1. Véges testek és kvadratikus maradékok

Ismertnek tekintjük a következőket.

1.1. Állítás. *Ha q prím, akkor minden $n \geq 1$-re izomorfia erejéig pontosan egy q^n elemű test létezik. Ennek multiplikatív csoportja ciklikus, és ezért minden $d \mid q^n - 1$-re van d rendű eleme. A $\varphi(x) = x^q$ leképezés testautomorfizmus, melynek fixpontjai pontosan a prímtest, vagyis az 1 által generált, $\mathbb{Z}_q$-val izomorf résztest elemei.*

Ha $q \nmid p$ prím, akkor $p \mid q^{p-1} - 1$, és így a q^{p-1} elemű testben van p rendű elem.

1.2. Állítás [Euler-lemma]. *Ha p páratlan prím és $p \nmid b$, akkor az $x^2 \equiv b\ (p)$ kongruencia akkor és csak akkor oldható meg, ha $b^{(p-1)/2} \equiv 1\ (p)$. Az ilyen b számok az úgynevezett kvadratikus maradékok mod p, számuk $(p-1)/2$. A nullán kívüli másik $(p-1)/2$ darab $b \in \mathbb{Z}_q$-ra $b^{(p-1)/2} \equiv -1\ (p)$, ezek a kvadratikus nemmaradékok. A $\left(\frac{b}{p}\right)$ Legendre-szimbólum értéke 1 ha b kvadratikus maradék, és -1 ha b nemmmaradék. Mivel $\left(\frac{b}{p}\right) \equiv b^{(p-1)/2}\ (p)$, ezért ez b-nek multiplikatív függvénye.*

2. A kvadratikus reciprocitási tétel

Legyen $p > 2$ prím és ε rögzített, p rendű eleme egy T test multiplikatív csoportjának. Ha u egész, akkor *Gauss-ciklusnak* nevezzük az $S_u = \sum_{j=0}^{p-1} \varepsilon^{uj^2}$ összeget.

2.1. Lemma. $S_u = \left(\frac{u}{p}\right) S_1$.

Bizonyítás. Ha u kvadratikus maradék mod p, akkor az állítás nyilvánvaló. Ha u nemmaradék, akkor az S_u összegben a kitevők a nulla mellett minden nemmaradékot kétszer adnak ki. Ezért $S_1 + S_u = 2\sum_{j=0}^{p-1} \varepsilon^j$, ami nulla a mértani sor összegképlete miatt. □

2.2. Lemma. *A $j^2 - k^2$ számok, ahol $0 \leq j, k \leq p-1$, a nulla kivételével minden értéket pontosan $p-1$-szer vesznek föl mod p, a nullát pedig $2p-1$-szer.*

Bizonyítás. Legyen $a = j - k$. Ha $a \not\equiv 0\ (p)$, akkor $j^2 - k^2 = a(a+2k)$, és rögzített a esetén $a + 2k$ teljes maradékrendszert fut be mod p (hiszen p páratlan). □

2.3. Lemma. $S_1^2 = \left(\frac{-1}{p}\right) p$.

Bizonyítás. Az előző lemma miatt $S_1 S_{-1} = p + (p-1)\sum_{j=0}^{p-1} \varepsilon^j = p$, de $S_{-1} = \left(\frac{-1}{p}\right) S_1$. □

Mostantól legyen T karakterisztikája egy q prím, prímteste Q.

2.4. Lemma. *A $\left(\frac{-1}{p}\right) p$ szám akkor és csak akkor kvadratikus maradék mod q, ha $S_1 \in Q$.*

Bizonyítás. Ha $S_1 \in Q$, akkor az előző állítás miatt $\left(\frac{-1}{p}\right) p$ kvadratikus maradék. Megfordítva, ha $b^2 \equiv \left(\frac{-1}{p}\right) p\ (q)$, akkor $b^2 = S_1^2$ teljesül a T testben, és ezért $S_1 = \pm b \in Q$. □

2.5. Tétel. *Ha p és q páratlan prímek, akkor $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$.*

Bizonyítás. Az 1.1. Állítás miatt $S_1 \in Q$ akkor és csak akkor, ha $S_1^q = S_1$. Mivel a q-adik hatványra emelés automorfizmus, $S_1^q = S_q = \left(\frac{q}{p}\right) S_1$. Ezért $\left(\frac{q}{p}\right) = 1$ akkor és csak akkor, ha $\left(\frac{-1}{p}\right) p = (-1)^{(p-1)/2} p$ kvadratikus maradék mod q, azaz ha $\left(\frac{-1}{q}\right)^{(p-1)/2} \left(\frac{p}{q}\right) = 1$. □

2.6. Feladat. *Legyen ε rendje 8. Az $S = \varepsilon + \varepsilon^7$ összeg felhasználásával adaptáljuk a fenti bizonyítást $\left(\frac{2}{q}\right)$ kiszámítására.*