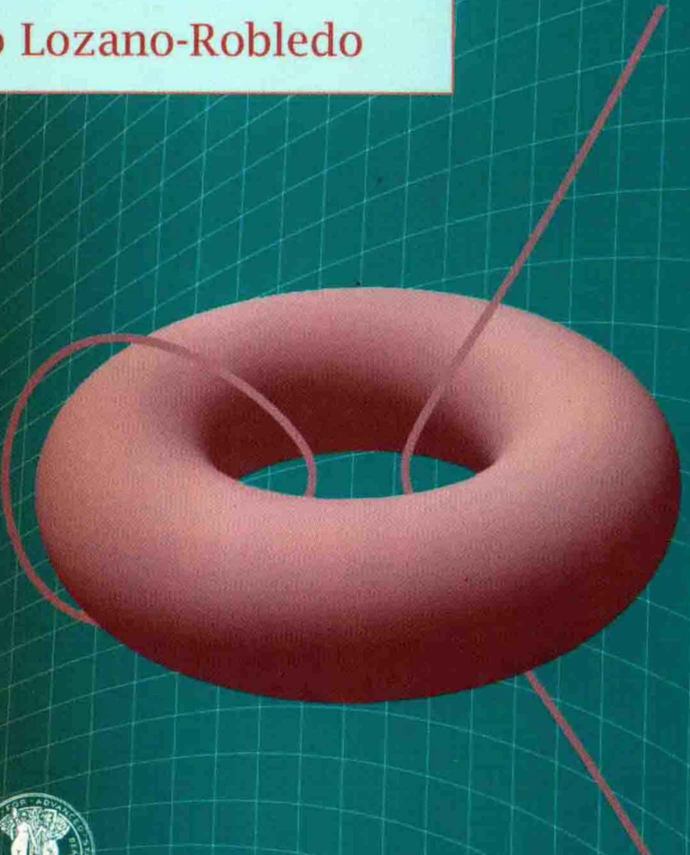
STUDENT MATHEMATICAL LIBRARY
IAS/PARK CITY MATHEMATICAL SUBSERIES
Volume 58

Elliptic Curves, Modular Forms, and Their L-functions

Álvaro Lozano-Robledo



American Mathematical Society
Institute for Advanced Study

STUDENT MATHEMATICAL LIBRARY
IAS/PARK CITY MATHEMATICAL SUBSERIES
Volume 58

Elliptic Curves, Modular Forms, and Their L-functions

Álvaro Lozano-Robledo

American Mathematical Society, Providence, Rhode Island
Institute for Advanced Study, Princeton, New Jersey

Cover art courtesy of Karl Rubin, using MegaPOV, which is based on POV-Ray, both of which are open source, freely available software.

2000 *Mathematics Subject Classification.* Primary 14H52, 11G05; Secondary 11F03, 11G40.

For additional information and updates on this book, visit
www.ams.org/bookpages/stml-58

Library of Congress Cataloging-in-Publication Data

Lozano-Robledo, Álvaro, 1978–
Elliptic curves, modular forms, and their L-functions / Álvaro Lozano-Robledo.
p. cm. — (Student mathematical library ; v. 58. IAS/Park City mathematical subseries)
Includes bibliographical references and index.
ISBN 978-0-8218-5242-2 (alk. paper)
1. Curves, Elliptic. 2. Forms, Modular. 3. L-functions. 4. Number theory. I. Title.

QA567.2.E44L69 2010
516.3′52—dc22

2010038952

10 9 8 7 6 5 4 3 2 1 16 15 14 13 12 11

Elliptic Curves, Modular Forms, and Their L-functions

A mis padres, que me enseñaron todo lo importante,
a mi abuela, por su sonrisa que no aparece en fotografías,
a Marisa, por lograr que siempre me supere,
y a "Sally", que nacerá pronto.

Preface

This book grew out of the lecture notes for a course on "Elliptic Curves, Modular Forms and L-functions" that the author taught at an undergraduate summer school as part of the 2009 Park City Mathematics Institute. These notes are an *introductory survey* of the theory of elliptic curves, modular forms and their L-functions, with an emphasis on examples rather than proofs. The main goal is to provide the reader with a *big picture* of the surprising connections among these three types of mathematical objects, which are seemingly so distinct. In that vein, one of the themes of the book is to explain the statement of the modularity theorem (Theorem 5.4.6), previously known as the Taniyama-Shimura-Weil conjecture (Conjecture 5.4.5). In order to underscore the importance of the modularity theorem, we also discuss in some detail one of its most renowned consequences: Fermat's last theorem (Example 1.1.5 and Section 5.5).

It would be impossible to give the proofs of the main theorems on elliptic curves and modular forms in one single course, and the proofs would be outside the scope of the undergraduate curriculum. However, the definitions, the statements of the main theorems and their corollaries can be easily understood by students with some standard undergraduate background (calculus, linear algebra, elementary number theory and a first course in abstract algebra). Proofs that are accessible to a student are left to the reader and proposed as exercises at the end of each chapter. The reader should be warned, though, that there are multiple references to mathematical objects and results that we will not have enough space to discuss in full, and the student will have to take these items on faith (we will provide references to other texts, however, for those students who wish to deepen their understanding). Some other objects and theorems are mentioned in previous chapters but only explained fully in later chapters. To avoid any confusion, we always try to clarify in the text which objects or results the student should take on faith, which ones we expect the student to be familiar with, and which will be explained in later chapters (by providing references to later sections of the book).

The book begins with some motivating problems, such as the congruent number problem, Fermat's last theorem, and the representations of integers as sums of squares. Chapter 2 is a survey of the algebraic theory of elliptic curves. In Section 2.9, we give a proof of the weak Mordell-Weil theorem for elliptic curves with rational 2-torsion and explain the method of 2-descent. The goal of Chapter 3 is to motivate the connection between elliptic curves and modular forms. To that end, we discuss complex lattices, tori, modular curves and how these objects relate to elliptic curves over the complex numbers. Chapter 4 introduces the spaces of modular forms for $\mathrm{SL}(2,\mathbb{Z})$ and other congruence subgroups (e.g., $\Gamma_0(N)$). In Chapter 5 we define the L-functions attached to elliptic curves and modular forms. We briefly discuss the Birch and Swinnerton-Dyer conjecture and other related conjectures. Finally, in Section 5.4, we justify the statement of the original conjecture of Taniyama-Shimura-Weil (which we usually refer to as the modularity theorem, since it was proved in 1999); i.e., we explain the surprising connection between elliptic curves and certain modular forms, and justify which modular forms correspond to elliptic curves.

In order to make this book as self-contained as possible, I have also included five appendices with concise introductions to topics that some students may not have encountered in their classes yet. Appendix A is a quick reference guide to two popular software packages: PARI and Sage. Throughout the book, we strongly recommend that the reader tries to find examples and do calculations using one of these two packages. Appendix B is a brief summary of complex analysis. Due to space limitations we only include definitions, a few examples, and a list of the main theorems in complex analysis; for a full treatment see [**Ahl79**], for instance. In Appendix C we introduce the projective line and the projective plane. The p-adic integers and the p-adic numbers are treated in Appendix D (for a complete reference, see [**Gou97**]). Finally, in Appendix E we list infinite families of elliptic curves over $\mathbb{Q}$, one family for each of the possible torsion subgroups over $\mathbb{Q}$.

I would like to emphasize once again that this book is, by no means, a thorough treatment of elliptic curves and modular forms. The theory is far too vast to be covered in one single volume, and the proofs are far too technical for an undergraduate student. Therefore, the humble goals of this text are to provide a *big picture* of the vast and fast-growing theory, and to be an "advertisement" for undergraduates of these very active and exciting areas of number theory. The author's only hope is that, after reading this text, students will feel compelled to study elliptic curves and modular forms in depth, and in all their full glory.

There are many excellent references that I would recommend to the students, and that I have frequently consulted in the preparation of this book:

(1) There are not that many books on these subjects at the *undergraduate level*. However, Silverman and Tate's book [**SiT92**] is an excellent introduction to elliptic curves for undergraduates. Washington's book [**Was08**] is also accessible for undergraduates and emphasizes the cryptography applications of elliptic curves. Stein's book [**Ste08**] also has an interesting chapter on elliptic curves.

(2) There are several *graduate-level* texts on elliptic curves. Silverman's book [**Sil86**] is the standard reference, but Milne's [**Mil06**] is also an excellent introduction to the theory of elliptic curves (and also includes a chapter on modular forms). Before reading Silverman or Milne, the reader would benefit

from studying some algebraic geometry and algebraic number theory. (Milne's book does not require as much algebraic geometry as Silverman's.)

(3) The theory of modular forms and L-functions is definitely a *graduate topic*, and the reader will need a strong background in algebra to understand all the fine details. Diamond and Shurman's book [**DS05**] contains a neat, modern and thorough account of the theory of modular forms (including much information about the modularity theorem). Koblitz's book [**Kob93**] is also a very nice introduction to the theory of elliptic curves and modular forms (and includes a lot of information about the congruent number problem). Chapter 5 in Milne's book [**Mil06**] contains a good, concise overview of the subject. Serre's little book [**Ser77**] is always worth reading and also contains an introduction to modular forms. Miyake's book [**Miy06**] is a very useful reference.

(4) Finally, if the reader is interested in computations, we recommend Cremona's [**Cre97**] or Stein's [**Ste07**] book. If the reader wants to play with fundamental domains of modular curves, try Helena Verrill's applet [**Ver05**].

I would like to thank the organizers of the undergraduate summer school at PCMI, Aaron Bertram and Andrew Bernoff, for giving me the opportunity to lecture in such an exciting program. Also, I would like to thank Ander Steele and Aaron Wood for numerous corrections and comments of an early draft. Last, but not least, I would like to express my gratitude to Keith Conrad, David Pollack and William Stein, whose abundant comments and suggestions have improved this manuscript much more than it would be safe to admit.

Álvaro Lozano-Robledo

Contents

Chapter 1

Introduction

Notation:

$\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of natural numbers.

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is the ring of integers.

$\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\}$ is the field of rational numbers.

$\mathbb{R}$ is the field of real numbers.

$\mathbb{C} = \{a + bi : a, b \in \mathbb{R},\ i^2 = -1\}$ is the field of complex numbers.

In this chapter, we introduce elliptic curves, modular forms and L-functions through examples that motivate the definitions.

1.1. Elliptic curves

For the time being, we define an elliptic curve to be any equation of the form

$$y^2 = x^3 + ax^2 + bx + c$$

with $a, b, c \in \mathbb{Z}$ and such that the polynomial $x^3 + ax^2 + bx + c$ does not have repeated roots. See Section 2.2 for a precise definition.

Example 1.1.1. *Are there three consecutive integers whose product is a perfect square?*

There are some trivial examples that involve the number zero, for example, $0, 1$ and 2, whose product equals $0 \cdot 1 \cdot 2 = 0 = 0^2$, a square.

Are there any non-trivial examples? If we try to assign variables to our problem, we see that we are trying to find solutions to

$$y^2 = x(x+1)(x+2) \tag{1.1}$$

with $x, y \in \mathbb{Z}$ and $y \neq 0$. Equation (1.1) defines an elliptic curve. It turns out that there are no integral solutions other than the trivial ones (see Exercise 1.4.1). Are there rational solutions, i.e., are there solutions with $x, y \in \mathbb{Q}$? This is a more delicate question, but the answer is still no (we will prove it in Example 2.7.6). Here is a similar question, with a very different answer:

- *Are there three integers that differ by* 5, *i.e.*, x, $x+5$ *and* $x+10$, *and whose product is a perfect square?*

In this case, we are trying to find solutions to $y^2 = x(x+5)(x+10)$ with $x, y \in \mathbb{Z}$. As in the previous example, there are trivial solutions (those which involve 0) but in this case, there are non-trivial solutions as well:

$$\begin{aligned} (-9)\cdot(-9+5)\cdot(-9+10) = (-9)\cdot(-4)\cdot 1 = 36 &= 6^2 \\ 40\cdot(40+5)\cdot(40+10) = 40\cdot 45\cdot 50 = 90000 &= 300^2. \end{aligned}$$

Moreover, there are also *rational* solutions, which are far from obvious:

$$\begin{aligned} \left(\frac{5}{4}\right)\cdot\left(\frac{5}{4}+5\right)\cdot\left(\frac{5}{4}+10\right) &= \left(\frac{75}{8}\right)^2 \\ \left(-\frac{50}{9}\right)\cdot\left(-\frac{50}{9}+5\right)\cdot\left(-\frac{50}{9}+10\right) &= \left(\frac{100}{27}\right)^2 \end{aligned}$$

and, in fact, there are infinitely many *rational* solutions! Here are some of the x-coordinates that work:

$$x = -9,\ 40,\ \frac{5}{4},\ \frac{-50}{9},\ \frac{961}{144},\ \frac{7200}{961},\ -\frac{12005}{1681},\ -\frac{16810}{2401},\ -\frac{27910089}{5094049},\ldots$$

In Sections 2.9 and 2.10 we will explain a method to find rational points on elliptic curves and, in Exercise 2.12.23, the reader will calculate all the rational points of $y^2 = x(x+5)(x+10)$. ■

Example 1.1.2 (The Congruent Number Problem). *We say that* $n \geq 1$ *is a congruent number if there exists a right triangle whose sides are rational numbers and whose area equals* n. *What natural numbers are congruent?*

For instance, the number 6 is congruent, because the right triangle with sides of length $(a, b, c) = (3, 4, 5)$ has area equal to $\frac{3\cdot 4}{2} = 6$. Similarly, the number 30 is the area of the right triangle with sides $(5, 12, 13)$; thus, 30 is a congruent number.

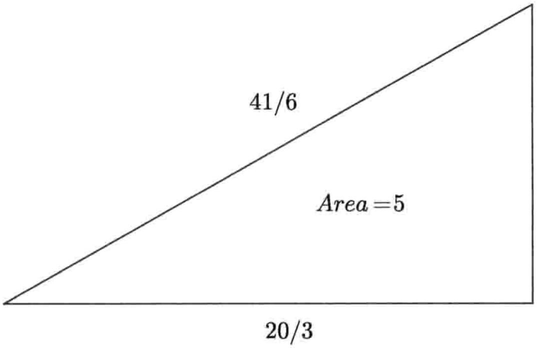


Figure 1. A right triangle of area 5 and rational sides.

The number 5 is congruent but there is no right triangle with integer sides and area equal to 5. However, our definition allowed *rational* sides, and the triangle with sides $\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$ has area exactly 5. We do not allow, however, triangles with irrational sides even if the area is an integer. For example, the right triangle $(1, 2, \sqrt{5})$ has area 1, but that does not imply that 1 is a congruent number (in fact, 1 is *not* a congruent number, as we shall see below).

The congruent number problem is one of the oldest open problems in number theory. For more than a millennium, mathematicians have attempted to provide a characterization of all congruent numbers. The oldest written record of the problem dates back to the early Middle Ages, when it appeared in an Arab manuscript written before 972 (a later 10th century manuscript written by Mohammed Ben Alcohain would go as far as to claim that the principal object of the theory of rational right triangles is to find congruent numbers). It is known that Leonardo Pisano, a.k.a. *Fibonacci*, was challenged around 1220 by Johannes of Palermo to find a rational right triangle of area

$n = 5$, and Fibonacci found the triangle $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$. We will explain a method to find this triangle below. In 1225, Fibonacci wrote a more general treatment about the congruent number problem, in which he stated (without proof) that if n is a perfect square, then n cannot be a congruent number. The proof of such a claim had to wait until Pierre de Fermat (1601-1665) settled that the number 1 (and every square number) is not a congruent number (a result that he showed in order to prove the case $n = 4$ of Fermat's last theorem).

The connection between the congruent number problem and elliptic curves is as follows:

Proposition 1.1.3. *The number $n > 0$ is congruent if and only if the curve $y^2 = x^3 - n^2x$ has a point (x, y) with $x, y \in \mathbb{Q}$ and $y \neq 0$. More precisely, there is a one-to-one correspondence $C_n \longleftrightarrow E_n$ between the following two sets:*

$$\begin{aligned} C_n &= \{(a,b,c) : a^2 + b^2 = c^2,\ \frac{ab}{2} = n\} \\ E_n &= \{(x,y) : y^2 = x^3 - n^2x,\ y \neq 0\}. \end{aligned}$$

Mutually inverse correspondences $f : C_n \to E_n$ and $g : E_n \to C_n$ are given by

$$f((a,b,c)) = \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right),\ g((x,y)) = \left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right).$$

The reader can provide a proof (see Exercise 1.4.3). For example, the curve $E : y^2 = x^3 - 25x$ has a point $(-4, 6)$ that corresponds to the triangle $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$. But E has other points, such as $(\frac{1681}{144}, \frac{62279}{1728})$ that corresponds to the triangle

$$\left(\frac{1519}{492}, \frac{4920}{1519}, \frac{3344161}{747348}\right)$$

which also has area equal to 5. See Figure 2.

Today, there are partial results toward the solution of the congruent number problem, and strong results that rely heavily on famous (and widely accepted) conjectures, but we do not have a full answer yet. For instance, in 1975 (see [**Ste75**]), Stephens showed that the Birch and Swinnerton-Dyer conjecture (which we will discuss in Section 5.2) implies that any positive integer $n \equiv 5$, 6 or 7 mod 8 is a

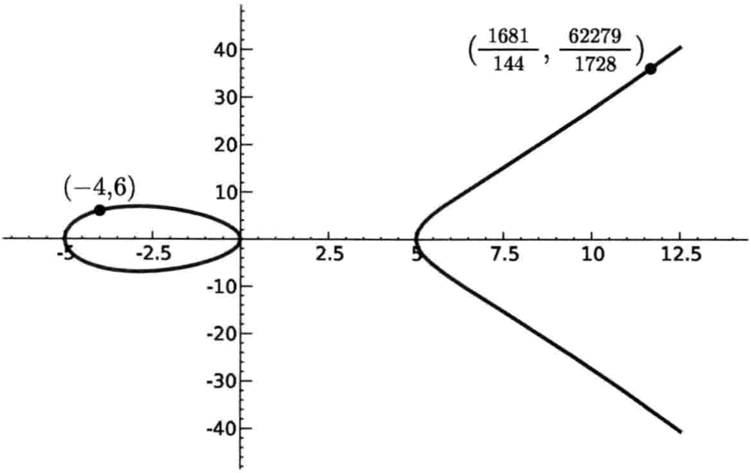


Figure 2. Two rational points on the curve $y^2 = x^3 - 25x$.

congruent number. For example, $n = 157 \equiv 5 \mod 8$ must be a congruent number and, indeed, Don Zagier has exhibited a right triangle (a, b, c) whose area equals 157. The hypotenuse of the simplest such triangle is:

$$c = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

In Example 5.2.7 we will see an application of the conjecture of Birch and Swinnerton-Dyer to find a rational point P on $y^2 = x^3 - 157^2 x$, which corresponds to a right triangle of area 157 via the correspondence in Proposition 1.1.3.

The best known result on the congruent number problem is due to J. Tunnell:

Theorem 1.1.4 (Tunnell, 1983, [**Tun83**]). *If n is an odd square-free positive integer and n is the area of a right triangle with rational sides, then the following cardinalities are equal:*

$$\begin{aligned}&\#\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2\}\\ &= \frac{1}{2}\left(\#\left\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2\right\}\right)\end{aligned}$$