

Most már tudunk minden szükségeset a komplex számokról. Következhet tehát az első részben már jelzett

### 3. Tétel.

$$(1) \quad \text{a) Ha } q \equiv 1(4) \text{ prím, akkor } \sum_{j=1}^{\frac{q-1}{2}} \varepsilon^{c_j} = \frac{\sqrt{q}-1}{2};$$

$$\text{b) Ha } q \equiv -1(4) \text{ prím, akkor } \sum_{j=1}^{\frac{q-1}{2}} \varepsilon^{c_j} = \frac{\sqrt{-q}-1}{2},$$

ahol  $\varepsilon = \cos \frac{2\pi}{q} + \sin \frac{2\pi}{q}$  és  $c_1, c_2, \dots, c_{\frac{q-1}{2}}$  vagy a  $q$  összes kvadratikus maradéka, vagy a  $q$  összes kvadratikus nemmaradéka (nyilván egy RMR-en belül).<sup>8</sup>

*Bizonyítás.* a) Könnyen látható, hogy  $\sum_{j=1}^{q-1} \varepsilon^j = -1$ , itt  $q$  prím voltából még csak a  $q > 1$  van kihasználva. Belátjuk,

$$\text{hogy } \left( \sum_{i=1}^{\frac{q-1}{2}} \varepsilon^{c_i} \right) \left( \sum_{j=1}^{\frac{q-1}{2}} \varepsilon^{d_j} \right) = \frac{1-q}{4}, \text{ ahol ezentúl } c_i \text{ jelölje a kvadratikus maradékokat, } d_i \text{ pedig a nemmaradékokat.}$$

A zárójelben lévő összegek tagonkénti szorzásakor  $\varepsilon$  kitevői összeadódnak, tehát azt kell megnézni, mit kapunk, ha az összes lehetséges módon összeadunk egy kvadratikus maradékot és egy nemmaradékot, vagyis képezzük az összes  $c_i + d_j$  alakú összeget. ( $1 \leq i \leq \frac{q-1}{2}$  és  $1 \leq j \leq \frac{q-1}{2}$ ; mint látjuk,  $i$  most nem a képzetes egység, hanem futóindex.) Írjuk ehhez a mod  $q$  maradékokat egy  $g$  primitív gyök hatványaiként. (A  $q = 17$  esetet szemlélteti a 2. ábra). Mivel  $g$  páros kitevőjű hatványai adják a kvadratikus maradékokat, és a páratlanok a nemmaradékokat, az összegek elkészítését a következő módon végezzük.  $k = 1$ -től  $\frac{q-1}{2}$ -ig minden  $k$ -ra képezzük az összes olyan  $c_i + d_j$  összeget, amelyre  $c_i$  és  $d_j$  „távolsága”  $2k - 1$ . Az ábrán az indexeket egy  $q - 1$  részre osztott körkerület osztópontjaival ábrázoljuk. Mivel  $\frac{q-1}{2}$  páros, azért egy kvadratikus maradéknak és egy kvadratikus nemmaradéknak megfelelő pont távolsága legfeljebb  $\frac{q-1}{2} - 1$  körívdarab lehet. Pontosabban fogalmazva azokat a  $c_i + d_j$ -ket képezzük, amelyekre  $g^i \text{ind } c_i - g^j \text{ind } d_j \pmod{q-1}$  legkisebb abszolút értékű maradéknak abszolút értéke  $2k - 1$ .

Ilyen módon az összes  $c_i + d_j$ -t megkapjuk, és mindegyiket pontosan egyszer. Mivel  $1 \leq k \leq \frac{q-1}{4}$ , ezért  $q-1 \nmid 4k-2$ , amiből  $g^{2k-1} \not\equiv -1 \pmod{q}$ , vagyis  $(g^{2k-1} + 1, q) = 1$ . Világos, hogy a rögzített  $k$  melletti összes  $c_i + d_j$  alakú összeg a következő alakban írható:

$$\{(g^{2k-1} + 1 \cdot g^l \mid 1 \leq l \leq q-1\},$$

ami az Euler–Fermat-ötlet szerint éppen egy RMR mod  $q$ . Ebből viszont már meg is kaptuk, hogy

$$\left( \sum_{i=1}^{\frac{q-1}{2}} \varepsilon^{c_i} \right) \left( \sum_{j=1}^{\frac{q-1}{2}} \varepsilon^{d_j} \right) = \frac{q-1}{4} \cdot \sum_{j=1}^{q-1} \varepsilon^j = \frac{1-q}{4},$$

mivel a  $k$  egymás után  $\frac{q-1}{4}$  darab értéket vesz fel.

Jelöljük az előbbi szorzat első tényezőjét  $x$ -szel, a másodikat pedig  $y$ -nal. Ekkor  $x + y = -1$  és  $xy = \frac{1-q}{4}$  miatt  $x = \frac{\sqrt{q}-1}{2}$  és  $y = \frac{-\sqrt{q}-1}{2}$  vagy  $x = \frac{-\sqrt{q}-1}{2}$  és  $y = \frac{\sqrt{q}-1}{2}$ , ami bizonyítja az a) állítást.

b) Lényegében az a)-val analóg módon bizonyítható, annyi csak az eltérés, hogy itt a  $c_i + d_j$  alakú összegek  $\frac{q-3}{4}$  RMR-t és  $\frac{q-1}{2}$  0-t adnak.

A 2. Tétel bizonyításához tekintsük a  $\sum_{j=0}^{q-2} a_j \varepsilon^j$  alakú számokat, ahol  $\varepsilon$  jelentése változatlan, az  $a_j$ -k pedig egész számok. Könnyen látható, hogy az említett alakú számok a  $\mathbf{C}$ -nek egy összeadásra, kivonásra és szorzásra zárt részhalmazát alkotják, amelyet  $\mathbf{Z}[\varepsilon]$ -nal jelöltünk. (Tehát  $\mathbf{Z}[\varepsilon]$  részgyűrűje a komplex számtestnek.) Mivel  $\mathbf{Z}[\varepsilon]$  az osztásra

<sup>7</sup> A cikk első része lapunk 1994/1. számában, (7–16. oldal) jelent meg.

<sup>8</sup> Megjegyzendő, hogy a fenti (1) egyenlőségeknél a  $c_j$ -k helyébe minden  $q$  esetén kvadratikus maradékok kerülnek. Ennek a bizonyítása azonban bonyolultabb és nem lesz rá szükségünk.

nem zárt, van értelme oszthatóságot definiálni.  $\alpha, \beta \in \mathbf{Z}[\varepsilon]$  esetén azt mondjuk, hogy  $\alpha$  osztható  $\beta$ -val, ha van olyan  $\gamma \in \mathbf{Z}[\varepsilon]$ , amelyre  $\alpha = \beta\gamma$ . Fel fogjuk használni azt a tényt, hogy az  $a$  és  $b$  egész számokra  $b \mid a$  pontosan akkor teljesül  $\mathbf{Z}$ -ben, ha teljesül  $\mathbf{Z}[\varepsilon]$ -ban is. Az állítás egyik oldala  $\mathbf{Z} \subset \mathbf{Z}[\varepsilon]$  miatt triviális, a másik oldal bizonyítása viszont egy-két olyan algebrai ismeret birtoklását feltételezi, amelyet a bevezetőben nem tárgyaltunk, így ezt csak lábjegyzetben<sup>9</sup> említjük meg. A  $\mathbf{Z}[\varepsilon]$ -beli kongruencia fogalmát szintén az egészekhez analóg módon definiáljuk. Végül az is magától értetődő, hogy  $\alpha \equiv \beta \pmod{\mu}$  és  $\gamma \equiv \delta \pmod{\mu}$  esetén fennáll az  $\alpha + \gamma \equiv \beta + \delta \pmod{\mu}$  és az  $\alpha \cdot \gamma \equiv \beta \cdot \delta \pmod{\mu}$  összefüggés.

Fogjunk hozzá a 2. Tétel bizonyításához. A 3. Tétel szerint

$$(2) \quad \sum_{j=1}^{q-1} \binom{j}{q} \varepsilon^j = \pm \sqrt{\left(\frac{-1}{q}\right) q};$$

itt figyelembe vettük a  $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$  egyenlőséget, amit könnyen megkaphatunk, ha  $-1$ -et egy primitív gyök hatványaként állítjuk elő mod  $q$ . Mivel  $j \neq 0, p$  esetén  $p \mid \binom{p}{j}$  és  $2 \nmid p$  miatt  $\binom{j}{p}^p = \binom{j}{p}$ , a binomiális tétel ismételt alkalmazásával azt kapjuk, hogy

$$(3) \quad \left(\sum_{j=1}^{q-1} \binom{j}{q} \varepsilon^j\right)^p = \sum_{j=1}^{q-1} \binom{j}{q} \varepsilon^{jp} \pmod{p}.$$

Emellett a Legendre-szimbólum (teljes) multiplikativitása és az Euler–Fermat ötlet alapján:

$$(4) \quad \sum_{j=1}^{q-1} \binom{j}{q} \varepsilon^{jp} = \binom{p}{q} \sum_{j=1}^{q-1} \binom{jp}{q} \varepsilon^{jp} = \binom{p}{q} \sum_{j=1}^{q-1} \binom{j}{q} \varepsilon^j.$$

(2)-t, (3)-at és (4)-rt összevetve a  $\sqrt{\left(\frac{-1}{q}\right) q}^p \equiv \binom{p}{q} \sqrt{\left(\frac{-1}{q}\right) q} \pmod{p}$  kongruenciához jutunk; ezt  $\sqrt{\left(\frac{-1}{q}\right) q}$ -val szorozva megkapjuk a

$$(5) \quad \left[\left(\frac{-1}{q}\right) q\right]^{\frac{p+1}{2}} \equiv \binom{p}{q} \cdot \left(\frac{-1}{q}\right) \cdot q \pmod{p}$$

összefüggést, amely egy nemrégiben tett megjegyzés szerint mint közönséges egészekre vonatkozó kongruencia is fennáll. Az egész számok gyűrűjében igaz a számelmélet alaptétele, így  $\left(\left(\frac{-1}{q}\right) \cdot q, p\right) = 1$  folytán (5)-öt egyszerűsíthetjük:

$$\left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \cdot q^{\frac{p-1}{2}} \equiv \binom{p}{q} \pmod{p}.$$

Innen pedig már valóban látszik a bizonyítandó

$$\binom{p}{q} \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2} \cdot \frac{p-1}{2}},$$

<sup>9</sup> Azt kell tehát belátni, hogy ha  $\beta\alpha = a$ , ahol  $a, b \in \mathbf{Z}, \alpha \in \mathbf{Z}[\varepsilon]$ , akkor  $\alpha \in \mathbf{Z}$ , hacsak  $a$  és  $b$  nem 0. (A  $0 \mid 0$  oszthatóság pedig nyilván  $\mathbf{Z}$ -ben is fennáll.) Tudjuk, hogy  $\varepsilon$  gyöke az  $f(x) = \sum_{j=0}^{q-1} x^j$  polinommal. Az ún. Schönemann–Eisenberg-kritérium szerint a  $\sum_{j=0}^{q-1} (x+1)^j =$

$\sum_{j=0}^{q-1} \binom{q}{j+1} x^j$  polinom irreducibilis  $\mathbf{Q}$  felett, ami nyilván ekvivalens az  $f$  irreducibilitásával. Belátjuk, hogy  $\varepsilon$  nem gyöke egyetlenegy  $(q-1)$ -nél alacsonyabb fokú racionális együtthatós ( $\neq 0$ ) polinomnak sem. Tegyük fel, hogy  $\varepsilon$  gyöke egy  $q-1 > n$ -edfokú polinomnak. A  $\mathbf{Q}[x]$ -beli polinomok körében alkalmazható az euklideszi algoritmus, ennélfogva  $f = g \cdot q_1 + r_1; g = r_1 q_2 + r_2; r_1 = r_2 q_3 + r_3, \dots$ , ahol  $\text{gr } q > \text{gr } r_1 > \text{gr } r_2 > \dots$ . Ez utóbbi 2-nél nagyobb egészek szigorúan csökkenő sorozata, ezért elég nagy  $k$ -re  $r_{k+1} = 0$ . Mivel  $\varepsilon$  gyöke  $f$ -nek és  $g$ -nek, gyöke  $r_k$ -nak is, ahol  $r_k$  az utolsó nem azonosan nulla maradék. Ezért  $\text{gr } r_k \geq 1$ , ugyanakkor  $r_{k-1} = r_k \cdot q_{k+1}$ , amiből látható, hogy  $r_k \mid f$  és  $r_k \mid g$ . Innen  $\text{gr } r_k \leq \text{gr } g < \text{gr } f$ , ami  $f$  irreducibilitásának ellentmond.

Legyen ezek után  $\alpha = \sum_{j=0}^{q-2} a_j \varepsilon^j$ , Ekkor  $0 = b\alpha - a = ba_0 - a + ba_1 \varepsilon + \dots + ba_{q-2} \varepsilon^{q-2}$ , tehát  $\varepsilon$  gyöke egy legfeljebb  $(q-2)$ -edfokú polinomnak, ami az előbbieket szerint csak a 0-polinom lehet, amiből  $\alpha = a_0 \in \mathbf{Z}$ , vagyis készen vagyunk.

hiszen  $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) (p)$ .

Elérkeztünk az 1. Tétel bizonyításához. Könnyen látható, hogy ha a szabályos  $n$ - és  $k$ -szög is megszerkeszthető, akkor  $(n, k) = 1$  esetén a szabályos  $nk$ -szög is az. Ennélfogva elég a következőket igazolni:

**1'. Tétel.** Ha az  $m$  természetes számra  $F_m$  prím, akkor a szabályos  $F_m$ -szög megszerkeszthető.

Mivel adott szakaszok összegét, különbségét, szorzatát, hányadosát és négyzetgyökét könnyen megszerkeszthetjük, azért a tétel bizonyításához elég belátni, hogy  $S(\varepsilon) = \varepsilon + \varepsilon^{-1} = 2 \cos \frac{2\pi}{F_m}$  előállítható racionális számokból alaplóműveletek és négyzetgyökvonások véges sokszori alkalmazásával.

Először is tetszőleges prímszám és  $n$  természetes szám esetére bevezetjük a következőt: Legyen

$$S_p(n, k) = \sum_{j=1}^{\frac{p-1}{(n, p-1)}} \varepsilon^{c_j},$$

ahol a  $c_j$ -k azon mod  $p$  maradékokat jelölik, amelyekre  $c_j^{\frac{p-1}{(n, p-1)}} \equiv k (p)$ . Megmutatjuk, hogy  $S_p(n, k)$  definíciója pontosan azokra a  $k$ -kre értelmes, amelyekhez van olyan  $t$  nemnegatív egész, hogy  $g^{t \frac{p-1}{(n, p-1)}} \equiv k (p)$ , ahol  $g$  a  $p$  egy tetszőlegesen rögzített primitív gyöke. Ha  $k \equiv g^{t \frac{p-1}{(n, p-1)}} (p)$  valamilyen  $t$ -vel, akkor az  $x^{\frac{p-1}{(n, p-1)}} \equiv k (p)$  kongruenciának  $g^{y \cdot (n, p-1) + t}$  minden  $y$ -ra megoldása, és  $0 \leq y < \frac{p-1}{(n, p-1)}$  esetén a kapott megoldások páronként inkongruensek mod  $p$ . A fokszámtétel miatt a szóban forgó kongruenciának több megoldása viszont nincs, így  $k \equiv g^{t \frac{p-1}{(n, p-1)}} (p)$  esetén a fenti definíció valóban értelmes. Ha  $k \equiv g^{t \frac{p-1}{(n, p-1)} + s}$ , ahol  $1 \leq s < \frac{p-1}{(n, p-1)}$ , akkor nem lehet semmilyen  $x$ -re  $x^{\frac{p-1}{(n, p-1)}} \equiv k (p)$ , mert ebből  $(n, p-1)$ -edik hatványra emeléssel  $g^{s \cdot (n, p-1)} \equiv 1 (p)$  adódna, ami az  $s$ -re vonatkozó feltevés és  $g$  primitív gyök volta miatt nem állhat fenn, az esetben tehát a fenti definíció értelmetlen.

Ezután ténylegesen elkezdhetjük az 1'. Tétel bizonyítását. Egyszerűség kedvéért az  $F_m$  rögzített Fermat-prímet ezentúl  $p$ -vel, az  $S_p(n, k)$  összeget pedig  $S(n, k)$ -val jelöljük.

Ezek alapján egy *valós számot megszerkeszthetőnek* fogunk hívni, ha előállítható racionális számokból az alaplóműveletek és a négyzetgyökvonás véges sokszori alkalmazásával. Könnyen látható, hogy  $S(1, 1) = -1$  (nyilván megszerkeszthető), és a 3. Tétel alapján megszerkeszthető  $S(2, 1)$  és  $S(2, -1)$  is. Világos továbbá, hogy  $S(\varepsilon) = \varepsilon + \varepsilon^{-1} = S\left(\frac{p-1}{2}, 1\right) = S\left(2^{2^{m-1}}, 1\right)$ .

A továbbiakban  $x$ -re vonatkozó teljes indukcióval belátjuk, hogy  $S\left(2^x, g^{t \frac{p-1}{2^x}}\right)$  minden nemnegatív  $t$  egészre megszerkeszthető ( $1 \leq x < 2^m$ ).

Legyen  $1 \leq x < 2^m$  és tegyük fel, hogy  $S\left(2^{x-1}, g^{t \frac{p-1}{2^{x-1}}}\right)$  minden  $t \geq 0$  egészre megszerkeszthető. Minden  $t$ -re kiszámítjuk  $S\left(2^x, g^{t \frac{p-1}{2^x}}\right)$ -et. Itt a  $t = 2^x$ -hez és a  $t = 2^{x-1}$ -hez tartozó összegek  $S(2^x, 1)$ , illetve  $S(2^x, -1)$ . Először ezeket határozzuk meg. Most nyilván azokat a  $c_i + d_j$  összegeket kell képezni, amelyekre  $c_i^{\frac{p-1}{2^x}} \equiv 1$  és  $d_j^{\frac{p-1}{2^x}} \equiv -1 (p)$ . Vegyünk egy olyan  $h$ -t, amelyre  $o_p(h) = \frac{p-1}{2^{x-1}}$ . Ilyen  $h$  létezik ( $g^{2^{x-1}}$  és annak páratlan kitevőjű hatványai). Írjuk fel  $h$  első  $\frac{p-1}{2^{x-1}}$  hatványát, és legyen a  $k$  pozitív egész szerepe itt is ugyanaz, mint ami a 3. Tétel bizonyításában volt. Könnyen ellenőrizhető az alábbi három állítás:

1.  $h$  páros hatványai adják a  $c_i$ -ket és a páratlanok a  $d_j$ -ket.

2. Ha a  $c_i + d_j$  összegek elkészítését ugyanúgy végezzük, ahogy azt a 3. Tétel bizonyításánál tettük, akkor mialatt a  $k$  1-től  $\frac{p-1}{2^{x+1}}$ -ig fut, mindegyik  $c_i + d_j$ -t pontosan egyszer kapjuk meg.

3. Rögzített  $k$  esetén azon  $c_i + d_j$ -k halmaza, amelyekre  $c_i$  és  $d_j$  „Ívtávolsága”  $2k - 1$  (lásd a 3. ábrát), a következő:  $\left\{ (h^{2k-1} + 1) h^l \mid 1 \leq l \leq \frac{p-1}{2^{x-1}} \right\}$ . Az utolsó állítás megfogalmazását pontosná tehetjük azáltal, hogy két elem ívtávolsága helyett azok  $h$  alapú indexei különbségének mod  $\frac{p-1}{2^{x-1}}$  legkisebb abszolút értékű maradékának abszolút értékét szerepeltetjük. A szóban forgó ívtávolság nyilván ez utóbbinak egy szemléletes elnevezése.

Mivel  $2 \leq 4k - 2 \leq \frac{p-1}{2^{x-1}} - 2$  és  $o(h) = \frac{p-1}{2^{x-1}}$ , ezért  $(h^{2k-1} + 1, p) = 1$ , tehát minden  $k$ -hoz van olyan  $\alpha(k)$  pozitív egész, amelyre  $h^{2k-1} + 1 \equiv g^{\alpha(k)} (p)$ , amiből minden  $l$ -re  $[(h^{2k-1} + 1)h^l]^{\frac{p-1}{2^x}} \equiv g^{\alpha(k) \cdot \frac{p-1}{2^x}} (p)$  adódik. Ebből viszont az induktív feltevés figyelembevételével azt kapjuk, hogy a  $\sum_{l=1}^{\frac{p-1}{2^x-1}} \varepsilon^{[(h^{2k-1}+1)h^l]}$  összeg mindegyik

$k$  esetén megszerkeszthető, tehát megszerkeszthető a  $\sum_{k=1}^{\frac{p-1}{2x+1}} \sum_{l=1}^{\frac{p-1}{2x-1}} \varepsilon^{[(h^{2k-1}+1)h^l]} = S(2^x, 1) \cdot S(2^x, -1)$  is. Tudjuk, hogy  $S(2^x, 1) + S(2^x, -1) = s(2^{x-1}, 1)$ , tehát a másodfokú egyenlet gyökei és együttthatói összefüggéséből:

$$S(2^x, \pm 1) = \frac{1}{2} \left( s(2^{x-1}, 1) \pm \sqrt{s^2(2^{x-1}, 1) - 4S(2^x, 1)S(2^x, -1)} \right).$$

$S(2^x, 1)$  és  $S(2^x, -1)$  megszerkeszthetőségéhez már csak annyit kell belátnunk, hogy az iménti gyökjel alatt nemnegatív szám áll. Az induktív feltevés miatt egyrészt  $S(2^{x-1}, 1)$  valós, másrészt  $x < 2^m$ , aminek köszönhetően  $\frac{p-1}{2^x}$  páros. Ennélfogva  $a^{\frac{p-1}{2^x}} \equiv (-a)^{\frac{p-1}{2^x}} \pmod{p}$ , mely szerint ha  $\varepsilon^a$  szerepel az  $S(s^x, 1)$  tagjai között, akkor kell, hogy a konjugáltja,  $\varepsilon^{-a}$  is szerepeljen ugyanott, így megkaptuk, hogy  $S(2^x, 1)$  és  $S(2^x, -1)$  valós. Tehát a fenti gyökjel alatti kifejezés értéke valóban nemnegatív, amivel  $S(2^x, 1)$  és  $S(2^x, -1)$  megszerkeszthetőségét igazoltuk.

Megállapodásunk szerint  $S\left(2^x, g^{t \cdot \frac{p-1}{2^x}}\right) = \sum_{i=1}^{\frac{p-1}{2^x}} \varepsilon^{a_i}$ , ahol  $a_i^{\frac{p-1}{2^x}} \equiv g^{t \cdot \frac{p-1}{2^x}} \pmod{p}$ . Az  $S(2^x, 1)$  definíciójában szereplő  $c_i$ -kre pedig

$$(6) \quad c_i^{\frac{p-1}{2^x}} \equiv 1 \pmod{p}, \text{ amiből } (c_i g^t)^{\frac{p-1}{2^x}} \equiv g^{t \cdot \frac{p-1}{2^x}} \pmod{p}.$$

Mivel a  $c_i$ -k páronként inkongruensek voltak, azért a  $c_i g^t$  maradékok is páronként inkongruensek mod  $p$ , s így (6), valamint amiatt, hogy az  $a_i$ -k száma megegyezik a  $c_i$ -k számával, az  $a_i$ -k mindegyike kongruens pontosan egy  $c_i g^t$ -vel.

Ebből viszont azt kapjuk, hogy  $S\left(2^x, g^{t \cdot \frac{p-1}{2^x}}\right) = \sum_{i=1}^{\frac{p-1}{2^x}} \varepsilon^{c_i g^t}$ . Ugyanezzel a gondolatmenettel az is belátható, hogy

$$S\left(2^x, -g^{t \cdot \frac{p-1}{2^x}}\right) = \sum_{j=1}^{\frac{p-1}{2^x}} \varepsilon^{d_j g^t},$$

ahol

$$d_j^{\frac{p-1}{2^x}} \equiv -1 \pmod{p}.$$

Így az  $S(2^x, 1)S(2^x, -1)$ -re kapott eredmény felhasználásával:

$$S\left(2^x, g^{t \cdot \frac{p-1}{2^x}}\right) S\left(2^x, -g^{t \cdot \frac{p-1}{2^x}}\right) = \sum_{k=1}^{\frac{p-1}{2x+1}} \sum_{l=1}^{\frac{p-1}{2x-1}} \varepsilon^{g^{t+\alpha(k)} \cdot h^l}.$$

Az indukciós feltevés szerint a

$$\sum_{l=1}^{\frac{p-1}{2x-1}} \varepsilon^{g^{t+\alpha(k)} \cdot h^l} = S\left(2^{x-1}, g^{(t+\alpha(k)) \cdot \frac{p-1}{2x-1}}\right)$$

összeg minden  $1 \leq k \leq \frac{p-1}{2x+1}$  esetén megszerkeszthető, ezért megszerkeszthető az

$$S\left(2^x, g^{t \cdot \frac{p-1}{2^x}}\right) S\left(2^x, -g^{t \cdot \frac{p-1}{2^x}}\right)$$

is, továbbá ezen szorzat tényezőinek összege nyilván  $S(2^{x-1}, g^{t \cdot \frac{p-1}{2x-1}})$ , ami ugyancsak az indukciós feltevés miatt szintén megszerkeszthető.  $S(2^x, g^{t \cdot \frac{p-1}{2^x}})$  megszerkeszthetősége innen már ugyanúgy belátható, mint ahogy beláttuk az előzőekben  $S(2^x, \pm 1)$  megszerkeszthetőségét.

Igazoltuk, hogy minden  $0 \leq x < 2^m$  és minden  $t$  nemnegatív egész esetén  $S(2^x, g^{t \cdot \frac{p-1}{2^x}})$  megszerkeszthető, ennélfogva megszerkeszthető  $S(2^{2^m-1}, 1) = 2 \cos \frac{2\pi}{p}$  is, amivel az 1'. Tétel, és ennek eredményeképpen az 1. Tétel bizonyítást nyert.<sup>10</sup>

Befejezésül, a leírtak elmélyítése céljából megoldásra javasolok néhány feladatot.

1. Számítsuk ki  $2 \cos \frac{2\pi}{17}$ -et a fenti gondolatmenettel. (Ez nem olyan hosszú.)

<sup>10</sup>Ha valaki egy konkrét  $p$  Fermat-prím esetén meg akarja határozni az itt megadott módon  $2 \cos \frac{2\pi}{p}$ -t, akkor minden lépésnél tudnia kell, hogy a „megoldóképletben” a gyökjel előtti előjelek közül melyik érvényes. Ez viszont az adott esetben mindig megállapítható.

2. Bizonyítsuk be, hogy  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ .

3. Igazoljuk, hogy  $m > 0$  esetén  $F_m$  akkor és csak akkor prím, ha  $3^{\frac{F_m-1}{2}} \equiv -1 \pmod{F_m}$ .

4. Mutassuk meg az előző két feladat felhasználásával, hogy minden 5-nél nagyobb Fermat-prímnél a 3 a legkisebb primitív gyöke.

5. Adjuk meg annak a szükséges és elégséges feltételét, hogy a  $p$  prímszámmra  $S_p(4, 1) = \frac{-1 + \sqrt{p} \pm \sqrt{2(p - \sqrt{p})}}{4}$  igaz legyen.

6. Mi dönti el, hogy az előző feladatban szereplő egyenlőségben ( $p = 8k + 1$  alakú prím) melyik előjel érvényes? (Ha ezt tudjuk, akkor az is kiderül, hogy az 5.-ben lévő feltétel teljesülése esetén mindig az  $S_p(4, 1) = \frac{-1 + \sqrt{p} + \sqrt{2(p - \sqrt{p})}}{4}$  áll fenn.) Nézzük meg, hogy az  $S_p(4, 1)$  összeggel mi a helyzet, ha  $p = 8k + 5$  alakú.

**Borsányi Ákos**