

3. A LÁNCTÖRTEK ALKALMAZÁSAI.

3.1. Diofantikus approximáció.

Alapkérdés: Mennyire jól közelíthetők az irracionálisok racionális számokkal?

Megjegyzés. Mindenek előtt azt kell tisztázni, hogy mit jelent a „jószág”.

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 bármely $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ 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 „jószág” 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 messzebbre vezet, már bizonyos értelemben „méri a jószágot”.

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 mellékterméke a következő tétel.

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

Bizonyítás. Legyen α valós szám, konstruáljuk meg lánc tört 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 az α_n és az 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 egyenletrendszer. 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 érdeklőznünk, amikor a megoldás nemzéró, és ellentétes előjelűek, azaz $x_0 y_0 < 0$.

Ugyanis, ha $x_0 = 0$, akkor

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

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

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

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 abszolút értéke megegyezik abszolút értékeik összegével:

$$\begin{aligned} |b\alpha - a| &= |\alpha(q_nx_0 + q_{n+1}y_0) - (p_nx_0 + p_{n+1}y_0)| \\ &= |x_0(q_n\alpha - p_n) + y_0(q_{n+1}\alpha - p_{n+1})| \\ &= |x_0| \cdot |q_n\alpha - p_n| + |y_0| \cdot |q_{n+1}\alpha - p_{n+1}| \\ &\geq |x_0| \cdot |q_n\alpha - p_n| \geq |q_n\alpha - p_n|. \end{aligned}$$

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 $\alpha_n = \frac{p_n}{q_n}$ lánctört alakjának n -edik kezdő szelete. Ha $1 \leq b \leq q_n$ egész, akkor bármely $\frac{a}{b} \in \mathbb{Q}$ -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 lemmánkkal.

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 $\frac{a}{b}$, ($b \geq 1$, 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 nemzéro 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 $\frac{a}{b}$ ($a, b \in \mathbb{Z}$, $b > 0$, 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 feltételek 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

$$(2 \cdot 3 \cdot 5 \cdot 13 \cdot 41 \cdot 47)^3$$

egészset 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

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

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

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

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

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

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 fölkelte. 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 nevéhez kapcsolta Euleré, vagy Lagrange-é helyett.

Az $x^2 - dy^2 = 1$ (ahol $d \in \mathbb{Z}$, $d \neq 0$) 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

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

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

$$|p - q\sqrt{d}| < \frac{1}{q}. \quad (1)$$

Egyszerű rutin becslésekkel kapjuk, hogy

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

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 $\sqrt{d}$ lánc tört 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 $\sqrt{d}$ lánc tört alakjának $\alpha_m = \frac{p_m}{q_m}$ az m -edik kezdő szelete. Ha $\sqrt{d}$ lánc tört alakjának periódusának hossza n , akkor

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

Bizonyítás. Legyen $k \geq 1$, és tekintsük $\sqrt{d}$ lánc tört 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

$$\sqrt{d}(a_0q_{kn-1} + q_{kn-2} - p_{kn-1}) = a_0p_{kn-1} + p_{kn-2} - dq_{kn-1}$$

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

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

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

$$x^2 - dy^2 = 1 \tag{3}$$

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

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

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

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

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

formulák szolgáltatják.

Bizonyítás. A 3.3.1. Tételből tudjuk, hogy (3) minden pozitív megoldása $\sqrt{d}$ lánctört alakjának valamely kezdő szeletéből származik.

A 3.3.3. Lemma alapján $x = p_{nk-1}$, $y = q_{nk-1}$ 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:

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

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 előbbieik közül — a 3. a 7. és a 11. kezdő szeletek tesznek eleget, így

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

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 lánc tört első 10 kezdő szelete:

$$\begin{array}{ccccc} \frac{3}{1}, & \frac{4}{1}, & \frac{7}{2}, & \frac{11}{3}, & \frac{18}{5}, \\ \frac{119}{33}, & \frac{137}{38}, & \frac{256}{71}, & \frac{393}{109}, & \frac{649}{180}. \end{array}$$

A 13. Tétel (u) 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 $\sqrt{1000099}$ lánc tört alakjának periódushossza 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:

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

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

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

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

Egy legenda szerint Archimédész 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 Archimédész. 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.