3.1. Diofantikus approximáció.

Alapkérdés: Mennyire jól közelíthetők az irracionálisok racionális számokkal?

Megjegyzés. Mindenek előtt azt kell tisztázni, hogy mit jelent a „jóság".

Egy triviális válasz: Első látásra akármilyen jól, hiszen tudjuk, hogy a racionális számok mindenütt sűrűn helyezkednek el a valós számok között, azaz bármely valós szám tetszőleges környezetében végtelen sok racionális szám van, így bámely $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ irracionális számhoz és $\varepsilon > 0$-hoz van olyan $\frac{a}{b}$, $b > 0$ racionális szám, hogy $\left|\alpha - \frac{a}{b}\right| < \varepsilon$.

Mi most pontosítani fogjuk a „jóság" fogalmát. Mindig föltesszük, hogy a közelítő $\frac{a}{b}$ racionális számaink olyanok, hogy $b > 0$. Első lépésként rögzítsük ezen közelítő $\frac{a}{b}$ racionális számok $b > 0$ nevezőjét. Megmutatható, hogy ha α irracionális szám, akkor van olyan $c \in \mathbb{Z}$ egész, hogy

$$\left|\alpha - \frac{c}{b}\right| < \frac{1}{b}.$$

A következő fogalom lényegesen messzebre vezet, már bizonyos értelemben „méri a jóságot".

Definíció. Legyen $t \in \mathbb{N}$, $t > 1$ tetszőleges. Azt mondjuk, hogy az α valós szám *t-edrendben approximálható* racionális számokkal, ha végtelen sok olyan $\frac{a}{b}$, $b \geq 1$ racionális szám létezik, hogy

$$\left|\alpha - \frac{a}{b}\right| < \frac{c(\alpha)}{b^t},$$

ahol $c(\alpha)$ csak α-tól függő konstans.

Egy korábbi bizonyításunk melléktermeke a következő tétel.

3.1.1. Tétel. *Az irracionális számok másodrendben approximálhatók racionális számokkal.*

Bizonyítás. Legyen α valós szám, konstruáljuk meg lánctört alakjából a p_k, q_k sorozatokat, és jelölje — mint korábban is — $\alpha_k = \frac{p_k}{q_k}$ a k-adik kezdő szeletet. Tudjuk, hogy bármely $n \in \mathbb{N}$-re α a α_n és α_{n+1} között van, így

$$\begin{aligned} 0 < |\alpha - \alpha_n| &< |\alpha_{n+1} - \alpha_n| \\ &= \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}} |p_{n+1}q_n - p_n q_{n+1}| \\ &= \frac{1}{q_n q_{n+1}} < \frac{1}{{q_n}^2}. \end{aligned}$$

Az elkövetkezőkben azt mutatjuk meg, hogy a lánctört alak kezdő szeletei a legjobb másodfokú approximációk. Ennek első lépése a következő lemma lesz.

3.1.2. Lemma. *Legyen $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $n \in \mathbb{N}$, továbbá α_n, p_n, q_n a „szokásosak". Ha $a, b \in \mathbb{Z}$ és $1 \leq b < q_{n+1}$, akkor*

$$|q_n\alpha - p_n| \leq |b\alpha - a|.$$

Bizonyítás. Tekintsük a

$$p_n x + p_{n+1} y = a$$
$$q_n x + q_{n+1} y = b$$

lineáris egyenletrendszert. Ez nyilván megoldható, sőt pontosan egy egész megoldása van (determinánsa ugyanis $(-1)^{n+1}$)):

$$x_0 = (-1)^{n+1}(aq_{n+1} - bp_{n+1})$$
$$y_0 = (-1)^{n+1}(bp_n - aq_n)$$

Állítjuk, hogy csak azzal az esetel kell érdemben foglalkoznunk, amikor a megoldás nemzéró, és ellentétes előjelűek, azaz $x_0 y_0 < 0$.

Ugyanis, ha $x_0 = 0$, akkor

$$aq_{n+1} = bp_{n+1} \quad \Rightarrow \quad q_{n+1} | b,$$

ami lehetetlen a b választása miatt. Ha pedig $y_0 = 0$, akkor

$$a = p_n x_0 \quad \text{és} \quad b = q_n x_0,$$

ami maga után vonja, hogy

$$|b\alpha - a| = |\alpha q_n x_0 - p_n x_0| = |x_0| \cdot |q_n \alpha - p_n| \geq |q_n \alpha - p_n|,$$

azaz teljesül a lemma állítása.

Marad annak megmutatása, hogy x_0 és y_0 ellentétes előjelű, valahányszor nemzérók. Ha $y_0 < 0$ akkor

$$q_n x_0 = b - q_{n+1} y_0, \text{ amiből } \; q_n x_0 > 0.$$

Tudjuk, hogy a q_k sorozat minden tagja pozitív, így $x_0 > 0$ adódik.

Ha pedig $y_0 > 0$, akkor

$$b < q_{n+1} \quad \Rightarrow \quad b < q_{n+1} y_0 \quad \Rightarrow \quad q_n x_0 < 0 \quad \Rightarrow \quad x_0 < 0.$$

Ismét azt használjuk ki, hogy α lánctört alakjának két szomszédos kezdő szelete között helyezkedik el, azaz bármely $n \in \mathbb{N}$-re

$$\alpha_n < \alpha < \alpha_{n+1} \quad \text{vagy} \quad \alpha_n > \alpha > \alpha_{n+1},$$

azaz

$$\frac{p_n}{q_n} < \alpha < \frac{p_{n+1}}{q_{n+1}} \quad \text{vagy} \quad \frac{p_n}{q_n} > \alpha > \frac{p_{n+1}}{q_{n+1}}.$$

Ezekből

$$p_n < q_n \alpha \quad \text{és} \quad q_{n+1}\alpha < p_{n+1}, \tag{1}$$

vagy

$$p_n > q_n\alpha \quad \text{és} \quad q_{n+1}\alpha > p_{n+1}, \tag{2}$$

adódik, és (1)-ből

$$q_n\alpha - p_n > 0 \quad \text{és} \quad q_{n+1}\alpha - p_{n+1} < 0,$$

míg (2)-ből

$$q_n\alpha - p_n < 0 \quad \text{és} \quad q_{n+1}\alpha - p_{n+1} > 0,$$

azaz

$$q_n\alpha - p_n \quad \text{és} \quad q_{n+1}\alpha - p_{n+1}$$

ellentétes előjelűek, ezért ezeket rendre az ellentétes előjelű x_0 és y_0 egészekkel szorozva azonos előjelű számokat kapunk, és így összegük abszolut értéke megegyezik abszolut értékeik összegével:

$$\begin{aligned} |b\alpha - a| &= |\alpha(q_n x_0 + q_{n+1}y_0) - (p_n x_0 + p_{n+1}y_0)| \\ &= |x_0(q_n\alpha - p_n) + y_0(q_{n+1}\alpha - p_{n+1}| \\ &= |x_0| \cdot |q_n\alpha - p_n| + |y_0| \cdot |q_{n+1}\alpha - p_{n+1}| \\ &\geq |x_0| \cdot |q_n\alpha - p_n| \geq |q_n\alpha - p_n|. \end{aligned}$$

E lemmából már könnyen adódik az ígért tétel

3.1.3. Tétel. *Legyen $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ tetszőleges irracionális szám, és bármely $n \in \mathbb{N}$-re $\alpha_n = \dfrac{p_n}{q_n}$ lánctört alakjának n-edik kezdő szelete. Ha $1 \leq b \leq q_n$ egész, akkor bármely $\dfrac{a}{b} \in \mathbb{Q}$-ra*

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \left|\alpha - \frac{a}{b}\right|.$$

Megjegyzés. Tételünk azt állítja, hogy a lánctört alak n-edik kezdő szelete a legjobb azon $\frac{a}{b}$ közelítések között, amelyek b nevezője nem nagyobb q_n-nél.

Bizonyítás. Tegyük föl, hogy állításunk nem igaz, azaz van olyan $a \in \mathbb{Z}$, hogy bár $1 \leq b \leq q_n$, mégis

$$\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{p_n}{q_n}\right|.$$

Ekkor azonban

$$|q_n\alpha - p_n| = q_n\left|\alpha - \frac{p_n}{q_n}\right| > b\left|\alpha - \frac{a}{b}\right| = |b\alpha - a|,$$

adódik, ami ellentétes lemmánkal.

Tudjuk, hogy az irracionálisokat lánctörtjeik kezdő szeletei másodrendben approximálják, de jogosak azok a kérdések, hogy egyrészt javítható-e az approximáció foka, másrészt csak a lánctörtből nyerhető másodfokú approximáció, vagy más úton is. Előbb a másodikra válaszolunk.

3.1.4. Tétel. *Legyen α irracionális szám. Ha az $\frac{a}{b}$, $(b \geq 1,\ \text{ln. k. o.}(a,b) = 1)$ racionális szám, és*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2},$$

akkor valamely $n \in \mathbb{N}$-re

$$\frac{a}{b} = \alpha_n = \frac{p_n}{q_n},$$

ahol α_n az α lánctört alakjának n-edik kezdő szelete.

Bizonyítás. Tegyük föl, hogy $\frac{a}{b}$-re teljesülnek a tétel föltételei, de nem egyezik meg egyetlen kezdő szelettel sem. Mivel a q_k sorozat szigorúan monoton növekvő, pontosan egy olyan $n \in \mathbb{N}$ van, amelyre $q_n \leq b < q_{n+1}$. Ezen n-re teljesül az

$$|q_n\alpha - p_n| \leq |b\alpha - a| = b\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b}$$

egyenlőtlenségsorozat részben az előbbi lemma, részben a bevezetőben említettek miatt.

Ebből egyszerűen kapható, hogy

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2bq_n}.$$

Mivel föltételünk szerint $\frac{a}{b} \neq \frac{p_n}{q_n}$, a $bp_n - aq_n$ különbség nemzéró egész, így $1 \leq |bp_n - aq_n|$. Ebből azonban következik, hogy

$$\begin{aligned}\frac{1}{bq_n} \leq \left|\frac{bp_n - aq_n}{bq_n}\right| &= \left|\frac{p_n}{q_n} - \frac{a}{b}\right| \\ &\leq \left|\frac{p_n}{q_n} - \alpha\right| + \left|\alpha - \frac{a}{b}\right| < \frac{1}{2bq_n} + \frac{1}{2b^2}.\end{aligned}$$

A kapott

$$\frac{1}{bq_n} < \frac{1}{2bq_n} + \frac{1}{2b^2}$$

egyenlőtlenségből $b < q_n$ adódik, ami ellentmond n választásának.

Foglalkozzunk most approximációnk javíthatóságával. Két mély tételt említünk bizonyítás nélkül.

3.1.5. Tétel. (Hurwitz tétele) *Bármely α irracionális számhoz végtelen sok olyan $\frac{a}{b}$ $(a, b \in \mathbb{Z},\ b > 0,\ \text{ln. k. o.}(a,b) = 1)$ racionális szám létezik, amelyre*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{\sqrt{5}b^2}.$$

Utolsó tételünk azt mondja, hogy a Hurwitz tételben szereplő konstans nem növelhető.

3.1.6. Tétel. *Van olyan α irracionális szám, amelyhez csak véges sok olyan $\frac{a}{b}$ racionális szám létezik (a további föltételek ugyanazok, mint az előbbi tételben), amelyre*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{(\sqrt{5} + \varepsilon)b^2}$$

ahol $\varepsilon > 0$ tetszőleges valós szám.

Példa. Ilyen szám az $\alpha = \frac{1+\sqrt{5}}{2}$, amelynek lánctört alakjának minden jegye 1.

3.2. Lineáris diofantikus egyenletek.

A módszer megtalálása egyéni földolgozásra szánt feladat.

3.3. A Pell-egyenlet.

1657-ben Fermat — bár ez nem volt szokása — két probléma megoldására hívta föl a matematikus társadalmat. Vélhetően indirekte J. Wallisnak címezte, aki a Newtont megelőző kor egyik legnagyobbra értékelt angol matematikusa volt. A következő kérdéseket tette föl.

1. Adjunk meg olyan köbszámot, amelyből valódi osztói összegével növelve négyzetszámot kapunk. Például, $7^3 + (1 + 7 + 7^2) = 20^2$.
2. Adjunk meg olyan négyzetszámot, amelyből valódi osztói összegével növelve köbszámot kapunk.

A problémák Wallist hidegen hagyták, de például egyik kortársa — a francia Bernhard Frénicle de Bessy — a következő megoldást adta az első problémára:

> Ha a
> $$(2 \cdot 3 \cdot 5 \cdot 13 \cdot 41 \cdot 47)^3$$
> egészet megnöveljük valódi osztói összegével, akkor a kapott szám négyzetszám, nevezetesen
> $$(2^7 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 13 \cdot 17 \cdot 29)^2.$$

Fermat nem ilyen példákat, hanem általános eredményt keresett. Először azzal az esettel foglalkozott, amikor a köbszám egy prím köbe. Ennek általánosításaként az

$$x^3 + (1 + x + x^2) = y^3$$

egyenlet megoldására hívott föl föltéve, hogy x páratlan. Ha egyenletünket

$$(1 + x)(1 + x^2) = y^2$$

alakra írjuk át, akkor az

$$ab = \left(\frac{y}{2}\right)^2, \qquad \text{ln. k. o.}(a, b) = 1$$

alakban írható, mivel a bal oldalon álló két tényezőnek egyedül a 2 prímosztója. Világos, hogy a, b mindegyike négyzetszám, mondjuk $a = u^2$ és $b = v^2$, így

$$1 + x = 2a = 2u^2, \qquad 1 + x^2 = 2b = 2v^2.$$

Ez azt jelenti, hogy ha egy x egész megoldása Fermat első problémájának, akkor szükségképp megoldása a következő egyenletpárnak:

$$x = 2u^2 - 1, \qquad x^2 = 2v^2 - 1.$$

A második speciális esete az

$$x^2 = dy^2 \pm 1$$

alakú egyenleteknek.

Ez utóbbi fölismerésen alapulhatott Fermat azon — egy hónappal később közzétett — problémája, miszerint:

3. Adjunk meg olyan y egészet, amelyre dy^2+1 négyzetszám, ahol $d \in \mathbb{N}$ nem négyzetszám. Például, $3 \cdot 1^2 + 1 = 2^2$, vagy $5 \cdot 4^2 + 1 = 9^2$.

3'. Ha általános megoldást nem sikerül találni, akkor keressük meg a legkisebb olyan y egészet, amelyre $61y^2 + 1 = x^2$, vagy $109y^2 + 1 = x^2$.

A már említett Frénicle megadta az $x^2 - dy^2 = 1$ egyenletek legkisebb megoldásait $d \leq 15$-re, de ez már mások érdeklődését is fölkeltette. Például egy angol lord, Wallis patrónusa kiszámolta, hogy

$$(126862368)^2 - 313(7170685)^2 = -1,$$

így

$$y = 2 \cdot 7170685 \cdot 126862368$$

a legkisebb megoldása az $x^2 - 313y^2 = 1$ egyenletnek.

1759-ben Euler, majd valamivel később Lagrange rájött arra, hogy a probléma megoldása szorosan kapcsolódik $\sqrt{d}$ lánctört alakjához. Euler nem fejezte be vizsgálatait, Lagrange azonban 1768-ban publikálta azon eredményét, miszerint az $x^2 - dy^2 = 1$ alakú egyenletek, ahol $d \in \mathbb{N}$ és nem négyzetszám, megoldásai a $\sqrt{d}$ lánctört alakjából nyerhetők.

Később az angol John Pell néhány jelentéktelen eredményt publikált ezen egyenletekről, de valami fatális tévedés révén ezen egyenlettípust az utókor az ő nevéhet kapcsolta Euleré, vagy Lagrange-é helyett.

Az $\mathbf{x^2 - dy^2 = 1}$ (ahol $\mathbf{d \in \mathbb{Z},\ d \neq 0}$) egyenlet, az ún. Pell-egyenlet vizsgálata.
Vannak triviális megoldások: $x = \pm 1,\ y = 0$.
Ha $d < -1$, akkor $x^2 - dy^2 > 1$, kivéve, ha $x = y = 0$, így ez esetekben nincs megoldás. Ha pedig $d = -1$, akkor további két triviális megoldás van: $x = 0,\ y = \pm 1$.

Végül, a $d = n^2$ esetben is csak triviális megoldások vannak, hiszen az

$$x^2 - dy^2 = x^2 - n^2y^2 = (x + ny)(x - ny) = 1$$

esetben

$$x + ny = x - ny = \pm 1,$$

ami ismét csak az $x = \pm 1,\ y = 0$ esetekben áll fönn.
Így csak azt az esetet kell vizsgálni, amikor $d > 0$, és nem négyzetszám. Nyilvánvaló, hogy elegendő a pozitív megoldásokat megkeresni, és ha $p, q \in \mathbb{N}$ megoldás, akkor ln. k. o.$(p, q) = 1$.

3.3.1. Tétel. *Ha $p, q \in \mathbb{N}$ megoldása az $x^2 - dy^2 = 1$ egyenletnek, akkor $\frac{p}{q}$ a $\sqrt{d}$ lánctört alakjának valamely kezdő szelete.*
Bizonyítás. Tegyük föl, hogy $p^2 - dq^2 = 1$, azaz

$$(p - \sqrt{d}q)(p + \sqrt{d}q) = 1, \tag{1}$$

amiből $p > q\sqrt{d}$ és

$$\frac{p}{q} - \sqrt{d} = \frac{1}{q(p + q\sqrt{d})}$$

adódik.

Mivel

$$0 < \frac{p}{q} - \sqrt{d} = \frac{1}{q(p + q\sqrt{d})} < \frac{\sqrt{d}}{q(q\sqrt{d} + q\sqrt{d})} = \frac{\sqrt{d}}{2q^2\sqrt{d}} = \frac{1}{2q^2},$$

a

$$0 < \frac{p}{q} - \sqrt{d} < \frac{1}{2q^2}$$

egyenlőtlenség adódik, ami a 3.1.4. Tétel szerint a bizonyítandó állítást jelenti.

E tétel megfordítása általában nem igaz, a $\sqrt{d}$ nem mindegyik kezdő szelete szolgáltat megoldást. Valamivel kevesebb azonban bizonyítható. Nevezetesen, ha e kezdő szeleteket $\frac{p_n}{q_n}$ alakban írjuk, akkor becslést tudunk adni a $p_n^2 - dq_n^2$ kifejezés lehetséges értékeire. Igaz ugyanis a következő állítás.

3.3.2. Tétel. *Ha $\frac{p}{q}$ egyik kezdő szelete $\sqrt{d}$ lánctört alakjának, akkor $x = p$, $y = q$ megoldása az*

$$x^2 - dy^2 = k$$

egyenletnek valamely $|k| < 1 + 2\sqrt{d}$-re.

Bizonyítás. Legyen $\frac{p}{q}$ a $\sqrt{d}$ lánctört alakjának egy tetszőleges kezdő szelete. A 3.1.1. Tétel szerint

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

és így

$$|p - q\sqrt{d}| < \frac{1}{q}. \tag{1}$$

Egyszerű rutin becslésekkel kapjuk, hogy

$$\begin{aligned} |p + q\sqrt{d}| &= |(p - q\sqrt{d}) + 2q\sqrt{d}| \\ &< \frac{1}{q} + 2q\sqrt{d} < (1 + 2\sqrt{d})q. \end{aligned} \tag{2}$$

Az (1) és (2) egyenlőtlenségeket összeszorozva kapjuk, hogy

$$\begin{aligned} |p^2 - dq^2| &= |p - q\sqrt{d}| \cdot |p + q\sqrt{d}| \\ &< \frac{1}{q}(1 + 2\sqrt{d})q = 1 + 2\sqrt{d}, \end{aligned}$$

ami épp a bizonyítandó egyenlőtlenség.

Példa. Legyen $d = 7$. Ekkor $\sqrt{7} = \langle 2, \overline{1, 1, 1, 4} \rangle$ amelynek néhány kezdő szelete

$$\frac{2}{1},\ \frac{3}{1},\ \frac{5}{2},\ \frac{8}{3}, \dots$$

Ezek közül az $x = 8,\ y = 3$ lesz megoldása az $x^2 - 7y^2 = 1$ Pell-egyenletnek.

A 3.3.1. Tétel szerint ha az $x^2 - dy^2 = 1$ egyenletnek van megoldása, akkor azok megtalálhatók $\sqrt{d}$ lánctört alakjának kezdő szeletei között. Pontosabban, ha x, y egy megoldás, akkor — a korábbi jelöléseinkkel — van olyan $\alpha_k = \frac{p_k}{q_k}$ kezdő szelet, hogy $x = p_k,\ y = q_k$. Megvizsgáljuk, hogy mely kezdő szeletek szolgáltatnak megoldásokat. Első lépésünk a következő lemma.

3.3.3. Lemma. *Legyen (a szokásos módon) a $\sqrt{d}$ lánctört alakjának $\alpha_m = \frac{p_m}{q_m}$ az m-edik kezdő szelete. Ha $\sqrt{d}$ lánctört alakjának periódusának hossza n, akkor*

$$p_{kn-1}^2 - dq_{kn-1}^2 = (-1)^{kn} \qquad (k = 1, 2, 3, \dots)$$

Bizonyítás. Legyen $k \geq 1$, és tekintsük $\sqrt{d}$ lánctört alakját a következő formában:

$$\sqrt{d} = \langle a_0, a_1, a_2, \dots, a_{kn-1}, x_{kn} \rangle,$$

ahol

$$x_{kn} = \langle 2a_0, \overline{a_1, a_2, \dots, a_{n-1}, 2a_0} \rangle = a_0 + \sqrt{d}.$$

A 2.3.1. Lemma bizonyításában használt észrevétel szerint

$$\sqrt{d} = \frac{x_{kn} p_{kn-1} + p_{kn-2}}{x_{kn} q_{kn-1} + q_{kn-2}}.$$

Ha elvégezzük az $x_{kn} = a_0 + \sqrt{d}$ helyettesítést, akkor a

$$\sqrt{d}(a_0 q_{kn-1} + q_{kn-2} - p_{kn-1}) = a_0 p_{kn-1} + p_{kn-2} - dq_{kn-1}$$

egyenlőséghez jutunk. Látható, hogy ezen egyenlőség bal oldalán irracionális, míg jobb oldalán racionális szám áll, ami lehetetlen. Ezért szükségképp fönnállnak az

$$a_0 q_{kn-1} + q_{kn-2} = p_{kn-1} \qquad \text{és} \qquad a_0 p_{kn-1} + p_{kn-2} = dq_{kn-1}$$

egyenlőségek. Szorozzuk meg ezeket rendre p_{kn-1}-gyel, illetve $-q_{kn-1}$-gyel, majd adjuk össze őket. Így a következő egyenlőséget kapjuk:

$$p_{kn-1}^2 - dq_{kn-1}^2 = p_{kn-1} q_{kn-2} - q_{kn-1} p_{kn-2}.$$

A 2.3.2. Lemma (a) állítása szerint a jobb oldal egyenlő $(-1)^{kn-2} = (-1)^{kn}$-nel, és így

$$p_{kn-1}^2 - dq_{kn-1}^2 = (-1)^{kn}.$$

3.3.4. Tétel. *Tekintsük az*

$$x^2 - dy^2 = 1 \tag{4}$$

Pell-egyenletet, ahol $d \in \mathbb{N}$ tetszőleges nem-négyzetszám. A szokásos jelölésekkel legyen $\alpha_k = \dfrac{p_k}{q_k}$ a $\sqrt{d}$ lánctört alakjának k-adik kezdő szelete, és n e lánctört periódusának hossza.

(1) *Ha n páros, akkor (4) összes pozitív megoldása a következő:*

$$x = p_{kn-1}, \quad y = q_{kn-1} \qquad k = 1, 2, \dots \ .$$

(2) *Ha n páratlan, akkor az összes pozitív megoldást az*

$$x = p_{2kn-1}, \quad y = q_{2kn-1} \qquad k = 1, 2, \dots \ ,$$

formulák szolgáltatják.

Bizonyítás. A 3.3.1. Tételből tudjuk, hogy (4) minden pozitív megoldása $\sqrt{d}$ lánctört alakjának valamely kezdő szeletéből származik.

A 3.3.3. Lemma alapján $x = p_{nk-1},\ yq_{nk-1}$ pontosan akkor megoldása (4)-nek, ha $(-1)^{nk} = 1$. Ha n páros, akkor ez minden $k \in \mathbb{N}$-re teljesül, míg ha páratlan, akkor a páros k-kra.

Példák.

1. Keressük meg az $x^2 - 7y^2 = 1$ egyenlet néhány pozitív megoldását.

$$\sqrt{7} = [2; \overline{1, 1, 1, 4}]$$

Az első néhány kezdő szelet:

$$\frac{2}{1}, \quad \frac{3}{1}, \quad \frac{5}{2}, \quad \frac{8}{3},$$
$$\frac{37}{14}, \quad \frac{45}{17}, \quad \frac{82}{31}, \quad \frac{127}{48},$$
$$\frac{590}{223}, \quad \frac{717}{271}, \quad \frac{1307}{494}, \quad \frac{2024}{765}.$$

Mivel a $\sqrt{7}$ lánctört alakjának periódusa 4, így a

$$\frac{p_{4k-1}}{q_{4k-1}}$$

alakú kezdő szeletek szolgáltatják a megoldások. Ezen föltételnek — az előbbiek közül — a 3. a 7. és a 11. kezdő szeletek tesznek eleget, így

$$x_1 = 8 \ y_1 = 3, \quad x_2 = 127 \ y_2 = 48, \quad x_3 = 2024 \ y_3 = 765$$

az első három pozitív megoldás.

2. Keressük meg az $x^2 - 13y^2 = 1$ egyenlet legkisebb pozitív megoldását.

$$\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}]$$

a periódushossz: 5.
A lánctört első 10 kezdő szelete:

$$\frac{3}{1}, \quad \frac{4}{1}, \quad \frac{7}{2}, \quad \frac{11}{3}, \quad \frac{18}{5},$$

$$\frac{119}{33}, \quad \frac{137}{38}, \quad \frac{256}{71}, \quad \frac{393}{109}, \quad \frac{649}{180}.$$

A 13. Tétel (*ii*) állítása szerint a kezdő szeletek közül a $\frac{p_9}{q_9}$, — tehát az előbbi fölsorolásban a 10. — adja a legkisebb pozitív megoldást, tehát az az

$$x_1 = 649, \quad y_1 = 180.$$

3. Az $x^2 - 991y^2 = 1$ egyenlet legkisebb pozitív megoldása:

$$x = 397.516.400.906.811.930.638.014.896.080$$

$$y = \ 12.055.735.790.331.359.447.442.538.767$$

4. Az $x^2 - 1000099y^2 = 1$ egyenlet legkisebb pozitív megoldása x-re egy 1118 (decimális) jegyű szám, ugyanis a $\sqrt{1000099}$ lánctört alakjának peródushossza 2174.

Megjegyzés. Ez az eset — az igen hosszú periódus — kis számok esetén is előfordul, és így kis d-re is elég nagy lehet a legkisebb pozitív megoldás. Ez a következő példából is jól látható.
5. Az $x^2 - 61y^2 = 1$ egyenlet legkisebb pozitív megoldása:

$$x = 17.663.319.049 \qquad y = 226.153.980,$$

míg ugyanez az $x^2 - 60y^2 = 1$, ill. az $x^2 - 62y^2 = 1$ egyenleteknél rendre

$$x = 31 \quad y = 4, \qquad x = 63 \quad y = 8.$$

A megoldásokból látható, hogy $\sqrt{61}$ periódusa igen hosszú, míg 60 és 62 esetén ez meglehetősen rövid.

Egy legenda szerint Archimédesz epigramma formában elküldött Erathosztenésznek egy feladatot, amely 4 különböző színű tehénnel és bikával volt kapcsolatos, így 8 ismeretlen mennyiség szerepelt benne, s közöttük 9 föltétel teljesült. Ez az un. diofantikus probléma az

$$x^2 - 4.729.494y^2 = 1$$

Pell-egyenletre vezet, de nem valószínű, hogy meg tudta volna oldani akár maga Archimédesz. Az egyik keresett mennyiség (a 8 közül) egy olyan számnak adódik, amelynek 206.545 decimális jegye van. Ha e számot le akarnánk írni és egy centiméterre 4 számjegyet írunk (ez sűrűbb a normál nyomtatásnál), akkor a szám hossza kb. 516 méter lenne.

3.4. Algebrai számok.

Definíció. Azt mondjuk, hogy az $\alpha \in \mathbb{C}$ komplex szám *algebrai szám*, ha van olyan nemkonstans $f \in \mathbb{Q}[x]$ polinom, hogy $f(\alpha) = 0$. A nem algebrai komplex számokat *transzcendens számoknak* nevezzük.
Definíció. Legyen $\alpha \in \mathbb{C}$ algebrai szám, és $n \in \mathbb{N}$. Azt mondjuk, hogy α *n-edfokú algebrai szám*, ha van olyan n-edfokú racionális együtthatós f polinom, hogy $f(\alpha) = 0$, és egyetlen n-nél alacsonyabb fokú nemkonstans polinomnak sem gyöke α. Ezen polinomot az α algebrai szám *minimálpolinomjának*, vagy olykor *definiáló polinomjának* nevezzük.
Megjegyzések.
(1) Világos, hogy egyrészt az előbbi definícióbeli f polinom irreducibilis, másrészt racionális együtthatós polinomok helyett egész együtthatósokkal is dolgozhatunk.
(2) Algebrai szám helyett használhatjuk a „racionális számtest fölötti algebrai szám" elnevezést is, sőt, a „racionális számtest fölött algebrai elem" terminológiát is.
Példák.
(1) Minden racionális szám (elsőfokú) algebrai szám.
(2) A $\sqrt{2}$ másodfokú, míg a $\sqrt[13]{15}$ 13-adfokú algebrai szám. Ugyancsak algebrai szám a $\sqrt{2} + \sqrt[5]{3}$.
(3) A komplex egységgyökök algebrai számok.

3.4.1. Tétel. *Az összes algebrai számok a komplex számok testének résztestét alkotják.*
Jelölés. Az algebrai számok testét az elkövetkezőkben $\mathbb{A}$ fogja jelölni.
Bizonyítás. Egyszerűen belátható, hogy ha $\alpha \in \mathbb{A}$, akkor $-\alpha, \frac{1}{\alpha} \in \mathbb{A}$ is áll. A bizonyítás elvégzése hasznos gyakorló feladat.

Így már csak azt kell igazolnunk, hogy két algebrai szám összege és szorzata szintén algebrai. Legyen α, β két algebrai szám, minimálpolinomjaik pedig legyenek

$$f = \prod_{i=1}^{m}(x - \alpha_i), \quad \text{illetve} \quad g = \prod_{j=1}^{n}(x - \beta_j),$$

ahol $\alpha = \alpha_1$ és $\beta = \beta_1$. A szimmetrikus polinomok alaptétele segítségével egyszerűen kapható, hogy a

$$h = \prod_{i=1}^{m}\prod_{j=1}^{n}(x - \alpha_i - \beta_j) = \prod_{i=1}^{n}(x - \beta_j)$$

olyan racionális együtthatós polinom, amelynek $\alpha + \beta$ gyöke.

Hasonlóan látható be (ennek önálló elvégzése ugyancsak ajánlott), hogy $\alpha\beta$ gyöke az ugyancsak racionális együtthatós

$$\prod_{i=1}^{m}\prod_{j=1}^{n}(x - \alpha_i\beta_j) = \prod_{i=1}^{m}\alpha_i^n g\left(\frac{x}{\alpha_i}\right)$$

polinomnak. Vegyük észre, hogy itt föltételeztük, hogy α, β nemzérók, de ezzel nem korlátoztuk az általánosságot.
3.4.2. Következmény. *Az $\alpha = a + bi$ komplex szám $(a, b \in \mathbb{R})$ pontosan akkor algebrai, ha $a, b \in \mathbb{A}$.*

Az algebrai számok teste hatványozásra nem zárt. Az egyszerűen igazolható, hogy tetszőleges $\alpha \in \mathbb{A}$-ra $\alpha^s \in \mathbb{A}$ valahányszor $s \in \mathbb{Q}$, de több már nem igaz. A nem racionális kitevős hatványok esetén az egyik legegyszerűbb kérdés az, hogy a $2^{\sqrt{2}}$ algebrai szám, vagy transzcendens. Sőt az sem nyilvánvaló, hogy egyáltalán irracionális-e. Ez a kérdés illusztráló példaként szerepel Hilbert VII. problémájában, amelyben az algebrai számok irracionális kitevős hatványainak természetére kérdezett rá. Ő maga ezt a problémát, az α^β alakú hatványok algebrai vagy transzcendens voltának kérdését irracionális algebrai kitevő esetén nagyon nehéznek tartotta. Nehezebbnek, mint Fermat- vagy a Riemann sejtést. Sőt még az igen egyszerű speciális esetet, a $2^{\sqrt{2}}$-t is szinte reménytelennek vélte.

Mindez nem riasztotta el a matematikusokat, hiszen 1934-ben Gelfond és Schneider egymástól függetlenül és különböző módszerekkel igazolta a következő tételt.

3.4.3. Tétel. (Gelfond-Schneider tétel.) *Ha α, β algebrai számok, $\alpha \neq 0, 1$ és β irracionális, akkor α^β transzcendens szám.*

Megjegyzések.

(1) A tételből viszonylag egyszerűen következik Euler azon sejtése, miszerint ha n egész, de nem 10 hatvány, akkor $\lg n$ transzcendens.

(2) A tétel az általában végtelen sok értékű komplex kitevős hatványokra is vonatkozik. Így például i^{2i} mindegyik értéke, köztük az e^π is transzcendens.

(3) Mint azzal majd később részletesebben is foglalkozunk, a XIX. század végétől ismeretes, hogy e, π transzcendens számok. Az azonban a mai napig sem ismert, hogy $e + \pi$ transzcendens-e, vagy egyáltalán irracionális-e.

(4) Az algebrai számok teste algebrailag zárt, azaz az algebrai szám együtthatós polinomok (komplex) gyökei algebrai számok.

3.5. Az algebrai számok approximációja.

Definíció. Azt mondjuk, hogy az $\alpha \in \mathbb{R}$ t-edrendben approximálhazó racionális számokkal, ha végtelen sok olyan $\frac{a}{b}$, $b > 0$ racionális szám van, amelyre

$$\left|\alpha - \frac{a}{b}\right| < \frac{c(\alpha)}{b^t},$$

ahol $c(\alpha)$ csak α-tól függő konstans.

Megjegyzések.

(1) Minden irracionális valós szám másodrendben approximálható racionális számokkal.

(2) A Hurvitz-tételben szereplő $\frac{1}{\sqrt{5}}$ konstans nem csökkenthető, e tétel a lehető legjobb általános érvényű becslést adja meg.

(3) A továbbiakban csak valós algebrai számokkal foglalkozunk.

3.5.1. Tétel. *Legyen $\alpha \in \mathbb{A} \cap \mathbb{R}$ valós n-edfokú algebrai szám. Létezik olyan $c = c(\alpha) > 0$ valós konstans, hogy bármely $r/s \in \mathbb{Q}$-ra*

$$\left|\alpha - \frac{r}{s}\right| > \frac{c(\alpha)}{s^n}. \tag{3}$$

Megjegyzések.
(1) Másképp fogalmazva tételünk azt állítja, hogy létezik olyan $c'(\alpha)$ pozitív valós konstans, hogy az

$$\left|\alpha - \frac{r}{s}\right| < \frac{c'(\alpha)}{s^n}$$

egyenlőtlenség csak véges sok $r/s \in \mathbb{Q}$-ra áll fönn.
(2) Előbbi megjegyzésünk azt is jelenti, hogy csak véges sok olyan $r/s \in \mathbb{Q}$ létezhet, amelyre (3) nem teljesül. Ez meg is szüntethető azáltal, hogy a „rossz" r/s-től függően alkalmas, kisebb értéket választunk c-nek.
(3) A 3.5.1. Tételből az is következik, hogy bármely $t > n$ és $c^* \in \mathbb{R}$ esetén az

$$\left|\alpha - \frac{r}{s}\right| < \frac{c^*}{s^t}$$

egyenlőtlenség csak véges sok $r/s \in \mathbb{Q}$-ra teljesülhet, azaz az n-edfokú valós algebrai számok nem approximálhatók n-edrendnél jobban.

Bizonyítás. Tegyük föl, hogy bármely $c > 0$-hoz van olyan $r/s \in \mathbb{Q}$, amelyre

$$\left|\alpha - \frac{r}{s}\right| < \frac{c}{s^n}.$$

Ez azt jelenti, hogy létezik racionális számok olyan $r_i/s_i,\ s_i > 0$ végtelen sorozata, amelyre

$$\lim_{i\to\infty} s_i^n \left(\alpha - \frac{r_i}{s_i}\right) = 0. \tag{4}$$

Ebből

$$\lim_{i\to\infty} \left(\alpha - \frac{r_i}{s_i}\right) = 0, \qquad \text{azaz} \quad \lim_{i\to\infty} \frac{r_i}{s_i} = \alpha. \tag{5}$$

Jelölje

$$f_\alpha = a_0 + a_1 x + \ldots + a_n x^n = a_n \prod_{j=1}^{n} (x - \alpha_j) \tag{6}$$

az α $\mathbb{Z}$ fölötti minimálpolinomját, ahol $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ e polinom összes komplex gyöke, amelyek nyilván páronként különbözők, lévén f_α irreducibilis. Helyettesítsünk r_i/s_i-t

$$f_\alpha\left(\frac{r_i}{s_i}\right) = a_0 + a_1\frac{r_i}{s_i} + \ldots + a_n\left(\frac{r_i}{s_i}\right)^n = a_n\left(\frac{r_i}{s_i} - \alpha\right)\prod_{j=2}^{n}\left(\frac{r_i}{s_i} - \alpha_j\right) \tag{7}$$

A bal oldalon s_i^n nevezőjű tört áll, amely biztosan nemzéró, hiszen f_α-nak nem lehet racionális gyöke. Ez maga után vonja, hogy (7) bal oldalának abszolut értéke legalább s_i^{-n}. Így belőle az

$$1 \le \left| s_i^n \left(\alpha - \frac{r_i}{s_i}\right) \prod_{j=2}^{n} \left(\frac{r_i}{s_i} - \alpha_j\right)\right| \tag{8}$$

egyenlőtlenség adódik. (4) és (5)-ből

$$\lim_{i\to\infty}\prod_{j=2}^{n}\left(\frac{r_i}{s_i}-\alpha_j\right)=\prod_{j=2}^{n}(\alpha-\alpha_j)$$

következik, ami ellentmond (8)-nak, hiszen ez alapján annak jobb oldala 0-hoz tart, ha $i\to\infty$, ami (8) szerint lehetetlen.

3.5.2. Következmény. Ha egy valós szám tetszőleges rendben approximálható, akkor az szükségképp transzcendens. Ezért úgy igazolható transzcendens szám létezése, hogy keresünk „nagyon jól approximálható" valós számot.

Megjegyzés. Egyszerű halmazelméleti eszközökkel ugyan belátható, hogy kontinuum sok transzcendens valós szám van, azaz „majdnem minden" valós szám transzcendens, de ez egy ún. tiszta egzisztencia bizonyítás, ami semmit sem mond e számok mibenlétéről.

3.5.3. Tétel. (Liouville 1844) *Az*

$$\alpha=\sum_{k=1}^{\infty}\frac{1}{10^{k!}}=0,110001000000000000000001\ldots \tag{9}$$

szám transzcendens.

Megjegyzés. Vegyük észre, hogy a tételbeli szám n-edik jegye 1-es, ha $n=m!$ valamely $m\in\mathbb{N}$-re, különben zéró. Ebből az is világos, hogy α irracionális.

Bizonyítás. Az α-t definiáló sor nyilván konvergens, hiszen majorálja a $\sum 10^{-k}$ konvergens mértani sor.

Tekintsük a (9)-beli sor m-edik részletösszegét valamely $m\in\mathbb{N}$-re.

$$\alpha=\sum_{k=1}^{m}\frac{1}{10^{k!}}=\frac{10A+1}{10^{m!}}=\frac{r_m}{s_m}.$$

Ebből

$$0<\alpha-\frac{r_m}{s_m}=\sum_{k=m+1}^{\infty}\frac{1}{10^{k!}}<\sum_{j=(m+1)!}^{\infty}\frac{1}{10^{j}}=\frac{10}{9\cdot 10^{(m+1)!}}=\frac{10}{9s_m^{m+1}},$$

továbbá

$$\left|\alpha-\frac{r_m}{s_m}\right|<\frac{10}{9s_m^{m+1}} \tag{10}$$

adódik. Ha α algebrai lenne, mondjuk n-edfokú ($n\geq 2$, ugyanis α irracionális). Előző tételünk értelmében van olyan $c(\alpha)$ konstans, hogy bármely $r/s\in\mathbb{Q}$-ra (3)-nak kell teljesülnie, speciálisan $\frac{r_m}{s_m}$-re is, így figyelembe véve (10)-et is

$$\frac{c(\alpha)}{s_m^n}<\left|\alpha-\frac{r_m}{s_m}\right|<\frac{10}{9s_m^{m+1}}$$

adódik. Ez azonban lehetetlen, ugyanis belőle

$$s_m^{m-n+1} < \frac{10}{9c(\alpha)}$$

következik, amely nem állhat fönn nagy m-ekre. Ezen ellentmondás igazolja állításunkat: a Liouville által definiált α szám transzcendens.

E rész zárásaként megfogalmazzuk a 3.5.1. Tétel két élesítését, de egyiket sem bizonyítjuk.

3.5.4. Tétel. (Thue) *Ha α n-edfokú ($n \geq 3$) valós algebrai szám, akkor bámely $c > 0$ konstans esetén az*

$$\left|\alpha - \frac{r}{s}\right| < \frac{c}{c^n}$$

egyenlőtlenség csak véges sok $r/s \in \mathbb{Q}$-ra teljesül.

3.5.5. Tétel. (Roth) *Ha α valós algebrai szám és $\kappa > 0$ tetszőleges valós szám, akkor az*

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^{2+\kappa}}$$

egyenlőtlenséget csak véges sok r/s racionális szám elégíti ki.

Megjegyzések.
(1) Világos, hogy Roth tétele erősebb Thue tételénél.
(2) Azt hihetnénk, hogy a valós transzcendens számok épp a tetszőleges rendben approximálhatók, de ez — mint arra a következő tételünk rámutat — messze nem így van. Csak az igaz, hogy a tetszőlegesen magas rendben approximálható valós számok transzcendensek.

3.5.6. Tétel. *Legyen $\kappa > 0$ valós szám, és H azon α valós számok halmaza, amelyekhez végtelen sok olyan r/s racionális szám van, melyekre*

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^{2+\kappa}}$$

teljesül. Ekkor H nullamértékű halmaz.

3.5.7. Következmények.
(1) Az előbbi H halmaz minden eleme transzcendens.
(2) Csak megszámlálható sok tetszőleges rendben approximálható transzcendens szám létezik, így majdnem minden transzcendens szám „rosszul” approximálható.