

E cikkben az F.2468. feladatban kimondott állítást bizonyítjuk be, nevezetesen a következőt:

Akkor és csak akkor létezik olyan konvex n -szög, melynek szögei egyenlők, oldalai pedig valamilyen sorrendben $1, 2, 3, \dots, n$ egységnyi hosszúak, ha n nem egy prímszám hatványa.

A feladat megoldásában ¹ megmutattuk, hogy a kérdéses n -szög $n = 10$ esetén létezik, és azt is láttuk, hogy a bizonyítandó állítás ekvivalens a következővel:

Legyenek $\mathbf{x}_1, \dots, \mathbf{x}_n$ egy szabályos n -szög középpontjából a csúcsokba mutató vektorok. Akkor és csak akkor létezik az $1, 2, \dots, n$ számoknak olyan $a_1, a_2, \dots, a_n$ permutációja, amivel az

$$a_1 \mathbf{x}_1 + a_2 \mathbf{x}_2 + \dots + a_n \mathbf{x}_n$$

vektorösszeg a nullvektor, ha n nem egy prímszám hatványa.

Bizonyításunk két részre oszlik attól függően, hogy n prímszám-e vagy sem.

1. *n nem prímszám.* Ebben az esetben n felbomlik két egymánál nagyobb, egymáshoz relatív prím egész szorzatára, legyen $n = p \cdot q$ egy ilyen felbontás. Jelöljük $p(i)$ -vel, illetve $q(i)$ -vel azt a maradékot, ami i -nek p -vel, q -val való osztásakor adódik. A p függvény értéke minden p -edik egész számra ugyanaz, tehát $p(1), p(2), \dots, p(n)$ között pontosan q darab 0 , q darab 1 -es stb. fordul elő.

Így

$$(1) \quad p(1)\mathbf{x}_1 + p(2)\mathbf{x}_2 + \dots + p(n)\mathbf{x}_n = \mathbf{0},$$

hiszen azok az $\mathbf{x}_i$ vektorok, amelyekre $p(i)$ egy rögzített (0 és $p-1$ közé eső) értéket vesz fel, egy szabályos q -szög csúcsaiba mutatnak – s egy szabályos sokszög középpontjából a csúcsokba mutató vektorok összege mindig $\mathbf{0}$. Ezért (1) bal oldala p darab nullvektor összege, s ezért maga is $\mathbf{0}$.

Hasonlóan kapjuk, hogy

$$q(1)\mathbf{x}_1 + q(2)\mathbf{x}_2 + \dots + q(n)\mathbf{x}_n = \mathbf{0},$$

csak most q darab szabályos p -szöget kifesztő részüsszege bontható a bal oldal. Ha most az $a_i = 1 + p(i) + p \cdot q(i)$ értékeket választjuk, akkor a kérdéses vektorösszeg

$$\sum_{i=1}^n a_i \mathbf{x}_i = \sum_{i=1}^n \mathbf{x}_i + \sum_{i=1}^n p(i) \mathbf{x}_i + p \cdot \sum_{i=1}^n q(i) \mathbf{x}_i = \mathbf{0}.$$

Ezek az a_i értékek nyilván 1 és $n = p \cdot q = 1 + (p-1) + p \cdot (q-1)$ közé eső egészek.

Tehát a keresett permutáció létezését azonnal igazoltuk, mihelyst beláttuk, hogy az így definiált $a_1, a_2, \dots, a_n$ számok között nincs két egyenlő. Ám $a_i = a_j$ csak úgy lehet, ha $p(i) = p(j)$ (összük el a_i -t és a_j -t is p -vel), de ekkor $q(i) = q(j)$ is fennáll. Ám $p(i) = p(j)$ azt jelenti, hogy $i-j$ osztható p -vel, $q(i) = q(j)$ pedig azt, hogy $i-j$ osztható q -val. p és q relatív prímek, tehát $i-j$ osztható $p \cdot q = n$ -nel is, ami lehetetlen, mivel i és j is 1 és n közé eső egészek. Ezzel igazoltuk az állítást mindazon értékekre, amikor n nem prímszám.

A bizonyításnak ez a fele lényegében *Kaiser Andrástól* (Bp., József A. Gimn.) származik. Rajta kívül még *Megyesi Gábor* (akkor a szegedi Ságvári Endre Gyak. Gimn. tanulója volt) küldte be ennek a résznek a bizonyítását.

2. *n prímszám.* Az állítás e felének bizonyítása lényegesen nehezebb, mint az előzőé. Azt kell ugyanis megmutatni, hogy *nem létezik* az $1, 2, \dots, n$ számoknak megfelelő permutációja. Míg előbb elegendő volt egyetlen ilyen találni és arról igazolni, hogy az jó (bár arról nem esett szó, hogyan találtuk meg ezt a bizonyos permutációt), jelen esetben az összes permutációról kell igazolnunk, hogy rossz. Ezek száma már $n = 20$ esetén is olyan óriási, hogy egyesével végignézni lehetetlenség. A helyzet kissé hasonlít a szabályos sokszögek szerkeszthetőségéhez. Könnyű szabályos ötszöget szerkeszteni, s a szerkesztés helyességének igazolása sem túl bonyolult. Magát a szerkesztést valószínűleg már Pitagorasz is ismerte (i. e. 550 körül). Ám annak bizonyítása, hogy semmiféle (euklideszi) szerkesztési eljárással nem tudunk szabályos hétszöget szerkeszteni, csak majd 2000 év múlva sikerült Gaussnak, a „matematika fejedelmének”. Ő a geometriai szerkesztési feladatot algebrai, pontosabban polinomokra vonatkozó feladattá fogalmazta át, amit végül is sikerrel megoldott.

1985-03-098-1.eps

Mi is ezt az utat követjük: a bizonyítandó állítást egy algebrai állítássá fogalmazzuk át. Majd az apró lemmák kimondása után az átfogalmazott állításra kerül sor. Érdekesképpen megjegyezzük, hogy a fenti párhuzam nem csupán illusztráció: a felhasználásra kerülő algebrai apparátus, sőt a lemmák is megegyeznek azokkal, amiket Gauss az idézett tétel bizonyítására használt.

¹Lásd e számunk 104. oldalán.

Lássuk először az átfogalmazást. Az $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ egységnyi hosszúságú vektorok egy pozitív körüljárású szabályos n -szög csúcsaiba mutatnak. Helyezzük el ezeket a vektorokat a komplex számsíkon úgy, hogy a sokszög középpontja a számsík origójába, az $\mathbf{x}_n$ vektor végpontja pedig a valós számegyenes $+1$ pontjába essen. Jelöljük ε -nal azt a komplex számot, amelybe az $\mathbf{x}_1$ vektor végpontja mutat. Az ε abszolút értéke (hossza) 1, modulusa (a pozitív valós tengellyel bezárt szöge) $2\pi/n$. Így az ε -nal történő szorzás egy pozitív irányú $2\pi/n$ nagyságú szöggel való elforgatást jelent, például $\varepsilon^2 = \varepsilon \cdot \varepsilon$ -t úgy kapjuk, hogy ε -t elforgatjuk az origó körül $2\pi/n$ szöggel. Tehát $\mathbf{x}_2$ végpontja ε^2 , s hasonlóan $\mathbf{x}_i$ végpontja ε^i . Speciálisan $\varepsilon^n = 1$, ahonnan

$$0 = \varepsilon^n - 1 = (\varepsilon - 1)(\varepsilon^{n-1} + \varepsilon^{n-2} + \dots + \varepsilon + 1).$$

Mivel $\varepsilon \neq 1$, azért a második tényezőnek kell nullának lennie. Komplex számokat vektorként kell összeadni, az

$$(2) \quad \varepsilon^{n-1} + \varepsilon^{n-2} + \dots + \varepsilon^2 + \varepsilon + 1 = 0$$

összefüggés azt mondja ki, hogy a szabályos n -szög középpontjából a csúcsokba mutató vektorok összege nulla, ahogyan azt már korábban állítottuk. Az $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}$ számokat n -edik *egységgyököknek* szokás nevezni, hiszen ezek (és csak ezek) n -edik hatványa 1.

A (2) összefüggést még úgy is értelmezhetjük, hogy ε gyöke az

$$(3) \quad f(x) = x^{n-1} + x^{n-2} + \dots + x^2 + x + 1$$

polinomnak. A bizonyítandó állítás, mármint az, hogy az $1, 2, \dots, n$ számok tetszőleges $a_1, a_2, \dots, a_n$ permutációjára $\sum a_i x_i \neq 0$, komplex számokkal megfogalmazva azt mondja, hogy $\sum a_i \varepsilon^i \neq 0$, vagyis hogy ε *nem gyöke* a

$$(4) \quad g(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_2x^2 + a_1x + a_n$$

polinomnak. Ezzel elérkeztünk a keresett átfogalmazáshoz:

Az $a_1, a_2, \dots, a_n$ számok tetszőleges megengedett megválasztása mellett az $f(x)$ és $g(x)$ polinomoknak nem lehet közös (komplex) gyöke.

Hogy ne szakítsuk meg a bizonyítás menetét, előre bocsátunk két, polinomokra vonatkozó segédtevélt. Ezek bizonyítása – mint látni fogjuk – sok ötletet igényel és meglehetősen hosszú. Mindamellett ezek a lemmák sokszor alkalmazhatók, például a szerkeszthetőség elméletében alapvető jelentőségűek.

1. Lemma *Ha n prímszám, akkor az $f(x) = x^{n-1} + \dots + x^2 + x + 1$ polinom nem bontható fel két (legalább elsőfokú) racionális együtthatós polinom szorzatára. (Ezt úgy mondjuk, hogy $f(x)$ irreducibilis a racionális számtest felett.)*

2. Lemma *Legyen $f(x)$ és $g(x)$ két tetszőleges racionális együtthatójú polinom, és tegyük föl, hogy az α (komplex) szám mindkettőnek gyöke. Ekkor vannak olyan $f_1(x), g_1(x)$ és $h(x)$ racionális együtthatós polinomok, hogy*

$$f(x) = f_1(x) \cdot h(x), \quad g(x) = g_1(x) \cdot h(x)$$

és α a gyöke $h(x)$ -nek. (Elképzelhetők, hogy $f_1(x)$ vagy $g_1(x)$ azonosan konstans polinom.)

Legyen tehát most n prímszám, és tegyük fel, hogy a (3) és (4) alatt definiált f és g egész együtthatós, tehát speciálisan racionális együtthatós polinomoknak volna közös gyöke. Ekkor a 2. lemma szerint $f(x) = f_1(x) \cdot h(x)$ és $g(x) = g_1(x) \cdot h(x)$ alakban szorzattá bonthatók, ahol f_1, g_1 és h racionális együtthatósak. Az 1. lemma szerint f nem bontható fel legalább elsőfokú racionális együtthatós polinomok szorzatára, tehát f_1 szükségképpen azonosan konstans, mondjuk mindenütt az $1/r$ racionális értéket veszi fel. Ekkor $f(x) = f_1(x) \cdot h(x)$ alapján

$$h(x) = r \cdot x^{n-1} + r \cdot x^{n-2} + \dots + r \cdot x^2 + r \cdot x + r.$$

Tudjuk, hogy $g(x) = g_1(x) \cdot h(x)$. Ha g_1 legalább elsőfokú lenne, akkor a $g_1(x) \cdot h(x)$ szorzat legalább n -edfokú polinom lenne, noha (4) szerint $g(x)$ pontosan $(n-1)$ -edfokú. Ezért g_1 is nulladfokú, mondjuk azonosan s értéket vesz föl, ezért $g(x) = g_1(x) \cdot h(x)$ miatt $g(x)$

$$(rs) \cdot x^{n-1} + (rs) \cdot x^{n-2} + \dots + (rs) \cdot x^2 + (rs) \cdot x + (rs)$$

alakú. Ennek minden együtthatója egyenlő, tehát például $a_1 = a_2$. Ez pedig lehetetlen, hiszen $a_1, a_2, \dots, a_n$ az $1, 2, \dots, n$ számok egy permutációja, így páronként különböző számokból áll. Ellentmondásra jutottunk abból a feltevésből, hogy a (3) és (4) alatti polinomoknak van közös gyökük (legalábbis abban az esetben, ha n prím), így az állítást bizonyítottuk.

A bizonyítás egy kicsit többet adott, nevezetesen a következőt. Ha $a_1, a_2, \dots, a_n$ olyan egész számok, amelyekre a (3) és (4) alatti polinomoknak van közös gyökük, akkor szükségképpen $a_1 = a_2 = \dots = a_n$. „Visszagöngyölve” azokat az átfogalmazásokat, átalakításokat, amiket az eredeti feladaton csináltunk, ebből az alábbi tételt kapjuk:

Legyen n egy prímszám. Ha egy n oldalú konvex n -szög minden szöge egyenlő és minden oldalának mértékszáma egész, akkor a sokszög szabályos (és persze az oldalak egyenlők).

A téglalap mutatja, hogy ez az állítás nem marad érvényben, ha n -et prímszám helyett prímhatalványnak választjuk. Mivel ezt a következményt kizárólag az 1. és 2. lemmából vezettük le, azért az 1. lemma állítása nem maradhat érvényben $n = 4$ -re. (Tehát abból, hogy létezik 1 és 2 oldalhosszúságú téglalap, következtetünk arra, hogy az $x^3 + x^2 + x + 1$ polinom felbomlik két racionális együtthatójú polinom szorzatára! S valóban, $x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$.) Prímhatványra tehát általában a fenti gondolatmenet nem használható, ráadásul ha n nem prímszám, a (3) alatti polinom biztosan nem irreducibilis. Ahhoz, hogy mégis mentsük ami menthető, elsőként olyan irreducibilis polinomot kell találnunk, aminek a legkisebb modulusú n -edik egységgyökök, amit ε -nal jelölünk, gyöke. Legyen tehát $n = p^k$, ahol p prím és $k \geq 1$ egész szám. Jelöljük a p^{k-1} számot q -val, ekkor $n = p \cdot q$, tehát $\varepsilon^n = \varepsilon^{pq} = 1$, és persze $\varepsilon^q \neq 1$. Így

$$0 = \varepsilon^n - 1 = (\varepsilon^q)^p - 1 = (\varepsilon^q - 1)(\varepsilon^{(p-1)q} + \varepsilon^{(p-2)q} + \dots + \varepsilon^q + 1),$$

következésképp ε gyöke az

$$(5) \quad f^*(x) = x^{(p-1)q} + x^{(p-2)q} + \dots + x^{2q} + x^q + 1$$

polinomnak.

3. Lema Az $f^*(x)$ egész együtthatós polinom irreducibilis a racionális számtest felett.

Vegyük észre, hogy az 1. lemma speciális esete a 3. lemmának $k = 1$, azaz $q = 1$ mellett.

Legyen most $n = p^k$ és tegyük fel, hogy az $a_1, a_2, \dots, a_n$ egész számok olyanok, hogy a

$$g(x) = a_{n-1}x^{n-1} + \dots + a_2x^2 + a_1x + a$$

polinomnak és a fenti $f^*(x)$ polinomnak van közös gyöke. Pontosan ugyanúgy, mint az előbb, csak most a 2. és 3. lemma segítségével adódik, hogy van olyan racionális együtthatójú $g_1(x)$ polinom, amivel

$$g(x) = g_1(x) \cdot f^*(x).$$

Az $f^*(x)$ fokszáma $(p-1) \cdot q$, a $g(x)$ -é $n-1 = pq-1$, ezért $g_1(x)$ fokszáma $(pq-1) - (p-1) \cdot q = q-1$, vagyis

$$g_1(x) = b_{q-1}x^{q-1} + b_{q-2}x^{q-2} + \dots + b_1x + b_0.$$

Ekkor viszont a $g_1(x) \cdot f^*(x)$ szorzatban minden $0 \leq i \leq q-1$ mellett az $x^i, x^{i+q}, \dots, x^{i+(p-1)q}$ együtthatója mind b_i , tehát $g(x)$ -ben a megfelelő hatványok együtthatói is egyenlők. Következésképp $a_1, a_2, \dots, a_n$ nem lehet mind különböző, és így nem lehet az $1, 2, \dots, n$ számok egy permutációja sem. A tételt ezzel igazoltuk.

A bizonyítás most azt adta, hogy $g(x)$ -ben minden $q = p^{k-1}$ -edik együttható megegyezik. Ezt az egyenlőszögű n -szögekre a következőképpen fogalmazhatjuk át:

Legyen $n = p^k$, ahol p prímszám. Ha egy n oldalú konvex n -szög minden szöge egyenlő és oldalainak mértékszáma egész, akkor a sokszög minden p^{k-1} -edik oldala ugyanolyan hosszú.

Ebből: $k = 1$ -re visszaadódik az előző követelmény, $n = 8$ -ra pedig a 2137-es gyakorlat általánosítása: ha egy konvex sokszög minden szöge 135° és oldalai egészek, akkor szemközti oldalai egyenlő hosszúak.

Ami hátra van, a korábban kimondott három lemma bizonyítása. Valójában elég csak az utóbbi kettőt belátni, hiszen a 3. lemmának speciális esete az 1.

A 2. lemma bizonyítása

Legyenek $f(x)$ és $g(x)$ olyan racionális együtthatós polinomok, amelyeknek az α (komplex) szám közös gyöke. Olyan $f_1(x)$, $g_1(x)$ és $h(x)$ racionális együtthatójú polinomokat kell találnunk, amelyekre

$$f(x) = f_1(x) \cdot h(x), \quad g(x) = g_1(x) \cdot h(x),$$

és α gyöke $h(x)$ -nek.

Az állítást $f(x)$ és $g(x)$ fokszámának összegére vonatkozó teljes indukcióval bizonyítjuk. Feltehetjük, hogy $f(x)$ és $g(x)$ legalább elsőfokú, így

$$f(x) = a_0x^m + a_1x^{m-1} + \dots + a_{m-1}x + a_m$$

és

$$g(x) = b_0x^n + b_1x^{n-1} + \dots + b_{n-1}x + b_n,$$

ahol $a_0 \neq 0$ és $b_0 \neq 0$, és mondjuk $n \leq m$. Indukciós feltevésünk szerint az állítás igaz az összes olyan polinom párra, melyek fokszámainak összege kisebb $(m+n)$ -nél.

Tekintsük most az $\bar{f}(x) = f(x) - \frac{a_0}{b_0} \cdot x^{m-n} \cdot g(x)$ polinomot. Ez nyilván racionális együtthatós, fokszáma m -nél kisebb, és mivel α gyöke volt $f(x)$ -nek és $g(x)$ -nek is, gyöke lesz $\bar{f}(x)$ -nek is. Ha most $\bar{f}(x)$ nulladfokú, akkor $\bar{f}(\alpha) = 0$ miatt azonosan nulla, és ekkor

$$f(x) = \frac{a_0}{b_0} x^{m-n} \cdot g(x) \quad \text{és} \quad g(x) = 1 \cdot g(x)$$

megfelelő felbontás. Ha viszont $\bar{f}(x)$ legalább elsőfokú, akkor $\bar{f}(x)$ -re és $g(x)$ -re az állítást már tudjuk, hiszen fokszámaik összege kisebb $(m+n)$ -nél. Tehát vannak $f_1(x)$, $g_1(x)$ és $h(x)$ racionális együtthatójú polinomok, amikre $h(x)$ -nek α gyöke, továbbá

$$\bar{f}(x) = f_1(x) \cdot h(x) \quad \text{és} \quad g(x) = g_1(x) \cdot h(x).$$

Ekkor viszont

$$f(x) = \bar{f}(x) + \frac{a_0}{b_0} x^{m-n} g(x) = \left(f_1(x) + \frac{a_0}{b_0} x^{m-n} g_1(x) \right) \cdot h(x)$$

és

$$g(x) = g_1(x) \cdot h(x)$$

adja a keresett felbontást. Ezzel a 2. lemmát bizonyítottuk.

A 3. lemma bizonyítása

A lemma egy bizonyos egész együtthatós polinomról állítja, hogy nem bontható fel két racionális együtthatójú polinom szorzatára. Elsőként azt mutatjuk meg, hogy ha a polinom felbomlik racionális együtthatójú polinomok szorzatára, akkor egész együtthatós polinomok szorzataként is felírható. Ez az állítás *Gauss-féle lemma* néven ismeretes, és természetesen Gausstól származik.

Legyen tehát

$$\begin{aligned} f(x) &= x^n + A_1 x^{n-1} + \dots + A_{n-1} x + A_n = \\ &= (x^r + b_1 x^{r-1} + \dots + b_{r-1} x + b_r)(x^s + c_1 x^{s-1} + \dots + c_{s-1} x + c_s), \end{aligned}$$

ahol $A_1, A_2, \dots, A_n$ egész számok, a b_i, c_i együtthatók pedig racionálisak. Tegyük fel, hogy b_i, c_i már tovább nem egyszerűsíthető alakban van felírva, és legyen B_0 a b_i együtthatók nevezőinek legkisebb közös többszöröse, C_0 pedig a c_i együtthatóké. Legyen még

$$b_i = \frac{B_i}{B_0}, \quad c_i = \frac{C_i}{C_0}.$$

Világos, hogy nincs olyan prímszám, ami osztója lenne a $B_0, B_1, \dots, B_r$ számok mindegyikének, s olyan sincs, ami a $C_0, C_1, \dots, C_s$ mindegyikét osztaná.

A fenti szorzat mindkét oldalát $B_0 C_0$ -al szorozva kapjuk, hogy

$$B_0 C_0 f(x) = (B_0 x^r + B_1 x^{r-1} + \dots + B_r)(C_0 x^s + C_1 x^{s-1} + \dots + C_s).$$

A bal és jobb oldalon a megfelelő hatványok együtthatóinak meg kell egyeznie, tehát

$$\begin{aligned} B_0 C_0 A_1 &= B_0 C_1 + B_1 C_0, \\ B_0 C_0 A_2 &= B_0 C_2 + B_1 C_1 + B_2 C_0, \\ &\dots \\ B_0 C_0 A_{i+j} &= \\ &= B_0 C_{i+j} + B_1 C_{i+j-1} + \dots + B_{i-1} C_{j+1} + B_i C_j + B_{i+1} C_{j-1} + \dots + B_{i+j} C_0 \\ &\dots \end{aligned}$$

Legyen p tetszőleges prímosztója a $B_0 C_0$ szorzatnak. Előző megjegyzésünk értelmében p nem lehet osztója az összes B_i számnak, van olyan $0 \leq i \leq r$, hogy p osztója $B_0, B_1, \dots, B_{i-1}$ -nek, de nem osztója B_i -nek. Ugyanígy van olyan $0 \leq j \leq s$ is, hogy p osztója $C_0, C_1, \dots, C_{j-1}$ mindegyikének, de nem osztója C_j -nek. Ez a p osztója $B_0 C_0 A_{i+j}$ -nek. A fenti kifejezésekben $B_0 C_0 A_{i+j}$ jobb oldalán viszont mindegyik összeadandó – az egyetlen $B_i C_j$ kivételével – osztható p -vel, $B_i C_j$ nem osztható, ezért a jobb oldal sem osztható p -vel.

Az ellentmondás azt jelenti, hogy nem lehet $B_0 C_0$ -nek prímosztója, vagyis $B_0 C_0 = 1$, ahonnan $B_0 = C_0 = 1$. Ez viszont azt mutatja, hogy az $f(x)$ szorzat előállításában a b_i, c_i együtthatók szükségszerűen egészek. A Gauss-lemmát bizonyítottuk.

Ennek alapján annak bizonyításához, hogy egy 1 főegyütthatójú, egész együtthatós polinom nem bontható fel racionális együtthatójú polinomok szorzatára, elegendő megmutatni, hogy nem bontható *egész* együtthatójú polinomok

szorzatára. Erre ad elégséges feltételt az alábbi, *Schoenemann és Eisenstein*, a múlt század közepén működő német matematikusokról elnevezett kritérium:

Ha az egész együtthatós

$$f(x) = x^n + A_1x^{n-1} + \dots + A_{n-1}x + A_n$$

polinom $A_1, A_2, \dots, A_n$ együtthatói mind oszthatók a p prímszámmal, és A_n nem osztható p^2 -tel, akkor a polinom nem bontható fel egész együtthatós polinomok szorzatára.

Tegyük fel ugyanis, hogy $f(x)$ felírható

$$(x^r + B_1x^{r-1} + \dots + B_r)(x^s + C_1x^{s-1} + \dots + C_s)$$

alakban, ahol B_i és C_i egészek. Ekkor $B_rC_s = A_n$ miatt ez a szorzat osztható p -vel, de nem osztható p^2 -tel — következésképp B_r és C_s közül pontosan az egyik osztható p -vel. Legyen ez mondjuk C_s . Ekkor

$$A_{n-1} = B_{r-1}C_s + B_rC_{s-1}$$

szerint $B_rC_{s-1} = A_{n-1} - B_{r-1}C_s$ is osztható p -vel, de mivel B_r nem osztható vele, ezért C_{s-1} -nek kell p -vel oszthatónak lennie. Hasonlóan

$$A_{n-2} = B_{r-2}C_s + B_{r-1}C_{s-1} + B_rC_{s-2}$$

alapján az adódik, hogy C_{s-2} is osztható p -vel stb., végül

$$A_r = B_{r-s}C_s + B_{r-s+1}C_{s-1} + \dots + B_{r-1}C_1 + B_rC_0$$

miatt azt kapjuk, hogy $C_0 = 1$ is osztható p -vel, ami ellentmondás. Ez pedig a Schoenemann–Eisenstein kritérium helyességét igazolja.

Most már rátérhetünk a 3. lemma állításának bizonyítására. Legyen p egy prímszám, $q = p^{k-1}$ valamely $k \geq 1$ egészre. Azt szeretnénk belátni, hogy az

$$f(x) = x^{(p-1)q} + x^{(p-2)q} + \dots + x^{2q} + x^q + 1$$

egész együtthatós polinom irreducibilis. A Gauss-lemma alapján ehhez elég belátnunk, hogy $f(x)$ nem bontható fel két egész együtthatós polinom szorzatára. Ez utóbbi igazolására a Schoenemann–Eisenstein kritériumot szeretnénk használni. Ez persze közvetlenül nem megy, egy picit ravaszkodnunk kell. Tekintsük a

$$g(x) = f(x+1) = (x+1)^{(p-1)q} + \dots + (x+1)^{2q} + (x+1)^q + 1$$

egész együtthatós polinomot. Ha $f(x)$ felbomlana két egész együtthatós polinom szorzatára, akkor persze $g(x)$ is felbomlana. Így abból, hogy $g(x)$ irreducibilis, következtethetünk arra, hogy $f(x)$ is az. $g(x)$ -re viszont már működik a kritérium. A binomiális tétel alapján világos, hogy $g(x)$ legmagasabb fokú tagja $x^{(p-1)q}$ konstans tagja pedig p (hiszen $p-1$ darab $(x+1)$ -hatványt kell összeadnunk). Ezért elég belátni, hogy $g(x)$ -ben az összes többi előforduló hatvány együtthatója osztható p -vel.

Elsőként számítsuk ki $(x+1)^q$ -t:

$$(x+1)^q = x^q + 1 + \sum_{i=1}^{q-1} \binom{q}{i} x^i.$$

A szumma-jel mögött álló binomiális együtthatók mind oszthatók p -vel, hiszen

$$\binom{q}{i} = \frac{q}{i} \binom{q-1}{i-1},$$

a második tényező egész $1 \leq i \leq q-1$ esetén, és az első tényező számlálója az egyszerűsítések után is osztható p -vel. Ezért

$$(x+1)^q = x^q + 1 + p \cdot G(x),$$

és így

$$(x+1)^{iq} = (x^q + 1 + p \cdot G(x))^i = (x^q + 1)^i + p \cdot G_i(x)$$

szintén a binomiális tétel alapján, ahol $G(x)$ és $G_i(x)$ is egész együtthatós polinomok. Ezekkel a $g(x)$ polinomot a következőképpen írhatjuk föl:

$$g(x) = \sum_{i=0}^{p-1} (x+1)^{iq} = \sum_{i=0}^{p-1} (x^q + 1)^i + p \cdot \sum_{i=0}^{p-1} G_i(x).$$

A jobb oldalon az első szumma $x^q = ((x^q + 1) - 1)$ -szerese éppen $(x^q + 1)^p - 1$, ami a binomiális tétel szerint a következővel egyezik meg:

$$x^{qp} + \binom{p}{1}x^{q(p-1)} + \dots + \binom{p}{p-1}x^q = x^q(x^{(p-1)q} + p \cdot H(x)),$$

ahol $H(x)$ egész együtthatójú. Ezért

$$g(x) = x^{(p-1)q} + p \cdot H(x) + p \cdot \sum_{i=0}^{p-1} G_i(x),$$

vagyis $g(x)$ -ben valóban az összes többi együttható osztható p -vel, amint állítottuk. Innen a Schoenemann–Eisenstein kritérium alapján $g(x)$ irreducibilis – tehát $f(x)$ is az, ez pedig a 3. lemma állítása volt.