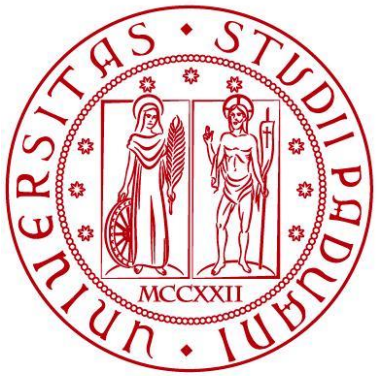


UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI CIVITA"

Corso di Laurea Triennale in Matematica

Elliptic Curves and the Congruent Number Problem

Relatore:
Prof. Matteo Longo

Candidato: **Francesco Barban**
Matricola: **2000418**

ANNO ACCADEMICO 2022/2023

22 settembre 2023

Contents

Introduction

Congruent numbers are rational numbers which are the area of a right trangle having rational sides. Recognizing these numbers is a classic, still unsolved, problem in Number Theory known as *the Congruent Number Problem.*

In this context, the word "congruent" comes from the Latin word *congruum*, meaning an arithmetic progression of three square rational numbers.

As we shall see in Chapter 1, congruent numbers are precisely those that appear as difference in two consecutive terms in these progressions. We will also see that it suffices to limit our study to squarefree positive integers, rather than considering all positive rational numbers.

While it is clear that any rational right triangle has rational area, the converse is false.

Example 0.1. *The first squarefree integers that happen to be congruent numbers are*

- $n = 5$ *is the area of the* $(3/2, 20/3, 41/6)$ *triangle.*
- $n = 6$ *is the area of the* $(3, 4, 5)$ *triangle.*
- $n = 7$ *is the area of the* $(35/12, 24/5, 337/60)$ *triangle.*

At first glance it is not obvious at all whether or not a given integer is a congruent number. To give an idea, $n = 53$ is a congruent number, and a rational right triangle that has area 53 has sides

$$\left(\frac{1472112483}{202332130}, \frac{21447205780}{1472112483}, \frac{48504938973297859 61}{297855654284978790}\right)$$

while $n = 1$, the simplest squarefree positive integer, is not congruent. We shall prove it later.

The goal of this thesis is to show how the Congruent Number Problem can be studied using the arithmetic of elliptic curves, which allows us to give a different and deeper characterization of congruent numbers.

The link between congruent numbers and elliptic curves will be made clear in Chapter 1, while in Chapter 2 we will introduce the theory of elliptic functions and elliptic curves defined over $\mathbb{C}$. In Chapter 3 we will consider elliptic curves defined over finite fields, which we will need in Chapter 4. In Chapter 4 we will state and prove the main results, namely we show that a squarefree positive integer n is a congruent number if and only if a specific elliptic curve over $\mathbb{Q}$ has non-torsion rational points.

The study of congruent numbers goes far beyond this last result, and in Chapter 5 we give a glimpse at how L-functions allow us to go even deeper.

Chapter 1

Congruent numbers

In this chapter we explain how congruent numbers are related to a particular family of elliptic curves over $\mathbb{Q}$.

Definition 1.1. A *congruent number* is a positive rational number that is the area of a rational-sided right triangle.

If $r \in \mathbb{Q}$, then we can find another rational number $s \in \mathbb{Q}$ such that $s^2 r$ is a squarefree positive integer. Indeed, suppose $r = a/b$ and that a and b are coprime integers and have prime decompositions $p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ and $q_1^{f_1} q_2^{f_2} \cdots q_n^{f_m}$ respectively. Let $l = b/a \cdot C$, where $C = (\prod q_j) \cdot (\prod p_i)$ and the products are taken over all primes having odd exponent. It is easy to check that l is the square of some rational number s having the desired property.

Now let $r \in \mathbb{Q}$ be the area of a right triangle with sides $X, Y, Z \in \mathbb{Q}$. If we take $s \in \mathbb{Q}$ as above then the triangle sX, sY, sZ has area $s^2 r$, which is a squarefree positive integer. Thus we can assume without loss of generality that congruent numbers are squarefree positive integers.

The condition that n is a congruent number says that the equations $X^2 + Y^2 = Z^2$ and $XY/2 = n$ have a simultaneous rational solution X, Y, Z. In the following proposition we derive an equivalent condition for n to be a congruent number.

Proposition 1.2. *Let n be be a fixed squarefree positive integer. Let X, Y, Z denote rational numbers, with $X < Y < Z$ and $X^2 + Y^2 = Z^2$. There is a one-to-one correspondence between right triangles with legs X and Y, hypotenuse Z, and area n and rational numbers x for which x, $x + n$ and*

$x - n$ are each the square of a rational number. The correspondence is:

$$\begin{aligned}(X, Y, Z) \mapsto &\quad x = (Z/2)^2 \\ x \mapsto &\quad (\sqrt{x+n} - \sqrt{x-n}, \quad \sqrt{x+n} + \sqrt{x-n}, \quad 2\sqrt{x})\end{aligned}$$

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

Proof. First suppose that X, Y, Z is a triple with the desired properties: $X^2 + Y^2 = Z^2$, $XY/2 = n$. 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 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 this map is injective. Assume, for the sake of contradiction, that two different triples (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) lead to the same x, this forces $Z_1 = Z_2$ and $X_1 \neq X_2, Y_1 \neq Y_2$. We still have that $X_1 Y_1 = X_2 Y_2 = 2n$, thus $X_1/X_2 = Y_2/Y_1 = k$ for some $k > 0$. Together with the relations $X_1^2 + Y_1^2 = Z_1^2$ and $X_2^2 + Y_2^2 = Z_2^2$, this gives $(X_2^2 - Y_1^2)(k^2 - 1) = 0$. It must be $X_2 = Y_1$ otherwise we would have $X_1 = X_2$ and $Y_1 = Y_2$. Now, if $0 < k < 1$ then $Y_2 < Y_1 = X_2$ contradicting the fact that $X_2 < Y_2$. If instead $k > 1$ then $X_1 > X_2 = Y_1$ contradicting $X_1 < Y_1$. This proves that two such different triples cannot exist and the map is injective. □

In the proof of the previous proposition we obtained the equations

$$(X \pm Y)^2/4 = (Z/2)^2 \pm n$$

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 $u^6 - n^2 u^2 = (uv)^2$. If we set $x = u^2 = (Z/2)^2$ and further set $y = uv = (X^2 - Y^2)Z/8$, then we have a pair of rational numbers (x, y) satisfying the following cubic equation:

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

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 ? To answer this question we first give the following lemma.

Lemma 1.3. *A Pythagorean triple verifies* $\gcd(X, Y, Z) = 1$ *if and only if there exists two relatively prime positive integers* $a < b$*, not both odd, and such that* $X = a^2 - b^2, Y = 2ab, Z = a^2 + b^2$*. We will call these Pythagorean triples* primitive*.*

Proof. ($\Rightarrow$) Suppose that X, Y, Z is a primitive Pythagorean triple. Observe that X and Y cannot both be odd, otherwise Z would not be divisible by four and hence would not be the square of an even integer. Suppose without loss of generality that Y is even, then we have $(Y/2)^2 = (Z + X)/2 \cdot (Z - X)/2$, and since $\gcd(X, Z) = 1$ then $\gcd((Z + X)/2, (Z - X)/2) = 1$. Since we have an equality between a square integer the product of two coprime integers this implies that $(Z + X)/2$ and $(Z - X)/2$ are both squares. If we put $a^2 = (Z + X)/2$, $b^2 = (Z - X)/2$ then we have that $X = a^2 - b^2$, $Y = 2ab$ and $Z = a^2 + b^2$.

($\Leftarrow$) Let $a < b$ be two positive coprime integers, not both odd. Let $X = a^2 - b^2$, $Y = 2ab$, $Z = a^2 + b^2$. It is immediate to check that X, Y, Z is a Pythagorean triple, we only need to prove that it is primitive. Suppose, for the sake of contradiction, that $\gcd(X, Y, Z) > 1$, then there exists a prime integer p such that $p \mid (a^2 - b^2)$, $p \mid 2ab$, $p \mid (a^2 + b^2)$. If $p = 2$ then $p \mid (a + b)$, so a and b have the same parity, contradicting the hypothesis. If intead $p > 2$ then from $p \mid (a + b)(a - b)$ follows that $p \mid \gcd(a, b)$, again contradicting the hypothesis. This proves the lemma. □

We are now ready to give a necessary and sufficient condition for a *rational point* on the curve $y^2 = x^3 - n^2x$ to come from a right triangle X, Y, Z with rational sides and area n.

Proposition 1.4. *Let* (x, y) *be a point with rational coordinates on the curve given by the equation* $y^2 = x^3 - n^2x$*. Then there exists a right triangle with rational sides and area* n *which corresponds to* x *(under the correspondence in Proposition* 1.2*) if and only if* x *satisfies the two conditions:* (i) *it is the square of a rational number and* (ii) *its denominator is even.*

Proof. ($\Rightarrow$) Suppose that X, Y, Z is a right triangle with rational sides and area n such that $x = (Z/2)^2$. Obviously x is the square of a rational number. To see why is must have denominator divisible by 2 notice that the triangle X, Y, Z can be obtained strting with a primitive Pythagorean triple X', Y', Z' corresponding to a right triangle with integral sides X', Y', Z' and area $s^2 n$, and then dividing the sides by s to get X, Y, Z. But in a primitive Pythagorean triple X' and Y' have different parity, and Z' is odd. We conclude that (1) $x = (Z/2)^2 = (Z'/2s)^2$ has denominator divisible by 2 and (2) the power of 2 dividing the denominator of Z is equal to the power of 2 dividing the denominator of one of the other two sides, while a strictly lower power of 2 divides the denominator of the third side.

($\Leftarrow$) Let $u = \sqrt{x} \in \mathbb{Q}^+$. We work backwards through the sequence of steps that brought us to the cubic equation. That is, set $v = y/u$ so that $v^2 = y^2/x = x^2 - n^2$, i.e. $v^2 + n^2 = x^2$. Now let t be the denominator of u, i.e. the smallest positive integer such that $tu \in \mathbb{Z}$. By assumption, t is even. Notice that the denominators of v^2 and x^2 are both equal to t^4. Thus $t^2 v,\ t^2 n,\ t^2 x$ is a primitive Pythagorean triple, with $t^2 n$ even. By Lemma 1.3, there exist integers a and b such that: $t^2 n = 2ab,\ t^2 v = a^2 - b^2,\ t^2 x = a^2 + b^2$. Then the right triangle with sides $2a/t,\ 2b/t,\ 2u$ has area $2ab/t^2 = n$, as desired. The image of this triangle $X = 2a/t,\ Y = 2b/t,\ Z = 2u$ under the correspondence in Proposition 1.2 is $x = (Z/2)^2 = u^2$. This proves the proposition. □

Remark 1.5. Proposition 1.4 implies that if we restrict the codomain of the map described in Proposition 1.2 to rational numbers x with even denominator such that $x,\ x + n,\ x - n$ are all squares of rational numbers then the correspondence is also surjective.

Now we prove that $n = 1$ is not a congruent number.

Theorem 1.6. *1 is not a congruent number.*

Proof. Suppose, for the sake of contradiction, that $n = 1$ is a congruent number and let $X, Y, Z \in \mathbb{Q}$ be the sides of the associated rational right triangle. It is easy to show that there exists a rational number $s \in \mathbb{Q}^+$ such that sX, sY, sZ are relatively prime integers. Rename the sides as X', Y', Z'. Thus $X'^2 + Y'^2 = Z'^2$ is a primitive Pythagorean triple whose triangle has area s^2. By the above lemma there exist $a > b$ relatively prime positive

integers of opposite parity such that

$$X' = a^2 - b^2 \qquad Y' = 2ab \qquad Z' = a^2 + b^2.$$

The (X', Y', Z') triangle has area $X'Y'/2 = ab(a+b)(a-b) = s^2$. This means that s is an integer, and since a and b are coprime $a+b$ and $a-b$ also are. So s^2 is a square which is a product of coprime integers, thus $a, b, a+b, a-b$ are all squares. Call $a = \alpha^2, b = \beta^2$, so

$$\alpha^2\beta^2(\alpha^4 - \beta^4) = s^2 \quad \Longrightarrow \quad \alpha^4 - \beta^4 = \left(\frac{s}{\alpha\beta}\right)^2.$$

Thus $(\alpha, \beta, s/\alpha\beta)$ is an integer primitive solution to the equation $x^4 - y^4 = u^2$ with x and u odd, and y even (because α and β have opposite parity and so $s/\alpha\beta$ is odd, and $(u)^2 + (y^2)^2 = (x^2)^2$ is a primitive Pythagorean triple).

For the next step we are using Fermat's descent method. Let x be the smallest odd integer for which there exists a solution to $x^4 - y^4 = u^2$. By the above lemma there exist $r > s$ positive coprime integers of opposite parity such that

$$u^2 = r^2 - s^2 \qquad y^2 = 2rs \qquad x^2 = r^2 + s^2.$$

Observe that the third equality identifies another primitive Pythagorean triple, so we repeat the last step:

$$r = l^2 - m^2 \qquad s = 2lm \qquad x = l^2 + m^2$$

where l and m have the same properties as a and b and we suppose, without loss of generality, that s is even. This means that

$$y^2 = 4lm(l^2 - m^2)$$

and since l and m are coprime then $l,\ m,\ l^2 - m^2$ are all squares. If we rename $l = \gamma^2,\ m = \delta^2,\ l^2 - m^2 = t^2$ we get $\gamma^4 - \delta^4 = t^2$. Thus γ is odd and in conclusion we observe that

$$\gamma \leq \gamma^2 = l \leq l^2 \lneq x$$

contradicting the minimality of x. This shows that the equation $x^4 - y^4 = u^2$ cannot have integer solutions and thus concludes the proof. □

We shall see that the cubic equation $y^2 = x^3 - n^2x$ defines an object called *elliptic curve*. In the next chapters we will study elliptic curves in more detail.

1.1 Finding congruent numbers

In Lemma 1.3 we saw three equations that parametrize all primitive Pythagorean triples. These equations can be used to "generate" congruent numbers: if a and b are as in Lemma 1.3 (we will say that these pairs are *admissible*), then $X = a^2 - b^2,\ Y = 2ab,\ Z = a^2 + b^2$ is a primitive Pythagorean triple and the triangle X, Y, Z has area $XY/2$. Let n be the squarefree part of the area, and let s be an integer such that $XY/2 = s^2 n$. Then the new right triangle with rational sides $X' = X/s$, $Y' = Y/s$, $Z' = Z/s$ has area n.

Table 1 illustrates this process for all admissible pairs (a, b) such that $a + b \leq 13$.

(a, b)	(X, Y, Z)	Area	(X', Y', Z')	n
$(2, 1)$	$(3, 4, 5)$	$2 \cdot 3$	$(3, 4, 5)$	6
$(4, 1)$	$(15, 8, 17)$	$2^2 \cdot 3 \cdot 5$	$(15/2, 4, 17/2)$	15
$(3, 2)$	$(5, 12, 13)$	$2 \cdot 3 \cdot 5$	$(5, 12, 13)$	30
$(6, 1)$	$(35, 12, 37)$	$2 \cdot 3 \cdot 5 \cdot 7$	$(35, 12, 37)$	210
$(5, 2)$	$(21, 20, 29)$	$2 \cdot 3 \cdot 5 \cdot 7$	$(21, 20, 29)$	210
$(4, 3)$	$(7, 24, 25)$	$2^2 \cdot 3 \cdot 7$	$(7/2, 12, 25/2)$	21
$(8, 1)$	$(63, 16, 65)$	$2^3 \cdot 3^2 \cdot 7$	$(21/2, 8/3, 65/6)$	14
$(7, 2)$	$(45, 28, 53)$	$2 \cdot 3^2 \cdot 5 \cdot 7$	$(15, 28/3, 53/3)$	70
$(5, 4)$	$(9, 40, 41)$	$2^2 \cdot 3^2 \cdot 5$	$(3/2, 20/3, 41/6)$	5
$(10, 1)$	$(99, 20, 101)$	$2 \cdot 3^2 \cdot 5 \cdot 11$	$(33, 20/3, 101/3)$	110
$(9, 2)$	$(77, 36, 85)$	$2 \cdot 3^2 \cdot 7 \cdot 11$	$(77/3, 12, 85/3)$	154
$(8, 3)$	$(55, 48, 73)$	$2^3 \cdot 3 \cdot 5 \cdot 11$	$(55/2, 24, 73/2)$	330
$(7, 4)$	$(33, 56, 65)$	$2^2 \cdot 3 \cdot 7 \cdot 11$	$(33/2, 28, 65/2)$	231
$(6, 5)$	$(11, 60, 61)$	$2 \cdot 3 \cdot 5 \cdot 11$	$(11, 60, 61)$	330
$(12, 1)$	$(143, 24, 145)$	$2^2 \cdot 3 \cdot 11 \cdot 13$	$(143/2, 12, 145/2)$	429
$(11, 2)$	$(117, 44, 125)$	$2 \cdot 3^2 \cdot 11 \cdot 13$	$(39, 44/3, 125/3)$	286
$(10, 3)$	$(91, 60, 109)$	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	$(91, 60, 109)$	2730
$(9, 4)$	$(65, 72, 97)$	$2^2 \cdot 3^2 \cdot 5 \cdot 13$	$(65/6, 12, 97/6)$	65
$(8, 5)$	$(39, 80, 89)$	$2^3 \cdot 3 \cdot 5 \cdot 13$	$(39/2, 40, 89/2)$	390
$(7, 6)$	$(13, 84, 85)$	$2 \cdot 3 \cdot 7 \cdot 13$	$(13, 84, 85)$	546

Table 1

This procedure eventually lists all congruent numbers, but they do not show up in order and repetitions are possible, such as $n = 210$ and $n = 330$. This means that we cannot use this procedure to determine if a squarefree integer is not a congruent number.

Chapter 2

Elliptic curves over $\mathbb{C}$

2.1 Elliptic curves: a brief introduction

Definition 2.1. An *elliptic curve* E over a field K, written E/K is a nonsingular projective cubic curve, with a specified K-rational point $\mathcal{O}$. If K' is an extension of K then the set of points of E that have homogeneus coordinates in K' are denoted as $E(K')$.

The general equation for a cubic curve in $\mathbb{P}^2_{K'}$ is given by

$$\tilde{F}(x,y,z) = c_1x^3 + c_2y^3 + c_3z^3 + c_4x^2y + c_5x^2z + c_6xy^2 + c_7y^2z + c_8xz^2 + c_9yz^2 + c_{10}xyz = 0 \quad (2.1)$$

however, for nonsingular cubic curves, in any field this equation can be simplified using linear linear changes of variable. This is summarized in the following proposition.

Proposition 2.2. *Let K be a field and E/K an elliptic curve of the form (2.1), then:*

1. *E is isomorphic to a curve with equation*

$$y^2z + a_1xyz + a_2yz^2 = x^3 + a_3x^2z + a_4xz^2 + a_5z^3$$

2. *If $\mathrm{char}(K) \neq 2$ then E is isomorphic to a curve with equation*

$$y^2z = x^3 + a_1x^2z + a_2xz^2 + a_3z^3$$

3. *If $\mathrm{char}(K) \neq 2, 3$ the E is isomorphic to a curve with equation*

$$y^2z = x^3 + a_1xz^2 + a_2z^3$$

Either of these equations is called Weierstrass normal form.

Proof. See [8]. □

Remark 2.3. Throughout this thesis we will work using the affine equations obtained by dehomogenizing the projective equations with respect to the third coordinate, i.e., $F(x, y) = \tilde{F}(x, y, 1) = 0$. We will identifiy points $[x, y, 1]$ on the projective plane with pairs (x, y) in the affine plane. The points on the curve with third coordinate equal to zero are the *points at infinity* and we will still denote them using projective coordinates.

Example 2.4. *It's easy to check that the cubic curve* $y^2 = x^3 - n^2x$ *is nonsingular when* $\mathrm{char}(K) \nmid 2n$*, and its point at infinty is* $[0, 1, 0]$*. From now on we shall denote the curve* $y^2 = x^3 - n^2x$ *over* $\mathbb{Q}$ *by* E_n*.*

Example 2.5. *In Table 2 (see at the end of this chapter) there are some examples of elliptic curves given by a Weierstrass equation* $y^2 = x^3+a_1x+a_2$*.*

2.2 Elliptic functions

To begin our study of elliptic curves defined over $\mathbb{C}$ we first need to introduce the concept of *doubly periodic functions*.

Definition 2.6. A *lattice* in the complex plane is the set of all integral linear combinations of two given $\mathbb{R}$-linearly independent complex numbers ω_1 and ω_2. That is

$$L = \{n\omega_1 + m\omega_2 \mid n, m \in \mathbb{Z}\}$$

We shall always assume that ω_1/ω_2 has positive imaginary part. We also define the *fundamental parallelogram* for ω_1, ω_2 as

$$\Pi = \{a\omega_1 + b\omega_2 \mid 0 \leq a, b \leq 1\}$$

Definition 2.7. Let L be a lattice. An *elliptic function* relative to L is a meromorphic function $f(z)$ such that $f(z + l) = f(z)$ for all $l \in L$. The set of all elliptic functions is denoted by $\mathscr{E}_L$.

Remark 2.8. $\mathscr{E}_L$ is a subfield of the field of all meromorphic functions, moreover it is closed under differentiation.

In other words, an elliptic function is doubly periodic with periods ω_1 and ω_2. This implies that an elliptic function $f(z)$ is determined by the values it takes on the fundamental parallelogram Π and that two points on the boundary of Π that differ by a period have the same image. If we introduce the quotient topology on $\mathbb{C}$ which identifies points modulo L, the resulting topological space (which happens to be a complex manifold) is a torus, written as $\mathbb{C}/L$, thus we can think of an elliptic function as a meromorhic function defined on the torus. See Miranda [11] for more informations about meromorphic functions on Riemann surfaces.

Now we study some properties of elliptic functions.

Proposition 2.9. *A function $f(z) \in \mathscr{E}_L$ which has no pole in the fundamental parallelogram Π must be constant.*

Proof. Since Π is compact, any such function must be bounded on Π, say, by a constant M. By periodicity we have $f(z) \leq M$ for all z. The result follows by Liouville's theorem. □

Proposition 2.10. *Let $\alpha + \Pi$ denote the translate of Π by the complex number α. Suppose that $f(z) \in \mathscr{E}_L$ has no poles on the boundary C of $\alpha + \Pi$. Then the sum of the residues of $f(z)$ in $\alpha + \Pi$ is zero.*

Proof. By the residue theorem, this sum is equal to

$$\frac{1}{2\pi i} \int_C f(z)dz.$$

But the integral over opposite sides cancel. Thus the integral is zero, and so the sum of the residues is zero. □

Remark 2.11. Proposition 2.10 immediately implies that a noncostant elliptic function $f(z)$ must have at least two simple poles (or a multiple pole), since if it had a single simple pole, then the sum of the residues would not be zero.

Proposition 2.12. *Under the conditions of Proposition* 2.10*, suppose that $f(z)$ has no zeros or poles on the boundary of $\alpha + \Pi$. Let $\{m_i\}$ be the orders of the various zeros in $\alpha + \Pi$, and let $\{n_j\}$ be the orders of the various poles. Then $\sum m_i = \sum n_j$.*

Proof. Recall that the logarithmic derivative $f'(z)/f(z)$ has a simple pole precisely where $f(z)$ has a zero or pole, and the residue there is equal to the order zero or pole of the original $f(z)$, thus the sum of residues is $\sum m_i - \sum n_j$. Since $f'(z)/f(z)$ is an elliptic function we can apply Proposition 2.10 to get the result. □

We now construct a special noncostant elliptic function.

Definition 2.13. The Weierstrass *$\wp$-function* and *ζ-function* relative to the lattice L are defined by the series

$$\wp(z) = \wp(z; L) = \frac{1}{z^2} + \sum_{\substack{l \in L \\ l \neq 0}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right) \tag{2.2}$$

$$\zeta(z) = \zeta(z; L) = \frac{1}{z} + \sum_{\substack{l \in L \\ l \neq 0}} \left(\frac{1}{(z-l)} + \frac{1}{l} + \frac{z}{l^2} \right) \tag{2.3}$$

Proposition 2.14. *The sums in (2.2) and (2.3) converge absolutely and uniformly for z in any compact subset of $\mathbb{C} - L$.*

Proof. See [9]. □

Proposition 2.15. *$\wp(z) \in \mathscr{E}_L$, and its only pole is a double pole at each lattice point.*

Proof. From Proposition 2.14 follows that 2.2 defines a holomorphic function on $\mathbb{C} - L$ and from the series expansion is clear that $\wp(z)$ has a double pole with residue zero at each lattice point. Next, note that $\wp(z) = \wp(-z)$ (to see why just replace l with $-l$ in the sum). To prove double periodicity we look at the derivative. Since the series for $\wp(z)$ is uniformly convergent, we can compute $\wp'(z)$ by termwise differentiation:

$$\wp'(z) = -2 \sum_{l \in L} \frac{1}{(z-l)^3}.$$

Now $\wp'(z)$ is clearly doubly periodic, thus $\wp'(z) \in \mathscr{E}_L$. To prove that $\wp(z) \in \mathscr{E}_L$ we integrate $\wp'(z+l)$ for a fixed $l \in L$: $\wp(z+l) = \wp(z) + C(l)$, where $C(l)$ is a constant independent of z. Now let $z = -l/2$ and using the fact that $\wp$ is an even function we conclude that $C(l) = \wp(l/2) - \wp(-l/2) = 0$. This concludes the proof. □

Remark 2.16. Observe that

1. $\zeta'(z) = -\wp(z)$.
2. $\zeta(z)$ is not an elliptic function as it is not doubly periodic.
3. We can prove in the same way as $\wp(z)$ that $\zeta(z)$ defines a holomorphic function on $\mathbb{C} - L$ and that its poles are simple poles at each lattice point.

Since $\wp(z)$ has exactly one double pole in a fundamental domain of the form $\alpha+\Pi$, by Proposition 2.12 it has exactly simple two zeros or one double zero there. It is not hard to show that $\wp(z)$ takes every value $u \in \mathbb{C} \cup \{\infty\}$ exactly twice on the torus, counting multiplicity. Indeed if $u = \infty$ then it suffices to take $z = 0$ since that is the only double pole of $\wp(z)$ in Π, whereas if $u \in \mathbb{C}$ then $f(z) = \wp(z) - u$ is an elliptic function relative to the same lattice, with the same poles as $\wp(z)$. Thus $f(z)$ either has two simple zeros or a double zero in Π. We can also find the values for u such that $f(z)$ has a double zero. Let $l \in L$ be such that $l/2 \notin L$, then since $\wp'(z)$ is odd we have $\wp'(l/2) = -\wp'(-l/2) = -\wp'(l/2)$, so $\wp'(l/2) = 0$. In Π the only such points are $\omega_1/2,\ \omega_2/2,\ (\omega_1+\omega_2)/2$. We set $e_1 = \wp(\omega_1/2),\ e_2 = \wp(\omega_2/2)$, and $e_3 = \wp(\omega_1+\omega_2)/2$, these are the values of u for which $\wp(z) - u$ has a double zero. Notice that e_1, e_2, e_3 are all distinct because otherwise $\wp'(z)$ would have a double zero and $\wp(z) - u$ would have a triple zero, which is impossible.

This tells us that $\wp(z)$ is a degree 2 meromorphic map from the torus $\mathbb{C}/L$ to the Riemann sphere $\mathbb{C} \cup \{\infty\}$ having branch points. at e_1, e_2, e_3, ∞.

2.3 The field of elliptic functions

In the next proposition we explain the structure of the field of elliptic functions $\mathscr{E}_L$.

Proposition 2.17. *$\mathscr{E}_L = \mathbb{C}(\wp, \wp')$, i.e., any elliptic function for L is a rational expression in $\wp(z; L)$ and $\wp'(z; L)$. More precisely, given $f(z) \in \mathscr{E}_L$, there exist two rational functions $g(X), h(X)$ such that*

$$f(z) = g(\wp(z)) + \wp'(z)h(\wp(z)).$$

Proof. If $f(z)$ is an elliptic function for L, then so are the two even functions

$$\frac{f(z)+f(-z)}{2} \qquad \text{and} \qquad \frac{f(z)-f(-z)}{2\wp'(z)}.$$

Since $f(z)$ is equal to the first of these functions plus $\wp'(z)$ times the second, to prove the proposition it suffices to prove that $\mathscr{E}_L^+$, the subfield of $\mathscr{E}_L$ of even elliptic functions relative to L, is generated by $\wp(z)$. To do this we are going to construct a function which has the same zeros and poles as $f(z)$ using only functions of the form $\wp(z)-u$ with u a costant. The ratio of $f(z)$ to such a function is an elliptic function with no poles, an so must be constant by Proposition 2.9.

Let $f(z) \in \mathscr{E}_L^+$, then 0 has even order, say $2m$, and $f(z) = \wp(z)^{-m}g(z)$, where $g(z)$ is an even elliptic function with no zeros or poles on the associated lattice L. If a is a zero of $\wp(z)-u$, then so is $l-a$ for $l \in L$, and if a is a zero or pole of $g(z)$, then so is $l-a$. If $2a \in L$, then the zero (or pole) is of order at least 2 since $g'(z) = -g'(z)$ and so $g'(a) = g'(-a) = -g'(a)$. Thus

$$g(z) = c \cdot \frac{\Pi_i(\wp(z)-\wp(a_i))^{m_i}}{\Pi_j(\wp(z)-\wp(b_j))^{n_j}}$$

where $\{a_i, l-a_i\}$ are the zeros of $g(z)$ and $\{b_j, l-b_j\}$ are the poles of $g(z)$ in its fundamental domain, and m_i, n_j are the respective multiplicities. This proves the theorem. □

2.4 The Weierstrass form of an elliptic curve

From the proof of Proposition 2.17 follows that the even function $\wp'(z)^2$ is equal to a cubic polynomial in $\wp(z)$, since $\wp'(z)$ has a triple pole in 0 and three simple zeros. More precisely we know that $\wp'(z)^2$ has a double zero at $\omega_1/2,\ \omega_2/2,\ (\omega_1+\omega_2)/2$. Hence we have

$$\begin{aligned}\wp'(z)^2 &= C \cdot (\wp(z)-\wp(\omega_1/2)) \cdot (\wp(z)-\wp(\omega_2/2)) \cdot (\wp(z)-\wp((\omega_1+\omega_2)/2)) \\ &= C \cdot (\wp(z)-e_1) \cdot (\wp(z)-e_2) \cdot (\wp(z)-e_3)\end{aligned}$$

where C is some constant. We can easily find C by comparing the coefficients of the lowest power of z in the Laurent expansion at the origin. On the left side the leading term is $4z^{-6}$ while at the right side we have $C(z^{-2})^3$, thus $C=4$. Hence $\wp(z)$ satisfies the differential equation

$$\wp'(z)^2 = f(\wp(z)), \quad \text{where} \quad f(x) = 4(x-e_1)(x-e_2)(x-e_3) \in \mathbb{C}[x]. \tag{2.4}$$

We now give an alternative derivation of the differential equation by finding a cubic polynomial $f(x)$ such that the negative powers of the Laurent expansion of $f(\wp(z))$ at 0 coincide with the one of $\wp'(z)^2$. By Proposition 2.9 $f(\wp(z))$ and $\wp'(z)^2$ differ only by a constant, and that constant is zero if we suitably choose the constant term in $f(x)$.

In what follows the lattice $L = \{m\omega_1 + n\omega_2\}$ is fixed. We consider the Laurent expansion of $\zeta(z), \wp(z)$ and $\wp'(z)$ at the origin. From the geometric series we have

$$\frac{1}{z-l} = -\frac{1}{l}\sum_{n\geq 0}\left(\frac{z}{l}\right)^n \qquad \text{and} \qquad \frac{1}{z-l} + \frac{1}{l} + \frac{z}{l^2} = -\frac{1}{l}\sum_{n\geq 2}\left(\frac{z}{l}\right)^n$$

which converge for $|z| < |l|$. Thus

$$\begin{aligned}\zeta(z) &= \frac{1}{z} + \sum_{\substack{l\in L\\ l\neq 0}}\left(\frac{1}{z-l} + \frac{1}{l} + \frac{z}{l^2}\right)\\ &= \frac{1}{z} - \sum_{n\geq 2} z^n \sum_{\substack{l\in L\\ l\neq 0}} \frac{1}{l^{n+1}}.\end{aligned}$$

Observe that if n is even, then $\sum \frac{1}{l^{n+1}}$ is zero, so if we let $G_k(L) = \sum_{l\in L-0} l^{-2k}$, then

$$\zeta(z) = \frac{1}{z} - \sum_{k\geq 2} G_k(L) z^{2k-1}.$$

The sum that defines $G_k(L)$ converges for $k \geq 2$.

Finally we can derive the Laurent series for $\wp(z)$ and $\wp'(z)$ by differentiating the series for $-\zeta(z)$:

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + \sum_{k\geq 2} G_k(L)(2k-1)z^{2k-2},\\ \wp'(z) &= \frac{-2}{z^3} + \sum_{k\geq 2} G_k(L)(2k-1)(2k-2)z^{2k-3}.\end{aligned}$$

In order to derive the differential equation for $\wp(z)$ we write out the first few terms of the expansion at 0 for the elliptic functions $\wp(z), \wp'(z)$, and

various combinations of these functions:

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + 3G_2 z^2 + 5G_3 z^4 + \cdots, \\
\wp'(z) &= \frac{-2}{z^3} + 6G_2 z + 20G_3 z^3 + \cdots, \\
\wp'(z)^2 &= \frac{4}{z^6} - \frac{24G_2}{z^2} - 80G_3 + \cdots, \\
4\wp(z)^3 &= \frac{4}{z^6} + \frac{36G_2}{z^2} + 60G_3 + \cdots, \\
60G_2\wp(z) &= \frac{60G_2}{z^2} + 180G_2^2 z^2 + \cdots,
\end{aligned}$$

Hence the following equation

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_2\wp(z) - 140G_3.$$

It is standard notation to set

$$\begin{aligned}
g_2 = g_2(L) &= 60G_4 = 60 \sum_{\substack{l \in L \\ l \neq 0}} l^{-4}, \\
g_3 = g_3(L) &= 140G_6 = 140 \sum_{\substack{l \in L \\ l \neq 0}} l^{-6}.
\end{aligned}$$

We have thereby derived a second form for the differential equation (2.4):

$$\wp'(z) = f(\wp(z)), \qquad \text{where} \qquad f(x) = 4x^3 - g_2 x - g_3 \in \mathbb{C}[x]. \tag{2.5}$$

This last equation has an elegant geometric interpretation. Suppose that we take the function from the torus $\mathbb{C}/L$ to $\mathbb{P}^2_{\mathbb{C}}$ defined by

$$\begin{cases} z \mapsto [\wp(z),\ \wp'(z),\ 1] & \text{for} \quad z \neq 0 \\ 0 \mapsto \mathcal{O} := [0, 1, 0] \end{cases} \tag{2.6}$$

The image of any nonzero point z of $\mathbb{C}/L$ is a point in the affine plane (with complex coordinates) whose x-coordinate and y-coordinate satisfy the relationship $y^2 = f(x)$ because of (2.5). The image of 0 in $\mathbb{C}/L$ is the point at infinty. Thus, every point in $\mathbb{C}/L$ maps to a point on the curve $y^2 = f(x)$ in the complex projective plane, which happens to be an elliptic curve since its roots, namely e_1, e_2, e_3 are distinct. It's not hard to

show that this map is a one-to-one correspondence between $\mathbb{C}/L$ and the elliptic curve. Moreover this map is analytic because near nonzero points the map is given by $z \mapsto [\wp(z), \wp'(z), 1)]$ and near zero the map is given by $z \mapsto [\wp(z)/\wp'(z), 1, 1\wp'(z)]$. We have proved the following proposition.

Proposition 2.18. *The map (2.6) is an analytic one-to-one correspondence between the torus $\mathbb{C}/L$ and the elliptic curve $y^2 = 4x^3 - g_2(L)x - g_3(L)$ in $\mathbb{P}^2_{\mathbb{C}}$.*

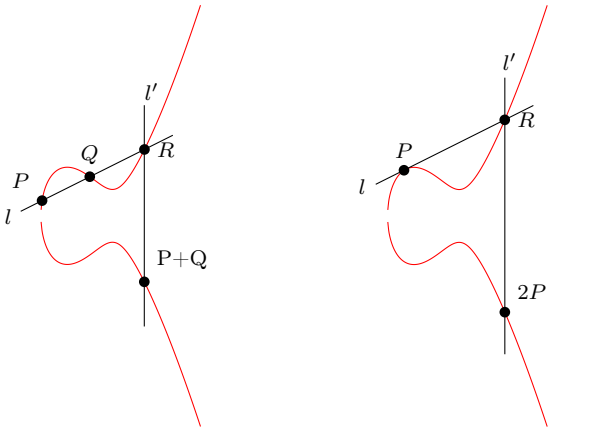
Remark 2.19. Every elliptic curve E_n has an associated lattice which is a multiple of the Gaussian integers $\mathbb{Z}[i]$. In particular we have that $\omega_1 = i\omega_2$ and thus $L = \omega_2\mathbb{Z}[i]$. See Silvermann [7] and Miranda [11] for more details on periods of Abelian varieties.

2.5 The group law

2.5.1 General definition

Let K be a field, E an elliptic curve defined over K given by a Weierstrass equation and let $\mathcal{O} \in E$ be a K-rational point. By Bézout theorem we have that a line $l \subseteq \mathbb{P}^2_K$ intersects E in three points (counted with multiplicity). We define a composition law on E by the following rule.

Definition 2.20 (Composition law)**.** Let $P, Q \in E$ and $l = P \vee Q$ be the line connecting P and Q (if $P = Q$ then l is the tangent line at E in P). Let $R \in E$ be the third point of intersection of l with E and let l' be the line connecting R and $\mathcal{O}$. We define $P + Q$ to be third point of intersection of the line l' with E.



Case $P \neq Q$ Case $P = Q$

We now prove that $(E, +, O)$ is an abelian group.

Theorem 2.21. *The composition law (2.20) has the following properties:*

(a) If a line l intersects E in three points (counted with multiplicity) P, Q, R, then

$$(P + Q) + R = \mathcal{O}$$

(b) $P + \mathcal{O} = P$ for all $P \in E$.

(c) $P + Q = Q + P$ for all $P, Q \in E$.

(d) Let $P \in E$. There is a point of E, that we denote as $-P$, such that $P + (-P) = \mathcal{O}$.

(e) Let $P, Q, R \in E$. Then

$$(P + Q) + R = P + (Q + R).$$

Proof. (a) Follows immediatley from the definition.
(b) If we take $Q = \mathcal{O}$ in Definition 2.20 then the line l coincides with l'. The former intersects E at $P, \mathcal{O}, R$, and the latter at $R, \mathcal{O}, P+O$, so $P+\mathcal{O} = P$.
(c) Trivial, since the construction in Definition 2.20 is symmetric in P and Q.
(d) Let the line through P and $\mathcal{O}$ also intersect E at R. Then using (a) and (b) we have

$$\mathcal{O} = (P + \mathcal{O}) + R = P + R$$

(e) See [7]. □

Example 2.22. *Let K be a field with* $\mathrm{char}(K) \neq 2$ *and let E be an elliptic curve over K defined by Weierstrass equation*

$$g(x, y) = y^2 - ax^3 - bx^2 - cx - d = 0.$$

We calculate the points of order two, i.e., those points P such that $2P = \mathcal{O}$. Before proceeding with the calculations observe that the line tangent to E at P must meet E at $-\mathcal{O}$, but that is $\mathcal{O}$ itself.

We first calculate the equation of the line tangent to a point of E and to do so we use homogeneus coordinates, hence let $G(x, y, z) = z^3 g(x/z, y/z)$

be the homogeneization of $g(x, y)$. If $P = [x_0, y_0, z_0]$ is a point on the curve then the line tangent to E at P is defined by the equation

$$t_P : \frac{\partial G}{\partial x}(P)x + \frac{\partial G}{\partial y}(P)y + \frac{\partial G}{\partial z}(P)z = 0.$$

By our previous observation the point $\mathcal{O} = [0, 1, 0]$ must lie on t_P, this forces

$$\frac{\partial G}{\partial y}(P) = 0 \qquad \Longleftrightarrow \qquad 2y_0z_0 = 0.$$

If $z_0 = 0$ we find the point $\mathcal{O}$, whereas if $y_0 = 0$ we find $P = [x_0, 0, 1]$. These points also lie on the curve if and only if

$$G(x_0, 0, 1) = -(ax_0^3 + bx_0^2 + cx_0 + d) = 0.$$

This shows that the only nontrivial points of order two are precisely those with y-coordinate equal to zero. Thus for example, on the curves we are cosindering, namely $E_n : y^2 = x^3 - n^2x$, the points of order two are the point at infinity, $(0, 0), (n, 0)$ and $(-n, 0)$.

Remark 2.23. Let K be a field and let K'/K be an extension. Let E be an elliptic curve defined over K and consider two K'-rational points $P_1 = (x_1,\ y_1)$ and $P_2 = (x_2, y_2)$. Then the coordinates of the point $P_1 + P_2$ are given by rational functions of the coordinates of P_1 and P_2. This means that the third point also has coordinates in K' and thus we have the following inclusion of groups: $E(K) \leq E(K')$.

From the arithmetic point of view, the most interesting cases are those in which K is a number field. If that's the case then we have the following theorem, proved by Mordell in the case of elliptic curves defined over $\mathbb{Q}$ and later generalised by Weil to Abelian varieties over any number field.

Theorem 2.24 (Mordell-Weil)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Then the group $E(\mathbb{Q})$ is finitely generated.*

This theorem tells us that $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$, where $E(\mathbb{Q})_{\text{tors}}$ is the torsion subgroup, and the nonnegative integer r is called the *rank* of the curve E. Currently we have at disposition tools to study $E(\mathbb{Q})_{\text{tors}}$, such as the Nagell-Lutz theorem which provides an effective way to compute it. Barry Mazur in [10] characterized all the possible isomorphism classes of $E(\mathbb{Q})_{\text{tors}}$. The study of the elements of infinite order is much more difficult.

The study of the group $E(\mathbb{Q})$, called the Mordell-Weil group of the curve, turns out to be crucial step in our study of the Congruent Number Problem.

2.5.2 The group law for elliptic curves over $\mathbb{C}$

When an elliptic curve E is defined over $\mathbb{C}$ we can give an alternative definition for the group law. In fact we have a natural way of adding points in $\mathbb{C}/L$, that is ordinary addition modulo L. The structure of additive group of $\mathbb{C}/L$ can be carried over the curve $y^2 = 4x^3 - g_2(L)x - g_3(L)$ through the analytic map defined in (2.6), i.e., given two points $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ of E, let z_1, z_2 be two points of $\mathbb{C}/L$ such that $P_1 = (\wp(z_1), \wp'(z_1))$ and $P_2 = (\wp(z_2), \wp'(z_2))$, and then set

$$P_1 + P_2 = (\wp(z_1 + z_2),\ \wp'(z_1 + z_2)) = (\wp(z_3), \wp'(z_3)).$$

Now we prove that this definition of the group law leads to the same geometric interpretation. We first prove that the definition of additive inverse coincide.

The additive identity is $\wp(0) = P_0 = \mathcal{O}$ since clearly we have that $P_z + P_0 = P_z$ for any z. Now suppose that P_{z_1} and P_{z_2} are two distinct points of E having the same x-coordinate. Observe that this only happens when $z_1 = -z_2$ due to the simmetries of $\wp$ and $\wp'$. Thus we have that $P_{z_1} + P_{z_2} = \mathcal{O}$ and this is totally coherent with the geometric definition given in Definition 2.20.

Thus we have proved the following proposition.

Proposition 2.25. *The additive inverse of (x, y) is $(x, -y)$.*

We shall now consider the case where neither $P_1 = P_{z_1}$ nor $P_2 = P_{z_2}$ is the identity point $\mathcal{O}$ and also $P_1 \neq -P_2$. Given two such points there is always a line joining them. If $P_1 = P_2$ we take the tangent line to the elliptic curve E at P_1. We claim that the third point of intersection of $l = P_1 \vee P_2$ with E is $-P_3 = (x_3, -y_3)$ where $P_3 = P_1 + P_2$, i.e., the second definition of the group law again coincides with the geometric one.

Proposition 2.26. *If $P_3 = P_1 + P_2$, then $-P_3$ is the third point of intersection of $l = P_1 \vee P_2$ with the elliptic curve. If $P_1 = P_2$ then by $P_1 \vee P_2$ we mean the tangent line at P_1.*

Proof. See [9]. □

We can esily turn this geometric procedure into formulas. Let E be and elliptic curve over a field K with $\mathrm{char}(K) \neq 2$, then E has Weierstrass normal

form $y^2 = f(x)$ where $f(x) = ax^3 + bx^2 + cx + d$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on the curve, and $P_3 = P_1 + P_2 = (x_3, y_3)$. We already considered the cases in which P_1 or P_2 is $\mathcal{O}$, and $P_1 + P_2 = \mathcal{O}$, so now we suppose that neither P_1 nor P_2 is the point at infinity and that they are not opposites. In this case the line through P_1 and P_2 has equation of the form $y = mx + \beta$, where $\beta = y_1 - mx_1$ and $m = (y_2 - y_1)/(x_2 - x_1)$ if $P_1 \neq P_2$, otherwise $m = f'(x_1)/2y_1$. Let's do the calculations in the first case:

$$\begin{aligned} y^2 &= m^2x^2 + \beta^2 + 2m\beta x \\ &= m^2x^2 + (2my_1 - 2m^2x_1)x + y_1^2 + m^2x_1^2 - 2mx_1y_1. \end{aligned}$$

Knowing that x_1 and x_2 are two distinct roots of $f(x) - (mx + \beta)^2$ and that the coefficient of x^2 is $-(x_1 + x_2 + x_3)$ divided by the leading coefficient we can calculate x_3:

$$f(x) - (mx + \beta)^2 = ax_3 + (b - m^2)x^2 + \cdots \qquad \text{and thus}$$

$$x_3 = -x_1 - x_2 + \frac{1}{a}(m^2 - b) = -x_1 - x_2 - \frac{b}{a} + \frac{1}{a}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2.$$

While if $P_1 = P_2$ we get

$$x_3 = -2x_1 - \frac{b}{a} + \frac{1}{a}\left(\frac{f'(x_1)}{2y_1}\right)^2.$$

So, to get P_3 we only have to reflect the third point of intersection. Thus $P_3 = (x_3, y_3)$ where $y_3 = -mx_3 - \beta$.

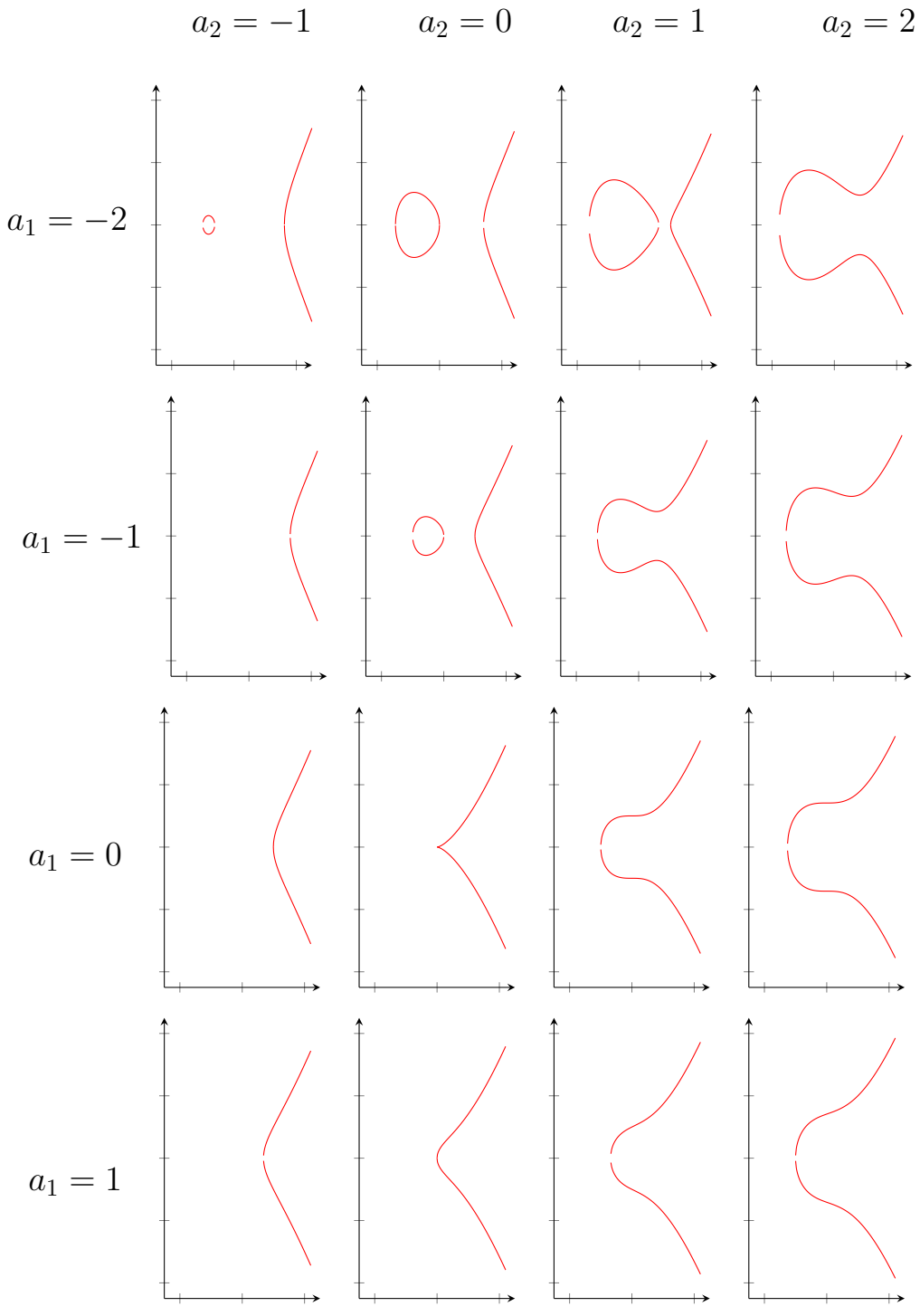
To conclude this section we characterize points of finite order of elliptic curves over $\mathbb{C}$. These are the points for which there exists a nonnegative integer N such that $NP = \mathcal{O}$. Let $y^2 = 4x^3 - g_2(L)x - g_3(L)$ be an elliptic curve associated to the lattice $L = \{m\omega_1 + n\omega_2\}$. Let $z \in \mathbb{C}/L$ and $P = (\wp(z), \wp'(z))$. According to the second interpretation of the group law we have that

$$NP = \mathcal{O} \qquad \text{if and only if} \qquad Nz \in L.$$

The only such points on the torus are those of the form $\frac{a}{N}\omega_1 + \frac{b}{N}\omega_2$ with $0 \leq a, b < N$, thus taking their image under (2.6) gives all the points whose order divides N.

Table 2

Here some examples of elliptic curves given by Weierstrass equation $y^2 = x^3 + a_1x + a_2$. Notice that when $a_1 = 0$ and $a_2 = 0$ the curve is not smooth, hence it is not an elliptic curve.



Chapter 3

Elliptic curves over finite fields

In this chapter we give some notions about elliptic curves defined over a finite field $K = \mathbb{F}_q$ where $q = p^r$ for some prime p and positive integer r. For our purposes we can suppose $\text{char}(K) \neq 2$, so any elliptic curve over K has Weierstrass normal form

$$y^2 = f(x) \qquad \text{where} \qquad f(x) = ax^3 + bx^2 + cx + d.$$

The addition law described in Section 2.1 still makes sense since it does not rely on the field, so for E defined over $\mathbb{F}_q$, the set $E(\mathbb{F}_{q^r})$ of all points with coordinates in $\mathbb{F}_{q^r}$ is still an Abelian group for all $r \geq 1$, in particular it is finte since elliptic curves over $\mathbb{F}_q$ have a finite number of points. It is natural to ask what the size of this group is (recall that $\text{char}(K) \neq 2$). Intuitively, if $f(x) = 0$ then the only solution is $y = 0$. Otherwise, it is known that among the nonzero elements of K half of them are quadratic residues and half of them are not. So each value for x yields either one solution or has a 50% probability of producing two solutions and 50% probability of producing no solution. So for q values of x we expect approximately q solutions, and then include the point at infinty $\mathcal{O}$. This heuristic argument does not costitute a proof, but it turns out that is not far from the truth. A theorem proved by Hasse for elliptic curves and later generalized by Weil summarizes this argument. For a proof see Silvermann [7].

Theorem 3.1 (Hasse-Weil Theorem)**.** *Let E/K be an elliptic curve defined over the finite field with q elements. Then*

$$|\#E(K) - q - 1| \leq 2\sqrt{q}.$$

3.1 Reduction mod p

Definition 3.2. Let $\mathbb{P}^2_{\mathbb{Q}}$ be the projective plane over the rational numbers. We say that a homogeneous coordinate triple (A, B, C) is *normalized* if A, B, C are integers with no common divisor.

Let p be a fixed prime number, and for each integer $m \in \mathbb{Z}$ let $\bar{m} \in \mathbb{F}_p$ denote its residue modulo p. If $[l, m, n]$ is a normalized coordinate triple for a point $P \in \mathbb{P}^2_{\mathbb{Q}}$, then the triple $[\bar{l}, \bar{m}, \bar{n}]$ defines a point $\bar{P}$ in $\mathbb{P}^2_{F_p}$, since at least one of the numbers l, m, n is not divisible by p. Since the point P determines the triple $[l, m, n]$ up to sign, the point $\bar{P}$ depends only on P, not on the choice of coordinates for P. Thus $P \mapsto \bar{P}$ gives a well-defined map

$$r_p : \mathbb{P}^2_{\mathbb{Q}} \longrightarrow \mathbb{P}^2_{\mathbb{F}_p}, \qquad P \mapsto \bar{P}$$

called the *reduction* mod p *map*.

Now let $C/\mathbb{Q}$ be a curve defined by an equation F with rational coefficients. Without loss of generality we can suppose that these coefficients are integers with no common divisor. Then $\bar{F}$, the polynomial that we obtain by reducing the coefficients of F modulo p, is non-zero and defines a curve $\bar{C}$ in characteristic p. Its points are obtained by reducing the points of C as we saw before.

In the case of elliptic curves $E/\mathbb{Q}$ we need to pay attention to whether or not the reduced curve $\bar{E}$ modulo some prime p is still an elliptic curve (i.e. is still nonsigular).

Definition 3.3. Let $E/\mathbb{Q}$ be a rational elliptic curve. Let p be a fixed prime and let $\bar{E}$ be the reduced curve. We say that E has *good reduction* at p if $\bar{E}$ is nonsingular and thus defines an elliptic curve $\bar{E}/\mathbb{F}_p$, E has *bad reduction* at p otherwise.

Checking if a curve E has good or bad reduction at some prime p is easy. Assuming that all the coefficients of its defining equation are integers with no common factor, we just need to check if the discriminant of the equation is divisible by p. If that's the case then the curve will be singular once reduced, and nonsigular otherwise.

Example 3.4. *Consider the curve $E_n : y^2 = x^3 - n^2x$. The discriminant is equal to $4n^6$. Thus the curve has good reduction at every prime p that does not divide $2n$.*

Proposition 3.5. *The restriction of r_p from $E(\mathbb{Q})$ to $\bar{E}(\mathbb{F}_p)$ is a group homomorphism if p is a prime of good reduction.*

Proof. Clearly $r_p([0,1,0]) = [0,1,0]$. Let P, Q be two distinct points of $E(\mathbb{Q})$ and let $l_{PQ} = P \vee Q$. We have that $\bar{l} = r_p(l_{PQ}) = l_{\bar{P}\bar{Q}}$, thus the third point of intersection between $\bar{E}$ and $\bar{l}$ is the reduction of the third point of intersection between E and l. This means that $-(\bar{P}+\bar{Q}) = \overline{-(P+Q)} = -\overline{(P+Q)}$ and so $\overline{P+Q} = \bar{P}+\bar{Q}$. The same argument applies if $P = Q$ and l is the line tangent to E at P. □

In the next chapter we will go back to the Congruent Number Problem apply what we saw in the last chapters.

Chapter 4

Congruent numbers and the rank of E_n

In this chapter we show that a squarefree positive n is a congruent number if and only if the corresponding curve E_n has positive rank.

We need to compute the torsion subgroup $E_n(\mathbb{Q})_{\text{tors}}$, and to do so we first calculate the number of points in $\bar{E}_n$ over $\mathbb{F}_q$ for some specific prime powers $q = p^r$.

Lemma 4.1. *Suppose that $q \equiv 3 (\text{mod } 4)$. Then -1 is not a square modulo q.*

Proof. If -1 was a square modulo q then the polynomial $f(x) = x^4 - 1$ would split in $\mathbb{F}_q$, in particular there would be a fourth root of unity α in $\mathbb{F}_q$. Thus the order of the cyclic group generated by α divides the order of $\mathbb{F}_q^*$, i.e., $4 \mid (q-1)$. This is impossible since $q - 1 \equiv 2 (\text{mod } 4)$. □

Proposition 4.2. *Let $q = p^r$, $p \nmid 2n$. Suppose that $q \equiv 3 (\text{mod } 4)$. Then there are $q + 1$ points over $\mathbb{F}_q$ on the elliptic curve $y^2 = x^3 - n^2 x$.*

Proof. We saw in Chapter 2 that there are four points of order 2: the point at infinity, $(0, 0)$ and $(\pm n, 0)$. We now count all the pairs (x, y) where $x \notin \{0, n, -n\}$. We arrange these $q - 3$ x's in pairs $x, -x$. Since $f(x) = x^3 - n^2 x$ is an odd function and, by Lemma 4.1, -1 is not a square in $\mathbb{F}_q$, it follows that exactly one of the two elements $f(x)$ and $f(-x) = -f(x)$ is a square in $\mathbb{F}_q$. In both cases we obtain exactly two points $(x, \pm\sqrt{f(x)})$ or else $(-x, \pm\sqrt{f(-x)})$. Thus, the $(q-3)/2$ pairs give us $q - 3$ points. Along with the four points of order two, we have in all $q + 1$ points over $\mathbb{F}_q$, as claimed. □

Next we compute the torsion subgroup of E_n. The idea is to show that the reduction modulo p homomorphism from $E_n(\mathbb{Q})_{\text{tors}}$ to $E_n(\mathbb{F}_p)$ is injective

for all p sufficiently large primes of good reduction. For such p's we have $\#E_n(\mathbb{Q})_{\text{tors}} \mid \#E_n(\mathbb{F}_p)$. This forces $\#E_n(\mathbb{Q})_{\text{tors}} \leq 4$ since $\#E_n(\mathbb{F}_p)$ runs through all prime numbers of the form $p+1$ for $p \equiv 3 (\text{mod } 4)$.

Proposition 4.3. $\#E_n(\mathbb{Q})_{\text{tors}} = 4$.

The following lemma is needed to prove Proposition 4.3.

Lemma 4.4. *Let p be a prime number and let*

$$P_1 = [x_1, y_1, z_1] \quad \textit{and} \quad P_2 = [x_2, y_2, z_2]$$

be two points in $\mathbb{P}^2_{\mathbb{Q}}$ with normalized coordinates. Denote with $\bar{P}_1 = [\bar{x}_1, \bar{y}_1, \bar{z}_1]$, $\bar{P}_2 = [\bar{x}_2, \bar{y}_2, \bar{z}_2]$ their reduction modulo p as defined in the previous chapter. Then $\bar{P}_1 = \bar{P}_2$ if and only if p divides the coordinates of the cross-product of P_1 and P_2, namely the real vector

$$(y_1 z_2 - y_2 z_1,\ x_2 z_1 - x_1 z_2,\ x_1 y_2 - x_2 y_1).$$

Proof of Lemma 4.4. First suppose the p divides the cross-product. We consider two cases:

1. p divides x_1. Then p divides $x_2 z_1$ and $x_2 y_1$, and therefore divides x_2, because it cannot divide x_1, y_1 and z_1. Suppose, for example that $p \nmid y_1$. Then

   $$\bar{P}_2 = [0,\ \bar{y}_1\bar{y}_2,\ \bar{y}_1\bar{z}_2] = [0,\ \bar{y}_1\bar{y}_2,\ \bar{y}_2\bar{z}_1] = [0, \bar{y}_1, \bar{z}_1] = \bar{P}_1$$

   (where we used the fact that p divides $y_1 z_2 - y_2 z_1$). An analogous argument will apply if $p \nmid z_1$.

2. p does not divide x_1. Then

   $$\bar{P}_2 = [\bar{x}_1\bar{x}_2,\ \bar{x}_1\bar{y}_2,\ \bar{x}_1\bar{z}_2] = [\bar{x}_1\bar{x}_2,\ \bar{x}_2\bar{y}_1,\ \bar{x}_2\bar{z}_1] = [\bar{x}_1, \bar{y}_1, \bar{z}_1] = \bar{P}_1.$$

Conversely, suppose that $\bar{P}_1 = \bar{P}_2$ and that $p \nmid x_1$ (an analogous argument will apply if $p \nmid y_1$ or $p \nmid z_1$). Then since $\bar{P}_1 = (\bar{x}_2, \bar{y}_2, \bar{z}_2)$, we also have $p \nmid x_2$. Hence,

$$(\bar{x}_1\bar{x}_2,\ \bar{x}_1\bar{y}_2,\ \bar{x}_1\bar{z}_2) = \bar{P}_2 = \bar{P}_1 = (\bar{x}_1\bar{x}_2,\ \bar{x}_2\bar{y}_1,\ \bar{x}_2\bar{z}_1).$$

Since the first coordinate are the same, these two points can be equal only if the second and third coordinates are equal, i.e., if p divides $x_1 y_2 - x_2 y_1$

and $x_1z_2 - x_2z_1$. Finally, we must show that p divides $y_1z_2 - y_2z_1$. If both y_1 and z_1 are divisible by p, then this is trivial. Otherwise, the conclusion will follow by repeating the above argument with x_1, x_2 replaced by y_1, y_2 or z_1, z_2. This concludes the proof of the lemma. □

Proof of Proposition 4.3. We determine when reduction modulo p is not injective. Suppose that the proposition is false, i.e., that $E_n(\mathbb{Q})$ contains a point of finite order grater than 2. Then either it contains an element of odd order, or else the group of points of order 4 contains either 8 or 16 elements. In either case we have a subgroup $S = \{P_1, P_2, \ldots, P_m\}$ of $E_n(\mathbb{Q})_{\text{tors}}$ where $m = \#S$ is either 8 or else an odd number. Let us write all of the points $P_i, i = 1, \ldots, m$ as in Lemma 4.4: $P_i = (x_i, y_i, z_i)$. For each pair of points P_i, P_j, consider the cross-product vector $(y_iz_j - y_jz_i,\ x_jz_i - x_iz_j,\ x_iy_j - x_jy_i) \in \mathbb{R}^3$. Since P_i and P_j are distinct points, as vectors in $\mathbb{R}^3$ they are not proportional, and so their cross-product is not the zero vector. Let n_{ij} be the greatest common divisor of the coordinates of the cross-product. According to Lemma 4.4, the points P_i and P_j have the same image $\bar{P}_i = \bar{P}_j$ in $E_n(\mathbb{F}_p)$ if and only if p divides n_{ij}. Thus if p is a prime of good reduction which is greater than all of the n_{ij}, it follows that all the images are distinct, i.e., the map reduction modulo p gives an injection of S in $E_n(\mathbb{F}_p)$.

This means that for all but finitely many p the number m must divide $\#E_n(\mathbb{F}_p)$, because the image of S is a subgroup of order m. Then for all but finitely primes congruent to 3 modulo 4, by Proposition 4.2 we must have $p \equiv -1 (\text{mod } m)$. But this contradicts Dirichlet's theorem on primes in arithmetic progression. Namely, if $m = 8$ this would mean that there are only finitely many primes of the form $8k + 3$. If m is odd, it would mean that there are only finitely many primes of the form $4mk + 3$ (if $3 \nmid m$), and that there are only finitely many primes of the form $12k + 7$ if $3 \mid m$. In all cases, Dirichlet's theorem tells us that there are infinitely many primes of the given type. This concludes the proof of the proposition. □

We are now ready to prove the main result.

Lemma 4.5. *Let $P = (x_P, y_P)$ be a rational point on the curve E_n. Then the x-coordinate of $2P$ is the square of a rational number having even denominator.*

Proof. Using the formulas we saw in section 2.4 we have that

$$x_{2P} = -2x_P + \left(\frac{f'(x_P)}{2y_P}\right)^2 = -2x_P + \frac{(3x_P^2 - n^2)^2}{(2y_P)^2}$$
$$= \left(\frac{x_P^2 + n^2}{2y_P}\right)^2$$

where we used the relation $y_P^2 = x_P^3 - n^2 x_P$. □

Theorem 4.6. *A squarefree positive integer n is a congruent number if and only if $E_n(\mathbb{Q})$ has positive rank.*

Proof. Suppose that n is a congruent number. Then there exists a rational right triangle with area n that corresponds to a nontrivial rational point on the curve E_n (in particular the x-coordinate is the square of a nonzero rational number). By Proposition 4.3 this point must be a point of infinite order and thus E_n has nonzero rank. Conversely, suppose that E_n has positivie rank and let $P = (x_P, y_P)$ be a point of infinite order (in particular P has not order 2). By Lemma 4.5 the x-coordinate of $2P$ is the square of a rational number having even denominator, hence we can conclude by Proposition 1.4. □

Example 4.7. *In Chapter 1 we proved that* 1 *is not a congruent number. By the above theorem we have that the curve $E_1 : y^2 = x^3 - x$ has rank* 0*.*

Denote with $2E_n(\mathbb{Q}) \setminus \{\mathcal{O}\}$ the set $\{2P \mid P \in E_n(\mathbb{Q}),\ 2P \neq \mathcal{O}\}$. Now we explore in more detail the relationship between rational right trangles with area n and rational points of infinite order on the curve E_n. We want to show that there is a one-to-one correspondence between such triangles and pairs of points $(x, \pm y) \in 2E_n(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Observe this set is empty if and only if E_n has rank zero, otherwise it is isomorphic to the direct sum of $\mathrm{rk}(E_n)$ (i.e., rank of E_n) copies of $\mathbb{Z}$.

Recall that in Chapter 1 we obtained a rational point on the curve E_n starting from a rational right triangle with area n. We prove that this point is the double of another rational point. Given a rational right triangle X, Y, Z with area n, let $Q = (\frac{Z^2}{4}, \frac{Z(X^2-Y^2)}{8})$ be the point obtained in Chapter 1. We construct another correspondence between these triangles and rational points of E_n. This new correspondence yields a point P and we will show that $Q = 2P$.

Rescale the triangle so that the hypotenuse has unitary length: let $u = X/Z$ and $v = Y/Z$. By using the parametrization of the unitary circle we can find a $t \in \mathbb{R}^+$ such that $u = \frac{1-t^2}{1+t^2}$ and $v = \frac{2t}{1+t^2}$. Given that our initial triangle has area n we have that

$$\frac{XY}{Z^2} = \frac{2n}{Z^2} = uv = \frac{2t(1-t^2)}{(1+t^2)^2} \qquad \text{and thus} \qquad \frac{n}{Z^2} = \frac{t(1-t^2)}{(1+t^2)^2}. \tag{4.1}$$

Now set $x_P = -nt$ and $y_P = \frac{n^2(1+t^2)}{Z}$. Using the relation (4.1) it is easy to show that the point $P = (x_P, y_P)$ lies on the curve E_n, indeed

$$y_P^2 = \frac{n^4(1+t^2)^2}{Z^2} \overset{(4.1)}{=} n^3 t(1-t^2) = -n^3t^3 + n^3t = x_P^3 - n^2 x_P.$$

At this point we express x_P and y_P in terms of X, Y, Z. From the definitions of u and v we obtain that $t = \frac{1-u}{v} = \frac{Y}{X+Z}$. Hence, in combination with the relation $X^2 + Y^2 = Z^2$ we obtain

$$x_P = -nt = -\left(\frac{XY}{2}\right)\left(\frac{Y}{X+Z}\right) = \frac{X(X-Z)}{2},$$
$$y_P = \frac{n^2(1+t^2)}{Z} = \left(\frac{XY}{2}\right)^2 \cdot \frac{1}{Z}\left(1 + \frac{Y^2}{(X+Z)^2}\right) = \frac{X^2(Z-X)}{2}.$$

Thus from the right triangle X, Y, Z we obtain the point

$$P = \left(\frac{X(X-Z)}{2},\ \frac{X^2(Z-X)}{2}\right).$$

Finally, using the formulas from Section 2.5.2 we calculate $2P$ (we omit the full calculations, they are carried out by substituting x_P, y_P, n, m, β with their respective expression in terms of X, Y, Z):

$$x_{2P} = \left(\frac{x_P^2 + n^2}{2y_P}\right)^2 = \left(\frac{Z}{2}\right)^2 = x_Q,$$
$$y_{2P} = -mx_{2P} - \beta \qquad \text{where} \qquad m = \frac{3x_P^2 - n^2}{2y_P} \quad \text{and} \quad \beta = y_P - mx_P$$
$$= \frac{Z(X^2 - Y^2)}{8} = y_Q.$$

Thus $Q = 2P$, as desired.

Now we can give a characterization of the points in $2E_n(\mathbb{Q})$.

Lemma 4.8. *Let $Q \in E_n(\mathbb{Q})\backslash\{\mathcal{O}\}$. Then Q is the double of another rational point if and only if the x-coordinate is the square of a rational number having even denominator.*

Proof. ($\Rightarrow$) See Lemma 4.5.

($\Leftarrow$) Let x_Q have the desired properties. By Proposition 1.4 there exists a rational right triangle with area n that corresponds to Q through Proposition 1.2. By our discussion above we have that Q is the double of some other rational point. □

Lemma 4.9. *There is a one to one and onto correspondence between pairs of points $(x, \pm y) \in 2E_n(\mathbb{Q}) \setminus \{\mathcal{O}\}$ and rational numbers with even denominator x such that $x, x+n, x-n$ are all squares of rational numbers. The correspondence is:*

$$\begin{aligned}(x, \pm y) &\mapsto \quad x \\ x &\mapsto (x, \pm\sqrt{x(x+n)(x-n)})\end{aligned}$$

Proof. Call the two maps φ and ψ respectively. First, observe that φ and ψ are well-defined, indeed let $P = (x_P, y_P)$ be a point in $E_n(\mathbb{Q}) \setminus \{\mathcal{O}\}$, then $x_{2P},\ x_{2P}+n,\ x_{2P}-n$ are all squares of rational numbers:

$$\begin{aligned}x_{2P} &= \left(\frac{x_P^2 + n^2}{2y_p}\right)^2, \\ x_{2P} + n &= \left(\frac{(x_P+n)^2 - 2n^2}{2y_P}\right)^2, \\ x_{2P} - n &= \left(\frac{(x_P-n)^2 - 2n^2}{2y_P}\right)^2,\end{aligned}$$

so each element of $2E_n(\mathbb{Q}) \setminus \{\mathcal{O}\}$ gets mapped to a rational number with the desired property. Now suppose that x is a rational number with the desired property, then its image is a rational point on E_n whose x-coordinate is the square of a rational number having even denominator, hence by Lemma 4.8 it is the double of another rational point.

Now we prove that the map in the statement is a bijection. It is immediate to check that $(\varphi \circ \psi)(x) = x$ and that $(\psi \circ \varphi)(x, \pm y) = (x, \pm y)$. This proves the lemma. □

Finally we can prove the following theorem.

Theorem 4.10. *There is a bijection between rational right triangles with sides X, Y, Z and area n and pairs of points $(x, \pm y)$ in $2E_n(\mathbb{Q}) \setminus \{\mathcal{O}\}$. The correspondence is:*

$$(X, Y, Z) \longmapsto \left(\frac{Z^2}{4},\ \pm\frac{Z(X^2 - Y^2)}{8}\right)$$
$$(x, \pm y) \longmapsto (\sqrt{x+n} - \sqrt{x-n},\ \sqrt{x+n} + \sqrt{x-n},\ 2\sqrt{x})$$

Proof. We just have to compose the bijection we saw in Proposition 1.2 with the one described in Lemma 4.9. □

In Koblitz [9] we find an alternative proof of Theorem 4.10 which is based on the following proposition.

Proposition 4.11. *Let E be the elliptic curve $y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_1, e_2, e_3 \in \mathbb{Q}$. Let $P = (x_0, y_0) \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Then $P \in 2E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ if and only if $x_0 - e_1, x_0 - e_2, x_0 - e_3$ are all squares of rational numbers.*

Proof. We first note that, without loss of generality, we may asssume that $x_0 = 0$. To see this, make the change of variables $x' = x - x_0$. The point $P' = (0, y_0)$ on the curve $E' : y^2 = (x - e_1')(x - e_2')(x - e_3')$, where $e_i' = e_i - x_0$, is in $2E_n'(\mathbb{Q}) \setminus \{\mathcal{O}\}$ if and only if our original P were in $2E_n(\mathbb{Q}) \setminus \{\mathcal{O}\}$. And trivially, the $x_0 - e_i$ are all squares if and only if the $(0 - e_i')$ are. So it suffices to prove the proposition with $x_0 = 0$.

Next, note that if there exists $Q \in E(\mathbb{Q})$ such that $2Q = P$, then there are exacly four points $Q, Q_1, Q_2, Q_3 \in E(\mathbb{Q})$ with $2Q_i = P$. To obtain Q_i, simply add to Q the point of order two $(e_i, 0) \in E(\mathbb{Q})$.

Choose a point $Q = (x, y)$ such that $2Q = P = (0, y_0)$. We want to find conditions for the coordinates of one such Q (and hence all four) to be rational. Now a point Q on the elliptic curve satisfies $2Q = P$ if and only if the tangent line the the curve at Q passes through $-P = (0, -y_0)$. That is, the four possible points Q are obtained geometrically by drawing the four distinct lines emanating from $-P$ which are tangent to the curve.

We readily verify that the coordinates (x, y) are rational if and only if the slope of the line from $-P$ to Q is rational.

($\Rightarrow$) Trivial.

($\Leftarrow$) If the slope m is rational, then the x-coordinate of Q, which is the double root of the cubic $(mx - y_0)^2 = (x - e_1)(x - e_2)(x - e_3)$, must also

be rational. In this case the y-coordinate of Q is also rational: $y = mx - y_0$. Thus, we want to know when one (and hence all four) slopes of the lines from $-P$ which are tangent to E are rational.

A number $m \in \mathbb{C}$ is the slope of a line from $-P$ which is tangent to E if and only if the following equation has a double root:

$$(mx - y_0)^2 = (x - e_1)(x - e_2)(x - e_3) = x^3 + ax^2 + bx + c, \tag{4.2}$$

with

$$a = -e_1 - e_2 - e_3, \qquad b = e_1e_2 + e_1e_3 + e_2e_3, \qquad c = -e_1e_2e_3 = y_0^2, \tag{4.3}$$

where the last equality $c = y_0^2$ comes from the fact that $(0, y_0)$ is on the curve $y^2 = x^3 + ax^2 + bx + c$. Now if we simplify (4.2) and factor out a x, our condition becomes: the following quadratic equation has a double root:

$$x^2 + (a - m^2)x + (b + 2my_0) = 0.$$

This is equivalent to saying that its discriminant must vanish, i.e.,

$$(a - m^2)^2 - 4(b + 2my_0) = 0. \tag{4.4}$$

Thus, our task is to determine when one (and hence all four) roots of this quadratic polynomial in m are rational.

We want to find a condition in terms of the e_i's (namely, our claim is that an equivalent condition is: $-e_i \in \mathbb{Q}^2$). In (4.4), the a and the b are symmetric polynomials in the e_i, but the y_0 is not. However, y_0, is a symmetric polynomial in the $\sqrt{e_i}$. That is, we introduce f_i satisfying $f_i^2 = -e_i$. There are two possible choices for f_i, unless $e_i = 0$. Choose the f_i in any of the possible ways, subject to the condition that $y_0 = f_1f_2f_3$. If all the e_i's are nonzero, this meas that the sign of f_1 and f_2 are arbitrary, and the sign of f_3 is chosen so that y_0 and $f_1f_2f_3$ are the same square root of $-e_1e_2e_3$. If, say, $e_3 = 0$, then either choice can be made for the sign of f_1, f_2, and of course $f_3 = 0$. In all cases there are four possible choices of the f_i's consistent with the requirements that $y_0 = f_1f_2f_3$. Once we fix one such choice f_1, f_2, f_3, we can list all the four choices as follows (here we are supposing that e_1 and e_2 are nonzero):

$$f_1, f_2, f_3; \qquad f_1, -f_2, -f_3 : \qquad -f_1, f_2, -f_3; \qquad -f_1, -f_2, f_3. \tag{4.5}$$

The advantage of going from the e_i's to the f_i's is that now the coefficients of our equation (4.4) are symmetric functions of f_1, f_2, f_3. More precisely, if we set $s_1 = f_1+f_2+f_3$, $s_2 = f_1f_2+f_1f_3+f_2f_3$, $s_3 = f_1f_2f_3$, the elementary symmetric functions, then

$$\begin{aligned} a &= f_1^2 + f_2^2 + f_3^2 = s_1^2 - 2s_2; \\ b &= f_1^2f_2^2 + f_1^2f_3^2 + f_2^2f_3^2; \\ y_0 &= s_3. \end{aligned}$$

Thus, equation (4.4) becomes

$$\begin{aligned} 0 &= (m^2 - s_1^2 + 2s_2)^2 - 4(s_2^2 - 2s_1s_3 + 2ms_3) \\ &= (m^2 - s_1^2)^2 + 4s_2(m^2 - s_1^2) - 8s_3(m - s_1). \end{aligned} \tag{4.6}$$

We see at first glance that the polynomial in (4.6) is divisible by $m - s_1$, i.e., $m = s_1 = f_1+f_2+f_3$ is a root. Since we could have made three other choices for the signs of the f_i, the other roots must correspond to these choices, i.e., the four solutions of equation (4.4) are:

$$\begin{aligned} m_1 &= f_1 + f_2 + f_3, & m_2 &= f_1 - f_2 - f_3, \\ m_3 &= -f_1 + f_2 - f_3, & m_4 &= -f_1 - f_2 + f_3. \end{aligned} \tag{4.7}$$

We want to know whether the four values in (4.7) are rational. Clearly, if all of the f_i are rational, then so are the m_i. Conversely, suppose the m_i are rational. Then $f_1 = (m_1 + m_2)/2$,$f_2 = (m_1 + m_3)/2$,$f_3 = (m_1 + m_4)/2$ are rational. The conclusion of this string of equivalent conditions is: the coordinates (x, y) of a point Q for which $2Q = P$ are rational if and only if the $f_i = \sqrt{-e_i}$ are rational. This proves the proposition. □

Second proof of Theorem 4.10. We are considering the case $e_1 = -n$, $e_2 = 0$, $e_3 = n$. By Proposition 4.11 we have that $P \in 2E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ if and only if $x_0 + n$, x_0, $x_0 - n$ are all squares of rational numbers. We conclude by Proposition 1.2. □

Chapter 5

An overview of the connection with L-functions

In the previous chapter we saw that in order to determine whether or not a squarefree positive integer n is a congruent number we need to study the rank of the curve E_n. This task is much more difficult than calculating the torsion subgroup and more machinery is needed.

Following Koblitz [9], the aim of this chapter is to talk without going too much into details about the Hasse-Weil L-functions of the elliptic curves E_n and how they serve for our purpose. In the context of arithmetic geometry, L-functions are analytical objects that encode the arithmetic properties of the object they are related to. In our case we are interested in the information about the rank of E_n. Discussing how L-functions are defined in general is beyond the scope of this thesis, for more details see Husemöller [8], Farmer et al. [6] and Bruin [3].

5.1 Local zeta-function and L-function of E_n

We begin fixing a prime of good reduction p, and then we encode the numbers $\#E_n(\mathbb{F}_{p^r})$ into a generating function called the *local zeta-function* of E at p:

$$Z(E_n/\mathbb{F}_p; T) = \exp\left(\sum_{r=1}^{\infty} \#E_n(\mathbb{F}_{p^r})\frac{T^r}{r}\right). \tag{5.1}$$

Using the theory of Dirichlet characters, Gauss sums and Jacobi sums we can find a closed form for (5.1). In particular there exists a complex number

$\alpha = \alpha_{n,p}$ in $\mathbb{Q}(i)$ such that $|\alpha| = \sqrt{p}$ and

$$Z(E_n/\mathbb{F}_p; T) = \frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-T)(1-pT)} = \frac{1-2aT+pT^2}{(1-T)(1-pT)} \tag{5.2}$$

where $a = a_{n,p} = \operatorname{Re}\alpha$.

As an example we calculate $Z(E_n/\mathbb{F}_p; T)$ for a prime of bad reduction p. We need to count the number of point in $E_n(\mathbb{F}_{p^r})$. If $p = 2$ and $p \nmid n$ then the curve E_n reduced modulo 2 is defined by the equation $y^2 = x^3 + x$. Using the linear change of variables $y = v + u$ and $x = u + 1$ we obtain the equation $v^2 = u^3$. If instead $p \mid n$ then the curve E_n reduced modulo p is defined by the equation $y^2 = x^3$. Thus for any prime of bad reduction p we only need to count the points on the singular curve defined by $y^2 = x^3$. Using Theorem 2.5.21 in Cohen [5] we obtain that $\#\{(x,y) \in \mathbb{F}_{p^r}^2 \mid y^2 = x^3\} = p^r$. There is only one point at infinity, namely $[0,1,0]$, and thus the total number of points is $p^r + 1$ for all $r \geq 1$. Plugging this into (5.1) we get

$$\begin{aligned} Z(E_n/\mathbb{F}_p; T) &= \exp\left(\sum_{r=1}^{\infty}(p^r+1)\frac{T^r}{r}\right) \\ &= \exp\left(\sum_{r=1}^{\infty}\frac{(pT)^r}{r}\right)\exp\left(\sum_{r=1}^{\infty}\frac{T^r}{r}\right) \\ &= \exp(-\log(1-pT))\exp(-\log(1-T)) \\ &= \frac{1}{(1-pT)(1-T)}. \end{aligned}$$

Remark 5.1. In general one can form the local zeta-function for a smooth projective variety V defined over a finite field as we did above. There is a series of conjectures due to Weil (and later proved by Weil, Dwork and Deligne) regarding some properties of these functions. In particular these conjectures concern the rationality of local zeta-functions, a functional equation that they saitsfy and how numerator and denominator factor into degree one polynomials. See Silvermann [7] for more details.

At this point all local zeta-functions, as p varies, are used to build the Hasse-Weil L-function of the curve E_n:

$$L(E_n; s) = \frac{\zeta(s)\zeta(s-1)}{\Pi_p Z(E_n/\mathbb{F}_p; p^{-s})}.$$

The Riemann ζ-function $\zeta(s)$ appears in the expression of $L(E_n; s)$ because the Euler products of $\zeta(s)$ and $\zeta(s-1)$ cancel with the denominator of $\prod_p Z(E_n/\mathbb{F}_p; T)$, which do not carry any relevant information. All is left is the Euler product for $L(E_n; s)$:

$$L(E_n; s) = \prod_{p \nmid 2n} \frac{1}{1 - 2a_{n,p}p^{-s} + p^{1-2s}}. \tag{5.3}$$

Proposition 5.2. *The product (5.3) converges for* $\mathrm{Re}(s) > 3/2$.

Proof. We have that

$$\begin{aligned} L(E_n; s) < \infty &\Leftrightarrow -\sum_{p \nmid 2n} \log(1 - 2a_{n,p}p^{-s} + p^{1-2s}) < \infty \\ &\Leftrightarrow \sum_{p \nmid 2n} \log(1 - \alpha_{n,p}p^{-s}) + \sum_{p \nmid 2n} \log(1 - \bar{\alpha}_{n,p}p^{-s}) < \infty. \end{aligned}$$

We check for uniform convergence on the first summation using the Weierstrass M-test:

$$\begin{aligned} |\log(1 - \alpha_{n,p}p^{-s})| &\leq \sum_{k \geq 1} \frac{|\alpha_{n,p}p^{-s}|}{k} \\ &\leq \sum_{k \geq 1} \frac{p^{1/2 - \mathrm{Re}(s)}}{k} \\ &= -\log(1 - p^{1/2-\mathrm{Re}(s)}) \leq \frac{1}{p^{\mathrm{Re}(s)-1/2}}. \end{aligned}$$

Now fix $\delta > 0$ and suppose that $\mathrm{Re}(s) \geq 3/2 + \delta$. This implies that

$$\frac{1}{p^{\mathrm{Re}(s)-1/2}} \leq \frac{1}{p^{1+\delta}}.$$

Since that the series $\sum_p \frac{1}{p^{1+\delta}}$ converges we have that $\sum_{p \nmid 2n} \log(1 - \alpha_{n,p}p^{-s})$ converges uniformly in $\{z \in \mathbb{C} \mid \mathrm{Re}(s) \geq 3/2 + \delta\}$. This is true for all $\delta > 0$ and thus we have proved uniform convergence in $\{z \in \mathbb{C} \mid \mathrm{Re}(s) > 3/2\}$. □

Using Fourier analysis a much stronger result can be proved.

Theorem 5.3. *The Hasse-Weil L-function* $L(E_n; s)$ *defined by (5.3) for* $\mathrm{Re}(s) > 3/2$, *extends analytically to an entire function on the whole complex plane.*

Proof. See Koblitz [9]. □

One of the main conjectures in the study of L-functions concerns whether or not any L-function can be analytically extended to a meromorphic function on $\mathbb{C}$. In the case of L-functions that come from elliptic curves over $\mathbb{Q}$ this is a consequence of the modularity theorem, proved by A. Wiles in [14] for a large class of elliptic curves, and later fully proved by Breuil et al. [2]. This theorem states that elliptic curves over $\mathbb{Q}$ are closely related to another mathematical object called *modular forms*. We just say that as for elliptic curves, we can associate an L-function to a modular form and it was proved by Hecke that these L-functions admit an analytic extension to an entire function on $\mathbb{C}$ and satisfy a functional equation.

5.2 L-functions and the Congruent Number Problem

For our purpose, the interesting connection between L-functions and the Congruent Number Problem is another conjecture, which we state in its weak form.

Conjecture 5.4 (Birch and Swinnteron-Dyer, weak form [1])**.** *Let E be a rational elliptic curve. Then E has rank r if and only if $L(E;s)$ has a zero of order r at $s = 1$.*

Observe that thanks to the modularity theorem it makes sense to talk about $L(E;s)$ at $s = 1$. As of today only special cases of the cojecture have been proved. We would like to point the attention to one of these special cases but first we give a definition.

Definition 5.5. Let E be an elliptic curve over $\mathbb{C}$ associated to the lattice L. The curve E is said to have *complex multiplication* if there exists a $c \in \mathbb{C} \setminus \mathbb{R}$ such that $cL = L$.

A more detailed explanation of complex multiplication and morphisms between elliptic curves can be found in Tate and Silvermann [12] and Silvermann [7].

The curves E_n all have complex multiplication because as we pointed out in Remark 2.19, their associated lattice is a square lattice and thus it is invariant under multiplication by $c = i$.

Theorem 5.6 (A. Wiles and J. Coates [4])**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ and having complex multiplication. If E has positive rank then $L(E;1) = 0$.*

This special case of the Birch and Swinnerton-Dyer conjecture gives us a sufficient condition for n *not* to be a congruent number, as $L(E_n;1) \neq 0$ implies $\mathrm{rk}(E_n) = 0$, and by Theorem 4.6 we have that n is not a congruent number.

If instead we just assume this weak form of the conjecture we have a sufficient condition for n to be a congruent number.

Proposition 5.7. *If $n \equiv 5, 6, 7 (\mathrm{mod}\ 8)$, and if the weak form of the Birch and Swinnerton-Dyer conjecture holds for E_n, then n is a congruent number.*

Proof. See Koblitz [9] □

To conclude this chapter we state another result proved by J. B. Tunnell [13]. It is a crucial step towards the solution to the Congruent Number Problem since, if the weak Birch and Swinnteron Dyer conjecture was true, we would have a necessary and sufficient condition for a squarefree positive integer to be a congruent number which has the advantage of being easy to verify.

Theorem 5.8 (J. B. Tunnell)**.** *Let n be a sqaurefree positive integer. For n odd define the quantities*

$$A_n = \#\{x, y, z \in \mathbb{Z} \mid n = 2x^2 + y^2 + 32z^2\},$$
$$B_n = \#\{x, y, z \in \mathbb{Z} \mid n = 2x^2 + y^2 + 8z^2\},$$

while for n even define

$$C_n = \#\{x, y, z \in \mathbb{Z} \mid n/2 = 4x^2 + y^2 + 32z^2\},$$
$$D_n = \#\{x, y, z \in \mathbb{Z} \mid n/2 = 4x^2 + y^2 + 8z^2\}.$$

If n is the area of a right triangle with rational sides then we have that $A_n = \frac{1}{2}B_n$ if n is odd and $C_n = \frac{1}{2}D_n$ is n is even. If the weak Birch and Swinnerton-Dyer conjecture is true for the elliptic curves $E_n : y^2 = x^3 - n^2x$, then, conversely, these equalities imply that n is a congruent number.

Bibliography

[1] Bryan John Birch and Henry Peter Francis Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965. available at http://eudml.org/doc/150676.

[2] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over Q: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14:843–939, 2001. available at https://doi.org/10.1090/S0894-0347-01-00370-8.

[3] Peter Bruin. What is... an L-function?, 2012. pdf availabe at https://www.math.leidenuniv.nl/ pbruin/L-functions.pdf.

[4] John Coates and Andrew Wiles. On the conjecture of birch and swinnerton-dyer. *Inventiones mathematicae*, 39(3):223–251, 1977. available at https://doi.org/10.1007/BF01402975.

[5] Henri Cohen. *Number Theory. Volume I: Tools and Diophantine Equations*, volume 239 of *Graduate texts in Mathematics*. Springer-Verlag, New York, 2007.

[6] David W. Farmer, Ameya Pitale, Nathan C. Ryan, and Ralf Schmidt. Analytic L-functions: definitions, theorems and connections. *Bulletin of the American Mathematical Society*, 56(2):261–280, 2019. available at https://doi.org/10.1090/bull/1646.

[7] Joseph H. Silvermann. *The arithmetic of elliptic curves*, volume 106 of *Graduate texts in Mathematics*. Springer-Verlag, New York, 1986.

[8] Dale Husemöller. *Elliptic Curves*, volume 111 of *Graduate texts in Mathematics*. Springer-Verlag, New York, second edition, 2004.

[9] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate texts in Mathematics*. Springer-Verlag, New York, 1984.

[10] Berry Mazur. Rational isogenies of prime degree. *Inventiones mathematicae*, 44(2):129–162, 1978. available at https://doi.org/10.1007/BF01390348.

[11] Rick Miranda. *Algebraic Curves and Riemann Surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, 1995.

[12] Joseph H. Silvermann and John T. Tate. *Rational Points on Elliptc Curves*. Undergraduate texts in Mathematics. Springer-Verlag, Cham, second edition, 2015.

[13] J. B. Tunnell. A classical diophantine problem and modular forms of weight 3/2. *Inventiones mathematicae*, 72(2):323–334, 1983. available at https://doi.org/10.1007/BF01389327.

[14] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 141(3):443–551, 1995. available at https://doi.org/10.2307/2118559.