Units and Diophantine Equations.

Dedicated to the 60th birthday of Michael Pohst

Attila Pethő, University of Debrecen

Berlin, June 10, 2005.

1. Prolog

I know Michael since nearly 30 years. He visited the Lajos Kossuth University Debrecen at the first time in 1979. My university had a computer and mathematics students had to learn to write programs, but the idea to apply computers to solve number theoretical problems was for me new and fascinating.

As a Student of Kálmán Győry I just learned A. Bakers's method. It serves effective upper bound for many diophantine problems, but the bounds were astronomic even for very simple questions.

Consider for example the cubes in the Fibonacci sequence, i.e. the equation

$$F_n = x^3.$$

I was able to prove $n \leq 10^{50}$ with Baker's theory and asked Michael whether it is possible to test the remaining finitely many cases. You see his answer in the next slides.

Mathematical Sciences Department
International Business Machines Corporation
Thomas J. Watson Research Center
Box 218, Yorktown Heights, N. Y. 10598
(914) 945-3000

M. POHST

10-24-80

Lieber Herr Pethö!

Ihr Brief vom 2.9. gelangte erst auf einigen Umwegen zu mir, so daß ich mich erst heute bedanken kann. Im August und September war ich wieder in Columbus bei Zassenhaus und fuhr anschließend über Penn State und Maryland an das hiesige IBM-Forschungscenter. Die Arbeit hier ist für mich sehr interessant, insbesondere auf dem Gebiet symbolischer Sprachen. So lassen sich z.B. Polynome in mehreren Variablen durch einen Aufruf faktorisieren, Resultanten berechnen, etc.. Diese Möglichkeiten haben wir in Köln leider nicht, da uns dort der benötigte virtuelle Speicherplatz (mindestens 2 Megabyte) fehlt.

Ich habe die Leute hier auch bezüglich Ihres Problems der vollständigen Kuben in der Fibonacci-Folge befragt. Es scheint leider ziemlich aussichtslos zu sein, F_n bis $n = e^{50}$ zu berechnen, bereits F_{1000} ist ganz hübsch groß. Haben Sie schon diesbezügliche Erfahrungen?

In diesem Wintersemester werde ich eine Vorlesung über Geometrie der Zahlen halten, insbesondere in bezug auf Anwendungen in der Zahlentheorie. Außerdem habe ich ein Seminar, in dem wir Shanks' Methode zur Faktorisierung von ganzen Zahlen x in $O(x^{1/4})$ Schritten besprechen werden. Ich traf Shanks in Maryland, und er führte mir auf seinem Taschenrechner die Faktorisierung von 20-stelligen Zahlen vor, es war schon erstaunlich. Er benutzt jetzt allerdings eine neue Methode, die aus der Kettenbruchentwicklung abgeleitet ist.

Mit herzlichen Grüßen
Ihr
Michael Pohst

I realized nearly in the same time a sieve method, which enabled me to compute all cubes and later the fifth powers. Im 2003 proved Bugeaud, Mignotte and Siksek, that $0, 1, 8$ and 144 are the only perfect powers in the Fibonacci sequence.

2. Thue Equations

The connection between units and Diophantine equations better to understand consider the Thue equations.

Let $F(x,y) \in \mathbf{Z}[x,y]$ of degree $n \geq 3$, irreducible over $\mathbf{Q}[x,y]$. Assume that the coefficient of x^n is one. Let $0 \neq m \in \mathbf{Z}$, then

$$F(x,y) = m \tag{1}$$

is a Thue equation.

In $\mathbf{C}[x,y]$ we can factorize $F(x,y) = \prod_{i=1}^{n}(x - \alpha^{(i)}y)$.

Let $\alpha = \alpha^{(1)}$ and $\mathbf{K} = \mathbf{Q}(\alpha)$ then we can rewrite (1) in the form

$$\prod_{i=1}^{n}(x - \alpha^{(i)}y) = N_{\mathbf{K}/\mathbf{Q}}(x - \alpha y) = m. \tag{2}$$

The element $x - \alpha y$ has Norm m and belongs to $M = \mathbf{Z}[\alpha] \subseteq \mathbf{Z_K}$.

• Denote $\mathcal{O}_M$ the coefficient ring of M, i.e.

$$\mathcal{O}_M = \{\lambda : \lambda M \subseteq M\}.$$

• Denote E_M the group of units of infinite order of $\mathcal{O}_M$ and $\varepsilon_1, \dots, \varepsilon_r$ a system of fundamental units of E_M.
• Let A a maximal set of non-associated elements of M with Norm m. The set A is finite. Then

Theorem 1. *Let $x, y \in \mathbf{Z}$ a solution of (1). Then there exist a $\mu \in A$ and $u_1, \dots, u_r \in \mathbf{Z}$ such that*

$$\beta = x - \alpha y = \mu \varepsilon,$$

where $\varepsilon = \varepsilon_1^{u_1} \cdots \varepsilon_r^{u_r}$.

Considering conjugates we get the system of equations

$$\beta^{(i)} = x - \alpha^{(i)} y = \mu^{(i)} \varepsilon^{(i)}, \quad i = 1, \ldots, r.$$

Choosing $1 \leq j < k < h \leq n$ we obtain the Siegel's relations:

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

Division by $(\alpha^{(h)} - \alpha^{(k)})\mu^{(j)}\varepsilon^{(j)} \neq 0$ implies the unit equation

$$A_1 E_1 + A_2 E_2 = 1, \tag{3}$$

where

$$A_1 = \frac{(\alpha^{(j)} - \alpha^{(k)})\mu^{(h)}}{(\alpha^{(h)} - \alpha^{(k)})\mu^{(j)}},\ E_1 = \left(\frac{\varepsilon_1^{(h)}}{\varepsilon_1^{(j)}}\right)^{u_1} \cdots \left(\frac{\varepsilon_r^{(h)}}{\varepsilon_r^{(j)}}\right)^{u_r}$$

and

$$A_2 = \frac{(\alpha^{(h)} - \alpha^{(j)})\mu^{(k)}}{(\alpha^{(h)} - \alpha^{(k)})\mu^{(j)}},\ E_2 = \left(\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}\right)^{u_1} \cdots \left(\frac{\varepsilon_r^{(k)}}{\varepsilon_r^{(j)}}\right)^{u_r}.$$

Choosing k such that $|x-\alpha^{(k)}y| = \min_{1\le i\le n} |x-\alpha^{(i)}y|$, we obtain after some computation

$$\left|\log A_1 + u_1 \log \frac{\varepsilon_1^{(h)}}{\varepsilon_1^{(j)}} + \cdots + u_r \log \frac{\varepsilon_r^{(h)}}{\varepsilon_r^{(j)}} + u_{r+1} 2\pi i\right| < c_1 \exp(-c_2 U), \tag{4}$$

with $U = \max\{|u_1|, \ldots, |u_r|\}$.
Here is $u_{r+1} = 0$, if A_1 and E_1 are real.
A. Baker combined this inequality with his theorem of linear forms and proved

$$U \le C(n, m, D_{\mathbf{K}}),$$

which implies $\max\{|x|, |y|\} \le C'$ nearly immediately.

For given $F(x, y)$ and m we need the following data to solve completely equation (1):

a. A fundamental system of units of E_M or of $E_{\mathbf{K}}$.
b. The elements of A, i.e. a maximal system of non-associated elements with norm m.
c. The solutions of the inequality (4).

3. Units

At the International Conference on Number Theory in 1981 in Budapest delivered Michael a talk with title: On constructive methods in algebraic number theory. We cite from his paper of the Proceedings of this meeting:

Over the past ten years the application of computers to problems of algebraic number theory has rapidly increased. Especially the explicit computation of invariants of arbitrary algebraic number fields $\mathbf{F}$ *requires the use of electronic calculators in most cases.*

Hence, the four fundamental tasks of constructive number theory are to develop efficient algorithms

- *for determining the Galois group of* $\mathbf{F}$,
- *a* $\mathbf{Z}$*-basis for the integers of* $\mathbf{F}$,
- *a system of fundamental units of* $\mathbf{F}$,
- *and a set of representatives of the ideal classes of* $\mathbf{F}$.

In this paper we desribe a new combined procedure for the computation of the unit group and the class group."

Details were published in 1982 in Math. Comp. in two papers. To compute unit group and class group simultanously were used afterward in most of the later methods. They differ basically in the generation of sufficiently many algebraic integers or ideals with bounded norm.

He wrote later: *A computer program of our method for fundamental units written in FORTRAN is already operating at the University of Cologne, a suitable supplement for the computation of the class group and related problems is planned. We note that the application of that program to "arbitrary" number fields is limited by the fact that all calculations are carried out in single precision (14 decimal digits). Also the field degree should be less than 10 because of computation time.*

Hence, at the beginning of the 80's there were available a program to compute a basis of the unit group. But how to solve the inequality

$$\left|\log A_1 + u_1 \log \frac{\varepsilon_1^{(h)}}{\varepsilon_1^{(j)}} + \cdots + u_r \log \frac{\varepsilon_r^{(h)}}{\varepsilon_r^{(j)}} + u_{r+1} 2\pi i\right| < c_1 \exp(-c_2 U),$$

mit $U = \max\{|u_1|, \ldots, |u_r|\}$? If $r = 2$ and $u_{r+1} = 0$, then one can use the extremal property of continued fraction expansion. In the general case the lattice basis reduction of Lenstra, Lenstra und Lovász can applied.

5. 8. 82

Lieber Attila!

Das Paper von Lenstra etc. über Polynomfaktorisierung kenne ich. Ich hatte ihn deswegen eingeladen, und er hat hier im Mai darüber vorgetragen. – Meine Arbeit an dem Buch über Konstruktive Zahlentheorie geht nur langsam voran. Es soll 4 Kapitel über die Berechnung von Galoisgruppe, Ganzheitsbasis, Einheitengruppe sowie Klassengruppe und einen Anhang über Hilfsmittel aus der Geometrie der Zahlen und der Analytischen Zahlentheorie enthalten. Sobald ein Kapitel getippt ist, schicke ich Dir eine Kopie. Für Deine Kommentare wäre ich Dir dankbar. – Zum Abschluß noch ein Problem von einem Kölner Kollegen: Kannst Du die Fibonacci-Zahlen der Form $2x^2 - 3y^2$ bzw. $\frac{1}{2}(x^3 \pm y^3)$ angeben?

Dir, Piroska und den Kindern

herzliche Grüße,

Michael

In the Diophantine approximation problem one have to compute the data with very high accuracy. The first program to solve Thue equations was written by Ralf Schulenberg at the University of Cologne in 1985. It assumed $|m| = 1$ and $\mathbf{K}$ totally real and used Peter Weiler's program to compute a basis of the unit group.
The algorithmic theory of Thue equation was further developed by de Weger and Tzanakis, as well as by Bilut and Hanrot. Today there exist at least two independent implementations in KANT and in PARI. In the solution of Lehmer's primitive divisor problem in 2001 solved Bilu, Hanrot and Voutier Thue equations up to degree 260. These were lucky cases, because a maximal system of independent units was known.

4. Regulator estimates.

In some applications, e.g. to compute fundamental units from an independent system or to solve Thue equations, if we know only an independent system of units it is required a lower bound for the regulator. In 1931 Remak proved $R \geq 0.001$, provided R is the regulator of a totally real number field.
In 1978 Michael improved this estimate to

$$R > \left(\frac{1}{n}\left(\left(\log\frac{1+\sqrt{5}}{2}\right)^2 \pi n/2\right)^{n-1}\right)^{1/2} \left(\Gamma\left(\frac{n+3}{2}\right)\right)^{-1},$$

where n denotes the degree of the field. This implies $R > 0.315$.

Later, with Zassenhaus, he proved a bound, which depends on the discriminant to:

$$R \geq \left(\left(\frac{12 \log^2 \sqrt{|D_{\mathbf{K}}|/n^n}}{(n-1)n(n+1) - 6r_2} \right)^r \frac{2^{r_2}}{\gamma_r^r n} \right)^{1/2},$$

where r_2 denotes the number of non-real conjugates of $\mathbf{K}$ and γ_r^r is Hermite's constant for positive definite quadratic forms.

In 1996 Halter-Koch, Lettl, Tichy and I proved the following theorem.

Theorem 2. *Let $n \geq 3$, $a_1 = 0, a_2, \ldots, a_{n-1}$ be distinct integers and $a_n = a$ an integral parameter. Let $\alpha = \alpha(a)$ be a zero of $P(x) = \prod_{i=1}^{n}(x - a_i) \pm 1$ and suppose that the index I of $\langle \alpha - a_1, \ldots, \alpha - a_{n-1} \rangle$ in $U_{\mathcal{O}}$ is bounded by a constant J for every a from some subset $\Omega \subseteq \mathbf{Z}$. Assume further that the Lang-Waldschmidt conjecture is true. Then for all but finitely many values $a \in \Omega$ the diophantine equation*

$$\prod_{i=1}^{n} (x - a_i y) \pm y^n = \pm 1 \tag{5}$$

only has trivial solutions $\pm(x, y) = (1, 0), (a_i, 1),\ i = 1, \ldots, n$, except when $n = 3$ and $|a_2| = 1$, or when $n = 4$ and $(a_2, a_3) \in \{(1, -1), (\pm 1, \pm 2)\}$, in which cases (5) has exactly one more parametrized solution.

In the proof of this theorem was playing Michael's regulator estimate an important role. Remark that if the field $\mathbf{K} = \mathbf{Q}(\alpha)$ is primitive, for example n is prime then is J always bounded and we need only the Lang-Waldschmidt conjecture.

5. Indexformgleichungen

Michael visited Hungary after 1979 regularly. During one of his visits in Sátoraljaújhely was taking this photo.

I was in 1984/85 an Alexander von Humboldt fellow of Peter Bundschuh and of Michael. From 1987 started to work István Gaál with us. He studied first with Nicole Schulte index form equations in cubic number fields, which are essentially cubic Thue equations.

Let $\mathbf{K}$ be a number field of degree n, $\mathbf{Z}_\mathbf{K}$ its ring of integers and $\omega_1 = 1, \omega_2, \ldots, \omega_n$ an integral basis of $\mathbf{Z}_\mathbf{K}$. Put

$$L(X) = x_0 + \omega_2 x_1 + \cdots + \omega_n x_{n-1}.$$

The polynomial

$$I_{\mathbf{K}/\mathbf{Q}}(X) = \prod_{1 \le i < j \le n} (L^{(i)}(X) - L^{(j)}(X))/D_\mathbf{K}^{1/2},$$

is homogenous, has rational integer coefficients and degree $n(n-1)/2$. It is called an index form of $\mathbf{K}$.

If $m \in \mathbf{Z}$, then

$$I(X) = m \tag{6}$$

is called an index form equation, provided its solutions $x_2, \ldots, x_{n-1}$ belong to $\mathbf{Q}$. We published between 1991 and 1996 eight papers on index form equation in quartic fields.

To formulate our most general result we need some notations. Let $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 \in \mathbf{Z}[x]$ the minimal polynomial of ξ, and put $\mathbf{K} = \mathbf{Q}(\xi)$. Represent $\alpha \in \mathbf{Z_K}$ in the form

$$\alpha = \frac{x_0 + x_1\xi + x_2\xi^2 + x_3\xi^3}{d}$$

with $x_0, \ldots, x_3, d \in \mathbf{Z}$.

We proved the following theorem:

Theorem 3. *Let $i_m = d^6 m/n$ where n is the index of ξ. The element α satisfies $I(\alpha) = m$ if and only if there are $u, v \in \mathbf{Z}$ with*

$$F(u,v) = u^3 - a_2 u^2 v + (a_1 a_3 - 4a_4) u v^2 + (4 a_2 a_4 - a_3^2 - a_1^2 a_4) v^3 = \pm i_m$$

such that x_1, x_2, x_3 satisfies

$$\begin{aligned} x_1^2 - a_1 x_1 x_2 + a_2 x_2^2 + (a_1^2 - 2a_2) x_1 x_3 + \\ (a_3 - a_1 a_2) x_2 x_3 - (a_1 a_3 - a_2^2 - a_4) x_3^2 &= u \\ x_2^2 - x_1 x_3 - a_1 x_2 x_3 + a_2 x_3^2 &= v. \end{aligned}$$

We proved moreover, that the resolution of the system of the above quadratic equations can be transformed to a single quartic Thue equation, which splits over $\mathbf{K}$. This theorem made it possible for us to solve Index form equations in totally real quartic fields with Galois group S_4, which is certainly the most complicated case.

Herzliche Glückwunsch zum

60-sten Geburtstag!