$x^2 - my^2 = 1$, $m > 0$ <u>nem</u> négyzetszám : Pell - egyenlet.

<u>Tétel</u> $m>0$ egész, nem négyzet $\Rightarrow$ a Pell-egyenletnek $\exists\ \infty$ sok mo.-a. $\mathbb{Z}$-ben

<u>Biz.:</u> $x^2 - my^2 = 1 \iff \left(\frac{x}{y}\right)^2 - m = \frac{1}{y^2}$

$$\left(\frac{x}{y} - \sqrt{m}\right)\left(\frac{x}{y} + \sqrt{m}\right) = \frac{1}{y^2}$$

$$\frac{x}{y} - \sqrt{m} = \frac{1}{y(x+\sqrt{m}\,y)}$$

múlt órán: $\alpha \in \mathbb{R}$ irrac. $\Rightarrow \exists\ \infty$ sok $p_j, q_j \in \mathbb{Z}$

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^2}$$

$$\left|p_j^2 - q_j^2 m\right| = \Big|\underbrace{q_j^2\left(\frac{p_j}{q_j} - \sqrt{m}\right)}_{|\quad\quad|<1}\left(\frac{p_j}{q_j} + \sqrt{m}\right)\Big| < \left|\frac{p_j}{q_j} + \sqrt{m}\right|$$

$$< 2\sqrt{m} + 1$$

$$\Rightarrow \quad \exists \ |t| < 2\sqrt{m} + 1 \quad \infty \text{ sok } j\text{-re}$$

$$p_j^2 - q_j^2 m = t. \qquad t \text{ rögz.}$$

$$\exists^{\infty} \text{ sol } (p_j, q_j) \qquad p_i \equiv p_j \quad (|t|)$$

$$q_i \equiv q_j \quad (|t|)$$

$$p_1^2 - q_1^2 m = t = p_2^2 - q_2^2 m \quad , \quad p_1 \equiv p_2 \quad , \quad q_1 \equiv q_2 \quad (|t|) \Longrightarrow$$

$$A + B\sqrt{m} = \frac{p_1 + q_1\sqrt{m}}{p_2 + q_2\sqrt{m}} = \frac{(p_1 + q_1\sqrt{m})(p_2 - q_2\sqrt{m})}{p_2^2 - q_2^2 m} = \frac{(p_1 p_2 - m q_1 q_2) + (q_1 p_2 - p_1 q_2)\sqrt{m}}{t}$$

$$p_1 \equiv p_2 \qquad q_1 \equiv q_2 \quad (|t|)$$

$$p_1 p_2 - m q_1 q_2 \equiv p_1^2 - m q_1^2 = t \equiv 0 \quad (|t|)$$

$$q_1 p_2 - p_1 q_2 \equiv 0 \quad (|t|)$$

$(A, B) \in \mathbb{Z}^2$ megoldása a Pell-egyenletnek. $\Rightarrow$ ∞ sok van. ∎

$\sqrt{m} \notin \mathbb{Q} \Rightarrow (p_1, q_1)$ végt. $\Rightarrow (p_2, q_2)$ fut.

! itt m nem négyzet.

Összes m.o.?

$\mathbb{Z}[\sqrt{m}]$-ben az 1-normájú elemek.

Ábel-csoport a szorzásra.

$$H = \left\{ a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}] \;\middle|\; N(a+b\sqrt{m}) := a^2 - b^2 m = 1 \right\}$$

<u>Tétel</u> $H \simeq \underbrace{\mathbb{Z}}_{\text{generátora}} \times \underbrace{C_2}_{\{\pm 1\}}$

generátora: $x_0, y_0 > 0$, $x_0 + \sqrt{m}\, y_0 \in H$, $(\,> 1)$ minimális.

Azaz H minden eleme (egyértelműen) írható $\pm (x_0 + \sqrt{m}\, y_0)^k$ alakba.

$k \in \mathbb{Z}$.

Biz.: $1 < x_0 + \sqrt{m}\, y_0$ ∞ rendű

$\pm (x_0 + y_0\sqrt{m})^k$ mind ilye.

$1^2 - 1^2 m \neq 1$.

$\alpha = x + y\sqrt{m} \in H$ $\quad (x^2 - y^2 m = 1) \Rightarrow \alpha$ ilyen alakú.

$\alpha > 0$ feltehető.

$$\exists \quad (x_0 + y_0\sqrt{m})^k \leq \alpha < (x_0 + y_0\sqrt{m})^{k+1}$$

$\alpha = (x_0 + y_0\sqrt{m})^k$ ✓

Tfh. $1 < \underbrace{\frac{\alpha}{(x_0 + y_0\sqrt{m})^k}}_{\in H} < x_0 + y_0\sqrt{m}$ $\quad \frac{\alpha}{(x_0 + y_0\sqrt{m})^k} = x_1 + y_1\sqrt{m}$.

$$0 < x_1 - y_1\sqrt{m} = \frac{1}{x_1 + y_1\sqrt{m}} < 1 < x_1 + y_1\sqrt{m} \Rightarrow y_1 > 0.$$

$$\Rightarrow x_1 > 0.$$ y, mert

$$\frac{\alpha}{(x_0 + y_0\sqrt{m})^2} = \alpha (x_0 - y_0\sqrt{m})^2 \in \mathbb{Z}[\sqrt{m}]$$ $\square$

$\mathbb{Q}(\sqrt{m})$ algebrai egészei $\supseteq \mathbb{Z}[\sqrt{m}]$

Ha m négyzetmentes

$$m \equiv 2,3 \ (4) \Rightarrow \mathbb{Z}[\sqrt{m}] = \overline{\mathbb{Z}} \cap \mathbb{Q}(\sqrt{m})$$

$$m \equiv 1 \ (4) \Rightarrow \mathbb{Z}\left(\frac{\sqrt{m}+1}{2}\right) = \overline{\mathbb{Z}} \cap \mathbb{Q}(\sqrt{m})$$

Tétel $K = \mathbb{Q}(\sqrt{m})$, $\mathcal{O}_K := \overline{\mathbb{Z}} \cap K$. $\mathcal{O}_K^\times$ $\to$ vég. generált, **rangja** 1.

$$\mathcal{O}_K^\times = \{\pm 1\} \times \mathbb{Z}$$

A vég. gen. Abel-csoport $\overset{\text{alaptétel}}{\Longrightarrow}$ $\bigoplus_j \mathbb{Z}/(p_j^{\alpha_j}) \oplus \bigoplus_{i=1}^{r} \mathbb{Z}$

rang: r.

$K/\mathbb{Q}$ tetsz. véges bővítés, $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K$.

$$\mathcal{O}_K^\times = \mu(K) \times \mathbb{Z}^{r+s-1}$$

Dirichlet tétele

$\mu(K)$: K-beli egységgyökök

$K = \mathbb{Q}(\alpha)$

α min. $f(x) \in \mathbb{Q}[x]$

f-nek r db valós, s pár komplex gyöke

Tétel (Liouville) $\alpha \in \overline{\mathbb{Q}} \cap \mathbb{R}$ n-edfokú $\Rightarrow \exists\, c > 0$.

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n} \quad \forall\, p, q \in \mathbb{Z}, \; q \neq 0$$

Tétel (Thue) (NB) $\alpha \in \overline{\mathbb{Q}} \cap \mathbb{R}$ n-edfokú $\Rightarrow$

(Roth $\forall \varepsilon > 0$ $\exists\, c = c(\varepsilon, \alpha) > 0$ $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^{2+\varepsilon}}$)

$\forall\, c > 0$ csak véges sok $(p, q) \in \mathbb{Z}^2$ pár van, amire

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^n}.$$

Köv.: $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$ irreducibilis $(a_n \neq 0)$.

$\Rightarrow \forall b \in \mathbb{Z}$-re

$$y^n f\left(\frac{z}{y}\right) = a_0 y^n + a_1 y^{n-1} z + \ldots + a_n z^n = b$$

egyenletnek legfeljebb véges sok mo.-a van.

Biz.: Tfh. (y, z) mo. $\Rightarrow$

$$f\left(\frac{z}{y}\right) = \frac{b}{y^n} \qquad \text{Tfh. } y_i, z_i \in \mathbb{Z} \ \infty \text{ sok mo.}$$

$\Rightarrow y_i$ is ∞ sokféle. $\lim\limits_{i \to \infty} f\left(\frac{z_i}{y_i}\right) = 0$.

$\exists$ részsorozat $(y_i, z_i) \in \mathbb{Z}^2$ párokra, amire $\frac{y_i}{z_i} \longrightarrow \alpha$

$f(\alpha) = 0$.

$$\left|\frac{z_i}{y_i}-\alpha\right| = \left|\frac{f\left(\frac{z_i}{y_i}\right)}{a_n\left(\frac{z_i}{y_i}-\alpha_2\right)\cdots\cdots\left(\frac{z_i}{y_i}-\alpha_n\right)}\right| < \frac{C}{|y_i|^n}$$

$\alpha = \alpha_1 \qquad f(x) = a_n(x-\alpha_1)\cdots\cdots(x-\alpha_n)$ $\qquad$ y (Thue). $\square$

<u>Tétel</u> (Gelfond – Schneider, 1934) $a, b \in \mathbb{C}$ algebrai

függetlenül

$a \neq 0, 1$ és b irracionális $\Rightarrow$ a^b transzcendens.

$$a^b = \exp(b \cdot \log a) \qquad \exp(z) = 1 + z + \frac{z^2}{2!} + \dots + \frac{z^n}{n!} + \dots$$

$$\exp(2\pi i k) = 0. \qquad e^{i\varphi} = \cos\varphi + i\sin\varphi$$

<u>Pl.:</u> 1) $2^{\sqrt{2}} \notin \overline{\mathbb{Q}}$.

2) $(\sqrt{2})^{\sqrt{2}}$ transc., de $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^2 = 2$ alg.

3) $b = \frac{\log 2}{\log 3} \notin \overline{\mathbb{Q}}$ b irrac. Ha $b \in \overline{\mathbb{Q}}$ lenne $\overset{G-Sch.}{\Longrightarrow}$ $3^b = 2$ transzcendens lenne ↯.

4) $e^{\pi} \notin \overline{\mathbb{Q}}$, mert $(e^{\pi})^i = -1$ algebrai. $i \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$

5) $i^i = \left(e^{\frac{\pi i}{2}}\right)^i = e^{-\frac{\pi}{2}} \notin \overline{\mathbb{Q}}$

<u>Tétel</u> (Baker 1967) $\mathbb{L} := \{ \lambda \in \mathbb{C} \mid e^{\lambda} \in \overline{\mathbb{Q}} \}$.

Tfh. $\lambda_1, \dots, \lambda_n \in \mathbb{L}$ lin. ftlen $\mathbb{Q}$ fölött $\Rightarrow$

$1, \lambda_1, \dots, \lambda_n$ lin. ftlen. $\overline{\mathbb{Q}}$ fölött.

[Sőt, $\beta_0, \beta_1, \dots, \beta_n \in \overline{\mathbb{Q}}$ nem mind 0

$$|\beta_0 + \beta_1 \lambda_1 + \dots + \beta_n \lambda_n| > H^{-C}$$

H: csak a β-któl függ

C: n, λ_i-től, β-k fokának max-tól függ.
mindkettő effektív.]

Ie. 7 1) ~~Baker~~ $\Rightarrow$ Gelfond – Schneider: $a \neq 0, 1$, $b \in \overline{\mathbb{Q}}$, $b \notin \mathbb{Q}$. Tfh. $a^b \in \overline{\mathbb{Q}}$ $\qquad \log a$, $\log a^b = b \cdot \log a \in \mathbb{L}$

$\mathbb{Q}$ fölött lin. ftlen: $\qquad \alpha_1, \alpha_2 \in \mathbb{Q}$

$$\alpha_1 \log a + \alpha_2 b \cdot \log a = 0$$

$$b = -\frac{\alpha_1}{\alpha_2} \in \mathbb{Q} \qquad ↯$$

$\Rightarrow 1, \log a, b \log a$ l. ftlen $\overline{\mathbb{Q}}$ fölött.

$$b \cdot \log a - 1 \cdot b \log a = 0. \quad ↯$$

2) $1 \notin \mathbb{L}$, azaz e transzcendens, mert $\{1\}$ l. ftlen $\mathbb{Q}$ fölött, de $(1, 1)$ ÖF $\overline{\mathbb{Q}}$ fölött.

3) $\pi \notin \overline{\mathbb{Q}}$ $\quad e^{\pi i} = -1 \Rightarrow \pi i \in \mathbb{L}$ $\quad \{\pi i\}$ l. FTLEN

$\Rightarrow$ $1, \pi i$ l. Ftlen $\overline{\mathbb{Q}}$ fölött $\Rightarrow$ $\pi i \notin \overline{\mathbb{Q}} \Rightarrow \pi \notin \overline{\mathbb{Q}}$

Az e és a π transzcendens

Ha $f(x) \in \mathbb{C}[x]$, $n = \deg f$, $I_f(t) := \int_0^t e^{t-u} f(u)\,du$

Lemma 1 $I_f(t) = e^t \sum_{j=0}^{\infty} f^{(j)}(0) - \sum_{j=0}^{\infty} f^{(j)}(t)$

Biz.: $\left(-e^{t-u} f(u)\right)' = e^{t-u}\left(f(u) - f'(u)\right)$ parciális integrálás

$$I_f(t) = \left[-e^{t-u} f(u)\right]_{u=0}^{t} - \int_0^t \left(-e^{t-u}\right) f'(u)\,du =$$

$$= e^t f(0) - f(t) + I_{f'}(t)$$ indukció $n = \deg f$-re. $\square$

<u>Lemma 2</u> $$\left| I_f(t) \right| \le |t|\, e^{|t|}\, \tilde{f}(|t|),$$ ahol

$$\tilde{f}(x) := |a_0| + |a_1| x + \dots + |a_n| x^n \quad \left(f(x) = a_0 + a_1 x + \dots + a_n x^n \right).$$

<u>Biz.:</u> Triviális becslés. $\square$