Diofantikus egyenletek numerikus megoldása

Pethő Attila

Debreceni Egyetem

Magyar Tudományos Akadémia, 2011. április 20.

1. Hilbert 10. problémája

A probléma (1900): *Eine D i o p h a n t i s c h e Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

Adott egy tetszőleges ismeretlen számú, racionális egész együtthatós diofantikus egyenlet: Adjunk olyan eljárást, amely véges sok művelettel eldönti, hogy az egyenletnek van-e megoldása a racionális egész számok körében.

Klasszikus diofantikus egyenletek

Kétváltozós lineáris: Legyenek $a, b, c \in \mathbb{Z}$. Az

$$ax + by = c.$$

egyenlet kiterjesztett euklideszi algoritmussal oldható meg.

Többváltozós lineáris: Lagrange algoritmus

Kétváltozós kvadratikus: Legyenek $d, n \in \mathbb{Z}$. Az egyenlet

$$x^2 - dy^2 = n.$$

- $d \leq 0$ Pozitív definit kvadratikus forma.
- $d = k^2 \rightarrow (x - ky)(x + ky) = n \rightarrow$ faktorizálás.
- Különben Pell egyenlet, melynek a megoldhatósága az n prímosztóitól függ.

Magasabbfokú egyenletekre kevés szisztematikus eredmény.

Kurt Gödel, Martin Davis, Julia Robinson, David Putnam előkészítő és részeredményei után

Ju.V. Matijasevič (1970): Hilbert 10. problémája nem oldható meg. Nincs olyan algoritmus, amely tetszőleges diofantikus egyenletről eldönthetné annak megoldhatóságát.

Reális cél: **Adjunk algoritmust diofantikus egyenletek széles osztályainak megoldására!**

Hilbert 7. problémája: Az α^β kifejezés, ahol az α alap algebrai, a β kitevő pedig irracionális szám, például $2^{\sqrt{2}}$ vagy $e^\pi = i^{-2i}$, mindig transzcendens vagy legalább is irracionális számot jelöl.

A.O. Gelfond (1934) és Th. Schneider (1934) pozitív választ adott Hilbert 7. problémájára.

Ekvivalens megfogalmazás: Legyenek α, γ algebrai számok, $\alpha \neq 0, 1$. Tegyük fel, hogy $1, \beta$ $\mathbb{Q}$-lineárisan függetlenek. Akkor

$$\beta \log \alpha + \log \gamma \neq 0.$$

2. Effektív eredmények

A. Baker (1967) általánosította Gelfond és Schneider tételét.
Legyenek $\alpha_1, \ldots, \alpha_k \neq 0, 1$ algebrai számok ($k \geq 2$). Legyen $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ és $n = [\mathbb{K} : \mathbb{Q}]$. Az α módosított magassága

$$h_m(\alpha) = \max\left\{h(\alpha), \frac{|\log \alpha|}{n}, \frac{1}{n}\right\}.$$

1. Tétel. *[A. Baker and G. Wüstholz (1993)] Legyenek* $b_1, \ldots, b_k \in \mathbb{Z}$ *olyanok, hogy*

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_k \log \alpha_k \neq 0.$$

Akkor

$$\log |\Lambda| > -c_1 h_m(\alpha_1) \ldots h_m(\alpha_k) \log B,$$

ahol $B = \max\{|b_1|, \ldots, |b_k|, 3\}$ *és*

$$c_1 = 18(k+1)!k^{k+1}(32n)^{k+2} \log(2kn).$$

Baker $\rightarrow$ effektív (kiszámítható) felső korlát diofantikus egyenletek megoldásaira. Példák:

• Thue-egyenlet (Baker (1968)) $F(x, y) = m$, ahol $F(x, y) \in \mathbb{Z}[x, y]$, homogén, irreducibilis és $\deg F \geq 3$.

• Elliptikus egyenlet (Baker (1968))
$y^2 = ax^3 + bx^2 + cx + d, \quad a, b, c, d \in \mathbb{Z}$.

• Hiperelliptikus egyenlet (Baker (1969))
$y^2 = P(x), P(x) \in \mathbb{Z}[x], \deg P \geq 4$.

• Diszkrimináns forma egyenlet (Győry (1976)).

A korlát nagyon nagy. Közvetlen számolásra alkalmatlan.

A. Baker és H. Davenport (1969) a nagy korlát redukciójával megoldották az $3x^2 - 2 = y^2, 8x^2 - 7 = z^2$ egyenletrendszert.

3. Példa: négyzetszámok a Fibonacci sorozatban

Legyen $a \geq 1, u_0 = 0, u_1 = 1$ és $u_{n+2} = au_{n+1} + u_n,\ n \geq 0$. Ha $a = 1$, akkor u_n a Fibonacci-sorozat. Legyenek $\alpha(a) = \alpha$ és $\beta(a) = \beta$ az $X^2 - aX - 1$ polinom gyökei. Akkor

$$u_n = \frac{\alpha^n - \beta^n}{\sqrt{a^2 + 4}},\ n \geq 0.$$

2. Tétel. *[Nakamula,Pethő(1996)] Az $u_n(a) = x^2$ egyenlet összes megoldása: $n = 0, 1$, a tetszőleges; $n = 2$, a négyzetszám;* $(n, a) = (7, 2), (12, 1)$.

Fibonacci-sorozatra J.H.E. Cohn (1964) elemi bizonyítás.

Ha $u_{2n+1} = x^2$, akkor az analitikus formulából

$$\alpha^{2n+2} + \beta^{2n} = \alpha\sqrt{5}x^2 \;\Rightarrow\; (\beta^n + x\theta)(\beta^n - x\theta) = -\alpha^{2n+2},$$

ahol $\theta = \sqrt{\alpha\sqrt{5}}$.

Legyen $K = \mathbb{Q}(\theta)$, akkor $[K : \mathbb{Q}] = 4$.

$\mathbb{Z}[\alpha, \theta]$ egységcsoportja generátorai: $\alpha, (1+\theta)/\alpha, \alpha + \theta$.

Egyszerű átalakításokkal kapjuk a

$$\begin{aligned}(\beta^n + x\theta)\alpha^{-n-1} &= (-1)^n\alpha^{-2n-1} + \sqrt{1 + \alpha^{-4n-2}} \\ &= ((1+\theta)/\alpha)^j(\alpha+\theta)^{-k}\end{aligned}$$

egységegyenletet.

Belátható, hogy $0 < j < 2n + 1$, $0 < k < j$ és

$$0 < |j \log((1 + \theta)/\alpha) - k \log(\alpha + \theta)| < \alpha^{-2n-1} < \alpha^{-j}.$$

Innentől $a = 1$.

A Baker-Wüstholz tétel miatt

$$\exp(-2.184 \cdot 10^{12} \log(j)) < |j \log((1 + \theta)/\alpha) - k \log(\alpha + \theta)|.$$

Összehasonlítva az alsó és a felső korlátokat

$$j \log \alpha < 2.184 \cdot 10^{12} \log(j),$$

amelyből $j < 1.5 \cdot 10^{14}$ adódik.

Elosztva az egyenlőtlenségünket $\log(\alpha+\theta)$-val a $\delta = \frac{\log((1+\theta)/\alpha)}{\log(\alpha+\theta)}$ jelöléssel kapjuk:

$$0 < |j\delta - k| < \alpha^{-j}/\log(\alpha+\theta).$$

A δ lánctört-előállítása
$[0, 2, 6, 2, 20, 4, 2, 1, 2, 1, 2, 2, 7, 13, 6, 33, 1, 7, 3, 4, 1, 3, 1, 7, 21, \ldots]$
és a 25-dik közelítő tört nevezője $q_{25} > 1.5 \cdot 10^{14}$.

A közelítő törtek extremális tulajdonsága miatt

$$6.5 \cdot 10^{-14} < |p_{25}\delta - q_{25}| < |j\delta - k| < \alpha^{-j}/\log(\alpha+\theta),$$

amelyből $j < 72$. Háromszori iteráció után $j < 13$-at kapunk.

Probléma: *A tribonacci sorozatot a* $T_0 = T_1 = 0, T_2 = 1$ *kezdőértékekkel és a*

$$T_{n+3} = T_{n+2} + T_{n+1} + T_n,\ n \geq 0$$

rekurzióval definiáljuk. Igaz-e, hogy a tribonacci sorozatban csak $T_0 = T_1 = 0, T_2 = T_3 = 1, T_5 = 4, T_{10} = 81, T_{16} = 3136 = 56^2$ *és* $T_{18} = 10609 = 103^2$ *a négyzetszámok?*

3. Tétel. *[Pethő (2001)] A* T_n *sorozatnak csak véges sok olyan tagja van, amelyik teljes hatvány.*

4. Numerikus módszer

Legyen $[\mathbb{K} : \mathbb{Q}] = k$ jelölje $\alpha^{(1)}, \ldots, \alpha^{(k)}$ az $\alpha \in \mathbb{K}$ konjugáltjait és $\mathbb{Z}_{\mathbb{K}}$ a $\mathbb{K}$ egészeinek a gyűrűjét. Legyenek $\varepsilon_1, \ldots, \varepsilon_r$ független egységek $\mathbb{Z}_{\mathbb{K}}$-ban.

4.1. Általános stratégia (Pethő (1990))

1.) (Problémafüggő) Transzformáljuk az eredeti problémát véges sok egységegyenletre. Azaz

$$\alpha_1 \left(\varepsilon_1^{(i)}\right)^{n_1} \ldots \left(\varepsilon_r^{(i)}\right)^{n_r} + \alpha_2 \left(\varepsilon_1^{(j)}\right)^{m_1} \ldots \left(\varepsilon_r^{(j)}\right)^{m_r} = 1$$

egyenletre, ahol $1 \leq i < j \leq k; n_h, m_h \in \mathbb{Z}$ és α_1, α_2 rögzített elemek.

2.) Ha $N_0 \leq N = \max\{|n_1|, \ldots, |n_r|\} \leq M = \max\{|m_1|, \ldots, |m_r|\}$, akkor

$$\left|\log \alpha_1 + n_1 \log \varepsilon_1^{(i)} + \cdots + n_r \log \varepsilon_r^{(i)}\right| < c_1 \exp(-c_2 M) \leq c_1 \exp(-c_2 N),$$

ahol c_1, c_2 konstansok.

3.) Baker típusú tétellel felső korlátot (N_1) adunk N-re.

4.) Numerikus diofantikus approximációs módszerrel redukáljuk N_1-et addig, amíg az új korlát N_0 alá csökken.

2.,3. és 4. probléma független!

5.) Keressük meg az N_0-nál kisebb megoldásokat az eredeti probléma specialitásait kihasználva.

4.2. Thue-egyenletek

Legyen $F(x,y) \in \mathbb{Z}[x,y]$ irreducibilis, homogén és $k \geq 3$-ad fokú. Tegyük fel, hogy az x^k tag együtthatója 1. Legyen $0 \neq m \in \mathbb{Z}$, akkor

$$F(x,y) = m$$

Thue-egyenlet.

4. Tétel. *[Bugeand és Győry (1996)] Legyen F együtthatói abszolút értékének maximuma H. Akkor az előbbi Thue-egyenlet minden megoldására teljesül*

$$\max\{|x|,|y|\} < \exp\left\{3^{3(k+9)}k^{18(k+1)}H^{2k-2}(\log H)^{2k-1}\log^*|m|\right\},$$

ahol $\log^*|m| = \max\{\log|m|, 1\}$.

• Pethő és Schulenberg (1985): Fortran program, amikor $F(x, 1)$ minden gyöke valós, $m = 1$.

• Pethő (1987): Kis megoldások meghatározása lánctörtredukcióval. $\rightarrow$ Thue-egyenletek megoldása

$$O(3^{6(k+9)}k^{36(k+1)}H^{4(k-1)}(\log H)^{4k-2}(\log^* |m|)^2)$$

időben meghatározható.

• Tzanakis és de Weger (1989): Általános, 1 egyenlőtlenséget használ a redukcióhoz.

• Bilu és Hanrot (1996): Általános, kihasznál minden egyenlőtlenséget. $\rightarrow$ Lehmer-probléma megoldásánál 260-ad fokú Thue-egyenletet oldottak meg!

• Implementáció: KASH, MAGMA, PARI

E. Thomas (1990) bizonyította: ha $a \geq 1.365 \cdot 10^7$, akkor az

$$x^3 + (a-1)x^2y - (a-2)xy^2 + y^3 = 1$$

egyenletnek csak $(1,0), (0,1), (-1,-1)$ a megoldásai.

Mignotte (1990) kiterjesztette minden a-ra.

5. Tétel. *[Mignotte, Pethő, Lemmermeyer (1996)] Legyenek* $a \geq 1650$ *és* k *egészek. Ha* $x, y \in \mathbb{Z}$ *megoldásai az*

$$|x^3 + (a-1)x^2y - (a-2)xy^2 + y^3| \leq k$$

egyenletnek, akkor

$$\log |y| < 1957 \log^2(a+2) + 31 \log a \log k.$$

$k = 2a + 1$-re meghatároztuk az összes megoldást.

Legyen $a \neq (-1 \pm 3\sqrt{-3})/2$ egy imaginárius másodfokú egész szám és μ egységgyök $\mathbb{Q}(a)$-ban. Heuberger, Pethő és Tichy (2006) meghatározták az

$$x^3 + (a-1)x^2y - (a-2)xy^2 + y^3 = \mu$$

egyenlet összes $x, y \in \mathbb{Z}_{\mathbb{Q}(a)}$ (756) megoldását is.
Ha $a = (-1 \pm 3\sqrt{-3})/2$, akkor az egyenletnek minden $\mu \in \mathbb{Q}(\sqrt{-3})$ egységgyökre végtelen sok megoldása van.

Heuberger, Jadrijevič, Mignotte, Lettl, Pethő, Tichy, Voutier, Wakabayashi és Ziegler számos parametrizált Thue-egyenletet oldott meg.

6. Tétel. *[Halter-Koch, Lettl, Pethő, Tichy (1999)]*
Legyen $n \geq 3$ *prímszám,* $a_1 = 0, a_2, \ldots, a_{n-1}$ *páronként különböző egészek és* $a_n = a$ *egész paraméter.*
Legyen $\alpha = \alpha(a)$ *a* $P(x) = \prod_{i=1}^{n}(x - a_i) - d,\ d = \pm 1$ *polinom gyöke. Tegyük fel, hogy igaz a Lang-Waldschmidt sejtés. Akkor véges sok kivételével minden* a*-ra a*

$$\prod_{i=1}^{n}(x - a_i y) - dy^n = \pm 1 \tag{1}$$

Thue-egyenlet minden (x, y) *megoldására* $|y| = 1$ *teljesül, kivéve, ha* $n = 3$ *és* $|a_2| = 1$*, vagy ha* $n = 4$ *és* $(a_2, a_3) \in \{(1, -1), (\pm 1, \pm 2)\}$*, amikor (1)-nek még egy további megoldása van.*

Lang-Waldschmidt sejtés

Legyenek $\alpha_1, \ldots, \alpha_k \neq 0, 1$ *algebrai számok és* $b_1, \ldots, b_k \in \mathbb{Z}$ *olyanok, hogy*

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_k \log \alpha_k \neq 0.$$

Akkor

$$\log |\Lambda| > -c \cdot (h_m(\alpha_1) + \cdots + h_m(\alpha_k)) \log B,$$

ahol $B = \max\{|b_1|, \ldots, |b_k|, 3\}$ *és* c *egy* k*-tól és a* $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ *test fokszámától függő konstans.*

4.3. Numerikus diofantikus approximáció

Feladat: *Legyenek* $0 \neq \vartheta_1, \ldots, \vartheta_r \in \mathbb{C}$, $\vartheta_{r+1} \in \mathbb{C}$, $c_1, c_2, B_0 \in \mathbb{R}$. *Határozzuk meg azokat a* $b_1, \ldots, b_r, b_{r+1} \in \mathbb{Z}$, *amelyekre*

$$B = \max_{1 \leq j \leq r+1} \{|b_j|\} \leq B_0 \qquad \text{és} \tag{2}$$

$$\left| \sum_{j=1}^{r} b_j \vartheta_j + \vartheta_{r+1} + b_{r+1} \right| < c_2 \exp\{-c_1 B\} \tag{3}$$

egyidejüleg teljesül.

I. eset. $r = 1$, $\vartheta_1 \in \mathbb{R}$, $\vartheta_2 = 0$. Határozzuk meg a ϑ_1 közelítő törtjeit $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$, amíg $q_n > B_0$ nem teljesül. Akkor $|b_1|, |b_2| \leq B_0 < q_n$ és

$$|p_n - q_n\vartheta_1| < |b_1\vartheta_1 + b_2| < c_2 \exp\{-c_1 B\}$$

igaz a közelítő törtek extremális tulajdonsága miatt. Így

$$B < \frac{1}{c_1} \log\left(c_2 |p_n - q_n\vartheta_1|^{-1}\right).$$

II. eset $r \geq 1$, $\vartheta_{r+1} \neq 0$ Baker és Davenport (1968), Pethő és Schulenberg (1987). A lemmában $\|x\|$ jelöli az $x \in \mathbb{R}$-hez legközelebbi egész számot.

1. Lemma. *[]Legyen $C > B_0^r$. Tegyük fel, hogy vannak olyan $D \in \mathbb{R}$, $q, p_1, \ldots, p_r \in \mathbb{Z}$, amelyekre $1 \leq q \leq DC$,*

$$\begin{aligned} |q\vartheta_j - p_j| &< \frac{1}{DC^{1/r}}, \qquad j = 1, \ldots, r \\ \|q\vartheta_{r+1}\| &\geq \frac{2r}{D}. \end{aligned}$$

igaz. Akkor

$$B \leq \frac{1}{c_1} \log \frac{D^2 C c_2}{r}$$

teljesül a (2), (3) *egyenlőtlenségrendszer minden* $(b_1, \ldots, b_{r+1})^T \in \mathbb{Z}^{r+1}$ *megoldására.*

III. Általános eset:

2. Lemma. *[Lenstra, Lenstra, Lovász (1982)] Legyenek* $\vartheta_1, \ldots, \vartheta_r \in \mathbb{Q}$ *nullától különböző elemek,* $Q > 2^{r(r+1)/4}$ *egész szám. Az* LLL*-algoritmust alkalmazva olyan* $p_1, \ldots, p_r, q$ *egészeket kapunk, hogy* $p_1, \ldots, p_r$ *nem mind* 0 *és*

$$|p_i| \leq Q, \qquad 1 \leq i \leq r, \tag{4}$$

$$\left| \sum_{i=1}^{r} p_i \vartheta_i + q \right| \leq 2^{r^2(r+1)/4} Q^{-n}. \tag{5}$$

Bizonyítás Legyenek $C = 2^{-r(r+1)^2/4} Q^{r+1}$,
$\mathbf{b}_i = \mathbf{e}_i + (0, \ldots, 0, C\vartheta_i)^T$, $i = 1, \ldots, r$ és $\mathbf{b}_{r+1} = C\mathbf{e}_{r+1}$.
Alkalmazzuk a $\mathbf{b}_1, \ldots, \mathbf{b}_{r+1}$ bázisú $\mathcal{L}$ rácsra az LLL-algoritmust.

Legyen $Q = DB_0, D \geq 1$.
Ha $0 \neq (b_1, \ldots, b_{r+1})^T \in \mathbb{Z}^{r+1}$ a (2), (3) egyenletrendszer megoldása, akkor $\mathbf{b} = (b_1, \ldots, b_r, \sum_{j=1}^{r} b_j C\vartheta_j + Cb_{r+1})^T \in \mathcal{L}$.
A $\mathcal{L}$ egy LLL-bázisa alsó korlátot ad a $\mathcal{L}$ legrövidebb nullától különböző elemének hosszára

$$\lambda(\mathcal{L}) \geq 2^{-r/2}|\mathbf{a}_1|.$$

Másrészt

$$\lambda(\mathcal{L})^2 \leq |\mathbf{b}|^2 \leq rB_0^2 + C^2 \left(\sum_{j=1}^{r} b_j \vartheta_j + b_{r+1} \right)^2$$
$$\leq rB_0^2 + C^2 c_2^2 \exp\{-2c_1 B\}.$$

Ha tehát $2^{-r}|\mathbf{a}_1|^2 - rB_0^2 > 0$ - amelyet a D megfelelő megválasztásával el lehet érni - akkor

$$B \leq \frac{1}{c_1} \log(Cc_2(2^{-r}|\mathbf{a}_1|^2 - rB_0^2)^{-1/2}).$$

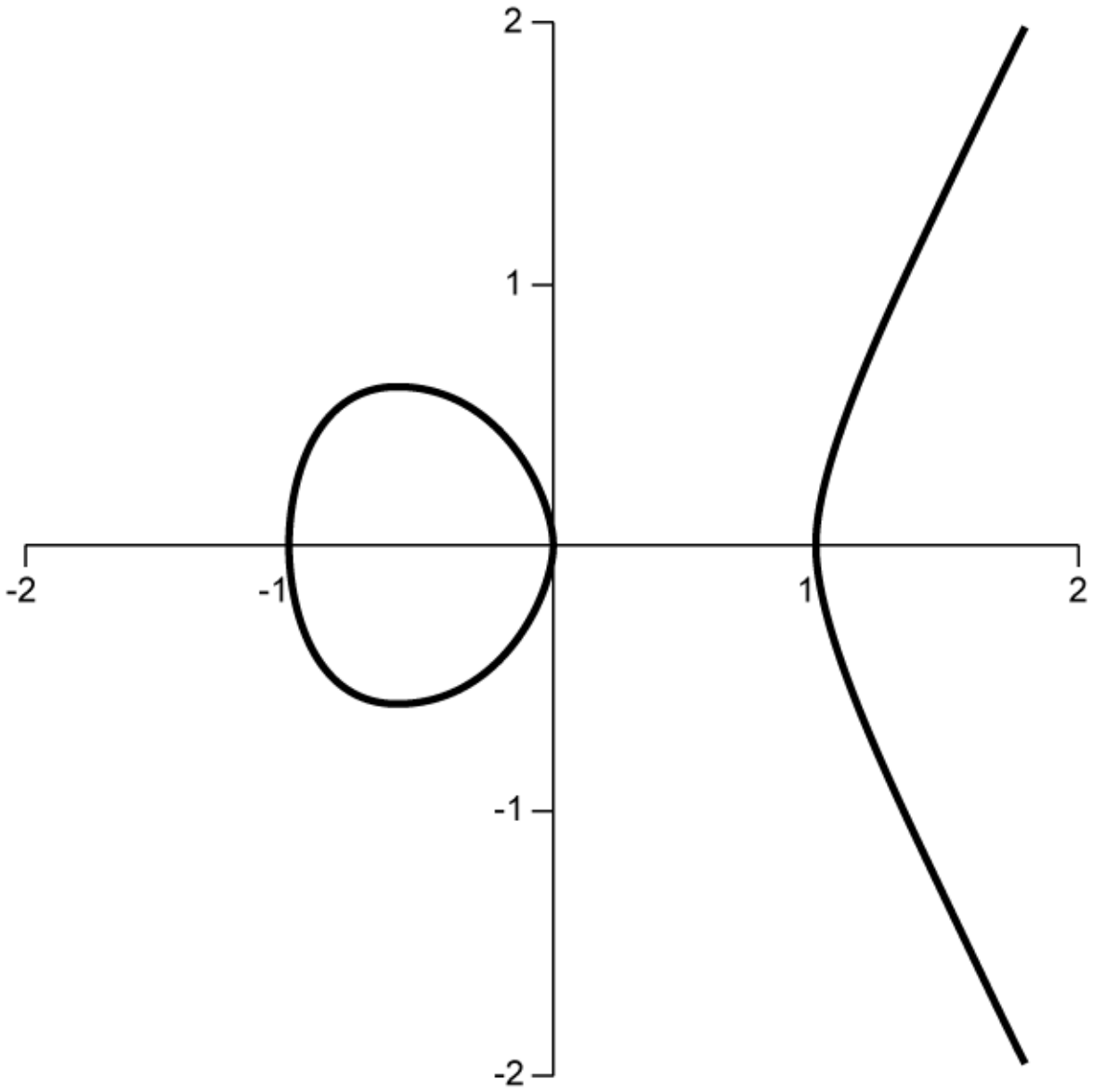
4.4. Elliptikus egyenletek

Legyen K egy test, $A, B \in K$.

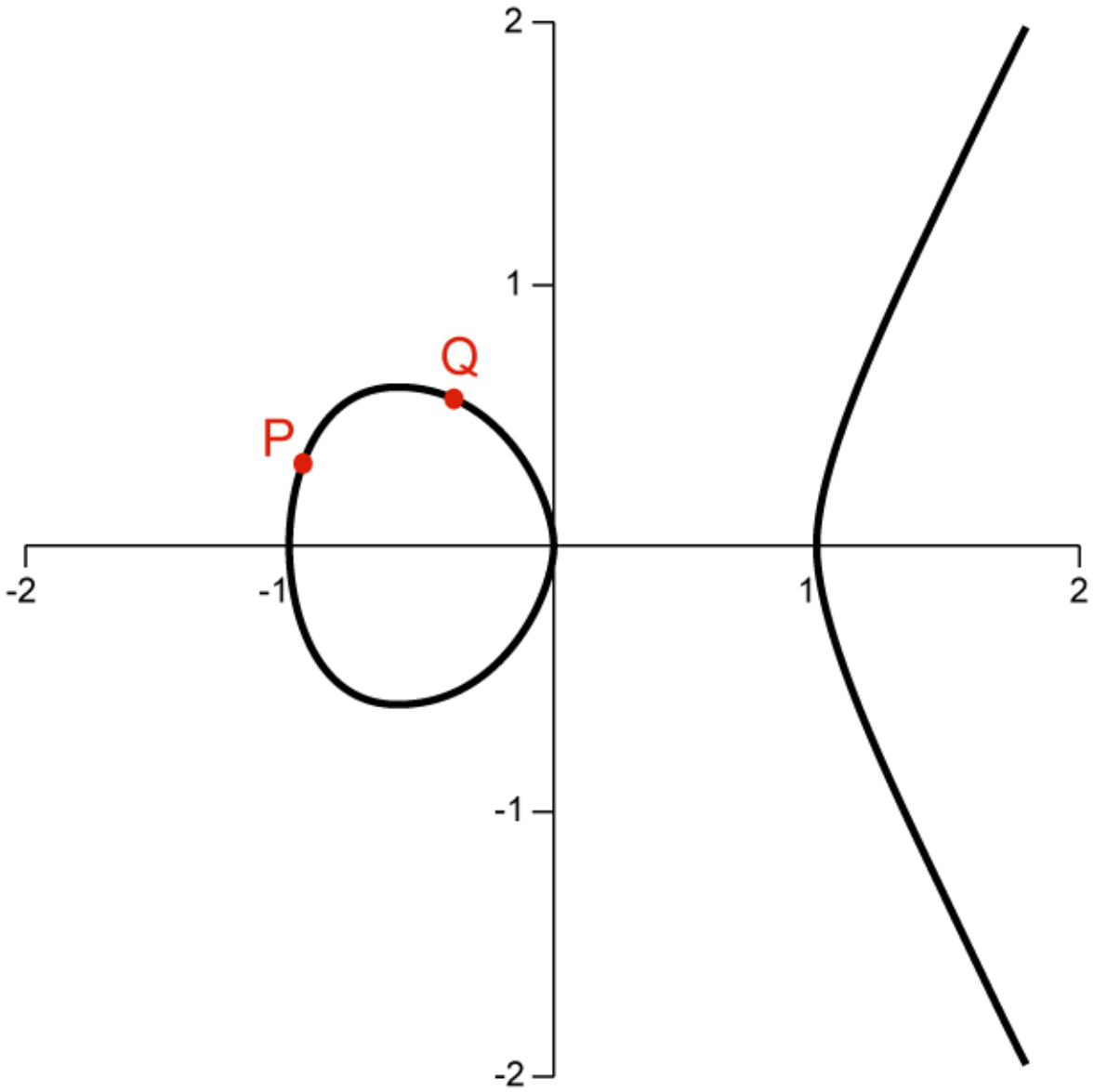
$$E(K) = \{(x, y) \in K^2 \ : \ y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

halmazt K feletti elliptikus görbének nevezzük.
$E(\mathbb{Z}) = E \cap \mathbb{Z}^2$ az E-re illeszkedő egész pontok halmaza $\rightarrow$ elliptikus egyenlet.

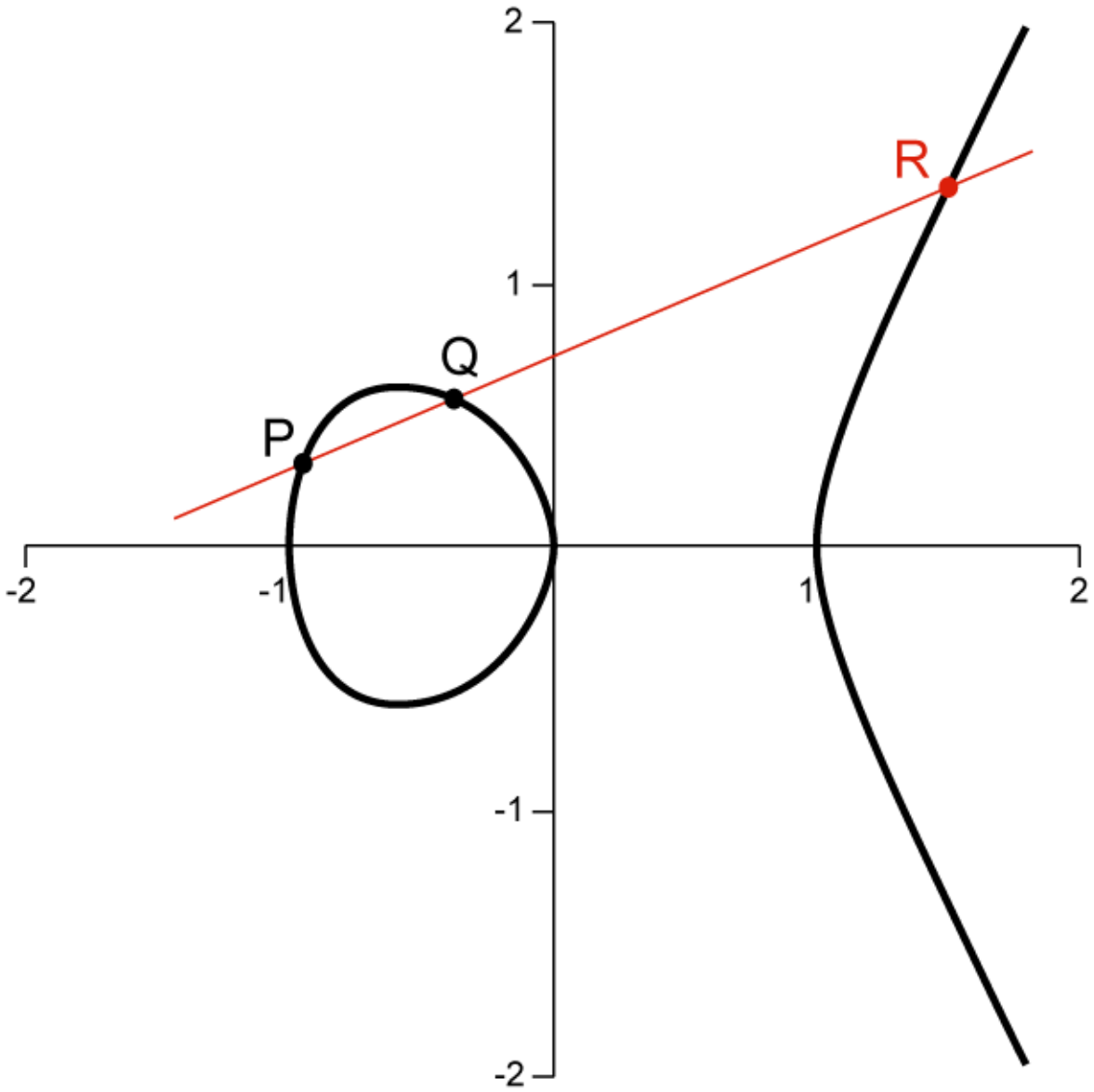
Az elliptikus logaritmus módszer $E(\mathbb{Z})$ meghatározásához
$E(\mathbb{Q}) \subset E(\mathbb{R}) \subset E(\mathbb{C})$ tulajdonságait használja fel.



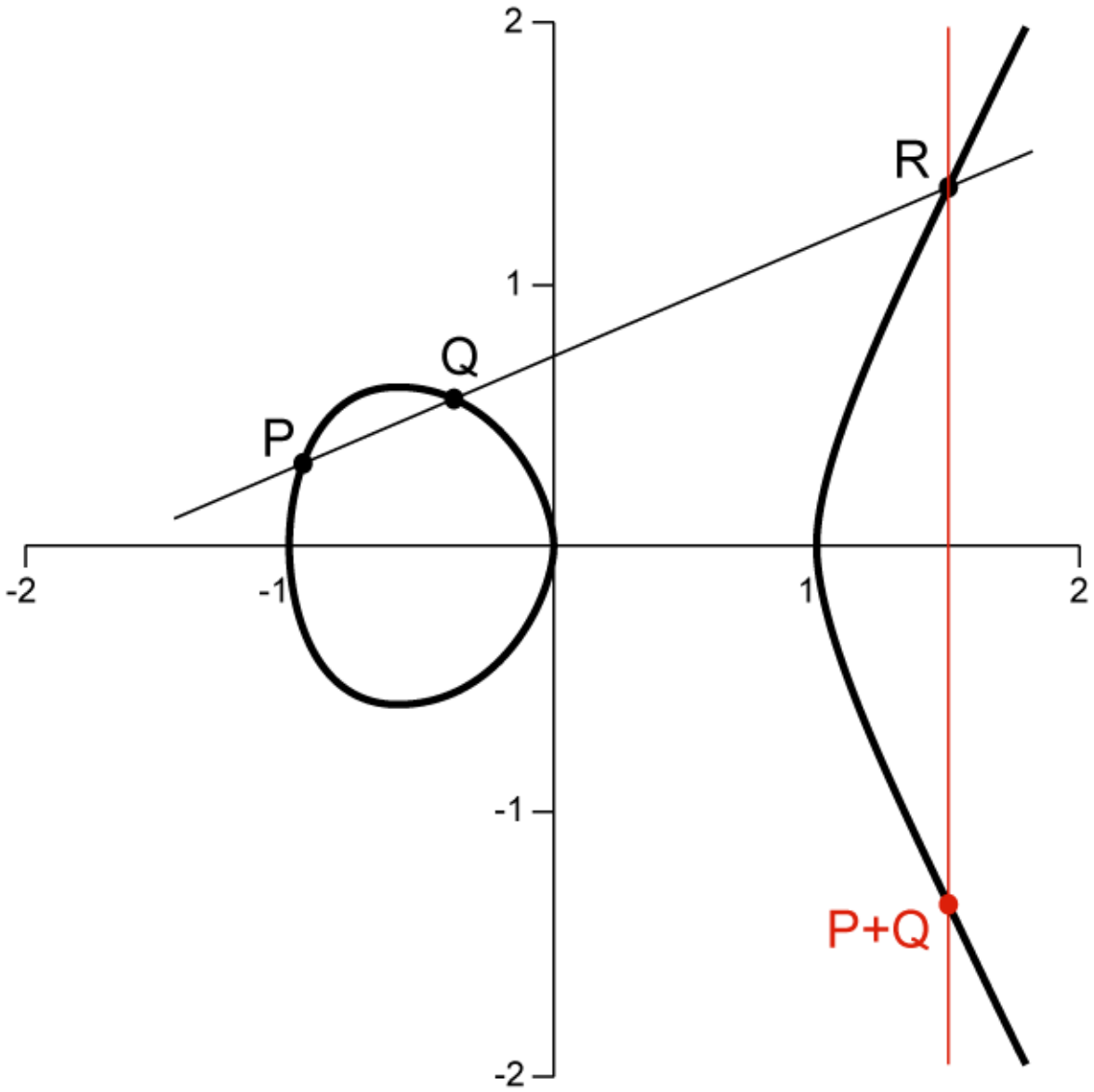
Összeadás az $y^2 = x^3 - x$ görbén $K = \mathbb{R}$-re. 1. lépés.



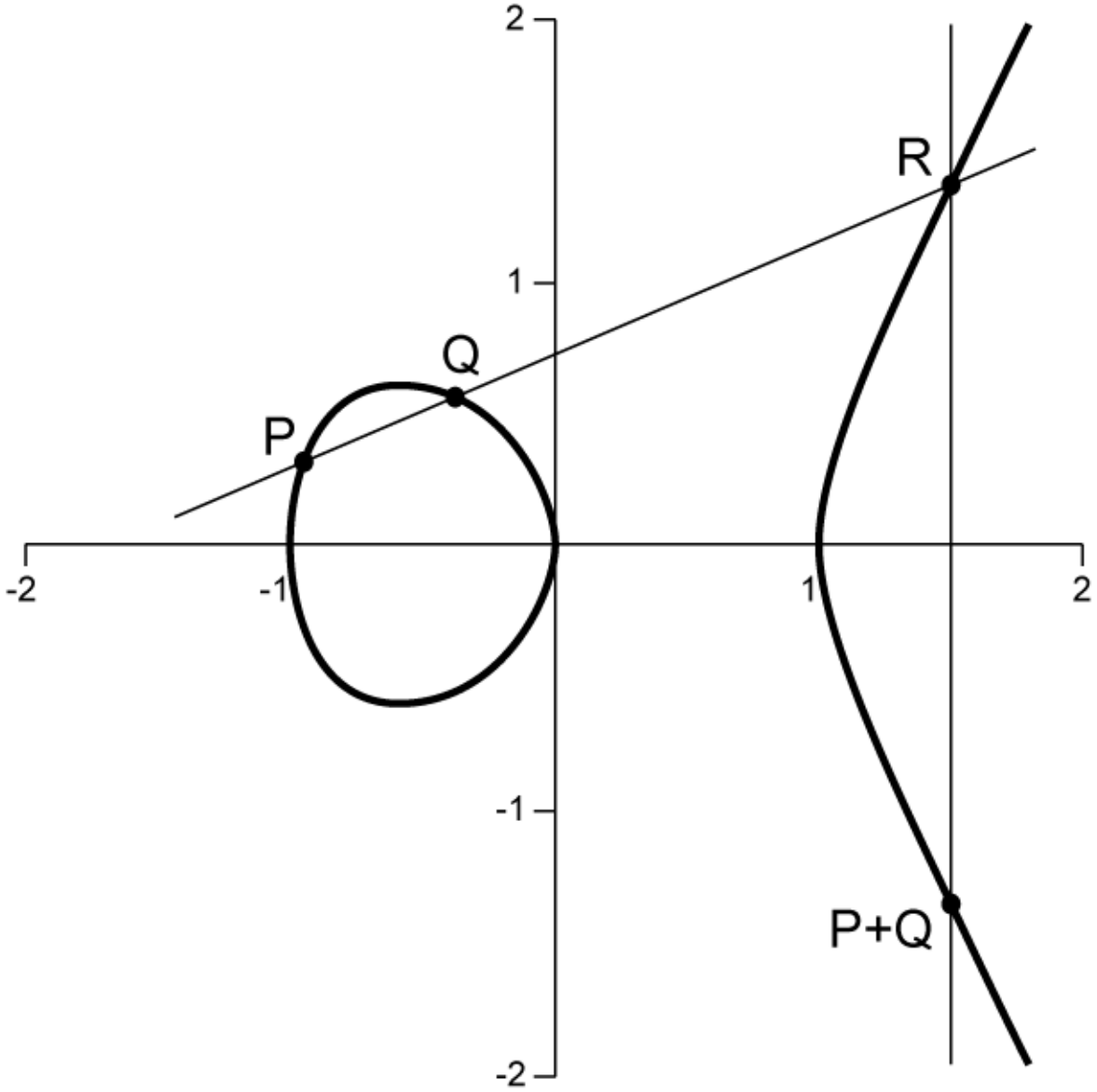
Összeadás az $y^2 = x^3 - x$ görbén $K = \mathbb{R}$-re. 2. lépés.



Összeadás az $y^2 = x^3 - x$ görbén $K = \mathbb{R}$-re. 3. lépés.



Összeadás az $y^2 = x^3 - x$ görbén $K = \mathbb{R}$-re. 4. lépés.



Összeadás az $y^2 = x^3 - x$ görbén $K = \mathbb{R}$-re. 5. lépés.

7. Tétel. *[Mordell-Weil] Ha K egy algebrai számtest, akkor $< E(K), + >$ egy végesen generált Ábel-csoport. Tehát vannak olyan $P_1, \ldots, P_r \in E(K)$, hogy bármely $P \in E(K)$-hoz vannak $n_1, \ldots, n_r \in \mathbb{Z}$ és $T \in E(K)$ véges rendű elem, hogy*

$$P = T + n_1 P_1 + \cdots + n_r P_r.$$

Weierstraß klasszikus eredménye szerint minden $E(\mathbb{C})$-hez van olyan $\wp(z)$ komplex függvény, amelyre

$$E(\mathbb{C}) = \{(\wp(z), \wp'(z)) \ : \ z \in \mathbb{C}\}.$$

A $\wp$ Weierstraß-függvény duplán periodikus. Két, független minimális periódusa ω_1, ω_2 egy paralellogrammát - Λ - határoz meg a komplex számsíkon.

Teljesülnek a következők:

• Bármely $P = (x, y) \in E(\mathbb{C})$-hez van *egyértelműen meghatározott* $t \in \Lambda$ úgy, hogy $x = \wp(t), y = \wp'(t)$.

• A $t = u(P)$ függvényt elliptikus logaritmusnak nevezzük.

• Ha $P_1, P_2 \in E(\mathbb{C})$ és $t_1 = u(P_1), t_2 = u(P_2)$, akkor $u(P_1 + P_2) = t_1 + t_2$ mod Λ.

8. Tétel. *[Gebel, Herrmann, Pethő, Zimmer (1999)] Legyen*

$$P = (x, y) = T + n_1 P_1 + \cdots + n_r P_r \in E(\mathbb{Z})$$

és $N = \max\{|n_1|, \ldots, |n_r|\}$. *Akkor*

$$N \leq N_1 \leq \sqrt{(k_1 + k_2)/\lambda}.$$

Ha még $|x| > x_0$ *is teljesül, akkor van olyan* $n_{r+1} \in \mathbb{Z}$, *hogy*

$$|n_1 u(P_1) + \cdots + n_r u(P_r) + n_{r+1}| \leq k_3 \exp(-\lambda N^2/2 + (k_1 + \log 2)/2).$$

A fentiekben

$$k_1 = \log \max\{|2A|^{1/2}, |4B|^{1/3}\}, \quad k_2 = 5 \cdot 10^{64} \cdot k_2(A, B)$$

és λ, k_3 *a görbétől,* $k_2(A, B)$ *csak* A *és* B*-től függő konstansok.*

A bizonyításban fontos szerepet játszott Hajdu és Herendi (1998) egy eredménye.

- Alapötlet: S. Lang (1964), D. Zagier (1987)
- Alsó korlát elliptikus logaritmusokból képzett lineáris formákra. S. David (1995)
- Racionális eset: Stroeker és Tzanakis valamint Gebel, Pethő és Zimmer (1994)
- S-egész pontok: Gebel, Herrmann, Pethő, Zimmer (1999)
- Implementáció: SIMATH, MAGMA

9. Tétel. *[Gebel,Pethő,Zimmer(1998)] Az* $y^2 = x^3 + k$ *Mordell egyenlet minden* $x, y \in \mathbb{Z}$ *megoldására teljesül, hogy*

$$
\begin{aligned}
|x| &\leq 110\ 781\ 386, \textit{ha}\ 0 < k \leq 10\ 000\ (k = 8\ 569) \\
|x| &\leq 6\ 369\ 039, \textit{ha}\ 0 > k \geq -10\ 000\ (k = -7\ 670) \\
|x| &\leq 3\ 790\ 689\ 201, \textit{ha}\ 0 < k \leq 100\ 000\ (k = 28\ 024) \\
|x| &\leq 3\ 171\ 881\ 612, \textit{ha}\ 0 > k \geq -100\ 000\ (k = -64\ 432).
\end{aligned}
$$

Az állítás $k = 7823$*-ra és* $|k| > 10\ 000$*-re csak a Birch és Swinnerton Dyer sejtés mellett igaz.*

Miért nem tudtuk megoldani az $y^2 = x^3 + 7823$ *egyenletet?*

- *A görbe rangja* 1, *de bázisának magassága igen nagy.*
- *A* $\mathbb{Q}(\sqrt{7823})$ *alapegysége:*

$$785263060418685068630050794 88+88782731643283356194423195 29\sqrt{7823}$$

- *A* $\mathbb{Q}(\sqrt[3]{7823})$ *alapegysége:*

$$
\begin{aligned}
&208399981911487168690387163002166487651591965014819930628143805363058341543647236666884578970673416349040119362326561305568880508738966902319776111670292648802993388311506529912783213771157522388019086949628971551424042659566131334476167845203055319563651408640396973678652003699599666656992564871239247581563459975027682884938838956345192448887561081917368569214320205162297891694644340572192161077979973592441653194336998769333323406115893349439952825409164289725634832715941712935408754291537908503459228364548333830266140875568306853472282879498264780603612045057582094895010329122654594233035293518993285818521253422182408778048266747217852326985693815725946772035264295729469025818346235133937719790337114455030110595666569420759195519750319296860661005475439924205927041527754705431789664943971114256796344613657594615412858454439026762492493020449824236577957341884193823349839832078508652094150099864111302793228016054708119340452602064720266451591650727517647162149951526347966253963327088964168093863653462776052073685276986635729698649063087838976949020903924853869758455280037066733199549850345428676559403576648041451015291944556829533718410529320531872693775092013828122883427258825645367670270303886624852346425059224420132143274310595795080326700671789927312955190540154966016408270952405094956365477167861027189889865373367013744161662606903491869183352 + 109727557035788192103578244433107312850514715670914396468792049390701002750882554736583209505430033931217624912929970326741887428355072121620768766037171877556725353735030247963186556463569277649467259212867832453161906925247416224321532209549815063669990318459910159856655622943382780666744926218615332043493420280724877659601826732855403423112036307207159315377327297854545342347476851041072882695231197172449156261301241368195810891114589421319627645209333063826949136057433668682012095383135642233969121157331312795754100826318872653734776220280554251832683000867339158718678705446246275089377244751518791655478786966541683505837290726953797281573934593754336867267377862400320312462518065827977848442797127712360014787044493128747400297737231040647023420123337893532
$$

$$
\begin{aligned}
&1559294332420721750280159273078536841930854957259477436292320538889093973586941171412340950289594707812253766768199984941189499629756288008304686552268955472875118345736176979065535459181165327356972036683032449402982829088781909780813817682432810466810887177417142294256204259596086325335867866923457703728556375035709173003011418014439963794249677453387803276064625570019158711482351225855655940481203916829111550144069042154329842330256629577627416790825698734335827047992445449010731215738886186377080688182698423312737836836508652983728168783060428698314765461732012190966403291794392034870 6\theta \\
&+ 4735547642383422487799072684595439737493794497719550937152719602378702359861569332318030739696224642597955314792312408817261070891771055142613056312857008346940100673806496608461565866534864181246638209200769583519950394777250001454651606732060288379588360095925255733996876620231058338986034597557868377625628257267379489942853943291833006886081901478465251245969261429882215168044616261811372403145214403103084663098902072450488610694876615988048546409780681839715170228725815222055648833453717878639558208938525254441307651532530745055607288843070877203376036121926970012779708713836287441701356372795448964485885521950671695815658843037457850586609486177289448172639248058350809025108782074348511220147279698562998123039688176868616057655387945883757905779035131261846336898554341076374539628165532752385616431377612561855644527520762963868638771703835984484765972335341873696670307412122183630830408677691833605181050699084085204627144852780507276393682788635992021218721892038223711495358433110166136130064277290410706221578813873532886961693168336986647897903258924992668804217972512600537296771798288283824478910216486993804775094516579338502785031014958498371988564525202210321098298751795219787737537175731575382400395138149502461347224721797326551053710378126809431320617143432770004118122195027943838816951552098780276466921154982831935780892083133823818 8\theta^2,
$$

$$
\mathit{ahol}\ \theta = \sqrt[3]{7823}.\ \ \mathit{(Klaus\ Wildanger)}
$$

M. Stoll (2002).

"I proudly present the generator of the Mordell-Weil group of $y^2 = x^3 + 7823$ *:*

$$\begin{aligned} x &= 2263582143321421502100209233517777 \\ &/ \quad 11981673410095561^2 \\ y &= -18639815258462330562483755148559677002814477665575 6 \\ &/ \quad 11981673410095561^3 \end{aligned}$$

This point has canonical height 77.617773768638... *as expected."*

Ezzel a Mordell-egyenletre vonatkozó eredményünk $|k| < 10\ 000$*-re teljessé vált.*

5. Hozadék

a) *Kölcsönhatás a komputeralgebra-rendszerek fejlesztésével.*

•• *Nagy pontosságú (több ezer számjegyig) egész, lebegőpontos és p-adikus aritmetika.*

•• *Algoritmusok polinomok gyökeinek, komplex, p-adikus, elliptikus, p-adikus elliptikus logaritmus közelítő számítására.*

•• *Algebrai számelméleti algoritmusok: műveletek, egészbázis, maximális független egységrendszer.*

•• *Elliptikus görbéken: Pontok összeadása, magasságuk számítása, Mordell-Weil csoport bázisának meghatározása.*

•• *Numerikus diofantikus approximációs algoritmusok: lánctört, Lenstra, Lenstra, Lovász algoritmus.*

b) *Sok egyenlet számítógéppel automatikusan megoldható (Bazsó, Bérczes, Győry, Hajdu, Pintér, Rakaczky, Tengely).*
Árnyoldal: a felhasználók sokszor formálisan, de nem tudatosan használják a számítógépes eljárásokat. Ha a gép nem tudja megoldani az egyenletüket, akkor nem tesznek erőfeszítést egyedi eljárás kidolgozására. Pedig az ilyen problémák jelentik ma az igazi intellektuális kihívást.

c) *Nagy táblázatok készültek: Mordell-egyenlet, index forma egyenletek (Gaál, Nyúl G., Olajos, Járási, Pohst), John Cremona: Elliptic curve data, William Stein: modular forms database.*

d) *Megváltozott az elképzelésünk a vizsgált diofantikus egyenletek megoldásainak eloszlásáról: Nagyon ritka a "nem triviális" megoldás.*

e) *Szimultán diofantikus approximáció szempontjából az algebrai számok logaritmusai úgy viselkednek, mint a tipikus valós számok.*

Köszönöm a megtisztelő figyelmet!