Solving Diophantine Equations

Guillaume Hanrot
Projet Polka, Inria Lorraine

December 1st, 1997

[summary by F. Morain]

1. Introduction

Solving Diophantine equations, that is finding integer solutions to polynomial equations, is one of the oldest mathematical problems. The very name "Diophantine" reminds us of the great Greek mathematician Diophante who solved some of the most basic equations.

At the beginning of the twentieth century, Hilbert asked about the existence of a universal algorithm that would compute all integer solutions of a polynomial equation, and it was not until 1970 that Matiyasevich [13] showed the inexistence of such an algorithm.

Even before the negative answer to this problem, many mathematicians have developed algorithms for special cases. For the univariate case, the problem is related to good rational approximations of a non rational root α of a polynomial P with integer coefficients. Let n be the degree of P and p/q a rational number. Put $\delta(\alpha) = |\alpha - p/q|$. Thue [19] showed that

$$\delta(\alpha) \geq \frac{C_1}{q^{n/2+\varepsilon}},$$

with the consequence that there are only a finite number of solutions of the equation $Q(X, Y) = 1$, where Q is an homogeneous, irreducible polynomial of degree ≥ 3. Siegel [17] improved the bound to:

$$\delta(\alpha) \geq \frac{C_2(\varepsilon)}{q^{2\sqrt{n}+1+\varepsilon}}$$

which was enough to prove the finiteness of the number of solutions of $y^p = f(x)$ for f a separable polynomial of degree ≥ 3 and $p \geq 2$ [18]. Later, in 1955, Roth proved [16]:

$$\delta(\alpha) \geq \frac{C_3(\varepsilon)}{q^{2+\varepsilon}}$$

a result that is the best possible, due to well known results in continued fraction theory, namely that if α is irrational, then there exists an infinite number of rational numbers p/q such that

$$\delta(\alpha) \leq \frac{1}{2q^2}.$$

As is often the case, the constants are ineffective and this does not help us when we want to find the solutions of a given equation. Around 1966, Baker [1] (see also [3]) found a very deep bound:

Theorem 1. *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ denote algebraic numbers. Then for every n-tuple of integers $(b_1, b_2, \ldots, b_n)$, we have*

$$K = 0 \quad \textit{or} \quad K \geq \exp(-C_4 \log \max_i |b_i|), \quad \textit{where} \quad K = |b_1 \log \alpha_1 + b_2 \log \alpha_2 + \cdots + b_n \log \alpha_n|.$$

Unfortunately, the constant C_4, though effective, is very huge and specialists thought it was completely useless. However, Baker and Davenport [2] gave the first use of such a bound, for solving a system of simultaneous Pell equations.

2. Solving Homogeneous Equations

2.1. **Statement of the Problem.** Let $P(X,Y)$ be a homogeneous polynomial of degree n, monic in Y, and let α_i denote the roots of $P(1,Z)$. In this section, we want to solve the equation $P(X,Y)=1$ in integers X and Y, which we rewrite as:

$$\prod_{i=1}^{n}(Y-\alpha_i X)=1. \tag{1}$$

Suppose (X_0,Y_0) is an integer solution of this equation. In view of (1), it is obvious that at least one of the terms $Y_0-\alpha_i X_0$ is small. This implies that:

$$Y_0-\alpha_j X_0 \approx (\alpha_j-\alpha_i)X_0$$

when $j\neq i$. Using (1) again, we get that:

$$\left|\alpha_i-\frac{Y_0}{X_0}\right| \approx \frac{1}{|X_0|^n}\prod_{j\neq i}\frac{1}{|\alpha_j-\alpha_i|}$$

or in other words, Y_0/X_0 is a very good approximation of α_i.

2.2. **Using the Baker Bound.** In algebraic terms, equation (1) tells us that for each i, the number $Y_0-\alpha_i X_0$ is a unit in $\mathbb{Q}(\alpha_i)$.

One knows that the set of units of a number field $\mathbb{Q}(\alpha)$ is a group of finite type. There exists a set of units, the so-called *fundamental units* $\eta_1,\eta_2,\ldots,\eta_r$ such that every unit can be written as: $\zeta^{b_0}\prod_{i=1}^{r}\eta_i^{b_i}$ where ζ denotes a root of unity in $\mathbb{Q}(\alpha)$ and the b_i's are integers. Without loss of generality, it can be shown that we can restrict to the case where $\zeta=-1$.

Now suppose that α_1 is a real root of $P(1,Z)$. If $j\neq k\neq 1$, we can write:

$$\left|\frac{Y_0-\alpha_j X_0}{Y_0-\alpha_k X_0}\frac{\alpha_k-\alpha_1}{\alpha_j-\alpha_1}-1\right| \leq \frac{C_5(P)}{|X_0|^n}.$$

From this, we deduce that:

$$\left|\log\frac{Y_0-\alpha_j X_0}{Y_0-\alpha_k X_0}\frac{\alpha_k-\alpha_1}{\alpha_j-\alpha_1}\right| \leq \frac{C_6(P)}{|X_0|^n}.$$

Write $Y_0-\alpha_k X_0=\eta_{k,1}^{b_1}\cdots\eta_{k,r}^{b_r}$. We can rewrite the last inequality as:

$$\left|-\log\frac{\alpha_k-\alpha_1}{\alpha_j-\alpha_1}+\sum_{\ell=1}^{r}b_\ell\log\frac{\eta_{k,\ell}}{\eta_{j,\ell}}+2ik\pi\right| \leq \frac{C_7}{|X_0|^n}. \tag{2}$$

It is not hard to see that $\log|X_0|\approx B=\max_\ell|b_\ell|$, so that the right-hand side of the inequality is bounded by

$$C_7\exp(-nC_8B).$$

For the left hand side, we use the Baker bound to finally obtain the lower bound

$$\exp(-C_9\log B)\leq C_7\exp(-nC_8B).$$

This clearly gives a bound $\mathcal{B}$ on B.

Unfortunately, this bound is much too large to be useful. For instance, in the case of the equations

$$X^{19} + 2Y^{19} = \pm 1, \text{ or } \pm 2, \tag{3}$$

one finds $\mathcal{B} = 2.32 \times 10^{92}$.

2.3. **Refining the Bound.** Once we know that the b_i's are bounded, we would like to find a better bound. The idea is the following. Suppose the b_i's are integers subject to $|b_i| \leq \mathcal{B}$. We would like to prove some result on the minimum of the quantity $|\sum_{\ell=1}^{r} b_\ell \lambda_\ell|$ where the λ_ℓ's are real numbers. Using the Lenstra-Lenstra-Lovász theory [12] as in [8], it is possible to show that this minimum is bounded from below by $C_{10}/\mathcal{B}^{r-1}$. Since we also have the Baker bound:

$$\exp(-C_{11}\mathcal{B}) \geq \left|\sum_{\ell=1}^{r} b_\ell \lambda_\ell\right|,$$

we get

$$\mathcal{B} \leq \log(\mathcal{B}^{r-1}/C_{10}) = (r-1)\log \mathcal{B} - \log C_{10}$$

or a bound which is logarithmically smaller.

For instance, for our example, we find that $\mathcal{B} = 29$ instead of 2.32×10^{92}.

2.4. **Finishing the Computations.** At this point, one can finish the computations by enumerating all solutions. As easy as it seems, do not forget that there could be a lot of computations still to be done. In our example, there are 9 values for the b_i's, with $|b_i| \leq 29$, which amounts to 59^9 combinations.

This is enough when n is small, but can be quite cumbersome when n increases, since the computational determination of units in a general number field is no easy task at all (see for example [7, 14, 15]).

3. A Faster Approach

The idea of Bilu and the speaker [4, 5] is the following: we can rewrite equation (2) as:

$$\mathcal{L}_{0,j} + \sum_{\ell=1}^{r} b_\ell \mathcal{L}_{\ell,j},$$

that is we have r linear forms in $r+1$ logarithms. The idea is to transform these forms so as to obtain a new form of the type $\theta = |a\alpha + b\beta + \delta|$ where the integers a and b are bounded. Minimizing such a form can be done using continued fractions, and therefore is very fast. Once this is done, and using a bound as $C/|X_0|^n$, there are two cases. Either $\theta < 1/2$ and we can easily deduce b from a, or $\theta > 1/2$ and since $C/|X_0|^n > 1/2$, $|X_0|$ is quite small and we are done. In brief, we have reduced a large enumeration problem in a large number of unknowns to one in a single unknown.

For our leading example, we get that $\mathcal{B} = 4$ and it takes 12 seconds on a workstation to find all the solutions.

4. Conclusions

We have shown how to solve some special cases of Diophantine equations by a clever use of Baker's bound combined with casual ingenuity. It is possible to use more tricks, for example using units that are not fundamental, or to work with relative norms. For instance, the speaker has the world record in the field, with the solution of the equation

$$\prod_{k=1}^{2505}(Y - \cos(2k\pi/5011)X) = \pm 1$$

using an intermediate field of degree 3. The original Baker bound, 10^{40}, was reduced to 46, yielding a total running time of 8 minutes. More examples are given in [6] and in [10, 11], refinements are given when one does not have the full unit group of the number field under consideration.

The ideas we have described above can be used *mutatis mutandis* to solve equations of the type $Y^p = f(X)$. The only difference comes from the construction of the units. We refer to the speaker's thesis for this.

As a final comment, we note that similar techniques can be used to solve equations on elliptic curves [9, 20].

Bibliography

[1] Baker (A.). – Linear forms in the logarithms of algebraic numbers I, II, III, IV. *Mathematika*, vol. 13, 14, 14, 15, 1966, 1967, 1967, 1968, pp. 204–216, 102–107, 220–228, 204–216.

[2] Baker (A.) and Davenport (H.). – The equations $3x^2-2 = y^2$ and $8x^2-7 = z^2$. *Quarterly Journal of Mathematics, Oxford Series*, vol. 20, 1969, pp. 129–137.

[3] Baker (A.) and Wüstholz (G.). – Logarithmic forms and group varieties. *Journal für die reine und angewandte Mathematik*, vol. 442, 1993, pp. 19–62.

[4] Bilu (Yu.) and Hanrot (G.). – Solving Thue equations of high degree. *Journal of Number Theory*, vol. 60, 1996, pp. 373–392.

[5] Bilu (Yu.) and Hanrot (G.). – Solving superelliptic diophantine equations by Baker's method. – 1998. To appear in Compositio Mathematica.

[6] Bilu (Yu.) and Hanrot (G.). – Thue equations with composite fields. – 1998. To appear in Acta Arithmetica.

[7] Cohen (Henri). – *A course in computational algebraic number theory.* – Springer-Verlag, Berlin, 1993, *Graduate Texts in Mathematics*, vol. 138, xii+534p.

[8] de Weger (B. M. M.). – Solving exponential diophantine equations using lattice basis reduction algorithms. *Journal of Number Theory*, vol. 26, 1987, pp. 325–367.

[9] Gebel (J.), Pethő (A.), and Zimmer (H.). – Computing S-integral points on elliptic curves. In Cohen (H.) (editor), *Algorithmic Number Theory.* – Springer-Verlag, 1996. Proceedings of the Second International Symposium ANTS II.

[10] Hanrot (G.). – *Résolution effective d'équations diophantiennes : algorithmes et applications.* – PhD thesis, Université de Bordeaux I, 1997.

[11] Hanrot (G.). – Solving Thue equations without the full unit group. – 1998. To appear in Mathematics of Computation.

[12] Lenstra (A. K.), Lenstra (H. W. Jr.), and Lovász (L.). – Factoring polynomials with rational coefficients. *Mathematische Annalen*, vol. 261, 1982, pp. 515–534.

[13] Matiyasevich (Yu.). – Enumerable sets are diophantine. *Soviet Mathematics. Doklady*, vol. 12, 1971, pp. 249–254.

[14] Pohst (M.). – *Computational Algebraic Number Theory.* – Birkhäuser, 1993, *DMV Seminar*, vol. 21.

[15] Pohst (M.) and Zassenhaus (H.). – *Algorithmic Algebraic Number Theory.* – Cambridge University Press, 1989.

[16] Roth (K. F.). – Rational approximations to algebraic numbers. *Mathematika*, vol. 2, 1955, pp. 1–20.

[17] Siegel (C. L.). – Approximation algebraischer Zahlen. *Mathematische Zeitschrift*, vol. 10, 1921, pp. 173–213.

[18] Siegel (C. L.). – The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$ (extract from a letter to Prof. L. J. Mordell unter dem Pseudonym X). *Journal of the London Mathematical Society*, vol. 1, 1926, pp. 66–68.

[19] Thue (A.). – Über Annäherungswerte algebraischer Zahlen. *Journal für die reine und angewandte Mathematik*, vol. 135, 1909, pp. 284–305.

[20] Tzanakis (N.). – Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. the case of quartic equations. *Acta Arithmetica*, vol. 75, 1996, pp. 165–190.