Υπολογιστική Θεωρία Αριθμών και Κρυπτογραφία

Εισαγωγή στη Θεωρία Αριθμών

Άρης Παγουρτζής – Στάθης Ζάχος

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Διαιρετότητα

Ορισμός

Για $a, b \in \mathbb{Z}$ θα λέμε ότι ο "a διαιρεί τον b", συμβολικά $a \mid b$, αν υπάρχει $c \in \mathbb{Z}$ τέτοιο ώστε $b = ca$.

Θα λέμε ότι ο a δεν διαιρεί τον b, συμβολικά $a \nmid b$, αν $\forall c \in \mathbb{Z}, b \neq ca$.

Ιδιότητες

Για κάθε $a, b, c \in \mathbb{Z}$:

1. $a \mid a,\ 1 \mid a,\ a \mid 0$.
2. $0 \mid a \Leftrightarrow a = 0$.
3. $a \mid b \wedge b \mid c \Rightarrow a \mid c$.
4. $a \mid b \wedge b \mid a \Rightarrow a = \pm b$.
5. $a \mid b \Rightarrow a \mid bc$.
6. $a \mid b \wedge a \mid c \Rightarrow a \mid (xb + yc) \forall x, y \in \mathbb{Z}$.
7. $a \mid b \Rightarrow |a| \leq |b|$ και $a \mid b \wedge b \geq 0 \Rightarrow a \leq b$.

Διαιρετότητα

Η διαιρετότητα είναι μια σχέση μερικής διάταξης στο $\mathbb{N}$.

Ορολογία

- a γνήσιος διαιρέτης του b: $a \mid b$ και $0 < a < |b|$.
- a μη τετριμμένος διαιρέτης του b: $a \mid b$ και $1 < a < |b|$.
- $p > 1$ πρώτος αριθμός: μοναδικοί διαιρέτες του ο 1 και ο p.
- p, q σχετικά πρώτοι (coprime): μοναδικός κοινός διαιρέτης ο 1.

Ακέραια διαίρεση

Θεώρημα (Ακέραιας Διαίρεσης)

Για κάθε $a, b \in \mathbb{Z}$ με $b > 0$ υπάρχουν μοναδικά q (quotient, πηλίκο), r (remainder, υπόλοιπο) $(q, r \in \mathbb{Z})$ τέτοια ώστε:

$$a = qb + r \qquad \text{και} \qquad 0 \leq r < b$$

Απόδειξη

Έστω το σύνολο $S = \{a - xb \mid x \in \mathbb{Z}, a - xb \geq 0\}$.

- $S \neq \emptyset$ (π.χ. $a - (-|a|b) \in S$) συνεπώς έχει ελάχιστο στοιχείο $r < b$ (γιατί;). Υπάρχει επομένως $q \in \mathbb{Z}$ τέτοιο ώστε

$$a - qb = r \Rightarrow a = qb + r, \quad 0 \leq r < b.$$

Ακέραια διαίρεση

Θεώρημα (Ακέραιας Διαίρεσης)

Για κάθε $a, b \in \mathbb{Z}$ με $b > 0$ υπάρχουν μοναδικά q (quotient, πηλίκο), r (remainder, υπόλοιπο) ($q, r \in \mathbb{Z}$) τέτοια ώστε:

$$a = qb + r \qquad \textit{και} \qquad 0 \le r < b$$

Απόδειξη

Έστω το σύνολο $S = \{a - xb \mid x \in \mathbb{Z}, a - xb \ge 0\}$.

- $S \ne \emptyset$ (π.χ. $a - (-|a|b) \in S$) συνεπώς έχει ελάχιστο στοιχείο $r < b$ (γιατί;). Υπάρχει επομένως $q \in \mathbb{Z}$ τέτοιο ώστε
$$a - qb = r \Rightarrow a = qb + r, \quad 0 \le r < b.$$
- Έστω $q', r' \in \mathbb{Z}$ τέτοια ώστε
$$a = q'b + r', \quad 0 \le r' < b, \text{ επομένως } 0 \le |r' - r| < b.$$
- $qb + r = q'b + r' \Rightarrow (q - q')b = (r' - r) \Rightarrow |q - q'|b = |r' - r|$. Αν $q \ne q'$ τότε $b \le |r' - r|$, άτοπο. Συνεπώς $q = q'$ και $r = r'$.

□

Μέγιστος Κοινός Διαιρέτης (Greatest Common Divisor)

Θεώρημα (ΜΚΔ)

Έστω $a, b \in \mathbb{Z}$ *και* $d = \min\{xa + yb \mid x, y \in \mathbb{Z}, xa + yb \geq 0\}$. *Τότε:*

(i) $d \mid a$ *και* $d \mid b$.

(ii) $d' \mid a \wedge d' \mid b \Rightarrow d' \leq d$.

Μέγιστος Κοινός Διαιρέτης (Greatest Common Divisor)

Θεώρημα (ΜΚΔ)

Έστω $a, b \in \mathbb{Z}$ *και* $d = \min\{xa + yb \mid x, y \in \mathbb{Z}, xa + yb \geq 0\}$. *Τότε:*
(i) $d \mid a$ *και* $d \mid b$.
(ii) $d' \mid a \wedge d' \mid b \Rightarrow d' \leq d$.

Απόδειξη

- (i) Έστω $\kappa, \lambda \in \mathbb{Z}$ τ.ώ. $d = \kappa a + \lambda b$. Θ.δ.ο. $d \mid a$.

Μέγιστος Κοινός Διαιρέτης (Greatest Common Divisor)

Θεώρημα (ΜΚΔ)

Έστω $a, b \in \mathbb{Z}$ *και* $d = \min\{xa + yb \mid x, y \in \mathbb{Z}, xa + yb \geq 0\}$. *Τότε:*
(i) $d \mid a$ *και* $d \mid b$.
(ii) $d' \mid a \wedge d' \mid b \Rightarrow d' \leq d$.

Απόδειξη

- (i) Έστω $\kappa, \lambda \in \mathbb{Z}$ τ.ώ. $d = \kappa a + \lambda b$. Θ.δ.ο. $d \mid a$.
  Έστω $d \nmid a$. Τότε υπάρχουν $q, r \in \mathbb{Z}$ τέτοια ώστε
  $$a = qd + r, \quad 0 < r < d,$$
  $\Rightarrow r = a - qd = a - q(\kappa a + \lambda b) = (1 - q\kappa)a + (-\lambda q)b$
  οπότε $r \in \{xa + yb \mid x, y \in \mathbb{Z}, xa + yb \geq 0\}$ και $r < d$, άτοπο.

Μέγιστος Κοινός Διαιρέτης (Greatest Common Divisor)

Θεώρημα (ΜΚΔ)

Έστω $a, b \in \mathbb{Z}$ *και* $d = \min\{xa + yb \mid x, y \in \mathbb{Z}, xa + yb \geq 0\}$. *Τότε:*
(i) $d \mid a$ *και* $d \mid b$.
(ii) $d' \mid a \wedge d' \mid b \Rightarrow d' \leq d$.

Απόδειξη

- (i) Έστω $\kappa, \lambda \in \mathbb{Z}$ τ.ώ. $d = \kappa a + \lambda b$. Θ.δ.ο. $d \mid a$.
  Έστω $d \nmid a$. Τότε υπάρχουν $q, r \in \mathbb{Z}$ τέτοια ώστε
  $$a = qd + r, \quad 0 < r < d,$$
  $\Rightarrow r = a - qd = a - q(\kappa a + \lambda b) = (1 - q\kappa)a + (-\lambda q)b$
  οπότε $r \in \{xa + yb \mid x, y \in \mathbb{Z}, xa + yb \geq 0\}$ και $r < d$, άτοπο.
  Όμοια δείχνουμε $d \mid b$.

Μέγιστος Κοινός Διαιρέτης (Greatest Common Divisor)

Θεώρημα (ΜΚΔ)

Έστω $a, b \in \mathbb{Z}$ *και* $d = \min\{xa + yb \mid x, y \in \mathbb{Z}, xa + yb \geq 0\}$. *Τότε:*
(i) $d \mid a$ *και* $d \mid b$.
(ii) $d' \mid a \wedge d' \mid b \Rightarrow d' \leq d$.

Απόδειξη

- (i) Έστω $\kappa, \lambda \in \mathbb{Z}$ τ.ώ. $d = \kappa a + \lambda b$. Θ.δ.ο. $d \mid a$.
  Έστω $d \nmid a$. Τότε υπάρχουν $q, r \in \mathbb{Z}$ τέτοια ώστε
  $$a = qd + r, \quad 0 < r < d,$$
  $\Rightarrow r = a - qd = a - q(\kappa a + \lambda b) = (1 - q\kappa)a + (-\lambda q)b$
  οπότε $r \in \{xa + yb \mid x, y \in \mathbb{Z}, xa + yb \geq 0\}$ και $r < d$, άτοπο.
  Όμοια δείχνουμε $d \mid b$.
- (ii) Έστω d' τέτοιο ώστε $d' \mid a$ και $d' \mid b$. Τότε
  $a = c_1 d', b = c_2 d'$. Επομένως:
  $$d = \kappa c_1 d' + \lambda c_2 d' \Rightarrow d' \mid d \Rightarrow d' \leq d.$$

ΜΚΔ: χρήσιμες ιδιότητες

Σαν πορίσματα του προηγούμενου θεωρήματος προκύπτουν τα παρακάτω:

- ο αλγόριθμος του Ευκλείδη βρίσκει τον ΜΚΔ δύο ακεραίων αριθμών (βλ. παρακάτω).
- $\gcd(a, b) = 1 \Rightarrow \exists \kappa, \lambda \in \mathbb{Z}, \quad \kappa a + \lambda b = 1$

  (χρήση σε εύρεση *αντιστρόφου modulo* b: $\kappa a \bmod b = 1$).

ΜΚΔ: χρήσιμες ιδιότητες

Σαν πορίσματα του προηγούμενου θεωρήματος προκύπτουν τα παρακάτω:

- ο αλγόριθμος του Ευκλείδη βρίσκει τον ΜΚΔ δύο ακεραίων αριθμών (βλ. παρακάτω).
- $\gcd(a, b) = 1 \Rightarrow \exists \kappa, \lambda \in \mathbb{Z}, \quad \kappa a + \lambda b = 1$

  (χρήση σε εύρεση *αντιστρόφου modulo* b: $\kappa a \bmod b = 1$).
- Αν $c \mid ab \wedge \gcd(a, c) = 1$ τότε $c \mid b$:

  $\gcd(a, c) = 1 \Rightarrow \exists \kappa, \lambda \in \mathbb{Z} : \kappa c + \lambda a = 1 \Rightarrow \kappa cb + \lambda ab = b \Rightarrow c \mid b$.

ΜΚΔ: χρήσιμες ιδιότητες

Σαν πορίσματα του προηγούμενου θεωρήματος προκύπτουν τα παρακάτω:

- ο αλγόριθμος του Ευκλείδη βρίσκει τον ΜΚΔ δύο ακεραίων αριθμών (βλ. παρακάτω).
- $\gcd(a, b) = 1 \Rightarrow \exists \kappa, \lambda \in \mathbb{Z}, \quad \kappa a + \lambda b = 1$

  (χρήση σε εύρεση *αντιστρόφου modulo* b: $\kappa a \bmod b = 1$).
- Αν $c \mid ab \wedge \gcd(a, c) = 1$ τότε $c \mid b$:

  $\gcd(a, c) = 1 \Rightarrow \exists \kappa, \lambda \in \mathbb{Z} : \kappa c + \lambda a = 1 \Rightarrow \kappa cb + \lambda ab = b \Rightarrow c \mid b$.
- Αν p πρώτος $\wedge\, p \mid ab$ τότε $p \mid a \,\vee\, p \mid b$:

  Αν $gcd(p, a) = p$ τότε $p \mid a$. Αν $gcd(p, a) = 1$, αφού $p \mid ab$ θα πρέπει $p \mid b$.

Θεμελιώδες Θεώρημα Αριθμητικής

Κάθε ακέραιος αριθμός $n > 1$ μπορεί να γραφτεί με μοναδικό τρόπο ως πεπερασμένο γινόμενο πρώτων αριθμών.

- Απόδειξη ύπαρξης: με τη μέθοδο της επαγωγής.
- Απόδειξη μοναδικότητας: στηρίζεται στην ιδιότητα "αν p πρώτος $\wedge\, p \mid ab$ τότε $p \mid a \vee p \mid b$" σε συνδυασμό με χρήση επαγωγής.

  Άσκηση: συμπληρώστε τις λεπτομέρειες.

Παραδείγματα

- $2, 3, 5, \ldots, 1997, \ldots, 6469, \ldots$
- $(333 + 10^{793})10^{791} + 1$ (με 1585 ψηφία, παλίνδρομος βρέθηκε το 1987 από τον H. Dubner)
- $2^{1257787} - 1$ (με 378632 ψηφία βρέθηκε το 1996)
- $2^{13466917} - 1$ (με 4053946 ψηφία βρέθηκε το 2001)
- $2^{43112609} - 1$ (με 12978189 ψηφία βρέθηκε το 2008)
- $2^{57885161} - 1$ (με 17425170 ψηφία βρέθηκε το 2013)
- $2^{74207281} - 1$ (με 22338618 ψηφία βρέθηκε το 2016)

Θεώρημα (Ευκλείδη)

Οι πρώτοι αριθμοί είναι άπειροι σε πλήθος.

Απόδειξη. Εστω ότι οι πρώτοι είναι πεπερασμένοι σε πλήθος, συγκεκριμένα $p_1, p_2, \ldots, p_n$. Τότε ο αριθμός $p_1 p_2 \ldots p_n + 1$ δε διαιρείται από κανένα πρώτο παρά μόνο από το 1 και τον εαυτό του, άρα είναι πρώτος, κάτι που είναι άτοπο. □

Αλγόριθμος Ευκλείδη

function gcd(a,b: integer);
  if $b = 0$ **then** gcd $\leftarrow a$ **else** gcd $\leftarrow \text{gcd}(b, a \bmod b,)$

Αλγόριθμος Ευκλείδη

function gcd(a,b: integer);

  if $b = 0$ **then** gcd $\leftarrow a$ **else** gcd $\leftarrow \text{gcd}(b, a \bmod b,)$

Θεώρημα (ορθότητα Ευκλείδειου αλγορίθμου)

ο αλγόριθμος του Ευκλείδη βρίσκει τον ΜΚΔ δύο ακεραίων αριθμών.

Απόδειξη

- Βρίσκει διαιρέτη: αν $a, b > 0 \in \mathbb{Z}$ τότε $\text{gcd}(a, b) = \text{gcd}(b, a \bmod b)$.
- Ο διαιρέτης που βρίσκει μπορεί να γραφτεί σαν γραμμικός συνδυασμός των a, b (γιατί;).
- Επομένως είναι ο ΜΚΔ.

Αλγόριθμος Ευκλείδη

$$
\begin{aligned}
1742 &= 3 \cdot 494 + 260 & 132 &= 3 \cdot 35 + 27 \\
494 &= 1 \cdot 260 + 234 & 35 &= 1 \cdot 27 + 8 \\
260 &= 1 \cdot 234 + 26 & 27 &= 3 \cdot 8 + 3 \\
234 &= 9 \cdot 26 + 0 & 8 &= 2 \cdot 3 + 2 \\
 & & 3 &= 1 \cdot 2 + 1 \\
 & & 2 &= 2 \cdot 1 + 0
\end{aligned}
$$

$\gcd(1742, 494) = 26, \quad \gcd(132, 35) = 1.$

Αλγόριθμος Ευκλείδη

$$\begin{aligned} 1742 &= 3 \cdot 494 + 260 \\ 494 &= 1 \cdot 260 + 234 \\ 260 &= 1 \cdot 234 + 26 \\ 234 &= 9 \cdot 26 + 0 \end{aligned} \qquad \begin{aligned} 132 &= 3 \cdot 35 + 27 \\ 35 &= 1 \cdot 27 + 8 \\ 27 &= 3 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$\gcd(1742, 494) = 26, \quad \gcd(132, 35) = 1.$$

- Χρόνος εκτέλεσης: $O(\log a)$ διαιρέσεις, $O(\log^3 a)$ bit operations (υποθέτοντας $a \geq b$).

Αλγόριθμος Ευκλείδη

$$\begin{aligned} 1742 &= 3 \cdot 494 + 260 \\ 494 &= 1 \cdot 260 + 234 \\ 260 &= 1 \cdot 234 + 26 \\ 234 &= 9 \cdot 26 + 0 \end{aligned} \qquad \begin{aligned} 132 &= 3 \cdot 35 + 27 \\ 35 &= 1 \cdot 27 + 8 \\ 27 &= 3 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$\gcd(1742, 494) = 26, \quad \gcd(132, 35) = 1.$

- Χρόνος εκτέλεσης: $O(\log a)$ διαιρέσεις, $O(\log^3 a)$ bit operations (υποθέτοντας $a \geq b$).
- Τα κ, λ τ.ώ. $d = \kappa a + \lambda b$ μπορούν να υπολογιστούν στον ίδιο χρόνο: επεκτατεμένος αλγόριθμος Ευκλείδη.
- Χρήσεις: υπολογισμός αντιστρόφων modulo n, επίλυση γραμμικών ισοτιμιών, κρυπτογραφία δημοσίου κλειδιού (RSA, El Gamal, κ.ά.).

Συνάρτηση ϕ του Euler

Ορισμός

$\phi(n)$ είναι το πλήθος των αριθμών από το 1 μέχρι και n που είναι σχετικά πρώτοι με τον n.

Υπενθύμιση: m, n σχετικά πρώτοι (coprime): μοναδικός κοινός διαιρέτης ο 1.

Ιδιότητες

- $\phi(p) = p - 1$ για p πρώτο.
- $\phi(p^a) = p^a(1 - \frac{1}{p})$ για p πρώτο.
- $\phi(mn) = \phi(m)\phi(n)$ για m, n σχετικά πρώτους.
  Άσκηση: αποδείξτε το.

Παρατήρηση: για σύνθετο n, $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$.

Αριθμητική modulo, ο δακτύλιος $\mathbb{Z}_m$

Σχέση ισοτιμίας (congruence)

- Η πράξη $\bmod m$, $m \in \mathbb{Z}, m > 0$, απεικονίζει το $\mathbb{Z}$ στο $\mathbb{Z}_m = \{0, \ldots, m-1\}$.
- Δύο αριθμοί a, b λέγονται *ισότιμοι modulo* m, συμβολικά $a \equiv b \pmod{m}$, αν έχουν την ίδια απεικόνιση με την πράξη $\bmod m$:

$$a \equiv b \pmod{m} \overset{\text{def}}{\Leftrightarrow} a \bmod m = b \bmod m \Leftrightarrow m \mid (a-b)$$

- Άλλοι συμβολισμοί: $a = b \pmod{m}$ ή και $a \equiv b\ (m)$.
- Είναι σχέση ισοδυναμίας. Κάθε κλάση C_k, $0 \leq k \leq m-1$, περιέχει τους ακεραίους που αφήνουν υπόλοιπο k αν διαιρεθούν με το m.
- $\mathbb{Z}_m = \{C_0, C_1, C_2, \ldots, C_{m-1}\}$. Πιο απλά: $\mathbb{Z}_m = \{0, \ldots, m-1\}$.

Πράξεις στο $\mathbb{Z}_m$

- Πρόσθεση: $C_k + C_j = C_{(k+j) \bmod m}$.
- Πολλαπλασιασμός: $C_k \cdot C_j = C_{kj \bmod m}$.
- Η απεικόνιση $(\mod m) : \mathbb{Z} \mapsto \mathbb{Z}_m$ είναι ομομορφισμός (ακριβέστερα: *επιμορφισμός*).
- Πιο απλά:

$$(a + b) \bmod m = (a \bmod m + b \bmod m) \bmod m \ ,$$
$$(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m \ .$$

- *Πρακτική σημασία*: αντί να κάνουμε τις πράξεις στο $\mathbb{Z}$ και στο τέλος να βρίσκουμε το υπόλοιπο της διαίρεσης με m, μπορούμε να κάνουμε τις πράξεις κατευθείαν στο $\mathbb{Z}_m$: σημαντική μείωση χρόνου εκτέλεσης σε πολλές περιπτώσεις.

Ύψωση σε δύναμη modulo m

Επαναλαμβανόμενος Τετραγωνισμός (Repeated Squaring)

Είσοδος: $a, n, m \in \mathbb{Z}_+$
Έξοδος: $a^n \bmod m$

$x \leftarrow a \bmod m; y \leftarrow 1;$
while $n > 0$ **do**
  if $n \bmod 2 \neq 0$ **then** $y \leftarrow y \cdot x \bmod m;$
  $x \leftarrow x^2 \bmod m$
  $n \leftarrow n \div 2$
end while
output y

Χρόνος εκτέλεσης: $O(\log n)$ επαναλήψεις, $O(\log n \ \log^2 m)$ bit operations.

Θεωρία ομάδων

- Ομάδα (group): ζεύγος $(G, *)$ τέτοιο ώστε:
  - $\forall a, b \in G: \; a * b \in G$
  - $\forall a, b, c \in G: \; a * (b * c) = (a * b) * c$
  - $\exists e \in G, \forall a \in G : a * e = a$ (το e είναι μοναδικό)
  - $\forall a \in G : \exists a^{-1} \in G : a * a^{-1} = e$

Αντιμεταθετική (Αβελιανή) ομάδα: επιπλέον $a * b = b * a$.

Θεωρία ομάδων

- Ομάδα (group): ζεύγος $(G, *)$ τέτοιο ώστε:
  - $\forall a, b \in G : \; a * b \in G$
  - $\forall a, b, c \in G : \; a * (b * c) = (a * b) * c$
  - $\exists e \in G, \forall a \in G : a * e = a$ (το e είναι μοναδικό)
  - $\forall a \in G : \exists a^{-1} \in G : a * a^{-1} = e$

Αντιμεταθετική (Αβελιανή) ομάδα: επιπλέον $a * b = b * a$.
Το ζεύγος $(\mathbb{Z}_m, +)$ είναι αντιμεταθετική ομάδα.

Θεωρία ομάδων

- Ομάδα (group): ζεύγος $(G, *)$ τέτοιο ώστε:
  - $\forall a, b \in G: \; a * b \in G$
  - $\forall a, b, c \in G: \; a * (b * c) = (a * b) * c$
  - $\exists e \in G, \forall a \in G : a * e = a$ (το e είναι μοναδικό)
  - $\forall a \in G : \exists a^{-1} \in G : a * a^{-1} = e$

  Αντιμεταθετική (Αβελιανή) ομάδα: επιπλέον $a * b = b * a$.
  Το ζεύγος $(\mathbb{Z}_m, +)$ είναι αντιμεταθετική ομάδα.
- Τάξη (order) πεπερασμένης ομάδας: η πληθικότητά της.

Θεωρία ομάδων

- Ομάδα (group): ζεύγος $(G, *)$ τέτοιο ώστε:
  - $\forall a, b \in G: \; a * b \in G$
  - $\forall a, b, c \in G: \; a * (b * c) = (a * b) * c$
  - $\exists e \in G, \forall a \in G : a * e = a$ (το e είναι μοναδικό)
  - $\forall a \in G : \exists a^{-1} \in G : a * a^{-1} = e$

  Αντιμεταθετική (Αβελιανή) ομάδα: επιπλέον $a * b = b * a$.
  Το ζεύγος $(\mathbb{Z}_m, +)$ είναι αντιμεταθετική ομάδα.
- Τάξη (order) πεπερασμένης ομάδας: η πληθικότητά της.
- Υποομάδα (subgroup):

$$(S, *) \text{ υποομάδα της } (G, *) \overset{\text{def}}{\Leftrightarrow} S \subseteq G \wedge (S, *) \text{ ομάδα}$$

Θεωρία ομάδων

- Ομάδα (group): ζεύγος $(G, *)$ τέτοιο ώστε:
  - $\forall a, b \in G: \; a * b \in G$
  - $\forall a, b, c \in G: \; a * (b * c) = (a * b) * c$
  - $\exists e \in G, \forall a \in G : a * e = a$ (το e είναι μοναδικό)
  - $\forall a \in G : \exists a^{-1} \in G : a * a^{-1} = e$

  Αντιμεταθετική (Αβελιανή) ομάδα: επιπλέον $a * b = b * a$.
  Το ζεύγος $(\mathbb{Z}_m, +)$ είναι αντιμεταθετική ομάδα.
- Τάξη (order) πεπερασμένης ομάδας: η πληθικότητά της.
- Υποομάδα (subgroup):

$$(S, *) \text{ υποομάδα της } (G, *) \overset{\text{def}}{\Leftrightarrow} S \subseteq G \wedge (S, *) \text{ ομάδα}$$

- **Πρόταση.** $(S, *)$ είναι υποομάδα της $(G, *)$ ανν $S \subseteq G$ και S κλειστό ως προς $*$.

Η πολλαπλασιαστική ομάδα $(U(\mathbb{Z}_m), \cdot)$

Πρόταση. $\gcd(a, m) = 1$ *αν και μόνο αν* $\exists c \in \mathbb{Z}_m$ *τέτοιο ώστε* $a \cdot c \equiv 1 \pmod{m}$.

Η πολλαπλασιαστική ομάδα $(U(\mathbb{Z}_m), \cdot)$

Πρόταση. $\gcd(a, m) = 1$ *αν και μόνο αν* $\exists c \in \mathbb{Z}_m$ *τέτοιο ώστε* $a \cdot c \equiv 1 \pmod{m}$.

Απόδειξη. (i) Ευθύ: με χρήση Θεωρ. ΜΚΔ.

(ii) Αντίστροφο: $\exists x \in \mathbb{Z},\ ax \equiv 1 \pmod{m} \Rightarrow m \mid (ax - 1)$.
Αν $\gcd(a, m) = d > 1$ τότε $d \mid m \mid (ax - 1) \Rightarrow d \mid 1$, άτοπο.

Η πολλαπλασιαστική ομάδα $(U(\mathbb{Z}_m), \cdot)$

Πρόταση. $\gcd(a, m) = 1$ *αν και μόνο αν* $\exists c \in \mathbb{Z}_m$ *τέτοιο ώστε* $a \cdot c \equiv 1 \pmod{m}$.

Απόδειξη. (i) Ευθύ: με χρήση Θεωρ. ΜΚΔ.

(ii) Αντίστροφο: $\exists x \in \mathbb{Z},\ ax \equiv 1 \pmod{m} \Rightarrow m \mid (ax - 1)$.
Αν $\gcd(a, m) = d > 1$ τότε $d \mid m \mid (ax - 1) \Rightarrow d \mid 1$, άτοπο.

Ορισμός

$U(\mathbb{Z}_m) = \{a \in \mathbb{Z}_m : \gcd(a, m) = 1\}$ είναι το σύνολο των σχετικά πρώτων με τον m, που λέγονται και units του $\mathbb{Z}_m$. Περιέχει ακριβώς τα στοιχεία του $\mathbb{Z}_m$ που έχουν αντίστροφο modulo m.

Η πολλαπλασιαστική ομάδα $(U(\mathbb{Z}_m), \cdot)$

Πρόταση. $\gcd(a, m) = 1$ *αν και μόνο αν* $\exists c \in \mathbb{Z}_m$ *τέτοιο ώστε* $a \cdot c \equiv 1 \pmod{m}$.

Απόδειξη. (i) Ευθύ: με χρήση Θεωρ. ΜΚΔ.

(ii) Αντίστροφο: $\exists x \in \mathbb{Z},\ ax \equiv 1 \pmod{m} \Rightarrow m \mid (ax - 1)$.
Αν $\gcd(a, m) = d > 1$ τότε $d \mid m \mid (ax - 1) \Rightarrow d \mid 1$, άτοπο.

Ορισμός

$U(\mathbb{Z}_m) = \{a \in \mathbb{Z}_m : \gcd(a, m) = 1\}$ είναι το σύνολο των σχετικά πρώτων με τον m, που λέγονται και units του $\mathbb{Z}_m$. Περιέχει ακριβώς τα στοιχεία του $\mathbb{Z}_m$ που έχουν αντίστροφο modulo m.

Το $(U(\mathbb{Z}_m), \cdot)$ είναι αντιμεταθετική ομάδα με πληθάριθμο $\phi(m)$.

Για p πρώτο: $U(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^*$.

- Τάξη (order) στοιχείου

$$\text{τάξη } a \stackrel{\text{def}}{=} min\{y \in \mathbb{N} : a^y = e\}$$

- Κυκλική ομάδα (cyclic group):

$$(G, *) \text{ κυκλική} \stackrel{\text{def}}{\Leftrightarrow} \exists g \in (G, *) : \forall x \in G : \exists y \in \mathbb{N} : x = g^y$$

- Γεννήτορας (generator)

$$a \text{ γεννήτορας της } G \stackrel{\text{def}}{\Leftrightarrow} \text{τάξη } a = |G|$$

Πρόταση: μια ομάδα έχει γεννήτορα ανν είναι κυκλική. Η τάξη της ομάδας ισούται με την τάξη του γεννήτορα. (**Άσκηση**: αποδείξτε.)

Άλλες αλγεβρικές δομές: δακτύλιοι, σώματα

Δακτύλιος (ring)

$$
\begin{aligned}
&(R,+,\cdot) \text{ δακτύλιος} \overset{\text{def}}{\Leftrightarrow}\\
&\qquad (R,+) \text{ αντιμεταθετική ομάδα}\\
&\qquad (R,\cdot) \text{ μονοειδές (προσεταιριστική, ουδέτερο)}\\
&\qquad \forall\, a,b,c \in R:\\
&\qquad\quad a\cdot(b+c) = (a\cdot b + a\cdot c)\\
&\qquad\quad (b+c)\cdot a = b\cdot a + c\cdot a \qquad \text{(επιμεριστική)}
\end{aligned}
$$

Το $(\mathbb{Z}_m,+,\cdot)$ είναι αντιμεταθετικός δακτύλιος (commutative ring): η πράξη $\cdot$ έχει επιπλέον την αντιμεταθετική ιδιότητα.

Σώμα (field)

$$(F, +, \cdot) \text{ σώμα } \overset{\text{def}}{\Leftrightarrow} \begin{array}{l} (F, +, \cdot) \text{ αντιμεταθετικός δακτύλιος} \\ (F \setminus \{e_+\}, \cdot) \text{ αντιμεταθετική ομάδα} \end{array}$$

Το $(\mathbb{Z}_p, +, \cdot)$, p πρώτος, είναι σώμα (και συμβολίζεται και $GF(p)$ ή $\mathbb{F}_p$).

Πρόταση. *Κάθε σώμα τάξης p είναι ισομορφικό με το $\mathbb{F}_p$.*

Μικρό Θεώρημα Fermat

Θεώρημα (μικρό Fermat)

$\forall \text{prime } p,\ \forall a \in \mathbb{Z},\ p \nmid a:\ \ a^{p-1} \equiv 1 \pmod{p}$

Απόδειξη.

Για $a \in \mathbb{Z}$ με $p \not| \, a$, τα στοιχεία

$$a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)$$

είναι διαφορετικά ανά δύο στο $\mathbb{Z}_p^*$:

$i \cdot a \equiv j \cdot a \pmod{p} \Rightarrow p \mid a(i-j) \Rightarrow p \mid (i-j) \Rightarrow i \equiv j \pmod{p}$

Επομένως $a^{p-1}(p-1)! \equiv (p-1)! \Rightarrow a^{p-1} \equiv 1 \pmod{p}$. $\square$

Μικρό Θεώρημα Fermat

Θεώρημα (μικρό Fermat)

$\forall \text{prime } p,\ \forall a \in \mathbb{Z},\ p \nmid a:\ \ a^{p-1} \equiv 1 \pmod{p}$

Απόδειξη.

Για $a \in \mathbb{Z}$ με $p \not| a$, τα στοιχεία

$$a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)$$

είναι διαφορετικά ανά δύο στο $\mathbb{Z}_p^*$:

$i \cdot a \equiv j \cdot a \pmod{p} \Rightarrow p \mid a(i-j) \Rightarrow p \mid (i-j) \Rightarrow i \equiv j \pmod{p}$

Επομένως $a^{p-1}(p-1)! \equiv (p-1)! \Rightarrow a^{p-1} \equiv 1 \pmod{p}$. $\square$

Παρόμοια αποδεικνύεται το πιο γενικό:

Θεώρημα (Euler)

$\forall a \in \mathbb{Z}, \gcd(a, m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \pmod{m}$.

Σύμπλοκα, ομάδα πηλίκο

- Σύμπλοκο (coset): το σύνολο $H * a = \{h * a : h \in H, a \in G\}$ λέγεται
  δεξί σύμπλοκο (coset) της H στη G για υποομάδα H της $(G, *)$.

Σύμπλοκα, ομάδα πηλίκο

- Σύμπλοκο (coset): το σύνολο $H * a = \{h * a : h \in H, a \in G\}$ λέγεται
  δεξί σύμπλοκο (coset) της H στη G για υποομάδα H της $(G, *)$.
- Ομάδα πηλίκο (Quotient group) G/H: το σύνολο των συμπλόκων της H στην G
  Το $(G/H, \circledast)$ είναι ομάδα με πράξη
  $(H * a) \circledast (H * b) = H * (a * b)$.

Θεώρημα Lagrange

Αν H είναι υποομάδα της πεπερασμένης ομάδας G τότε

$$|G| = |G/H| \cdot |H|$$

Απόδειξη. Στηρίζεται στο γεγονός ότι δύο σύμπλοκα ταυτίζονται ή είναι ξένα μεταξύ τους.

Θεώρημα Lagrange

Αν H είναι υποομάδα της πεπερασμένης ομάδας G τότε

$$|G| = |G/H| \cdot |H|$$

Απόδειξη. Στηρίζεται στο γεγονός ότι δύο σύμπλοκα ταυτίζονται ή είναι ξένα μεταξύ τους.

Πόρισμα (σημαντικό!): η τάξη ενός στοιχείου μιας πεπερασμένης ομάδας διαιρεί την τάξη της ομάδας:

$$\forall a \in G : \; a^{|G|} = e$$

Αν H είναι υποομάδα της πεπερασμένης ομάδας G τότε

$$|G| = |G/H| \cdot |H|$$

Απόδειξη. Στηρίζεται στο γεγονός ότι δύο σύμπλοκα ταυτίζονται ή είναι ξένα μεταξύ τους.

Πόρισμα (σημαντικό!): η τάξη ενός στοιχείου μιας πεπερασμένης ομάδας διαιρεί την τάξη της ομάδας:

$$\forall a \in G: \ a^{|G|} = e$$

Περαιτέρω πορίσματα: μικρό Θεώρημα Fermat (ομάδα $(\mathbb{Z}_p^*, \cdot)$), Θεώρημα Euler (ομάδα $(U(\mathbb{Z}_m), \cdot)$). Οι αποδείξεις τους χωρίς χρήση Θ. Lagrange προϋπήρχαν.

Θεώρημα Lagrange

Αν H είναι υποομάδα της πεπερασμένης ομάδας G τότε

$$|G| = |G/H| \cdot |H|$$

Απόδειξη. Στηρίζεται στο γεγονός ότι δύο σύμπλοκα ταυτίζονται ή είναι ξένα μεταξύ τους.

Πόρισμα (σημαντικό!): η τάξη ενός στοιχείου μιας πεπερασμένης ομάδας διαιρεί την τάξη της ομάδας:

$$\forall a \in G: \; a^{|G|} = e$$

Περαιτέρω πορίσματα: μικρό Θεώρημα Fermat (ομάδα $(\mathbb{Z}_p^*, \cdot)$), Θεώρημα Euler (ομάδα $(U(\mathbb{Z}_m), \cdot)$). Οι αποδείξεις τους χωρίς χρήση Θ. Lagrange προϋπήρχαν.

Πόρισμα: κάθε ομάδα με τάξη πρώτο αριθμό είναι κυκλική (γιατί; *βρείτε έναν γεννήτορα*).

Μέγεθος γνήσιας υποομάδας

Πόρισμα του Θ. Lagrange

Αν $(S, *)$ *υποομάδα της (πεπερασμένης) ομάδας* $(G, *)$ *και* $S \neq G$ *τότε:*

$$|S| \leq |G|/2$$

Fermat (primality) test

Έλεγχος πρώτων αριθμών Fermat

Για να δούμε αν ένας δοσμένος ακέραιος n είναι πρώτος:

Επιλέγουμε τυχαία $a \in \mathbb{Z}_n$: αν $a^{n-1} \not\equiv 1 \pmod{n}$ τότε n σύνθετος (με βεβαιότητα), αλλιώς λέμε ότι το *n περνάει το test* (ίσως είναι πρώτος).

Στην δεύτερη περίπτωση επαναλαμβάνουμε.

Fermat (primality) test

Έλεγχος πρώτων αριθμών Fermat

Για να δούμε αν ένας δοσμένος ακέραιος n είναι πρώτος:

Επιλέγουμε τυχαία $a \in \mathbb{Z}_n$: αν $a^{n-1} \not\equiv 1 \pmod{n}$ τότε n σύνθετος (με βεβαιότητα), αλλιώς λέμε ότι το *n περνάει το test* (ίσως είναι πρώτος).

Στην δεύτερη περίπτωση επαναλαμβάνουμε.

Πρόταση.

Αν για σύνθετο n υπάρχει ένας μάρτυρας (compositeness witness), δηλ. $\exists a \in \mathbb{Z}_n$, $a^{n-1} \not\equiv 1 \pmod{n}$, τότε υπάρχουν τουλάχιστον $n/2$ μάρτυρες.

Απόδειξη. Χρήση Θ. Lagrange σε ομάδα μη μαρτύρων του $U(\mathbb{Z}_n)$.

Fermat (primality) test

Έλεγχος πρώτων αριθμών Fermat

Για να δούμε αν ένας δοσμένος ακέραιος n είναι πρώτος:

Επιλέγουμε τυχαία $a \in \mathbb{Z}_n$: αν $a^{n-1} \not\equiv 1 \pmod{n}$ τότε n σύνθετος (με βεβαιότητα), αλλιώς λέμε ότι το *n περνάει το test* (ίσως είναι πρώτος).

Στην δεύτερη περίπτωση επαναλαμβάνουμε.

Πρόταση.

Αν για σύνθετο n υπάρχει ένας μάρτυρας (compositeness witness), δηλ. $\exists a \in \mathbb{Z}_n$, $a^{n-1} \not\equiv 1 \pmod{n}$, τότε υπάρχουν τουλάχιστον $n/2$ μάρτυρες.

Απόδειξη. Χρήση Θ. Lagrange σε ομάδα μη μαρτύρων του $U(\mathbb{Z}_n)$.

Έλεγχος Fermat ορθός (*whp*) για σχεδόν όλους τους αριθμούς.

Fermat (primality) test

Έλεγχος πρώτων αριθμών Fermat

Για να δούμε αν ένας δοσμένος ακέραιος n είναι πρώτος:

Επιλέγουμε τυχαία $a \in \mathbb{Z}_n$: αν $a^{n-1} \not\equiv 1 \pmod{n}$ τότε n σύνθετος (με βεβαιότητα), αλλιώς λέμε ότι το *n περνάει το test* (ίσως είναι πρώτος).

Στην δεύτερη περίπτωση επαναλαμβάνουμε.

Πρόταση.

Αν για σύνθετο n υπάρχει ένας μάρτυρας (compositeness witness), δηλ. $\exists a \in \mathbb{Z}_n$, $a^{n-1} \not\equiv 1 \pmod{n}$, τότε υπάρχουν τουλάχιστον $n/2$ μάρτυρες.

Απόδειξη. Χρήση Θ. Lagrange σε ομάδα μη μαρτύρων του $U(\mathbb{Z}_n)$.

Έλεγχος Fermat ορθός (*whp*) για σχεδόν όλους τους αριθμούς.
Εξαίρεση: αριθμοί Carmichael – σύνθετοι χωρίς μάρτυρα Fermat.

Fermat (primality) test

Έλεγχος πρώτων αριθμών Fermat

Για να δούμε αν ένας δοσμένος ακέραιος n είναι πρώτος:

Επιλέγουμε τυχαία $a \in \mathbb{Z}_n$: αν $a^{n-1} \not\equiv 1 \pmod{n}$ τότε n σύνθετος (με βεβαιότητα), αλλιώς λέμε ότι το *n περνάει το test* (ίσως είναι πρώτος).

Στην δεύτερη περίπτωση επαναλαμβάνουμε.

Πρόταση.

Αν για σύνθετο n υπάρχει ένας μάρτυρας (compositeness witness), δηλ. $\exists a \in \mathbb{Z}_n$, $a^{n-1} \not\equiv 1 \pmod{n}$, τότε υπάρχουν τουλάχιστον $n/2$ μάρτυρες.

Απόδειξη. Χρήση Θ. Lagrange σε ομάδα μη μαρτύρων του $U(\mathbb{Z}_n)$.

Έλεγχος Fermat ορθός (*whp*) για σχεδόν όλους τους αριθμούς.
Εξαίρεση: αριθμοί Carmichael – σύνθετοι χωρίς μάρτυρα Fermat.
Αντιμετώπιση: Miller-Rabin test (αργότερα).

Ισοτιμία σε $\mathbb{Z}_m, \mathbb{Z}_n \Leftrightarrow$ ισοτιμία σε $\mathbb{Z}_{mn}$

Πρόταση

Για κάθε $m, n \in \mathbb{N}$ *τ.ω.* $\gcd(m, n) = 1$, *για κάθε* $a, b \in \mathbb{Z}$:

$$a \equiv b \pmod{m} \wedge a \equiv b \pmod{n} \Leftrightarrow a \equiv b \pmod{mn}.$$

Ισοτιμία σε $\mathbb{Z}_m, \mathbb{Z}_n \Leftrightarrow$ ισοτιμία σε $\mathbb{Z}_{mn}$

Πρόταση

Για κάθε $m, n \in \mathbb{N}$ τ.ω. $\gcd(m,n) = 1$, για κάθε $a, b \in \mathbb{Z}$:

$$a \equiv b \pmod{m} \wedge a \equiv b \pmod{n} \Leftrightarrow a \equiv b \pmod{mn}.$$

Απόδειξη.

(i) Ευθύ: $\exists x, y \in \mathbb{Z} : a - b = xm = yn$. Από Θ. ΜΚΔ:

$$\begin{aligned} 1 = \kappa m + \lambda n \Rightarrow x = \kappa x m + \lambda x n &= \kappa y n + \lambda x n \\ &\Rightarrow n \mid x \Rightarrow nm \mid xm = a - b. \end{aligned}$$

Ισοτιμία σε $\mathbb{Z}_m, \mathbb{Z}_n \Leftrightarrow$ ισοτιμία σε $\mathbb{Z}_{mn}$

Πρόταση

Για κάθε $m, n \in \mathbb{N}$ *τ.ω.* $\gcd(m, n) = 1$, *για κάθε* $a, b \in \mathbb{Z}$:

$$a \equiv b \pmod{m} \wedge a \equiv b \pmod{n} \Leftrightarrow a \equiv b \pmod{mn}.$$

Απόδειξη.

(i) Ευθύ: $\exists x, y \in \mathbb{Z} : a - b = xm = yn$. Από Θ. ΜΚΔ:

$$\begin{aligned} 1 = \kappa m + \lambda n \Rightarrow x = \kappa x m + \lambda x n &= \kappa y n + \lambda x n \\ &\Rightarrow n \mid x \Rightarrow nm \mid xm = a - b. \end{aligned}$$

(ii) Αντίστροφο: $a \equiv b \pmod{mn} \Rightarrow mn \mid (a - b) \Rightarrow m \mid (a - b)$, όμοια για n.

$\square$

Δηλαδή, ισοτιμία στο $\mathbb{Z}_m$ και στο $\mathbb{Z}_n$ συνεπάγεται ισοτιμία στο $\mathbb{Z}_{mn}$ και αντίστροφα.

Επιπλέον, *οι ισότιμοι* a_m, a_n *ενός ακεραίου* a *σε* $\mathbb{Z}_m, \mathbb{Z}_n$ *αντίστοιχα καθορίζουν μοναδικά τον ισότιμό του, έστω* a_{mn} *στο* $\mathbb{Z}_{mn}$*, και αντίστροφα.*

Δηλαδή, ισοτιμία στο $\mathbb{Z}_m$ και στο $\mathbb{Z}_n$ συνεπάγεται ισοτιμία στο $\mathbb{Z}_{mn}$ και αντίστροφα.

Επιπλέον, *οι ισότιμοι* a_m, a_n *ενός ακεραίου* a *σε* $\mathbb{Z}_m, \mathbb{Z}_n$ *αντίστοιχα καθορίζουν μοναδικά τον ισότιμό του, έστω* a_{mn} *στο* $\mathbb{Z}_{mn}$*, και αντίστροφα.*

Ο a_{mn} υπάρχει πάντα για m, n σχετικά πρώτους – αποδεικνύεται με χρήση του Θ. ΜΚΔ:
$\exists \kappa, \lambda : 1 = \kappa m + \lambda n \Rightarrow \kappa m \equiv 1 \pmod{n}, \quad \lambda n \equiv 1 \pmod{m}$

Δηλαδή, ισοτιμία στο $\mathbb{Z}_m$ και στο $\mathbb{Z}_n$ συνεπάγεται ισοτιμία στο $\mathbb{Z}_{mn}$ και αντίστροφα.

Επιπλέον, *οι ισότιμοι* a_m, a_n *ενός ακεραίου* a *σε* $\mathbb{Z}_m, \mathbb{Z}_n$ *αντίστοιχα καθορίζουν μοναδικά τον ισότιμό του, έστω* a_{mn} *στο* $\mathbb{Z}_{mn}$*, και αντίστροφα.*

Ο a_{mn} υπάρχει πάντα για m, n σχετικά πρώτους – αποδεικνύεται με χρήση του Θ. ΜΚΔ:
$\exists \kappa, \lambda : 1 = \kappa m + \lambda n \Rightarrow \kappa m \equiv 1 \pmod{n}, \quad \lambda n \equiv 1 \pmod{m}$

Τι μπορούμε να πούμε για την ισοτιμία $\pmod{n}$, $\pmod{m}$ των αριθμών: $\kappa m a_n, \quad \lambda n a_m$

Δηλαδή, ισοτιμία στο $\mathbb{Z}_m$ και στο $\mathbb{Z}_n$ συνεπάγεται ισοτιμία στο $\mathbb{Z}_{mn}$ και αντίστροφα.

Επιπλέον, *οι ισότιμοι* a_m, a_n *ενός ακεραίου* a *σε* $\mathbb{Z}_m, \mathbb{Z}_n$ *αντίστοιχα καθορίζουν μοναδικά τον ισότιμό του, έστω* a_{mn} *στο* $\mathbb{Z}_{mn}$*, και αντίστροφα.*

Ο a_{mn} υπάρχει πάντα για m, n σχετικά πρώτους – αποδεικνύεται με χρήση του Θ. ΜΚΔ:
$\exists \kappa, \lambda : 1 = \kappa m + \lambda n \Rightarrow \kappa m \equiv 1 \pmod{n}, \quad \lambda n \equiv 1 \pmod{m}$

Τι μπορούμε να πούμε για την ισοτιμία $\pmod{n}$, $\pmod{m}$ των αριθμών: $\kappa m a_n, \quad \lambda n a_m$

Ποιος είναι τελικά ο a_{mn};

Δηλαδή, ισοτιμία στο $\mathbb{Z}_m$ και στο $\mathbb{Z}_n$ συνεπάγεται ισοτιμία στο $\mathbb{Z}_{mn}$ και αντίστροφα.

Επιπλέον, *οι ισότιμοι a_m, a_n ενός ακεραίου a σε $\mathbb{Z}_m, \mathbb{Z}_n$ αντίστοιχα καθορίζουν μοναδικά τον ισότιμό του, έστω a_{mn} στο $\mathbb{Z}_{mn}$, και αντίστροφα.*

Ο a_{mn} υπάρχει πάντα για m, n σχετικά πρώτους – αποδεικνύεται με χρήση του Θ. ΜΚΔ:
$\exists \kappa, \lambda : 1 = \kappa m + \lambda n \Rightarrow \kappa m \equiv 1 \pmod{n}, \quad \lambda n \equiv 1 \pmod{m}$

Τι μπορούμε να πούμε για την ισοτιμία $\pmod{n}$, $\pmod{m}$ των αριθμών: $\kappa m a_n, \quad \lambda n a_m$

Ποιος είναι τελικά ο a_{mn};

Αυτή η ιδιότητα γενικεύεται και διατυπώνεται πιο αυστηρά στο περίφημο Κινέζικο Θεώρημα Υπολοίπων.

Κινέζικο Θεώρημα Υπολοίπων (Chinese Remainder Theorem - CRT)

Θεώρημα (Κινέζικο Θεώρημα Υπολοίπων)

Εστω ένα σύστημα ισοτιμιών

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

ώστε $\gcd(m_i, m_j) = 1$ *για* $i \neq j$. *Τότε το σύστημα έχει μοναδική λύση στον δακτύλιο* $\mathbb{Z}_M$, $M = m_1 m_2 \ldots m_k$. *Ισοδύναμα: το σύστημα έχει άπειρες λύσεις στο* $\mathbb{Z}$ *και αν* s_1, s_2 *δύο λύσεις ισχύει* $s_1 \equiv s_2 \pmod{M}$.

Απόδειξη.

Για κάθε $i \in \{1, \ldots, k\}$ ορίζουμε $M_i = \frac{M}{m_i}$. Ισχύει $\gcd(M_i, m_i) = 1$.
Επομένως $\exists N_i \in \mathbb{Z}_{m_i} : N_i \cdot M_i \equiv 1 \pmod{m_i}$.
Επίσης $\forall i \neq j : N_i \cdot M_i \equiv 0 \pmod{m_j}$.

Απόδειξη.

Για κάθε $i \in \{1, \dots, k\}$ ορίζουμε $M_i = \frac{M}{m_i}$. Ισχύει $\gcd(M_i, m_i) = 1$.
Επομένως $\exists N_i \in \mathbb{Z}_{m_i}$: $N_i \cdot M_i \equiv 1 \pmod{m_i}$.
Επίσης $\forall i \neq j$: $N_i \cdot M_i \equiv 0 \pmod{m_j}$.
Οπότε μία λύση είναι η παρακάτω (επαληθεύστε):

$$y = \sum_{i=1}^{k} N_i \cdot M_i \cdot a_i$$

Απόδειξη.

Για κάθε $i \in \{1, \ldots, k\}$ ορίζουμε $M_i = \frac{M}{m_i}$. Ισχύει $\gcd(M_i, m_i) = 1$.
Επομένως $\exists N_i \in \mathbb{Z}_{m_i}$: $N_i \cdot M_i \equiv 1 \pmod{m_i}$.
Επίσης $\forall i \neq j$: $N_i \cdot M_i \equiv 0 \pmod{m_j}$.
Οπότε μία λύση είναι η παρακάτω (επαληθεύστε):

$$y = \sum_{i=1}^{k} N_i \cdot M_i \cdot a_i$$

Αν s_1, s_2 δύο διαφορετικές λύσεις τότε έχουμε ότι για κάθε i,

$$s_1 \equiv s_2 \pmod{m_i}$$

Από πρόταση προηγούμενης διαφάνειας και επαγωγή προκύπτει:

$$s_1 \equiv s_2 \pmod{M}$$

$\square$

Απόδειξη.

Για κάθε $i \in \{1, \ldots, k\}$ ορίζουμε $M_i = \frac{M}{m_i}$. Ισχύει $\gcd(M_i, m_i) = 1$.
Επομένως $\exists N_i \in \mathbb{Z}_{m_i}$: $N_i \cdot M_i \equiv 1 \pmod{m_i}$.
Επίσης $\forall i \neq j$: $N_i \cdot M_i \equiv 0 \pmod{m_j}$.
Οπότε μία λύση είναι η παρακάτω (επαληθεύστε):

$$y = \sum_{i=1}^{k} N_i \cdot M_i \cdot a_i$$

Αν s_1, s_2 δύο διαφορετικές λύσεις τότε έχουμε ότι για κάθε i,

$$s_1 \equiv s_2 \pmod{m_i}$$

Από πρόταση προηγούμενης διαφάνειας και επαγωγή προκύπτει:

$$s_1 \equiv s_2 \pmod{M}$$

□

Πολυπλοκότητα: η επίλυση του συστήματος γίνεται σε πολυωνυμικό χρόνο.