THE BLUNDON LECTURE

APICS

OCTOBER 28, 1994 (ACADIA)

THE THUE EQUATION

C. L. Stewart

Let f be in $\mathbb{Z}[x_1, \dots, x_n]$. A typical problem of Diophantine equations is to determine all of the solutions of $f(x_1, \dots, x_n) = 0$ in integers $x_1, \dots, x_n$. The name Diophantine comes from the Greek mathematician Diophantus of Alexandria, who worked about 250 A.D. and who laid the foundations for the study of equations in integers. His great work, the Arithmetica, was apparently 13 volumes, but only 6 have survived. He studied problems connected with elliptic curves which are current today, he knew that no integer of the form $8n+7$ can be a sum of 3 squares and he found the correct formula for the solutions of the equation $x^2 + y^2 = z^2$ in integers. Approximately 1400 years later Fermat revived the subject. In about 1637 he stated in the margin of one of the pages of his copy of the Arithmetica that if n exceeds 2 there are no solutions of $x^n + y^n = z^n$ in positive integers x, y and z. However, the margin was too small to contain his truly marvelous proof. We live in exciting mathematical times. Wiles and Taylor have apparently closed the gap in Wiles' previously announced proof of Fermat's Last Theorem. That is the news as of October 26.

In spite of the work of Fermat and the many great mathematicians who followed him, a basic question remained open. This was posed by Hilbert in 1900 as the 10th of 23 problems which he felt were of fundamental importance to mathematics. "Give a way in which it is possible to determine after a finite number of operations whether any given equation $f(x_1, \dots, x_n) = 0$, with f in $\mathbb{Z}[x_1, \dots, x_n]$, has a solution in rational integers." In 1970 Matijasevic, completing work of Davis, Robinson and Putnam, proved that such a general algorithm does not exist, even if we restrict the number of unknowns to 13. Perhaps for 2 unknowns the situation is different. Let us now restrict our attention to such equations.

Consider, for example:

$$\begin{aligned} &(1) \quad 166x + 57y = 2, \\ &(2) \quad x^2 - 1141y^2 = 1, \\ &(3) \quad x^3 - 2y^3 = 6. \end{aligned}$$

The first equation has infinitely many solutions in integers x and y. To solve it, we apply the Euclidean Algorithm to the pair (166, 57). We find a particular solution $x = -46, y = 134$. The general solution is then $\{(-46 + 57n, 134 - 166n) | n \epsilon \mathbb{Z}\}$.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Equation (2) also has infinitely many solutions and they can be found by the Continued Fraction Algorithm, which may be viewed as a generalization of the Euclidean Algorithm. The smallest positive solution is given by

$$x = 1,036,782,394,157,223,963,237,125,215$$

$$y = 30,693,385,322,765,657,197,397,208.$$

On the other hand (3) has only the solution $x = 2, y = 1$.

Equation (3) is an example of a Thue equation. Axel Thue was a profound and original mathematician from Norway. Let F in $\mathbb{Z}[x, y]$ be a binary form with integer coefficients, content 1, non-zero discriminant D and degree at least 3. Thus $F(x, y) = a_r x^r + a_{r-1}x^{r-1}y + \cdots + a_0 y^r$ with r an integer larger than 2 and with $a_0, \ldots, a_r$ integers whose greatest common divisor is 1. Futher, the roots of $F(x, 1)$ are distinct. Let h be a positive integer. The equation

$$F(x, y) = h \,, \tag{4}$$

is known as a Thue equation. In 1909, Thue proved that if F is irreducible then (4) has only finitely many solutions in integers x and y. Thue deduced his result from the following result. He proved that if α is an algebraic number of degree $r(> 1)$ and ϵ is a positive real number then there exists a positive number $C(\alpha, \epsilon)$, which depends on α and ϵ, such that

$$|\alpha - p/q| > \frac{C(\alpha, \epsilon)}{q^{\frac{r}{2}+1+\epsilon}} \,, \tag{5}$$

for all p, q in $\mathbb{Z}$ with $q > 0$. In 1844, Liouville had established (5) with $\dfrac{r}{2} + 1 + \epsilon$, the exponent of q, replaced by r. Let us now apply (5) to show that the Thue equation $x^3 - 2y^3 = 6$ has only finitely many solutions. Let $\omega = \frac{1+\sqrt{-3}}{2}$ so $\omega^3 = 1$. Then, by Thue's result,

$$\left|\frac{6}{y^3}\right| = \left|\left(\frac{x}{y}\right)^3 - 2\right| = \left|\frac{x}{y} - \sqrt[3]{2}\,\right| \,\left|\frac{x}{y} - \omega\sqrt[3]{2}\,\right|\frac{x}{y} - \omega^2\sqrt[3]{2}\right|$$

$$> \left|\frac{x}{y} - \sqrt[3]{2}\right| > \frac{C(\sqrt[3]{2}, 1/4)}{|y|^{\frac{3}{2}+1+\frac{1}{4}}} \,.$$

Thus $|y|^{1/4} \leq \dfrac{6}{C(\sqrt[3]{2}, 1/4)}$ and so $|y|$ and $|x|$ are bounded. Notice that to bound $|x|$ and $|y|$ all we had to do was improve on the Liouville exponent of 3. Building on Thue's work, Siegel, in 1921, replaced $\dfrac{r}{2} + 1 + \epsilon$ in (5) by $2\sqrt{r} + \epsilon$. Finally, in 1955, Roth obtained the best possible exponent $2 + \epsilon$ and on the strength of this he was awarded a Fields medal in 1958.

Let us return to the Thue equation $F(x, y) = h$. The question of estimating the number of solutions of (4) has been the subject of many papers by authors such as Mahler, Siegel, Davenport, Lewis and Roth. For any integer h, let $\omega(h)$ denote the number of distinct prime factors of h. In 1984, Evertse resolved a conjecture of Siegel by proving that (4) has at most $2 \cdot 7^{r^3(2\omega(h)+3)}$ primitive solutions; a solution (x, y) is said to be primitive if x and y are coprime. The key feature here is that the bound is independent of the coefficients of F. In 1987, Bombieri and Schmidt refined this result, for F irreducible, to

$$cr^{1+\omega(h)} ,$$

where c is an absolute constant; c may be taken to be 430 for r sufficiently large. Let $\epsilon > 0$. In 1991 I showed that if g is a divisor of h with $g \geq |h|^{2/r+\epsilon}$ and $|h| > |D|^{1/\epsilon}$ then the number of primitive solutions of (4) is at most

$$c_\epsilon r^{1+\omega(g)} ,$$

where $c_\epsilon = 2800\left(1 + \dfrac{1}{12\epsilon}\right)$. Note that if ϵ is less than $\dfrac{r-2}{r}$ then for a positive proportion of integers we may take g to be a prime and then $r^{1+\omega(g)} = r^2$.

One of the main lessons which mathematicians have learned from the last century of mathematics is that the real numbers and the p-adic numbers should be viewed on an equal footing. The p-adic numbers were introduced by Hensel. Let F be a field and let $|| \; || : F \to \mathbb{R}^{\geq 0}$ such that for all x, y in F:

$$\begin{array}{rc} i) & ||x|| = 0 \Leftrightarrow x = 0, \\ ii) & ||xy|| = ||x|| \; ||y||, \\ iii) & ||x+y|| \leq ||x|| + ||y||. \end{array}$$

$|| \; ||$ is said to be a norm. If we put $d(x, y) = ||x - y||$ then d is a metric induced by the norm. Two metrics d_1 and d_2 on a set are equivalent if a sequence is Cauchy with respect to d_1 if and only if it is Cauchy with respect to d_2. Two norms are equivalent if they induce equivalent metrics. Recall that a metric d on X is a map $d : X \times X \to \mathbb{R}$ such that for all x, y, z in X:

$$\begin{array}{rc} i) & d(x, y) = 0 \Leftrightarrow x = y \\ ii) & d(x, y) = d(y, x), \\ iii) & d(x, y) \leq d(x, z) + d(z, y). \end{array}$$

The trivial norm $|| \; ||$ is such that $||0|| = 0$ and $||x|| = 1$ for $x \neq 0$. Take $F = \mathbb{Q}$. The usual absolute value $| \; |$ is a norm. For each prime p and non-zero integer x we define $\text{ord}_p x$ to be l where $p^l | x$ and $p^{l+1} \not| x$. Next we define $\text{ord}_p a/b$ for non-zero integers a and b to be $\text{ord}_p a-$ $\text{ord}_p b$. Then, for each prime p, $| \; |_p$ is a norm where $|0| = 0$ and $\left|\dfrac{a}{b}\right|_p = p^{-\text{ord}_p(a/b)}$ for a and b non-zero integers. Ostrowski proved that every non-trivial norm on $\mathbb{Q}$ is equivalent to $| \; |$ or to $| \; |_p$ for some prime p.

Just as one constructs $\mathbb{R}$ by completing $\mathbb{Q}$ with respect to $| \; |$, so one constructs the p-adic numbers $\mathbb{Q}_p$ by completing $\mathbb{Q}$ with respect to $| \; |_p$. By working in $\mathbb{Q}_p$ and finite extensions of $\mathbb{Q}_p$ for various primes p, Mahler was able to extend Thue's result in 1933. Let $p_1, \ldots, p_r$ be distinct primes. The equation

$$F(x, y) = p_1^{k_1} \ldots p_r^{k_r} ,$$

in coprime integers x and y and non-negative integers $k_1, \dots, k_r$ is known as a Thue-Mahler equation and Mahler showed that it has finitely many solutions. We remark that Schmidt has studied the class of norm form equations. For F irreducible with $F(x,y) = (x - \alpha_1 y) \cdots (x - \alpha_r y)$ it follows that $F(x,y) = N_{\mathbb{Q}(\alpha_1)/\mathbb{Q}}\ (x - \alpha_1 y)$ where $N_{\mathbb{Q}(\alpha_1)/\mathbb{Q}}$ denotes the norm from $\mathbb{Q}(\alpha_1)$ to $\mathbb{Q}$. Let $L = \beta_1 x_1 + \beta_2 x + \cdots + \beta_n x_n$ and put $K = \mathbb{Q}(\beta_1, \dots, \beta_n)$. Then $N_{K/\mathbb{Q}}(L) = h$ is a norm form equation and Schmidt has determined when such equations have infinitely many solutions. Schlickewei has extended this to the p-adic case. All of this work is built on the original work of Thue and it has a serious flaw. The work is "ineffective" in the sense that while one can bound the number of solutions one can't bound the size of the largest solution. The reason for this is that Thue assumed the existence of a very large solution of (4), and then showed there couldn't be many still larger solutions.

How does one solve a Thue equation effectively? Of course one can try congruence arguments. Let me conclude this lecture by mentioning three other general approaches. The first is the hypergeometric method. It applies to special numbers α of the form $\sqrt[n]{a}$ for a in $\mathbb{Z}$ and was initiated by Thue. In 1964 Baker proved, with this method, that for all integers p and q with q positive,

$$|\sqrt[3]{2} - p/q| > \frac{c}{q^\kappa} ,$$

where $c = 10^{-6}$ and $\kappa = 2.955$. Chudnovsky, in 1983, replaced κ by 2.43, although he did not compute c, and in 1987 Easton, a Ph.D. student of mine, showed that one may take $c = 10^{-6}$ and $\kappa = 2.8$. The above proofs depend upon an examination of a sequence of Padé approximants $\dfrac{p_n(x)}{q_n(x)}$ to $(1-x)^{1/3}$. Thus $(1-x)^{1/3} q_n(x) - p_n(x) = x^{2n+1} R_n(x)$ where $p_n(x)$ and $q_n(x)$ are polynomials in x of degree n with rational coefficients and where $R_n(x)$ is a power series in x with rational coefficients. For an appropriate choice of x we find a sequence of rational approximations to $(1-x)^{1/3}$ which yield an irrationality measure for $(1-x)^{1/3}$.

Bombieri, in 1982, reworked the Thue-Siegel theorem to find some special cases where it gave effective improvements on the Liouville exponent. Both this approach and the hypergeometric approach depend on the existence of a very good approximation for their success.

In 1966, Baker proved a result that led to the first general effective improvement on the Liouville estimate. He was awarded a Fields medal for this work in 1970. The work originated in transcendence theory and it allows one to effectively solve all Thue equations, at least in principle. In 1986, Baker and I sharpened these arguments in the special case $\alpha = \sqrt[3]{a}$ for a a positive integer which is not a perfect cube. Let ϵ be the smallest unit larger than one in the ring of algebraic integers of $\mathbb{Q}(\sqrt[3]{a})$. Then for all integers p and q with q positive,

$$|\sqrt[3]{a} - p/q| > c/q^\kappa ,$$

where $c = \dfrac{1}{3ac_1}$, $\kappa = 3 - 1/c_2$ and

$$c_1 = \epsilon^{(50 \log\log \epsilon)^2} , \quad c_2 = 10^{12} \log \epsilon .$$

Further if m is a positive integer, all solutions of $x^3 - ay^3 = m$ satisfy

$$\max(|x|, |y|) < (c_1 m)^{c_2} .$$

For example, for the cube root of 14 we have $\epsilon = 29 + 12\sqrt[3]{14} + 5(\sqrt[3]{14})^2$. Thus we can take $c = 10^{-11,000}$ and

$$\kappa = 2.9999999999998 .$$

The best previous result needed about 150 9's after the decimal point. In spite of the small size of c and the closeness of κ to 3, it is possible to solve these equations completely for small a and m. One of the ingredients used in the determination of the complete list of solutions is the Lenstra-Lenstra-Lovasz algorithm.

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, CANADA N2L 3G1

E-mail address: cstewart@watserv1.uwaterloo.ca