数理解析研究所講究録 1219 巻 2001 年 159-184

The first hundred years of algorithmic theory of diophantine equations

Attila Pethő

Debrecen, Hungary

Kyoto, October 26, 2000

II. International Congress of Mathematicians, Paris
Aug 6.-12. ~~2000~~ 1900
D. Hilbert

7. Irrationality and Transcendence of Certain Numbers.

Hermite's arithmetical theorems on the exponential function and their extension by Lindemann are certain of the admiration of all generations of mathematicians. Thus the task at once presents itself to penetrate further along the path here entered, as A. Hurwitz has already done in two interesting papers,* "Ueber arithmetische Eigenschaften gewisser transzendenter Funktionen." I should like, therefore, to sketch a class of problems which, in my opinion, should be attacked as here next in order. That certain special transcendental functions, important in analysis, take algebraic values for certain algebraic arguments, seems to us particularly remarkable and worthy of thorough investigation. Indeed, we expect transcendental functions to assume, in general, transcendental values for even algebraic arguments; and, although it is well known that there exist integral transcendental functions which even have rational values for all algebraic arguments, we shall still consider it highly probable that the exponential function $e^{i\pi z}$, for example, which evidently has algebraic values for all rational arguments z, will on the other hand always take transcendental values for irrational algebraic values of the argument z. We can also give this statement a geometrical form, as follows:

If, in an isosceles triangle, the ratio of the base angle to the angle at the vertex be algebraic but not rational, the ratio between base and side is always transcendental.

In spite of the simplicity of this statement and of its similarity to the problems solved by Hermite and Lindemann, I consider the proof of this theorem very difficult; as also the proof that

The expression α^{β}, for an algebraic base α and an irrational algebraic exponent β, e. g., the number $2^{\sqrt{2}}$ or $e^{\pi} = i^{-2i}$, always represents a transcendental or at least an irrational number.

It is certain that the solution of these and similar problems must lead us to entirely new methods and to a new insight into the nature of special irrational and transcendental numbers.

10. Determination of the Solvability of a Diophantine Equation.

Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Why formulated Hilbert the 10^{th} problem in positive form ?

Because the notion of algorithm was defined precisely only 30 years later by K. Gödel.

Hilbert's 10^{th} problem: Let $P(x_1, .., x_n) \in \mathbb{Z}[x_1, .., x_n]$. Give an algorithm, which decides whether

$$P(x_1, .., x_n) = 0$$

is solvable or not.

M. Davis, H. Putnam and J. Robinson (1961): Hilbert's 10^{th} problem is unsolvable, if we allow exponential terms $y = a^x$ in the construction of P too.

Theorem (Yu. V. Matijasevich, 1970) There exists a polynomial $P(a_1, .., a_m, x_1, .., x_n) \in \mathbb{Z}[a_1, .., a_m, x_1, .., x_n]$ for which the solvability of the diophantine equation

$$P(a_1, .., a_m, x_1, .., x_n) = 0$$

for any values of the parameters $a_1, .., a_m \in \mathbb{Z}$ is algorithmically unsolvable.

J. Robinson & Yu. V. Matijasevich, 1986 $n \leq 14$.

For exponential diophantine equations $n \leq 3$.

Conjecture (L. Cerlienco, M. Mignotte and F. Piras (1987)).

There exists a positive integer k and linear recursive sequences of integers $\xi^{(1)}, \dots, \xi^{(k)}$ such that the property: There exist $n_1, \dots, n_k \in \mathbb{N}$ such that

$$\xi^{(1)}_{n_1} + \dots + \xi^{(k)}_{n_k} = 0$$

is algorithmically not decidable.

We do not know the answer for $k = 2$!

II. Algorithmically solvable d.e.

In the sequel I concentrate on results, which were obtained by the use of A. Baker-type lower bounds for linear forms of logarithms of algebraic numbers.

A – not at al complet – list of such equations:

- Thue equations $F(x,y) = m$, where $m \in \mathbb{Z}$, $F(x,y) \in \mathbb{Z}[x,y]$ irreducible, of degree ≥ 3. A. Baker, 1968.
- Elliptic equations: $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$, A. Baker, 1968.
- $f(x,y) = 0$, where $f \in \mathbb{Z}[x,y]$ is absolutely irreducible and of genus one, A. Baker and J. Coates (1970).

- Hyperelliptic equations : $ay^2 = f(x)$, $f(x) \in \mathbb{Z}[x]$ with at least three simple zeros. A. Baker, 1969.
- Superelliptic equations $y^m = f(x)$, $f(x) \in \mathbb{Z}[x]$, with at least two simple zeros, $m \geq 3$. A. Baker, 1969.
- Discriminant- and indexform equations : $\mathbb{K}$ a number field of degree $n \geq 3$; $\omega_0 = 1, \ldots, \omega_{n-1}$ an integral basis of $\mathbb{Z}_{\mathbb{K}}$, $m \in \mathbb{Z}$,

$$L^{(i)}(\underline{x}) = \omega_0 x_0 + \omega_1 x_1 + \ldots + \omega_{n-1} x_{n-1}$$

$$\mathrm{Disc}_{\mathbb{K}/\mathbb{Q}}(L^{(i)}(\underline{x})) = m$$

$$I_{\mathbb{K}/\mathbb{Q}} = \left(\mathrm{Disc}_{\mathbb{K}/\mathbb{Q}}(L(\underline{x}))/D_{\mathbb{K}}\right)^{1/2} = m$$

K. Győry, 1973

- Catalan's equation $x^p - y^q = 1$. R. Tijdeman, 1976.
- Perfect powers in second order recurrences. T.N. Shorey and C.L. Stewart and A. Pethő 1982.

Generalizations to
- S-integral solutions
- solutions in integers in algebraic number fields
- in finitely generated integral domains

Common feature: One proves an upper bound for the height of the solutions.

This bound depends only on

- the height of the coefficients and
- on the degree

of the appearing expressions and

- is computable

There are only finitely many unknowns $\Rightarrow$ the search region is bounded $\Rightarrow$ after finitely many trying we find all the solutions.

Two examples:

$$x^3 - 1649x^2y - 1652xy^2 - y^3 = \pm 1 \Rightarrow |x|, |y| \leq 10^{46649}.$$

$$y^2 = x^3 - 228x + 848 \Rightarrow |x|, |y| \leq 10^{7 \cdot 10^{75}}$$

To enumerate all of the pairs below these bounds is hopeless!

II.1. Introduction to Baker's method

Heights of algebraic numbers. Let α be an algebraic number with defining polynomial $a_d x^d + \dots + a_0 \in \mathbb{Z}[x]$ and with conjugates $\alpha^{(1)}, \dots, \alpha^{(d)}$.

$$H(\alpha) = \max_{1 \le j \le d} \{|a_j|\}$$

$$\overline{|\alpha|} = \max_{1 \le j \le d} \{|\alpha^{(j)}|\}$$

$$h(\alpha) = \frac{1}{d} \log\left(|a_d| \prod_{j=1}^{d} \max\{1, |\alpha^{(j)}|\}\right)$$

These heights are equivalent!

Let $\mathbb{L} \subseteq \mathbb{K}$ be number fields with $[\mathbb{L}:\mathbb{Q}] = d_{\mathbb{L}}$ and $[\mathbb{K}:\mathbb{Q}] = d_{\mathbb{K}}$.

$\mathbb{Z}_{\mathbb{L}}$, $\mathbb{Z}_{\mathbb{K}}$ denote the ring of integers of $\mathbb{L}$ and $\mathbb{K}$.

Let $P(x_1, \dots, x_n) \in \mathbb{Z}_{\mathbb{L}}[x_1, \dots, x_n]$ and $m \in \mathbb{Z}_{\mathbb{L}}$.

Goal: Find a computable constant c, which depends only on the degree and on the heights of the coefficients of P such that for any solutions $(x_1, \dots, x_n) \in \mathbb{Z}_{\mathbb{L}}^n$ of the diophantine equation

$$P(x_1, \dots, x_n) = m \qquad (1)$$

$= \max\{h(x_1), \dots, h(x_n)\} \le c$ holds.

Example: Thue equations over number fields.

Let $F(x_1, x_2) \in \mathbb{Z}_{\mathbb{L}}[x_1, x_2]$ be such that

- $F(x_1, x_2)$ be homogenous,
- irreducible,
- of degree $k \geq 3$
- monic in the main term of x_1.

$0 \neq m \in \mathbb{Z}_{\mathbb{L}}$.

We are going to prove a computable upper bound for the solutions of

$$F(x_1, x_2) = m . \qquad (T1)$$

Step 1. Let $f(x_1) = F(x_1, 1)$ and denote by $\alpha = \alpha^{(1)}, \ldots, \alpha^{(k)}$ the roots of $f(x_1)$. Let $\mathbb{L}_1 = \mathbb{L}(\alpha)$.

Then $(T1) \Rightarrow$

$$\mathrm{Norm}_{\mathbb{L}_1/\mathbb{L}}(x_1 - \alpha x_2) = \prod_{j=1}^{k} (x_1 - \alpha^{(j)} x_2) = m .$$

Hence

$$x_1 - \alpha^{(j)} x_2 = \mu^{(j)} \cdot \varepsilon^{(j)} \quad , \ j = 1, \ldots, k , \qquad (T2)$$

where $\mu \in \mathcal{A} \subseteq \mathbb{Z}_{\mathbb{L}_1}$, $\mathcal{A}$ finite and ε a unit in $\mathbb{Z}_{\mathbb{L}_1}$.

$(T2) \Rightarrow \ 1 \leq j < h < t \leq k$

$$(\alpha^{(j)} - \alpha^{(h)}) \mu^{(t)} \varepsilon^{(t)} + (\alpha^{(t)} - \alpha^{(j)}) \mu^{(h)} \varepsilon^{(h)} + (\alpha^{(h)} - \alpha^{(t)}) \mu^{(j)} \varepsilon^{(j)} = 0$$

Dividing by $(\alpha^{(j)} - \alpha^{(h)}) \mu^{(j)} \varepsilon^{(j)}$ we obtain

$$a' E_1' + b' E_2' = 1 , \qquad (T3)$$

where

$$a' = \frac{\alpha^{(j)} - \alpha^{(k)}}{\alpha^{(t)} - \alpha^{(k)}} \; \frac{\mu^{(t)}}{\mu^{(j)}} , \qquad E_1' = \frac{\varepsilon^{(t)}}{\varepsilon^{(j)}} ,$$

$$b' = \frac{\alpha^{(t)} - \alpha^{(j)}}{\alpha^{(t)} - \alpha^{(k)}} \cdot \frac{\mu^{(k)}}{\mu^{(j)}} , \qquad E_2' = \frac{\varepsilon^{(k)}}{\varepsilon^{(j)}} .$$

(T3) is a <u>unit equation</u> in $\mathbb{K} = \mathbb{L}(\alpha^{(1)}, \dots, \alpha^{(k)})$.

<u>Step 2</u> Let $\vartheta_1, \dots, \vartheta_r$ be a system of fundamental relative units of $\mathbb{Z}_{\mathbb{L}_1}$. Then

$$\varepsilon = \zeta_1 \cdot \vartheta_1^{a_1} \cdots \vartheta_r^{a_r} .$$

Putting

$$U_1 = \left\langle \frac{\vartheta_1^{(t)}}{\vartheta_1^{(j)}}, \dots, \frac{\vartheta_r^{(t)}}{\vartheta_r^{(j)}} \right\rangle \text{ and } U_2 = \left\langle \frac{\vartheta_1^{(k)}}{\vartheta_1^{(j)}}, \dots, \frac{\vartheta_r^{(k)}}{\vartheta_r^{(j)}} \right\rangle$$

we obtain

$$a E_1 + b E_2 = 1 \qquad (T4)$$

with

$$E_1 = E_1' \frac{\zeta_1^{(j)}}{\zeta_1^{(t)}} , \qquad a = a' \cdot \frac{\zeta_1^{(t)}}{\zeta_1^{(j)}} ,$$

$$E_2 = E_2' \cdot \frac{\zeta_1^{(j)}}{\zeta_1^{(k)}} , \qquad b = b' \frac{\zeta_1^{(k)}}{\zeta_1^{(j)}} .$$

$$B = A = \max\{|a_1|, \dots, |a_r|\}$$

<u>Step 3</u> $X = \max\{h(x_1), h(x_2)\} \le c_2 A + c_1$

Step 1. Transform (1) to finitely many unit equations

$$a E_1 + b E_2 = 1 \qquad (2)$$

in an appropriate extension $\mathbb{K}$ of $\mathbb{L}$.

Step 2. Let $\mathcal{U}$ be the unit group of $\mathbb{Z}_{\mathbb{K}}$. Choose subgroups $\mathcal{U}_1, \mathcal{U}_2$ of $\mathcal{U}$ such that $E_1 \in \mathcal{U}_1$, $E_2 \in \mathcal{U}_2$ hold for any units E_1, E_2, which can occour in (2).

- Fix a basis $\varepsilon_1, \dots, \varepsilon_{r_1}$ of $\mathcal{U}_1$ and $\eta_1, \dots, \eta_{r_2}$ of $\mathcal{U}_2$.
- Write $E_1 = \varepsilon_1^{a_1} \cdots \varepsilon_{r_1}^{a_{r_1}}$, $E_2 = \eta_1^{b_1} \cdots \eta_{r_2}^{b_{r_2}}$; $a_j, b_j \in \mathbb{Z}$.
- Put $A = \max_{1 \le j \le r_1} \{|a_j|\}$, $B = \max_{1 \le j \le r_2} \{|b_j|\}$.

Step 3. Find a function f s.t. $X \le f(\max\{A, B\})$.

Step 4. If $B \le A$ then there exists a conjugate $1 \le j \le d_{\mathbb{K}}$ s.t.

$$|1 - b^{(j)} \eta_1^{(j) b_1} \cdots \eta_{r_2}^{(j) b_{r_2}}| < c_3' \exp(-c_4 A),$$

which implies

$$|\Lambda| = \left| \log b^{(j)} + \sum_{v=1}^{r_2} b_v \log \eta_v^{(j)} + b_{r_2+1} \pi i \right| < c_3 \exp(-c_4 A). \quad (3)$$

Step 5. If $|\Lambda| \ne 0$ then

$$|\Lambda| \ge \exp(-c_5 \log B \dots). \qquad (4)$$

$(3) \,\&\, (4) \Rightarrow B \le A \le A_0$

Step 6 (Only for explicite solutions.) Reduce the upper bound A_0 by solving the diophantine approximati problem (3). Denote the final bound by A_1.

Step 7. Put $X_1 = f(A_1)$ and find the solutions of (1) below X_1.

II.2. Variants to the general scheme

- To find S-integral solutions of (1) we have to work with S-units and use p-adic linear forms in logs.
- Sometimes it is possible to transform (1) directly to (3). This happens for example for equations

$$G_n = H_m,$$

where G_n and H_m are linear recursive sequences.

- For elliptic equations

$$y^2 = x^3 + ax + b \quad , a, b \in \mathbb{Z}$$

we can use an alternative way proposed by S. Lang.

It is not algorithmic, but practical!

- Compute – if succeed – a basis $P_1, \ldots, P_r$ of the torsion's free part of $E(\mathbb{Q})$.
- Write $P = (x, y) \in E(\mathbb{Q})$ in the form

$$P = b_1 P_1 + \ldots + b_r P_r + T, \quad b_j \in \mathbb{Z}, \quad T \in E(\mathbb{Q})_{tors}$$

- If $P \in E(\mathbb{Z})$ then with $B = \max_{1 \le j \le r} \{|b_j|\}$

$$|b_1 \psi(P_1) + \ldots + b_r \psi(P_r) + b_{r+1}\omega_1| < c_3 \exp(-c_4 B^2),$$

where ψ is called elliptic logarithm

$$\psi(P) = t \iff P = (\wp(t), \wp'(t)) \bmod \omega_1$$

and ω_1 is the real period of $E(\mathbb{C})$.

- To find the elements of $E(\mathbb{Z}_S)$ use p-adic elliptic logarithms.

III 3. Reduction of the large bound

A. Baker and H. Davenport (1968)
W.J. Ellison (1970)
A. Pethő and R. Schulenberg (1986)
B.M.M. de Weger (1987)

Goal: Let $0 \neq \vartheta_1, \ldots, \vartheta_r \in \mathbb{R}$, $\vartheta_{r+1}, c_1, c_2, B_0 \in \mathbb{R}$. Find all $b_1, \ldots, b_r, b_{r+1} \in \mathbb{Z}$ such that with $B = \max_{1 \le j \le r+1}\{|b_j|\}$

$$\left|\sum_{j=1}^{r} b_j \vartheta_j + b_{r+1} + \vartheta_{r+1}\right| < c_2 \exp(-c_1 B), \qquad (R1)$$

$$B \le B_0. \qquad (R2)$$

By Hinchin's theorem

$$\left|\sum_{j=1}^{r} b_j \vartheta_j + b_{r+1} + \vartheta_{r+1}\right| < B^{-r-1-\varepsilon}$$

has for any $\varepsilon > 0$ and for almost all $(\vartheta_1, \ldots, \vartheta_{r+1}) \in \mathbb{R}^{r+1}$ only finitely many solutions.

If we are able to proof for given $(\vartheta_1, \dots, \vartheta_{r+1}) \in \mathbb{R}^{r+1}$ that

$$\left|\sum_{j=1}^{r} b_j \vartheta_j + b_{r+1} + \vartheta_{r+1}\right| > c_3 \, B_0^{-r+1} \qquad (R3)$$

holds for all $(b_1, \dots, b_{r+1}) \in \mathbb{Z}^{r+1}$ with $\max\{|b_j|\} \leq B \leq B_0$,

then (R1) & (R3) implies

$$B < \frac{1}{c_1} \log\left(\frac{c_2}{c_3} B_0^{r+1}\right) \approx (r+1) \log B_0 ,$$

provided B_0 is large enough!

<u>Case I</u>. $r = 1$, $\vartheta_{r+1} = \emptyset$.

$$|b_1 \vartheta_1 + b_2| < c_2 \exp(-c_1 B)$$
$$\max\{|b_1|, |b_2|\} = B < B_0 .$$

<u>Extremality property</u> of <u>continued fractions</u>:

Let $\frac{p_0}{q_0}, \dots, \frac{p_n}{q_n}, \dots$ be the sequence of convergents of ϑ_1.

If $q_n > B_0$, then

$$|p_n - q_n \vartheta_1| < |b_1 \vartheta_1 + b_2| < c_2 \exp(-c_1 B).$$

Here $|p_n - q_n \vartheta_1|$ is known and we get a new bound for B.

Case II. $r \geq 1$, $\vartheta_{r+1} \neq 0$. Simultaneous approximation.

Lemma. Let $C > B_0^r$. Assume that there exist $D \in \mathbb{R}$, $q, p_1, \dots, p_r \in \mathbb{Z}$ such that

$$1 \leq q \leq DC, \qquad (R4)$$

$$|q\vartheta_j - p_j| < \frac{1}{DC^{1/r}}, \quad j = 1, \dots, r \qquad (R5)$$

$$\|q\vartheta_{r+1}\| \geq \frac{2r}{D}.$$

Then we have
$$B \leq \frac{1}{c_1} \log\left(\frac{D^2 C c_2}{r}\right)$$
for any solutions $(b_1, \dots, b_{r+1}) \in \mathbb{Z}^{r+1}$ of (R1) and (R2).

Proof. (R1) & (R4) $\Rightarrow$

$$\left|\sum_{j=1}^{r} q\, b_j \vartheta_j + q\, b_{r+1} + q\,\vartheta_{r+1}\right| < q c_2 \exp(-c_1 B) \leq CDc_2 \exp(-c_1 B).$$

On the other hand (R5) implies

$$\left|\sum_{j=1}^{r} b_j (q\vartheta_j - p_j)\right| \leq \sum_{j=1}^{r} |b_j|\,|q\vartheta_j - p_j| < \frac{r}{D}.$$

Hence

$$\left|\sum_{j=1}^{r} b_j q\vartheta_j + q b_{r+1} + q\vartheta_{r+1}\right| = \left|\sum_{j=1}^{r} b_j (q\vartheta_j - p_j) + \sum_{j=1}^{r} b_j p_j + q b_{r+1} + q\vartheta_{r+1}\right|$$

$$\geq \left|\sum_{j=1}^{r} b_j p_j + q b_{r+1} + q\vartheta_{r+1}\right| - \left|\sum_{j=1}^{r} b_j (q\vartheta_j - p_j)\right|$$

$$\geq \|q\vartheta_{r+1}\| - \frac{r}{D} \geq \frac{r}{D}$$

$$\Rightarrow \qquad B < \frac{1}{c_1} \log \frac{D^2 C c_2}{r}.$$

$r=1$ use continued fractions

$r\geqslant 1$ LLL-algorithm

II.4 LLL-algorithm and de Weger reduction

Let the lattice $\mathcal{L} \subseteq \mathbb{Z}^n$ be given by the basis $\underline{b}_1, \ldots, \underline{b}_n \in \mathbb{Z}^n$.

The LLL-algorithm (A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász (1982)) computes in – the size of $\underline{b}_1, \ldots, \underline{b}_n$ – polynomial time an other basis $\underline{a}_1, \ldots, \underline{a}_n$ of $\mathcal{L}$ such that

$$|\underline{a}_1| < 2^{\frac{n(n-1)}{4}} \, d(\mathcal{L})^{1/n}$$

$$|\underline{a}_1| \leq 2^{(n-1)/2} \, \lambda(\mathcal{L}) \quad , \text{ where}$$

$$\lambda(\mathcal{L}) = \min_{\underline{x} \neq 0} \{ |\underline{x}| : \underline{x} \in \mathcal{L} \}.$$

Case III. $r>1$, $\vartheta_{r+1}=0$ (General, homogenous case)

<u>Theorem</u> (de Weger, 1987). Let $0\neq b=(b_1,\dots,b_{r+1})\in\mathbb{Z}^{r+1}$ be a solution of

$$\Big|\sum_{j=1}^{r} b_j\vartheta_j + b_{r+1}\Big| < c_2\exp(-c_1B)$$

$$\max_{1\le j\le r+1}\{|b_j|\} = B \le B_0 .$$

Let $C\geq B_0^{r+1}$ an integer and the lattice $\mathcal{L}$ be generated by the columns of the matrix

$$L=\begin{pmatrix} 1 & & & \\ 0 & \ddots & & \mathcal{O} \\ \vdots & & & \\ 0 & & 1 & \\ [C\vartheta_1] & \dots & [C\vartheta_r] & C \end{pmatrix}.$$

Let $\underline{a}_1,\dots,\underline{a}_{r+1}$ be the LLL-reduced basis of $\mathcal{L}$ and assume

$$G=\left(2^{-r}|\underline{a}_1|^2-rB_0^2\right)^{1/2}-\frac{r}{2}B_0>0 .$$

Then
$$B\le\frac{1}{c_1}\log\frac{Cc_2}{G} .$$

II.5 Improvements

1.) To Step 2. Keep U_1 and U_2 as small as possible.
Index form equations.

Let $\mathbb{L}$ be a number field of degree $d_{\mathbb{L}} = d$.

Let $1 = \omega_0, \omega_1, \dots, \omega_{d-1}$ be an integral basis of $\mathbb{Z}_{\mathbb{L}}$.

Let $\underline{x}' = (x_0, \dots, x_{d-1}) \in \mathbb{Z}^d$ and $\underline{x} = (x_1, \dots, x_{d-1}) \in \mathbb{Z}^{d-1}$ and

$$L^{(j)}(\underline{x}') = \sum_{i=0}^{d-1} x_i \omega_i^{(j)} \quad , j = 1, \dots, d .$$

Then

$$I_{\mathbb{L}/\mathbb{Q}}(\underline{x}) = \frac{1}{D_{\mathbb{L}}^{1/2}} \prod_{1 \le j < k \le d} \left(L^{(j)}(\underline{x}') - L^{(k)}(\underline{x}') \right) \in \mathbb{Z}[\underline{x}],$$

homogenous and of degree $\frac{d(d-1)}{2}$.

Let $m \in \mathbb{Z}$ and consider the index form equation

$$I_{\mathbb{L}/\mathbb{Q}}(\underline{x}) = m . \qquad (I1)$$

Let $\mathbb{K}$ be the normal closure of $\mathbb{L}$.

K. Győry's original approach to solve (I 1):

Let $\underline{x} = (x_1, \dots, x_{d-1}) \in \mathbb{Z}^{d-1}$ be a solution of (I 1). Put

$$\beta_{j,k} = L^{(j)}(\underline{x}) - L^{(k)}(\underline{x}) \in \mathbb{Z}_{\mathbb{K}} \ , \ 1 \le j < k \le d .$$

As $\beta_{j,k} \mid m D_{\mathbb{K}}^{1/2}$ in $\mathbb{Z}_{\mathbb{K}}$ we have $\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\beta_{j,k}) \mid \mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(m D_{\mathbb{K}}^{1/2})$.

There exist a finite set $\mathcal{A} \subseteq \mathbb{Z}_{\mathbb{K}}$ such that

$$\beta_{j,k} = \mu_{j,k} \, \varepsilon_{j,k}$$

with $\mu_{j,k} \in \mathcal{A}$, $\varepsilon_{j,k}$ a unit in $\mathbb{Z}_{\mathbb{K}}$.

The obvious relation

$$\beta_{jk} + \beta_{\ell j} + \beta_{k\ell} = 0$$

implies the unit equation

$$\mu_{jk} \varepsilon_{jk} + \mu_{\ell j} \varepsilon_{\ell j} + \mu_{k\ell} \varepsilon_{k\ell} = 0$$

in $\mathbb{Z}_{\mathbb{K}}$!

The unit group of $\mathbb{Z}_{\mathbb{K}}$ is usually very large!

For example if $d=4$, $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \simeq S_4$ and $\mathbb{L}$ is totally real, then $\mathrm{rank}\ \mathbb{Z}_{\mathbb{K}}^{*} = 23$.

<u>Theorem</u> (I. Gaál, A. Pethő and M. Pohst, 1996). If $d=4$, then (I 1) can be transformed into finitely many quartic Thue equations $F_i(x_1, x_2) = m_i$ such that one of the roots of $F_i(x_1, 1)$ belongs to $\mathbb{L}$.

Adventages:

- rank $\mathbb{Z}_{\mathbb{L}}^{*} \leq 4$
- we can solve (I1) within the arithmetic of $\mathbb{L}$.

N. Smart and independently K. Wildanger proved that (I1) can be transformed to unit equations in number fields of degree at most $d(d-1)$.

I. Gaál and K. Győry (1999) proved that (I1) over quintic fields can be transformed to unit equations such that the ranks of the unit groups involved is at most 10!

They computed all power integral bases in the fields generated by a root of the polynomials

$$x^5-5x^3+x^2+3x-1$$

and

$$x^5-6x^3+x^2+4x+1.$$

In both cases the quintic fields are totally real and their Galois groups ~~are~~ isomorphic to S_5.

<u>Problem</u> Is it possible to solve (I1) within the arithmetic of $\mathbb{L}$?

Connection between the computation of the upper bound and its reduction.

6.) To Step 5. To compute an upper bound for B it is not necessary to use inequality (3). This happens if

- no explicite lower bound for $|\Lambda|$ is available, e.g. p-adic elliptic logarithms.
- different methods yield different bounds.

A. Pethő, H.G. Zimmer, J. Gebel, E. Herrmann (2000)

Consider

$$y^2 = x^3 + ax + b \quad .$$

The elliptic logarithm approach yields an inequality

$$|b_1 \psi(P_1) + \ldots + b_r \psi(P_r) + b_{r+1} \omega_1| < c_2 \exp(-c_1 B^2).$$

S. David's theorem implies an upper bound B_D for B

On the other hand Baker's approach implies a bound X_0 for $\max\{|x|, |y|\}$. The best bound is due to L. Hajdu and T. Herendi (1997).

Using elementary properties of height functions associated to elliptic curves we obtain

$$\max_{1 \le i \le r+1} \{|b_i|\} \le c_3 \log \max\{|x|, |y|\}, \text{ i.e.}$$

$$B \le c_3 \log X_0 = B_H$$

Comparison of N_0' and N_1 for $s = 1$.
The first set of examples is taken from Gebel, Pethő and Zimmer for the Mordell equations

$$y^2 = x^3 + k$$

with $|k| \leq 10^5$.

Table 1

k	r_k	B_D	B_H
108	1	$2.8 \cdot 10^{26}$	$1.8 \cdot 10^{41}$
225	2	$1.3 \cdot 10^{41}$	$4.5 \cdot 10^{41}$
1025	3	$5.5 \cdot 10^{60}$	$3.1 \cdot 10^{42}$
2089	4	$1.1 \cdot 10^{84}$	$7.7 \cdot 10^{42}$
-28279	5	$2.1 \cdot 10^{112}$	$2.0 \cdot 10^{42}$

In Table 2, we take some examples from Bremner, Stroeker and Tzanakis, where the family of elliptic curves

$$y^2 = x^3 - 36x - 864k(k-1)(2k-1)$$

was considered.

Table 2

k	r_k	B_D	B_H
1	1	$8.9 \cdot 10^{23}$	$1.3 \cdot 10^{41}$
3	2	$5.8 \cdot 10^{39}$	$1.8 \cdot 10^{44}$
7	3	$2.4 \cdot 10^{60}$	$5.9 \cdot 10^{45}$
20	4	$2.1 \cdot 10^{86}$	$2.9 \cdot 10^{47}$

Finally we consider some curves of high rank considered by Gebel, Pethő and Zimmer as well as by Stroeker and Tzanakis

$$y^2 = x^3 + ax + b.$$

Table 3

a	b	r	B_D	B_H
-203472	18487440	5	$2.3 \cdot 10^{111}$	$7.9 \cdot 10^{47}$
-1642032	628747920	6	$1.1 \cdot 10^{144}$	$2.1 \cdot 10^{49}$
-147952	21183760	7	$2.7 \cdot 10^{187}$	$1.1 \cdot 10^{47}$
-5818216808130	5401285759982786436	8	$8.67 \cdot 10^{224}$	$2.33 \cdot 10^{58}$

:) To Step 6 To reduce the upper bound it is not necessary to use (3).

Yu. Bilu and G. Hanrot (1996).

Consider a Thue equation

$$F(x_1,x_2)=m \qquad (F1)$$

with $F(x_1,x_2)\in \mathbb{Z}[x_1,x_2]$, $m\in\mathbb{Z}$.

Assume you have already an upper bound X_0 for $\max\{|x_1|,|x_2|\}$.

Let α be a zero of $F(x_1,1)$ and order the conjugates $\alpha=\alpha^{(1)},\dots,\alpha^{(d)}$ such that $\alpha^{(1)},\dots,\alpha^{(r_1)}\in\mathbb{R}$, $\alpha^{(r_1+1)},\dots,\alpha^{(d)}\notin\mathbb{R}$.

Lemma Let $(x_1,x_2)\in\mathbb{Z}^2$ a solution of (F1) such that $|x_2|$ is large enough. Then there exist $1\le u\le r_1$ s.t.

$$|x_1-\alpha^{(u)}x_2| < c_1|x_2|^{-(d-1)} \qquad (F2)$$

$$c_2|x_2| < |x_1-\alpha^{(v)}x_2| < c_3|x_2| \qquad v\in\{1,\dots,d\}\setminus\{u\}.$$

Let $\varepsilon_1,\dots,\varepsilon_r$ be a basis of $\mathbb{Z}_{\mathbb{L}}^*$. ($\mathbb{L}=\mathbb{Q}(\alpha)$) Let $(x_1,x_2)\in\mathbb{Z}^2$ be a solution of (F1) with $|x_2|$ large enough.

Write

$$\mu^{(v)}=x_1-\alpha^{(v)}x_2=\mu_c^{(v)}\varepsilon_1^{(v)b_1}\cdots\varepsilon_r^{(v)b_r},\quad v=1,\dots,d.$$

It is easy to prove

$$\max_{1\le i\le r}\{|b_i|\}\le c_4\log|x_2|+c_5.$$

Let $v \in \{1,\dots,d\}\setminus\{u\}$. Then

$$\left|\frac{\mu^{(v)}}{x_2(\alpha^{(u)}-\alpha^{(v)})}-1\right| = \left|\frac{x_1 - x_2\alpha^{(v)} - x_2\alpha^{(u)} + x_2\alpha^{(v)}}{x_2(\alpha^{(u)}-\alpha^{(v)})}\right| < \frac{c_1}{|\alpha^{(u)}-\alpha^{(v)}|}|x_2|^{-d},$$

Hence

$$\left|\sum_{j=1}^{r} b_j \log|\varepsilon_j^{(v)}| - \log|x_2| + \log\left|\frac{\mu_\tau^{(v)}}{\rho^{(u)}-\rho^{(v)}}\right|\right| < c_5 |x_2|^{-d} \quad v\in\{1,\dots,d\}\setminus\{u\}.$$

Eliminating here $\log|x_2|$ we obtain $r-1$ linear inequalities in the r unknowns $b_1,\dots,b_r$, which can be transformed into the inequalities

$$\left| b_1 \frac{\vartheta_s}{\vartheta_1} + \lambda_{1s} - b_s \right| < c_6 |x_2|^{-d} < c_7 \exp(-dB + c_8) \quad s = 2,\dots,r.$$

The reduction can be done by using continued fractions!

III. Epilog

20 years ago it took me several moth to solve the Thue equation

$$x^3 + 3x^2y - 12xy^2 - 4y^3 = \pm 1.$$

G. Hanrot (2000) was able to solve completely the equation

$$\prod_{1\le k\le 2000}\left(Y - 2\left(\cos\frac{2k\pi}{4000}\right)X\right) = \pm 1, \pm 4001.$$

This is a 2000 degree Thue equation!

Theorem (Yu. Bilu, G. Hanrot, P. Voutier, ?) For $n \geq 30$ the n-t element of a Lucas or a Lehmer sequence has a primiti divisor.

Let α, β be algebraic numbers such that $\alpha\beta$ and $\alpha+\beta$ or $(\alpha+\beta)^2$ is a non-zero integer. Define

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \text{ if } \alpha+\beta \in \mathbb{Z} \qquad \text{(Lucas sequence)}$$

$$u_n = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta}, \text{ if } n \text{ is odd} \\ \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, \text{ if } n \text{ is even} \end{cases} \qquad \text{(Lehmer sequence)}$$

p is a primitive divisor of u_n if $p \nmid (\alpha-\beta)^2 u_1 \cdots u_{n-1}$.

Implementations:

KANT : Thue over $\mathbb{Z}$

MAGMA : Thue over $\mathbb{Z}$, elliptic over $\mathbb{Z}$, $\mathbb{Z}_S$

PARI : Thue over $\mathbb{Z}$

SIMATH : elliptic over $\mathbb{Z}$

MAPLE : ~~restricted Thue~~ over $\mathbb{Z}$.

IV. Problems

The method of Yu. Bilu and G. Hanrot means:

Solution of Thue equations over $\mathbb{Z}$

$=$

Computation of parameters in an algebraic # field.

Problem 1. Find similar result for other classes of diophantine equations.

Let $\mathcal{D}$ be a class of diophantine equations, like:

{Thue equations over $\mathbb{Z}$} = Thue
{Elliptic equations over $\mathbb{Z}$} = Elliptic
{Index form equations} = Index

Let Dec($\mathcal{D}$) be the following problem: Decide for every $E \in \mathcal{D}$ whether it is solvable.

Let Solve($\mathcal{D}$) be the following problem: If $E \in \mathcal{D}$ is solvable, then find a solution; otherwise give the answer "there are no solutions".

Problem 2 What is the connection - from complexity theory point of view - between the following problems

Dec (Thue) Solve (Thue)

Dec (Elliptic) Solve (Elliptic)

Dec (Index) Solve (Index) ?

Problem 3. Find a practical method for the solution of hyperelliptic equations

$$y^2 = f(x) \quad , \; f(x) \in \mathbb{Z}[x] \text{ of degree } \geq 5.$$

(Chabauty ?)

Problem 4. Find all solutions of

$$x^2 - x = y^5 - y \quad !$$

Problem 5. Let $T_0 = T_1 = 0$, $T_2 = 1$, $T_{n+3} = T_{n+2} + T_{n+1} + T_n$.
We have $T_0 = T_1 = 0$, $T_2 = T_3 = 1$, $T_5 = 4$, $T_{10} = 81$, $T_{16} = 3136 = 56^2$ and $T_{18} = 10609 = 103^2$. Prove that there are no more squares in this sequence!

Remark: $T_n = x^q$ has only finitely many solutions, if $|x| > 1$!

Problem 6 Let $\overline{T}_0 = 0$, $\overline{T}_1 = 1$, $\overline{T}_2 = -1$ and

$\overline{T}_{n+3} = -\overline{T}_{n+2} - \overline{T}_{n+1} + \overline{T}_n$. Prove that there are only finitely many perfect powers in $\{\overline{T}_n\}$.

Remark $T_{-n} = \overline{T}_n$