Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Χρήστος Κούτρας
Γιώργος Παναγιωτάκος

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

5 Νοεμβρίου 2012

1 Αλγόριθμος Ευκλείδη

Χρησιμοποιούμε τον αλγόριθμο του Ευκλείδη για να υπολογίσουμε τον μέγιστο κοινό διαιρέτη(*gcd*).
Χρησιμοποιώντας το "στυλ" του συναρτησιακού προγραμματισμού:

$$\begin{aligned}\text{gcd}(a,b) &= \text{if } (b|a)\ b.\\ \text{gcd}(a,b) &= \text{if } (a>b)\ \ \text{gcd}(a \bmod b, b)\\ &\qquad\quad \text{else}\ \ \text{gcd}(b \bmod a, a).\end{aligned}$$

Και σε προστακτικό στυλ (και χωρίς έλεγχο αν $a > b$):

$$\begin{aligned}&\text{function gcd}(a, b\text{: natural })\\ &\quad \text{if } (b|a) \text{ then return } b\\ &\quad \text{else return } \ \text{gcd}(b, a \bmod b)\end{aligned}$$

Η πολυπλοκότητα του παραπάνω αλγορίθμου είναι O(log(a + b)) = O(log(max (a, b))).
Κάθε 2 το πολύ βήματα ο μεγαλύτερος αριθμός υποδιπλασιάζεται.

Παρατήρηση : Το bit-complexity είναι O($\log^3$(max(a, b)))

Θεώρημα : Υπάρχει *πολλαπλασιαστικός αντίστροφος* του $a \bmod n \Leftrightarrow \text{gcd}(a, n) = 1$

Πώς τον βρίσκουμε:
$\forall a, n \in \mathbb{Z}$, τ.ω $\text{gcd}(a, n) = 1, \exists \kappa, \lambda \in \mathbb{Z}$ τ.ω : $1 = \kappa a + \lambda n$
$\Rightarrow \kappa a = 1 (\text{mod} n)$
$\Rightarrow \kappa$ *πολλαπλασιαστικός αντίστροφος* του $a \bmod n$
Ο υπολογισμός των κ, λ επιτυγχάνεται με τον παρακάτω αλγόριθμο.

2 Επεκτεταμένος Ευκλείδειος αλγόριθμος

$\forall a, n \in \mathbb{Z}, \exists \kappa, \lambda \in \mathbb{Z}$ τ.ω $\text{gcd}(a, n) = \kappa a + \lambda n$

Με τον επεκτεταμένο Ευκλείδειο αλγόριθμο μπορούμε να υπολογίσουμε τα κ, λ
και επομένως να βρούμε τον πολλαπλασιαστικό αντίστροφο του $a \bmod n$.
Π.χ. gcd(91, 35) :

κ, λ	gcd(a,n)		κ, λ
$(1, 0)$	91	35	$(0, 1)$
$(0, 1)$	35	21	$(1, -2)$
$(1, -2)$	21	14	$(-1, 3)$
$(-1, 3)$	14	7	$(2, -5)$

Άρα $7 = 2 \cdot 91 - 5 \cdot 35$

Στον παραπάνω πίνακα, μέσα στις παρενθέσεις εμφανίζονται οι συντελεστές κ, λ των διαδοχικών υπολοίπων ως προς τους αρχικούς αριθμούς, π.χ. $14 = -1 \cdot 91 + 3 \cdot 35$.

Ιδιότητες
Χρησιμοποιούμε τον εναλλακτικό συμβολισμό για την gcd(a, b): (a, b)
$\forall a, b \in \mathbb{Z}, m, n \in \mathbb{N}$

- $(ma, mb) = m(a, b)$
- $(a, m) = (b, m) = 1 \Rightarrow (ab, m) = 1$
- $(a, b) = (a, b + ka)$
- $(m|a) \wedge (n|a) \wedge (m, n) = 1 \Rightarrow mn|a$

3 Συνάρτηση ϕ του Euler

Ορισμός : $\phi(n) = |\{m | m \in \mathbb{N}, m < n, \text{gcd}(m, n) = 1\}|, \forall n \in \mathbb{N}$

Ιδιότητες

- Αν p πρώτος τότε : $\phi(p) = p - 1$
- Αν p πρώτος τότε : $\phi(p^a) = p^a - p^{a-1}$
- Αν gcd$(m, n) = 1$ τότε $\phi(mn) = \phi(m)\phi(n)$
- $\forall n \in \mathbb{N}$ έστω $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \Rightarrow \phi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_k})$

Θεώρημα(Euler) : $\forall n \geq 1 : n = \sum_{d|n} \phi(d)$

4 Αντιμεταθετικές ομάδες

Ορισμός : Ομάδα είναι ένα ζεύγος $(G, *) : * (G \times G \to G)$ έτσι ώστε $\forall a, b, c \in G$:

- $a * (b * c) = (a * b) * c$ (Προσεταιριστική)
- $\exists e \in G, \forall a \in G : a * e = a$ (Μοναδιαίο στοιχείο)
- $\forall a \in G, \exists a^{-1} \in G : a * a^{-1} = e$ (Αντίστροφο)
- αν ισχυει ότι $a * b = b * a$ (Αντιμεταθετικη) τότε η ομάδα λέγεται αντιμεταθετική ή αβελιανή

Π.χ. $(\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}, +_{\text{ mod } n})$ ή πιο απλά $(\mathbb{Z}_n, +)$ είναι αντιμεταθετική ομάδα.
Όμοια και οι $(\mathbb{Z}_p^*, \cdot)$ και $(U(\mathbb{Z}_n), \cdot)$ [1]

Ορισμός : *Δακτύλιος* $(R, +, *)$ όπου το $(R, +)$ αντιμεταθετική ομάδα και για το $*$ ισχύουν οι προσεταιριστική ιδιότητα και η επιμεριστική ως προς την προσθεση.

Ορισμός : *Σώμα* $(F, +, *)$ όπου το $(F, +, *)$ δακτύλιος και το ($F \setminus \{e_+\}, *$) είναι αντιμεταθετική ομάδα.

Π.χ. $\forall p$ πρώτο $(\mathbb{Z}_p, +, *)$ είναι σώμα.

5 Αντιμεταθετικές υποομάδες

Ορισμός : Υποομάδα μιας ομάδας $(G, *)$ είναι κάθε $S \subseteq G$ τ.ω $(S, *)$ είναι ομάδα.

Θεώρημα : αν $(G, *)$ είναι αντιμεταθετική πεπερασμένη ομάδα, κάθε $S \subseteq G$ κλειστό ως προς $*$, ειναι υποομάδα.

Απόδειξη : Ισχύουν προφανώς η προσεταιριστική και η αντιμεταθετική ιδιότητα στην $(S, *)$.
Έστω ότι $\nexists m$, τ.ω $a^m = e_G$.Τότε :
$\exists \kappa, \lambda$ με $\kappa > \lambda$ τ.ω. $a^\kappa = a^\lambda \Rightarrow a^\lambda * a^{\kappa-\lambda} = a^\lambda \Rightarrow (a^{-1})^\lambda * a^\kappa * a^{\kappa-\lambda} = (a^{-1})^\lambda * a^\lambda \Rightarrow a^{\kappa-\lambda} = e$
Άτοπο από υπόθεση.

Τελικά $\exists m$ τ.ω. $a^m = e$ και άρα $e \in S$ με $a^{-1} * a^{m-1} = e$ όπου a^{-1} ο αντίστροφος του a.

Ορισμός : Μια ομάδα $(G, *)$ λέγεται *κυκλική* αν υπαρχει $g \in G$ με την ιδιότητα $\forall x \in G, \exists y : x = g^y$. Το στοιχείο αυτό το ονομάζουμε και γεννήτορα της $(G, *)$.

Ορισμός : *Τάξη στοιχείου* ($ord_G(a)$) $= min\{y | a^y = e\}$.

[1] Με $U(\mathbb{Z}_n)$ συμβολίζουμε το σύνολο των στοιχείων που ειναι σχετικά πρώτα με το n.
$|U(\mathbb{Z}_n)| = \phi(n)$

Παρατήρηση : $ord_G(a) = |G|$ όπου a γεννήτορας της $(G, *)$.

Ορισμός : Έστω $(H, *)$ υποομάδα της $(G, *)$ και $a \in G$. Τότε το $H * a = \{h * a | h \in H\}$ ονομάζεται *δεξί σύμπλοκο(coset)* της H στην G.

Ιδιότητα : Έστω $H \subseteq G, (H, *)$ υποομάδα της $(G, *)$.
$\forall a, b \in G$ είτε $H * a = H * b$ είτε $H * a \cap H * b = \varnothing$.

Πρόταση : Το σύνολο των συμπλόκων της H στην G (G/H) με την πράξη $\circledast$: $(H * a) \circledast (H * b) = H * (a * b)$ είναι ομάδα τάξης $|G|/|H|$.

Θεώρημα Lagrange : Η τάξη κάθε υποομάδας $(H, *)$ της $(G, *)$ διαιρεί την ταξη της $G : |H| \mid |G|$.

Πόρισμα : Έστω $(G, *)$ πεπερασμένη ομάδα και $(H, *)$ υποομάδα της. Τότε, $\exists g \in G \setminus H \Rightarrow |H| \leq |G|/2$ (επομένως η ιδιότητα ισχύει για κάθε $H \subseteq G$ κλειστό ως προς $*$).

Θεώρημα : Έστω $(G, *)$ πεπερασμένη ομάδα. Τότε $\forall a \in G : a^{|G|} = e$.

Θεώρημα (Euler) : $\forall a, m \in \mathbb{Z} : \forall a \in U(\mathbb{Z}_m) : a^{\phi(m)} \equiv 1 (\mod m)$.

Θεώρημα (Fermat) : $\forall a \in \mathbb{Z}^* : a^{p-1} \equiv 1 (\mod p - 1)$.

Πρόταση : Αν $a \in \mathbb{Z}_p^*$ γεννήτορας της $\mathbb{Z}_p^*$, $a^m \equiv a^n (\mod p) \Leftrightarrow m \equiv n (\mod p - 1)$ (Αν $a \in \mathbb{Z}_p^*$ αλλά δεν είναι γεννήτορας ισχύει μόνο το "$\Leftarrow$").

Θεμελιώδες θεώρημα υποομάδων Έστω G κυκλική ομάδα τάξης n. Τότε οποιαδήποτε υποομάδα H της G είναι κυκλική. Η τάξη της H, έστω t, διαιρεί την τάξη της $G : h|n$. Επιπλέον, η H ειναι η μοναδική υποομάδα της G τάξης t.

Βιβλιογραφία

Zac12 : Σημειώσεις Ζάχου, ΕΜΠ, 2012.

Sti06 : Douglas Stinson: "Cryptography: Theory and Practice", 3rd edition, CRC Press, 2005.

Sho07 : Victor Shoup: "A Primer on Algebra and Number Theory for Computer Scientists".