Graduate Texts in Mathematics

Neal Koblitz

Introduction to Elliptic Curves and Modular Forms

Second Edition

椭圆曲线和模型式引论

第2版

Springer-Verlag

世界图书出版公司

Neal Koblitz

Introduction to Elliptic Curves and Modular Forms

Second Edition

With 24 Illustrations

Springer

书　　名：Introduction to Elliptic Curves and Modular Forms 2nd ed.
作　　者：N. Koblitz
中 译 名：椭圆曲线和模形式引论　第 2 版
出 版 者：世界图书出版公司北京公司
印 刷 者：北京世图印刷厂
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：010-64015659, 64038347
电子信箱：kjsk@vip.sina.com
开　　本：24　　印　张：11
出版年代：2003 年 6 月
书　　号：7-5062-6014-X/ O・403
版权登记：图字: 01-2003-3601
定　　价：27.00 元

Neal Koblitz
Department of Mathematics
University of Washington
Seattle, WA 98195
USA

Mathematics Subject Classification (2000): 11-01, 11Dxx, 11Gxx, 11Rxx, 14H45

Library of Congress Cataloging-in-Publication Data
Koblitz, Neal.
Introduction to elliptic curves and modular forms / Neal Koblitz.
— 2nd ed.
p. cm. — (Graduate texts in mathematics; 97)
ISBN 0-387-97966-2
1. Curves, Elliptic. 2. Forms, Modular. 3. Number Theory.
I. Title. II. Series.
QA567.2E44K63 1993
516.3'52—dc20 92-41778

Printed on acid-free paper.

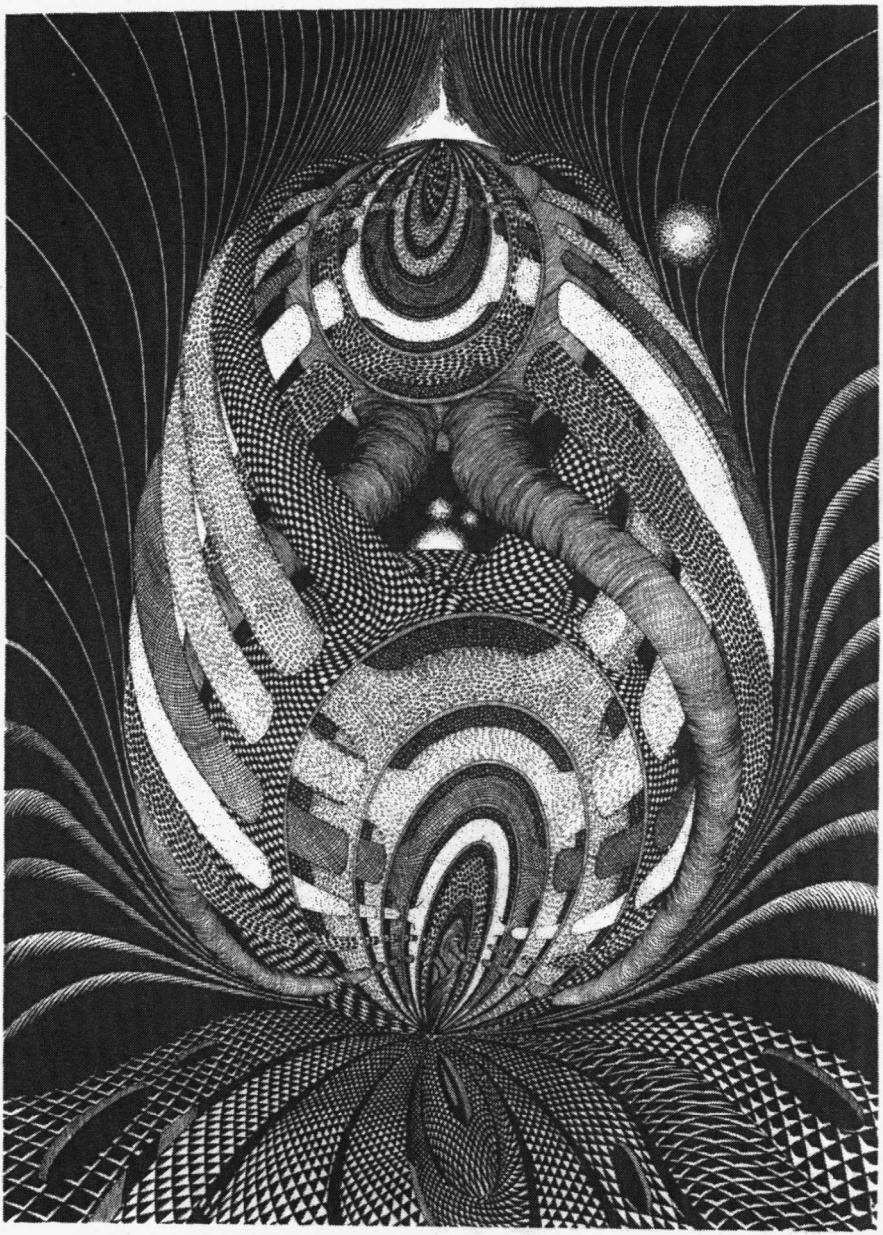
9 8 7 6 5 4

ISBN 0-387-97966-2
ISBN 3-540-97966-2 SPIN 10838196

Springer-Verlag New York Berlin Heidelberg
A member of BertelsmannSpringer Science+Business Media GmbH

Graduate Texts in Mathematics 97

Springer
New York
Berlin
Heidelberg
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo



Preface to the First Edition

This textbook covers the basic properties of elliptic curves and modular forms, with emphasis on certain connections with number theory. The ancient "congruent number problem" is the central motivating example for most of the book.

My purpose is to make the subject accessible to those who find it hard to read more advanced or more algebraically oriented treatments. At the same time I want to introduce topics which are at the forefront of current research. Down-to-earth examples are given in the text and exercises, with the aim of making the material readable and interesting to mathematicians in fields far removed from the subject of the book.

With numerous exercises (and answers) included, the textbook is also intended for graduate students who have completed the standard first-year courses in real and complex analysis and algebra. Such students would learn applications of techniques from those courses, thereby solidifying their understanding of some basic tools used throughout mathematics. Graduate students wanting to work in number theory or algebraic geometry would get a motivational, example-oriented introduction. In addition, advanced undergraduates could use the book for independent study projects, senior theses, and seminar work.

This book grew out of lecture notes for a course I gave at the University of Washington in 1981–1982, and from a series of lectures at the Hanoi Mathematical Institute in April, 1983. I would like to thank the auditors of both courses for their interest and suggestions. My special gratitude is due to Gary Nelson for his thorough reading of the manuscript and his detailed comments and corrections. I would also like to thank Professors J. Buhler, B. Mazur, B. H. Gross, and Huynh Mui for their interest, advice and encouragement.

The frontispiece was drawn by Professor A. T. Fomenko of Moscow State University to illustrate the theme of this book. It depicts the family of elliptic curves (tori) that arises in the congruent number problem. The elliptic curve corresponding to a natural number n has branch points at $0, \infty, n$ and $-n$. In the drawing we see how the elliptic curves interlock and deform as the branch points $\pm n$ go to infinity.

Note: References are given in the form [Author year]; in case of multiple works by the same author in the same year, we use a, b, ... after the date t indicate the order in which they are listed in the Bibliography.

Seattle, Washington NEAL KOBLITZ

Preface to the Second Edition

The decade since the appearance of the first edition has seen some major progress in the resolution of outstanding theoretical questions concerning elliptic curves. The most dramatic of these developments have been in the direction of proving the Birch and Swinnerton-Dyer conjecture. Thus, one of the changes in the second edition is to update the bibliography and the discussions of the current state of knowledge of elliptic curves.

It was also during the 1980s that, for the first time, several important practical applications were found for elliptic curves. In the first place, the algebraic geometry of elliptic curves (and other algebraic curves, especially the curves that parametrize modular forms) were found to provide a source of new error-correcting codes which sometimes are better in certain respects than all previously known ones (see [van Lint 1988]). In the second place, H.W. Lenstra's unexpected discovery of an improved method of factoring integers based on elliptic curves over finite fields (see [Lenstra 1987]) led to a sudden interest in elliptic curves among researchers in cryptography. Further cryptographic applications arose as the groups of elliptic curves were used as the "site" of so-called "public key" encryption and key exchange schemes (see [Koblitz 1987], [Miller 1986], [Menezes and Vanstone 1990]).

Thus, to a much greater extent than I would have expected when I wrote this book, readers of the first edition came from applied areas of the mathematical sciences as well as the more traditional fields for the study of elliptic curves, such as algebraic geometry and algebraic number theory.

I would like to thank the many readers who suggested corrections and improvements that have been incorporated into the second edition.

Contents

CHAPTER I

From Congruent Numbers to Elliptic Curves

The theory of elliptic curves and modular forms is one subject where the most diverse branches of mathematics come together: complex analysis, algebraic geometry, representation theory, number theory. While our point of view will be number theoretic, we shall find ourselves using the type of techniques that one learns in basic courses in complex variables, real variables, and algebra. A well-known feature of number theory is the abundance of conjectures and theorems whose statements are accessible to high school students but whose proofs either are unknown or, in some cases, are the culmination of decades of research using some of the most powerful tools of twentieth century mathematics.

We shall motivate our choice of topics by one such theorem: an elegant characterization of so-called "congruent numbers" that was proved by J. Tunnell [Tunnell 1983]. A few of the proofs of necessary results go beyond our scope, but many of the ingredients in the proof of Tunnell's theorem will be developed in complete detail.

Tunnell's theorem gives an almost complete answer to an ancient problem: find a simple test to determine whether or not a given integer n is the area of some right triangle all of whose sides are rational numbers. A natural number n is called "congruent" if there exists a right triangle with all three sides rational and area n. For example, 6 is the area of the 3–4–5 right triangle, and so is a congruent number.

Right triangles whose sides are integers X, Y, Z (a "Pythagorean triple") were studied in ancient Greece by Pythagoras, Euclid, Diophantus, and others. Their central discovery was that there is an easy way to generate all such triangles. Namely, take any two positive integers a and b with $a > b$, draw the line in the uv-plane through the point $(-1, 0)$ with slope b/a. Let (u, v) be the second point of intersection of this line with the unit circle (see Fig. I.1). It is not hard to show that

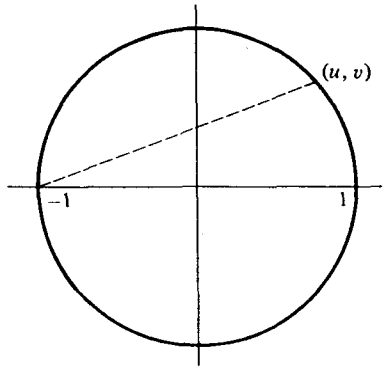


Figure I.1

$$u = \frac{a^2 - b^2}{a^2 + b^2}, \qquad v = \frac{2ab}{a^2 + b^2}.$$

Then the integers $X = a^2 - b^2$, $Y = 2ab$, $Z = a^2 + b^2$ are the sides of a right triangle; the fact that $X^2 + Y^2 = Z^2$ follows because $u^2 + v^2 = 1$. By letting a and b range through all positive integers with $a > b$, one gets all possible Pythagorean triples (see Problem 1 below).

Although the problem of studying numbers n which occur as areas of rational right triangles was of interest to the Greeks in special cases, it seems that the congruent number problem was first discussed systematically by Arab scholars of the tenth century. (For a detailed history of the problem of determining which numbers are "congruent", see [L. E. Dickson 1952, Ch. XVI]; see also [Guy 1981, Section D27].) The Arab investigators preferred to rephrase the problem in the following equivalent form: given n, can one find a rational number x such that $x^2 + n$ and $x^2 - n$ are both squares of rational numbers? (The equivalence of these two forms of the congruent number problem was known to the Greeks and to the Arabs; for a proof of this elementary fact, see Proposition 1 below.)

Since that time, some well-known mathematicians have devoted considerable energy to special cases of the congruent number problem. For example, Euler was the first to show that $n = 7$ is a congruent number. Fermat showed that $n = 1$ is *not*; this result is essentially equivalent to Fermat's Last Theorem for the exponent 4 (i.e., the fact that $X^4 + Y^4 = Z^4$ has no nontrivial integer solutions).

It eventually became known that the numbers 1, 2, 3, 4 are not congruent numbers, but 5, 6, 7 are. However, it looked hopeless to find a straightforward criterion to tell whether or not a given n is congruent. A major advance in the twentieth century was to place this problem in the context of the arithmetic theory of elliptic curves. It was in this context that Tunnell was able to prove his remarkable theorem.

Here is part of what Tunnell's theorem says (the full statement will be given later):

Theorem (Tunnell). *Let n be an odd squarefree natural number. Consider the two conditions:*

(A) *n is congruent;*
(B) *the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ is equal to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = n$.*

Then (A) *implies* (B)*; and, if a weak form of the so-called Birch–Swinnerton-Dyer conjecture is true, then* (B) *also implies* (A).

The central concepts in the proof of Tunnell's theorem—the Hasse–Weil L-function of an elliptic curve, the Birch–Swinnerton-Dyer conjecture, modular forms of half integer weight—will be discussed in later chapters. Our concern in this chapter will be to establish the connection between congruent numbers and a certain family of elliptic curves, in the process giving the definition and some basic properties of elliptic curves.

§1. Congruent numbers

Let us first make a more general definition of a congruent number. A positive rational number $r \in \mathbb{Q}$ is called a "congruent number" if it is the area of some right triangle with rational sides. Suppose r is congruent, and $X, Y, Z \in \mathbb{Q}$ are the sides of a triangle with area r. For any nonzero $r \in \mathbb{Q}$ we can find some $s \in \mathbb{Q}$ such that $s^2 r$ is a squarefree integer. But the triangle with sides sX, sY, sZ has area $s^2 r$. Thus, without loss of generality we may assume that $r = n$ is a squarefree natural number. Expressed in group language, we can say that whether or not a number r in the multiplicative group $\mathbb{Q}^+$ of positive rational numbers has the congruent property depends only on its coset modulo the subgroup $(\mathbb{Q}^+)^2$ consisting of the squares of rational numbers; and each coset in $\mathbb{Q}^+/(\mathbb{Q}^+)^2$ contains a unique squarefree natural number $r = n$. In what follows, when speaking of congruent numbers, we shall always assume that the number is a squarefree positive integer.

Notice that the definition of a congruent number does not require the sides of the triangle to be integral, only rational. While $n = 6$ is the smallest possible area of a right triangle with integer sides, one can find right triangles with rational sides having area $n = 5$. The right triangle with sides $1\frac{1}{2}, 6\frac{2}{3}, 6\frac{5}{6}$ is such a triangle (see Fig. I.2). It turns out that $n = 5$ is the smallest congruent number (recall that we are using "congruent number" to mean "congruent squarefree natural number").

There is a simple algorithm using Pythagorean triples (see the problems below) that will eventually list all congruent numbers. Unfortunately, given

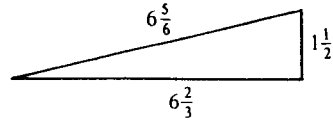


Figure I.2

n, one cannot tell how long one must wait to get n if it is congruent; thus, if n has not appeared we do not know whether this means that n is not a congruent number or that we have simply not waited long enough. From a practical point of view, the beauty of Tunnell's theorem is that his condition (B) can be easily and rapidly verified by an effective algorithm. Thus, his theorem almost settles the congruent number problem, i.e., the problem of finding a verifiable criterion for whether a given n is congruent. We must say "almost settles" because in one direction the criterion is only known to work in all cases if one assumes a conjecture about elliptic curves.

Now suppose that X, Y, Z are the sides of a right triangle with area n. This means: $X^2 + Y^2 = Z^2$, and $\frac{1}{2}XY = n$. Thus, algebraically speaking, the condition that n be a congruent number says that these two equations have a simultaneous solution X, Y, $Z \in \mathbb{Q}$. In the proposition that follows, we derive an alternate condition for n to be a congruent number. In listing triangles with sides X, Y, Z, we shall not want to list X, Y, Z and Y, X, Z separately. So for now let us fix the ordering by requiring that $X < Y < Z$ (Z is the hypotenuse).

Proposition 1. *Let n be a fixed squarefree positive integer. Let X, Y, Z, x always denote positive rational numbers, with $X < Y < Z$. There is a one-to-one correspondence between right triangles with legs X and Y, hypotenuse Z, and area n; and numbers x for which x, $x + n$, and $x - n$ are each the square of a rational number. The correspondence is:*

$$X, Y, Z \to x = (Z/2)^2$$

$$x \to X = \sqrt{x+n} - \sqrt{x-n}, \quad Y = \sqrt{x+n} + \sqrt{x-n}, \quad Z = 2\sqrt{x}.$$

In particular, n is a congruent number if and only if there exists x such that x, $x + n$, and $x - n$ are squares of rational numbers.

PROOF. First suppose that X, Y, Z is a triple with the desired properties: $X^2 + Y^2 = Z^2$, $\frac{1}{2}XY = n$. If we add or subtract four times the second equation from the first, we obtain: $(X \pm Y)^2 = Z^2 \pm 4n$. If we then divide both sides by four, we see that $x = (Z/2)^2$ has the property that the numbers $x \pm n$ are the squares of $(X \pm Y)/2$. Conversely, given x with the desired properties, it is easy to see that the three positive rational numbers $X < Y < Z$ given by the formulas in the proposition satisfy: $XY = 2n$, and $X^2 + Y^2 = 4x = Z^2$. Finally, to establish the one-to-one correspondence, it only remains

to verify that no two distinct triples X, Y, Z can lead to the same x. We leave this to the reader (see the problems below). □

PROBLEMS

1. Recall that a Pythagorean triple is a solution (X, Y, Z) in positive integers to the equation $X^2 + Y^2 = Z^2$. It is called "primitive" if X, Y, Z have no common factor. Suppose that $a > b$ are two relatively prime positive integers, not both odd. Show that $X = a^2 - b^2$, $Y = 2ab$, $Z = a^2 + b^2$ form a primitive Pythagorean triple, and that all primitive Pythagorean triples are obtained in this way.

2. Use Problem 1 to write a flowchart for an algorithm that lists all squarefree congruent numbers (of course, not in increasing order). List the first twelve distinct congruent numbers your algorithm gives. Note that there is no way of knowing when a given congruent number n will appear in the list. For example, 101 is a congruent number, but the first Pythagorean triple which leads to an area s^2 101 involves twenty-two-digit numbers (see [Guy 1981, p. 106]). One hundred fifty-seven is even worse (see Fig. I.3). One cannot use this algorithm to establish that some n is *not* a congruent number. Technically, it is not a real algorithm, only a "semi-algorithm".

3. (a) Show that if 1 were a congruent number, then the equation $x^4 - y^4 = u^2$ would have an integer solution with u odd.
   (b) Prove that 1 is not a congruent number. (Note: A consequence is Fermat's Last Theorem for the exponent 4.)

4. Finish the proof of Proposition 1 by showing that no two triples X, Y, Z can lead to the same x.

5. (a) Find $x \in (\mathbb{Q}^+)^2$ such that $x \pm 5 \in (\mathbb{Q}^+)^2$.
   (b) Find $x \in (\mathbb{Q}^+)^2$ such that $x \pm 6 \in (\mathbb{Q}^+)^2$.

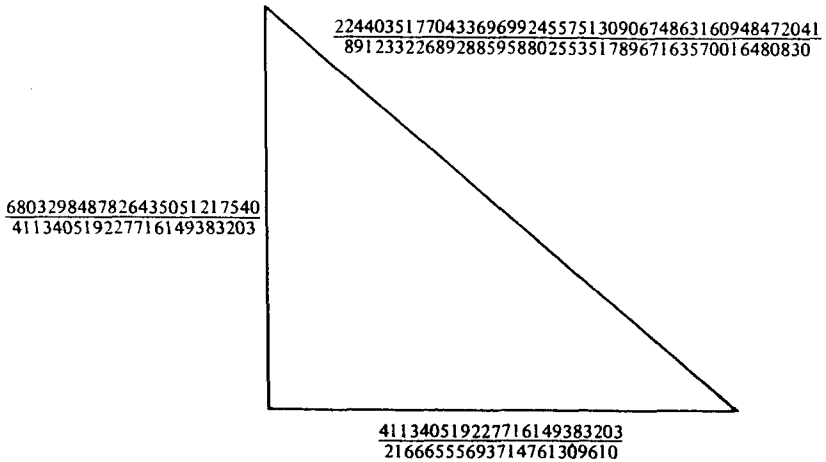


Figure I.3. The Simplest Rational Right Triangle with Area 157 (computed by D. Zagier).

(c) Find two values $x \in (\mathbb{Q}^+)^2$ such that $x \pm 210 \in (\mathbb{Q}^+)^2$. At the end of this chapter we shall prove that if there is one such x, then there are infinitely many. Equivalently (by Proposition 1), if there exists one right triangle with rational sides and area n, then there exist infinitely many.

6. (a) Show that condition (B) in Tunnell's theorem is equivalent to the condition that the number of ways n can be written in the form $2x^2 + y^2 + 8z^2$ with x, y, z integers and z odd, be equal to the number of ways n can be written in this form with z even.
   (b) Write a flowchart for an algorithm that tests condition (B) in Tunnell's theorem for a given n.

7. (a) Prove that condition (B) in Tunnell's theorem always holds if n is congruent to 5 or 7 modulo 8.
   (b) Check condition (B) for all squarefree $n \equiv 1$ or 3 (mod 8) until you find such an n for which condition (B) holds.
   (c) By Tunnell's theorem, the number you found in part (b) should be the smallest congruent number congruent to 1 or 3 modulo 8. Use the algorithm in Problem 2 to find a right triangle with rational sides and area equal to the number you found in part (b).

§2. A certain cubic equation

In this section we find yet another equivalent characterization of congruent numbers.

In the proof of Proposition 1 in the last section, we arrived at the equations $((X \pm Y)/2)^2 = (Z/2)^2 \pm n$ whenever X, Y, Z are the sides of a triangle with area n. If we multiply together these two equations, we obtain $((X^2 - Y^2)/4)^2 = (Z/2)^4 - n^2$. This shows that the equation $u^4 - n^2 = v^2$ has a rational solution, namely, $u = Z/2$ and $v = (X^2 - Y^2)/4$. We next multiply through by u^2 to obtain $u^6 - n^2u^2 = (uv)^2$. If we set $x = u^2 = (Z/2)^2$ (this is the same x as in Proposition 1) and further set $y = uv = (X^2 - Y^2)Z/8$, then we have a pair of rational numbers (x, y) satisfying the cubic equation:

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

Thus, given a right triangle with rational sides X, Y, Z and area n, we obtain a point (x, y) in the xy-plane having rational coordinates and lying on the curve $y^2 = x^3 - n^2x$. Conversely, can we say that any point (x, y) with $x, y \in \mathbb{Q}$ which lies on the cubic curve must necessarily come from such a right triangle? Obviously not, because in the first place the x-coordinate $x = u^2 = (Z/2)^2$ must lie in $(\mathbb{Q}^+)^2$ if the point (x, y) can be obtained as in the last paragraph. In the second place, we can see that the x-coordinate of such a point must have its denominator divisible by 2. To see this, notice that the triangle X, Y, Z can be obtained starting with a primitive Pythagorean triple X', Y', Z' corresponding to a right triangle with integral sides X', Y', Z' and area s^2n, and then dividing the sides by s to get X, Y, Z. But in a primitive