτοιοι ώστε $d|m$. Τότε για κάθε ακέραιο r έχουμε την ξένη ένωση

$$[r]_d = [r]_m \cup [r + d]_m \cup \cdots \cup \left[r + \left(\frac{m}{d} - 1\right) d\right]_m.$$

Η απόδειξη αφήνεται σαν άσκηση.

Συστήματα ισοτιμιών

Στη συνέχεια θα θεωρήσουμε συστήματα ισοτιμιών. Όταν λέμε λύση ενός συστήματος ισοτιμιών εννοούμε κάθε ακέραιο που ικανοποιεί όλες τις ισοτιμίες του συστήματος.

Αρχικά παρατηρούμε ότι είναι δυνατόν ένα σύστημα να μην έχει λύση αν και κάθε ισοτιμία του συστήματος έχει λύση. Ας θεωρήσουμε, για παράδειγμα, το σύστημα

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 2 \mod 6. \end{aligned}$$

Αυτό δεν έχει λύση, γιατί από την πρώτη ισοτιμία παίρνουμε $2|x-1$ και από τη δεύτερη παίρνουμε $2|x-2$ και επομένως $2|1$.

Στην περίπτωση που υπάρχουν ακέραιοι x, x' που ικανοποιούν το σύστημα

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}$$

παίρνουμε $x \equiv x' \mod m$ και $x \equiv x' \mod n$, δηλαδή $m|x-x'$ και $n|x-x'$, και επομένως $e|x-x'$, όπου $e = \epsilon\kappa\pi(m,n)$. Συνεπώς, αν υπάρχει λύση, αυτή είναι μοναδική $\mod e$. Στην ειδική περίπτωση που ισχύει $\mu\kappa\delta(m,n)=1$, τότε μπορούμε να δείξουμε ότι το προηγούμενο σύστημα έχει λύση (και είναι μοναδική $\mod e$, δηλαδή $\mod (mn)$). Σχετικό είναι το παρακάτω Θεώρημα.

1.5.5 Θεώρημα (*Κινεζικό Θεώρημα Υπολοίπων*). *Έστω $m_1, m_2, \ldots, m_r$ ανά δύο σχετικά πρώτοι θετικοί ακέραιοι. Τότε το σύστημα ισοτιμιών*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ &\vdots \\ x &\equiv a_r \mod m_r \end{aligned}$$

έχει μοναδική λύση modulo $M = m_1 m_2 \ldots m_r$.

Απόδειξη. Ύπαρξη: Θέτουμε $M_k = \dfrac{M}{m_k}$ και παρατηρούμε ότι, λόγω της υπόθεσης, ισχύει $\mu\kappa\delta(M_k, m_k) = 1$. Επομένως το M_k είναι αντιστρέψιμο modulo m_k Έστω $M_k y_k \equiv 1 \mod m_k$. Θέτουμε

$$x = a_1 M_1 y_1 + \cdots + a_r M_r y_r \tag{5}$$

Επειδή για $i \neq k$ έχουμε $m_i | M_k$ η (5) δίνει $x \equiv a_k M_k y_k \mod m_k$, $k = 1, 2, \ldots, r$. Άρα $x \equiv a_k \mod m_k$, $k = 1, 2, \ldots, r$.

Μοναδικότητα: Έστω x και x' δύο λύσεις του αρχικού συστήματος. Τότε για κάθε $k = 1, 2, \ldots, r$ έχουμε $x \equiv x' \mod m_k$, δηλαδή $m_k | x - x'$. Από το Παράδειγμα 1.2.8 2) συμπεραίνουμε ότι $M | x - x'$, αφού οι m_k είναι ανά δύο σχετικά πρώτοι. ⊺

Τονίζουμε εδώ, ότι το σύνολο των ακεραίων που είναι λύσεις του συστήματος του προηγουμένου Θεωρήματος είναι η τομή των κλάσεων $[a_1]_{m_1}, \ldots, [a_r]_{m_r}$.

1.5.6 Παραδείγματα.

1) Για να λύσουμε το σύστημα

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 5 \\ x &\equiv 3 \mod 7 \end{aligned}$$

θέτουμε, σύμφωνα με την απόδειξη του Θεωρήματος 1.5.5, $M = 3 \cdot 5 \cdot 7 = 105$, $M_1 = \dfrac{105}{3} = 35$, $M_2 = \dfrac{105}{5} = 21$ και $M_3 = \dfrac{105}{7} = 15$. Για να βρούμε το y_1 λύνουμε την ισοτιμία $35y_1 \equiv 1 \mod 3$, δηλαδή την $2y_1 \equiv 1 \mod 3$. Έχουμε $y_1 \equiv 2 \mod 3$. Βρίσκουμε το y_2 από την $21y_2 \equiv 1 \mod 5$. Έχουμε $y_2 \equiv 1 \mod 5$. Βρίσκουμε το y_3 από την $15y_3 \equiv 1 \mod 7$. Έχουμε $y_3 \equiv 1 \mod 7$. Τελικά

$$x \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \mod 105,$$

δηλαδή $x \equiv 157 \equiv 52 \mod 105$.

2) Μπορούμε συχνά να λύσουμε συστήματα ισοτιμιών και με διαδοχικές αντικαταστάσεις. (Για τη μέθοδο αυτή δεν χρειάζονται τα moduli m_k να είναι ανά δύο σχετικά πρώτοι, αλλά στην περίπτωση αυτή δεν γνωρίζουμε εκ των προτέρων αν υπάρχει λύση). Για παράδειγμα έστω

$$\begin{aligned} x &\equiv 1 \mod 5 \\ x &\equiv 2 \mod 6 \\ x &\equiv 3 \mod 7 \end{aligned}$$

Γνωρίζουμε από το Κινεζικό Θεώρημα Υπολοίπων ότι το σύστημα έχει μοναδική λύση $\mod 210$ την οποία μπορούμε να βρούμε ως εξής. Από την πρώτη ισοτιμία έχουμε $x = 5t + 1$, $t \in \mathbb{Z}$. Αντικαθιστώντας στη δεύτερη έχουμε $5t \equiv 1 \mod 6$, την οποία λύνουμε για να βρούμε $t \equiv 5 \mod 6$. Άρα $t = 6u + 5$, $u \in \mathbb{Z}$. Συνεπώς $x = 5(6u + 5) + 1 = 30u + 26$.

Αντικαθιστώντας στην τρίτη ισοτιμία παίρνουμε $30u \equiv 5 \mod 7$. Η λύση είναι $u \equiv 6 \mod 7$. Άρα $u = 7v+6$, $v \in \mathbb{Z}$. Τελικά $x = 30(7v+6)+26 = 210v + 206$.
Συνεπώς $x \equiv 206 \mod 210$.

3) Με τη βοήθεια του Κινεζικού Θεωρήματος Υπολοίπων μπορούμε μερικές φορές να λύσουμε ισοτιμίες πιο πολύπλοκες από αυτές που μελετήσαμε στο Θεώρημα 1.5.3. Για παράδειγμα, ας θεωρήσουμε την $x^2 \equiv 1 \mod 77$. Επειδή $x^2 - 1 = (x+1)(x-1)$ και $77 = 7 \cdot 11$, εύκολα επαληθεύουμε ότι η εν λόγω ισοτιμία ισοδυναμεί με τα εξής 4 συστήματα ισοτιμιών

α) $x + 1 \equiv 0 \mod 77$

β) $x - 1 \equiv 0 \mod 77$

γ) $x + 1 \equiv 0 \mod 7$
$x - 1 \equiv 0 \mod 11$

δ) $x + 1 \equiv 0 \mod 11$
$x - 1 \equiv 0 \mod 7$.

Οι α) και β) λύνονται άμεσα ενώ στα γ) και δ) εφαρμόζουμε το Κινεζικό Θεώρημα Υπολοίπων. Βλέπουμε ότι οι λύσεις είναι: α) $x \equiv 76 \mod 77$, β) $x \equiv 1 \mod 77$, γ) $x \equiv 34 \mod 77$, δ) $x \equiv 43 \mod 77$.

4) Ας θεωρήσουμε το σύστημα

$$\begin{aligned} 2x &\equiv 1 \mod 3 \\ 5x &\equiv 2 \mod 7. \end{aligned}$$

Παρατηρούμε ότι σε αυτό δεν μπορούμε να εφαρμόσουμε άμεσα το Κινεζικό Θεώρημα Υπολοίπων. Επειδή το 2 είναι αντιστρέψιμο modulo 3 (και ένα αντίστροφό του είναι το 2), η πρώτη ισοτιμία του συστήματος είναι ισοδύναμη με την $x \equiv 2 \mod 3$. Με παρόμοιο τρόπο, βλέπουμε ότι η δεύτερη ισοτιμία είναι ισοδύναμη με την $x \equiv 6 \mod 7$. Συνεπώς το αρχικό σύστημα είναι ισοδύναμο με το

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 6 \mod 7. \end{aligned}$$

Το σύστημα αυτό μπορεί να λυθεί με το Κινεζικό Θεώρημα Υπολοίπων.

Ασκήσεις 1.5

1. Λύστε τις παρακάτω Διοφαντικές εξισώσεις.

   i) $5x + 8y = 99$

   ii) $6x + 4y = 100$

   iii) $6x + 4y = 99$

   iv) $110x + 150y = 30$

   v) $14x + 49y = 42$

2. Πόσα ζεύγη $(x, y) \in \mathbb{N} \times \mathbb{N}$ υπάρχουν τέτοια ώστε $2x + 3y = 70$;

3. Κατά πόσους διαφορετικούς τρόπους μπορεί να σχηματιστεί ένα ποσό 510 Ευρώ από χαρτονομίσματα των 20 και 50 Ευρώ;

4. Έστω $a, b, c \in \mathbb{Z} - \{0\}$ και $d \in \mathbb{Z}$.

   i) Αποδείξτε ότι η Διοφαντική εξίσωση $ax + by + cz = d$ έχει λύση αν και μόνο αν $\mu\kappa\delta(a, b, c)|d$.

   ii) Αποδείξτε ότι αν η Διοφαντική εξίσωση $ax + by + cz = d$ έχει μία λύση, τότε έχει άπειρες.

5. Λύστε τις Διοφαντικές εξισώσεις

   i) $2x + 3y + 4z = 79$
   Υπόδειξη: Θέστε $w = 3y + 4z$ και λύστε πρώτα την $2x + w = 79$.

   ii) $10x + 6y + 15z = 40$

6. Να βρεθούν οι ακέραιοι $x, y, z \in \mathbb{Z}$ που είναι λύσεις του συστήματος

$$x + y + z = 100$$
$$x + 8y + 50z = 156.$$

7. Είναι δυνατόν με συνολικά 50 νομίσματα των 2, 10 και 50 Ευρώ να σχηματιστεί ποσό 760 Ευρώ;

8. Ποιες από τις παρακάτω ισοτιμίες έχουν λύσεις; Βρείτε τις λύσεις (όπου υπάρχουν)

   i) $2x \equiv 6 \mod 12$

   ii) $101x \equiv 7 \mod 102$

iii) $14x \equiv 3 \mod 21$

iv) $9x \equiv 5 \mod 35$.

9. Ποια από τα παρακάτω συστήματα έχουν λύσεις; Βρείτε τις λύσεις (όπου υπάρχουν).

   i) $x \equiv 3 \mod 5$
      $x \equiv 5 \mod 6$
      $x \equiv 1 \mod 7$

   ii) $2x \equiv 1 \mod 7$
       $x \equiv 4 \mod 8$

   iii) $6x \equiv 2 \mod 9$
        $5x \equiv 1 \mod 10$

   iv) $4x \equiv 2 \mod 10$
       $3x \equiv 4 \mod 11$

10. Βρείτε τον ελάχιστο θετικό ακέραιο που όταν διαιρεθεί με τους 5, 7 και 9 αφήνει υπόλοιπα 1, 2, 3 αντίστοιχα.

11. Λύστε το σύστημα

$$x \equiv 4 \mod 6$$
$$x \equiv 13 \mod 15$$

12. Ένας δορυφόρος που κινείται γύρω από την Γη έχει περίοδο t που είναι ακέραιο πολλαπλάσιο της μιας ώρας. Γνωρίζουμε ότι

    i) $t \leq 24$, και

    ii) ο δορυφόρος συμπληρώνει 11 περιστροφές σε χρονική περίοδο που αρχίζει όταν ένα 24ωρο ρολόι δείχνει 0 και λήγει (κάποιες ημέρες αργότερα) όταν το ρολόι δείχνει 17.
    Να βρεθεί ο t.

13. Βρείτε όλους τους $x \in \mathbb{Z}$ τέτοιους ώστε $x^2 \equiv 1 \mod 91$.

14. Έστω $m \in \mathbb{N}$ περιττός και $m = p_1^{m_1} \dots p_r^{m_r}$ η ανάλυσή του σε γινόμενο πρώτων με $p_i \neq p_j$ αν $i \neq j$. Αποδείξτε ότι η ισοτιμία $x^2 \equiv 1 \mod m$ έχει ακριβώς 2^r λύσεις $\mod m$.

15. Βρείτε όλους τους $x, y \in \mathbb{Z}$ ώστε το σύστημα

$$\begin{aligned} 2x + 4y &\equiv 3 \mod 11 \\ 3x + 2y &\equiv 5 \mod 11 \end{aligned}$$

να έχει λύση.

16. Θεωρούμε το σύστημα

$$\begin{aligned} ax + by &\equiv e \mod m \\ cx + dy &\equiv f \mod m \end{aligned}$$

και θέτουμε $\Delta = ad - bc$. Αποδείξτε ότι αν $\mu\kappa\delta(\Delta, m) = 1$, τότε υπάρχει μοναδική λύση $\mod m$ που δίνεται από

$$\begin{aligned} x &= \bar{\Delta}(de - bf) \mod m \\ y &= \bar{\Delta}(af - ce) \mod m, \end{aligned}$$

όπου $\bar{\Delta}$ είναι το αντίστροφο του Δ modulo m. (Συγκρίνατε με τον κανόνα του Cramer για τη λύση 2×2 γραμμικών συστημάτων επί του $\mathbb{R}$).

17. (Ένα αρχαίο Ινδικό πρόβλημα). Αν αφαιρεθούν τα αυγά από ένα καλάθι ανά 2, 3, 4, 5 και 6 τότε παραμένουν αντίστοιχα 1, 2, 3, 4, 5 αυγά. Όταν όμως αφαιρεθούν τα αυγά ανά 7 στο τέλος το καλάθι είναι άδειο. Ποιος είναι ο ελάχιστος αριθμός αυγών που θα μπορούσε να περιέχει το καλάθι;

18. Εξετάστε αν οι παρακάτω προτάσεις που αφορούν το $\mathbb{Z}_m$ είναι αληθείς ή ψευδείς

    i) Κάθε εξίσωση της μορφής $ax - b = 0$ $(a, b \in \mathbb{Z}_m, a \neq [0])$ έχει λύση στο $\mathbb{Z}_m$.

    ii) Κάθε εξίσωση της μορφής $ax - b = 0$ $(a, b \in \mathbb{Z}_m)$ έχει το πολύ μια λύση στο $\mathbb{Z}_m$.

    iii) Αν $x^2 = [1]$ στο $\mathbb{Z}_m$, τότε $x = [1]$ ή $x = [-1]$.

    iv) Αν $x^2 = [0]$ στο $\mathbb{Z}_m$, τότε $x = [0]$.

19. Έστω m ένας θετικός ακέραιος. Αποδείξτε ότι υπάρχουν m το πλήθος διαδοχικοί θετικοί ακέραιοι καθένας από τους οποίους διαιρείται με ένα τουλάχιστον τετράγωνο ακεραίου μεγαλυτέρου του 1.

20. Αποδείξτε ότι δεν υπάρχει ακέραιος αριθμός τέτοιος ώστε τα δύο τελευταία ψηφία του τετραγώνου του (στη συνήθη δεκαδική γραφή) να είναι 35.

21. Εξετάστε αν υπάρχει $b \in \mathbb{Z}$, $0 \leq b \leq 60$ τέτοιος ώστε το σύστημα

$$\begin{aligned} 12x &\equiv b \mod 30 \\ 22x &\equiv b \mod 11 \end{aligned}$$

να έχει λύση.

22. Βρείτε όλους τους ακεραίους x τέτοιους ώστε $x^3 + 2x^2 - x - 5 \equiv 0 \mod 105$.
Υπόδειξη: Έστω $f(x) = x^3 + 2x^2 - x - 5$. Με δοκιμές λύστε κάθε μία από τις ισοτιμές $f(x) \equiv 0 \mod 3$, $f(x) \equiv 0 \mod 5$, $f(x) \equiv 0 \mod 7$. Συνεχίστε εφαρμόζοντας το Κινεζικό Θεώρημα.

1.6 Η Συνάρτηση του Euler

Η συνάρτηση του Euler

Θα συμβολίζουμε με $\varphi(m)$ το πλήθος των στοιχείων του συνόλου $U(\mathbb{Z}_m)$ των αντιστρέψιμων στοιχείων του $\mathbb{Z}_m$. Τότε, ορίζεται μια συνάρτηση $\phi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$, που ονομάζεται ***συνάρτηση του Euler***. Από την Πρόταση 1.4.5 έπεται ότι $\varphi(m)$ είναι το πλήθος των ακεραίων a, οι οποίοι είναι τέτοιοι ώστε

$$1 \leq a \leq m \quad \text{και} \quad \mu\kappa\delta(a, m) = 1.$$

Για παράδειγμα έχουμε $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$. Είναι φανερό ότι χρησιμοποιώντας τον ορισμό δεν είναι εύκολο να υπολογιστούν οι τιμές $\varphi(m)$ για μεγάλα m. Η παρακάτω Πρόταση παρέχει έναν διαφορετικό τρόπο υπολογισμού του ακεραίου $\varphi(m)$.

1.6.1 Πρόταση.

1) Για κάθε πρώτο p ισχύει $\varphi(p^i) = p^i - p^{i-1}$.

2) Αν $\mu\kappa\delta(m, n) = 1$, τότε $\varphi(mn) = \varphi(m)\varphi(n)$.

3) Αν η ανάλυση του n σε γινόμενο πρώτων είναι $n = p_1^{n_1} \dots p_s^{n_s}$, όπου οι p_i είναι διακεκριμένοι πρώτοι αριθμοί, τότε

$$\begin{aligned}\varphi(n) &= (p_1^{n_1} - p_1^{n_1-1})(p_2^{n_2} - p_2^{n_2-1}) \dots (p_s^{n_s} - p_s^{n_s-1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_s}\right).\end{aligned}$$

Απόδειξη. Υπενθυμίζουμε από την Παράγραφο 1.4 ότι

$$U(\mathbb{Z}_m) = \{[\alpha] \in \mathbb{Z}_m | \mu\kappa\delta(\alpha, m) = 1\}$$

1) Οι θετικοί ακέραιοι που είναι μικρότεροι του p^i και δεν είναι σχετικά πρώτοι με αυτόν είναι τα πολλαπλάσια του p της μορφής ap, όπου $1 \leq a \leq p^{i-1}$. Το πλήθος τους είναι p^{i-1}. Συνεπώς το πλήθος των θετικών ακεραίων που είναι μικρότεροι του p^i και σχετικά πρώτοι προς αυτόν είναι $p^i - p^{i-1}$.

2) Αρκεί να δείξουμε ότι υπάρχει 1-1 και επί απεικόνιση

$$\psi : U(\mathbb{Z}_{mn}) \to U(\mathbb{Z}_m) \times U(\mathbb{Z}_n).$$

Ορίζουμε $\psi([a]_{mn}) = ([a]_m, [a]_n)$, όπου με $[a]_k \in \mathbb{Z}_k$ παριστάνουμε την κλάση υπολοίπων modulo k του a. Η αντιστοιχία ψ είναι μια απεικόνιση, γιατί αν $[a]_{mn} = [b]_{mn}$, τότε $mn|a-b$, οπότε $m|a-b$ και $n|a-b$, δηλαδή $[a]_m = [b]_m$ και $[a]_n = [b]_n$.

Επιπλέον, αν $[a]_{mn} \in U(\mathbb{Z}_{mn})$ τότε $([a]_m, [a]_n) \in U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$, γιατί αν $\mu\kappa\delta(mn, a) = 1$, τότε $\mu\kappa\delta(m, a) = \mu\kappa\delta(n, a) = 1$. Η ψ είναι 1-1, γιατί αν $\psi(a) = \psi(b)$, τότε $[a]_m = [b]_m$ και $[a]_n = [b]_n$, οπότε $m|a-b$ και $n|a-b$. Επειδή όμως $\mu\kappa\delta(m, n) = 1$, έχουμε $mn|a-b$, δηλαδή $[a]_{mn} = [b]_{mn}$. Τέλος, για να δούμε ότι η ψ είναι επί, παρατηρούμε ότι δοθέντος του $([a]_m, [b]_n) \in U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$, από το Κινεζικό Θεώρημα Υπολοίπων υπάρχει ακέραιος x με $x \equiv a \mod m$ και $x \equiv b \mod n$. Για το x αυτό έχουμε $\mu\kappa\delta(x, m) = \mu\kappa\delta(a, m) = 1$ και $\mu\kappa\delta(x, n) = \mu\kappa\delta(b, n) = 1$. Συνεπώς, $\mu\kappa\delta(x, mn) = 1$ και άρα $[x]_{mn} \in U(\mathbb{Z}_{mn})$. Επίσης, $\psi([x]_{mn}) = ([x]_m, [x]_n) = ([a]_m, [b]_n)$.

3) Η σχέση αυτή προκύπτει από τις 1) και 2):

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{n_1} \dots p_s^{n_s}) = \\
&= \varphi(p_1^{n_1}) \dots \varphi(p_s^{n_s}) = \\
&= (p_1^{n_1} - p_1^{n_1-1}) \dots (p_s^{n_s} - p_s^{n_s-1}) = \\
&= p_1^{n_1} \dots p_s^{n_s} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right) = \\
&= n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right).
\end{aligned}$$

Η σχέση 3) είναι χρήσιμη για υπολογισμούς. Για παράδειγμα, έχουμε $\varphi(1000) = \varphi(2^3 5^3) = \varphi(2^3)\varphi(5^3) = (8-4)(125-25) = 400$.

Σημειώνουμε ότι η σχέση 2) στο προηγούμενο Θεώρημα μπορεί να αποδειχθεί χωρίς τη χρήση του Κινεζικού Θεωρήματος Υπολοίπων. Όμως η απόδειξη που δώσαμε εδώ παρουσιάζει ενδιαφέρον γιατί χρησιμοποιεί μια διασύνδεση μεταξύ των $U(\mathbb{Z}_{mn}), U(\mathbb{Z}_m), U(\mathbb{Z}_n)$ που θα μελετηθεί γενικότερα στην Ενότητα 2.

Θεώρημα του Euler

Από το Μικρό Θεώρημα του Fermat γνωρίζουμε ότι $a^{p-1} \equiv 1 \mod p$, όταν ο p είναι ένας πρώτος αριθμός με $\mu\kappa\delta(a, p) = 1$. Θα αποδείξουμε εδώ μια γενίκευση που λέει ότι $a^{\varphi(m)} \equiv 1 \mod m$, όπου $a, m \in \mathbb{Z}$, $m > 0$ και $\mu\kappa\delta(a, m) = 1$.

Έστω $[a], [b] \in U(\mathbb{Z}_m)$. Επειδή $\mu\kappa\delta(a, m) = \mu\kappa\delta(b, m) = 1$ έχουμε $\mu\kappa\delta(ab, m) = 1$. Πράγματι, κάθε πρώτος αριθμός που είναι κοινός διαιρέτης των ab και m θα διαιρεί έναν τουλάχιστον από τα a, b (Λήμμα 1.2.5) και κατά συνέπεια θα διαιρεί έναν τουλάχιστον από τους $\mu\kappa\delta(a, m)$, $\mu\kappa\delta(b, m)$. Αυτό είναι άτοπο. Συνεπώς αποδείξαμε ότι

$$[a], [b] \in U(\mathbb{Z}_m) \Rightarrow [ab] \in U(\mathbb{Z}_m). \tag{1}$$

Έστω

$$U(\mathbb{Z}_m) = \{[a_1], \dots, [a_k]\}, \quad k = \varphi(m). \tag{2}$$

Έστω $[a] \in U(\mathbb{Z}_m)$. Από το (1) έχουμε ότι $[aa_i] \in U(\mathbb{Z}_m)$, $i = 1, \ldots, k$. Επιπλέον τα στοιχεία αυτά είναι ανά δύο διάφορα, γιατί αν $[aa_i] = [aa_j]$, τότε $m|a(a_i - a_j)$, οπότε $m|a_i - a_j$, αφού $\mu\kappa\delta(a, m) = 1$, και άρα $[a_i] = [a_j]$. Επειδή τώρα το πλήθος των $[aa_i]$ είναι k, που είναι ο πληθάριθμος του $U(\mathbb{Z}_m)$, και επειδή το k είναι πεπερασμένο, παίρνουμε

$$U(\mathbb{Z}_m) = \{[aa_1], \ldots, [aa_k]\}. \tag{3}$$

Σχηματίζουμε το γινόμενο όλων των στοιχείων του $U(\mathbb{Z}_m)$. Από τις (3) και (2) παίρνουμε

$$\begin{aligned} &[aa_1] \ldots [aa_k] = [a_1] \ldots [a_k] \Rightarrow \\ &[a^k][a_1 \ldots a_k] = [a_1 \ldots a_k]. \end{aligned} \tag{4}$$

Από τη σχέση (1) έχουμε $[a_1 \ldots a_k] \in U(\mathbb{Z}_m)$. Πολλαπλασιάζοντας την (4) με το αντίστροφο του $[a_1 \ldots a_k]$ παίρνουμε

$$[a^k] = [1],$$

δηλαδή

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Έχουμε αποδείξει το ακόλουθο αποτέλεσμα.

1.6.2 Θεώρημα (*Euler*). [1] *Έστω $a, m \in \mathbb{Z}$ και $m > 0$. Αν $\mu\kappa\delta(a, m) = 1$, τότε*

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Από το Θεώρημα αυτό βλέπουμε ότι αν $\mu\kappa\delta(a, m) = 1$, τότε το αντίστροφο του $[a] \in \mathbb{Z}_m$ είναι το $[a^{\varphi(m)-1}]$.

Στην ειδική περίπτωση του Θεωρήματος του Euler που ο $m = p$ είναι πρώτος, έχουμε $\varphi(m) = p - 1$ και επιπλέον ισχύει $\mu\kappa\delta(a, p) = 1$ αν και μόνο αν ο p δεν διαιρεί τον a. Άρα προκύπτει μια άλλη απόδειξη για το Μικρό Θεώρημα του Fermat.

Το Θεώρημα του Euler μας επιτρέπει συχνά να υπολογίζουμε υπόλοιπα διαιρέσεων μεγάλων αριθμών. Για παράδειγμα, ας βρούμε το υπόλοιπο της διαίρεσης του 365^{2002} με το 24. Ισχύει $365 = 15 \cdot 24 + 5$ και άρα $365 \equiv 5 \mod 24$. Επίσης

[1] Ο Euler (1707-1783) ξεκίνησε στις σπουδές του στο Πανεπιστήμιο του Basel της Ελβετίας όταν ήταν μόλις 13 χρονών και τρία χρόνια αργότερα απέκτησε master's στη Φιλοσοφία. Εργάστηκε δε σε πολλούς τομείς των Μαθηματικών αλλά και άλλων κλάδων, όπως είναι για παράδειγμα η Ναυπηγική, Υδροδυναμική και Μηχανική. Το επιστημονικό έργο του είναι τεράστιο και ο Euler θεωρείται ο πολυγραφότατος Μαθηματικός όλων των εποχών.

$\varphi(24) = \varphi(2^3 3) = (2^3 - 2^2)(3-1) = 8$ (Πρόταση 1.6.1). Καθώς $\mu\kappa\delta(5, 24) = 1$, από το Θεώρημα του Euler έχουμε $5^8 \equiv 1 \mod 24$. Επειδή $2002 = 250 \cdot 8 + 2$ έχουμε

$$365^{2002} = (365^8)^{250} \cdot 365^2 \equiv (5^8)^{250} \cdot 5^2 \equiv 1^{250} \cdot 5^2 \equiv 1 \mod 24.$$

1.6.3 Παραδείγματα.

1. Για κάθε ακέραιο a με $\mu\kappa\delta(a, 72) = 1$ ισχύει $a^{12} \equiv 1 \mod 72$.
   Αν εφαρμόσουμε άμεσα το Θεώρημα του Euler, λαμβάνουμε $a^{\varphi(72)} = a^{\varphi(8)\varphi(9)} = a^{24} \equiv 1 \mod 72$ που δεν είναι η ζητούμενη ισοτιμία. Για αυτό εργαζόμαστε κάπως διαφορετικά: Αρκεί να δείξουμε ότι $a^{12} \equiv 1 \mod 8$ και $a^{12} \equiv 1 \mod 9$, γιατί οι ακέραιοι 8,9 είναι σχετικά πρώτοι. Επειδή $\mu\kappa\delta(a, 72) = 1$ έχουμε ότι $\mu\kappa\delta(a, 8) = 1$ και άρα από το Θεώρημα του Euler ισχύει $a^{\varphi(8)} = a^4 \equiv 1 \mod 8$. Επομένως έχουμε $a^{12} = (a^4)^3 \equiv 1 \mod 8$. Όμοια αποδεικνύεται και η ισοτιμία $a^{12} \equiv 1 \mod 9$.

2. Έστω $a, m \in \mathbb{Z}$ με $m > 0$ και $\mu\kappa\delta(a, m) = 1$. Έστω k ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $a^k \equiv 1 \mod m$ (τέτοιος k υπάρχει από το Θεώρημα του Euler και το Αξίωμα Ελαχίστου). Τότε $k|\varphi(m)$.
   Πράγματι, από τον Αλγόριθμο Διαίρεσης έχουμε $\varphi(m) = qk + r, 0 \leq r < k$. Συνεπώς $a^{\varphi(m)} = (a^k)^q a^r$. Από το Θεώρημα του Euler και τον ορισμό του k παίρνουμε $1 \equiv a^r \mod m$. Λόγω του ελαχίστου του k παίρνουμε $r = 0$. Άρα $k|\varphi(m)$.

Η μέθοδος κρυπτογράφησης RSA

Η Κρυπτογραφία ασχολείται με την εύρεση και υλοποίηση μεθόδων αποστολής και λήψης μυστικών μηνυμάτων. Θα περιγράψουμε εδώ το σύστημα κρυπτογράφησης RSA.[2] Αυτό είναι από τα πιο διαδεδομένα συστήματα καθώς χρησιμοποιείται από κράτη και οργανισμούς για διπλωματικούς, στρατιωτικούς και οικονομικούς σκοπούς, όπως και από πολίτες σε καθημερινές οικονομικές συναλλαγές (π.χ. αγορές με πιστωτική κάρτα).

Το RSA συνίσταται στα επόμενα βήματα.

Βήμα 1: Ο προτιθέμενος παραλήπτης του μηνύματος επιλέγει δύο διακεκριμένους μεγάλους πρώτους αριθμούς (πχ της τάξης του 10^{100}). Στη συνέχεια θέτει $n = pq$ και επιλέγει έναν θετικό ακέραιο e σχετικά πρώτο με τον $\varphi(n) = (p-1)(q-1)$. Το ζεύγος (e, n) γνωστοποιείται στον προτιθέμενο αποστολέα (κατά φανερό τρόπο).

Βήμα 2 (κρυπτογράφηση): Ο αποστολέας μετατρέπει το μήνυμα που θέλει να στείλει σε μια σειρά από ψηφία σύμφωνα με την 1-1 αντιστοιχία $A \mapsto 01, B \mapsto$

[2] Το σύστημα RSA επινοήθηκε από τους Rivest, Shamir και Adleman το 1978.

$02, \ldots, \Omega \mapsto 24$. Στη συνέχεια ομαδοποιεί τα ψηφία σε τετραψήφιους αριθμούς. Για καθέναν, X, από τους τετραψήφιους αυτούς αριθμούς υπολογίζει

$$Y(X) \equiv X^e \mod n, \quad 0 < Y(X) < n.$$

Δηλαδή, $Y(X)$ είναι το υπόλοιπο της διαίρεσης του X^e με τον n. Οι αριθμοί $Y(X)$ στέλνονται στον παραλήπτη (κατά φανερό τρόπο).

Βήμα 3 (αποκρυπτογράφηση): Καθώς από την υπόθεση είναι $\mu\kappa\delta(e, \varphi(n)) = 1$, η κλάση $[e]$ στο $\mathbb{Z}_{\varphi(n)}$ είναι αντιστρέψιμη (Πρόταση 1.4.5). Άρα υπάρχει $d \in \mathbb{N}$ με $de = k\varphi(n) + 1$, για κάποιο $k \in \mathbb{Z}$. Ο παραλήπτης υπολογίζει ένα τέτοιο d (πχ με τον Ευκλείδειο Αλγόριθμο). Στη συνέχεια υψώνει κάθε $Y(X)$ στη δύναμη d και εφαρμόζει το Θεώρημα του Euler

$$Y(X)^d \equiv X^{ed} = X^{k\varphi(n)+1} = (X^{\varphi(n)})^k X \equiv X \mod n.$$

(Παρατηρούμε ότι η υπόθεση του Θεωρήματος του Euler, $\mu\kappa\delta(X, n) = 1$, ισχύει εδώ γιατί τα p, q είναι τουλάχιστον πενταψήφιοι αριθμοί ενώ οι X είναι τετραψήφιοι). Έτσι επανακτώνται οι αριθμοί X, δηλαδή το αρχικό μη κρυπτογραφημένο μήνυμα.

Για παράδειγμα, έστω $p = 43$ και $q = 59$. (Στην πράξη θα επιλέγαμε μεγάλους αριθμούς). Τότε $n = pq = 2537$ και $\varphi(n) = (p-1)(q-1) = 2436$. Έστω $e = 13$ οπότε $\mu\kappa\delta(13, 2436) = 1$. Ας υποθέσουμε ότι θέλουμε να στείλουμε το παρακάτω μήνυμα (χωρίς την τελεία)

ΤΑ ΜΑΘΗΜΑΤΙΚΑ ΕΙΝΑΙ ΧΡΗΣΙΜΑ.

Μετατρέπουμε το μήνυμα σε μια σειρά από ψηφία και ομαδοποιούμε σε τετραψήφιους αριθμούς λαμβάνοντας

1901 1201 0807 1201 1909 1001
0509 1301 1922 1707 1809 1201

σύμφωνα με το πρώτο τμήμα του Βήματος 2. (Αν στην τελευταία ομαδοποίηση είχαμε 2 ψηφία, θα προσθέταμε το "ανύπαρκτο γράμμα" 25 δύο φορές). Υπολογίζοντας τα $Y(X)$ βρίσκουμε[3]

0445 2224 1123 2224 0572 0304
2315 2326 2256 0155 2334 2224

που είναι το κρυπτογραφημένο μήνυμα που στέλνουμε στον παραλήπτη.

[3]Οι συγκεκριμένοι υπολογισμοί έγιναν με το πρόγραμμα GAP

Ο παραλήπτης υπολογίζει με τη βοήθεια του Ευκλείδειου αλγόριθμου ότι στο $\mathbb{Z}_{2436}$ το αντίστροφο του [13] είναι το [937] (βλ Εφαρμογή 1.4.6). Στη συνέχεια υπολογίζει τους X σύμφωνα με το Βήμα 3,

$$X \equiv Y(X)^{937} \mod 2537, \quad 0 \leq X < 2537,$$

εφόσον $\mu\kappa\delta(X, 2537) = 1$. (Ελέγχουμε ότι στο συγκεκριμένο παράδειγμα ικανοποιείται αυτή η συνθήκη για κάθε X. Αν είχαμε επιλέξει μεγάλα p, q τότε αυτός ο έλεγχος δεν θα ήταν απαραίτητος).

Παρατηρήσεις

1. Η ασφάλεια της μεθόδου RSA οφείλεται στο γεγονός ότι μέχρι σήμερα και παρά την ταχύτητα των υπολογιστών είναι εξαιρετικά χρονοβόρο - και άρα πρακτικά αδύνατο - να παραγοντοποιηθούν μεγάλοι αριθμοί. Αν η παραγοντοποίηση του n ήταν γνωστή (σε έναν υποκλοπέα του μηνύματος) τότε θα ήταν γνωστή η τιμή $\varphi(n)$ λόγω της Πρότασης 1.6.1. Συνεπώς θα μπορούσε να υπολογιστεί ο ακέραιος d και στη συνέχεια να γίνει η αποκρυπτογράφηση. Μέχρι σήμερα, είναι ανοικτό ερώτημα αν υπάρχει τρόπος αποκρυπτογράφησης μηνυμάτων που έχουν κρυπτογραφηθεί με το RSA, χωρίς να χρησιμοποιείται η παραγοντοποίηση του n.

2. Η εύρεση μεγάλων πρώτων αριθμών p, q δεν απαιτεί παρά ελάχιστα λεπτά σε υπολογιστές. Οι υπολογισμοί στα Βήματα 2 και 3 του RSA απαιτούν λίγα δευτερόλεπτα σε υπολογιστές όταν οι αριθμοί n, e, d έχουν το πολύ 200 ψηφία.

3. Ένας τρόπος επιλογής του e είναι η εύρεση ένος πρώτου μεγαλύτερου των p, q αφού τότε $\mu\kappa\delta(e, (p-1)(q-1)) = 1$. Πάντως, όπως και να επιλεγεί ο e θα πρέπει να ικανοποιεί την ανισότητα $101^e > n$ (ο αριθμός 101=0101 αντιστοιχεί στα γράμματα AA). Αν είχαμε $2424^e < n$ (ο αριθμός 2424 αντιστοιχεί στα γράμματα $\Omega\Omega$), τότε το κρυπτογραφημένο μήνυμα θα μπορούσε να αποκρυπτογραφηθεί απλά λαμβάνοντας ρίζες e-τάξης των $Y(X)$. Με άλλα λόγια, το e πρέπει να είναι αρκετά μεγάλο ώστε στο Βήμα 2 να συμβαίνει αναγωγή modulo n.

4. Η ομαδοποίηση στο Βήμα 2 θα μπορούσε να γίνει και σε εξάδες, οκτάδες κλπ.

Ασκήσεις 1.6

1. Βρείτε το υπόλοιπο της διαίρεσης του 5^{1000} με το 14.

2. Ποιά είναι τα τελευταία 2 ψηφία του 7^{100} στο δεκαδικό σύστημα;

3. Ποιά ένδειξη θα δείχνει ένα 24ωρο ρολόι 7^{19} ώρες μετά τις 1:00;

4. Έστω $a, b \in \mathbb{Z}$ σχετικά πρώτοι ακέραιοι. Αποδείξτε ότι $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \mod ab$.

5. Αποδείξτε ότι $a^7 \equiv a \mod 63$ αν $\mu\kappa\delta(a, 3) = 1$.

6. Έστω a, m θετικοί ακέραιοι με $\mu\kappa\delta(a, m) = \mu\kappa\delta(a-1, m) = 1$. Αποδείξτε ότι $1 + a + a^2 + \cdots + a^{\varphi(m)-1} \equiv 0 \mod m$.

7. i) Να βρεθεί ο ελάχιστος θετικός ακέραιος k ώστε $2^k \equiv 1 \mod 7$.
   ii) Έστω m ένας θετικός ακέραιος, $a \in \mathbb{Z}$, με $\mu\kappa\delta(a, m) = 1$, και k ο ελάχιστος θετικός ακέραιος ώστε $a^k \equiv 1 \mod m$. Αν $k > \varphi(m)/2$, αποδείξτε ότι $k = \varphi(m)$.

8. Αποδείξτε ότι η μοναδική λύση modulo M του συστήματος

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ &\vdots \\ x &\equiv a_r \mod m_r \end{aligned}$$

   όπου τα m_i είναι ανά δύο σχετικά πρώτοι ακέραιοι, δίνεται από

$$x \equiv a_1 M_1^{\varphi(m_1)} + \cdots + a_r M_r^{\varphi(m_r)} \mod M,$$

   όπου $M_i = M/m_i$, $M = m_1 m_2 \ldots m_r$.

9. Αποδείξτε ότι αν ο n διαιρείται με k διακεκριμένους περιττούς πρώτους, τότε $2^k | \varphi(n)$.

10. Αποδείξτε ότι

$$\varphi(2n) = \begin{cases} \varphi(n), & \text{αν } n \text{ περιττός} \\ 2\varphi(n), & \text{αν } n \text{ άρτιος} \end{cases}$$

11. Για κάθε θετικούς ακεραίους n, k αποδείξτε ότι $\varphi(n^k) = n^{k-1}\varphi(n)$.

12. Αποδείξτε ότι $\varphi(mn) = \dfrac{d}{\varphi(d)}\varphi(m)\varphi(n)$, όπου $d = \mu\kappa\delta(a, b)$.

13. Για ποια n ο $\varphi(n)$ είναι άρτιος;

14. Αποδείξτε ότι $\varphi(n)|n$ αν και μόνο αν $n = 1$, 2^a ή $2^a \cdot 3^b$, όπου a, b είναι θετικοί ακέραιοι.

15. Ένα κλάσμα $\frac{a}{b}$, όπου $a, b \in \mathbb{Z} - \{0\}$, ονομάζεται ανάγωγο αν $\mu\kappa\delta(a, b) = 1$. Αποδείξτε ότι το πλήθος των αναγώγων κλασμάτων $\frac{a}{b}$ με $1 \leq a < b \leq n$ είναι $\sum_{k=1}^{n} \varphi(k)$.

16. Έστω d, n θετικοί ακέραιοι με $d|n$. Θέτουμε $A_d = \{m \in \{1, \ldots, n\} | \mu\kappa\delta(m, n) = d\}$.

    1) Αποδείξτε ότι το σύνολο A_d περιέχει ακριβώς $\varphi(n/d)$ στοιχεία.
    2) Συμπεράνατε ότι $n = \sum_{d|n} \varphi(n/d)$ από την ξένη ένωση $\{1, \ldots, n\} = \bigcup_{d|n} A_d$.
    3) Άρα $n = \sum_{d|n} \varphi(d)$.

17. Έστω m, n θετικοί ακέραιοι και $a \in \mathbb{Z}$ με $\mu\kappa\delta(m, n) = \mu\kappa\delta(a, mn) = 1$. Αποδείξτε ότι $a^k \equiv 1 \mod mn$ για κάθε κοινό πολλαπλάσιο k των $\varphi(m)$ και $\varphi(n)$.

18. Αποκρυπτογραφήσετε το μήνυμα

    0456 1863 2228 1736 1588 2132 1134
    2225 1092 1593 1278 0095 1588 0739
    2495 0129 1157 0629 1786

    που κρυπτογραφήθηκε με τη μέθοδο RSA για $n = 43 \cdot 59 = 2537$ και $e = 13$. (Θα χρειαστείτε κάποιο υπολογιστικό πρόγραμμα γιατί διαφορετικά οι πράξεις θα είναι χρονοβόρες).

19. Γιατί στο Βήμα 2 του RSA έχουμε $0 < Y(X) < n$ και όχι $0 \leq Y(X) < n$;