# Diophantine Equations

Michael E. Pohst

Institut für Mathematik
Technische Universität Berlin

May 24, 2013

# Mordell's equation

$$y^2 = x^3 + \kappa$$

is one of the classical diophantine equations. In his famous book Mordell already carries out investigations on determining all integer solutions $x, y$ for given $\kappa \in \mathbb{Z}$.

Mordell observed that the discriminant of the cubic polynomial

$$t^3 - 3xt - 2y$$

in the variable $t$ is

$$\Delta := -108\kappa \ .$$

Hence, it suffices to determine all monic cubic polynomials $g(t) = t^3 + at^2 + bt + c \in \mathbb{Z}[T]$ of discriminant $\Delta$.

# The case of irreducible polynomials $g(t)$

Any zero $\rho$ in $\bar{\mathbb{Q}}$ generates a cubic extension $F = \mathbb{Q}(\rho)$. The discriminant $d(g)$ of the minimal polynomial $g(t)$ of $\rho$ coincides with the discriminant of the equation order $\mathbb{Z}[\rho]$. We get

$$\Delta = d_F \lambda^2$$

for the discriminant $d_F$ of $F$ and some $\lambda \in \mathbb{Z}$. This yields a – usually small – list of candidates for $F$.

# Example I

When do a square and a cube only differ by 1?

This means to solve $y^2 = x^3 \pm 1$. In this case we have $\Delta = \mp 108$.

For $\Delta > 0$ there are only two totally real cubic fields with discriminants below 108, $d_F \in \{49, 81\}$. In each case the quotient $\Delta/d_F$ is not an integer.

For $\Delta = -108$ there is exactly one cubic field $F$ such that $\Delta/d_F$ is a square, namely $F = \mathbb{Q}(\sqrt[3]{-2})$ with $d_F = \Delta$. Hence, we need to determine all integers of $F$ of index $\pm 1$. We note that $1, \alpha = \sqrt[3]{-2}, \alpha^2$ is an integral basis of $F$.

# Index form equations

For the candidates $F$ of that list we need to test whether $o_F$ contains elements $\alpha$ whose minimal polynomials have a discriminant $\lambda^2 d_F$. Also, the trace $tr(\alpha)$ must be divisible by 3. We can generate $F$ by adjoining an element $\rho \in o_F$ to $\mathbb{Q}$ such that a $\mathbb{Z}$-Basis of $o_F$ is of the form

$$\omega_1 = 1\,,\ \omega_2 \;=\; \rho\,,\ \omega_3 = (\rho^2 + A\rho + B)/N\ .$$

Let

$$m_\rho(t) = t^3 - Ut^2 + Vt - W$$

be the minimal polynomial of $\rho$.

# Index form equations

We can assume that the candidates for $\alpha$ are of the form $\alpha = x\omega_2 + y\omega_3$. The corresponding discriminants satisfy

$$d(\alpha) = d(\rho)\left(x^3 + \frac{1}{N}A_{21}x^2y + \frac{1}{N^2}A_{12}xy^2 + \frac{1}{N^3}A_{03}y^3\right)^2 \ .$$

with $A_{21} = 2U + 3A$, $A_{12} = 3A^2 + 4Au + U^2 + V$, $A_{03} = A(A+U)^2 + V(A+U) - W$. We note that $d_E N^2 = d(\rho)$. We set $z = Nx$ and need to calculate solutions of the **index form equation**

$$z^3 + A_{21}z^2y + A_{12}zy^2 + A_{03}y^3 \ = \ \pm\lambda N^2 \ .$$

This equation is a so–called Thue equation. It has only finitely many solutions $(z, y) \in \mathbb{Z}^2$.

# Example of $F(x, y) = |\lambda|$ over $\mathbb{Z}$

$$
\begin{gathered}
x^3 + 611210797432150799284 9263\ x^2y\ + \\
12452621296588189269900266038037428582780346546733\ xy^2\ + \\
84568628808980564343951899932328789454828660147759928385569 \\
40143384916601\ y^3 \\
= \ 10533161204076626648936 97
\end{gathered}
$$

# Example of Mordell's equation

The curve $y^2 = x^3 + 1000000025$ has the solutions

$$(x, \pm y) \in \{ \begin{array}{l} (-1000, 5) \\ (-170, 31545) \\ (1271, 55256) \\ (2614, 137337) \\ (90000002000, 27000000900000005) \; \} \end{array}$$

# Thue equations

We discuss the computation of the solutions of an equation of the form

$$F(x,y) = m \text{ in } x,y \in \mathbb{Z}$$

for given $m \in \mathbb{Z}$. Here, $F(x,y) \in \mathbb{Z}[x,y]$ is an irreducible homogeneous polynomial of degree $n \geq 3$.

For simplicity's sake we assume that the coefficient of the leading term $x^n$ is 1, hence $z = x$.

If $\alpha^{(1)}, ..., \alpha^{(n)}$ denote the zeros of $F(x,1)$ in $\bar{\mathbb{Q}}$ then the polynomial $F(x,y)$ splits as follows:

$$F(x,y) = \prod_{j=1}^{n}(x - \alpha^{(j)}y) \ .$$

# Thue equations

We only consider the most difficult case in which $F(x,1)$ is irreducible in $\mathbb{Z}[x]$.

For solutions $(x,y) \in \mathbb{Z}^2$ we set $\beta^{(j)} = x - \alpha^{(j)} y \ \ (1 \leq j \leq n)$. We let

$$|\beta^{(i)}| = \min_{1 \leq j \leq n} |\beta^{(j)}| \ .$$

In order to make the presentation easier we assume $i = 1$ in the following.

# Thue equations

Because of $|\beta^{(1)}| \leq \sqrt[n]{|m|}$ we obtain for $1 < j \leq n$:

$$\begin{aligned} |\beta^{(j)}| &\geq |\beta^{(j)} - \beta^{(1)}| - |\beta^{(1)}| \\ &\geq |\alpha^{(j)} - \alpha^{(1)}||y| - \sqrt[n]{|m|} \\ &\geq |\alpha^{(j)} - \alpha^{(1)}||y|/2 \qquad , \end{aligned}$$

if $|y|$ is large enough, i.e. for $|y| > 2\sqrt[n]{|m|}/|\alpha^{(j)} - \alpha^{(1)}|$.
This implies

$$\left|\alpha^{(1)} - \frac{x}{y}\right| < \frac{c_1}{|y|^n} \text{ with } c_1 = \frac{2^{n-1}|m|}{\prod_{j=2}^{n} |\alpha^{(j)} - \alpha^{(1)}|} \ .$$

# Thue equations

What can we say about about the values $|\alpha^{(j)} - x/y|$ for $j > 1$?

We start with the elementary inequality $|\log(x)| < 2|x-1|$ which holds for $|x-1| < 0.795$.

Then we get

$$\log\left|\frac{\alpha^{(j)} - x/y}{\alpha^{(1)} - \alpha^{(j)}}\right| \;=\; \log\left|1 - \frac{\alpha^{(1)} - x/y}{\alpha^{(1)} - \alpha^{(j)}}\right| \;<\; \frac{2}{|\alpha^{(1)} - \alpha^{(j)}|}\left|\alpha^{(1)} - x/y\right| \;,$$

and consequently for sufficiently large $|y|$:

$$\log\left|x - \alpha^{(j)}y\right| \;<\; 2\log|y| \;.$$

# Thue's Theorem

**Theorem** For every $\varepsilon > 0$ there exists a constant $c > 0$ such that

$$\left|\alpha^{(j)} - \frac{x}{y}\right| > \frac{c}{|y|^{0.5(n+2)+\varepsilon}} \;\; (1 \leq j \leq n) \; .$$

# Thue equations

The calculation of all solutions became feasible only via Baker's lower estimates for linear forms in logarithms, about 60 years after Thue's result.

We let $F = \mathbb{Q}(\alpha^{(1)})$. By $\varepsilon_i \ (1 \leq i \leq r)$ we denote a full set of fundamental units of $F$. For all non–associate elements $\mu \in o_F$ of norm $\pm m$ and all roots of unity $\xi \in TU_F$ we then need to test, whether

$$\beta = \xi \mu \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$$

is a solution of the Thue equation.

# Thue equations

We set $A = \max(|a_1|, ..., |a_r|)$ and obtain a system of equations

$$a_1 \log|\varepsilon_1^{(j)}| + ... + a_r \log|\varepsilon_r^{(j)}| = \log\left|\frac{\beta^{(j)}}{\mu^{(j)}}\right| \quad (2 \le j \le r_1 + r_2)$$

in the variables $a_1, ..., a_r$.

We denote the corresponding matrix of coefficients by $\Gamma$ and let $\Gamma^{-1} = (u_{kj})$ with row norm $c_2$. This gives the following upper bound for $A$:

$$A \ \le \ c_2 \max \log\left|\frac{\beta^{(j)}}{\mu^{(j)}}\right| \ \le \ c_3 \log|y| \ .$$

In view of the previous slide we can choose $c_3 = 2c_2$ for sufficiently large values of $|y|$.

# Example I

We recall that $r = 1$ and calculate a fundamental unit $\varepsilon_1 = 1 - \alpha + \alpha^2 = 3.847$. The absolute values of the differences of disfferent roots all are $\sqrt[3]{2}\sqrt{3}$. The corresponding Thue equation is

$x^3 + 2y^3 = \pm 1.$

Any solution $\beta = x + \alpha y$ is of the form $\pm\varepsilon_1^{a_1}$ and we have $A = |a_1|$.

We get matrices $\Gamma = (\log|\varepsilon_1|) = (1.3474)$ and $\Gamma^{-1} = (1/\log|\varepsilon_1|) = (0.7422)$.

Therefore the first three constants are

$$c_1 = 0.84,\ c_2 = o.742,\ c_3 = 1.484\ .$$

# Siegel's identity

For $1 < k < \ell$ we divide Siegel's identity

$$(\alpha^{(1)} - \alpha^{(k)})\beta^{(\ell)} + (\alpha^{(k)} - \alpha^{(\ell)})\beta^{(1)} + (\alpha^{(\ell)} - \alpha^{(1)})\beta^{(k)} \ = \ 0$$

by the last summand on the left–hand side:

$$\frac{(\alpha^{(1)} - \alpha^{(k)})\beta^{(\ell)}}{(\alpha^{(1)} - \alpha^{(\ell)})\beta^{(k)}} - 1 \ = \ \frac{(\alpha^{(\ell)} - \alpha^{(k)})\beta^{(1)}}{(\alpha^{(1)} - \alpha^{(\ell)})\beta^{(k)}} \ .$$

From this we obtain an upper bound for the linear form in logarithms

$$\Lambda \ := \ \left| \log \left| \frac{(\alpha^{(1)} - \alpha^{(k)})\mu^{(\ell)}}{(\alpha^{(1)} - \alpha^{(\ell)})\mu^{(k)}} \right| + a_1 \log \left| \frac{\varepsilon_1^{(\ell)}}{\varepsilon_1^{(k)}} \right| + \ldots + a_r \log \left| \frac{\varepsilon_r^{(\ell)}}{\varepsilon_r^{(k)}} \right| \right| \ .$$

# Siegel's identity

Using equations and estimates from above we get

$$\Lambda \;<\; 2\left|\frac{(\alpha^{(1)}-\alpha^{(k)})\beta^{(\ell)}}{(\alpha^{(1)}-\alpha^{(\ell)})\beta^{(k)}}-1\right| \;=\; 2\left|\frac{(\alpha^{(\ell)}-\alpha^{(k)})\beta^{(1)}}{(\alpha^{(1)}-\alpha^{(\ell)})\beta^{(k)}}\right| \;\le c_4\exp(-c_5 A)$$

with

$$c_4 = 4c_1\left|\frac{\alpha^{(k)}-\alpha^{(\ell)}}{(\alpha^{(1)}-\alpha^{(k)})(\alpha^{(1)}-\alpha^{(\ell)})}\right|,\; c_5 = \frac{n}{c_3}\;.$$

On the other hand, Baker's method produces a lower bound of the form $\exp(-c_6 \log A)$.

From these two bounds we derive an upper bound $M$ for $A$. The latter is quite large, e.g. $> 10^{18}$.

# Baker's method

Let $\beta$ be a non–zero algebraic number with minimal polynomial $f(x) = b_0x^m + b_1x^{m-1} + ... + b_m \in \mathbb{Z}[x]$, i.e. $\gcd\{b_0, ..., b_m\} = 1$.

In $\bar{\mathbb{Q}}[x]$ we have $f(x) = b_0 \prod_{j=1}^{m}(x - \beta^{(j)})$ with $\beta = \beta^{(1)}$.

Then

$$h(\beta) := \frac{1}{m} \log \left( |b_0| \prod_{j=1}^{m} \max(1, |\beta^{(j)}|) \right)$$

is called the **absolute logarithmic height** of $\beta$.

# Theorem Baker/Wüstholz

Let $\alpha_1, ..., \alpha_k$ be non–zero algebraic numbers and $a_1, ..., a_k \in \mathbb{Z}$. For $1 \leq i \leq k$ we choose a branch of the complex logarithm such that

$$\Lambda \ := \ a_1 \log(\alpha_1) + ... + a_k \log(\alpha_k)) \ \neq \ 0 \ .$$

For $1 \leq i \leq k$ we set

$$A_i = \max\left\{ h(\alpha_i), \ \frac{1}{[\mathbb{Q}(\alpha_i : \mathbb{Q}]}, \frac{|\log(\alpha_i)|}{[\mathbb{Q}(\alpha_i : \mathbb{Q}]} \right\} \ .$$

**Theorem** For $D := [\mathbb{Q}(\alpha_1, ..., \alpha_k] : \mathbb{Q}]$ and $A := \max\{a_1, ..., a_k, e\}$ we have

$$\log|\Lambda| \ \geq \ -18(k+1)! k^{k+1} (32D)^{k+2} A_1 \cdots A_k \log(A) \ .$$

# Example I

We calculate constants

$$c_4 = 1.54,\ c_5 = 2.022\ .$$

The height $h(\varepsilon)$ becomes 1.283 and from Baker's Theorem we obtain

$$c_6 := -3.27 * 10^8\ .$$

The inequality $-c_6 \log(A) < \log(c_4) - c_5 A$ is violated for $A > 4 * 10^9$.

# Thue equations, Bilu and Hanrot

From the system of equations

$$a_1 \log|\varepsilon_1^{(j)}| + ... + a_r \log|\varepsilon_r^{(j)}| = \log\left|\frac{\beta^{(j)}}{\mu^{(j)}}\right| \quad (2 \leq j \leq r_1 + r_2)$$

we get

$$\begin{aligned} a_k &= \sum_{j=1}^r u_{kj} \log\left|\frac{x-\alpha^{(j)}y}{\mu^{(j)}}\right| \\ &= (\log|y|)\sum_{j=1}^r u_{kj} + \sum_{j=1}^r u_{kj}\left(\log\left|\frac{\alpha^{(j)}-\frac{x}{y}}{\alpha^{(i)}-\alpha^{(j)}}\right| + \log\left|\frac{\alpha^{(i)}-\alpha^{(j)}}{\mu^{(j)}}\right|\right) \ . \end{aligned}$$

# Thue equations, Bilu and Hanrot

We set

$$\delta_k := \sum_{j=1}^{r} u_{kj},\ \nu_k := \sum_{j=1}^{r} u_{kj} \log\left|\frac{\alpha^{(i)}-\alpha^{(j)}}{\mu^{(j)}}\right|, c_6 := 2c_1 \sum_{j=1}^{r}\left|\frac{u_{kj}}{\alpha^{(i)}-\alpha^{(j)}}\right| ,$$

and the equation for $a_k$ yields the inequality

$$|\delta_k \log|y| - a_k + \nu_k| < c_6 \exp(-c_5 A) .$$

From two such inequalities, say for conjugates $k, \ell$, we eliminate $\log|y|$.

# A lemma of Davenport

The result is an inequality of the form

$$|a_k\vartheta + a_\ell - \delta| < c_7 \exp(-c_5 A)$$

with $\vartheta = -\delta_\ell/\delta_k$, $\delta = (\delta_k\nu_\ell - \delta_\ell\nu_k)/\delta_k$, $c_7 = c_6(\delta_k + \delta_\ell)/\delta_k$.

Then the huge bound for $A$ can be drastically reduced.
**Lemma** Let $M, B, q$ be positive integers satisfying

$$1 \le q \le MB,\ \| q\vartheta \| < 2(MB)^{-1},\ \| q\delta \| > 3/B\ .$$

Then the previous inequality has no solutions $a_k, a_\ell$ with

$$\frac{\log(MB^2c_7)}{c_5} \le A \le M\ .$$

Appropriate starting values are the upper bound $M$ for $A$ and $B = 1000$.
$q$ can be detected as the denominator of a convergent of the continuous fraction expansion of $\vartheta$.

# Example of an index form equation

The Thue equation

$$
\begin{aligned}
&x^3+\\
&6112107974321507992849263 * x^2y+\\
&1245262129658818926990026603803742858278034654673 3 * xy^2+\\
&845686288089805643439518999323287894548 28\\
&\quad 6601477599283855694014338491660 1 * y^3\\
&= 1053316120407662664893697
\end{aligned}
$$

has no solutions.