$$\delta_Q(0) \approx \left(\frac{1}{2\pi}\int_{-\infty}^{+\infty} \left|K\left(\frac{1}{2}+it\right)\right|^2 dt\right)^{-1} a^2(1)\log Q,$$
$$\delta_Q(0) \sim \left(\frac{1}{2\pi}\int_{-\infty}^{+\infty} \left|K\left(\frac{1}{2}+it\right)\right|^2 dt\right)^{-1} a^2(1)\log Q, \tag{20}$$

and if $\alpha \neq 0$, $\delta_Q(\alpha) \to 0$. Furthermore

$$\int_{-\infty}^{+\infty} \delta_Q(\alpha)\, d\alpha = \frac{Q\log Q}{N_K(Q)}\int_0^{+\infty} a^2(u)du = 1 \quad \text{for all } Q, \tag{21}$$

the last step being achieved through the use of Plancherel's Theorem for the Mellin transform in the form

$$\frac{1}{2\pi}\int_{-\infty}^{+\infty} \left|K\left(\frac{1}{2}+it\right)\right|^2 dt = \int_0^{+\infty} a^2(u)du. \tag{22}$$

References

[1] *H. Davenport,* Multiplicative Number Theory, Second edition, Berlin—Heidelberg—New York 1980.

[2] *P.X. Gallagher,* Pair correlation of zeros of the zeta function. J. reine angew. Math. **362** (1985), 72—86.

[3] *D.A. Goldston,* On the pair correlation conjecture for zeros of the Riemann zeta-function. J. reine angew. Math. **385** (1988), 24—40.

[4] *D.R. Heath–Brown,* Gaps between primes, and the pair correlation of zeros of the zeta–function. Acta Arithmetica **41** (1982), 85—99.

[5] *H.L. Montgomery,* The pair correlation of zeros of the zeta function. Proc. Sympos. Pure. Math. Vol. 24, Amer. Math. Soc., Providence, RI, 1973, 181—193.

[6] *A.M. Odlyzko,* On the distribution of spacings between zeros of the zeta function. Mathematics of Computation, Vol. 48, **117** (1987), 273—308.

[7] *A.E. Özlük,* Pair correlation of zeros of Dirichlet L–functions. Ph.D. Thesis, University of Michigan, 1982.

Department of Mathematics, University of Maine, 418 Neville Hall, Orono, ME 04469

Computational Methods For the Resolution of Diophantine Equations

Attila Pethö [1]

1. Introduction

Recently, considerable progress was made in the practical resolution of large classes of diophantine equations. Several authors worked out methods based on combinations of results in the following fields.

1. Applications of lower bounds for linear forms in the logarithms of algebraic numbers to establish effective upper bounds for the solutions of large classes of diophantine equations.
2. New algorithms for the solution of diophantine approximation problems.
3. New algorithms in algebraic number theory.

The most important tool of the methods are the lower bounds for linear forms in the logarithms as well as p–adic logarithms of algebraic numbers. Gelfond [21] proved a bound in the complex case for two algebraic numbers. This was completely generalized by Baker [1]. He himself [3] and [4], Waldschmidt [41] and recently Blass, Glass, Manski, Meronk and Steiner [8], [9] gave improvements and refinements. From a computational point of view, the last three papers are the most important because the occurring absolute constants are not too large.

Similarly to the complex case lower bounds for linear forms of p–adic logarithms of algebraic numbers were found. Schinzel [35] proved such a result for two numbers,

[1] Research supported by Hungarian National Foundation for Scientific Research grant no. 273/86.

Kaufman [24] obtained the general case. Van der Poorten [34] and Yu [40] gave the best lower bounds, so far.

Using these results several authors found effective upper bounds for solutions of large classes of diophantine problems. For references we refer to the books of Baker [5], Györy [22] and Shorey and Tijdeman [36]. These types of results make it theoretically possible to find all solutions because one has to check only finitely many possibilities. But finitely many may be so many that a direct search is hopeless. As we shall see later a typical upper bound is 10^{30} even in the most modest cases.

Baker and Davenport [6], Ellison [14] and Ellison *et al.* [15] used continued fraction expansion of suitable real numbers to reduce Baker's upper bound to a much smaller one, and finally to solve some diophantine problems. Although Ellison [14] pointed out that his method is applicable in higher dimensions too, and a lot of interesting applications of Baker's method were found, only a little progress was made in the numerical resolution of diophantine problems.

The lattice basis reduction algorithm of Lenstra, Lenstra Jr. and Lovász [25] solves multidimensional diophantine approximation problems. Several mathematicians realized independently that this algorithm is applicable combined with Baker–type upper bounds for the complete resolution of diophantine equations.

Baker and Davenport [6] determined all common terms in two second order linear recurrence sequences and so solved a system of Pell's equations. Pethö [27], [28] computed all third and fifth powers in the Fibonacci sequence. These are the only cases when forward searches were used to exclude large solutions. Ellison [14], Ellison *et al* [15] and Steiner [37] solved third degree; Blass *et al* [7], Pethö and Schulenberg [32], Tzanakis and de Weger [39] and Zagier [46] solved fourth degree Thue equations. In many of the above papers the results were used to find all integer points on elliptic curves. Gaál [18] described a method to solve third degree inhomogeneous Thue equations. Gaál and Schulte [19] and Gaál *et al* [20] computed all power bases in several third and fourth degree number fields by solving completely the corresponding index form equations. Cherubini and Walliser [11] used the reduction method to find all imaginary quadratic fields with class number one.

P–adic linear form estimates and computer search were applied by Pethö [29], and Pethö and de Weger [33] and by de Weger [42] to find prime powers as well as products of prime powers in second order linear recurrences. De Weger [43] solved S–unit equations over $\mathbb{Z}$ and tested numerically the Oesterlé–Masser conjecture. Finally de Weger [45] used the combination of complex and p–adic arguments to solve third degree Thue–Mahler equations.

In this paper we describe the common ideas in the methods of the above papers. In section 2 we give the outline of the method. Sections 3 and 4 deal with the general components of the method; we cite the best known lower bound for linear forms in the logarithms of algebraic numbers, as well as the application of the lattice basis reduction algorithm of Lenstra, Lenstra Jr. and Lovász [25] to the reduction of a large upper bound for the solution of diophantine inequalities. The method of section 2 has two problem–specific components, we illustrate them in section 5 on Thue equations. Finally, in section 6, we report on a conjecture on the representation of one by cubic forms.

2. General Description of the Method

In the sequel we shall deal only with the classical complex case, for p–adic variants we refer to the thesis of de Weger [44].

Let K be an algebraic number field of degree k over $\mathbb{Q}$—the field of rational numbers—and let G be the normal closure of K. Let $\mathbb{Z}_K$ denote the ring of integers of K and $\alpha^{(1)},\ldots,\alpha^{(k)}$ denote the conjugates of $\alpha \in K$. Finally, let $\varepsilon_1,\ldots,\varepsilon_r$ be a system of independent units of $\mathbb{Z}_K$. With this notation the methods used in the papers mentioned above can be divided into four steps.

1. Transformation of the original problem to finitely many unit equations of type

$$\alpha_1\left(\frac{\varepsilon_1^{(i)}}{\varepsilon_1^{(q)}}\right)^{n_1}\cdots\left(\frac{\varepsilon_r^{(i)}}{\varepsilon_r^{(q)}}\right)^{n_r}+\alpha_2\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(q)}}\right)^{m_1}\cdots\left(\frac{\varepsilon_r^{(j)}}{\varepsilon_r^{(q)}}\right)^{m_r}=1, \qquad (1)$$

where $1\le i, j, q \le k$, $n_h, m_h \in \mathbb{Z}$ $(h=1,\ldots,r)$ and α_1, α_2 are fixed elements from G.

2. If $N_0 \le N = \max\{|n_1|,\ldots,|n_r|\} \le M = \max\{|m_1|,\ldots,|m_r|\}$, then taking the logarithm we get finitely many inequalities

$$\left| n_1 \log\left(\frac{\varepsilon_1^{(i)}}{\varepsilon_1^{(q)}}\right) + \ldots + n_r \log\left(\frac{\varepsilon_r^{(i)}}{\varepsilon_r^{(q)}}\right) + \log \alpha_1 \right| < c_1 \exp(-c_2 N), \tag{2}$$

where c_1, c_2 are constants. If $N \ge M$, then we have to exchange the role of N and M.

Using a suitable effective lower bound for linear forms in the logarithms of algebraic numbers compute an upper bound N_1 for N from (2).

3. Reduce N_1 iteratively until either the new bound will be smaller than N_0 or the iteration does not give a better bound. For the reduction, one can use numerical diophantine approximation techniques.

4. Search for the actual solutions either solving (2) in the remaining range or using specific properties of the original problem.

We remark that steps 1 and 4 depend strongly on the original problem, while the other two steps can be done automatically.

3. A Lower Bound For Linear Forms in the Logarithms of Algebraic Numbers

The first general, non–trivial component in the method is the lower bound for linear forms in the logarithms of algebraic numbers. In this section we cite the best known general bound due to Blass *et al* [8]. We shall mention that until today most of the applications used a weaker theorem of Waldschmidt [41].

Let $\alpha_1,\ldots,\alpha_n$, $\beta_0, \ldots, \beta_n$ be algebraic numbers with $\alpha_1,\ldots,\alpha_n$ non–zero. Let

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + \ldots + \beta_n \log \alpha_n$$

and $D = [K : \mathbb{Q}]$, where $K = \mathbb{Q}(\alpha_1,\ldots,\alpha_n, \beta_0,\ldots,\beta_n)$. Let $h(\alpha)$ be the absolute logarithmic height of the algebraic number α. Define

2. If $N_0 \le N = \max\{|n_1|,\dots,|n_r|\} \le M = \max\{|m_1|,\dots,|m_r|\}$, then taking the logarithm we get finitely many inequalities

$$\left| n_1 \log\left(\frac{\varepsilon_1^{(i)}}{\varepsilon_1^{(q)}}\right) + \dots + n_r \log\left(\frac{\varepsilon_r^{(i)}}{\varepsilon_r^{(q)}}\right) + \log \alpha_1 \right| < c_1 \exp(-c_2 N), \tag{2}$$

where c_1, c_2 are constants. If $N \ge M$, then we have to exchange the role of N and M.

Using a suitable effective lower bound for linear forms in the logarithms of algebraic numbers compute an upper bound N_1 for N from (2).

3. Reduce N_1 iteratively until either the new bound will be smaller than N_0 or the iteration does not give a better bound. For the reduction, one can use numerical diophantine approximation techniques.

4. Search for the actual solutions either solving (2) in the remaining range or using specific properties of the original problem.

We remark that steps 1 and 4 depend strongly on the original problem, while the other two steps can be done automatically.

3. A Lower Bound For Linear Forms in the Logarithms of Algebraic Numbers

The first general, non–trivial component in the method is the lower bound for linear forms in the logarithms of algebraic numbers. In this section we cite the best known general bound due to Blass *et al* [8]. We shall mention that until today most of the applications used a weaker theorem of Waldschmidt [41].

Let $\alpha_1,\dots,\alpha_n$, $\beta_0, \dots, \beta_n$ be algebraic numbers with $\alpha_1,\dots,\alpha_n$ non–zero. Let

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + \dots + \beta_n \log \alpha_n$$

and $D = [K:\mathbb{Q}]$, where $K = \mathbb{Q}(\alpha_1,\dots,\alpha_n, \beta_0,\dots,\beta_n)$. Let $h(\alpha)$ be the absolute logarithmic height of the algebraic number α. Define

$$V_1 = \max\left\{ h(\alpha_1), \frac{1}{D}, \frac{|\log \alpha_1|}{D} \right\}$$

and

$$V_{j+1} = \max\left\{ h(\alpha_{j+1}), V_j, \frac{|\log \alpha_{j+1}|}{D} \right\} \quad (1 \le j \le n-1).$$

Let $a_j = \dfrac{DV_j}{|\log \alpha_j|}$ $(1 \le j \le n)$ and $\dfrac{1}{a} = \dfrac{1}{n}\sum_{j=1}^{n} \dfrac{1}{a_j}$. Let $V_j' = jV_j$, $V_0^+ = \overline{V}_0 = 1$, $V_j^+ = \max\{V_j, 1\}$ and $\overline{V}_j = \max\{V_j', 1\}$. Let $W = h(\beta_j)$ $(0 \le j \le n)$ and q be a prime number. Let $\overline{E}_2 = \min\{e^{qDV_1}, 2qa\}$ and $\overline{M} = 2(2^6 q^2 nD\overline{V}_{n-1}\overline{E}_2)^n$. Finally, let

$$x_n^* = \begin{cases} \log(2^{13}\overline{V}_1), & \text{if } n = D = 1 \\ n^2(n+1)\log\left(\dfrac{6n}{\log D}\right) + n(n+1)\log(n!) + \log n, & \text{if } D \ge 2 \\ n^2(n+1)\log(9n) + n(n+1)\log(n!) + \log n, & \text{if } D = 1 < n. \end{cases}$$

Theorem 1. *(Blass et al [8]) If $\Lambda \ne 0$, then*

$$|\Lambda| > \exp\left\{ -C_1(n) D^{n+2} \frac{V_1 \dots V_n}{(\log \overline{E}_2)^{n+1}} (\log \overline{M})(W + C_2(n)) \right\}$$

where

$$C_1(n) = \begin{cases} n^{2n+1}(24e^2)^n 2^{20}, & \text{if } n \ge 3 \\ n^{2n+1}(24e^2)^n 2^{21}, & \text{if } n < 3 \end{cases}$$

and

$$C_2(n) = n(n+1)\log(D^3\overline{V}_n) + \frac{x_n^*}{n}.$$

4. Reduction of the Large Upper Bound

Now let us turn our attention to step 3 of the algorithm of section 2. In the sequel we assume that the left hand side of (2) does not vanish, $\alpha_1 \ne 1$ and $r \ge 2$. Dividing (2) by $\log(\varepsilon_r^{(i)}/\varepsilon_r^{(q)})$ we get

$$0 \neq \left| n_1\delta_1 + \ldots + n_{r-1}\delta_{r-1} + n_r + \delta_{r+1} \right| < c_3 \exp(-c_2 N), \tag{3}$$

where $\delta_h = \dfrac{\log\left(\dfrac{\varepsilon_h^{(i)}}{\varepsilon_h^{(q)}}\right)}{\log\left(\dfrac{\varepsilon_r^{(i)}}{\varepsilon_r^{(q)}}\right)}$, $h = 1,\ldots,r-1$ and $\delta_{r+1} = \dfrac{\log \alpha_1}{\log\left(\dfrac{\varepsilon_r^{(i)}}{\varepsilon_r^{(q)}}\right)}$.

The following lemma is the generalization of a lemma of Baker and Davenport [6]. For the proof see Pethö and Schulenberg [32].

Lemma 1. *Let Q_1, Q_2 and Q_3 be real numbers such that $Q_2 \geq 1$, $Q_1 > 2^{r-1}((r-1)Q_2 + 1)$. If there exists an integer q with*

$$1 \leq q \leq Q_1 Q_3 \tag{4}$$

$$\left\| q\delta_i \right\| \leq Q_2 (Q_1 Q_3)^{-1/(r-1)}, \quad i = 1,\ldots,r-1 \tag{5}$$

and

$$\left\| q\delta_{r+1} \right\| \geq ((r-1)Q_2 + 1) Q_1^{-1/(r-1)} \tag{6}$$

then (3) has no solutions $n_1,\ldots,n_r \in \mathbb{Z}$ with

$$\frac{\log (Q_1^{r/(r-1)} Q_3 c_3)}{\log c_2} < N \leq Q_3^{\frac{1}{r-1}}, \tag{7}$$

where $N = \max\left\{|n_1|,\ldots,|n_r|\right\}$ and $\|x\|$ denotes the distance of the real number x to the nearest integer.

If $r = 2$ then the $t-$th denominator q_t with $q_t \leq Q_1 Q_3 < q_{t+1}$ of the continued fraction expansion of δ_1 solves (4) and (5) with $Q_2 = 1$. In the general case one can use the LLL lattice basis reduction algorithm of Lenstra, Lenstra Jr. and Lovász [25] or its modified version by de Weger [43]. The following theorem is a reformulation of Proposition (1.39) of Lenstra, Lenstra Jr. and Lovász [25].

Theorem 2. *Let* $\boldsymbol{b}_1 = p_1\boldsymbol{e}_1 + \ldots + p_{r-1}\boldsymbol{e}_{r-1} + q\boldsymbol{d}$, $\boldsymbol{b}_2, \ldots, \boldsymbol{b}_r$ *be an LLL–reduced basis of the lattice spanned by the column vectors* $\boldsymbol{e}_i$, $i = 1, \ldots, r-1$ *whose* i*–th coordinate is* 1 *all others* 0 *and by*

$$\boldsymbol{d} = (-\delta_1, \ldots, -\delta_{r-1}, 2^{r/4}(Q_1Q_3)^{-r/(r-1)})^T.$$

Then q *solves* (4) *and* (5) *with* $Q_2 = 2^{r/4}$.

The reduction procedure works in practice in the following way. Assume that we want to solve (1) with $N \le M$ and $N_0 \le N \le N_1$, where N_1 is much larger than N_0.

(i) Compute $\delta_1, \ldots, \delta_{r-1}, \delta_{r+1}$ with the required (high) accuracy, see Pethö and Schulenberg [32] Lemma 3. Put $Q_2 = 2^{r/4}$ and $Q_1 = (10r\,Q_2^{r})^{r-1}$.

(ii) Put $Q_3 = N_1^{r-1}$ and solve the diophantine approximation problem (4), (5) using the LLL–reduction.

(iii) If (6) holds, then let S be the smallest value of Q_1 with (4) and (5) and put $N_2 = \dfrac{\log(S^{r/(r-1)}Q_3c_3)}{\log c_2}$, otherwise let $N_0 = N_1$ and terminate.

If the algorithm terminates at (iii) then, as Baker and Davenport [6] pointed out, the solutions of (3) can be found by solving a linear diophantine equation. The occurrence of this case was never reported in the literature.

De Weger [43] discussed the cases, when $r = 1$ or $\alpha_1 = 1$ or when $\delta_1, \ldots, \delta_{r-1}, \delta_{r+1}$ are linearly dependent over $\mathbb{Q}$. Tzanakis and de Weger [39] used another reduction technique, which was also based on the LLL basis reduction algorithm. The key idea of their reduction technique is, that small values of the linear form

$$n_1\delta_1 + \ldots + n_r\delta_r + \delta_{r+1}$$

correspond to short vectors of an appropriately defined lattice.

5. Thue Equations

So far we focussed our attention on the general elements of the method from section 2. In this section we shall describe, using the example of Thue equations, how to transform them into finitely many unit equations, and how to find their "small" solutions. Here, small means the magnitude of 10^{100}, because the reduction procedure of section 4 cannot give a better upper bound in this case.

Let $F(x,y)=a_0x^k+a_1x^{k-1}y+\ldots+a_ky^k\in\mathbb{Z}[x,y]$ be irreducible over $\mathbb{Q}[x,y]$, $k\geq 3$ and $0\neq m\in\mathbb{Z}$. The diophantine equation

$$F(x,y)=m \tag{8}$$

is called a Thue equation. Thue [38] proved that (8) has finitely many solutions $x,y\in\mathbb{Z}$. Baker [2] has given an effectively computable upper bound for $\max\{|x|,|y|\}$. In the transformation of (8) into finitely many unit equations we use Baker's method, which was refined by Györy and Papp [23].

5.1 Transformation of (8) to finitely many unit equations

Let β be a root of $F(x,1)$ and $K=\mathbb{Q}(\beta)$, then $[K:\mathbb{Q}]=k$. To avoid technical difficulties, we assume in the sequel that K is totally real. Let $r=k-1$, and ξ be the group generated by the multiplicatively independent units $\varepsilon_1,\ldots,\varepsilon_r$ of norm 1 of $\mathbb{Z}_K$. Let $|\bar{\tau}|=\max\left\{\left|\tau^{(i)}\right|,\ 1\leq i\leq k\right\}$. Take

$$c_4=\max\left\{\log|\bar{\varepsilon}_i|,\ 1\leq i\leq r\right\},$$

$$c_5=\prod_{j=1}^{r}\max\left\{\log|\bar{\varepsilon}_j|,\ 1\right\},$$

$$M=\frac{m}{a_0}.$$

The following lemma is easy to prove using the geometrical representation of K (see Györy and Papp [23]).

Lemma 2. *There exists a finite set $\mathcal{A}\subset K$ with the following properties*

(i) *If* $x, y \in \mathbb{Z}$ *is a solution of* (8) *then there exist* $\gamma \in \mathcal{A}$ *and* $b_1, \ldots, b_r \in \mathbb{Z}$ *with*

$$x - By = \gamma \varepsilon_1^{b_1} \ldots \varepsilon_r^{b_r}, \tag{9}$$

(ii) *For all* $\gamma \in \mathcal{A}$ $\mathrm{Norm}_{K/\mathbb{Q}}(\gamma) = M$ *and* $O \log \left| M^{-1/k} \gamma \right| \leq \frac{r c_4}{2}$.

Let $I = \{1, \ldots, k\}$ and fix a $u \in I$. Let $T_{u,j} = \left| \beta^{(u)} - \beta^{(j)} \right|$ for all $j \in I$, $0 < t_u < \min \{T_{u,j}, j \in I, j \neq u\}$ and $T_u = T_{u,q} = \max \{T_{u,j}, j \in I\}$. With this notation it is easy to prove the following lemma.

Lemma 3. *Let* $x, y \in \mathbb{Z}$, $y \neq 0$ *be a solution of* (8) *with* $\left| x - \beta^{(u)} y \right| < \left| x - \beta^{(j)} y \right|$ *for all* $j \in I \setminus \{u\}$ *and with* $\left| x - \beta^{(u)} y \right| \leq T_u |y|$. *Then*

$$\left| x - \beta^{(u)} y \right| \leq \left(\left| M \right| \prod_{\substack{j=1 \\ j \neq u}}^{k} \frac{1}{T_{u,j} - t_{u,j}} \right) \frac{1}{|y|^{k-1}} = c_6 |y|^{-k+1}. \tag{10}$$

Further, if $|y| > Y_0 \geq \max \left\{ \left(\frac{2c_6}{T_u} \right)^{1/(k-1)}, \left(\frac{8c_6}{t_u} \right)^{1/k}, T_u \right\}$ *also holds, then*

$$\left| x - \beta^{(u)} y \right| \leq (1 + T_{u,j}) |y|, \text{ for all } j \in I \tag{11}$$

and

$$\left| x - \beta^{(q)} y \right| > \frac{T_u |y|}{2}. \tag{12}$$

In the sequel denote by R the regulator of ξ, (9) and (11) imply

$$\left| \gamma^{(j)} \varepsilon_1^{(j)b_1} \ldots \varepsilon_r^{(j)b_r} y \right| \leq (1 + T_u) |y|$$

for all $j \in I$. Taking the logarithm we get

$$\log |y| \geq \frac{R}{r! c_5} B - \log \left(\left| \gamma^{-1} \right| (1 + T_u) \right), \tag{13}$$

where $B = \max \{ |b_1|, \ldots, |b_r| \}$. Now fix a $j \in I \setminus \{u, q\}$, then

$$(\beta^{(q)}-\beta^{(j)})(x-\beta^{(u)}y)+(\beta^{(u)}-\beta^{(q)})(x-\beta^{(j)}y)=(\beta^{(u)}-\beta^{(j)})(x-\beta^{(q)}y)$$

holds. Using the conjugates of (9) and dividing the last equation by $(\beta^{(u)}-\beta^{(j)})\times(x-\beta^{(q)})$ we get the required unit equation. This implies, from (10) and (12), that

$$\left|\frac{\beta^{(u)}-\beta^{(q)}}{\beta^{(u)}-\beta^{(j)}}\frac{\gamma^{(j)}}{\gamma^{(q)}}\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(q)}}\right)^{b_1}\cdots\left(\frac{\varepsilon_r^{(j)}}{\varepsilon_r^{(q)}}\right)^{b_r}-1\right|\le\frac{4c_6}{t_u}|y|^{-k}.$$

Now let

$$\xi_\nu(u,q,j,\gamma)=\xi_\nu=\begin{cases}\dfrac{\varepsilon_\nu^{(j)}}{\varepsilon_\nu^{(q)}} & \text{, if } 1\le\nu\le r\\[2ex] \dfrac{\beta^{(u)}-\beta^{(q)}}{\beta^{(u)}-\beta^{(j)}}\dfrac{\gamma^{(j)}}{\gamma^{(q)}} & \text{, if } \nu=r+1\end{cases}$$

$$c_7=\log\left(\frac{8c_6}{t_u}\right)+k\log(|\overline{\gamma^{-1}}|(1+T_u))$$

$$c_8=\frac{kR}{r!\,c_5}$$

$$B_0=\frac{r!\,c_5}{R}(\log Y_0+\log(|\overline{\gamma^{-1}}|(1+T_u))),$$

Then we have the following:

Theorem 2. *Let $x,y\in\mathbb{Z}$ be a solution of* (8) *and let $\gamma\in\mathcal{A}$, $b_1,\dots,b_r\in\mathbb{Z}$ defined by* (9). *If $B=\max\{|b_1|,\dots,|b_r|\}>B_0$, then there exist pairwise distinct indices $1\le u,q,j\le k$ such that*

$$0<\left|b_1\log|\delta_1|+\dots+b_r\log|\delta_r|+\log|\delta_{r+1}|\right|<\exp(c_8-c_9B).\qquad(14)$$

The example of Thue equations shows that the method of section 2 is applicable for polynomial diophantine equations, too. Furthermore, this is the only known general method for the complete resolution of Thue equations. Although we must remark that

the transformation is very redundant. Namely, Bombieri and Schmidt [10] proved that the number of solutions of (8) is $O(k)$. Further, Everste and Győry [17] proved that if K and m are fixed then there exist only finitely many inequivalent forms $F(x, y) \in \mathbb{Z}$ with splitting field K such that the number of solutions of (9) is larger than 2.

In spite of this, the above described transformation yields $O(k^2)$ essentially different unit equations because we have to choose two parameters u and q independently. Hence most of the solutions of the linear form inequalities (14) correspond, by (9), either to the same solutions or do not give solutions of (8).

To find the solutions of (8) with some hundred or thousand decimal digits there is a much more economical method. Using it we have to solve only $O(k)$ diophantine approximation problems. We shall describe it in the next section.

5.2 Continued fraction method for the computation of small solutions of (8)

It is clear form the preceding section that (8) implies (14) only if $\max\{|x|, |y|\}$, and consequently B, is large enough. Furthermore, the reduced upper bound for B implies by (9) an upper bound for $\max\{|x|, |y|\}$ which is of magnitude from 10^{100} to 10^{1000}. To find the solutions of (8) up to such an upper bound one can use another reduction technique based on the continued fraction expansion of the real roots of $F(x, 1)$.

Let $u \in I$ be fixed such that $\beta^{(u)}$ is real and for $h > 0$ define the polynomial

$$H_h(t) = \prod_{\substack{j=1 \\ j \neq u}}^{k} (T_{u,j} - t) - t^{k-2} \left| \frac{m}{a_0} \right|^{2/k} \frac{1}{h}.$$

$\beta^{(u)} = [b_0; b_1, \ldots]$ will denote the simple continued fraction expansion of the irrational number β, while $\frac{p_n}{q_n}$ the $n-$th convergent to β. With this notation we have:

Theorem 3 [30]. *Let y_0 be a given real number, and $(x, y) \in \mathbb{Z}^2$ a solution of the inequality*

$$|F(x, y)| \leq m$$

with $\left|x - \beta^{(u)} y\right| \le \left|x - \beta^{(i)} y\right|$ $(i = 1,\ldots,k)$, *such that* $y \neq 0$, $(x, y) = 1$ *and* $|y| \le y_0$. *Let* $\beta^{(u)} = [b_0; b_1, \ldots, b_v, \ldots]$, *where* v *is chosen so that* $q_{v-1} > y_0$. *Let* $w \ge 1$, $B = \max_{w \le j \le v} b_j$, *and let* $T = T_{\alpha^{(u)}}$ *be the smallest positive root of* $H_{1/2}(t)$. *Then either*

$$|y| \le \min\left\{y_0, \frac{1}{T}\left|\frac{m}{a_0}\right|^{1/k}\right\}$$

or $\frac{x}{y}$ *is a convergent to* α *with*

$$|y| \le \max\left\{q_{w-1}, \frac{1}{T}\left|\frac{m}{a_0}\right|^{1/k}\left(\frac{B+2}{2}\right)^{1/(k-2)}\right\}.$$

We remark that in the reduction based on Theorem 3 we do not compute the exact value of the denominators of the convergents, only the partial quotients. This observation speeds up the method essentially.

5.3 Results

Using variants of the method described in the preceding sections Ellison *et al* [15], Steiner [37] and Pethö and Schulenberg [32] solved several third degree Thue equations. Gaál and Schulte [19] computed all power bases in totally real cubic fields with discriminant at most 3137 solving also third degree Thue equations.

Pethö and Schulenberg [32] and Tzanakis and de Weger [39] solved the following fourth degree Thue equations:

$F(x, y)$	m	solutions (x, y)
$x^4 + 5x^3y + 4x^2y^2 - 5xy^3 - y^4$	1	$(\pm1,0)$; $(\pm2,+1)$
	-1	$(0,+1)$
$x^4 - 4x^3y + 8xy^3 - y^4$	1	$(\pm1,0)$
	-1	$(\pm2,\pm1)$; $(0,+1)$
$x^4 + x^3y - 3x^2y^2 - xy^3 + y^4$	1	$(\pm1,0)$; $(0,\pm1)$
	-1	$(\pm2,+1)$; $(\pm1,\pm2)$; $(\pm1,\pm1)$; $(\pm1,+1)$
$x^4 - 4x^3y - 12x^2y^2 + 4y^4$	1	$(\pm1,0)$
$x^4 - 12x^3y - 8xy^3 + 4y^4$	1	$(\pm1,0)$; $(\pm1,+1)$; $(\pm1,\pm3)$; $(\pm3,+1)$

6. Representation of One by Cubic Forms

Numerical methods are useful not only to solve completely diophantine equations but also for finding solutions up to a prescribed large upper bound. Using the continued fraction reduction of section 5.2 we computed (*cf.* Pethö [31]) the solutions with $|y| < 10^{41}$ of approximately 3000 equations of type

$$f(x, y) = 1,$$

where the discriminant D_f of $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \in \mathbb{Z}[x, y]$ is positive. A form with $a = d = 1$ will be called reversible.

Two cubic forms $f_1(x, y)$, $f_2(x, y) \in \mathbb{Z}[x, y]$ are called equivalent if there exist integers a_1, a_2, a_3, a_4 with $|a_1a_4 - a_2a_3| = 1$ such that

$$f_2(x, y) = f_1(a_1x + a_2y, a_3x + a_4y).$$

Summarizing the observations we conjecture the following connection between cubic forms $f(x, y)$ with $D_f > 0$ and the number of solutions N_f of (1)

$$N_f = \begin{cases} 0,1,2 \text{ or } 3, & \text{if } f \text{ is not equivalent to a reversible form} \\ 2,3,4 \text{ or } 5, & \text{if } f \text{ is equivalent to a reversible form} \\ 6, & \text{if } D_f = 81,229,257,361, ? \\ 7, & \text{none} \\ 8, & \text{none} \\ 9, & \text{if } D_f = 49. \end{cases}$$

Analogous results for cubic forms with negative discriminant were proved by Delone [12] and Nagell [26], see also Delone and Faddeev [13].

References

[1] *A. Baker*, Linear forms in the logarithms of algebraic numbers. Mathematica **13** (1966), 204—216.

[2] *A. Baker*, Contribution to the theory of Diophantine equations I. On the representation of integers by binary forms. Philos. Trans. Roy. Soc. London Ser. A **263** (1968), 173—191.

[3] *A. Baker*, A sharpening of the bounds for linear forms in logarithms I. Acta Arith. **21** (1972), 117—129.

[4] *A. Baker*, The theory of linear forms in logarithms. In: Transcendence Theory: Advances and Applications, Academic Press, London, 1977, 1—27.

[5] *A. Baker*, Transcendental Number Theory. Cambridge Univ. Press, Cambridge, 1975.

[6] *A. Baker* and *H. Davenport*, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. Quart. J Math. Oxford **20** (1969), 129—137.

[7] *J. Blass, A.M.W. Glass, D.B. Meronk and R.P. Steiner*, Practical solutions to Thue equations over the rational integers. To appear.

[8] *J. Blass, A.M.W. Glass, D. Manski, D.B. Meronk* and *R.P. Steiner*, Constants for lower bounds for linear forms in the logarithms of algebraic numbers I: The general case. Acta Arith., to appear.

[9] *J. Blass, A.M.W. Glass, D. Manski, D.B. Meronk and R.P. Steiner*, Constants for lower bounds for linear forms in the logarithms of algebraic numbers II: The rational case. Acta Arith., to appear.

[10] *E. Bombieri* and *W. M. Schmidt*, On Thue's equation. Invent. Math. **88** (1987), 69—82.

[11] *J.M. Cherubini* and *R.V. Wallisser*, On the computation of all imaginary quadratic fields of class number one. Math. Comp. **49** (1987), 295—299.

[12] *B.N. Delone (Delaunay)*, Über die Darstellung der Zahlen durch die binäre kubischen Formen von negativer Diskriminante. Math. Zeitschr. **31** (1930), 1—26.

[13] *B.N. Delone* and *D.K. Faddeev*, The Theory of Irrationalities of the Third Degree. Amer. Math. Soc. Transl. of Math. Monographs 10. Providence, 1964.

[14] *W.J. Ellison*, Recipes for solving diophantine problems by Baker's method. Sem. Th. Nombr., 1970–1971. Exp. No. 11. Talence: Lab. Theorie Nombres, C.N.R.S.

[15] *W.J. Ellison, F. Ellison, J. Pesek, C.E. Stahl* and *D.S. Stall*, The diophantine equation $y^2 + k = x^3$. J. Number Theory **4** (1972), 107—117.

[16] *J.H. Evertse*, On the representation of integers by binary cubic forms of positive discriminant. Invent Math. **73** (1983), 117—138.

[17] *J.H. Evertse* and *K. Győry*, Thue–Mahler equations with a small number of solutions. To appear.

[18] *I. Gaál*, On the resolution of inhomogeneous norm form equations in two dominating variables. Math. Comp., **51** (1988), 359—373.

[19] *I. Gaál* and *N. Schulte*, Computing all power integral bases to cubic fields. Math. Comp., to appear.

[20] *I. Gaál, A. Pethö* and *M. Pohst*, On the resolution of index form equations corresponding to biquadratic number fields I, and II. To appear.

[21] *A.O. Gelfond*, On the approximation of transcendental numbers by algebraic numbers. Dokl. Akad. Nauk. SSSR. **2** (1935), 177—182. (Russian)

[22] *K. Györy*, Resultats Effectives Sur la Representation des Entiers Par des Formes Decomposables. Queen's Papers in Pure and Applied Math., No. 56, Kingston, Canada, 1980.

[23] *K. Györy* and *Z.Z. Papp*, Norm form equations and explicit lower bounds for linear forms with algebraic coefficients. In: Studies in Pure Mathematics (To the Memory of Paul Turán), Akadémiai Kiadó, Budapest (1983), 245—267.

[24] *R.M. Kaufman*, A bound for linear forms in logarithms of algebraic numbers in P-adic metric. Vest. Mosk. Univ. Ser. Mat. Meh. **2** (1971), 3—10. (Russian)

[25] *A.K. Lenstra, H.W. Lenstra Jr.* and *L. Lovász*, Factoring polynomials with rational coefficients. Math. Ann., **261** (1982), 515—534.

[26] *T. Nagell*, Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante. Math. Zeitschr. **28** (1928), 10—29.

[27] *A. Pethö*, Perfect powers in second order recurrences. In: Topics in Classical Number Theory, Colloq. Math. Soc. János Bolyai, Vol. 34, Budapest, 1981, 1217—1227.

[28] *A. Pethö*, Full cubes in the Fibonacci sequences. Publ. Math. Debrecen, **30** (1983), 117—127.

[29] *A. Pethö*, On the solution of the diophantine equation $G_n = p^z$. In: Proceedings EUROCAL '85, Vol. 2, Lecture Notes in Comput. Sci. Vol. 204, Springer–Verlag, 1985, 503—512.

[30] *A. Pethö*, On the resolution of Thue inequalities. J. Symbolic Computation **4** (1987), 103—109.

[31] *A. Pethö*, On the representation of 1 by binary cubic forms with positive discriminant. In: Proceedings Journees Arithmetiques, Ulm, to appear.

[32] *A. Pethö* and *R. Schulenberg*, Effektives Lösen von Thue Gleichungen. Publ. Math. Debrecen **34** (1987), 189—196.

[33] *A. Pethö* and *B.M.M. de Weger*, Products of prime powers in binary recurrence sequences I: The hyperbolic case, with an application to the generalized Ramanujan–Nagell equation. Math. Comp. **47** (1986), 713—727.

[34] *A.J. van der Poorten*, Linear forms in logarithms in the p-adic case. In: Transcendence Theory: Advances and Applications, Academic Press, London, 1977, 29—57.

[35] *A. Schinzel,* On two theorems of Gelfond and some of their applications. Acta Arith. **13** (1967), 177—236.

[36] *T.N. Shorey* and *R. Tijdeman,* Exponential Diophantine Equations. Cambridge Univ. Press, Cambridge, 1986.

[37] *R.P. Steiner,* On Mordell's equation $y^2 - k = x^3$: A problem of Stolarsky. Math. Comp. **46** (1986), 703—714.

[38] *A. Thue,* Annäherungswarte algebraischer Zahlen. J. reine angew. Math. **135** (1909), 284—305.

[39] *N. Tzanakis* and *B.M.M. de Weger,* On the practical solution of the Thue equation. Memorandum **668**, Faculty of Applied Mathematics, University of Twente (1987).

[40] *K. Yu,* Linear forms in the $p-$adic logarithms. MPI/87–20.

[41] *M. Waldschmidt,* A lower bound for linear forms in logarithms. Acta Arith. **37** (1980), 257—283.

[42] *B.M.M. de Weger,* Products of prime powers in binary recurrence sequences II: The elliptic case, with an application to a mixed exponential equation. Math. Comp. **47** (1986), 729—739.

[43] *B.M.M. de Weger,* Solving exponential diophantine equations using lattice basis reduction algorithms, J. Number Theory **26** (1987), 325—367.

[44] *B.M.M. de Weger,* Algorithms for diophantine equations, Ph.D. Thesis, Amsterdam, 1987.

[45] *B.M.M. de Weger,* On the practical solution of Thue–Mahler equations, an outline. Memorandum **649**, Faculty of Applied Mathematics, University of Twente (1987).

[46] *D. Zagier,* Large integral points on elliptic curves. Math Comp. **48** (1987), 425—436.

Mathematical Institute, Kossuth Lajos University, 4010 Debrecen, P.O. Box 12, HUNGARY.