Számelméleti 5letek

Gyarmati Katalin

katalin.gyarmati@ttk.elte.hu

Eötvös Loránd Tudományegyetem

Egyetemi Jegyzet

ELTE TTK Matematikai Intézet

Tartalomjegyzék

Bevezetés

Az alábbi kurzust (specit) BSc matematikus hallgatóknak tartom a számelmélet néhány olyan tételéről, illetve fejezetéről, amelyek megértéséhez elegendő a középiskolás és az elsőéves egyetemi algebra és számelmélet tananyag ismerete. Sokszor hosszasan kerestem az alábbi érdekes és olykor meglepő eredményeket. A fejezetek végén az irodalomjegyzékben tüntettem fel a tételek eredeti (legtöbbször angol nyelvű) forrását.

Azonban a bizonyítások elemi volta mellett, a tételek bizonyítása néha koránt sem egyszerű... Így a kurzus végén a jegyszerzés kétféle módon is történhet: feladatmegoldással vagy vizsgával az elméleti anyagból.

1. Geometriai bizonyítások a számelméletben

A számelméletben gyakran alkalmaznak más területeken is hasznos módszereket. Ezek közül néhány mély matematikai ismereteket kíván, azonban vannak olyanok is, amelyek megértéséhez a középiskolás ismeretanyag is elég. Ezek közül a bizonyítások közül ismertetünk most kettőt, amelyek geometriára épülnek.

1.1. A kis-Fermat tétel geometriai bizonyítása

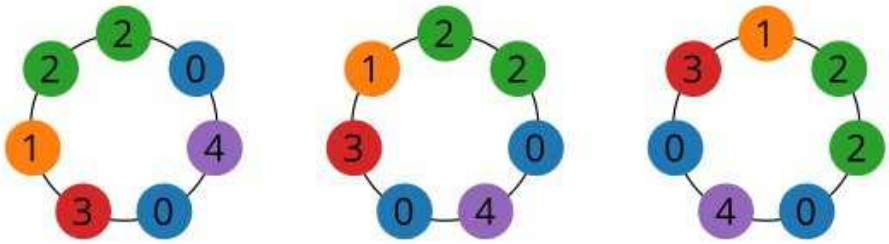
A kis Fermat tételt leggyakrabban kongruenciák felhasználásával bizonyítják. Azonban van egy olyan bizonyítás is, amelyben még csak a kongruencia definíciójára sincs szükség. A tétel a következőképpen szól:

1.1. TÉTEL. *Minden p prímre és a természetes számra*

$$p \mid a^p - a.$$

A 1.1. Tétel bizonyítása. A tétel bizonyítását [9] alapján ismertetjük. A szabályos p-szög csúcsaiba természetes számokat írunk, mégpedig 1-től a-ig terjedően. (Hívjuk ezt az eljárást „színezésnek"). Ekkor minden csúcsba a-féle számot írhatunk, tehát az ilyen színezések száma pontosan a^p.

Szokás ezt a bizonyítást nyakláncokkal is illusztrálni, a gyöngyök a nyaklláncban a szabályos p-szög csúcsai, a gyöngyök színe pedig a számok 1-től a-ig.



A fenti színezések között a darab olyan van, ahol minden csúcsba ugyanazt a számot írtunk. A többi színezést csoportokba osztjuk egy csoportba téve azokat, amelyek egymásból elforgatással megkaphatók.

Ha T egy csoportbeli színezés, ahol $(k/p \cdot 360)°$ jelöli azt a legkisebb szögű forgatást, amely T-t önmagába viszi, akkor szükségszerűen $k \mid p$. Ugyanis tegyük fel $k \nmid p$. Tudjuk a $(2k/p \cdot 360)°$, $(3k/p \cdot 360)°, \ldots$ szögű forgatások is T-t önmagába viszik, viszont a $(\lceil \frac{p}{k} \rceil k/p \cdot 360)°$ forgatás szöge (a $360°$ fokot levonva belőle) olyan alakba írható, hogy $(j/p \cdot 360)°$, ahol $0 < j < k$ (itt $j = \lceil \frac{p}{k} \rceil k - p < (\frac{p}{k} + 1)k - p = k$), és ez ellentmondás.

Vagyis, ha a T színezés benne van egy csoportban, akkor T-nek a p darab különböző elforgatottja is, és ezzel látható, hogy minden csoportban p-vel osztható számú színezés van. Azaz $p \mid a^p - a$.

1.2. Wilson tétel geometriai bizonyítása

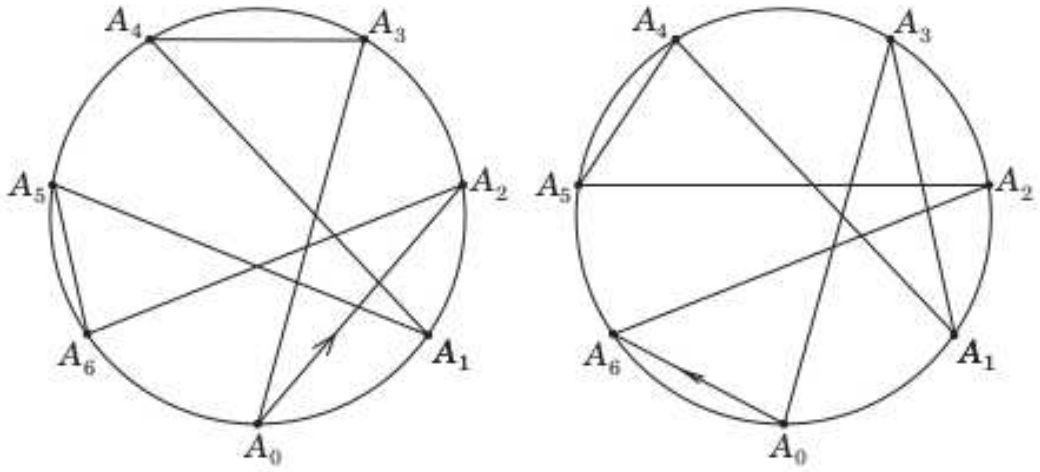
A Wilson tétel [8] bizonyításához sem szükséges a kongruenciák ismerete. A most következő bizonyítás Erdős-Surányi könyvéből [4] való, és az ábránkat is onnan vettük.

Wilson tétele a következőképpen szól:

1.2. TÉTEL. *Ha p prím, akkor $p \mid (p-1)! + 1$.*

Az 1.2. Tétel bizonyítása. Ez $p = 2$-re teljesül hiszen $2 \mid 1! + 1$, így a továbbiakban elég páratlan prímekre belátni az állítást. Ehhez permutációkat veszünk. Az $1, 2, \ldots, p-1$ számok permutációinak (lehetséges elrendezéseinek egy sorozatba) a száma $(p-1)!$. Minden ilyen permutációhoz hozzárendelünk egy körbe írt, irányított, zárt töröttvonalat.

Legyen $A_0, A_1, \ldots, A_{p-1}$ egy körbe írt szabályos p-szög csúcsai. Egy $j_1 j_2 \ldots j_{p-1}$ permutációhoz hozzárendeljük az A_0-ból sorra az A_{j_1}-be, A_{j_2}-be, ..., $A_{j_{p-1}}$-be menő, majd A_0-ba visszatérő zárt töröttvonalat. (Az alábbi ábra első körén $p = 7$ és a 265143 permutációt ábrázoló töröttvonal látható.)



Tekintsünk egy adott T_0 töröttvonalat, és azt ismételten elforgatjuk a kör középpontja körül $(360/p)°$-kal, így keletkezik a töröttvonalaknak egy $T_0, T_1, \ldots, T_n, \ldots$ sorozata. (Az első ábrán lévő töröttvonalat pl. az első elforgatás a második ábrába viszi át.)

Ekkor $T_p = T_0$, de a $T_0, T_1, \ldots, T_{p-1}$ töröttvonalak között is lehetnek megegyezők. Az első megegyezés nyilván $T_0 = T_k$ alakú, hiszen ha $T_i = T_k$, ahol $i \geq 1$, akkor $T_0 = T_{k-i}$ is teljesül.

Ha k jelöli a legkisebb pozitív egészet, amelyre $T_0 = T_k$, akkor a $T_0, T_1, T_2, \ldots$ sorozat k-val periodikus, és k a legkisebb periódushossz Mivel $T_0 = T_p$ ezért $k \mid p$. Vagyis k csak 1 vagy p lehet.

A töröttvonalakat csoportokba osztjuk. Egy T_0 töröttvonal csoportja a hozzárendelt $T_0, T_1, \ldots, T_{k-1}$ töröttvonalakból áll, ahol $T_0 = T_k$. Mivel itt k csak 1 vagy p lehet, így vannak csoportok, amelyek egyetlen töröttvonalból állnak, a többiek p eleműek.

Azokat a töröttvonalakat, amelyeket már az első elfordítás önmagába viszi át, úgy kaphatjuk meg, hogy húzunk A_0-ból egy szakaszt valamelyik A_k-ba, és ezt körbe forgatjuk. Így mindig egy p szögpontú zárt töröttvonalat kapunk.

Az egy darab töröttvonalból álló osztályok száma tehát pontosan annyi, ahányféleképpen az A_0-ból induló oldal választható, azaz $p-1$. A többi $(p-1)!-(p-1) = (p-1)!+1-p$ töröttvonalat p elemű osztályokba tudtuk sorolni, így azt kapjuk, hogy $p \mid (p-1)!+1-p$. Azaz $p \mid (p-1)!+1$, és ez éppen a bizonyítandó állítás.

Feladatok

1. Találjunk minél több prímet, amelyre $p^2 \mid (p-1)!+1$.
2. Találjuk meg az összes p prímet és α természetes számot, amelyre $(p-1)!+1 = p^\alpha$ (Liouville tétele).

1.3. Behrend konstrukciója

Ebben a fejezetben megadunk egy viszonylag nagy részhalmazát $\{1, 2, 3, \ldots, N\}$-nek, mely nem tartalmaz 3-tagú számtani sorozatot.

A következő tétel Behrend [1] konstrukciója lesz, amelynek alapja egy szórakoztató geometriai konstrukció. Az ismertetés során a [5] cikk terminológiáját használjuk.

1.3. TÉTEL. (Behrend, 1946.) *Létezik egy pozitív konstans c, hogy minden N-re meg tudunk adni egy*

$$\mathcal{A} \subset \{1, 2, 3, \ldots, N\}$$

halmazt, melyre

$$|\mathcal{A}| \geq N \exp(-c\sqrt{\log N})$$

és $\mathcal{A}$ nem tartalmaz 3-tagú számtani sorozatot.

A 1.3. Tétel bizonyítása. Behrend konstrukciója azon az észrevételen alapul, hogy egy egyenes egy gömböt legfeljebb 2 pontban metsz.

Ha $\mathrm{x}, \mathrm{y}, \mathrm{z}$ egy 3-tagú számtani sorozat, akkor $\mathrm{y} = \frac{\mathrm{x}+\mathrm{z}}{2}$.

Először megadunk egy n dimenziós konstrukciót, egy gömbhéjat, mely gömbhéj semely két pontjának nem tartalmazza az átlagát, mivel egy egyenes maximum két pontban metsz egy gömbhéjat.

Ezután a gömbhéj egész pontjaihoz hozzárendelünk egy $\mathcal{A} \subseteq \{1, 2, 3, \ldots, N\}$ halmazt.

Az n és M pozitív egészek értékét később rögzítjük.

Tekintsük az $\mathbf{x} = (x_1, x_2, ..., x_n) \in [1, M]^n$ halmazt. A fenti M^n darab pont mindegyikéhez hozzárendeljük az origótól vett távolság négyzetét, azaz az $r^2 = x_1^2 + ... + x_n^2$ egész számot.

Ezek a hozzárendelt értékek az $[n, nM^2]$ intervallumból valóak. Vagyis létezik egy r sugár, amelyre $S_n(r)$ gömbhéj legalább

$$|S_n(r)| \geq \frac{M^n}{nM^2 - n + 1} \geq \frac{M^n}{nM^2} \geq \frac{M^{n-2}}{n}$$

darab egész pontot tartalmaz.

Ezek után az $S_n(r)$ egész pontjaihoz egy egész számot rendelünk a következő $P : \mathbb{Z}^n \to \mathbb{Z}$ függvénnyel:

$$P(\mathbf{x}) \stackrel{\text{def}}{=} \frac{1}{2M} \sum_{i=1}^{n} x_i (2M)^i.$$

A P függvény alap tulajdonságai a következők:

1. P egész értékű.
2. $1 \leq P(\mathbf{x}) \leq (2M)^n$ minden $\mathbf{x} \in [1, M]^n$-re.
3. P lineáris.
4. P injektív $[1, M]^n$-en.
5. $P(\mathbf{z}) - P(\mathbf{y}) = P(\mathbf{y}) - P(\mathbf{x}) \Rightarrow \mathbf{z} - \mathbf{y} = \mathbf{y} - \mathbf{x}$ minden $\mathbf{x}, \mathbf{y}, \mathbf{z} \in [1, M]^n$ esetén.

Az 1. tulajdonság nyilvánvaló, hiszen a szummában minden tag osztható $2M$-mel.

A 2. tulajdonság is igaz, hiszen $P(\mathbf{x})$ pozitív és a függvény a maximumát akkor éri el, ha minden x_i maximális, azaz pont M. Ekkor

$$P(\mathbf{x}) \leq P(M, M, \ldots, M) = \frac{1}{2M} \sum_{i=1}^{n} M(2M)^i$$
$$= M\frac{(2M)^n - 1}{2M - 1} \leq M\frac{(2M)^n}{2M} < (2M)^n.$$

A 3. tulajdonság szintén nyilvánvaló, legyen ugyanis $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$ és $a, b \in \mathbb{Z}$. Ekkor P definíciójából könnyen látható, hogy

$$P(a\mathbf{x} + b\mathbf{y}) = aP(\mathbf{x}) + bP(\mathbf{y}).$$

A 4. és 5. tulajdonságok igazolásához a következő lemmára van szükségünk:

1.4. LEMMA. *Legyen $\mathbf{x} \in (-2M, 2M)^n$. Ekkor $P(\mathbf{x}) = 0$ akkor és csak akkor, ha $\mathbf{x} = 0$.*

A 1.4. Lemma bizonyítása. Ha $\mathbf{x} = 0$, akkor $P(\mathbf{x}) = 0$.

Megfordítva, tegyük fel, hogy létezik egy $\mathbf{x} \neq 0$, amelyre $P(\mathbf{x}) = 0$. Ekkor vegyük az $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ vektor koordinátái közül a legkisebb indexűt, amely nem 0, legyen ez x_j. Ekkor

$$P(\mathbf{x}) = \frac{1}{2M} \sum_{i=j}^{n} x_i(2M)^i = 0.$$

Rendezve, azt kapjuk, hogy

$$-x_j = \sum_{i=j+1}^{n} x_i(2M)^{j-i},$$

ahol a jobboldal osztható $2M$-mel, míg a baloldalon $1 \leq x_j < 2M$, ami ellentmondás. Ezzel a lemma bizonyítását befejeztük.

A lemmát használva, bebizonyítjuk a 4. és 5. tulajdonságot.

A 4. tulajdonsághoz tegyük fel, hogy $\boldsymbol{P(\mathbf{x}) = P(\mathbf{y})}$ fennáll egy $\mathbf{x}, \mathbf{y} \in [1, M]^n$ párra.

A linearitás alapján $\mathbf{0 = P(\mathbf{x}) - P(\mathbf{y}) = P(\mathbf{x} - \mathbf{y})}$, de $\mathbf{x - y} \in (-M, M)^n \subset (-2M, 2M)^n$, így a lemma alapján $\mathbf{x - y = 0}$, azaz $\mathbf{x = y}$. Eredményképpen megkaptuk, hogy $\boldsymbol{P}$ injektív.

Utoljára már csak az 5. tulajdonságot kell igazolnunk.

Tegyük fel, hogy $\boldsymbol{P(\mathbf{z}) - P(\mathbf{y}) = P(\mathbf{y}) - P(\mathbf{x})}$ eleget tesz egy $\mathbf{x}, \mathbf{y}, \mathbf{z} \in [1, M]^n$ számhármasra. Ekkor $\boldsymbol{P(\mathbf{z}) - 2P(\mathbf{y}) + P(\mathbf{x}) = P(\mathbf{z} - 2\mathbf{y} + \mathbf{x}) = 0}$. Azonban most $\mathbf{z - 2y + x} \in (-2M, 2M)^n$, így alkalmazhatjuk megint a lemmát, mely szerint $\mathbf{z - 2y + x = 0}$, azaz $\mathbf{z - y = y - x}$. Ezzel a lemma állítását igazoltuk.

Ezután rögzítjük n és M értékét. Legyen $n = \lceil \sqrt{\log N} \rceil$, $M = [N^{1/n}/2]$.

Ekkor $\mathcal{A} \subset [1, (2M)^n] \subset [1, N]$.

A $\boldsymbol{P}$ függvény 5. tulajdonsága miatt tudjuk, hogy $\mathcal{A}$ nem tartalmaz 3-tagú számtani sorozatot.

Most már csak $\mathcal{A}$ elemszámát kell becsülnünk.

$$|\mathcal{A}| \geq \frac{M^{n-2}}{n} = \frac{[N^{1/n}/2]^{n-2}}{n} \geq \frac{\left(N^{1/n}/e\right)^{n-2}}{n} = e^{2-n} N^{1-2/n} \cdot \frac{1}{n}$$
$$= N e^{2-\lceil \sqrt{\log N} \rceil} \cdot N^{-2/\lceil \sqrt{\log N} \rceil} \cdot \frac{1}{\lceil \sqrt{\log N} \rceil}$$

$$\geq Ne^{2-\left(\sqrt{\log N}+1\right)} \cdot N^{-2/\sqrt{\log N}} \cdot \frac{1}{\sqrt{\log N}+1}$$
$$\geq Ne^{1-\left(\sqrt{\log N}\right)} \cdot e^{-2\log N/\sqrt{\log N}} \cdot e^{-\sqrt{\log N}}$$
$$> Ne^{-4\sqrt{\log N}}.$$

A másik oldalról, Roth [7] 1953-ban azt bizonyította, hogy ha $A \subseteq \{1, 2, 3, \ldots, N\}$ nem tartalmaz 3-tagú számtani sorozatot, akkor $|\mathcal{A}| \ll \frac{N}{\log\log N}$. Azóta ezt az eredményt folyamatosan javítgatták. A legjobb mostani eredmény Bloom és Sisasktól [2] származik, akik bebizonyították, hogy létezik olyan $c > 0$ konstans, amelyre $|\mathcal{A}| \ll \frac{N}{(\log N)^{1+c}}$.

A legjobb alsó becslés is Bloom és Sisasktól [3] származik (akik valójában Kelley és Meka [6] eredményét egyszerűsítették). Eszerint létezik olyan 3-tagú számtani sorozat mentes halmaz, amelynek elemszáma $\geq \exp(-c(\log N)^{1/11})N$.

Az Erdős-Surányi könyvben [4] sok más mellett a geometriai számelméletről is olvashatunk egy nagyon érdekes fejezetet.

Hivatkozások

[1] F. A. Behrend, *On the sets of integers which contain no three in arithmetic progression*, Proceedings of the National Academy of Sciences 23 (1946), 331-332.

[2] T. F. Bloom, O. Sisask, *Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions*, link.

[3] T. F. Bloom, O. Sisask, *The Kelley–Meka bounds for sets free of three-term arithmetic progressions*, link.

[4] Erdős Pál, Surányi János, *Válogatott Fejezetek a Számelméletből*, 127-128. oldal, link.

[5] B. Gillespie, *Behrend's Construction*, link.

[6] Z. Kelley, R. Meka, *Strong Bounds for 3-Progressions*, link.

[7] K. Roth, *On certain sets of integers*. Journal of the London Mathematical Society. 28 (1) (1953), 104–109.

[8] E. Waring, *Meditationes Algebraicae* (Cambridge, Anglia: 1770) (latinul). Waring, Meditationes című munkájának harmadik kiadásában Wilson tétele az 5. probléma a 380. oldalon. Waring a következőt írja: "Hanc maxime elegantem primorum numerorum proprietatem invenit vir clarissimus, rerumque mathematicarum peritissimus Joannes Wilson Armiger." (Egy ember, aki a legkiválóbb és legügyesebb a matematikában, John Wilson Squire találta meg a prímszámok legelegánsabb tulajdonságát.)

[9] Wikipédia, *A kis Fermat-tétel bizonyításai*, link

[10] Ábra, Basketball Clip Art, link.

[11] Ábra, Brent, *Nyakláncok*, link

[12] Ábra, Erdős Pál, Surányi János, *Válogatott Fejezetek a Számelméletből*, 127. oldal, link.

2. Végtelen leszállás módszere

„Mivel a közönséges módszerek, mint amilyenek a könyvekben találhatók, nem alkalmasak ilyen nehéz állítások bizonyítására, végre felfedeztem egy rendkívül egyedi módszert..., amit végtelen leszámlálásnak neveztem el.”

Fermat, 1659.

A módszer: Ahhoz, hogy bebizonyítsuk, hogy egy egyenletnek nincs egészekből álló megoldása, bebizonyítjuk, hogy egy megoldás kikényszerítene egy „kisebb” megoldás létezését, ezzel előállítva pozitív egész a_i-knak egy

$$a_1 > a_2 > a_3 > \cdots > 0$$

végtelen sorozatát, amely nyilván nem lehetséges.

A módszert használják irracionalitás bizonyításához, diofantikus egyenletek megoldásához, de pl. Fermat ezzel bizonyította be, hogy minden $4k + 1$ alakú prím előáll két négyzetszám összegeként.

A következőkben bebizonyítjuk a végtelen leszállás módszerével, hogy a $\sqrt{2}$ irracionális.

Tegyük fel, hogy $\sqrt{2}$ racionális. Mivel $1 < \sqrt{2} < 2$, így $\sqrt{2}$ felírható

$$\sqrt{2} = 1 + \frac{a}{b}$$

alakban, ahol $0 < \frac{a}{b} < 1$. Emeljük mindkét oldalt négyzetre, és utána szorozzunk b^2-tel:

$$2b^2 = b^2 + 2ab + a^2.$$

Átrendezve:

$$a^2 = b^2 - 2ab = (b - 2a)b,$$

így

$$\frac{a}{b} = \frac{b - 2a}{a}.$$

Most:

$$\sqrt{2} = 1 + \frac{a}{b} = 1 + \frac{b - 2a}{a}.$$

De az utóbbi tört nevezőjében $0 < a < b$. Így a végtelen leszállás módszerét alkalmazva, egyre kisebb nevezőjű törteket kapunk, ami ellentmondás.

Feladatok

1. Bizonyítsa be, hogy ha az x, y, z egészekre $x^3 + 3y^3 + 9z^3 = 9xyz$, akkor $x = y = z = 0$. (Kürschák József Matematika Tanulóverseny, 1983.)

2. Találjuk meg az összes p prímet, amelyre $p^n = x^3 + y^3$ alakú, ahol x, y, n pozitív egészek. (Magyar MO 2000.)

3. Legyen $a_1, a_2, \ldots a_{2n+1}$ olyan $2n+1$ darab egész szám, hogy bármelyik elemet elhagyva közülük, a maradék $2n$ darab elemet két n elemű csoportra osztható úgy, hogy bennük az ele-

mek összege azonos. Bizonyítsa be, hogy $a_1 = a_2 = \cdots = a_{2n+1}$. (Putnam vizsga, 1973.)

4. Bizonyítsa be, hogyha az a és b pozitív egészekre $ab+1$ osztója a^2+b^2-nek, akkor $\frac{a^2+b^2}{ab+1}$ négyzetszám. (IMO 1988.)

Hivatkozások

[1] Keith Conrad, *Infinite Descent*, 2008, link.

[2] Kép, Pierre de Fermat, link

3. Polinomok számelmélete

Kriptográfiában (azaz különböző titkosítások során) különösen fontos szerepet töltenek be a prímek (ld. pl. RSA), de vannak olyan alkalmazások is, amikor egész számok helyett polinomokat használunk. Ezek között kiemelt szerepet kapnak a prímek általánosításai, az ún. irreducibilis polinomok.

Most csak egyet kiemelve a sok alkalmazás közül: létezik pl. az RSA-nak egy polinomokra való általánosításáról egy nagyon érdekes BSc szakdolgozat is 2015-ből [4].

3.1. Definíció. *Azt mondjuk egy $f(x) \in \mathbb{Z}[x]$ polinom irreducibilis, ha nem konstans és nem írható fel két legalább elsőfokú $\mathbb{Z}[x]$-beli polinom szorzataként.*

A leghíresebb az irreducibilitási kritériumok közül a Schönemann-Eisenstein-féle irreducibilitási kritérium.

3.2. Tétel. *Legyen $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ egy olyan egész együtthatós polinom, amelyre $p \nmid a_n$, de p osztja a többi együtthatót: $p \mid a_{n-1}, a_{n-2}, \ldots, a_1, a_0$, viszont $p^2 \nmid a_0$, akkor f irreducibilis.*

A 3.2. Tétel bizonyítása. A tételben szereplő f polinomunk

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

alakú. Indirekten bizonyítunk, feltesszük, hogy f felírható két legalább elsőfokú polinom szorzataként, azaz

$$f(x) = g(x)h(x),$$

ahol

$$g(x) = b_r x^r + b_{r-1} x^{r-1} + \cdots + b_1 x + b_0$$

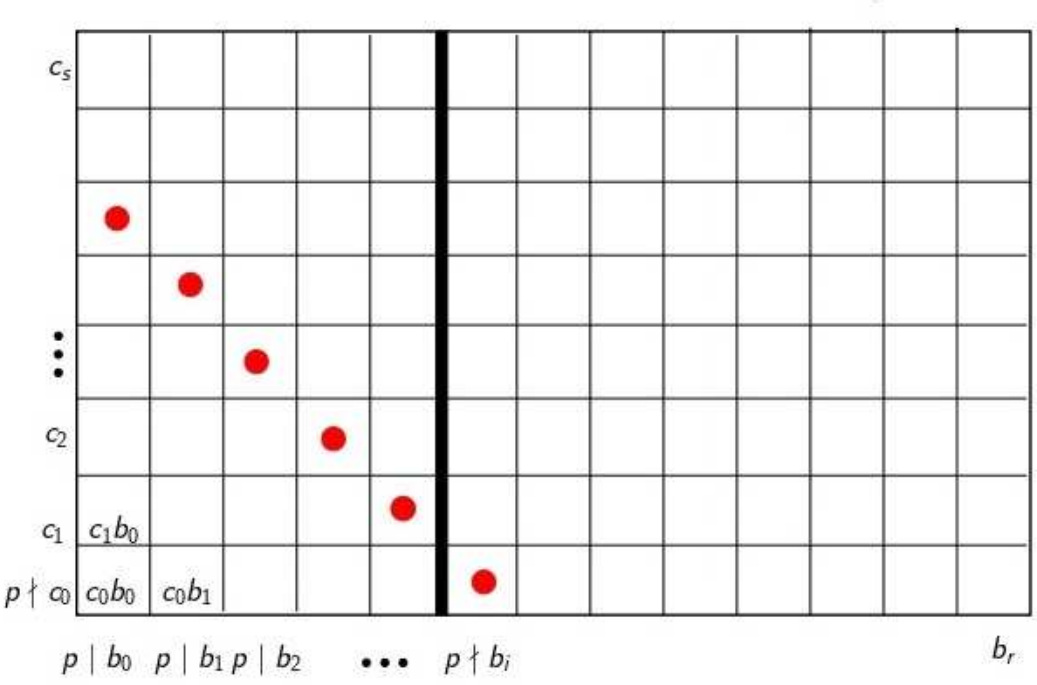
és

$$h(x) = c_s x^s + c_{s-1} x^{s-1} + \cdots + c_1 x + c_0,$$

valamint $r, s \geq 1$.

Tekintsünk egy $(r+1) \times (s+1)$-es téglalapot, amelynek az oldalaira rendre felírjuk a g és h együtthatóit a konstans tagoktól kezdve.

Az f polinom konstans tagja p-vel osztható, azaz $p \mid a_0 = b_0 c_0$. Tehát p osztója b_0-nak vagy c_0-nak. Szimmetrikus okokból feltehető $p \mid b_0$. De $p^2 \nmid a_0 = b_0 c_0$, azaz ekkor $p \nmid c_0$.



Jelölje b_i a legkisebb indexű együtthatóját $g(x)$-nek, amelyre $p \nmid b_i$. (Az nem lehet, hogy p mindegyik b_i-t osztja, mert akkor $f(x)$-ben is minden együttható osztható p-vel.)

Tehát $p \mid b_0, b_1, b_2, \ldots, b_{i-1}$. Ezután a nagy téglalapban lévő egységnégyzetekbe beírjuk az f és g megfelelő együtthatóinak a szorzatát (lásd ábra). Ekkor az f polinom a_i együtthatóját az ábrán piros pöttyökkel jelölt egységnégyzetekben lévő szorzatok összege adja meg:

$$a_i = b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c_1 + b_ic_0.$$

Azonban $p \mid b_0, b_1, \ldots, b_{i-1}$, tehát $p \mid b_0c_i, b_1c_{i-1}, \ldots, b_{i-1}c_1$ (a vastag vonaltól balra minden szorzat osztható p-vel). Viszont $p \nmid b_i$ és $p \nmid c_0$, azaz $p \nmid b_ic_0$. Vagyis:

$$p \nmid a_i = b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c_1 + b_ic_0.$$

Azonban a_i nem a főegyüttható a_n, hiszen $a_n = b_rc_s$, ahol $s \geq 1$. Ez ellentmond a tétel feltételeinek, és ezzel a tétel állítását beláttuk.

Példa. $x^4 + 3x^3 + 6x^2 + 9x + 21$ irreducibilis $\mathbb{Z}[x]$-ben. Valóban: $3 \nmid 1$, de $3 \mid 3, 6, 9, 21$ és $9 \nmid 21$.

Első ránézésre nem látszik, de a következő is igaz:

3.3. KÖVETKEZMÉNY. *Ha p prím, akkor az*

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

polinom irreducibilis $\mathbb{Z}[x]$-ben.

A 3.3. Következmény bizonyítása. Az $f(x)$ polinom pontosan akkor irreducibilis, amikor az $f(x+1)$. De:

$$
\begin{aligned}
f(x+1) &= (x+1)^{p-1} + (x+1)^{p-2} + \cdots + 1 \\
&= \sum_{i=0}^{p-1} \left(\binom{p-1}{i} + \binom{p-2}{i-1} + \cdots + \binom{p-1-i}{0} \right) x^{p-1-i} \\
&= \sum_{i=0}^{p-1} \binom{p}{i} x^{p-1-i}.
\end{aligned}
$$

Itt $p \nmid \binom{p}{0} = 1$, de $p \mid \binom{p}{i}$ ha $1 \leq i \leq p-1$, és végül $p^2 \nmid \binom{p}{p-1} = p$.

Azaz $f(x+1)$, és így $f(x)$ is irreducibilis.

Az $x^{p-1} + x^{p-2} + \cdots + x + 1$ a p-edik körosztási polinom. A körosztási polinomok mindig irreducibilisek, erről bővebben pl. [5]-ben vagy [6]-ban olvashatunk.

Mi azonban térjünk vissza az irreducibilitási kritériumokhoz. Vajon vannak-e a Schönemann-Eisenstein-en túl más irreducibilitási kritériumok? Igen, szerencsénkre léteznek ilyenek. Csak néhányat említve a leghíresebbek közül: Perron [10], Cohn [1], [12].

Most csak néhány kevésbé ismert irreducibilitási kritériumot bizonyítunk, amelyek fő előnye egyszerűségükben rejlik (sőt mi több, még a bizonyítások is egyszerűek).

Schur kérdezte a következőt: Ha az $a_1, a_2, \ldots, a_n$ különböző egész számok, akkor Vajon az

$$f_1(x) = (x - a_1)(x - a_2) \cdots (x - a_n) - 1$$

és

$$f_2(x) = (x - a_1)(x - a_2) \cdots (x - a_n) + 1$$

polinomok irreducibilisek-e? (ld. [11]). Westlund [13] bebizonyította, hogy f_1 mindig irreducibilis, míg f_2 csak akkor lehet reducibilis, ha

teljes négyzet. Még ugyanabban az évben Flügel [3] meghatározta az összes ilyen f_2 polinomot.

Ezek közül az utóbbit feladatnak szánjuk az olvasóknak. Sőt, van itt még egy feladat Sklarszkij, Csencov, Jaglom [2, o. 48] feladatgyűjteményéből:

3.4. Feladat. *Mely egymástól különböző egész $a_1, a_2, \ldots, a_n$ számok esetén lesz irreducibilis az*

$$(x - a_1)(x - a_2) \cdots (x - a_n) + 1$$

polinom?

3.5. Feladat. *Mely egymástól különböző egész $a_1, a_2, \ldots, a_n$ számok esetén lesz irreducibilis az*

$$(x - a_1)^2(x - a_2)^2 \cdots (x - a_n)^2 + 1$$

polinom?

Most pedig bebizonyítjuk a következőt

3.6. Tétel. (Westlund) *Ha az $a_1, a_2, \ldots, a_n$ különböző egész számok, akkor az*

$$f_1(x) = (x - a_1)(x - a_2) \cdots (x - a_n) - 1$$

polinom irreducibilis.

A 3.6. Tétel bizonyítása. Tegyük fel, hogy f reducibilis, azaz léteznek olyan legalább elsőfokú $g(x)$ és $h(x) \in \mathbb{Z}[x]$ polinomok, amelyekre

$$f(x) = g(x)h(x).$$

Ekkor az a_i helyen

$$-1 = f(a_i) = g(a_i)h(a_i).$$

Ez csak úgy lehet, ha $g(a_i) = 1$, $h(a_i) = -1$ vagy $g(a_i) = -1$, $h(a_i) = 1$. Mindkét esetben

$$g(a_i) + h(a_i) = 0,$$

azaz a $g(x) + h(x)$ polinomnak van n darab gyöke: $a_1, a_2, \ldots, a_n$. De $g(x) + h(x)$ foka kisebb egyenlő mint $g(x)$ és $h(x)$ fokának a maximuma, ami kisebb mint $f(x)$ foka n.

Azaz a fokszám tétel miatt $g(x) + h(x)$-nek kevesebb mint n gyöke van, ami ellentmondás, kivéve, ha $g(x) + h(x)$ az azonosan nulla polinom. Vagyis most $g(x) = -h(x)$. Ekkor

$$(x - a_1)(x - a_2)\cdots(x - a_n) - 1 = -g(x)^2,$$

ami ellentmondás, hiszen a jobboldalon a főegyüttható negatív szám, míg a baloldalon 1.

Az eddigi irreducibilitási kritériumokban az együtthatók valamilyen értelemben az oszthatósághoz kapcsolódtak, de néha olyan kritériumra is szükség lehet, amelyben a főszerepet nagyságrendbeli becslések adják. Egy ilyen kritérium Perron [10] kritériuma:

3.7. TÉTEL. *Legyen $f(x) \in \mathbb{Z}[x]$ egy*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$

polinom, ahol $a_0 \neq 0$. Tegyük fel, hogy a következő két feltétel közül valamelyik fennáll:

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_0|$$

vagy

$$|a_{n-1}| = 1 + |a_{n-2}| + \cdots + |a_0|, \quad f(\pm 1) \neq 0.$$

Ekkor $f(x)$ irreducibilis.

Ennek a tételnek a bizonyítását Panitopol [8] kicsit leegyszerűsítette, de az érdeklődők utána nézhetnek pl. a kapcsolódó Wikipédia oldalon [14]-ben vagy [15]-ban is.

Következőleg egy hasonló jellegű tétel igazolunk mint Perron kritériuma, ugyanakkor a bizonyítása kicsit egyszerűbb annál. A tétel Panitopol és Stephănescu [9] eredménye.

3.8. TÉTEL. *Legyen $f(x) \in \mathbb{Z}[x]$ egy*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

polinom, ahol

$$|a_0| > |a_1| + |a_2| + \cdots + |a_{n-1}| + |a_n|.$$

Tegyük fel, hogy a_0 prím vagy $\sqrt{|a_0|} - \sqrt{|a_n|} < 1$ (elég ha a két feltétel közül az egyik fennáll). Ekkor $f(x)$ irreducibilis.

Példák.

a) Ha p prím, akkor az $x^n + x^m + p$ polinom irreducibilis.

b) Tetszőleges a egész számra az $ax^n + x^m + a + 2$ polinom irreducibilis.

A 3.8. Tétel bizonyítása. Legyen $\alpha_1, \alpha_2, \ldots, \alpha_n$ az $f(x)$ polinom gyökei. Ekkor

$$|\alpha_i| > 1.$$

Valóban, tegyük fel, hogy az állítással ellentétben valamelyik i-re $|\alpha_i| \leq 1$. Ekkor:

$$a_0 = -(a_n\alpha_i^n + a_{n-1}\alpha_i^{n-1} + \cdots + a_1\alpha_i).$$

A háromszög-egyenlőtlenség szerint

$$\begin{aligned} |a_0| &\leq \left|a_n\alpha_i^n\right| + \left|a_{n-1}\alpha_i^{n-1}\right| + \cdots + |a_1\alpha_i| \\ &= |a_n|\,|\alpha_i|^n + |a_{n-1}|\left|{\alpha_i}^{n-1}\right| + \cdots + |a_1|\,|\alpha_i| \\ &\leq |a_{n-1}| + |a_{n-2}| + \cdots + |a_1| < |a_0|, \end{aligned}$$

ami ellentmondás.

Tegyük fel, hogy létezik $g(x)$ és $h(x)$ polinom, amelyre

$$f(x) = g(x)h(x),$$

ahol $\deg g, \deg h \geq 1$. Legyen

$$g(x) = b_r x^r + b_{r-1}x^{r-1} + \cdots + b_1 x + b_0$$

és

$$h(x) = c_s x^s + c_{s-1}x^{s-1} + \cdots + c_1 x + c_0,$$

Először azt tesszük fel, hogy a_0 prím. Ekkor $a_0 = b_0c_0$. Igen ám, de a_0 prím, tehát b_0 és c_0 valamelyike ± 1. Mondjuk $b_0 = \pm 1$. A $g(x)$ polinom gyökei részhalmazát alkotják az $f(x)$ polinom gyökeinek, tehát a gyökök az α_i-k közül kerülnek ki, mondjuk $g(x)$ gyökei $\alpha_1, \alpha_2, \ldots, \alpha_r$.

A gyökök és együtthatók közötti összefüggés szerint

$$|b_0| = |b_r|\,|\alpha_1| \cdot |\alpha_2| \cdots |\alpha_r|\,, \tag{3.1}$$

de minden i-re $|\alpha_i| > 1$, a főegyütthatóra pedig nyilván $|b_r| \geq 1$, azaz $|b_0| > 1$, ami ellentmondás.

Ezután tegyük fel, hogy $\sqrt{|a_0|} - \sqrt{|a_n|} < 1$. Akárcsak az előző esetben, most is használhatjuk az eddig bevezetett jelöléseket. Ekkor (3.1)-ből adódóan

$$|b_0| > |b_r| .$$

Tehát

$$|b_0| \geq |b_r| + 1.$$

Hasonlóan

$$|c_0| \geq |c_s| + 1.$$

Azaz

$$\begin{aligned} |a_0| &= |b_0| \cdot |c_0| \\ &\geq (|b_r| + 1) \cdot (|c_s| + 1) \\ &= |b_r| \cdot |c_s| + |b_r| + |c_s| + 1 \\ &\geq |b_r| \cdot |c_s| + 2\sqrt{|b_r| \cdot |c_s|} + 1 \\ &= |a_n| + 2\sqrt{|a_n|} + 1 \\ &= \left(\sqrt{|a_n|} + 1\right)^2 . \end{aligned}$$

Így

$$\sqrt{|a_0|} \geq \sqrt{|a_n|} + 1,$$

ami ellentmond a feltételezésünknek. Ezzel a tételt beláttuk.

Az érdekesség kedvéért leírjuk Cohn kritériumát is (ld. [1], [12]).

3.9. TÉTEL. *A p prímet írjuk fel tízes számrendszerben:*

$$p = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0.$$

Ekkor az

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

polinom irreducibilis.

A tétel tízes helyett tetszőleges számrendszerben is igaz ld. [1].

Természetesen a polinomok kapcsán egyéb kérdéseket is felvethetünk, nem csak irreducibilitással kapcsolatosokat. Itt van mindjárt egy az algebrában már járatos olvasóknak szánt feladat, amely Pólyától és Szegőtől [12, o. 132] származik.

3.10. FELADAT. *Ha egy $f(x) \in \mathbb{Z}[x]$ polinom csak négyzetszámokat vesz fel, akkor vajon mindig igaz-e, hogy $f(x) = g^2(x)$ alakú, ahol $g(x) \in \mathbb{Z}[x]$?*

Van a feladatra (viszonylag elemi) algebrai megoldás is, de ha gyors megoldást szeretnének találni, akkor javaslom az exponenciális és karakter összegek tanulmányozását, amely tárgyként az ELTE MSc matematikus szakán is felvehető.

Ezt a kérdést többváltozós polinomokra Murty [7] általánosította.

Hivatkozások

[1] J. Brillhart, M. Filaseta, A. Odlyzko, *On an irreducibility theorem of A. Cohn*, Canadian Journal of Mathematics. 33 (5) (1981), 1055–1059.

[2] D. O. Skljarszkij, Ny. Ny. Csencov, I. M. Jaglom, *Válogatott feladatok és tételek az elemi matematika köréből 1, Aritmetika és algebra*, Typotex (2009), 2. kiadás, link.

[3] W. Flügel, *Solution to problem 226*, Archiv. der Math. und Physic 15 (3), (1909), o. 271.

[4] I. B. Gafitoui, *Polynomial based RSA*, BSc Thesis, Linnæus Egyetem, Svédország, link.

[5] Kiss E., *Bevezetés az Algebrába*.

[6] Laczkovich M. *A körosztási polinomokról*, Új matematikai mozaik, Typotex, Budapest, 2002, 243-250.

[7] M. Ram Murty, *Polynomials assuming square values*, Balasubramanian, R. (szerk.) et al., Number theory and discrete geometry, Proceedings of the international conference in honour of Prof. R. P. Bambah, Chandigarh, India, 2005, Ramanujan Mathematical Society Lecture Notes Series 6 (2008), 155-163, link.

[8] L. Panitopol, *Criteriul lui Perron de ireductibilitate a polinoamelor cu coeficienti intregi*, Gazeta Matematică 98 (10), 39–340

[9] L. Panitopol, D. Stefănescu, *Some criteria for irreducibility of polynomials*, Bull. Math. de la Soc. Sci. Math. de la R. S. de Roumanie, Nouvelle Série, 29 (77) no. 1 (1985), 69-74.

[10] O. Perron, *Neue kriterien für die irreduzibilität algebraischer gleichungen*, Journal für die Mathematik. Walter de Gruyter. 132 (197), 288–307.

[11] G. Pólya, *Verschiedene Bemerkungen zur Zahlentheorie*, Jahresbericht der Deutschen Mathematiker-Vereinigung (németül) 28 (1919), 31–40.

[12] G. Pólya, G. Szegő, *Aufgaben und Lehrsätze aus der Analysis*, Bd 2. Springer, Berlin. (1925), angol fordítás: Problems and theorems in analysis, Springer 2004, 2. kötet, o. 137.

[13] J. Westlund, *On the irreducibility of certain polynomials*, The American Mathematical Monthly, (16:4) (1909), 66-67.

[14] Wikipédia, *Perron's irreducibility criteria*, link

[15] Y. Zhao, *Integer Polynomials* (2007), link.

4. Amikor halmazokat adunk össze...

4.1. Cauchy-Davenport tétel

Az első ismert eredmény az additív csoportelméletből a híres Cauchy-Davenport tétel, mely a fejeztünk témája lesz. Először egy új definíció következik. Az $\mathcal{A}$ és $\mathcal{B} \subseteq \mathbb{Z}_m$ halmazok összege az

$$\mathcal{A} + \mathcal{B} = \{a + b : \ a \in \mathcal{A}, \ b \in \mathcal{B}\}$$

halmaz, amely nem „multihalmaz”, azaz minden elem egyszer szerepel az összeghalmazban.

A következő tételt Cauchy [1] fedezte fel 1813-ban, majd Davenport [2] (nem ismerve Cauchy eredményét) újra felfedezte 1935-ben. (ld. még pl. [3]).

H. Davenport

A. Cauchy

A tétel alsó becslést ad $|\mathcal{A} + \mathcal{B}|$-re $|\mathcal{A}|$ és $|\mathcal{B}|$ függvényében, ha $\mathcal{A}$ és $\mathcal{B}$ a $\mathbb{Z}_p$ halmaznak nem üres részhalmazai, ahol p prím.

4.1. TÉTEL. (Cauchy–Davenport) *Legyen p prím és $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_p$ nem üres részhalmazok. Ekkor*

$$|\mathcal{A} + \mathcal{B}| \geq \min\{p, |\mathcal{A}| + |\mathcal{B}| - 1\}.$$

A 4.1. Tétel bizonyítása. A következő lemmát használjuk:

4.2. LEMMA. *Legyen* $\mathcal{A} \subseteq \mathbb{Z}_p$, $d \in \mathbb{Z}_p$, $d \neq 0$. *Ha*

$$\mathcal{A} + d \subseteq \mathcal{A},$$

akkor

$$\mathcal{A} = \mathbb{Z}_p.$$

A 4.2. Lemma bizonyítása. Ha $\mathcal{A} + d \subseteq \mathcal{A}$, akkor $a \in \mathcal{A} \Longrightarrow a + d \in \mathcal{A}$. Ezt az állítást többször alkalmazva kapjuk

$$a, a + d, a + 2d, \ldots, a + (p-1)d \in \mathcal{A}. \tag{4.1}$$

De $a, a + d, a + 2d, \ldots, a + (p-1)d$ egy teljes maradékrendszert alkot modulo p, mivel a fenti halmaznak p darab eleme van, és bármely két elem inkongruens modulo p. Valóban, ha

$$a + id \equiv a + jd \pmod{p}$$

egy $0 \leq i, j \leq p-1$ párra, akkor

$$\begin{aligned} id &\equiv jd \pmod{p} \quad / : d \\ i &\equiv j \pmod{p} \\ i &= j. \end{aligned}$$

Így (4.1) alapján

$$\mathbb{Z}_p \subseteq \mathcal{A}.$$

Mivel $\mathcal{A} \subseteq \mathbb{Z}_p$ szintén fennáll:

$$\mathcal{A} = \mathbb{Z}_p.$$

4.3. LEMMA. *Legyen* $\mathcal{A} \subseteq \mathbb{Z}_p$, $x, y \in \mathbb{Z}_p$, $x \neq y$. *Ekkor ha*

$$\mathcal{A} + x \subseteq \mathcal{A} + y,$$

akkor

$$\mathcal{A} = \mathbb{Z}_p.$$

A 4.3. Lemma bizonyítása. Ha $\mathcal{A} + x \subseteq \mathcal{A} + y$, akkor

$$\mathcal{A} + (x - y) \subseteq \mathcal{A}.$$

Legyen $x - y = d$, ekkor

$$\mathcal{A} + d \subseteq \mathcal{A}.$$

A 4.2. Lemma alapján $\mathcal{A} = \mathbb{Z}_p$.

Feladat

Bizonyítsuk be a Cauchy–Davenport tételt ha $|\mathcal{B}| = 1$ vagy $|\mathcal{B}| = 2$.

Megoldás

Legyen

$$\mathcal{A} = \{\alpha_1, \alpha_2, \ldots, \alpha_m\},$$
$$\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_n\}$$

Ha $n = 1$, akkor

$$|\mathcal{A} + \mathcal{B}| = |\mathcal{A} + \beta_1| = |\mathcal{A}| = m$$
$$= m + 1 - 1 = m + n - 1.$$

Így $n = 1$ esetén beláttuk a tétel állítását.

Következőleg azt az esetet tanulmányozzuk, amikor $n = 2$. Legyen $\mathcal{B} = \{\beta_1, \beta_2\}$ jelölje d a két elem különbségét, azaz $d = \beta_2 - \beta_1$.

$$\beta_1 \not\equiv \beta_2 \pmod{p} \implies (d, p) = 1.$$

Két esetet különböztetünk meg.

I. Eset: $\mathcal{A} + d \subseteq \mathcal{A}$.

Ekkor 4.2. Lemma alapján $\mathcal{A} = \mathbb{Z}_p$, így $\mathcal{A} + \mathcal{B} = \mathbb{Z}_p$, azaz

$$|\mathcal{A} + \mathcal{B}| = |Z_p| = p \geq \min\{p, |\mathcal{A}| + |\mathcal{B}| - 1\},$$

vagyis az I. Esetben fennáll a tétel állítása.

II. Eset: $\mathcal{A} + d \not\subseteq \mathcal{A}$.

Ekkor $\exists\, \alpha \in \mathcal{A}$, amelyre $\alpha + d \notin \mathcal{A}$.
Feltehetjük, hogy $\alpha = \alpha_1$. Így

$$\begin{aligned} \alpha_1 + d &\notin \mathcal{A}, \\ \alpha_1 + \beta_2 - \beta_1 &\notin \mathcal{A}, \\ \alpha_1 + \beta_2 - \beta_1 &\neq \alpha_i \text{ ahol } 1 \leq i \leq m, \\ \alpha_1 + \beta_2 &\neq \alpha_i + \beta_1 \text{ ahol } 1 \leq i \leq m, \end{aligned}$$

Ekkor:

$$\{\alpha_1 + \beta_2\} \cap \{\alpha_i + \beta_1,\ 1 \leq i \leq m\} = \emptyset,$$
$$|\mathcal{A} + \mathcal{B}| \geq 1 + m = m + 2 - 1 = m + n - 1.$$

Ezzel bebizonyítottuk a Cauchy-Davenport tételt $n = 1$-re és $n = 2$-re.

Amikor $|\mathcal{A}| = p$ vagy $|\mathcal{B}| = p$ (azaz $\mathcal{A} = \mathbb{Z}_p$ vagy $\mathcal{B} = \mathbb{Z}_p$), akkor a tétel triviális.

Ezután bebizonyítjuk a Cauchy-Davenport tételt teljes általánosságában n-re vonatkozó teljes indukcióval.

Az $n = 1$ és $n = 2$ esetben már láttuk a bizonyítást.

Az indukciós feltevés szerint, feltehetjük, hogy a tételt már bizonyítottuk minden olyan $\mathcal{A}'$ és $\mathcal{B}'$ halmazpárra, ahol

$$1 \leq |\mathcal{B}'| < n,$$

és ebből következőleg beszeretnék látni egy olyan $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_p$ halmazpárra, ahol $|\mathcal{B}| = n < p$ és $|\mathcal{A}| < p$. (Ez az indukciós lépés.)

Először tekintsük a következő speciális esetet:

I. Eset: Amikor $\mathcal{A} \cap \mathcal{B}$ nem üres, valódi részhalmaza $\mathcal{B}$-nek.

Legyen

$$\mathcal{A}' \stackrel{\text{def}}{=} \mathcal{A} \cup \mathcal{B},$$
$$\mathcal{B}' \stackrel{\text{def}}{=} \mathcal{A} \cap \mathcal{B}.$$

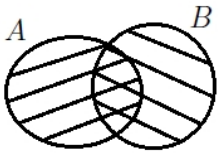
Ekkor $\mathcal{B}'$ valódi nem üres részhalmaza $\mathcal{B}$-nek, így

$$1 \leq |\mathcal{B}'| < |\mathcal{B}| = n.$$

Az indukciós feltevés szerint:

$$|\mathcal{A}' + \mathcal{B}'| \geq \min\{p, |\mathcal{A}'| + |\mathcal{B}'| - 1\}, \tag{4.2}$$

A következőt tetszőleges $\mathcal{A}$ és $\mathcal{B}$ halmazokra tudjuk:



$$|\mathcal{A}| + |\mathcal{B}| = |\mathcal{A} \cup \mathcal{B}| + |\mathcal{A} \cap \mathcal{B}| = |\mathcal{A}'| + |\mathcal{B}'|.$$

Másrészt, be fogjuk látni, hogy

$$\mathcal{A}' + \mathcal{B}' \subseteq \mathcal{A} + \mathcal{B}. \tag{4.3}$$

Valóban, tegyük fel, hogy $x \in \mathcal{A}' = \mathcal{A} \cup \mathcal{B}$ és $y \in \mathcal{B}' = \mathcal{A} \cap \mathcal{B}$. Bebizonyítjuk, hogy $x + y \in \mathcal{A} + \mathcal{B}$.

Ha $x \in \mathcal{A}$ akkor $y \in \mathcal{B}$ miatt $x + y \in \mathcal{A} + \mathcal{B}$. Ha $x \in \mathcal{B}$ akkor $y \in \mathcal{A}$ miatt $x + y \in \mathcal{A} + \mathcal{B}$. Így beláttuk (4.3)-t.

Ekkor (4.2) és (4.3) alapján kapjuk, hogy

$$|\mathcal{A} + \mathcal{B}| \geq |\mathcal{A}' + \mathcal{B}'| \geq \min\{p, |\mathcal{A}'| + |\mathcal{B}'| - 1\} = \min\{p, |\mathcal{A}| + |\mathcal{B}| - 1\}.$$

Ezzel az I. Esetben beláttuk a Cauchy–Davenport tétel állítását.

Az általános esetet (vagyis, ha $\mathcal{A} \cap \mathcal{B}$ nem szükségszerűen üres, valódi részhalmaza $\mathcal{B}$-nek) a következőkben fogjuk tanulmányozni. Ekkor a következőt állítjuk:

4.4. LEMMA. *Létezik egy $c \in \mathbb{Z}_p$ elem, amelyre $\mathcal{B} \cap (\mathcal{A} + c)$ nem üres valódi részhalmaza $\mathcal{B}$-nek.*

A 4.4. Lemma bizonyítása. Legyen

$$\mathcal{A} = \{\alpha_1, \alpha_2, \ldots, \alpha_m\},$$
$$\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_n\}.$$

Ha c-t $\beta_i - \alpha_j$ alakban keressük, akkor $\mathcal{B} \cap (\mathcal{A} + c) = \mathcal{B} \cap (\mathcal{A} + \beta_i - \alpha_j)$ nem üres halmaz, mivel

$$\beta_i \in \mathcal{B} \quad \text{és} \quad \beta_i = \alpha_j + \beta_i - \alpha_j \in \mathcal{A} + (\beta_i - \alpha_j).$$

Először két elemet rögzítünk $\mathcal{B}$-ben: β_k-t és β_i-t, ahol $\beta_k \neq \beta_i$. Feltehetjük, hogy

$$\mathcal{A} + (\beta_k - \beta_i) \not\subseteq \mathcal{A},$$

mivel különben a 4.2. Lemma miatt $\mathcal{A} = \mathbb{Z}_p$, és akkor a tétel triviális.

Legyen α_j olyan, hogy $\alpha_j + (\beta_k - \beta_i) \notin \mathcal{A}$. Ekkor

$$\beta_k \notin \mathcal{A} + \beta_i - \alpha_j,$$
$$\beta_k \notin \mathcal{B} \cap (\mathcal{A} + \beta_i - \alpha_j).$$

Azaz $\mathcal{B} \cap (\mathcal{A} + \beta_i - \alpha_j) \neq \mathcal{B}$ és nem üres halmaz (mivel $\beta_i \in \mathcal{B} \cap (\mathcal{A} + \beta_i - \alpha_j)$), így valódi részhalmaza $\mathcal{B}$-nek. Ezzel a lemma állítását igazoltuk.

Ezután visszatérünk a Cauchy-Davenport tétel bizonyításához. Rögzítünk egy $c \in \mathbb{Z}_p$ elemet, melyre a 4.4. Lemma fennáll. A már igazolt I. Eset miatt az $\mathcal{A} + c$ és $\mathcal{B}$ halmazokra alkalmazhatjuk a Cauchy-Davenport tételt. Ekkor:

$$\begin{aligned} |\mathcal{A} + \mathcal{B}| &= |(\mathcal{A} + c) + \mathcal{B}| \\ &\geq \min\{p, |\mathcal{A} + c| + |\mathcal{B}| - 1\} \\ &= \min\{p, |\mathcal{A}| + |\mathcal{B}| - 1\}. \end{aligned}$$

4.2. Erdős-Ginzburg-Ziv Tétel

Az Erdős-Ginzburg-Ziv tétel jól szemlélteti a Cauchy-Davenport-tétel alkalmazhatóságát, amelyet szerzői (Erdős, Ginzburg és Ziv) 1961-ben dolgoztak ki [4].

4.5. TÉTEL. (Erdős–Ginzburg–Ziv) *Tetszőlegesen megadott* $2m-1$ *darab egész szám közül mindig kiválasztható* m *darab, amelyek összege osztható* m*-mel.*

A 4.5. Tétel bizonyítása. Először a tételt csak prímekre igazoljuk.

Legyen p prímszám, és jelöljük az adott egészeket $a_1, a_2, \ldots, a_{2p-1}$-gyel. Feltehetjük, hogy

$$0 \leq a_1 \leq a_2 \leq \ldots \leq a_{2p-1} < p.$$

Ha $a_i = a_{i+p-1}$ valamilyen $1 \leq i \leq p-1$-re, ekkor

$$a_i + a_{i+1} + \ldots + a_{i+p-1} = pa_i = 0 \quad (\mathbb{Z}_p\text{-ben}),$$

amiből a kívánt eredmény következik. Különben meg, definiáljuk az A_i kételemű halmazokat

$$A_i = \{a_i, a_{i+p-1}\}$$

képlettel. A Cauchy-Davenport tétel ismételt alkalmazásával

$$\{A_1 + A_2 + \ldots + A_{p-1}\} \geq \min\{p, |A_1| + \ldots + |A_{p-1}| - (p-2)\} = p.$$

Azaz azt kaptuk, hogy minden mod p maradékosztály felírható $p-1$ darab elem összegeként, ahol az elemek a $a_1, a_2, \ldots, a_{2p-2}$ halmazból valóak. Speciálisan $-a_{2p-1}$ is felírható, amely egyenletet rendezve, megkapjuk a tétel állítását.

A jövőben az Erdős-Ginzburg-Ziv tételt EGZT-nek rövidítjük.

4.6. LEMMA. *Az EGZT prímekre igaz.*

Ezt az állítást most láttuk be.

4.7. LEMMA. *Ha az EGZT igaz az m és n természetes számokra, akkor mn-re is igaz.*

A 4.7. Lemma bizonyítása. Először k-ra vonatkozó teljes indukcióval belátjuk, hogy $k \cdot m + m - 1$ darab egész közül mindig kiválasztható $a_1, a_2, \ldots, a_{km}$ egészek, melyekre $0 \leq i \leq k-1$ esetén

$$a_{im+1} + a_{im+2} + \ldots + a_{(i+1)m} \tag{4.4}$$

osztható m-mel.

Így $k = 1$ esetén az állítás egyszerűen az EGZT az m modulusra, amelynek igazsága a 4.7. Lemma feltételei között szerepel.

Ezután tegyük fel, hogy az állítást igazoltuk $k \cdot m + (m-1)$ darab egészre és beszeretnénk bizonyítani $k \cdot m + (2m-1) = (k+1)m + m - 1$ darab egészre.

Az indukciós feltevés szerint léteznek $a_1, a_2, \ldots, a_{km}$ egészek, melyekre

$$a_{im+1} + a_{im+2} + \ldots + a_{(i+1)m}$$

osztható m-mel, ha $0 \leq i \leq k-1$.

Egy rövid időre töröljük ki a halmazunkból az $a_1, a_2, \ldots, a_{km}$ egészeket.

Ekkor csak $2m-1$ darab egész marad, amelyek közül kiválaszthatunk m darabot, úgy hogy az összegük osztható m-mel. Jelöljük ezeket a számokat

$$a_{km+1}, a_{km+2}, \ldots, a_{km+m}\text{-mel.}$$

(Ez az EGZT az m modulusra.) Így beláttuk (4.4)-t.

Ezután (4.4)-t használjuk $k = 2n - 1$-re, és azt kapjuk, hogy

$$(2n-1)m + m - 1 = 2nm - 1$$

darab egész között létezik $(2n-1)m$ darab, nevezetesen $a_1, a_2, \ldots, a_{(2n-1)m}$, melyekre

$$b_i \overset{\text{def}}{=} \frac{a_{im+1} + a_{im+2} + \ldots + a_{(i+1)m}}{m} \tag{4.5}$$

mindig egész szám, ha $0 \leq i \leq 2n-2$.

Ha az EGZT használjuk az n modulusra és a $b_0, b_1, \ldots, b_{2n-2}$ egész számokra, azt kapjuk, hogy a b_i egész számok között van n darab, melyek összege osztható n-nel.

Tekintsük most azokat az a_j-ket, melyek összege meghatározta a fenti n darab kiválasztott b_i-t (4.5)-ben. Ezekből az a_i-kből összesen nm darab van, és az összegük osztható nm-mel. Ezzel a tétel állítását beláttuk.

Hivatkozások

[1] A. L. Cauchy, *Recherches sur les nombres*, J. École Polytech. 9 (1813), 99–123.

[2] H. Davenport, *On the addition of residue classes*, J. London Math. Soc.,10 (1935), 30–32.

[3] H. Davenport, *A historical note*, J. London Math. Soc. 22 (1947), 100–101.

[4] P. Erdős, A. Ginzburg és A. Ziv, *Theorem in the additive number theory*. Bull. Res. Council Israel. 10F (1961), 41–43.

[5] Kép, Augustin Louis Cauchy, Wikipedia, link.

[6] Kép, Harold Davenport, Wikimedia Commons, link.

5. Egy diofantikus egyenlet

A fejezetben a következő feladattal foglalkozunk:

5.1. FELADAT. *Keressük meg a*

$$3^a + 4^b = 5^c$$

egyenlet összes nem negatív egész megoldását.

Létezik ennek a feladatnak egy könnyített változata is, mégpedig:

5.2. FELADAT. *Keressük meg a*

$$3^n + 4^n = 5^n$$

egyenlet összes nem negatív egész megoldásait.

Vigyázat a következőkben a feladatok megoldásai következnek! Először a könnyebb feladatot nézzük meg.

Itt csak azt kell észrevenni, hogy az 5^n sokkal gyorsabban nő mint a $3^n + 4^n$. Precízen megfogalmazva: $n \geq 3$ esetén:

$$3^n + 4^n < 5^n.$$

Ezt teljes indukcióval bizonyíthatjuk. Kezdőlépés: $n = 3$ esetén

$$3^3 + 4^3 = 91 < 125 = 5^3.$$

Indukciós lépés: Feltesszük, hogy az állítás igaz $n = k$-ra, azaz $3^k + 4^k < 5^k$. Ebből bebizonyítjuk, hogy $n = k + 1$-re. Ekkor a bizonyítandó állítás

$$3^{k+1} + 4^{k+1} < 5^{k+1}.$$

Valóban:

$$3^{k+1} + 4^{k+1} < 4 \cdot 3^k + 4^{k+1} = 4 \cdot (3^k + 4^k) < 4 \cdot 5^k < 5^{k+1}.$$

Ezzel az állításunkat beláttuk. Az $n = 0, 1, 2$ eseteket megnézve, azt kaptuk, hogy az egyetlen megoldása a feladatnak az $n = 2$.

Kicsit bonyolultabb a helyzet a

$$3^a + 4^b = 5^c$$

egyenlet esetében.

Ilyenkor a kongruenciamódszer és a Pitagoraszi számhármasokra vonatkozó tétel segít. Könnyen látható, hogy ha $a \geq 1$ akkor 3^a osztható 3-mal, ha $b \geq 1$, akkor 4^b osztható 4-gyel, és ha $c \geq 1$, akkor 5^c osztható 5-tel. Ez az egyszerű észrevétel sokat segít a feladat megoldásában, de hogy használni tudjuk, először meg kell vizsgálni az $a = 0$, $b = 0$ és $c = 0$ eseteket.

A c szám nem lehet 0 mert $3^a + 4^b \geq 3^0 + 4^0 = 2 > 1 = 5^0$.

Feltehető tehát $c \geq 1$. Ha $b = 0$, akkor $3^a + 1 = 5^c$. Vizsgáljuk ezt az egyenletet modulo 4:

$$3^a + 1 \equiv 5^c \pmod 4$$
$$(-1)^a + 1 \equiv 1^c \pmod 4,$$

igen ám, de itt a baloldal mindig 0-val vagy 2-vel kongruens modulo 4, míg a jobboldal 1-gyel, ami ellentmondás. Tehát $b \geq 1$ is feltehető.

Végül legyen $a = 0$. Ekkor $1 + 4^b = 5^c$. Ha modulo 3 vizsgáljuk az egyenletet csak az derül ki, hogy c páratlan, hiszen ekkor:

$$1 + 4^b \equiv 5^c \pmod 3$$

$$1 + 1^b \equiv (-1)^c \pmod 3$$
$$2 \equiv (-1)^c \pmod 3.$$

Ilyenkor egy újabb modulus szükséges ahhoz, hogy továbblépjünk. Ez pedig most a 8-as lesz. Ha $b = 1$, akkor $1 + 4 = 5$: megkaptunk egy megoldást, nevezetesen $a = 0$, $b = 1$, $c = 1$. Ha $b \geq 2$, akkor $8 \mid 4^b$ tehát:

$$1 + 4^b \equiv 5^c \pmod 8$$
$$1 \equiv 5^c \pmod 8$$

Készítsünk egy táblázatot az 5 hatványok 8-as maradékaival

c	1	2	3	4	...
$5^c \pmod 8$	5	1	5	1	...

Látható, hogy ez a táblázat periodikus 2 hosszal, és $5^c \equiv 1 \pmod 8$ csak akkor lehetséges, ha c páros. Ezzel megint ellentmondásra jutottunk, hisz az előbb bebizonyítottuk, hogy c páratlan.

A fenti módszert kongruenciamódszernek hívjuk.

A továbbiakban feltesszük, hogy $a, b, c \geq 1$, és szintén a kongruenciamódszerrel folytatjuk a megoldást.

Vizsgáljuk meg először az egyenletet modulo 3:

$$3^a + 4^b \equiv 5^c \pmod 3$$
$$4^b \equiv 5^c \pmod 3$$
$$1^b \equiv (-1)^c \pmod 3$$
$$1 \equiv (-1)^c \pmod 3.$$

Az utolsó kongruenciából látszik, hogy c páros. Ezután a 4-es modulussal próbálkozunk:

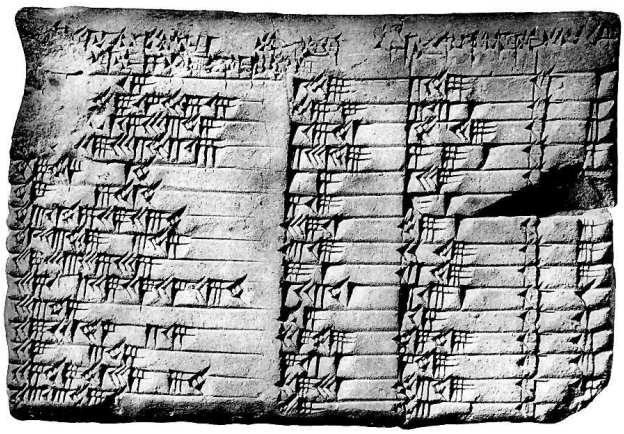
$$3^a + 4^b \equiv 5^c \pmod 4$$
$$3^a \equiv 5^c \pmod 4$$
$$(-1)^a \equiv 1^c \pmod 3$$
$$(-1)^a \equiv 1 \pmod 3.$$

Ebből adódóan a is csak páros lehet. Tovább azonban hiába próbálkozunk más modulusokkal, nem jutunk közelebb a feladat megoldásához. Szerencsére, az kiderült, hogy a és c páros, tehát $a = 2a_1$, $c = 2c_1$, ahol $a_1, c_1 \in \mathbb{Z}^+$. Ekkor egyenletünk a következő alakú:

$$3^a + 4^b = 5^c$$
$$3^{2a_1} + 2^{2b} = 5^{2c_1}$$
$$(3^{a_1})^2 + (2^b)^2 = (5^{c_1})^2$$

Vagyis van itt egy primitív pitagoraszi számhármas: $3^{a_1}, 2^b, 5^{c_1}$.

Legkorábbi számelméleti emlékünk pitagoraszi számhármasokról egy agyag táblatöredék kb. i.e. 1800-ból való és Mezopotámiából származik. Úgynevezett pitagoraszi számhármasokat tartalmazott, azaz olyan a, b, c egész számokat, amelyre $a^2 + b^2 = c^2$. A számhármasok túl nagyok ahhoz, hogy egyszerű próbálgatással találták volna őket. A Plimpton 322 névre keresztelt tábla, így nézett ki:



Egy a, b, c pitagoraszi számhármas primitív, ha a legnagyobb közös osztójuk 1.

Azonban létezik a primitív pitagoraszi számhármasok felírhatóak paraméteres alakban, amely a következő:

5.3. TÉTEL. *Legyen a, b, c primitív pitagoraszi számhármas. Ekkor $\exists\, u, v \in \mathbb{Z}^+$, $u > v$, $(u, v) = 1$, $u \not\equiv v \pmod 2$, hogy*

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2,$$

vagy fordítva

$$a = 2uv, \quad b = u^2 - v^2, \quad c = u^2 + v^2.$$

A tétel bizonyítása a legtöbb elemi számelmélettel foglalkozó könyvben megtalálható, ld. pl. [1], [5], [6], [7], [8] vagy [9].

Fontos megjegyezni, hogy a tételben szereplő paraméteres alak nem adja ki az összes pitagoraszi számhármast, hanem csak a primitíveket. De ezekből az összes pitagoraszi számhármas könnyen megkapható, ha bevezetünk egy újabb paramétert mondjuk k-t, és beszorozzuk vele a hármas összes tagját.

Térjünk vissza a feladat megoldásához. Tehát

$$(3^{a_1})^2 + \left(2^b\right)^2 = (5^{c_1})^2$$

egy primitív pitagoraszi számhármas, azaz $u^2 - v^2, 2uv, , u^2 + v^2$ alakú. Mivel itt $u \not\equiv v \pmod 2$, ezért $u^2 - v^2$ páratlan, $2uv$ pedig nyilván páros. Ez csak úgy lehet (itt használjuk, hogy 3^{a_1} páratlan és 2^b páros):

$$\begin{aligned} 3^{a_1} &= u^2 - v^2 \\ 2^b &= 2uv \\ 5^{c_1} &= u^2 + v^2. \end{aligned}$$

A középső egyenletből adódik, hogy u és v kettőhatvány. Az első egyenlet szerint pedig

$$3^{a_1} = (u - v)(u + v).$$

Vagyis $u - v$ és $u + v$ háromhatvány. Itt $u - v$ és $u + v$ közül $u + v$ a nagyobb. Ha $u - v > 1$, akkor $u - v$ és $u + v$ is osztható 3-mal, tehát az összegük és különbségük is. Azaz $3 \mid 2u, 2v$, vagyis $3 \mid u, v$. Ez azonban ellentmond annak, hogy u és v kettőhatvány.

Tehát $u - v = 1$. Két kettőhatvány különbsége csak akkor lehet 1, ha az egyik a 2 a másik az 1. Vagyis $u = 2$ és $v = 1$. Ekkor

$$\begin{aligned} 3^{a_1} &= u^2 - v^2 = 3 \\ 2^b &= 2uv = 2 \\ 5^{c_1} &= u^2 + v^2 = 5. \end{aligned}$$

Tehát $a_1 = 1$, $b = 2$, $c_1 = 1$. Vagyis $a = 2a_1 = 2, b = 2, c = 2c_1 = 2$. Ezzel az egyenlet összes megoldását meghatároztuk, és

azt kaptuk az $(1, 0, 1)$ és $(2, 2, 2)$ számhármason kívül nincs más megoldás.

Diofantikus egyenletek elemi megoldása során sok más trükk is bevethető. Erről Andrescu, Andrica és Cucurezeanu [1] írt egy kitűnő könyvet, melyben az elmélet mellett számos feladat is szerepel. Itthon Debrecenben van egy kitűnő diofantikus számelméleti iskola, ahol az elemi módszerek mellett mélyebb eszközöket (pl. Baker-módszer, S-egyenletek, s.i.t.) is tanítanak.

Jan-Henrik Evertse és Győry Kálmán több könyvet is írt a Diofantikus egyenletek elméletéről [2], [3], [4] ezeket azonban inkább felsőbb éves hallgatóknak, PhD diákoknak ajánljuk.

Hivatkozások

[1] T. Andrescu, D. Andrica, I. Cucurezeanu, *An Introduction to Diophantine Equations*, Birkhäuser, 2010, link.

[2] J.-H. Evertse, K. Győry, *Unit Equations in Diophantine Number Theory*, Cambridge University Press, 2015.

[3] J.-H. Evertse, K. Győry, *Discriminant Equations in Diophantine Number Theory*, Cambridge University Press, 2016.

[4] J.-H. Evertse, K.Győry, *Effective results and methods for Diophantine equations over finitely generated domains*, Cambridge University Press, 2022.

[5] Erdős Pál, Surányi János, *Válogatott Fejezetek a Számelméletből*, Polygon, 2004, link.

[6] Freud Róbert, Gyarmati Edit, *Számelmélet*, Nemzedékek Tudása Tankönyvkiadó, 2006, link.

[7] Fried Katalin, Korándi József, Török Judit, *Számelmélet*, ELTE TTK, 2011, link.

[8] Gyarmati Edit, Turán Pál, *Számelmélet*, Tankönyvkiadó, 1975. link.

[9] Sárközy A., *Számelmélet*, Műszaki, Budapest, 1976, link.

6. Lánctörtek és Pell egyenletek

A fejezetben először a lánctörtek és Pell egyenletek általános elméletét ismertetjük Ben Lynn [10] munkája alapján. Majd az utolsó alfejezetben Keith Conrad [3] cikke alapján megismerkedünk az általánosított Pell egyenletekkel. Az érdeklődő olvasók magyar irodalmat is találnak a területen, pl. a [5], [6] és [12] könyvekben.

A Pell egyenletek története egészen i.e. 400-ig nyúlik vissza, az ókori Indiáig és Görögországig, ahol az

$$x^2 - 2y^2 = 1$$

és

$$x^2 - 2y^2 = -1$$

egyenletek egész megoldásait tanulmányozták a $\sqrt{2}$ közelítése céljából.

A mai Pell-egyenletek nevüket John Pell matematikus után kapták, aki Angliában újra divatba hozta a területet.

6.1. Lánctörtek - Alapok

A lánctörteknek sok gyakorlati alkalmazásuk van, mind az ókorban, mind a mai napig. Használják valós számok racionálisakkal való közelítésére, a Pell-egyenletek megoldására, de pl. a wifi hálózatok sebességének optimalizálására is (ld. [2]). Említhetjük itt nagy méretű mátrixok sajátértékeinek, sajátvektorainak kiszámítását is (Lánczos algoritmus [9]). Használják még nagy számok gyors faktorizálás során is [11], sőt egy komoly RSA támadás is alapozódott lánctörtekre [4] (ezekről bővebben magyarul is olvashatunk pl. [7]-ban).

6.1. DEFINÍCIÓ. *Az egyszerű lánctört egy*

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

alakú kifejezés, ahol a_0 *nem negatív egész szám (tehát akár* 0 *is lehet),* $a_1, a_2, a_3, \ldots$ *pedig pozitív egészek. Jelölése:*

$$[a_0; a_1, a_2, \ldots].$$

Amennyiben a_k-nál megállunk, tehát

$$[a_0; a_1, a_2, \ldots, a_k] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{1}{a_{k-1} + \cfrac{1}{a_k}}}} \tag{6.1}$$

kifejezést tekintjük, s annak értékét kiszámítjuk, megkapjuk a k-adik közelítő tört értékét, $\frac{p_k}{q_k}$-t.

Az első három közelítő tört:

$$\frac{p_0}{q_0} = a_0,$$
$$\frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = \frac{a_0a_1 + 1}{a_1},$$
$$\frac{p_2}{q_2} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} = \frac{a_0a_1a_2 + a_0 + a_2}{a_1a_2 + 1}.$$

Teljes indukcióval be lehet látni, hogy

$$\begin{aligned} p_k &= a_k p_{k-1} + p_{k-2} \\ q_k &= a_k q_{k-1} + q_{k-2}, \end{aligned} \tag{6.2}$$

ha $k \geq 2$. Ehhez először csak azt látjuk be, hogy ha a (p_k, q_k) sorozatot a $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0a_1 + 1$, $q_1 = a_1$-vel és $k \geq 2$ esetén (6.2) rekurzióval definiáljuk, akkor

$$\frac{p_k}{q_k} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{1}{a_{k-1} + \cfrac{1}{a_k}}}} = [a_0; a_1, a_2, \ldots, a_k] \tag{6.3}$$

valóban fennáll. A második lépés során belátjuk, hogy p_k és q_k legnagyobb közös osztójára $(p_k, q_k) = 1$ teljesül, s ebből állításunk valóban következik.

Igazából az első lépés során többet igazolunk. Belátjuk, hogy a (6.2) rekurzióval megadott sorozat esetén (6.3) tetszőleges valós a_i-kre fennáll. (Viszont p_k és q_k csak akkor lesznek biztosan relatív prímek, ha a_i-k egészek.)

Az indukció kezdőlépései:

$$p_0 = a_0, q_0 = 1, [a_0] = \frac{p_0}{q_0},$$
$$p_1 = a_0a_1, q_1 = a_1, [a_0; a_1] = a_1 + \frac{1}{a_1} = \frac{p_1}{q_1}.$$

Ezután rátérhetünk az indukciós lépésre. Tegyük fel, hogy (6.3)-t beláttuk $k = n$-re. Belátjuk $k = n + 1$-re is. Ehhez bevezetünk egy a_n' számot: $a_n' = a_n + \frac{1}{a_{n+1}}$. Ekkor:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n + \cfrac{1}{a_{n+1}}}}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n'}}}}$$

De itt a jobboldalon már eggyel kevesebb lánctört jegy van. Tehát használhatjuk az indukciós feltevést:

$$\begin{aligned}
[a_0; a_1, \ldots, a_{n+1}] &= \frac{a_n{}' \, p_{n-1} + p_{n-2}}{a_n{}' \, q_{n-1} + q_{n-2}} = \frac{\left(a_{n-1} + \frac{1}{a_n}\right) p_{n-1} + p_{n-2}}{\left(a_{n-1} + \frac{1}{a_n}\right) q_{n-1} + q_{n-2}} \\
&= \frac{(a_{n-1}a_n + 1)p_{n-1} + a_n p_{n-2}}{(a_{n-1}a_n + 1)q_{n-1} + a_n q_{n-2}} \\
&= \frac{a_n(a_{n-1}p_{n-1} + p_{n-2}) + p_{n-1}}{a_n(a_{n-1}q_{n-1} + q_{n-2}) + q_{n-1}} \\
&= \frac{a_n p_n + p_{n-1}}{a_n q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}
\end{aligned}$$

valóban.

6.2. FELADAT. *Bizonyítsuk be teljes indukcióval az alábbi lemmát.*

6.3. LEMMA. *A* $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0a_1 + 1$, $q_1 = a_1$ *és ha* $k \geq 3$

$$p_k = a_k p_{k-1} + p_{k-2}$$
$$q_k = a_k q_{k-1} + q_{k-2}$$

rekurzióval megadott p_k, q_k *számokra fennáll a*

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}. \tag{6.4}$$

összefüggés.

A bizonyítás kivitelezését az olvasóra bízzuk.

A $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$ összefüggésből adódik, hogy $(p_k, q_k) = 1$, hiszen ha $d = (p_k, q_k)$, akkor

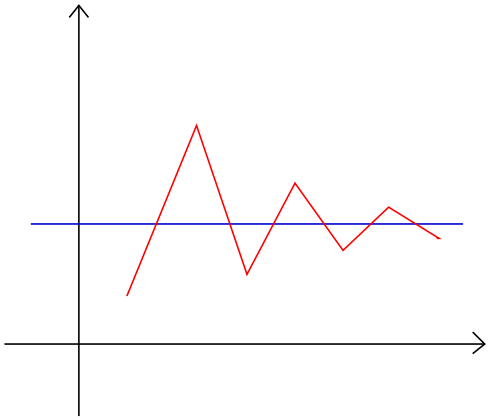
$$d \mid p_q q_{k-1} - p_{k-1} q_k = (-1)^{k-1},$$

amiből $d = 1$. Ezzel beláttuk, hogy a lánctört alakkal megadott közelítő törtek (ld. (6.1)) és a rekurzióval megadott közelítő törtek (ld. (6.2)) valóban azonosak. Azért szeretjük jobban a rekurzióval megadott definíciót, mert az nem egész a_i-k esetén is könnyen értelmezhető. Erre későbbi bizonyítások során nagy szükség lesz.

A (6.4) egyenletet $q_k q_{k-1}$-gyel leosztva

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

adódik, azaz az egymást követő közelítő törtek távolsága 0-hoz tart, illetve a különbség mindig előjelet vált, amiből következik, hogy a lánctört mindig egy valós számhoz tart.



Szintén teljes indukcióval bebizonyítható a következő feladat:

6.4. FELADAT. *A* $\frac{p_k}{q_k}$ *közelítő törtekre fennáll*

$$p_k q_{k-2} - q_k p_{k-2} = (-1)^{k-1} a_k.$$

A feladat megoldását az olvasóra bízzuk. Ebből látszik, hogy a

$\frac{p_0}{q_0}, \frac{p_2}{q_2}, \frac{p_4}{q_4}, \dots$ sorozat monoton növekvő, azaz alulról közelíti a határértéket,

$\frac{p_1}{q_1}, \frac{p_3}{q_3}, \frac{p_5}{q_5}, \dots$ sorozat monoton csökkenő, azaz felülről közelíti a határértéket.

6.5. FELADAT. *Határozzuk meg az*

$$[1; 2, 2, 2, \dots] = 1 + \cfrac{1}{2 + \cfrac{2}{1 + \cfrac{2}{\ddots}}}$$

lánctört értékét.

A 6.5. Feladat megoldása. Vegyük észre, hogy A-val jelölve a

lánctört értékét

$$A = 1 + \cfrac{1}{2 + \cfrac{2}{1 + \cfrac{2}{\ddots}}} = 1 + \frac{1}{1 + A}.$$

Így

$$A(A+1) = (A+1) + 1$$
$$A^2 = 2,$$

amiből $A = \sqrt{2}$, hiszen A pozitív.

6.6. TÉTEL. *Legyen a nem negatív valós szám. Ha α irracionális, akkor egyértelmű a lánctört alakja, ha racionális, akkor kétféleképpen írható lánctört alakban, nevezetesen*

$$[a_0; a_1, a_2, \ldots, a_{n-1}, a_n, 1] = [a_0; a_1, a_2, \ldots, a_{n-1}, a_n + 1].$$

A 6.6. Tétel bizonyítása. Legyen

$$x_i = [a_i; a_{i+1}, a_{i+2}, \ldots].$$

Ekkor:

$$x_i = a_i + \frac{1}{x_{i+1}}$$

Itt $0 \leq \frac{1}{x_{i+1}} \leq 1$, azaz ha $\frac{1}{x_{i+1}} \neq 1$ ($x_{i+1} \neq 1$), akkor

$$a_i = [x_i],$$

vagyis a lánctörtjegyek egyértelműen adódnak. Ha egy $x_{i+1} = 1$, akkor a szám racionális, és a tételbeli két felírás adódik.

Van egy kis hiányosság ebben a bizonyításban. Mi történik akkor, ha a lánctört végtelen és a közelítő törtek egy racionális számhoz konvergálnak? Ilyen számnak háromféle előállítása is lehet. Ezen úgy segítünk, hogy egy teljes indukciót becsempészünk a bizonyításba.

Az 1 nevezőjű törtekre igaz az állítás. Ha beláttuk az állítást $n = 1, 2, \ldots, k$ nevezőre, akkor az $n = k + 1$ nevezőre is tudjuk, hiszen ha α nevezője $k + 1$, akkor

$$\alpha = a_0 + \frac{1}{x_1},$$

ahol x_1 nevezője $\leq k$. Innen az indukciós feltevést használva adódik az állítás.

6.2. Racionális számok közelítése lánctörtekkel

A következőkben a π és az e konstansoknak írjuk fel a lánctört alakját pár számjegy pontossággal:

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, \ldots]$$
$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots, 1, 2k, 1, \ldots]$$

Amikor a nevezetes konstansok valamelyikét, pl. a $\pi = 3.141592\ldots$-t racionális számokkal becsüljük, gyakran közelítő törteket használunk, pl.

$$\pi \sim 3 + \frac{1}{7} = \frac{22}{7} = 3.142867\ldots$$

vagy kicsit pontosabban

$$\pi \sim 3 + \cfrac{1}{7 + \cfrac{1}{106}} = \frac{333}{106} = 3.141509\ldots$$

Ennek okai olyan általános tételekben rejlenek miszerint egy irracionális számot legjobban a közelítő törtjeivel lehet becsülni. Az alfejezetben ezt a témakört járjuk körül.

6.7. TÉTEL. *Legyen $\frac{p}{q}$ az α nem negatív valós számnak egy közelítő törtje. Ha $\frac{p'}{q'}$ közelebb van α-hoz mint $\frac{p}{q}$, akkor $q' > q$.*

A 6.7. Tétel bizonyítása. Emlékeztetünk arra, hogy a közelítő törtek konvergálnak α-hoz, és felváltva, alatta, illetve felette vannak α-nak. Tudjuk

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}.$$

A következő lemmát használva adódik a tétel állítása:

6.8. LEMMA. *Tegyük fel, hogy*

$$\frac{a}{b} < \frac{c}{d} < \frac{a'}{b'},$$

ahol $ab' - a'b = -1$. Ekkor $d > b$ és $d > b'$.

A 6.8. Lemma bizonyítása. Azt bizonyítjuk csak, hogy $d > b'$, hiszen $d > b$ bizonyítása teljesen hasonló ehhez. Valóban:

$$\frac{c}{d} > \frac{a}{b}.$$

Ekkor:

$$0 < \frac{cb - ad}{bd} = \frac{c}{d} - \frac{a}{b} < \frac{a'}{b'} - \frac{a}{b} = \frac{a'b - ab'}{b'b} = \frac{1}{b'b}.$$

Itt $cb - ad > 0$, tehát $cb - ad \geq 1$, vagyis

$$\frac{1}{bd} \leq \frac{cb - ad}{bd} < \frac{1}{b'b}$$
$$b' < d.$$

A bizonyítás $b < d$-re hasonló.

6.3. Approximáció lánctörtek közelítő törtjeivel

Egy nagyon fontos lemmával kezdünk, amelyet többször is használunk a fejezetben.

6.9. LEMMA. *Legyen a lánctörtünk $\alpha = [a_0; a_1, a_2, \dots]$, és legyen a k-adik kiegészítő tört*

$$x_k = [a_k; a_{k+1}, a_{k+2}, \dots].$$

Ekkor

$$\alpha = \frac{x_{k+1}p_k + p_{k-1}}{x_{k+1}q_k + q_{k-1}}.$$

A 6.9. Lemma bizonyítása. Valójában α felfogható úgyis, mint egy véges lánctört: $[a_0; a_1, a_2, \dots, a_k, x_{k+1}]$. Most ugyan a jegyek nem egészek, pontosabban a $k+2$-edik jegy nem egész.

Definiáljuk a p_i és q_i számokat a $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0a_1+1$, $q_1 = a_1$-vel és a

$$p_\ell = a_\ell p_{\ell-1} + p_{\ell-2}$$
$$q_\ell = a_\ell q_{\ell-1} + q_{\ell-2},$$

ha $k \geq \ell \geq 3$, valamint

$$p'_{k+1} = x_{k+1}p_{k-1} + p_{k-2}$$

$$q'_{k+1} = x_{k+1}q_{k-1} + q_{k-2},$$

Ezzel a rekurzióval megadott sorozatra fennáll a fejezet legelején bizonyított (6.3) képlet (mégpedig k helyén $k+1$-gyel és ahol az utolsó lánctört jegy már nem a_{k+1}, hanem x_{k+1}), ha azt az $\alpha = [a_0; a_1, a_2, \ldots, a_k, x_{k+1}]$ lánctörtre alkalmazzuk. (A (6.3) képlet bizonyítása során sehol nem használtuk, hogy a számjegyek egészek.)

A fenti véges lánctörtben a $k+1$-edik közelítő tört maga a szám α, ezért

$$\frac{p'_{k+1}}{q'_{k+1}} = \alpha = \frac{x_{k+1}p_k + p_{k-1}}{x_{k+1}q_k + q_{k-1}}.$$

Ezzel a lemmát beláttuk.

Ekkor

$$\begin{aligned}\alpha - \frac{p_k}{q_k} &= \frac{x_{k+1}p_k + p_{k-1}}{x_{k+1}q_k + q_{k-1}} - \frac{p_k}{q_k} \\ &= \frac{p_{k-1}q_k - q_{k-1}p_k}{q_k(x_{k+1}q_k + q_{k-1})} \\ &= \frac{(-1)^k}{q_k(x_{k+1}q_k + q_{k-1})}.\end{aligned}$$

Itt

$$x_{k+1}q_k + q_{k-1} \geq a_{k+1}q_k + q_{k-1} = q_{k+1} \geq q_k$$

Fordítva pedig

$$\begin{aligned}x_{k+1}q_k + q_{k-1} &= (x_{k+1} - a_k)q_k + a_kq_k + q_{k-1} \\ &= (x_{k+1} - a_k)q_k + q_{k+1} \leq q_k + q_{k+1} \\ &< 2q_{k+1}.\end{aligned}$$

E két becslésből a következő adódik:

6.10. TÉTEL. *Legyen $\frac{p_k}{q_k}$ közelítő törtje a nem negatív valós α-nak. Ekkor*

$$\frac{1}{2q_kq_{k+1}} < \left|\alpha - \frac{p_k}{q_k}\right| \leq \frac{1}{q_kq_{k+1}} < \frac{1}{q_k^2}.$$

A tételben a fordított irány is nagyon érdekes, ez lesz a következő alfejezetünk témája.

6.4. Lánctörtek - Approximáció

A következőkben egy olyan tételt igazolunk, mely mind a diofantikus approximáció egyik alaptétele, s melynek segítségével a későbbiekben látni fogjuk, hogy lánctörtek segítségével, hogyan oldhatók meg az ún. Pell-egyenletek.

6.11. TÉTEL. (Lagrange) *Ha*

$$\left|\frac{p}{q} - \alpha\right| < \frac{1}{2q^2}, \tag{6.5}$$

ahol p és q relatív prímek, akkor $\frac{p}{q}$ az α lánctörtjének egy közelítő törtje.

A bizonyítás a következő lemmán alapul:

6.12. LEMMA. *Ha*

$$\alpha = \frac{P\zeta + R}{Q\zeta + S},$$

ahol $\zeta > 1$ és P, Q, R, S egész számokra

$$Q > S > 0, \quad PS - QR = \pm 1,$$

akkor $\frac{R}{S}$ *és* $\frac{P}{Q}$ *két egymást követő közelítő törtje* α *lánctört alakjának. Amennyiben* $\frac{R}{S}$ *az* $n-1$*-edik közelítő tört,* $\frac{P}{Q}$ *pedig az* n*-edik, akkor* ζ *az úgynevezett* $n+1$*-edik kiegészítő lánctört, vagyis*

$$\zeta = a_{n+1} + \cfrac{1}{a_{n+2} + \cfrac{1}{\ddots}},$$

ahol a_i*-k az* α *szám lánctört számjegyei.*

6.12. Lemma bizonyítása: Írjuk fel $\frac{P}{Q}$-t lánctört alakban:

$$\frac{P}{Q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} = \frac{p_n}{q_n}. \tag{6.6}$$

Itt tetszés szerint feltehetjük, hogy n páros vagy páratlan, ugyanis minden véges lánctörtnek két alakja van, az egyikben a lánctört jegyek száma páros, a másikban páratlan. Ez az állítás a következő észrevételre alapozódik: ha $a_k \geq 2$, akkor:

$$a_0 + \cfrac{1}{a_0 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1} + \cfrac{1}{a_k}}}} = a_0 + \cfrac{1}{a_0 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1} + \cfrac{1}{a_k - 1 + \cfrac{1}{1}}}}}.$$

Így (6.6)-ben választhatjuk úgy n paritását, hogy

$$PS - QR = (-1)^{n-1}$$

teljesüljön. Ekkor $(P, Q) = 1$, $Q > 0$ és $(p_n, q_n) = 1$. Így (6.6) alapján $P = p_n$, $Q = q_n$. Vagyis

$$p_n S - q_n R = PS - QR = (-1)^{n-1} = p_n q_{n-1} - p_{n-1} q_n.$$

Átrendezve

$$p_n(S - q_{n-1}) = q_n(R - p_{n-1}).$$

Mivel $(p_n, q_n) = 1$, ezért

$$q_n \mid S - q_{n-1}. \tag{6.7}$$

De

$$q_n = Q > S > 0,\ q_n \geq q_{n-1} > 0,$$

és így

$$|S - q_{n-1}| < q_n.$$

De (6.7) miatt ez csak úgy lehet, ha $S - q_{n-1} = 0$. Vagyis

$$S = q_{n-1},\quad R = p_{n-1}.$$

Összefoglalva az eddigieket

$$\alpha = \frac{p_n \zeta + p_{n-1}}{q_n \zeta + q_{n-1}}.$$

Tekintsük most azt a lánctörtet, amelynek az első n darab lánctört jegye megegyezik α lánctört jegyeivel, az $n+1$-edik lánctört jegy pedig „ζ”, ami ugyan nem egész szám, de mint mondtuk, egy

előző tételben ez nem is kell, hogy kikötés legyen. A tétel értelmében, az $n+1$-edik közelítő törtre $\frac{p'_n}{q'_n}$-re tudjuk, hogy

$$p'_n = p_n\zeta + p_{n-1},$$
$$q'_n = q_n\zeta + q_{n-1}.$$

Írjuk fel ζ-t lánctört alakban, ahol a lánctört számjegyeit rendre $a_{n+1}, a_{n+2}, \dots$ jelöli, vagyis

$$\zeta = [a_{n+1}; a_{n+2}, a_{n+3}, \dots].$$

A tételben szereplő feltétel miatt $a_{n+1} = [\zeta] \geq 1$, így valóban α lánctört alakja

$$\alpha = [a_0; a_1, a_2, a_3, \dots].$$

Ezzel pedig a tételben szereplő összes állítást igazoltuk.

Térjünk vissza a 6.11. Tétel igazolásához. Legyen

$$\frac{p}{q} - \alpha = \frac{\varepsilon\theta}{q^2},$$

ahol a tételben szereplő (6.5) feltétel miatt feltehető, hogy

$$\varepsilon = \pm 1, \quad 0 < \theta < \frac{1}{2}.$$

Írjuk fel $\frac{p}{q}$-t lánctört alakban

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} = \frac{p_n}{q_n}, \tag{6.8}$$

ahol n paritását tetszés szerint választhatjuk, most legyen n olyan, hogy

$$\varepsilon = (-1)^{n-1}.$$

Definiáljuk ζ-t az

$$\alpha = \frac{\zeta p_n + p_{n-1}}{\zeta q_n + q_{n-1}},$$

összefüggéssel, ahol p_n/q_n és p_{n-1}/q_{n-1} az utolsó és utolsó előtti közelítő törtek $\frac{p}{q}$-nak (6.8) lánctört alakjából. Ekkor

$$\frac{\varepsilon\theta}{q_n^2} = \frac{p_n}{q_n} - \alpha = \frac{p_n q_{n-1} - p_{n-1} q_n}{q_n\left(\zeta q_n + q_{n-1}\right)} = \frac{(-1)^{n-1}}{q_n\left(\zeta q_n + q_{n-1}\right)},$$

így

$$\theta = \frac{q_n}{\zeta q_n + q_{n-1}}.$$

Mivel $0 < \theta < \frac{1}{2}$

$$\zeta = \frac{1}{\theta} - \frac{q_{n-1}}{q_n} > 1.$$

A 6.12. Lemma alapján $\frac{p_{n-1}}{q_{n-1}}$ és $\frac{p_n}{q_n}$ egymást követő közelítő törtek α lánctört alakjában. Ezzel az állítást igazoltuk.

6.5. Periodikus lánctörtek

6.13. Definíció. *Az $[a_0; a_1, a_2, \ldots,]$ lánctört periodikus, ha $\exists\ N_0$ és M pozitív egészek, hogy $n \geq N_0$ esetén*

$$a_n = a_{n+M}.$$

6.14. Tétel. *Minden periodikus lánctört egy egész együtthatós másodfokú egyenlet gyökét reprezentálja.*

A 6.14. Tétel bizonyítása. Legyen $x_k = [a_k; a_{k+1}, a_{k+2}, \dots]$. Tudjuk, hogy létezik $m > n$, melyre $x_m = x_n$. Ekkor

$$x_n = [a_n; a_{n+1}, \dots, a_{m-1}, x_m],$$

amely felírásban az utolsó lánctörtjegy nem egész, de ez nem zavar most minket.

Jelölje x_n, közelítő törtjeit $\frac{p'_0}{q'_0}, \frac{p'_1}{q'_1}, \dots, \frac{p'_{m-n-1}}{q'_{m-n-1}}, \frac{p'_{m-n}}{q'_{m-n}}$. A 6.9. Lemmában tanult rekurzió szerint

$$x_n = \frac{x_m p'_{m-n-1} + p'_{m-n}}{x_m q'_{m-n-1} + q'_{m-n}}.$$

Mivel $x_m = x_n$ így:

$$x_m = \frac{x_m p'_{m-n-1} + p'_{m-n}}{x_m q'_{m-n-1} + q'_{m-n}},$$

amit rendezve megkapjuk, hogy x_m eleget tesz egy másodfokú egész együtthatós egyenletnek. Ha $x_0 = [a_0; a_1, a_2, \dots]$ lánctört közelítő töltjei $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}$, akkor a szokott rekurziót felírva

$$x_0 = \frac{x_m p_{m-1} + p_{m-2}}{x_m q_{m-1} + q_{m-2}}$$

is gyöke egy másodfokú egész együtthatós egyenletnek.

Ez onnan látszik, hogy a másodfokú egész együtthatós egyenletek gyökei felírhatóak $r_1 + r_2\sqrt{D}$ alakban, ahol $r_1, r_2 \in \mathbb{Q}$, $D \in \mathbb{Z}$.

Ha pedig x_m felírható ilyen alakban, azaz

$$x_m = r_1 + r_2\sqrt{D},$$

akkor gyöktelenítés után ezt kapjuk, hogy

$$x_0 = \frac{x_m p_{m-1} + p_{m-2}}{x_m q_{m-1} + q_{m-2}}$$

is ilyen alakú. Ezzel a tétel állítását beláttuk.

6.15. TÉTEL. *Az $ax^2 + bx + c = 0$ egyenlet, ahol a, b, c egész, irracionális gyökeinek lánctört alakja periodikus.*

A 6.15. Tétel bizonyítása. Jelöljük az irracionális gyököt x-szel, és írjuk fel lánctört alakban:

$$x = [a_0; a_1, a_2, \dots]$$

Definiáljuk az x_k számokat az

$$x_k = [a_k; a_{k+1}, a_{k+2} \dots]$$

kiegészítő lánctörttel.

Ha bebizonyítjuk, hogy az x_k számok között van két azonos, azzal beláttuk, hogy x lánctört alakja periodikus.

Legyen

$$x = [a_0; a_1, a_2, \dots]$$

közelítőtörtjei $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \dots$, mivel

$$x = [a_0; a_1, a_2, \dots, a_{k-1}, x_k],$$

ezért a 6.9. Lemmabeli rekurzió szerint

$$x = \frac{x_k p_{k-1} + p_{k-2}}{x_k q_{k-1} + q_{k-2}}.$$

Azt is tudjuk (ld. 6.10. Tétel), hogy

$$\left| x - \frac{p_{k-1}}{q_{k-1}} \right| \leq \frac{1}{q_{k-1}^2} \text{ és } \left| x - \frac{p_{k-2}}{q_{k-2}} \right| \leq \frac{1}{q_{k-2}^2}. \tag{6.9}$$

A továbbiakban térjünk át az $r = p_{k-1}$, $t = q_{k-1}$ és $s = p_{k-2}$, $u = q_{k-2}$ jelölésekre. Ekkor:

$$x = \frac{rx_k + s}{tx_k + u}, \text{ ahol } |ru - ts| = 1. \tag{6.10}$$

Ez utóbbi a (6.4) képlet következménye. Továbbá (6.9) miatt

$$x = \frac{r}{t} + \frac{\varepsilon}{t^2} = \frac{s}{u} + \frac{\eta}{u^2}, \text{ ahol } |\varepsilon|, |\eta| < 1.$$

Könnyen látható, hogy ha az

$$ax^2 + bx + c = 0$$

egyenletbe $x = \frac{rx_k+s}{tx_k+u}$ kifejezést írva x_k gyöke az

$$Ax^2 + Bx + C = 0$$

egyenletnek, ahol

$$\begin{aligned} A &= ar^2 + brt + ct^2 \\ B &= 2ars + b(ru + ts) + 2ctu \\ C &= as^2 + bsu + cu^2. \end{aligned}$$

Amennyiben megmutatjuk, hogy $|A|, |B|, |C|$-re adható egy a, b, c és x-től függő felső korlát, akkor x_k (amint $k = 1, 2, 3, \dots$) csak véges sokféle másodfokú egyenletnek lehet gyöke, és így van az x_k között két azonos.

Ez pedig azt jelenti, hogy x lánctörténet alakja periodikus.

Ehhez

$$\begin{aligned} \frac{A}{t^2} &= a\left(\frac{r}{t}\right)^2 + b\frac{r}{t} + C \\ &= a\left(x - \frac{\varepsilon}{t^2}\right)^2 + b\left(x - \frac{\varepsilon}{t}\right) + c \\ &= ax^2 + bx + c - \frac{2a\varepsilon x}{t^2} + a\frac{\varepsilon^2}{t^4} - \frac{b\varepsilon}{t^2}. \end{aligned}$$

De $ax^2 + bx + c = 0$. Ezt és $|\varepsilon| \leq 1$-t használva

$$|A| \leq |2ax| + |a| + |b|$$

adódik, azaz A korlátos. Hasonló gondolatmenettel kapjuk, hogy C korlátos.

Ami pedig B-t illeti, egyszerű számolás mutatja, hogy

$$4AC - B^2 = (4ac - b^2)(ru - st).$$

De (6.10) alapján $|ru - st| = 1$. Így

$$\left|4AC - B^2\right| = \left|4ac - b^2\right|.$$

A háromszög-egyenlőtlenség szerint:

$$\begin{aligned} \left|B^2\right| - |4AC| &\leq \left|4ac - b^2\right| \\ |B|^2 &\leq |4AC| + \left|4ac - b^2\right|, \end{aligned}$$

azaz B korlátos. Ezzel a tétel állítását beláttuk.

Szerencsénkre, ma már remek online kalkulátorok vannak másodfokú egyenletek gyökei lánctört alakjának meghatározására. Az érdeklődő olvasók megnézhetik pl. a link-et vagy link-t is.

6.6. Tisztán periodikus lánctörtek

Tegyük fel, hogy $a > 1$ és

$$a = [a_0; a_1, a_2, \ldots, a_k, a_0, a_1, a_2, \ldots, a_k, \ldots]$$

egy tisztán periodikus lánctört. Ekkor a 6.9. alapján

$$a = \frac{p_k a + p_{k-1}}{q_k a + q_{k-1}},$$

így a gyöke a következő másodfokú egyenletnek:

$$q_k x^2 + (q_{k-1} - p_k)x - p_{k-1} = 0 \tag{6.11}$$

A (6.11) baloldal negatív, ha $x = 0$, és pozitív, ha $x = -1$. Így a (6.11) egyenletnek van egy gyöke a $(-1, 0)$ intervallumban, ami különbözik a-tól, azaz a-nak konjungáltja.

Egy egész együtthatós másodfokú egyenlet pozitív gyökét redukált kvadratikus gyöknek nevezzük, ha egynél nagyobb és a konjugáltja a $(-1, 0)$ intervallumban fekszik.

6.16. TÉTEL. *Egy valós szám lánctört alakja pontosan akkor tisztán periodikus, ha redukált kvadratikus gyök.*

A 6.16. Tétel bizonyítása. Az egyik irányt már láttuk. A másik irányhoz legyen a, egy redukált kvadratikus gyök. Jelölje f azt a másodfokú egész együtthatós egyenletet, amelynek a gyöke.

Tehát f-nek van egy pozitív gyöke: a, és egy másik gyöke a $(-1, 0)$ intervallumban.

Írjuk fel a lánctört alakját.

$$a = [a_0; a_1, a_2, \dots],$$

és legyen $x_k = [a_k; a_{k+1}, a_{k+2}, \dots]$.

Legyen y_0 az a konjugáltja.

Ekkor $a = a_0 + \frac{1}{x_1}$, $f(a) = 0$, tehát

$$f(a_0 + \frac{1}{x_1}) = 0,$$

amelyet x_1-re rendezve a fentivel ekvivalens, egész együtthatós egyenletet kapunk.

Legyen ennek az egyenletnek a másik gyöke y_1. Ekkor tudjuk,

$$f(y_0) = 0$$

és

$$f(a_0 + \frac{1}{y_1}) = 0.$$

Mivel egyik gyök sem a, ezért a két gyök megegyezik.

$$a_0 + \frac{1}{y_1} = y_0,$$

amiből

$$y_0 - \frac{1}{y_1} = a_0.$$

Mivel $a_0 \geq 1$, $y_0 < 0$, $y_1 = -\frac{1}{a_0 - y_0}$ ezért $-1 < y_1 < 0$, azaz x_1 szintén redukált kvadratikus gyök.

Az eljárást folytatva azt kapjuk, hogy minden k-ra x_k redukált kratatatikus gyök és

$$y_k = a_k + \frac{1}{y_{k+1}}.$$

Mivel $0 < -y_k < 1$, ebből

$$a_k = \left[-\frac{1}{y_{k+1}} \right] \tag{6.12}$$

adódik. Ezután tegyük fel, hogy az első ismétlődés a lánctört jegyeiben

$$a_r = a_{r+k}.$$

(Mivel a gyöke egy egész együtthatós másodfokú egyenletnek, így az előző alfejezetből, a 6.15. Tételből tudjuk, hogy a lánctört alakja

periódikus, csak azt nem tudjuk, hogy tisztán periódikus. Ezt szeretnénk most bizonyítani.) Ekkor:

$$x_r = x_{r+k}$$

$$y_r = y_{r+k}$$

és (6.12) alapján (k helyén $r-1$-gyel):

$$a_{r-1} = a_{r-k-1}.$$

Ismételve az eljárást

$$a = [a_0; a_1, a_2, \dots, a_k, a_0, a_1, \dots, a_k, \dots]$$

adódik.

6.17. KÖVETKEZMÉNY. *Ha D egy pozitív egész szám, amely nem négyzetszám, akkor $\sqrt{D}$ lánctört alakja*

$$\sqrt{D} = [a_0; a_1, a_2, \dots, a_k, a_1, a_2, \dots, a_k, \dots]$$

alakú

Megjegyzés: ugyanez igaz $\sqrt{D} + n$-re is, ahol $n \in \mathbb{Z}$.

A 6.17. Következmény bizonyítása. Azt kell bizonyítani, hogy ha

$$\sqrt{D} = [a_0; a_1, a_2, \dots],$$

akkor $\frac{1}{\sqrt{D}-a_0}$ redukált kvadratikus gyök, ugyanis ez jelenti azt, hogy a lánctört a_1-től kezdve periodikus.

Ehhez az kell, hogy $\frac{1}{\sqrt{D}-a_0}$ konjugáltja a $(-1, 0)$ intervallumba esik. Nyilván $a_0 = [\sqrt{D}]$. Ekkor $\frac{1}{\sqrt{D}-a_0}$ konjugáltja:

$$\overline{\frac{1}{\sqrt{D}-a_0}} = \frac{\overline{\sqrt{D}+a_0}}{D-a_0^2} = \frac{-\sqrt{D}+a_0}{D-a_0^2}.$$

Itt $0 < D - a_0^2$, így $1 \leq D - a_0^2$. Továbbá $-1 < a_0 - \sqrt{D} < 0$, ami alapján

$$\frac{-\sqrt{D} + a_0}{D - a_0^2} \in (-1, 0),$$

amit bizonyítani kellett.

A következő tételt nem bizonyítjuk.

6.18. TÉTEL. *$\sqrt{D}$ lánctört alakja:*

$$\sqrt{D} = [a_0; a_1, a_2, a_3, \ldots, a_3, a_2, a_1, 2a_0, a_1, a_2, \ldots],$$

ahol a periódikus rész palindrom tagja tartalmazhat, illetve nem tartalmazhat középső tagot.

6.7. Pell egyenletek

Amennyiben D pozitív egész nem négyzetszám, akkor az

$$x^2 - Dy^2 = 1$$

egyenletet Pell egyenletnek nevezzük.

6.19. TÉTEL. *Ha $D \in \mathbb{Z}^+$ nem négyzetszám és $\sqrt{D}$ lánctört alakjában a periódushoz k, akkor $k \mid r$ esetén a $\frac{p_{r-1}}{q_{r-1}}$ közelítő törtekre fennáll, a*

$$p_{r-1}^2 - Dq_{r-1}^2 = (-1)^r$$

összefüggés.

A 6.19. Tétel bizonyítása. Legyen $\sqrt{D} = [a_0; a_1, a_2, \dots,$ és $x_i = [a_i; a_{i+1}, a_{i+2}, \dots]$. Tudjuk, hogy

$$x_1 = x_{r+1},$$

hiszen a lánctört periódushosszára $k \mid r$ fennáll. Tudjuk, hogy:

$$\sqrt{D} = \frac{x_{r+1}p_r + p_{r-1}}{x_{r+1}q_r + q_{r-1}}.$$

Itt $x_{r+1} = x_1 = \frac{1}{\sqrt{D}-a_0}$, ahonnan

$$\sqrt{D} = \frac{p_r + p_{r-1}(\sqrt{D} - a_0)}{q_r + q_{r-1}(\sqrt{D} - a_0)}.$$

Rendezve és különválasztva a racionális részt és $\sqrt{D}$ együtthatóját:

$$q_r - a_0 q_{r-1} - p_{r-1} = 0 \tag{6.13}$$

$$p_r - a_0 p_{r-1} - q_{r-1} D = 0 \tag{6.14}$$

Ekkor (6.13)-ből a_0-et kifejezve, és azt (6.14)-be írva, majd rendezve, azt kapjuk, hogy

$$-p_{r-1}q_r + q_{r-1}p_r + p_{r-1}^2 - Dq_{r-1}^2 = 0.$$

Itt

$$p_r q_{r-1} - p_{r-1} q_r = (-1)^{r-1},$$

amiből a tétel adódik.

6.20. Tétel. *Ha p és q megoldása az*

$$x^2 - Dy^2 = \pm 1$$

egyenletnek, akkor p, q relatív prímek és $\frac{p}{q}$ közelítő törtje $\sqrt{D}$-nek.

A 6.20. Tétel bizonyítása. Tudjuk

$$\left|\frac{p}{q}-\sqrt{D}\right| = \left|\frac{p-\sqrt{D}q}{q}\right| = \left|\frac{p^2-Dq^2}{(p+\sqrt{D}q)q}\right| = \frac{1}{(p+q\sqrt{D})q}.$$

Amennyiben $D \geq 5$, ebből, azonnal adódik

$$\left|\frac{p}{q}-\sqrt{D}\right| < \frac{1}{2q^2},$$

s a 6.11. tétel szerint $\frac{p}{q}$ közelítő törtje $\sqrt{D}$-nek. Ha $D = 2, 3$ kicsit több számolás szükséges:

$$\begin{aligned} p^2 - Dq^2 &= (-1)^k \\ p^2 &= Dq^2 + (-1)^k \\ p &\geq \sqrt{Dq^2-1} \geq \sqrt{D}q + 1 - \sqrt{2}. \end{aligned}$$

Így:

$$\left|\frac{p}{q}-\sqrt{D}\right| = \frac{1}{(p+q\sqrt{D})q} \leq \frac{1}{(2\sqrt{D}q+1-\sqrt{2})} < \frac{1}{2q^2},$$

s megint csak azt kapjuk, hogy $\frac{p}{q}$ közelítő törtje $\sqrt{D}$-nek.

Az eddigiekből világos, hogy a közelítő törtek értékei adják meg a Pell egyenletek megoldásait. Ezt tovább pontosíthatjuk a következővel:

6.21. TÉTEL. *Ha k jelöli $\sqrt{D}$ lánctört alakjában a periódus hosszát, akkor az $x^2 - Dy^2 = \pm 1$ Pell egyenlet megoldásait azon $\frac{p_{r-1}}{q_{r-1}}$ közelítő törtek adják, ahol $k \mid r$.*

A 6.21. Tétel bizonyítása. Deiniáljuk az x_k kiegészítő lánctörtet, az $x_k = [a_k; a_{k+1}, a_{k+2}, \dots]$ képlettel.

Az a 6.19. Tételből világos, hogy $k \mid r$ esetén a p_{r-1}/q_{r-1} közelítő törtek egy-egy megoldását adják a Pell-egyenletnek, s ekkor $x_1 = x_{r+1}$ fennáll.

A következőt szeretnénk bebizonyítani: Ha p_{r-1}, q_{r-1} megoldása a Pell-egyenletnek, akkor

$$x_{r+1} = x_1. \tag{6.15}$$

Ez valóban elegendő ugyanis, ha P, Q a Pell egyenlet egy megoldása, akkor az előző tétel értelmében P/Q közelítő törtje $\sqrt{D}$-nek, mondjuk az r-edik közelítő tört. Ekkor ha (6.15)-et használjuk (amit később be is fogunk bizonyítani), akkor azt kapjuk, hogy $x_{r+1} = x_1$. Mivel k a periódushossza a lánctörtnek $k \mid r$.

Lássuk tehát (6.15) bizonyítását. A Pell egyenlet jobboldalán álló ± 1-et lecserélhetjük $(-1)^r$-re, hiszen a páratlan közelítő törtek kisebbek mint $\sqrt{D}$, a párosak pedig nagyobbak mint $\sqrt{D}$.

Tudjuk, hogy

$$\sqrt{D} = \frac{x_{r+1}p_{r-1} + p_{r-2}}{x_{r+1}q_{r-1} + q_{r-2}},$$

(ahol $r = 1$ esetén a $p_{-1} = 1,\ q_{-1} = 0$ konvenciót használjuk), amelyet rendezve

$$(p_{r-1} - \sqrt{D}q_{r-1})x_{r+1} = -p_{r-2} + \sqrt{D}q_{r-2}.$$

Megszorozva ezt $p_{r-1} + \sqrt{D}q_{r-1}$-rel, és a $p_{r-1}^2 - Dq_{r-1}^2 = (-1)^r$, illetve a $p_{r-1}q_{r-2} - p_{r-1}q_{r-2} = (-1)^r$ összefüggéseket használva

$$x_{r+1} = \sqrt{D} + (-1)^r(Dq_{r-1}q_{r-2} - p_{r-1}p_{r-2})$$

adódik, azaz x_{r+1} az $\sqrt{D}$ plusz egy egész szám. Mivel a lánctört jegyeit úgy kapjuk, hogy a kiegészítő törtek egészrészét vesszük mindig, s a törtrész reciproka az új kiegészítő tört, ezért ebből adódóan $x_{r+1} = x_1$ valóban fennáll. Ezzel a bizonyítást befejeztük.

6.22. TÉTEL. *Ha p és q legkisebb pozitív megoldása az $x^2 - Dy^2 = \pm 1$ egyenletnek, akkor az összes pozitív p_n, q_n megoldása az adott Pell egyenletnek (vagy $+1$ vagy -1 rögzített előjellel), megadható a*

$$(p + \sqrt{D}q)^n = p_n + \sqrt{D}q_n$$

képlettel, ahol $n > 0$ páratlan, ha $p^2 - Dq^2 = -1$, és n bármilyen természetes szám lehet, ha $p^2 - Dq^2 = 1$.

A 6.22. Tétel bizonyítása. A tételt csak $x^2 - Dy^2 = 1$ esetben igazoljuk. Tegyük fel, hogy r, s megoldása a Pell egyenletnek, és

$$\begin{aligned} (p + \sqrt{D}q)^m < r + \sqrt{D}s < (p + \sqrt{D}q)^{m+1} \qquad (6.16)\\ p_m + q_m\sqrt{D} < r + \sqrt{D}s < p_{m+1} + \sqrt{D}q_{m+1}. \end{aligned}$$

Ekkor $p_m + \sqrt{D}q_m$-mel osztva (azaz

$$\frac{1}{p_m + \sqrt{D}q_m} = \frac{p_m - \sqrt{D}q_m}{p_m^2 - Dq_m^2} = p_m - q_m\sqrt{D}\text{-vel szorozva),}$$

olyan egyenlethez jutunk, hogy

$$1 < t + \sqrt{D}u < p + \sqrt{D}q,$$

ahol

$$t + u\sqrt{D} = (r + s\sqrt{D})(p_m - \sqrt[D]{q}_m).$$

Ekkor

$$t - u\sqrt{D} = (r - s\sqrt{D})(p_m + \sqrt[D]{q}_m),$$

és az utóbbi két egyenlőtlenséget összeszorozva

$$t^2 - Du^2 = (r^2 - Ds^2)(p_m^2 - Dq_m^2) = 1.$$

Azaz t, u megoldása a Pell egyenletnek. Ha megmutatjuk, hogy $t, u > 0$, akkor van egy p, q-nál kisebb megoldásunk, és ezzel ellentmondásra jutottunk.

Ekkor

$$t = p_m r - q_m s D$$

De itt $r > s\sqrt{D}$ és $p_m > q_m\sqrt{D}$, amiből $t > 0$.

Az u értéke $u = sq_m - q_m r$, de u előjele azonos

$$\begin{aligned}(sp_m - q_m r)(sp_m + q_m r) &= p_m^2 s^2 - q_m^2 r^2 \\ &= s^2(Dq_m^2 + 1) - q_m^2(Ds^2 + 1) \\ &= s_m^2 - q_m^2.\end{aligned}$$

Mivel $s > q_m$ (hiszen tudjuk, hogy $p_m + q_m\sqrt{D} < r + s\sqrt{D}$, azaz $\sqrt{1 + q_m^2 D} + q_m\sqrt{D} < \sqrt{1 + s^2 D} + s\sqrt{D}$. Deriválással látszik, hogy az $\sqrt{1 + x^2 D} + x\sqrt{D}$ monoton növő függvény, azaz az utóbbi egyenlőtlenségből valóban következik $s > q_m$), ezért $u > 0$.

Az $x^2 - Dy^2 = -1$ Pell egyenlet hasonlóan kezelhető, csak (6.16)-ban m-et és $m + 2$-t írunk m és $m + 1$ helyén.

6.8. Általánosított Pell egyenletek

A következőkben az általánosított Pell egyenletekre ismertetünk néhány tételt, bizonyítás nélkül Keith Conrad [3] cikkéből.

6.23. TÉTEL. *Rögzítsük $u = a + b\sqrt{D}$-t, ahol $a^2 - Db^2 = 1$, $a, b \in \mathbb{Z}^+$. Ekkor tetszőleges n nem nulla egész számra az*

$$x^2 - Dy^2 = n$$

általánosított Pell egyenlet megoldása felírható

$$x + \sqrt{D}y = (x' + \sqrt{D}y')u^k$$

alakban, ahol

$$|x'| \leq \frac{\sqrt{|n|}\left(\sqrt{u} + \frac{1}{\sqrt{u}}\right)}{2} \quad \text{és} \quad |y'| \leq \frac{\sqrt{|n|}\left(\sqrt{u} + \frac{1}{\sqrt{u}}\right)}{2\sqrt{D}}$$

Továbbá $n > 0$ esetén az $|y'|$-re adott felső becslés élesíthető

$$|y'| \leq \frac{\sqrt{|n|}\left(\sqrt{u} - \frac{1}{\sqrt{u}}\right)}{2\sqrt{D}} < \frac{\sqrt{nu}}{2\sqrt{D}}\text{-re.}$$

Megjegyezzük, hogy néhány alkalmazásban elegendő a kicsit gyengébb

$$|x'| \leq \sqrt{|n|u} \quad \text{és} \quad |y'| \leq \sqrt{\frac{|n|u}{D}}$$

becsléseket használni.

Dario Arpen készített egy honlapot, amelynek segítségével megtalálhatjuk az általánosított Pell egyenletek összes megoldását mint rekurzív sorozatot. A honlap itt érhető el: link.

Általánosított Pell engyeleteknél a kongruencia módszer nem mindig mondja meg, hogy nincs megoldás. Például a

$$x^2 - 37y^2 = 11 \quad \text{és} \quad x^2 - 194y^2 = -1$$

egyenleteknek nincs megoldása $\mathbb{Z}$-ben, de $\mathbb{Q}$-ban van. Pl. $x^2 - 37y^2 = 11$ megoldásai $(\frac{9}{2}, \frac{1}{2})$ és $(\frac{32}{3}, \frac{5}{3})$; az $x^2 - 194y^2 = -1$ megoldásai: $(\frac{13}{5}, \frac{1}{5})$, $(\frac{5}{13}, \frac{1}{13})$.

Végül egy tétel következik, hogy bizonyos általánosított Pell egyenletek megoldásait hogy kapjuk meg lánctörtekből.

6.24. TÉTEL. *Ha az x és y eleget tesz az*

$$x^2 - Dy^2 = n$$

általánosított Pell egyenletnek, ahol $|n| < \sqrt{D}$, akkor x/y közelítő törtje a $\sqrt{D}$ lánctört alakjának.

A bizonyítás a 6.11. Tételre épül, miszerint ha $\left|\frac{p}{q} - \alpha\right| < \frac{1}{2q^2}$, akkor p/q közelítő törtje az α-nak. A fenti tételt alkalmazzuk $\alpha = \sqrt{D}$-re, ha $n > 0$, és $\alpha = \frac{1}{\sqrt{D}}$-re, ha $n < 0$.

Hivatkozások

[1] D. Alpetron, *Web applications written by Dario Alpern*, link.

[2] H. Afifi, S. Auroux, H. Karl, *MARVELO: Wireless virtual network embedding for overlay graphs with loops*. 2018 IEEE Wireless Communications and Networking Conference (WCNC). IEEE. pp. 1–6. arXiv:1712.06676

[3] K. Conrad, *Pell's equation II*, link.

[4] J. DeLaurentis, *A further weakness in the common modulus protocol for the RSA cryptoalgorithm*, Cryptologia 8 (1984), 253–259.

[5] Freud R., Gyarmati E., *Számelmélet*, Nemzedékek Tudása Tankönyvkiadó, 2006, link.

[6] Gyarmati E., Turán P., *Számelmélet*, Tankönyvkiadó, 1975. link.

[7] Gyarmati K., *Számítógépes Számelmélet*, ELTE, egyetemi jegyzet, 2022.

[8] R, Knott, *An introduction to Continued Fractions*, link.

[9] C. Lanczos, *An iteration method for the solution of the eigenvalue problem of linear differential and integral operators*, Journal of Research of the National Bureau of Standards. 45 (4) (1950) 255–282.

[10] B. Lynn, *Continued Fractions*, link.

[11] M. A. Morrison, J. Brillhart, *A method of factoring and the factorization of F7*. Mathematics of Computation. American Mathematical Society. 29 (129) (1975), 183–205.

[12] Sárközy A., *Számelmélet*, Műszaki, Budapest, 1976, link.

[13] Kép, Wikipédia, *John Pell*, link.

7. Rámánudzsan és a taxiszám probléma

Srínivásza Rámánudzsan a 20. századi matematika egyik legkiemelkedőbb és legrejtélyesebb alakja. Gyakorlatilag magasabb matematikai képzettség nélkül olyan felfedezéseket tett, amelyek nagyon meglepőek voltak és jelentős hatással bírtak az akkori kutatásokra.

1912 és '13 között tételeit ismertető leveleket küldött először indiai, majd angol matematikusoknak. Egy ilyen levelet kapott Hardy is, aki felfigyelt a rendkívül szegény fiatalember meghökkentő és zseniális felfedezéseire. A körülbelül 10 oldalas levél bizonyítás nem, de számos összefüggést ismertetett, amely közül volt ismert is, de olyan is, amelyekkel Hardy még sohasem találkozott.

A levél hatására Hardy meghívta Angliába Rámánudzsant, aki az elkövetkező években több mint 3900 összefüggéstételt fedezett fel.

Sajnos az angliai esős borús éghajlat és a nem megfelelő táplálkozás hiányában (Rámánudzsan vegetáriánus volt, ez Indiában megszokott, de Angliában a háborús időkben akkoriban nehéz volt az indiai étrendnek megfelelő élelmiszereket beszerezni) Rámánudzsan alig 33 évesen elhunyt.

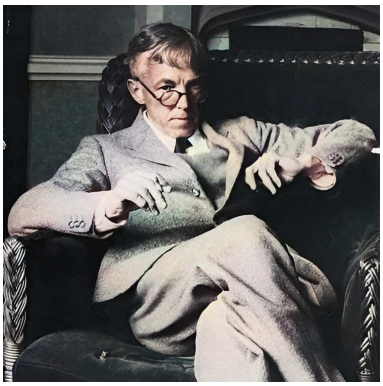
Hardy hatására Rámánudzsan megtanulta leírni bizonyításait. Eredményeit egy jegyzetfüzetbe írogatta, amelyekre ma az elveszett jegyzetfüzet, angolul „lost notebook" elnevezést ragadt rá.

A jegyzetfüzetet George Andrews találta meg újra 1976-ban, egy dobozban, a Wren könyvtárában, a Trinity College-ban, Cambridgeben.

Egy anekdota szerint egy nap Rámánudzsan betegen feküdt, Hardy elment hozzá, hogy meglátogassa. Hardy amikor megérkezett, arról panaszkodott, hogy a taxi rendszáma 1729 volt, ami talán egy nagyon unalmas szám, és ez nem jó előjel.

De Rámánudzsan megnyugtatta, hogy minden rendben van, ugyanis 1729 egy nagyon érdekes szám, ugyanis ez a legkisebb pozitív egész, ami kétféleképpen is felírható két köbszám összegeként:

$$1729 = 9^3 + 10^3 = 12^3 + 1^3$$



G. H. Hardy

S. Rámánudzsan

A következőkben Michel D. Hirschorn írása alapján, „Ramanjan and Fermat's Last Theorem" című cikkére alapozva [1], mutatunk egy érvelést, amely talán Rámánudzsan is átgondolhatott akár egykoron.

Euler óta tudjuk, hogy két pozitív köbszám összege sosem köbszám. Viszont a fenti példa mutatja, hogy két köbszám összege lehet majdnem köbszám, azaz olyan szám, ami egy köbszámtól csak eggyel tér el.

Rámánudzsan végtelen sok példát talált a fenti jelenségre, mint ahogy azt az elveszett jegyzetfüzetben lejegyezte. Hirschorn, a „Mathematics Magazine”-ban két cikket [2], [3] is írt a fenti felfedezéssel kapcsolatosan.

Az első megközelítés lánctörtekkel kapcsolatos. Tekintsünk egy példát. A $\sqrt{2}$ lánctört alakja

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}.$$

Ha a közelítő törteket $\frac{p_n}{q_n}$-nel jelöljük, akkor

$$\begin{bmatrix} p_0 \\ q_0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad \begin{bmatrix} p_1 \\ q_1 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}, \quad \begin{bmatrix} p_2 \\ q_2 \end{bmatrix} = \begin{bmatrix} 7 \\ 5 \end{bmatrix}$$

és

$$\begin{bmatrix} p_{n+2} \\ q_{n+2} \end{bmatrix} = 2 \begin{bmatrix} p_{n+1} \\ q_{n+1} \end{bmatrix} + \begin{bmatrix} p_n \\ q_n \end{bmatrix}, \quad \text{ha} \quad n \geq 1.$$

De ez utóbbit

$$\begin{bmatrix} p_{n+1} \\ q_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} p_n \\ q_n \end{bmatrix}.$$

alakban is írhatjuk (ez teljes indukcióval könnyen igazolható.) Így:

$$\begin{bmatrix} p_n \\ q_n \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}^n \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

(Megjegyezzük, hogy p_n, q_n a $p_n^2 - 2q_n^2 = \pm 1$ megoldásai. A fenti észrevétel arra inspirálta Hirschorn-t, hogy olyan M mátrixot keressen, amelyre a Rámánudszan által megadott x_n, y, z_n hármasra

(ahol $x_n^3 + y_n^3 = z_n^2 \pm 1$) fennáll az

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = M \cdot \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix}$$

mátrixszorzás. Ilyen M pedig tényleg létezik, nevezetesen,

$$\begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} = \begin{bmatrix} 63 & 104 & -68 \\ 64 & 104 & -67 \\ 80 & 131 & -85 \end{bmatrix}^n \cdot \begin{bmatrix} -1 \\ 2 \\ 2 \end{bmatrix}.$$

De hogyan lehet rájönni egy ilyen összefüggésre? Hirschorn a következőt javasolta. Vegyük észre, hogy az

$$(x^2 + 16x - 21)^3 + (2x^2 - 4x + 42)^3$$

polinom páros, azaz a kifejtésben minden x hatvány kitevője páros. Ebből adódóan

$$(x^2+16x-21)^3+(2x^2-4x+42)^3 = (x^2-16x-21)^3+(2x^2+4x+42)^3.$$

Ekkor x-et $2x + 1$-gyel helyettesítve, és 64-gyel osztva:

$$(x^2+9x-1)^3+(2x^2+10)^3 = (x^2-7x-9)^3+(2x^2+4x+12)^3.$$

Ezután x-et helyettesítve $\frac{v}{u}$-val, majd u^6-nal szorozva, végül rendezve:

$$(9u^2+7uv-v^2)^3+(10u^2+2v^2)^3 = (12u^2+4uv+2v^2)^3+(u^2-9uv-v^2)^3.$$

Itt pedig jöhet a Rámánudzsan-szerű gondolat. Legyen $u = h_n$, $v = h_{n-1}$, ahol a $\{h_n\}$ sorozatot

$$h_0 = 0,\ h_1 = 1,\ h_{n+2} = 9h_{n+1} + h_n \text{ ha } n \geq 1.$$

Az így definiált sorozatra

$$u^2 - 9uv - v^2 = (-1)^{n+1}.$$

Ezért ha

$$x_n = 9u^2 + 7uv - v^2,\ y_n = 10u^2 + 2v^2,\ z_n = 12u^2 + 4uv + 2v^2,$$

akkor

$$x_n^3 + y_n^3 = z_n^3 + (-1)^{n+1},$$

amely megadja a Rámánudzsan által definiált x_n, y_n, z_n-et.

Hivatkozások

[1] M. D. Hirschorn, *Ramanujan and Fermat's last theorem*, Aust. Math. Soc. Gaz. 31, No. 4, 256-257 (2004).

[2] M. D. Hirschhorn, *An amazing identity of Ramanujan*, Math. Mag. 68 (1995), 199–201.

[3] M. D. Hirschhorn, *A proof in the spirit of Zeilberger of anamazing identity of Ramanujan*, Math. Mag. 69 (1996), 267–269.

[4] Kép, Wikipédia, Godfrey Harold Hardy, link.

[5] Kép, Wikipédia, Srinivasa Ramanujan, link.

8. Négyzetgyökvonás modulo p

Ebben a fejezetben a négyzetgyökvonásra modulo p adunk egy alternatív trükkös módszert, Perelta [2] algoritmusát. Az algoritmust Robin Chapman jegyzete [1] alapján ismertetjük, aki Perelta algoritmusának egy nagyon ügyes mátrixokkal való leírását adta meg.

Azt mondjuk két egész számokból álló mátrix, A és B kongruensek modulo p, ha a megfelelő elemeik kongruensek modulo p. Jelölése:

$$A \equiv B \pmod{p}.$$

Mátrixok kongruenciái ugyanúgy kezelhetőek, ahogy az egész számok esetében.

Legyen p páratlan prím, a pedig egy kvadratikus maradék, azaz $\left(\frac{a}{p}\right) = 1$. Tegyük fel, hogy az

$$x^2 \equiv a \pmod{p}$$

kongruenciát szeretnénk megoldani.

Első lépésben keresünk egy b egész számot, amelyre

$$\left(\frac{b^2 - a}{p}\right) = -1. \tag{8.1}$$

Ezt véletlen módszerekkel érjük el, annak az esélye, hogy egy véletlenül választott b-re $b^2 - a$ kvadratikus nem maradék körülbelül $1/2$. Így ezt a lépést párszor megismételve, előbb-utóbb eljutunk egy olyan b maradékosztályhoz, amelyre (8.1) fennáll. Definiáljuk az A és B mátrixokat az

$$A = \begin{bmatrix} 0 & 1 \\ a & 0 \end{bmatrix}, \qquad B = bI + A = \begin{bmatrix} b & 1 \\ a & b \end{bmatrix},$$

ahol I a 2×2-es egységmátrix. Ezek után számoljuk ki a $B^{(p-1)/2}$ mátrixot modulo p, ismételt négyzetre emeléssel. Csodálatosképpen azt találjuk, hogy

$$B^{(p-1)/2} \equiv \begin{bmatrix} 0 & r \\ s & 0 \end{bmatrix} \pmod{p},$$

ahol $s^2 \equiv a \pmod{p}$.

Nézzük miért is működik ez az algoritmus. Először számítsuk ki az $B^p = (bI + A)^p$ mátrixot a binomiális tétel alapján:

$$B^p = \sum_{j=0}^{p} \binom{p}{j} b^{p-j} A^j \equiv b^p I + A^p \pmod{p}, \qquad (8.2)$$

mivel $1 \leq j \leq p-1$ esetén a $\binom{p}{j}$ binomiális együttható osztható p-vel. A kis-Fermat Tétel szerint $b^p \equiv b \pmod{p}$. Az Euler lemma szerint $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) = 1 \pmod{p}$ (ld. 3. fejezet). Egyszerű mátrix szorzás mutatja, hogy $A^2 = aI$, így

$$A^p = A \cdot \left(A^2\right)^{(p-1)/2} = A \cdot (aI)^{(p-1)/2} = a^{(p-1)/2} A \equiv A \pmod{p}.$$

A fentieket összevetve (8.2)-mal:

$$B^p \equiv bI + A = B \pmod{p}. \qquad (8.3)$$

Mivel a B mátrix determinánsa nem nulla modulo p, így létezik modulo p vett inverze B^*. Az (8.3) kongruenciát B^*-gal szorozva

$$B^{p-1} \equiv I \pmod{p} \qquad (8.4)$$

adódik. Az $A^2 = aI$ egyenletet használva teljes indukcióval igazolható, hogy minden n természetes számra

$$B^n = x_n I + y_n A$$

alakú, ahol x_n és y_n egész számok. Valóban az indukció kezdőlépése $n = 1$ esetén $B = bI + A$ esetén $x_1 = b, y_1 = 1$. Tegyük fel, hogy az állítást beláttuk n-re, és most bebizonyítjuk $n + 1$-re:

$$\begin{aligned} B^{n+1} &= B^n \cdot B = (x_n A + y_n I) \cdot (bA + I) \\ &= x_n b A^2 + (x_n + y_n b)A + y_n I \\ &= x_n ab I + (x_n + y_n b)A + y_n I \\ &= (x_n + y_n b)A + (x_n ab + y_n), \end{aligned}$$

így $x_{n+1} = x_n + y_n b$ és $y_n = x_n ab + y_n$ jó választás. Állításunkat $B^{(p-1)/2}$ felírva kapjuk, hogy létezik t és r, amelyre

$$B^{(p-1)/2} = tI + rA = \begin{bmatrix} t & r \\ ar & t \end{bmatrix}. \tag{8.5}$$

Emlékezzünk vissza arra, hogy $B^{p-1} = I$ (ld. (8.4)), viszont (8.5) mátrix négyzetének jobb felső eleme a $2rt$ szám, így azt kapjuk

$$2rt \equiv 0 \pmod{p},$$

amiből $r \equiv 0 \pmod{p}$ vagy $t \equiv 0 \pmod{p}$. Először kizárjuk azt az esetet, hogy $r \equiv 0 \pmod{p}$. Valóban, ha $r \equiv 0 \pmod{p}$, akkor (8.5) alapján $B^{(p-1)/2} \equiv tI \pmod{p}$. Így:

$$I \equiv B^{p-1} = (B^{(p-1)/2})^2 \equiv (tI)^2 = t^2 I \pmod{p}.$$

Azaz $t^2 \equiv 1 \pmod{p}$. Ekkor $\det\left(B^{(p-1)/2}\right) \equiv t^2 \equiv 1 \pmod{p}$, viszont a determinánsok szorzástétele miatt

$$\begin{aligned} \det\left(B^{(p-1)/2}\right) &= (\det B)^{(p-1)/2} \\ &= (b^2 - a)^{(p-1)/2} \equiv \left(\frac{b^2 - a}{p}\right) \equiv -1 \pmod{p}, \end{aligned}$$

ami ellentmondás. Tehát $r \not\equiv 0 \pmod{p}$, s így $t \equiv 0 \pmod{p}$. Ekkor:

$$B^{(p-1)/2} \equiv rA = \begin{bmatrix} 0 & r \\ ra & 0 \end{bmatrix} \pmod{p}.$$

Így:

$$I \equiv B^{p-1} \equiv (rA)^2 = r^2 aI \pmod{p}.$$

Azaz $r^2 a \equiv 1 \pmod{p}$. Az s definíciója alapján $s \equiv ra \pmod{p}$, így $s^2 \equiv r^2 a^2 \equiv a \pmod{p}$, amivel a bizonyítást befejeztük.

Hátra van még annak bizonyítása, hogy a maradékosztályok legalább felére $b^2 - a$ kvadratikus nem-maradék, a másik felére kvadratikus maradék, kivéve az $x^2 \equiv a \pmod{p}$ kongruencia két megoldását s és $-s$-t, amikor is $b^2 - a \equiv 0 \pmod{p}$. Ehhez tekintsük a

$$\sum_{b=0}^{p-1} \left(\frac{b^2 - a}{p} \right)$$

szummát. Ha ez -1, akkor készen vagyunk. Ehhez írjunk a helyébe s^2-et, majd használjuk a következő azonosságot:

$$\sum_{b=0}^{p-1} \left(\frac{b^2 - a}{p} \right) = \sum_{b=0}^{p-1} \left(\frac{b^2 - s^2}{p} \right) = \sum_{b=0}^{p-1} \left(\frac{(b-s)(b+s)}{p} \right)$$
$$= \sum_{b=0,\ b \neq -s}^{p-1} \left(\frac{(b-s)/(b+s)}{p} \right)$$

Könnyű ellenőrizni, hogy ahogy b fut az utolsó szummán $(b-s)/(b+s)$ egy teljes maradékrendszer elemeit veszi fel kivéve az 1-et. Ezért:

$$\sum_{b=0}^{p-1} \left(\frac{b^2 - a}{p} \right) = -1,$$

és ezzel az utolsó állításunkat is beláttuk.

Hivatkozások

[1] R. Chapman, *Perelta's algorithm*, link.

[2] R. C. Perelta, *A simple and fast probabilistic algorithm for computing square roots modulo a prime number*, I. E. E. E. Trans. Inform. Theory 32 (1986), 846-847.

9. Speciális prímtesztek

Azokra a p prímekre, amelyekre $M_p \stackrel{\text{def}}{=} 2^p - 1$ is prím M_p-t Mersenne prímnek hívjuk.

Van a Wikipédián egy folyamatosan frissülő oldal, amely az eddig talált legnagyobb prímeket gyűjti össze: link.

Eszerint az első 10 legnagyobb ismert prím a következő:

Helyezés	Szám	Megtalálás ideje	számjegyek száma
1.	$2^{82589933} - 1$	2018 december	24,862,048
2.	$2^{77232917} - 1$	2017 december	23,249,425
3.	$2^{74207281} - 1$	2016 január	22,338,618
4.	$2^{57885161} - 1$	2013 január	17,425,170
5.	$2^{43112609} - 1$	2008 augusztus	12,978,189
6.	$2^{42643801} - 1$	2009 június	12,837,064
7.	$\phi_3(-465859^{1048576})$	2023 május	11,887,192
8.	$2^{37156667} - 1$	2008 szeptember	11,185,272
9.	$2^{32582657} - 1$	2006 szeptember	9,808,358
10.	$10223 \times 2^{31172165} + 1$	2016 október	9,383,761

Itt $\phi_3(x)$ a $\phi_3(x) = x^2 + x + 1$ polinomot jelöli.

Fontos kiemelni, hogy a legnagyobb prímek kutatásában számos magyar rekord született az elmúlt 30 évben. Például Csajbók T., Farkas G., Járai A., Járai Z. és Kasza J. [3] az ELTE IK-ról tartotta a világrekordot 2006-ban a legnagyobb ikerprím kutatásban. További rekordok elérhetőek a következő honlapon is: link. Az ún. Járai módszerről pedig az érdeklődők érdekes cikket olvashatnak pl. [4]-ben is.

Látható, hogy a legnagyobb ismert prímek közül az első tíz helyezett között jelentős túlsúlyban vannak a Mersenne prímek. Ennek az egyik oka, hogy a Mersenne prímekre létezik egy speciális prímteszt, a Lucas-Lehmer prímteszt, amelyet hamarosan ismertetünk.

Előtte azonban nézzünk meg egy másik prímtesztet, amely az ún. Fermat-számok tesztelésére szolgál. Az n-edik Fermat szám definíciója a következő: $F_n = 2^{2^n} + 1$. A Pépin teszt a Fermat számok prímtesztelésére egy módszer.

9.1. TÉTEL. (Pépin teszt) *Az n-edik Fermat szám F_n akkor és csak akkor prímszám, ha $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.*

A $3^{(F_n-1)/2} \pmod{F_n}$ kifejezés értéke moduláris hatványozással gyorsan számolható, időigénye mindössze $O\left((\log F_N)^2\right)$.

Az első öt Fermat szám prímszám, azonban $5 \leq n \leq 32$ esetén F_n mindig összetett.

Jelenleg a 33. Fermat-számról nem tudjuk eldönteni, hogy vajon prímszám-e. Érdekességként megemlítjük, hogy néhány ennél is nagyobb Fermat számról azonban biztosan tudjuk, hogy összetett, mégpedig azért mert van egy viszonylag „kicsi” (ez relatív, csak F_n-hez képest kicsi, valójában azért elég nagy) prímosztója.

A Pépin teszt bizonyítását a Wikipédia [10] alapján ismertetjük.

A 9.1. Tétel bizonyítása. Először azt bizonyítjuk, hogy ha a $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ kongruencia fennáll, akkor F_n prím.

Ekkor

$$3^{F_n-1} \equiv 1 \pmod{F_n},$$

tehát a 3 rendjére modulo F, azaz $o(3)$-ra fennáll, hogy $o(3) \mid F_n - 1$, de $o(3) \nmid (F_n - 1)/2$.

Mivel $F_n - 1$ kettőhatvány, ez csak úgy lehet, ha $o(3) = F_n - 1$.

Vagyis a 3 olyan primitív gyök mod F_n, amelynek rendje $F_n - 1$, tehát létezik $F_n - 1$ darab redukált maradékosztály. Vagyis F_n prímszám.

Ezután rátérünk annak bizonyítására, hogy ha F_n prím, akkor $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

Az Euler lemma szerint ugyanis $3^{(F_n-1)/2} \equiv \left(\frac{3}{F_n}\right) \pmod{F_n}$, ahol $\left(\frac{3}{F_n}\right)$ a Legendre szimbólumot jelöli.

Teljes indukcióval könnyen igazolható, hogy $2^{2^n} \equiv 1 \pmod 3$, azaz $F_n \equiv 2 \pmod 3$.

Gauss kvadratikus reciprocitási tételét használva tudjuk, hogy ha egy p prímre $p \equiv 5 \pmod{12}$ vagy $p \equiv 7 \pmod{12}$ akkor $\left(\frac{3}{p}\right) = -1$. Így $\left(\frac{3}{F_n}\right) = -1$, amiből állításunk következik.

Az első 100 legnagyobb prím között nem találunk Fermat prímet, csak ún. általánosított Fermat prímet, azaz olyan prímeket, amelyek $a^{2^n} + b^{2^n}$ alakúak. A fejezet elején ismertetett táblázatban a 10. legnagyobb prím is általánosított Fermat prím, bár ez első ránézésére nem látszik...

A következőkben rátérünk a Lucas-Lehmer prímtesztre, mely a Mersenne prímek tesztelése során segít.

A tesztet Édouard Lucas fejlesztette ki és Lehmer bizonyította 1930-ban. (ld. [6]).

9.2. TÉTEL. (Lucas-Lehmer teszt) *Legyen $M_p = 2^p - 1$ egy Mersenne szám, ahol is p prímszám. Definiáljuk az $\{t_i\}$ modulo M_p sorozatot a következőképpen:*

$$t_i \equiv \begin{cases} 4 \pmod{M_p} & \text{ha } i = 0; \\ t_{i-1}^2 - 2 \pmod{M_p} & \text{ha } i \geq 1. \end{cases}$$

Ekkor az M_p Mersenne szám, akkor és csak akkor prímszám, ha $t_{p-2} \equiv 0 \pmod{M_p}$.

A 9.2. Tétel bizonyítása. Az itt ismertetett bizonyítás kicsit egyszerűbb mint Lehmer bizonyítása, és a Wikipédia [9] oldalon találtam.

Definiáljuk a $\{s_i\}$ sorozatot a következőképpen:

$$s_i = \begin{cases} 4 & \text{ha } i = 0; \\ s_{i-1}^2 - 2 & \text{ha } i \geq 1. \end{cases}$$

A fenti $\{s_i\}$ sorozatnak a $\{t_i\}$ sorozat a modulo M_p redukált változata, de a gyakorlati alkalmazások során felesleges $\{s_i\}$ elemeit teljes egészében meghatározni, hiszen ez egy nagyon gyorsan növekvő sorozat, elég mindig csak az M_p-vel vett osztási maradékokkal számolni, ami a $\{t_i\}$ sorozat.

Viszont a bizonyítás az $\{s_i\}$ sorozatot használja, mégpedig kezdőlépésként explicit képletet ad $\{s_i\}$ elemeire. Később azt szeretnénk bizonyítani, hogy M_p pontosan akkor prímszám, ha $M_p \mid s_{p-2}$.

Legyen $\omega = 2 + \sqrt{3}$ és $\overline{\omega} = 2 - \sqrt{3}$. Teljes indukcióval könnyű bebizonyítani, hogy

$$s_i = \omega^{2^i} + \overline{\omega}^{2^i}.$$

Valóban:

$$s_0 = \omega^{2^0} + \overline{\omega}^{2^0} = \left(2+\sqrt{3}\right) + \left(2-\sqrt{3}\right) = 4$$

és

$$\begin{aligned} s_n &= s_{n-1}^2 - 2 \\ &= \left(\omega^{2^{n-1}} + \overline{\omega}^{2^{n-1}}\right)^2 - 2 \\ &= \omega^{2^n} + \overline{\omega}^{2^n} + 2(\omega\overline{\omega})^{2^{n-1}} - 2 \\ &= \omega^{2^n} + \overline{\omega}^{2^n}. \end{aligned}$$

Az utolsó lépés azon múlik, hogy $\omega\overline{\omega} = \left(2+\sqrt{3}\right)\left(2-\sqrt{3}\right) = 1.$

Először azt bizonyítjuk, ha $s_{p-2} \equiv 0 \pmod{M_p}$ akkor M_p prímszám. A következők alapja J. W. Bruce [1] és Jason Wojciechowski [12] cikkei.

Legyen $s_{p-2} \equiv 0 \pmod{M_p}$. Ekkor

$$\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} = kM_p,$$

ahol k egész szám. Ezt az egyenletet $\omega^{2^{p-2}}$-vel szorozva

$$\left(\omega^{2^{p-2}}\right)^2 + (\omega\overline{\omega})^{2^{p-2}} = kM_p\omega^{2^{p-2}}$$

De $\omega\overline{\omega} = 1$, így

$$\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1. \tag{9.1}$$

Indirekten bizonyítunk. Tegyük fel, hogy M_p-nek van egy $q > 2$ prímosztója. Jelölje X a következő halmazt:

$$X = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}_q\right\}$$

Az összeadást és szorzást a szokásos módon definiáljuk X-en, de ha nagyon precízek szeretnénk lenni akkor:

$$\left(a+\sqrt{3}b\right)+\left(c+\sqrt{3}d\right) \stackrel{\text{def}}{=} [(a+b) \pmod q] + \sqrt{3}[(c+d) \pmod q]$$

és

$$\left(a+\sqrt{3}b\right)\cdot\left(c+\sqrt{3}d\right) \stackrel{\text{def}}{=} [(ac+3bd) \pmod q] + \sqrt{3}[(ad+bc) \pmod q].$$

Az X halmaz méretét $|X|$-szel jelöljük.

Ekkor X-ben vannak invertálható elemek, ezek halmazát jelölje X^*. Mielőtt továbbhaladnánk itt egy olvasónak szánt feladat:

9.3. FELADAT. *Határozzuk meg X^* elemeit, azaz azon $a+b\sqrt{3} \in X$ elemeket, amelyeknek létezik inverze.*

Szerencsére, a bizonyítás további részleteiben nem használjuk az előző feladat megoldását, csak azt, hogy X^* az X-nek részcsoportja. Mivel X-nek van egy eleme, aminek nincs inverze, nevezetesen 0, ezért

$$|X^*| \leq |X| - 1 = q^2 - 1.$$

Tegyük fel, hogy $M_p \equiv 0 \pmod q$, és tudjuk. hogy $\omega = 2+\sqrt{3} \in X$, így

$$kM_p\omega^{2^{p-2}} = 0$$

szintén teljesül X-ben. Azaz (9.1) szerint

$$\omega^{2^{p-1}} = -1$$

teljesül X-ben. Mindkét oldalt négyzetre emelve

$$\omega^{2^p} = 1.$$

Tehát ω az X^* halmaznak is eleme, mert van egy inverze: ω^{2^p-1}. Továbbá ω rendje osztója 2^p-nek, de nem osztója 2^{p-1}-nek azaz ω rendje pont 2^p.

Lagrange tétele szerint elem rendje mindig osztja a csoport rendjét. Ezt most az ω elemre alkalmazva ($2^p \mid |X^*|$), azonnal látszódik a következő egyenlőtlenség

$$2^p \leq |X^*| \leq q^2 - 1 < q^2,$$

így

$$2^p < q^2.$$

De q a legkisebb prímosztója M_p-nek, azaz

$$q^2 \leq M_p = 2^p - 1.$$

Vagyis $2^p < q \leq 2^p - 1$, ami ellentmondás. Tehát M_p prímszám.

A következőkben azt bizonyítjuk, hogy ha M_p prímszám, akkor $s_{p-2} \equiv 0 \pmod{M_p}$.

Ez az egyszerűsített bizonyítás Rödseth-től [7] származik.

Mivel $2^p - 1 \equiv 7 \pmod{12}$ ha $p > 1$ páratlan szám, azért a Legendre szimbólum alaptulajdonságai miatt:

$$\left(\frac{3}{M_p}\right) = -1.$$

Az Euler-lemma szerint ez ekvivalens a

$$3^{\frac{M_p-1}{2}} \equiv -1 \pmod{M_p}$$

kongruenciával. Azt is tudjuk, hogy a 2 kvadratikus maradék mod M_p, hiszen M_p nyolcas maradéka -1 (szintén a Legendre szimbólum alaptulajdonságai miatt). Az Euler-lemma szerint:

$$2^{\frac{M_p-1}{2}} \equiv 1 \pmod{M_p}.$$

Vagyis

$$24^{\frac{M_p-1}{2}} \equiv \left(2^{\frac{M_p-1}{2}}\right)^3 \left(3^{\frac{M_p-1}{2}}\right) \equiv (1)^3(-1) \equiv -1 \pmod{M_p}.$$

Legyen $\sigma = 2\sqrt{3}$, és definiáljuk X halmazt hasonlóan mint az előbb $X = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}_{M_p}\}$. Mivel M_p prím a következő binomiális együtthatók oszthatók M_p-vel: $\binom{M_p}{1}, \binom{M_p}{2}, \ldots, \binom{M_p}{M_p-1}$. Így a binomiális tételt és kis Fermat tételt használva:

$$\begin{aligned}(6+\sigma)^{M_p} &= 6^{M_p} + \left(2^{M_p}\right)\left(\sqrt{3}^{M_p}\right) \\ &= 6 + 2\left(3^{\frac{M_p-1}{2}}\right)\sqrt{3} \\ &= 6 + 2(-1)\sqrt{3} \\ &= 6 - \sigma.\end{aligned}$$

A σ értéket úgy választottuk, hogy $\omega = \frac{(6+\sigma)^2}{24}$. Azaz (9) alapján az X gyűrűben teljesül a következő:

$$\begin{aligned}\omega^{\frac{M_p+1}{2}} &= \frac{(6+\sigma)^{M_p+1}}{24^{\frac{M_p+1}{2}}} \\ &= \frac{(6+\sigma)(6+\sigma)^{M_p}}{24 \cdot 24^{\frac{M_p-1}{2}}} \\ &= \frac{(6+\sigma)(6-\sigma)}{-24} \\ &= -1.\end{aligned}$$

Mindkét oldalt $(\overline{\omega})^{\frac{M_p+1}{4}}$-gyel szorozva és az $\omega\overline{\omega} = 1$ összefüggést használva kapjuk, hogy

$$\begin{aligned}\omega^{\frac{M_p+1}{2}} \cdot \overline{\omega}^{\frac{M_p+1}{4}} &= -\overline{\omega}^{\frac{M_p+1}{4}} \\ \omega^{\frac{M_p+1}{4}} + \overline{\omega}^{\frac{M_p+1}{4}} &= 0 \\ \omega^{\frac{2^p-1+1}{4}} + \overline{\omega}^{\frac{2^p-1+1}{4}} &= 0 \\ \omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} &= 0 \\ s_{p-2} &= 0.\end{aligned}$$

Mivel s_{p-2} a 0 elem X-ben, így $s_{p-2} \equiv 0 \pmod{M_p}$.

Természetesen, a Lucas-Lehmer teszt önmagában nem lenne elegendő ahhoz, hogy új rekord nagyságú Mersenne prímeket találjanak. De ha a kutatásba sok-sok számítógépet bevonunk, ahol is párhuzamosan futnak a különböző számítások, akkor a hatékonyság többszörösére növelhető.

Ecélból alakult meg a „Nagy Internetes Mersenne Prím Kutatás”, amelyhez bárki, aki PC-vel rendelkezik szabadon csatlakozhat. Kérdés, hogy a háttérben futó programok vajon mennyire lassítják a számítógépet... Az érdeklődők [2] és [8] oldalon több információt találnak a fenti kutatásról.

A Mersenne prímeknek a prímrekordokban szereplő gyakoriságán túl is, sok gyakorlati alkalmazása van: kriptográfiában, elliptikus görbéknél (angolul „Elliptic Curve Cryptography”), kódelméletben és kvantumszámítógépeknél is.

Természetesen olyan általános prímtesztek is vannak, amelyek nem speciális alakú számok (pl. általánosított Fermat vagy Mersenne számok) tesztelésére alkalmasak csak, hanem egy tetszőlegesen megválasztott számról polinomiális időben eldönti, hogy vajon prím-e. Erről bővebben pl. [5]-ben és [11]-ben olvashatunk.

Hivatkozások

[1] J. W. Bruce, *A Really Trivial Proof of the Lucas–Lehmer Test*, The American Mathematical Monthly. 100 (4) (1993) 370–371.

[2] *Great Internet Mersenne Prime Search GIMPS*, link.

[3] T. Csajbók, G. Farkas, A. Járai, Z. Járai, J. Kasza, *Report on the largest known Sophie Germain and twin primes*, Ann. Univ. Sci. Budap. Rolando Eötvös, Sect. Comput. 26 (2006), 181-183.

[4] G. Farkas, G. Gévay, P. Magyar, B. Szekeres *Járai's prime hunting methods reloaded (the largest known Cunningham chain of length 2 of the 2nd kind)*, Ann. Univ. Sci. Budap. Rolando Eötvös, Sect. Comput. 51 (2020), 69-75.

[5] K. Gyarmati, *Számítógépes Számelmélet*, ELTE egyetemi jegyzet (2022), link.

[6] J. H. Jaroma, *Note on the Lucas–Lehmer Test*, Irish Math. Soc. Bulletin (2004) 54 (2), 63-72.

[7] Ö. J. Rödseth, *A note on primality tests for* $N = h \cdot 2^n - 1$, BIT Numerical Mathematics. 34 (3) (1994) 451–454.

[8] Wikipedia, *Great Internet Mersenne Prime Search*, link.

[9] Wikipédia, *Lucas–Lehmer primality test* (2023, August 15), link.

[10] Wikipedia, *Pépin's test*, link.

[11] Wikipedia, *Primality test*, link

[12] J. Wojciechowski, *Mersenne Primes, An Introduction and Overview* 2003, link.