How to Solve a Diophantine Equation: A Number-Theoretic Excursion

R. J. Stroeker

The American Mathematical Monthly, Vol. 91, No. 7 (Aug. - Sep., 1984), 385-392.

Stable URL:
http://links.jstor.org/sici?sici=0002-9890%28198408%2F09%2991%3A7%3C385%3AHTSADE%3E2.0.CO%3B2-%23

The American Mathematical Monthly is currently published by Mathematical Association of America.

HOW TO SOLVE A DIOPHANTINE EQUATION

A NUMBER-THEORETIC EXCURSION

R. J. STROEKER
Econometric Institute, Erasmus University Rotterdam, P.O. Box 1738, 3000 DR Rotterdam, The Netherlands

1. Introduction. Some time ago I was asked by Richard T. Bumby to investigate the equation

$$(x^2 - 2)^2 - 2 = 2y^2 \tag{1}$$

in rational integers x and y. In his letter Bumby explained that he had stumbled on a brief proof of the assertion that this diophantine equation has no other solutions than those given by $y = \pm 1$. Without hinting in any way at his own line of reasoning, he asked me to test the hypothesis that his proof is the obvious one in the sense that any "reasonable person" would discover the same proof. Flattered by being considered a reasonable person by implication, I set to work and although I did also find a solution not quite like Bumby's, there is no reason to reject his hypothesis. For, curiously enough, first I found a proof on a par with Bumby's descent argument (see Section 5) and soon after I realized that a more elementary and straightforward solution is possible. Subsequently I learned that equation (1) arose in the context of a search for squares amongst the elements of certain recurrences of order two [**5**].

In the course of my investigations I bumped into several blank walls. That is to say, some natural ways of tackling the problem apparently do not lead to the required solution. However, I also discovered some useful approaches, so that I can offer a few different proofs. What made me write all this down was the realization that quite a few methods for solving diophantine equations can be illustrated non-trivially by this particular equation. Thus, this paper has an expository character; it discusses certain number-theoretic methods which are especially useful for solving diophantine equations.

In the following sections I shall give a systematic exposition of the arguments leading to a solution. Occasionally, a digression is made from the main path for reasons of clarification and illustration. In the final section I shall briefly discuss a selection of references chosen from the most relevant literature.

2. Factorization. First of all it should be noted that the diophantine equation (1) has but finitely many solutions. This can be shown as an application of a famous theorem by A. Thue [**32**] published in 1909, which states that, for any irreducible form $f \in \mathbb{Z}[x, y]$ of degree at least three, the equation

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

admits at most finitely many solutions $(x, y) \in \mathbb{Z}^2$ for any rational integer m. At the end of this section it will become clear how this theorem may be used in connection with equation (1).

Roughly speaking, the methods used for solving diophantine equations either are essentially of an analytic nature or use mainly algebraic techniques. The class of analytic methods is based on the theory of diophantine approximation culminating in the so-called Gel'fond-Baker method. This is very high-powered stuff and it seems advisable to consider first something of a more elementary nature. In Section 6 we shall briefly return to this very powerful method.

R. J. Stroeker: I received my mathematical education at the University of Amsterdam. In 1975 I took my doctor's degree there under the guidance of F. Oort. The years 1966–1971 I spent in Manchester (UK), where I taught at the University. During Lent term of 1969 I stayed at Oxford University with B. J. Birch. Since 1971 I have been teaching at Erasmus University, Rotterdam. My mathematical interests are in diophantine analysis, elliptic curves, classical approximation theory, and mathematical economics. I am a fervent bookbinder, I like to play badminton, and I play the cello occasionally.

The most down-to-earth approach is to merely use divisibility techniques such as unique factorization, congruences, quadratic reciprocity and the like. So, to start with, let us look upon our problem from an elementary point of view.

Suppose $(x, y) \in \mathbb{Z}^2$ is a solution of (1). Clearly x is even and this forces y to be odd. Put $x =: 2z$ and rewrite the equation to look like

$$y^2 + 1 = 2(2z^2 - 1)^2. \tag{2}$$

Assuming $y^2 \neq 1$, it follows that $y^2 + 1$ is divisible by an odd prime p which is necessarily of the form $p \equiv 1 \pmod 4$. From (2) it can be seen that each such prime divides $y^2 + 1$ to an even power, so that

$$y^2 + 1 = 2\Pi p^{2\alpha_p} \quad \text{and} \quad 2z^2 - 1 = \Pi p^{\alpha_p} \qquad (\alpha_p \in \mathbb{N}),$$

where the nonempty products are to be taken over all distinct primes $p \equiv 1 \pmod 4$ dividing $y^2 + 1$. Since we do not know anything of the primes p involved beyond the fact that they belong to the infinite set of primes of the form $\equiv 1 \pmod 4$, and because the values of the exponents α_p are also unknown, we soon realize that our line of reasoning most likely leads nowhere. Let us turn our attention in (we hope) a more promising direction.

A widely used technique in diophantine analysis is the technique of factorization. It is based on the application of the *fundamental theorem of arithmetic* (FTA) or its generalization to algebraic number fields. (An algebraic number field is understood to be a finite extension of the field of rationals $\mathbb{Q}$.) This FTA says that every positive integer can be written in one way only as a product of primes, except for the order in which the primes occur in the product. Another way of saying this is that the domain of integers $\mathbb{Z}$ is a *unique factorization domain* (UFD). Unlike $\mathbb{Z}$, the ring of integers O_K of an algebraic number field K often does not have this property. If O_K is a UFD, then K is said to have the unique factorization property. A few examples of such fields are: $\mathbb{Q}$, $\mathbb{Q}(i)$ (the field of Gaussian numbers), $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\exp(2\pi i/5))$. Fields that do not have the unique factorization property are, for instance, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt[3]{7})$ and $\mathbb{Q}(\exp(2\pi i/23))$. For more details on unique factorization it is suggested that the reader consult [**4**], Chapter 3 or [**29**], Chapter 8. In fields that do not have the unique factorization property, unique factorization can be restored in the following sense: replace in our formulation of the FTA the words *positive integer* by *integral ideal* and the word *prime* by *prime ideal*. This leads to Dedekind's celebrated unique factorization theorem of ideals in number fields (cf. [**13**], Theorem I.4.2.).

Factorization of (2) in the ring of Gaussian integers $\mathbb{Z}[i]$ yields

$$y + i = \varepsilon(1 + i)(a + bi)^2$$

for rational integers a and b and $\varepsilon \in \{\pm 1, \pm i\}$. Indeed, $y^2 + 1 = (y + i)(y - i)$ and hence every Gaussian prime divisor of $y + i$ not dividing 2 divides $y + i$ to an even power. Then

$$2z^2 = 1 + a^2 + b^2 \quad \text{with} \quad |a^2 - b^2 \pm 2ab| = 1,$$

so that in particular a and b are relatively prime. Without loss of generality we may choose a and b such that $a^2 - b^2 \pm 2ab = 1$. Hence

$$2z^2 = 1 + a^2 + b^2 = (a^2 - b^2 \pm 2ab) + a^2 + b^2 = 2a(a \pm b)$$

Since a and $a \pm b$ are relatively prime, factorization of $z^2 = a(a \pm b)$ in $\mathbb{Z}$ leads to

$$a = \delta B^2, \quad a \pm b = \delta A^2$$

with $\delta = \pm 1$ and $z = AB$. Substitution of these expressions for a and b into $a^2 - b^2 \pm 2ab = 1$ gives

$$A^4 - 4A^2B^2 + 2B^4 = -1. \tag{3}$$

The equations (2) and (3)—and consequently also (1) and (3)—are equivalent in the sense that the solutions of one lead to all solutions of the other and conversely. But equation (3) has the

advantage of homogeneity, so that Thue's theorem, mentioned at the beginning of this section, can be directly applied. Unfortunately, this theorem does not give the solutions (if they exist) explicitly; the proof of Thue's result has a noneffective character. This leaves us as far from the actual solution of the problem as we were right at the start. Or does equation (3) after all provide a more natural way to look at the problem?

3. Norm Form Equations. Instead of merely asking for rational integers A and B satisfying (3), we may reformulate equation (3) in the following algebraic way.

The polynomial $f(t) := t^4 - 4t^2 + 2$ is irreducible over $\mathbb{Z}$ and the equation $f(t) = 0$ has four real roots, namely θ, $-\theta$, θ' and $-\theta'$, where $\theta := (2 + \sqrt{2})^{1/2}$ and $\theta' := (-1 + \sqrt{2})\theta$. Put $K := \mathbb{Q}(\theta)$, the extension of $\mathbb{Q}$ by θ. Then equation (3) takes the form

$$(A + B\theta)(A - B\theta)(A + B\theta')(A - B\theta') = -1$$

or, written in terms of the norm function,

$$\text{Norm}_{K/\mathbb{Q}}(A + B\theta) = -1. \tag{4}$$

This so-called norm form equation means that $\varepsilon := A + B\theta$ is a unit of O_K of a very special sort. What is so remarkable about it? Let me explain. As it happens, the basis $\{1, \theta, \theta^2, \theta^3\}$ of K as a vector space over $\mathbb{Q}$ is also an integral basis. That is to say, each integer of O_K can be uniquely expressed as a linear combination of these first four powers of θ with rational integral coefficients. The special character of ε lies in the fact that its expression as a linear combination of 1, θ, θ^2 and θ^3 has vanishing coefficients of θ^2 and θ^3.

Now if the structure of the group of units in O_K were known, the extra information on ε provided by its special form could be used to further restrict the possibilities for ε and hence also for the values of A and B. Fortunately, *Dirichlet's unit theorem* gives exact information on the structure of this unit group. To be precise, it says that the group of units in the ring of integers O_L of an algebraic number field L is the direct product of a finite cyclic group of roots of unity and a free abelian group of rank $r + s - 1$, where r is the number of real conjugate fields of L and s is the number of pairs of complex conjugate fields of L (see for instance [**13**], Theorem I.11.19).

In our case, the number field K has no roots of unity other than 1 and -1. Moreover, K is totally real so that $r = 4$ and $s = 0$. This implies that the free abelian group has three generators, ε_1, ε_2, ε_3 say. The set of these so-called *fundamental units* $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ can be effectively computed. A very clear and detailed account of such a process is given in the two papers of Pohst and Zassenhaus [**23**].

As a result of all this, we deduce from the norm form equation (4) the equation

$$A + B\theta = \pm\varepsilon_1^{e_1}\varepsilon_2^{e_2}\varepsilon_3^{e_3}, \tag{5}$$

where the exponents e_i are rational integers. We also get similar expressions for $A - B\theta$, $A + B\theta'$ and $A - B\theta'$ by considering the conjugation maps characterized by $\theta \mapsto -\theta$, $\theta \mapsto \theta'$ and $\theta \mapsto -\theta'$. Elimination of the unknown A and B from (5) and its conjugate equations yields a set of two equations in the three unknown exponents e_1, e_2 and e_3. Unfortunately, this is one unknown too many; Skolem's p-adic method, which is standard in this context, only works if the number of equations equals the number of unknown exponents. A detailed discussion of this method goes far beyond the scope of this paper. The persevering reader is referred to [**4**] or [**17**] (see also [**28**]). We shall only, be it very superficially, describe how the method often works.

Suppose certain expressions E involving the unknown exponents can be shown to satisfy congruences of the form

$$E \equiv 0 \pmod{p^\alpha}$$

for suitable rational primes p and all positive rational integers $\alpha > \alpha_0$. Then necessarily these expressions E must vanish. For instance, if in (5) it could be shown that each of the expressions $E_1 = e_1 - 1$, $E_2 = e_2$, $E_3 = e_3$ vanishes, then $A + B\theta = \pm\varepsilon_1$ which gives essentially one possi-

ble value for A as well as B. One could take $\varepsilon_1 = 1 + \theta$ (check that this is indeed a unit) and then $A = B = \pm 1$ would solve equation (3). Alas, Skolem's method does not apply in this particular case.

We have arrived at yet another dead end, it would seem. Sometimes one may succeed in restoring the conditions necessary for applying Skolem's method successfully, by considering a suitable finite extension of K. However, calculations tend to get very messy (cf. [**18**]), so much so that it often is more reasonable to try something else instead.

4. Recurrences. An obvious way of solving a diophantine equation which has not been mentioned so far, at least not in so many words, is simply that of reducing it to an equation that has already been solved.

Returning to equation (3), we rewrite it this time as

$$(A^2 - 2B^2)^2 - 2B^4 = -1. \tag{6}$$

This equation looks familiar; in [**19**] Ljunggren shows that the only positive integer solutions of the equation

$$y^2 + 1 = 2x^4 \tag{7}$$

are given by $(x, y) = (1, 1)$ and $(13, 239)$. For equation (6) Ljunggren's result means that the only solutions are given by $A^2 = B^2 = 1$ as a quick calculation confirms. *So we are done and the solution to our original problem is a fact.* However, this way of solving it is not quite satisfactory in the sense that Ljunggren's solution of (7) is very difficult. Couldn't we find a more elementary way of solving (6)? The answer is affirmative, as we shall see shortly.

Factorization of (6) in $\mathbb{Q}(\sqrt{2})$ yields

$$\mathrm{Norm}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(A^2 - 2B^2 + B^2\sqrt{2}) = -1.$$

Since all units of $\mathbb{Q}(\sqrt{2})$, disregarding their sign, are integral powers of $1 + \sqrt{2}$, we deduce that

$$A^2 - 2B^2 + B^2\sqrt{2} = \pm(1 + \sqrt{2})^{2k-1}, \quad k \in \mathbb{Z}. \tag{8}$$

It is easy to see that the $\pm$ sign in (8) may be dropped.

By the binomial theorem it can be seen that the numbers x_k and y_k, defined by the formula

$$x_k + y_k\sqrt{2} = (1 + \sqrt{2})^k, \quad k \in \mathbb{Z} \tag{9}$$

are rational integers. On taking the conjugate equation of (9) into account—this conjugate equation is obtained from (9) on replacing $\sqrt{2}$ by $-\sqrt{2}$ both times—we arrive at the following expressions for x_k and y_k:

$$x_k = \frac{\varepsilon^k + \varepsilon'^k}{\varepsilon + \varepsilon'} \quad \text{and} \quad y_k = \frac{\varepsilon^k - \varepsilon'^k}{\varepsilon - \varepsilon'}, \tag{10}$$

where we have written $\varepsilon := 1 + \sqrt{2}$ and $\varepsilon' := 1 - \sqrt{2}$ for convenience. Using these expressions for x_k and y_k, it is not difficult to verify the formulae:

$$\begin{array}{lll} \text{(i)} & x_0 = 1, x_1 = 1 \quad \text{and} \quad x_{k+1} = 2x_k + x_{k-1} & \\ & y_0 = 0, y_1 = 1 \quad \text{and} \quad y_{k+1} = 2y_k + y_{k-1} & \\ \text{(ii)} & y_{k+1} = y_k + x_k \quad \text{and} \quad x_{k+1} = x_k + 2y_k & , \quad k \in \mathbb{Z}. \\ \text{(iii)} & x_{-k} = (-1)^k x_k \quad \text{and} \quad y_{-k} = (-1)^{k-1} y_k & \end{array} \tag{11}$$

From (8) we deduce immediately that $A^2 - 2B^2 = x_{2k-1}$ and $B^2 = y_{2k-1}$ for some $k \in \mathbb{Z}$, $k \geqslant 0$, or by (11) (ii)

$$A^2 = x_{2k}, \; B^2 = y_{2k-1}. \tag{12}$$

This leads to yet another interpretation of equation (3): the solutions of (3) are characterized by

simultaneous squares in the sequences of rational integers $(x_{2n})_n$ and $(y_{2n-1})_n$ defined by (9). Apparently, a possible way to deal with our problem in this form is to use congruence considerations and "in particular" quadratic reciprocity. From (11) (i) we deduce that both x_{2n} and y_{2n-1} are odd for all n. So, from (12) we have

$$x_{2k} = A^2 \equiv 1 \pmod 8,$$

which implies that k is even. Put $k =: 2l$. It can be shown using the expressions (10) that for all n

$$x_{2n} + (-1)^{n+1} = (2y_n)^2.$$

Thus $A^2 - 1 = x_{4l} - 1 = (2y_{2l})^2$ and hence

$$A - 2y_{2l} = A + 2y_{2l} = \pm 1.$$

Clearly this is only possible when $y_{2l} = 0$ and $A^2 = 1$, implying also that $B^2 = 1$ in (3). *This solves equation* (3) *and we have discovered an elementary solution to our problem.* Unexpectedly, this solution turns out to be rather uncomplicated: we merely needed to show that the only square amongst elements of the sequence $(x_n)_{n \geqslant 0}$ with even index is $x_0 = 1$. This simplicity is coincidental. In general it is not so easy to determine all squares in a given linear recurrent sequence of order two. See [**6**], [**7**] and [**14**]. In this particular case Ljunggren's result [**19**] shows that the only squares in the sequence $(x_n)_{n \geqslant 0}$ are $x_0 = 1$, $x_1 = 1$ and those in the sequence $(y_n)_{n \geqslant 0}$ are $y_1 = 1$, $y_7 = 13^2$.

5. Infinite Descent. Although we have settled the problem we set out to solve, our method of proof is not the one Bumby had in mind. In fact, he was thinking of a so-called descent argument, which may be described as follows.

Imagine we are looking for all solutions of problem P in positive integers s. Suppose that, given a solution s of P, it can be proved that a smaller solution s' of P exists. In this way, given an initial positive integer solution, an infinite strictly decreasing sequence of positive integer solutions of P is obtained. However, a nonempty set of positive integers contains a smallest element. We have arrived at a contradiction. Consequently, there exists no such positive integer solution of P.

In the lines to follow we apply this descent argument to our equation. We return to equation (2). Let z be a positive integer satisfying C: $2(2z^2 - 1)^2 - 1 =$ square, subject to $z > 1$.

In the notation of Section 2 we have $z = AB$, where A and B satisfy equation (3). Once again, according to (12), a nonnegative rational integer k exists such that

$$A^2 = x_{2k} \quad \text{and} \quad B^2 = y_{2k-1}.$$

From the formulae (11) we deduce that $k \equiv 0 \pmod 4$. Put $k =: 4m$, then $m \geqslant 1$ because $z > 1$. As before, it can be shown using (10) that for all n

$$x_{2n} + (-1)^n = 2x_n^2.$$

Successive application of this identity with $n = 2m$ and $n = 4m$ yields

$$2\left(2x_{2m}^2 - 1\right)^2 - 1 = x_{8m} = A^2 = \text{square},$$

so that x_{2m} also satisfies C (note that $x_{2m} = 1$ implies $z = 1$). Finally, from

$$1 < x_{2m}^2 < x_{8m} y_{8m-1} = A^2 B^2 = z^2$$

it follows that $1 < x_{2m} < z$, which completes our descent argument. Our conclusion must be that $z = 0$ and $z = \pm 1$ are the only solutions of (2). *We have obtained a third solution to our problem, this time based on the classic idea of infinite descent, attributed to Pierre de Fermat.*

6. Diophantine Approximation. Suppose for the moment that all elementary and algebraic ideas considered so far have failed to produce a complete solution. Which other methods can be tried? Are there any more useful approaches to problems of this type? Certainly, the determina-

tion of integer solutions of a given diophantine equation may often be effected by looking for good rational approximations of certain algebraic, irrational numbers. To illustrate this point, consider again equation (8)

$$A^2 - 2B^2 + B^2\sqrt{2} = (1 + \sqrt{2})^{2k-1} \tag{13}$$

and assume $k \in \mathbb{N}$. This assumption does not cause a loss of generality, because an analogous argument can be used when $k \leqslant -1$, $k \in \mathbb{Z}$.

On taking the conjugate equation of (13) and dividing through by B^2, we have

$$2 + \sqrt{2} - \left(\frac{A}{B}\right)^2 = \frac{(1 + \sqrt{2})^{1-2k}}{B^2}.$$

Put $\theta := (2 + \sqrt{2})^{1/2}$, $\varepsilon := 1 + \sqrt{2}$ and assume A and B to be positive. It follows that

$$\theta\left|\theta - \frac{A}{B}\right| < \left|\theta + \frac{A}{B}\right|\left|\theta - \frac{A}{B}\right| = \frac{\varepsilon^{1-2k}}{B^2}$$

and thus

$$\left|\theta - \frac{A}{B}\right| < \frac{\varepsilon^{1-2k}}{\theta B^2} < \frac{1}{2B^2}. \tag{14}$$

In particular, this shows that A/B is a convergent of the regular continued fraction expansion of θ (cf. [**29**], Chapter 7). It also shows that A/B is very close to θ compared with B^{-2} when k is large. However, A/B cannot be too close to θ compared with B^{-4}. To be more precise, N. I. Feldman showed in 1971 [**10**] (see also [**11**]), using the powerful method developed by Gelfond and Baker that, given an algebraic number of degree $n \geqslant 3$ (in our case $n = 4$), effectively computable positive constants c and δ (depending on θ only) may be determined such that

$$\left|\theta - \frac{A}{B}\right| > \frac{1}{cB^{n-\delta}}$$

for any rational integers A, $B > 0$. Combining this with (14), we have

$$B^{2-\delta} > \frac{\theta\varepsilon^{2k-1}}{c}. \tag{15}$$

From (13) it is obvious that $A^2 - 2B^2 \geqslant 1$ since $k \geqslant 1$, and hence $B^2\sqrt{2} < \varepsilon^{2k-1}$. In view of (15), this implies

$$B^{\delta} < \frac{c}{\theta}B^2\varepsilon^{1-2k} < \frac{c}{\theta\sqrt{2}} < \frac{1}{2}c.$$

This inequality means that we have established an effectively computable upper bound B_0 for B. So, at least in principle, all solutions of (13) with $k \geqslant 1$ can be determined by checking the convergents of the regular continued fraction expansion of θ with denominators bounded from above by B_0. However, this constant B_0 may be spoiling the fun by being exceedingly large.

At this stage it may be proper to briefly comment on Baker's method, which has given the study of diophantine equations a tremendous impetus. Its most useful application to the theory of diophantine equations to date is probably given by the following inequality

$$0 < |b_1\log\alpha_1 + b_2\log\alpha_2 + \cdots + b_n\log\alpha_n| < e^{-\delta H}, \tag{16}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are given algebraic numbers ($\alpha_i \neq 0$ or 1), $0 < \delta \leqslant 1$ is a given real number and $b_1, b_2, \ldots, b_n$ are unknown rational integers with $H := \max(|b_1|, |b_2|, \ldots, |b_n|)$. If such an inequality holds, then Baker showed that $H < C$, where C is effectively computable in terms of the α's, δ and n. Many polynomial and exponential diophantine equations can be 'reduced' to inequalities of type (16), where the b's correspond to the unknown solutions. Usually, the

constant C is large. This may cause considerable practical problems in the sense that it could make a computer search utterly unfeasible. As an illustration, consider the Catalan equation $x^m - y^n = 1$. Tijdeman [**34**] proved that this equation has only finitely many solutions in integers $x > 1$, $y > 1$, $m > 1$, $n > 1$ and Langevin [**15**] calculated that for a solution (x, y, m, n) the following inequality holds:

$$x^m < \exp\exp\exp(250).$$

It seems that by the existing techniques this hopelessly large upper bound cannot be significantly lowered. This means that Catalan's conjecture (i.e., the only perfect powers differing by 1 are 3^2 and 2^3) is still not resolved.

Possibly the best known example of a successful attempt to solve a diophantine equation by Baker's method, not only in theory but also practically, is that of [**2**]. In order to solve the system of equations

$$3x^2 - 2 = y^2, \quad 8x^2 - 7 = z^2, \tag{17}$$

Baker and Davenport showed by factorization in $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ that to each solution (x, y, z) of (17) a pair (m, n) corresponds with

$$0 < m\log\alpha_1 - n\log\alpha_2 + \log\alpha_3 < 0.11\alpha_1^{-2m},$$

where $\alpha_1 := 2 + \sqrt{3}$, $\alpha_2 := 3 + 2\sqrt{2}$ and $\alpha_3 := 2(1 + \sqrt{3})\sqrt{2}/(\pm 1 + 2\sqrt{2})\sqrt{3}$. They estimated that $m < 10^{487}$ This huge m-region to be checked was reduced to the region $m < 500$ by applying a simple but ingenious lemma from diophantine approximation theory which involved the calculation of the two numbers $\log\alpha_3/\log\alpha_2$ (both signs) to 600 decimal places. Ultimately it was concluded that the only positive solutions of (17) are given by $x = 1$ and $x = 11$. In 1978 Grinstead [**12**] indicated how most of this very large number of m-values to be checked initially could be ruled out quickly by using a simple computer technique based on congruence considerations. It should also be mentioned that in [**14**] an elementary, but complicated, solution to problem (17) is given by means of quadratic reciprocity techniques.

For more examples on the solving of diophantine equations by Baker's method the reader is referred to Ellison [**9**].

We have already indicated a few times how the computer can be used to assist in the process of solving diophantine equations. More facts and ways on this particular approach may be found in [**31**] which also contains an extensive list of references.

7. Literature. Although the field of diophantine analysis is very old, relatively few books have been published dealing with diophantine equations exclusively. Best known are the books written by Mordell [**21**] and Skolem [**27**]. Less well known is the booklet by Bašmakova [**3**]. It is rather elementary, but it contains some interesting historical information. Most textbooks on number theory contain a chapter on diophantine equations. We mention only a few: Borevich & Shafarevich [**4**], LeVeque [**16**], Nagell [**22**] and Stark [**29**]. The algebraic background necessary can be found in Janusz [**13**], Ribenboim [**24**] and Stewart & Tall [**30**]. Schmidt's book [**25**] is a very nice book on diophantine approximation. Information on computer methods useful for diophantine problems can be obtained from Grinstead [**12**], Pohst & Zassenhaus [**23**], Stroeker & Tijdeman [**31**] and Williams [**35**]. Articles of an expository nature treating diophantine equations are: Baker [**1**], Shorey et al [**26**], Tijdeman [**33**], Stroeker & Tijdeman [**31**] and London & Finkelstein [**20**].

Finally, from a historical point of view, Dickson's famous history on the theory of numbers deserves to be mentioned [**8**]. It contains information on most results in diophantine analysis prior to 1920.

References

1. A. Baker, Effective Methods in Diophantine Problems, Proc. Symp. Pure Math., AMS, Providence, RI, vol. 20, 1971, 195–205; vol. 24, 1973, 1–7.

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

3. I. G. Bašmakova, Diophant und diophantische Gleichungen, Uni-Taschenbücher 360, Birkhäuser Verlag, Basel und Stuttgart, 1974.

4. Z. I. Borevich and I. R. Shafarevich, Number theory, Pure and Appl. Math. Ser., 20, Academic Press, London and New York, 1966.

5. R. T. Bumby, Unpublished manuscript of a talk held at the AMS meeting at San Francisco, Jan. 1981, on the integer solutions of the diophantine equation $Ax^2 + By^4 = 4$ ($A, B \in \mathbb{Z}, AB < 0$).

6. J. H. E. Cohn, Eight diophantine equations, Proc. London Math. Soc. (3), 16 (1966) 153–166.

7. _____, Five diophantine equations, Math. Scand., 21 (1967) 61–70.

8. L. E. Dickson, History of the Theory of Numbers, vol. II: Diophantine analysis, Chelsea, New York, 1971 (reprinted from the 1920 edition).

9. W. J. Ellison, Recipes for solving diophantine problems by Baker's method, Sém. Th. Nombr. 1970/71, Exp. no. 11, Lab. Théorie des Nombres, CNRS, Talence, 1971.

10. N. I. Feldman, An effective power sharpening of a theorem of Liouville, Izv. Akad. Nauk. SSSR, Ser. Mat., 35 (1971) 973–990 (Russian).

11. _____, Rational approximations of algebraic numbers, in: Topics in number theory, P. Turán, ed., Coll. Math. Soc. János Bolyai, no. 13, North-Holland Publ. Co., 1976, 31–39.

12. C. M. Grinstead, On a method of solving a class of diophantine equations, Math. Comp., 32, no. 143 (1978) 936–940.

13. G. J. Janusz, Algebraic number fields, Pure and Appl. Math. Ser., 55, Academic Press, New York and London, 1973.

14. P. Kanagasabapathy and Tharmambikai Ponnudurai, The simultaneous diophantine equations $y^2 - 3x^2 = -2$ and $z^2 - 8x^2 = -7$, Quart. J. Math. Oxford (3), 26 (1975) 275–278.

15. M. Langevin, Quelques applications de nouveaux résultats de van der Poorten, Sém. Delange-Pisot-Poitou, 17 (1976) no. G12.

16. W. J. LeVeque, Topics in Number Theory, vol. II, Addison-Wesley, Reading, MA, 1956.

17. D. J. Lewis, Diophantine equations: p-adic methods, in: W. J. LeVeque (ed.), Studies in number theory, MAA 1969, 25–75.

18. W. Ljunggren, Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante, Acta Math., 75 (1942) 1–21.

19. _____, Zur Theorie der Gleichung $x^2 + 1 = Dy^4$, Avh. Norske Vid. Akad. Oslo I, no. 5, 1942.

20. H. London and R. Finkelstein, On Mordell's equation $y^2 - k = x^3$, Bowling Green State University Press, Ohio, 1973.

21. L. J. Mordell, Diophantine equations, Pure and Appl. Math. Ser., 30, Academic Press, New York and London, 1969.

22. T. Nagell, Introduction to Number Theory, Chelsea, New York, 1964 (reprint of the second edition 1951).

23. M. Pohst and H. Zassenhaus, On effective computation of fundamental units, I, II, Math. Comp., 38, no. 157 (1982) 275–291 and 293–329.

24. P. Ribenboim, Algebraic numbers, Pure and Appl. Math. Vol. XXVII, Wiley-Interscience, 1972.

25. W. M. Schmidt, Diophantine approximation, Lecture Notes in Math., 785, Springer Verlag, 1980.

26. T. N. Shorey, A. J. van der Poorten, R. Tijdeman and A. Schinzel, Applications of the Gel'fond-Baker method to diophantine equations, in: A. Baker and D. W. Masser (eds.), Transcendence theory: Advances and applications, Academic Press, London and New York 1977, 59–78.

27. T. Skolem, Diophantische Gleichungen, Erg. Math. Grenzgeb. Bd. 5, Heft 4, Springer 1938 (reprinted by Chelsea, New York, 1950).

28. _____, The use of p-adic methods in the theory of diophantine equations, Bull. Soc. Math. Belg., 7 (1955) 83–95.

29. H. M. Stark, An Introduction to Number Theory, MIT Press, 1978 (reprint of Markham Publ., 1970).

30. I. N. Stewart and D. O. Tall, Algebraic Number Theory, Chapman and Hall, London, 1979.

31. R. J. Stroeker and R. Tijdeman, Diophantine equations (with an appendix by P. L. Cijsouw, A. Korlaar and R. Tijdeman), in: Computational methods in number theory, H. W. Lenstra, Jr., and R. Tijdeman, eds., Math. Centre Tracts, vols. 154, 155 (1982), 321–369.

32. A. Thue, Über Annäherungswerte algebraischer Zahlen, J. Reine Angew. Math. (Crelle), 135 (1909) 284–305.

33. R. Tijdeman, Exponential diophantine equations, in: Proc. Int. Congress of Math., Helsinki 1978, 381–387.

34. _____, On the equation of Catalan, Acta Arithm., 29 (1976), 197–209.

35. H. C. Williams, The influence of computers in the development of number theory, Comput. Math. Appl. vol. 8 (2), (1982) 75–93.