1 Στοιχειώδης Θεωρία Αριθμών

1.1. Θεωρία αριθμών στους ακέραιους

Σε αυτό το κεφάλαιο θα δούμε μερικές βασικές ιδιότητες των ακέραιων αριθμών σχετικά με τη διαίρεση. Ο αναγνώστης θα μπορούσε να συμβουλευτεί ένα βιβλίο θεωρίας αριθμών για περισσότερες πληροφορίες όπως τα (Αντωνιάδης και Κοντογεώργης 2015), (Λάκκης 1990) ή το (Stein 2008).

1.1.1 Θεώρημα:
Έστω $a, b \in \mathbb{Z}$ *με* $b \neq 0$. *Υπάρχουν μονοσήμαντα ορισμένα* $p, q \in \mathbb{Z}$ *ώστε*

$$a = bq + r,$$

με $0 \leqslant r < |b|$.

Απόδειξη: Θα υποθέσουμε για απλότητα ότι $b > 0$. Θεωρούμε το σύνολο

$$M = \{a - bt : t \in \mathbb{Z}, a - bt \geq 0\}.$$

Παρατηρούμε ότι το σύνολο M είναι ένα μη κενό σύνολο φυσικών άρα έχει ένα ελάχιστο στοιχείο r. Το στοιχείο αυτό θα είναι το υπόλοιπο της διαίρεσης, ενώ το $q = t$ στο οποίο αντιστοιχεί το r, θα είναι το πηλίκο. Είναι σαφές ότι $0 \leqslant r < b$, γιατί διαφορετικά θα μπορούσαμε να αφαιρέσουμε ακόμα ένα b και να καταλήξουμε σε ένα ακόμα μικρότερο στοιχείο του M, άτοπο.

Για τη μοναδικότητα θεωρούμε δύο διαφορετικές γραφές του a ως

$$a = bq_1 + r_1, a = bq_2 + r_2$$

τις οποίες και αφαιρούμε για να πάρουμε:

$$b(q_1 - q_2) = r_2 - r_1,$$

ενώ

$$-b < r_2 - r_1 < b \Rightarrow -1 < q_1 - q_2 < 1$$

άρα, αφού τα $q_1 - q_2$ είναι ακέραιοι, έχουμε ότι $q_1 = q_2$ άρα και $r_1 = r_2$.

Η περίπτωση $b < 0$ ανάγεται στην περίπτωση $b > 0$ πολλαπλασιάζοντας με -1.

1.1.2 Ορισμός:
Για $a, b \in \mathbb{Z}$ *θα λέμε ότι ο* a *διαιρεί τον* b *και θα γράφουμε* $a \mid b$ *αν και μόνο υπάρχει ακέραιος αριθμός* c *ώστε* $b = ca$. *Ισοδύναμα, το υπόλοιπο της διαίρεσης του* b *με* a *θα πρέπει να είναι ίσο με* 0.

1.1.1. Ιδιότητες διαίρεσης.

1. Αν $a \mid b$ και $a \mid c$, τότε για κάθε $x, y \in \mathbb{Z}$ $a \mid xb + yc$.
2. Αν $a \mid b$ και $b \mid c$, τότε $a \mid c$.
3. Αν $a \mid b$ και $b \mid a$, τότε $a = \pm b$.

1.1.3 Ορισμός:
Ένας φυσικός αριθμός $p > 1$ *θα λέγεται πρώτος αν οι μόνοι θετικοί διαιρέτες του είναι ο εαυτός του και η μονάδα.*

1.1.4 Θεώρημα:
Κάθε θετικός ακέραιος γράφεται ως γινόμενο πρώτων.

Απόδειξη Ας υποθέσουμε ότι το σύνολο των φυσικών αριθμών A που δεν γράφονται ως γινόμενο πρώτων είναι μη κενό. Τότε το σύνολο αυτό έχει ένα ελάχιστο στοιχείο n.

Αν είναι ήδη πρώτος, τότε γράφεται ως γινόμενο πρώτων με τετριμμένο τρόπο, άρα δεν θα μπορούσε να είναι στοιχείο του συνόλου M. Αν δεν είναι πρώτος τότε γράφεται ως γινόμενο

$$n = a \cdot b,$$

όπου τα a, b είναι μη τετριμμένοι διαιρέτες του n, οπότε $1 < a, b < n$. Όμως, αφού το n είναι το ελάχιστο στοιχείο του M, θα έχουμε ότι $a, b \notin M$ και, συνεπώς, τα a, b θα αναλύονται σε γινόμενο πρώτων. Συνεπώς, το ίδιο θα συμβαίνει για το n, άτοπο.

1.1.5 Θεώρημα:
Ευκλείδη Υπάρχουν άπειροι πρώτοι.

Απόδειξη: Έστω ότι υπήρχαν πεπερασμένοι το πλήθος πρώτοι

$$\{p_1, p_2, \ldots, p_N\}.$$

Τότε, το γινόμενό τους

$$S = p_1 \cdot p_2 \cdots p_N$$

θα ήταν ένας φυσικός αριθμός. Ο αριθμός $S + 1$ θα έπρεπε να έχει έναν πρώτο διαιρέτη p, ο οποίος θα ήταν ένας παράγοντας του S. Αφού $p \mid S + 1$ και $p \mid S$, θα έχουμε ότι $p \mid 1$, άτοπο.

$n = x_0 a + y_0 b$

$n \mid a$

$a = nq + r$

$= (x_0 a + y_0 b) q + r$

$(1 - q x_0) a + y_0 b q = r$

$r \in A$ → $0 \le r < n$ (ελάχιστο στοιχείο του A)

$\Rightarrow r = 0$

$n \mid a$

$n \mid b$ άρα το n είναι ένας κοινός διαιρέτης των a, b

Αν $\delta \mid a$, $\delta \mid b$ (τυχαίος κοινός διαιρέτης)

$a = \delta \lambda$

$b = \delta \mu$

$n = x_0 a + y_0 b$

$= x_0 \delta \lambda + y_0 \delta \mu =$

$= \delta (x_0 \lambda + y_0 \mu) \Rightarrow \delta \mid n$

1.1.6 Ορισμός:
Θεωρούμε τους ακέραιους a, b. *Θα ονομάζουμε μέγιστο κοινό διαιρέτη των* a, b *και θα τον συμβολίζουμε με* (a, b), *έναν φυσικό αριθμό* d *ο οποίος ικανοποιεί:*

1. $d \mid a$ *και* $d \mid b$
2. *Αν* $\delta \mid a$ *και* $\delta \mid b$ *τότε* $\delta \mid d$.

Για τους $a, b \in \mathbb{Z}$ θεωρούμε το σύνολο

$$A = \{xa + yb > 0, \text{ με } x, y \in \mathbb{Z}\} \subset \mathbb{N}.$$

Το σύνολο αυτό έχει ένα ελάχιστο στοιχείο, το οποίο ταυτίζεται με τον μέγιστο κοινό διαιρέτη των a, b.

Πράγματι, αν το $n = x_0a + y_0b$ είναι το ελάχιστο στοιχείο του A, τότε

$$n = \pi a + \upsilon \text{ με } 0 \leqslant \upsilon < a.$$

Στην περίπτωση που $\upsilon > 0$ θα είχαμε:

$$n - \pi a = x_0a + y_0b - \pi a = (x_0 - \pi)a + y_0b = \upsilon > 0,$$

δηλαδή το $n - \pi a$ είναι στοιχείο του A γνήσια μικρότερο του ελαχίστου n. Άρα $\upsilon = 0$ και $a \mid n$. Με όμοιο τρόπο $b \mid n$. Τέλος, αν δ είναι ένας άλλος κοινός διαιρέτης των a, b, τότε αυτός θα πρέπει να διαιρεί και το $n = x_0a + y_0b$.

Αποδείξαμε παραπάνω ότι ο μέγιστος κοινός διαιρέτης δύο ακέραιων a, b γράφεται ως $\mathbb{Z}$-γραμμικός συνδυασμός των a, b. Θα δούμε έναν αποτελεσματικό τρόπο εύρεσης των αριθμών $x_0, y_0 \in \mathbb{Z}$ ώστε $(a, b) = x_0a + y_0b$, όταν θα μιλήσουμε για τον αλγόριθμο του Ευκλείδη.

1.1.7 Πρόταση:
Αν ένας πρώτος αριθμός $p \mid ab$, *τότε* $p \mid a$ *είτε* $p \mid b$.

Απόδειξη: Αν $p \mid a$ τότε η απόδειξη έχει τελειώσει. Αν όχι τότε $(a, p) = 1$ συνεπώς υπάρχουν $x, y \in \mathbb{Z}$ με $xa + yp = 1$. Πολλαπλασιάζουμε με b και έχουμε

$$abx + ypb = b,$$

από όπου προκύπτει το ζητούμενο, αφού ο p διαιρεί και τους δύο προσθετέους.

1.1.8 Θεώρημα:
Η ανάλυση ενός ακέραιου αριθμού σε γινόμενο πρώτων παραγόντων είναι μονοσήμαντη αν δεν ληφθεί υπόψη η σειρά των παραγόντων.

Απόδειξη: Ας υποθέσουμε ότι

$$a = \pm p_1^{\nu_1} \cdots p_r^{\nu_r} = \pm q_1^{\mu_1} \cdots q_s^{\mu_s}$$

είναι δύο διαφορετικές αναλύσεις του a ως γινόμενο πρώτων. Επιπλέον, ας υποθέσουμε ότι $r \leqslant s$. Ο πρώτος p_1 διαιρεί το γινόμενο $q_1^{\nu_1} \cdots q_s^{\nu_s}$ άρα ο p_1 διαιρεί κάποιον q_i, και συνεπώς ταυτίζεται με αυτόν. Στην παραπάνω ισότητα διαγράφουμε τους p_1 και q_1 και συνεχίζουμε μέχρι να εξαντληθούν οι

$p \mid \alpha\beta$ αν ο p δεν είναι πρωτος αυτο είναι λαθος

$4 \mid 12 = 6 \cdot 2$ το $4 \nmid 6$ $4 \nmid 2$

$2 \cdot 2 \qquad 2 \cdot 3 \cdot 2$

$r \leq s$

$a = \pm p_1^{\nu_1} \cdots p_r^{\nu_r} = q_1^{\mu_1} \cdots q_s^{\mu_s}$

$p_1 \mid q_1^{\mu_1} \cdots q_s^{\mu_s} \Rightarrow p_1 \mid q_t$ q_t είναι πρωτος οι μοναδικοι διαιρετες του είναι $1, q_t$

$p_1^{\nu_1 - 1} \cdots p_r^{\nu_r} = q_1^{\mu_1} \cdots q_t^{\mu_t - 1} \cdots q_s^{\mu_s}$ $p_1 \neq 1$

$p_1 = q_t$

$1 = q_k^{\alpha_k} \cdots q_s^{\alpha_s}$

δινομενο πρώτων. άτοπο $a > 1$ ∈

$r = s$

Κάθε p_i αριστερα είναι ίσος με κάποιον q_i' δεξιά.

$\alpha = p_1^{\nu_1} \cdots p_r^{\nu_r}$

$\beta = p_1^{\mu_1} \cdots p_r^{\mu_r}$

$\delta = p_1^{\delta_1} \cdots p_r^{\delta_r} \mid \alpha$ αν και μονο αν

$\delta \mid \beta \left[\begin{array}{l} \delta_i \leq \nu_i \\ \delta_i \leq \mu_i \end{array}\right.$

$5^2 \cdot 7 \quad \nmid 5 \cdot 7$

ν_i

εξαναγκάζουν ότι το δ είναι κοινος διαιρετης.

πρώτοι στο αριστερό μέρος. Επειδή το γινόμενο πρώτων δεν μπορεί να είναι μονάδα, ταυτόχρονα θα εξαντληθούν οι πρώτοι και στο δεξί μέρος, οπότε προκύπτει το ζητούμενο.

1.1.9 Πρόταση:
Αν $a = p_1^{\nu_1} \cdots p_r^{\nu_r}$ *και* $b = p_1^{\mu_1} \cdots p_r^{\mu_r}$ *είναι οι αναλύσεις των* a, b *σε γινόμενο πρώτων παραγόντων τότε*

$$(a, b) = p_1^{\min\{\nu_1,\mu_1\}} \cdots p_r^{\min\{\nu_r,\mu_r\}}.$$

Μπορούμε να ορίσουμε τους πρώτους αριθμούς ως εξής:

```
sage: P = Primes(); P
Set of all prime numbers: 2, 3, 5, 7, ...
sage: P.cardinality()
+Infinity
```

Αν θέλουμε να πάρουμε τον n-οστό πρώτο δίνουμε

```
sage: P = Primes()
sage: P.next(10^20)
100000000000000000039
```

Ενώ μπορούμε να παραγοντοποιήσουμε ως εξής:

```
sage:factor(28397492387492387429387)
13 * 2551 * 856300467011198849
```

Μπορούμε να ελέγξουμε αν ένας αριθμός είναι πρώτος

```
sage: 856300467011198849 in P
True
```

Interactive

1.1.2. Γραμμικές Ισοδυναμίες mod m.

1.1.10 Ορισμός:
Θα λέμε ότι οι αριθμοί a, b *είναι ισοδύναμοι modulo* m *και θα το συμβολίζουμε με*

$$a \equiv b \bmod m$$

αν και μόνο αν $m \mid b - a$.

Η σχέση $\equiv$ είναι μια σχέση ισοδυναμίας δηλαδή ικανοποιεί:

1. $a \equiv a \bmod m$
2. $a \equiv b \bmod m \Leftrightarrow b \equiv a \bmod m$
3. Αν $a \equiv b \bmod m$ και $b \equiv c \bmod m$, τότε $a \equiv c \bmod m$.

1.1.11 Πρόταση:
Δύο αριθμοί είναι ισοδύναμοι modulo m αν και μόνο αν έχουν το ίδιο υπόλοιπο όταν διαιρεθούν με m.

Απόδειξη: Γράφουμε $a = \pi_a m + u_a$ και $b = \pi_b m + u_b$. Παρατηρούμε ότι $b - a = m(\pi_b - \pi_a) + u_b - u_a$, άρα $m \mid b - a$ αν και μόνο αν $m \mid (u_b - u_a)$. Όμως, $0 \leqslant u_a, u_b < m$, συνεπώς $-m < u_b - u_a < m$. Άρα $m \mid u_b - u_a$ αν και μόνο αν $u_b = u_a$.

1.1.12 Πρόταση:
Ισχύει ότι αν $a \equiv a' \bmod m$ και $b \equiv b' \bmod m$, τότε

- $a + b \equiv a' + b' \bmod m$
- $a \cdot b \equiv a' \cdot b' \bmod m$

Απόδειξη: Γράφουμε $a = a' + km$, $b = b' + lm$ από όπου έχουμε

$$a + b = (a' + b') + m(k + l)$$

και

$$a \cdot b = (a' + km)(b' + lm) = a' \cdot b' + m(a'l + b'k) + klm^2.$$

Το σύνολο των κλάσεων ισοδυναμίας της σχέσης $\equiv$ εφοδιάζεται με τη δομή αντιμεταθετικού δακτυλίου. Είναι δε ισόμορφο με τον δακτύλιο $\mathbb{Z}/m\mathbb{Z}$, των ακέραιων modulo το κύριο ιδεώδες $m\mathbb{Z}$.

Θα δούμε πώς μπορούμε να κάνουμε κάνουμε πράξεις στο πρόγραμμα sage:

```
sage:Mod(10,3)+Mod(2,3)
0
sage:p=P.next(10^10)
sage:Mod(2^(p-1),p)
1
```

Interactive

1.1.3. Ο αλγόριθμος του Ευκλείδη. Ο αλγόριθμος του Ευκλείδη είναι μια διαδικασία η οποία δέχεται ως είσοδο δύο ακέραιους αριθμούς και όταν ολοκληρωθεί δίνει τον μέγιστο κοινό τους διαιρέτη. Θεωρητικά, για τον υπολογισμό του μέγιστου κοινού διαιρέτη θα μπορούσε να χρησιμοποιηθεί η παραγοντοποίηση των αριθμών. Η μέθοδος αυτή όμως δεν είναι καλή, ιδιαίτερα όταν οι αριθμοί που

Αλγεβρα

Ομάδα, δακτύλιος, σώμα

πράξη

αναρτιση $+ : G \times G \longrightarrow G$

$(\alpha, \beta) \longrightarrow \alpha+\beta$

$\alpha+\beta$

$\alpha+(\beta+\gamma)=(\alpha+\beta)+\gamma$

για κάθε $\alpha \in G$ να υπάρχει 0_G ουδέτερο στοιχείο

$\alpha+0_G = 0_G+\alpha = \alpha$

να υπάρχει το $-\alpha \in G$

$\alpha+(-\alpha)=(-\alpha)+\alpha=0$

ομάδα

Δ Δ Δ

ΟΟΟ

Αφαιρετική διαδικασία

3 αριθμός

$3+4=7$

$A+B$ πρόσθεση πινάκων

$f+g$

Αν επιπλέον ισχύει $\alpha+\beta=\beta+\alpha$ η ομάδα λέγεται αντιμεταθετική αβελιανή.

δακτύλιος

R

$+ \; R \times R \longrightarrow R$

$\cdot \; R \times R \longrightarrow R$

$(\alpha, \beta) \longrightarrow \alpha \cdot \beta$

(αβελιανή ομάδα)

$\alpha \cdot (\beta \cdot \gamma) = (\alpha \beta)\gamma$

$\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$

$(\alpha+\beta)\gamma = \alpha\gamma + \beta\gamma$

δακτύλιος

$\alpha \cdot \beta = \beta\alpha$ αντιμεταθετικο δακτύλιο

$1_R \in R$ $\quad 1_R \alpha = \alpha 1_R = \alpha$ δακτύλιο με μονάδα.

έχουμε να διαχειριστούμε είναι πολύ μεγάλοι αφού, όπως θα δούμε στη συνέχεια, η παραγοντοποίηση είναι μια ακριβή διαδικασία.

Ξεκινάμε με τους αριθμούς $a, b \in \mathbb{Z}$ και εκτελούμε τη διαίρεση με πηλίκο και υπόλοιπο.

$$a = \pi_1 b + u_1, \qquad 0 \leqslant u_1 < |b|$$

Παρατηρούμε ότι $(a, b) = (b, u_1)$ (γιατί;). Στη συνέχεια υπολογίζουμε

$$b = \pi_2 u_1 + u_2 \qquad 0 \leqslant u_2 < u_1.$$

Και πάλι έχουμε $(a, b) = (b, u_1) = (u_1, u_2)$. Συνεχίζουμε με αυτόν τον τρόπο, σχηματίζοντας μια ακολουθία υπολοίπων

$$|b| > u_1 > u_2 > \cdots > u_n > \cdots$$

Είναι σαφές ότι μετά από πεπερασμένα το πλήθος βήματα ($|b|$ το πολύ!) η ακολουθία αυτή θα μηδενιστεί. Ο μέγιστος κοινός διαιρέτης θα είναι ο τελευταίος μη μηδενικός όρος της ακολουθίας αυτής.

$$12839 = 7 \cdot 1728 + 743$$
$$1728 = 2 \cdot 743 + 242$$
$$743 = 3 \cdot 242 + 17$$
$$242 = 14 \cdot 17 + 4$$
$$17 = 4 \cdot 4 + 1$$
$$4 = 4 \cdot 1 + 0$$

Μπορούμε εκτελώντας ανάποδα τον αλγόριθμο του Ευκλείδη να υπολογίσουμε $x, y \in \mathbb{Z}$ ώστε $ax + by = (a, b)$.

Για παράδειγμα

$$1 = 17 - 4 \cdot 4 = 17 - 4(242 - 14 \cdot 17) = 57 \cdot 17 - 4 \cdot 242$$
$$= (743 - 3 \cdot 242)57 - 4 \cdot 242 = 57 \cdot 743 - 175 \cdot 242 =$$
$$= 57 \cdot 743 - 175(1728 - 2 \cdot 743) = 407 \cdot 743 - 175 \cdot 1728 =$$
$$= 407(12839 - 7 \cdot 1728) - 175 \cdot 1728 = 407 \cdot 12839 - 3024 \cdot 1728.$$

Δηλαδή υπολογίσαμε ότι $x = 407$ και $y = -3024$ και για την επιλογή αυτών των αριθμών έχουμε

$$(12839, 1728) = 1 = 407 \cdot 12839 - 3024 \cdot 1728.$$

Μπορούμε να υπολογίσουμε το παραπάνω στο sage ως

```
d,u,v = xgcd(12839,1728);d;u;v
1
407
-3024
```

και να επαληθεύσουμε το αποτέλεσμα

```
d == u*12839 + v*1728
True
```

Interactive

1.1.4. Το Θεώρημα του Κινέζου. Το παρακάτω θεώρημα δίνει μια φυσιολογική διάσπαση του δακτυλίου των ακέραιων modulo m.

1.1.13 Θεώρημα:
Έστω $m = \prod_{i=1}^{n} m_i$ η γραφή ενός φυσικού αριθμού ως γινόμενο αριθμών m_i που είναι ανά δύο πρώτοι μεταξύ τους. Οι παρακάτω δακτύλιοι είναι ισόμορφοι:

$$\frac{\mathbb{Z}}{m\mathbb{Z}} = \prod_{i=1}^{n} \frac{\mathbb{Z}}{m_i\mathbb{Z}}.$$

Απόδειξη: Θεωρούμε τον ομομορφισμό δακτυλίων

$$\psi : \frac{\mathbb{Z}}{m\mathbb{Z}} \longrightarrow \prod_{i=1}^{n} \frac{\mathbb{Z}}{m_i\mathbb{Z}},$$
$$x \bmod m \mapsto (x \bmod m_1, \ldots, x \bmod m_n).$$

Παρατηρούμε ότι $\ker(\psi) = \{0\}$. Πράγματι, αν ένας αριθμός x διαιρείται από τους πρώτους μεταξύ τους αριθμούς m_i, τότε διαιρείται και από τον m. Άρα η συνάρτηση ψ είναι 1-1. Επειδή οι δακτύλιοι έχουν τον ίδιο πληθάριθμο, η συνάρτηση ψ είναι αναγκαστικά και επί.

Παραδοσιακά στα μαθήματα Θεωρίας Αριθμών το παραπάνω θεώρημα εκφράζεται ως εξής: Το σύστημα γραμμικών ισοδυναμίων $(m_i, m_j) = 1$ για $i \neq j$, $m = m_1 \cdots m_n$

$$\begin{aligned} x &\equiv x_1 \bmod m_1 \\ x &\equiv x_2 \bmod m_2 \\ &\vdots \\ x &\equiv x_n \bmod m_n \end{aligned}$$

έχει μοναδική λύση $\bmod m$.

1.1.14 Πρόταση:
Η λύση στο πρόβλημα ισοδυναμιών του Κινέζου υπολογίζεται ως εξής: Υπολογίζουμε τον αριθμό $m = m_1 \cdots m_n$, αλλά και τους αριθμούς $M_i = \frac{m}{m_i}$. Εξ υποθέσεως $(M_i, m_i) = 1$, οπότε υπολογίζουμε μια λύση b_i της εξίσωσης

$$M_i y \equiv 1 \bmod m_i$$

Το

$$x_0 = \sum_{i=1}^{n} x_i M_i b_i$$

είναι μια λύση του συστήματος.

$(R, +, \cdot) \xrightarrow{f} (S, \oplus, \odot)$

η f θα λέγεται ομομορφισμός δακτυλίων.

$$f(a+b) = f(a) \oplus f(b)$$
$$f(a \cdot b) = f(a) \odot f(b)$$

πράξεις στο S

πράξεις στο R

---

f ομομορφισμός δακτυλίων f 1-1 $\Rightarrow$

$$\operatorname{Ker} f = \{ r \in R : f(r) = 0_S \} = \{0_R\}$$

$$m\mathbb{Z} = \bigcap m_i \mathbb{Z}$$

$m_i \mid m \Rightarrow m\mathbb{Z} \subset m_i\mathbb{Z}$ οτιδήποτε είναι πολ/σιο του m είναι και πολ/σιο του m_i

$m\mathbb{Z} \subset \bigcap m_i \mathbb{Z}$

$x = mk = (m_i l) k$

αν έχεις $x = \lambda_i m_i$ τότε

x είναι πολ/σιο του m

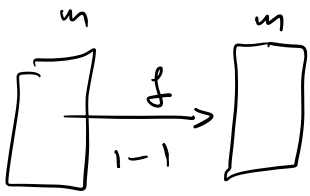
$m = m_1 \cdots m_2 \cdots m_3$

$p_{1,1}^{r_1} \cdots p_{1,k}^{r_k} \quad p_{2,1}^{r_2} \cdots p_{2,k_2}^{r_2} \cdots$

$n = \#\, \mathbb{Z}/n\mathbb{Z}$

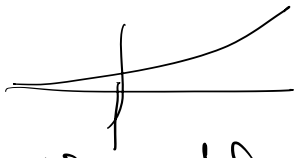
$\#\left(\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z} \right) = n$

m_1 m_2 m_3



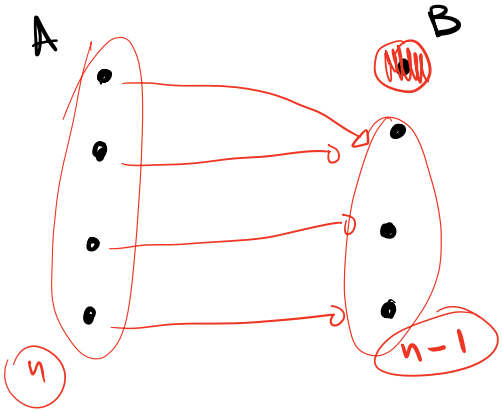
άρα η f είναι επί

$e^x : \mathbb{R} \xrightarrow{1-1} \mathbb{R}$ αλλά όχι επί



πεπερασμένα σύνολα με τον ίδιο πληθάριθμο

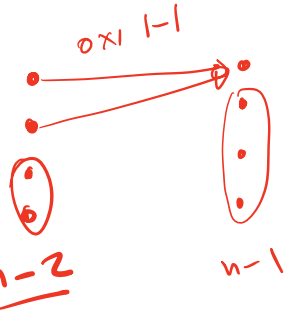
$f : A \longrightarrow B$ αυτή είναι 1-1 αν και μόνο αν είναι επί



Αρχή του "περιστερώνα"

$n-1$

n



$$ax + my = b$$

$(a, m) \mid b$

$b = (a, m)\, b_0$

$(a, m) \mid b$

$b_0 = \frac{b}{(a,m)} \in \mathbb{Z}$

~~Βπάρχουν~~ x_0, y_0

$$ax_0 + my_0 = (a, m)$$

$$\Downarrow$$

$$a(b_0 x_0) + m(y_0 b_0) = (a, m)\, b_0 = b$$

$$ax + my$$

$M_i y \equiv 1 \bmod m_i$

$$x_0 = \sum_{i=1}^{n} x_i M_i b_i$$

Απόδειξη Αρκεί να θεωρήσουμε το x_0 modulo m_i και να παρατηρήσουμε ότι οι προσθετέοι $x_j M_j b_j$ για $i \neq j$ μηδενίζονται, ενώ ο $x_i M_j b_j \equiv x_i \bmod m_i$.

Παράδειγμα Να λυθεί το σύστημα:

$$x \equiv 3 \bmod 5$$

$$x \equiv 3 \bmod 7$$

$$x \equiv 8 \bmod 9$$

Λύση Υπολογίζουμε $m = 5 \cdot 7 \cdot 9 = 315$, $M_1 = 63$, $M_2 = 45$ και $M_3 = 35$. Οι ισοτιμίες $M_i x \equiv 1 \bmod m_i$, $i = 1, 2, 3$ γράφονται $63x \equiv 1 \bmod 5$, $45x \equiv 1 \bmod 7$ και $35x \equiv 1 \bmod 9$ και έχουν λύσεις $b_1 \equiv 2 \bmod 5$, $b_2 \equiv 5 \bmod 7$ και $b_3 \equiv 8 \bmod 9$ αντίστοιχα. Επομένως, η μοναδική λύση του αρχικού συστήματος είναι

$$x_0 \equiv (a_1 M_1 b_1 + a_2 M_2 b_2 + a_3 M_3 b_3) \bmod 315$$

δηλαδή $x_0 = 143 \bmod 315$.

Για να λύσουμε το παραπάνω πρόβλημα στο sage δίνουμε

```
sage:CRT_list([3,3,8], [5,7,9])
143
```

Interactive

1.1.5. Αντιστρέψιμα στοιχεία modulo m..

1.1.5.1. *Η εξίσωση* $ax \equiv b \bmod m$. Παρατηρούμε ότι αναγκαία συνθήκη για να έχει λύση η εξίσωση

$$ax \equiv b \bmod m$$

είναι $(a, m) \mid b$. Η συνθήκη αυτή είναι και ικανή αφού μπορούμε να βρούμε ακέραιους $x, y \in \mathbb{Z}$ ώστε

$$ax + by = (a, b).$$

Άρα, αν $(a, b) \mid b$, τότε $\frac{b}{(a,b)} \in \mathbb{Z}$ και συνεπώς

$$ax\frac{m}{(a,b)} + by\frac{m}{(a,b)} = \frac{m}{(a,b)}(a, b) = m,$$

όπου τα $X := x\frac{m}{(a,b)}$ και $Y := y\frac{m}{(a,b)}$ αποτελούν λύσεις. Αποδείξαμε ότι

1.1.15 Πρόταση:
η εξίσωση $ax + by = d$ *έχει λύσεις αν και μόνο αν* $(a, b) \mid d$.

1.1.5.2. *Αντιστρέψιμα στοιχεία modulo* m.. Η αντιστρεψιμότητα του στοιχείου $a \bmod m$ είναι ισοδύναμη με την υπάρξη λύσης της εξίσωσης $ax \equiv 1 \bmod m$. Άρα με βάση την προηγούμενη πρόταση καταλήγουμε στην

1.1.16 Πρόταση:
Τα αντιστρέψιμα στοιχεία $\mathrm{mod}\,m$ *είναι αυτά τα οποία έχουν μέγιστο κοινό διαιρέτη* $(m, a) = 1$.

Ας υπολογίσουμε τον αντίστροφο του $10\mathrm{mod}13$

```
sage:Mod(10,13)^(-1)
4
```

Interactive

1.1.5.3. *Πλήθος αντιστρέψιμων στοιχείων modulo* m.. Θα συμβολίζουμε με $\phi(m)$ το πλήθος των στοιχείων $0 \leqslant a < m$ που είναι πρώτα προς τον m, δηλαδή

$$\phi(m) = \{a \in \mathbb{Z} : 0 \leqslant a < m, (a, m) = 1\}.$$

Παρατηρούμε ότι αν ο p είναι πρώτος, τότε

$$\phi(p) = p - 1.$$

Ομοίως, στο σύνολο $0 \leqslant a \leqslant p^t$ υπάρχουν p^{t-1} αριθμοί που διαιρούνται με p, αφού αυτοί είναι της μορφής $x = pa'$, και $0 \leqslant a < p^t$, αν και μόνο αν $0 \leqslant a' < p^{t-1}$. Συνεπώς

$$\phi(p^t) = p^t - p^{t-1}.$$

Για να υπολογισουμε την τιμή του ϕ σε σύνθετους αριθμούς χρειαζόμαστε την παρακάτω

1.1.17 Πρόταση:
Αν $(m, n) = 1$ *τότε ισχύει* $\phi(m \cdot n) = \phi(m)\phi(n)$.

Απόδειξη: Παρατηρούμε ότι η συνάρτηση ϕ ταυτίζεται με την τάξη της ομάδας των μονάδων $U(\mathbb{Z}/m\mathbb{Z})$ του δακτυλίου $\mathbb{Z}/m\mathbb{Z}$. Το θεώρημα του Κινέζου εξασφαλίζει ότι

$$U\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right) = \prod_{i=1}^{n} U\left(\frac{\mathbb{Z}}{m_i\mathbb{Z}}\right).$$

Από την παραπάνω σχέση προκύπτει το ζητούμενο αποτέλεσμα.

1.1.18 Πρόταση:
Για κάθε $a \in \mathbb{Z}$, $(a, m) = 1$ *ισχυεί ότι*

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

Απόδειξη: Η τάξη κάθε στοιχείου στην ομάδα $U(\mathbb{Z}/m\mathbb{Z})$ είναι διαιρέτης της τάξης της ομάδας που είναι ίση με $\phi(m)$. Το αποτέλεσμα έπεται.

Ας υπολογίσουμε λίγο με τη συνάρτηση του Euler. Θα την υπολογίσουμε με δύο τρόπους για τον $n = 2015$. Η συνάρτηση prime divisors επιστρέφει ως λίστα τους πρώτους διαιρέτες του n. Παρατηρήστε τη σύνταξη της εντολής prod που διατρέχει τους πρώτους διαιρέτες του n. Η συνάρτηση euler_phi είναι η ενσωματωμένη συνάρτηση του sage.

```
sage:n=2015
sage:prime_divisors(n)
[5, 13, 31]
sage:phi = n*prod([1 - 1/p for p in prime_divisors(n)]); phi
1440
sage:euler_phi(n)
1440
```

Interactive

1.1.6. Αριθμητικές Συναρτήσεις.

1.1.19 Ορισμός:
Μία συνάρτηση $f : \mathbb{N} \to \mathbb{C}$ *θα λέγεται αριθμητική συνάρτηση.*

Ενδιαφέρουσες αριθμητικές συναρτήσεις είναι οι παρακάτω:

1. $d(n) =$ ο αριθμός των (θετικών) διαιρετών του n.
2. $\sigma(n) =$ το άθροισμα των θετικών διαιρετών του n.
3. $\phi(n) =$ ο αριθμός των θετικών ακέραιων $\leqslant n$ που είναι πρώτοι προς τον n.
4. $\nu(n) =$ ο αριθμός των διακεκριμένων πρώτων παραγόντων του n
5. $\Omega(n) =$ ο αριθμός των πρώτων παραγόντων του n
6. $\mu(n) = \begin{cases} 0 & \text{αν ένα τετράγωνο διαιρεί τον } n \\ (-1)^{\nu(n)} & \text{αν ο } n \text{ είναι ελεύθερος τετραγώνου} \end{cases}$

Η $\phi(n)$ λέγεται συνάρτηση του Euler και η $\mu(n)$ συνάρτηση του Möbius.

1.1.20 Θεώρημα:
Θεωρούμε τον φυσικό $n > 1$ *με ανάλυση* $n = \prod_{i=1}^{r} p_i^{a_i}$, $a_i > 0$. *Τότε*

$$d(n) = \prod_{i=1}^{r} (a_i + 1).$$

Απόδειξη Κάθε διαιρέτης του n θα έχει μια παράσταση της μορφής

$$m = p_1^{\ell_1} p_2^{\ell_2} \dots p_r^{\ell_r},$$