Υπολογιστική Θεωρία Αριθμών και Κρυπτογραφία

Εισαγωγή στη Θεωρία Αριθμών

Άρης Παγουρτζής – Στάθης Ζάχος

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

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

- Έστω $q', r' \in \mathbb{Z}$ τέτοια ώστε
  $a = q'b + r', \quad 0 \leq r' < b$, επομένως $0 \leq |r' - r| < b$.
- $qb + r = q'b + r' \Rightarrow (q - q')b = (r' - r) \Rightarrow |q - q'|b = |r' - r|$.
  Αν $q \neq q'$ τότε $b \leq |r' - r|$, άτοπο. Συνεπώς $q = q'$ και $r = r'$. $\square$

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 $d = \kappa a + \lambda b$, $\kappa, \lambda \in \mathbb{Z}$. 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:
  $$d = \kappa c_1 d' + \lambda c_2 d' \Rightarrow d' \mid d \Rightarrow d' \leq d.$$

$\square$

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 $p \mid b$.

Αλγόριθμος Ευκλείδη

function gcd(a,b: integer);

if $b = 0$ **then** gcd $\leftarrow a$ **else** gcd $\leftarrow$ 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 $\gcd(a, b) = \gcd(b, a \bmod b)$.
- Ο διαιρέτης που βρίσκει μπορεί να γραφτεί σαν γραμμικός συνδυασμός των a, b (γιατί;).
- Επομένως είναι ο ΜΚΔ.

Αλγόριθμος Ευκλείδη

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

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

- 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: επεκτεταμένος αλγόριθμος Ευκλείδη.
- Χρήσεις: υπολογισμός αντιστρόφων modulo n, επίλυση γραμμικών ισοτιμιών, κρυπτογραφία δημοσίου κλειδιού (RSA, El Gamal, κ.ά.).

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.

Πρώτοι αριθμοί

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)
- $2^{43112609} - 1$ (με 12978189 ψηφία βρέθηκε το 2008)
- ....(2013, 2016, 2017)
- $2^{82589933} - 1$ (με 24862048 ψηφία βρέθηκε το 2018)

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. $\square$

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: $a = b \pmod{m}$, $a \equiv b\,(m)$, $a \equiv_m b$.
- Είναι σχέση ισοδυναμίας. Κάθε κλάση C_k, $0 \le k \le m-1$, 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 '$\bmod m$' : $\mathbb{Z} \mapsto \mathbb{Z}_m$ 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.

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)

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

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 $n \mod 2 \neq 0$ **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 $a * b = b * a$.
  Το ζεύγος $(\mathbb{Z}_m, +)$ είναι αντιμεταθετική ομάδα.
- Τάξη (order) πεπερασμένης ομάδας: η πληθικότητά της.
- Υποομάδα (subgroup):
  $(S, *)$ υποομάδα της $(G, *)$ $\overset{\text{def}}{\Leftrightarrow}$ $S \subseteq G \wedge (S, *)$ ομάδα

Πρόταση. Έστω $(G, *)$ πεπερασμένη ομάδα. Η $(S, *)$ είναι υποομάδα της $(G, *)$ ανν $S \subseteq G$ και S κλειστό ως προς $*$.
(Άσκηση: αποδείξτε.)

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

Θεωρία ομάδων

- 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.)

Δακτύλιος (ring)

$(R, +, \cdot)$ δακτύλιος $\overset{\text{def}}{\Leftrightarrow}$

$(R, +)$ αντιμεταθετική ομάδα

$(R, \cdot)$ μονοειδές (προσεταιριστική, ουδέτερο)

$\forall\, a, b, c \in R:$

$$a \cdot (b + c) = (a \cdot b + a \cdot c)$$

$$(b + c) \cdot a = b \cdot a + c \cdot a \quad \text{(επιμεριστική)}$$

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

Άλλες αλγεβρικές δομές: δακτύλιοι, σώματα

Σώμα (field)

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

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 $\mathbb{F}_p$.*

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.

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.

Κάθε ομάδα με τάξη πρώτο αριθμό είναι κυκλική (άρα έχει γεννήτορα). Προσοχή: η $\mathbb{Z}_p^*$ *δεν* έχει τάξη πρώτο (αλλά *είναι* κυκλική!).

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 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 (witness) (δηλ. $a \in \mathbb{Z}_n$, $a^{n-1} \not\equiv 1 \pmod{n}$), τότε υπάρχουν τουλάχιστον $n/2$ μάρτυρες.

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

Πόρισμα: ο έλεγχος Fermat απαντάει σωστά με πολύ μεγάλη πιθανότητα για τους περισσότερους αριθμούς. Εξαιρούνται όμως οι αριθμοί Carmichael: σύνθετοι για τους οποίους δεν υπάρχει μάρτυρας Fermat. Για να καλύψουμε και αυτούς: Miller-Rabin test (αργότερα).

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:

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

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

$\square$

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

- Με άλλα λόγια, *οι ισότιμοι ενός ακεραίου στο $\mathbb{Z}_m$ και στο $\mathbb{Z}_n$, έστω a_m, a_n αντίστοιχα, καθορίζουν μοναδικά τον ισότιμό του στο $\mathbb{Z}_{mn}$, και αντίστροφα*.
- Ο εν λόγω (μοναδικός) ισότιμος υπάρχει πάντα για κάθε $a_m \in \mathbb{Z}_m, a_n \in \mathbb{Z}_n$, για m, n σχετικά πρώτους – αποδεικνύεται με χρήση του Θ. ΜΚΔ:
  $1 = km + ln \Rightarrow km \equiv 1 \pmod{n} \wedge ln \equiv 1 \pmod{m}$
  Άσκηση: συμπληρώστε την απόδειξη. (υπόδειξη: τι ισοτιμίες δίνουν τα παραπάνω αν αντιμεταθέσουμε τους διαιρέτες;)

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 $\forall i \neq j$: $N_i \cdot M_i \equiv 0 \pmod{m_j}$.
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.

Σημαντικές συνέπειες του CRT

Δύο ισομορφισμοί:

$\mathbb{Z}_{m_1 m_2 \ldots m_k} \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_k}$
ως προς πρόσθεση, αφαίρεση και πολλαπλασιασμό (οι πράξεις στις k-άδες ορίζονται κατά μέλη με τον προφανή τρόπο: τα στοιχεία στη θέση i αθροίζονται / πολλαπλασιάζονται στον δακτύλιο $\mathbb{Z}_{m_i}$.)

$U(\mathbb{Z}_{m_1 m_2 \ldots m_k}) \cong U(\mathbb{Z}_{m_1}) \times U(\mathbb{Z}_{m_2}) \times \ldots \times U(\mathbb{Z}_{m_k})$
ως προς πολλαπλασιασμό και διαίρεση.

Η δομή της ομάδας $\mathbb{Z}_p^*$

Η πολλαπλασιαστική ομάδα $\mathbb{Z}_p^*$

- Είναι κυκλική: π.χ. $\mathbb{Z}_{11}^* = \{1, 2, \ldots, 10\} = \{2^1, 2^2, \ldots, 2^{10}\} \pmod{11}$.
- Για κάθε $d \mid (p-1)$ περιέχει ακριβώς μία κυκλική υποομάδα τάξης d (βλ. και Θεμελιώδες Θεώρημα Κυκλικών Ομάδων).
- Περιέχει ακριβώς $\phi(p-1)$ γεννήτορες:
  - μία κυκλική ομάδα τάξης r περιέχει $\phi(r)$ γεννήτορες
  - για $p = 2q+1$, q πρώτο, υπάρχουν $q-1$ γεννήτορες.

Η πολλαπλασιαστική ομάδα $\mathbb{Z}_p^*$

- Έλεγχος αν a γεννήτορας: $\forall d \mid p-1, d < p-1: \ a^{\frac{p-1}{d}} \not\equiv 1 \pmod{p}$. Για $p = 2q+1$, q prime, αν $a \not\equiv -1 \wedge a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, τότε a είναι γεννήτορας.
- Ακριβώς τα μισά στοιχεία είναι τετραγωνικά υπόλοιπα (quadratic residues) modulo p, δηλ. είναι τετράγωνα κάποιου αριθμού modulo p. Τα στοιχεία αυτά ταυτίζονται με τις άρτιες δυνάμεις ενός γεννήτορα:

$$QR(p) = \{g^{2i} \mid 1 \leq i \leq \frac{p-1}{2}\}$$

Η δομή της ομάδας $U(\mathbb{Z}_{pq})$

Η πολλαπλασιαστική ομάδα $U(\mathbb{Z}_{pq})$, p, q πρώτοι

- Δεν είναι κυκλική: κάθε στοιχείο έχει τάξη το πολύ $lcm(p-1, q-1) \mid \frac{(p-1)(q-1)}{2}$ (βλ. και συνάρτηση Carmichael).
  Π.χ. στην $U(\mathbb{Z}_{15}) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ πράγματι, κάθε στοιχείο έχει τάξη το πολύ $4 = lcm(3-1, 5-1)$.
- Περιέχει υποομάδα τάξης $lcm(p-1, q-1)$.
- Ακριβώς το $\frac{1}{4}$ των στοιχείων είναι τετραγωνικά υπόλοιπα (quadratic residues) modulo n, δηλ. είναι τετράγωνα κάποιου αριθμού modulo n. Τα στοιχεία αυτά προκύπτουν συνδυάζοντας με CRT τετραγωνικά υπόλοιπα modulo p με τετραγωνικά υπόλοιπα modulo q.

Τετραγωνικά Υπόλοιπα (Quadratic Residues)

Ορισμός

Ένας ακέραιος $k \in \mathbb{Z}_m$ λέγεται *τετραγωνικό υπόλοιπο modulo m* αν υπάρχει $l \in \mathbb{Z}_m$ τ.ώ. $k \equiv l^2 \pmod{m}$. Τότε ο l λέγεται *τετραγωνική ρίζα του k modulo m*.

Παρατήρηση: όπως είδαμε, τα μισά στοιχεία του $\mathbb{Z}_p$ και το $\frac{1}{4}$ των στοιχείων του $\mathbb{Z}_{pq}$ (για p, q πρώτους) είναι τετραγωνικά υπόλοιπα (modulo p και pq αντίστοιχα).

Για αυτά τα στοιχεία και μόνο οι ισοτιμίες:

$$x^2 \equiv a \pmod{p} \qquad x^2 \equiv a \pmod{pq}$$

έχουν λύση. *Παρατήρηση:* αν x_0 είναι λύση τότε και $-x_0$ είναι λύση. Πόσες λύσεις υπάρχουν;

Πλήθος τετραγωνικών ριζών modulo n

Πρόταση

Έστω p, q πρώτοι. Τότε:

1. *Η ισοτιμία $x^2 \equiv a \pmod{p}$ έχει είτε 0 είτε 2 λύσεις στο $\mathbb{Z}_p^*$.*
2. *Η ισοτιμία $x^2 \equiv a \pmod{pq}$ έχει είτε 0 είτε 4 λύσεις στο $U(\mathbb{Z}_{pq})$.*

Απόδειξη.

1. Αν x_1, x_2 λύσεις της ισοτιμίας τότε $x_1^2 \equiv x_2^2 \pmod{p}$ άρα
   $p \mid (x_1^2 - x_2^2) \Rightarrow p \mid (x_1 - x_2)(x_1 + x_2) \Rightarrow$
   $p \mid (x_1 - x_2) \vee p \mid (x_1 + x_2) \Rightarrow x_1 \equiv x_2 \vee x_1 \equiv -x_2 \pmod{p}$
2. Η λύση της ισοτιμίας ισοδυναμεί με τη λύση των δύο ισοτιμιών $x^2 \equiv a \pmod{p}$, $x^2 \equiv a \pmod{q}$.

   Εστω ότι η πρώτη έχει λύσεις τις $x_p, -x_p$ και η δεύτερη τις $x_q, -x_q$. Για καθε ένα από τους συνδυασμούς των λύσεων αυτών (που είναι 4) προκύπτει, με χρήση CRT, μια διαφορετική λύση για την ισοτιμία στο $U(\mathbb{Z})$, από το σύστημα

$$x \equiv \pm x_p \pmod{p}, x \equiv \pm x_q \pmod{q}.$$

Τετραγωνικές ρίζες modulo n: πρόσθετες ιδιότητες

- Η προηγούμενη πρόταση μπορεί να γενικευτεί για $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ όπου η αντίστοιχη εξίσωση έχει είτε 0 είτε 2^k λύσεις.
- Τετριμμένες περιπτώσεις: στο $\mathbb{Z}_p$, το $x^2 \equiv 0 \pmod{p}$ έχει μία (διπλή) τετραγωνική ρίζα, την $x \equiv 0 \pmod{p}$, αντίστοιχα στο $\mathbb{Z}_{pq}$ (4πλή ρίζα). Στο $\mathbb{Z}_{pq}$, αν $a \equiv 0 \pmod{p}$, και $a \not\equiv 0 \pmod{q}$ τότε το a έχει 2 (διπλές) ρίζες που προκύπτουν από το σύστημα $x \equiv 0 \pmod{p}$, $x \equiv \pm x_q \pmod{q}$ με χρήση CRT.

Τετραγωνικές ρίζες modulo n και παραγοντοποίηση

Ο αριθμός 1 έχει δύο τετραγωνικές ρίζες modulo p : ± 1.
Επίσης έχει 4 τετραγωνικές ρίζες modulo pq: τις ± 1, και άλλες δύο ($\pm u \not\equiv 1 \pmod{pq}$) που λέγονται μη τετριμμένες ρίζες της μονάδας modulo n.

Η ύπαρξη μη τετριμμένων ριζών του 1 modulo n συνιστά απόδειξη ότι ο n είναι σύνθετος, και συγχρόνως δίνει άμεσα δύο παράγοντες του n: $\gcd(n, u \pm 1)$.

Παρόμοια πληροφορία παίρνουμε από την ύπαρξη 2 μη αντίθετων τετραγωνικών ριζών οποιουδήποτε αριθμού $a \in \mathbb{Z}_n$.

Η ιδιότητα αυτή χρησιμοποιείται στην απόδειξη ορθότητας του Miller-Rabin primality test, και σε διάφορες άλλες αποδείξεις (κρυπτοσυστήματα RSA, Rabin, κ.λπ.).

Τετραγωνικές ρίζες modulo n: έλεγχος ύπαρξης

Πρόταση (Κριτήριο Euler)

Για p πρώτο, η ισοτιμία $x^2 \equiv a \pmod{p}$ έχει λύση αν και μόνο αν

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Απόδειξη.

Θα δείξουμε ότι και οι δύο συνθήκες ισχύουν αν και μόνο αν το a είναι άρτια δύναμη ενός γεννήτορα. Έστω ότι $a \equiv g^k \pmod{p}$ για γεννήτορα g της $\mathbb{Z}_p^*$.

Τότε:

$$\exists x : x^2 \equiv a \pmod{p} \Leftrightarrow \exists l : g^{2l} \equiv g^k \pmod{p} \Leftrightarrow 2l \equiv k \pmod{p-1} \Leftrightarrow k \bmod 2 = 0.$$

Επίσης, από μικρό Θ. Fermat.:

$$a^{\frac{p-1}{2}} \equiv g^{\frac{k}{2}(p-1)} \equiv 1 \pmod{p} \Leftrightarrow p-1 \mid \tfrac{k}{2}(p-1) \Leftrightarrow k \bmod 2 = 0$$

□

Παρατήρηση. για κάθε $a \in \mathbb{Z}_p^*$ ισχύει $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Η ιδιότητα αυτή σχετίζεται άμεσα με τη συνάρτηση που είναι γνωστή ως σύμβολο Legendre και τη γενίκευσή της, το σύμβολο Jacobi. Το τελευταίο χρησιμοποιείται στο Solovay-Strassen primality test.

Ορισμός

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } \exists x : x^2 \equiv a \pmod{p} \\ -1, & \text{if } \nexists x : x^2 \equiv a \pmod{p} \\ 0, & \text{if } p \mid a \end{cases}$$

Αν $\left(\frac{a}{p}\right) = 1$ τότε το a ονομάζεται *τετραγωνικό υπόλοιπο modulo p*. Αν $\left(\frac{a}{p}\right) = -1$ τότε το a ονομάζεται *τετραγωνικό μη υπόλοιπο modulo p*.

Ιδιότητες συμβόλου Legendre

Πρόταση

1. $m \equiv n \pmod p \Rightarrow \left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$
2. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Απόδειξη.

(1): άμεσα από τον ορισμό.

(2): αν $a \equiv 0 \pmod p$ ισχύει.

Αλλιώς $a \in \mathbb{Z}_p^*$, οπότε αν $a \in QR(n)$ τότε από κριτήριο Euler ισχύει $a^{\frac{p-1}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod p$.

Αν $a \notin QR(n)$ τότε επειδή $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$, θα έχουμε αναγκαστικά:

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

(3) από ιδιότητα 2. □

Σημαντικό: η ιδιότητα (2) δίνει έναν αποδοτικό αλγόριθμο υπολογισμού του συμβόλου Legendre.

Ιδιότητες συμβόλου Legendre

Πρόταση

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \textit{if } p \equiv 1 \pmod 4 \\ -1, & \textit{if } p \equiv 3 \pmod 4 \end{cases}$
2. $\left(\frac{2}{p}\right) = \begin{cases} 1, & \textit{if } p \equiv 1 \pmod 8 \vee p \equiv 7 \pmod 8 \\ -1, & \textit{if } p \equiv 3 \pmod 8 \vee p \equiv 5 \pmod 8 \end{cases}$

Η απόδειξη βασίζεται στο ακόλουθο:

Λήμμα

(Gauss) Αν το πλήθος των στοιχείων του συνόλου $\{a \bmod p, 2a \bmod p, \ldots, \frac{p-1}{2}a \bmod p\}$ *που είναι μεγαλύτερα του* $\frac{p}{2}$ *το συμβολίσουμε με* μ *τότε ισχύει ότι* $\left(\frac{a}{p}\right) = (-1)^{\mu}$.

Ιδιότητες συμβόλου Legendre

Θεώρημα (Νόμος Τετραγωνικής Αντιστροφής (Quadratic Reciprocity Law))

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right), & \text{αν } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{q}{p}\right), & \text{αλλιώς.} \end{cases}$$

Με χρήση του νόμου τετραγωνικής αντιστροφής, και των προηγούμενων ιδιοτήτων έχουμε έναν πιο γρήγορο υπολογισμό του συμβόλου Legendre: $O(\log^2 p)$.

Ορισμός (Σύμβολο Jacobi)

Για $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ ορίζουμε το σύμβολο Jacobi ως εξής:

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{k} \left(\frac{m}{p_i}\right)^{a_i}.$$

- Το σύμβολο Jacobi είναι γενίκευση του συμβόλου Legendre και ικανοποιεί τις ίδιες ιδιότητες εκτός της $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$. Το γεγονός αυτό χρησιμοποιείται στον έλεγχο πρώτων αριθμών Solovay-Strassen.
- Το σύμβολο Jacobi $\left(\frac{a}{n}\right)$ δεν χαρακτηρίζει πλήρως την ύπαρξη λύσεων της ισοτιμίας $x^2 \equiv a \pmod{n}$. Πράγματι, αν η ισοτιμία αυτή έχει λύσεις τότε $\left(\frac{a}{n}\right) = 1$ αλλά δεν ισχύει το αντίστροφο (π.χ. για $n = pq$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1 \Rightarrow \left(\frac{a}{n}\right) = 1$.

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \ldots, n-1]$. Αν $b^{n-1} \mod n \neq 1$, τότε το n δεν περνάει τον έλεγχο (είναι σίγουρα σύνθετος).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.
4. Αν $b^t \mod n \equiv \pm 1 \pmod{n}$, τότε το n περνάει τον έλεγχο (πιθανόν πρώτος).
5. Αλλιώς, υψώνουμε το $b^t \mod n$ στο τετράγωνο: $b^{2t} \mod n$, έπειτα ξανά στο τετράγωνο $\mathrm{mod}\, n$ κ.ο.κ. εως ότου πάρουμε ± 1 (το πολύ $s - 1$ επαναλήψεις).
6. Αν πάρουμε πρώτα -1 τότε το n περνάει τον έλεγχο (πιθανόν πρώτος), αλλιώς δεν περνάει τον έλεγχο (σίγουρα σύνθετος).

Ορθότητα: Θα αποδείξουμε ότι η πιθανότητα αποτυχίας είναι $< \frac{1}{2}$. Μπορεί να γίνει *αμελητέα (negligible)* με επαναλήψεις του ελέγχου για άλλο b κάθε φορά.

Έλεγχος πρώτων αριθμών Miller-Rabin: ορθότητα

Πρόταση

Αν n πρώτος, τότε περνάει τον έλεγχο πάντοτε (για όλα τα b). Αν n σύνθετος τότε περνάει τον έλεγχο για λιγότερα από τα μισά b.

Απόδειξη.

Βασίζεται στην απεικόνιση $b \mapsto \langle b^t, b^{2t}, \ldots, b^{2^i t}, \ldots b^{2^s t} \rangle \pmod{n}$.

Factoring sequence: $\langle \not\equiv \pm 1, \ldots, \not\equiv \pm 1, \equiv 1, \ldots \equiv 1 \rangle \pmod{n}$.

Αποδεικνύεται με χρήση του Θ. Lagrange ότι τα στοιχεία που απεικονίζονται σε non-factoring sequences είναι το πολύ τα μισά.

Λεπτομέρειες: στον πίνακα. $\square$

Ευεπίλυτα αριθμητικά προβλήματα

Χαρακτηρίζονται από την ύπαρξη αποδοτικού (πολυωνυμικού χρόνου) αλγορίθμου, ντετερμινιστικού ή πιθανοτικού.

- $\textsc{GCD}(a, n)$: εύρεση ΜΚΔ(a, n).
- $\textsc{Inverse}(a, n)$: υπολογισμός $a^{-1} \bmod n$.
- $\textsc{Power}(a, y, n)$: υπολογισμός $a^y \bmod n$.
- $\textsc{Primality}(n)$: έλεγχος αν ο n είναι πρώτος αριθμός.
- $\textsc{Find-Prime}(n)$: εύρεση πρώτου $> n$.
- $\textsc{Quad-Res}(a, n)$: έλεγχος αν $\exists x : x^2 \equiv a \pmod{n}$. Για n πρώτο, ή σύνθετο με γνωστή παραγοντοποίηση.
- $\textsc{Square-Root}(a, n)$: εύρεση $x : x^2 \equiv a \pmod{n}$, αν υπάρχει. Για n πρώτο, ή σύνθετο με γνωστή παραγοντοποίηση.

Δυσεπίλυτα αριθμητικά προβλήματα

Χαρακτηρίζονται από την μη ύπαρξη (ως τώρα) αποδοτικού (πολυωνυμικού χρόνου) αλγορίθμου, ντετερμινιστικού ή πιθανοτικού.

- $\textsc{Factor}(n)$: παραγοντοποίηση του n.
- $e\textsc{-th-Root}(c, n)$: εύρεση $m : m^e \equiv c \pmod{n}$. Γνωστό και ως $\textsc{RSA-Decrypt}(c, n)$. Δύσκολο για n σύνθετο με άγνωστη παραγοντοποίηση.
- $\textsc{Discrete-Log}(g, a, p)$: εύρεση $x : g^x \equiv a \pmod{p}$. Δύσκολο για p πρώτο.
- $\textsc{Quad-Res}(a, n)$: έλεγχος αν $\exists x : x^2 \equiv a \pmod{n}$. Δύσκολο για n σύνθετο με άγνωστη παραγοντοποίηση.
- $\textsc{Square-Root}(a, n)$: εύρεση $x : x^2 \equiv a \pmod{n}$, αν υπάρχει. Δύσκολο για n σύνθετο με άγνωστη παραγοντοποίηση.