The first hundred years of algorithmic theory of diophantine equations

Attila Pethő
Debrecen, Hungary

Kyoto, October 26, 2000
7. Irrationality and Transcendence of Certain Numbers.

Hermite's arithmetical theorems on the exponential function and their extension by Lindemann are certainly 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 \( e^x \), for example, which evidently has algebraic values for all rational arguments, will on the other hand always take transcendental values for irrational algebraic values of the argument \( x \). We can also give this statement a geometrical form, as follows:

If, in an isosceles triangle, the ratio of the base angle to the base 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 \( e^x \), for an algebraic base \( a \) and an irrational algebraic exponent \( \beta \), e. g., the number \( 2^{\sqrt{2}} \) or \( e^{\pi} \), 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 10th problem in positive form?

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

Hilbert's 10th problem: let \( P(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n] \).
Give an algorithm which decides whether
\[
P(x_1, \ldots, x_n) = 0
\]
is solvable or not.

H. Davis, H. Putnam and J. Robinson (1961): Hilbert's 10th 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
\[
P(a_{11}, a_{1n}, x_1, \ldots, x_n) \in \mathbb{Z}[a_{11}, \ldots, a_{1n}, x_1, \ldots, x_n]
\]
for which the solvability of the diophantine equation
\[
P(a_{11}, a_{1n}, x_1, \ldots, x_n) = 0
\]
for any values of the parameters \( a_{11}, \ldots, a_{1n} \in \mathbb{Z} \) is algorithmically unsolvable.

J. Robinson & Yu. V. Matijasevich, 1985 \( n \leq 14 \).

For exponential diophantine equations \( n \leq 3 \).
Conjecture (L. Carlitz, N. Mignotte and F. Piras (1987)).

There exists a positive integer $k$ and linear recursive sequences of integers $\xi^{(2)}, \ldots, \xi^{(k)}$ such that the property: There exist $n_1, \ldots, n_k \in \mathbb{N}$ such that

$$\xi^{(n_1)} + \ldots + \xi^{(n_k)} = 0$$

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 all complete) 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 $\geq 3$. 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
- 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 index form equations: \( K \) a number field of degree \( n \geq 3 \), \( \omega_1, \ldots, \omega_n \) an integral basis of \( \mathcal{O}_K \), \( m \in \mathbb{Z} \),
  \[
  L(x) = \omega_0 x^0 + \omega_1 x^1 + \ldots + \omega_n x^n
  \]
  \[
  \text{Disc}_{K/\mathbb{Q}}(L(x)) = m
  \]
  \[
  I_{K/\mathbb{Q}} = \left( \frac{\text{Disc}_{K/\mathbb{Q}}(L(x))}{D_K} \right)^{1/2} = m
  \]

  K. Győry, 1973

- Catalan's equation \( x^p - y^q = 1 \). R. Tijdeman, 1976.

- Perfect powers in second order recurrences.

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 => the search region is bounded => after finitely many trying we find all the solutions.

Two examples:

\[ x^3 - 1649x^2y - 1652xy^2 - y^3 = \pm 1 \Rightarrow |x_1, y_1| \leq 10^{664.9} \]

\[ y^2 = x^3 - 228x + 848 \Rightarrow |x_1, y_1| \leq 10^{7.10^{7.5}} \]

To enumerate all of the pairs below these bounds is hopeless!
II.1. Introduction to Baker's method

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

\[
H(\alpha) = \max \left\{ \frac{1}{d} |a_j| \right\}_{1 \leq j \leq d}
\]

\[
|\alpha|_\infty = \max \left\{ |\alpha^{(j)}| \right\}_{1 \leq j \leq d}
\]

\[
h(\alpha) = \frac{1}{d} \log \left( \frac{1}{d} \max \left\{ 1, |\alpha^{(1)}|, \ldots, |\alpha^{(d)}| \right\} \right)
\]

These heights are equivalent!

Let \( L \subseteq K \) be number fields with \( [L: \mathbb{Q}] = d_L \) and \( [K: \mathbb{Q}] = d_K \).

\( \mathbb{Z}_L, \mathbb{Z}_K \) denote the ring of integers of \( L \) and \( K \).

Let \( P(x_1, \ldots, x_n) \in \mathbb{Z}_L[x_1, \ldots, x_n] \) and \( m \in \mathbb{Z}_L \).

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 \( (x_1, \ldots, x_n) \in \mathbb{Z}_L^n \) of the Diophantine equation

\[
P(x_1, \ldots, x_n) = m
\]

\[
= \max \{ h(x_1), \ldots, h(x_n) \} \leq c \text{ holds.}
\]
Example: Three equations over number fields.

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

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

$0 \neq m \in \mathbb{Z}_L$.

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

$$F(x_1, x_2) = m.$$  \hfill (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 $L_1 = L(\alpha)$.

Then (T1) $\Rightarrow$

$$\text{Norm}_{L_1/L}(x_1 - \alpha^{(i)} x_2) = \frac{1}{\alpha^{(i)}} (x_1 - \alpha^{(i)} x_2) = m.$$  

Hence

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

where $\mu \in \mathfrak{A} \subseteq \mathbb{Z}_{L_1}$, $\varepsilon$ finite and $\varepsilon$ a unit in $\mathbb{Z}_{L_1}$.

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

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

Dividing by $(\alpha^{(k)} - \alpha^{(k)}) \mu^{(t)} \varepsilon^{(j)}$ we obtain
\[ a' E_1' + b' E_2' = 1 \quad \text{(T2)} \]

where

\[
\begin{align*}
  a' &= \frac{\alpha^{(b)} - \alpha^{(c)}}{\alpha^{(b)} - \alpha^{(c)}}, \quad \frac{\mu^{(c)}}{\mu^{(c)}}, \quad E_1' = \frac{\varepsilon^{(c)}}{\varepsilon^{(c)}}, \\
  b' &= \frac{\alpha^{(b)} - \alpha^{(c)}}{\alpha^{(b)} - \alpha^{(c)}}, \quad \frac{\mu^{(c)}}{\mu^{(c)}}, \quad E_2' = \frac{\varepsilon^{(c)}}{\varepsilon^{(c)}}.
\end{align*}
\]

(T3) is a unit equation in \( \mathbb{K} = \mathbb{L}(\alpha^{(c)}, \ldots, \alpha^{(c)}) \).

**Step 2**

Let \( v_1, \ldots, v_r \) be a system of fundamental relative units of \( \mathbb{Z}_{\mathbb{L}} \). Then

\[ E = \xi_1 v_1^{a_1} \cdots v_r^{a_r}. \]

Putting

\[ u_1 = \left( \frac{v_1^{a_1}}{\xi_1^{c_1}}, \ldots, \frac{v_r^{a_r}}{\xi_r^{c_r}} \right) \quad \text{and} \quad u_2 = \left( \frac{v_1^{b_1}}{\xi_1^{c_1}}, \ldots, \frac{v_r^{b_r}}{\xi_r^{c_r}} \right) \]

we obtain

\[ a' E_1 + b' E_2 = 1 \quad \text{(T4)} \]

with

\[ E_1 = E_1' \frac{\xi_1^{c_1}}{\xi_1^{c_1}}, \quad a = a' \frac{\xi_1^{c_1}}{\xi_1^{c_1}}, \]

\[ E_2 = E_2' \frac{\xi_1^{c_1}}{\xi_1^{c_1}}, \quad b = b' \frac{\xi_1^{c_1}}{\xi_1^{c_1}}. \]

\[ B = A = \max \{|a_1|, \ldots, |a_r|\} \]

**Step 3**

\[ X = \max \{|b_1|, \ldots, |b_r|\} \leq c_2 A + c_2 \]

\[ X = \max \{|b_1|, \ldots, |b_r|\} \leq c_2 A + c_2 \]
Step 1. Transform (1) to finitely many unit equations
\[ aE_1 + bE_2 = 1 \] (2)
in an appropriate extension \( K \) of \( \mathbb{U} \).

Step 2. Let \( U \) be the unit group of \( \mathbb{Z}_K \). Choose subgroups \( U_1, U_2 \) of \( U \) such that \( E_1 \in U_1, E_2 \in U_2 \) hold for any units \( E_1, E_2 \), which can occur in (2).

- Fix a basis \( \eta_{i_1}, ..., \eta_{i_r} \) of \( U_1 \) and \( \gamma_{j_1}, ..., \gamma_{j_r} \) of \( U_2 \).
- While \( E_1 = a_{i_1} \eta_{i_1}^{q_1}... \eta_{i_r}^{q_r} \), \( E_2 = \eta_{j_1}^{q_{i_1}}... \eta_{j_r}^{q_{i_r}} \), \( a_{i_1}, b_{j_1} \in \mathbb{Z} \).
- Put \( A = \max \{ 1, a_{i_1} \} \), \( B = \max \{ 1, b_{j_1} \} \).

Step 3. Find a function \( f \) s.t. \( \lambda x \leq \max \{ A, B \} \).

Step 4. If \( B \leq A \) then there exists a conjugate \( 1 \leq d_k \leq \lambda \) s.t.
\[ |1 - a_{i_1}^{(i)} \eta_{j_1}^{(j)} \eta_{j_2}^{(j_2)}... \eta_{j_r}^{(j_r)}| < C_3 \exp(-c_4 A), \]
which implies
\[ |\Lambda| = |\log b^{(i)} + \sum_{\nu=1}^{\tau_k} b_{\nu} \log \eta_{j_\nu}^{(j_\nu)} + b_{\tau_k+1} \Pi e| < C_3 \exp(-c_4 A), \] (3)

Step 5. If \( |\Lambda| = 0 \) then
\[ |\Lambda| \geq \exp(-c_5 \log B...). \] (4)

(3) \& (4) \Rightarrow \ B \leq A \leq A_0.
Step 6. (Only for explicit solutions.) Reduce the upper
bound $A_0$ by solving the Diophantine approximations
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

$$P = b_1 P_1 + \ldots + b_r P_r + T, \quad b_j \in \mathbb{Z}, \quad T \in E(\mathbb{Q})_{tor},$$
If \( PE \in E(\mathbb{Z}) \) then with \( B_0 \) max \( \{ |b_i| \} \)

\[
|b_1 \psi(P_1) + \ldots + b_r \psi(P_r) + b_{r+1} \omega_1| < c_1 \exp(-c_2 B) ,
\]

where \( \psi \) is called elliptic logarithm

\[
\psi(P) = t \Leftrightarrow P = (\rho(t), \rho'(t)) \mod \omega_1
\]

and \( \omega_1 \) is the real period of \( E(\mathbb{C}) \).

To find the elements of \( E(\mathbb{Z}_5) \) use \( p \)-adic elliptic logarithms.

### 16.3. Reduction of the large bound

A. Baker and H. Davenport (1968)
W.J. Ellison (1970)
A. Pethö and R. Schanuel (1986)
B.H. de Weger (1987)

**Goal:** Let \( 0 \neq v_1, \ldots, v_r \in \mathbb{R}, v_{r+1}, c_1, c_2, B_0 \in \mathbb{R} \). Find all \( b_1, \ldots, b_r, b_{r+1} \in \mathbb{Z} \) such that with \( B = \max \{ |b_i| \} \)

\[
|\sum_{j=1}^{r} b_j v_j + b_{r+1} v_{r+1}| < c_2 \exp(-c_1 B) ,
\]

\[
B \leq B_0 .
\]

By Hinchin's theorem

\[
|\sum_{j=1}^{r} b_j v_j + b_{r+1} v_{r+1}| < B^{-r-1-\varepsilon}
\]

has for any \( \varepsilon > 0 \) and for almost all \((v_1, \ldots, v_r) \in \mathbb{R}^r\)
only finitely many solutions.
If we are able to prove for given \((\nu_1, \ldots, \nu_{n_0}) \in \mathbb{R}^{n_0}\) that
\[
\left| \sum_{j=1}^{n_0} b_j \nu_j + b_{n_0} \right| > c_3 B_0^{-r+1}
\] (R3)
holds for all \((b_1, \ldots, b_{n_0}) \in \mathbb{Z}^{n_0}\) with \(\max |b_j| \leq B \leq B_0\),

then (R1) \& (R3) implies
\[
B < \frac{1}{c_4} \log \left( \frac{c_2}{c_5} B_0^{-r+1} \right) \approx (r+1) \log B_0,
\]
provided \(B_0\) is large enough!

**Case 1.** \(r = 1\), \(S_{n_0} = \emptyset\).

\[
|b_1 \nu_1 + b_2| < c_2 \exp(-c_1 B)
\]

\(\max |b_1, b_2| = B < B_0\).

**Extremality property of continued fractions:**

Let \(\frac{p_0}{q_0}, \ldots, \frac{p_n}{q_n}, \ldots\) be the sequence of convergents of \(\nu_1\).

If \(q_n > B_0\), then
\[
|p_n - q_n \nu_1| < |b_1 \nu_1 + b_2| < c_2 \exp(-c_1 B).
\]

Here \(|p_n - q_n \nu_1|\) is known and we get a new bound for \(B\).
Case II. \( r \gg 1, \delta_{r n} \neq 0 \). Simultaneous approximation.

Lemma: Let \( C > B_{\delta} \). Assume that there exist \( D \in \mathbb{R}, q, p_1, \ldots, p_r \in \mathbb{Z} \) such that

\[
\begin{align*}
1 \leq q & \leq DC, \\
|q \delta_{r} - p_{r}| & < \frac{1}{DC^{1/r}}, \quad \delta_{r} \approx 1 - r \\
\|q \delta_{r n}\| & \geq \frac{2^{m+1}}{D}.
\end{align*}
\]

Then we have

\[ B \leq \frac{1}{e_{2}} \log \left( \frac{D^{2}C_{1}}{\epsilon} \right) \]

for any solutions \( (b_{1}, \ldots, b_{n}) \in \mathbb{Z}^{+n} \) of \((R1)\) and \((R2)\).

Proof. \((R4) \Rightarrow (R4) \Rightarrow \)

\[ \left| \sum_{b_{1}} q_{b_{1}} \delta_{r} + q b_{r n} + q \delta_{r n} \right| < q e_{2} \exp(-c_{1}B) \leq CD e_{2} \exp(-c_{1}B). \]

On the other hand \((R5)\) implies

\[ \left| \sum_{b_{1}} b_{1}(q \delta_{r} - p_{r}) \right| \leq \sum_{b_{1}} |b_{1}| |q \delta_{r} - p_{r}| < \frac{e_{2}}{D}. \]

Hence

\[ \left| \sum_{b_{1}} b_{1} q \delta_{r} + q b_{r n} + q \delta_{r n} \right| = \left| \sum_{b_{1}} b_{1}(q \delta_{r} - p_{r}) + \sum_{b_{1}} b_{1} p_{r} + q b_{r n} + q \delta_{r n} \right| \]

\[ \geq \left| \sum_{b_{1}} b_{1} p_{r} + q b_{r n} + q \delta_{r n} \right| - \left| \sum_{b_{1}} b_{1}(q \delta_{r} - p_{r}) \right| \]

\[ \geq \|q \delta_{r n}\| - \frac{e_{2}}{D} \geq \frac{e_{2}}{D} \]

\[ \Rightarrow \quad B < \frac{1}{e_{2}} \log \left( \frac{D^{2}C_{1}}{\epsilon} \right). \]
\[ r=1 \text{ use continued fractions} \]

\[ r \geq 1 \quad \text{LLL-algorithm} \]

\[ \text{II.4 LLL-algorithm and de Weges reduction} \]

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

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

\[ |a_1| < 2^{\frac{n(n-1)}{4}} \lambda(\mathcal{L})^{1/n} \]

\[ |a_1| \leq 2^{(n-1)/2} \lambda(\mathcal{L}) \], where

\[ \lambda(\mathcal{L}) = \min_{x \neq 0} \{ |x| : x \in \mathcal{L} \} \].
Case III. \( r > 1 \), \( \delta_{r+1} = 0 \) (General, homogeneous case)

**Theorem** (de Weger, 1987). Let \( 0 \neq b = (b_1, \ldots, b_m) \in \mathbb{Z}^m \) be a solution of

\[
| \sum_{i=1}^{r} b_i v_i + b_{r+1} | < c_2 \exp (-c_1 B)
\]

\[
\max_{1 \leq j \leq r+1} \{ |b_j| \} = B \leq B_0.
\]

Let \( c > B_0^{r+1} \) an integer and the lattice \( L \) be generated by the columns of the matrix

\[
L = \begin{pmatrix}
1 & \cdots & 0 \\
0 & \ddots & 0 \\
\vdots & \ddots & 1 \\
[0] & \ldots & [C^r] \\
[0] & \ldots & [C^r] \\
\vdots & \ldots & \vdots \\
[0] & \ldots & [C^r] \\
\end{pmatrix}.
\]

Let \( a_1, \ldots, a_m \) be the LLL-reduced basis of \( L \) and assume

\[
G = \left( 2^{-r} a_1^2 - \frac{r \delta_1^2}{2} \right) - \frac{r}{2} B_0 > 0.
\]

Then

\[
B \leq \frac{A}{C_1} \log \frac{Cc_2}{G}.
\]
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 $\mathbb{L} = \omega_0, \omega_1, \ldots, \omega_{d-1}$ be an integral basis of $\mathbb{Z}_\mathbb{L}$.
Let $x' = (x_0, \ldots, x_{d-1}) \in \mathbb{Z}^d$ and $\mathbf{x} = (x_0, \ldots, x_{d-1}) \in \mathbb{Z}^{d-1}$ and

$$L(x') = \sum_{\delta = 0}^{d-1} x_\delta \omega^\delta, \quad \delta = 0, \ldots, d - 1.$$

Then,

$$\Gamma_{\mathbb{L}/\mathbb{Q}}(x) = \frac{1}{D_{\mathbb{L}}^{1/2}} \prod_{1 \leq i < k \leq d} \left( L^{(i)}(x') - L^{(k)}(x') \right) \in \mathbb{Z}[z],$$

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

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

$$\Gamma_{\mathbb{L}/\mathbb{Q}}(x) = m \quad (\text{II})$$

Let $K$ be the normal closure of $\mathbb{L}$.
K. G. L. Y's original approach to solve (I I):

Let \( \mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^{d-1} \) be a solution of (I I). Put

\[
\beta_{jk}^i = L^{(i)}(x) - L^{(k)}(x) \in \mathbb{Z}_K, \quad 1 \leq j \leq k \leq d.
\]

As \( \beta_{jk} \in \mathbb{Z}_K^d \) in \( \mathbb{Z}_K \) we have \( \text{Norm}_{K/Q}(\beta_{jk}) \leq \text{Norm}_{K/Q}(w) \).

There exists a finite set \( \mathbf{u} \subseteq \mathbb{Z}_K \) such that

\[
\beta_{jk} = \mu_{jk} \mathbf{u} \mathbf{e}_i
\]

with \( \mu_{jk} \in K, \mathbf{e}_i \) a unit in \( \mathbb{Z}_K \).

The obvious relation

\[
\beta_{jk} + \beta_{ji} + \beta_{ik} = 0
\]

implies the unit equation

\[
\mu_{jk} \mathbf{u} + \mu_{ji} \mathbf{u} \mathbf{e}_i + \mu_{ik} \mathbf{u} \mathbf{e}_k = 0
\]

in \( \mathbb{Z}_K \)!

The unit group of \( \mathbb{Z}_K \) is usually very large!

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

**Theorem** (I. Sabl, A. Petzold, and R. Pollard, 1996). If \( d = 4 \), then (I I) can be transformed into finitely many quadratic Thue equations \( F_i(x_1, x_2) = 1 \) such that one of the roots of \( F_i(x_1, 1) \) belongs to \( L \).
Advantages:

- rank $\mathbb{Z}_2^* \leq 4$
- we can solve (II) within the arithmetic of $\mathbb{Z}$.

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

I. Gadal and K. Gyöngi (1999) proved that (II) 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 $S_5$.

**Problem.** Is it possible to solve (II) within the arithmetic of $\mathbb{Z}$?
Connection between the computation of the upper bound and its reduction.

6. To compute an upper bound for $B$ it is not necessary to use inequality (3). This happens if
   - no explicit lower bound for $|\Lambda|$ is available, e.g.
     - $p$-adic elliptic logarithms.
   - different methods yield different bounds.


Consider

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

The elliptic logarithm approach yields an inequality

$$|b_2 \Psi(P_2) + \ldots + b_r \Psi(P_r) + b_{r+1} \omega| < c_2 \exp(-c_1 B^3).$$

S. David's theorem implies an upper bound $B_D$ for $B$. On the other hand, Baker's approach implies a bound $\mu_0$ 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

$$\max \{ |b_2|, |b_3|, \ldots, |b_r| \} \leq c_3 \log \max \{ |x|, |y| \}, \text{ i.e.}$$

$$B \leq c_3 \log \mu_0 = B_D.$$
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>
<thead>
<tr>
<th>$k$</th>
<th>$r_k$</th>
<th>$B_D$</th>
<th>$B_H$</th>
</tr>
</thead>
<tbody>
<tr>
<td>108</td>
<td>1</td>
<td>$2.8 \cdot 10^{28}$</td>
<td>$1.8 \cdot 10^{41}$</td>
</tr>
<tr>
<td>225</td>
<td>2</td>
<td>$1.3 \cdot 10^{41}$</td>
<td>$4.5 \cdot 10^{41}$</td>
</tr>
<tr>
<td>1025</td>
<td>3</td>
<td>$5.5 \cdot 10^{60}$</td>
<td>$3.1 \cdot 10^{42}$</td>
</tr>
<tr>
<td>2089</td>
<td>4</td>
<td>$1.1 \cdot 10^{84}$</td>
<td>$7.7 \cdot 10^{42}$</td>
</tr>
<tr>
<td>-28279</td>
<td>5</td>
<td>$2.1 \cdot 10^{112}$</td>
<td>$2.0 \cdot 10^{42}$</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>$k$</th>
<th>$r_k$</th>
<th>$B_D$</th>
<th>$B_H$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>$8.9 \cdot 10^{23}$</td>
<td>$1.3 \cdot 10^{41}$</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>$5.8 \cdot 10^{39}$</td>
<td>$1.8 \cdot 10^{44}$</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>$2.4 \cdot 10^{60}$</td>
<td>$5.9 \cdot 10^{45}$</td>
</tr>
<tr>
<td>20</td>
<td>4</td>
<td>$2.1 \cdot 10^{86}$</td>
<td>$2.9 \cdot 10^{47}$</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$r$</th>
<th>$B_D$</th>
<th>$B_H$</th>
</tr>
</thead>
<tbody>
<tr>
<td>-203472</td>
<td>18487440</td>
<td>5</td>
<td>$2.3 \cdot 10^{111}$</td>
<td>$7.9 \cdot 10^{47}$</td>
</tr>
<tr>
<td>-1642032</td>
<td>628747920</td>
<td>6</td>
<td>$1.1 \cdot 10^{144}$</td>
<td>$2.1 \cdot 10^{49}$</td>
</tr>
<tr>
<td>-147952</td>
<td>21183760</td>
<td>7</td>
<td>$2.7 \cdot 10^{187}$</td>
<td>$1.1 \cdot 10^{47}$</td>
</tr>
<tr>
<td>-5818216808130</td>
<td>5401285759982786436</td>
<td>8</td>
<td>$8.67 \cdot 10^{224}$</td>
<td>$2.33 \cdot 10^{58}$</td>
</tr>
</tbody>
</table>
To reduce the upper bound it is not necessary to use (3).


Consider the Thue equation

$$F(x_1, x_2) = m$$  \hspace{1cm} (T1)

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

Assume you have already an upper bound $\gamma_0$ for

$$\max \{ |x_1|, |x_2| \}.$$

Let $\alpha$ be a zero of $F(x_1, 1)$ and order the conjugates

$$\alpha = \alpha^{(1)}, \ldots, \alpha^{(d)}$$

such that $\alpha^{(1)}, \ldots, \alpha^{(r_2)} \in \overline{\mathbb{Q}}, \alpha^{(r_2+1)}, \ldots, \alpha^{(d)} \in \mathbb{R}$.

Lemma. Let $(x_1, x_2) \in \mathbb{Z}^2$ a solution of (T1) such that $|x_2|$ is large enough. Then there exist $1 \leq u \leq r_2$ s.t.

$$|x_1 - \alpha^{(u)} x_2| < c_1 |x_2|^{-d+1}$$  \hspace{1cm} (T2)

$$c_2 |x_2| < |x_1 - \alpha^{(u)} x_2| < c_3 |x_2|$$

for $u \in \{ 1, \ldots, r_2 \}$.

Let $\varepsilon_1, \ldots, \varepsilon_d$ be a basis of $\mathbb{Z}^{\overline{\mathbb{Q}}}/(L = Q(\alpha))$ s.t.

$(x_1, x_2) \in \mathbb{Z}^2$ be a solution of (T1) with $|x_2|$ large enough.

Write

$$\mu^{(u)} = x_1 - \alpha^{(u)} x_2 = \mu^{(u)} \varepsilon_1 \cdots \varepsilon_d$$

for $u = 1, \ldots, d$.

It is easy to prove

$$\max \{ |\varepsilon_i| \leq c_4 \log |x_2| + c_5 \}$$

for $1 \leq i \leq d$. 

Let $\nu \in \{1, \ldots, 3\}\setminus \xi u_3$. Then

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

Hence

$$\left| \sum_{j=1}^{r} b_j \log |e_j^{(u)}| - \log |x_2| + \log \left| \frac{\mu^{(u)}}{\mu^{(w)} - \mu^{(u)}} \right| \right| < c_5 |x_2|^{-d} \quad \forall \nu \in \{1, \ldots, 3\}\setminus \xi u_3.$$ 

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

$$\left| b_j \frac{\xi}{\xi} + \gamma_1 \frac{\xi}{\xi} - b_3 \right| < c_6 |x_2|^{-d} < c_7 \exp (-d B + c_8) \quad \forall \nu = 2, \ldots, 4.$$ 

The reduction can be done by using continued fractions!

III. Epilogue

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

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

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

$$\forall \nu \in \{1, \ldots, 2000\} \quad (Y - 2(\cos \frac{2\nu}{4000})X) = \pm 1, \pm 4001.$$ 

This is a 2000 degree Thue equation!
Theorem (Yu. Bilu, G. Hanrot, P. Mouhier, ?) For \( n \geq 30 \) the \( n \)-th element of a Lucas or a Selmer sequence has a primitive divisor.

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

\[
U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \text{ if } n \text{ is even}
\]

\[
U_n = \begin{cases} 
\frac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } n \text{ is odd} \\
\frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{if } n \text{ is even}
\end{cases}
\]

\( p \) is a primitive divisor of \( U_n \) if \( p \mid (\alpha - \beta)U_1 \cdot \ldots \cdot U_{n-1} \).

Implementation:

- **KANT**: Thue over \( \mathbb{Z} \)
- **MAGMA**: Thue over \( \mathbb{Z} \), elliptic over \( \mathbb{Z}, \mathbb{Z}_5 \)
- **PARI**: Thue over \( \mathbb{Z} \)
- **SINGH**: elliptic over \( \mathbb{Z} \)
- **MAPLE**: restricted Thue over \( \mathbb{Z} \).
IV. Problems

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

Solution of Three equations over \( \mathbb{Z} \)

\[ = \]

Computation of parameters in an algebraic number field.

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

Let \( \mathcal{D} \) be a class of diophantine equations like:

\[
\begin{align*}
\{ & \text{True equations over } \mathbb{Z} \} = \text{True} \\
\{ & \text{Elliptic equations over } \mathbb{Z} \} = \text{Elliptic} \\
\{ & \text{Index form equations} \} = \text{Index} \\
\end{align*}
\]

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

Let \( \text{Solve}(\mathcal{D}) \) 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:

\[ \text{Sec}(\text{True}) \quad \text{Solve}(\text{True}) \]

\[ \text{Sec}(\text{Elliptic}) \quad \text{Solve}(\text{Elliptic}) \]

\[ \text{Sec}(\text{Index}) \quad \text{Solve}(\text{Index}) \]
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

\[ x^2 - x = y^5 - y. \]

Problem 5. Let \( T_0 = T_1 = 0, T_2 = 1, T_{n+2} = T_{n+1} + T_n. \)

We have \( T_0 = T_1 = 0, T_2 = 1, T_3 = 2, T_4 = 5, T_5 = 11, T_{16} = 3136 = 56^2 \)

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: \( T_n = \overline{T}_n \)