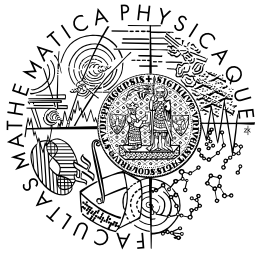

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Jan Kotyk

Congruent numbers, elliptic curves, and L-functions

Department of Algebra

Supervisor of the bachelor thesis: doc. Mgr. Vítězslav Kala, Ph.D.

Study programme: General mathematics

Study branch: Mathematical Structures

Prague 2024

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date ....

Author's signature

I would like to primarily thank my consultant Stevan Gajović for his scholarly advice and commentary during creation of this thesis as well as my advisor Vítězslav Kala who has given me the opportunity to work under him. It was pleasure to meet and discus mathematics with both of them.

I also cannot forget my family and close friends who all were very supportive during past months.

Title: Congruent numbers, elliptic curves, and L-functions
Author: Jan Kotyk
Department: Department of Algebra
Supervisor: doc. Mgr. Vítězslav Kala, Ph.D., Department of Algebra
Consultant: Stevan Gajović, Ph.D.

Abstract: The main goal of this thesis is to connect the ideas surrounding the congruent number problem. At first we define congruent numbers and elliptic curves which naturally emerge from this problem. We then define the addition law on points lying on such curves and show that it actually defines an abelian group structure on the set of those points. We then focus on the study of elliptic curves and their groups over finite fields to give us new insight on the congruent number problem. With this we then later define Zeta-functions and L-functions. At the end we see a connection between the property of being a congruent number and the rank of the corresponding elliptic curve which is then used to classify first few congruent and non-congruent numbers.

Keywords: congruent numbers, elliptic curves, Zeta-functions, L-functions

Název práce: Kongruentní čísla, eliptické křivky a L-funkce
Autor: Jan Kotyk
Katedra: Katedra algebry
Vedoucí bakalářské práce: doc. Mgr. Vítězslav Kala, Ph.D., Katedra algebry
Konzultant: Stevan Gajović, Ph.D.

Abstrakt: Hlavním cílem této práce je propojení výsledků týkající se problému kongruentních čísel. Zprvu zadefinujeme pojmy kongruentních čísel a eliptických křivek, které z tohoto problému přirozeně vyplývají. Následně zadefinujeme operaci sčítání bodů na eliptické křivce a ukážeme, že tato operace tvoří strukturu abelovské grupy na množině těchto bodů. Poté se zaměříme na eliptické křivky a jejich grupy definované nad konečnými tělesy abychom získaly nový pohled do problému kongruentních čísel. Díky němu později definujeme Zeta-funkce a L-funkce. Ke konci bude prezentován souvislost mezi vlastností být kongruentním číslem a hodností korespondující eliptické křivky, což bude využito v klasifikaci několika prvních kongruentních čísel.

Klíčová slova: kongruentní čísla, eliptické křivky, Zeta-funkce, L-funkce

Contents

1 Introduction **2**

2 Congruent numbers **4**

3 Elliptic curves, point addition **6**

4 Rank and congruent numbers **11**

5 Elliptic curves over finite fields **14**

6 L-functions **16**

7 Examples/Calculations **23**

Bibliography **28**

1. Introduction

In this thesis we will look into the problem of congruent numbers. A natural number n is called congruent if it is an area of a right triangle with all three sides rational. A congruent number problem asks whether a given number n is congruent or not. So far this problem has not been fully solved. Congruent numbers are closely related to elliptic curves which will also be looked into in this thesis. Tools which will be defined here are not specific just for congruent numbers, but also make appearance in many famous open problems like the Birch and Swinnerton-Dyer conjecture – one of the Millennium Problems.

Chapter 2 shows the definition and a simple characterization for congruent numbers from [Kob93] and it then presents few examples of such congruent numbers. We can also see Proposition 2.2 proving that the number 1 is not congruent which is later seen in Chapter 7 to imply Fermat's Last theorem for $n = 4$.

In Chapter 3 we define a binary operation on points lying on arbitrary elliptic curve E, which forms an abelian group structure on said points. We are then presented with two formulae which give us concrete ways to calculate coordinates of point resulting by doubling a point or adding two points on this curve E.

Chapter 4 has the same goal as Chapter 1 in [Kob93], that is to prove the Theorem 4.7 which states that n is congruent if and only if the corresponding elliptic curve E_n over $\mathbb{Q}$ has a positive rank. The thesis goes by a different, more computationally oriented, path than in the mentioned book.

In Chapter 5 we are presented with Hasse's theorem without proof which is then later used in Chapter 6, in Proposition 6.2 to show convergence of Zeta-functions and in Proposition 6.8 for convergence of L-functions. We are then shown in Proposition 5.3 formula for the number of points on elliptic curves over finite fields and with example formulae for the number of $\mathbb{F}_{3^r}$ and $\mathbb{F}_{5^r}$-points on elliptic curves of the form $y^2 = x^3 - n^2x$.

Zeta-functions are defined in Chapter 6 with detailed proof of how they can be expressed for primes of good reduction in Proposition 6.3 and bad reduction in Proposition 6.4. Following this we are shown the definition of L-functions and their expression as an Euler product in Proposition 6.6. The L-functions are then used to make one final theorem connecting congruent numbers and elliptic curves in Theorem 6.10 which states that if n is congruent then the L-function of corresponding elliptic curve E_n evaluated at 1 is zero.

The whole thesis ends with Chapter 7 which classifies the congruent and non-congruent numbers up to 20 using the tools introduced in this thesis.

The thesis serves mainly as a summarization of ideas from two books: *Introduction to elliptic curves and modular forms* by Koblitz [Kob93] which looks directly on the congruent number problem and *Rational points on elliptic curves* by Silverman and Tate [ST92] which introduces with elliptic curves in general.

In Chapter 2 the author gives his proof of Proposition 2.2 stating that the number 1 is not congruent. He then proceeds to prove a characterization of congruent numbers from [Kob93] in Proposition 2.3 in more detail than was given in the cited book as one part of the proposition was left as an exercise. In Chap-

ter 3 the author proves some of the properties of elliptic curves in Propositions 3.4 and 3.5. He then presents two formulae for point addition on elliptic curves from [Sil09] which were in this book proven for general cases of curves, so the author gives more computationally oriented proof. Chapter 4 has the same goal as [Kob93], but the author approaches the final Theorem 4.7 in a new and unique way than the cited book. His work includes stating and subsequently proving Lemmas 4.4, 4.5 and Proposition 4.6 as well as own proof of the second implication of the mentioned Theorem 4.7. It is worth noting that in the book [Kob93] they prove the theorem via different methods using lemmas revolving around group homomorphisms, but in the final proof they unintentionally leave out one non-trivial detail, so the proof is incomplete. Chapter 5 does not contain many new ideas, as its purpose is just to give an insight into elliptic curves over finite fields, with the exceptions of worked-out Examples 6 and 7 given at the end. In [Kob93] the statements regarding Zeta-functions and L-functions are often given without proof, given as exercises or proven via other methods using character functions. Therefore for the propositions in Chapter 6, which are taken from the book, author provides his own proofs of which can be seen in Propositions 6.2, 6.4, 6.6 and 6.8 as well as Lemmas 6.7, 6.13 and 6.14. The book [Kob93] uses these lemmas in one example of determining if 1 is or is not a congruent number, which was an inspiration for Chapter 7. Using this inspiration, the author independently worked out the full classification of which natural numbers up to twenty are congruent, in Propositions 7.1 up to 7.9. At the end, the author shows how non-congruence of 1 implies Fermat's Last theorem for $n = 4$. The author also implements two algorithms in SageMath which he used for validation of before mentioned classification results.

2. Congruent numbers

We begin with the definition of a congruent number and show a simple characterization for such numbers which will slowly lead us into the world of elliptic curves.

Definition 2.1. A natural number n is called a *congruent number* if there exists a right triangle with rational sides and area n.

In other words, there exist rational numbers $a, b, c \in \mathbb{Q}^+$ such that $a^2+b^2 = c^2$ and $\frac{1}{2}ab = n$. In this text we will note right triangles with sides a, b, c as (a, b, c).

Example 1. The number 6 is a congruent number as the well-known (3,4,5) right triangle has area equal to 6. The number 5 is also a congruent number with a bit more complicated triangle whose sides are as follows: $(\frac{40}{6}, \frac{9}{6}, \frac{41}{6})$.

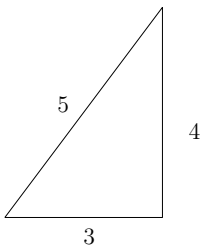

Figure 2.1: Triangle with area 6

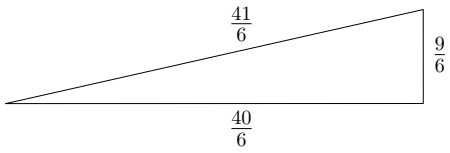

Figure 2.2: Triangle with area 5

If n is a congruent number, it does not necessarily mean that there exists only one such triangle as for example the triangles $(3, 4, 5)$ and $(\frac{1200}{70}, \frac{49}{70}, \frac{1201}{70})$ both have area of 6 but are not similar.

Let n be a congruent number with corresponding right triangle (a, b, c). It is easy to see that we can always find $t \in \mathbb{Q}^*$ such that t^2n is a square-free natural number. On the other hand, rescaling the triangle by t we obtain a right triangle (ta, tb, tc) which has area precisely t^2n and therefore this new number is also congruent. Due to this fact we can without loss of generality often assume that n is square-free natural number.

Example 2. 24, 54 and 150 are congruent numbers since they are equivalent to 6 modulo $(\mathbb{Q}^*)^2$ – by this we mean that if x is one of the numbers, there exist some $t \in \mathbb{Q}^*2$ such that $xt^2 = 6$.

Proposition 2.2. *The number 1 is not a congruent number.*

Proof. Suppose 1 was a congruent number, then there would exist a right triangle $(A, B, C) \in \mathbb{N}^3$ with area $D^2 \in \mathbb{N}$ and without loss of generality we can also suppose that A, B, C are pairwise coprime. The area of our triangle is given by the expression $\frac{1}{2}AB = D^2$ which is equivalent to $AB = 2D^2$. Since $(A, B) = 1$ we can see, that one of the numbers is an odd square and the other one is two times a square, let us say $A = 2k^2, B = l^2$ with l odd. Plugging the expression for A into the right triangle identity we get

$$4k^4 + C^2 = B^2 \iff k^4 = \frac{C-B}{2}\frac{C+B}{2}.$$

Using $(B, C) = 1$ we can conclude that $\frac{C-B}{2} = m^4$ and $\frac{C+B}{2} = n^4$ for some $m, n \in \mathbb{N}$ and so we get $m^4 - n^4 = B = l^2$, therefore we just need to show that the equation $x^4 = y^4 + l^2$ where l is odd has no solutions. Suppose it had at least one solution (x, y, l) and take one with x being smallest possible. We could write

$$x^2 = p^2 + q^2, y^2 = 2pq, l = p^2 - q^2$$

with p, q coprime since (y^2, l, x^2) is a primitive Pythagorean triple (there are many sources, for example see [ST92, Section 1.1]). We have got another primitive Pythagorean triple (p, q, x) and so we could again write the following

$$x = r^2 + s^2, p = 2rs, q = r^2 - s^2$$

with $r, s \in \mathbb{N}$ coprime. But $y^2 = 2pq = 4rs(r^2 - s^2) \neq 0$ so $r, s, (r^2 - s^2)$ are all squares. If we write $r = \tilde{x}^2, s = \tilde{y}^2, r^2 - s^2 = \tilde{z}^2$ then we arrive again at the equation $\tilde{x}^4 - \tilde{y}^4 = \tilde{z}^2$ with $0 < \tilde{x} = \sqrt{r} \leq r < x$ and so we have found a smaller solution to the original equation in $\mathbb{N}$ which is a contradiction since we assumed x to be smallest possible. □

Proposition 2.3. *A natural number n is congruent if and only if there exists $x \in \mathbb{Q}$ such that $x - n, x$ and $x + n$ are all squares of some rational numbers.*

Proof. We will follow a proof given in [Kob93, Chapter 1, Proposition 1].

" $\Longrightarrow$ " Suppose n is a congruent number and (A, B, C) is a right triangle with area n. We have the following two equations: $A^2 + B^2 = C^2$ and $\frac{1}{2}AB = n$. Adding or subtracting four-times the second equation to the first we get $(A \pm B)^2 = C^2 \pm 4n$. Dividing by four and substituting $x = (C/2)^2$ we get $(\frac{A \pm B}{2})^2 = x \pm n$ from which we see that all three numbers $x - n, x, x + n$ are squares of some rational numbers.

" $\Longleftarrow$ " Working backwards we can easily check that the map

$$x \mapsto (\sqrt{x+n} - \sqrt{x-n}, \sqrt{x+n} + \sqrt{x-n}, \sqrt{4x})$$

gives a right triangle with rational sides and area n. Indeed:

$$\left(\sqrt{x+n} - \sqrt{x-n}\right)^2 + \left(\sqrt{x+n} + \sqrt{x-n}\right)^2 = 4x = \left(\sqrt{4x}\right)^2$$

and

$$\frac{1}{2}\left(\sqrt{x+n} - \sqrt{x-n}\right)\left(\sqrt{x+n} + \sqrt{x-n}\right) = \frac{1}{2}(x + n - x + n) = \frac{1}{2}(2n) = n.$$

□

In the proof we stumbled upon two equations $(A \pm B)^2 = C^2 \pm 4n$. We can multiply them together to get $(A^2 - B^2)^2 = C^4 - 16n^2$ and by setting the values $\alpha = (A^2 - B^2)/4$, $\beta = C/2$ we obtain

$$\alpha^2 = \beta^4 - n^2.$$

Now multiply by β^2 both sides, so we have $(\alpha\beta)^2 = \beta^6 - n^2\beta^2$. Substituting $x = \beta^2, y = \alpha\beta$ we arrive at

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

This means that if we get a rational right triangle (A, B, C) with area n, we can use it to find a rational solution to the equation $y^2 = x^3 - n^2 x$ with $y \neq 0$.

This gives us a motivation to look into the structure of a family of curves known as *elliptic curves* which we will rigorously define in the next chapter.

3. Elliptic curves, point addition

Elliptic curves are special objects in that they are algebraic curves on one hand, but also one can define a group structure on them which is often regarded as the main reason to research such curves. The study of elliptic curves takes place over projective plane rather than affine plane (= K^2 for K a field).

Let K be a field and consider the monomial $a_{i,j}x^iy^j$ with $a_{i,j} \in K$. By the total degree of such monomial we mean the value $i+j$. If $F(x,y)$ is a polynomial over K, then by its total degree we understand the maximum degrees of all monomials which occur in F.

If we are given a polynomial $F(x,y)$ of total degree n, we may create a corresponding *homogeneous polynomial* $\tilde{F}(x,y,z)$ by multiplying each monomial $a_{i,j}x^iy^j$ of F by the value z^{n-i-j}. For example, the total degree of the polynomial $F(x,y) = y^2 - x^3 - n^2x$ is 3 and the corresponding homogeneous polynomial is $\tilde{F}(x,y,z) = y^2z - x^3 - n^2xz^2$.

Notice that for any homogeneous polynomial $\tilde{F}$ and any scalar $k \in K$ we have $k^n\tilde{F}(x,y,z) = \tilde{F}(kx,ky,kz)$ and $z^nF(\frac{x}{z},\frac{y}{z}) = \tilde{F}(x,y,z)$. This gives us a motivation into the definition of projective plane.

To define a projective plane, we begin with a 2-dimensional affine plane defined over a field K: $\{(x,y) \mid x,y \in K\}$. We then introduce a third coordinate z to create a set $\{(x,y,z) \neq (0,0,0) \mid x,y,z \in K\}$ and define an equivalence relation $\sim$ on this set which says that two points (x,y,z) and (x',y',z') are equivalent if there exists a nonzero $k \in K$ such that $(x,y,z) = (kx',ky',kz')$. With this we define a projective plane as the following object:

$$\mathbb{P}^2_K = \{(x,y,z) \neq (0,0,0) \mid x,y,z \in K\}/\sim .$$

This is a generalization of classical xy-plane as each point (x,y) embeds into $\mathbb{P}^2_K$ as $[(x,y,1)]_\sim$. These points due to our equivalence relation make up for all points with non-zero z-coordinate. The other equivalence classes, namely $[(x,y,0)]_\sim$, form what we call a *line at infinity*.

One point of interest from this set is the point $(0,1,0)$. If we have a cubic polynomial $f(x) = x^3 + ax^2 + bx + c$ then the homogeneous polynomial corresponding to $F(x,y) = y^2 - f(x)$ is $g(x,y,z) = y^2z - x^3 - ax^2z - bxz^2 - cz^3$. If a point (x,y,z) lies on this polynomial and $z = 0$ then we automatically get that x is also 0 therefore this point must be (0,1,0). We call this point the *point at infinity* and denote it by $\mathcal{O}$.

Definition 3.1. Let K be a field of characteristic not equal to 2 and $f(x) \in K[x]$ be a cubic polynomial with distinct roots in $\overline{K}$. We call the locus of all points (x,y) satisfying the equation $y^2 = f(x)$, together with the point at infinity $\mathcal{O}$, an *elliptic curve* defined over the field K.

If we have defined E over some field K we sometimes write it simply as E/K.

Definition 3.2. Let E/K be an elliptic curve defined by $y^2 = f(x) = x^3 + ax^2 + bx + c$. The set of *$K$-rational points on E* is the set

$$E(K) := \{(x,y,z) \in \mathbb{P}^2_K \mid y^2z = x^3 + ax^2z + bxz^2 + cz^3\}.$$

When $K = \mathbb{Q}$ we call the set $E(\mathbb{Q})$ rational points.

Since there is only point at infinity all other points lying on E belong to the affine plane K^2, so we can identify

$$E(K) = \{\mathcal{O}\} \cup \{(x, y) \in K^2 \mid y^2 = f(x)\}.$$

Due to this identification, we can simply work with elliptic curves as affine curves with one added point at infinity, so we do not forget that they are projective curves.

Definition 3.3. Let E be an elliptic curve over a field K given by an equation $y^2 = f(x)$ and define $F(x, y) := y^2 - f(x)$. Let $P = (x_0, y_0) \in E(K) \setminus \mathcal{O}$ then we say that the elliptic curve E is *smooth* at point P if the partial derivatives $\partial F/\partial x, \partial F/\partial y$ are not simultaneously zero at P. Furthermore if E is smooth at all points from $E(\overline{K})$ we say that E is *non-singular* (otherwise we call it *singular*).

Remark 3. Since $\mathcal{O}$ is given in projective coordinates the definition of smoothness at $\mathcal{O}$ is slightly different, but it can be checked that $\mathcal{O}$ is always smooth on E. For this reason we only check the smoothness at points of affine plane.

Proposition 3.4. *Let E/K be an elliptic curve. Then E is smooth.*

Proof. Assume that (x, y) is a point at which E is not smooth. Since $0 = \partial F/\partial y = 2y$ and K is not a field of characteristic 2 then $y = 0$. Thus $f(x) = 0$ and by assumption $\partial F/\partial x = -f'(x) = 0$ which implies that $f(x)$ has double root, therefore it does not satisfy the definition of an elliptic curve. □

Example 4. Consider a curve E defined by $F(x, y) := y^2 - x^3 - 1$ over $\mathbb{Q}$. The partial derivatives are $\partial F/\partial x = 3x^2$ and $\partial F/\partial y = 2y$ which are simultaneously zero if and only if $x = y = 0$. Since the point $(0, 0)$ does not lie on E then this curve is smooth at every point and therefore it is an elliptic curve.

On the other hand, if we defined it over the field $\mathbb{F}_3$ then the equation is $y^2 = (x + 1)^3$, so it is singular and it is not an elliptic curve ($f(x)$ has triple root at $x = -1$).

Remark 5. There exist elliptic curves over fields of characteristic 2. However, the curves in the form $y^2 = f(x)$ are always singular.

We are interested in the special kind of elliptic curves given by the equation $y^2 = x^3 - n^2x$. We denote these elliptic curves by E_n. So far we have defined them over the rational numbers $\mathbb{Q}$, but we can easily extend the definition to any field K.

Proposition 3.5. *Let K be a field of characteristic p. The equation $y^2 = x^3 - n^2x$ defines an elliptic curve over K if and only if p does not divide $2n$.*

Proof. Let p be the characteristic of K. By Remark 5 we may assume that $p \neq 2$. By the definition of an elliptic curve the polynomial $x^3 - n^2x$ must have 3 distinct roots. This expression factors into $(x + n)x(x - n)$ and so the roots are $\pm n$ and 0. For them to be distinct in characteristic p, they must not be pairwise congruent modulo p, in other words $-n \not\equiv n \not\equiv 0 \pmod{p}$. This happens if and only if $p \nmid 2n$. □

Let us also quickly remind of Bézout's Theorem (see [ST92, Appendix A]) which tells us about intersecting points of two projective curves.

Theorem 3.6 (Bézout's Theorem)**.** *Let $A, B \in K[x, y, z]$ be homogeneous polynomials of degrees a and b respectively with no common factors. Then A and B intersect in $\overline{K}$ at exactly ab points.*

As stated earlier if we are given any elliptic curve E over $\mathbb{Q}$ we can define a group structure on its set of points $E(\mathbb{Q})$ which we call *Mordell-Weil group* and denote the same way. The group addition on its elements is defined as follows:

- Given points $P, Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ such that their x-coordinates are not the same, we take a line going through P and Q. By Bézout's theorem this line must intersect E at some third point (which can be equal to P or Q, should the line be tangent at such point). Bézout's theorem does not right away say that this point belongs to K, but since elliptic curves are given by cubic polynomials and we already have two points in K, then this third one must also belong to K and not just $\overline{K}$ (see the proof of Proposition 3.9). If we now take this intersecting point and mirror it over the x-axis (effectively flipping the sign in y-coordinate) we obtain new point which we call $P + Q$.
- If the line through P and Q is vertical we define $P + Q$ as $\mathcal{O}$.
- If we want to double one of the points, say the point P, we take a tangent line to E at the point P and proceed as before – take the intersecting point and mirror it over x-axis. Such a point will be denoted by $2P$ (see Figure 3.2).
- For $P \in E(\mathbb{Q}) \setminus \mathcal{O}$ and $Q = \mathcal{O}$ we take the line going through P and Q as the vertical line through P. Therefore result of $P + \mathcal{O}$ is again P as the third point of intersection is P flipped over the x-axis.
- Finally for $P = Q = \mathcal{O}$ we define $\mathcal{O} + \mathcal{O} = \mathcal{O}$.

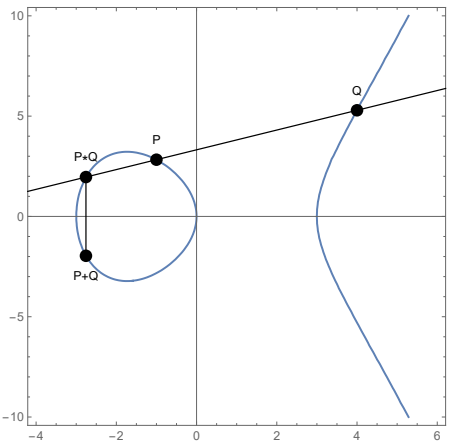

Figure 3.1: Point addition

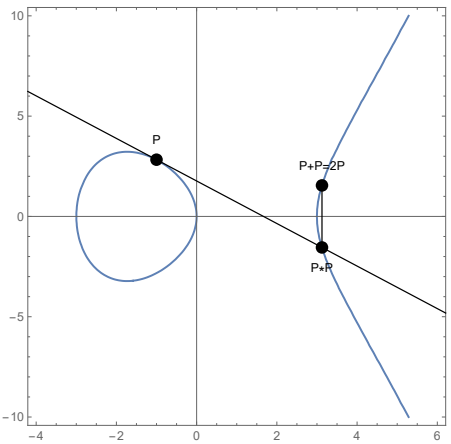

Figure 3.2: Point doubling

We have to remember, that we view E as a projective curve and therefore we must not omit the point at infinity. For example if we take P and Q such

that they both lie on a line which is parallel to y-axis then, if viewed as affine curve, E would not intersect this line in any third point, but since we take E as projective curve, $P + Q$ is the point at infinity $\mathcal{O}$ (as $\mathcal{O}$ flipped is again $\mathcal{O}$).

To see that this operation indeed defines a group we have to check the basic axioms of group:

- The *identity element* of this group is the point at infinity $\mathcal{O}$ as seen by how we defined point addition.
- It can also be easily seen that the *inverse* to any point $P = (x_0, y_0)$ is simply $(x_0, -y_0)$ since line going through such points will intersect E at $\mathcal{O}$ which we have established as the identity element. By $-P$ we will mean the point which is inverse to $P \in E(\mathbb{Q})$.
- *Associativity* is the only hard thing to show and if one wants to see proof of this fact, we recommend reading it in [ST92, Pages 14-16].

What is more interesting is the fact, that this operation is commutative – a line going though P and Q is the same as the line going though Q and P therefore $P + Q = Q + P$.

Definition 3.7. Let E be an elliptic curve and $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$. By *order* of P we mean the smallest $n \in \mathbb{N}$ such that $nP = \mathcal{O}$. If no such number exists, we say that P has order ∞.

Proposition 3.8. *Let E be an elliptic curve defined over $\mathbb{Q}$ by the equation $y^2 = f(x)$ where $f(x)$ is cubic polynomial. The value x_0 is root of $f(x)$ if and only if the order of $P = (x_0, 0)$ is 2.*

Proof. " $\implies$ " To obtain the order of P we at first have to double the point P which requires us to take a tangent line to E through P. This line is perpendicular to the x-axis because the partial derivative with respect to y at this point is zero. It therefore intersects E twice at P and once at $\mathcal{O}$. The result of such operation is therefore $\mathcal{O}$ which is the identity element and so P must have order of 2.

" $\impliedby$ " For a point $P \neq \mathcal{O}$ to satisfy the identity $2P = \mathcal{O}$ is equivalent to satisfying $P = -P$ and so $(x_0, y_0) = (x_0, -y_0) \implies y_0 = -y_0 \implies y_0 = 0$ and so x_0 is root of $f(x)$. □

The following two propositions give us concrete formulae which tell us how to calculate coordinates of $P + Q$ for $P, Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}, P \neq \pm Q$. In the book [Sil09, Chapter 3, 2.3.] one can see an algorithm for more general types of curves, which we fortunately do not discus in this work.

Proposition 3.9. *Let E be an elliptic curve given by $y^2 = x^3 + ax^2 + bx + c$ and $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ such that $P \neq \pm Q$. Then the point $P + Q = (x_3, y_3) \in E(\mathbb{Q})$ has coordinates*

$$x_3 = \lambda^2 - a - x_1 - x_2$$

$$y_3 = -(\lambda x_3 + \nu)$$

where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = y_1 - \lambda x_1$

Proof. The line going through points P and Q is given by the equation

$$\frac{y_2 - y_1}{x_2 - x_1}(x - x_1) = y - y_1$$

and so by setting $\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \nu = y_1 - \lambda x_1$ we get $y = \lambda x + \nu$. Plugging this value into the expression for E and putting all terms to the right-side yields

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + c - \nu^2.$$

We also know that this cubic equation has three roots x_1, x_2, x_3 and so using the Vieta's formulae for coefficient of x^2 we get

$$a - \lambda^2 = -x_1 - x_2 - x_3 \implies x_3 = \lambda^2 - a - x_1 - x_2.$$

Thus, from the equation of the line we get the value for $\tilde{y_3}$ as $\tilde{y_3} = \lambda x_3 - \nu$. Finally we need to flip the sign of $\tilde{y_3}$ to obtain the value of y_3 due to how we defined addition on this group. □

Proposition 3.10 (Duplication formula)**.** *Let E be an elliptic curve as above and $P = (x_0, y_0) \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ a point not of order 2. Then the x-coordinate of $2P$ are given by the following formula:*

$$x[2P] = \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c}. \tag{3.1}$$

Proof. The proof is essentially the same as in Proposition 3.9 with the difference that λ the slope of tangent line at the point P. We calculate λ as following:

$$y^2 = f(x)$$

$$\frac{d}{dx}(y^2) = \frac{d}{dx}(f(x))$$

$$2y\frac{dy}{dx} = f'(x)$$

$$\frac{dy}{dx} = \frac{f'(x)}{2y} \implies \lambda = \frac{dy}{dx}\Big|_P = \frac{f'(x_0)}{2y_0}$$

Now the tangent line at P is given by the equation

$$\lambda(x - x_0) = y - y_0.$$

Set $\nu = y_0 - \lambda x_0$ to obtain $y = \lambda x + \nu$. Now the proof is essentially the same as in the previous proposition with the difference that $x_1 = x_2$, so the expression for $x[2P]$ looks like

$$x[2P] = \lambda^2 - a - 2x_0 = \frac{(f'(x_0))^2}{4y_0^2} - a - 2x_0 = \frac{(f'(x_0))^2 - 4y_0^2 a - 8y_0^2 x_0}{4y_0^2}.$$

Since $y_0^2 = x_0^3 + ax_0^2 + bx_0 + c$ we can replace by it the expression in the denominator at arrive at

$$x[2P] = \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c}.$$

□

4. Rank and congruent numbers

In this section we will define and use the concept of a rank of an elliptic curve and how it is connected to congruent numbers. To do so we will use a well-known theorem by Mordell whose proof we will not present – we recommend looking into [ST92, Section 3] for a proof. We will also use a rather strong theorem given by Mazur which will likewise now be proven here.

Theorem 4.1 (Mordell's Theorem)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Then the group $E(\mathbb{Q})$ is finitely generated.*

Proof. See [ST92, Theorem 3.10]. □

The fundamental theorem of finitely generated abelian groups says that any abelian group A can be decomposed as a direct product of a torsion subgroup $\mathrm{Tor}(A)$ and $\mathbb{Z}^r$ for some non-negative integer r. This leads us into definition of an object we call rank of elliptic curve.

Definition 4.2. Let E be an elliptic curve defined over $\mathbb{Q}$. The *rank* of E is a non-negative integer r such that

$$E(\mathbb{Q}) \cong \mathrm{Tor}(E(\mathbb{Q})) \oplus \mathbb{Z}^r.$$

The rank is an important object in studies of elliptic curves. In the context of congruent number problem, it can be used to create new characterization for congruent numbers.

To make such characterization we will use the following highly non-trivial but important theorem of Mazur.

Theorem 4.3 (Mazur's Theorem, [Maz78, Theorem 2])**.** *Let ϕ be the torsion subgroup of Mordell-Weil group of an elliptic curve over $\mathbb{Q}$. Then ϕ is isomorphic to*

$$\begin{array}{lll} \text{(A)} & \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 10 \text{ or } m = 12; \\ \text{(B)} & \mathbb{Z}/2m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & 1 \leq m \leq 4. \end{array}$$

Lemma 4.4. *In $E_n(\mathbb{Q})$ the only points of order dividing 2 are $(\pm n, 0)$, $(0,0)$ and $\mathcal{O}$.*

Proof. By Proposition 3.8 we know that points of order 2 are only the points with x-coordinate being the root of $x^3 - n^2x$, those are precisely $(\pm n, 0)$, $(0,0)$. For the point $\mathcal{O}$ the statement holds trivially. □

Lemma 4.5. *$E_n(\mathbb{Q})$ has no points of orders 3 and 4.*

Proof. Case 1. First, we will look at the points of order 3. Let $P = (x, y)$ be such point. Then P has to satisfy the identity $2P = -P \neq \mathcal{O}$. Using duplication formula (3.1) to calculate the x-coordinate of $2P$ we get

$$x[2P] = \frac{(x^2 + n^2)^2}{4x(x^2 - n^2)}.$$

On the other hand, $x[2P] = x[-P] = x$ and so we get the following equation:

$$x = \frac{(x^2+n^2)^2}{4x(x^2-n^2)} \iff 4x^2(x^2-n^2) = (x^2+n^2)^2 \iff 3x^4 - 6x^2n^2 - n^4 = 0,$$

which after a substitution $t = x^2$ simplifies into:

$$3t^2 - 6tn^2 - n^4 = 0.$$

Since $x \in \mathbb{Q}$ then $t \in \mathbb{Q}^2$ and so the discriminant of the quadratic equation above must be a rational square, but that is not the case because

$$\Delta = (-6n^2)^2 - 4(3)(-n^4) = 36n^4 + 12n^4 = 48n^4 \notin \mathbb{Q}^2$$

and therefore such point P cannot exist, so there are no points of order 3.

Case 2. Now suppose P has order 4. Using duplication formula (3.1) we get an expression for the x-coordinate and thanks to the equation of a line $y = \lambda x + \nu$ we obtain the y-coordinate:

$$y[2P] = \frac{n^6 - 5n^4x^2 - 5n^2x^4 + x^6}{8y^3}.$$

P being a point of order 4 implies that $2P$ is point of order 2, but those are only the 3 points $(\pm n, 0)$, $(0,0)$ by Lemma 4.4. All of them lie on the x-axis so $y[2P] = 0$. This holds if and only if the numerator is equal to zero and after factoring out (x^2+n^2) (which is always non-zero for $x \in \mathbb{Q}$), we get $x^4 - 6x^2n^2 + n^4$. Again substitute $t = x^2$ and we arrive at

$$t^2 - 6tn^2 + n^4 = 0.$$

(As in *Case 1.*) The discriminant being equal to $32n^4$ is not a rational square thus there are no points of order 4. □

Proposition 4.6. $\#\operatorname{Tor}(E_n(\mathbb{Q})) = 4$.

Proof. Mazur's Theorem implies that $\operatorname{Tor}(E_n(\mathbb{Q}))$ is isomorphic to one of the groups

$$\text{(A) } \mathbb{Z}/m\mathbb{Z}, m \in \{1, \cdots, 10\} \cup \{12\}$$
$$\text{(B) } \mathbb{Z}/2m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, m \in \{1,2,3,4\}.$$

Lemma 4.4 implies $\operatorname{Tor}(E_n(\mathbb{Q}))$ must have subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ which immediately removes case (A). From the 4 other possibilities, Lemma 4.5 removes $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We are left with only one possibility: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and so $\operatorname{Tor}(E_n(\mathbb{Q}))$ is isomorphic to Klein four-group which has precisely 4 elements. □

Theorem 4.7. *A natural number n is congruent if and only if E_n has positive rank r over $\mathbb{Q}$.*

Proof. " $\implies$ " At the end of Chapter 2 we have seen that if we have a rational right triangle (A, B, C) we can then obtain a point (x, y) on E_n via the map $(A, B, C) \to (C^2/4, (A^2 - B^2) \cdot C/8)$. The values $A^2 - B^2$ and C can never be zero, therefore the y-coordinate of this point is non-zero. From Proposition 4.6 we know

that the only points of finite order are either $\mathcal{O}$ or points with zero y-coordinate. Since our newly obtained point has neither property it must necessarily be a point of infinite order and therefore the rank of E over $\mathbb{Q}$ is positive.

" $\Longleftarrow$ " Suppose now that E_n over $\mathbb{Q}$ has positive rank. Then we can find some point $\tilde{P} \in E_n(\mathbb{Q}), \tilde{P} = (\tilde{x}, \tilde{y}) \neq \mathcal{O}$ of infinite order and set $P = 2\tilde{P}$. The reason for this doubling of point is to utilize the duplication formula (3.1) in the following: let $P = (x, y)$, then we have

$$x = \frac{(\tilde{x}^2 + n^2)^2}{4\tilde{y}^2},$$
$$y = \sqrt{x^3 - n^2 x}.$$

Now if we can make these simple observations:
1) x is a square of a rational number
2) $x + n$ is a square of a rational number as it is equal to

$$\frac{(\tilde{x}^2 + n^2)^2 + 4\tilde{y}^2 n}{4\tilde{y}^2} = \frac{n^4 - 4n^3\tilde{x} + 2n^2\tilde{x}^2 + 4n\tilde{x}^3 + \tilde{x}^4}{4\tilde{y}^2} = \left(\frac{-n^2 + 2n\tilde{x} + \tilde{x}^2}{2\tilde{y}}\right)^2.$$

3) $x - n$ is also a square of a rational number, similarly as in previous case we have

$$\frac{(\tilde{x}^2 + n^2)^2 - 4\tilde{y}^2 n}{4\tilde{y}^2} = \frac{n^4 + 4n^3\tilde{x} + 2n^2\tilde{x}^2 - 4n\tilde{x}^3 + \tilde{x}^4}{4\tilde{y}^2} = \left(\frac{n^2 + 2n\tilde{x} - \tilde{x}^2}{2\tilde{y}}\right)^2.$$

Finally, we can use the Proposition 2.3 which tells us that n must be congruent. □

Back in Chapter 2 we have seen that we can have multiple triangles which show the congruence property of a number. One interesting consequence of this theorem is the fact, that we actually have infinitely many of such triangles – we have infinitely many points in $E_n(\mathbb{Q})$ therefore we have infinitely many values of $x \in \mathbb{Q}$ which, thanks again to Proposition 2.3, generate non-congruent right triangles with area n.

We end this chapter with a note that this exact theorem is also proven in [Kob93] in Chapter 1 Proposition 18, although in a completely different way using group homomorphisms and in the last part one small non-trivial detail is missing (more specifically: in their proof they need the value n to be coprime with the numerator of $x[2P]$, which they do not show).

5. Elliptic curves over finite fields

So far, we have been looking at elliptic curves over $\mathbb{Q}$, but our definition allows us to look at any field. In this chapter we will look into elliptic curves defined over finite fields $\mathbb{F}_q$, q is a power of prime. We will later use these results to define two new types of functions which will be used for another ways of determining if a number is congruent.

Definition 5.1. Let p be a prime and E be an elliptic curve defined over $\mathbb{Q}$ by an equation $y^2 = f(x)$. The equation of E considered over a finite field $\mathbb{F}_p$ defines new curve which we call a *reduction modulo p*.

If this new curve is an elliptic curve, we call the prime p *a prime of good reduction*, otherwise we call p *a prime of bad reduction*.

For our elliptic curves of interest, E_n, it follows by Proposition 3.5 that p is a prime of good reduction if and only if $p \nmid 2n$.

Similarly to looking over fields $\mathbb{F}_p$, we can also look over fields $\mathbb{F}_q$ for q being a power of p. We are mainly interested in the number of points of $E(\mathbb{F}_q)$.

Since $\mathbb{F}_q$ is finite, then $E(\mathbb{F}_q)$ is also finite and we can make a crude estimate for the number of points which is $q^2 + 1$ (q^2 combinations of (x, y) plus one point at infinity). Much better estimate is using the fact that for every value of x we get at most 2 values for y, giving us an upper bound of $2q + 1$. Statistically, a randomly chosen quadratic equation from $\mathbb{F}_q$ has generally 50% chance of being solvable over $\mathbb{F}_q$, therefore we should expect the number of points to be more likely around the value $q + 1$. This is actually the case which is shown by the following theorem of Hasse.

Theorem 5.2 (Hasse's theorem, [Has36, Page 206])**.** *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ where q is a power of a prime. Then*

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

The "error" value $q + 1 - \#E(\mathbb{F}_q)$ is a very useful object which comes up very often when dealing with elliptic curves over finite fields and so we label it by $a_{E,q}$. Some of properties of $a_{E,q}$ are captured in the following proposition taken from [Sil09, Chapter 5, 2.3.1].

Proposition 5.3. *Let $\alpha, \beta \in \mathbb{C}$ be roots of the quadratic equation $x^2 - a_{E,q}x + q$, then*

(A) either $\alpha = \beta \in \mathbb{R}$ or α, β are complex conjugates
(B) $|\alpha| = |\beta| = \sqrt{q}$
(C) $\#E(\mathbb{F}_{q^r}) = q^r + 1 - \alpha^r - \beta^r$

Proof. (A) Consider the discriminant of $x^2 - a_{E,q}x + q$:

$$\Delta = a_{E,q}^2 - 4q \leq (2\sqrt{q})^2 - 4q = 4q - 4q = 0.$$

This means, that either α and β are the same real number or they are both complex. In both cases we have $\alpha = \bar{\beta}$ since the quadratic polynomial has coefficients in $\mathbb{Z}$.

(B) Comparing constant terms of the polynomial $x^2 - a_{E,q}x + q = (x-\alpha)(x-\beta)$ we get: $q = \alpha\beta \implies |q| = |\alpha\beta| = |\alpha|\,|\beta| = |\alpha|\,|\bar{\alpha}| = |\alpha|^2 \implies \sqrt{q} = |\alpha| = |\beta|$.

(C) This part is hard to prove and can be seen in [Sil09, Chapter 5, 2.3.1]. □

This proposition says that the number of points of $E(\mathbb{F}_{p^r})$ for fixed prime p has in a sense one degree of freedom, meaning that we just need to calculate the number of $\mathbb{F}_{p^r}$-points for one choice of r and then we can easily find the number of $\mathbb{F}_{p^r}$-points for any value of r. This will become handy in the next chapter.

Example 6. Consider an elliptic curve E_n such that $3 \nmid n$ and take the prime $p = 3$. Over the field $\mathbb{F}_3$ the equation defining E_n simplifies into

$$y^2 = x^3 - x = x(x+1)(x-1)$$

as $n^2 \equiv 1 \pmod 3$. Every choice of x gives us 0 and therefore we have $E_n(\mathbb{F}_3) = \{(0,0),(1,0),(2,0),\mathcal{O}\}$, $\implies$ $\#E_n(\mathbb{F}_3) = 4$. Let us continue by calculating the number of $\mathbb{F}_{3^r}$-points. We begin with $a_{E_n,3} = 3 + 1 - \#E(\mathbb{F}_3) = 0$, now we find the two roots of the polynomial $x^2 - a_{E_n,3}x + 3 = x^2 + 3 = (x + i\sqrt{3})(x - i\sqrt{3})$. By Proposition 5.3 (C) we obtain formula for the number of points over $\mathbb{F}_{3^r}$: $\#E(\mathbb{F}_{3^r}) = 3^r + 1 - \left(i^r + (-i)^r\right)\sqrt{3}^r$. We can simplify this formula a bit by considering the parity of r:

- If $r = 2s + 1$ is odd then $(i^r + (-i)^r) = 0$ and so $\#E(\mathbb{F}_{3^r}) = 3^r + 1$.
- If $r = 2s$ is even then $(i^r + (-i)^r) = 2(-1)^s$ so $\#E(\mathbb{F}_{3^r}) = 9^s + 1 - 2(-3)^s$.

Example 7. Let us go through the same calculations but with $p = 5$ and $5 \nmid n$. We have to consider 2 cases: $n \equiv \pm 1 \pmod 5$ and $n \equiv \pm 2 \pmod 5$.

If $n \equiv \pm 1 \pmod 5$ then the equation for E_n similarly simplifies into $x^3 - x = x(x+1)(x+4)$. The values $x = 0, 1, 4$ force the value of y to be only 0, while plugging $x = 2$ gives 1 with $y^2 = 1$ having 2 solutions ($y = 1, y = 4$) and $x = 3$ gives the number 4 with also two values for y ($y = 2, y = 3$). We have $\#E(\mathbb{F}_5) = 8, a_{E_n,5} = -2$ and the roots of corresponding quadratic polynomial $x^2 + 2x + 5$ are $-1 \pm 2i$. Putting this to the expression for number of points over general field $\mathbb{F}_{5^r}$ we get:

$$\#E(\mathbb{F}_{5^r}) = 5^r + 1 - \left((-1-2i)^r + (-1+2i)^r\right).$$

If $n \equiv \pm 2 \pmod 5$ then the equation simplifies into

$$y^2 = x^3 + x = x(x+2)(x+3).$$

All of the values $x = 0, 2, 3$ again create one possibility for y, namely 0, while $x = 1$ gives $y^2 = 2$ which is not a square and so from this number we do not get any points, same with $x = 4$ as we get $y^2 = 3$. We get $\#E(\mathbb{F}_5) = 4, a_{E_n,5} = 2$ and so the roots of the quadratic polynomial $x^2 - 2x + 5$ are $1 \pm 2i$. This gives us similarly looking expression for the number of points over $\mathbb{F}_{5^r}$:

$$\#E(\mathbb{F}_{5^r}) = 5^r + 1 - \left((1-2i)^r + (1+2i)^r\right).$$

6. L-functions

With a bit of insight to finite fields from last chapter, we will here define L-functions and mention a theorem by Coates and Wiles. This theorem combined with the result from the end of Chapter 4 will give us new characterization for congruent numbers.

To define these L-functions we firstly need to define a helpful function we call Congruence Zeta-function. Later we will see that these Zeta-functions of elliptic curves of our form of interest are actually really easy to calculate since we will only need to find the number of $\mathbb{F}_p$-points on E_n.

Definition 6.1. Let C be a curve defined over $\mathbb{F}_p$ for p a prime number and let $N_r = \#C(\mathbb{F}_{p^r})$. We define a *Congruence Zeta-function* of C over $\mathbb{F}_p$ as:

$$Z(C/\mathbb{F}_p, T) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right).$$

The word *Congruence* is often omitted from the name, so we also not use it from now on.

Proposition 6.2. *Let E be an elliptic curve defined over $\mathbb{F}_p$. Its corresponding Zeta-function $Z(E/\mathbb{F}_p, T)$ converges on the open disc $|T| < \frac{1}{p}$.*

Proof. From the Hasse's theorem (Theorem 5.2) we have an upper bound on $\#E(\mathbb{F}_{p^r})$, that is $\#E(\mathbb{F}_{p^r}) \leq p^r + 1 + 2\sqrt{p^r}$. Since the terms of the sum in $\exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right)$ are all positive, it converges if the sum inside of the exponential (namely $\sum_{r=1}^{\infty} N_r \frac{T^r}{r}$) converges. We can then deduce the convergence from the following:

$$\sum_{r=1}^{\infty} N_r \frac{T^r}{r} \leq \sum_{r=1}^{\infty} (p^r + 1 + 2\sqrt{p^r}) \frac{T^r}{r} = \sum_{r=1}^{\infty} \frac{(pT)^r}{r} + \sum_{r=1}^{\infty} \frac{T^r}{r} + 2\sum_{r=1}^{\infty} \frac{(Tp^{1/2})^r}{r}$$

where the radii of convergence are $\frac{1}{p}, 1$ and $\frac{1}{\sqrt{p}}$ respectively. From these three numbers the value $\frac{1}{p}$ is smallest and so the original series also converges on the disc $|T| < \frac{1}{p}$. □

For primes of good reduction we have an alternative expression of Zeta-functions as presented for example in [Sil09, Chapter 5, Theorem 2.4].

Theorem 6.3. *Let E_n be an elliptic curve defined over $\mathbb{F}_p$ such that p is a prime of good reduction of $E_n(\mathbb{Q})$, then*

$$Z(E_n/\mathbb{F}_p, T) = \frac{1 - a_{E_n,p}T + pT^2}{(1-T)(1-pT)}.$$

Proof. Let α, β be roots of the polynomial $x^2 - a_{E_n,p}x + p$, then

$$\begin{aligned}\sum_{r=1}^{\infty} N_r \frac{T^r}{r} &= \sum_{r=1}^{\infty} (p^r + 1 - \alpha^r - \beta^r) \frac{T^r}{r} = \\ &= -\log(1-pT) - \log(1-T) + \log(1-\alpha T) + \log(1-\beta T) = \\ &= \log\left(\frac{(1-\alpha T)(1-\beta T)}{(1-pT)(1-T)}\right) = \log\left(\frac{1 - a_{E_n,p}T + pT^2}{(1-T)(1-pT)}\right)\end{aligned}$$

and therefore

$$Z(E_n/\mathbb{F}_p, T) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right) = \frac{1 - a_{E_n,p}T + pT^2}{(1-T)(1-pT)}.$$

□

Defining the Zeta-function for $y^2 = x^3 - n^2x$ still makes sense over fields with characteristic dividing $2n$. The following proposition shows that the Zeta-function for these curves over such field can also be expressed as a quotient of two polynomials with the difference of how the numerator looks like.

Proposition 6.4. *Let E_n be a curve defined by the equation $y^2 = x^3 - n^2x$ over $\mathbb{F}_p$ such that p is a prime of bad reduction of $E_n(\mathbb{Q})$, then*

$$Z(E_n/\mathbb{F}_p, T) = \frac{1}{(1-T)(1-pT)}.$$

Proof. We discern two cases, when $p = 2$ and when $p \mid n$.

Case $p = 2$. Now we have to calculate the number of solutions over the fields $\mathbb{F}_{2^r}$. These fields have characteristic equal to 2 and therefore we can rewrite the equation $x^3 - n^2x$ as $x(x+n)^2$. Left hand side y^2 is a square so x on its own must also be a square, which means that we need to calculate the number of squares in $\mathbb{F}_{2^r}$. First of 0 is trivially a square. The set $\tilde{\mathbb{F}} := \mathbb{F}_{2^r}\backslash\{0\}$ forms a multiplicative group. On this group consider an endomorphism

$$\begin{aligned} f\colon \tilde{\mathbb{F}} &\to \tilde{\mathbb{F}} \\ x &\mapsto x^2. \end{aligned}$$

Looking at the kernel: $\ker(f) = \{x \in \tilde{\mathbb{F}} | x^2 = 1\} = \{1\}$ as $x^2 - 1 = (x-1)^2 = 0$. This implies that f is actually an automorphism, thus every element is a square.

If we go back to the original equation, we see that we have exactly 2^r possible values for x and each one of them corresponds to exactly one value of y – this is because $y = -y$ and $(\pm y)^2 = y^2$). Adding one other solution for the point at infinity we finally have $N_r = 2^r + 1$.

What remains is to calculate the corresponding Zeta-function:

$$\begin{aligned} \sum_{r=1}^{\infty} N_r \frac{T^r}{r} &= \sum_{r=1}^{\infty} (2^r + 1)\frac{T^r}{r} = \sum_{r=1}^{\infty} \frac{(2T)^r}{r} + \sum_{r=1}^{\infty} \frac{T^r}{r} = \\ &= -\log(1-2T) - \log(1-T) = -\log((1-2T)(1-T)) \end{aligned}$$

and therefore

$$\begin{aligned} Z(E_n/\mathbb{F}_2, T) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right) = \\ = \exp(-\log((1-2T)(1-T))) = \frac{1}{(1-2T)(1-T)}. \end{aligned}$$

Case $p \mid n$. We can also assume that $p \neq 2$ since then we can use the previous case. Considering such a field $\mathbb{F}_{p^r}$ will reduce the equation of $E_n : y^2 = x^3 - n^2x$ into $y^2 = x^3$, so we have to calculate the number of solutions to this equation

over $\mathbb{F}_{p^r}$. Again (0,0) is a solution and we can look at $\tilde{\mathbb{F}} := \mathbb{F}_{p^r}\backslash\{0\}$. We now need to consider two cases: when 3 divides the order of $\tilde{\mathbb{F}}$ and when it does not.

If $3 \nmid p^r - 1$ we consider an endomorphism

$$\begin{aligned} f\colon \tilde{\mathbb{F}} &\to \tilde{\mathbb{F}} \\ x &\mapsto x^3. \end{aligned}$$

Then the kernel of f if trivial (by the same argumentation as in the case when $p = 2$) so every element from $\tilde{\mathbb{F}}$ is a cube. This means, that the number of solutions to $y^2 = x^3$ is the same as to $y^2 = x$ which is $p^r - 1$ because for every $y \in \tilde{\mathbb{F}}$ there exists only one $x \in \tilde{\mathbb{F}}$ for which the second equation holds.

If $3 \mid p^r - 1$ then since p is odd, we actually have that $6 \mid p^r - 1$. If we consider an endomorphism

$$\begin{aligned} f\colon \tilde{\mathbb{F}} &\to \tilde{\mathbb{F}} \\ x &\mapsto x^6. \end{aligned}$$

then the kernel of f is a subgroup $\{1, a, a^2, a^3, a^4, a^5\}$ for some $a \in \tilde{\mathbb{F}}$. This implies that $|\mathrm{im}(f)| = \frac{p^r-1}{6}$. Therefore, we have $\frac{p^r-1}{6}$ sixth powers and each one of them is created by exactly 6 different elements in $\tilde{\mathbb{F}}$. Putting all of this together means that in this case we also have $p^r - 1$ solutions to $y^2 = x^3$.

In both cases we have $p^r - 1$ solutions from $\tilde{\mathbb{F}}$, then one solution for (0,0) and finally one solution for the point at infinity. Overall, we have $p^r + 1$ total solutions and the corresponding Zeta-function is in the form of:

$$\begin{aligned} \sum_{r=1}^{\infty} N_r \frac{T^r}{r} &= \sum_{r=1}^{\infty} (p^r + 1)\frac{T^r}{r} = \sum_{r=1}^{\infty} \frac{(pT)^r}{r} + \sum_{r=1}^{\infty} \frac{T^r}{r} = \\ &= -\log(1 - pT) - \log(1 - T) = -\log((1 - pT)(1 - T)) \end{aligned}$$

$$\implies Z(E_n/\mathbb{F}_p, T) = \exp(-\log((1 - pT)(1 - T))) = \frac{1}{(1 - pT)(1 - T)}.$$

□

Definition 6.5. Let $s \in \mathbb{C}$ and $E/\mathbb{Q}$ an elliptic curve. We define the *Hasse–Weil L-function* $L(E, s)$ as:

$$L(E, s) = \frac{\zeta(s)\zeta(s - 1)}{\prod_{p\in\mathbb{P}} Z(E/\mathbb{F}_p, p^{-s})}$$

where $\mathbb{P}$ stands for the set of primes.

As for Zeta-functions, the L-functions can also be rewritten in a bit easier to work with equivalent form which is given by the following proposition.

Proposition 6.6. *Let $s \in \mathbb{C}$ and $E_n/\mathbb{Q}$ an elliptic curve. Then the Hasse–Weil L-function of this special type of elliptic curves can be written in the form:*

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

Proof.

$$L(E_n, s) = \frac{\zeta(s)\zeta(s-1)}{\prod_{p\in\mathbb{P}} Z(E_n/\mathbb{F}_p, p^{-s})} = \\ = \zeta(s)\zeta(s-1)\frac{1}{\prod_{p|2n} Z(E_n/\mathbb{F}_p, p^{-s})}\frac{1}{\prod_{p\nmid 2n} Z(E_n/\mathbb{F}_p, p^{-s})}$$

The denominator of Zeta-function $Z(E_n/\mathbb{F}_p, T)$ is always $(1-T)(1-pT)$ no matter the value of p, thus from the expression above we can factor out the product $\prod_{p\in\mathbb{P}}\left(\left(1-p^{-s}\right)\left(1-p^{-s+1}\right)\right)$. The Proposition 6.4 states that the Zeta-functions in the first product all have numerators equal to 1 therefore after we have factored out the denominators, we are left with 1. The Proposition 6.3 on the other hand tells us that what is left of the second product are terms of the form $(1-a_{E_n,p}p^{-s}+p^{1-2s})^{-1}$. Putting it all together we have

$$L(E_n, s) = \zeta(s)\zeta(s-1)\frac{1}{\prod_{p|2n} Z(E_n/\mathbb{F}_p, p^{-s})}\frac{1}{\prod_{p\nmid 2n} Z(E_n/\mathbb{F}_p, p^{-s})} = \\ = \zeta(s)\zeta(s-1)\prod_{p\in\mathbb{P}}\left(\left(1-\frac{1}{p^s}\right)\left(1-\frac{1}{p^{s-1}}\right)\right)\prod_{p\nmid 2n}\frac{1}{(1-a_{E_n,p}p^{-s}+p^{1-2s})} = \\ = \prod_{p\nmid 2n}\frac{1}{(1-a_{E_n,p}p^{-s}+p^{1-2s})}$$

since the Riemann Zeta-function is defined as:

$$\zeta(s) = \prod_{p\in\mathbb{P}}\frac{1}{1-p^{-s}} = \prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^s}\right)^{-1}.$$

□

Lemma 6.7. *Let $\{a_i\}_{i=1}^{\infty}$ be a sequence of positive real numbers. If the sum $\sum_{i\in\mathbb{N}}\log(a_i)$ converges, then the product $\prod_{i\in\mathbb{N}} a_i$ converges to non-zero real number.*

Proof. Suppose that the sum $\sum_{i\in\mathbb{N}}\log(a_i)$ converges. Then the value of the expression $\exp\left(\sum_{i\in\mathbb{N}}\log(a_i)\right)$ also converges, this time to a non-zero real number. Since exp is continuous we can quick manipulation this expression to get:

$$\exp\left(\sum_{i\in\mathbb{N}}\log(a_i)\right) = \prod_{i\in\mathbb{N}} e^{\log(a_i)} = \prod_{i\in\mathbb{N}} a_i.$$

The left-hand side is a non-zero real number and therefore so is the right-hand side. □

Proposition 6.8. *Let $E_n/\mathbb{F}_p$ be an elliptic curve. Its corresponding L-function $L(E_n, s)$ converges for $\mathrm{Re}(s) > \frac{3}{2}$.*

Proof. From Proposition 6.6 we have that $L(E_n, s) = \prod_{p\nmid 2n}\frac{1}{1-a_{E_n,p}p^{-s}+p^{1-2s}}$. By the convergence criterion from Lemma 6.7 we know that this product converges to

a non-zero real number if the sum $\sum_{p\nmid 2n} \log\left(\frac{1}{1-a_{E_n,p}p^{-s}+p^{1-2s}}\right)$ converges. We can manipulate this sum as such:

$$\sum_{p\nmid 2n} \log\left(\frac{1}{1-a_{E_n,p}p^{-s}+p^{1-2s}}\right) = -\sum_{p\nmid 2n} \log\left(1-a_{E_n,p}p^{-s}+p^{1-2s}\right) = \\ = -\sum_{p\nmid 2n} \log\left(1+\left(-a_{E_n,p}p^{-s}+p^{1-2s}\right)\right)$$

which converges if and only if the sum $\sum_{p\nmid 2n} -a_{E_n,p}p^{-s}+p^{1-2s}$ converges. We have an upper bound on $a_{E_n,p}$ from Hasse's theorem (Theorem 5.2) so we have

$$\sum_{p\nmid 2n} \left|\frac{p^{1-s}-a_{E_n,p}}{p^s}\right| \leq \sum_{p\nmid 2n} \frac{p^{\mathrm{Re}(1-s)}+|a_{E_n,p}|}{p^{\mathrm{Re}(s)}} \leq \\ \leq \sum_{p\nmid 2n} \frac{p^{1-\mathrm{Re}(s)}+2\sqrt{p}}{p^{\mathrm{Re}(s)}} = \sum_{p\nmid 2n} \frac{p^{\frac{1}{2}-\mathrm{Re}(s)}+2}{p^{\mathrm{Re}(s)-\frac{1}{2}}}$$

which converges absolutely if and only if $\mathrm{Re}(s)-\frac{1}{2}>1$, equivalently saying $\mathrm{Re}(s)>\frac{3}{2}$. □

Luckily, these L-functions can be analytically extended to whole complex plane $\mathbb{C}$, which can be seen, for example, in [Kob93, Chapter 2, page 84]. This will be essential for us later since we will need to get the value of L-functions at $s=1$.

The L-function admits the Euler product and so after a bit of manipulation terms corresponding to individual primes, we can rewrite the product as:

$$L(E_n,s)=\sum_{m=1}^{\infty} b_{m,n}m^{-s}.$$

This form of L-function is called Dirichlet series and we will use the terms $b_{m,n}$ later in the text to estimate some values of L-functions for some examples of elliptic curves.

Theorem 6.9 ([CW77, Theorem 1])**.** *Let E be any elliptic curve defined over $\mathbb{Q}$. If E has infinitely many $\mathbb{Q}$-points, then $L(E,1)=0$.*

Corollary 6.10. *Let n be a natural number. If n is congruent then $L(E_n,1)=0$.*

Proof. Immediate consequence of Theorem 6.9 and Theorem 4.7. □

This is rather powerful consequence which can be used (with the help of a few calculations) to show if a number is not congruent simply by bounding the value of corresponding L-function away from zero.

There is exists slightly better form of the sum for specific values of n. We will show an upper bound on the error term made after summing the first M entries.

Proposition 6.11. *The value of Hasse–Weil L-function at $s=1$ of the elliptic curve E_n for square-free $n\equiv 1,2,3 \pmod 8$ is given by:*

$$L(E_n,1)=2\sum_{m=1}^{\infty}\frac{b_{m,n}}{m}e^{-\frac{\pi m}{\gamma}} \text{ where } \gamma=\begin{cases}2n\sqrt{2} & n \text{ odd}\\ 2n & n \text{ even}\end{cases}$$

Moreover $|b_{m,n}|\leq \sigma_0(m)\sqrt{m}$, where $\sigma_0(m)$ denotes the number of divisors of m.

Proof. See [Kob93, Chapter 2, Proposition 13]. □

Definition 6.12. Let $R_{M,n} = 2\sum_{m\geq M} \frac{b_{m,n}}{m} e^{-m\frac{\pi}{\gamma}}$.

We will use this notion of $R_{M,n}$ to calculate approximate values of L-functions. To do so, we will in the rest of this chapter derive the upper bound of $R_{M,n}$.

Lemma 6.13. *For all natural numbers m the value $\sigma_0(m)$ is bounded from above by $\sigma_0(m) \leq 2\sqrt{m}$.*

Proof. Given $m \in \mathbb{N}$ we know that its divisors come in pairs: if x is divisor of m then so is m/x. The number of such pairs is at most $\sqrt{m}$ since if $x \geq \sqrt{m}$ then $m/x \leq \sqrt{m}$. Therefore, we have at most $2\sqrt{m}$ divisors (2 for each pair) which is an upper bound for $\sigma_0(m)$. □

Lemma 6.14.

$$|R_{M,n}| \leq \frac{4}{1-e^{-\frac{\pi}{\gamma}}} e^{-M\frac{\pi}{\gamma}}$$

Proof.

$$\begin{aligned}
|R_{M,n}| &= \left|2\sum_{m=M}^{\infty} \frac{b_{m,n}}{m} e^{-m\frac{\pi}{\gamma}}\right| \leq 2\sum_{m=M}^{\infty} \left|\frac{b_{m,n}}{m} e^{-m\frac{\pi}{\gamma}}\right| = \\
&= 2\sum_{m=1}^{\infty} \left|\frac{b_{m+M-1,n}}{m+M-1} e^{-m\frac{\pi}{\gamma}} e^{(1-M)\frac{\pi}{\gamma}}\right| < \\
&< 2e^{(1-M)\frac{\pi}{\gamma}} \sum_{m=1}^{\infty} \frac{\sigma_0(m+M-1)\sqrt{m+M-1}}{m+M-1} e^{-m\frac{\pi}{\gamma}} \leq \\
&\leq 2e^{(1-M)\frac{\pi}{\gamma}} \sum_{m=1}^{\infty} \frac{2(m+M-1)}{m+M-1} e^{-m\frac{\pi}{\gamma}} = 4e^{(1-M)\frac{\pi}{\gamma}} \sum_{m=1}^{\infty} (e^{-\frac{\pi}{\gamma}})^m = \\
&= 4e^{M\frac{\pi}{\gamma}} \sum_{m=0}^{\infty} (e^{-\frac{\pi}{\gamma}})^m = \frac{4}{1-e^{-\frac{\pi}{\gamma}}} e^{M\frac{\pi}{\gamma}}
\end{aligned}$$

where we used bounds for $b_{m,n}$ from Proposition 6.11, $\sigma_0(m)$ from Lemma 6.13 and in the last step we used the sum formula for geometrical series. □

Before diving into some concrete examples let us to the end of this chapter mention one of the most famous open problems surrounding elliptic curves and L-functions.

Conjecture (Birch and Swinnerton-Dyer (BSD))**.** *Let E be an elliptic curve of rank r defined over $\mathbb{Q}$. Then the order of zero at $s = 1$ of the Hasse–Weil L-function $L(E, s)$ is precisely equal to r.*

Only a little bit of progress has been made so far. One notable result is due to Gross – Zagier ([GZ85, Theorem 7.3]) who showed in 1986 that if the zero at $s = 1$ of $L(E, s)$ is of order 1 then $E(\mathbb{Q})$ has a point of infinite order. Another notable result is by Kolyvagin ([KL89, Theorem 0.1]) which came 3 years later shows that if $L(E, 1) \neq 0$ then E has rank 0 over $\mathbb{Q}$ and if $L(E, 1) = 0$ is a zero of order equal to 1, then E has rank 1 over $\mathbb{Q}$.

There are some other very interesting results which give some insight into this conjecture, but only these two specifically call out the rank and order of zeros.

We therefore only know that the BSD conjecture holds for $r = 0, 1$ and only in one implication.

One last interesting fact to mention is that if $n \equiv 5, 6, 7 \pmod 8$ and one assumes that the BSD conjecture is true for E_n, then n is congruent (see [Kob93, Chapter 2 Proposition 2] for proof).

7. Examples/Calculations

In this chapter we will present computations of some L-functions and subsequently determine which numbers up to 20 are congruent and which are not. At the end we will also show a simple algorithm which generates congruent numbers.

Proposition 7.1. *1 is not a congruent number.*

Proof. With the help of newly obtained tools, the L-functions, we may approach the problem as following. The $b_{1,n}$ term is always 1 no matter the curve we focus on. Therefore, using the Proposition 6.11 we compute that

$$L(E_1, 1) = 2e^{-\frac{\pi}{2\sqrt{2}}} + R_{2,1} \approx 0.65864 + R_{2,1}.$$

We have an upper bound for $R_{2,1}$ from Lemma 6.14 which in this case is $|R_{2,1}| < 0.65$, therefore even if all of the other $b_{m,1}, m \geq 2$ terms were with negative sign, the value of $L(E_1, 1)$ cannot reach zero. This means that the value $L(E_1, 1) \neq 0$ and so Corollary 6.10 implies that 1 is not a congruent number. □

Recall that we have seen an alternative proof of this proposition back in Chapter 2 in Proposition 2.2. A consequence of that proof is special case of Fermat's Last Theorem, namely for $n = 4$: if there existed a triple (X, Y, Z) such that $X^4 + Y^4 = Z^4$, then we would also have a solution to the equation in the form of $Z^4 - Y^4 = (X^2)^2$ which contradicts second part of mentioned proof. One small detail which has to be noted is that in the proposition we proved that no such triple (X, Y, Z) exists if X is odd, but fortunately can without loss of generality assume that X is indeed odd, otherwise we would switch it with Y (should both X and Y be even then so must be Z and therefore we could divide all of the numbers by 2 to get smaller triple).

Overall, there may be other methods to show (non)-congruence of numbers like with the case of 1, but using L-functions is a much faster way.

One useful observation while computing L-functions is that if we look at the structure of the L-function in Proposition 6.6 we see that since the number 2 divides $2n$ it is not included in the product. This means that for every even $k \in \mathbb{N}$ the term $b_{2k,n}$ is zero. In the same spirit if p divides $2n$ then for every $m \in \mathbb{N} : b_{pm,n} = 0$.

Proposition 7.2. *2 is not a congruent number.*

Proof. Let us proceed in the same way as in previous case.

$$L(E_2, 1) = 2e^{-\frac{\pi}{4}} + R_{2,2} \approx 0.91187 + R_{2,2}.$$

but now $|R_{2,2}| > 1.5$ so we cannot conclude anything so far. Luckily $b_{2,n} = 0$ so we can replace $R_{2,2}$ with $R_{3,2}$ since the next term adds zero to the sum. Now $|R_{3,2}| < 0.7$ and so as before the value of this L-function cannot be zero so 2 is not congruent. □

Proposition 7.3. *3 is not a congruent number.*

Proof. As before if we calculate the first term of the sum and get

$$L(E_3, 1) = 2e^{-\frac{\pi}{6\sqrt{2}}} + R_{2,3} \approx 1,38114 + R_{2,3}.$$

Unfortunately, the bound on $|R_{2,3}|$ from the Lemma 6.14 is too high (numerically $\frac{4}{1-e^{-\frac{\pi}{6\sqrt{2}}}} e^{-\frac{\pi}{3\sqrt{2}}} \approx 6.16465 > 6$) so we cannot conclude anything and have to continue with next terms. The values $b_{2,3}, b_{3,3}$ and $b_{4,3}$ are all zero since 2 and 3 divide $2n = 6$, but upgrading the error term to $R_{5,3}$ is still not sufficient since its bound is greater than 2. Let us calculate the value of $b_{5,3}$ for which we need to know the value $a_{E_3,5}$. We can utilize the Example 7 from the end of Chapter 5 where we have already calculated the number of $\mathbb{F}_5$-points and its corresponding value $a_{E_n,5}$, which in this case with $n = 3$ gives $a_{E_3,5} = 2$. To obtain the next terms we expand the product $L(E_3, 1)$ as

$$\begin{aligned} L(E_3, 1) &= \frac{1}{1 - 2 \cdot 5^{-s} + 5^{1-2s}} \frac{1}{1 + 7^{1-2s}} \frac{1}{1 + 11^{1-2s}} \frac{1}{1 + 6 \cdot 13^{-s} + 13^{1-2s}} \cdots = \\ &= 1 + 2 \cdot 5^{-s} - 6 \cdot 13^{-s} - 2 \cdot 17^{-s} - 5 \cdot 25^{-s} + \cdots . \end{aligned}$$

From this expansion we get that $b_{5,3} = 2$. The value is now:

$$L(E_3, 1) = 2e^{-\frac{\pi}{6\sqrt{2}}} + \frac{4}{5} e^{-\frac{5\pi}{6\sqrt{2}}} + R_{7,3} \approx 1.50678 + R_{7,3}$$

and because

$$|R_{7,3}| < 0.97$$

we again conclude that 3 is not congruent because $L(E_3, 1)$ cannot be equal to zero. □

Proposition 7.4. *4 is not a congruent number.*

Proof. We cannot use the Theorem 6.11 since $n \not\equiv 1, 2$ nor $3 \pmod 8$. Fortunately, n is not a square-free number since 4 is a square number itself. It is therefore equivalent to 1 modulo $(\mathbb{Q}^*)^2$ and so is also not a congruent number. □

In fact, no square number is congruent since it is always equivalent to 1 modulo $(\mathbb{Q}^*)^2$.

Proposition 7.5. *5, 6 and 7 are congruent numbers.*

Proof. We have already seen a proof of this proposition for 5 and 6 back in Chapter 2 at the beginning with triangles $(\frac{40}{6}, \frac{9}{6}, \frac{41}{6})$ for 5 and $(3, 4, 5)$ for 6. For the number 7 one can find the triangle $(\frac{175}{60}, \frac{288}{60}, \frac{337}{60})$. □

Proposition 7.6. *8, 9, 12, 16 and 18 are not congruent numbers.*

Proof. We have

$$\begin{aligned} 16 \equiv 9 \equiv 1 \pmod{(\mathbb{Q}^*)^2} \\ 18 \equiv 8 \equiv 2 \pmod{(\mathbb{Q}^*)^2} \\ 12 \equiv 3 \pmod{(\mathbb{Q}^*)^2} \end{aligned}$$

therefore, none of the numbers are congruent. □

Proposition 7.7. *10, 11, 17 and 19 are not congruent numbers.*

Proof. Number 10. The following is a table of $\mathbb{F}_p$-points and corresponding values of $a_{E_{10},p}$ for primes $p \leq 17, p \nmid 20$:

p	3	7	11	13	17
$\#E_{10}(\mathbb{F}_p)$	4	8	12	8	20
$a_{E_{10},p}$	0	0	0	6	-2

From this we obtain the values of $b_{m,10}$:

m	1	3	5	7	9	11	13	15	17
$b_{m,10}$	1	0	0	0	-3	0	6	0	-2

and after summation of the first 17 terms:

$$L(E_{10},1) = 2\sum_{m=1}^{17} \frac{b_{m,10}}{m} e^{-\frac{\pi m}{20}} + R_{19,10} \approx 1.65061 + R_{19,10}$$

with $|R_{19,10}| < 1.4$. Thus $L(E_{10},1)$ cannot be zero and again due to Corollary 6.10, 10 is not congruent.

Number 11. Similar tables can be constructed for the number 11:

p	3	5	7	13	17	19	23	29	31	37
$\#E_{11}(\mathbb{F}_p)$	4	8	8	20	20	20	24	20	32	40
$a_{E_{11},p}$	0	-2	0	-6	-2	0	0	10	0	-2

m	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39
$b_{m,11}$	1	0	-2	0	-3	0	-6	0	-2	0	0	0	-5	0	10	0	0	0	-2	0

For the summation:

$$L(E_{11},1) = 2\sum_{m=1}^{37} \frac{b_{m,11}}{m} e^{-\frac{\pi m}{22\sqrt{2}}} + R_{40,11} \approx 0.76795 + R_{40,11}$$

and $|R_{40,11}| < 0.74$ which implies that 11 is not congruent.

Number 17. In this case we will have to sum up the first 49 terms until $|R_{M,n}|$ will be sufficiently small. We have:

p	3	5	7	11	13	19	23	29	31	37	41	43	47
$\#E_{17}(\mathbb{F}_p)$	4	4	8	12	8	20	24	20	32	36	32	44	48
$a_{E_{17},p}$	0	2	0	0	6	0	0	10	0	2	-10	0	0

and the table for $b_{m,17}$:

m	1	5	9	13	25	29	37	41	45	49
$b_{m,17}$	1	2	-3	6	-5	10	2	-10	6	-7

(where we show only non-zero terms to conserve space)

Approximating $L(E_{17}, 1)$ in this case goes as follows:

$$L(E_{17}, 1) = 2 \sum_{m=1}^{49} \frac{b_{m,17}}{m} e^{-\frac{\pi m}{34\sqrt{2}}} + R_{50,17} \approx 2.47926 + R_{50,17}$$

and $|R_{50,17}| < 2.42 \implies 17$ is not congruent.

Number 19. The number of terms we need to sum grows quite fast where now we have to sum up the first 85 terms to obtain a sufficiently small bound on $|R_{M,n}|$:

p	3	5	7	11	13	17	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83
$\#E_{19}(\mathbb{F}_p)$	4	8	8	12	20	16	24	20	32	36	52	44	48	68	60	72	68	72	80	80	84
$a_{E_{19},p}$	0	-2	0	0	-6	2	0	10	0	2	-10	0	0	-14	0	-10	0	0	-6	0	0

and the table for $b_{m,19}$:

m	1	5	9	13	17	25	29	37	41	45	49	53	61	65	73	85
$b_{m,19}$	1	-2	-3	-6	2	-5	10	2	-10	-6	-7	-14	-10	-12	-6	4

$$L(E_{19}, 1) = 2 \sum_{m=1}^{85} \frac{b_{m,19}}{m} e^{-\frac{\pi m}{38\sqrt{2}}} + R_{87,19} \approx 0.474 + R_{87,19}$$

with $|R_{87,19}| < 0.44 \implies 19$ is not congruent. □

Proposition 7.8. *13, 14 and 15 are congruent numbers.*

Proof. Triangles which show the congruence property for these numbers are: $(\frac{323}{30}, \frac{780}{323}, \frac{106921}{9690})$ for number 13, $(\frac{21}{2}, \frac{8}{3}, \frac{65}{6})$ for number 14 and $(\frac{15}{2}, 4, \frac{17}{2})$ for number 15. All of these we found thanks to the already mentioned algorithm shown after the next proposition. □

Proposition 7.9. *20 is a congruent number.*

Proof. Similarly to previous numbers like 12 or 18 we have equivalence

$$20 \equiv 5 \pmod{(\mathbb{Q}^*)^2}$$

and since 5 is a congruent number 20 is also. □

Example 8. Except for numbers 5 and 6, all of the triangles from previous propositions, which show the congruence property, were generated by an algorithm. Pseudo-code goes as following:

```
congruent_numbers = set()

x = 1
while True:
    for y in range(1,x):
        if (gcd(x,y) == 1) and (x mod 2 != y mod 2):
            n = remove_squares(x*y*(x**2-y**2))
            congruent_numbers.add(n)
            #a, b = x**2-y**2, 2*x*y
    x += 1
```

The algorithm lists through all primitive Pythagorean triples (A, B, C) which we know can be generated by pair of coprime numbers x, y via the map $(x, y) \to (x^2 - y^2, 2xy, x^2 + y^2)$. This triangle then has area equal to $\frac{1}{2}(x^2 - y^2) \cdot 2xy = xy(x^2 - y^2)$. If we then divide $xy(x^2 - y^2)$ by the largest possible square of an integer which divides it (in other words calculating remainder mod $(\mathbb{Q}^*)^2$) with the `remove_squares()` function we are left with a square-free representative of one of the equivalence classes of congruent numbers.

Until a number shows up, one cannot know if some specific number is indeed congruent. For example, the right triangle $(\frac{8897}{360}, \frac{720}{287}, \frac{2566561}{103320})$ of area 31 first shows up in the iteration when $x = 1600$ so some numbers really take time.

At last, we will show a program which runs in SageMath that either outputs user that inputted N is not congruent or prints an example of Pythagorean triangle with are N:

```
n = N
E = EllipticCurve([-n^2,0])
if E.rank() > 0:
    P = E.gens()
    Q = P[0]*2
    x = Q[0]
    print(sqrt(x+n)-sqrt(x-n),sqrt(x+n)+sqrt(x-n),2*sqrt(x))
else:
    print(f"{n} is not congruent")
```

Unfortunately, this code also has disadvantages. Those are computer impressions as for example SageMath struggles with the input as low as $n = 155$ and throws an error.

Bibliography

[CW77] John Coates and Andrew Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Inventiones mathematicae*, 39(3):223–251, 1977.

[GZ85] Benedict Gross and Don Zagier. Heegner points and derivatives of L-series. 1985.

[Has36] Helmut Hasse. Zur theorie der abstrakten elliptischen funktionenkörper iii. die struktur des meromorphismenrings. die riemannsche vermutung. *Journal für die reine und angewandte Mathematik*, 175:193–208, 1936.

[KL89] Victor A Kolyvagin and Dmitry Yu Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.

[Kob93] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97. Springer Science & Business Media, 1993.

[Maz78] Barry Mazur. Rational isogenies of prime degree. *Inventiones mathematicae*, 44:129–162, 1978.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[ST92] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992.