Algebrai gyorstalpaló

Csoportok

Meghatározás. A $(G,\cdot)$ csoport ciklikus, ha $\exists x \in G$ úgy, hogy $G = \langle x \rangle = \{x^k | k \in \mathbb{Z}\}$.

Tétel. Ha $(G,\cdot)$ véges csoport és $|G| = n$, akkor $x^n = 1$, $\forall x \in G$-re.

Maradékosztályok gyűrűje modulo $n \geq 2$

Tétel. A $(\mathbb{Z}_n, +, \cdot)$ egységelemes kommutatív gyűrűnek van zérusosztója $\iff$ n összetett szám.

Tétel. $\exists \hat{a}^{-1} \in \mathbb{Z}_n \iff \mathrm{lnko}(a, n) = 1$. $(U(\mathbb{Z}_n), \cdot)$ csoport, ahol $U(\mathbb{Z}_n) = \{\hat{a} \in \mathbb{Z}_n \,|\, \exists \hat{a}^{-1} \in \mathbb{Z}_n\}$.
$|U(\mathbb{Z}_n)| = \varphi(n) = |\{0 \leq a < n \,|\, \mathrm{lnko}(a, n) = 1\}|$, ahol $\varphi(n)$ az Euler-féle számelméleti függvény.

Tétel. Ha $n = p_1^{\alpha_1} \cdot \dots \cdot p_\ell^{\alpha_\ell}$, akkor $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_\ell}\right)$. Sajátos esetben, ha p prím, akkor $\varphi(p) = p - 1$.

Maradékosztályok gyűrűje modulo $n \geq 2$

Tétel. $(\mathbb{Z}_p, +, \cdot)$ test $\iff$ p prím.

Tétel (Euler). Ha $\mathrm{lnko}(a, n) = 1$, akkor $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Bizonyítás.

Elég annyit belátni, hogy $\mathrm{lnko}(a, n) = 1 \implies \hat{a} \in U(\mathbb{Z}_n)$, ahol $U(\mathbb{Z}_n)$ csoport, és $|U(\mathbb{Z}_n)| = \varphi(n)$. $\square$

Tétel (Fermat). Ha $p \nmid a$, akkor $a^{p-1} \equiv 1 \pmod{p}$.

Bizonyítás.

Euler-tétel alkalmazása $n = p$-re. $\square$

Véges testek

Tétel. Minden véges test kommutatív.

Tétel. Ha $(K, +, \cdot)$ véges test, akkor $|K| = p^n$, ahol p prímszám.

Tétel. Ha $(K, +, \cdot)$ véges test, akkor $(K^*, \cdot)$ csoport ciklikus.

Tétel. Izomorfizmus erejéig egyetlen $q = p^n$ elemszámú test létezik. A q elemszámú test egyik alakja $\mathbb{F}_q = \mathbb{Z}_p[X]/(f)$, ahol f egy n-ed fokú irreducibilis főpolinom $\mathbb{Z}_p[X]$-ben.
$\mathbb{F}_q = \mathbb{Z}_p[X]/(f) = \{a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \bmod f \mid a_i \in \mathbb{Z}_p\}$.

Véges testek

Az $\mathbb{F}_q$ testbeli műveletek:

- Összeadás: polinomok összeadása.
- Szorzás: polinomok szorzása, majd redukálása modulo f (vagyis f-fel való osztási maradék).

Az $\mathbb{F}_q$ testben egy $g = a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \neq 0$ elemet a következő módon invertálunk (megszerkesztjük $g^{-1} \bmod f$-et): mivel f irreducibilis n-ed fokú, következik, hogy $\mathrm{lnko}(g, f) = 1$, tehát kiterjesztett euklideszi algoritmussal lehet találni olyan $u, v \in \mathbb{Z}_p[X]$ elemeket, hogy $gu + fv = 1 \implies gu \equiv 1 \pmod{f}$, ahol $g^{-1} \bmod f = u$.

Véges testek

Példa. Legyen a véges test $\mathbb{F}_q = \mathbb{Z}_3[X]/(X^2 - X - 1)$, ahol $q = 3^2$ és $f = X^2 - X - 1$ irreducibilis $\mathbb{Z}_3[X]$-ben. Nyilván $X^2 - X - 1 \equiv 0 \pmod{f} \Longrightarrow$
$X^2 \equiv X + 1 \pmod{f}$.
$X(X+1) \equiv X^2 + X \equiv 2X + 1 \pmod{f}$.

$$
\begin{array}{r|l}
X^2 + X & X^2 - X - 1 \\ \cline{2-2}
-X^2 + X + 1 & \qquad\qquad 1 \\ \cline{1-1}
2X + 1 &
\end{array}
$$

$\mathrm{lnko}(X, f) = 1$, tehát X invertálható.

Véges testek

Példa (folytatás). Határozzuk meg inverzét, $X^{-1} \bmod f$-et.
A kiterjesztett euklideszi algoritmust fogjuk használni:
$X^2 - X - 1 = X(X-1) - 1 \Longrightarrow 1 = X(X-1) - (X^2 - X - 1) \Longrightarrow$
$X(X-1) \equiv 1 \pmod{f} \Longrightarrow X^{-1} \equiv X - 1 \pmod{f}$.

Valóban, $X(X-1) = X^2 - X = \underbrace{X^2 - X - 1}_{\equiv 0} + 1 \equiv 1 \pmod{f}$.

Diszkrét logaritmus

Meghatározás. Legyen $(G, \cdot)$ egy véges csoport és $g \in G$ úgy, hogy $ord(g) = n$ (vagyis $n > 0$ a legkisebb természetes szám, amelyre teljesül, hogy $g^n = 1$). Tételezzük fel, hogy $y \in G$ a g-nek valamilyen hatványa. Ekkor y g-alapú diszkrét logaritmusa $\log_g y = x \in \{0, \ldots, n-1\}$, ha $g^x = y$.

Diszkrét logaritmus

Példa. Legyen $G = (\mathbb{F}_9^*, \cdot)$ úgy, hogy $\mathbb{F}_9 = \mathbb{Z}_3[X]/(f)$, ahol $f = X^2 - X - 1$. Ekkor tudjuk, hogy $(\mathbb{F}_9^*, \cdot)$ ciklikus, és belátható, hogy $\mathbb{F}_9^* =< X >$. Valóban:

$$X^0 \equiv 1 \pmod{f}$$
$$X^1 \equiv X \pmod{f}$$
$$X^2 \equiv X + 1 \pmod{f}$$
$$X^3 \equiv X^2 + X \equiv 2X + 1 \pmod{f}$$
$$X^4 \equiv X^2 + 2X + 1 \equiv 3X + 2 \equiv 2 \pmod{f}$$
$$X^5 \equiv 2X \pmod{f}$$
$$X^6 \equiv 2X^2 \equiv 2X + 2 \pmod{f}$$
$$X^7 \equiv 2X^2 + 2X \equiv X + 2 \pmod{f}$$

Ekkor $\log_X(2X+1) = 3$, $\log_X(X+1) = 2$, $\log_X X = 1$, $\log_X(2X) = 5$, $\log_X(2X+2) = 6$ és $\log_X(X+2) = 7$.

Nagy prímszámok véletlenszerű generálása

Tétel (Hadamard, de la Vallée-Poussin, Erdős, Selberg).

$$\lim_{n\to\infty} \frac{|\{p \le n | p \text{ prím}\}|}{\frac{n}{\ln n}} = 1.$$

A fenti tétel szerint, ha n elég nagy, akkor 1 és n között körülbelül $\frac{n}{\ln n}$ prímszám van. Tehát 100 számjegyű prímből van körülbelül $\frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}}$, ami a 100 számjegyű páratlan számoknak nagyjából a 0,9%-a.

Nagy prímszámok véletlenszerű generálása

Tétel. Ha n prím és $n-1 = 2^s t$, ahol s páratlan, akkor bármely b-re úgy, hogy $\mathrm{lnko}(b,n) = 1$ fennáll a következő két összefüggés valamelyike:

1. $b^t \equiv 1 \pmod{n}$
2. $\exists r \in \mathbb{N}$, $0 \leq r \leq s-1$ úgy, hogy $b^{2^r t} \equiv -1 \pmod{n}$.

Meghatározás. Legyen n egy páratlan összetett szám, $n-1 = 2^s t$, t páratlan és legyen b olyan, hogy $\mathrm{lnko}(b,n) = 1$. Ekkor azt mondjuk, hogy n erős pszeudoprím a b alapra nézve, ha $b^t \equiv 1 \pmod{n}$ vagy $\exists r \in \mathbb{N}$, $0 \leq r \leq s-1$ úgy, hogy $b^{2^r t} \equiv -1 \pmod{n}$.

Tétel. Ha n páratlan összetett szám, akkor n a lehetséges b alapok legtöbb legtöbb 25%-ára lehet erős pszeudoprím (ahol $0 < b < n$, $\mathrm{lnko}(b,n) = 1$).

Nagy prímszámok véletlenszerű generálása

A Miller–Rabin-teszt segítségével el tudjuk dönteni, hogy egy nagy (több száz számjegyű) természetes n szám prímszám-e vagy sem. A következő módon járunk el:

- Meghatározzuk az s és t értékeket úgy, hogy $n - 1 = 2^s t$ úgy, és t páratlan.
- Végezzük el k-szor a következőket:
  - Választunk egy véletlenszerű b természetes számot úgy, hogy $0 < b < n$ és $\mathrm{lnko}(b, n) = 1$.
  - Ha $b^t \bmod n \neq \pm 1$, akkor kiszámoljuk sorra $b^{2t} \bmod n$, $b^{2^2 t} \bmod n$, $\ldots$, $b^{2^{s-1} t} \bmod n$ értékeket. Ha ezek közül egyik sem -1, akkor n elbukta a b alapra a tesztet, következésképpen n biztosan összetett.
- Ha n átmegy a teszten k darab különböző alapra, akkor a fenti tétel alapján annak az esélye, hogy n mégis összetett legyen $\left(\frac{1}{4}\right)^k$, tehát az n szám $1 - \left(\frac{1}{4}\right)^k$ valószínűséggel prímszám.