Diophantine equations

V. Srinivas

This article gives an introduction, accessible to non-specialists, to the topic of Diophantine equations. Mainly, this is the study of solutions of polynomial equations $f(x_1,\ldots,x_n)=0$ in whole numbers (integers), where the polynomial f has integer coefficients. This is broadened to include the study of solutions of one or more such equations in rational numbers (fractions) and algebraic numbers. A famous example of a Diophantine problem is given by Fermat's Last Theorem, which is the statement that $x^n+y^n=z^n$ has no solutions where x, y, z are positive whole numbers (natural numbers), if n is at least 3. This problem is still unsolved. Another well-known equation is $x^2 - Ny^2 = 1$, where N is at least 2; this equation was studied by Indian mathematicians like Brahmagupta and Bhaskara. The article gives some historical background, including the works of Fermat, Gauss and others, leading up to a discussion of some current development—the work of Faltings, and new ideas related to Fermat's Last Theorem.

Diophantine equations are polynomial equations with integer coefficients, for which we wish to find integer solutions.

For example, consider the equations

$$x^2=2y^2, \tag{1}$$
$$x^2=2y^2+1. \tag{2}$$

The first equation has only one integer solution, $x=y=0$, since $\sqrt{2}$ is irrational. However, the second has infinitely many integer solutions (one verifies, with a bit of algebra, that if we write $(1+\sqrt{2})^{2n}$ in the form $a_n+\sqrt{2}b_n$ for some integers a_n, b_n, then $x=a_n$, $y=b_n$ is a solution of equation (2); for example, if $n=1$, we have $(1+\sqrt{2})^2=3+2\sqrt{2}$, and $x=3$, $y=2$ is a solution of equation (2)).

Certain problems, stated in geometrical language, reduce to Diophantine equations. For example, consider the problem of finding right angled triangles in the plane whose sides have integral length; from Pythagoras' theorem, this reduces to finding positive integer solutions of the equation

$$x^2+y^2=z^2.$$

This problem has infinitely many solutions; one may verify that for any positive integers a, b with $a>b$, we have a solution

$$x=a^2-b^2,\ y=2ab,\ z=a^2+b^2;$$

this is equivalent to the algebraic identity

$$(a^2-b^2)^2+4a^2b^2=(a^2+b^2)^2.$$

From our first pair of examples, one sees that in order to understand integer solutions of Diophantine equations, there is sometimes an advantage in considering related problems over larger number systems, which contain the integers. In our examples, one considers the number system consisting of all numbers of the form $a+b\sqrt{2}$, where a, b are integers. Such a number system will form a *ring*, i.e. it will be closed under addition and multiplication; it is called a ring of algebraic numbers.

Next, if we seek integer solutions to $x^2+y^2=z^2$ with the additional condition $z\neq 0$ (which is not a severe restriction, since $x=y=z=0$ is the only solution with $z=0$), then a solution

$$x=a,\ y=b,\ z=c$$

yields a solution in *rational numbers* (fractions) of the equation

$$X^2+Y^2=1,$$

given by $X=a/c$, $Y=b/c$. Conversely, if we have a solution $X=A$, $Y=B$ of $X^2+Y^2=1$, where A, B are rational numbers, then we can write A, B as fractions with a common denominator, say

$$A=a/c,\ B=b/c;$$

then $x=a$, $y=b$, $z=c$ is an integer solution of $x^2+y^2=z^2$.

The term *Diophantine equation*[1] originates from the work of Diophantus of Alexandria, who first studied integer and rational solutions of equations. One of Diophantus' main results is about linear equations—if a, b, c are given integers, then the equation

$$ax+by=c$$

either has no integer solutions (x, y), or it has infinitely many; there are infinitely many solutions precisely when the *greatest common divisor* (g.c.d.) of a and b divides c. Thus,

$$25x+15y=127$$

has no integer solutions, since the g.c.d. of 25 and 15 is 5, which does not divide 127, while

$$25x+15y=125$$

has infinitely many solutions (5 divides 125). Diophantus

V. Srinivas is in the School of Mathematics, Tata Institute of Fundamental Research, Bombay 400 005.

also discusses certain quadratic equations (e.g. $x^2+y^2=z^2$).

Ancient Indian mathematicians were also interested in integer solutions of problems[2]. The solution of linear equations mentioned above was known to Aryabhatta (5th–6th century AD). The equation $x^2-ny^2=1$, for any positive n, was studied by Brahmagupta (7th century), and the general solution was found independently by Jayadeva (11th century) and Bhaskara (12th century).

Probably the most famous (infamous?) Diophantine equation is 'Fermat's Last Theorem'[3]. The chapter on Fermat in E. T. Bell's *Men of Mathematics*[4] is titled 'The Prince of Amateurs'. This refers to the fact that Fermat is the m st famous example of a mathematician who was not a 'professional', i.e. a professor at a university, or supported by a wealthy patron. Pierre Fermat (1601–1665) was a commissioner of requests, and later a King's councilor in the *parlement* (the provincial High Court of Judicature) at Toulouse, in France. He seems to have become interested in mathematics in his late twenties, perhaps through the influence of d'Espagnet, also a magistrate, who was mathematically inclined. Fermat published none of his results, but communicated them to some friends, notably Father Mersenne, in personal letters. Nevertheless, when he died, he was one of the most famous mathematicians in Europe. Today he is best remembered for his work on number theory, particularly Diophantine equations; yet, in his day, he was better known for his work on geometry, calculus, probability, and optics. In his book[5] *Number theory—An approach through history*, Andre Weil writes of Fermat, '. . . it is clear that he always experienced unusual difficulties about writing up his proofs for publication; this awkwardness verged on paralysis when number theory was concerned, since there were no models there, ancient or modern, for him to follow.' Quite clearly, if Fermat were alive today, he would still have to remain an amateur! Weil also writes (of the notoriety of 'Fermat's Last Theorem') that 'his (Fermat's) reputation in the eyes of the ignorant came to rest chiefly upon it'.

'Fermat's Last Theorem' is the statement that for any integer $n\geqslant 3$, the equation

$$x^n+y^n=z^n$$

has no *positive* integer solutions (x, y, z) (equivalently, if (x, y, z) is an integer solution, at least one of x, y, z is zero). Fermat did not announce this result. However, after Fermat's death in 1665, his personal annotated copy of Bachet's *Diophantus* was examined by his son Samuel, while preparing an edition of his father's works. In the margin alongside Diophantus' discussion of $x^2+y^2=z^2$, Fermat remarks, 'No cube can be split into two cubes, nor any biquadrate into two biquadrates, nor generally any power beyond the second into two of the same kind'. He adds that he has discovered a 'truly remarkable proof' for this fact, which 'this margin is too narrow to hold'. Since this notation was found, many mathematicians have struggled (without success) to prove (or disprove) Fermat's assertion. A lot of partial progress has been made, including some recent progress (which we describe later). There were controversies and priority disputes between prominent mathematicians over claimed proofs, which eventually turned out to be incorrect; a prize of 100,000 Marks was offered by Prof. Paul Wolfskehl, a German mathematician, for the first correct solution. This prize amount was greatly devalued after the First World War, but in the foreward to his book[6] on Fermat's Last Theorem, H. E. Edwards wrote (in 1977) that the prize still existed, and was then worth DM 10,000. Claimants for the prize should submit their proofs for scrutiny to the Academy of Sciences in Göttingen.

New light on the subject of prizes (and perhaps on Hilbert!) is shed by the following anecdote[7] about the mathematician David Hilbert, of Göttingen. Hilbert was the chairman of the prize committee that decided on the correctness of proofs of Fermat's Last Theorem; as long as the prize money remained unclaimed, the interest on it was available to the Göttingen mathematics department to invite prominent academic visitors to Göttingen. Hilbert is reputed to have said, 'It's lucky that I am probably the only person who can crack that nut. But I shall take very great care not to kill the goose that lays us such splendid golden eggs'.

Fermat himself described a proof that the special case $x^4+y^4=z^4$ has no positive integer solution, by a new technique, now called Fermat's method of *infinite descent*. In fact, Fermat proved the more general statement[8] that

$$x^4+y^4=w^2$$

has no 'non-trivial' (i.e. with $w\neq 0$) solutions. If $x=a$, $y=b$, $w=c$ is a nontrivial solution, let

$$h=\text{maximum of } a, b, c;$$

call h the *height* of the solution. Then h is a positive integer. However, Fermat was able to show that, given one non-trivial solution (a, b, c) with height h, one must have another non-trivial solution (a', b', c'), with height h', such that $h'<h$. Repeating Fermat's argument, one would obtain an infinite sequence (a_n, b_n, c_n), $n=1, 2, 3, \ldots$ of solutions, with heights $h_1=h$, $h_2=h'$, $h_3, \ldots$ which form an *infinite, strictly decreasing sequence of positive integers*. This is clearly a contradiction; such a sequence does not exist.

Let $\zeta_n=\exp(2\pi i/n)$, which is an nth root of unity (i.e. the nth power of ζ_n equals 1). One can consider the number system consisting of all complex numbers of the form

$$a_0+a_1\zeta_n+a_2\zeta_n^2+\ldots+a_{n-1}\zeta_n^{n-1},$$

where the a_j are all integers. This system forms a ring (i.e. is closed under addition and multiplication), as one can see by using the equation $\zeta_n^n = 1$. It is a familiar fact, first proved by Euclid, that any natural number can be factorized into prime factors, and the factorization is essentially unique. If one assumes an analogous statement for the number system obtained from ζ_n, it is possible to prove by 'infinite descent' that Fermat's Last Theorem is true. Some mathematicians believe that this might be the argument that Fermat had in mind; however, the German mathematician Kummer found that unique factorization is *false* for the number system formed from $\zeta_{23} = \exp(2\pi i/23)$ (and this turns out to be the case for infinitely many ζ_n).

Certain mathematicians, the most prominent of whom was Carl Friedrich Gauss, were less interested in solving specific equations, like the one in Fermat's Last Theorem. They preferred to try to understand why some equations could be solved, and not others, and why there were sometimes only a finite number of solutions, and why there were infinitely many solutions in other cases. In other words, they wished to develop a *theory*[9] of Diophantine equations. Gauss himself, based on his famous quadratic reciprocity law, achieved a thorough understanding of *quadratic* diophantine equations in 2 variables

$$f(x, y) = 0.$$

For example, consider the equation

$$x^2 + xy + 5y^2 = p,$$

where p is a given prime number. Gauss' methods show that this equation has an integer solution (x, y) (which is essentially unique) precisely when $p = 19$ (when $x = -1$, $y = 2$ is a solution), or else, on dividing p by 19, one obtains one of the following remainders:

1,4,5,6,7,9,11,16,17,

(these are the possible non-zero remainders obtained by dividing *squares* of integers by 19). For example, it is known that $p = 2^{127} - 1$ is a prime number[10]. One computes that p leaves a remainder of 1 on division by 19 (since $2^9 = 512$ leaves a remainder of 18, i.e. of '-1', $2^{18} - 1$ is divisible by 19; but

$$(2^{127} - 1) - 1 = 2^{127} - 2 = 2\,(2^{126} - 1) = 2\,((2^{18})^7 - 1)$$

which is divisible by $2^{18} - 1$, and hence by 19. Hence

$$x^2 + xy + 5y^2 = 2^{127} - 1$$

has an integer solution. The special role played by 19 is because the *discriminant* of the quadratic expression is -19 (the discriminant of $ax^2 + bxy + cy^2$ is $b^2 - 4ac$). A more spectacular example is the statement that

$$x^2 + 5xy + 47y^2 = 2^{11213} - 1$$

has an integer solution[11]. Gauss also studied generalizations of quadratic reciprocity, which eventually led Hilbert and others to what is now called *class field theory*[12].

The first general result on higher degree equations was obtained by the Norwegian mathematician Axel Thue, in 1910. Let $f(x, y)$ be a homogeneous polynomial of degree $d \geqslant 3$, i.e. we can write

$$f(x, y) = \sum_{r=0}^{d} a_r x^r y^{d-r},$$

where the a_r are all integers; assume $a_d \neq 0$. Suppose f cannot be factorized as a product of two polynomials of smaller degree, with integer coefficients. Then for any integer $m \neq 0$, Thue showed that the equation

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

has only a *finite number* of integer solutions. The proof is based on the following idea: write

$$f(x, y) = a_d \prod_{r=1}^{d} (x - \alpha_r y),$$

where $\alpha_1, \alpha_2, \ldots, \alpha_d$ are the (complex) roots of the equation

$$f(t, 1) = a_0 + a_1 t + a_2 t^2 + \ldots a_d t^d = 0.$$

If $x = p$, $y = q$ is an integer solution of $f(x, y) = m$, then

$$a_d \prod_{r=1}^{d} (p - \alpha_r q) = m,$$

so that on division by q^d we get

$$\prod_{r=1}^{d} \left(\frac{p}{q} - \alpha_r\right) = \frac{m}{a_d q^d}$$

If q is very large, then since $m/(a_d q^d)$ is very small, p/q must be a very good approximation to one of the roots α_r. On the other hand, Thue managed to show that such a good approximation cannot exist[13]. Thus, the integer solutions of $f(x, y) = m$ have a bounded value of y; this easily shows that the corresponding x values are also bounded, and hence there are only a finite number of solutions. Carl Ludwig Siegel refined Thue's ideas to find necessary and sufficient conditions for an arbitrary Diophantine equation (in 2 variables, with integer coefficients)

$$f(x, y) = 0$$

to have infinitely many integer solutions. These conditions are best understood in terms of the geometry of the *algebraic curve* given by the solutions of the above equation over **C**, the complex numbers.

If $f(x, y)$ has degree d, we can uniquely decompose f as

$$f(x, y) = h\,(x, y) + k\,(x, y)$$

where h is the sum of the terms in f of degree exactly d (i.e. the terms involving $x^i y^{d-i}$ for $0 \leqslant i \leqslant d$), and k the sum of the terms of f of degree $\leqslant d-1$. Since h is homogeneous of degree d we may factorize it (as seen earlier during the discussion of Thue's work)

$$h(x, y)=a \prod_{i=1}^{d} (x-\alpha_i y)$$

for certain complex numbers $\alpha_1 \cdot \alpha_2, \ldots, \alpha_d$, and a non-zero integer a (this assumes that h has a non-zero coefficient of x^d, but this can be arranged after a homogeneous linear change of variables). Some of the α_i may be repeated; suppose there are exactly s distinct α_i. It turns out that if we let U be the subset of the complex 2-dimensional space $\mathbf{C}^2$ consisting of the complex solutions to the equation $f(x, y)=0$, then one can 'adjoin' s points to U, to get a space X which is a 'compact Riemann surface with singularities'. Intuitively, we may argue that $\mathbf{C}^2$ is 4-dimensional, while the equation $f(x, y)=0$ with complex coefficients really defines 2 equations with real coefficients; now the space of solutions of a system of 2 equations in a 4-dimensional space ought to be 2-dimensional, in general.

One can prove that, in fact, such a space X has the following description. Punch an even number of circular holes (say, $2g$) in the surface of a (two-dimensional) sphere; then attach g (hollow) cylinders to the punctured sphere, so that each boundary circle of each cylinder exactly matches the boundary of one of the holes; further, the cylinders do not intersect each other, or the sphere (except along the bounding circles). One obtains a surface without a boundary, which looks like a sphere with g hollow cylindrical 'handles', also called a *g-holed torus*. The number of handles is called the *genus* of the surface. Finally, to obtain our space X, one may have to pinch this surface in a finite number of places; these are the 'singularities' of X.

There are theorems which allow one to compute the genus g of X by simple algebraic procedures starting with the polynomial $f(x, y)$; for a 'general' polynomial f of degree d (i.e. when the space X has no singularities), one has the formula

$$g=(d-1)(d-2)/2.$$

In general, one subtracts a positive correction term which is a measure of the singularities[14].

Siegel's result states that if $g>0$, then the Diophantine equation $f(x, y)=0$ has only a finite number of integer solutions; further, even if $g=0$, only certain very special equations can have infinitely many solutions.

The problem of finding all *rational* solutions to Diophantine equations $f(x, y)=0$ is harder. It turns out that equations[15] of genus 0 and 1 may have infinitely many rational solutions. For equations of genus 0, one can decide if this is the case by simple calculations involving f, and Gauss' quadratic reciprocity law. However, it is a very difficult problem, and the subject of much contemporary research on Diophantine equations, to prove such a criterion for equations of genus 1. One knows that the solutions to an equation of genus 1 form a *group* (after we add on a finite number of 'solutions at infinity'). An important result due to Mordell is that this group is *finitely generated*.

For equations of genus $\geqslant 2$, the *Mordell Conjecture* asserts that there are only a *finite number of rational solutions*. Thus, for the Fermat equation

$$x^n+y^n=1,$$

it turns out that there are no singularities, so that the genus is

$$(n-1)(n-2)/2,$$

which is $\geqslant 2$ if $n \geqslant 4$. Thus the Mordell Conjecture implies that, for each $n \geqslant 4$, the Fermat equation has only a finite number of rational solutions.

The Mordell Conjecture was proved by the German mathematician Gerd Faltings[16] (now at Princeton University), in 1983; he was awarded the Fields Prize for this work in 1986, at the International Congress of Mathematicians held at Berkeley, California, in the USA. As the reader may know, there is no Nobel Prize in mathematics; however, there is the Fields Prize, awarded every four years to two to four mathematicians at the International Congress. One difference with the Nobel Prize is that there is an age limit: only mathematicians below forty can qualify! The Fields Prize is not nearly as large a sum of money as a Nobel Prize, but of course it carries enormous prestige in the mathematical community. Incidentally, the Swedish Academy has recently instituted a prize in mathematics, the Crafoord Prize; the first persons to whom this was awarded (in 1988) were Alexandre Grothendieck and Pierre Deligne (both Fields Prize winners). However Grothendieck turned it down![17]

Faltings' proof is quite difficult, using advanced techniques from algebraic geometry and number theory developed by many mathematicians (following ideas of Grothendieck). However, one key step in the proof is an argument reminiscent of Fermat's method of infinite descent, again involving the notion of *heights*. Fermat's Last Theorem has been verified for all values of n up to 100,000; however, Faltings' result gives the best known result valid for *all n*. Of course, Fermat's Last Theorem concerns only one equation for each degree n, while Faltings' result applies to virtually *all* equations of degree $\geqslant 4$.

Finally, we describe two recent developments relating to Fermat's Last Theorem. The first one is regarded by some number theorists as the first 'real' evidence in favour of the truth of Fermat's assertion. There is a vast program of research (it is too wide in scope to be called a mere conjecture!) proposed by the Canadian born mathematician Robert Langlands (now at the Institute for Advanced Study in Princeton). Very roughly, this seeks to tie together the representation theory of Galois groups of fields of algebraic numbers (like the field of rationals), and Fourier analysis on so called *adele groups*, built out of real Lie groups and *p-adic groups* (like GL_n $(\mathbf{Q}_p)$, the group of $n \times n$-invertible matrices of *p-adic numbers*[18]) for all primes p. Fourier analysis on such groups is an active area of current research, which is built on the tremendous work[19] of Harish-Chandra, arguably the greatest Indian mathematician after Srinivasa Ramanujan.

Class field theory (the generalization of Gauss' quadratic reciprocity found by Hilbert and others, mentioned earlier), which includes a sizeable chunk of all results in algebraic number theory until a few decades ago, is reinterpreted as the simplest case of the Langlands program. This theory also generalizes the theory of certain functions called *modular forms*, which many number theorists have been interested in during the last 100 years or so. For example, Ramanujan was interested in the function (which is a modular form)

$$\Delta(z) = q \prod_{n=1}^{\infty} (1-q^n)^{24} \text{ (where } q = \exp(2\pi i z));$$

one of his most famous conjectures[20] about the Fourier coefficients $\tau(n)$ of the function $\Delta(z)$ (which was proved by Deligne in 1973) has been vastly generalized by Langlands. There is a lot of recent research giving impressive evidence in support of the Langlands program[21].

One consequence of the theory is a certain property of equations of genus 1 with rational coefficients, which goes under the name of the *Taniyama–Weil Conjecture* (after the mathematicians Taniyama and Weil). Recently, it has been observed by several mathematicians that this conjecture implies Fermat's Last Theorem. The idea is as follows—if a, b, c are integers satisfying $a^n + b^n = c^n$, one considers the cubic equation

$$y^2 = (x-a^n)(x-b^n)(x-c^n).$$

Then one is able to show that this cubic has genus 1, and would contradict the Taniyama–Weil Conjecture. Since Taniyama and Weil are backed up by Langlands, it seems unimaginable (to some) that Fermat's Last Theorem could be false! The auxilliary cubic obtained from a possible counterexample to the Fermat problem is called the Frey curve, after the mathematician Frey who first had the idea of studying this curve.

A variant of this method, again by considering the Frey curve, is to try to obtain a contradiction using another new topic in geometrical number theory, called *Arakelov theory*. This theory originates in a paper of the Soviet mathematician Arakelov[22]. Roughly speaking, Arakelov exploits an analogy between the geometry of surfaces and the theory of solutions of Diophantine equations $f(x, y) = 0$. A forerunner was the work of Weil[23], formulating such an analogy between the theory of algebraic curves, and the study of solutions of equations $f(x) = 0$ in one variable, i.e. of the rings of algebraic numbers we mentioned earlier.

There was much excitement in the mathematical community when in 1988, a Japanese mathematician announced that he could extend to the 'Arakelov situation' a geometrical theorem about algebraic surfaces which he had proved a few years earlier, and that this yields Fermat's Last Theorem. Unfortunately the proof was incorrect. However, these methods could still potentially lead to a proof.

Rational solutions of equations in 2 variables are related to integer solutions of equations in 3 variables (as in Fermat's Last Theorem). What about integer solutions of equations in $\geqslant 4$ variables? In his famous address to the International Congress of Mathematicians in 1900 in Paris, Hilbert listed 23 outstanding problems in different branches of mathematics, as a challenge to future mathematicians[24]. *Hilbert's 10th problem* asks for an algorithm (or systematic 'mechanical' procedure) for deciding if a given Diophantine equation has a positive integer solution. Using methods of mathematical logic (related to Gödel's famous *incompleteness theorems*, and to certain techniques in modern theoretical computer science), the Soviet mathematician Matijasevic, building on work of Martin Davis, Julia Robinson and Hilary Putnam, showed that there is *no such procedure*[25]. Refinements of the proof show that such a decision procedure is impossible for equations in 4 variables! Among the other striking consequences of this work, Matijasevič constructs an explicit polynomial f in 26 variables (named $a, b, \ldots, z$, of course!) such that for *any* positive integer solution of

$$f(a, b, \ldots, z) = 0,$$

a is a *prime number*, and *every prime number occurs in this way*!

[1] See Hardy, G. H. and Wright, E. M., *An Introduction to the Theory of Numbers*, 4th edn, Oxford, 1960; and Weil, A., *Number Theory: An Approach Through History, 'from Hammurapi to Legendre'*, Birkhäuser Boston, 1983, for historical background and further references.

[2] See Weil, A., *loc. cit.*, Chapter 1.

[3] See Edwards, H. M., *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Grad. Texts in Math., No. 50, Springer-Verlag, New York, 1977.

[4] Bell, E. T., *Men of Mathematics*, Simon and Schuster, New York, 1965.

[5] Weil, A., *loc. cit.*

[6] Edwards, H. E., *loc. cit.*

[7] Jungk, R., *Brighter than a Thousand Suns*, Penguin Books Ltd. 1964.

[8] Use the substitution $w = z^2$.

[9] Weil (*loc. cit.*) states that the majority of Fermat's work on Diophantine equations was concerned with the systematic study of equations of genus 0 and 1 (see Notes 14, 15 for genus). Thus Fermat initiated the 'theory' of these equations.

[10] See Hardy, G. H. and Wright, E. M., *loc. cit.*, Section 15.5.

11. It is known that 2^{11213}—1 is a prime; granting this, the verification of this statement using quadratic reciprocity took the author less than 10 minutes of computation, without a calculator; essentially, one must compute the remainder obtained on dividing 2^{11213}—1 by 163, the discriminant in this case.
12. For the algebraic number theory needed to perform the above calculations, see any one of the following books: Borevich, Z. I. and Shafarevich, I. R., *Number Theory, Pure and Applied Mathematics*, Vol. 20, Academic Press, New York, 1966; Marcus, J. A., *Number Fields*, Universitext, Springer-Verlag, New York, 1977; Serre, J. -P., *A Course in Arithmetic*, Grad. Texts in Math., No. 7, Springer-Verlag, New York, 1978 (also available in International Student Edition, Narosa, New Delhi, 1979); Marcus' book also contains an introduction to class field theory.
13. Thue showed that if α is a root of $f(t, 1) = 0$, and C is any positive constant, then there is an explicit positive number $C_1(\alpha, C)$ such that there is *at most one* solution of

$$\left|\alpha - = \frac{p}{q}\right| < \frac{C}{q^d},$$

with max $(|p|, |q|) > C_1$; hence this inequality has only a finite number of solutions. But one is unable to decide if this exceptional approximation exists, so one cannot *explicitly* bound all the solutions of the Diophantine equation, using Thue's method. Thus, one is unable to run a computer program to test all integers p, q with $|p|$, $|q| < D$ for an explicit constant D, computable directly from the equation, to get a complete list of solutions of our Diophantine equation. But one could (in principle) do this to obtain a list of solutions, such that at most d solutions are missing (one for each root α_r). This state of affairs is expressed by saying that Thue's method is not *effective*.

An effective decision procedure for finding solutions of certain Diophantine equations (including the Thue equation, but not the more general equations considered by Siegel) has been found by Baker and others; see Baker, A., *'Transcendental Number Theory'*, Cambridge Univ. Press, Cambridge, 1975.

14. See Hartshorne, R., *Algebraic Geometry*, Grad. Texts in Math. No. 52, Springer-Verlag, New York, 1977, for results on algebraic curves, genus, etc.
15. We refer to the genus of the underlying Riemann surface of complex solutions as the genus of the equation. Equations of genus 1 describe *elliptic curves*; see Silverman, J. H., *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. No. 106, Springer-Verlag, New York, 1986, for an introduction, and a survey of current research on Diophantine properties of elliptic curves.
16. Faltings, G., *Invent. Math.*, 1983, **73**, 349; see also Cornell, G. and Silverman, J. H. (eds), *Arithmetic Geometry*, Springer-Verlag, New York, 1986, which contains a translation of Faltings article into English, background for that article, as well as other related material.
17. A translation of Grothendieck's letter to the Swedish Academy, explaining the reasons for his refusal, can be found in the *Mathematical Intelligencer*, 1988.
18. See Varadarajan, V. S. (ed), *Harish-Chandra, Collècted Papers*, Springer-Verlag, New York, 1983 (an Indian edition is published by Narosa, N. Delhi, 1985. Harish-Chandra was Langland's colleague at the Institute for Advanced Study in Princeton, until his death in 1983; Langlands has written an obituary for Harish-Chandra, which makes fascinating reading—see Langlands, R. P., 'Harish-Chandra', *Biog. Mem. Fellows of Royal Soc.*, 1985, **31**, 199.
19. See any of the books mentioned in Note 12 for the definition and many properties of p-adic numbers.
20. Ramanujan, S., *Trans. Cambridge Philos. Soc.*, 1916, **22**, 159. (see Hardy, G. H., Seshu Iyer, G. and Watson, G. M. (ed), *Collected Papers of Srinivasu Ramanujan*, Cambridge Univ. Press, Cambridge, 1927). Ramanujan's conjecture is that for any $\varepsilon > 0$, there is a positive constant C such that $|\tau(n)| < Cn^{11/2+\varepsilon}$. The mysterious exponent 11/2 is related to the *weight* of $\Delta(z)$, and to Weil's Riemann Hypothesis for algebraic varieties over finite fields, proved by Deligne. See Browder, F. E., (cd.) Note 24 for an exposition of Deligne's proof.
21. See Gelbart, S., *Bull. Am. Math. Soc.* (*New Ser.*), 1984, **10**, for an introduction to the Langlands program.
22. See C. Soulè, 'Gèomètrie d'Arakelov des surfaces arithmètiques', *Sèminaire Bourbaki*, No. 713, June, 1989, (to appear in *Astèrique*, *Soc. Math. France*), for an introduction.
23. This analogy is brought out in the book, Weil, A., *Basic Number Theory*, Springer-Verlag, New York, 1968.
24. See Browder, F. E. (ed.), *Mathematical Developments arising from the Hilbert Problems*. Proc. Symp. Pure Math. No. 28, Am. Math. Soc., Providence, 1976.
25. See Yu. Matijasevič, *Russian Math. Surveys*, vol. 27, No. 5, 1972, for a self-contained account of this work.

ACKNOWLEDGEMENTS. This article was written at the urging of M. S. Raghunathan; I also thank him for his numerous suggestions and for providing me with some interesting references. I also thank Kirti Joshi, Dipendra Prasad, T. N. Shorey, B. Sury and T. N. Venkataramana for helpful comments.