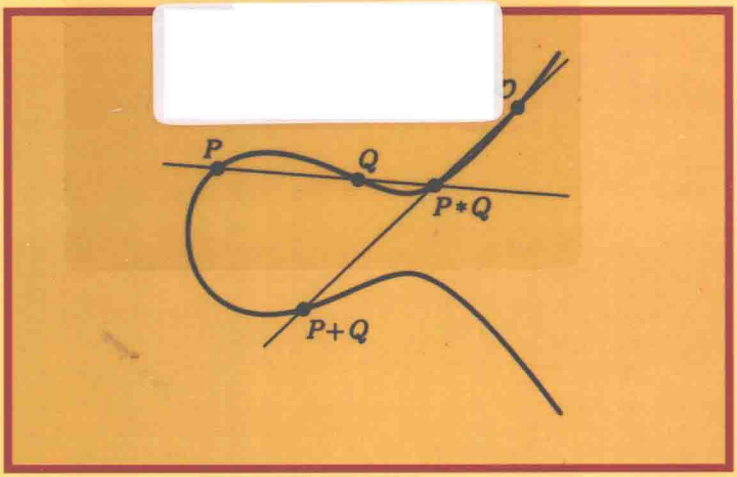
Undergraduate Texts in Mathematics

Joseph H. Silverman
John Tate

Rational Points on Elliptic Curves

椭圆曲线上的有理点



Springer

世界图书出版公司
www.wpcbj.com.cn

Joseph H. Silverman John Tate

Rational Points on Elliptic Curves

With 34 Illustrations

Springer

图书在版编目（CIP）数据

椭圆曲线上的有理点 = Rational points on elliptic curves：英文/（美）西尔弗曼（Silverman，J. H.）著. —影印本. —北京：世界图书出版公司北京公司，2014. 9

ISBN 978-7-5100-8632-8

Ⅰ. ①椭… Ⅱ. ①西… Ⅲ. ①椭圆曲线—英文 Ⅳ. ① O187. 1

中国版本图书馆 CIP 数据核字（2014）第 211035 号

书　　名：	Rational Points on Elliptic Curves
作　　者：	Joseph H. Silverman，John Tate
中 译 名：	椭圆曲线上的有理点
责任编辑：	高蓉　刘慧
出 版 者：	世界图书出版公司北京公司
印 刷 者：	三河市国英印务有限公司
发　　行：	世界图书出版公司北京公司（北京朝内大街 137 号 100010）
联系电话：	010-64021602，010-64015659
电子信箱：	kjb@ wpcbj. com. cn
开　　本：	24 开
印　　张：	12. 5
版　　次：	2015 年 1 月
版权登记：	图字：01-2013-9347
书　　号：	978-7-5100-8632-8　　**定　　价：** 59. 00 元

Preface

In 1961 the second author delivered a series of lectures at Haverford College on the subject of "Rational Points on Cubic Curves." These lectures, intended for junior and senior mathematics majors, were recorded, transcribed, and printed in mimeograph form. Since that time they have been widely distributed as photocopies of ever decreasing legibility, and portions have appeared in various textbooks (Husemöller [1], Chahal [1]), but they have never appeared in their entirety. In view of the recent interest in the theory of elliptic curves for subjects ranging from cryptography (Lenstra [1], Koblitz [2]) to physics (Luck-Moussa-Waldschmidt [1]), as well as the tremendous purely mathematical activity in this area, it seems a propitious time to publish an expanded version of those original notes suitable for presentation to an advanced undergraduate audience.

We have attempted to maintain much of the informality of the original Haverford lectures. Our main goal in doing this has been to write a textbook in a technically difficult field which is "readable" by the average undergraduate mathematics major. We hope we have succeeded in this goal. The most obvious drawback to such an approach is that we have not been entirely rigorous in all of our proofs. In particular, much of the foundational material on elliptic curves presented in Chapter I is meant to explain and convince, rather than to rigorously prove. Of course, the necessary algebraic geometry can mostly be developed in one moderately long chapter, as we have done in Appendix A. But the emphasis of this book is on the number theoretic aspects of elliptic curves; and we feel that an informal approach to the underlying geometry is permissible, because it allows us more rapid access to the number theory. For those who wish to delve more deeply into the geometry, there are several good books on the theory of algebraic curves suitable for an undergraduate course, such as Reid [1], Walker [1] and Brieskorn-Knörrer [1]. In the later chapters we have generally provided all of the details for the proofs of the main theorems.

The original Haverford lectures make up Chapters I, II, III, and the first two sections of Chapter IV. In a few places we have added a small amount of explanatory material, references have been updated to include some discoveries made since 1961, and a large number of exercises have

been added. But those who have seen the original mimeographed notes will recognize that the changes have been kept to a minimum. In particular, the emphasis is still on proving (special cases of) the fundamental theorems in the subject: (1) the Nagell-Lutz theorem, which gives a precise procedure for finding all of the rational points of finite order on an elliptic curve; (2) Mordell's theorem, which says that the group of rational points on an elliptic curve is finitely generated; (3) a special case of Hasse's theorem, due to Gauss, which describes the number of points on an elliptic curve defined over a finite field.

In the last section of Chapter IV we have described Lenstra's elliptic curve algorithm for factoring large integers. This is one of the recent applications of elliptic curves to the "real world," to wit the attempt to break certain widely used public key ciphers. We have restricted ourselves to describing the factorization algorithm itself, since there have been many popular descriptions of the corresponding ciphers. (See, for example, Koblitz [2].)

Chapters V and VI are new. Chapter V deals with integer points on elliptic curves. Section 2 of Chapter V is loosely based on an IAP undergraduate lecture given by the first author at MIT in 1983. The remaining sections of Chapter V contain a proof of a special case of Siegel's theorem, which asserts that an elliptic curve has only finitely many integral points. The proof, based on Thue's method of Diophantine approximation, is elementary, but intricate. However, in view of Vojta's [1] and Faltings' [1] recent spectacular applications of Diophantine approximation techniques, it seems appropriate to introduce this subject at an undergraduate level. Chapter VI gives an introduction to the theory of complex multiplication. Elliptic curves with complex multiplication arise in many different contexts in number theory and in other areas of mathematics. The goal of Chapter VI is to explain how points of finite order on elliptic curves with complex multiplication can be used to generate extension fields with abelian Galois groups, much as roots of unity generate abelian extensions of the rational numbers. For Chapter VI only, we have assumed that the reader is familiar with the rudiments of field theory and Galois theory.

Finally, we have included an appendix giving an introduction to projective geometry, with an especial emphasis on curves in the projective plane. The first three sections of Appendix A provide the background needed for reading the rest of the book. In Section 4 of Appendix A we give an elementary proof of Bezout's theorem, and in Section 5 we provide a rigorous discussion of the reduction modulo p map and explain why it induces a homomorphism on the rational points of an elliptic curve.

The contents of this book should form a leisurely semester course, with some time left over for additional topics in either algebraic geometry or number theory. The first author has also used this material as a supplementary special topic at the end of an undergraduate course in modern algebra, covering Chapters I, II, and IV (excluding IV §3) in about four weeks of classes. We note that the last five chapters are essentially

independent of one another (except IV §3 depends on the Nagell-Lutz theorem, proven in Chapter II). This gives the instructor maximum freedom in choosing topics if time is short. It also allows students to read portions of the book on their own (e.g., as a suitable project for a reading course or an honors thesis.) We have included many exercises, ranging from easy calculations to published theorems. An exercise marked with a (*) is likely to be somewhat challenging. An exercise marked with (**) is either extremely difficult to solve with the material we cover or actually a currently unsolved problem.

It has been said that "it is possible to write endlessly on elliptic curves."† We heartily agree with this sentiment, but have attempted to resist succumbing to its blandishments. This is especially evident in our frequent decision to prove special cases of general theorems, even when only a few more pages would be required to prove a more general result. Our goal throughout has been to illuminate the coherence and the beauty of the arithmetic theory of elliptic curves; we happily leave the task of being encyclopedic to the authors of more advanced monographs.

Computer Packages

The first author has written two computer packages to perform basic computations on elliptic curves. The first is a stand-alone application which runs on any variety of Macintosh. The second is a collection of *Mathematica* routines with extensive documentation included in the form of Notebooks in Macintosh *Mathematica* format. Instructors are welcome to freely copy and distribute both of these programs. They may be obtained via anonymous ftp at

gauss.math.brown.edu (128.148.194.40)

in the directory dist/EllipticCurve.

Acknowledgments

The authors would like to thank Rob Gross, Emma Previato, Michael Rosen, Seth Padowitz, Chris Towse, Paul van Mulbregt, Eileen O'Sullivan, and the students of Math 153 (especially Jeff Achter and Jeff Humphrey) for reading and providing corrections to the original draft. They would also like to thank Davide Cervone for producing beautiful illustrations from their original jagged diagrams.

† From the introduction to *Elliptic Curves: Diophantine Analysis*, Serge Lang, Springer-Verlag, New York, 1978. Professor Lang follows his assertion with the statement that "This is not a threat," indicating that he, too, has avoided the temptation to write a book of indefinite length.

The first author owes a tremendous debt of gratitude to Susan for her patience and understanding, to Debby for her fluorescent attire brightening up the days, to Danny for his unfailing good humor, and to Jonathan for taking timely naps during critical stages in the preparation of this manuscript.

The second author would like to thank Louis Solomon for the invitation to deliver the Philips Lectures at Haverford College in the Spring of 1961.

Joseph H. Silverman
John Tate

March 27, 1992

Acknowledgments for the Second Printing

The authors would like to thank the following people for sending us suggestions and corrections, many of which have been incorporated into this second printing: G. Allison, D. Appleby, K. Bender, G. Bender, P. Berman, J. Blumenstein, D. Freeman, L. Goldberg, A. Guth, A. Granville, J. Kraft, M. Mossinghoff, R. Pries, K. Ribet, H. Rose, J.-P. Serre, M. Szydlo, J. Tobey, C.R. Videla, J. Wendel.

Joseph H. Silverman
John Tate

June 13, 1994

Contents

Introduction

The theory of Diophantine equations is that branch of number theory which deals with the solution of polynomial equations in either integers or rational numbers. The subject itself is named after one of the greatest of the ancient Greek algebraists, Diophantus of Alexandria,[1] who formulated and solved many such problems.

Most readers will undoubtedly be familiar with Fermat's Last Theorem.[2] This theorem says that if $n \geq 3$ is an integer, then the equation

$$X^n + Y^n = Z^n$$

has no solutions in non-zero integers X, Y, Z. Equivalently, the only solutions in rational numbers to the equation

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

are those with either $x = 0$ or $y = 0$. Fermat's Theorem is now known to be true for all exponents $n \leq 125000$, so it is unlikely that anyone will find a counterexample by random guessing. On the other hand, there are still a lot of possible exponents left to check between 125000 and infinity!

As another example, we consider the problem of writing an integer as the difference of a square and a cube. In other words, we fix an integer $c \in \mathbb{Z}$ and look for solutions to the Diophantine equation[3]

$$y^2 - x^3 = c.$$

---

[1] Diophantus lived sometime before the 3$^{\text{rd}}$ century A.D. He wrote the *Arithmetica*, a treatise on algebra and number theory in 13 volumes, of which 6 volumes have survived.

[2] Fermat's Last "Theorem" is really a conjecture, because it is still unsolved after more than 350 years. Fermat stated his "Theorem" as a marginal note in his copy of Diophantus' *Arithmetica*; unfortunately, the margin was too small for him to write down his proof!

[3] This equation is often called Bachet's equation, after the 17$^{\text{th}}$ century mathematician who originally discovered the duplication formula. It is also sometimes called Mordell's equation, in honor of the 20$^{\text{th}}$ century mathematician L.J. Mordell, who made a fundamental contribution to the solution of this and many similar Diophantine equations. We will be proving a special case of Mordell's theorem in Chapter III.

Suppose we are interested in solutions in rational numbers $x, y \in \mathbb{Q}$. An amazing property of this equation is the existence of a *duplication formula*, discovered by Bachet in 1621. If (x, y) is a solution with x and y rational, then it is easy to check that

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3}\right)$$

is a solution in rational numbers to the same equation. Further, it is possible to prove (although Bachet was not able to) that if the original solution has $xy \neq 0$ and if $c \neq 1, -432$, then repeating this process leads to infinitely many distinct solutions. So if an integer can be expressed as the difference of a square and a cube of non-zero rational numbers, then it can be so expressed in infinitely many ways. For example, if we start with the solution $(3, 5)$ to the equation

$$y^2 - x^3 = -2$$

and apply Bachet's duplication formula, we find a sequence of solutions that starts

$$(3, 5), \quad \left(\frac{129}{10^2}, \frac{-383}{10^3}\right), \quad \left(\frac{2340922881}{7660^2}, \frac{113259286337292}{7660^3}\right), \ldots .$$

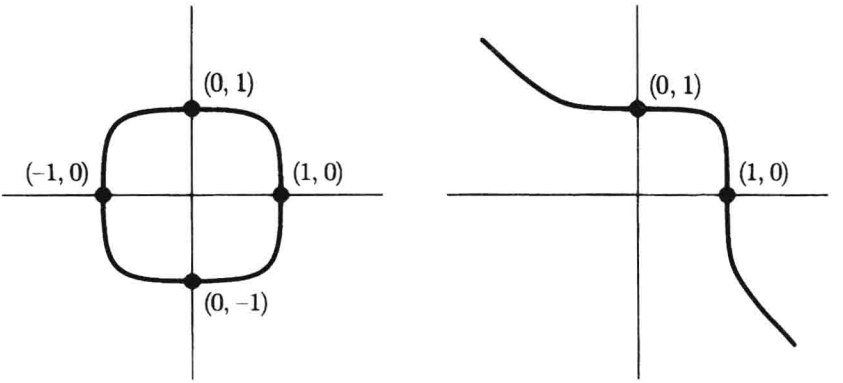
As you can see, the numbers rapidly get extremely large.

Next we'll take the same equation

$$y^2 - x^3 = c$$

and ask for solutions in integers $x, y \in \mathbb{Z}$. In the 1650's Fermat posed as a challenge to the English mathematical community the problem of showing that the equation $y^2 - x^3 = -2$ has only two solutions in integers, namely $(3, \pm 5)$. This is in marked contrast to the question of solutions in rational numbers, since we have just seen there are infinitely many of those. None of Fermat's contemporaries appears to have solved the problem, which was solved incorrectly by Euler in the 1730's, and given a correct proof 150 years later! Then in 1908, Axel Thue[4] made a tremendous breakthrough; he showed that for any non-zero integer c, the equation $y^2 - x^3 = c$ can have only a finite number of solutions in integers x, y. This is a tremendous (qualitative) generalization of Fermat's challenge problem; among the infinitely many solutions in rational numbers, there can be but finitely many integer solutions.

[4] Axel Thue made important contributions to the theory of Diophantine equations, especially to the problem of showing that certain equations have only finitely many solutions in integers. These theorems about integer solutions were generalized by C.L. Siegel during the 1920's and 1930's. We will prove a version of the Thue-Siegel theorem (actually a special case of Thue's original result) in Chapter V.



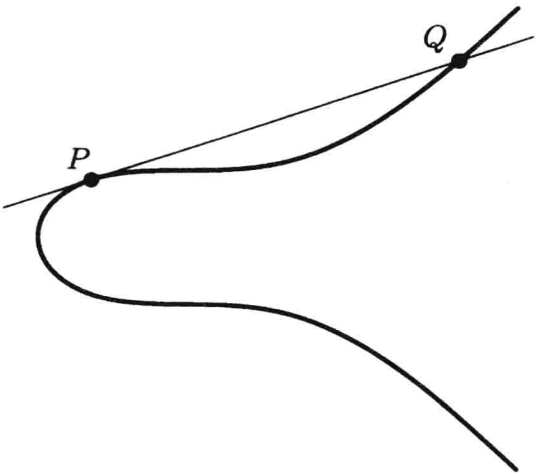
The Fermat Curves $x^4 + y^4 = 1$ and $x^5 + y^5 = 1$

Figure 0.1

The 17^{th} century witnessed Descartes' introduction of coordinates into geometry, a revolutionary development which allowed geometric problems to be solved algebraically and algebraic problems to be studied geometrically. For example, if n is even, then the real solutions to Fermat's equation $x^n + y^n = 1$ in the xy plane form a geometric object that looks like a squashed circle. Fermat's Theorem is then equivalent to the assertion that the only points on that squashed circle having rational coordinates are the four points $(\pm 1, 0)$ and $(0, \pm 1)$. The Fermat equations with odd exponents look a bit different. We have illustrated the Fermat curves with exponents 4 and 5 in Figure 0.1.

Similarly, we can look at Bachet's equation $y^2 - x^3 = c$, which we have graphed in Figure 0.2. Recall that Bachet discovered a duplication formula which allows us to take a given rational solution and produce a new rational solution. Bachet's formula is rather complicated, and one might wonder where it comes from. The answer is, it comes from geometry! Thus, suppose we let $P = (x, y)$ be our original solution, so P is a point on the curve (as illustrated in Figure 0.2). Next we draw the tangent line to the curve at the point P, an easy exercise suitable for a first semester calculus course.[5] This tangent line will intersect the curve at one further point, which we have labeled Q. Then, if you work out the algebra to calculate the coordinates of Q, you will find Bachet's duplication formula. So Bachet's complicated algebraic formula has a simple geometric interpretation in terms of the intersection of a tangent line with a curve. This is our first intimation of the fruitful interplay that is possible among algebra, number theory, and geometry.

[5] Of course, Bachet had neither calculus nor analytic geometry; so he probably discovered his formula by clever algebraic manipulation.



Bachet's Equation $y^2 - x^3 = c$

Figure 0.2

The simplest sort of Diophantine equation is a polynomial equation in one variable:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

Assuming that $a_0, \ldots, a_n$ are integers, how can we find all integer and all rational solutions? Gauss' lemma provides the simple answer. If p/q is a rational solution written in lowest terms, then Gauss' lemma tells us that q divides a_n and p divides a_0. This gives us a small list of possible rational solutions, and we can substitute each of them into the equation to determine the actual solutions. So Diophantine equations in one variable are easy.

When we move to Diophantine equations in two variables, the situation changes dramatically. Suppose we take a polynomial $f(x, y)$ with integer coefficients and look at the equation

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

For example, Fermat's and Bachet's equations are equations of this sort. Here are some natural questions we might ask:

(a) Are there any solutions in integers?
(b) Are there any solutions in rational numbers?
(c) Are there infinitely many solutions in integers?
(d) Are there infinitely many solutions in rational numbers?

In this generality, only question (c) has been fully answered, although much progress has recently been made on (d).[6]

[6] For polynomials $f(x_1, \ldots, x_n)$ with more than two variables, our four questions have only

The set of real solutions to an equation $f(x, y) = 0$ forms a curve in the xy plane. Such curves are often called *algebraic curves* to indicate that they are the solutions of a polynomial equation. In trying to answer questions (a)–(d), we might begin by looking at simple polynomials, such as polynomials of degree 1 (also called linear polynomials, because their graphs are straight lines.) For a linear equation

$$ax + by = c$$

with integer coefficients, it is easy to answer our questions. There are always infinitely many rational solutions, there are no integer solutions if $\gcd(a, b)$ does not divide c, and otherwise there are infinitely many integer solutions. So linear equations are even easier than equations in one variable.

Next we might turn to polynomials of degree 2 (also called quadratic polynomials). Their graphs are conic sections. It turns out that if such an equation has one rational solution, then there are infinitely many. The complete set of solutions can be described very easily using geometry. We will explain how this is done in the first section of Chapter I. We will also briefly indicate how to answer question (b) for quadratic polynomials. So although it would be untrue to say that quadratic polynomials are easy, it is fair to say that their solutions are completely understood.

This brings us to the main topic of this book, namely, the solution of degree 3 polynomial equations in rational numbers and in integers. One example of such an equation is Bachet's equation $y^2 - x^3 = c$ which we looked at earlier; some other examples which will appear during our studies are

$$y^2 = x^3 + ax^2 + bx + c \qquad \text{and} \qquad ax^3 + by^3 = c.$$

The real solutions to these equations are called *cubic curves* or *elliptic curves*. (However, they are not ellipses, since ellipses are conic sections, and conic sections are given by quadratic equations! The curious chain of events that led to elliptic curves being so named will be recounted in Chapter I, Section 3.) In contrast to linear and quadratic equations, the rational and integer solutions to cubic equations are still not completely understood; and even in those cases where the complete answers are known, the proofs involve a subtle blend of techniques from algebra, number theory, and geometry. Our main goal in this book is to introduce you to the beautiful subject of Diophantine equations by studying in depth the first case of such equations which are still imperfectly understood, namely cubic equations in two variables. To give you an idea of the sorts of results we will be studying, we briefly indicate what is known about questions (a)–(d).

---

been answered for some very special sorts of equations. Even worse, work of Davis, Matijasevič, and Robinson has shown that in general it is not possible to find a solution to question (a). That is, there does not exist an algorithm which takes as input the polynomial f and produces as output either "YES" or "NO" as an answer to question (a).

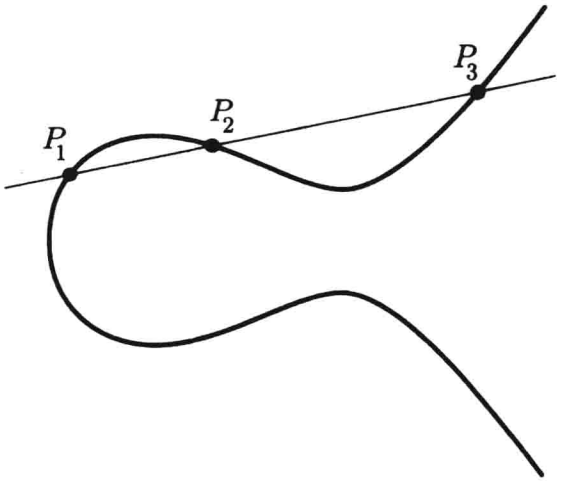
First, a cubic equation has only finitely many integer solutions[7] (Siegel, 1920's); and there is an explicit upper bound for the largest solution in terms of the coefficients of the polynomial (Baker-Coates, 1970). This provides a satisfactory answer to (a) and (c), although the actual bounds for the largest solution are generally too large to be practical. We will prove a special case of Siegel's theorem (for equations of the form $ax^3 + by^3 = c$) in Chapter V.

Second, all of the (possibly infinitely many) rational solutions to a cubic equation may be found by starting with a finite set of solutions and repeatedly applying a geometric procedure similar to Bachet's duplication formula. The fact that there exists such a finite generating set was suggested by Poincaré in 1901 and proven by L.J. Mordell in 1923. We will prove (a special case of) Mordell's theorem in Chapter III. However, we must in truth point out that Mordell's theorem does not really answer questions (b) and (d). As we will see, the proof of Mordell's theorem gives a procedure which *often* allows one to find a finite generating set for the set of rational solutions. But it is only conjectured, and not yet proven, that Mordell's method always yields a generating set. So even for special sorts of cubic equations, such as $y^2 - x^3 = c$ and $ax^3 + by^3 = c$, there is no general method (i.e., algorithm) currently known which is guaranteed to answer question (b) or (d).

We have mentioned several times the idea that the study of Diophantine equations involves an interplay among algebra, number theory, and geometry. The geometric component is clear, because the equation itself defines (in the case of two variables) a curve in the plane; and we have already seen how it may be useful to consider the intersection of that curve with various lines. The number theory is also clearly present, because we are searching for solutions in either integers or rational numbers, and what else is number theory other than a study of the relations between integers and/or rational numbers. But what of the algebra? We could point out that polynomials are essentially algebraic objects. However, algebra plays a much more important role than this.

Recall that Bachet's duplication formula can be described as follows: start with a point P on a cubic curve, draw the tangent line at P, and take the third point of intersection of the line with the curve. Similarly, if we start with two points P_1 and P_2 on the curve, we can draw the line through P_1 and P_2 and look at the third intersection point P_3. (This will work for most points, because the intersection of a line and a cubic curve will usually consist of exactly three points.) We might describe this procedure, which we illustrate in Figure 0.3, as a way to "add" two points on the curve and get a third point on the curve. Amazingly enough, we will show that with a slight modification this geometric operation takes the set of rational

[7] Actually, Siegel's theorem applies only to "non-singular" cubic equations. However, most cubic equations are non-singular; and in practice it is quite easy to check whether or not a given equation is non-singular.



"Adding" Two Points on a Cubic Curve

Figure 0.3

solutions to a cubic equation and turns it into an abelian group! And Mordell's theorem alluded to earlier can be rephrased by saying that this group has a finite number of generators. So here is algebra, number theory, and geometry all packaged together in one of the greatest theorems of this century.

We hope that the foregoing introduction has convinced you of some of the beauty and elegance to be found in the theory of Diophantine equations. But the study of Diophantine equations, in particular the theory of elliptic curves, also has its practical applications. We will study one such application in this book. Everyone is familiar with the Fundamental Theorem of Arithmetic, which asserts that every positive integer factors uniquely into a product of primes. It is less well known that if the integer is fairly large, say on the order of 10^{100} or 10^{200}, it may be virtually impossible to perform that factorization. This is true even though there are very quick ways to check that an integer of this size is not itself a prime. In other words, if one is presented with an integer N with (say) 150 digits, then one can easily check that N is not prime, even though one cannot in general find any of the prime factors of N.

This curious state of affairs has been used by Rivest, Shamir, and Adleman to construct what is known as a public key cipher based on a trapdoor function. These are ciphers in which one can publish, for all to see, the method of enciphering a message; but even with the encipherment method on hand, a would-be spy will not be able to decipher any messages. Needless to say, such ciphers have numerous applications, ranging from espionage to ensuring secure telecommunications between banks and other

financial institutions. To describe the relation with elliptic curves, we will need to briefly indicate how such a "trapdoor cipher" works.

First one chooses two large primes, say p and q, each with around 100 digits. Next one publishes the product $N = pq$. In order to encipher a message, your correspondent only needs to know the value of N. But in order to decipher a message, the factors p and q are needed. So your messages will be safe as long as no one is able to factor N. This means that in order to ensure the safety of your messages, you need to know the largest integers that your enemies are able to factor in a reasonable amount of time.

So how does one factor a large number which is known to be composite? One can start trying possible divisors 2, 3,..., but this is hopelessly inefficient. Using techniques from number theory, various algorithms have been devised, with exotic sounding names like the continued fraction method, the ideal class group method, the $p - 1$ method, and the quadratic sieve method. But one of the best methods currently available is Lenstra's Elliptic Curve Algorithm, which as the name indicates relies on the theory of elliptic curves. So it is essential to understand the strength of Lenstra's algorithm if one is to ensure that one's public key cipher will not be broken. We will describe how Lenstra's algorithm works in Chapter IV.