# Θεωρία Αριθμών

## Πρόχειρες Σημειώσεις

Μιχάλης Παπαδημητράκης

Τμήμα Μαθηματικών

Πανεπιστήμιο Κρήτης

# Περιεχόμενα

# Κεφάλαιο 1

# Προκαταρκτικά.

Το σύνολα των **ακεραίων**

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

συμβολίζεται $\mathbb{Z}$ και το σύνολο των θετικών ακεραίων ή **φυσικών**

$$1, 2, 3, \ldots$$

συμβολίζεται $\mathbb{N}$.

Οι τέσσερις πράξεις - πρόσθεση, αφαίρεση, πολλαπλασιασμός και διαίρεση - και οι ιδιότητές τους καθώς και οι ιδιότητες της διάταξης των ακεραίων ως προς το μέγεθός τους θεωρούνται γνωστές.

Επίσης, θεωρούνται γνωστοί οι **ρητοί**, οι **πραγματικοί** και οι **μιγαδικοί**, των οποίων τα σύνολα συμβολίζονται $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$, αντιστοίχως.

Αναφέροντάς τες ξεχωριστά, θα τονίσουμε μερικές ιδιότητες των ακεραίων, οι οποίες δεν ισχύουν για τους ρητούς, πραγματικούς και μιγαδικούς αριθμούς. Και αυτές οι ιδιότητες θεωρούνται γνωστές.

1. *Κάθε ακέραιος $a$ έχει δυο γειτονικούς ακέραιους: τον προηγούμενό του $a-1$ και τον επόμενό του $a+1$. Δεν υπάρχει άλλος ακέραιος ανάμεσα στους $a-1, a+1$ εκτός από τον $a$.* Αυτή η ιδιότητα παίρνει και την εξής ισοδύναμη μορφή: *αν $a, b$ είναι ακέραιοι και $a < b$, τότε $a+1 \leq b$ και $a \leq b-1$.*

2. *Κάθε μη-κενό υποσύνολο του $\mathbb{Z}$, το οποίο είναι κάτω φραγμένο, έχει ελάχιστο στοιχείο.* Η ιδιότητα αυτή του $\mathbb{Z}$ ονομάζεται **αρχή της καλής διάταξης** και έχει την εξής ισοδύναμη μορφή: *κάθε μη-κενό υποσύνολο του $\mathbb{Z}$, το οποίο είναι άνω φραγμένο, έχει μέγιστο στοιχείο.*

3. *Αν μια ιδιότητα ισχύει για κάποιον συγκεκριμένο ακέραιο $a_0$ και αν, με την υπόθεση ότι η ιδιότητα αυτή ισχύει για τον οποιονδήποτε ακέραιο $a \geq a_0$, αποδείξουμε ότι η ιδιότητα ισχύει και για τον $a+1$, τότε θα έχουμε ως συμπέρασμα ότι η ιδιότητα ισχύει για κάθε ακέραιο $a \geq a_0$.* Αυτό είναι η γνωστή **αρχή της μαθηματικής επαγωγής** και έχει και την εξής ισοδύναμη μορφή: *αν μια ιδιότητα ισχύει για κάποιον συγκεκριμένο ακέραιο $a_0$ και αν, με την υπόθεση ότι η ιδιότητα αυτή ισχύει για κάθε ακέραιο $k$ με $a_0 \leq k < a$, αποδείξουμε ότι η ιδιότητα ισχύει και για τον ακέραιο $a > a_0$, τότε θα έχουμε ως συμπέρασμα ότι η ιδιότητα ισχύει για κάθε ακέραιο $a \geq a_0$.*

4. *Για κάθε πραγματικό $x$ υπάρχει μοναδικός ακέραιος $m$ ώστε $m \leq x < m+1$.* Ο $m$ ονομάζεται **ακέραιο μέρος** του $x$ και συμβολίζεται $[x]$.

5. *Το πλήθος των ακεραίων που βρίσκονται ανάμεσα σε δυο ακέραιους είναι πεπερασμένο.* Πιο συγκεκριμένα, *αν οι $a, b$ είναι ακέραιοι με $a \leq b$, τότε το πλήθος των ακεραίων $k$ με $a \leq k \leq b$ είναι $b-a+1$.*

Από τώρα και στο εξής, όταν αναφέρουμε την λέξη “αριθμός” θα εννοούμε πάντοτε ακέραιος. Άρα “θετικός αριθμός” θα σημαίνει φυσικός. Οποιοιδήποτε άλλοι αριθμοί θα αναφέρονται οπωσδήποτε ως “ρητοί” ή “πραγματικοί” ή “μιγαδικοί”, ανάλογα με την περίπτωση.

Όλα τα μικρά ελληνικά ή λατινικά γράμματα θα συμβολίζουν ακέραιους (εκτός αν καθορίζεται ότι πρόκειται για ρητούς ή πραγματικούς ή μιγαδικούς).

Όταν λέμε “γραμμικός συνδυασμός” των ακεραίων $a, b, \ldots, f$ θα εννούμε μια παράσταση της μορφής

$$xa + yb + \cdots + wf,$$

όπου οι $x, y, \ldots, w$ είναι ακέραιοι.

# Κεφάλαιο 2

# Διαιρετότητα.

## 2.1 Διαιρετότητα.

**ΟΡΙΣΜΟΣ.** *Λέμε ότι ο* $a \neq 0$ **διαιρεί** *τον* $b$ *αν υπάρχει* $q$ *ώστε*

$$b = qa.$$

*Αντιθέτως, λέμε ότι ο* $a \neq 0$ **δεν διαιρεί** *τον* $b$ *αν δεν υπάρχει* $q$ *ώστε* $b = qa$*. Στην πρώτη περίπτωση συμβολίζουμε*

$$a \mid b$$

*και στην δεύτερη περίπτωση συμβολίζουμε* $a \nmid b$*.*

Παρατηρήστε ότι οι εκφράσεις "ο $a$ διαιρεί τον $b$" και "ο $a$ δεν διαιρεί τον $b$" και οι συμβολισμοί $a \mid b$ και $a \nmid b$ δεν έχουν νόημα όταν $a = 0$.

Το $a \mid b$ εκφράζεται και ως εξής: "ο $b$ διαιρείται από τον $a$", "ο $b$ είναι πολλαπλάσιο του $a$", "ο $a$ είναι παράγων του $b$" και "ο $a$ είναι διαιρέτης του $b$".

**Παράδειγμα.** $2 \mid 8,\ -3 \mid 6,\ -7 \mid -21,\ 4 \mid -20,\ 7 \nmid 8,\ 8 \nmid 2.$

**Παράδειγμα.** $1 \mid b.$

**Παράδειγμα.** Αν $a \neq 0$, τότε $a \mid a$ και $a \mid 0$.

Η επόμενη πρόταση καταγράφει μερικές στοιχειώδεις ιδιότητες της διαρετότητας.

**Πρόταση 2.1.** [α] *Η σχέση διαιρετότητας δυο αριθμών δεν επηρεάζεται από οποιεσδήποτε αλλαγές στα πρόσημα των δυο αριθμών. Δηλαδή,*

$$a \mid b \quad \Rightarrow \quad a \mid -b,\ -a \mid b,\ -a \mid -b.$$

[β] *Η σχέση διαιρετότητας συνεπάγεται σχέση διάταξης. Δηλαδή,*

$$a \mid b,\ b \neq 0 \quad \Rightarrow \quad |a| \leq |b|.$$

[γ] *Η σχέση διαιρετότητας είναι αντισυμμετρική. Δηλαδή,*

$$a \mid b,\ b \mid a \quad \Rightarrow \quad a = \pm b.$$

[δ] *Η σχέση διαιρετότητας είναι μεταβατική. Δηλαδή,*

$$a \mid b,\ b \mid c \quad \Rightarrow \quad a \mid c.$$

[ε] *Η σχέση διαιρετότητας δυο αριθμών δεν επηρεάζεται αν πολλαπλασιάσουμε ή διαιρέσουμε τους δυο αριθμούς με τον ίδιο μη-μηδενικό αριθμό. Δηλαδή,*

$$a \mid b,\ c \neq 0 \quad \Leftrightarrow \quad ac \mid bc.$$

[στ] *Αν ένας αριθμός διαιρεί κάποιους άλλους αριθμούς, τότε διαιρεί και κάθε γραμμικό συνδυασμό αυτών των αριθμών. Δηλαδή,*

$$a \mid b,\ a \mid c,\ \ldots,\ a \mid f \quad \Rightarrow \quad a \mid xb + yc + \cdots + wf.$$

*Απόδειξη.* [α] Έστω $a \mid b$. Τότε $a \neq 0$, οπότε και $-a \neq 0$. Επίσης, ισχύει $b = qa$ για κάποιον $q$. Άρα

$$-b = (-q)a, \quad b = (-q)(-a), \quad -b = q(-a).$$

Άρα $a \mid -b$, $-a \mid b$, $-a \mid -b$.

[β] Έστω $a \mid b$, $b \neq 0$. Τότε ισχύει $b = qa$ για κάποιον $q$. Και, επειδή $b \neq 0$, συνεπάγεται $q \neq 0$, οπότε $|q| \geq 1$. Άρα

$$|b| = |q||a| \geq |a|.$$

[γ] Έστω $a \mid b$, $b \mid a$. Τότε $a, b \neq 0$ και από την ιδιότητα [β] συνεπάγεται $|a| \leq |b|$ και $|b| \leq |a|$. Άρα $|a| = |b|$, οπότε $a = \pm b$.

[δ] Έστω $a \mid b$, $b \mid c$. Τότε $a \neq 0$. Επίσης, ισχύει $b = q_1 a$ και $c = q_2 b$ για κάποιους $q_1, q_2$. Άρα

$$c = q_2(q_1 a) = (q_2 q_1)a$$

και, επομένως, $a \mid c$.

[ε] Έστω $a \mid b$ και $c \neq 0$. Τότε $a \neq 0$, οπότε $ac \neq 0$. Επίσης, ισχύει $b = qa$ για κάποιον $q$. Συνεπάγεται

$$bc = (qa)c = q(ac)$$

και άρα $ac \mid bc$.

Αντιστρόφως, έστω $ac \mid bc$. Τότε $ac \neq 0$, οπότε $a, c \neq 0$. Επίσης, ισχύει

$$bc = q(ac) = (qa)c$$

για κάποιον $q$ και, επειδή $c \neq 0$, συνεπάγεται $b = qa$. Άρα $a \mid b$.

[στ] Έστω $a \mid b$, $a \mid c,\ \ldots,\ a \mid f$. Τότε $a \neq 0$. Επίσης, ισχύει $b = qa$, $c = ra,\ \ldots,\ f = ta$ για κάποιους $q, r, \ldots, t$. Άρα

$$xb + yc + \cdots + wf = xqa + yra + \cdots + wta = (xq + yr + \cdots + wt)a$$

και, επομένως, $a \mid xb + yc + \cdots + wf$. □

## 2.2 Η Ευκλείδεια διαίρεση.

Τώρα έχουμε το εξής πολύ σημαντικό αποτέλεσμα.

**Θεώρημα 2.1.** *Για κάθε $a > 0$ και $b$, υπάρχουν μοναδικοί $q, r$ ώστε*

$$\boxed{b = qa + r, \quad 0 \leq r < a.}$$

*Απόδειξη. Ύπαρξη των $q, r$.* Θεωρούμε το σύνολο $A$ όλων των πολλαπλασίων του $a$ τα οποία είναι $\leq b$. Δηλαδή,

$$A = \{xa \,|\, xa \leq b\}.$$

Η επιλογή $x = -|b|$ δίνει

$$xa = (-|b|)a \leq -|b| \leq b.$$

Άρα το $A$ είναι μη-κενό. Επίσης, το $A$ είναι άνω φραγμένο από τον $b$. Άρα το $A$ έχει μέγιστο στοιχείο και ας υποθέσουμε ότι αυτό το μέγιστο στοιχείο του $A$ είναι το $qa$. Τότε

$$qa \leq b < (q+1)a.$$

Θέτουμε

$$r = b - qa$$

και τότε

$$b = qa + r, \quad 0 \leq r < a.$$

*Μοναδικότητα των $q, r$.* Έστω

$$b = q_1 a + r_1, \quad 0 \leq r_1 < a$$

$$b = q_2 a + r_2, \quad 0 \leq r_2 < a.$$

Τότε

$$(q_2 - q_1)a = r_1 - r_2, \qquad -a < r_1 - r_2 < a.$$

Άρα

$$-1 < q_2 - q_1 < 1.$$

Συνεπάγεται $q_2 - q_1 = 0$, οπότε $q_2 = q_1$ και, επομένως, $r_2 = r_1$. □

Αν $a < 0$, έχουμε μια παραλλαγή του προηγούμενου αποτελέσματος. Και πάλι υπάρχουν μοναδικοί $q, r$ ώστε

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

Πράγματι, εφαρμόζουμε το αποτέλεσμα που αποδείξαμε στους $|a|, b$ και βρίσκουμε $q', r$ ώστε $b = q'|a| + r$ και $0 \leq r < |a|$ και κατόπιν θέτουμε $q = -q'$.

Οι δυο σχέσεις

$$b = qa + r, \quad 0 \leq r < a$$

μαζί ονομάζονται **ταυτότητα της Ευκλείδειας διαίρεσης** του $b$ από τον $a$. Οι $q, r$ ονομάζονται **πηλίκο** και **υπόλοιπο**, αντιστοίχως, της Ευκλείδειας διαίρεσης του $b$ από τον $a$.

Από την ταυτότητα της Ευκλείδειας διαίρεσης έχουμε

$$\frac{b}{a} = q + \frac{r}{a}, \qquad 0 \leq \frac{r}{a} < 1$$

και, επομένως,

$$q \leq \frac{b}{a} < q + 1.$$

Άρα

$$q = \left[\frac{b}{a}\right]$$

και συμπεραίνουμε ότι το πηλίκο της διαίρεσης του $b$ από τον $a > 0$ είναι το ακέραιο μέρος του ρητού $\frac{b}{a}$.

Βλέπουμε, λοιπόν, ότι η διαίρεση του $b$ από τον $a > 0$ καταλήγει σε ένα από τα εξής πιθανά υπόλοιπα:

$$0,\ 1,\ \ldots,\ a - 1.$$

Το πλήθος των πιθανών υπολοίπων είναι $a$.

**Παράδειγμα.** Αν $a = 2$, τα πιθανά υπόλοιπα είναι $0$ και $1$. Αν $b = 2q$, τότε ο $b$ ονομάζεται **άρτιος** ή **ζυγός**. Αν $b = 2q + 1$, τότε ο $b$ ονομάζεται **περιττός** ή **μονός**.

Παρατηρούμε ότι, αν $a > 0$, η σχέση $a \mid b$ ισοδυναμεί με το να έχουμε υπόλοιπο $r = 0$ στην Ευκλείδεια διαίρεση του $b$ από τον $a$.

## 2.3 Ασκήσεις.

1. Χωρίς να χρησιμοποιήσετε την αρχή της επαγωγής, αποδείξτε ότι κάθε αριθμός $n(n+1)$ είναι άρτιος και ότι κάθε αριθμός $n(n+1)(n+2)$ διαιρείται από τον 6.

2. Αποδείξτε ότι, αν ένας αριθμός γράφεται $6k+5$ για κάποιον $k$, τότε γράφεται $3l+2$ για κάποιον $l$. Αποδείξτε ότι το αντίστροφο δεν ισχύει.

3. Αποδείξτε ότι οι $a, a+2, a+4$ δίνουν τα τρία διαφορετικά υπόλοιπα $0, 1, 2$ όταν διαιρεθούν από τον 3.

4. Αποδείξτε ότι κανένας αριθμός της μορφής $3k-1$ δεν είναι τέλειο τετράγωνο.

5. Αποδείξτε ή δώστε αντιπαράδειγμα: $a \mid b+c \;\Rightarrow\; a \mid b$ ή $a \mid c$.

6. Αποδείξτε την εξής παραλλαγή της ταυτότητας της Ευκλείδειας διαίρεσης: για κάθε $a > 0$ και κάθε $b, m$ υπάρχουν μοναδικοί $q, r$ ώστε

$$b = qa + r, \quad m \leq r < m + a.$$

   Μπορείτε είτε να χρησιμοποιήσετε την συνήθη ταυτότητα της Ευκλείδειας διαίρεσης είτε να μιμηθείτε την απόδειξή της.

7. Αποδείξτε ότι $15 \mid 2^{4n} - 1$.

8. Αποδείξτε με την αρχή της επαγωγής ότι για κάθε φυσικό $n$ το $n! = 1 \cdot 2 \cdots n$ διαιρεί το γινόμενο $(m+1)(m+2)\cdots(m+n)$ οποιωνδήποτε $n$ διαδοχικών φυσικών.

## 2.4 Λύσεις ασκήσεων.

1. Γνωρίζουμε ότι από δυο διαδοχικούς αριθμούς $n, n+1$ ακριβώς ο ένας είναι άρτιος και, επομένως, ο $n(n+1)$ είναι άρτιος. Πιο συγκεκριμένα, κάθε $n$ είναι είτε της μορφής $2k$ είτε της μορφής $2k+1$. Οπότε διακρίνουμε περιπτώσεις:

$$\begin{aligned} n = 2k &\quad\Rightarrow\quad n(n+1) = 2k(2k+1) = 2m \\ n = 2k+1 &\quad\Rightarrow\quad n(n+1) = 2(2k+1)(k+1) = 2m, \end{aligned}$$

   οπότε σε κάθε περίπτωση ο $n(n+1)$ είναι πολλαπλάσιο του 2.
   Τώρα, κάθε $n$ είναι είτε της μορφής $6k$ είτε της μορφής $6k+1$ είτε της μορφής $6k+2$ είτε της μορφής $6k+3$ είτε της μορφής $6k+4$ είτε της μορφής $6k+5$. Πάλι διακρίνουμε περιπτώσεις:

$$\begin{aligned} n = 6k &\quad\Rightarrow\quad n(n+1)(n+2) = 12k(6k+1)(3k+1) = 6m \\ n = 6k+1 &\quad\Rightarrow\quad n(n+1)(n+2) = 6(6k+1)(3k+1)(2k+1) = 6m \\ n = 6k+2 &\quad\Rightarrow\quad n(n+1)(n+2) = 12(3k+1)(2k+1)(3k+2) = 6m \\ n = 6k+3 &\quad\Rightarrow\quad n(n+1)(n+2) = 6(2k+1)(3k+2)(6k+5) = 6m \\ n = 6k+4 &\quad\Rightarrow\quad n(n+1)(n+2) = 12(3k+2)(6k+5)(k+1) = 6m \\ n = 6k+5 &\quad\Rightarrow\quad n(n+1)(n+2) = 6(6k+5)(k+1)(6k+7) = 6m. \end{aligned}$$

   Άρα σε κάθε περίπτωση ο $n(n+1)(n+2)$ είναι πολλαπλάσιο του 6.

2. Αυτό είναι εύκολο:

$$6k+5 = 6k+3+2 = 3(2k+1)+2 = 3l+2.$$

   Όσο για το αντίστροφο, με $l = 0$ έχουμε $3 \cdot 0 + 2 = 2$ και ο 2 δεν είναι της μορφής $6k+5$.

4. Κάθε $n$ είναι είτε της μορφής $3m$ είτε της μορφής $3m+1$ είτε της μορφής $3m+2$. Διακρίνουμε περιπτώσεις:

$$\begin{aligned} n = 3m &\Rightarrow n^2 = 9m^2 = 3k \\ n = 3m+1 &\Rightarrow n^2 = 9m^2 + 6m + 1 = 3m(3m+2) + 1 = 3k+1 \\ n = 3m+2 &\Rightarrow n^2 = 9m^2 + 12m + 1 = 3m(3m+4) + 1 = 3k+1. \end{aligned}$$

Άρα κάθε τετράγωνο $n^2$ είναι είτε της μορφής $3k$ είτε της μορφής $3k+1$ και, επομένως, δεν είναι της μορφής $3k-1$.

7. Απλό:

$$2^{4n} - 1 = 16^n - 1 = (16-1)(16^{n-1} + \cdots + 16 + 1).$$

# Κεφάλαιο 3

# Μέγιστος κοινός διαιρέτης.

## 3.1 Μέγιστος κοινός διαιρέτης.

Ο $0$ έχει ως διαιρέτες όλους τους αριθμούς. Αλλά κάθε $a \neq 0$ έχει πεπερασμένου πλήθους διαιρέτες. Αυτό είναι άμεση συνέπεια της Πρότασης 2.1[β], αφού κάθε διαιρέτης του $a \neq 0$ είναι ανάμεσα στους $-|a|$ και $|a|$. Επομένως, δυο αριθμοί $a, b$ που δεν είναι και οι δύο $0$ έχουν πεπερασμένου πλήθους κοινούς διαιρέτες.

**ΟΡΙΣΜΟΣ.** *Αν οι $a, b$ δεν είναι και οι δύο $0$, τότε ο μεγαλύτερος από τους κοινούς διαιρέτες τους ονομάζεται* **μέγιστος κοινός διαιρέτης** *των $a, b$ και συμβολίζεται*

$$(a, b).$$

*Αν οι $a, b$ δεν είναι και οι δύο $0$ και $(a, b) = 1$, τότε λέμε ότι οι $a, b$ είναι* **πρώτοι προς αλλήλους** *ή* **σχετικά πρώτοι**.

Δυο ακόμη σύμβολα για τον μέγιστο κοινό διαιρέτη των $a, b$ είναι τα μκδ$(a, b)$ και gcd$(a, b)$.

**Παράδειγμα.** Στην πρώτη γραμμή είναι οι θετικοί διαιρέτες του $18$, στην δεύτερη γραμμή οι θετικοί διαιρέτες του $30$ και στην τρίτη γραμμή οι κοινοί θετικοί διαιρέτες.

| | |
|---|---|
| 18 | 1, 2, 3, 6, 9, 18 |
| 30 | 1, 2, 3, 5, 6, 10, 15, 30 |
| κ.δ. | 1, 2, 3, 6 |

Άρα $(18, 30) = 6$.

**Πρόταση 3.1.** [α] *Ο μέγιστος κοινός διαιρέτης δυο αριθμών δεν επηρεάζεται από οποιεσδήποτε αλλαγές στα πρόσημα των δυο αριθμών. Δηλαδή,*

$$(a, b) = (a, -b) = (-a, b) = (-a, -b).$$

[β] *Ο μέγιστος κοινός διαιρέτης είναι συμμετρικός ως προς τις δύο μεταβλητές του. Δηλαδή,*

$$(a, b) = (b, a).$$

[γ] *Ο μέγιστος κοινός διαιρέτης είναι θετικός. Δηλαδή,*

$$(a, b) \geq 1.$$

[δ] *Ισχύει*

$$a \mid b \quad \Rightarrow \quad (a, b) = |a|.$$

*Απόδειξη.* [α] Ένας αριθμός και ο αντίθετός του έχουν τους ίδιους διαιρέτες.

[β] Προφανές.

[γ] Ο $1$ είναι κοινός διαιρέτης των $a, b$. Άρα ο μέγιστος κοινός διαιρέτης των $a, b$ είναι $\geq 1$.

[δ] Αν $a \mid b$, τότε κάθε διαιρέτης του $a$ είναι διαιρέτης και του $b$. Άρα οι κοινοί διαιρέτες των $a, b$ είναι οι ίδιοι με τους διαιρέτες του $a$. Ο μεγαλύτερος από τους διαιρέτες του $a$ είναι ο $|a|$. □

**Λήμμα 3.1.** *Αν $a \neq 0$ και $b = ma + c$, τότε οι κοινοί διαιρέτες των $a, b$ είναι οι ίδιοι με τους κοινούς διαιρέτες των $a, c$. Ειδικώτερα, $(a, b) = (a, c)$.*

*Απόδειξη.* Αν $d \mid a$ και $d \mid b$, τότε $d \mid b - ma = c$. Άρα $d \mid a$ και $d \mid c$. Επομένως, κάθε κοινός διαιρέτης των $a, b$ είναι και κοινός διαιρέτης των $a, c$.

Αντιστρόφως, αν $d \mid a$ και $d \mid c$, τότε $d \mid ma + c = b$. Άρα $d \mid a$ και $d \mid b$. Επομένως, κάθε κοινός διαιρέτης των $a, c$ είναι και κοινός διαιρέτης των $a, b$. □

Από την Πρόταση 3.1[α] βλέπουμε ότι τα πρόσημα των $a, b$ δεν επηρεάζουν τον μέγιστο κοινό διαιρέτη τους και, επομένως, μπορούμε να θεωρούμε ότι κανένας από τους $a, b$ δεν είναι $< 0$.

Τώρα θα περιγράψουμε τον λεγόμενο *Ευκλείδειο αλγόριθμο* εύρεσης του μέγιστου κοινού διαιρέτη των $a, b$. Ένας τουλάχιστον από τους $a, b$ είναι $\neq 0$, οπότε μπορούμε να θεωρήσουμε ότι $a > 0$. Αν $a \mid b$, τότε $(a, b) = a$. Αν, όμως, $a \nmid b$, τότε η ταυτότητα της Ευκλείδειας διαίρεσης του $b$ από τον $a$ γράφεται

$$b = q_1 a + r_1, \quad 0 < r_1 < a.$$

Αν $r_1 \mid a$, τότε έχουμε

$$a = q_2 r_1.$$

Αν, όμως, $r_1 \nmid a$, τότε η ταυτότητα της Ευκλείδειας διαίρεσης του $a$ από τον $r_1$ γράφεται

$$a = q_2 r_1 + r_2, \quad 0 < r_2 < r_1.$$

Αν $r_2 \mid r_1$, τότε έχουμε

$$r_1 = q_3 r_2.$$

Αν, όμως, $r_2 \nmid r_1$, τότε η ταυτότητα της Ευκλείδειας διαίρεσης του $r_1$ από τον $r_2$ γράφεται

$$r_1 = q_3 r_2 + r_3, \quad 0 < r_3 < r_2.$$

Συνεχίζουμε αυτήν την διαδικασία και σε κάθε στάδιό της βρίσκουμε είτε μηδενικό υπόλοιπο είτε θετικό υπόλοιπο. Η διαδικασία αυτή δεν μπορεί να συνεχιστεί απεριόριστα βρίσκοντας πάντοτε θετικό υπόλοιπο, διότι τα διαδοχικά υπόλοιπα διαρκώς μικραίνουν και κάποια στιγμή θα βρούμε μηδενικό υπόλοιπο. Όταν βρούμε για πρώτη φορά μηδενικό υπόλοιπο σταματάμε την διαδικασία.

Η διαδικασία την οποία μόλις περιγράψαμε ονομάζεται **Ευκλείδειος αλγόριθμος** με αρχή τους $a, b$ και σχηματοποιείται ως εξής:

$$\boxed{\begin{array}{ll} b = q_1 a + r_1, & 0 < r_1 < a \\ a = q_2 r_1 + r_2, & 0 < r_2 < r_1 \\ r_1 = q_3 r_2 + r_3, & 0 < r_3 < r_2 \\ \cdots\cdots\cdots & \cdots\cdots\cdots \\ r_{n-2} = q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} = q_{n+1} r_n. & \end{array}} \tag{3.1}$$

Ο $r_n$ είναι το τελευταίο μη-μηδενικό υπόλοιπο του Ευκλείδειου αλγόριθμου. Παρατηρήστε ότι αν $a \mid b$, οπότε $b = q_1 a$, τότε μπορούμε να θεωρήσουμε ότι έχουμε βρει κατευθείαν την τελευταία ισότητα $r_{n-1} = q_{n+1} r_n$ του Ευκλείδειου αλγόριθμου, αν θέσουμε $n = 0$ και $r_{-1} = b$, $r_0 = a$. Δηλαδή, σ' αυτήν την περίπτωση μπορούμε να θεωρήσουμε ότι ο ίδιος ο $a$ είναι το τελευταίο μη-μηδενικό υπόλοιπο του Ευκλείδειου αλγόριθμου (ο οποίος δεν ξεκινά καν).

**Πρόταση 3.2.** *Αν $a > 0$, τότε οι κοινοί διαιρέτες των $a, b$ είναι οι ίδιοι με τους διαιρέτες του τελευταίου μη-μηδενικού υπολοίπου του Ευκλείδειου αλγόριθμου με αρχή τους $a, b$. Ειδικώτερα, ο μέγιστος κοινός διαιρέτης των $a, b$ είναι το τελευταίο μη-μηδενικό υπόλοιπο του Ευκλείδειου αλγόριθμου με αρχή τους $a, b$.*

*Απόδειξη.* Σύμφωνα με το Λήμμα 3.1, οι κοινοί διαιρέτες των $b, a$ είναι οι ίδιοι με τους κοινούς διαιρέτες των $a, r_1$ κι αυτοί είναι οι ίδιοι με τους κοινούς διαιρέτες των $r_1, r_2$ κλπ κλπ κι αυτοί είναι οι ίδιοι με τους κοινούς διαιρέτες των $r_{n-2}, r_{n-1}$ κι αυτοί είναι οι ίδιοι με τους κοινούς διαιρέτες των $r_{n-1}, r_n$ κι αυτοί είναι οι ίδιοι με τους διαιρέτες του $r_n$. □

Παρατηρήστε ότι η Πρόταση 3.2 λέει ότι οι κοινοί διαιρέτες των $a, b$ είναι οι ίδιοι με τους διαιρέτες του $(a, b)$. Με άλλα λόγια:

$$\boxed{d \mid a,\ d \mid b \quad \Leftrightarrow \quad d \mid (a, b).} \tag{3.2}$$

Αυτό είναι φανερό στο προηγούμενο παράδειγμα: οι κοινοί διαιρέτες των $18, 30$ είναι οι $1, 2, 3, 6$ και αυτοί είναι ακριβώς οι διαιρέτες του μέγιστου κοινό διαιρέτη $6$. Ας δούμε ένα ακόμη παράδειγμα.

**Παράδειγμα.**

| | |
|---|---|
| 96 | 1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 96 |
| 240 | 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 30, 40, 48, 60, 80, 120, 240 |
| κ.δ. | 1, 2, 3, 4, 6, 8, 12, 16, 24, 48 |

Άρα $(96, 240) = 48$ και οι κοινοί διαιρέτες των $96$, $240$ είναι ακριβώς οι διαιρέτες του μέγιστου κοινού διαιρέτη $48$.

Στην ισοδυναμία (3.2) η μία συνεπαγωγή είναι στοιχειώδης. Πράγματι, αν ο $d$ είναι διαιρέτης του $(a, b)$, τότε, επειδή ο $(a, b)$ είναι κοινός διαιρέτης των $a, b$, συνεπάγεται ότι και ο $d$ είναι κοινός διαιρέτης των $a, b$. Η αντίστροφη συνεπαγωγή, δηλαδή ότι αν ο $d$ είναι κοινός διαιρέτης των $a, b$ τότε είναι διαιρέτης και του $(a, b)$, δεν είναι στοιχειώδης και για να αποδειχθεί χρησιμοποιήσαμε τον Ευκλείδειο αλγόριθμο.

**Πρόταση 3.3.** *Αν οι $a, b$ δεν είναι και οι δύο $0$ και $m \neq 0$, τότε*

$$(ma, mb) = |m|(a, b).$$

*Απόδειξη.* Κατ' αρχάς θεωρούμε την περίπτωση που $a, m > 0$.
Γράφουμε τον Ευκλείδειο αλγόριθμο (3.1) με αρχή τους $a, b$. Όπως είδαμε, ισχύει

$$(a, b) = r_n.$$

Κατόπιν πολλαπλασιάζουμε κάθε εξίσωση και ανίσωση του (3.1) με τον $m > 0$ και βρίσκουμε

$$\begin{aligned}
mb &= q_1(ma) + mr_1, && 0 < mr_1 < ma \\
ma &= q_2(mr_1) + mr_2, && 0 < mr_2 < mr_1 \\
mr_1 &= q_3(mr_2) + mr_3, && 0 < mr_3 < mr_2 \\
&\cdots\cdots\cdots && \cdots\cdots\cdots \\
mr_{n-2} &= q_n(mr_{n-1}) + mr_n, && 0 < mr_n < mr_{n-1} \\
mr_{n-1} &= q_{n+1}(mr_n).
\end{aligned} \tag{3.3}$$

Είναι σαφές ότι κάθε γραμμή εκφράζει μια αντίστοιχη Ευκλείδεια διαίρεση, οπότε το σχήμα (3.3) εκφράζει τον Ευκλείδειο αλγόριθμο με αρχή τους $ma, mb$. Επομένως

$$(ma, mb) = mr_n.$$

Άρα $(ma, mb) = m(a, b)$.
Τώρα, αν $a < 0, m > 0$, έχουμε $(ma, mb) = (-ma, mb) = m(-a, b) = m(a, b)$.
Αν $a \neq 0, m < 0$, έχουμε $(ma, mb) = (-ma, -mb) = (-m)(a, b) = |m|(a, b)$.
Άρα σε κάθε περίπτωση ισχύει $(ma, mb) = |m|(a, b)$. □

**Πρόταση 3.4.** *Αν οι $a, b$ δεν είναι και οι δύο $0$ και $m \mid a, m \mid b$, τότε*

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

*Ειδικώτερα,*

$$\Big(\frac{a}{(a, b)}, \frac{b}{(a, b)}\Big) = 1.$$

*Απόδειξη.* Κατ' αρχάς παρατηρούμε ότι, αν $m \mid a, m \mid b$, τότε βάσει της (3.2) συνεπάγεται ότι $|m| \mid (a, b)$, οπότε και οι τρεις αριθμοί $\frac{a}{m}, \frac{b}{m}, \frac{(a,b)}{|m|}$ είναι ακέραιοι.
Κατόπιν, από την Πρόταση 3.3 έχουμε

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

οπότε η απόδειξη έχει τελειώσει. □

**Πρόταση 3.5.** *Αν $(a, b) = 1$ και $c \neq 0$, τότε $(a, bc) = (a, c)$.*

*Απόδειξη.* Έστω $d \mid a, d \mid c$. Τότε $d \mid a, d \mid bc$.
Άρα κάθε κοινός διαιρέτης των $a, c$ είναι κοινός διαιρέτης και των $a, bc$.
Έστω $d \mid a, d \mid bc$. Τότε, $d \mid ac, d \mid bc$, οπότε βάσει της (3.2) συνεπάγεται

$$d \mid (ac, bc) = |c|(a, b) = |c|.$$

Άρα $d \mid c$.
Άρα κάθε κοινός διαιρέτης των $a, bc$ είναι κοινός διαιρέτης και των $a, c$.
Συμπεραίνουμε ότι οι κοινοί διαιρέτες των $a, bc$ είναι οι ίδιοι με τους κοινούς διαιρέτες των $a, c$ και, επομένως, $(a, bc) = (a, c)$. □

**Πρόταση 3.6.** *Ισχύει*

$$\boxed{(a, b) = 1,\ a \mid bc \quad \Rightarrow \quad a \mid c.}$$

*Απόδειξη.* Έστω $(a, b) = 1$ και $a \mid bc$.
Επειδή $a \mid bc$, έχουμε $(a, bc) = |a|$.
Τώρα, επειδή $(a, b) = 1$, από την Πρόταση 3.5 συνεπάγεται ότι $(a, bc) = (a, c)$.
Άρα $(a, c) = |a|$ και, επομένως, $a \mid c$. □

**Πρόταση 3.7.** *Έστω $m, n, a > 0$, $(m, n) = 1$ και $a \mid mn$. Τότε υπάρχουν μοναδικοί $m', n' > 0$ ώστε $a = m'n'$, $m' \mid m$, $n' \mid n$.*

*Απόδειξη.* Θεωρούμε τους

$$m' = (m, a), \quad n' = \frac{a}{m'}.$$

Είναι σαφές ότι ο $n'$ είναι φυσικός και ότι

$$a = m'n'.$$

Επίσης, ο $\frac{m}{m'}$ είναι φυσικός και

$$\Big(\frac{m}{m'}, n'\Big) = \Big(\frac{m}{m'}, \frac{a}{m'}\Big) = 1.$$

Επειδή $a \mid mn$, έχουμε

$$mn = qa$$

για κάποιον $q$, οπότε

$$mn = qm'n'$$

και, επομένως,

$$\frac{m}{m'}\, n = qn'.$$

Άρα $n' \mid \frac{m}{m'}\, n$ και, επειδή $(\frac{m}{m'}, n') = 1$, έχουμε

$$n' \mid n.$$

Άρα υπάρχουν $m', n' > 0$ ώστε $a = m'n'$, $m' \mid m$, $n' \mid n$.
Τώρα, ας υποθέσουμε ότι υπάρχουν και $m'', n'' > 0$ ώστε $a = m''n''$, $m'' \mid m$, $n'' \mid n$.
Επειδή $(m, n) = 1$ και $m' \mid m$, $n'' \mid n$, συνεπάγεται $(m', n'') = 1$. Πράγματι, αν οι $m', n''$ είχαν κοινό διαιρέτη $d > 1$, τότε ο $d$ θα ήταν κοινός διαιρέτης και των $m, n$.
Ομοίως, επειδή $(m, n) = 1$ και $m'' \mid m$, $n' \mid n$, συνεπάγεται $(m'', n') = 1$.
Από την σχέση

$$m'n' = m''n''$$

συνεπάγεται $m' \mid m''n''$ και, επειδή $(m', n'') = 1$, έχουμε

$$m' \mid m''.$$

Ομοίως, από την ίδια σχέση συνεπάγεται $m'' \mid m'n'$ και, επειδή $(m'', n') = 1$, συνεπάγεται

$$m'' \mid m'.$$

Άρα

$$m' = m''$$

και τώρα είναι προφανές ότι $n' = n''$. □

## 3.2 Ελάχιστο κοινό πολλαπλάσιο.

Αν οι $a, b$ και οι δύο δεν είναι $0$, τότε μπορούμε να θεωρήσουμε τα κοινά θετικά πολλαπλάσιά τους. Προφανώς, ένα τέτοιο είναι ο αριθμός $|ab|$, οπότε, βάσει της αρχής της καλής διάταξης, μπορούμε να θεωρήσουμε το μικρότερο από τα κοινά θετικά πολλαπλάσια των $a, b$.

**ΟΡΙΣΜΟΣ.** *Αν οι $a, b$ και οι δύο δεν είναι $0$, τότε το μικρότερο από τα κοινά θετικά πολλαπλάσιά τους ονομάζεται* **ελάχιστο κοινό πολλαπλάσιο** *των $a, b$ και συμβολίζεται*

$$[a, b].$$

**Παράδειγμα.** Στην πρώτη γραμμή είναι τα θετικά πολλαπλάσια του $4$, στην δεύτερη γραμμή τα θετικά πολλαπλάσια του $6$ και στην τρίτη γραμμή τα κοινά θετικά πολλαπλάσια.

| | |
|---|---|
| 4 | 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, … |
| 6 | 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, … |
| κ.π. | 12, 24, 36, 48, 60, 72, 84, … |

Άρα $[4, 6] = 12$.

**Πρόταση 3.8.** *Αν οι $a, b$ και οι δύο δεν είναι $0$, τότε τα κοινά πολλαπλάσια των $a, b$ είναι τα ίδια με τα πολλαπλάσια του $\frac{ab}{(a,b)}$. Ειδικώτερα,*

$$[a, b] = \frac{|ab|}{(a, b)}.$$

*Απόδειξη.* Ο αριθμός $\frac{a}{(a,b)}$ είναι ακέραιος, οπότε ο $\frac{ab}{(a,b)} = \frac{a}{(a,b)}b$ είναι πολλαπλάσιο του $b$. Ομοίως, ο $\frac{b}{(a,b)}$ είναι ακέραιος, οπότε ο $\frac{ab}{(a,b)} = a\frac{b}{(a,b)}$ είναι πολλαπλάσιο του $a$.
Άρα ο $\frac{ab}{(a,b)}$ είναι κοινό πολλαπλάσιο των $a, b$. Επομένως, και κάθε πολλαπλάσιο του $\frac{ab}{(a,b)}$ είναι κοινό πολλαπλάσιο των $a, b$.
Αντιστρόφως, έστω ότι ο $m$ είναι κοινό πολλαπλάσιο των $a, b$.
Επειδή ο $m$ είναι πολλαπλάσιο του $a$, έχουμε

$$m = qa$$

για κάποιον $q$.
Επειδή ο $m$ είναι πολλαπλάσιο και του $b$, συνεπάγεται

$$b \mid qa.$$

Θεωρούμε τους $\frac{a}{(a,b)}, \frac{b}{(a,b)}$, οι οποίοι είναι σχετικά πρώτοι και έχουμε

$$\frac{b}{(a, b)} \Big| q\frac{a}{(a, b)}.$$

Από την Πρόταση 3.6 συνεπάγεται ότι

$$\frac{b}{(a, b)} \Big| q.$$

Άρα ισχύει

$$q = k\frac{b}{(a, b)}$$

για κάποιον $k$. Άρα

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

οπότε ο $m$ είναι πολλαπλάσιο του $\frac{ab}{(a,b)}$.
Άρα, λοιπόν, κάθε κοινό πολλαπλάσιο των $a, b$ είναι πολλαπλάσιο του $\frac{ab}{(a,b)}$.
Συμπεραίνουμε ότι τα κοινά πολλαπλάσια των $a, b$ είναι τα ίδια με τα πολλαπλάσια του $\frac{ab}{(a,b)}$. □

Άμεση συνέπεια της Πρότασης 3.7 είναι ότι τα κοινά πολλαπλάσια των $a, b$ είναι τα ίδια με τα πολλαπλάσια του $[a, b]$. Δηλαδή,

$$\boxed{a \mid m,\ b \mid m \quad \Leftrightarrow \quad [a, b] \mid m.}$$

Αυτό διαφαίνεται και στο προηγούμενο παράδειγμα: τουλάχιστον τα αρχικά θετικά κοινά πολλαπλάσια των $4, 6$ ταυτίζονται με τα αρχικά θετικά πολλαπλάσια του $[4, 6] = 12$.

## 3.3 Ασκήσεις.

1. Βρείτε τους $(1769, 2378)$, $(5033464705, 3137640337)$.

2. Αποδείξτε ότι

$(a, a+n) \mid n$ αν $n \neq 0$.

$(5a+2, 7a+3) = 1$.

$(a,4) = 2,\ (b,4) = 2 \ \Rightarrow\ (a+b,4) = 4$.

$(a,b) = 1 \ \Rightarrow\ (a+2b, 2a+b) = 1$ ή $3$.

$(a,b) = 1 \ \Rightarrow\ (a+b, a^2+b^2) = 1$ ή $2$.

3. Αποδείξτε ότι

   $(a,b) = 1,\ c \mid a \ \Rightarrow\ (c,b) = 1$.

   $a \mid c,\ b \mid c,\ (a,b) = 1 \ \Rightarrow\ ab \mid c$. Βάσει αυτού αποδείξτε ότι το γινόμενο πέντε διαδοχικών ακεραίων διαιρείται από το $120$.

   $(a,b) = 1,\ (a,c) = 1 \ \Rightarrow\ (a,bc) = 1$.

   $(a,b) = 1,\ d \mid ac,\ d \mid bc \ \Rightarrow\ d \mid c$.

   $(a,b) = 1 \ \Rightarrow\ (a^m, b^n) = 1$.

4. Αποδείξτε ότι: $a^n \mid b^n \ \Rightarrow\ a \mid b$.

5. Βρείτε το $[306, 657]$.

6. Αποδείξτε ότι $[ma, mb] = |m|[a,b]$.

7. Αποδείξτε ότι $[a,b] = (a,b)$ αν και μόνο αν $a = \pm b$.

8. Αν $d, e \geq 1$, αποδείξτε ότι υπάρχουν $a, b$ ώστε $(a,b) = d, [a,b] = e$ αν και μόνον αν $d \mid e$.

9. Αποδείξτε ότι δεν υπάρχουν $a, b \geq 1$, $n \geq 2$ ώστε $a^n - b^n \mid a^n + b^n$.

10. Αν $a, b \geq 3$, αποδείξτε ότι ο $2^b - 1$ δεν διαιρεί τον $2^a + 1$.

11. Αν οι $a_1, \ldots, a_n$ δεν είναι όλοι $0$, τότε με $(a_1, \ldots, a_n)$ συμβολίζουμε τον μέγιστο κοινό διαιρέτη των $a_1, \ldots, a_n$.
    Αν $a_1 \neq 0$, τότε ορίζουμε διαδοχικά τους

    $$d_2 = (a_1, a_2),\ d_3 = (d_2, a_3),\ \ldots,\ d_n = (d_{n-1}, a_n).$$

    Αποδείξτε ότι $(a_1, \ldots, a_n) = d_n$.

12. Αν οι $a_1, \ldots, a_n$ όλοι δεν είναι $0$, τότε με $[a_1, \ldots, a_n]$ συμβολίζουμε το ελάχιστο κοινό θετικό πολλαπλάσιο των $a_1, \ldots, a_n$.
    Αν $a_1, \ldots, a_n \neq 0$, τότε ορίζουμε διαδοχικά τους

    $$e_2 = [a_1, a_2],\ e_3 = [e_2, a_3],\ \ldots,\ e_n = [e_{n-1}, a_n].$$

    Αποδείξτε ότι $[a_1, \ldots, a_n] = e_n$.

13. Βρείτε όλες τις τριάδες $a, b, c$ ώστε $(a,b,c) = 10, [a,b,c] = 100$.

## 3.4 Λύσεις ασκήσεων.

2. (i) Υποθέτοντας ότι $n \neq 0$ εξασφαλίζουμε ότι τουλάχιστον ένας από τους $a, a+n$ δεν είναι $0$, οπότε ορίζεται ο $(a, a+n)$.
Ορίζουμε $d = (a, a+n)$. Τότε $d \mid a$ και $d \mid a+n$. Άρα

$$d \mid (a+n) - a = n.$$

(ii) Ορίζουμε $d = (5a+2, 7a+3)$. Τότε $d \geq 1$ και $d \mid 5a+2$ και $d \mid 7a+3$. Άρα

$$d \mid 5(7a+3) - 7(5a+2) = 1.$$

Άρα $d = 1$.
(iii) Έστω $(a, 4) = 2$. Οι θετικοί διαιρέτες του $4$ είναι οι $1, 2, 4$. Επειδή ο μέγιστος κοινός διαιρέτης των $a, 4$ είναι ο $2$, συνεπάγεται ότι ο $2$ διαιρεί τον $a$ και ότι ο $4$ δεν διαιρεί τον $a$. Γνωρίζουμε, όμως, ότι ο $a$ είναι είτε της μορφής $4k$ είτε της μορφής $4k+1$ είτε της μορφής $4k+2$ είτε της μορφής $4k+3$. Βλέπουμε αμέσως ότι η μόνη περίπτωση να είναι ο $a$ πολλαπλάσιο του $2$ και όχι του $4$ είναι όταν ο $a$ είναι της μορφής $4k+2$.
Προφανώς, τα ίδια μπορούμε να πούμε αν $(b, 4) = 2$.
Επομένως, αν $(a, 4) = 2$ και $(b, 4) = 2$, τότε $a = 4k+2$ και $b = 4l+2$ και άρα

$$a + b = 4(k + l + 1).$$

Άρα $4 \mid a+b$, οπότε $(a+b, 4) = 4$.
(iv) Έστω $(a, b) = 1$. Ορίζουμε $d = (a+2b, 2a+b)$. Τότε $d \geq 1$ και $d \mid a+2b$ και $d \mid 2a+b$. Άρα

$$d \mid 2(2a+b) - (a+2b) = 3a, \qquad d \mid 2(a+2b) - (2a+b) = 3b.$$

Άρα

$$d \mid (3a, 3b) = 3(a, b) = 3.$$

Άρα $d = 1$ ή $3$.
Παίρνοντας $a = 1, b = 0$, έχουμε $(a, b) = 1$ και $(a+2b, 2a+b) = (1, 2) = 1$. Παίρνοντας $a = 1, b = 1$, έχουμε $(a, b) = 1$ και $(a+2b, 2a+b) = (3, 3) = 3$.

3. (i) Έστω $(a, b) = 1$ και $c \mid a$. Ορίζουμε $d = (c, b)$. Τότε $d \geq 1$ και $d \mid c$ και $d \mid b$. Τώρα,

$$d \mid c,\ c \mid a \quad \Rightarrow \quad d \mid a.$$

Τέλος,

$$d \mid a,\ d \mid b \quad \Rightarrow \quad d \mid (a, b) = 1.$$

Άρα $d = 1$.
(ii) Έστω $a \mid c$, $b \mid c$ και $(a, b) = 1$. Επειδή $a \mid c$, συνεπάγεται ότι

$$c = ka$$

για κάποιο $k$. Επειδή $b \mid c$, συνεπάγεται

$$b \mid ka.$$

Τώρα,

$$b \mid ka,\ (a, b) = 1 \quad \Rightarrow \quad b \mid k.$$

Άρα

$$k = bl$$

για κάποιο $l$. Άρα

$$c = ka = lab,$$

οπότε $ab \mid c$.
(iii) Έστω $(a, b) = 1$ και $(a, c) = 1$. Επειδή $(a, b) = 1$, από την Πρόταση 3.5 συνεπάγεται

$$(a, bc) = (a, c) = 1.$$

Με δεύτερο τρόπο. Θέτουμε $d = (a, bc)$. Τότε $d \geq 1$ και $d \mid a$ και $d \mid bc$. Επειδή $d \mid a$ και $(a, b) = 1$, από το (i) συνεπάγεται ότι $(d, b) = 1$. Τώρα,

$$d \mid bc,\ (d, b) = 1 \quad \Rightarrow \quad d \mid c.$$

Τέλος,

$$d \mid a,\ d \mid c \quad \Rightarrow \quad d \mid (a, c) = 1.$$

Άρα $d = 1$.
(iv) Έστω $(a, b) = 1$, $d \mid ac$ και $d \mid bc$. Τότε

$$d \mid (ac, bc) = (a, b)c = c.$$

(v) Έστω $(a, b) = 1$. Εφαρμόζοντας επανειλλημένα την Πρόταση 3.5, έχουμε διαδοχικά:

$$(a, b^2) = (a, b) = 1, \quad (a, b^3) = (a, b^2) = 1, \quad \ldots \quad (a, b^n) = (a, b^{n-1}) = 1.$$

Πάλι από την αρχή, επειδή $(a, b^n) = 1$, έχουμε:

$$(a^2, b^n) = (a, b^n) = 1, \quad (a^3, b^n) = (a^2, b^n) = 1, \quad \ldots \quad (a^m, b^n) = (a^{m-1}, b^n) = 1.$$

4. Έστω $a^n \mid b^n$. Θέτουμε $d = (a, b)$. Τότε $d \geq 1$ και $d \mid a$ και $d \mid b$.
Ορίζουμε

$$a_1 = \frac{a}{d}, \quad b_1 = \frac{b}{d}.$$

Γνωρίζουμε ότι

$$(a_1, b_1) = 1.$$

Από την $a^n \mid b^n$ συνεπάγεται

$$b^n = ka^n$$

για κάποιον $k$, οπότε

$$d^n b_1^n = k d^n a_1^n$$

και άρα

$$b_1^n = k a_1^n.$$

Συνεπάγεται ότι $a_1 \mid b_1^n$ και, επειδή $(a_1, b_1) = 1$, έχουμε διαδοχικά:

$$a_1 \mid b_1^{n-1}, \quad a_1 \mid b_1^{n-2}, \quad \ldots \quad a_1 \mid b_1, \quad a_1 \mid 1.$$

Άρα $a_1 = \pm 1$, οπότε $a = \pm d$ και, επομένως, $a \mid b$.

8. Έστω ότι υπάρχουν $a, b$ ώστε $(a, b) = d$ και $[a, b] = e$. Τότε,

$$d \mid a,\ a \mid e \quad \Rightarrow \quad d \mid e.$$

Αντιστρόφως, έστω $d, e \geq 1$ και $d \mid e$. Θα αποδείξουμε ότι υπάρχουν $a, b \geq 1$ ώστε $(a, b) = d$ και $[a, b] = e$.
Επειδή $[a, b] = \frac{ab}{(a,b)}$, έχουμε

$$(a, b) = d,\ [a, b] = e \quad \Leftrightarrow \quad (a, b) = d,\ ab = de. \tag{3.4}$$

Θέτουμε

$$a_1 = \frac{a}{d}, \quad b_1 = \frac{b}{d},$$

οπότε

$$(a_1, b_1) = 1$$

και το σύστημα (3.4) γίνεται

$$(a_1, b_1) = 1, \ a_1 b_1 = \frac{e}{d}.$$

(Παρατηρήστε ότι η υπόθεση $d \mid e$ εξασφαλίζει ότι ο $\frac{e}{d}$ είναι ακέραιος.)
Μια προφανής λύση του τελευταίου είναι η $a_1 = 1, b_1 = \frac{e}{d}$ και άρα μια λύση του αρχικού συστήματος είναι η $a = d, b = e$.

# Κεφάλαιο 4

# Πρώτοι αριθμοί.

## 4.1 Πρώτοι αριθμοί.

Ο $1$ έχει μόνο έναν θετικό διαιρέτη. Κάθε $n > 1$ έχει τουλάχιστον δύο θετικούς διαιρέτες, τον $1$ και τον $n$.

**ΟΡΙΣΜΟΣ.** *Αν ο $n > 1$ έχει μόνο δύο θετικούς διαιρέτες, τους $1, n$, τότε ο $n$ χαρακτηρίζεται* **πρώτος**. *Αν ο $n > 1$ έχει περισσότερους από δύο θετικούς διαιρέτες, τότε ο $n$ χαρακτηρίζεται* **σύνθετος**.

Παρατηρούμε ότι ο $1$ δεν είναι πρώτος ούτε σύνθετος.
Είναι σαφές ότι ο $n$ είναι σύνθετος αν και μόνον αν υπάρχει $d$ ώστε

$$d \mid n, \quad 1 < d < n.$$

Οι αρχικοί πρώτοι είναι οι

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

Ο $2$ είναι ο μοναδικός άρτιος πρώτος. Όλοι οι άλλοι πρώτοι είναι περιττοί. Αυτό είναι προφανές, αφού ένας πρώτος $> 2$ δεν μπορεί να διαιρείται από τον $2$.

**Πρόταση 4.1.** *Έστω $n > 1$. Ο μικρότερος διαιρέτης $> 1$ του $n$ είναι πρώτος. Αν ο $n$ είναι σύνθετος, τότε ο μικρότερος διαιρέτης $> 1$ του $n$ είναι $\leq \sqrt{n}$.*

*Απόδειξη.* Έστω $p$ ο μικρότερος διαιρέτης $> 1$ του $n$. Αν ο $p$ είναι σύνθετος, τότε υπάρχει διαιρέτης $d$ του $p$ ώστε $1 < d < p$. Τότε, όμως, ο $d$ είναι διαιρέτης $> 1$ του $n$ και καταλήγουμε σε άτοπο. Κατόπιν, έστω ότι ο $n$ είναι σύνθετος και έστω $p$ ο μικρότερος διαιρέτης $> 1$ του $n$. Τότε

$$1 < p < n$$

και

$$n = mp$$

για κάποιον $m$.
Τότε ο $m$ είναι διαιρέτης $> 1$ του $n$, οπότε ισχύει

$$p \leq m.$$

Άρα

$$n = mp \geq p^2,$$

οπότε $p \leq \sqrt{n}$. □

Από την Πρόταση 4.1 συμπεραίνουμε ότι *κάθε $n > 1$ έχει τουλάχιστον έναν πρώτο διαιρέτη*.
Από τώρα και στο εξής με το γράμμα

$$p$$

θα συμβολίζουμε, συνήθως, πρώτους αριθμούς.

Το Θεώρημα 4.1 αποδείχθηκε πρώτη φορά από τον Ευκλείδη.

**Θεώρημα 4.1.** *Υπάρχουν άπειροι πρώτοι.*

*Απόδειξη.* Έστω ότι υπάρχουν πεπερασμένου πλήθους πρώτοι και έστω ότι αυτοί είναι οι

$$p_1, p_2, \ldots, p_k.$$

Θεωρούμε τον

$$n = p_1 \cdots p_k + 1.$$

Ο $n$ είναι $> 1$, οπότε έχει τουλάχιστον έναν πρώτο διαιρέτη. Αυτός ο διαιρέτης πρέπει να είναι ένας από τους $p_1, \ldots, p_k$ και έστω ότι είναι ο $p_l$.
Τότε, όμως,

$$p_l \mid n, \quad p_l \mid p_1 \cdots p_k,$$

οπότε

$$p_l \mid n - p_1 \cdots p_k = 1$$

και καταλήγουμε σε άτοπο. □

**Πρόταση 4.2.** *Αν ο $p$ είναι πρώτος, τότε κάθε αριθμός είναι είτε πολλαπλάσιο του $p$ είτε σχετικά πρώτος με τον $p$.*

*Απόδειξη.* Ο $(n, p)$ είναι διαιρέτης του $p$, οπότε

$$(n, p) = 1 \quad \text{ή} \quad (n, p) = p.$$

Στην πρώτη περίπτωση ο $n$ είναι σχετικά πρώτος με τον $p$ και στην δεύτερη περίπτωση ο $p$ διαιρεί τον $n$. □

**Παράδειγμα.** Το συμπέρασμα της Πρότασης 4.2 δεν ισχύει αν ο $p$ δεν είναι πρώτος.
Για παράδειγμα, ο $p = 4$ δεν είναι πρώτος και ο $n = 2$ δεν είναι ούτε πολλαπλάσιο του $4$ ούτε σχετικά πρώτος με τον $4$.

**Πρόταση 4.3.** *Αν ο $p$ είναι πρώτος και διαιρεί το γινόμενο κάποιων αριθμών, τότε διαιρεί τουλάχιστον έναν από αυτούς τους αριθμούς.*

*Απόδειξη.* Έστω

$$p \mid n_1 \cdots n_k.$$

Αν ο $p$ δεν διαιρεί τον $n_1$, τότε είναι σχετικά πρώτος με τον $n_1$, οπότε

$$p \mid n_2 \cdots n_k.$$

Αν ο $p$ δεν διαιρεί τον $n_2$, τότε είναι σχετικά πρώτος με τον $n_2$, οπότε

$$p \mid n_3 \cdots n_k.$$

Συνεχίζοντας, είναι σαφές ότι αν ο $p$ δεν διαιρεί κανέναν από τους $n_1, \ldots, n_{k-1}$, τότε θα καταλήξουμε στο ότι ο $p$ διαιρεί τον $n_k$. □

**Παράδειγμα.** Το συμπέρασμα της Πρότασης 4.3 δεν ισχύει αν ο $p$ δεν είναι πρώτος.
Για παράδειγμα ο $p = 8$ δεν είναι πρώτος. Ο $8$ διαιρεί το γινόμενο $2 \cdot 4$ αλλά δεν διαιρεί κανέναν από τους $2, 4$.

**Θεώρημα 4.2.** *Κάθε αριθμός $> 1$ γράφεται με μοναδικό τρόπο ως γινόμενο πρώτων.*

*Απόδειξη.* Ο $n = 2$ γράφεται ως γινόμενο πρώτων.
Έστω $n > 2$ και ότι κάθε $m$ με $2 \leq m < n$ γράφεται ως γινόμενο πρώτων.
Αν ο $n$ είναι πρώτος, τότε ο $n$ γράφεται ως γινόμενο ενός πρώτου. Αν ο $n$ είναι σύνθετος, τότε έχει έναν τουλάχιστον πρώτο διαιρέτη $p$ και

$$n = pm$$

για κάποιον $m$ με $2 \leq m < n$.
Από την επαγωγική υπόθεση, ο $m$ γράφεται ως γινόμενο πρώτων, οπότε και ο $n$ γράφεται ως γινόμενο πρώτων.
Άρα κάθε $n > 1$ γράφεται ως γινόμενο πρώτων.
Τέλος, έστω ότι κάποιος $n > 1$ γράφεται

$$n = p'_1 \cdots p'_k = p''_1 \cdots p''_m,$$

όπου όλοι οι $p'_1, \ldots, p'_k, p''_1, \ldots, p''_m$ είναι πρώτοι.
Τότε ο $p'_1$ διαιρεί το γινόμενο $p''_1 \cdots p''_m$, οπότε διαιρεί έναν από τους $p''_1, \ldots, p''_m$. Αλλάζοντας αν χρειάζεται την αρίθμηση των $p''_1, \ldots, p''_m$, μπορούμε να υποθέσουμε ότι $p'_1 \mid p''_1$. Επειδή, όμως, ο $p''_1$ είναι πρώτος, συνεπάγεται ότι

$$p'_1 = p''_1.$$

Άρα

$$p'_2 \cdots p'_k = p''_2 \cdots p''_m,$$

Με τον ίδιο τρόπο και, αλλάζοντας αν χρειάζεται την αρίθμηση των $p''_2, \ldots, p''_m$ βλέπουμε ότι

$$p'_1 = p''_1, p'_2 = p''_2.$$

Συνεχίζοντας και, αλλάζοντας κάθε φορά την αρίθμηση των πρώτων με τους δύο τόνους, βλέπουμε ότι $k \leq m$ και

$$p'_1 = p''_1, \ldots, p'_k = p''_k.$$

Αν $k < m$, καταλήγουμε στην ισότητα

$$1 = p''_{k+1} \cdots p''_m,$$

η οποία είναι αδύνατη.
Άρα $k = m$ και, επομένως, ο $n$ γράφεται με μοναδικό τρόπο ως γινόμενο πρώτων. □

Έστω, τώρα, ότι γράφουμε έναν $n > 1$ ως γινόμενο πρώτων. Αν $p$ είναι ένας από αυτούς και εμφανίζεται $\alpha \geq 1$ φορές στο γινόμενο, τότε μπορούμε να γράψουμε το $p \cdots p$ ($\alpha$ φορές) ως $p^\alpha$. Άρα ο $n$ μπορεί να γραφτεί

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

όπου οι $p_1, \ldots, p_k$ είναι πρώτοι και

$$p_1 < \ldots < p_k, \quad \alpha_1, \ldots, \alpha_k \geq 1.$$

**ΟΡΙΣΜΟΣ.** *Η παραπάνω (μοναδική) αναπαράσταση του $n > 1$ ονομάζεται* **κανονική αναπαράσταση** *του $n$ ως γινόμενο πρώτων.*

**Πρόταση 4.4.** *Αν $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ είναι η κανονική αναπαράσταση του $n > 1$ ως γινόμενο πρώτων, τότε οι θετικοί διαιρέτες του $n$ είναι οι αριθμοί*

$$p_1^{\beta_1} \cdots p_k^{\beta_k}, \qquad 0 \leq \beta_1 \leq \alpha_1, \ldots, 0 \leq \beta_k \leq \alpha_k.$$

*Απόδειξη.* Κατ' αρχάς είναι σαφές ότι καθένας από αυτούς τους αριθμούς είναι διαιρέτης του $n$, αφού

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = p_1^{\beta_1} \cdots p_k^{\beta_k} \cdot p_1^{\alpha_1 - \beta_1} \cdots p_k^{\alpha_k - \beta_k}.$$

Κατόπιν, έστω $d$ ένας διαιρέτης του $n$.
Αν $d = 1$, τότε

$$d = p_1^0 \cdots p_k^0.$$

Αν $d > 1$, γράφουμε την κανονική αναπαράσταση του $d$:

$$d = q_1^{\gamma_1} \cdots q_m^{\gamma_m}.$$

Κάθε πρώτος $q_l$ διαιρεί το γινόμενο $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, οπότε είναι ίσος με έναν από τους $p_1, \ldots, p_k$. Άρα οι $q_1, \ldots, q_m$ είναι κάποιοι από τους $p_1, \ldots, p_k$ και μπορούμε στο γινόμενο $d = q_1^{\gamma_1} \cdots q_m^{\gamma_m}$ να εμφανίσουμε όλους τους $p_1, \ldots, p_k$, γράφοντας αυτούς που λείπουν με εκθέτη $0$. Άρα έχουμε

$$d = p_1^{\gamma_1} \cdots p_k^{\gamma_k},$$

όπου $\gamma_1, \ldots, \gamma_k \geq 0$.
Επειδή $d \mid n$, έχουμε

$$n = qd$$

για κάποιον $q$, οπότε

$$p_1^{\alpha_1} \cdots p_k^{\alpha_k} = q p_1^{\gamma_1} \cdots p_k^{\gamma_k}.$$

Αν $\gamma_1 > \alpha_1$, τότε

$$p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q p_1^{\gamma_1 - \alpha_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}.$$

Τότε, όμως, ο $p_1$ διαιρεί τον αριθμό στην δεξιά μεριά της ισότητας αλλά δεν διαιρεί τον αριθμό στην αριστερή της μεριά.
Άρα $\gamma_1 \leq \alpha_1$ και με τον ίδιο τρόπο βλέπουμε ότι $0 \leq \gamma_l \leq \alpha_l$ για κάθε $l$. □

**Παράδειγμα.** Η κανονική αναπαράσταση του $18$ είναι η

$$18 = 2 \cdot 3^2.$$

Άρα οι θετικοί διαιρέτες του $18$ είναι οι

$$2^0 3^0 = 1, \quad 2^0 3^1 = 3, \quad 2^0 3^2 = 9, \quad 2^1 3^0 = 2, \quad 2^1 3^1 = 6, \quad 2^1 3^2 = 18.$$

Αν γνωρίζουμε τις κανονικές αναπαραστάσεις των $n, m > 1$, μπορούμε να γράψουμε τους $n, m$ ως γινόμενα των *ίδιων* πρώτων. Πράγματι, αν κάποιος από τους πρώτους που εμφανίζονται στην κανονική αναπαράσταση του $n$ δεν εμφανίζεται στην κανονική αναπαράσταση του $m$, τότε μπορούμε να τον εμφανίσουμε και στην κανονική αναπαράσταση του $m$ με εκθέτη $0$. Το ίδιο γίνεται και με την κανονική αναπαράσταση του $n$.

**Παράδειγμα.** Οι κανονικές αναπαραστάσεις των $18, 375$ είναι

$$18 = 2^1 \cdot 3^2, \quad 375 = 3^1 \cdot 5^3.$$

Μπορούμε να γράψουμε

$$18 = 2^1 \cdot 3^2 \cdot 5^0, \quad 375 = 2^0 \cdot 3^1 \cdot 5^3.$$

**Πρόταση 4.5.** *Έστω ότι, χρησιμοποιώντας τις κανονικές αναπαραστάσεις των $n, m > 1$, έχουμε*

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad m = p_1^{\beta_1} \cdots p_k^{\beta_k},$$

*όπου οι $p_1, \ldots, p_k$ είναι πρώτοι με $p_1 < \ldots < p_k$ και $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k \geq 0$. Τότε*

$$(n, m) = p_1^{\gamma_1} \cdots p_k^{\gamma_k}, \quad [n, m] = p_1^{\delta_1} \cdots p_k^{\delta_k},$$

*όπου $\gamma_l = \min\{\alpha_l, \beta_l\}$ και $\delta_l = \max\{\alpha_l, \beta_l\}$ για κάθε $l$.*

*Απόδειξη.* Έστω $d$ ένας κοινός διαιρέτης των $n, m$. Τότε η δύναμη $p_l^{\gamma_l}$ μπορεί να εμφανίζεται ως παράγων του $d$ αν και μόνον αν

$$0 \leq \gamma_l \leq \alpha_l \quad \text{και} \quad 0 \leq \gamma_l \leq \beta_l$$

ή, ισοδύναμα, αν

$$0 \leq \gamma_l \leq \min\{\alpha_l, \beta_l\}.$$

Προφανώς, αν ο $d$ είναι ο μέγιστος κοινός διαιρέτης των $n, m$, θα ισχύει $\gamma_l = \min\{\alpha_l, \beta_l\}$.
Τώρα, έστω $e$ ένα κοινό θετικό πολλαπλάσιο των $n, m$. Τότε η δύναμη $p_l^{\alpha_l}$ καθώς και η δύναμη $p_l^{\beta_l}$ πρέπει να εμφανίζονται ως παράγοντες του $e$. Επομένως, η δύναμη $p_l^{\delta_l}$, όπου $\delta_l = \max\{\alpha_l, \beta_l\}$, πρέπει να εμφανίζεται ως παράγων του $e$. Πιθανόν ο $p_l$ να εμφανίζεται με εκθέτη $> \delta_l$ ως παράγων του $e$ και πιθανόν να εμφανίζονται και άλλοι πρώτοι πέρα από τους $p_1, \ldots, p_k$ ως παράγοντες του $e$. Αλλά είναι σαφές ότι το ελάχιστο κοινό θετικό πολλαπλάσιο των $n, m$ είναι αυτό που έχει ως παράγοντες μόνο τους $p_l^{\delta_l}$. □

**Παράδειγμα.** Από το προηγούμενο παράδειγμα βλέπουμε ότι

$$(18, 375) = 2^0 \cdot 3^1 \cdot 5^0 = 3, \quad [18, 375] = 2^1 \cdot 3^2 \cdot 5^3 = 2250.$$

**ΟΡΙΣΜΟΣ.** *Αν $n \geq 1$, τότε με*

$$\tau(n), \quad \sigma(n)$$

*συμβολίζουμε το πλήθος και το άθροισμα, αντιστοίχως, των θετικών διαιρετών του $n$.*

**Παράδειγμα.** Ο 6 έχει τους $1, 2, 3, 6$ ως θετικούς διαιρέτες, οπότε

$$\tau(6) = 4, \quad \sigma(6) = 1 + 2 + 3 + 6 = 12.$$

**Πρόταση 4.6.** *Αν $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ είναι η κανονική αναπαράσταση του $n > 1$, τότε*

$$\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1), \quad \sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

*Απόδειξη.* Είδαμε ότι οι θετικοί διαιρέτες του $n$ είναι οι αριθμοί

$$p_1^{\beta_1} \cdots p_k^{\beta_k}, \qquad 0 \leq \beta_1 \leq \alpha_1, \ldots, 0 \leq \beta_k \leq \alpha_k.$$

Επειδή έχουμε $a_l + 1$ επιλογές για τον εκθέτη $\beta_l$, βλέπουμε ότι μπορούμε να σχηματίσουμε ακριβώς $(\alpha_1 + 1) \cdots (\alpha_k + 1)$ τέτοια γινόμενα. Άρα το πλήθος των θετικών διαιρετών του $n$ είναι

$$\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1).$$

Κατόπιν, θεωρούμε το γινόμενο

$$(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k}).$$

Όταν αναπτύξουμε το γινόμενο θα προκύψει άθροισμα όρων καθένας από τους οποίους είναι γινόμενο ενός αριθμού από κάθε παρένθεση. Αυτοί οι όροι είναι ακριβώς οι παραπάνω θετικοί διαιρέτες του $n$. Άρα

$$\sigma(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k}) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

□

**Παράδειγμα.** Από τα προηγούμενα παραδείγματα έχουμε

$$375 = 3^1 \cdot 5^3.$$

Άρα

$$\tau(375) = (1 + 1)(3 + 1) = 8, \quad \sigma(375) = \frac{3^2 - 1}{3 - 1} \frac{5^4 - 1}{5 - 1} = 624.$$

## 4.2 Εικασίες, ιστορικά στοιχεία και αποτελέσματα για τους πρώτους.

Ήδη από την αρχαιότητα οι πρώτοι θεωρήθηκαν σημαντικοί αριθμοί και ένας προφανής λόγος για την σπουδαιότητά τους είναι ότι κάθε αριθμός $> 1$ είναι γινόμενο πρώτων. Κατά κάποιον τρόπο, οι αριθμοί "δημιουργούνται" από τους πρώτους. Οι πρώτοι είναι τα "δομικά υλικά" όλων των αριθμών. Ήταν, επομένως, φυσιολογικό να προκύψουν από την αρχαιότητα ερωτήματα σχετικά με την κατανομή των πρώτων ανάμεσα στους υπόλοιπους αριθμούς: πόσο "πυκνοί" ή πόσο "αραιοί" είναι οι πρώτοι;

Κατ' αρχάς έχουμε το εξής αποτέλεσμα.

**Πρόταση 4.7.** *Μπορούμε να βρούμε όσο θέλουμε μεγάλα διαστήματα διαδοχικών φυσικών που αποτελούνται μόνο από σύνθετους.*

*Απόδειξη.* Επιλέγουμε έναν $n$ οσοδήποτε μεγάλο. Τότε οι $n$ διαδοχικοί αριθμοί

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

είναι όλοι σύνθετοι.
Πράγματι, για κάθε $l$ με $2 \leq l \leq n+1$ ο $l$ διαιρεί τον $(n+1)!$ (είναι προφανώς ένας από τους παράγοντες του $(n+1)!$) και τον $l$, οπότε διαιρεί και τον $(n+1)!+l$. □

Από την άλλη μεριά, εκτός από τους $2, 3$ δεν υπάρχει άλλο ζεύγος διαδοχικών πρώτων. Πράγματι, από δυο διαδοχικούς ακεραίους ο ένας είναι οπωσδήποτε άρτιος. Προκύπτει, όμως, το ερώτημα αν υπάρχουν ζεύγη πρώτων με διαφορά $2$ και πόσα είναι αυτά τα ζεύγη.

**ΟΡΙΣΜΟΣ.** *Δυο πρώτοι χαρακτηρίζονται* **δίδυμοι** *αν διαφέρουν κατά* $2$.

Να μερικά τέτοια ζεύγη δίδυμων πρώτων:

$$3,5 \quad 5,7 \quad 11,13 \quad 17,19 \quad 29,31 \quad 41,43.$$

Μπορεί κάποιος να προχωρήσει και να υπολογίσει πολλά τέτοια ζεύγη δίδυμων πρώτων. Και έχουμε τώρα το φυσιολογικό:

**Ερώτημα.** *Υπάρχουν άπειρα ζεύγη δίδυμων πρώτων;*

Το ερώτημα αυτό δεν έχει απαντηθεί ακόμη. Το μέγιστο μέχρι στιγμής γνωστό ζεύγος δίδυμων πρώτων είναι το

$$3756801695685 \cdot 2^{666669} \pm 1.$$

Οι αριθμοί αυτοί έχουν $200700$ ψηφία.

Ένα άλλο είδος ερωτημάτων σχετικά με την κατανομή των πρώτων είναι αν κάποιοι πρώτοι μπορούν να έχουν κάποια συγκεκριμένη "μορφή" ή να ενταχθούν σε κάποια συγκεκριμένη "δομή". Ένα παράδειγμα τέτοιας "δομής" είναι μια αριθμητική πρόοδος, δηλαδή αριθμοί της μορφής $an+b$, όπου $b$ είναι ο αρχικός αριθμός (με $n=0$) και κάθε δυο διαδοχικοί τέτοιοι αριθμοί διαφέρουν κατά $a > 0$ (το "βήμα" της αριθμητικής προόδου):

$$b, a+b, 2a+b, 3a+b, 4a+b, \dots .$$

Είναι προφανές ότι υπάρχει μόνο ένας πρώτος της μορφής $2n$ (ο $2$) και άπειροι πρώτοι της μορφής $2n+1$ (όλοι οι υπόλοιποι πρώτοι).

Κάθε αριθμός είναι είτε της μορφής $4n$ είτε της μορφής $4n+1$ είτε της μορφής $4n+2$ είτε της μορφής $4n+3$. Αυτό προκύπτει αμέσως από την ταυτότητα της Ευκλείδειας διαίρεσης. Τώρα, δεν υπάρχει κανείς πρώτος της μορφής $4n$ και μόνο ένας της μορφής $4n+2$ (ο $2$). Άρα όλοι οι υπόλοιποι πρώτοι είναι είτε της μορφής $4n+1$ είτε της μορφής $4n+3$.

**Λήμμα 4.1.** *Γινόμενο αριθμών της μορφής* $4n+1$ *είναι αριθμός της μορφής* $4n+1$.

*Απόδειξη.* Έστω $a = 4n' + 1$ και $b = 4n'' + 1$. Τότε

$$ab = (4n' + 1)(4n'' + 1) = 16n'n'' + 4n' + 4n'' + 1 = 4(4n'n'' + n' + n'') + 1.$$

Άρα το γινόμενο δύο αριθμών της μορφής $4n + 1$ είναι αριθμός της μορφής $4n + 1$.
Για περισσότερους από δύο αριθμούς προχωράμε επαγωγικά. □

**Πρόταση 4.8.** *Υπάρχουν άπειροι πρώτοι της μορφής* $4n + 3$.

*Απόδειξη.* Έστω ότι υπάρχουν πεπερασμένου πλήθους πρώτοι της μορφής $4n + 3$ και έστω ότι αυτοί είναι οι

$$p_1, p_2, \ldots, p_k.$$

Θεωρούμε τον αριθμό

$$N = 4p_1 \cdots p_k - 1.$$

Ο $N$ είναι $> 1$, οπότε γράφεται ως γινόμενο πρώτων. Ο $N$ είναι περιττός, οπότε ο 2 δεν είναι πρώτος παράγων του $N$. Άρα κάθε πρώτος παράγων του $N$ είναι είτε της μορφής $4n + 1$ είτε της μορφής $4n + 3$.
Αν καθένας από τους πρώτους παράγοντες του $N$ ήταν της μορφής $4n + 1$, τότε και ο $N$ θα ήταν της μορφής $4n + 1$. Αυτό, όμως, είναι άτοπο, διότι

$$N = 4(p_1 \cdots p_k - 1) + 3.$$

Άρα ένας τουλάχιστον πρώτος διαιρέτης του $N$ είναι της μορφής $4n+3$. Αυτός ο διαιρέτης πρέπει να είναι ένας από τους $p_1, \ldots, p_k$ και έστω ότι είναι ο $p_l$.
Τότε, όμως,

$$p_l \mid N, \quad p_l \mid p_1 \cdots p_k,$$

οπότε

$$p_l \mid 4p_1 \cdots p_k - n = 1$$

και καταλήγουμε σε άτοπο. □

Μπορεί να αποδειχθεί, αλλά αρκετά πιο δύσκολα, ότι υπάρχουν και άπειροι πρώτοι της μορφής $4n + 1$.

Όμως, η πλήρης απάντηση για πρώτους της μορφής $an + b$ δίνεται από το επόμενο θεώρημα. Πριν από αυτό ας παρατηρήσουμε ότι, αν $(a, b) > 1$, τότε υπάρχει το πολύ ένας πρώτος της μορφής $an + b$. Πράγματι, ο $(a, b)$ διαιρεί τους $a, b$, οπότε διαιρεί και τον $an + b$ για κάθε $n$ και, επομένως, ο $an + b$ μπορεί να είναι πρώτος μόνο αν είναι ίσος με τον $(a, b)$ και ο $(a, b)$ είναι πρώτος. Άρα η μόνη περίπτωση να υπάρχουν άπειροι πρώτοι της μορφής $an + b$ είναι όταν $(a, b) = 1$.

**Θεώρημα 4.3.** *Αν* $a \geq 1$, $(a, b) = 1$, *τότε υπάρχουν άπειροι πρώτοι της μορφής* $an + b$.

Το θεώρημα αυτό αποδείχθηκε από τον Dirichlet το 1837 και η απόδειξη είναι πολύ δύσκολη.
Τώρα πάμε σε κάτι διαφορετικό.

**ΟΡΙΣΜΟΣ.** *Αν* $n \geq 1$, *τότε με*

$$\pi(n)$$

*συμβολίζουμε το πλήθος των πρώτων οι οποίοι είναι* $\leq n$.

Για παράδειγμα:

$$\pi(1) = 0, \quad \pi(2) = 1, \quad \pi(3) = \pi(4) = 2, \quad \pi(5) = \pi(6) = 3,$$

$$\pi(7) = \pi(8) = \pi(9) = \pi(10) = 4, \quad \pi(11) = \pi(12) = 5.$$

Είναι φανερό ότι, αν $p_n$ είναι ο $n$-οστός πρώτος, τότε

$$\pi(p_n) = \pi(p_n + 1) = \ldots = \pi(p_{n+1} - 1) = n.$$

Η συνάρτηση $\pi(n)$ είναι προφανώς αύξουσα και, επειδή οι πρώτοι είναι άπειροι,

$$\pi(n) \to +\infty \qquad \text{όταν } n \to +\infty.$$

**ΟΡΙΣΜΟΣ.** *Αν $f(n)$, $g(n)$ είναι δυο θετικές συναρτήσεις του $n$ και*

$$\frac{f(n)}{g(n)} \to 1 \qquad \textit{όταν } n \to +\infty,$$

*τότε γράφουμε*

$$f(n) \sim g(n)$$

*και λέμε ότι οι δυο συναρτήσεις είναι* **ασυμπτωτικά ίσες**.

Η συνάρτηση $\pi(n)$ μετράει πόσοι πρώτοι είναι πριν από τον $n$ και, επομένως, η ασυμπτωτική συμπεριφορά της παρέχει ένα "μέτρο" της κατανομής των πρώτων.

Ο Legendre το 1798 διατύπωσε την εικασία:

$$\pi(n) \sim \frac{n}{\log n - 1.08366}.$$

Ο Dirichlet το 1838 διατύπωσε την εικασία:

$$\pi(n) \sim \mathrm{Li}(n) = \int_2^n \frac{1}{\log t}\, dt.$$

Είναι εύκολο να δει κανείς ότι και οι δύο εικασίες λένε περίπου το ίδιο πράγμα, αφού

$$\frac{n}{\log n - 1.08366} \sim \frac{n}{\log n} \sim \mathrm{Li}(n).$$

Η απόδειξη του ότι $\frac{n}{\log n - 1.08366} \sim \frac{n}{\log n}$ είναι πολύ εύκολη και η απόδειξη του $\mathrm{Li}(n) \sim \frac{n}{\log n}$ γίνεται αν περάσουμε σε συνεχή μεταβλητή $x$ και χρησιμοποιήσουμε για παράδειγμα τον κανόνα του l' Hopitâl. Πράγματι,

$$\frac{\mathrm{Li}'(x)}{(x/\log x)'} = \frac{1/\log x}{(\log x - 1)/\log^2 x} = \frac{\log x}{\log x - 1} \to 1 \qquad \text{όταν } x \to +\infty.$$

Όμως, το 1843 σε ένα γράμμα του και το 1869 σε μια δημοσίευσή του ο Gauss έγραψε ότι γύρω στο 1792, όταν ήταν περίπου 15 ετών και αρκετά πριν από τον Legendre, είχε σκεφτεί τις παραπάνω εικασίες μετά από εκτενείς υπολογισμούς.

Το πρώτο αποτέλεσμα σ' αυτήν την κατεύθυνση ήταν το εξής.

**Πρόταση 4.9.** *Υπάρχουν δυο αριθμοί $A, B$ τέτοιοι ώστε $0 < A < 1 < B$ και ώστε να ισχύει*

$$A \leq \frac{\pi(n)}{n/\log n} \leq B \qquad \textit{για κάθε } n \geq 2.$$

*Επίσης, αν υπάρχει το $\lim_{n\to+\infty} \frac{\pi(n)}{n/\log n}$, τότε αυτό είναι ίσο με 1.*

Η απόδειξη δόθηκε από τον Tchebychef το 1850.

Τώρα θα πάμε λίγο πιο πίσω για να αναφέρουμε ένα φαινομενικά άσχετο θέμα. Το 1740 ο Euler μελέτησε την σειρά

$$\sum_{n=1}^{+\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{n^s} + \cdots.$$

Από τα μαθήματα του Απειροστικού Λογισμού γνωρίζουμε ότι αυτή η σειρά συγκλίνει όταν $s > 1$ και αποκλίνει στο $+\infty$ όταν $s \leq 1$. Αυτή η σειρά έπαιξε και συνεχίζει να παίζει σημαντικό ρόλο στην Θεωρία Αριθμών (αλλά και σε άλλες περιοχές των Μαθηματικών). Θα πούμε αρκετά γι αυτήν παρακάτω.

Τώρα, όπως ακριβώς ορίζεται η σύγκλιση μιας σειράς (δηλαδή ενός άπειροαθροίσματος) μέσω της συμπεριφοράς των μερικών αθροισμάτων της, έτσι ορίζεται και η σύγκλιση ενός **απειρογινομένου** μέσω της συμπεριφοράς των μερικών γινομένων του. *Πολύ πρόχειρα* (διότι δεν έχουμε σκοπό να ασχοληθούμε μεθοδικά με το θέμα) λέμε ότι ένα απειρογινόμενο

$$\prod_{n=1}^{+\infty} a_n$$

συγκλίνει αν η ακολουθία των μερικών γινομένων $b_n = a_1 a_2 \cdots a_n$ συγκλίνει σε κάποιον αριθμό.

Ας θεωρήσουμε τώρα την ακολουθία $p_n$ των πρώτων. Αυτό που απέδειξε ο Euler και αποτελεί μια πρώτη ένδειξη σύνδεσης της παραπάνω σειράς με τους πρώτους είναι η ισότητα:

$$\sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{n=1}^{+\infty} \frac{1}{1-\frac{1}{p_n^s}} = \frac{1}{1-\frac{1}{2^s}} \frac{1}{1-\frac{1}{3^s}} \frac{1}{1-\frac{1}{5^s}} \frac{1}{1-\frac{1}{7^s}} \cdots .$$

Βασισμένος σ' αυτήν την ισότητα, ο Euler απέδειξε ότι

$$\sum_{n=1}^{+\infty} \frac{1}{p_n} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots = +\infty.$$

Ένα προφανές πόρισμα είναι η απειρία των πρώτων. Πράγματι, αν το πλήθος των πρώτων ήταν πεπερασμένο, τότε το $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots$ θα ήταν ένα πεπερασμένο άθροισμα, οπότε η τιμή του θα ήταν αριθμός και όχι $+\infty$.

Τώρα, ξαναγυρνώντας στο θέμα μας με την συνάρτηση $\pi(n)$, μετά από το αποτέλεσμα του Tchebychef το 1850 έρχεται ο Riemann το 1859 και σε μια πολύ σημαντική εργασία του επεκτείνει το σύνολο από το οποίο παίρνει τιμές η μεταβλητή $s$ στην σειρά $\sum_{n=1}^{+\infty} \frac{1}{n^s}$ από το σύνολο $\mathbb{R}$ των πραγματικών στο σύνολο $\mathbb{C}$ των μιγαδικών. Δηλαδή, γράφει

$$\sum_{n=1}^{+\infty} \frac{1}{n^s} \qquad \text{με } s = \sigma + i\tau \ (\sigma, \tau \in \mathbb{R}).$$

Αποδεικνύεται ότι η σειρά αυτή συγκλίνει (σε μιγαδικό αριθμό) αν $\mathrm{Re} s = \sigma > 1$ και ορίζει μια συνάρτηση

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} \qquad \text{με } s = \sigma + i\tau \ (\sigma > 1, \tau \in \mathbb{R}). \tag{4.1}$$

Δηλαδή, η συνάρτηση $\zeta(s)$ ορίζεται μέσω της σειράς στο ημιεπίπεδο του μιγαδικού επιπέδου που βρίσκεται δεξιά της κατακόρυφης ευθείας $s = 1 + i\tau \, (\tau \in \mathbb{R})$.

Ο Riemann δεν μένει εκεί αλλά αποδεικνύει ότι η συνάρτηση $\zeta(s)$ μπορεί να ορισθεί σε ολόκληρο το μιγαδικό επίπεδο εκτός του σημείου $s = 1$, δηλαδή στο $\mathbb{C} \setminus \{1\}$, και ότι η συνάρτηση $\zeta(s)$ είναι (αυτό που λένε στην Μιγαδική Ανάλυση) μια **ολόμορφη συνάρτηση** στο $\mathbb{C} \setminus \{1\}$ (και ότι έχει πόλο τάξης 1 στο σημείο $s = 1$). Προσέξτε: *Ο τύπος της $\zeta(s)$ είναι ο (4.1) μόνο στο ημιεπίπεδο $s = \sigma + i\tau \ (\sigma > 1, \tau \in \mathbb{R})$. Στο υπόλοιπο πεδίο ορισμού της $\zeta(s)$ ο τύπος της $\zeta(s)$ είναι διαφορετικός (και δεν μας ενδιαφέρει εδώ).*

Τέλος, ο Riemann συσχετίζει την κατανομή των πρώτων με τις θέσεις των ριζών της $\zeta(s)$ στο μιγαδικό επίπεδο.

Η συνάρτηση $\zeta(s)$ ονομάζεται **ζήτα-συνάρτηση του Riemann**.

Χρησιμοποιώντας αυτήν την σχέση ανάμεσα στους πρώτους και στην ζήτα-συνάρτηση και χρησιμοποιώντας μεθόδους της Μιγαδικής Ανάλυσης, ο Hadamard και ο de la Valée Poussin έκλεισαν, ανεξάρτητα ο ένας από τον άλλον, το ζήτημα αποδεικνύοντας το 1896 το λεγόμενο

**Θεώρημα των Πρώτων Αριθμών.**

$$\pi(n) \sim \frac{n}{\log n}.$$

Έτσι, οι εικασίες των Gauss, Legendre και Diriclet αποδείχθηκαν σωστές.

Το 1949 ο Selberg απέδειξε με "στοιχειώδη" τρόπο (δηλαδή, χωρίς χρήση Μιγαδικής Ανάλυσης) το Θεώρημα των Πρώτων Αριθμών.

Πριν ξαναγυρίσουμε στους πρώτους, ας αναφέρουμε ότι η ζήτα-συνάρτηση έχει να κάνει με ένα από τα σημαντικότερα ανοικτά προβλήματα των Μαθηματικών, ίσως το δυσκολότερο. Είναι γνωστό ότι οι μόνες πραγματικές ρίζες της $\zeta(s)$ είναι οι αρνητικοί άρτιοι $s = -2, -4, -6, \ldots$. Επίσης, είναι γνωστό ότι οι γνησίως μιγαδικές ρίζες της $\zeta(s)$ βρίσκονται όλες μέσα στην κατακόρυφη ζώνη

$$s = \sigma + i\tau \ (0 < \sigma < 1, \tau \in \mathbb{R}).$$

Λοιπόν, το ανοικτό πρόβλημα είναι η λεγόμενη

**Εικασία του Riemann.** *Οι γνησίως μιγαδικές ρίζες της $\zeta(s)$ βρίσκονται όλες πάνω στην κατακόρυφη ευθεία*

$$s = \frac{1}{2} + i\tau \ (\tau \in \mathbb{R}).$$

Αν δεν κάνω λάθος, έχει υπολογισθεί ότι $10^{13}$ γνησίως μιγαδικές ρίζες της $\zeta(s)$ βρίσκονται πάνω στην **κρίσιμη ευθεία** $s = \frac{1}{2} + i\tau \ (\tau \in \mathbb{R})$ και δεν έχει βρεθεί καμιά εκτός της κρίσιμης ευθείας.

Πάμε παρακάτω σε περισσότερα προβλήματα.

**Ερώτημα.** *Υπάρχουν άπειροι πρώτοι της μορφής $n^2 + 1$;*

**Ερώτημα.** *Υπάρχει για κάθε $n$ πρώτος ανάμεσα στους $n^2$ και $(n+1)^2$;*

Το επόμενο πολύ γνωστό ανοικτό πρόβλημα διατυπώθηκε το 1742 από τον Goldbach.

**Εικασία του Goldbach.** *Κάθε άρτιος $\geq 4$ είναι άθροισμα δύο πρώτων.*

Για παράδειγμα:

$$4 = 2+2, \quad 6 = 3+3, \quad 8 = 3+5, \quad 10 = 3+7 = 5+5, \quad 12 = 5+7, \quad 14 = 3+11 = 7+7.$$

Η εικασία του Goldbach θεωρείται εξαιρετικά δύσκολο πρόβλημα. Μέχρι στιγμής έχει ελεγχθεί και ισχύει για όλους τους άρτιους $\leq 4 \cdot 10^{18}$.

Ο Goldbach διατύπωσε και την επόμενη εικασία.

**Ασθενής εικασία του Goldbach.** *Κάθε περιττός $\geq 7$ είναι άθροισμα τριών πρώτων.*

Είναι σχεδόν προφανές ότι, αν είναι αληθής η εικασία του Goldbach, τότε είναι αληθής και η ασθενής εικασία του Goldbach. (Διότι, αν ο $n$ είναι περιττός, τότε ο $n-2$ είναι άρτιος και ο $2$ είναι πρώτος.)

Ο Vinogradov το 1937 απέδειξε το:

**Θεώρημα 4.4.** *Υπάρχει $n_0$ ώστε κάθε περιττός $\geq n_0$ είναι άθροισμα τριών πρώτων.*

Επομένως, για να αποδειχθεί η ασθενής εικασία του Goldbach ήταν αρκετό να προσδιορισθεί ο $n_0$ και μετά να ελεγχθεί αν κάθε περιττός $< n_0$ είναι άθροισμα τριών πρώτων. Μια εκτίμηση για τον $n_0$ ήταν η $n_0 \approx 3^{3^{15}}$, οπότε είναι εξαιρετικά δύσκολο να γίνει ο απαραίτητος έλεγχος με τους υπάρχοντες υπολογιστές. Αν δεν κάνω λάθος ο Helfgott το 2012 έκλεισε το ζήτημα των υπολογισμών και τώρα η ασθενής εικασία του Goldbach θεωρείται αποδειγμένη.

Υπήρχε και η Εικασία του Bertrand η οποία αποδείχθηκε από τον Tchebychef το 1850. Ιδού.

**Θεώρημα 4.5.** *Για κάθε $n$ υπάρχει πρώτος ανάμεσα στους $n$ και $2n$.*

Τέλος, θα πούμε μερικά πράγματα για το παλιό ζήτημα των *τέλειων* αριθμών.

**ΟΡΙΣΜΟΣ.** *Ένας φυσικός χαρακτηρίζεται* **τέλειος** *αν είναι ίσος με το άθροισμα των θετικών διαιρετών του που είναι μικρότεροί του.*

Με άλλα λόγια, ο φυσικός $n$ είναι τέλειος αν ο $2n$ είναι ίσος με το άθροισμα των θετικών διαιρετών του $n$ (του $n$ συμπεριλαμβανομένου):

$$\sigma(n) = 2n.$$

Για παράδειγμα, από την αρχαιότητα είχαν δει ότι ο $6$ και ο $28$ είναι τέλειοι, αφού

$$1 + 2 + 3 + 6 = 2 \cdot 6, \qquad 1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28.$$

Οι δυο επόμενοι τέλειοι είναι ο $496$ και ο $8128$. Και οι τέσσερις αριθμοί είναι άρτιοι.

**Ερώτημα.** *Υπάρχει έστω και ένας περιττός τέλειος;*

Μέχρι τώρα δεν έχει βρεθεί ούτε ένας περιττός τέλειος!

**Ερώτημα.** *Υπάρχουν άπειροι άρτιοι τέλειοι;*

Ας παρατηρήσουμε ότι κάθε άρτιος μπορεί να γραφτεί στην μορφή

$$\text{άρτιος} = 2^{k-1}\text{περιττός} \qquad \text{με } k \geq 2.$$

(Ο $2^{k-1}$ είναι η μέγιστη δύναμη του $2$ που διαιρεί τον άρτιο.)

Σχετικά με τους άρτιους τέλειους ο Ευκλείδης είχε αποδείξει το εξής.

**Πρόταση 4.10.** *Αν ο άρτιος φυσικός $n$ είναι της μορφής*

$$n = 2^{k-1}(2^k - 1),$$

*όπου $k \geq 2$ και ο $2^k - 1$ είναι πρώτος, τότε ο $n$ είναι τέλειος.*

*Απόδειξη.* Έστω ότι $k \geq 2$ και ότι ο

$$p = 2^k - 1$$

είναι πρώτος.
Τότε οι διαιρέτες του $n = 2^{k-1}p$ είναι οι

$$1, 2, \ldots, 2^{k-1}, p, 2p, \ldots, 2^{k-1}p.$$

Άρα

$$\sigma(n) = 1+2+\cdots+2^{k-1}+p+2p+\cdots+2^{k-1}p = \big(1+2+\cdots+2^{k-1}\big)(1+p) = (2^k-1)2^k = 2n,$$

οπότε ο $n$ είναι τέλειος. □

Πολλά χρόνια αργότερα ο Euler απέδειξε το αντίστροφο της Πρότασης του Ευκλείδη.

Ας κάνουμε πρώτα μια απλή παρατήρηση. *Αν $k \geq 2$ και ο $2^k - 1$ είναι πρώτος, τότε ο $k$ είναι πρώτος.* Πράγματι, ας υποθέσουμε ότι ο $k \geq 2$ είναι σύνθετος, οπότε $k = lm$ με $1 < l < k$ και $1 < m < k$. Τότε

$$2^k - 1 = (2^l)^m - 1 = (2^l - 1)\big(1 + 2^l + \cdots + (2^l)^{m-1}\big),$$

οπότε ο $2^k - 1$ είναι γινόμενο δυο αριθμών $> 1$ και άρα είναι σύνθετος.

Άρα η Πρόταση του Ευκλείδη ουσιαστικά διατυπώνεται ως εξής: *Αν ο άρτιος φυσικός $n$ είναι της μορφής $n = 2^{p-1}(2^p - 1)$, όπου ο $p$ είναι πρώτος και ο $2^p - 1$ είναι πρώτος, τότε ο $n$ είναι τέλειος.* Το αποτέλεσμα του Euler είναι ακριβώς το αντίστροφο.

**Πρόταση 4.11.** *Αν ο άρτιος φυσικός $n$ είναι τέλειος, τότε είναι της μορφής*

$$n = 2^{p-1}(2^p - 1),$$

*όπου ο $p$ είναι πρώτος και ο $2^p - 1$ είναι πρώτος.*

*Απόδειξη.* Έστω ότι ο άρτιος φυσικός $n$ είναι τέλειος.
Γράφουμε

$$n = 2^{k-1}m, \tag{4.2}$$

όπου $k \geq 2$ και ο $m$ είναι περιττός.
Οι $2^{k-1}, m$ είναι προφανώς σχετικά πρώτοι, οπότε από την Πρόταση 3.7 συνεπάγεται ότι οι θετικοί διαιρέτες του $n$ είναι οι αριθμοί

$$2^l d,$$

όπου ο $2^l$ διατρέχει τους $1, 2, 2^2, \ldots, 2^{k-1}$ και ο $d$ διατρέχει τους θετικούς διαιρέτες του $m$.
Άρα το άθροισμα των θετικών διαιρετών του $n$ είναι ίσο με

$$\big(1 + 2 + \cdots + 2^{k-1}\big)\big(\text{άθροισμα των θετικών διαιρετών } d \text{ του } m\big).$$

Δηλαδή,

$$\sigma(n) = (2^k - 1)\sigma(m).$$

Επειδή ο $n$ είναι τέλειος, έχουμε ότι

$$2n = (2^k - 1)\sigma(m)$$

και, λόγω της (4.2),

$$2^k m = (2^k - 1)\sigma(m).$$

Αυτό μας λέει ότι ο $2^k$ διαιρεί τον $(2^k - 1)\sigma(m)$. Τώρα, επειδή οι $2^k, 2^k - 1$ είναι σχετικά πρώτοι, συνεπάγεται ότι

$$2^k \mid \sigma(m).$$

Άρα

$$\sigma(m) = 2^k q \tag{4.3}$$

για κάποιον $q$, οπότε

$$2^k m = (2^k - 1)2^k q$$

και άρα

$$m = (2^k - 1)q. \tag{4.4}$$

Από τις (4.3), (4.4) παίρνουμε

$$\sigma(m) = q + m.$$

Η (4.4) λέει ότι ο $q$ είναι θετικός διαιρέτης του $m$ μικρότερος του $m$, οπότε η τελευταία ισότητα λέει ότι το $\sigma(m)$ είναι το άθροισμα των θετικών διαιρετών $q, m$ του $m$. Όμως, το $\sigma(m)$ είναι εξ ορισμού το άθροισμα *όλων* των θετικών διαιρετών του $m$, δύο από τους οποίους είναι αναγκαστικά οι $1, m$. Άρα ο $m$ έχει ακριβώς δύο θετικούς διαιρέτες, οπότε είναι πρώτος, και

$$q = 1.$$

Τώρα από την (4.4) έχουμε ότι $m = 2^k - 1$ και, επειδή ο $m$ είναι πρώτος, θα είναι και ο $k$ πρώτος. Άρα μπορούμε να αλλάξουμε το σύμβολο του $k$ σε $p$ και η (4.2) γίνεται

$$n = 2^{p-1}(2^p - 1)$$

και η απόδειξη έχει τελειώσει. □

Παρατηρήστε ότι και οι τέσσερις τέλειοι που είδαμε μέχρι τώρα επιβεβαιώνουν την Πρόταση 4.11 του Euler:

$$6 = 2^{2-1}(2^2-1), \quad 28 = 2^{3-1}(2^3-1), \quad 496 = 2^{5-1}(2^5-1), \quad 8128 = 2^{7-1}(2^7-1).$$

**ΟΡΙΣΜΟΣ.** *Ένας πρώτος $p$ χαρακτηρίζεται* **Mersenne-πρώτος** *αν και ο $2^p-1$ είναι πρώτος.*

Για παράδειγμα οι $2, 3, 5, 7, 13$ είναι Mersenne-πρώτοι ενώ ο πρώτος $11$ δεν είναι Mersenne-πρώτος. Πράγματι,

$$2^{11} - 1 = 23 \cdot 89.$$

Μετά από την προηγούμενη συζήτηση είναι σαφές ότι *ο πρώτος $p$ είναι Mersenne-πρώτος αν και μόνο αν ο άρτιος $n = 2^{p-1}(2^p-1)$ είναι τέλειος*. Με άλλα λόγια οι Mersenne-πρώτοι και οι άρτιοι τέλειοι είναι σε αμφιμονοσήμαντη αντιστοιχία. Επομένως, το τελευταίο *ερώτημα* διατυπώνεται ισοδύναμα ως εξής:

**Ερώτημα.** *Υπάρχουν άπειροι Mersenne-πρώτοι;*

Απ' όσο γνωρίζω, η κατάσταση έχει ως εξής. Μέχρι σήμερα έχουν βρεθεί όλοι οι Mersenne-πρώτοι μέχρι και τον πρώτο $30402457$. Δηλαδή, έχει βρεθεί ποιοί από τους πρώτους μέχρι τον συγκεκριμένο πρώτο είναι Mersenne-πρώτοι και ποιοί δεν είναι Mersenne-πρώτοι. Το πλήθος των Mersenne-πρώτων μέχρι και τον $30402457$ είναι σαράντα τρία. Μετά από αυτόν τον πρώτο είναι γνωστοί άλλοι πέντε Mersenne-πρώτοι, οι $32582657$, $37156667$, $42643801$, $43112609$, $57885161$. Δηλαδή, γνωρίζουμε συνολικά σαράντα οκτώ Mersenne-πρώτους. Για να πάρετε μια ιδέα, αναφέρω τα εξής λίγα ιστορικά στοιχεία. Ο Euler απέδειξε το 1772 ότι ο $31$ είναι Mersenne-πρώτος. Ο Lucas απέδειξε το 1867 ότι ο πρώτος $67$ δεν είναι Mersenne-πρώτος, δηλαδή ότι ο $2^{67}-1$ είναι σύνθετος, αλλά χωρίς να βρει συγκεκριμένη παραγοντοποίηση του $2^{67}-1$, ενώ το 1903 ο Cole βρήκε την παραγοντοποίηση

$$2^{67} - 1 = 193707721 \cdot 761838257287$$

μετά από πολλά χρόνια πράξεων. Τέλος, το 1984, μετά από 32 ώρες εργασίας ενός supercomputer, βρέθηκε συγκεκριμένη παραγοντοποίηση του $2^{251}-1$.

## 4.3 Ασκήσεις.

1. Είναι οι αριθμοί $701, 1009$ πρώτοι;
2. Βρείτε την κανονική αναπαράσταση των $10140, 36000, 255255$.
3. Βρείτε πρώτο $p$ ώστε ο $p+3$ να είναι πρώτος. Πόσοι τέτοιοι $p$ υπάρχουν;
4. Αν ο $p$ είναι πρώτος και $p \mid a^n$, αποδείξτε ότι $p^n \mid a^n$.
   Αν ο $p$ είναι πρώτος και $(a,b) = p$, βρείτε τους $(a^2, b^2), (a^2, b), (a^3, b^2)$.
   Αν ο $p$ είναι πρώτος και $(a, p^2) = p, (b, p^3) = p^2$, βρείτε τους $(ab, p^4), (a+b, p^4)$.
5. Βρείτε την κανονική αναπαράσταση του $832!$. Ξαναδοκιμάστε αφού λύσετε την άσκηση 25.
6. Αποδείξτε ότι
$$(a, [b,c]) = [(a,b),(a,c)], \quad [a,(b,c)] = ([a,b],[a,c]).$$
7. Έστω $a > 1$. Αποδείξτε ότι ο $a$ είναι $n$-οστή δύναμη αν και μόνο αν όλοι οι εκθέτες στην κανονική αναπαράσταση του $a$ είναι πολλαπλάσια του $n$.

8. Βρείτε την γενική μορφή των φυσικών οι οποίοι είναι διπλάσιοι τετραγώνου και τριπλάσιοι τρίτης δύναμης και πενταπλάσιοι πέμπτης δύναμης. Ποιός είναι ο ελάχιστος τέτοιος φυσικός;

9. Έστω $(x,3)=(y,3)=1$. Αποδείξτε ότι ο $x^2+y^2$ δεν είναι τετράγωνο.

10. Αν ο $p$ είναι πρώτος και $p\neq 2,5$, αποδείξτε ότι $10 \mid p^2-1$ ή $10 \mid p^2+1$.

11. Αν ο $p$ είναι πρώτος, αποδείξτε ότι $\sqrt{p}$ είναι άρρητος.

    Έστω $n\geq 2$. Αν ο $\sqrt[n]{a}$ είναι ρητός, αποδείξτε ότι είναι ακέραιος.

    Αν $n\geq 2$, αποδείξτε ότι ο $\sqrt[n]{n}$ είναι άρρητος.

12. Ο $a>1$ ονομάζεται *ελεύθερος τετραγώνου* αν δεν διαιρείται από κανένα τετράγωνο $>1$. Αποδείξτε ότι ο $a>1$ είναι ελεύθερος τετραγώνου αν και μόνο αν είναι γινόμενο διαφορετικών πρώτων.

    Αποδείξτε ότι κάθε $a>1$ γράφεται με μοναδικό τρόπο ως $a=bc$, όπου ο $b$ είναι ελεύθερος τετραγώνου και ο $c$ είναι τετράγωνο.

13. Αποδείξτε ότι κάθε $a>1$ γράφεται με μοναδικό τρόπο ως $a=2^k m$, όπου $k\geq 0$ και ο $m$ είναι περιττός.

14. Έστω $k\geq 2$, $a,b,c\geq 1$, $ab=c^k, (a,b)=1$. Αποδείξτε ότι υπάρχουν $m,n\geq 1$ ώστε $a=m^k, b=n^k, c=mn$.

15. Αν $n>1$, αποδείξτε ότι ο $n^4+4$ είναι σύνθετος.

16. Αν ο $n>4$ είναι σύνθετος, αποδείξτε ότι $n \mid (n-1)!$.

17. Αν $ad-bc=\pm 1, u=am+bn, v=cm+dn$, αποδείξτε ότι $(m,n)=(u,v)$.

18. Αν ο $2^n+1$ είναι πρώτος, αποδείξτε ότι ο $n$ είναι δύναμη του 2.

19. Αν $n>2$, αποδείξτε ότι υπάρχει πρώτος $p$ ώστε $n<p<n!$. (Υπόδειξη: υπάρχει πρώτος διαιρέτης του $n!-1$.)

20. Έστω $p_n$ ο $n$-οστός πρώτος. Αποδείξτε ότι $p_n\leq 2^{2^{n-1}}$. (Υπόδειξη: αποδείξτε ότι $p_{n+1}\leq p_1\cdots p_n+1$.)

21. Αν $\sigma_m(a)$ είναι το άθροισμα των $m$-οστών δυνάμεων των θετικών διαιρετών του $a>1$ και αν $a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ είναι η κανονική αναπαράσταση του $a$, αποδείξτε ότι

$$\sigma_m(a)=\frac{p_1^{m(\alpha_1+1)}-1}{p_1^m-1}\cdots\frac{p_k^{m(\alpha_k+1)}-1}{p_k^m-1}.$$

22. Χρησιμοποιώντας την εικασία του Bertrand, αποδείξτε ότι για τον $n$-οστό πρώτο $p_n$ ισχύει $p_n\leq 2^n$.

23. Αποδείξτε ότι κάθε πρώτος $>3$ είναι είτε της μορφής $6n+1$ είτε της μορφής $6n+5$.

    Αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $6n+5$.

24. Έστω $2^k$ η μέγιστη δύναμη του 2 ανάμεσα στους $1,2,\ldots,n$. Αποδείξτε ότι ο $2^k$ δεν διαιρεί κανέναν από τους $1,2,\ldots,n$, εκτός από τον ίδιο τον $2^k$.

    Αποδείξτε ότι ο $\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$ δεν είναι ακέραιος.

25. Αν $m,n\geq 1$, αποδείξτε ότι το πλήθος των θετικών διαιρετών του $m$ οι οποίοι είναι $\leq n$ ισούται με $[\frac{n}{m}]$.

Αν $n \geq 1$ και ο $p$ είναι πρώτος, αποδείξτε ότι ο εκθέτης του $p$ στην κανονική αναπαράσταση του $n!$ είναι ίσος με

$$\sum_{k=1}^{+\infty} \Big[\frac{n}{p^k}\Big].$$

Παρατηρήστε ότι η τελευταία σειρά είναι στην πραγματικότητα πεπερασμένο άθροισμα.

Αποδείξτε ότι ισχύει $[x] + [y] \leq [x + y]$ για κάθε $x, y \in \mathbb{R}$.

Αν $n, m \geq 1$, αποδείξτε ότι ο $\frac{(n+m)!}{n!m!}$ είναι ακέραιος.

Αν $n \geq 1$, αποδείξτε ότι ο $\binom{2n}{n}$ είναι άρτιος.

Αν $n \geq 1$ και ο $p$ είναι πρώτος, αποδείξτε ότι ο εκθέτης του $p$ στην κανονική αναπαράσταση του $\binom{2n}{n}$ είναι ίσος με

$$\sum_{k=1}^{+\infty} \Big( \Big[\frac{2n}{p^k}\Big] - 2\Big[\frac{n}{p^k}\Big] \Big).$$

Αν $n < p < 2n$, τότε αυτός ο εκθέτης είναι ίσος με 1.

## 4.4 Λύσεις ασκήσεων.

1. Αν ο $701$ είναι σύνθετος, τότε έχει πρώτο παράγοντα $\leq \sqrt{701}$ ή, ισοδύναμα, $\leq 26$. Αυτό σημαίνει ότι θα δοκιμάσουμε τους πρώτους $2, 3, 5, 7, 11, 13, 17, 19, 23$ για να δούμε αν κάποιος από αυτούς διαιρεί τον $701$. Αν κάποιος διαιρεί τον $701$, τότε ο $701$ είναι σύνθετος ενώ, αν κανένας δεν διαιρεί τον $701$, τότε ο $701$ είναι πρώτος. Δοκιμάζουμε και προκύπτει η δεύτερη περίπτωση, οπότε ο $701$ είναι πρώτος.

3. Είναι σαφές ότι ακριβώς ένας από τους $p, p+3$ είναι άρτιος. Άρα η μόνη περίπτωση να είναι οι $p, p + 3$ πρώτοι είναι όταν $p = 2$.

4. (i) Έστω ότι ο πρώτος $p$ διαιρεί το $a^n$. Τότε ο $p$ διαιρεί έναν τουλάχιστον από τους παράγοντες του $a^n = a \cdots a$, οπότε ο $p$ διαιρεί το $a$. Άρα

$$a = kp$$

για κάποιο $k$ και, επομένως,

$$a^n = k^n p^n.$$

Άρα ο $p^n$ διαιρεί το $a^n$.
(ii) Έστω $(a, p) = p$ και ο $p$ είναι πρώτος. Μπορούμε, επίσης, να υποθέσουμε ότι $a, b \geq 0$. Αν $a = 0$, τότε $b = p$, οπότε $(a^3, b^2) = (0, p^2) = p^2$. Ομοίως, αν $b = 0$, τότε $a = p$, οπότε $(a^3, b^2) = (p^3, 0) = p^3$.
Αν $a, b \geq 1$, επειδή $(a, b) = p$, συνεπάγεται ότι ο $p$ είναι ο μοναδικός πρώτος που εμφανίζεται και στις δύο κανονικές αναπαραστάσεις, των $a, b$. Δηλαδή, αν οι κανονικές αναπαραστάσεις των $a, b$ είναι

$$a = p^{\alpha} q_1^{\alpha_1} \cdots q_n^{\alpha_n}, \qquad b = p^{\beta} r_1^{\beta_1} \cdots r_m^{\beta_m},$$

όπου οι $q_1, \ldots, q_n, r_1, \ldots, r_m$ είναι οι αντίστοιχοι πρώτοι παράγοντες, τότε καθένας από τους $q_1, \ldots q_n$ είναι διαφορετικός από καθέναν από τους $r_1, \ldots r_m$.
Τώρα, επειδή $(a, b) = p$, συνεπάγεται ότι

$$\min\{\alpha, \beta\} = 1,$$

οπότε $\alpha = 1$ ή $\beta = 1$.
Επίσης,

$$a^3 = p^{3\alpha} q_1^{3\alpha_1} \cdots q_n^{3\alpha_n}, \qquad b^2 = p^{2\beta} r_1^{2\beta_1} \cdots r_m^{2\beta_m},$$

οπότε

$$(a^3, b^2) = p^{\min\{3\alpha, 2\beta\}}.$$

Άρα, αν $\alpha \geq 1, \beta = 1$, τότε $(a^3, b^2) = p^2$ και, αν $\alpha = 1, \beta \geq 2$, τότε $(a^3, b^2) = p^3$.

5. Ας δούμε πρώτα μερικά απλούστερα παραδείγματα:

$$10! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot (2 \cdot 3) \cdot 7 \cdot 2^3 \cdot 3^2 \cdot (2 \cdot 5) = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7.$$

$$\begin{aligned} 20! &= 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \cdot 17 \cdot 18 \cdot 19 \cdot 20 \\ &= 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot (2 \cdot 3) \cdot 7 \cdot 2^3 \cdot 3^2 \cdot (2 \cdot 5) \cdot 11 \cdot (2^2 \cdot 3) \cdot 13 \cdot (2 \cdot 7) \cdot (3 \cdot 5) \cdot \\ &\quad \cdot 2^4 \cdot 17 \cdot (2 \cdot 3^2) \cdot 19 \cdot (2^2 \cdot 5) \\ &= 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19. \end{aligned}$$

Είναι φανερό ότι η περίπτωση του $832!$ είναι ανέφικτη σε λογικό χρόνο.

9. Στην άσκηση 1.4 είχαμε δει ότι κάθε τετράγωνο $n^2$ είναι είτε της μορφής $3k$ είτε της μορφής $3k + 1$ και όχι της μορφής $3k + 2$. Μάλιστα, το $n^2$ είναι της μορφής $3k$ αν και μόνο αν το $n$ είναι της μορφής $3m$.
Τώρα, επειδή $(x, 3) = 1$ και ο 3 είναι πρώτος, συνεπάγεται ότι το 3 δεν διαιρεί το $x$, οπότε το $x^2$ είναι της μορφής $3k + 1$. Για τον ίδιο λόγο, και το $y^2$ είναι της μορφής $3l + 1$. Άρα

$$x^2 + y^2 = 3(k + l) + 2,$$

οπότε το $x^2 + y^2$ δεν είναι τετράγωνο.

14. Αν $a = 1$ ή $b = 1$, τότε το συμπέρασμα είναι προφανές. Οπότε υποθέτουμε ότι $a, b, c > 1$ και θεωρούμε την κανονική αναπαράσταση του $c$:

$$c = p_1^{\alpha_1} \cdots p_l^{\alpha_l}.$$

Τότε η κανονική αναπαράσταση του $c^k$ είναι η

$$c^k = p_1^{k\alpha_1} \cdots p_l^{k\alpha_l}.$$

Επειδή $ab = c^k$, κάθε πρώτος παράγων των $a, b$ είναι και πρώτος παράγων του $c^k$. Άρα οι κανονικές αναπαραστάσεις των $a, b$ είναι γινόμενα δυνάμεων των $p_1, \ldots, p_l$. Και επειδή $(a, b) = 1$, οι $a, b$ δεν έχουν κοινούς πρώτους παράγοντες, οπότε οι πρώτοι που οι δυνάμεις τους περιέχονται στην κανονική αναπαράσταση του $a$ είναι διαφορετικοί από τους πρώτους που οι δυνάμεις τους περιέχονται στην κανονική αναπαράσταση του $b$. Τώρα, θεωρώντας έναν οποιονδήποτε παράγοντα $p_j^{k\alpha_j}$, βλέπουμε ότι αυτός περιέχεται *ολόκληρος* είτε στην κανονική αναπαράσταση του $a$ είτε στην κανονική αναπαράσταση του $b$. Άρα η κανονική αναπαράσταση του $a$ είναι το γινόμενο κάποιων από τους παράγοντες $p_j^{k\alpha_j}$ και η κανονική αναπαράσταση του $b$ είναι το γινόμενο των υπόλοιπων παραγόντων $p_j^{k\alpha_j}$. Άρα καθένας από τους $a, b$ είναι το γινόμενο δυνάμεων με εκθέτη $k$ και άρα καθένας από τους $a, b$ είναι δύναμη με εκθέτη $k$.

15. Γράφουμε

$$n^4 + 4 = (n^2 + 2)^2 - 4n^2 = (n^2 + 2 - 2n)(n^2 + 2 + 2n).$$

Επειδή $n > 1$, συνεπάγεται ότι $n^2 + 2 - 2n > 1$, οπότε ο $n^4 + 4$ είναι σύνθετος.

23. (i) Κάθε αριθμός είναι είτε της μορφής $6n$ είτε της μορφής $6n+1$ είτε της μορφής $6n+2$ είτε της μορφής $6n+3$ είτε της μορφής $6n+4$ είτε της μορφής $6n+5$. Τώρα, ένας πρώτος δεν μπορεί να είναι της μορφής $6n$, διότι δεν είναι πολλαπλάσιο του 6. Αν ένας πρώτος είναι της μορφής $6n+2$, τότε είναι πολλαπλάσιο του 2, οπότε είναι ο 2. Αν ένας πρώτος είναι της μορφής $6n+4$, τότε είναι πολλαπλάσιο του 2, οπότε είναι ο 2 και έχουμε άτοπο διότι ο 2 δεν είναι της μορφής $6n+4$. Τέλος, αν ένας πρώτος είναι της μορφής $6n+3$, τότε είναι πολλαπλάσιο του 3, οπότε είναι ο 3. Το συμπέρασμα είναι ότι ένας πρώτος $>3$ είναι είτε της μορφής $6n+1$ είτε της μορφής $6n+5$.
(ii) Ας υποθέσουμε (για να καταλήξουμε σε άτοπο) ότι υπάρχουν μόνο πεπερασμένου πλήθους πρώτοι της μορφής $6n+5$ και ας υποθέσουμε ότι όλοι οι πρώτοι της μορφής $6n+5$ είναι οι

$$p_1, \ldots, p_m.$$

Σχηματίζουμε τον αριθμό

$$N = 6p_1 \cdots p_m - 1.$$

Παραδείγματα πρώτων της μορφής $6n+5$ είναι οι $5, 11, 17$. Άρα $N > 1$, οπότε ο $N$ είναι γινόμενο πρώτων παραγόντων.
Έστω $p$ ένας πρώτος παράγων του $N$. Αν ο $p$ είναι ένας από τους $2, 3, p_1, \ldots, p_m$, τότε:

$$p \mid N,\ p \mid 6p_1 \cdots p_m \quad \Rightarrow \quad p \mid 1$$

το οποίο είναι αδύνατο. Άρα ο $p$ είναι πρώτος $>3$ και διαφορετικός από όλους τους πρώτους της μορφής $6n+5$. Βάσει του (i), ο $p$ είναι της μορφής $6n+1$.
Αποδείξαμε, λοιπόν, ότι κάθε πρώτος παράγων του $N$ είναι της μορφής $6n+1$ και, επειδή ο $N$ είναι ίσος με το γινόμενο των πρώτων παραγόντων του, συμπεραίνουμε ότι ο $N$ είναι ίσος με το γινόμενο αριθμών της μορφής $6n+1$. Όμως, αυτό συνεπάγεται ότι ο $N$ είναι της μορφής $6n+1$. Πράγματι, το γινόμενο δύο αριθμών της μορφής $6n+1$ είναι αριθμός της μορφής $6n+1$, διότι

$$(6n'+1)(6n''+1) = 6(n'n''+n'+n'')+1 = 6n+1,$$

και αυτό επεκτείνεται με επαγωγή για το γινόμενο περισσοτέρων των δύο αριθμών.
Όμως, το ότι ο $N$ είναι της μορφής $6n+1$ είναι άτοπο, αφού ο $N$ είναι της μορφής

$$N = 6(p_1 \cdots p_m - 1) + 5 = 6n+5.$$

25. (i) Τα θετικά πολλαπλάσια του $m$ τα οποία είναι $\leq n$ είναι οι διαδοχικοί αριθμοί

$$m, \quad 2m, \quad 3m, \quad \ldots, \quad qm,$$

όπου

$$qm \leq n < (q+1)m.$$

Από την τελευταία σχέση συνεπάγεται

$$q \leq \frac{n}{m} < q+1$$

οπότε το πλήθος είναι ίσο με $q = [\frac{n}{m}]$.
(ii) Για καθέναν από τους $m = 1, 2, 3, \ldots, n$ βρίσκουμε την μέγιστη δύναμη $p^{\alpha_m}$ που διαιρεί τον $m$. Τότε η μέγιστη δύναμη του $p$ που διαιρεί τον $n!$ είναι ο

$$p^{\alpha_1} p^{\alpha_2} p^{\alpha_3} \cdots p^{\alpha_n} = p^{\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_n}.$$

Άρα ο εκθέτης $k$ που ζητάμε είναι ο

$$k = \alpha_1 + \cdots + \alpha_n.$$

Τώρα, γράφουμε σε μια σειρά τους αριθμούς $1, \ldots, n$ και κάτω από κάθε $m = 1, \ldots, n$ σχηματίζουμε μια στήλη με $\alpha_m$ διαδοχικές κουκίδες. Έτσι θα σχηματιστεί ένας πίνακας στην τελευταία γραμμή του οποίου γράφουμε το πλήθος των κουκίδων που εμφανίζονται σε κάθε στήλη και στην τελευταία στήλη του οποίου γράφουμε το πλήθος των κουκίδων που εμφανίζονται σε κάθε γραμμή.
Παρατηρούμε ότι, προφανώς, το πλήθος όλων των κουκίδων είναι

$$\alpha_1 + \cdots + \alpha_m + \cdots + \alpha_n.$$

Αυτό προκύπτει μετά από μέτρημα των κουκίδων της κάθε στήλης. Όμως, το ίδιο αποτέλεσμα πρέπει να προκύψει αν μετρήσουμε τις κουκίδες που εμφανίζονται σε κάθε γραμμή.
Σκεφτόμαστε ότι το να εμφανίζεται μια κουκίδα στην πρώτη γραμμή σημαίνει ότι ο αντίστοιχος αριθμός από πάνω της διαιρείται από τον $p$. Ομοίως, το να εμφανίζεται μια κουκίδα στην δεύτερη γραμμή σημαίνει ότι ο αντίστοιχος αριθμός από πάνω της διαιρείται από τον $p^2$, το να εμφανίζεται μια κουκίδα στην τρίτη γραμμή σημαίνει ότι ο αντίστοιχος αριθμός από πάνω της διαιρείται από τον $p^3$ και ούτω καθ' εξής. Άρα το πλήθος των κουκίδων στην πρώτη γραμμή είναι ίσο με το πλήθος των πολλαπλασίων του $p$ που είναι $\leq n$, το πλήθος των κουκίδων στην δεύτερη γραμμή είναι ίσο με το πλήθος των πολλαπλασίων του $p^2$ που είναι $\leq n$, το πλήθος των κουκίδων στην τρίτη γραμμή είναι ίσο με το πλήθος των πολλαπλασίων του $p^3$ που είναι $\leq n$ και ούτω καθ' εξής. Άρα, σύμφωνα με το (i), το πλήθος των κουκίδων στην πρώτη γραμμή είναι ίσο με $[\frac{n}{p}]$, το πλήθος των κουκίδων στην δεύτερη γραμμή είναι ίσο με $[\frac{n}{p^2}]$, το πλήθος των κουκίδων στην τρίτη γραμμή είναι ίσο με $[\frac{n}{p^3}]$ και ούτω καθ' εξής.
Άρα το συνολικό πλήθος των κουκίδων είναι ίσο με

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

και, επομένως,

$$k = \alpha_1 + \cdots + \alpha_m + \cdots + \alpha_n = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots .$$

| | | | | | |
|---|---|---|---|---|---|
| $1$ | $\ldots$ | $m$ | $\ldots$ | $n$ | |
| $\bullet$ | $\ldots$ | $\bullet$ | $\ldots$ | $\bullet$ | $[\frac{n}{p}]$ |
| $\bullet$ | $\ldots$ | $\bullet$ | $\ldots$ | $\bullet$ | $[\frac{n}{p^2}]$ |
| $\vdots$ | $\ldots$ | $\vdots$ | $\ldots$ | $\vdots$ | $\vdots$ |
| $\bullet$ | $\ldots$ | $\bullet$ | $\ldots$ | $\bullet$ | $[\frac{n}{p^{\alpha_1}}]$ |
| $-$ | $\ldots$ | $\vdots$ | $\ldots$ | $\vdots$ | $\vdots$ |
| $-$ | $\ldots$ | $\bullet$ | $\ldots$ | $\bullet$ | $[\frac{n}{p^{\alpha_n}}]$ |
| $-$ | $\ldots$ | $\vdots$ | $\ldots$ | $-$ | $\vdots$ |
| $-$ | $\ldots$ | $\bullet$ | $\ldots$ | $-$ | $[\frac{n}{p^{\alpha_m}}]$ |
| $-$ | $\ldots$ | $-$ | $\ldots$ | $-$ | $\vdots$ |
| $\alpha_1$ | $\ldots$ | $\alpha_m$ | $\ldots$ | $\alpha_n$ | $k$ |

Και τώρα θα ξαναγυρίσουμε σε μια προηγούμενη άσκηση, την 2.5 και θα δούμε πώς θα βρούμε την κανονική αναπαράσταση του αριθμού $100!$, αφήνοντας την περίπτωση του $832!$

για περαιτέρω εξάσκηση.
Η κανονική αναπαράσταση του $100!$ περιέχει δυνάμεις των πρώτων διαιρετών του $100!$. Αλλά οι πρώτοι διαιρέτες του $100!$ είναι οι πρώτοι διαιρέτες των αριθμών $1, 2, \ldots, 100$ και, επομένως, είναι οι πρώτοι που είναι $\leq 100$. Άρα πρέπει να βρούμε όλους τους πρώτους που είναι $\leq 100$ και για καθέναν από αυτούς να βρούμε την μέγιστη δύναμή του που διαιρεί το $100!$. Αυτό το τελευταίο γίνεται με τη βοήθεια της άσκησης 2.25(ii).
Πώς θα βρούμε όλους τους πρώτους που είναι $\leq 100$; Σ' αυτό θα μας βοηθήσει η μέθοδος που ονομάζεται **κόσκινο του Ερατοσθένη** και έχει ως εξής. Γράφουμε όλους τους αριθμούς από το 2 έως το 100 (ο 1 δεν είναι πρώτος).
Με το πρώτο κοσκίνισμα κρατάμε τον πρώτο 2 και διαγράφουμε όλα τα υπόλοιπα πολλαπλάσια του 2:

$$\boxed{2}, 3, \not{4}, 5, \not{6}, 7, \not{8}, 9, \not{10}, 11, \not{12}, 13, \not{14}, 15, \not{16}, 17, \not{18}, 19, \not{20},$$

$$21, \not{22}, 23, \not{24}, 25, \not{26}, 27, \not{28}, 29, \not{30}, 31, \not{32}, 33, \not{34}, 35, \not{36}, 37, \not{38}, 39, \not{40},$$

$$41, \not{42}, 43, \not{44}, 45, \not{46}, 47, \not{48}, 49, \not{50}, 51, \not{52}, 53, \not{54}, 55, \not{56}, 57, \not{58}, 59, \not{60},$$

$$61, \not{62}, 63, \not{64}, 65, \not{66}, 67, \not{68}, 69, \not{70}, 71, \not{72}, 73, \not{74}, 75, \not{76}, 77, \not{78}, 79, \not{80},$$

$$81, \not{82}, 83, \not{84}, 85, \not{86}, 87, \not{88}, 89, \not{90}, 91, \not{92}, 93, \not{94}, 95, \not{96}, 97, \not{98}, 99, \not{100}.$$

Τώρα βλέπουμε ότι αμέσως μετά από τον 2 ο αριθμός που δεν έχει διαγραφεί είναι ο 3 και αυτός πρέπει να είναι πρώτος. Πράγματι, αν ήταν σύνθετος θα διαιρείτο από κάποιον μικρότερό του πρώτο. Αλλά οι μικρότεροί του αριθμοί είναι ο πρώτος 2 και τα πολλαπλάσια του 2, οπότε ο μόνος πρώτος που είναι μικρότερός του είναι ο 2 και ο 2 δεν τον διαιρεί (διότι ο 3 δεν έχει διαγραφεί).
Με το δεύτερο κοσκίνισμα κρατάμε τον πρώτο 3 και διαγράφουμε όλα τα υπόλοιπα πολλαπλάσια του 3:

$$\boxed{2}, \boxed{3}, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20},$$

$$\not{21}, \not{22}, 23, \not{24}, 25, \not{26}, \not{27}, \not{28}, 29, \not{30}, 31, \not{32}, \not{33}, \not{34}, 35, \not{36}, 37, \not{38}, \not{39}, \not{40},$$

$$41, \not{42}, 43, \not{44}, \not{45}, \not{46}, 47, \not{48}, 49, \not{50}, \not{51}, \not{52}, 53, \not{54}, 55, \not{56}, \not{57}, \not{58}, 59, \not{60},$$

$$61, \not{62}, \not{63}, \not{64}, 65, \not{66}, 67, \not{68}, \not{69}, \not{70}, 71, \not{72}, 73, \not{74}, \not{75}, \not{76}, 77, \not{78}, 79, \not{80},$$

$$\not{81}, \not{82}, 83, \not{84}, 85, \not{86}, \not{87}, \not{88}, 89, \not{90}, 91, \not{92}, \not{93}, \not{94}, 95, \not{96}, 97, \not{98}, \not{99}, \not{100}.$$

Αμέσως μετά από τους $2, 3$ ο αριθμός που δεν έχει διαγραφεί είναι ο 5 και αυτός πρέπει να είναι πρώτος. Πράγματι, αν ήταν σύνθετος θα διαιρείτο από κάποιον μικρότερό του πρώτο. Αλλά οι μικρότεροί του αριθμοί είναι ο πρώτοι $2, 3$ και τα πολλαπλάσιά τους, οπότε οι μόνοι πρώτοι που είναι μικρότεροί του είναι οι $2, 3$ και οι $2, 3$ δεν τον διαιρούν (διότι ο 5 δεν έχει διαγραφεί).
Με το δεύτερο κοσκίνισμα κρατάμε τον πρώτο 5 και διαγράφουμε όλα τα υπόλοιπα πολλαπλάσια του 5:

$$\boxed{2}, \boxed{3}, \not{4}, \boxed{5}, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20},$$

$$\not{21}, \not{22}, 23, \not{24}, \not{25}, \not{26}, \not{27}, \not{28}, 29, \not{30}, 31, \not{32}, \not{33}, \not{34}, \not{35}, \not{36}, 37, \not{38}, \not{39}, \not{40},$$

$$41, \not{42}, 43, \not{44}, \not{45}, \not{46}, 47, \not{48}, 49, \not{50}, \not{51}, \not{52}, 53, \not{54}, \not{55}, \not{56}, \not{57}, \not{58}, 59, \not{60},$$

$$61, \not{62}, \not{63}, \not{64}, \not{65}, \not{66}, 67, \not{68}, \not{69}, \not{70}, 71, \not{72}, 73, \not{74}, \not{75}, \not{76}, 77, \not{78}, 79, \not{80},$$

$$\not{81}, \not{82}, 83, \not{84}, \not{85}, \not{86}, \not{87}, \not{88}, 89, \not{90}, 91, \not{92}, \not{93}, \not{94}, \not{95}, \not{96}, 97, \not{98}, \not{99}, \not{100}.$$

Αμέσως μετά από τους $2, 3, 5$ ο αριθμός που δεν έχει διαγραφεί είναι ο 7 και αυτός πρέπει να είναι πρώτος. Πράγματι, αν ήταν σύνθετος θα διαιρείτο από κάποιον μικρότερό του πρώτο.

Αλλά οι μικρότεροί του αριθμοί είναι ο πρώτοι $2, 3, 5$ και τα πολλαπλάσιά τους, οπότε οι μόνοι πρώτοι που είναι μικρότεροί του είναι οι $2, 3, 5$ και οι $2, 3, 5$ δεν τον διαιρούν (διότι ο $7$ δεν έχει διαγραφεί).
Με το δεύτερο κοσκίνισμα κρατάμε τον πρώτο $7$ και διαγράφουμε όλα τα υπόλοιπα πολλαπλάσια του $7$:

$$\boxed{2}, \boxed{3}, \not{4}, \boxed{5}, \not{6}, \boxed{7}, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20},$$

$$\not{21}, \not{22}, 23, \not{24}, \not{25}, \not{26}, \not{27}, \not{28}, 29, \not{30}, 31, \not{32}, \not{33}, \not{34}, \not{35}, \not{36}, 37, \not{38}, \not{39}, \not{40},$$

$$41, \not{42}, 43, \not{44}, \not{45}, \not{46}, 47, \not{48}, \not{49}, \not{50}, \not{51}, \not{52}, 53, \not{54}, \not{55}, \not{56}, \not{57}, \not{58}, 59, \not{60},$$

$$61, \not{62}, \not{63}, \not{64}, \not{65}, \not{66}, 67, \not{68}, \not{69}, \not{70}, 71, \not{72}, 73, \not{74}, \not{75}, \not{76}, \not{77}, \not{78}, 79, \not{80},$$

$$\not{81}, \not{82}, 83, \not{84}, \not{85}, \not{86}, \not{87}, \not{88}, 89, \not{90}, \not{91}, \not{92}, \not{93}, \not{94}, \not{95}, \not{96}, 97, \not{98}, \not{99}, \not{100}.$$

Αυτά τα κοσκινίσματα μπορούν να συνεχισθούν.
Είναι σαφές ότι μετά από τα πρώτα $m$ κοσκινίσματα των πολλαπλασίων των $m$ αρχικών πρώτων $p_1, \ldots, p_m$ ο μικρότερος (μετά από τους $p_1, \ldots, p_m$) από τους αριθμούς που απομένουν είναι ο επόμενος πρώτος $p_{m+1}$.
Στην συγκεκριμένη περίπτωση που εξετάζουμε βρήκαμε τους $4$ αρχικούς πρώτους $2, 3, 5, 7$. Αμέσως μετά από αυτούς ο αριθμός που δεν έχει διαγραφεί είναι ο $11$ και αυτός είναι πρώτος. Αλλά δεν χρειάζεται να συνεχίσουμε τα κοσκινίσματα! Με μια απλή σκέψη θα καταλάβουμε ότι *όλοι οι αριθμοί που έχουν απομείνει είναι πρώτοι*! Πράγματι, αν κάποιος από τους αριθμούς που έχουν απομείνει, έστω ο $k$, είναι σύνθετος, τότε θα έχει έναν πρώτο παράγοντα $\leq \sqrt{k} \leq \sqrt{100} = 10$. Αλλά οι πρώτοι που είναι $\leq 10$ είναι οι $2, 3, 5, 7$ και όλα τα πολλαπλάσιά τους έχουν ήδη διαγραφεί. Άρα οι πρώτοι που είναι $\leq 100$ είναι οι αριθμοί που έχουν απομείνει:

$$\boxed{2}, \boxed{3}, \not{4}, \boxed{5}, \not{6}, \boxed{7}, \not{8}, \not{9}, \not{10}, \boxed{11}, \not{12}, \boxed{13}, \not{14}, \not{15}, \not{16}, \boxed{17}, \not{18}, \boxed{19}, \not{20},$$

$$\not{21}, \not{22}, \boxed{23}, \not{24}, \not{25}, \not{26}, \not{27}, \not{28}, \boxed{29}, \not{30}, \boxed{31}, \not{32}, \not{33}, \not{34}, \not{35}, \not{36}, \boxed{37}, \not{38}, \not{39}, \not{40},$$

$$\boxed{41}, \not{42}, \boxed{43}, \not{44}, \not{45}, \not{46}, \boxed{47}, \not{48}, \not{49}, \not{50}, \not{51}, \not{52}, \boxed{53}, \not{54}, \not{55}, \not{56}, \not{57}, \not{58}, \boxed{59}, \not{60},$$

$$\boxed{61}, \not{62}, \not{63}, \not{64}, \not{65}, \not{66}, \boxed{67}, \not{68}, \not{69}, \not{70}, \boxed{71}, \not{72}, \boxed{73}, \not{74}, \not{75}, \not{76}, \not{77}, \not{78}, \boxed{79}, \not{80},$$

$$\not{81}, \not{82}, \boxed{83}, \not{84}, \not{85}, \not{86}, \not{87}, \not{88}, \boxed{89}, \not{90}, \not{91}, \not{92}, \not{93}, \not{94}, \not{95}, \not{96}, \boxed{97}, \not{98}, \not{99}, \not{100}.$$

Με το κόσκινο του Ερατοσθένη μπορούμε να βρούμε όλους τους πρώτους μέχρι έναν δεδομένο αριθμό.
Τώρα, για κάθε πρώτο $p$ που είναι $\leq 100$ βρίσκουμε την μέγιστη δύναμη $p^k$ η οποία διαιρεί

τον $100!$. Οι αντίστοιχοι εκθέτες $k$ είναι οι εξής:

$$\left[\frac{100}{2}\right]+\left[\frac{100}{2^2}\right]+\left[\frac{100}{2^3}\right]+\left[\frac{100}{2^4}\right]+\left[\frac{100}{2^5}\right]+\left[\frac{100}{2^6}\right]=97.$$
$$\left[\frac{100}{3}\right]+\left[\frac{100}{3^2}\right]+\left[\frac{100}{3^3}\right]+\left[\frac{100}{3^4}\right]=48.$$
$$\left[\frac{100}{5}\right]+\left[\frac{100}{5^2}\right]=24.$$
$$\left[\frac{100}{7}\right]+\left[\frac{100}{7^2}\right]=16.$$
$$\left[\frac{100}{11}\right]=9.$$
$$\left[\frac{100}{13}\right]=7.$$
$$\left[\frac{100}{17}\right]=5.$$
$$\left[\frac{100}{19}\right]=5.$$
$$\left[\frac{100}{23}\right]=4.$$
$$\left[\frac{100}{29}\right]=3.$$
$$\left[\frac{100}{31}\right]=3.$$
$$\left[\frac{100}{37}\right]=2.$$
$$\left[\frac{100}{41}\right]=2.$$
$$\left[\frac{100}{43}\right]=2.$$
$$\left[\frac{100}{47}\right]=2.$$
$$\left[\frac{100}{53}\right]=1.$$

Είναι προφανές ότι για όλους τους υπόλοιπους πρώτους το αποτέλεσμα είναι ίσο με $1$. Άρα η κανονική αναπαράσταση του $100!$ είναι

$$2^{97}\cdot 3^{48}\cdot 5^{24}\cdot 7^{16}\cdot 11^9\cdot 13^7\cdot 17^5\cdot 19^5\cdot 23^4\cdot 29^3\cdot 31^3\cdot 37^2\cdot 41^2\cdot$$

$$\cdot 43^2\cdot 47^2\cdot 53\cdot 59\cdot 61\cdot 67\cdot 71\cdot 73\cdot 79\cdot 83\cdot 89\cdot 97.$$

# Κεφάλαιο 5

# Διοφαντικές εξισώσεις.

Μια εξίσωση χαρακτηρίζεται **Διοφαντική** αν ψάχνουμε να βρούμε τις ακέραιες λύσεις της.

## 5.1 Γραμμικές Διοφαντικές εξισώσεις ax+by=c.

**Θεώρημα 5.1.** *Έστω $a, b$ όχι και οι δύο ίσοι με $0$. Τότε ο $(a, b)$ είναι ο ελάχιστος θετικός γραμμικός συνδυασμός των $a, b$. Επίσης, το σύνολο των γραμμικών συνδυασμών των $a, b$ ταυτίζεται με το σύνολο των πολλαπλασίων του $(a, b)$.*

*Απόδειξη. Πρώτη:* Κατ' αρχάς θα αποδείξουμε ότι ο $(a, b)$ είναι γραμμικός συνδυασμός των $a, b$. Θεωρούμε τον Ευκλείδειο αλγόριθμο για την εύρεση του $(a, b)$ στην περίπτωση που είναι $a > 0$:

$$\begin{aligned}
b &= q_1 a + r_1, & 0 < r_1 < a \\
a &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2 \\
&\cdots\cdots\cdots & \cdots\cdots\cdots \\
r_{n-2} &= q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}$$

Το τελευταίο μη-μηδενικό υπόλοιπο $r_n$ ταυτίζεται με τον $(a, b)$.
Τώρα, έχουμε επαγωγικά ότι κάθε υπόλοιπο $r_1, r_2, \ldots, r_{n-1}, r_n$ είναι γραμμικός συνδυασμός των $a, b$:

$$\begin{aligned}
r_1 &= -q_1 a + b = x_1 a + y_1 b \\
r_2 &= a - q_2 r_1 = a - q_2(x_1 a + y_1 b) = (1 - q_2 x_1)a - q_2 y_1 b = x_2 a + y_2 b \\
r_3 &= r_1 - q_3 r_2 = x_1 a + y_1 b - q_3(x_2 a + y_2 b) = (x_1 - q_3 x_2)a + (y_1 - q_3 y_2)b = x_3 a + y_3 b \\
&\cdots\cdots\cdots \\
r_n &= r_{n-2} - q_n r_{n-1} = (x_{n-2} a + y_{n-2} b) - q_n(x_{n-1} a + y_{n-1} b) \\
&= (x_{n-2} - q_n x_{n-1})a + (y_{n-2} - q_n y_{n-1})b = x_n a + y_n b.
\end{aligned}$$

Άρα υπάρχουν $x, y$ ώστε

$$(a, b) = xa + yb.$$

Αν $a < 0$, τότε, εφαρμόζοντας το προηγούμενο στους $-a, b$, βρίσκουμε ότι υπάρχουν $x, y$ ώστε

$$(a, b) = (-a, b) = x(-a) + yb = (-x)a + yb,$$

οπότε πάλι ο $(a, b)$ είναι γραμμικός συνδυασμός των $a, b$.
Αν $a = 0$, τότε $b \neq 0$, οπότε $(a, b) = \pm b = 0a + (\pm 1)b$ και πάλι ο $(a, b)$ είναι γραμμικός

συνδυασμός των $(a, b)$.
Θέτουμε

$$d = (a, b)$$

και έχουμε αποδείξει ότι υπάρχουν $x_0, y_0$ ώστε

$$d = x_0 a + y_0 b.$$

Τώρα θα αποδείξουμε ότι το σύνολο των πολλαπλασίων του $d$ ταυτίζεται με το σύνολο των γραμμικών συνδυασμών των $a, b$. Δηλαδή,

$$\{nd \,|\, n \in \mathbb{Z}\} = \{xa + yb \,|\, x, y \in \mathbb{Z}\}. \tag{5.1}$$

Για κάθε $n$ έχουμε

$$nd = n(x_0 a + y_0 b) = (nx_0)a + (ny_0)b = xa + yb,$$

οπότε κάθε στοιχείο του πρώτου συνόλου είναι στοιχείο και του δεύτερου συνόλου.
Αντιστρόφως, για κάθε $x, y$ έχουμε

$$d \mid a,\ d \mid b \quad \Rightarrow \quad d \mid xa + yb,$$

οπότε το $xa+yb$ είναι πολλαπλάσιο του $d$. Άρα κάθε στοιχείο του δεύτερου συνόλου είναι στοιχείο και του πρώτου συνόλου.
Άρα τα δυο σύνολα είναι ίσα.
Απομένει να αποδείξουμε ότι ο $d = (a, b)$ είναι ο ελάχιστος θετικός γραμμικός συνδυασμός των $a, b$. Αυτό, όμως, προκύπτει από την ισότητα (5.1) αφού αυτή γράφεται

$$\{xa + yb \,|\, x, y \in \mathbb{Z}\} = \{0, \pm d, \pm 2d, \pm 3d, \ \dots\}.$$

*Δεύτερη:* Θεωρούμε το σύνολο

$$K = \{xa + yb \,|\, x, y \in \mathbb{Z}\}.$$

Οι αριθμοί $\pm a, \pm b$ είναι στοιχεία του $K$ και ένας τουλάχιστον από αυτούς είναι θετικός. Άρα το σύνολο $K \cap \mathbb{N}$ είναι μη-κενό και κάτω φραγμένο σύνολο ακεραίων και, επομένως, έχει ελάχιστο στοιχείο. Θέτουμε

$$d = \min(K \cap \mathbb{N}),$$

οπότε το $d$ είναι ο ελάχιστος θετικός γραμμικός συνδυασμός των $a, b$. Ειδικώτερα, υπάρχουν $x_0, y_0$ ώστε

$$d = x_0 a + y_0 b.$$

Θα αποδείξουμε ότι το σύνολο $K$ ταυτίζεται με το σύνολο των πολλαπλασίων του $d$. Δηλαδή,

$$\{nd \,|\, n \in \mathbb{Z}\} = \{xa + yb \,|\, x, y \in \mathbb{Z}\}. \tag{5.2}$$

Για κάθε $n$ έχουμε

$$nd = n(x_0 a + y_0 b) = (nx_0)a + (ny_0)b = xa + yb,$$

οπότε κάθε στοιχείο του πρώτου συνόλου είναι στοιχείο και του δεύτερου συνόλου.
Αντιστρόφως, για κάθε $x, y$ η ταυτότητα της Ευκλείδειας διαίρεσης του $xa+yb$ από το $d$ γράφεται

$$xa + yb = qd + r, \qquad 0 \le r < d,$$

οπότε

$$r = (xa + yb) - q(x_0 a + y_0 b) = (x - qx_0)a + (y - qy_0)b.$$

Έτσι, το $r$ είναι γραμμικός συνδυασμός των $a, b$ και, επομένως, είναι στοιχείο του $K$. Αν $0 < r < d$, τότε το $r$ είναι στοιχείο του $K \cap \mathbb{N}$ μικρότερο από το ελάχιστο στοιχείο $d$ του ίδιου συνόλου. Αυτό είναι αδύνατο, οπότε $r = 0$.
Άρα για κάθε $x, y$ το $xa+yb$ είναι πολλαπλάσιο του $d$, οπότε κάθε στοιχείο του δεύτερου συνόλου στην (5.2) είναι στοιχείο και του πρώτου συνόλου.
Άρα τα δυο σύνολα είναι ίσα.
Μένει να αποδείξουμε ότι

$$d = (a, b).$$

Τα $a, b$ είναι στοιχεία του $\{xa + yb \,|\, x, y \in \mathbb{Z}\}$, οπότε είναι και πολλαπλάσια του $d$. Δηλαδή,

$$d \mid a,\ d \mid b.$$

Από την άλλη μεριά,

$$d' \mid a,\ d' \mid b \quad \Rightarrow \quad d' \mid x_0 a + y_0 b = d.$$

Άρα κάθε κοινός διαιρέτης των $a, b$ είναι διαιρέτης και του κοινού τους θετικού διαιρέτη $d$. Αυτό σημαίνει ότι ο $d$ είναι ο μέγιστος κοινός διαιρέτης των $a, b$. □

Με βάση το Θεώρημα 5.1 θα αποδείξουμε το Θεώρημα 5.2 που περιγράφει πλήρως την κατάσταση σχετικά με την γραμμική Διοφαντική εξίσωση

$$ax + by = c, \tag{5.3}$$

όπου οι συντελεστές $a, b, c$ είναι, φυσικά, ακέραιοι.

Το πρόβλημα με την εξίσωση (5.3) είναι ότι, αν θέσουμε σ' αυτήν κάποια ακέραια τιμή του $x$ και λύσουμε ως προς $y$, θα βρούμε $y = \frac{-ax+c}{b}$ και αυτή η τιμή του $y$ μπορεί να μην είναι ακέραια.

**Θεώρημα 5.2.** *Έστω $a, b$ όχι και οι δύο ίσοι με $0$. Τότε η Διοφαντική εξίσωση (5.3) έχει λύση αν και μόνο αν $(a, b) \mid c$. Επίσης, αν $d = (a, b) \mid c$ και $a = da_1, b = db_1$ και αν $x_1, y_1$ είναι μία λύση της (5.3), τότε όλες οι λύσεις της (5.3) είναι οι*

$$x = x_1 + kb_1,\ y = y_1 - ka_1 \qquad (k \in \mathbb{Z}).$$

*Απόδειξη.* Αν η (5.3) έχει κάποια λύση $x_1, y_1$, τότε

$$d \mid a,\ d \mid b \quad \Rightarrow \quad d \mid ax_1 + by_1 = c.$$

Αντιστρόφως, έστω $d \mid c$, οπότε

$$c = kd$$

για κάποιο $k$.
Από το Θεώρημα 5.1 γνωρίζουμε ότι υπάρχουν $x_0, y_0$ ώστε

$$d = ax_0 + by_0.$$

Άρα

$$c = kd = a(kx_0) + b(ky_0),$$

οπότε η (5.3) έχει λύση $x = kx_0, y = ky_0$.
Τώρα, έστω $x_1, y_1$ μια λύση της (5.3). Δηλαδή,

$$ax_1 + by_1 = c.$$

Για κάθε $k$ έχουμε

$$a(x_1 + kb_1) + b(y_1 - ka_1) = ax_1 + by_1 + kab_1 - ka_1 b = c + k\frac{ab}{d} - k\frac{ab}{d} = c.$$

Άρα για κάθε $k$ η $x = x_1 + kb_1, y = y_1 - ka_1$ είναι λύση της (5.3).
Αντιστρόφως, έστω $x, y$ οποιαδήποτε λύση της (5.3). Δηλαδή,

$$ax + by = c = ax_1 + by_1,$$

οπότε

$$a(x - x_1) = b(y_1 - y),$$

οπότε

$$a_1(x - x_1) = b_1(y_1 - y). \tag{5.4}$$

Άρα

$$b_1 \mid a_1(x - x_1)$$

και, επειδή $(a_1, b_1) = 1$, συνεπάγεται

$$b_1 \mid x - x_1,$$

οπότε υπάρχει $k$ ώστε

$$x - x_1 = kb_1$$

ή, ισοδύναμα,

$$x = x_1 + kb_1.$$

Από την (5.4) έχουμε ότι

$$y = y_1 - ka_1$$

και συμπεραίνουμε ότι κάθε λύση $x, y$ γράφεται

$$x = x_1 + kb_1,\ y = y_1 - ka_1$$

για κάποιο $k$. □

**Παράδειγμα.** Η Διοφαντική εξίσωση

$$85x + 745y = 22$$

δεν έχει λύση.
Πράγματι, έχουμε

$$(85, 745) = 5$$

και $5 \nmid 22$.

**Παράδειγμα.** Η Διοφαντική εξίσωση

$$85x + 745y = 25 \tag{5.5}$$

έχει λύση, διότι $(85, 745) = 5$ και $5 \mid 25$.
Για να βρούμε τις λύσεις της (5.5) πρέπει πρώτα να βρούμε μία λύση της. Για να γίνει αυτό, θα γράψουμε τον $(85, 745) = 5$ ως γραμμικό συνδυασμό των $85, 745$ μέσω του Ευκλείδειου αλγόριθμου με τον τρόπο που περιγράφεται στην πρώτη απόδειξη του Θεωρήματος 5.1:

$$\begin{aligned} 745 &= 8 \cdot 85 + 65 \\ 85 &= 1 \cdot 65 + 20 \\ 65 &= 3 \cdot 20 + 5 \\ 20 &= 4 \cdot 5. \end{aligned}$$

Και τώρα,

$$\begin{aligned} 65 &= -8 \cdot 85 + 745 \\ 20 &= 85 - 1 \cdot 65 = 85 - 1 \cdot (-8 \cdot 85 + 745) = 9 \cdot 85 - 1 \cdot 745 \\ 5 &= 65 - 3 \cdot 20 = (-8 \cdot 85 + 745) - 3 \cdot (9 \cdot 85 - 1 \cdot 745) = -35 \cdot 85 + 4 \cdot 745. \end{aligned}$$

Άρα

$$25 = -175 \cdot 85 + 20 \cdot 745,$$

οπότε

$$x_1 = -175,\ y_1 = 20$$

είναι μια λύση της (5.5).
Τώρα γράφουμε

$$a_1 = \frac{85}{5} = 17,\ b_1 = \frac{745}{5} = 149$$

και η γενική λύση της (5.5) γράφεται

$$x = -175 + 149k,\ y = 20 - 17k \qquad (k \in \mathbb{Z}).$$

## 5.2 Η Διοφαντική εξίσωση $x^2 + y^2 = z^2$.

Η Διοφαντική εξίσωση

$$x^2 + y^2 = z^2 \tag{5.6}$$

έχει τις προφανείς λύσεις

$$x = 0,\ y = \eta,\ z = \pm\eta \qquad (\eta \in \mathbb{Z})$$

και τις ανάλογες

$$x = \xi,\ y = 0,\ z = \pm\xi \qquad (\xi \in \mathbb{Z}).$$

Αυτές οι λύσεις ονομάζονται **τετριμμένες λύσεις** της (5.6).

Οι μη-τετριμμένες λύσεις της (5.6) ονομάζονται, για προφανή λόγο, **Πυθαγόρειες τριάδες**. Μια τέτοια Πυθαγόρεια τριάδα είναι η

$$x = 3,\ y = 4,\ z = 5.$$

Το Θεώρημα 5.3 περιγράφει όλες τις Πυθαγόρειες τριάδες. Για την απόδειξή του θα χρειαστούμε δύο λήμματα. Και τα δύο λήμματα έχουν λυθεί ως ασκήσεις και εδώ θα δούμε νέες αποδείξεις.

**Λήμμα 5.1.** *Αν $d^k \mid a^k$, τότε $d \mid a$.*

*Απόδειξη.* Μπορούμε να υποθέσουμε ότι $d \geq 1$ και $a \geq 0$. Αν $a = 0$, το αποτέλεσμα είναι προφανές. Άρα υποθέτουμε ότι $d, a \geq 1$. Αν $d = 1$, το αποτέλεσμα είναι και πάλι προφανές. Οπότε υποθέτουμε ότι $d > 1$ και, επομένως, $a > 1$ και θεωρούμε τις κανονικές αναπαραστάσεις των $d, a$.
Αν η κανονική αναπαράσταση του $d$ είναι

$$d = p_1^{\alpha_1} \cdots p_n^{\alpha_n},$$

τότε για κάθε $p_m$ έχουμε

$$p_m \mid d \quad \Rightarrow \quad p_m \mid d^k \quad \Rightarrow \quad p_m \mid a^k \quad \Rightarrow \quad p_m \mid a.$$

Άρα κάθε $p_m$ εμφανίζεται στην κανονική αναπαράσταση του $a$, οπότε η κανονική αναπαράσταση του $a$ είναι της μορφής

$$a = p_1^{\beta_1} \cdots p_n^{\beta_n} \cdots,$$

όπου οι επιπλέον τελείες δηλώνουν την πιθανή ύπαρξη επιπλέον πρώτων παραγόντων.
Από την $d^k \mid a^k$ συνεπάγεται

$$a^k = qd^k$$

για κάποιο $q$, οπότε

$$p_1^{k\beta_1} \cdots p_n^{k\beta_n} \cdots = q p_1^{k\alpha_1} \cdots p_n^{k\alpha_n}.$$

Συνεπάγεται

$$k\alpha_m \leq k\beta_m$$

και άρα

$$\alpha_m \leq \beta_m$$

για κάθε $m$.
Άρα $d \mid a$. □

**Λήμμα 5.2.** *Έστω $k \geq 2$, $a, b, c \geq 1$, $ab = c^k$, $(a, b) = 1$. Τότε υπάρχουν $m, n \geq 1$ ώστε $a = m^k$, $b = n^k$.*

*Απόδειξη.* Θεωρούμε τα

$$d = (a, c), \quad a_1 = \frac{a}{d}, \quad c_1 = \frac{c}{d},$$

οπότε

$$(a_1, c_1) = 1.$$

Η σχέση $ab = c^k$ γίνεται

$$a_1 b = d^{k-1} c_1^k.$$

Από την Πρόταση 3.5 έχουμε

$$(a_1, c_1) = 1 \quad \Rightarrow \quad (a_1, c_1^2) = 1 \quad \Rightarrow \quad \cdots\cdots \quad \Rightarrow \quad (a_1, c_1^k) = 1.$$

Και τώρα, επειδή $c_1^k \mid a_1 b$, συνεπάγεται

$$c_1^k \mid b,$$

οπότε

$$b = q c_1^k$$

για κάποιο $q$.
Άρα

$$a_1 q = d^{k-1}.$$

Τώρα,

$$d \mid a, \ q \mid b$$

και, επειδή $(a, b) = 1$, συνεπάγεται

$$(d, q) = 1.$$

Άρα, πάλι από την Πρόταση 3.5 έχουμε

$$(d, q) = 1 \quad \Rightarrow \quad (d^2, q) = 1 \quad \Rightarrow \quad \cdots\cdots \quad \Rightarrow \quad (d^{k-1}, q) = 1.$$

Και, επειδή $q \mid d^{k-1}$, συνεπάγεται

$$q = 1.$$

Άρα

$$b = c_1^k$$

και $a_1 = d^{k-1}$, οπότε και

$$a = d^k.$$

□

**Θεώρημα 5.3.** *Οι μη-τετριμμένες λύσεις της $x^2 + y^2 = z^2$ δίνονται από τους τύπους*

$$x = \pm d(u^2 - v^2), \quad y = \pm d2uv, \quad z = \pm d(u^2 + v^2) \tag{5.7}$$

*ή*

$$x = \pm d2uv, \quad y = \pm d(u^2 - v^2), \quad z = \pm d(u^2 + v^2), \tag{5.8}$$

*όπου*
*(i) τα πρόσημα είναι αυθαίρετα,*
*(ii)* $d \geq 1$*,*
*(iii)* $u > v \geq 1$*,* $(u, v) = 1$ *και*
*(iv) ο ένας από τους* $u, v$ *είναι άρτιος και ο άλλος περιττός.*

*Απόδειξη.* Είναι πολύ εύκολο να δούμε ότι οι αριθμοί που δίνονται με τους τύπους (5.7) αποτελούν λύσεις της $x^2 + y^2 = z^2$. Πράγματι,

$$(\pm d(u^2 - v^2))^2 + (\pm d2uv)^2 = d^2(u^4 + v^4 - 2u^2v^2 + 4u^2v^2) = d^2(u^2 + v^2)^2 = (\pm d(u^2 + v^2))^2.$$

Το ίδιο ισχύει και με τους τύπους (5.8).
Τώρα, αντιστρόφως, έστω $x = \xi$, $y = \eta$, $z = \zeta$ μια τυχούσα μη-τετριμμένη λύση της $x^2 + y^2 = z^2$. Δηλαδή

$$\xi^2 + \eta^2 = \zeta^2, \quad \xi \neq 0,\ \eta \neq 0,\ \zeta \neq 0.$$

Λόγω των τετραγώνων της εξίσωσης, τα πρόσημα των $\xi, \eta, \zeta$ δεν παίζουν κανένα ρόλο, οπότε μπορούμε να υποθέσουμε ότι

$$\xi, \eta, \zeta > 0.$$

Αν ο $d$ είναι κοινός διαιρέτης των $\xi, \eta$, από το Λήμμα 5.1 συνεπάγεται

$$d \mid \xi,\ d \mid \eta \quad \Rightarrow \quad d^2 \mid \xi^2,\ d^2 \mid \eta^2 \quad \Rightarrow \quad d^2 \mid \xi^2 + \eta^2 = \zeta^2 \quad \Rightarrow \quad d \mid \zeta,$$

οπότε ο $d$ είναι διαιρέτης και του $\zeta$.
Με τον ίδιο τρόπο βλέπουμε ότι, αν ο $d$ είναι κοινός διαιρέτης των $\xi, \zeta$, τότε ο $d$ είναι διαιρέτης και του $\eta$ και ότι, αν ο $d$ είναι κοινός διαιρέτης των $\eta, \zeta$, τότε ο $d$ είναι διαιρέτης και του $\xi$.
Άρα το ζευγάρι $\xi, \eta$, το ζευγάρι $\xi, \zeta$ και το ζευγάρι $\eta, \zeta$ έχουν τους ίδιους κοινούς διαιρέτες και, επομένως, τα τρία ζευγάρια έχουν τον ίδιο μέγιστο κοινό διαιρέτη. Άρα μπορούμε να θέσουμε

$$d = (\xi, \eta) = (\xi, \zeta) = (\eta, \zeta).$$

Επίσης, θέτουμε

$$\xi_1 = \frac{\xi}{d}, \quad \eta_1 = \frac{\eta}{d}, \quad \zeta_1 = \frac{\zeta}{d},$$

οπότε

$$\xi_1^2 + \eta_1^2 = \zeta_1^2, \quad \xi_1, \eta_1, \zeta_1 > 0, \quad (\xi_1, \eta_1) = (\xi_1, \zeta_1) = (\eta_1, \zeta_1) = 1.$$

Επειδή οι $\xi_1, \eta_1, \zeta_1$ είναι ανά δύο σχετικά πρώτοι, συνεπάγεται ότι το πολύ ένας από τους τρεις αριθμούς είναι άρτιος. Τώρα, αν οι $\xi_1, \eta_1$ είναι και οι δύο περιττοί, έχουμε ότι

$$\zeta_1^2 = \xi_1^2 + \eta_1^2 = (2n + 1)^2 + (2m + 1)^2 = 4(n^2 + n + m^2 + m) + 2 = 4k + 2.$$

Αυτό, όμως, είναι αδύνατο, διότι, είτε ο $\zeta_1$ είναι άρτιος είτε ο $\zeta_1$ είναι περιττός, ο $\zeta_1^2$ δεν είναι της μορφής $4k + 2$.
Άρα ο ένας από τους $\xi_1, \eta_1$ είναι άρτιος και ο άλλος είναι περιττός και, επομένως, ο $\zeta_1$ είναι περιττός.
Θα υποθέσουμε ότι ο $\eta_1$ είναι άρτιος και θα οδηγηθούμε στις τύπους (5.7). Λόγω προφανούς

συμμετρίας, αν υποθέσουμε ότι ο $\xi_1$ είναι άρτιος, θα οδηγηθούμε στους τύπους (5.8).
Τώρα, έχουμε

$$\eta_1^2 = \zeta_1^2 - \xi_1^2,$$

οπότε

$$\Big(\frac{\eta_1}{2}\Big)^2 = \frac{\zeta_1+\xi_1}{2}\,\frac{\zeta_1-\xi_1}{2}. \tag{5.9}$$

Οι αριθμοί $\frac{\eta_1}{2}$, $\frac{\zeta_1+\xi_1}{2}$, $\frac{\zeta_1-\xi_1}{2}$ είναι ακέραιοι και

$$\begin{aligned} a \mid \frac{\zeta_1+\xi_1}{2},\ a \mid \frac{\zeta_1-\xi_1}{2} \quad &\Rightarrow \quad a \mid \frac{\zeta_1+\xi_1}{2} + \frac{\zeta_1-\xi_1}{2} = \zeta_1,\ a \mid \frac{\zeta_1+\xi_1}{2} - \frac{\zeta_1-\xi_1}{2} = \xi_1 \\ &\Rightarrow \quad a \mid (\zeta_1, \xi_1) = 1 \quad \Rightarrow \quad a = \pm 1. \end{aligned}$$

Άρα

$$\Big(\frac{\zeta_1+\xi_1}{2}, \frac{\zeta_1-\xi_1}{2}\Big) = 1.$$

Άρα από την (5.9) και το Λήμμα 5.2 συνεπάγεται ότι υπάρχουν $u, v > 0$ ώστε

$$\frac{\zeta_1+\xi_1}{2} = u^2, \quad \frac{\zeta_1-\xi_1}{2} = v^2 \quad \text{και άρα} \quad \frac{\eta_1}{2} = uv.$$

Επομένως,

$$\xi_1 = u^2 - v^2, \quad \eta_1 = 2uv, \quad \zeta_1 = u^2 + v^2. \tag{5.10}$$

Τώρα,

$$\begin{aligned} a \mid u,\ a \mid v \quad &\Rightarrow \quad a \mid u^2,\ a \mid v^2 \quad \Rightarrow \quad a \mid (u^2, v^2) = \Big(\frac{\zeta_1+\xi_1}{2}, \frac{\zeta_1-\xi_1}{2}\Big) = 1 \\ &\Rightarrow \quad a = \pm 1, \end{aligned}$$

οπότε

$$(u, v) = 1.$$

Τέλος, επειδή οι $\xi_1, \zeta_1$ είναι περιττοί, από τις (5.10) συνεπάγεται ότι ο ένας από τους $u, v$ είναι άρτιος και ο άλλος περιττός.
Έτσι καταλήγουμε στους τύπους (5.7) με τους αναφερόμενους στην διατύπωση του θεωρήματος περιορισμούς (i)-(iv). □

**Παραδείγματα.** Επιλέγοντας $d = 1$ και $u = 2, v = 1$, προκύπτει $x = 3, y = 4, z = 5$.
Επιλέγοντας $d = 1$ και $u = 3, v = 2$, προκύπτει $x = 5, y = 12, z = 13$.
Επιλέγοντας $d = 1$ και $u = 4, v = 3$, προκύπτει $x = 7, y = 24, z = 25$.

## 5.3 Η Διοφαντική εξίσωση $\mathbf{x^n + y^n = z^n}$.

Κατ' αρχάς θα ασχοληθούμε με την Διοφαντική εξίσωση

$$x^4 + y^4 = z^2.$$

Η εξίσωση αυτή έχει τετριμμένες λύσεις, δηλαδή λύσεις όπου ένα τουλάχιστον από τα $x, y$ είναι ίσο με $0$, τις

$$x = \pm\xi,\ y = 0,\ z = \pm\xi^2 \qquad \text{και} \qquad x = 0,\ y = \pm\eta,\ z = \pm\eta^2.$$

**Πρόταση 5.1.** *Η Διοφαντική εξίσωση $x^4 + y^4 = z^2$ δεν έχει μη-τετριμμένη λύση.*

*Απόδειξη.* Έστω ότι η Διοφαντική εξίσωση $x^4 + y^4 = z^2$ έχει κάποια μη-τετριμμένη λύση $x = \xi, y = \eta, z = \zeta$, όπου $\xi, \eta \neq 0$ και, επομένως, $\zeta \neq 0$. Τότε μπορούμε, προφανώς, να υποθέσουμε ότι $\zeta > 0$.
Το σχέδιο της απόδειξης είναι να αποδείξουμε ότι τότε υπάρχει μία ακόμη μη-τετριμμένη λύση $x = \xi_1, y = \eta_1, z = \zeta_1$ με $0 < \zeta_1 < \zeta$ και κατόπιν με ένα απλό λογικό επιχείρημα να οδηγηθούμε σε άτοπο.
Εκτός από $\zeta > 0$, μπορούμε να υποθέσουμε ότι $\xi > 0, \eta > 0$.
Το Θεώρημα 5.3 λέει ότι υπάρχουν $d, u, v$ ώστε

$$\xi^2 = d(u^2 - v^2), \quad \eta^2 = d2uv, \quad \zeta = d(u^2 + v^2)$$

ή

$$\xi^2 = d2uv, \quad \eta^2 = d(u^2 - v^2), \quad \zeta = d(u^2 + v^2),$$

όπου
(ii) $d \geq 1$,
(iii) $u > v \geq 1$, $(u, v) = 1$ και
(iv) ο ένας από τους $u, v$ είναι άρτιος και ο άλλος περιττός.
Από την απόδειξη του Θεωρήματος 5.3 έχουμε ότι $d = (\xi^2, \eta^2)$. Τώρα, αν θέσουμε $f = (\xi, \eta)$, έχουμε ότι $\xi = f\xi_1$, $\eta = f\eta_1$ με $(\xi_1, \eta_1) = 1$, οπότε

$$d = (\xi^2, \eta^2) = (f^2\xi_1^2, f^2\eta_1^2) = f^2(\xi_1^2, \eta_1^2) = f^2.$$

Στην περίπτωση που είναι $d > 1$, θεωρούμε τους

$$\xi_1 = \frac{\xi}{f}, \quad \eta_1 = \frac{\eta}{f}, \quad \zeta_1 = \frac{\zeta}{d},$$

για τους οποίους ισχύει

$$\xi_1^2 = u^2 - v^2, \quad \eta_1^2 = 2uv, \quad \zeta_1 = u^2 + v^2$$

ή

$$\xi_1^2 = 2uv, \quad \eta_1^2 = u^2 - v^2, \quad \zeta_1 = u^2 + v^2,$$

και τότε έχουμε βρει μη-τετριμμένη λύση $x = \xi_1, y = \eta_1, z = \zeta_1$ με $0 < \zeta_1 < \zeta$ και έχουμε τελειώσει με το πρώτο μέρος του σχεδίου μας.
Άρα μένει να εξετάσουμε την περίπτωση που είναι $d = 1$. Δηλαδή υποθέτουμε ότι

$$\xi^2 = u^2 - v^2, \quad \eta^2 = 2uv, \quad \zeta = u^2 + v^2 \tag{5.11}$$

ή

$$\xi^2 = 2uv, \quad \eta^2 = u^2 - v^2, \quad \zeta = u^2 + v^2, \tag{5.12}$$

όπου
(iii) $u > v \geq 1$, $(u, v) = 1$ και
(iv) ο ένας από τους $u, v$ είναι άρτιος και ο άλλος περιττός.
Οι περιπτώσεις (5.11) και (5.12) είναι συμμετρικές, οπότε αρκεί να εξετάσουμε την (5.11).
Η πρώτη από τις σχέσεις (5.11) γράφεται

$$\xi^2 + v^2 = u^2.$$

Στην απόδειξη του Θεωρήματος 5.3 είχαμε δει ότι $(\xi, v) = (\xi, u) = (v, u)$, οπότε, επειδή $(v, u) = 1$, συνεπάγεται ότι

$$(\xi, v) = (\xi, u) = (v, u) = 1.$$

Επίσης, στην απόδειξη του Θεωρήματος 5.3 είχαμε δει ότι ένας από τους $\xi, v$ είναι άρτιος και ο άλλος είναι περιττός, καθώς και ότι ο $u$ είναι περιττός. Επειδή, όμως, ο ένας από τους $u, v$ είναι

άρτιος και ο άλλος περιττός, συμπεραίνουμε ότι ο $v$ είναι άρτιος και οι $\xi, u$ είναι περιττοί.
Μετά από αυτά, το Θεώρημα 5.3 λέει ότι υπάρχουν $k, l$ ώστε

$$\xi = k^2 - l^2, \quad v = 2kl, \quad u = k^2 + l^2 \tag{5.13}$$

όπου
(iii') $k > l \geq 1$, $(k, l) = 1$ και
(iv') ο ένας από τους $k, l$ είναι άρτιος και ο άλλος περιττός.
Τώρα, η δεύτερη από τις σχέσεις (5.11) γράφεται

$$\left(\frac{\eta}{2}\right)^2 = u\,\frac{v}{2}.$$

Επειδή $(u, v) = 1$, συνεπάγεται $(u, \frac{v}{2}) = 1$, οπότε από το Λήμμα 5.2 συνεπάγεται ότι υπάρχουν $\zeta_1, n > 0$ ώστε

$$u = \zeta_1^2, \quad \frac{v}{2} = n^2.$$

Τώρα, η δεύτερη από τις σχέσεις (5.13) γράφεται

$$n^2 = kl$$

και, επειδή $(k, l) = 1$, πάλι από το Λήμμα 5.2 συνεπάγεται ότι υπάρχουν $\xi_1, \eta_1$ ώστε

$$k = \xi_1^2, \quad l = \eta_1^2.$$

Τέλος, η τρίτη από τις σχέσεις (5.13) γράφεται

$$\xi_1^4 + \eta_1^4 = \zeta_1^2$$

και

$$0 < \zeta_1 \leq \zeta_1^2 = u \leq u^2 < \zeta.$$

Άρα η $x = \xi_1, y = \eta_1, z = \zeta_1$ είναι μη-τετριμμένη λύση της $x^4 + y^4 = z^2$ με $0 < \zeta_1 < \zeta$ και συμπληρώσαμε το πρώτο μέρος του σχεδίου μας.
Έχουμε, λοιπόν, αποδείξει ότι, όταν έχουμε μια μη-τετριμμένη λύση $x = \xi, y = \eta, z = \zeta$ με $\zeta > 0$, τότε έχουμε και μια άλλη μη-τετριμμένη λύση $x = \xi_1, y = \eta_1, z = \zeta_1$ με

$$0 < \zeta_1 < \zeta.$$

Άρα έχουμε και μια μη-τετριμμένη λύση $x = \xi_2, y = \eta_2, z = \zeta_2$ με

$$0 < \zeta_2 < \zeta_1.$$

Άρα έχουμε και μια μη-τετριμμένη λύση $x = \xi_3, y = \eta_3, z = \zeta_3$ με

$$0 < \zeta_3 < \zeta_2.$$

Αυτό συνεχίζεται επ' άπειρον και βρίσκουμε μια απειρία μη-τετριμμένων λύσεων $x = \xi_n, y = \eta_n, z = \zeta_n$ με

$$0 < \ldots < \zeta_n < \ldots < \zeta_2 < \zeta_1 < \zeta.$$

Αυτό είναι αδύνατον διότι ανάμεσα στους $0$ και $\zeta$ υπάρχουν πεπερασμένου πλήθους (ακέραιοι) αριθμοί.
Έτσι καταλήγουμε σε άτοπο, οπότε δεν υπάρχει μη-τετριμμένη λύση $x = \xi, y = \eta, z = \zeta$ με $\zeta > 0$ και, επομένως, δεν υπάρχει μη-τετριμμένη λύση. □

Η μέθοδος που χρησιμοποιήθηκε στην απόδειξη της Πρότασης 5.1 ονομάζεται **μέθοδος της καθόδου** και περιγράφεται ως εξής. *Έστω ότι έχουμε κάποιο πρόβλημα και θέλουμε να δούμε αν επιδέχεται λύση η οποία έχει κάποια θετική ακέραια παράμετρο $n$. Έστω ότι αποδεικνύουμε το εξής: αν υπάρχει κάποια λύση του προβλήματος με θετική την τιμή της παραμέτρου $n = n_1$, τότε υπάρχει και μια άλλη λύση του προβλήματος με θετική την αντίστοιχη τιμή της παραμέτρου $n = n_2$ και ώστε $n_2 < n_1$. Τότε το συμπέρασμα είναι ότι το πρόβλημα δεν επιδέχεται λύση με θετική τιμή της παραμέτρου $n$.*

Άμεσο πόρισμα της Πρότασης 5.1 είναι η Πρόταση 5.2.

**Πρόταση 5.2.** *Η Διοφαντική εξίσωση $x^4 + y^4 = z^4$ δεν έχει μη-τετριμμένη λύση.*

*Απόδειξη.* Πράγματι, αν η $x^4 + y^4 = z^4$ έχει μη-τετριμμένη λύση την $x = \xi$, $y = \eta$, $z = \zeta$, τότε η $x^4 + y^4 = z^2$ έχει μη-τετριμμένη λύση την $x = \xi$, $y = \eta$, $z = \zeta^2$. □

Και τώρα ας δούμε μερικά ιστορικά στοιχεία σε σχέση με την Διοφαντική εξίσωση

$$x^n + y^n = z^n. \tag{5.14}$$

Το 1637 ο Fermat διάβαζε την λατινική μετάφραση του βιβλίου "Αριθμητικά" του Διόφαντου και όταν είδε το Θεώρημα 5.3 σημείωσε στο περιθώριο της σελίδας ότι "έχει μια καταπληκτική απόδειξη του ότι η Διοφαντική εξίσωση (5.14) δεν έχει μη-τετριμμένες λύσεις όταν $n \geq 3$ αλλά δεν φτάνει ο χώρος του περιθωρίου για να την γράψει". Έκτοτε ο Fermat δεν ανέφερε καμία απόδειξη του ισχυρισμού του και από τότε ξεκινά ένα διάσημο κυνήγι απόδειξης του ισχυρισμού:

**Εικασία του Fermat.** *Όταν $n \geq 3$, η Διοφαντική εξίσωση (5.14) δεν έχει μη-τετριμμένη λύση.*

Η Πρόταση 5.2 επιβεβαιώνει την εικασία όταν $n = 4$. Το 1770 ο Euler απέδειξε την εικασία όταν $n = 3$, το 1825 οι Dirichlet και Legendre απέδειξαν την εικασία όταν $n = 5$ και το 1839 ο Lamé απέδειξε την εικασία όταν $n = 7$.

Είναι εύκολο να δει κανείς ότι, αν θέλουμε να αποδείξουμε την εικασία για κάθε $n \geq 3$, αρκεί να την αποδείξουμε για κάθε *πρώτο* $p \geq 3$. Πράγματι, έστω ότι η εικασία είναι σωστή για κάθε πρώτο $p \geq 3$ και έστω $n \geq 3$. Αν ο $n$ έχει κάποιον πρώτο παράγοντα $p \geq 3$, τότε έχουμε $n = pm$ για κάποιον $m$ οπότε η εξίσωση (5.14) γράφεται

$$(x^m)^p + (y^m)^p = (z^m)^p$$

και δεν έχει μη-τετριμμένη λύση: διότι αν είχε την μη-τετριμμένη λύση $x = \xi, y = \eta, z = \zeta$, τότε η $x^p + y^p = z^p$ θα είχε την μη-τετριμμένη λύση $x = \xi^m, y = \eta^m, z = \zeta^m$. Αν ο $n \geq 3$ δεν έχει πρώτο παράγοντα $\geq 3$, τότε έχει παράγοντα το $4$, οπότε έχουμε $n = 4m$ για κάποιον $m$ οπότε η εξίσωση (5.14) γράφεται

$$(x^m)^4 + (y^m)^4 = (z^m)^4$$

και δεν έχει μη-τετριμμένη λύση: διότι αν είχε την μη-τετριμμένη λύση $x = \xi, y = \eta, z = \zeta$, τότε η $x^4 + y^4 = z^4$ θα είχε την μη-τετριμμένη λύση $x = \xi^m, y = \eta^m, z = \zeta^m$.

Κατόπιν, το 1843 ο Kummer πίστεψε ότι απέδειξε την εικασία για κάθε πρώτο $p \geq 3$ χρησιμοποιώντας τους λεγόμενους *αλγεβρικούς αριθμούς*, αλλά ο Dirichlet βρήκε λάθος στην απόδειξη του Kummer. Ο Kummer επέμεινε και στην προσπάθειά του να αποδείξει την εικασία του Fermat εισήγαγε την έννοια του *ιδεώδους αριθμού*. Με τη βοήθεια των ιδεωδών αριθμών κατάφερε να αποδείξει ότι η εικασία του Fermat είναι σωστή για κάθε *κανονικό πρώτο* $p$. Δεν θα ασχοληθούμε με τους ορισμούς των ιδεωδών αριθμών και των κανονικών πρώτων, αλλά θα πούμε ότι οι μόνοι πρώτοι που είναι $\leq 100$ και δεν είναι κανονικοί είναι οι $37, 59, 67$. Δηλαδή, ο Kummer κατάφερε να αποδείξει την εικασία για κάθε πρώτο $p \leq 100$ εκτός των $37, 59, 67$. Αυτό θεωρήθηκε σημαντικό για εκείνη την εποχή, αφού μέχρι τότε οι αποδείξεις αφορούσαν κάθε φορά έναν πρώτο και γίνονταν όλο και πιο δύσκολες. Κάτι άλλο, ακόμη πιο σημαντικό, είναι ότι από τις μεθόδους

του Kummer για την απόδειξη της εικασίας του Fermat μπήκαν οι βάσεις της λεγόμενης Αλγεβρικής Θεωρίας Αριθμών. Επίσης, πρέπει να αναφέρουμε ότι η έννοια του ιδεώδους αριθμού ήταν ο πρόδρομος της έννοιας του ιδεώδους που μαθαίνουμε στην Άλγεβρα.

Ένας ακόμη σταθμός στην ιστορία της εικασίας του Fermat ήταν όταν το 1983 ο νεαρός Faltings απέδειξε ότι, όταν $n \geq 3$, η Διοφαντική εξίσωση (5.14) έχει το πολύ πεπερασμένο πλήθος λύσεων.

Τέλος, αφού η εικασία του Fermat συνδέθηκε με την (φαινομενικά πολύ διαφορετική) εικασία των Taniyama - Shimura - Weyl και μετά από μια μακριά αλυσίδα αποτελεσμάτων πολλών μαθηματικών (Frey, Ribet και άλλων), το 1995, 358 χρόνια μετά από το 1637, ο Wiles απέδειξε την εικασία του Fermat.

## 5.4 Ασκήσεις.

1. Λύστε τις Διοφαντικές εξισώσεις $14x + 35y = 93$ και $56x + 72y = 40$.
2. Λύστε τις Διοφαντικές εξισώσεις $18x + 5y = 48$ και $158x - 57y = 7$ για $x, y > 0$.
3. Έστω $a, b > 0$, $(a, b) = 1$. Αποδείξτε ότι η Διοφαντική εξίσωση $ax - by = c$ για $x, y > 0$ έχει άπειρες λύσεις.
4. Έστω $a, b, c > 0$, $(a, b) = d$, $ab = c^2$. Αποδείξτε ότι υπάρχουν $m, n > 0$ ώστε $a = dm^2$, $b = dn^2$.
5. Για ποιούς $n$ έχει τουλάχιστον μία λύση η Διοφαντική εξίσωση $x^2 - y^2 = n$;
6. Βρείτε όλες τις Πυθαγόρειες τριάδες $(\xi, \eta, \zeta)$ με $\xi = 40$.

   Βρείτε όλες τις Πυθαγόρειες τριάδες $(\xi, \eta, \zeta)$ με $\xi, \eta, \zeta > 0$ έτσι ώστε τα $\xi, \eta, \zeta$ να αποτελούν διαδοχικούς όρους αριθμητικής προόδου.
7. Έστω Πυθαγόρεια τριάδα $(\xi, \eta, \zeta)$. Αποδείξτε ότι τουλάχιστον ένα από τα $\xi, \eta$ διαιρείται από το 3 και ότι τουλάχιστον ένα από τα $\xi, \eta, \zeta$ διαιρείται από το 5.
8. Έστω τυχόν $n$. Αποδείξτε ότι υπάρχει Πυθαγόρεια τριάδα $(\xi, \eta, \zeta)$ ώστε τουλάχιστον ένα από τα $\xi, \eta, \zeta$ να είναι ίσο με $n$.
9. Αποδείξτε ότι η Διοφαντική εξίσωση $15x^2 - 7y^2 = 9$ δεν έχει λύσεις.
10. Αποδείξτε ότι η Διοφαντική εξίσωση $x^2 + y^2 = 9z + 3$ δεν έχει λύσεις.
11. Αποδείξτε ότι η Διοφαντική εξίσωση $x^4 - 2y^2 = 1$ έχει μόνο δύο λύσεις.
12. Βρείτε όλες τις λύσεις της Διοφαντικής εξίσωσης $x^2 + y^2 = 2z^2$.

## 5.5 Λύσεις ασκήσεων.

3. Γνωρίζουμε ότι η Διοφαντική εξίσωση $ax - by = c$ έχει τουλάχιστον μία λύση $x = x_1$, $y = y_1$ και ότι οι λύσεις της δίνονται από τους τύπους

$$x = x_1 - kb, \ y = y_1 - ka \qquad (k \in \mathbb{Z}).$$

   Για να δούμε αν μπορεί να είναι $x, y > 0$, γράφουμε

$$x_1 - kb > 0, \ y_1 - ka > 0$$

   ή, ισοδύναμα,

$$k < \frac{x_1}{b}, \ k < \frac{y_1}{a}$$

ή, ισοδύναμα,

$$k < \min\left\{\frac{x_1}{b}, \frac{y_1}{a}\right\}.$$

Βλέπουμε, λοιπόν, ότι για άπειρες τιμές του $k$ έχουμε λύσεις με $x, y > 0$.

5. Κατ' αρχάς, αν $n = 0$, τότε η εξίσωση έχει άπειρες λύσεις: $x = \pm\xi, y = \pm\xi$.
Υποθέτουμε, λοιπόν, ότι $n \neq 0$. Η εξίσωση $x^2 - y^2 = n$ γράφεται

$$(x - y)(x + y) = n.$$

Αν το $n$ είναι περιττό, τότε μπορούμε να βρούμε $x, y$ ώστε

$$x - y = 1,\ x + y = n.$$

Πράγματι, αυτό το σύστημα έχει λύση

$$x = \frac{n+1}{2},\ y = \frac{n-1}{2}$$

και οι δυο αριθμοί $\frac{n+1}{2}, \frac{n-1}{2}$ είναι ακέραιοι.
Αν το $n$ είναι άρτιο, τότε τα $x, y$ είναι είτε και τα δύο άρτια είτε και τα δύο περιττά. Είναι εύκολο να δει κανείς ότι και στις δύο περιπτώσεις το $x^2 - y^2$ είναι πολλαπλάσιο του $4$. Άρα, αν το $n$ είναι άρτιο, τότε, για να έχει λύση η εξίσωση, πρέπει το $n$ να είναι πολλαπλάσιο του $4$.
Έστω, λοιπόν, ότι το $n$ είναι πολλαπλάσιο του $4$. Δηλαδή, έστω $n = 4m$.
Τότε, όμως, μπορούμε να βρούμε $x, y$ ώστε

$$x - y = 2,\ x + y = 2m.$$

Πράγματι, αυτό το σύστημα έχει λύση

$$x = m + 1,\ y = m - 1.$$

Άρα η Διοφαντική εξίσωση $x^2 - y^2 = n$ έχει τουλάχιστον μία λύση αν και μόνο αν το $n$ είναι είτε περιττό είτε πολλαπλάσιο του $4$. (Η περίπτωση $n = 0$ εντάσσεται στην περίπτωση που το $n$ είναι πολλαπλάσιο του $4$.)

5. Οι Πυθαγόρειες τριάδες με $x, y, z > 0$ δίνονται από τους τύπους

$$x = d(u^2 - v^2), \quad y = d2uv, \quad z = d(u^2 + v^2) \tag{5.15}$$

όπου
(ii) $d \geq 1$,
(iii) $u > v \geq 1$, $(u, v) = 1$ και
(iv) ο ένας από τους $u, v$ είναι άρτιος και ο άλλος περιττός.
Το $z$ είναι ο μεγαλύτερος από τους τρεις αριθμούς, οπότε το να αποτελούν τα $x, y, z$ διαδοχικούς όρους αριθμητικής προόδου ισοδυναμεί με το να ισχύει

$$x + z = 2y \qquad \text{ή} \qquad y + z = 2x.$$

Στην περίπτωση $x + z = 2y$, από τους τύπους (5.15) συνεπάγεται

$$u^2 = 2uv,$$

οπότε

$$u = 2v$$

και, από την (iii),

$$1 = (u, v) = (2v, v) = v$$

και άρα οι αντίστοιχες Πυθαγόρειες τριάδες είναι οι

$$x = 3d, \quad y = 4d, \quad z = 5d$$

(και, φυσικά, οι $x = 4d, y = 3d, z = 5d$.)
Στην περίπτωση $y + z = 2x$, από τους τύπους (5.15) συνεπάγεται

$$2uv + u^2 + v^2 = 2u^2 - 2v^2,$$

οπότε

$$u = 3v.$$

Αυτό, όμως, είναι αδύνατον λόγω της (iv).

9. Βλέπουμε εύκολα ότι δεν υπάρχουν λύσεις με $x = 0$ ή $y = 0$.
Άρα, αν η εξίσωση έχει λύσεις, μπορούμε να υποθέσουμε ότι $x, y > 0$.
Επειδή το 3 διαιρεί τα $15x^2$ και 9, συνεπάγεται ότι πρέπει να διαιρεί και το $y$.
Παραγοντοποιώντας το 3 στα $x, y$, γράφουμε

$$x = 3^\alpha x_1, \quad y = 3^\beta y_1,$$

όπου

$$\alpha \geq 0, \quad \beta \geq 1, \quad 3 \nmid x_1, \quad 3 \nmid y_1.$$

Τότε η εξίσωση $15x^2 - 7y^2 = 9$ γράφεται

$$5 \cdot 3^{2\alpha+1} x_1^2 - 7 \cdot 3^{2\beta} y_1^2 = 9 = 3^2.$$

Επειδή $2\beta \geq 2$, συνεπάγεται $2\alpha + 1 \geq 2$, οπότε

$$\alpha \geq 1.$$

Τώρα έχουμε

$$5 \cdot 3^{2\alpha-1} x_1^2 - 7 \cdot 3^{2\beta-2} y_1^2 = 1.$$

Επειδή $2\alpha - 1 \geq 1$, συνεπάγεται $2\beta - 2 = 0$, δηλαδή

$$\beta = 1.$$

Άρα

$$3 \mid 7y_1^2 + 1.$$

Επειδή $3 \nmid y_1$, ο $y_1$ είναι είτε της μορφής $3n + 1$ είτε της μορφής $3n + 2$. Και στις δυο περιπτώσεις ο $7y_1^2 + 1$ είναι της μορφής $3n + 2$ και καταλήγουμε σε άτοπο.

10. Έχουμε δει ότι το $x^2$ είναι είτε της μορφής $3n$ είτε της μορφής $3n+1$. Το ίδιο ισχύει και για το $y^2$. Επομένως, για να είναι το $x^2+y^2$ πολλαπλάσιο του 3, πρέπει τα $x^2$, $y^2$ να είναι και τα δύο της μορφής $3n$. Αυτό σημαίνει ότι τα $x, y$ πρέπει να είναι και τα δύο πολλαπλάσια του 3, οπότε το $x^2+y^2$ πρέπει να είναι πολλαπλάσιο του 9. Τότε, όμως, η ισότητα $x^2+y^2 = 9z+3$ είναι αδύνατη.

# Κεφάλαιο 6

# Αριθμοθεωρητικές συναρτήσεις.

## 6.1 Αριθμοθεωρητικές συναρτήσεις.

**Αριθμοθεωρητική συνάρτηση** χαρακτηρίζεται μια οποιαδήποτε συνάρτηση με πεδίο ορισμού το $\mathbb{N}$:

$$f : \mathbb{N} \to \mathbb{C}.$$

**ΟΡΙΣΜΟΣ.** *Μια αριθμοθεωρητική συνάρτηση $f$ χαρακτηρίζεται* **πολλαπλασιαστική** *αν*
*(i)* $f(n) \neq 0$ *για τουλάχιστον ένα* $n$*,*
*(ii)* $f(mn) = f(m)f(n)$ *όταν* $(m, n) = 1$.

Θα κάνουμε μια παρατήρηση. Έστω $f(n_0) \neq 0$. Επειδή $(n_0, 1) = 1$, από την (ii) συνεπάγεται

$$f(n_0) = f(n_0 1) = f(n_0)f(1)$$

και, επομένως,

$$f(1) = 1.$$

Άρα μια αριθμοθεωρητική συνάρτηση $f$ είναι πολλαπλασιαστική αν και μόνο αν
(i') $f(1) = 1$,
(ii) $f(mn) = f(m)f(n)$ όταν $(m, n) = 1$.

**Παράδειγμα.** Για κάθε πραγματική τιμή του $a$ η συνάρτηση με τύπο

$$f(n) = n^a$$

είναι, προφανώς, πολλαπλασιαστική.
Ειδικώτερα, η σταθερή συνάρτηση

$$f(n) = 1$$

και η ταυτοτική συνάρτηση

$$f(n) = n$$

είναι πολλαπλασιαστικές.

**Παράδειγμα.** Έστω η συνάρτηση $\tau$, όπου $\tau(n)$ είναι το πλήθος των θετικών διαιρετών του $n$.
Προφανώς, $\tau(1) = 1$.
Τώρα, αν θέλουμε να ελέγξουμε την (ii), αρκεί να θεωρήσουμε την περίπτωση $m, n > 1$.
Αν οι κανονικές αναπαραστάσεις των $m, n$ είναι οι

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad n = q_1^{\beta_1} \cdots q_l^{\beta_l},$$

τότε, επειδή $(m, n) = 1$, καθένας από τους $p_1, \ldots, p_k$ είναι διαφορετικός από καθέναν από τους $q_1, \ldots, q_l$.
Άρα η κανονική αναπαράσταση του $mn$ είναι η

$$mn = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}.$$

Τώρα, από την Πρόταση 4.6 έχουμε

$$\tau(mn) = (\alpha_1 + 1) \cdots (\alpha_k + 1)(\beta_1 + 1) \cdots (\beta_l + 1) = \tau(m)\tau(n).$$

Άρα η συνάρτηση $\tau$ είναι πολλαπλασιαστική.

**Παράδειγμα.** Τώρα θεωρούμε την συνάρτηση $\sigma$, όπου $\sigma(n)$ είναι το άθροισμα των θετικών διαιρετών του $n$.
Πάλι, είναι προφανές ότι $\sigma(1) = 1$.
Οπότε, και πάλι, για να ελέγξουμε την (ii), αρκεί να θεωρήσουμε την περίπτωση $m, n > 1$.
Θεωρούμε τις κανονικές αναπαραστάσεις των $m, n$:

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad n = q_1^{\beta_1} \cdots q_l^{\beta_l}.$$

Όπως και στο προηγούμενο παράδειγμα, η κανονική αναπαράσταση του $mn$ είναι η

$$mn = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}$$

και από την Πρόταση 4.6 έχουμε

$$\sigma(mn) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \frac{q_1^{\beta_1+1} - 1}{q_1 - 1} \cdots \frac{q_l^{\beta_l+1} - 1}{q_l - 1} = \sigma(m)\sigma(n).$$

Άρα η συνάρτηση $\sigma$ είναι πολλαπλασιαστική.

Τώρα θα δούμε ένα χρήσιμο σύμβολο για αθροίσματα:

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

Με το σύμβολο αυτό δηλώνουμε *το άθροισμα των τιμών της αριθμοθεωρητικής συνάρτησης $f$ στους θετικούς διαιρέτες $d$ του $n$.*
Για παράδειγμα:

$$\sum_{d|1} f(d) = f(1), \qquad \sum_{d|6} f(d) = f(1) + f(2) + f(3) + f(6).$$

**Θεώρημα 6.1.** *Αν η συνάρτηση $f$ είναι πολλαπλασιαστική, τότε η συνάρτηση $F$, η οποία ορίζεται με τον τύπο*

$$F(n) = \sum_{d|n} f(d),$$

*είναι κι αυτή πολλαπλασιαστική.*

*Απόδειξη.* Έστω ότι η $f$ είναι πολλαπλασιαστική.
Κατ' αρχάς

$$F(1) = f(1) = 1.$$

Τώρα, έστω $(m, n) = 1$.
Γνωρίζουμε ότι, όταν το $d_1$ διατρέχει όλους τους θετικούς διαιρέτες του $m$ και το $d_2$ διατρέχει όλους τους θετικούς διαιρέτες του $n$, τότε το $d_1 d_2$ διατρέχει όλους τους θετικούς διαιρέτες του

$mn$. Αυτό είναι το περιεχόμενο της Πρότασης 3.7.
Άρα

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d) = \sum_{d_1|m,d_2|n} f(d_1 d_2) = \sum_{d_1|m,d_2|n} f(d_1)f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= f(m)f(n). \end{aligned}$$

Για την τρίτη ισότητα χρησιμοποιήσαμε το ότι $f(d_1d_2) = f(d_1)f(d_2)$. Αυτό ισχύει διότι η $f$ είναι πολλαπλασιαστική και διότι $(d_1, d_2) = 1$. (Πράγματι, κάθε κοινός διαιρέτης των $d_1, d_2$ είναι κοινός διαιρέτης και των $m, n$.)
Άρα η $F$ είναι πολλαπλασιαστική. □

Πριν προχωρήσουμε, ας δούμε μια απλή ιδιότητα των πολλαπλασιαστικών συναρτήσεων. Αν η $f$ είναι πολλαπλασιαστική συνάρτηση, τότε

$$f(m_1 \cdots m_k) = f(m_1) \cdots f(m_k) \qquad \text{όταν οι } m_1, \ldots, m_k \text{ είναι ανά δύο σχετικά πρώτοι.}$$

Για $k = 2$, αυτό είναι στον ορισμό της πολλαπλασιαστικής συνάρτησης και με επαγωγή προκύπτει η γενικότερη περίπτωση.

Για παράδειγμα, αν η $f$ είναι πολλαπλασιαστική και ο $n > 1$ έχει κανονική αναπαράσταση

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

τότε

$$f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k}).$$

Αυτό είναι χρήσιμο όταν θέλουμε να βρούμε τον τύπο μιας πολλαπλασιαστικής συνάρτησης: *είναι αρκετό να βρούμε τον τύπο της στις δυνάμεις των πρώτων*.

Στα δυο επόμενα παραδείγματα θα (ξανα)αποδείξουμε ότι οι συναρτήσεις $\tau$ και $\sigma$ είναι πολλαπλασιαστικές. Προηγουμένως, το αποδείξαμε θεωρώντας γνωστούς τους τύπους των δυο συναρτήσεων. Τώρα θα το αποδείξουμε εφαρμόζοντας το Θεώρημα 6.1 και, βάσει της πολλαπλασιαστικότητας των δυο συναρτήσεων, θα βρούμε τους τύπους των.

**Παράδειγμα.** Θεωρούμε την πολλαπλασιαστική (σταθερή) συνάρτηση με τύπο $f(n) = 1$. Τότε η αντίστοιχη συνάρτηση $F$ του Θεωρήματος 6.1 είναι η

$$\tau(n) = \sum_{d|n} 1. \tag{6.1}$$

Πράγματι, αν σε κάθε θετικό διαιρέτη $d$ του $n$ αντιστοιχίσουμε μια μονάδα και αθροίσουμε αυτές τις μονάδες, τότε προκύπτει το πλήθος των θετικών διαιρετών του $n$.
Άρα από το Θεώρημα 6.1 προκύπτει ότι η $\tau$ είναι πολλαπλασιαστική.
Άρα, αν ο $n > 1$ έχει κανονική αναπαράσταση

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

τότε

$$\tau(n) = \tau(p_1^{\alpha_1}) \cdots \tau(p_k^{\alpha_k}).$$

Τώρα, αν ο $p$ είναι πρώτος, οι θετικοί διαιρέτες του $p^\alpha$ είναι οι $1, p, p^2, \ldots, p^\alpha$, οπότε το πλήθος τους είναι ίσο με

$$\tau(p^\alpha) = \alpha + 1.$$

Άρα ο τύπος της $\tau$ για $n > 1$ είναι

$$\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1).$$

**Παράδειγμα.** Θεωρούμε την πολλαπλασιαστική (ταυτοτική) συνάρτηση με τύπο $f(n) = n$. Η αντίστοιχη συνάρτηση $F$ του Θεωρήματος 6.1 είναι η

$$\sigma(n) = \sum_{d|n} d. \tag{6.2}$$

Πράγματι, το σύμβολο δεξιά δηλώνει το άθροισμα των θετικών διαιρετών του $n$.
Άρα από το Θεώρημα 6.1 προκύπτει ότι η $\sigma$ είναι πολλαπλασιαστική.
Άρα, αν ο $n > 1$ έχει κανονική αναπαράσταση

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

τότε

$$\sigma(n) = \sigma(p_1^{\alpha_1}) \cdots \sigma(p_k^{\alpha_k}).$$

Όπως στο προηγούμενο παράδειγμα, οι θετικοί διαιρέτες του $p^\alpha$ είναι οι $1, p, p^2, \ldots, p^\alpha$, οπότε το άθροισμά τους είναι ίσο με

$$\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

Άρα ο τύπος της $\sigma$ για $n > 1$ είναι

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

## 6.2 Η συνέλιξη και η συνάρτηση του Möbius.

**ΟΡΙΣΜΟΣ.** *Το $n > 1$ χαρακτηρίζεται* **ελεύθερο τετραγώνου** *αν δεν υπάρχει πρώτος $p$ ώστε $p^2 \mid n$.*

Για να ισχύει $p^2 \mid n$ προϋποτίθεται ότι ισχύει $p \mid n$. Επομένως, το να είναι ο $n > 1$ ελεύθερος τετραγώνου ισοδυναμεί με το ότι για κάθε πρώτο διαιρέτη $p$ του $n$ ισχύει $p^2 \nmid n$. Επομένως, το να είναι ο $n > 1$ ελεύθερος τετραγώνου ισοδυναμεί με το ότι η κανονική αναπαράστασή του είναι της μορφής

$$n = p_1 \cdots p_k,$$

όπου όλοι οι πρώτοι διαιρέτες του $n$ εμφανίζονται με εκθέτη 1.

**ΟΡΙΣΜΟΣ.** *Η αριθμοθεωρητική* **συνάρτηση Möbius** $\mu$ *ορίζεται με τον τύπο*

$$\mu(n) = \begin{cases} 1, & \text{αν } n = 1 \\ 0, & \text{αν } p^2 \mid n \text{ για κάποιον πρώτο } p \\ (-1)^k, & \text{αν } n = p_1 \cdots p_k \text{ και οι } p_1, \ldots, p_k \text{ είναι πρώτοι με } p_1 < \ldots < p_k \end{cases}$$

Για παράδειγμα,

$$\mu(1) = 1,\ \mu(2) = (-1)^1 = -1,\ \mu(4) = \mu(2^2) = 0,\ \mu(6) = \mu(2 \cdot 3) = (-1)^2 = 1,$$

$$\mu(20) = \mu(2^2 \cdot 5) = 0,\ \mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1.$$

**Πρόταση 6.1.** *Η συνάρτηση Möbius είναι πολλαπλασιαστική.*

*Απόδειξη.* Επειδή $\mu(1) = 1$, αρκεί να αποδείξουμε ότι ισχύει $\mu(mn) = \mu(m)\mu(n)$ όταν $(m, n) = 1$. Επίσης, είναι προφανές ότι η σχέση αυτή ισχύει αν ένας τουλάχιστον από τους $n, m$ είναι ίσος με 1.

Έστω, λοιπόν, $m, n > 1$ και $(m, n) = 1$.
Αν $p^2 \mid m$ για κάποιον πρώτο $p$, τότε $p^2 \mid mn$, οπότε

$$\mu(mn) = 0, \qquad \mu(m)\mu(n) = 0\mu(n) = 0.$$

Ομοίως, αν $p^2 \mid n$ για κάποιον πρώτο $p$.
Απομένει να υποθέσουμε ότι οι $m, n$ είναι ελεύθεροι τετραγώνου. Τότε οι κανονικές αναπαραστάσεις των $m, n$ είναι της μορφής

$$m = p_1 \cdots p_k, \qquad n = q_1 \cdots q_l.$$

Επειδή $(m, n) = 1$, καθένας από τους $p_1, \ldots, p_k$ είναι διαφορετικός από καθέναν από τους $q_1, \ldots, q_l$. Άρα η κανονική αναπαράσταση του $mn$ είναι η

$$mn = p_1 \cdots p_k q_1 \cdots q_l.$$

Άρα

$$\mu(mn) = (-1)^{k+l} = (-1)^k(-1)^l = \mu(m)\mu(n).$$

Άρα η $\mu$ είναι πολλαπλασιαστική. □

**Πρόταση 6.2.** *Ισχύει*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{αν } n = 1 \\ 0, & \text{αν } n > 1 \end{cases} \tag{6.3}$$

*Απόδειξη.* Ορίζουμε την αριθμοθεωρητική συνάρτηση $F$ με τύπο

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

Από το Θεώρημα 6.1 συνεπάγεται ότι η $F$ είναι πολλαπλασιαστική.
Έστω πρώτος $p$ και $\alpha \geq 1$. Τότε οι θετικοί διαιρέτες του $p^\alpha$ είναι οι $1, p, p^2, \ldots, p^\alpha$, οπότε

$$F(p^\alpha) = 1 + \mu(p) + \mu(p^2) + \cdots + \mu(p^\alpha) = 1 + (-1) + 0 + \cdots + 0 = 0.$$

Άρα, αν η κανονική αναπαράσταση του $n > 1$ είναι

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

τότε

$$F(n) = \mu(p_1^{\alpha_1}) \cdots \mu(p_k^{\alpha_k}) = 0 \cdots 0 = 0.$$

Το $F(1) = 1$ είναι προφανές. □

Θα κάνουμε μια παρατήρηση σε σχέση με αθροίσματα

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

*Όταν ο $d$ διατρέχει τους θετικούς διαιρέτες του $n$, τότε ο $c = \frac{n}{d}$ διατρέχει κι αυτός τους θετικούς διαιρέτες του $n$.* Για παράδειγμα, αν ο $d$ διατρέχει τους θετικούς διαιρέτες $1, 2, 3, 6$ του $6$, τότε ο $c = \frac{6}{d}$ διατρέχει, με αντίστροφη σειρά, τους θετικούς διαιρέτες $6, 3, 2, 1$ του $6$. Άρα στο παραπάνω άθροισμα μπορούμε να κάνουμε "αλλαγή μεταβλητής" από $d$ σε $c = \frac{n}{d}$ και έχουμε

$$\sum_{d|n} f(d) = \sum_{c|n} f\Big(\frac{n}{c}\Big).$$

Αλλάζοντας το σύμβολο της μεταβλητής στο δεξιό άθροισμα από $c$ σε $d$, καταλήγουμε στην ταυτότητα:

$$\sum_{d|n} f(d) = \sum_{d|n} f\Big(\frac{n}{d}\Big). \tag{6.4}$$

Αυτή η ταυτότητα θα μα φανεί χρήσιμη παρακάτω.

Υπάρχουν δυο βασικές "πράξεις" με αριθμοθεωρητικές συναρτήσεις. Η πρώτη "πράξη" είναι ο γνωστός πολλαπλασιασμός συναρτήσεων με τύπο:

$$(fg)(n) = f(n)g(n).$$

Είναι σχεδόν προφανές ότι, αν οι $f, g$ είναι πολλαπλασιαστικές, τότε και η $fg$ είναι πολλαπλασιαστική. Πράγματι:

$$(fg)(1) = f(1)g(1) = 1 \cdot 1 = 1,$$

$$(fg)(mn) = f(mn)g(mn) = f(m)f(n)g(m)g(n) = f(m)g(m)f(n)g(n) = (fg)(m)(fg)(n)$$

όταν $(m, n) = 1$.

Υπάρχει και μια δεύτερη "πράξη".

**ΟΡΙΣΜΟΣ.** *Έστω αριθμοθεωρητικές συναρτήσεις $f, g$. Ορίζουμε την αριθμοθεωρητική συνάρτηση $f * g$ με τύπο*

$$(f * g)(n) = \sum_{d|n} f(d)g\Big(\frac{n}{d}\Big).$$

*Η $f * g$ ονομάζεται* **συνέλιξη** *ή* **γινόμενο Dirichlet** *των $f, g$.*

Για παράδειγμα,

$$(f * g)(6) = f(1)g(6) + f(2)g(3) + f(3)g(2) + f(6)g(1).$$

Χρησιμοποιώντας την ταυτότητα (6.4) βρίσκουμε

$$(f * g)(n) = \sum_{d|n} f(d)g\Big(\frac{n}{d}\Big) = \sum_{d|n} f(\frac{n}{d})g\Big(\frac{n}{\frac{n}{d}}\Big) = \sum_{d|n} g(d)f\Big(\frac{n}{d}\Big) = (g * f)(n)$$

για κάθε $n$, οπότε

$$f * g = g * f.$$

Άρα η πράξη της συνέλιξης είναι *μεταθετική*.

Τώρα θα χρησιμοποιήσουμε την εξής παρατήρηση:

$$d \mid n,\ c \mid \frac{n}{d} \quad \Leftrightarrow \quad c \mid n,\ d \mid \frac{n}{c}.$$

Βάσει αυτής της παρατήρησης, έχουμε

$$\begin{aligned}
\big(f * (g * h)\big)(n) &= \sum_{d|n} f(d)(g * h)\Big(\frac{n}{d}\Big) = \sum_{d|n} f(d)\Big(\sum_{c|\frac{n}{d}} g\Big(\frac{n}{dc}\Big)h(c)\Big) \\
&= \sum_{d|n, c|\frac{n}{d}} f(d)g\Big(\frac{n}{dc}\Big)h(c) = \sum_{c|n, d|\frac{n}{c}} f(d)g\Big(\frac{n}{dc}\Big)h(c) \\
&= \sum_{c|n} \Big(\sum_{d|\frac{n}{c}} f(d)g\Big(\frac{n}{dc}\Big)\Big)h(c) = \sum_{c|n} (f * g)\Big(\frac{n}{c}\Big)h(c) \\
&= \big((f * g) * h\big)(n)
\end{aligned}$$

για κάθε $n$, οπότε

$$f * (g * h) = (f * g) * h.$$

Άρα η πράξη της συνέλιξης είναι *προσεταιριστική*.

Τέλος, ορίζουμε και την αριθμοθεωρητική συνάρτηση $e$ με τύπο

$$e(n) = \begin{cases} 1, & \text{αν } n = 1 \\ 0, & \text{αν } n > 1 \end{cases}$$

Η συνάρτηση $e$ είναι το *μοναδιαίο στοιχείο* της πράξης συνέλιξη. Πράγματι, για κάθε $n$ έχουμε

$$(f * e)(n) = \sum_{d|n} f(d)e\Big(\frac{n}{d}\Big) = f(n),$$

διότι, καθώς ο $d$ διατρέχει τους θετικούς διαιρέτες του $n$, μόνο στην περίπτωση $d = n$ θα έχουμε $e(\frac{n}{d}) = e(1) = 1$ και σε κάθε άλλη περίπτωση θα έχουμε $e(\frac{n}{d}) = 0$.

Άρα

$$f * e = f.$$

Είναι πολύ εύκολο να δει κανείς ότι η $e$ είναι και πολλαπλασιαστική συνάρτηση.

**Τύπος Αντιστροφής του Mobius.** *Αν*

$$F(n) = \sum_{d|n} f(d) \qquad \textit{για κάθε } n,$$

*τότε*

$$f(n) = \sum_{d|n} F(d)\mu\Big(\frac{n}{d}\Big) \qquad \textit{για κάθε } n.$$

*Απόδειξη.* Χρησιμοποιώντας την σταθερή συνάρτηση 1, έχουμε

$$F(n) = \sum_{d|n} f(d) = \sum_{d|n} f(d)1 = (f * 1)(n)$$

για κάθε $n$, οπότε

$$F = f * 1.$$

Με την ίδια λογική, ο τύπος (6.3) γράφεται

$$(\mu * 1)(n) = \sum_{d|n} \mu(d)1 = e(n)$$

για κάθε $n$, οπότε

$$\mu * 1 = e.$$

Επομένως,

$$F * \mu = (f * 1) * \mu = f * (1 * \mu) = f * e = f,$$

το οποίο σημαίνει ότι

$$f(n) = (F * \mu)(n) = \sum_{d|n} F(d)\mu\Big(\frac{n}{d}\Big)$$

για κάθε $n$. □

**Παράδειγμα.** Ας ξαναδούμε την ταυτότητα (6.1):

$$\tau(n) = \sum_{d|n} 1.$$

Αυτή μας λέει ότι, αν θεωρήσουμε ως $f$ την σταθερή συνάρτηση 1, τότε η αντίστοιχη συνάρτηση $F$ του τελευταίου Θεωρήματος είναι η $\tau$. Τότε ο τύπος αντιστροφής του Möbius γράφεται:

$$1 = \sum_{d|n} \tau(d)\mu\Big(\frac{n}{d}\Big).$$

**Παράδειγμα.** Η ταυτότητα (6.2),

$$\sigma(n) = \sum_{d|n} d,$$

μας λέει ότι, αν θεωρήσουμε ως $f$ την ταυτοτική συνάρτηση, τότε η αντίστοιχη συνάρτηση $F$ του τελευταίου Θεωρήματος είναι η $\sigma$. Τότε ο τύπος αντιστροφής του Möbius γράφεται:

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

**Πρόταση 6.3.** *Αν οι αριθμοθεωρητικές συναρτήσεις $f, g$ είναι πολλαπλασιαστικές, τότε και η $f * g$ είναι πολλαπλασιαστική.*

*Απόδειξη.* Έστω ότι οι $f, g$ είναι πολλαπλασιαστικές.
Κατ' αρχάς,

$$(f * g)(1) = \sum_{d|1} f(d)g\Big(\frac{1}{d}\Big) = f(1)g(1) = 1 \cdot 1 = 1.$$

Κατόπιν, έστω $(m, n) = 1$. Θα χρησιμοποιήσουμε πάλι το ότι, αν ο $d_1$ διατρέχει τους θετικούς διαιρέτες του $m$ και ο $d_2$ διατρέχει τους θετικούς διαιρέτες του $n$, τότε ο $d_1 d_2$ διατρέχει τους θετικούς διαιρέτες του $mn$. Επίσης, σκεφτόμαστε ότι, αν $(m, n) = 1$ και $d_1 \mid m$ και $d_2 \mid n$, τότε $(d_1, d_2) = 1$ και $(\frac{m}{d_1}, \frac{n}{d_2}) = 1$. Και, επειδή οι $f, g$ είναι πολλαπλασιαστικές, έχουμε:

$$\begin{aligned}
(f * g)(mn) &= \sum_{d|mn} f(d)g\Big(\frac{mn}{d}\Big) = \sum_{d_1|m, d_2|n} f(d_1 d_2)g\Big(\frac{mn}{d_1 d_2}\Big) \\
&= \sum_{d_1|m, d_2|n} f(d_1)f(d_2)g\Big(\frac{m}{d_1}\Big)g\Big(\frac{n}{d_2}\Big) \\
&= \sum_{d_1|m} f(d_1)g\Big(\frac{m}{d_1}\Big) \sum_{d_2|n} f(d_2)g\Big(\frac{n}{d_2}\Big) \\
&= (f * g)(m)(f * g)(n).
\end{aligned}$$

Άρα η $f * g$ είναι πολλαπλασιαστική. □

Παρατηρήστε ότι το Θεώρημα 6.1 είναι απλή εφαρμογή της Πρότασης 6.3. Πράγματι, είδαμε ήδη ότι η συνάρτηση $F$ του Θεωρήματος 6.1 γράφεται

$$F = f * 1,$$

οπότε, επειδή η σταθερή συνάρτηση 1 είναι πολλαπλασιαστική, αν η $f$ είναι πολλαπλασιαστική, τότε και η $F$ είναι πολλαπλασιαστική.

Το ότι, αν οι αριθμοθεωρητικές συναρτήσεις $f, g$ είναι πολλαπλασιαστικές συνεπάγεται ότι και οι $fg, f * g$ είναι πολλαπλασιαστικές, λέει με άλλα λόγια ότι το υποσύνολο του συνόλου των αριθμοθεωρητικών συναρτήσεων που αποτελείται από τις πολλαπλασιαστικές συναρτήσεις είναι *κλειστό* ως προς τις πράξεις πολλαπλασιασμός και συνέλιξη.

## 6.3 Η συνάρτηση $\phi$ του Euler.

**ΟΡΙΣΜΟΣ.** *Αν $n \geq 1$, με το σύμβολο*

$$\phi(n)$$

*δηλώνουμε το πλήθος των $k$ με $0 \leq k \leq n-1$ και $(k, n) = 1$.*
*Η αριθμοθεωρητική συνάρτηση $\phi$ ονομάζεται* **συνάρτηση $\phi$ του Euler.**

Για παράδειγμα:

$$\phi(1) = 1,\ \phi(2) = 1,\ \phi(3) = 2,\ \phi(4) = 2,\ \phi(5) = 4,\ \phi(6) = 2.$$

Είναι εύκολο να δει κανείς ότι

$$\phi(p) = p - 1 \qquad \text{για κάθε πρώτο } p.$$

Πράγματι, οι αριθμοί $1, 2, \ldots, p-1$ δεν διαιρούνται από τον $p$, οπότε είναι σχετικά πρώτοι με τον $p$.

Αλλά, πιο γενικά, θα δούμε ότι για κάθε πρώτο $p$ και κάθε $\alpha \geq 1$ ισχύει

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\Big(1 - \frac{1}{p}\Big). \tag{6.5}$$

Σκεφτόμαστε ότι από τους αριθμούς $0, 1, 2, \ldots, p^\alpha - 1$ εκείνοι οι οποίοι δεν είναι σχετικά πρώτοι με τον $p$ είναι τα πολλαπλάσια του $p$, δηλαδή οι

$$0,\ p,\ 2p,\ \ldots,\ lp, \tag{6.6}$$

όπου ο $l$ προσδιορίζεται από την διπλή ανισότητα

$$lp < p^\alpha \leq (l+1)p.$$

Προκύπτει

$$l = p^{\alpha-1} - 1,$$

οπότε το πλήθος των αριθμών (6.6) είναι $p^{\alpha-1}$. Αυτό αποδεικνύει την (6.5).

**Λήμμα 6.1.** $(k, m) = 1$ *και* $(k, n) = 1$ *αν και μόνο αν* $(k, mn) = 1$.

*Απόδειξη.* Έστω $(k, mn) = 1$.
Θέτουμε $d = (k, m)$. Τότε $d \mid k$ και $d \mid m$. Επομένως, $d \mid k$ και $d \mid mn$. Άρα $d \mid (k, mn) = 1$, οπότε $d = 1$.
Ομοίως, $(k, n) = 1$.
Το αντίστροφο έχει ήδη αποδειχθεί με δύο τρόπους στην άσκηση 1.10. Να και μια τρίτη απόδειξη.
Έστω $(k, m) = 1$ και $(k, n) = 1$ και ας υποθέσουμε (για άτοπο) ότι $(k, mn) > 1$.
Τότε υπάρχει κοινός πρώτος διαιρέτης $p$ των $k, mn$. Δηλαδή, $p \mid k$ και $p \mid mn$. Συνεπάγεται ότι είτε $p \mid k$ και $p \mid m$ είτε $p \mid k$ και $p \mid n$. Άρα είτε $p \mid (k, m) = 1$ είτε $p \mid (k, n) = 1$ και καταλήγουμε σε άτοπο. □

Στην απόδειξη του επόμενου Θεωρήματος, εκτός από το Λήμμα 6.1, θα χρησιμοποιήσουμε και το Λήμμα 3.1. Το Λήμμα 3.1 λέει ότι: *αν έχουμε την Ευκλείδεια διαίρεση*

$$b = qa + r, \quad 0 \leq r < a,$$

*τότε*

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

**Θεώρημα 6.2.** *Η συνάρτηση $\phi$ είναι πολλαπλασιαστική.*

*Απόδειξη.* Γνωρίζουμε ότι $\phi(1) = 1$. Άρα αρκεί να αποδείξουμε ότι ισχύει $\phi(mn) = \phi(m)\phi(n)$ όταν $(m, n) = 1$ και, επειδή είναι προφανές ότι η σχέση αυτή ισχύει αν ένας τουλάχιστον από τους $m, n$ είναι ίσος με 1, υποθέτουμε ότι $m, n > 1$ και $(m, n) = 1$.

Το $\phi(mn)$ είναι ίσο με το πλήθος των αριθμών από τους $0, 1, \ldots, mn-1$ οι οποίοι είναι σχετικά πρώτοι με τον $mn$. Γράφουμε τους αριθμούς αυτούς στη μορφή πίνακα με $m$ στήλες και $n$ γραμμές:

| | | | | |
|---|---|---|---|---|
| $0$ | ... | $r$ | ... | $m-1$ |
| $\vdots$ | ... | $\vdots$ | ... | $\vdots$ |
| $lm$ | ... | $lm+r$ | ... | $lm+(m-1)$ |
| $\vdots$ | ... | $\vdots$ | ... | $\vdots$ |
| $(n-1)m$ | ... | $(n-1)m+r$ | ... | $(n-1)m+(m-1)$ |

(6.7)

Στην γραμμή "0" γράφουμε τους $m$ αριθμούς $0, \ldots m-1$. Στην γραμμή "1" συνεχίζουμε με τους επόμενους $m$ αριθμούς $m, \ldots m+(m-1)$. Και ούτω καθ' εξής. Στην γραμμή "$l$" εμφανίζονται οι $m$ αριθμοί $lm, \ldots lm+(m-1)$. Στην τελευταία, την γραμμή "$n-1$" εμφανίζονται οι $m$ αριθμοί $(n-1)m, \ldots (n-1)m+(m-1)$. Ο τελευταίος αριθμός είναι πράγματι ο $(n-1)m+(m-1) = mn-1$.

Παρατηρούμε ότι στην στήλη "0" βρίσκονται οι $n$ αριθμοί $0, m, \ldots (n-1)m$ και στην στήλη "$m-1$" βρίσκονται οι $n$ αριθμοί $m-1, m+(m-1), \ldots (n-1)m+(m-1)$. Γενικότερα, στην στήλη "$r$" βρίσκονται οι $n$ αριθμοί $r, m+r, \ldots (n-1)m+r$.

Λόγω του Λήμματος 6.1, το να βρούμε ποιοί από τους αριθμούς του πίνακα (6.7) είναι σχετικά πρώτοι με τον $mn$ είναι ισοδύναμο με το να βρούμε ποιοί από τους αριθμούς του πίνακα είναι σχετικά πρώτοι με τον $m$ και με τον $n$. Η ιδέα της απόδειξης είναι η εξής: *πρώτα θα εντοπίσουμε τους αριθμούς που είναι σχετικά πρώτοι με τον $m$ και, κατόπιν, από αυτούς θα εντοπίσουμε αυτούς που είναι σχετικά πρώτοι και με τον $n$.*

Εντοπίζουμε, ανάμεσα στους αριθμούς της γραμμής "0" εκείνους που είναι σχετικά πρώτοι με τον $m$. Γνωρίζουμε ότι το πλήθος τους είναι $\phi(m)$. Έστω ότι αυτοί οι αριθμοί είναι, σε αύξουσα σειρά μεγέθους, οι:

$$r_1, \ldots, r_{\phi(m)}. \tag{6.8}$$

Σύμφωνα με το Λήμμα 3.1, οι $n$ αριθμοί που βρίσκονται στην ίδια στήλη του πίνακα (6.7) έχουν όλοι τον ίδιο μέγιστο κοινό διαιρέτη με τον $m$, διότι όλοι αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν από τον $m$. Άρα οι αριθμοί που βρίσκονται στις στήλες που αντιστοιχούν στους αριθμούς (6.8) είναι όλοι σχετικά πρώτοι με τον $m$ και οι αριθμοί που βρίσκονται σε όλες τις άλλες στήλες δεν είναι σχετικά πρώτοι με τον $m$.

Άρα οι αριθμοί του πίνακα (6.7) που είναι σχετικά πρώτοι με τον $m$ είναι ακριβώς οι αριθμοί που εμφανίζονται στον πίνακα (6.9):

| | | |
|---|---|---|
| $r_1$ | ... | $r_{\phi(m)}$ |
| $\vdots$ | ... | $\vdots$ |
| $lm+r_1$ | ... | $lm+r_{\phi(m)}$ |
| $\vdots$ | ... | $\vdots$ |
| $(n-1)m+r_1$ | ... | $(n-1)m+r_{\phi(m)}$ |

(6.9)

Ο πίνακας (6.9) περιέχει μόνο τις στήλες του πίνακα (6.7) που αντιστοιχούν στους αριθμούς (6.8) της γραμμής "0". Έχει $n$ γραμμές και $\phi(m)$ στήλες.

Απομένει να εντοπίσουμε ανάμεσα στους αριθμούς του πίνακα (6.9) εκείνους που είναι σχετικά πρώτοι με τον $n$.

Αυτό που θα αποδείξουμε είναι ότι *κάθε στήλη του πίνακα (6.9) έχει ακριβώς $\phi(n)$ αριθμούς σχετικά πρώτους με τον $n$.* Με αυτό θα τελειώσει η απόδειξη, διότι θα έχουμε αποδείξει ότι υπάρχουν

συνολικά $\phi(m)\phi(n)$ αριθμοί ($\phi(m)$ στήλες επί $\phi(n)$ αριθμοί σε κάθε στήλη) σχετικά πρώτοι με τον $m$ και με τον $n$ και, επομένως, $\phi(m)\phi(n)$ αριθμοί σχετικά πρώτοι με τον $mn$ και άρα

$$\phi(mn) = \phi(m)\phi(n).$$

Θεωρούμε, λοιπόν, τους αριθμούς

$$r_k, \ldots, lm + r_k, \ldots, (n-1)m + r_k \tag{6.10}$$

της στήλης "$r_k$".
Πρώτα θα αποδείξουμε ότι *οι αριθμοί αυτοί αφήνουν ανά δύο διαφορετικά υπόλοιπα όταν διαιρεθούν από τον* $n$.
Ας υποθέσουμε (για άτοπο) ότι δύο από τους αριθμούς (6.10) αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν από τον $n$. Δηλαδή, για κάποιους $l_1, l_2$ με $0 \leq l_1 < l_2 < n$ έχουμε:

$$l_1 m + r_k = q_1 n + r, \quad 0 \leq r < n,$$

$$l_2 m + r_k = q_2 n + r, \quad 0 \leq r < n.$$

Συνεπάγεται

$$(l_2 - l_1)m = (q_2 - q_1)n,$$

οπότε

$$n \mid (l_2 - l_1)m$$

και, επειδή $(m, n) = 1$, έχουμε

$$n \mid l_2 - l_1,$$

το οποίο είναι αδύνατο, επειδή $0 < l_2 - l_1 < n$.
Πράγματι, λοιπόν, οι αριθμοί (6.10) αφήνουν ανά δύο διαφορετικά υπόλοιπα όταν διαιρεθούν από τον $n$ και, *επειδή το πλήθος τους είναι ίσο με* $n$, αφήνουν τα υπόλοιπα

$$0, \ldots, n-1 \tag{6.11}$$

όταν διαιρεθούν από τον $n$.
Τώρα, λόγω του Λήμματος 3.1 και πάλι, από τους αριθμούς (6.10) οι αριθμοί που είναι σχετικά πρώτοι με τον $n$ αντιστοιχούν στα υπόλοιπα (6.11) που είναι σχετικά πρώτα με τον $n$. Άρα το πλήθος των αριθμών από τους (6.10) που είναι σχετικά πρώτοι με τον $n$ είναι ίσο με το πλήθος των υπολοίπων (6.11) που είναι σχετικά πρώτα με τον $n$, δηλαδή ίσο με $\phi(n)$.
Αποδείξαμε, λοιπόν, ότι κάθε στήλη του πίνακα (6.9) έχει ακριβώς $\phi(n)$ αριθμούς σχετικά πρώτους με τον $n$ και η απόδειξη τελείωσε. □

Τώρα μπορούμε να γράψουμε εύκολα τον τύπο της συνάρτησης $\phi$. Πράγματι, $\phi(1) = 1$ και, αν $n > 1$ και ο $n$ έχει κανονική αναπαράσταση

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

τότε

$$\phi(n) = \phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) = n\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_k}\Big).$$

Για παράδειγμα: από τους αριθμούς $0, 1, \ldots, 1799$ το πλήθος εκείνων που είναι σχετικά πρώτοι με τον $1800$ είναι ίσο με

$$\phi(1800) = \phi(2^3 3^2 5^2) = (2^3 - 2^2)(3^2 - 3)(5^2 - 5) = 480.$$

Η Πρόταση 6.4 αποδείχθηκε από τον Gauss.

**Πρόταση 6.4.** *Για κάθε $n \geq 1$ ισχύει*

$$\sum_{d|n} \phi(d) = n.$$

*Απόδειξη.* Ορίζουμε την αριθμοθεωρητική συνάρτηση $F$ με τύπο

$$F(n) = \sum_{d|n} \phi(d).$$

Έστω ότι ο $n$ είναι δύναμη πρώτου: $n = p^\alpha$ με πρώτο $p$ και $\alpha \geq 1$.
Τότε οι θετικοί διαιρέτες του $p^\alpha$ είναι οι $1, p, \ldots, p^\alpha$ και άρα

$$F(p^\alpha) = \phi(1) + \phi(p) + \cdots + \phi(p^\alpha) = 1 + (p-1) + \cdots + (p^\alpha - p^{\alpha-1}) = p^\alpha,$$

διότι το τελευταίο άθροισμα είναι τηλεσκοπικό.
Επειδή η $\phi$ είναι πολλαπλασιαστική, συνεπάγεται ότι και η $F$ είναι πολλαπλασιαστική.
Άρα

$$F(1) = 1$$

και, αν $n > 1$ και ο $n$ έχει κανονική αναπαράσταση

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

τότε

$$F(n) = F(p_1^{\alpha_1}) \cdots F(p_k^{\alpha_k}) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = n.$$

Άρα ισχύει $F(n) = n$ για κάθε $n \geq 1$ και η απόδειξη τελείωσε. □

## 6.4 Ασκήσεις.

1. Για κάθε πραγματικό $k$ ορίζουμε

$$\sigma_k(n) = \sum_{d|n} d^k.$$

   Αποδείξτε ότι η $\sigma_k$ είναι πολλαπλασιαστική συνάρτηση.

2. Έστω $f, g$ δυο πολλαπλασιαστικές συναρτήσεις. Αν ισχύει $f(p^\alpha) = g(p^\alpha)$ για κάθε πρώτο $p$ και κάθε $\alpha \geq 1$, αποδείξτε ότι $f = g$.

3. Αποδείξτε τις παρακάτω ταυτότητες:

$$\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}, \qquad \Big(\sum_{d|n} \tau(d)\Big)^2 = \sum_{d|n} \tau(d)^3,$$

$$\sum_{d|n} \sigma(d) = n \sum_{d|n} \frac{\tau(d)}{d}, \qquad n \sum_{d|n} \frac{\sigma(d)}{d} = \sum_{d|n} d\tau(d).$$

4. Αποδείξτε τις παρακάτω ταυτότητες:

$$\sum_{d|n} \mu(d)\tau(d) = \begin{cases} 1, & \text{αν } n = 1 \\ (-1)^k, & \text{αν } n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \end{cases}$$

$$\sum_{d|n} \mu(d)\sigma(d) = \begin{cases} 1, & \text{αν } n = 1 \\ (-1)^k p_1 \cdots p_k, & \text{αν } n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \end{cases}$$

$$\sum_{d|n}\frac{\mu(d)}{d}=\begin{cases}1, & \text{αν } n=1\\ (1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k})=\frac{\phi(n)}{n}, & \text{αν } n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}\end{cases}$$

$$\sum_{d|n}d\mu(d)=\begin{cases}1, & \text{αν } n=1\\ (1-p_1)\cdots(1-p_k), & \text{αν } n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}\end{cases}$$

5. Βρείτε το πλήθος των αριθμών $k$ με $1\le k\le 3600$ οι οποίοι έχουν έναν τουλάχιστον κοινό παράγοντα $>1$ με τον $3600$.

6. Βρείτε όλους τους $n$ ώστε $\phi(n)=24$.

7. Αν οι $p, 2p-1$ είναι και οι δύο περιττοί πρώτοι και αν $n=2(2p-1)$, αποδείξτε ότι $\phi(n+2)=\phi(n)$.

8. Αν $m,n\ge 1$ και $m\mid n$, αποδείξτε ότι $\phi(m)\mid\phi(n)$.

9. Αν $m,n\ge 1$, αποδείξτε ότι:

$$(m,n)\phi(m)\phi(n)=\phi((m,n))\phi(mn),\qquad \phi(m)\phi(n)=\phi((m,n))\phi([m,n]).$$

10. Αποδείξτε ότι

    $\phi(n)\ge\frac{1}{2}\sqrt{n}$ για κάθε $n\ge 1$.
    $\tau(n)\phi(n)\ge n$ για κάθε $n\ge 1$.
    $\phi(n)\le n-\sqrt{n}$ για κάθε σύνθετο $n>1$.

11. Έστω αριθμοθεωρητική συνάρτηση $f$ και έστω ότι η $F$ ορίζεται με τον τύπο

$$F(n)=\sum_{d|n}f(d).$$

    Αποδείξτε την ταυτότητα:

$$\sum_{n=1}^{N}F(n)=\sum_{k=1}^{N}f(k)\Big[\frac{N}{k}\Big].$$

    Βάσει αυτής της ταυτότητας, αποδείξτε τις

$$\sum_{k=1}^{N}\mu(k)\Big[\frac{N}{k}\Big]=1,\qquad \sum_{k=1}^{N}\phi(k)\Big[\frac{N}{k}\Big]=\frac{N(N+1)}{2},\qquad \sum_{n=1}^{N}\tau(n)=\sum_{k=1}^{N}\Big[\frac{N}{k}\Big].$$

12. Έστω $n\ge 1$.
    Ένας μιγαδικός $\zeta$ ονομάζεται **$n$-οστή ρίζα της μονάδας** αν $\zeta^n=1$.
    Αποδείξτε ότι υπάρχουν ακριβώς $n$ διαφορετικές $n$-οστές ρίζες της μονάδας, οι:

$$1=e^{2\pi i\frac{0}{n}},\quad e^{2\pi i\frac{1}{n}},\quad e^{2\pi i\frac{2}{n}},\quad \ldots,\quad e^{2\pi i\frac{n-1}{n}}.$$

    Ο μιγαδικός $\zeta$ ονομάζεται **πρωταρχική $n$-οστή ρίζα της μονάδας** αν $\zeta^n=1$ και ο $n$ είναι ο ελάχιστος φυσικός $m$ ώστε $\zeta^m=1$.
    (Για παράδειγμα: οι τέσσερις τέταρτες ρίζες της μονάδας είναι οι $1,i,-1,-i$. Από αυτές, πρωταρχικές είναι μόνο οι $i,-i$.)
    Αποδείξτε ότι από τις $n$-οστές ρίζες της μονάδας $e^{2\pi i\frac{k}{n}}$ $(0\le k\le n-1)$ οι πρωταρχικές είναι μόνο εκείνες που αντιστοιχούν σε $k$ με $(k,n)=1$. Άρα το πλήθος των πρωταρχικών

$n$-οστών ριζών της μονάδας είναι ίσο με $\phi(n)$.
Ονομάζουμε **κυκλοτομικό πολυώνυμο τάξης** $n$ το πολυώνυμο

$$\Phi_n(x) = x^{\phi(n)} + \cdots = \prod_{0\le k\le n-1,(k,n)=1} \big(x - e^{2\pi i\frac{k}{n}}\big),$$

το οποίο έχει ως ρίζες τις πρωταρχικές $n$-οστές ρίζες της μονάδας.
Αποδείξτε ότι

$$\prod_{d|n} \Phi_d(x) = x^n - 1, \qquad \Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}.$$

Αποδείξτε ότι οι συντελεστές του $\Phi_n(x)$ είναι ακέραιοι.

## 6.5 Λύσεις ασκήσεων.

3. Η πρώτη ταυτότητα έχει μια πολύ απλή απόδειξη βασισμένη στην ταυτότητα (6.4):

$$n\sum_{d|n}\frac{1}{d} = \sum_{d|n}\frac{n}{d} = \sum_{d|n} d = \sigma(n).$$

Θα δούμε, όμως, και μια δεύτερη λύση.
Ορίζουμε την αριθμοθεωρητική συνάρτηση $F$ με τύπο

$$F(n) = \sum_{d|n}\frac{1}{d}.$$

Είναι προφανές ότι

$$F(1) = \sum_{d|1}\frac{1}{d} = 1 = \frac{\sigma(1)}{1}.$$

Έστω ότι ο $n$ είναι δύναμη πρώτου: $n = p^\alpha$ με πρώτο $p$ και $\alpha \ge 1$.
Οι θετικοί διαιρέτες του $p^\alpha$ είναι οι $1, p, \ldots, p^\alpha$, οπότε

$$F(p^\alpha) = 1 + \frac{1}{p} + \cdots + \frac{1}{p^\alpha} = \frac{1}{p^\alpha}\,\frac{p^{\alpha+1}-1}{p-1}.$$

Επειδή η συνάρτηση με τύπο $\frac{1}{n}$ είναι πολλαπλασιαστική, συνεπάγεται ότι και η $F$ είναι πολλαπλασιαστική. Άρα, αν $n > 1$ και ο $n$ έχει κανονική αναπαράσταση

$$n = p_1^{\alpha_1}\cdots p_k^{\alpha_k},$$

τότε

$$F(n) = F(p_1^{\alpha_1})\cdots F(p_k^{\alpha_k}) = \frac{1}{p_1^{\alpha_1}}\,\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{1}{p_k^{\alpha_k}}\,\frac{p_k^{\alpha_k+1}-1}{p_k-1} = \frac{\sigma(n)}{n}.$$

Για την απόδειξη της δεύτερης ταυτότητας ορίζουμε τις αριθμοθεωρητικές συναρτήσεις $F, G$ με τύπους

$$F(n) = \sum_{d|n}\sigma(d), \qquad G(n) = n\sum_{d|n}\frac{\tau(d)}{d}.$$

Η συνάρτηση $\sigma$ είναι πολλαπλασιαστική, οπότε και η $F$ είναι πολλαπλασιαστική. Επίσης, η $\tau$ είναι πολλαπλασιαστική και η συνάρτηση με τύπο $\frac{1}{n}$ είναι πολλαπλασιαστική. Άρα και η συνάρτηση με τύπο $\frac{\tau(n)}{n}$ είναι πολλαπλασιαστική, οπότε και η συνάρτηση με τύπο $\sum_{d|n}\frac{\tau(d)}{d}$ είναι πολλαπλασιαστική. Τέλος, επειδή η συνάρτηση με τύπο $n$ είναι πολλαπλασιαστική,

καταλήγουμε στο ότι το γινόμενο $G$ των δυο τελευταίων συναρτήσεων είναι πολλαπλασιαστική συνάρτηση.
Άρα οι συναρτήσεις $F, G$ είναι και οι δύο πολλαπλασιαστικές.
Άρα

$$F(1) = 1 = G(1).$$

Τώρα, έστω πρώτος $p$ και $\alpha \geq 1$. Θα αποδείξουμε ότι

$$F(p^\alpha) = G(p^\alpha). \tag{6.12}$$

Οι θετικοί διαιρέτες του $p^\alpha$ είναι οι $1, p, \ldots, p^\alpha$, οπότε

$$\begin{aligned} F(p^\alpha) &= \sigma(1) + \sigma(p) + \cdots + \sigma(p^\alpha) = 1 + \frac{p^2-1}{p-1} + \cdots + \frac{p^{\alpha+1}-1}{p-1} \\ &= \frac{p + p^2 + \cdots + p^{\alpha+1} - (\alpha+1)}{p-1}. \end{aligned} \tag{6.13}$$

Ομοίως,

$$\begin{aligned} G(p^\alpha) &= p^\alpha\Big(\frac{\tau(1)}{1} + \frac{\tau(p)}{p} + \cdots + \frac{\tau(p^\alpha)}{p^\alpha}\Big) = p^\alpha\Big(1 + \frac{2}{p} + \cdots + \frac{\alpha+1}{p^\alpha}\Big) \\ &= p^\alpha + 2p^{\alpha-1} + \cdots + (\alpha+1). \end{aligned} \tag{6.14}$$

Λόγω των (6.13), (6.14), η (6.12) είναι ισοδύναμη με την

$$p + p^2 + \cdots + p^{\alpha+1} - (\alpha+1) = (p-1)\big(p^\alpha + 2p^{\alpha-1} + \cdots + (\alpha+1)\big)$$

και (κάνοντας τον πολλαπλασιασμό στο δεξιό μέλος) αυτή είναι ισοδύναμη με την

$$p+p^2+\cdots+p^{\alpha+1}-(\alpha+1) = p^{\alpha+1}+2p^\alpha+\cdots+p(\alpha+1)-p^\alpha-2p^{\alpha-1}-\cdots-(\alpha+1),$$

η οποία είναι σωστή.
Άρα η (6.12) είναι σωστή.
Τώρα, αν $n > 1$ και ο $n$ έχει κανονική αναπαράσταση

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

τότε

$$F(n) = F(p_1^{\alpha_1}) \cdots F(p_k^{\alpha_k}) = G(p_1^{\alpha_1}) \cdots G(p_k^{\alpha_k}) = G(n).$$

# Κεφάλαιο 7

# Ισοτιμίες.

## 7.1 Ισοτιμίες.

**ΟΡΙΣΜΟΣ.** *Έστω* $m \geq 1$.
*Λέμε ότι ο* $a$ *είναι* **ισότιμος** $\bmod m$ *με τον* $b$ *αν*

$$m \mid a - b.$$

*Αυτό το συμβολίζουμε*

$$a \equiv b \,(\mathrm{mod}\, m).$$

*Αν* $m \nmid a - b$, *λέμε ότι ο* $a$ *είναι* **ανισότιμος** $\bmod m$ *με τον* $b$ *και γράφουμε* $a \not\equiv b \,(\mathrm{mod}\, m)$.

Έτσι ορίζεται μια σχέση ανάμεσα στους ακεραίους: η σχέση ισοτιμίας $\bmod m$. Η Πρόταση 7.1 λέει ότι η ισοτιμία $\bmod m$ είναι *σχέση ισοδυναμίας*.

**Πρόταση 7.1.** *Έστω* $m \geq 1$.
(i) $a \equiv a \,(\mathrm{mod}\, m)$.
(ii) $a \equiv b \,(\mathrm{mod}\, m) \;\Rightarrow\; b \equiv a \,(\mathrm{mod}\, m)$.
(iii) $a \equiv b \,(\mathrm{mod}\, m),\; b \equiv c \,(\mathrm{mod}\, m) \;\Rightarrow\; a \equiv c \,(\mathrm{mod}\, m)$.

*Απόδειξη.* (i) $m \mid 0 \;\Rightarrow\; m \mid a - a \;\Rightarrow\; a \equiv a \,(\mathrm{mod}\, m)$.
(ii) $a \equiv b \,(\mathrm{mod}\, m) \;\Rightarrow\; m \mid a - b \;\Rightarrow\; m \mid b - a \;\Rightarrow\; b \equiv a \,(\mathrm{mod}\, m)$.
(iii) $a \equiv b \,(\mathrm{mod}\, m),\; b \equiv c \,(\mathrm{mod}\, m) \;\Rightarrow\; m \mid a - b,\; m \mid b - c \;\Rightarrow\; m \mid (a - b) + (b - c) = a - c \;\Rightarrow\; a \equiv c \,(\mathrm{mod}\, m)$. □

Επομένως, ορίζονται κλάσεις ισοδυναμίας οι οποίες ονομάζονται **κλάσεις ισοτιμίας** $\bmod m$.

**ΟΡΙΣΜΟΣ.** *Έστω* $m \geq 1$. *Για κάθε* $a$ *ορίζουμε το σύνολο*

$$[a]_m = \{x \mid x \equiv a \,(\mathrm{mod}\, m)\}.$$

*Το σύνολο* $[a]_m$ *ονομάζεται* **κλάση ισοτιμίας** $\bmod m$ **με αντιπρόσωπο** $a$.

Επειδή $a \equiv a \,(\mathrm{mod}\, m)$, συνεπάγεται ότι

$$a \in [a]_m.$$

**Πρόταση 7.2.** *Έστω* $m \geq 1$.
(i) *Είτε* $[a]_m = [b]_m$, *το οποίο είναι ισοδύναμο με* $a \equiv b \,(\mathrm{mod}\, m)$, *είτε* $[a]_m \cap [b]_m = \emptyset$, *το οποίο είναι ισοδύναμο με* $a \not\equiv b \,(\mathrm{mod}\, m)$.
(ii) *Η ένωση των διαφόρων κλάσεων ισοτιμίας* $\bmod m$ *ισούται με ολόκληρο το* $\mathbb{Z}$.

*Απόδειξη.* (i) Έστω $[a]_m = [b]_m$.
Επειδή $a \in [a]_m$, συνεπάγεται $a \in [b]_m$, οπότε $a \equiv b \pmod m$.
Αντιστρόφως, έστω $a \equiv b \pmod m$.
Τότε για κάθε $x \in [a]_m$ ισχύει $x \equiv a \pmod m$, οπότε $x \equiv b \pmod m$ και άρα $x \in [b]_m$. Επίσης, για κάθε $x \in [b]_m$ ισχύει $x \equiv b \pmod m$, οπότε $x \equiv a \pmod m$ και άρα $x \in [a]_m$. Άρα $[a]_m = [b]_m$.
Τώρα έστω $[a]_m \cap [b]_m = \emptyset$.
Επειδή $a \in [a]_m$, συνεπάγεται $a \notin [b]_m$, οπότε $a \not\equiv b \pmod m$.
Αντιστρόφως, έστω $a \not\equiv b \pmod m$.
Αν υπήρχε $c \in [a]_m \cap [b]_m$, τότε θα ήταν $c \equiv a \pmod m$ και $c \equiv b \pmod m$, οπότε $a \equiv b \pmod m$ και θα καταλήγαμε σε άτοπο. Άρα $[a]_m \cap [b]_m = \emptyset$.
(ii) Για κάθε $a$ ισχύει $a \in [a]_m$. Άρα κάθε $a$ ανήκει σε κάποια κλάση ισοτιμίας $\bmod m$, οπότε η ένωση των διαφόρων κλάσεων ισοτιμίας $\bmod m$ ισούται με ολόκληρο το $\mathbb{Z}$. □

Επομένως, καταλήγουμε στα εξής συμπεράσματα:
(i) *Έστω $[a]_m$ οποιαδήποτε κλάση ισοτιμίας $\bmod m$ με αντιπρόσωπο $a$. Αν $b \notin [a]_m$, δηλαδή αν $b \not\equiv a \pmod m$, τότε η κλάση ισοτιμίας $\bmod m$ $[b]_m$ είναι ξένη με την $[a]_m$. Αν $b \in [a]_m$, δηλαδή αν $b \equiv a \pmod m$, τότε η κλάση ισοτιμίας $\bmod m$ $[b]_m$ ταυτίζεται με την $[a]_m$.*
*Άρα οποιοδήποτε στοιχείο μιας κλάσης ισοτιμίας $\bmod m$ μπορεί να θεωρηθεί αντιπρόσωπός της. Και, επίσης, δυο κλάσεις ισοτιμίας $\bmod m$ είτε ταυτίζονται είτε είναι ξένες.*
(ii) *Το $\mathbb{Z}$ διαμερίζεται ως ένωση ξένων ανά δύο κλάσεων ισοτιμίας $\bmod m$.*

Η Πρόταση 7.3 παρέχει πλήρη εικόνα των διαφόρων κλάσεων ισοτιμίας $\bmod m$.

**Πρόταση 7.3.** *Έστω $m \geq 1$.*
(i) *Κάθε $a$ είναι ισότιμος $\bmod m$ με το υπόλοιπο της διαίρεσής του από το $m$.*
(ii) *Οι $a, b$ είναι ισότιμοι $\bmod m$ αν και μόνο αν δίνουν το ίδιο υπόλοιπο όταν διαιρεθούν από το $m$.*
(iii) *Υπάρχουν ακριβώς $m$ διαφορετικές, και άρα ξένες ανά δύο, κλάσεις ισοτιμίας $\bmod m$. Αυτές είναι οι:*

$$[0]_m,\ [1]_m,\ \ldots\ ,\ [m-1]_m.$$

*Απόδειξη.* (i) Αν $a = qm + r,\ 0 \leq r < m$, τότε $m \mid a - r$, οπότε $a \equiv r \pmod m$.
(ii) Έστω ότι οι $a, b$ δίνουν το ίδιο υπόλοιπο $r$ όταν διαιρεθούν από το $m$. Βάσει του (i), οι $a, b$ είναι ισότιμοι $\bmod m$ με το $r$, οπότε είναι μεταξύ τους ισότιμοι $\bmod m$.
Αντιστρόφως, έστω ότι οι $a, b$ είναι ισότιμοι $\bmod m$. Αν $r_1$ είναι το υπόλοιπο της διαίρεσης του $a$ από τον $m$ και $r_2$ είναι το υπόλοιπο της διαίρεσης του $b$ από τον $m$, τότε, βάσει του (i), οι $r_1, r_2$ είναι ισότιμοι $\bmod m$. Άρα $m \mid r_1 - r_2$ και, επειδή $-m < r_1 - r_2 < m$, συνεπάγεται ότι $r_1 - r_2 = 0$ και άρα $r_1 = r_2$.
(iii) Οι $0, 1, \ldots, m-1$ αφήνουν τους εαυτούς τους ως υπόλοιπα όταν διαιρεθούν από το $m$, οπότε, βάσει του (ii), είναι ανισότιμοι $\bmod m$ ανά δύο. Άρα οι αντίστοιχες κλάσεις ισοτιμίας $\bmod m$ είναι διαφορετικές και άρα ξένες ανά δύο.
Επίσης, βάσει του (i), κάθε αριθμός ανήκει σε μία από αυτές τις κλάσεις ισοτιμίας $\bmod m$, οπότε δεν υπάρχουν άλλες κλάσεις ισοτιμίας $\bmod m$. □

**Παράδειγμα.** Υπάρχουν ακριβώς 6 κλάσεις ισοτιμίας $\bmod 6$. Αυτές είναι οι

$$[0]_6,\ [1]_6,\ [2]_6,\ [3]_6,\ [4]_6,\ [5]_6.$$

Κάθε άλλη κλάση ισοτιμίας $\bmod 6$ ταυτίζεται με κάποια από αυτές. Για παράδειγμα η $[635]_6$ ταυτίζεται με την $[5]_6$, αφού $635 = 105 \cdot 6 + 5$ και άρα $635 \equiv 5 \pmod 6$.

Η Πρόταση 7.4 περιγράφει μερικές βασικές ιδιότητες της ισοτιμίας $\bmod m$.

**Πρόταση 7.4.** *Έστω $m \geq 1$.*
(i) $a \equiv b \pmod m,\ c \equiv d \pmod m\ \Rightarrow\ a \pm c \equiv b \pm d \pmod m,\ ac \equiv bd \pmod m$.

(ii) *Αν* $d \geq 1$, *τότε:* $a \equiv b \,(\mathrm{mod}\, m) \;\Leftrightarrow\; ad \equiv bd \,(\mathrm{mod}\, md)$.

(iii) $a \equiv b \,(\mathrm{mod}\, m),\ d \mid m \;\Rightarrow\; a \equiv b \,(\mathrm{mod}\, d)$.

(iv) $ad \equiv bd \,(\mathrm{mod}\, m) \;\Rightarrow\; a \equiv b \,(\mathrm{mod}\, \frac{m}{(m,d)})$.

*Ειδικώτερα, αν* $(m, d) = 1$, *τότε:* $ad \equiv bd \,(\mathrm{mod}\, m) \;\Rightarrow\; a \equiv b \,(\mathrm{mod}\, m)$.

(v) *Αν οι* $m_1, \ldots, m_k$ *είναι ανά δύο σχετικά πρώτοι:* $a \equiv b \,(\mathrm{mod}\, m_1), \ldots, a \equiv b \,(\mathrm{mod}\, m_k) \;\Leftrightarrow$ $a \equiv b \,(\mathrm{mod}\, m_1 \cdots m_k)$.

(vi) $a \equiv b \,(\mathrm{mod}\, m) \;\Rightarrow\; (a, m) = (b, m)$.

*Απόδειξη.* (i) $a \equiv b \,(\mathrm{mod}\, m),\ c \equiv d \,(\mathrm{mod}\, m) \;\Rightarrow\; m \mid a - b,\ m \mid c - d \;\Rightarrow m \mid (a - b) \pm (c - d),\ m \mid (a - b)c + (c - d)b \;\Rightarrow\; m \mid (a \pm c) - (b \pm d),\ m \mid ac - bd \;\Rightarrow\; a \pm c \equiv b \pm d \,(\mathrm{mod}\, m),\ ac \equiv bd \,(\mathrm{mod}\, m)$.

(ii) $a \equiv b \,(\mathrm{mod}\, m) \;\Leftrightarrow\; m \mid a - b \;\Leftrightarrow\; md \mid (a - b)d = ad - bd \;\Leftrightarrow\; ad \equiv bd \,(\mathrm{mod}\, md)$.

(iii) $a \equiv b \,(\mathrm{mod}\, m),\ d \mid m \;\Rightarrow\; m \mid a - b,\ d \mid m \;\Rightarrow\; d \mid a - b \;\Rightarrow\; a \equiv b \,(\mathrm{mod}\, d)$.

(iv) Έστω $ad \equiv bd \,(\mathrm{mod}\, m)$, οπότε $m \mid ad - bd = (a - b)d$.
Θέτουμε $m_1 = \frac{m}{(m,d)}$, $d_1 = \frac{d}{(m,d)}$, οπότε $(m_1, d_1) = 1$.
Από την $m \mid (a - b)d$ συνεπάγεται $m_1 \mid (a - b)d_1$ και άρα $m_1 \mid a - b$.
Επομένως $a \equiv b \,(\mathrm{mod}\, m_1)$.

(v) Έστω $a \equiv b \,(\mathrm{mod}\, m_1)$ και $a \equiv b \,(\mathrm{mod}\, m_2)$. Τότε $m_1 \mid a - b$ και $m_2 \mid a - b$. Άρα $[m_1, m_2] \mid a - b$. Επειδή $(m_1, m_2) = 1$, είναι $[m_1, m_2] = m_1 m_2$ και, επομένως, $m_1 m_2 \mid a - b$. Άρα $a \equiv b \,(\mathrm{mod}\, m_1 m_2)$.
Από $(m_1, m_3) = (m_2, m_3) = 1$ και από το Λήμμα 6.1 συνεπάγεται ότι $(m_1 m_2, m_3) = 1$.
Άρα, όπως από τις $a \equiv b \,(\mathrm{mod}\, m_1)$ και $a \equiv b \,(\mathrm{mod}\, m_2)$ συμπεράναμε ότι $a \equiv b \,(\mathrm{mod}\, m_1 m_2)$, έτσι και από τις $a \equiv b \,(\mathrm{mod}\, m_1 m_2)$ και $a \equiv b \,(\mathrm{mod}\, m_3)$ συμπεραίνουμε ότι $a \equiv b \,(\mathrm{mod}\, m_1 m_2 m_3)$.
Τώρα είναι φανερό ότι, επαγωγικά, καταλήγουμε στο ότι $a \equiv b \,(\mathrm{mod}\, m_1 \cdots m_k)$.

(vi) Έστω $a \equiv b \,(\mathrm{mod}\, m)$. Τότε τα $a, b$ δίνουν το ίδιο υπόλοιπο $r$ όταν διαιρεθούν από το $m$.
Συνεπάγεται $(a, m) = (r, m)$ και $(b, m) = (r, m)$, οπότε $(a, m) = (b, m)$. □

Σχόλια. 1. Το (i) της Πρότασης 7.4 συνεπάγεται ότι, αν σε οποιαδήποτε αλγεβρική παράσταση αριθμών, συνδυασμένων με προσθέσεις, αφαιρέσεις και πολλαπλασιασμούς, αντικαταστήσουμε αριθμούς με ισότιμους $\mathrm{mod}\, m$ αριθμούς, τότε το αποτέλεσμα θα είναι ισότιμο $\mathrm{mod}\, m$ με το προηγούμενο.

2. Το (ii) λέει ότι μπορούμε να πολλαπλασιάσουμε ή να διαιρέσουμε μια ισοτιμία $\mathrm{mod}\, m$ με έναν θετικό αριθμό χωρίς να αλλάξει η ισοτιμία, *αρκεί να πολλαπλασιάσουμε ή διαιρέσουμε και το* $m$ *με τον ίδιο αριθμό.*

3. Το (iii) λέει ότι μια ισοτιμία $\mathrm{mod}\, m$ δεν χαλάει αν αντικαταστήσουμε το $m$ με οποιονδήποτε θετικό διαιρέτη του.

4. Το (iv) περιγράφει την αλλαγή που πρέπει να υποστεί ο $m$ ώστε να διαιρέσουμε μια ισοτιμία $\mathrm{mod}\, m$ με έναν θετικό αριθμό.
Ειδικώτερα, *αν* $(m, d) = 1$, *τότε μια ισοτιμία* $\mathrm{mod}\, m$ *μπορεί να διαιρεθεί με τον* $d$ *χωρίς να χρειάζεται να μεταβληθεί ο* $m$.

5. Το (v) περιγράφει έναν τρόπο χειρισμού ισοτιμιών με διάφορα $m_1, \ldots, m_k$ ώστε όλες μαζί να αναχθούν σε μία ισοτιμία.

6. Το (vi) λέει ότι ισότιμοι $\mathrm{mod}\, m$ αριθμοί έχουν τον ίδιο μέγιστο κοινό διαιρέτη με το $m$. Άρα όλοι οι αριθμοί που ανήκουν σε μία κλάση ισοτιμίας $\mathrm{mod}\, m$ έχουν τον ίδιο μέγιστο κοινό διαιρέτη με τον $m$.

## 7.2 Πλήρη και περιορισμένα σύνολα υπολοίπων.

Έστω $m \geq 1$. Είδαμε ότι υπάρχουν ακριβώς $m$ κλάσεις ισοτιμίας mod $m$, οι:

$$[0]_m,\ [1]_m,\ \ldots\ ,\ [m-1]_m. \tag{7.1}$$

Ας επιλέξουμε $m$ αριθμούς, τους

$$a_1,\ a_2,\ \ldots\ ,\ a_m \tag{7.2}$$

έναν από κάθε κλάση ισοτιμίας mod $m$ (με οποιαδήποτε σειρά). Οι αριθμοί αυτοί είναι, προφανώς, ανά δύο ανισότιμοι mod $m$. Επίσης, αν πάρουμε οποιονδήποτε άλλον αριθμό $a$, τότε ο $a$ ανήκει σε μία από τις κλάσεις ισοτιμίας mod $m$ (7.1) και, επομένως, είναι ισότιμος mod $m$ με κάποιον από τους αριθμούς (7.2). Ένα σύνολο αριθμών, όπως το (7.2), έχει ιδιαίτερο όνομα.

**ΟΡΙΣΜΟΣ.** *Έστω $m \geq 1$.*
*Ένα σύνολο $m$ αριθμών $\{a_1, \ldots, a_m\}$ χαρακτηρίζεται* **πλήρες σύνολο υπολοίπων** mod $m$ *αν τα στοιχεία του είναι ανά δύο ανισότιμα* mod $m$.

Αν το $\{a_1, \ldots, a_m\}$ είναι ένα πλήρες σύνολο υπολοίπων mod $m$, τότε τα στοιχεία του, επειδή είναι ανά δύο ανισότιμα mod $m$, ανήκουν ένα σε καθεμία κλάση ισοτιμίας mod $m$ από τις (7.1) και, επομένως, κάθε άλλος αριθμός είναι ισότιμος mod $m$ με ένα από αυτά. Φυσικά, ένα απλό πλήρες σύνολο υπολοίπων mod $m$ είναι το $\{0, \ldots, m-1\}$.

**Παράδειγμα.** Έστω $m \geq 1$. Ένα σύνολο, του οποίου τα στοιχεία είναι $m$ διαδοχικοί ακέραιοι, είναι πλήρες σύνολο υπολοίπων mod $m$.
Πράγματι, οι αριθμοί $a, a+1, \ldots, a+(m-1)$ είναι ανά δύο ανισότιμοι mod $m$. Διότι δυο τέτοιοι αριθμοί διαφέρουν κατά αριθμό $k$ με $0 < k < m$ και, επομένως, η διαφορά $k$ δεν διαιρείται από τον $m$.

**Παράδειγμα.** Το $\{0, 1, 2, 3, 4, 5, \}$ είναι το προφανές πλήρες σύνολο υπολοίπων mod 6.
Ένα άλλο τέτοιο σύνολο είναι το $\{-2, -1, 0, 1, 2, 3\}$, το οποίο αποτελείται από 6 διαδοχικούς αριθμούς.
Επειδή οι $85, 28, -7, -3, 20, 36$ είναι ανά δύο ανισότιμοι mod 6, το $\{85, 28, -7, -3, 20, 36\}$ είναι ένα πλήρες σύνολο υπολοίπων mod 6.

Είδαμε στο σχόλιο 6 μετά από την Πρόταση 7.4 ότι όλοι οι αριθμοί που ανήκουν σε μία κλάση ισοτιμίας mod $m$ έχουν τον ίδιο μέγιστο κοινό διαιρέτη με τον $m$. Ειδικώτερα, είτε όλοι οι αριθμοί που ανήκουν σε μία κλάση ισοτιμίας mod $m$ είναι σχετικά πρώτοι με τον $m$ είτε κανένας από τους αριθμούς που ανήκουν σε μία κλάση ισοτιμίας mod $m$ δεν είναι σχετικά πρώτος με τον $m$. Τώρα, αν θεωρήσουμε ένα πλήρες σύνολο υπολοίπων mod $m$ $\{a_1, \ldots, a_m\}$, τότε οι αριθμοί που το αποτελούν είναι ισότιμοι mod $m$ με τους αριθμούς $0, \ldots, m-1$ και, επειδή ακριβώς $\phi(m)$ από αυτούς είναι σχετικά πρώτοι με τον $m$, συμπεραίνουμε ότι ακριβώς $\phi(m)$ από τους $a_1, \ldots, a_m$ είναι σχετικά πρώτοι με τον $m$.

**ΟΡΙΣΜΟΣ.** *Έστω $m \geq 1$.*
*Ένα σύνολο αριθμών $\{b_1, \ldots, b_{\phi(m)}\}$ χαρακτηρίζεται* **περιορισμένο σύνολο υπολοίπων** mod $m$ *αν τα στοιχεία του είναι ανά δύο ανισότιμα* mod $m$ *και είναι σχετικά πρώτα με τον $m$.*

Όπως είδαμε πριν από τον τελευταίο ορισμό, κάθε πλήρες σύνολο υπολοίπων mod $m$ περιέχει ένα περιορισμένο σύνολο υπολοίπων mod $m$. Ένα πλήρες σύνολο υπολοίπων mod $m$ περιέχει πάντοτε $m$ αριθμούς και ένα περιορισμένο σύνολο υπολοίπων mod $m$ περιέχει πάντοτε $\phi(m)$ αριθμούς.

**Παράδειγμα.** Έστω $m = 6$. Το πλήρες σύνολο υπολοίπων $\{0, 1, 2, 3, 4, 5\}$ περιέχει το περιορισμένο σύνολο υπολοίπων $\{1, 5\}$. Το πλήρες σύνολο υπολοίπων $\{-2, -1, 0, 1, 2, 3\}$ περιέχει το περιορισμένο σύνολο υπολοίπων $\{1, -1\}$. Το πλήρες σύνολο υπολοίπων $\{85, 28, -7, -3, 20, 36\}$ περιέχει το περιορισμένο σύνολο υπολοίπων $\{85, -7\}$.

**Πρόταση 7.5.** *Έστω* $m \geq 1$ *και* $(m, d) = 1$.
(i) *Αν το* $\{a_1, \ldots, a_m\}$ *είναι πλήρες σύνολο υπολοίπων* mod $m$*, το* $\{da_1 + l, \ldots, da_m + l\}$ *είναι πλήρες σύνολο υπολοίπων* mod $m$.
(ii) *Αν το* $\{a_1, \ldots, a_{\phi(m)}\}$ *είναι περιορισμένο σύνολο υπολοίπων* mod $m$*, το* $\{da_1, \ldots, da_{\phi(m)}\}$ *είναι περιορισμένο σύνολο υπολοίπων* mod $m$.

*Απόδειξη.* (i) Αρκεί να αποδείξουμε ότι οι $da_1 + l, \ldots, da_m + l$ είναι ανά δύο ανισότιμοι mod $m$. Λόγω της Πρότασης 7.4(i)(iv) έχουμε:

$$da_i + l \equiv da_j + l \,(\text{mod}\, m) \;\Rightarrow\; da_i \equiv da_j \,(\text{mod}\, m) \;\Rightarrow\; a_i \equiv a_j \,(\text{mod}\, m) \;\Rightarrow\; i = j.$$

(ii) Αρκεί να αποδείξουμε ότι οι $da_1, \ldots, da_{\phi(m)}$ είναι ανά δύο ανισότιμοι mod $m$ και σχετικά πρώτοι με τον $m$.
Το πρώτο έχει αποδειχθεί στο (i). Όσο για το δεύτερο, λόγω του Λήμματος 6.1, έχουμε

$$(d, m) = 1,\ (a_i, m) = 1 \;\Rightarrow\; (da_i, m) = 1.$$

□

Τώρα θα δούμε μια δεύτερη απόδειξη του ότι η συνάρτηση $\phi$ του Euler είναι πολλαπλασιαστική.

**Θεώρημα 6.2.** *Η συνάρτηση* $\phi$ *είναι πολλαπλασιαστική.*

*Απόδειξη.* Είναι προφανές ότι $\phi(1) = 1$.
Έστω $m, n \geq 1$ με $(m, n) = 1$.
Θεωρούμε ένα περιορισμένο σύνολο υπολοίπων mod $m$ και ένα περιορισμένο σύνολο υπολοίπων mod $n$:

$$A = \{a_1, \ldots, a_{\phi(m)}\}, \qquad B = \{b_1, \ldots, b_{\phi(n)}\},$$

αντιστοίχως.
Κατόπιν, θεωρούμε το σύνολο

$$K = \{na + mb \,|\, a \in A, b \in B\}.$$

Θα αποδείξουμε: (i) ότι τα στοιχεία του $K$ είναι ανά δύο ανισότιμα mod $mn$, (ii) ότι τα στοιχεία του $K$ είναι σχετικά πρώτα με το $mn$ και (iii) ότι κάθε αριθμός σχετικά πρώτος με το $mn$ είναι ισότιμος mod $mn$ με ένα από τα στοιχεία του $K$.
Τα (i), (ii), (iii) λένε ότι το $K$ είναι ένα περιορισμένο σύνολο υπολοίπων mod $mn$ και, επομένως, το πλήθος των στοιχείων του είναι ίσο με $\phi(mn)$. Από την άλλη μεριά, το πλήθος των στοιχείων του $K$ είναι $\phi(m)\phi(n)$, διότι έχουμε $\phi(m)$ επιλογές για το $a$ και $\phi(n)$ επιλογές για το $b$. Έτσι θα έχουμε αποδείξει την ισότητα $\phi(mn) = \phi(m)\phi(n)$.
(i) Έστω $a', a'' \in A$ και $b', b'' \in B$. Τότε, σύμφωνα με την Πρόταση 7.4:

$$\begin{aligned} na' + mb' \equiv na'' + mb'' \,(\text{mod}\, mn) \;&\Rightarrow\; na' + mb' \equiv na'' + mb'' \,(\text{mod}\, m) \\ &\Rightarrow\; na' \equiv na'' \,(\text{mod}\, m) \;\Rightarrow\; a' \equiv a'' \,(\text{mod}\, m) \;\Rightarrow\; a' = a''. \end{aligned}$$

Ομοίως:

$$\begin{aligned} na' + mb' \equiv na'' + mb'' \,(\text{mod}\, mn) \;&\Rightarrow\; na' + mb' \equiv na'' + mb'' \,(\text{mod}\, n) \\ &\Rightarrow\; mb' \equiv mb'' \,(\text{mod}\, n) \;\Rightarrow\; b' \equiv b'' \,(\text{mod}\, n) \;\Rightarrow\; b' = b''. \end{aligned}$$

Άρα τα στοιχεία του $K$ είναι ανά δύο ανισότιμα mod $mn$.
(ii) Από τα Λήμματα 3.1 και 6.1 έχουμε

$$(na + mb, m) = (na, m) = 1, \qquad (na + mb, n) = (mb, n) = 1$$

για κάθε $a \in A, b \in B$ και, πάλι από το Λήμμα 6.1,

$$(na + mb, mn) = 1.$$

Άρα τα στοιχεία του $K$ είναι σχετικά πρώτα με το $mn$.
(iii) Τέλος, έστω $(k, mn) = 1$.
Επειδή $(m, n) = 1$, από το Θεώρημα 5.1 ή το Θεώρημα 5.2 συνεπάγεται ότι υπάρχουν $a', b'$ ώστε

$$na' + mb' = k.$$

Αν $d \mid a'$ και $d \mid m$, τότε $d \mid k$ και, επειδή $(k, m) = 1$, συνεπάγεται $d = \pm 1$. Άρα $(a', m) = 1$. Ομοίως, $(b', n) = 1$.
Επειδή το $A$ είναι περιορισμένο σύνολο υπολοίπων mod $m$, υπάρχει $a \in A$ ώστε $a' \equiv a \,(\mathrm{mod}\, m)$ και άρα

$$na' \equiv na \,(\mathrm{mod}\, mn).$$

Ομοίως, υπάρχει $b \in B$ ώστε $b' \equiv b \,(\mathrm{mod}\, n)$ και άρα

$$mb' \equiv mb \,(\mathrm{mod}\, mn).$$

Συνεπάγεται ότι

$$k = na' + mb' \equiv na + mb \,(\mathrm{mod}\, mn).$$

Άρα κάθε $k$ σχετικά πρώτο με το $mn$ είναι ισότιμο mod $mn$ με κάποιο στοιχείο του $K$. □

## 7.3 Τα Θεωρήματα των Euler, Fermat, Wilson.

**Θεώρημα του Euler.** *Έστω $m \geq 1$. Αν $(a, m) = 1$, τότε*

$$a^{\phi(m)} \equiv 1 \,(\mathrm{mod}\, m).$$

*Απόδειξη.* Θεωρούμε ένα περιορισμένο σύνολο υπολοίπων mod $m$:

$$\{a_1, \ldots, a_{\phi(m)}\}.$$

Σύμφωνα με την Πρόταση 7.5(ii), το

$$\{aa_1, \ldots, aa_{\phi(m)}\}$$

είναι κι αυτό περιορισμένο σύνολο υπολοίπων mod $m$.
Άρα κάθε στοιχείο του δεύτερου συνόλου είναι ισότιμο mod $m$ με ακριβώς ένα στοιχείο του πρώτου συνόλου. Πολλαπλασιάζοντας τις ισοτιμίες και χρησιμοποιώντας την Πρόταση 7.4(i), έχουμε ότι

$$(aa_1) \cdots (aa_{\phi(m)}) \equiv a_1 \cdots a_{\phi(m)} \,(\mathrm{mod}\, m)$$

ή, ισοδύναμα,

$$a^{\phi(m)} a_1 \cdots a_{\phi(m)} \equiv a_1 \cdots a_{\phi(m)} \,(\mathrm{mod}\, m).$$

Επειδή $(a_j, m) = 1$ για κάθε $j$, από το Λήμμα 6.1 συνεπάγεται ότι

$$(a_1 \cdots a_{\phi(m)}, m) = 1.$$

Άρα

$$a^{\phi(m)} \equiv 1 \,(\mathrm{mod}\, m),$$

βάσει της Πρότασης 7.4(iv). □

**Θεώρημα του Fermat.** *Έστω πρώτος $p$.*
(i) *Αν $p \nmid a$, τότε*

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\, p).$$

(i) *Για κάθε $a$:*

$$a^p \equiv a \,(\mathrm{mod}\, p).$$

*Απόδειξη.* (i) Αν $p \nmid a$, συνεπάγεται $(a, p) = 1$ και το αποτέλεσμα είναι άμεση συνέπεια του Θεωρήματος του Euler.
(ii) Αν $p \nmid a$, τότε από το (i) έχουμε $a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$, οπότε $a^p \equiv a \,(\mathrm{mod}\, p)$.
Αν $p \mid a$, τότε $a \equiv 0 \,(\mathrm{mod}\, p)$ και $a^p \equiv 0 \,(\mathrm{mod}\, p)$, οπότε $a^p \equiv a \,(\mathrm{mod}\, p)$. □

**Θεώρημα του Wilson.** *Αν ο $p$ είναι πρώτος, τότε*

$$(p-1)! \equiv -1 \,(\mathrm{mod}\, p).$$

*Απόδειξη.* Το σύνολο

$$\{1, 2, \ldots, p-1\}$$

είναι περιορισμένο σύνολο υπολοίπων $\mathrm{mod}\, p$.
Αν $a$ είναι οποιοδήποτε στοιχείο αυτού του συνόλου, από την Πρόταση 7.5(ii) συνεπάγεται ότι και το

$$\{a, a2, \ldots, a(p-1)\}$$

είναι περιορισμένο σύνολο υπολοίπων $\mathrm{mod}\, p$.
Άρα ακριβώς ένα στοιχείο του δεύτερου συνόλου είναι ισότιμο $\mathrm{mod}\, p$ με το 1.
Αποδείξαμε, λοιπόν, ότι για κάθε $a \in \{1, \ldots, p-1\}$ υπάρχει ακριβώς ένα $b \in \{1, \ldots, p-1\}$ ώστε

$$ab \equiv 1 \,(\mathrm{mod}\, p).$$

Είναι δυνατόν να έχουμε $a = b$; Κάτι τέτοιο ισοδυναμεί με

$$a^2 \equiv 1 \,(\mathrm{mod}\, p) \;\Leftrightarrow\; p \mid a^2 - 1 \;\Leftrightarrow\; p \mid a-1 \text{ ή } p \mid a+1 \;\Leftrightarrow\; a = 1 \text{ ή } a = p-1.$$

Συμπεραίνουμε ότι για κάθε $a \in \{2, \ldots, p-2\}$ υπάρχει ακριβώς ένα $b \in \{2, \ldots, p-2\}$ ώστε

$$ab \equiv 1 \,(\mathrm{mod}\, p), \quad a \neq b.$$

Άρα οι αριθμοί $2, \ldots, p-2$ χωρίζονται σε $\frac{p-3}{2}$ ζευγάρια ώστε το γινόμενο των δυο αριθμών του κάθε ζευγαριού να είναι ισότιμο $\mathrm{mod}\, p$ με το 1 και, επομένως,

$$2 \cdots (p-2) \equiv 1 \,(\mathrm{mod}\, p)$$

και, τελικά,

$$(p-1)! = 1 \cdot 2 \cdots (p-2) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \,(\mathrm{mod}\, p).$$

□

**Παραδείγματα.** (i) Αν ο $a$ είναι περιττός, τότε $a^8 \equiv 1 \,(\mathrm{mod}\, 16)$.
(ii) Αν $7 \nmid a$, τότε $a^6 \equiv 1 \,(\mathrm{mod}\, 7)$.
(iii) $a^7 \equiv a \,(\mathrm{mod}\, 7)$.
(iv) $10! \equiv -1 \,(\mathrm{mod}\, 11)$.

## 7.4 Πολυωνυμικές ισοτιμίες.

Θεωρούμε έναν $m \geq 1$ και ένα πολυώνυμο με ακέραιους συντελεστές με τύπο

$$f(x) = c_n x^n + \cdots + c_1 x + c_0.$$

Μα ενδιαφέρουν οι ακέραιες λύσεις, αν υπάρχουν, της πολυωνυμικής ισοτιμίας $\bmod m$

$$f(x) \equiv 0 \,(\bmod m). \tag{7.3}$$

**ΟΡΙΣΜΟΣ.** *Λέμε ότι τα δυο πολυώνυμα $f, g$ με ακέραιους συντελεστές* **ταυτίζονται** $\bmod m$ *αν ισχύει $f(x) \equiv g(x) \,(\bmod m)$ για κάθε $x$.*

**Πρόταση 7.6.** *Αν $f(x) = c_n x^n + \cdots + c_1 x + c_0$ και $g(x) = d_n x^n + \cdots + d_1 x + d_0$ και αν $c_j \equiv d_j \,(\bmod m)$ για κάθε $j$, τότε τα $f, g$ ταυτίζονται* $\bmod m$.

*Απόδειξη.* Προφανής, λόγω της Πρότασης 7.4(i). □

Το αντίστροφο της Πρότασης 7.6 δεν ισχύει.

**Παράδειγμα.** Τα πολυώνυμα $f(x) = x^5$ και $g(x) = x$ ταυτίζονται $\bmod 5$, λόγω του Θεωρήματος του Fermat.

**Πρόταση 7.7.** *Αν το $f$ είναι πολυώνυμο με ακέραιους συντελεστές και αν $x_1 \equiv x_2 \,(\bmod m)$, τότε $f(x_1) \equiv f(x_2) \,(\bmod m)$.*

*Απόδειξη.* Προφανής, λόγω της Πρότασης 7.4(i). □

Επομένως, αν $\xi$ είναι μια λύση της (7.3), τότε κάθε $\eta$ με $\eta \equiv \xi \,(\bmod m)$ είναι, επίσης, λύση της (7.3). Με άλλη διατύπωση: αν ένας αντιπρόσωπος μιας κλάσης ισοτιμίας $\bmod m$ είναι λύση της (7.3), τότε κάθε άλλος αντιπρόσωπος της ίδιας κλάσης ισοτιμίας $\bmod m$ είναι, επίσης, λύση της (7.3).

**ΟΡΙΣΜΟΣ.** *Δυο λύσεις της (7.3) χαρακτηρίζονται διαφορετικές* $\bmod m$ *αν είναι ανισότιμες* $\bmod m$.

Επομένως, όταν ψάχνουμε για τις λύσεις της (7.3) αρκεί να περιοριστούμε σε ένα πλήρες σύνολο υπολοίπων $\bmod m$

$$\{a_1, \ldots, a_m\}$$

και να βρούμε τα στοιχεία του τα οποία είναι λύσεις της (7.3): αυτά τα στοιχεία είναι λύσεις της (7.3) διαφορετικές $\bmod m$ και δεν υπάρχει λύση της (7.3) διαφορετική $\bmod m$ από αυτές και άρα το πρόβλημα της (7.3) θα είναι λυμένο.

**Παράδειγμα.** Η $x^2 - 1 \equiv 0 \,(\bmod 4)$ έχει δυο ακριβώς λύσεις, τις $1, 3$, στο πλήρες σύνολο υπολοίπων $\bmod 4$ $\{0, 1, 2, 3\}$. Επίσης, έχει δυο ακριβώς λύσεις, τις $5, 7$, στο πλήρες σύνολο υπολοίπων $\bmod 4$ $\{5, 6, 7, 8\}$. Οι $1, 3$ είναι διαφορετικές $\bmod 4$ και οι $5, 7$ είναι διαφορετικές $\bmod 4$. Αλλά οι $1, 5$ είναι ίδιες $\bmod 4$ και οι $3, 7$ είναι ίδιες $\bmod 4$.
Για κάθε λύση $x$ της $x^2 - 1 \equiv 0 \,(\bmod 4)$ έχουμε είτε $x \equiv 1 \,(\bmod 4)$ είτε $x \equiv 3 \,(\bmod 4)$ και, επομένως, οι λύσεις είναι είτε της μορφής $x = 4q + 1$ είτε της μορφής $x = 4q + 3$.

**Παράδειγμα.** Η $x^2 - 1 \equiv 0 \,(\bmod 8)$ έχει τέσσερις ακριβώς λύσεις, τις $1, 3, 5, 7$, στο πλήρες σύνολο υπολοίπων $\bmod 8$ $\{0, 1, 2, 3, 4, 5, 6, 7\}$. Κάθε άλλη λύση είναι ισότιμη $\bmod 8$ με ακριβώς μία από αυτές.

**ΟΡΙΣΜΟΣ.** *Αν $f(x) = c_n x^n + \cdots + c_1 x + c_0$ και $c_n \not\equiv 0 \,(\bmod m)$, τότε ο $n$ χαρακτηρίζεται* **βαθμός** $\bmod m$ *του πολυωνύμου $f$.*

Προσοχή: μπορεί δυο πολυώνυμα με ακέραιους συντελεστές να ταυτίζονται $\bmod m$ αλλά να μην έχουν το ίδιο βαθμό $\bmod m$.

**Παράδειγμα.** Και πάλι έχουμε το παράδειγμα των πολυωνύμων $f(x) = x^5$ και $g(x) = x$, τα οποία ταυτίζονται $\bmod 5$, λόγω του Θεωρήματος του Fermat.

**Θεώρημα 7.1.** *Αν ο $p$ είναι πρώτος και το πολυώνυμο $f$ έχει βαθμό $\bmod p$ ίσο με $n$, τότε η*

$$f(x) \equiv 0 \,(\bmod p) \tag{7.4}$$

*έχει το πολύ $n$ λύσεις διαφορετικές $\bmod p$.*

*Απόδειξη.* Έστω $n = 1$, οπότε

$$f(x) = c_1 x + c_0, \qquad p \nmid c_1.$$

Αν το $x$ διατρέχει ένα πλήρες σύνολο υπολοίπων $\bmod p$, τότε από την Πρόταση 7.5(i) συνεπάγεται ότι το $f(x) = c_1 x + c_0$ διατρέχει, επίσης, ένα πλήρες σύνολο υπολοίπων $\bmod p$ και, επομένως, υπάρχει ακριβώς μία τιμή του $x$ για την οποία το $f(x)$ είναι ισότιμο $\bmod p$ με το $0$.
Τώρα, υποθέτουμε ότι το συμπέρασμα που θέλουμε να αποδείξουμε ισχύει για πολυώνυμα βαθμού $\bmod p$ ίσου με $n-1$ και έστω πολυώνυμο $f$ με βαθμό $\bmod p$ ίσο με $n$. Δηλαδή, έστω

$$f(x) = c_n x^n + \cdots + c_1 x + c_0, \qquad p \nmid c_n.$$

Αν η (7.4) δεν έχει καμία λύση, έχουμε τελειώσει. Έστω, λοιπόν, ότι $\xi$ είναι μια λύση της (7.4), οπότε

$$f(\xi) \equiv 0 \,(\bmod p).$$

Τότε, για κάθε τιμή του $x$ έχουμε:

$$\begin{aligned} f(x) &\equiv f(x) - f(\xi) \,(\bmod p) \\ &\equiv (c_n x^n + \cdots + c_1 x + c_0) - (c_n \xi^n + \cdots + c_1 \xi + c_0) \,(\bmod p) \\ &\equiv c_n (x^n - \xi^n) + \cdots + c_1 (x - \xi) \,(\bmod p) \\ &\equiv (x - \xi)(c_n x^{n-1} + \cdots) \,(\bmod p), \end{aligned}$$

όπου οι τελείες στην τελευταία παρένθεση δηλώνουν όρους με δυνάμεις του $x$ με εκθέτη $< n-1$. Άρα

$$f(x) \equiv (x - \xi) g(x) \,(\bmod p) \qquad \text{για κάθε } x,$$

όπου $g$ είναι ένα πολυώνυμο με βαθμό $\bmod p$ ίσο με $n-1$.
Έστω, τώρα, $\eta$ μια οποιαδήποτε λύση της (7.4) διαφορετική $\bmod p$ από την $\xi$. Δηλαδή,

$$p \nmid \eta - \xi.$$

Τότε,

$$(\eta - \xi) g(\eta) \equiv f(\eta) \equiv 0 \,(\bmod p),$$

και άρα

$$p \mid (\eta - \xi) g(\eta) \;\Rightarrow\; p \mid g(\eta) \;\Rightarrow\; g(\eta) \equiv 0 \,(\bmod p).$$

Άρα κάθε λύση της (7.4) η οποία είναι διαφορετική $\bmod p$ από την $\xi$ είναι λύση της

$$g(x) \equiv 0 \,(\bmod p) \tag{7.5}$$

Επομένως, αν η (7.4) είχε περισσότερες από $n$ (μαζί με την $\xi$) διαφορετικές $\bmod p$ λύσεις, τότε η (7.5) θα είχε περισσότερες από $n-1$ διαφορετικές $\bmod p$ λύσεις. Σύμφωνα με την επαγωγική μας υπόθεση, αυτό είναι άτοπο, οπότε η (7.4) έχει το πολύ $n$ διαφορετικές $\bmod p$ λύσεις. □

Το Θεώρημα 7.1 δεν ισχύει αν ο $p$ αντικατασταθεί με μη-πρώτο $m$.

**Παράδειγμα.** Είδαμε πριν λίγο το παράδειγμα της $x^2 - 1 \equiv 0 \,(\bmod 8)$ η οποία έχει τέσσερις διαφορετικές $\bmod 8$ λύσεις.

## 7.5 Γραμμικές ισοτιμίες.

Το Θεώρημα 7.2 περιγράφει πλήρως την κατάσταση για πολυωνυμικές ισοτιμίες πρώτου βαθμού.

**Θεώρημα 7.2.** *Έστω* $m \geq 1$.
(i) *Έστω* $(a, m) = 1$. *Τότε η εξίσωση*

$$ax + b \equiv 0 \,(\mathrm{mod}\, m) \tag{7.6}$$

*έχει ακριβώς μία* mod $m$ *λύση.*
(ii) *Έστω* $(a, m) > 1$. *Τότε η εξίσωση (7.6) λύνεται αν και μόνο αν* $(a, m) \mid b$. *Στην περίπτωση που* $(a, m) \mid b$ *το πλήθος των διαφορετικών* mod $m$ *λύσεων είναι ίσο με* $(a, m)$ *και οι λύσεις είναι ακριβώς οι αριθμοί που περιέχονται σε μία ακριβώς κλάση ισοτιμίας* mod $\frac{m}{(a,m)}$.

*Απόδειξη.* (i) Έστω $(a, m) = 1$.
Αν το $x$ διατρέχει ένα πλήρες σύνολο υπολοίπων mod $m$, τότε από την Πρόταση 7.5(i) συνεπάγεται ότι το $ax + b$ διατρέχει, επίσης, ένα πλήρες σύνολο υπολοίπων mod $m$ και, επομένως, υπάρχει ακριβώς μία τιμή του $x$ για την οποία το $ax + b$ είναι ισότιμο mod $m$ με το $0$.
(ii) Έστω $(a, m) > 1$ και $(a, m) \nmid b$.
Αν η (7.6) έχει κάποια λύση $\xi$, τότε $m \mid a\xi + b$. Άρα $(a, m) \mid a\xi + b$ και, επειδή $(a, m) \mid a$, συνεπάγεται $(a, m) \mid b$ και καταλήγουμε σε άτοπο.
Τώρα, έστω $(a, m) > 1$ και $(a, m) \mid b$.
Ορίζουμε

$$d = (a, m), \quad a_1 = \frac{a}{d}, \quad b_1 = \frac{b}{d}, \quad m_1 = \frac{m}{d}.$$

Τότε, σύμφωνα με την Πρόταση 7.4(ii) η (7.6) είναι ισοδύναμη με την

$$a_1 x + b_1 \equiv 0 \,(\mathrm{mod}\, m_1). \tag{7.7}$$

Επειδή $(a_1, m_1) = 1$, από το (i) συνεπάγεται ότι η (7.7) έχει ακριβώς μία mod $m_1$ λύση. Δηλαδή, υπάρχει $\xi_0$ λύση της (7.7) και οι λύσεις της (7.7) είναι ακριβώς τα στοιχεία της κλάσης ισοτιμίας mod $m_1$ με αντιπρόσωπο $\xi_0$.
Και, επειδή η (7.6) είναι ισοδύναμη με την (7.7), οι λύσεις της (7.6) είναι ακριβώς τα στοιχεία του συνόλου

$$[\xi_0]_{m_1} = \{\xi \,|\, \xi \equiv \xi_0 \,(\mathrm{mod}\, m_1)\} = \{qm_1 + \xi_0 \,|\, q \in \mathbb{Z}\}.$$

Τώρα, το ερώτημα είναι πόσες από αυτές τις λύσεις είναι ανά δύο ανισότιμες mod $m$.
Έχουμε:

$$q'm_1 + \xi_0 \equiv q''m_1 + \xi_0 \,(\mathrm{mod}\, m) \;\Leftrightarrow\; q'm_1 \equiv q''m_1 \,(\mathrm{mod}\, dm_1) \;\Leftrightarrow\; q' \equiv q'' \,(\mathrm{mod}\, d).$$

Άρα οι λύσεις $qm_1 + \xi_0$ οι οποίες είναι ανά δύο ανισότιμες mod $m$ προέρχονται από τιμές του $q$ οι οποίες είναι ανά δύο ανισότιμες mod $d$. Τέτοιες τιμές του $q$ είναι στοιχεία ενός πλήρους συστήματος υπολοίπων mod $d$, για παράδειγμα του $\{0, 1, \ldots, d-1\}$.
Συμπεραίνουμε ότι οι $d = (a, m)$ αριθμοί

$$\xi_0,\ m_1 + \xi_0,\ \ldots,\ (d-1)m_1 + \xi_0$$

είναι ανά δύο ανισότιμες mod $m$ λύσεις της (7.6) και ότι κάθε άλλη λύση της (7.6) είναι ισότιμη mod $m$ με κάποια από αυτές. □

**Παράδειγμα.** Θα λύσουμε την

$$287x + 183 \equiv 0 \,(\mathrm{mod}\, 597). \tag{7.8}$$

Παρατηρούμε ότι $(287, 597) = 1$. Άρα η (7.8) έχει ακριβώς μία $\bmod 597$ λύση.
Ένας τρόπος να λύσουμε την εξίσωση είναι να δοκιμάσουμε διαδοχικά τους $0, 1, \ldots, 596$ μέχρι να βρούμε τον αριθμό που λύνει την (7.8).
Ένας πιο αποτελεσματικός τρόπος είναι ο εξής. Με βάση τον Ευκλείδειο αλγόριθμο βρίσκουμε αριθμούς $x, y$ ώστε

$$597x + 287y = 1.$$

Πράγματι:

$$597 \cdot 25 + 287 \cdot (-52) = 1.$$

Πολλαπλασιάζουμε με τον $183$ και βρίσκουμε

$$597 \cdot 4575 - 287 \cdot 9516 = 183$$

και άρα

$$597 \mid 287 \cdot 9516 + 183.$$

Άρα η λύση που ζητάμε είναι η $9516 \equiv 561 \pmod{597}$. Κάθε άλλη λύση της (7.8) είναι ισότιμη $\bmod 597$ με αυτήν.

**Παράδειγμα.** Θα λύσουμε την

$$861x + 549 \equiv 0 \pmod{1791}. \tag{7.9}$$

Παρατηρούμε ότι $(861, 1791) = 3$ και ότι $3 \mid 549$. Άρα η (7.9) έχει ακριβώς τρεις $\bmod 1791$ λύσεις.
Απλοποιούμε την (7.9) και βρίσκουμε την ισοδύναμη (7.8). Έχουμε ήδη λύσει την (7.8) και έχουμε δει ότι έχει ακριβώς μία $\bmod 597$ λύση:

$$\xi_0 = 561.$$

Άρα οι ακέραιες λύσεις της (7.9) είναι οι

$$q597 + 561 \qquad (q \in \mathbb{Z}).$$

Από αυτές βρίσκουμε ακριβώς τρεις ανά δύο ανισότιμες $\bmod 1791$ λύσεις, δίνοντας τις τιμές $0, 1, 2$ στο $q$:

$$561, \ 1158, \ 1755.$$

Κάθε άλλη λύση της (7.9) είναι ισότιμη $\bmod 1791$ με μία από αυτές.

## 7.6 Συστήματα γραμμικών ισοτιμιών.

Θεωρούμε ένα σύστημα γραμμικών ισοτιμιών:

$$a_1x + b_1 \equiv 0 \pmod{m_1}, \ \ldots, \ a_nx + b_n \equiv 0 \pmod{m_n}. \tag{7.10}$$

Είδαμε στην προηγούμενη ενότητα ότι κάθε εξίσωση $ax+b \equiv 0 \pmod{m}$ ανάγεται σε εξίσωση της μορφής $x \equiv c \pmod{m'}$, όπου $m' = m$, αν $(a, m) = 1$, και $m' = \frac{m}{(a,m)}$, αν $(a, m) > 1$ και $(a, m) \mid b$.

Εργαζόμενοι με κάθε εξίσωση του συστήματος (7.10) ξεχωριστά, μπορούμε να φέρουμε το σύστημα στη μορφή

$$x \equiv c_1 \pmod{m_1}, \ \ldots, \ x \equiv c_n \pmod{m_n}. \tag{7.11}$$

(Όπου τα νέα $m_j$ μπορεί να διαφέρουν από τα αρχικά $m_j$.)

Θα ασχοληθούμε, λοιπόν, με συστήματα της μορφής (7.11) και, χάριν απλότητας, θα εξετάσουμε μόνο την περίπτωση που τα $m_1, \ldots, m_n$ είναι ανά δύο σχετικά πρώτα.

**Κινέζικο Θεώρημα Υπολοίπων.** *Έστω φυσικοί $m_1, \ldots, m_n$ ανά δύο σχετικά πρώτοι. Τότε το σύστημα (7.11) έχει λύσεις και οι λύσεις αυτές είναι ακριβώς όλα τα στοιχεία μιας κλάσης ισοτιμίας* $\bmod m_1 \cdots m_n$.

*Απόδειξη.* Θεωρούμε τους αριθμούς

$$M = m_1 \cdots m_n, \quad M_1 = \frac{M}{m_1}, \quad \ldots, \quad M_n = \frac{M}{m_n}.$$

Επειδή $(M_j, m_j) = 1$, κάθε εξίσωση $M_j x \equiv c_j \,(\bmod m_j)$ έχει ακριβώς μία $\bmod m_j$ λύση. Έστω $\xi_j$ λύση της εξίσωσης αυτής, οπότε

$$M_j \xi_j \equiv c_j \,(\bmod m_j).$$

Αν $i \neq j$, τότε $m_j \mid M_i$, οπότε $m_j \mid M_i \xi_i$ και άρα

$$M_i \xi_i \equiv 0 \,(\bmod m_j) \qquad \text{για } i \neq j.$$

Προσθέτοντας τις τελευταίες ισοτιμίες $\bmod m_j$ για όλες τις τιμές του $i$, βρίσκουμε ότι

$$M_1 \xi_1 + \cdots + M_n \xi_n \equiv c_j \,(\bmod m_j).$$

Ορίζουμε

$$a_0 = M_1 \xi_1 + \cdots + M_n \xi_n$$

και έχουμε ότι

$$a_0 \equiv c_j \,(\bmod m_j) \qquad \text{για κάθε } j. \tag{7.12}$$

Άρα το $a_0$ είναι λύση του συστήματος (7.11).
Έστω, τώρα, $a$ μια οποιαδήποτε λύση του (7.11). Δηλαδή,

$$a \equiv c_j \,(\bmod m_j) \qquad \text{για κάθε } j.$$

Λόγω της (7.12), αυτό ισοδυναμεί με

$$a \equiv a_0 \,(\bmod m_j) \qquad \text{για κάθε } j$$

και, σύμφωνα με την Πρόταση 7.4(v), το τελευταίο είναι ισοδύναμο με

$$a \equiv a_0 \,(\bmod m_1 \cdots m_n).$$

Άρα οι λύσεις του (7.10) είναι ακριβώς τα στοιχεία της κλάσης ισοτιμίας $\bmod m_1 \cdots m_n$ με αντιπρόσωπο $a_0$. □

**Παράδειγμα.** Θα βρούμε τον μικρότερο θετικό ακέραιο ο οποίος δίνει υπόλοιπα $1, 2, 3, 4, 5$ όταν διαιρεθεί από τους $3, 5, 7, 9, 11$, αντιστοίχως.
Ο αριθμός που ζητάμε είναι η μικρότερη θετική λύση του συστήματος

$$x \equiv 1 \,(\bmod 3),\ x \equiv 2 \,(\bmod 5),\ x \equiv 3 \,(\bmod 7),\ x \equiv 4 \,(\bmod 9),\ x \equiv 5 \,(\bmod 11). \tag{7.13}$$

Οι αριθμοί $3, 5, 7, 9, 11$ δεν είναι ανά δύο σχετικά πρώτοι. Το πρόβλημα βρίσκεται στους $3, 9$. Παρατηρούμε, όμως, ότι

$$x \equiv 4 \,(\bmod 9) \ \Rightarrow\ x \equiv 4 \,(\bmod 3) \ \Rightarrow\ x \equiv 1 \,(\bmod 3).$$

Άρα το σύστημα (7.13) είναι ισοδύναμο με το

$$x \equiv 2 \,(\bmod 5),\ x \equiv 3 \,(\bmod 7),\ x \equiv 4 \,(\bmod 9),\ x \equiv 5 \,(\bmod 11). \tag{7.14}$$

Τώρα οι αριθμοί $5, 7, 9, 11$ είναι ανά δύο σχετικά πρώτοι.
Θεωρούμε τους

$$M = 5 \cdot 7 \cdot 9 \cdot 11 = 3465,$$

$$M_1 = \frac{M}{5} = 693, \quad M_2 = \frac{M}{7} = 495, \quad M_3 = \frac{M}{9} = 385, \quad M_4 = \frac{M}{11} = 315.$$

Βρίσκουμε λύσεις των

$$693x \equiv 2 \,(\mathrm{mod}\, 5),\ 495x \equiv 3 \,(\mathrm{mod}\, 7),\ 385x \equiv 4 \,(\mathrm{mod}\, 9),\ 315x \equiv 5 \,(\mathrm{mod}\, 11),$$

αφού τις γράψουμε, ισοδύναμα,

$$3x \equiv 2 \,(\mathrm{mod}\, 5),\ 5x \equiv 3 \,(\mathrm{mod}\, 7),\ 7x \equiv 4 \,(\mathrm{mod}\, 9),\ 7x \equiv 5 \,(\mathrm{mod}\, 11).$$

Αντίστοιχες λύσεις είναι οι

$$\xi_1 = 4, \quad \xi_2 = 2, \quad \xi_3 = 7, \quad \xi_4 = 7.$$

Άρα ο

$$a_0 = M_1\xi_1 + M_2\xi_2 + M_3\xi_3 + M_4\xi_4 = 8662$$

είναι λύση του συστήματος (7.14) ή του ισοδύναμου (7.13). Η γενική λύση του (7.13) περιγράφεται από την

$$a \equiv 8662 \,(\mathrm{mod}\, 3465)$$

δηλαδή από την

$$a = q3465 + 8662 \qquad (q \in \mathbb{Z})$$

και η μικρότερη θετική λύση είναι ο $1732$.

## 7.7 Ασκήσεις.

1. Αποδείξτε ότι
$$7 \mid 111^{333} + 333^{111}.$$

2. Αποδείξτε ότι
$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \,(\mathrm{mod}\, 181).$$

3. Βρείτε το υπόλοιπο της διαίρεσης του $4444^{4444}$ από το $9$.

4. Βρείτε ένα πλήρες και ένα περιορισμένο σύστημα υπολοίπων mod $17$ τα οποία αποτελούνται από πολλαπλάσια του $3$.

5. Αποδείξτε ότι το $\{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ είναι περιορισμένο σύστημα υπολοίπων mod $14$ και ότι το $\{2, 2^2, 2^3, \ldots, 2^{18}\}$ είναι περιορισμένο σύστημα υπολοίπων mod $27$.

6. Γράψτε μία ισοτιμία ισοδύναμη με το σύστημα
$$\begin{cases} x \equiv 1 \,(\mathrm{mod}\, 4) \\ x \equiv 2 \,(\mathrm{mod}\, 3) \end{cases}$$

7. Λύστε την
$$x^3 + 4x + 8 \equiv 0 \,(\mathrm{mod}\, 15).$$

8. Έστω ότι ο $N \geq 1$ είναι γραμμένος στο δεκαδικό σύστημα στη μορφή
$$N = a_m a_{m-1} \ldots a_1 a_0.$$
Αποδείξτε ότι

$$9 \mid N \;\Leftrightarrow\; 9 \mid a_m + a_{m-1} + \cdots + a_1 + a_0.$$
$$11 \mid N \;\Leftrightarrow\; 11 \mid (-1)^m a_m + (-1)^{m-1} a_{m-1} + \cdots - a_1 + a_0.$$

9. Έστω πρώτος $p$ ώστε $1 \leq n < p < 2n$. Αποδείξτε ότι

$$\binom{2n}{n} \equiv 0 \,(\mathrm{mod}\, p).$$

10. Έστω περιττός $a$. Αποδείξτε ότι

$$a^{2^n} \equiv 1 \,(\mathrm{mod}\, 2^{n+2}).$$

11. Έστω $\{a_1, \ldots, a_{\phi(n)}\}$ οποιοδήποτε περιορισμένο σύνολο υπολοίπων $\mathrm{mod}\, n$. Αν $n \geq 3$, αποδείξτε ότι

$$a_1 + \cdots + a_{\phi(n)} \equiv 0 \,(\mathrm{mod}\, n).$$

12. Βρείτε τα δύο τελευταία δεκαδικά ψηφία του αριθμού $9^{9^9}$.

13. Αποδείξτε ότι για κάθε $a$ ισχύει

$$a^{21} \equiv a \,(\mathrm{mod}\, 15), \quad a^7 \equiv a \,(\mathrm{mod}\, 42), \quad a^9 \equiv a \,(\mathrm{mod}\, 30), \quad a^{37} \equiv a \,(\mathrm{mod}\, 1729)$$

και ότι, αν $(a, 35) = 1$, τότε

$$a^{12} \equiv 1 \,(\mathrm{mod}\, 35).$$

14. Έστω ότι οι $p, q$ είναι πρώτοι και $p \neq q$. Αποδείξτε ότι

$$a^p \equiv a \,(\mathrm{mod}\, q),\ a^q \equiv a \,(\mathrm{mod}\, p) \;\Rightarrow\; a^{pq} \equiv a \,(\mathrm{mod}\, pq).$$

15. Αν ο $p$ είναι πρώτος και $p \nmid a$, αποδείξτε ότι το $a^{p-2}b$ είναι λύση της

$$ax \equiv b \,(\mathrm{mod}\, p).$$

Λύστε τις

$$2x \equiv 1 \,(\mathrm{mod}\, 31), \qquad 3x \equiv 17 \,(\mathrm{mod}\, 29).$$

Αν $(a, n) = 1$, αποδείξτε ότι το $a^{\phi(n)-1}b$ είναι λύση της

$$ax \equiv b \,(\mathrm{mod}\, n).$$

Λύστε τις

$$3x \equiv 5 \,(\mathrm{mod}\, 26), \qquad 10x \equiv 21 \,(\mathrm{mod}\, 49).$$

16. Αν ο $p$ είναι πρώτος, αποδείξτε ότι:

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \,(\mathrm{mod}\, p).$$
$$1^p + 2^p + \cdots + (p-1)^p \equiv 0 \,(\mathrm{mod}\, p), \text{ όταν } p \neq 2.$$

17. Αν ο $p$ είναι πρώτος, αποδείξτε ότι

$$(a+b)^p \equiv a^p + b^p \,(\mathrm{mod}\, p).$$

18. Αποδείξτε ότι υπάρχουν άπειροι σύνθετοι $n$ για τους οποίους ισχύει

$$a^{n-1} \equiv 1 \,(\mathrm{mod}\, n).$$

19. Αν $m, n \geq 1$ και $(m, n) = 1$, αποδείξτε ότι

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \,(\mathrm{mod}\, mn).$$

20. Αν ο $p$ είναι πρώτος, $p \nmid a$, $p \nmid b$, αποδείξτε ότι

$$a^p \equiv b^p \,(\mathrm{mod}\, p) \;\Rightarrow\; a^p \equiv b^p \,(\mathrm{mod}\, p^2).$$

21. Αν ο $p \neq 2$ είναι πρώτος και $0 \leq k \leq p-1$, αποδείξτε ότι

$$\binom{p-1}{k} \equiv (-1)^k \,(\mathrm{mod}\, p).$$

22. Σχηματίζουμε την ακολουθία $(a_n)$ με $a_1 = 3$ και τον αναδρομικό τύπο

$$a_{n+1} = 3^{a_n} \qquad \text{για κάθε } n.$$

Ποιά είναι τα δύο τελευταία δεκαδικά ψηφία του $a_n$;

23. (Δεύτερη απόδειξη του Θεωρήματος του Fermat.)

Αν ο $p$ είναι πρώτος και $1 \leq k \leq p-1$, αποδείξτε ότι

$$\binom{p}{k} \equiv 0 \,(\mathrm{mod}\, p).$$

Αν ο $p$ είναι πρώτος, αποδείξτε με επαγωγή ότι

$$a^p \equiv a \,(\mathrm{mod}\, p)$$

για κάθε φυσικό $a$ και, κατόπιν, αποδείξτε το ίδιο για κάθε ακέραιο $a$.

Αν ο $p$ είναι πρώτος και $p \nmid a$, αποδείξτε ότι

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\, p).$$

24. (Δεύτερη απόδειξη του Θεωρήματος του Euler.) Θεωρήστε γνωστό το Θεώρημα του Fermat.

Αν ο $p$ είναι πρώτος και $p \nmid a$, αποδείξτε με επαγωγή ότι

$$a^{p^{\alpha-1}(p-1)} \equiv 1 \,(\mathrm{mod}\, p^\alpha)$$

για κάθε φυσικό $\alpha$.

Αν $(a, n) = 1$ και $n > 1$, χρησιμοποιήστε την κανονική αναπαράσταση του $n$ για να αποδείξετε ότι

$$a^{\phi(n)} \equiv 1 \,(\mathrm{mod}\, n).$$

25. Έστω $n \geq 2$. Αποδείξτε ότι:

$$\text{ο } n \text{ είναι πρώτος} \;\Leftrightarrow\; (n-2)! \equiv 1 \,(\mathrm{mod}\, n) \;\Leftrightarrow\; (n-1)! \equiv -1 \,(\mathrm{mod}\, n).$$

26. Αν ο $p \neq 2$ είναι πρώτος, αποδείξτε ότι

$$1^2 3^2 5^2 \cdots (p-4)^2 (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \,(\mathrm{mod}\, p).$$

27. Αν ο $p \neq 2$ είναι πρώτος, αποδείξτε ότι

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \,(\mathrm{mod}\, p).$$

Με βάση αυτό το αποτέλεσμα, αποδείξτε ότι

$$p \equiv 1 \pmod 4 \;\Rightarrow\; \text{η } x^2 + 1 \equiv 0 \pmod p \text{ έχει λύση.}$$

Ποιά είναι η λύση;
Λύστε τις

$$x^2 + 1 \equiv 0 \pmod{29}, \qquad x^2 + 1 \equiv 0 \pmod{37}.$$

Αντιστρόφως, αποδείξτε ότι

$$\text{η } x^2 + 1 \equiv 0 \pmod p \text{ έχει λύση} \;\Rightarrow\; p \equiv 1 \pmod 4.$$

28. Λύστε τις

$$36x \equiv 8 \pmod{102}, \qquad 5x \equiv 2 \pmod{26}, \qquad 6x \equiv 15 \pmod{21}.$$

29. Λύστε τα συστήματα

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases} \qquad \begin{cases} 2x \equiv 1 \pmod 5 \\ 3x \equiv 9 \pmod 6 \\ 4x \equiv 1 \pmod 7 \\ 5x \equiv 9 \pmod{11} \end{cases}$$

30. Αποδείξτε ότι το σύστημα

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$$

έχει λύση αν και μόνο αν $(m, n) \mid a - b$ και ότι, αν υπάρχει λύση, τότε αυτή είναι μοναδική $\bmod[m, n]$.

31. Θεωρήστε την εξίσωση

$$ax \equiv b \pmod{15}.$$

Αν επιλέγουμε το $a$ με τυχαίο τρόπο από τα $1, \ldots, 14$ και το $b$ από τα $0, 1, \ldots, 14$, τότε ποιά είναι η πιθανότητα να έχει λύση η εξίσωση και ποιά είναι η πιθανότητα να έχει ακριβώς μία λύση η εξίσωση;

32. Έστω ότι ο $p$ είναι πρώτος, $p \nmid a$, $r > 1$, $s > 1$, $rs > p$.

Θεωρήστε τους $rs$ αριθμούς

$$ax - y$$

όταν το $x$ διατρέχει τους $0, 1, \ldots, r - 1$ και το $y$ διατρέχει τους $0, 1, \ldots, s - 1$. Αποδείξτε ότι υπάρχουν δύο τουλάχιστον επιλογές ζευγαριών $x_1, y_1$ και $x_2, y_2$ ώστε

$$ax_1 - y_1 \equiv ax_2 - y_2 \pmod p.$$

Αποδείξτε ότι υπάρχουν $x, y$ ώστε

$$ax \equiv y \pmod p, \quad 1 \le |x| < r, 1 \le |y| < s.$$

## 7.8 Λύσεις ασκήσεων.

1. Αυτό που θέλουμε να αποδείξουμε διατυπώνεται ισοδύναμα ως εξής:

$$111^{333} + 333^{111} \equiv 0 \,(\mathrm{mod}\, 7).$$

Επομένως, θα εργαστούμε με ισοτιμίες.
Κατ' αρχάς,

$$111 \equiv 6 \,(\mathrm{mod}\, 7), \quad 333 \equiv 4 \,(\mathrm{mod}\, 7)$$

οπότε

$$111^{333} + 333^{111} \equiv 6^{333} + 4^{111} \,(\mathrm{mod}\, 7).$$

Από το Θεώρημα του Fermat έχουμε

$$6^6 \equiv 1 \,(\mathrm{mod}\, 7), \quad 4^6 \equiv 1 \,(\mathrm{mod}\, 7).$$

Επομένως,

$$6^{333} \equiv 6^{55\cdot 6+3} \equiv (6^6)^{55} 6^3 \equiv 6^3 \equiv (-1)^3 \equiv -1 \,(\mathrm{mod}\, 7)$$

και

$$4^{111} \equiv 4^{18\cdot 6+3} \equiv (4^6)^{18} 4^3 \equiv 4^3 \equiv 64 \equiv 1 \,(\mathrm{mod}\, 7).$$

Άρα

$$111^{333} + 333^{111} \equiv 6^{333} + 4^{111} \equiv -1 + 1 \equiv 0 \,(\mathrm{mod}\, 7).$$

4. Μια παραλλαγή: θα βρούμε ένα πλήρες και ενα περιορισμένο σύστημα υπολοίπων $\mathrm{mod}\, 12$ τα οποία αποτελούνται από πολλαπλάσια του $5$.
Θεωρούμε ένα οποιοδήποτε πλήρες σύστημα υπολοίπων $\mathrm{mod}\, 12$. Για παράδειγμα, το

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11.$$

Μέσα σ' αυτό βρίσκεται το περιορισμένο σύστημα υπολοίπων

$$1, 5, 7, 11.$$

Ο αριθμός $5$ είναι σχετικά πρώτος με τον $12$. Άρα το

$$5\cdot 0,\ 5\cdot 1,\ 5\cdot 2,\ 5\cdot 3,\ 5\cdot 4,\ 5\cdot 5,\ 5\cdot 6,\ 5\cdot 7,\ 5\cdot 8,\ 5\cdot 9,\ 5\cdot 10,\ 5\cdot 11$$

είναι ένα πλήρες σύστημα υπολοίπων $\mathrm{mod}\, 12$ και το

$$5\cdot 1,\ 5\cdot 5,\ 5\cdot 7,\ 5\cdot 11$$

είναι ένα περιορισμένο σύστημα υπολοίπων $\mathrm{mod}\, 12$.

8. Θα ασχοληθούμε μόνο με το δεύτερο ερώτημα.
Έχουμε ότι

$$N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0,$$

οπότε

$$N \equiv a_m (-1)^m + a_{m-1} (-1)^{m-1} + \cdots + a_1 (-1) + a_0 \,(\mathrm{mod}\, 11).$$

Άρα

$$N \equiv 0 \,(\mathrm{mod}\, 11) \ \Leftrightarrow\ a_m (-1)^m + a_{m-1} (-1)^{m-1} + \cdots + a_1 (-1) + a_0 \equiv 0 \,(\mathrm{mod}\, 11)$$

ή, ισοδύναμα,

$$11 \mid N \ \Leftrightarrow\ 11 \mid a_m (-1)^m + a_{m-1} (-1)^{m-1} + \cdots + a_1 (-1) + a_0.$$

10. Επειδή
$$\phi(2^{n+2}) = 2^{n+2} - 2^{n+1} = 2 \cdot 2^{n+1} - 2^{n+1} = 2^{n+1},$$
από το Θεώρημα του Euler (προσέξτε ότι οι $a$ και $2^{n+2}$ είναι σχετικά πρώτοι, αφού ο $a$ είναι περιττός) προκύπτει ότι
$$a^{2^{n+1}} \equiv 1 \,(\mathrm{mod}\, 2^{n+2})$$
και δεν είναι αυτό που θέλουμε να αποδείξουμε. Αυτό που αποδείξαμε λέει ότι
$$2^{n+2} \mid a^{2^{n+1}} - 1 = a^{2\cdot 2^{n+1}} - 1 = (a^{2^n} - 1)(a^{2^n} + 1) \tag{7.15}$$
ενώ αυτό που θέλουμε να αποδείξουμε λέει ότι
$$2^{n+2} \mid a^{2^n} - 1. \tag{7.16}$$
Η (7.16) θα μπορούσε να προκύψει από την (7.15) αν οι $2^{n+2}$ και $a^{2^n} + 1$ ήταν σχετικά πρώτοι. Αυτό, όμως, δεν είναι σωστό διότι ο $a^{2^n} + 1$ είναι άρτιος.
Επειδή $\phi(2^{n+1}) = 2^n$, θα μπορούσαμε να δοκιμάσουμε πάλι με το Θεώρημα του Euler να πούμε ότι
$$a^{2^n} \equiv 1 \,(\mathrm{mod}\, 2^{n+1}).$$
Αυτό σημαίνει ότι
$$2^{n+1} \mid a^{2^n} - 1,$$
αλλά και πάλι αυτό δεν είναι το (7.16) που θέλουμε να αποδείξουμε.
Γι αυτό κάνουμε το εξής: γράφουμε
$$a^{2^n} - 1 = a^{2\cdot 2^{n-1}} - 1 = (a^{2^{n-1}} + 1)(a^{2^{n-1}} - 1)$$
και εφαρμόζουμε αυτήν την ισότητα διαδοχικά για $n, n-1, n-2, \ldots, 1$. Έτσι έχουμε ότι
$$a^{2^n} - 1 = (a^{2^{n-1}} + 1)(a^{2^{n-2}} + 1) \cdots (a^{2^2} + 1)(a^2 + 1)(a + 1)(a - 1).$$
Τώρα παρατηρούμε ότι, επειδή ο $a$ είναι περιττός, κάθε παράγων του τελευταίου γινομένου είναι πολλαπλάσιος του 2. Επειδή το πλήθος των παραγόντων είναι ίσο με $n+1$, το γινόμενο είναι πολλαπλάσιο του $2^{n+1}$. Και πάλι δεν πετυχαίνουμε να αποδείξουμε ότι το γινόμενο είναι πολλαπλάσιο του $2^{n+2}$. Αν, όμως, παρατηρήσουμε πιο προσεκτικά, θα δούμε ότι οι δύο τελευταίοι παράγοντες του γινομένου έχουν γινόμενο ίσο με
$$(a + 1)(a - 1) = (2k + 2)2k = 4(k + 1)k = 8m,$$
διότι ένας από τους διαδοχικούς ακεραίους $k, k + 1$ είναι άρτιος.
Επειδή το γινόμενο των $n - 1$ αρχικών παραγόντων του γινομένου είναι πολλαπλάσιο του $2^{n-1}$, το συνολικό γινόμενο είναι πολλαπλάσιο του $2^{n-1}2^3 = 2^{n+2}$.

11. Θεωρούμε για καθέναν από τους $a_j$ τον αντίστοιχο αριθμό $-a_j$. Ο $a_j$ είναι σχετικά πρώτος με τον $n$ και, επομένως, ο $-a_j$ είναι κι αυτός σχετικά πρώτος με τον $n$. Άρα ο $-a_j$ είναι ισότιμος $\mathrm{mod}\, n$ με ακριβώς έναν από τους $a_1, \ldots, a_{\phi(n)}$. *Ερώτηση:* είναι δυνατόν να είναι ο $-a_j$ ισότιμος $\mathrm{mod}\, n$ με τον $a_j$ ; *Απάντηση:* όχι. Διότι αν
$$-a_j \equiv a_j \,(\mathrm{mod}\, n),$$
τότε
$$n \mid 2a_j$$
και, επειδή οι $n$ και $a_j$ είναι σχετικά πρώτοι,
$$n \mid 2$$

που είναι άτοπο.
Άρα για κάθε $a_j$ υπάρχει ακριβώς ένας αριθμός από τους $a_1, \ldots, a_{\phi(n)}$ ο οποίος είναι ισότιμος $\bmod n$ με τον $-a_j$ και αυτός ο αριθμός δεν είναι ο $a_j$.
Αυτό σημαίνει ότι οι $a_1, \ldots, a_{\phi(n)}$ χωρίζονται σε ζεύγη αριθμών έτσι ώστε το άθροισμα των αριθμών κάθε ζεύγους να είναι ισότιμο $\bmod n$ με το $0$. Άρα

$$a_1 + \cdots + a_{\phi(n)} \equiv 0 \,(\mathrm{mod}\, n).$$

13. Θα ασχοληθούμε μόνο με το πρώτο ερώτημα.
Επειδή $\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$, από το Θεώρημα του Euler συνεπάγεται

$$a^8 \equiv 1 \,(\mathrm{mod}\, 15)$$

αν $(a, 15) = 1$.
Επειδή αυτό δεν είναι το ίδιο με αυτό που θέλουμε να αποδείξουμε και επειδή και αυτό ισχύει με τον περιορισμό $(a, 15) = 1$, σκεφτόμαστε κάτι διαφορετικό.
Έχουμε ότι $(3, 5) = 1$ και $15 = 3 \cdot 5$, Άρα η

$$a^{21} \equiv a \,(\mathrm{mod}\, 15)$$

είναι ισοδύναμη με το σύστημα

$$a^{21} \equiv a \,(\mathrm{mod}\, 3), \qquad a^{21} \equiv a \,(\mathrm{mod}\, 5).$$

Από το Θεώρημα του Fermat συνεπάγεται ότι

$$a^3 \equiv a \,(\mathrm{mod}\, 3), \qquad a^5 \equiv a \,(\mathrm{mod}\, 5).$$

Από την πρώτη σχέση έχουμε

$$a^{21} \equiv (a^3)^7 \equiv a^7 \equiv (a^3)^2 a \equiv a^2 a \equiv a^3 \equiv a \,(\mathrm{mod}\, 3)$$

και από την δεύτερη σχέση έχουμε

$$a^{21} \equiv (a^5)^4 a \equiv a^4 a \equiv a^5 \equiv a \,(\mathrm{mod}\, 5).$$

14. Υψώνουμε την $a^p \equiv a \,(\mathrm{mod}\, q)$ στον εκθέτη $q$ και βρίσκουμε

$$a^{pq} \equiv a^q \,(\mathrm{mod}\, q).$$

Από το Θεώρημα του Fermat έχουμε ότι

$$a^q \equiv a \,(\mathrm{mod}\, q)$$

και άρα

$$a^{pq} \equiv a \,(\mathrm{mod}\, q).$$

“Συμμετρικά”, βρίσκουμε και το

$$a^{pq} \equiv a \,(\mathrm{mod}\, p).$$

Επειδή οι $p, q$ είναι σχετικά πρώτοι, συνεπάγεται

$$a^{pq} \equiv a \,(\mathrm{mod}\, pq).$$

15. Έχουμε ότι
$$a(a^{p-2}b) \equiv a^{p-1}b \equiv b \pmod{p}$$
από το Θεώρημα του Fermat.
Άρα η λύση της $ax \equiv b \pmod{p}$ είναι η
$$x \equiv a^{p-2}b \pmod{p}.$$
Ειδικώτερα, η λύση της $2x \equiv 1 \pmod{31}$ είναι η
$$x \equiv 2^{29} \pmod{31}.$$
Για να απλοποιήσουμε την λύση, βλέπουμε ότι
$$2^5 \equiv 32 \equiv 1 \pmod{31},$$
οπότε
$$2^{29} \equiv (2^5)^5 2^4 \equiv 2^4 \equiv 16 \pmod{31}.$$
Άρα η λύση είναι
$$x \equiv 16 \pmod{31}.$$

16. Από το Θεώρημα του Fermat έχουμε
$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv 1 + 1 + \cdots + 1 \equiv p - 1 \equiv -1 \pmod{p}.$$
Το δεύτερο ερώτημα είναι παρόμοιο.

17. Πάλι από το Θεώρημα του Fermat έχουμε
$$(a+b)^p \equiv a + b \pmod{p}, \quad a^p \equiv a \pmod{p}, \quad b^p \equiv b \pmod{p}.$$
Από αυτές τις σχέσεις προκύπτει αμέσως το ζητούμενο.

26. Ισχύει
$$\begin{aligned} 1 &\equiv (-1)(p-1) \pmod{p} \\ 3 &\equiv (-1)(p-3) \pmod{p} \\ &\cdots\cdot \\ &\cdots\cdot \\ p-4 &\equiv (-1)4 \pmod{p} \\ p-2 &\equiv (-1)2 \pmod{p}. \end{aligned}$$
Πολλαπλασιάζουμε και βρίσκουμε
$$1 \cdot 3 \cdots (p-4)(p-2) \equiv (-1)^{\frac{p-1}{2}} 2 \cdot 4 \cdots (p-3)(p-1) \pmod{p}.$$
Άρα
$$\begin{aligned} 1^2 3^2 \cdots (p-4)^2 (p-2)^2 &\equiv 1 \cdot 3 \cdots (p-4)(p-2)(-1)^{\frac{p-1}{2}} 2 \cdot 4 \cdots (p-3)(p-1) \\ &\equiv (-1)^{\frac{p-1}{2}} (p-1)! \equiv (-1)^{\frac{p-1}{2}} (-1) \equiv (-1)^{\frac{p+1}{2}} \pmod{p} \end{aligned}$$
σύμφωνα με το Θεώρημα του Wilson.

27. Ισχύει

$$\begin{aligned} 1 &\equiv (-1)(p-1) \,(\mathrm{mod}\, p) \\ 2 &\equiv (-1)(p-2) \,(\mathrm{mod}\, p) \\ &\cdots\cdot \\ &\cdots\cdot \\ \frac{p-1}{2} &\equiv (-1)\frac{p+1}{2} \,(\mathrm{mod}\, p). \end{aligned}$$

Πολλαπλασιάζουμε και βρίσκουμε

$$1 \cdot 2 \cdots \frac{p-1}{2} \equiv (-1)^{\frac{p-1}{2}} \frac{p+1}{2} \cdots (p-2)(p-1) \,(\mathrm{mod}\, p).$$

Άρα

$$\begin{aligned} \left(\left(\frac{p-1}{2}\right)!\right)^2 &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} (-1)^{\frac{p-1}{2}} \frac{p+1}{2} \cdots (p-2)(p-1) \\ &\equiv (-1)^{\frac{p-1}{2}} (p-1)! \equiv (-1)^{\frac{p-1}{2}} (-1) \equiv (-1)^{\frac{p+1}{2}} \,(\mathrm{mod}\, p) \end{aligned}$$

σύμφωνα με το Θεώρημα του Wilson.

# Κεφάλαιο 8

# Τετραγωνικά υπόλοιπα.

## 8.1 Τετραγωνικά υπόλοιπα.

**ΟΡΙΣΜΟΣ.** *Έστω* $m \geq 1$ *και* $(a, m) = 1$. *Αν η εξίσωση*

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

*έχει λύση, τότε λέμε ότι το* $a$ *είναι* **τετραγωνικό υπόλοιπο** $\bmod m$. *Αν η ίδια εξίσωση δεν έχει λύση, τότε λέμε ότι το* $a$ *είναι* **μη-τετραγωνικό υπόλοιπο** $\bmod m$.

Είναι προφανές ότι, αν $a \equiv b \pmod{m}$, τότε η εξίσωση $x^2 \equiv a \pmod{m}$ έχει λύση αν και μόνο αν η εξίσωση $x^2 \equiv b \pmod{m}$ έχει λύση. Άρα η ιδιότητα του $a$ να είναι τετραγωνικό υπόλοιπο $\bmod m$ ή μη-τετραγωνικό υπόλοιπο $\bmod m$ χαρακτηρίζει όλους τους αριθμούς που ανήκουν στην ίδια κλάση ισοτιμίας $\bmod m$ με το $a$. Γι αυτό, συνήθως αναφερόμαστε σε ένα περιορισμένο (αφού έχουμε θέσει τον περιορισμό $(a, m) = 1$) σύνολο υπολοίπων $\bmod m$ και χωρίζουμε τα στοιχεία του σε τετραγωνικά και μη-τετραγωνικά υπόλοιπα $\bmod m$.

Παρατηρούμε, επίσης, ότι αν $\xi$ είναι λύση της $x^2 \equiv a \pmod{m}$, τότε, εκτός από $(a, m) = 1$, έχουμε και $(\xi, m) = 1$. Άρα η μελέτη μας περιορίζεται και ως προς το $a$ αλλά και ως προς το $x$ σε περιορισμένο σύνολο υπολοίπων $\bmod m$.

**Παράδειγμα.** Έστω $m = 10$. Το $\{1, 3, 7, 9\}$ είναι περιορισμένο σύνολο υπολοίπων $\bmod 10$.
Ο πίνακας που ακολουθεί έχει τις τιμές του $a$ και τις λύσεις της εξίσωσης $x^2 \equiv a \pmod{10}$:

| $a$ | 1 | 3 | 7 | 9 |
|---|---|---|---|---|
| $x$ | 1, 9 | —- | —- | 3, 7 |

Άρα οι αριθμοί $1, 9$ είναι τετραγωνικά υπόλοιπα $\bmod 10$ και οι $3, 7$ είναι μη-τετραγωνικά υπόλοιπα $\bmod 10$.

Από εδώ και πέρα θα περιοριστούμε στην περίπτωση που το $m$ είναι πρώτος:

$$m = p, \quad \text{ο } p \text{ είναι πρώτος.}$$

Αν ο $p$ είναι πρώτος, το πιο συνηθισμένο περιορισμένο σύνολο υπολοίπων $\bmod p$ είναι το

$$\{1, 2, \ldots, p-1\}. \tag{8.1}$$

Τα διάφορα $a, x$ που θα εξετάζουμε θα περιέχονται, συνήθως, σ' αυτό το σύνολο ή θα είναι ισότιμα $\bmod p$ με στοιχεία αυτού του συνόλου.

Όταν $p = 2$, τότε έχουμε μόνο μία τιμή του $a$: $a = 1$. Τότε η $x^2 \equiv 1 \pmod{2}$ έχει ως λύση το $x = 1$. Άρα το (μοναδικό) $a = 1$ είναι τετραγωνικό υπόλοιπο $\bmod 2$.

Άρα οι ενδιαφέρουσες περιπτώσεις είναι όταν $p > 2$. Τότε ο πρώτος $p$ είναι περιττός, οπότε το σύνολο (8.1) έχει άρτιο πλήθος στοιχείων.

**Παράδειγμα.** Έστω $p = 11$.
Το $a$ παίρνει τιμές μέσα στο $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Για κάθε τιμή του $a$ εξετάζουμε αν έχει λύση η $x^2 \equiv a \pmod{11}$ και σχηματίζουμε τον παρακάτω πίνακα:

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $x$ | 1, 10 | —- | 5, 6 | 2, 9 | 4, 7 | —- | —- | —- | 3, 8 | —- |

Η διαδικασία είναι χρονοβόρα, διότι για κάθε $a$ πρέπει να δοκιμάσουμε διάφορα $x$.
Παρατηρούμε τα εξής:
(i) Τα τετραγωνικά υπόλοιπα $\bmod 11$ είναι οι αριθμοί $1, 3, 4, 5, 9$. Δηλαδή οι μισοί αριθμοί $a$ είναι τετραγωνικά υπόλοιπα $\bmod 11$ και οι άλλοι μισοί είναι μη-τετραγωνικά υπόλοιπα $\bmod 11$.
(ii) Για κάθε $a$ το οποίο είναι τετραγωνικό υπόλοιπο $\bmod 11$ υπάρχουν ακριβώς δύο λύσεις της $x^2 \equiv a \pmod{11}$.
(iii) Οι δύο λύσεις $x_1, x_2$ της $x^2 \equiv a \pmod{11}$ είναι συμμετρικές: δηλαδή $x_1 + x_2 = 11$, οπότε βρίσκονται εκατέρωθεν του $\frac{11}{2}$ και ισαπέχουν από το $\frac{11}{2}$.
Ένας δεύτερος και πιο σύντομος τρόπος να βρούμε τα τετραγωνικά υπόλοιπα $\bmod 11$ είναι να βρούμε τις τιμές του $x^2$ όταν το $x$ διατρέχει το $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. (Υπολογίζουμε αλγεβρικά το $x^2$ και μετά βρίσκουμε τον αριθμό με τον οποίο είναι αυτό ισότιμο $\bmod 11$.) Δείτε τον παρακάτω πίνακα:

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $x^2$ | 1 | 4 | 9 | 5 | 3 | 3 | 5 | 9 | 4 | 1 |

Οι τιμές του $a$ οι οποίες προκύπτουν ως τετράγωνα (δηλαδή τα τετραγωνικά υπόλοιπα $\bmod 11$) είναι οι αριθμοί $1, 3, 4, 5, 9$. Στον δεύτερο πίνακα φαίνεται και πάλι η συμμετρία που αναφέραμε προηγουμένως.

**Λήμμα 8.1.** *Έστω πρώτος $p > 2$. Αν η $x^2 \equiv a \pmod{p}$ έχει λύση $\xi$ στο διάστημα $1 \le x \le p-1$, τότε έχει και δεύτερη λύση, διαφορετική από το $\xi$, το $p - \xi$, στο ίδιο διάστημα. Οι δύο αυτές λύσεις είναι συμμετρικές ως προς τον (ρητό) $\frac{p}{2}$. Κάθε άλλη λύση είναι ισότιμη $\bmod p$ με ένα από τα $\xi, p - \xi$. Άρα η εξίσωση είτε δεν έχει λύση είτε έχει ακριβώς δύο $\bmod p$ λύσεις.*

*Απόδειξη.* Έστω

$$\xi^2 \equiv a \pmod{p}.$$

Τότε

$$(p - \xi)^2 \equiv (-\xi)^2 \equiv \xi^2 \equiv a \pmod{p}.$$

Είναι προφανές ότι, αν το $\xi$ είναι στο διάστημα $1 \le x \le p - 1$, τότε και το $p - \xi$ είναι στο ίδιο διάστημα.
Οι λύσεις $\xi, p - \xi$ είναι διαφορετικές: αν ήταν ίσες, τότε το $\xi$ θα ήταν ίσο με το μη-ακέραιο $\frac{p}{2}$.
Αν $\eta$ είναι οποιαδήποτε άλλη λύση της $x^2 \equiv a \pmod{p}$, τότε

$$\begin{aligned}
\eta^2 \equiv a \pmod{p} &\Leftrightarrow \eta^2 \equiv \xi^2 \pmod{p} \\
&\Leftrightarrow p \mid (\eta - \xi)(\eta + \xi) \\
&\Leftrightarrow p \mid \eta - \xi \text{ ή } p \mid \eta + \xi \\
&\Leftrightarrow \eta \equiv \xi \pmod{p} \text{ ή } \eta \equiv -\xi \pmod{p} \\
&\Leftrightarrow \eta \equiv \xi \pmod{p} \text{ ή } \eta \equiv p - \xi \pmod{p}.
\end{aligned}$$

□

**Θεώρημα 8.1.** *Έστω πρώτος $p > 2$. Τότε υπάρχουν ακριβώς $\frac{p-1}{2}$ ανά δύο ανισότιμα $\bmod p$ τετραγωνικά υπόλοιπα $\bmod p$. Τέτοια είναι οι αριθμοί*

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2. \tag{8.2}$$

*Απόδειξη.* Για να είναι το $a$ τετραγωνικό υπόλοιπο mod $p$, πρέπει και αρκεί να είναι ισότιμο mod $p$ με έναν από τους αριθμούς $1^2, 2^2, \ldots, (p-2)^2, (p-1)^2$.
Από το Λήμμα 8.1 γνωρίζουμε ότι τα $\xi, p-\xi$ έχουν ισότιμα mod $p$ τετράγωνα. Δηλαδή:

$$1^2 \equiv (p-1)^2, \quad 2^2 \equiv (p-2)^2, \quad \ldots, \quad \Big(\frac{p-1}{2}\Big)^2 \equiv \Big(\frac{p+1}{2}\Big)^2 \qquad (\mathrm{mod}\, p).$$

Τέλος, από το Λήμμα 8.1 γνωρίζουμε ότι οι αριθμοί (8.2) είναι ανά δύο ανισότιμοι mod $p$. □

Επομένως, όπως στο παράδειγμα με $p = 11$, για να βρούμε τα τετραγωνικά υπόλοιπα mod $p$, υπολογίζουμε τους αριθμούς (8.2) και μετά βρίσκουμε - αν χρειάζεται - τους αριθμούς $a$ στο διάστημα $1 \le a \le p-1$ με τους οποίους αυτοί είναι ισότιμοι mod $p$.

**ΟΡΙΣΜΟΣ.** *Έστω πρώτος $p > 2$ και $p \nmid a$. Ορίζουμε*

$$\Big(\frac{a}{p}\Big) = \begin{cases} 1, & \text{αν ο } a \text{ είναι τετραγωνικό υπόλοιπο mod } p \\ -1, & \text{αν ο } a \text{ είναι μη-τετραγωνικό υπόλοιπο mod } p \end{cases}$$

*Το $(\frac{a}{p})$ ονομάζεται* **σύμβολο του Legendre**.

Επομένως, για να αποφασίσουμε αν ένα $a$ είναι τετραγωνικό υπόλοιπο mod $p$, αρκεί να υπολογίσουμε το σύμβολο $(\frac{a}{p})$.

**Πρόταση 8.1.** *Έστω πρώτος $p > 2$.*
(i) $(\frac{1}{p}) = 1$.
(ii) *Αν $p \nmid k$, τότε* $(\frac{k^2}{p}) = 1$.
(iii) *Αν $a \equiv b\,(\mathrm{mod}\, p)$, τότε* $(\frac{a}{p}) = (\frac{b}{p})$.

*Απόδειξη.* (i) Η $x^2 \equiv 1\,(\mathrm{mod}\, p)$ έχει ως λύση το 1 (και το $p-1$).
(ii) Αν $p \nmid k$, τότε $p \nmid k^2$ και η $x^2 \equiv k^2\,(\mathrm{mod}\, p)$ έχει ως λύση το $k$ (και το $p-k$).
(iii) Αν $a \equiv b\,(\mathrm{mod}\, p)$, τότε η $x^2 \equiv a\,(\mathrm{mod}\, p)$ έχει λύση αν και μόνο αν η $x^2 \equiv b\,(\mathrm{mod}\, p)$ έχει λύση. □

## 8.2 Το Κριτήριο του Euler.

**Κριτήριο του Euler.** *Έστω πρώτος $p > 2$ και $p \nmid a$. Τότε*

$$\Big(\frac{a}{p}\Big) \equiv a^{\frac{p-1}{2}}\,(\mathrm{mod}\, p).$$

*Απόδειξη.* Από το Θεώρημα του Fermat έχουμε ότι για κάθε $a$ με $p \nmid a$ ισχύει

$$a^{p-1} \equiv 1\,(\mathrm{mod}\, p)$$

και, επομένως,

$$p \mid a^{p-1} - 1 = \big(a^{\frac{p-1}{2}} - 1\big)\big(a^{\frac{p-1}{2}} + 1\big) \;\Rightarrow\; p \mid a^{\frac{p-1}{2}} - 1 \text{ ή } p \mid a^{\frac{p-1}{2}} + 1.$$

Τα δυο τελευταία ενδεχόμενα δεν συμβαίνουν ταυτόχρονα, διότι αλλιώς θα είχαμε:

$$p \mid \big(a^{\frac{p-1}{2}} + 1\big) - \big(a^{\frac{p-1}{2}} - 1\big) = 2,$$

το οποίο είναι άτοπο.
Άρα για κάθε $a$ με $p \nmid a$ ισχύει ακριβώς μία από τις ισοτιμίες:

$$a^{\frac{p-1}{2}} \equiv 1\,(\mathrm{mod}\, p), \qquad a^{\frac{p-1}{2}} \equiv -1\,(\mathrm{mod}\, p).$$

Απομένει, λοιπόν, να αποδείξουμε ότι:

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv 1 \,(\mathrm{mod}\, p) \;\Leftrightarrow\; \text{το } a \text{ είναι τετραγωνικό υπόλοιπο } \mathrm{mod}\, p \\ a^{\frac{p-1}{2}} &\equiv -1 \,(\mathrm{mod}\, p) \;\Leftrightarrow\; \text{το } a \text{ είναι μη-τετραγωνικό υπόλοιπο } \mathrm{mod}\, p \end{aligned} \tag{8.3}$$

Τώρα θεωρούμε την εξίσωση

$$x^{\frac{p-1}{2}} \equiv 1 \,(\mathrm{mod}\, p) \tag{8.4}$$

Από το Θεώρημα 7.1 συνεπάγεται ότι η (8.4) έχει το πολύ $\frac{p-1}{2}$ λύσεις ανά δύο διαφορετικές $\mathrm{mod}\, p$. Από την άλλη μεριά, κάθε τετραγωνικό υπόλοιπο $\mathrm{mod}\, p$ είναι λύση της (8.4). Διότι, αν ισχύει

$$\xi^2 \equiv a \,(\mathrm{mod}\, p)$$

για κάποιο $\xi$, τότε, σύμφωνα με το Θεώρημα του Fermat,

$$a^{\frac{p-1}{2}} \equiv \xi^{p-1} \equiv 1 \,(\mathrm{mod}\, p).$$

Και το Θεώρημα 8.1 λέει ότι υπάρχουν ακριβώς $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα $\mathrm{mod}\, p$ ανά δύο ανισότιμα $\mathrm{mod}\, p$.
Άρα η (8.4) έχει ακριβώς $\frac{p-1}{2}$ λύσεις ανά δύο διαφορετικές $\mathrm{mod}\, p$ και αυτές είναι τα τετραγωνικά υπόλοιπα $\mathrm{mod}\, p$. Αυτό σημαίνει ότι αποδείξαμε τις (8.3). □

**Θεώρημα 8.2.** *Έστω πρώτος $p > 2$ και $p \nmid a_1 \cdots a_k$. Τότε*

$$\Big(\frac{a_1 \cdots a_k}{p}\Big) = \Big(\frac{a_1}{p}\Big) \cdots \Big(\frac{a_k}{p}\Big).$$

*Απόδειξη.* Το $p \nmid a_1 \cdots a_k$ είναι ισοδύναμο με τα $p \nmid a_1, \,\ldots\, , p \nmid a_k$.
Από το Κριτήριο του Euler έχουμε:

$$\Big(\frac{a_1 \cdots a_k}{p}\Big) \equiv (a_1 \cdots a_k)^{\frac{p-1}{2}} \,(\mathrm{mod}\, p)$$

και

$$\Big(\frac{a_1}{p}\Big) \equiv a_1^{\frac{p-1}{2}} \,(\mathrm{mod}\, p), \quad \ldots\,, \quad \Big(\frac{a_k}{p}\Big) \equiv a_k^{\frac{p-1}{2}} \,(\mathrm{mod}\, p).$$

Συνεπάγεται ότι

$$\Big(\frac{a_1 \cdots a_k}{p}\Big) \equiv \Big(\frac{a_1}{p}\Big) \cdots \Big(\frac{a_k}{p}\Big) \,(\mathrm{mod}\, p).$$

Καθεμία από τις πλευρές τις τελευταίας ισοτιμίας έχει τιμή $1$ ή $-1$. Αν ήταν διαφορετικές, θα είχαμε ότι $1 \equiv -1 \,(\mathrm{mod}\, p)$ και άρα $p \nmid 2$, το οποίο είναι άτοπο. Άρα οι δυο πλευρές είναι είτε και οι δύο ίσες με $1$ είτε και οι δύο ίσες με $-1$. □

**Θεώρημα 8.3.** *Έστω πρώτος $p > 2$. Γινόμενο δύο τετραγωνικών υπολοίπων $\mathrm{mod}\, p$ ή δύο μη-τετραγωνικών υπολοίπων $\mathrm{mod}\, p$ είναι τετραγωνικό υπόλοιπο $\mathrm{mod}\, p$. Γινόμενο τετραγωνικού υπόλοιπου $\mathrm{mod}\, p$ και μη-τετραγωνικού υπόλοιπου $\mathrm{mod}\, p$ είναι μη-τετραγωνικό υπόλοιπο $\mathrm{mod}\, p$.*

*Απόδειξη.* Αυτό είναι άμεση εφαρμογή του Θεωρήματος 8.2:

$$\Big(\frac{a_1 a_2}{p}\Big) = \Big(\frac{a_1}{p}\Big)\Big(\frac{a_2}{p}\Big).$$

Θα δούμε, όμως, και μια δεύτερη απόδειξη, η οποία δεν χρησιμοποιεί το Θεώρημα 8.2.
(i) Κατ' αρχάς, έστω $a, b$ δύο τετραγωνικά υπόλοιπα $\mathrm{mod}\, p$.
Τότε υπάρχουν $\xi, \eta$ ώστε $\xi^2 \equiv a \,(\mathrm{mod}\, p)$ και $\eta^2 \equiv b \,(\mathrm{mod}\, p)$. Συνεπάγεται ότι $(\xi\eta)^2 \equiv ab \,(\mathrm{mod}\, p)$.
Άρα το $ab$ είναι τετραγωνικό υπόλοιπο $\mathrm{mod}\, p$.
(ii) Κατόπιν, έστω $a$ ένα τετραγωνικό υπόλοιπο $\mathrm{mod}\, p$.

Θεωρούμε ότι το $b$ διατρέχει τους αριθμούς $1, \ldots, p-1$. Τότε το $ab$ διατρέχει τους αριθμούς $a1, \ldots, a(p-1)$, οι οποίοι (επειδή $(a,p)=1$) αποτελούν περιορισμένο σύνολο υπολοίπων mod $p$. Λόγω του Θεωρήματος 8.1, ακριβώς $\frac{p-1}{2}$ από αυτούς τους αριθμούς αποτελούν τετραγωνικά υπόλοιπα mod $p$ και οι υπόλοιποι $\frac{p-1}{2}$ αριθμοί είναι μη-τετραγωνικά υπόλοιπα mod $p$. Όμως, λόγω της περίπτωσης (i), αυτοί οι $ab$ που είναι τετραγωνικά υπόλοιπα mod $p$ προέρχονται από τις $\frac{p-1}{2}$ τιμές του $b$ που είναι τετραγωνικά υπόλοιπα mod $p$.
Άρα οι τιμές του $b$ που είναι μη-τετραγωνικά υπόλοιπα mod $p$ θα δίνουν τιμές του $ab$ που είναι μη-τετραγωνικά υπόλοιπα mod $p$.
(iii) Τέλος, έστω $a$ ένα μη-τετραγωνικό υπόλοιπο mod $p$.
Θεωρούμε πάλι ότι το $b$ διατρέχει τους αριθμούς $1, \ldots, p-1$. Τότε το $ab$ διατρέχει τους αριθμούς $a1, \ldots, a(p-1)$, οι οποίοι (επειδή $(a,p)=1$) αποτελούν περιορισμένο σύνολο υπολοίπων mod $p$. Λόγω του Θεωρήματος 8.1, ακριβώς $\frac{p-1}{2}$ από αυτούς τους αριθμούς αποτελούν τετραγωνικά υπόλοιπα mod $p$ και οι υπόλοιποι $\frac{p-1}{2}$ αριθμοί είναι μη-τετραγωνικά υπόλοιπα mod $p$. Όμως, λόγω του (ii), αυτοί οι $ab$ που είναι μη-τετραγωνικά υπόλοιπα mod $p$ προέρχονται από τις $\frac{p-1}{2}$ τιμές του $b$ που είναι τετραγωνικά υπόλοιπα mod $p$.
Άρα οι τιμές του $b$ που είναι μη-τετραγωνικά υπόλοιπα mod $p$ θα δίνουν τιμές του $ab$ που είναι τετραγωνικά υπόλοιπα mod $p$. □

Και τώρα θα κάνουμε την εξής παρατήρηση: χρησιμοποιώντας το Θεώρημα 8.3 με την δεύτερη απόδειξή του, η οποία δεν εξαρτάται από το Θεώρημα 8.2, μπορούμε να αποδείξουμε το Θεώρημα 8.2. Πράγματι, το Θεώρημα 8.3 μας λέει ότι:

$$\Big(\frac{a_1a_2}{p}\Big) = \Big(\frac{a_1}{p}\Big)\Big(\frac{a_2}{p}\Big).$$

Με επαγωγή καταλήγουμε στο Θεώρημα 8.2.

Άρα τα Θεωρήματα 8.2 και 8.3 είναι ισοδύναμα.

Το προφανές πρόβλημα είναι, δοθέντων πρώτου $p>2$ και $a$ με $(a,p)=1$, να αποφασίσουμε αν το $a$ είναι τετραγωνικό υπόλοιπο mod $p$ ή μη-τετραγωνικό υπόλοιπο mod $p$. Δηλαδή, να βρούμε ποιά από τις τιμές $\pm 1$ έχει το σύμβολο του Legendre $(\frac{a}{p})$.

Το πρόβλημα αυτό ανάγεται σε δυο απλούστερα προβλήματα ως εξής.
(i) Η περίπτωση $a=1$ είναι στοιχειώδης: $(\frac{1}{p})=1$.
(ii) Αν $a>1$ και $a = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ είναι η κανονική αναπαράσταση του $a$, τότε, σύμφωνα με το Θεώρημα 8.2, έχουμε

$$\Big(\frac{a}{p}\Big) = \Big(\frac{p_1}{p}\Big)^{\alpha_1}\cdots\Big(\frac{p_k}{p}\Big)^{\alpha_k}.$$

Παρατηρήστε ότι, επειδή $p \nmid a$, έχουμε $p \neq p_j$ για κάθε $j$. Επομένως, αναγόμαστε στον υπολογισμό της τιμής του $(\frac{q}{p})$ όταν ο $q$ είναι πρώτος $\neq p$.
(iii) Αν $a<0$, τότε $a=-|a|$ και άρα

$$\Big(\frac{a}{p}\Big) = \Big(\frac{-1}{p}\Big)\Big(\frac{|a|}{p}\Big).$$

Καταλήγουμε στο ότι το πρόβλημα ανάγεται στον υπολογισμό των τιμών των

$$\Big(\frac{-1}{p}\Big), \quad \Big(\frac{q}{p}\Big)$$

για πρώτους $p, q$ με $p \neq q$.

Το πρώτο πρόβλημα είναι σχετικά απλό.

**Θεώρημα 8.4.** *Έστω πρώτος $p>2$. Τότε*

$$\Big(\frac{-1}{p}\Big) = (-1)^{\frac{p-1}{2}}.$$

*Απόδειξη.* Από το Κριτήριο του Euler έχουμε ότι

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

και βλέπουμε ότι και οι δύο πλευρές αυτής της ισοτιμίας έχουν τιμές $\pm 1$. Όπως έχουμε ξαναπεί, επειδή $p \nmid 2$, οι δυο πλευρές πρέπει να έχουν είτε και οι δύο τιμή $1$ είτε και οι δύο τιμή $-1$. □

Γνωρίζουμε ότι κάθε πρώτος $p > 2$ είναι είτε της μορφής $4k+1$ είτε της μορφής $4k+3$. Με άλλα λόγια, για κάθε πρώτο $p > 2$ έχουμε είτε $p \equiv 1 \pmod{4}$ είτε $p \equiv 3 \pmod{4}$.

Τώρα, το Θεώρημα 8.4 μπορεί να διατυπωθεί με την εξής ισοδύναμη μορφή.

**Θεώρημα 8.4.** *Έστω πρώτος $p > 2$. Το $-1$ είναι τετραγωνικό υπόλοιπο $\bmod p$ αν $p \equiv 1 \pmod{4}$ και το $-1$ είναι μη-τετραγωνικό υπόλοιπο $\bmod p$ αν $p \equiv 3 \pmod{4}$*

*Απόδειξη.* Αν $p = 4k+1$ ή $p = 4k+3$, τότε

$$(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1 \quad \text{ή} \quad (-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1,$$

αντιστοίχως. □

Υπάρχει και μια άλλη μορφή του Θεωρήματος 8.4 διατυπωμένη με τέτοιο τρόπο που δεν θυμίζει τετραγωνικά υπόλοιπα $\bmod p$.

**Θεώρημα 8.5.** *Έστω αριθμός της μορφής $n^2+1$. Κάθε πρώτος διαιρέτης $p > 2$ του $n^2+1$ είναι $p \equiv 1 \pmod{4}$.*

*Απόδειξη.* Αν ο $p > 2$ πρώτος και $p \mid n^2+1$, συνεπάγεται ότι

$$n^2 \equiv -1 \pmod{p}.$$

Άρα το $-1$ είναι τετραγωνικό υπόλοιπο $\bmod p$, οπότε $p \equiv 1 \pmod{4}$. □

**Παράδειγμα.** Ο αριθμός $442 = 21^2 + 1$ γράφεται $442 = 2 \cdot 13 \cdot 17$. Εκτός από το 2, οι πρώτοι διαιρέτες του $442$ είναι οι $13, 17$ και, πράγματι, $13 \equiv 1 \pmod{4}$ και $17 \equiv 1 \pmod{4}$.

Τώρα θα απαντήσουμε σε ένα "ερώτημα" το οποίο τέθηκε αμέσως μετά από την Πρόταση 4.8.

**Πρόταση 8.2.** *Υπάρχουν άπειροι πρώτοι της μορφής $4n+1$.*

*Απόδειξη.* Έστω ότι υπάρχουν πεπερασμένου πλήθους πρώτοι της μορφής $4n+1$ και έστω ότι αυτοί είναι οι

$$p_1, p_2, \ldots, p_k.$$

Θεωρούμε τον αριθμό

$$N = (2p_1 \cdots p_k)^2 + 1.$$

Ο $N$ είναι $> 1$, οπότε γράφεται ως γινόμενο πρώτων.
Έστω $p$ οποιοσδήποτε πρώτος παράγων του $N$. Είναι προφανές ότι $p > 2$, αφού ο $N$ είναι περιττός.
Από το Θεώρημα 8.5 συνεπάγεται ότι $p \equiv 1 \pmod{4}$, οπότε ο $p$ είναι της μορφής $4n+1$.
Προφανώς, ο $p$ είναι διαφορετικός από τους $p_1, \ldots, p_k$ και καταλήγουμε σε άτοπο. □

## 8.3 Ο Νόμος της Τετραγωνικής Αντιστροφής.

**Λήμμα του Gauss.** *Έστω πρώτος $p > 2$ και $p \nmid a$. Αν $\mu$ ακριβώς από τους αριθμούς*

$$a1,\ a2,\ \ldots,\ a\frac{p-1}{2} \tag{8.5}$$

*δίνουν υπόλοιπο, όταν διαιρεθούν από τον $p$, το οποίο περιλαμβάνεται στους αριθμούς*

$$\frac{p+1}{2},\ \ldots,\ p-1, \tag{8.6}$$

*τότε*

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

*Απόδειξη.* Επειδή $(a,p)=1$, γνωρίζουμε ότι οι αριθμοί

$$a1,\ a2,\ \ldots,\ a(p-1)$$

αποτελούν περιορισμένο σύνολο υπολοίπων $\bmod p$. Δηλαδή, καθένας από αυτούς είναι ισότιμος $\bmod p$ με ακριβώς έναν από τους $1,\ \ldots,p-1$. Περιοριζόμαστε στους μισούς αριθμούς: τους (8.5). Κάποιοι από αυτούς δίνουν υπόλοιπα (όταν διαιρεθούν από τον $p$) από τους αριθμούς

$$1,\ \ldots,\ \frac{p-1}{2} \tag{8.7}$$

και οι υπόλοιποι δίνουν υπόλοιπα από τους αριθμούς (8.6).
Έστω ότι η πρώτη κατηγορία περιλαμβάνει $\lambda$ αριθμούς και η δεύτερη $\mu$ αριθμούς, οπότε

$$\lambda + \mu = \frac{p-1}{2}.$$

Επίσης, έστω ότι τα υπόλοιπα της πρώτης κατηγορίας είναι τα $r_1,\ \ldots,r_\lambda$, οπότε

$$1 \le r_1,\ \ldots,r_\lambda \le \frac{p-1}{2}, \tag{8.8}$$

και τα υπόλοιπα της δεύτερης κατηγορίας είναι τα $s_1,\ \ldots,s_\mu$, οπότε

$$\frac{p+1}{2} \le s_1,\ \ldots,s_\mu \le p-1.$$

Τώρα ορίζουμε

$$r_1' = p - s_1,\ \ldots,\ r_\mu' = p - s_\mu,$$

οπότε

$$1 \le r_1',\ \ldots,r_\mu' \le \frac{p-1}{2}. \tag{8.9}$$

Επομένως, οι αριθμοί (8.5) είναι ισότιμοι $\bmod p$ με τους αριθμούς

$$r_1,\ \ldots,\ r_\lambda,\ s_1,\ \ldots,\ s_\mu$$

ή, ισοδύναμα, με τους

$$r_1,\ \ldots,\ r_\lambda,\ -r_1',\ \ldots,\ -r_\mu'.$$

Άρα

$$(a1)(a2)\cdots\left(a\frac{p-1}{2}\right) \equiv r_1\cdots r_\lambda(-r_1')\cdots(-r_\mu') \,(\bmod p)$$

και άρα

$$a^{\frac{p-1}{2}}1\cdot 2\cdots\frac{p-1}{2} \equiv (-1)^{\mu} r_1\cdots r_\lambda r_1'\cdots r_\mu' \,(\bmod p). \tag{8.10}$$

Κατόπιν, παρατηρούμε ότι, επειδή οι αριθμοί $r_1, \ldots, r_\lambda, s_1, \ldots, s_\mu$ είναι ανά δύο ανισότιμοι $\bmod p$, είναι ανά δύο διαφορετικοί. Άρα οι $r_1, \ldots, r_\lambda$ είναι ανά δύο διαφορετικοί και οι $r'_1, \ldots, r'_\mu$ είναι ανά δύο διαφορετικοί.
Επίσης, εύκολα βλέπουμε ότι κάθε $r_i$ είναι διαφορετικός από κάθε $r'_j$.
Πράγματι, ας υποθέσουμε ότι $r_i = r'_j$, δηλαδή ότι

$$r_i + s_j = p.$$

Επειδή το $r_i$ είναι το υπόλοιπο της διαίρεσης κάποιου $ak$ από τον $p$, όπου $1 \leq k \leq \frac{p-1}{2}$, και το $s_j$ είναι το υπόλοιπο της διαίρεσης κάποιου $al$ από τον $p$, όπου $1 \leq l \leq \frac{p-1}{2}$, συνεπάγεται ότι

$$ak \equiv r_i \,(\mathrm{mod}\, p), \qquad al \equiv s_j \,(\mathrm{mod}\, p),$$

οπότε

$$a(k+l) \equiv r_i + s_j \equiv p \,(\mathrm{mod}\, p)$$

και άρα

$$p \mid a(k+l)$$

και άρα (διότι $(a,p) = 1$)

$$p \mid k + l.$$

Όμως $2 \leq k + l \leq p - 1$ και καταλήγουμε σε άτοπο.
Αποδείξαμε, λοιπόν, ότι οι αριθμοί $r_1, \ldots, r_\lambda, r'_1, \ldots, r'_\mu$ είναι ανά δύο διαφορετικοί. Επειδή αυτοί οι αριθμοί είναι κάποιοι από τους (8.7) και επειδή το πλήθος τους είναι ίσο με $\lambda + \mu = \frac{p-1}{2}$, συμπεραίνουμε ότι αυτοί οι αριθμοί είναι απλώς μια αναδιάταξη των αριθμών (8.7). Άρα

$$r_1 \cdots r_\lambda r'_1 \cdots r'_\mu = 1 \cdot 2 \cdots \frac{p-1}{2}$$

και η (8.10) γίνεται

$$a^{\frac{p-1}{2}} 1 \cdot 2 \cdots \frac{p-1}{2} \equiv (-1)^\mu 1 \cdot 2 \cdots \frac{p-1}{2} \,(\mathrm{mod}\, p).$$

Τώρα, ο $p$ δεν διαιρεί το $1 \cdot 2 \cdots \frac{p-1}{2}$, οπότε

$$a^{\frac{p-1}{2}} \equiv (-1)^\mu \,(\mathrm{mod}\, p).$$

Εφαρμόζουμε το Κριτήριο του Euler και βρίσκουμε ότι

$$\left(\frac{a}{p}\right) \equiv (-1)^\mu \,(\mathrm{mod}\, p).$$

Επειδή οι δυο πλευρές αυτής της ισοτιμίας έχουν τιμές $\pm 1$ και επειδή $p > 2$, συνεπάγεται

$$\left(\frac{a}{p}\right) = (-1)^\mu.$$

□

**Παράδειγμα.** Θα δούμε αν το 7 είναι τετραγωνικό υπόλοιπο $\bmod 11$.
Θεωρούμε τους αριθμούς

$$7 \cdot 1,\ 7 \cdot 2,\ 7 \cdot 3,\ 7 \cdot 4,\ 7 \cdot 5.$$

Τα υπόλοιπα που δίνουν οι αριθμοί αυτοί όταν διαιρεθούν από το 11 είναι οι αριθμοί

$$7,\ 3,\ 10,\ 6,\ 2.$$

Από αυτούς 2 είναι ανάμεσα στα υπόλοιπα $1, 2, 3, 4, 5$ και 3 είναι ανάμεσα στα $6, 7, 8, 9, 10$. Άρα

$$\left(\frac{7}{11}\right) = (-1)^3 = -1.$$

Άρα το 7 είναι μη-τετραγωνικό υπόλοιπο $\bmod 11$.

Άμεση εφαρμογή του Λήμματος του Gauss είναι το επόμενο Θεώρημα.

**Θεώρημα 8.6.** *Έστω πρώτος $p > 2$. Τότε*

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

*Απόδειξη.* Εφαρμόζουμε το Λήμμα του Gauss με $a = 2$.
Θεωρούμε τους αριθμούς

$$2 \cdot 1,\ 2 \cdot 2,\ \ldots,\ 2 \cdot \frac{p-1}{2}.$$

Οι αριθμοί αυτοί βρίσκονται στο διάστημα $1 \leq x \leq p-1$, οπότε ταυτίζονται με τα υπόλοιπά τους όταν διαιρεθούν από τον $p$.
Κατόπιν, προσδιορίζουμε πόσοι από αυτούς περιλαμβάνονται ανάμεσα στους

$$\frac{p+1}{2},\ \ldots,\ p-1.$$

Δηλαδή, βλέπουμε για πόσους $k$ ισχύει

$$\frac{p+1}{2} \leq 2k \leq p-1$$

ή, ισοδύναμα,

$$\frac{p+1}{4} \leq k \leq \frac{p-1}{2}. \tag{8.11}$$

Διακρίνουμε δύο περιπτώσεις:
(i) Αν ο $p$ είναι της μορφής $4n+1$, τότε η (8.11) γίνεται

$$n + \frac{1}{2} \leq k \leq 2n \ \Leftrightarrow\ n+1 \leq k \leq 2n,$$

οπότε το πλήθος των $k$ είναι ίσο με $2n - n = n$.
Άρα το $\mu$ του Λήμματος του Gauss είναι ίσο με $n$, οπότε

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

Από την άλλη μεριά:

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{2n^2+n} = (-1)^n,$$

και άρα

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

(ii) Αν ο $p$ είναι της μορφής $4n+3$, τότε η (8.11) γίνεται

$$n+1 \leq k \leq 2n+1,$$

οπότε το πλήθος των $k$ είναι ίσο με $2n+1-n = n+1$.
Άρα το $\mu$ του Λήμματος του Gauss είναι ίσο με $n+1$, οπότε

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

Όμως,

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{2n^2+3n+1} = (-1)^{n+1},$$

και άρα

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

Σε κάθε περίπτωση η απόδειξη έχει τελειώσει. □

**Θεώρημα 8.7.** *Έστω πρώτος $p > 2$. Το 2 είναι τετραγωνικό υπόλοιπο* $\bmod p$ *αν* $p \equiv 1$ *ή* $7 \pmod 8$ *και το 2 είναι μη-τετραγωνικό υπόλοιπο* $\bmod p$ *αν* $p \equiv 3$ *ή* $5 \pmod 8$

*Απόδειξη.* Ένας πρώτος $p > 2$ είναι είτε της μορφής $8k + 1$ είτε της μορφής $p = 8k + 3$ είτε της μορφής $8k + 5$ είτε της μορφής $p = 8k + 7$.
Στην πρώτη και στην τέταρτη περίπτωση, ο $\frac{p^2-1}{8}$ είναι άρτιος, ενώ στην δεύτερη και στην τρίτη περίπτωση ο $\frac{p^2-1}{8}$ είναι περιττός. □

Και φτάνουμε στον λαμπρό Νόμο της Τετραγωνικής Αντιστροφής που απέδειξε ο Gauss όταν ήταν δεκαεννέα ετών.

**Νόμος της Τετραγωνικής Αντιστροφής.** *Έστω πρώτοι $p, q > 2$ με $p \neq q$. Τότε*

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

*Απόδειξη.* Θα επιστρέψουμε στην απόδειξη του Λήμματος του Gauss με τυχόντα $a$ με $(a, p) = 1$. Θεωρήσαμε τους αριθμούς (8.5):

$$a1,\ a2,\ \ldots,\ a\frac{p-1}{2}.$$

Διαιρέσαμε καθέναν από αυτούς τους αριθμούς με το $p$ και θεωρήσαμε το αντίστοιχο υπόλοιπο. Τώρα θα γίνουμε πιο συγκεκριμένοι:

$$ak = \Big[\frac{ak}{p}\Big]p + u_k, \quad 1 \leq u_k \leq p - 1 \tag{8.12}$$

για κάθε $k = 1, \ldots, \frac{p-1}{2}$.
(Προσέξτε: το υπόλοιπο $u_k$ είναι $\neq 0$, διότι ο $p$ δεν διαιρεί το $ak$. Επίσης, χρησιμοποιούμε το ότι στην διαίρεση του $b$ από τον $a > 0$ το πηλίκο είναι ίσο με $[\frac{b}{a}]$.)
Το υπόλοιπο $u_k$ είναι, όπως είδαμε, δύο ειδών: είτε είναι κάποιο από τα $r_1, \ldots, r_\lambda$, όταν $1 \leq u_k \leq \frac{p-1}{2}$, είτε είναι κάποιο από τα $s_1, \ldots, s_\mu$ ή, ισοδύναμα, κάποιο από τα $p - r'_1, \ldots, p - r'_\mu$, όταν $\frac{p+1}{2} \leq u_k \leq p - 1$.
Επομένως, τα $u_1, \ldots, u_{\frac{p-1}{2}}$ είναι μια αναδιάταξη των $r_1, \ldots, r_\lambda, p - r'_1, \ldots, p - r'_\mu$ και άρα

$$u_1 + \cdots + u_{\frac{p-1}{2}} = r_1 + \cdots + r_\lambda + \mu p - (r'_1 + \cdots + r'_\mu).$$

Άρα, αν αθροίσουμε τις (8.12) για $k = 1, \ldots, \frac{p-1}{2}$, βρίσκουμε

$$a\Big(1 + \cdots + \frac{p-1}{2}\Big) = p\sum_{k=1}^{\frac{p-1}{2}}\Big[\frac{ak}{p}\Big] + r_1 + \cdots + r_\lambda + \mu p - (r'_1 + \cdots + r'_\mu)$$

και, επομένως,

$$a\,\frac{p-1}{2}\,\frac{p+1}{2} = p\sum_{k=1}^{\frac{p-1}{2}}\Big[\frac{ak}{p}\Big] + r_1 + \cdots + r_\lambda + \mu p - (r'_1 + \cdots + r'_\mu). \tag{8.13}$$

Είχαμε δει, επίσης, ότι οι αριθμοί $r_1, \ldots, r_\lambda, r'_1, \ldots, r'_\mu$ είναι μια αναδιάταξη των $1, \ldots, \frac{p-1}{2}$ και άρα

$$1 + \cdots + \frac{p-1}{2} = r_1 + \cdots + r_\lambda + r'_1 + \cdots + r'_\mu,$$

οπότε

$$\frac{p-1}{2}\,\frac{p+1}{2} = r_1 + \cdots + r_\lambda + r'_1 + \cdots + r'_\mu. \tag{8.14}$$

Προσθέτουμε τις (8.13), (8.14) και βρίσκουμε

$$(a+1)\,\frac{p-1}{2}\,\frac{p+1}{2} = p\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right] + 2(r_1+\cdots+r_\lambda) + \mu p. \tag{8.15}$$

Επειδή το $\frac{p-1}{2}\,\frac{p+1}{2}$ είναι γινόμενο δύο διαδοχικών ακεραίων, είναι άρτιος αριθμός. Επίσης, το $2(r_1+\cdots+r_\lambda)$ είναι άρτιο και, επειδή ο $p$ είναι περιττός, από την (8.15) συνεπάγεται ότι το

$$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right] + \mu$$

είναι άρτιο.
Άρα

$$(-1)^\mu = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{ak}{p}]}.$$

Επόμένως, από το Λήμμα του Gauss έχουμε

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{ak}{p}]}.$$

Θέτουμε $a=q$ και μετά εναλλάσσουμε τα $p,q$:

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{qk}{p}]}, \qquad \left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\frac{q-1}{2}}[\frac{pk}{q}]}.$$

Πολλαπλασιάζουμε:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{qk}{p}]+\sum_{k=1}^{\frac{q-1}{2}}[\frac{pk}{q}]}. \tag{8.16}$$

Τώρα θα προσπαθήσουμε να απλοποιήσουμε τον εκθέτη του $-1$ στην ισότητα (8.16).
Στο $xy$-επίπεδο θεωρούμε την ευθεία:

$$l: \qquad y = \frac{q}{p}x$$

και το ορθογώνιο παραλληλόγραμμο:

$$Q: \qquad 0<x<\frac{p}{2}, \quad 0<y<\frac{q}{2}.$$

Παρατηρούμε ότι η ευθεία $l$ διέρχεται από τις κορυφές $(0,0)$ και $(\frac{p}{2},\frac{q}{2})$ του $Q$.
Τώρα θα μετρήσουμε με δύο διαφορετικούς τρόπους το πλήθος των σημείων

$$(k,l): \qquad k,l \text{ ακέραιοι},$$

τα οποία περιέχονται στο ορθογώνιο παραλληλόγραμμο $Q$.
(i) Το $(k,l)$ με ακέραιες συντεταγμένες περιέχεται στο $Q$ αν και μόνο αν $1\le k\le\frac{p-1}{2}$ και $1\le l\le\frac{q-1}{2}$. Άρα το πλήθος των σημείων $(k,l)$ τα οποία περιέχονται στο $Q$ είναι ίσο με

$$\frac{p-1}{2}\,\frac{q-1}{2}.$$

(ii) Κατ' αρχάς παρατηρούμε ότι κανένα σημείο $(k,l)$ του $Q$ με ακέραιες συντεταγμένες δεν βρίσκεται πάνω στην ευθεία $l$.
Πράγματι, αν οι $k,l$ είναι ακέραιοι και $l=\frac{q}{p}k$, τότε $pl=qk$, οπότε (επειδή $(p,q)=1$) συνεπάγεται ότι $p\mid k$ και $q\mid l$. Αυτό είναι αδύνατο όταν $1\le k\le\frac{p-1}{2}$ και $1\le l\le\frac{q-1}{2}$.

Άρα τα σημεία $(k,l)$ του $Q$ με ακέραιες συντεταγμένες χωρίζονται σε δύο ομάδες: αυτά που είναι κάτω και αυτά που είναι πάνω από την διαγώνιο $l$ του $Q$.
Τα σημεία $(k,l)$ του $Q$ με ακέραιες συντεταγμένες που είναι κάτω από την $l$ περιγράφονται από τις

$$1 \leq k \leq \frac{p-1}{2}, \qquad 1 \leq l \leq \frac{q}{p}k.$$

Όταν σταθεροποιήσουμε ένα $k$ με $1 \leq k \leq \frac{p-1}{2}$, τότε τα αντίστοιχα σημεία $(k,l)$ περιγράφονται από την $1 \leq l \leq \frac{q}{p}k$ και άρα το πλήθος τους είναι ίσο με $[\frac{q}{p}k]$. Άρα το πλήθος των σημείων $(k,l)$ του $Q$ με ακέραιες συντεταγμένες που είναι κάτω από την $l$ είναι ίσο με

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right].$$

Τώρα, τα σημεία $(k,l)$ του $Q$ με ακέραιες συντεταγμένες που είναι πάνω από την $l$ περιγράφονται από τις

$$1 \leq l \leq \frac{q-1}{2}, \qquad 1 \leq k \leq \frac{p}{q}l.$$

Όταν σταθεροποιήσουμε ένα $l$ με $1 \leq l \leq \frac{q-1}{2}$, τότε τα αντίστοιχα σημεία $(k,l)$ περιγράφονται από την $1 \leq k \leq \frac{p}{q}l$ και άρα το πλήθος τους είναι ίσο με $[\frac{p}{q}l]$. Άρα το πλήθος των σημείων $(k,l)$ του $Q$ με ακέραιες συντεταγμένες που είναι πάνω από την $l$ είναι ίσο με

$$\sum_{l=1}^{\frac{q-1}{2}} \left[\frac{pl}{q}\right].$$

Άρα το πλήθος όλων των σημείων $(k,l)$ του $Q$ με ακέραιες συντεταγμένες είναι ίσο με

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right] + \sum_{l=1}^{\frac{q-1}{2}} \left[\frac{pl}{q}\right].$$

Εξισώνοντας τα αποτελέσματα των (i), (ii), συμπεραίνουμε ότι

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right] + \sum_{l=1}^{\frac{q-1}{2}} \left[\frac{pl}{q}\right] = \frac{p-1}{2}\,\frac{q-1}{2}.$$

Άρα η (8.16) γίνεται:

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

□

Μια παρατήρηση: επειδή $(\frac{q}{p}) = \pm 1$, ο τύπος στον Νόμο της Τετραγωνικής Αντιστροφής γράφεται ισοδύναμα:

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

Αυτός είναι ο τύπος που θα χρησιμοποιούμε για υπολογισμούς.

Τώρα θα δούμε πώς εφαρμόζουμε τα Θεωρήματα 8.2, 8.4, 8.6 και τον Νόμο της Τετραγωνικής Αντιστροφής για να υπολογίζουμε το σύμβολο του Legendre

$$\left(\frac{a}{p}\right).$$

Ακολουθούμε τους εξής απλούς κανόνες:
(i) Αν ο $a$ είναι αρνητικός, $a = -|a|$, τότε γράφουμε

$$\Big(\frac{a}{p}\Big) = \Big(\frac{-1}{p}\Big)\Big(\frac{|a|}{p}\Big)$$

και αναγόμαστε σε θετικό $a$, διότι, σύμφωνα με το Θεώρημα 8.4, το $(\frac{-1}{p})$ είναι υπολογίσιμο.
(ii) Όποτε εμφανίζεται $(\frac{a}{p})$ με $a > p$, διαιρούμε το $a$ με το $p$,

$$a = kp + r, \quad 0 < r < p,$$

και έχουμε

$$\Big(\frac{a}{p}\Big) = \Big(\frac{r}{p}\Big),$$

διότι $a \equiv r \pmod p$.
Άρα φροντίζουμε ο "πάνω" αριθμός στο σύμβολο του Legendre να είναι μικρότερος από τον "κάτω" αριθμό.
(iii) Αν $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ είναι η κανονική αναπαράσταση του $a$, τότε, σύμφωνα με το Θεώρημα 8.2, έχουμε

$$\Big(\frac{a}{p}\Big) = \Big(\frac{p_1}{p}\Big)^{\alpha_1} \cdots \Big(\frac{p_k}{p}\Big)^{\alpha_k}.$$

Επομένως, αναγόμαστε στον υπολογισμό της τιμής του $(\frac{q}{p})$ όταν ο $q$ είναι πρώτος $\neq p$.
(iv) Για το $(\frac{2}{p})$ εφαρμόζουμε το Θεώρημα 8.6.
(v) Τέλος, για το $(\frac{p}{q})$ με πρώτους $p, q \neq 2$ και $p < q$ χρησιμοποιούμε τον Νόμο της Τετραγωνικής Αντιστροφής και αναγόμαστε στο $(\frac{q}{p})$: έτσι μικραίνουμε διαρκώς τον "κάτω" αριθμό.

**Παράδειγμα.** Θα δούμε αν ο $-164$ είναι τετραγωνικό υπόλοιπο $\bmod 61$ ή, ισοδύναμα, αν υπάρχει ακέραιος $n$ ώστε $61 \mid 164 + n^2$.
Το $61$ είναι πρώτος και αρκεί να υπολογίσουμε το

$$\Big(\frac{-164}{61}\Big).$$

Αν αποφασίσουμε να εφαρμόσουμε το Κριτήριο του Euler, γράφουμε

$$\Big(\frac{-164}{61}\Big) \equiv (-164)^{\frac{61-1}{2}} \equiv (-164)^{30} \pmod{61}$$

και πρέπει να δούμε αν

$$(-164)^{30} \equiv 1 \pmod{61} \qquad \text{ή} \qquad (-164)^{30} \equiv -1 \pmod{61}.$$

Αυτό απαιτεί πολλές πράξεις, οπότε υπολογίζουμε το $(\frac{-164}{61})$ με την διαδικασία που περιγράψαμε πιο πριν.
Για την δεύτερη ισότητα χρησιμοποιούμε το ότι $164 \equiv 42 \pmod{61}$:

$$\begin{aligned}\Big(\frac{-164}{61}\Big) = \Big(\frac{-1}{61}\Big)\Big(\frac{164}{61}\Big) = (-1)^{\frac{61-1}{2}}\Big(\frac{42}{61}\Big) = \Big(\frac{2}{61}\Big)\Big(\frac{3}{61}\Big)\Big(\frac{7}{61}\Big)\\ = (-1)^{\frac{61^2-1}{8}}\Big(\frac{3}{61}\Big)\Big(\frac{7}{61}\Big) = -\Big(\frac{3}{61}\Big)\Big(\frac{7}{61}\Big).\end{aligned} \tag{8.17}$$

Κατόπιν, βλέποντας ότι $61 \equiv 1 \pmod 3$:

$$\Big(\frac{3}{61}\Big) = (-1)^{\frac{61-1}{2}\,\frac{3-1}{2}}\Big(\frac{61}{3}\Big) = \Big(\frac{1}{3}\Big) = 1. \tag{8.18}$$

Επίσης, βλέποντας ότι $61 \equiv 5 \pmod 7$ και $7 \equiv 2 \pmod 5$:

$$\begin{aligned}\left(\frac{7}{61}\right) = (-1)^{\frac{61-1}{2}\,\frac{7-1}{2}}\left(\frac{61}{7}\right) = \left(\frac{5}{7}\right) = (-1)^{\frac{5-1}{2}\,\frac{7-1}{2}}\left(\frac{7}{5}\right)\\ = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.\end{aligned} \tag{8.19}$$

Από τις (8.17), (8.18),(8.19) έχουμε

$$\left(\frac{-164}{61}\right) = 1.$$

Άρα ο $-164$ είναι τετραγωνικό υπόλοιπο $\bmod 61$.

## 8.4 Αθροίσματα δύο τετραγώνων.

Ο στόχος μας σ'αυτήν την ενότητα είναι να χαρακτηρίσουμε τους φυσικούς οι οποίοι είναι αθροίσματα δύο τετραγώνων.

**Λήμμα 8.2.** *Έστω πρώτος $p$ και $(a,p)=1$. Η εξίσωση*

$$ax \equiv y \pmod p$$

*έχει τουλάχιστον μία λύση $x_0, y_0$ με*

$$0 < |x_0| < \sqrt{p}, \quad 0 < |y_0| < \sqrt{p}.$$

*Απόδειξη.* Θεωρούμε όλους τους αριθμούς

$$ax - y$$

οι οποίοι σχηματίζονται παίρνοντας ζευγάρια $(x,y)$ με

$$0 \le x \le [\sqrt{p}], \quad 0 \le y \le [\sqrt{p}]. \tag{8.20}$$

Κατ' αρχάς παρατηρούμε ότι ο αριθμός $\sqrt{p}$ δεν είναι ακέραιος. (Αν ήταν θα ίσχυε $p = n^2$ για κάποιον ακέραιο $n$ και αυτό είναι αδύνατο.) Άρα

$$[\sqrt{p}] < p < [\sqrt{p}] + 1.$$

Το πλήθος των ζευγαριών $(x,y)$ που παίρνουμε είναι ίσο με $([\sqrt{p}]+1)^2 > (\sqrt{p})^2 = p$. Άρα οι αντίστοιχοι αριθμοί $ax-y$ δεν μπορεί να είναι ανά δύο ανισότιμοι $\bmod p$ και, επομένως, υπάρχουν δύο διαφορετικά ζευγάρια $(x_1,y_1)$ και $(x_2,y_2)$, τα οποία ικανοποιούν τις (8.20) και ώστε

$$ax_1 - y_1 \equiv ax_2 - y_2 \pmod p.$$

Ορίζουμε

$$x_0 = x_1 - x_2, \quad y_0 = y_1 - y_2$$

και τότε

$$ax_0 \equiv y_0 \pmod p.$$

Τώρα, είναι σαφές ότι

$$0 \le |x_0| \le [\sqrt{p}] < \sqrt{p}, \quad 0 \le |y_0| \le [\sqrt{p}] < \sqrt{p}.$$

Επίσης, επειδή τα δύο ζευγάρια είναι διαφορετικά, ένας τουλάχιστον από τους $x_0, y_0$ είναι διαφορετικός από το $0$.
Όμως, είναι εύκολο να δούμε ότι, αν ένας από τους $x_0, y_0$ είναι ίσος με $0$ τότε και οι δύο είναι

ίσοι με 0. Πράγματι, αν $x_0 = 0$, τότε $y_0 \equiv 0 \pmod p$, οπότε $p \mid y_0$ και, επειδή $-p < y_0 < p$, συνεπάγεται $y_0 = 0$. Επίσης, αν $y_0 = 0$, τότε $ax_0 \equiv 0 \pmod p$, οπότε $p \mid ax_0$, οπότε $p \mid x_0$ και, επειδή $-p < x_0 < p$, συνεπάγεται $x_0 = 0$.
Άρα κανένας από τους $x_0, y_0$ δεν είναι ίσος με 0 και άρα

$$0 < |x_0| < \sqrt{p}, \quad 0 < |y_0| < \sqrt{p}.$$

□

**Πρόταση 8.3.** *Αν ο $p > 2$ είναι πρώτος, τότε ο $p$ είναι άθροισμα δύο τετραγώνων αν και μόνο αν $p \equiv 1 \pmod 4$.*

*Απόδειξη.* Αν ο $p > 2$ είναι πρώτος, γνωρίζουμε ότι είναι είτε της μορφής $4n + 1$ είτε της μορφής $4n + 3$ και άρα είτε $p \equiv 1 \pmod 4$ είτε $p \equiv 3 \pmod 4$, αντιστοίχως.
Τώρα, κάθε αριθμός

$$x^2 + y^2$$

είναι είτε $\equiv 0 \pmod 4$ είτε $\equiv 1 \pmod 4$ είτε $\equiv 2 \pmod 4$.
Πράγματι, ο $x$ είναι είτε $\equiv 0 \pmod 4$ είτε $\equiv 1 \pmod 4$ είτε $\equiv 2 \pmod 4$ είτε $\equiv 3 \pmod 4$ και άρα ο $x^2$ είναι είτε $\equiv 0 \pmod 4$ είτε $\equiv 1 \pmod 4$. Ομοίως, ο $y^2$ είναι είτε $\equiv 0 \pmod 4$ είτε $\equiv 1 \pmod 4$.
Άρα ο $x^2 + y^2$ είναι είτε $\equiv 0 \pmod 4$ είτε $\equiv 1 \pmod 4$ είτε $\equiv 2 \pmod 4$.
Άρα, αν $p \equiv 3 \pmod 4$, τότε ο $p$ δεν είναι άθροισμα τετραγώνων.
Τώρα, έστω $p \equiv 1 \pmod 4$.
Σ' αυτήν την περίπτωση γνωρίζουμε ότι

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

που σημαίνει ότι το $-1$ είναι τετραγωνικό υπόλοιπο $\bmod p$ και άρα υπάρχει $a$ ώστε

$$a^2 \equiv -1 \pmod p. \tag{8.21}$$

Είναι σαφές ότι $(a, p) = 1$, οπότε από το Λήμμα 8.2 συνεπάγεται ότι υπάρχουν $x_0, y_0$ ώστε

$$ax_0 \equiv y_0 \pmod p \tag{8.22}$$

και

$$0 < |x_0| < \sqrt{p}, \quad 0 < |y_0| < \sqrt{p}. \tag{8.23}$$

Από τις (8.21), (8.22) συνεπάγεται

$${y_0}^2 \equiv a^2 {x_0}^2 \equiv -{x_0}^2 \pmod p$$

και, επομένως,

$$p \mid {x_0}^2 + {y_0}^2.$$

Από τις (8.23) συνεπάγεται

$$0 < {x_0}^2 + {y_0}^2 < 2p.$$

Το μοναδικό πολλαπλάσιο του $p$ ανάμεσα στους 0 και $2p$ είναι ο $p$. Άρα

$${x_0}^2 + {y_0}^2 = p.$$

□

**Λήμμα 8.3.** *Αν κάποιοι αριθμοί είναι αθροίσματα δύο τετραγώνων, τότε και το γινόμενό τους είναι άθροισμα δύο τετραγώνων.*

*Απόδειξη.* Έστω ότι

$$n = x^2 + y^2, \qquad m = z^2 + w^2.$$

Τότε

$$nm = x^2z^2 + x^2w^2 + y^2z^2 + y^2w^2 = (xz + yw)^2 + (xw - yz)^2.$$

Η περίπτωση περισσοτέρων των δύο αριθμών προκύπτει με επαγωγή. □

Η περίπτωση του 1 είναι απλή: ο 1 γράφεται

$$1 = 1^2 + 0^2$$

και άρα είναι άθροισμα δύο τετραγώνων.

**Θεώρημα 8.8.** *Ένας $n > 1$ είναι άθροισμα δύο τετραγώνων αν και μόνο αν κάθε πρώτος, ο οποίος εμφανίζεται στην κανονική αναπαράσταση του $n$ και ο οποίος είναι $\equiv 3 \pmod 4$, εμφανίζεται με άρτιο εκθέτη.*

*Απόδειξη.* Θεωρούμε την κανονική αναπαράσταση του $n$ και τις διάφορες δυνάμεις $p^\alpha$ που εμφανίζονται σ' αυτήν.
Αν ο εκθέτης $\alpha$ είναι άρτιος, $\alpha = 2\beta$, τότε γράφουμε $p^\alpha = (p^\beta)^2$. Αν ο εκθέτης $\alpha$ είναι περιττός, $\alpha = 2\beta + 1$, τότε γράφουμε $p^\alpha = (p^\beta)^2 p$.
Συγκεντρώνουμε όλα τα τετράγωνο που δημιουργούνται με αυτόν τον τρόπο και το γινόμενό τους το γράφουμε στη μορφή τετραγώνου ενός ακεραίου. Έτσι ο $n$ γράφεται

$$n = m^2 p_1 \cdots p_k,$$

όπου οι $p_1, \ldots, p_k$ είναι εκείνοι οι πρώτοι στην κανονική αναπαράσταση του $n$ οι οποίοι εμφανίζονται με περιττό εκθέτη.
Άρα πρέπει να αποδείξουμε ότι ο $n$ είναι άθροισμα δύο τετραγώνων αν και μόνο αν καθένας από τους $p_1, \ldots, p_k$ είτε είναι ο 2 είτε είναι $\equiv 1 \pmod 4$.
Κατ' αρχάς, αν καθένας από τους $p_1, \ldots, p_k$ είτε είναι ο 2 είτε είναι $\equiv 1 \pmod 4$, τότε όλοι είναι αθροίσματα δύο τετραγώνων: διότι $2 = 1^2 + 1^2$ και λόγω της Πρότασης 8.3. Άρα, σύμφωνα με το Λήμμα 8.3, το γινόμενο $p_1 \cdots p_k$ είναι άθροισμα δύο τετραγώνων, οπότε και ο $n$ είναι άθροισμα δύο τετραγώνων:

$$n = m^2(x^2 + y^2) = (mx)^2 + (my)^2.$$

Αντιστρόφως, έστω ότι ο $n$ είναι άθροισμα δύο τετραγώνων, οπότε

$$m^2 p_1 \cdots p_k = x^2 + y^2.$$

Αν

$$d = (x, y),$$

τότε

$$x = dx_1, \quad y = dy_1, \quad (x_1, y_1) = 1$$

και

$$m^2 p_1 \cdots p_k = d^2({x_1}^2 + {y_1}^2). \tag{8.24}$$

Ο $p_j$ εμφανίζεται στο $m^2$ με άρτιο εκθέτη (είτε διαιρεί το $m$ είτε όχι) και στο $d^2$ με άρτιο εκθέτη (είτε διαιρεί το $d$ είτε όχι). Επομένως, από την (8.24) συνεπάγεται ότι ο $p_j$ διαιρεί το ${x_1}^2 + {y_1}^2$:

$${x_1}^2 + {y_1}^2 \equiv 0 \pmod{p_j}.$$

Έτσι συνεπάγεται ότι $(x_1, p_j) = 1$ και τώρα γνωρίζουμε ότι υπάρχει $a$ ώστε

$$x_1 a \equiv 1 \pmod{p_j}.$$

Από τις δύο τελευταίες σχέσεις έχουμε ότι

$$0 \equiv {x_1}^2 a^2 + {y_1}^2 a^2 \equiv 1 + (y_1 a)^2 \,(\mathrm{mod}\, p_j)$$

και άρα

$$(y_1 a)^2 \equiv -1 \,(\mathrm{mod}\, p_j).$$

Δηλαδή το $-1$ είναι τετραγωνικό υπόλοιπο $\mathrm{mod}\, p_j$ και άρα είτε $p_j = 2$ είτε

$$p_j \equiv 1 \,(\mathrm{mod}\, 4).$$

Άρα ο καθένας από τους $p_1, \ldots, p_k$ είτε είναι ο 2 είτε είναι $\equiv 1 \,(\mathrm{mod}\, 4)$. □

## 8.5 Ασκήσεις.

1. Με την βοήθεια του Λήμματος του Gauss βρείτε τους

$$\Big(\frac{8}{11}\Big), \quad \Big(\frac{7}{13}\Big), \quad \Big(\frac{5}{19}\Big), \quad \Big(\frac{11}{23}\Big), \quad \Big(\frac{6}{31}\Big).$$

2. Υπολογίστε τους

$$\Big(\frac{1234}{4567}\Big), \quad \Big(\frac{3658}{12703}\Big).$$

3. Έστω πρώτος $p > 2$ και $p \nmid a$, $p \nmid b$. Αποδείξτε ότι είτε όλες οι εξισώσεις

$$x^2 \equiv a \,(\mathrm{mod}\, p), \quad y^2 \equiv b \,(\mathrm{mod}\, p), \quad z^2 \equiv ab \,(\mathrm{mod}\, p)$$

έχουν λύση είτε ακριβώς μία έχει λύση.
Με βάση το προηγούμενο, αποδείξτε ότι για κάθε πρώτο $p$ υπάρχει $n$ ώστε

$$p \mid (n^2 - 2)(n^2 - 3)(n^2 - 6).$$

4. Έχει λύση η εξίσωση

$$x^2 + 7y - 2 = 0;$$

5. Έστω πρώτοι $p, q$ ώστε $p \neq q$, $p \equiv q \equiv 3 \,(\mathrm{mod}\, 4)$. Αν η $x^2 \equiv p \,(\mathrm{mod}\, q)$ δεν έχει λύση, αποδείξτε ότι η $x^2 \equiv q \,(\mathrm{mod}\, p)$ έχει λύση.

6. Έστω πρώτος $p > 2$ ώστε $p \nmid a$. Αποδείξτε ότι η εξίσωση

$$ax^2 + bx + c \equiv 0 \,(\mathrm{mod}\, p)$$

έχει λύση αν και μόνο αν $p \mid b^2 - 4ac$ ή το $b^2 - 4ac$ είναι τετραγωνικό υπόλοιπο $\mathrm{mod}\, p$.
Λύστε την $x^2 + 7x + 10 \equiv 0 \,(\mathrm{mod}\, 11)$.
Αποδείξτε οτι η $6x^2 + 5x + 1 \equiv 0 \,(\mathrm{mod}\, p)$ έχει λύση για κάθε πρώτο $p$.

7. Προσδιορίστε τους πρώτους $p$ για τους οποίους η $x^2 \equiv 13 \,(\mathrm{mod}\, p)$ έχει λύση.

8. Έστω πρώτος $p$ ώστε $p \equiv 3 \,(\mathrm{mod}\, 4)$. Αν $a^2 + b^2 \equiv 0 \,(\mathrm{mod}\, p)$, αποδείξτε ότι $a \equiv b \equiv 0 \,(\mathrm{mod}\, p)$.

9. Χρησιμοποιώντας το ότι $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$ για κάθε πρώτο $p > 2$, αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $8k - 1$.

10. Έστω πρώτος $p > 2$. Αποδείξτε ότι

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & \text{αν } p \equiv 1 \text{ ή } 3 \pmod 8 \\ -1, & \text{αν } p \equiv 5 \text{ ή } 7 \pmod 8 \end{cases}$$

Με βάση αυτό το συμπέρασμα, αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $8k + 3$.

11. Έστω πρώτος $p > 3$. Αποδείξτε ότι

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{αν } p \equiv 1 \text{ ή } 11 \pmod{12} \\ -1, & \text{αν } p \equiv 5 \text{ ή } 7 \pmod{12} \end{cases}$$

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & \text{αν } p \equiv 1 \pmod 6 \\ -1, & \text{αν } p \equiv 5 \pmod 6 \end{cases}$$

Με βάση το πρώτο, αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $12k \pm 1$ και, με βάση το δεύτερο, αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $6k + 1$.

12. Αν ο $p > 3$ είναι πρώτος, αποδείξτε ότι ο $p$ διαιρεί το άθροισμα των τετραγωνικών υπολοίπων $\bmod p$.

## 8.6 Λύσεις ασκήσεων.

2. Θα υπολογίσουμε το $(\frac{1234}{4567})$ ή, ισοδύναμα, θα δούμε αν η

$$x^2 \equiv 1234 \pmod{4567}$$

έχει λύση.
Ο $4567$ είναι πρώτος και $1234 = 2 \cdot 617$. Ο $617$ ειναι κι αυτός πρώτος και έχουμε

$$\begin{aligned} \left(\frac{1234}{4567}\right) &= \left(\frac{2}{4567}\right)\left(\frac{617}{4567}\right) = (-1)^{\frac{4567^2-1}{8}}(-1)^{\frac{617-1}{2}\,\frac{4567-1}{2}}\left(\frac{4567}{617}\right) \\ &= \left(\frac{248}{617}\right) = \left(\frac{2}{617}\right)^3\left(\frac{31}{617}\right) = (-1)^{3\frac{617^2-1}{8}}(-1)^{\frac{31-1}{2}\,\frac{617-1}{2}}\left(\frac{617}{31}\right) \\ &= \left(\frac{28}{31}\right) = \left(\frac{2^2}{31}\right)\left(\frac{7}{31}\right) = (-1)^{\frac{7-1}{2}\,\frac{31-1}{2}}\left(\frac{31}{7}\right) = -\left(\frac{3}{7}\right) \\ &= -(-1)^{\frac{3-1}{2}\,\frac{7-1}{2}}\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1. \end{aligned}$$

3. Αυτό που πρέπει να αποδείξουμε είναι ισοδύναμο με το ότι από τις σχέσεις

$$\left(\frac{a}{p}\right) = 1, \quad \left(\frac{b}{p}\right) = 1, \quad \left(\frac{ab}{p}\right) = 1$$

είτε όλες είναι σωστές είτε ακριβώς μία είναι σωστή.
Αυτό, όμως, είναι άμεσο από την

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

4. Μια παραλλαγή: το να έχει λύση η εξίσωση

$$x^2 + 13y - 22 = 0$$

είναι ισοδύναμο με το να έχει λύση η

$$x^2 \equiv 22 \pmod{13}$$

και αυτό είναι ισοδύναμο με το να ισχύει

$$\left(\frac{22}{13}\right) = 1.$$

Όμως,

$$\left(\frac{22}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{3^2}{13}\right) = 1.$$

5. Επειδή $p \equiv q \equiv 3 \pmod 4$, κανένας από τους $p, q$ δεν είναι ίσος με 2 και, επίσης ο $\frac{p-1}{2}\,\frac{q-1}{2}$ είναι περιττός. Άρα

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

Αν η $x^2 \equiv p \pmod q$ δεν έχει λύση, τότε $(\frac{p}{q}) = -1$, οπότε $(\frac{q}{p}) = 1$ και άρα η $x^2 \equiv q \pmod p$ έχει λύση.

8. Αν ο $p$ δεν διαιρεί το $a$, τότε υπάρχει $x$ ώστε

$$ax \equiv 1 \pmod p.$$

Άρα η

$$a^2 + b^2 \equiv 0 \pmod p$$

γίνεται

$$0 \equiv (ax)^2 + (bx)^2 \equiv 1 + (bx)^2 \pmod p$$

και άρα

$$(bx)^2 \equiv -1 \pmod p.$$

Άρα ο $-1$ είναι τετραγωνικό υπόλοιπο mod $p$. Αυτό είναι άτοπο, διότι $p \equiv 3 \pmod 4$.
Άρα $p \mid a$ και από την $a^2 + b^2 \equiv 0 \pmod p$ συνεπάγεται ότι $p \mid b$.
Άρα $a \equiv b \equiv 0 \pmod p$.