GAUSS-EGÉSZEK ÉS DIRICHLET TÉTELE

KEITH KEARNES, KISS EMIL, SZENDREI ÁGNES

Első rész

1. Bevezetés

Tekintsük az $ak + b$ számtani sorozatot, ahol $a > 0$. Ha a és b nem relatív prímek, akkor $(a, b) > 1$ osztója a sorozat mindegyik tagjának, és így a sorozatban legföljebb egy prímszám szerepelhet (a kényelem kedvéért a prímszámokat pozitívnak tekintjük).

1.1. Tétel [Dirichlet, 1837]. *Ha $a > 0$ és a, b relatív prím egész számok, akkor az $ak + b$ $(k = 1, 2, \ldots)$ számtani sorozatban végtelen sok prímszám található.*

A tételnek csak olyan bizonyítása ismeretes, amely komplex analízist használ. Egy ilyen, középiskolások számára is érthetően leírt bizonyítás olvasható Szalay Mihály [6] középiskolás tagozatos tankönyvének függelékében.

Ugyanakkor a tételnek vannak olyan speciális esetei, melyeket elemi úton is be tudunk bizonyítani. Ebben a kétrészes cikkben így igazoljuk a tételnek az $nk + 1$, illetve az $nk - 1$ alakú számok sorozatára vonatkozó állítását. Az n betű végig ezt a pozitív egészet jelöli majd. Az a, b, c, d, i, j, k, ℓ, m, u és p betűk is végig egész számokat jelölnek, melyek közül p prímszám.

Feltételezzük, hogy az Olvasó ismeri a számelmélet alapvető fogalmait és tételeit, valamint a komplex számok és a polinomok legfontosabb tulajdonságait. Ezeknek a [2], illetve a [3] tankönyvek első fejezeteiben nézhet utána. Mindkét könyv tartalmazza az $nk+1$ eset bizonyítását is ([2], 5.3.4. tétel, illetve [3], 5.8.15. feladat, melynek megoldása az internetről letölthető). Az alább következő gondolatmenet kicsit elemibb. Ennek ismertetésével ér véget a cikk első része.

Bauer Mihály 1900 táján talált elemi bizonyítást a tétel $nk - 1$ esetére. Erdős Pál és Surányi János [1] könyvükben megemlítik a két alapötletet (203. oldal). Cikkünk második részében, a már bevezetett fogalmakra alapozva, egy ehhez hasonló gondolatmenetet mutatunk be. Szerepel egy bizonyítás Schur [5] cikkében is.

Felmerül a kérdés, hogy milyen számtani sorozatok esetében létezik még hasonló elemi bizonyítás. Erre Murty [4] eredménye ad választ: az $ak + b$ számok sorozata akkor és csak akkor ilyen, ha $b^2 \equiv 1\ (a)$. Érdekesség, hogy ennek igazolásához olyan mély tételt alkalmaz (Csebotarjov sűrűségi tételét 1922-ből), amely Dirichlet tételének általánosítása.

Murty bizonyítása az algebrai számelmélet eszköztárát használja. Ebből az Olvasó kap majd kis ízelítőt, mert a Gauss-egészek fogalmát mi is bevezetjük a cikk második

részében. Ugyanakkor cikkünk algebrai szempontból is elemi, a számelméleti elemrend és a körosztási polinomok fogalmát felhasználjuk majd, de testekről már nem beszélünk. A test fogalmának birtokában néhány számolás egyszerűsödött volna, de nem lényegesen. Az ilyen lehetőségre mindig utalunk a szövegben, biztatva az Olvasót, hogy az egyszerűsítést végezze el.

A bizonyítást feladatsorozat formájában ismertetjük. A feladatok nem nehezek, érdemes velük önállóan próbálkozni. Mindegyik feladat után közvetlenül szerepel a megoldása.

2. Két elemi bizonyítás

2.1. Feladat. *Igazoljuk, hogy végtelen sok $4k-1$ alakú prímszám van.*

Megoldás. Tegyük föl indirekt, hogy csak véges sok ilyen prímszám van, legyenek ezek $p_1, p_2, \ldots, p_\ell$. Tekintsük az $N = 4p_1p_2\ldots p_\ell - 1$ számot. Ez 1-nél nagyobb, ezért prímszámok szorzata. E prímtényezők mindegyike 2-től és mindegyik p_j-től különbözik, és így 4-gyel osztva már csak 1 maradékot adhat. Ekkor azonban a szorzatuk is 1-et ad maradékul, ami ellentmondás, mert $N \equiv -1$ (4). □

Megjegyezzük, hogy Dirichlet tételének analitikus bizonyítása már az egyszerű esetekben is többet ad, mint az elemi bizonyítások, mert segítségével meg lehet becsülni, hogy az adott számtani sorozatban „mennyi" prímszám van. Például ha $a = 12$, akkor csak négy sorozat jön szóba: $12k+1$, $12k+5$, $12k+7$, $12k+11$. Ezekben egymáshoz képest „ugyanannyi" prímszám van, a következő értelemben. Jelölje $\pi_b(x)$ a $12k+b$ alakú, x-nél nem nagyobb prímek számát. Ekkor $b = 1, 5, 7, 11$ mindegyikére

$$\frac{\pi_b(x)}{x/\log(x)} \to \frac{1}{4} \qquad (x \to \infty)$$

(a logaritmus természetes alapú). Vagyis a négy sorozat mindegyikébe a prímek körülbelül egynegyede esik. Ez az eredmény erősítése a Nagy Prímszámtételnek (mely szerint a prímek száma x-ig körülbelül $x/\log(x)$, lásd [2], 5.4.1. tétel).

Ugyanakkor a 2.1. feladat megoldása nagyon „kevés" $4k-1$ alakú prímet szolgáltat. A kapott „új" prímről ugyanis nem tudunk mást, mint hogy legföljebb N. Ez a sorozat pedig nagyon gyorsan növekszik: a 3-ból kiindulva a kapott számok 11, 131, 17291, 298995971. Az Olvasónak érdemes meggondolnia, hogy az eljárás x-ig csak körülbelül $\log\log(x)$ darab $4k-1$ alakú prímet biztosít. Ugyanakkor az x-nél nem nagyobb $4k-1$ alakú prímek számának nagyságrendje $x/2\log(x)$.

Elemien bizonyítható az is, hogy végtelen sok $4k+1$ alakú prím van. Ehhez már egy segédállításra van szükségünk.

2.2. Feladat. *Igazoljuk, hogy ha a p prímszám $4k-1$ alakú, akkor $p \mid a^2+b^2$-ből $p \mid a$ és $p \mid b$ következik. Speciálisan az u^2+1 alakú számok mindegyik páratlan prímosztója $4k+1$ alakú.*

Megoldás. Ha a és b valamelyike osztható p-vel, akkor $p \mid a^2 + b^2$ miatt a másik is. Ha egyik sem, akkor az $a^2 \equiv -b^2\ (p)$ kongruenciát $(p-1)/2$-edik hatványra emelve az Euler–Fermat-tétel miatt $1 \equiv (-1)^{(p-1)/2}\ (p)$ adódik. Mivel $p \equiv -1\ (4)$, ezért $(-1)^{(p-1)/2} = -1$. Így $1 \equiv -1\ (p)$, ami ellentmond annak, hogy p páratlan. □

2.3. Feladat. *Igazoljuk, hogy végtelen sok $4k+1$ alakú prímszám van.*

Megoldás. Tegyük föl indirekt, hogy csak véges sok ilyen prímszám van, legyenek ezek $p_1, p_2, \ldots, p_\ell$. Tekintsük az $N = (2p_1p_2 \ldots p_\ell)^2 + 1$ számot. Ez 1-nél nagyobb, ezért prímszámok szorzata. E tényezők mindegyike 2-től és mindegyik p_j-től különbözik, és a 2.2. feladat miatt 4-gyel osztva 1 maradékot ad. Ez az ellentmondás bizonyítja az állítást. □

3. Körosztási polinomok

A továbblépéshez érdemes másik megoldást adni a 2.2. feladat második állítására. Ez bonyolultabb lesz, mert felhasználja a számelméleti elemrend fogalmát, de lehetővé teszi az általánosítást. Emlékeztetőül összefoglaljuk a renddel kapcsolatos tudnivalókat (lásd [2], 3.2. szakasz).

3.1. Feladat. *Tegyük föl, hogy $(c, m) = 1$. Mutassuk meg, hogy van olyan pozitív k egész, melyre $c^k \equiv 1\ (m)$.*

Megoldás. Mivel véges sok modulo m maradék van, léteznek olyan $i < j$ egészek, hogy $c^i \equiv c^j\ (m)$. A modulushoz relatív prím c^i-vel egyszerűsítve $c^{j-i} \equiv 1\ (m)$ adódik. □

Ha r a legkisebb olyan tulajdonságú pozitív k szám, ami az előző feladatban szerepel, akkor c hatványai egy r hosszúságú periódus szerint ismétlődnek, és így c különböző hatványainak száma r. Ezt az r számot c *rendjének* nevezzük modulo m, jele $o_m(c)$. A periodicitás miatt $c^k \equiv 1\ (m) \Longleftrightarrow o_m(c) \mid k$. Az Euler–Fermat-tételből ezért következik, hogy $o_m(c) \mid \varphi(m)$.

3.2. Gyakorlat. Számítsuk ki 2 és 3 rendjét modulo 7.

Megoldás. Mivel 2 hatványai modulo 7 rendre 2, 4, $8 \equiv 1\ (7)$, ezért $o_7(2) = 3$. Hasonlóan, 3 első három hatványa modulo 7 rendre 3, $9 \equiv 2$ és $3^3 = 3^2 \cdot 3 \equiv 2 \cdot 3 = 6$. Tovább nem érdemes számolni a következő okból. Az eddigiek szerint 3 rendje nagyobb, mint 3. De ez a rend osztója $\varphi(7) = 6$-nak, ezért csakis 6 lehet. □

3.3. Feladat. *Legyen p prímosztója az $u^2 + 1$ számnak. Igazoljuk, hogy $o_p(u) = 4$ vagy $p = 2$.*

Megoldás. Mivel $p \mid u^2 + 1 \mid u^4 - 1$, ezért $u^4 \equiv 1\ (p)$, azaz $o_p(u) \mid 4$. Ha ez a rend nem 4, akkor 1 vagy 2. Mindkét esetben $u^2 \equiv 1\ (p)$. A feltétel szerint $u^2 \equiv -1\ (p)$, ezért $-1 \equiv 1\ (p)$, azaz $p = 2$. □

Innen persze páratlan p esetén $4 = o_p(u) \mid \varphi(p) = p-1$, azaz megkaptuk a 2.2. feladat második állítását. Ez a megoldás azt sugallja, hogy ha a $4k+1$ sorozat helyett az $nk+1$ sorozatban keresünk prímeket, akkor $u^2+1 \mid u^4-1$ helyett az u^n-1 kifejezés alkalmas tényezőjével célszerű dolgoznunk.

Az x^n-1 polinom szorzatra bontását *körosztási polinomok* segítségével végezhetjük el. Az x^n-1 gyökei az $\varepsilon_k = \cos(2\pi k/n) + i\sin(2\pi k/n)$ komplex számok, ahol $1 \le k \le n$, vagyis az n-edik komplex *egységgyökök* (lásd [3], 1.5. szakasz). Mivel egész együtthatós polinomokat szeretnénk kapni, ezért x^n-1 gyöktényezői közül bizonyosakat összevonunk. Legyen

$$\Phi_n(x) = \prod_{\substack{1\le k\le n\\(k,n)=1}} \left(x-\varepsilon_k\right).$$

E polinom gyökei a *primitív* n-edik egységgyökök, maga $\Phi_n(x)$ pedig az n-edik körosztási polinom. Az alábbi tétel x^n-1 kívánt szorzatra bontását szolgáltatja.

3.4. Tétel. *Ha $n \ge 1$, akkor a következők teljesülnek.*

(1) *$\Phi_n(x)$ foka $\varphi(n)$.*
(2) *Érvényes az*

$$x^n - 1 = \prod_{d\mid n} \Phi_d(x)$$

azonosság.
(3) *$\Phi_n(x)$ egész együtthatós.*

Az előző tételt az Olvasó könnyen igazolhatja, vagy megtalálhatja a bizonyítást a [3] könyv 3.9. szakaszában. A (2) pont képletéből a körosztási polinomokat kiszámíthatjuk rekurzívan, egységgyökökre való hivatkozás nélkül is.

3.5. Gyakorlat. Számítsuk ki a $\Phi_n(x)$ polinomokat, amikor $n = 1, 2, 3, 4, 12$.

Megoldás. Mivel a nevező $n=1$ esetén üres szorzat, $\Phi_1(x) = x-1$ (vagy a definícióból közvetlenül láthatjuk, hogy az 1 az egyetlen primitív 1-edik egységgyök). A képletből $\Phi_2(x) = (x^2-1)/(x-1) = x+1$ és $\Phi_3(x) = (x^3-1)/(x-1) = x^2+x+1$. Mivel $\Phi_1(x)\Phi_2(x) = x^2-1$, ezért $\Phi_4(x) = (x^4-1)/(x^2-1) = x^2+1$. Hasonlóan összevonva a nevezőben

$$\Phi_{12}(x) = \frac{x^{12}-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)} = \frac{x^{12}-1}{(x^6-1)\Phi_4(x)} = \frac{x^6+1}{x^2+1} = x^4-x^2+1$$

(hiszen $\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = x^6-1$). □

A $\Phi_4(x) = x^2+1$ összefüggés alapján a 3.3. Feladat állítása úgy is fogalmazható, hogy ha p prímosztója a $\Phi_4(u)$ számnak, akkor $o_p(u) = 4$ vagy $p \mid 4$. Ezt általánosítja a következő tétel, amit az utána következő három feladatban látunk be.

3.6. Tétel. *Legyen p prímosztója a $\Phi_n(u)$ számnak. Ekkor $o_p(u) = n$ vagy $p \mid n$.*

Mivel $\Phi_n(u) \mid u^n-1$, ezért p és u relatív prímek, tehát az $o_p(u)$ rend értelmes.

3.7. Feladat. *Legyenek $f(x)$, $g(x)$, $h(x)$ egész együtthatós polinomok, és tegyük föl, hogy f és g konstans tagja is osztható p-vel. Ekkor az $f(x)g(x)h(x)$ szorzatpolinomban a konstans tag is, az x-es tag együtthatója is osztható p-vel.*

Megoldás. Legyen $f(x) = a_0 + a_1x + \ldots$, $g(x) = b_0 + b_1x + \ldots$, $h(x) = c_0 + c_1x + \ldots$. Ekkor a szorzatpolinomban a konstans tag $a_0b_0c_0$, az x-es tag együtthatója pedig $a_0b_0c_1 + a_0b_1c_0 + a_1b_0c_0$. □

Megjegyezzük, hogy ha hajlandóak vagyunk polinomok együtthatóival modulo p számolni, akkor ez a megoldás egyszerűbben is megfogalmazható. A modulo p vett maradékok egy p elemű $\mathbb{Z}_p$ testet alkotnak. Vegyük mindhárom polinom együtthatóit modulo p, ekkor $\mathbb{Z}_p$ fölötti polinomokat kapunk. A feltétel szerint $f(x)$ és $g(x)$ is osztható x-szel $\mathbb{Z}_p[x]$-ben, tehát $f(x)g(x)h(x)$ osztható x^2-tel. Ennek a gondolatmenetnek a precíz megalapozása a [3] könyvben olvasható (1.1. szakasz, illetve 2.3.8. Gyakorlat).

3.8. Feladat. *Tegyük föl, hogy p prímosztója a $\Phi_n(u)$ számnak, de $o_p(u) \neq n$. Igazoljuk, hogy ekkor van olyan $m \mid n$, hogy $m \neq n$ és $p \mid \Phi_m(u)$.*

Megoldás. Mivel $p \mid \Phi_n(u) \mid u^n - 1$, ezért $u^n \equiv 1\ (p)$, és így $o_p(u) \mid n$. Legyen $o_p(u) = d < n$. Ekkor $u^d \equiv 1\ (p)$, azaz $p \mid u^d - 1 = \prod_{m|d} \Phi_m(u)$. Mivel p prím, osztója valamelyik tényezőnek. □

3.9. Feladat. *Igazoljuk a 3.6. tételt.*

Megoldás. Tegyük föl, hogy p prímosztója a $\Phi_n(u)$ számnak, de $o_p(u) \neq n$. Az előző feladat miatt van olyan $m \mid n$, hogy $m \neq n$ és $p \mid \Phi_m(u)$. Legyen $f(x) = \Phi_n(x+u)$, $g(x) = \Phi_m(x+u)$, továbbá legyen $h(x)$ mindazon $\Phi_\ell(x+u)$ polinomok szorzata, ahol $\ell \mid n$ de $\ell \neq n, m$. Ha a 3.4. tétel (2) állítását $x^n - 1$ helyett $(x+u)^n - 1$-re alkalmazzuk, akkor $f(x)g(x)h(x) = (x+u)^n - 1$ adódik. Helyettesítsünk $x = 0$-t, ekkor láthatjuk, hogy $f(x)$ és $g(x)$ konstans tagja is osztható p-vel. Ezért a 3.7. feladat miatt az $(x+u)^n - 1$ polinom x-es tagjának együtthatója osztható p-vel. A binomiális tétel szerint ez nu^{n-1}. Mivel $p \mid \Phi_n(u) \mid u^n - 1$ miatt p relatív prím u-hoz, ezért $p \mid n$. □

Az Olvasó a 3.6. tételt felhasználva most már könnyen általánosíthatja a 2.3. feladat megoldását, és beláthatja hogy végtelen sok $nk + 1$ alakú prímszám van. Mi ezt a lépést azért bontjuk három feladatra, mert így könnyebb lesz követni a cikk második részében az $nk - 1$ eset gondolatmenetét.

3.10. Feladat. *Mutassuk meg, hogy minden pozitív K egészhez van olyan u egész, hogy $\Phi_n(u)$ osztható egy K-nál nagyobb p prímszámmal.*

Megoldás. Legyen $u = LK!$, ahol az L pozitív egész értékét később választjuk meg. Mivel $\Phi_n(x) \to \infty$ ha $x \to \infty$, ezért L-et elég nagyra választva $\Phi_n(LK!) > 1$, és így $\Phi_n(u) = \Phi_n(LK!)$-nak van egy p prímosztója. Tudjuk, hogy $\Phi_n(u) \mid u^n - 1$, ezért p relatív prím $u = LK!$-hoz. Így $p > K$. □

3.11. Feladat. *Igazoljuk, hogy ha a p prím nagyobb n-nél, és u olyan egész szám, amelyre $p \mid \Phi_n(u)$, akkor a p prím $nk + 1$ alakú.*

Megoldás. A 3.6. tételből következik, hogy $o_p(u) = n$, hiszen $p > n$ miatt $p \mid n$ nem teljesül. Ezért $n = o_p(u) \mid \varphi(p) = p - 1$. □

3.12. Feladat. *Bizonyítsuk be, hogy minden $n > 0$ esetén végtelen sok $nk + 1$ alakú prímszám van.*

Megoldás. Tegyük föl indirekt, hogy csak véges sok ilyen prímszám van, legyenek ezek $p_1, p_2, \ldots, p_\ell$. Válasszuk a K számot úgy, hogy ezek mindegyikénél, továbbá n-nél is nagyobb legyen. A 3.10. feladat miatt van olyan u egész, továbbá egy K-nál nagyobb p prím, melyre $p \mid \Phi_n(u)$. Az előző feladat szerint a p prím $nk + 1$ alakú, ami ellentmondás. □

Ajánlott irodalom

[1] Erdős Pál, Surányi János: *Válogatott fejezetek a számelméletből.* Polygon Kiadó, 1996.
[2] Freud Róbert, Gyarmati Edit: *Számelmélet.* Nemzeti Tankönyvkiadó, 2006.
[3] Kiss Emil: *Bevezetés az algebrába.* TypoTEX Kiadó, 2007.
[4] M. R. Murty: *Primes in certain arithmetic progressions.* J. Madras Univ. (1988), 161–169.
[5] I. Schur: *Über die existenz unendlich vieler primzahlen in einiger speziellen arithmetischen progressionen.* Sitzungber. Berliner Math. Ges. **11** (1912), 40—50.
[6] Szalay Mihály: *Számelmélet.* TypoTEX Kiadó, 1998.