1. Binom kongruenciák

Diszkrét logaritmus

Definíció (FGy3.4.1)
Legyen p rögzített prím és g primitív gyök mod p. Ha $(a,p)=1$, akkor van olyan $0 \le k \le p-2$, hogy $g^k \equiv a\ (p)$. Ennek neve az a *diszkrét logaritmusa mod* g, jele $\log_{g,p}(a)$.

Mivel $o_p(g)=p-1$, ezért $g^k \equiv g^\ell\ (p)$ akkor és csak akkor, ha $k-\ell$ jó kitevője g-nek, azaz ha $k \equiv \ell\ (p-1)$. Ezért a diszkrét logaritmus mod $p-1$ lesz egyértelmű. A rá vonatkozó azonosságok ugyanazok, mint a közönséges logaritmuséi. Mindez elmondható minden olyan m modulusra, amire nézve van primitív gyök. Ekkor $p-1$ helyett $\varphi(m)$ szerepel. A diszkrét logaritmust néha *indexnek* is hívják.

Példa
Ha $p=7$, akkor $\log_{3,7}(4)=4$ és $\log_{3,7}(5)=5$.

Binom kongruenciák

Tétel (FGy3.5.1)
Legyen p prím és $(a,p)=1$. Az $x^k \equiv a\ (p)$ *binom kongruencia* pontosan akkor oldható meg, ha $a^{(p-1)/(k,p-1)} \equiv 1\ (p)$. Ilyenkor a mod p megoldások száma $(k,p-1)$. A megoldhatóság azzal ekvivalens, hogy $(k,p-1) \mid \log_{g,p}(a)$.

Diszkrét logaritmust használunk. Legyen g primitív gyök mod p, és $a \equiv g^m\ (p)$, azaz $m=\log_{g,p}(a)$, továbbá $y=\log_{g,p}(x)$. Ekkor $(g^y)^k \equiv g^m\ (p)$ azzal ekvivalens, hogy $yk \equiv m\ (p-1)$. Ez a lineáris kongruencia akkor oldható meg, ha $(k,p-1) \mid m$, és ilyenkor a mod $p-1$ megoldások száma $(k,p-1)$. Egy b pontosan akkor megoldás, ha g^b megoldása az eredeti kongruenciának, tehát $x^k \equiv a\ (p)$ megoldásszáma is $(k,p-1)$. Végül $a^{(p-1)/(k,p-1)} \equiv 1\ (p)$ azzal ekvivalens, hogy $m(p-1)/(k,p-1)$ jó kitevője g-nek, azaz $p-1$-gyel osztható. □

Hatványmaradékok

Ha p prím, akkor a k-adik *hatványmaradékok* a teljes k-adik hatványok maradékai mod p, de a nullát nem tekintjük hatványmaradéknak.
Számuk $(p-1)/(k,p-1)$. A többi nem nulla mod p maradék neve: k-adik *hatvány-nemmaradék*. (FGy3.5.2–3-ban egy alternatív leszámlálás van.)

Az a akkor lesz k-adik hatványmaradék, ha $x^k \equiv a\ (p)$ megoldható. Az előző tétel szerint a k-adik hatványmaradékok azok, amelyek indexe $(k,p-1)$-gyel osztható. Tekintsük az $x \mapsto x^k\ (p)$ függvényt, ahol $(x,p)=1$. Ennek képe a k-adik hatványmaradékok halmaza, ezért elég megmutatni, hogy mindegyiket $(k,p-1)$-szer kapjuk meg. Ha $d=c^k$, akkor $b^k \equiv d = c^k\ (p)$ akkor és csak akkor, ha $a=bc^{-1}$-re $a^k \equiv 1\ (p)$, ahol c^{-1} a b inverze mod p (amelyre $bc^{-1} \equiv 1\ (p)$). Így $b \equiv ca\ (p)$. Az előző tétel szerint ilyen a-ból $(k,p-1)$ van, tehát adott c-hez tényleg $(k,p-1)$ megfelelő b tartozik. □

2. Kvadratikus maradékok

Euler-lemma

Definíció (Fgy4.1.1)
A *kvadratikus maradékok* és nemmaradékok a k-adik hatványmaradékok, illetve nemmaradékok, amikor $k = 2$.

Legyen a p prím páratlan. Az előző tétel speciális esete a következő.

Euler-lemma (FGy4.1.2)
Ha $(a, p) = 1$, akkor $a^{(p-1)/2}$ aszerint kongruens 1-gyel vagy -1-gyel mod p, hogy a kvadratikus maradék-e vagy sem.
A kvadratikus maradékok és nemmaradékok száma is $(p-1)/2$. Ha a kvadratikus maradék, akkor $x^2 \equiv a\ (p)$-nek 2 megoldása van.

Ha $x^2 \equiv 1\ (p)$, akkor $p \mid x^2 - 1 = (x-1)(x+1)$, így $x \equiv \pm 1\ (p)$.
A kis Fermat-tétel miatt $a^{p-1} \equiv 1\ (p)$, ezért $x = a^{(p-1)/2} \equiv \pm 1\ (p)$. Az előző tétel miatt $a^{(p-1)/2} \equiv 1\ (p)$ ha a kvadratikus maradék, ezért a $(p-1)/2$ nemmaradék esetében -1-et kapunk mod p. □

Legendre-szimbólum

Definíció (FGy4.1.3)
Legyen $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék mod p, -1 ha nem, és 0, ha $p \mid a$. Ez a *Legendre szimbólum* (p páratlan prím).

Az Euler-lemma szerint $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}\ (p)$. Így igaz a következő.

Tétel (FGy4.1.4)
Tegyük fel, hogy p páratlan prím.

(1) Ha $a \equiv b\ (p)$, akkor $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(3) A -1 a $4k+1$ alakú prímekre lesz kvadratikus maradék. □

HF: Vezessük le a Wilson-tételből is, hogy -1 kvadratikus maradék a $4k+1$ alakú prímekre.
Ötlet: A $(p-1)!$ szorzatban párosítsunk minden számot az ellentettjével.

Kvadratikus reciprocitás

Tétel (Gauss, lásd FGy4.2.3), NB

Ha $p \neq q$ páratlan prímek, akkor $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$.

Tétel (FGy4.2.2, NB)

Ha p páratlan prím, akkor $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Azaz 2 akkor lesz kvadratikus maradék mod p, ha $p \equiv \pm 1$ (8).

A reciprocitási tétel nehéz, Gauss maga nyolc különböző bizonyítást adott rá, az egyik a Freud–Gyarmati-könyvben olvasható. Mi egy későbbi kurzus keretében egy elegáns bizonyítást fogunk látni, amely *Gauss-összegeken*, és a *véges testek* tulajdonságain alapszik.

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38$ (79) kongruencia?

$$\left(\frac{38}{79}\right) = \left(\frac{2}{79}\right)\left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}}(-1)^{\frac{19-1}{2}\frac{79-1}{2}}\left(\frac{79}{19}\right) =$$
$$= 1 \cdot (-1) \cdot \left(\frac{3}{19}\right) = -(-1)^{\frac{3-1}{2}\frac{19-1}{2}}\left(\frac{19}{3}\right) = -(-1) \cdot \left(\frac{1}{3}\right) = 1.$$

$79 \equiv 3$ (19) $19 \equiv 1$ (3)

Ezért a kongruencia megoldható. Az eredmény $x \equiv \pm 14$ (79), de a megoldást a fenti eljárás nem adja meg.

Probléma: Fel tudjuk-e a „számlálót” prímekre bontani?

Definíció (FGy4.3.1)

Ha az $m > 1$ páratlan szám a nem feltétlenül különböző $p_1, \ldots, p_k$ prímek szorzata, akkor legyen $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdot \ldots \cdot \left(\frac{a}{p_k}\right)$.

Ez a kiterjesztés a *Jacobi-szimbólum*, segít a faktorizáció-problémán.

A Jacobi-szimbólum tulajdonságai

Tétel (FGy4.3.2)
Tegyük fel, hogy $m, n > 1$ páratlan számok. Ekkor

(1) Ha $a \equiv b\ (m)$, akkor $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.

(2) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$ és $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

(3) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ és $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

(4) $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{m}{n}\right)$ (ha $(m,n) \neq 1$, akkor mindkettő 0).

E szabályok formálisan, azonnal következnek a Legendre-szimbólum tulajdonságaiból. Csak a számolás „közbülső" lépéseiben használjuk őket.
Például $\left(\frac{-1}{21}\right) = 1$, de $x^2 \equiv -1\ (21)$ nem oldható meg.

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183\ (8377)$ kongruencia? Itt 8377 prím.

$$\left(\frac{4183}{8377}\right) = \left(\frac{8377}{4183}\right) = \left(\frac{11}{4183}\right) = -\left(\frac{4183}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) =$$
$$= \left(\frac{-1}{3}\right) = -1,$$

tehát nem oldható meg. Valójában $4183 = 47 \cdot 89$, de ezt nem kellett észrevennünk, ez a Jacobi-szimbólumok előnye.

A reciprocitási tétel alkalmazásaként belátjuk a Pepin-teszt állítását.

Állítás
Ha $F_n = 2^{2^n} + 1 \geq 5$ Fermat-prím, akkor a 3 primitív gyök mod F_n.

Pepin-teszt (FGy5.2.2)
Az $F_n = 2^{2^n} + 1 \geq 5$ pontosan akkor prím, ha $3^{(F_n-1)/2} \equiv -1\ (F_n)$.

A Pepin-teszt bizonyítása
Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1\ (4)$.
Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1\ (3)$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1\ (3)$. Tehát a 3 kvadratikus nemmaradék mod F_n, és így $3^{(F_n-1)/2} \equiv -1\ (F_n)$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n, ekkor $t = \log_{g,F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt
$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g)/(o_{F_n}(g), t)$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így $o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n.

Tegyük föl, hogy $3^{(F_n-1)/2} \equiv -1\ (F_n)$.
Ekkor $o_{F_n}(3)$ nem osztója $(F_n - 1)/2 = 2^{2^n-1}$-nek. Viszont négyzetre emelve $3^{F_n-1} \equiv 1\ (F_n)$, azaz $o_{F_n}(3) \mid F_n - 1 = 2^{2^n}$. Tehát $o_{F_n}(3) = 2^\ell$, ahol $\ell \leq 2^n$, de $\ell \not\leq 2^n - 1$. Ezért $\ell = 2^n$, vagyis $o_{F_n}(3) = 2^{2^n} = F_n - 1$.
Ezért van $F_n - 1$ redukált maradékosztály mod F_n, így F_n prímszám. □

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak
Diszkrét logaritmus (index, FGy3.4.1).
k-adik hatványmaradék, kvadratikus maradék (FGy3.5.2, 4.1.1).
Legendre-szimbólum (FGy4.1.3). Jacobi-szimbólum (FGy4.3.1).

Tételek
A binom kongruencia megoldása (FGy3.5.1).
A hatványmaradékok jellemzése, száma (FGy3.5.3).
Euler-lemma (FGy4.1.2). A Legendre-szimbólum tulajdonságai (FGy4.1.4).
A kvadratikus reciprocitási tétel, $\left(\frac{2}{p}\right)$ (FGy4.2.2-3).
A Jacobi-szimbólum tulajdonságai (FGy4.3.2).
A 3 kvadratikus maradék a Fermat-prímekre, Pepin-teszt (FGy5.2.2).