Προηγμένα Θέματα Αλγορίθμων

Θεωρία Αριθμών και Πιθανοτικοί Αλγόριθμοι

Άρης Παγουρτζής

Ευχαριστίες: *σε κάποιες διαφάνειες χρησιμοποιήθηκε υλικό από σημειώσεις του Στάθη Ζάχου καθώς και από διαφάνειες του Πέτρου Ποτίκα.*

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. $a - (-|a| \cdot b) \in S$) 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
$$a = q'b + r', \quad 0 \leq r' < b, \text{ επομένως } 0 \leq |r' - r| < b.$$
- $qb + r = q'b + r' \Rightarrow (q - q')b = (r' - r) \Rightarrow |q - q'|b = |r' - r|$.
Αν $q \neq q'$ τότε $b \mid |r' - r| \Rightarrow b \leq |r' - r|$, 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) $d' \mid a \wedge d' \mid b \Rightarrow d' \leq d$.

Απόδειξη

- (i) Έστω $d = \kappa a + \lambda b,\ \kappa, \lambda \in \mathbb{Z}$, και d ελάχιστο. 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 (γιατί; βρίσκει διαιρέτη που είναι και γραμμικός συνδυασμός).
- $\gcd(a,b) = 1 \Rightarrow \exists \kappa, \lambda \in \mathbb{Z}, \quad \kappa a + \lambda b = 1$

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

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

  (γιατί; c διαιρεί το 1ο μέλος).
- Αν p πρώτος $\wedge\ p \mid ab$ τότε $p \mid a \ \vee\ p \mid b$:

  $gcd(p,a) \in \{1, p\}$. 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.

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)
- $2^{13466917} - 1$ (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, άτοπο. □

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

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

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

- 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 $\mod m$, $m \in \mathbb{Z}, m > 0$, 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 $\mod m$:

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

- 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.

Μικρό Θεώρημα Fermat

Θεώρημα (μικρό Fermat)

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

Απόδειξη.

Για $a \in \mathbb{Z}$ με $p \nmid a$, 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 $a^{p-1}(p-1)! \equiv (p-1)! \Rightarrow a^{p-1} \equiv 1 \pmod{p}$. □

Παρόμοια αποδεικνύεται το πιο γενικό:

Θεώρημα (Euler)

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

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* $\mathbb{Z}_M$, $M = m_1 m_2 \dots m_k$. *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.

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* $a \cdot c \equiv 1 \pmod{m}$.

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.)

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.

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:

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

Σημαντική εφαρμογή: πιθανοτικός έλεγχος πρώτων αριθμών Fermat και Miller-Rabin

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.
$\exists a \in U(\mathbb{Z}_n)$, $a^{n-1} \not\equiv 1 \pmod{n}$, 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: έλεγχος Miller-Rabin.

Τετραγωνικές ρίζες modulo n και παραγοντοποίηση

- Ο αριθμός 1 έχει δύο τετραγωνικές ρίζες modulo p : ± 1.
- Επίσης έχει 4 τετραγωνικές ρίζες modulo $n = pq$: τις ± 1, και άλλες δύο ($\pm u \not\equiv \pm 1 \pmod{n}$) που λέγονται μη τετριμμένες ρίζες της μονάδας modulo n.
- Η ύπαρξη μη τετριμμένων ριζών του 1 modulo n συνιστά απόδειξη ότι ο αριθμός 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 είναι κομβικής σημασίας για την κατανόηση της λειτουργίας και της ορθότητας του Miller-Rabin primality test.

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 $b^t \equiv \pm 1 \pmod n$, 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: $b^{2^2 t} \mod n$ κ.ο.κ. έως ότου πάρουμε ± 1 (το πολύ σε s 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: απόδειξη ορθότητας

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 $b \mapsto seq(b) = \langle b^t, b^{2t}, \ldots, b^{2^i t}, \ldots b^{2^s t} \rangle \pmod{n}$.

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 (μη μάρτυρες του n) είναι το πολύ τα μισά.

□

Έλεγχος πρώτων αριθμών Miller-Rabin: απόδειξη ορθότητας

Έστω $n = n_1 n_2, \gcd(n_1, n_2) = 1$ [αν $n = p^e, e > 1$, κανένα στοιχείο του $U(\mathbb{Z}_n)$ δεν περνάει τον έλεγχο Fermat (άσκηση)]. Θδο $\geq |U(\mathbb{Z}_n)|/2$ στοιχεία του $U(\mathbb{Z}_n)$ μάρτυρες συνθετότητας του n κατά Miller-Rabin.

- $j^* = \max\{j \mid \exists u \in U(\mathbb{Z}_n) : u^{2^j t} \equiv -1 \pmod{n}\}$: "δεξιότερη" θέση όπου συναντάμε -1 στις ακολουθίες $seq(b), b \in U(\mathbb{Z}_n)$.
- $B = \{b \in U(\mathbb{Z}_n) \mid b^{2^{j^*} t} \equiv \pm 1 \pmod{n}\}$: υπερσύνολο του $NW(n)$ (σύνολο μη μαρτύρων του n) – γιατί;
- B κλειστό ως προς $\cdot \pmod{n}$, επομένως υποομάδα!.
- $B \neq U(\mathbb{Z}_n)$: $\exists w \in U(\mathbb{Z}_n) : w \equiv 1 \pmod{n_1} \wedge w \equiv u \pmod{n_2}$ (CRT)
- $w^{2^i j^* t} \equiv 1 \pmod{n_1} \wedge w^{2^{j^*} t} \equiv -1 \pmod{n_2} \Rightarrow w^{2^j * t} \not\equiv \pm 1 \pmod{n}$
- Επομένως B είναι γνήσια υποομάδα του $U(\mathbb{Z}_n)$, και άρα: $|NW(n)| \leq |B| \leq \frac{|U(\mathbb{Z}_n)|}{2}$ (από Θ. Lagrange!)
- Άρα τουλάχιστον τα μισά στοιχεία του $U(\mathbb{Z}_n)$ δίνουν factoring sequence, πιθανότητα $\geq \frac{1}{2}$. Με k επαναλήψεις πιθανότητα $\geq 1 - \frac{1}{2^k}$.

Παραγοντοποίηση Pollard rho: προκαταρτικά

- Έστω p ο μικρότερος πρώτος διαιρέτης του n. Αναζητούμε $x \neq x' \in \mathbb{Z}_n$, τ.ώ. $x \equiv x' \pmod{p}$
- Τότε $gcd(x - x', n)$, ίσως είναι μη τετριμμένος διαιρέτης του n
- Επιλέγουμε τυχαία σύνολο $X \subseteq \mathbb{Z}_n$ και υπολογίζουμε για όλα τα $x, x' \in X$ το $gcd(x - x', n)$
- Από παράδοξο γενεθλίων, χρειάζεται $|X| \approx 1.17\sqrt{p}$ για να έχουμε σύγκρουση με πιθανότητα $\geq \frac{1}{2}$.
  Αν ελεγχθούν όλα τα x, x' ανά ζεύγη, το κόστος γίνεται τετραγωνικό στο $|X|$ άρα $O(p) = O(\sqrt{n})$, συγκρίσιμο με απλοϊκό αλγόριθμο!
- Μπορεί να γίνει με πλήθος συγκρίσεων γραμμικό στο $|X|$;

Παραγοντοποίηση Pollard rho: ο 'αργός' τρόπος

- Θεωρούμε f πολυώνυμο με ακέραιους συντελεστές, π.χ. $f(x) = x^2 + 1 \bmod n$
- Έστω $x_0 \in \mathbb{Z}_n$ και $x_1, x_2, \ldots$, όπου $x_j = f(x_{j-1})$, $j \geq 2$. Η f παράγει σχεδόν τυχαία στοιχεία.
- Χρειάζεται για κάθε νέο x_j, να υπολογίζουμε $gcd(x_i - x_j, n)$, για όλα τα $i < j$, τετραγωνικό κόστος (βλ. και προηγούμενη διαφάνεια)

Παραγοντοποίηση Pollard rho: η βασική ιδέα για βελτίωση

- Ιδέα της μεθόδου: Αν $x_i \bmod p = x_j \bmod p$, τότε $x_{i+1} \bmod p = x_{j+1} \bmod p$ (λόγω της πολυωνυμικής μορφής της f και του ότι $p|n$)
- Επαναλαμβάνοντας, αν $x_i \equiv x_j \pmod p$, τότε $x_{i+\delta} \equiv x_{j+\delta} \pmod p$, $\delta \geq 0$
- Γράφος G: κορυφές τα x_i, κατευθυνόμενες ακμές από το $x_i \bmod p$ στο $x_{i+1} \bmod p$.
- Έστω το πρώτο ζευγάρι x_i, x_j, με $i < j$ ώστε $x_i \equiv x_j \pmod p$, τότε ο γράφος έχει σχήμα ρ:
- $x_1 \bmod p \to x_2 \bmod p \cdots \to x_i \bmod p$ (ουρά)
  $x_i \bmod p \to x_{i+1} \bmod p \cdots \to x_j \bmod p \equiv x_i \bmod p$ (κύκλος)
- Από τη μορφή του γράφου, το όνομα της μεθόδου (ρ).

Παραγοντοποίηση Pollard rho: γραμμικός χρόνος

- Βελτίωση: δε χρειάζεται να βρούμε την πρώτη σύγκρουση, αντί για αυτήν αρκεί να ελέγξουμε $x_{i'}, x_{j'}$ για κατάλληλο k, όσο το δυνατόν μικρότερο, ώστε

$$i' = 2^k, j' = 2^k + j - i < 2^{k+1}$$

- Κάθε $x_{j'}$ ελέγχεται *μόνο* με $x_{i'}$, $i' = 2^k < j' \leq 2^{k+1}$: γραμμικός χρόνος!
- Για τον ελάχιστο i' που ικανοποιεί τις παραπάνω συνθήκες ισχύει $j \leq i' < 2j$ και επομένως $j' < 3j$
- Αναμενόμενος αριθμός επαναλήψεων: $O(j) = O(\sqrt{p})$
- Επειδή, $p < \sqrt{n}$, η αναμενόμενη πολυπλοκότητα είναι $O(n^{1/4})$ (όχι αυστηρή απόδειξη!)
- Αποτυχία αλγορίθμου (πότε?, τι πιθανότητα?, τι κάνουμε?) : όταν $x_i \equiv x_j \pmod{p}$ και $x_i \equiv x_j \pmod{n}$ (σχετικά μικρή πιθανότητα ($\approx \frac{p}{n}$)). Επαναλαμβάνουμε με άλλο x_0 ή/και άλλο πολυώνυμο.

Παραγοντοποίηση Pollard rho: ψευδοκώδικας

Αλγόριθμος `Pollard Rho Factoring` (n)

$i \leftarrow 0$
$x \leftarrow_R \{0, 1, \ldots, n-1\}, y = x, k = 1$
while true
  $i \leftarrow i + 1$
  $x \leftarrow f(x)$ (* e.g. $f(x) = (x^2 + 1) \bmod n$ *)
  $d \leftarrow gcd(|x - y|, n)$
  if $d \neq 1$ and $d \neq n$
    return d
  if $d = n$
    return 'fail'
  if $i = k$
    $y \leftarrow x$
    $k \leftarrow 2k$

Ευεπίλυτα αριθμητικά προβλήματα

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

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

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