Super Congruences

Master's Thesis Mathematical Sciences

Universiteit Utrecht

Department of Mathematics

Author:
Thomas Attema

Supervisor:
Prof. Dr. Frits Beukers
Second Reader:
Prof. Dr. Gunther L.M. Cornelissen

Abstract

In 2011 the Chinese mathematician Zhi-Wei Sun published an article containing 100 open conjectures about congruences involving hypergeometric sums. It happens to be the case that we can relate many of these congruences to the number of points on elliptic curves with complex multiplication. The complex multiplication property of these elliptic curves will give us a way to find the number of $\mathbb{F}_p$-points on these elliptic curves and by means of these cardinalities certain congruences are implied.

Preface

Number theory has always had my interest. This is why I asked Frits Beukers to be my supervisor. He first suggested another subject but later on came with the idea to write a thesis on *super congruences*. The starting point of this thesis was an article [Sun11c] of the Chinese mathematician Zhi-Wei Sun. In this article Sun collected 100 unsolved conjectures about super congruences. This thesis studies a new approach to solve some of these conjectures. At first elliptic curves were merely a tool to solve certain congruences. But since the results on this subject were very interesting a reasonable amount of this thesis is dedicated to elliptic curves. After a little work the congruences follow from the results on elliptic curves.

Acknowledgements

I would like to thank Frits Beukers for his active supervision the past year. I am very grateful for the many talks we had and for all of the useful suggestions he made. I would also like to thank Sander Dahmen, he helped solve some of the problems I encountered. Furthermore I would like to express my gratitude to the other staff members at the Department of Mathematics in Utrecht. They have taught me many courses and were always open to questions. These staff members have made the past five years at the University of Utrecht into a very pleasant and informative experience. In particular I would like to thank Gunther Cornelissen for taking the time to read my thesis. Furthermore I would like to thank Kasper Dokter for reading my thesis and suggesting some improvements.

Thomas Attema

24 June 2013

Contents

Introduction

Congruences appear very often in number theory and other fields of mathematics. Therefore congruences have been extensively studied. In this thesis we will study congruences modulo primes p. In particular we will be interested in *super congruences*. Super congruences are congruences that hold not only modulo p, but also modulo higher powers of p. These super congruences are not easily solved and require new tools.

The congruences we will study in this thesis are all related to hypergeometric sums. A hypergeometric sum is a sum $\sum_k c_k$, such that the ratio of successive terms c_{k+1}/c_k is a rational function of k. We will be interested in finite hypergeometric sums involving binomial coefficients. In particular sums of the form

$$\sum_{k=0}^{p-1} \frac{a_k}{m^k}$$

reduced modulo powers of a prime p, where a_k is a product of binomial coefficients.

The first one to study these truncated hypergeometric sums was Fernando Rodriguez-Villegas. In [RV03] Rodriguez-Villegas observed some congruences associated to truncated hypergeometric sums. He also observed the connection to certain manifolds and the number of their $\mathbb{F}_p$-points. Later Zhi-Wei Sun collected various conjectures on super congruences associated to hypergeometric sums in his paper [Sun11c]. One of the conjectures Zhi-Wei Sun published in his paper is the following one.

Conjecture ([Sun11c, A29])**.** *Let $p > 3$ be a prime. Then*

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} 256^{-m} \equiv \begin{cases} 4x^2 - 2p & \mod p^2 \quad \textit{if } \left(\frac{-2}{p}\right) = 1 \textit{ and } p = x^2 + 2y^2, \\ 0 & \mod p^2 \quad \textit{if } \left(\frac{-2}{p}\right) = -1, \textit{i.e. if } p \equiv 5, 7 \mod 8. \end{cases}$$

Here we see a hypergeometric sum on the left hand side of the congruence. The right hand side can be related to the number of $\mathbb{F}_p$-points on a specific elliptic curve. So if we are able to compute the number of $\mathbb{F}_p$-points on this elliptic curves we will be able to evaluate this hypergeometric sum modulo p. The key property that this elliptic curve possesses is complex multiplication. An elliptic curve has complex multiplication when its endomorphism ring is larger then the ring of integers $\mathbb{Z}$. The *CM*-property implies extra symmetries on the elliptic curve. These extra symmetries will enable us to find the cardinality of such elliptic curves over finite fields. The two cases of the congruence in the previous conjecture already show the relation with the endomorphism ring of the elliptic curve. The first case namely comes from the primes that split in the endomorphism ring and the second case comes from the primes that are inert in the endomorphism ring.

In chapter 1 we gather the necessary theory about elliptic curves. This enables us, in chapter 2, to compute the number of $\mathbb{F}_p$-points on elliptic curves $E/\mathbb{Q}$ with complex multiplication.

In chapter 4 we will relate these cardinalities to the hypergeometric sums as mentioned above. Before we can do this we need some extra theory about Gauss-sums and the p-adic Gamma function. This necessary theory is captured in chapter 3. Using the gathered theorems and propositions we are able to prove some congruences, some of which are super congruences.

The study of these congruences has led to conjectures about stronger results. In chapter 5 we state some conjectures on congruences modulo higher powers of primes. Some of these conjectures can be proven using the theorems in the paper [CVH91] of Coster and Van Hamme.

Chapter 1

Elliptic Curves

An elliptic curve is a non-singular projective curve of genus one with a specified point $\mathcal{O}$. Now let E be an elliptic curve over a field K. If the characteristic of K is not equal to 2 and 3 then the affine part of E/K can be written down explicitly by a short Weierstrass equation

$$E : y^2 = f(x) = x^3 + Ax + B, \tag{1.1}$$

where $A, B \in K$. From now on we will assume that $\mathrm{char}(K) \neq 2, 3$ unless specified otherwise. The elliptic curve E/K consists of all points $(x, y) \in \overline{K}^2$ satisfying this equation and the unique point $\mathcal{O}$ at infinity. The elliptic curve E/K is actually an algebraic group defined over K. The addition formulas make the set of points $E(\overline{K})$ into an additive abelian group with identity $\mathcal{O}$.

If we consider elliptic curves in short Weierstrass form the only change of variables preserving this form of the equation is given by

$$\begin{array}{lcl} x & = & u^2 x', \\ y & = & u^3 y', \\ u^4 A' & = & A, \\ u^6 B' & = & B, \end{array} \tag{1.2}$$

for some $u \in \overline{K}^{\times}$, where $\overline{K}$ is an algebraic closure of K. Here (x, y) satisfies the equation $E : y^2 = x^3 + Ax + B$ and (x', y') satisfies the equation $E' : y'^2 = x'^3 + A'x' + B'$. So we see there are not many choices for isomorphisms between elliptic curves in short Weierstrass form.

The discriminant of an elliptic curve E/K in short Weierstrass form is given by

$$\triangle(E) = -16(4A^3 + 27B^2).$$

So if we consider the change of variables as in equation 1.2 we see $\triangle(E) = u^{12}\triangle(E')$. The non-singularity of E/K is equivalent to $\triangle(E) \neq 0$. Hence if $u \in \overline{K}^{\times}$ then E is non-singular if and only if E' is non-singular.

The j-invariant of an elliptic curve is given by

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Now let E and E' be isomorphic elliptic curves. Then there exists an $u \in \overline{K}$ such that the

isomorphism between E and E' is given by a change of variables as in equation 1.2. Hence

$$\begin{aligned} j(E) &= 1728\frac{4A^3}{4A^3+27B^2} \\ &= 1728\frac{4(u^4A')^3}{4(u^4A')^3+27(u^6B')^2} \\ &= 1728\frac{4A'^3}{4A'^3+27B'^2} \\ &= j(E'). \end{aligned}$$

Therefore two isomorphic elliptic curves have the same j-invariant. We actually have the following proposition (see also [Sil09, p.45]).

Proposition 1.1. *Two elliptic curves are isomorphic over $\overline{K}$ if and only if they have the same j-invariant.*

Proof. We already saw that isomorphic curves have the same j-invariant. So let

$$\begin{aligned} E &: y^2 = x^3 + Ax + B, \\ E' &: y'^2 = x'^3 + A'x' + B' \end{aligned}$$

be elliptic curves with the same j-invariant. Hence

$$1728\frac{4A^3}{4A^3+27B^2} = 1728\frac{4A'^3}{4A'^3+27B'^2},$$

which implies

$$A^3(4A'^3+27B'^2) = A'^3(4A^3+27B'^2),$$

so

$$A^3B'^2 = A'^3B^2. \tag{1.3}$$

First suppose $AB \neq 0$. Then $j(E) = j(E') \neq 0, 1728$ and equation 1.3 shows that $A'B' = 0$ implies $A' = B' = 0$. But this can not happen since E' is non-singular and thus $\triangle(E') \neq 0$. So $A'B' \neq 0$. Now equation 1.3 can be rewritten as

$$\left(\frac{A}{A'}\right)^3 = \left(\frac{B}{B'}\right)^2.$$

Hence if we take

$$u = \left(\frac{A}{A'}\right)^{\frac{1}{4}} = \left(\frac{B}{B'}\right)^{\frac{1}{6}} \in \overline{K}^\times,$$

we obtain an isomorphism of the form as in equation 1.2.

Now suppose $A = 0$. Then $j(E) = j(E') = 0$, hence $A' = 0$. Moreover $B \neq 0$ and $B' \neq 0$, since E and E' are non-singular. So we obtain an isomorphism of the form as in equation 1.2 by taking $u = \left(\frac{B}{B'}\right)^{\frac{1}{6}} \in \overline{K}^\times$.

Finally suppose $B = 0$ then $j(E) = 1728$ and we find $A, A' \neq 0$ and $B' = 0$. So we can take $u = \left(\frac{A}{A'}\right)^{\frac{1}{4}} \in \overline{K}^\times$ to find an isomorphism. □

We say two elliptic curves E_1/K and E_2/K are isomorphic over a field L containing K if there exists an isomorphism from E_1 to E_2 defined over L.

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$. We then call any other elliptic curve over $\mathbb{Q}$ with the same j-invariant a *twist* of E. Note that any twist of E is isomorphic to E over $\overline{\mathbb{Q}}$ but not necessarily over $\mathbb{Q}$ itself. If now $j(E) \neq 0, 1728$, i.e. $A, B \neq 0$, then we see that any twist of E is given by $y^2 = x^3 + Au^4x + Bu^6$ and since this curve has to be defined over $\mathbb{Q}$ we see $u^4 \in \mathbb{Q}$ and $u^6 \in \mathbb{Q}$, therefore $u^2 \in \mathbb{Q}$. Hence if $j(E) \neq 0, 1728$ then any twist of E is given by

$$E_D : y^2 = x^3 + AD^2x + BD^3 \quad \text{for some } D \in \mathbb{Q}^\times.$$

These elliptic curves are called quadratic-twists since E and E_D are isomorphic over $\mathbb{Q}(\sqrt{D})$. If $j(E) = 0$ or $j(E) = 1728$ then also higher order twists are possible. An isomorphism between two quadratic twists is given by

$$\phi : E \longrightarrow E_D, \quad (x, y) \longmapsto (Dx, D\sqrt{D}y).$$

1.1 The group E/K

As mentioned before the set of points E/K is a group with identity element $\mathcal{O}$ at infinity. The addition formulas can be written down as quotients of polynomials. If we namely take two points (x_1, y_1) and (x_2, y_2) on the elliptic curve $E : y^2 = x^3 + Ax + B$ defined over K such that $x_1 \neq x_2$ then we can define

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2},$$

and we have $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{and} \quad y_3 = \lambda x_1 - \lambda x_3 - y_1.$$

It is an easy computation to check that these formulas define a point on E.

Now if we want to double a point (x, y) on the elliptic curve E then $2(x, y) = (x, y) + (x, y) = (x', y')$ with

$$x' = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4y^2} \quad \text{and} \quad y' = \frac{x^3 - Ax + 2B - 3x^2x' + Ax'}{2y}.$$

The final case consists of two distinct points P and Q on E with the same x-coordinates. We must then have $P = (x, y)$ and $Q = (x, -y)$. These points are inverses of each other so $P+Q = \mathcal{O}$ and $-P = Q$. These formulas define a group action on the elliptic curve E. Moreover all addition formulas are defined over K. So if two points P and Q are defined over K then so are their sum and inverses. Therefore the group E/K has a subgroup $E(K)$ of all K-rational points.

Theorem 1.2. *(**Mordell-Weil**) Let K be a number field. Then the group $E(K)$ is finitely generated.*

Proof. See [Sil09, p.207] □

By the Mordell-Weil theorem we see that the group $E(K)$ has the form

$$E(K) \cong E(K)_{tors} \times \mathbb{Z}^r,$$

where r is the rank of the group $E(K)$ and $E(K)_{tors}$ is the torsion subgroup of $E(K)$ (i.e. all points of finite order). Moreover by the Mordell-Weil theorem it follows that $E(K)_{tors}$ is finite.

From the addition formulas it follows that a point $P = (x, y) \in E$ has order 2 if and only if $y = 0$. The points P for which $2P = \mathcal{O}$ form a subgroup of E. We call this subgroup the 2-*torsion* subgroup of E and denote it by $E[2]$. Now since E/K is an additive group we can multiply points by integers. Namely for $m \in \mathbb{Z}$

$$mP = \underbrace{P + P + ... + P}_{m \text{ times}}.$$

Hence we can look at the m-torsion subgroup of E for any $m \in \mathbb{Z}$,

$$E[m] = \{P \in E : mP = \mathcal{O}\}.$$

The formulas for the multiplication by m will also be quotients of coprime polynomials in $K[x, y]$. From these polynomials the group $E[m]$ is easily deduced by setting the denominators equal to zero. Hence computing the group $E[m]$ comes down to solving polynomial equations. Note that we have

$$E_{tors} = \bigcup_{m \in \mathbb{Z}} E[m] \quad \text{and} \quad E(K)_{tors} = \bigcup_{m \in \mathbb{Z}} E(K)[m].$$

The polynomial whose roots are the x-coordinates of $E[m] \setminus \{\mathcal{O}\}$ is called the m^{th}-*division polynomial* of E/K and is denoted by ψ_m. These polynomials can be computed by using the addition formulas of the elliptic curve E/K. The division polynomials will be a useful tool in determining the torsion subgroups of elliptic curves.

We will now consider the case $K = \mathbb{Q}$. By performing a variable change as in (1.2), if necessary, any elliptic curve over $\mathbb{Q}$ can be written as

$$E : y^2 = x^3 + Ax + B \qquad \text{for some } A, B \in \mathbb{Z} \ .$$

So from now on we will assume that an elliptic curve over $\mathbb{Q}$ is given this way. Note that this also gives $\triangle(E) \in \mathbb{Z}$.

Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime. Then we can reduce A and B modulo p to obtain a curve $\overline{E} : y^2 = x^3 + \overline{A}x + \overline{B}$ over the finite field $\mathbb{F}_p$, where we use the fact that we can find a Weierstrass model with $A, B \in \mathbb{Z}$. Note that $\overline{E}$ has discriminant $\triangle(\overline{E}) = \overline{\triangle(E)} \in \mathbb{F}_p$, which might be zero. So $\overline{E}/\mathbb{F}_p$ may not be an elliptic curve since it can be singular. In particular we have that $\overline{E}$ is non-singular if and only if $p \nmid \triangle(E)$. We say E has good reduction modulo p if the elliptic curve $E/\mathbb{Q}$ has a model which reduces to a non-singular curve over $\mathbb{F}_p$. We say E has bad reduction modulo p otherwise. For the group of points of $\overline{E}/\mathbb{F}_p$ with coordinates in $\mathbb{F}_p$ we simply write $E(\mathbb{F}_p)$. Note that $E(\mathbb{F}_p)$ is a finite group since $\mathbb{F}_p$ is finite.

We can now count the number of points in $E(\mathbb{F}_p)$ the following way

$$|E(\mathbb{F}_p)| = 1 + \sum_{x \in \mathbb{F}_p} (1 + \left(\frac{x^3 + Ax + B}{p}\right)) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p}\right),$$

where we just count the number of solutions of $y^2 = x^3 + \overline{A}x + \overline{B}$ over $\mathbb{F}_p$. Here $\left(\frac{x}{p}\right)$ is the Legendre symbol defined for all $x \in \mathbb{Z}$ by

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \textit{if } x \textit{ is a quadratic residue modulo } p, \\ -1 & \textit{if } x \textit{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } p|x. \end{cases}$$

From number theory we know that

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \mod p.$$

Moreover we see, by the above formula, that

$$a(p) := -\sum_{x\in\mathbb{F}_p} \left(\frac{x^3+Ax+B}{p}\right) = p+1-|E(\mathbb{F}_p)|.$$

By the Hasse-Weil theorem (see for example [ST92, p.110]) we have the following estimate

$$|a(p)| < 2\sqrt{p},$$

for all primes p.

Also note that from the above formulas we find, for any quadratic twist E_D of E,

$$\begin{aligned} a_{E_D}(p) &= \sum_{x\in\mathbb{F}_p} \left(\frac{x^3+AD^2x+BD^3}{p}\right) \\ &= \sum_{Dx\in\mathbb{F}_p} \left(\frac{(Dx)^3+AD^2(Dx)+BD^3}{p}\right) \\ &= \left(\frac{D^3}{p}\right) \sum_{Dx\in\mathbb{F}_p} \left(\frac{x^3+Ax+B}{p}\right) \\ &= \left(\frac{D}{p}\right) a_E(p). \end{aligned}$$

1.2 Singular Cubic Curves

Let C be a cubic curve over K given by a short Weierstrass equation $y^2-x^3-Ax-B=0$ for some $A, B \in K$. We say C is singular if there exists a point $P \in C$ at which the partial derivatives of y^2-x^3-Ax-B vanish simultaneously. This means that if a cubic curve is non-singular it has a well-defined tangent line at every point. Now if these partial derivatives vanish at the point (x_0, y_0), then $y_0 = 0$ and x_0 is a double root of $f(x) = x^3+Ax+B$. Conversely if $f(x)$ has a double root at x_0, then $(x_0, 0)$ is a singular point of C.

There are two possible types of singularity depending on whether $f(x) = x^3+Ax+B$ has a double root or a triple root. When $f(x)$ has a double root at x_0, we say the singular point $(x_0, 0)$ is a *node*. In this case we can apply a coordinate change to find the following typical equation for a singular cubic curve with a node,

$$C : y^2 = x^2(x+1).$$

This curve has two distinct tangent directions in its singular point $(0, 0)$, as can be seen in the following figure. This figure displays the graph of the affine part of the singular cubic curve $C : y^2 = x^2(x+1)$ over $\mathbb{Q}$.

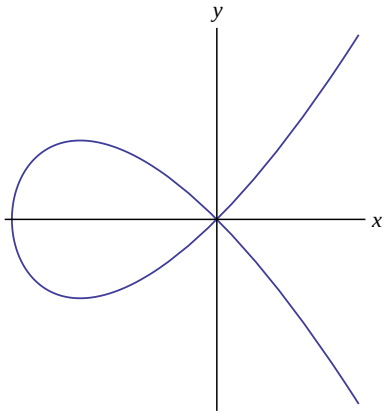

Figure 1.1: $C : y^2 = x^2(x+1)$

The other possible type of singularity happens when $f(x)$ has a triple root. After a change of coordinates we obtain the equation

$$C : y^2 = x^3.$$

This cubic curve has a singularity in $(0,0)$, which we call a *cusp*. The following figure shows the affine part of the curve $C : y^2 = x^3$ over $\mathbb{Q}$.

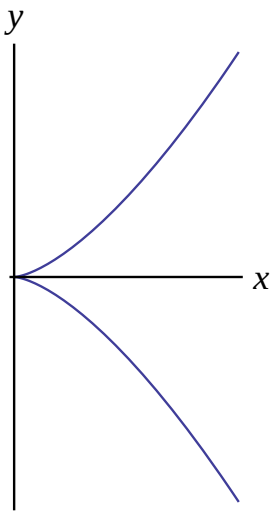

Figure 1.2: $C : y^2 = x^3$

We have already mentioned that a cubic curve is singular if and only if its discriminant equals 0. The next lemma enables us to determine the type of singularity by using the short Weierstrass equation.

Lemma 1.3. *Let $C : y^2 = x^3 + Ax + B$ be a cubic curve over a field K with $\mathrm{char}(K) \neq 2, 3$. Then*

a) C is non-singular if and only if $\triangle(C) \neq 0$,

b) C has a node if and only if $\triangle(C) = 0$ and $A \neq 0$,

c) C has a cusp if and only if $\triangle(C) = A = 0$.

Proof. See proposition 1.4 of [Sil09, p.45]. □

Remark. All quantities we define for cubic curves in short Weierstrass form are also defined for general cubic curves. The formulas for these quantities are more complicated, but the theorems and lemmas still hold in this more general case. We will however not bother the reader with these tedious formulas.

Singular cubic curves behave in a very different way from non-singular cubic curves. Any line through a singular point intersects this point with multiplicity at least two, therefore this line has at most one more intersection with the cubic curve. This means that we are able to parameterize singular cubic curves in a nice way. Lets start with the first type of singularity. We assume the cubic curve is given by $C : y^2 = x^2(x+1)$ over K. If we then take $t = \frac{y}{x}$, we find

$$(x, y) = (t^2 - 1, t^3 - t).$$

In particular we find all points of $C(K) \setminus \{\mathcal{O}\}$ by substituting different values of $t \in K$. Moreover $(t^2 - 1, t^3 - t) = (s^2 - 1, s^3 - s)$ implies either $t = s$ or $t = -s = \pm 1$. We thus find a bijection between $C(K) \setminus \{\mathcal{O}\}$ and $K \setminus \{1\}$, therefore $|C(K)| = |K|$.

If we now consider the singular cubic curve $C : y^2 = x^3$ over K, we find an even simpler parametrization by taking

$$(x, y) = (t^2, t^3).$$

Moreover $(t^2, t^3) = (s^2, s^3)$ implies $s = t$. We thus find a bijection between $C(K) \setminus \{\mathcal{O}\}$ and K.

Any singular cubic curve over $\mathbb{Q}$ with a node is isomorphic (over $\mathbb{Q}$) to a twist of $C : y^2 = x^2(x+1)$. Therefore we see that a general cubic curve C' over $\mathbb{Q}$ with a node C' is isomorphic to a curve of the form $y^2 = x^2(x + D)$ for some $D \in \mathbb{Z}$. Hence

$$C'(\mathbb{F}_p) = p + 1 - \left(\frac{D}{p}\right).$$

Since the cubic curve $C : y^2 = x^3$ has no twists other than itself we see that any cubic curve with a cusp is isomorphic to C over $\mathbb{Q}$. The following theorem now follows.

Theorem 1.4. *Let C be a singular cubic curve defined over $\mathbb{Q}$. Then C has a short Weierstrass model with coefficients in $\mathbb{Z}$. In particular $C : y^2 = x^3$ in which case*

$$|C(\mathbb{F}_p)| = p + 1,$$

or $C : y^2 = x^2(x + D)$ for some $D \in \mathbb{Z}$ in which case

$$|C(\mathbb{F}_p)| = p + 1 - \left(\frac{D}{p}\right).$$

1.3 Isogenies

We will now review some theory about maps between elliptic curves.

Definition 1.1. Let E/K and E'/K be elliptic curves. An *isogeny* from E to E' is a morphism

$$\phi : E \to E' \quad \text{such that} \quad \phi(\mathcal{O}_E) = \mathcal{O}_{E'},$$

defined over the algebraic closure $\overline{K}$. Two elliptic curves E and E' are called *isogenous* if there is an isogeny ϕ from E to E' such that $\phi(E) \neq \{\mathcal{O}_{E'}\}$.

We will see that isogenies have some nice properties. One of these properties is that isogenies are group homomorphisms. This statement is proven in theorem 4.8 of [Sil09, p.71].

Example 1.1. Let E/K be an elliptic curve. As E is an abelian group we can multiply points by integers. Since the addition formulas are quotients of polynomials in $K[x, y]$ we see that the multiplication by m map is a morphism of varieties with $m\mathcal{O} = \mathcal{O}$. So for every $m \in \mathbb{Z}$ there exists an isogeny

$$[m] : E/K \longrightarrow E/K, \qquad P \longmapsto mP.$$

Notice that the kernel of this map is exactly the m-torsion subgroup $E[m]$ of E.

A morphism between two curves is either constant or surjective (see [Sil09, p.20]). So an isogeny is either constant or surjective. Any morphism between varieties also has a degree $d \in \mathbb{Z}$. The geometric interpretation of the degree d of a morphism is that any separable morphism of degree d has d elements in its kernel. Moreover for any isogeny ϕ from E to E' of degree d there exists a unique dual isogeny $\hat{\phi}$ from E' to E such that $\hat{\phi} \circ \phi$ from E to E is given by multiplication by d (see [Sil09, III.6.1]). Hence the relation of being isogenous is actually an equivalence relation.

Example 1.2. Let $E_1 : y^2 = (x - a)(x^2 + ax + b)$ be an elliptic curve over $\mathbb{Q}$ with $a, b \in \mathbb{Z}$. And let $E_2 : y^2 = (x + 2a)(x^2 - 2ax - 7a^2 - 4b)$ be another elliptic curve. Then we have the following isogeny

$$\phi : E_1 \longrightarrow E_2, \qquad (x, y) \longmapsto \left(x + \frac{2a^2 + b}{x - a}, \left(1 - \frac{2a^2 + b}{(x - a)^2} \right) y \right).$$

It is now a simple calculation to check that this map is well-defined and indeed an isogeny.

For two elliptic curves E and E' we can now use the fact that these curves are abelian groups. We define the group of all isogenies from E to E' by

$$\mathrm{Hom}(E, E') := \{\text{isogenies from } E \text{ to } E'\}.$$

Since E' is a group, for any two isogenies ϕ, ψ there exists a new isogeny $\phi + \psi$ defined by $(\phi + \psi)(P) = \phi(P) + \psi(P)$, which implies $\mathrm{Hom}(E, E')$ is actually a group with as identity the trivial isogeny. If now $E = E'$ we can also compose isogenies, hence

$$\mathrm{End}(E) := \mathrm{Hom}(E, E)$$

is a ring. We call this ring the endomorphism ring of E. The multiplication on $\mathrm{End}(E)$ is given by the composition of morphisms. We omit here the full proof of the fact that $\phi + \psi$ is an isogeny and also the proof that $\mathrm{End}(E)$ really is a ring. For these proofs we refer to [Sil09].

As we have seen in example 1.1 there exists an endomorphism $[m]$ for every $m \in \mathbb{Z}$ and every elliptic curve E. So for every elliptic curve E we have $\mathbb{Z} \subset \mathrm{End}(E)$. However there may also exist other endomorphisms as the next example shows.

Example 1.3. Let $E : y^2 = x^3 - x$ be an elliptic curve over $\mathbb{Q}$. Then we can define the endomorphism

$$[i] : E \longrightarrow E, \qquad (x, y) \longmapsto (-x, iy).$$

This endomorphism is well defined since

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

Moreover the kernel of this endomorphism is $\{\mathcal{O}\}$, hence the isogeny $[i]$ is not given by a multiplication by m map. So $\mathrm{End}(E) \ncong \mathbb{Z}$.

Proposition 1.5. *The endomorphism ring of an elliptic curve E/K is either $\mathbb{Z}$, an order in an imaginary quadratic field or an order in a quaternion algebra. If $char(K) = 0$, then only the first two are possible and if $char(K) \neq 0$ then only the last two are possible.*

Proof. See corollary 9.4 of [Sil09, p.102] and theorem 3.1 of [Sil09, p.144]. □

There exist elliptic curves over a field with characteristic 0 such that the endomorphism ring is isomorphic to $\mathbb{Z}$. For $\text{char}(K) = 0$ we say E/K has *complex multiplication* or simply E/K is a CM-curve if the endomorphism ring is strictly larger then $\mathbb{Z}$. It is actually the case that for each of the 9 imaginary quadratic fields with class number 1 there is at least one order in that field appearing as endomorphism ring of an elliptic curve $E/\mathbb{Q}$ (see [Cre97, p.103]). Moreover all endomorphism rings of elliptic curves over $\mathbb{Q}$ are given as an order in such a field. If E/K is an elliptic curve with complex multiplication where the endomorphism ring is an order R in the quadratic imaginary field K we say "E has complex multiplication by K" or "E has complex multiplication by R." Also note that two elliptic curves over $\mathbb{Q}$ with the same j-invariant are isomorphic over $\overline{\mathbb{Q}}$. From this it follows that their endomorphism rings are isomorphic. We can now create table 1.3 in which we find a CM-curve for every possible endomorphism ring of elliptic curves over $\mathbb{Q}$.

Elliptic Curve	**Endomorphism Ring**	**j-invariant**
$E_1 : y^2 = x^3 - x$	$\mathbb{Z}[i]$	1728
$E_2 : y^2 = x^3 - 11x - 14$	$\mathbb{Z}[2i]$	66^3
$E_3 : y^2 = x^3 + 1$	$\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$	0
$E_4 : y^2 = x^3 - 15x + 22$	$\mathbb{Z}[\sqrt{-3}]$	2×30^3
$E_5 : y^2 = x^3 - 270x - 1512$	$\mathbb{Z}[\sqrt{-2}]$	20^3
$E_6 : y^2 = x^3 - 35x - 98$	$\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$	-15^3
$E_7 : y^2 = x^3 - 595x - 5586$	$\mathbb{Z}[\sqrt{-7}]$	255^3
$E_8 : y^2 = x^3 - 480x + 4048$	$\mathbb{Z}[\frac{1+3\sqrt{-3}}{2}]$	-3×160^3
$E_9 : y^2 = x^3 - 9504x + 365904$	$\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$	-32^3
$E_{10} : y^2 = x^3 - 608x + 5776$	$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$	-96^3
$E_{11} : y^2 = x^3 - 13760x + 621264$	$\mathbb{Z}[\frac{1+\sqrt{-43}}{2}]$	-960^3
$E_{12} : y^2 = x^3 - 117920x + 15585808$	$\mathbb{Z}[\frac{1+\sqrt{-67}}{2}]$	-5280^3
$E_{13} : y^2 = x^3 - 34790720x + 78984748304$	$\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$	-640320^3

Table 1.1: Elliptic Curves with Complex Multiplication

Note that these equations are not uniquely determined by their j-invariant. We could also have taken twists. These curves and their twist are the only elliptic curves over $\mathbb{Q}$ with complex multiplication. Moreover all these endomorphism rings have a field of fractions with class number 1, which implies that the integral closures of these rings are principal ideal domains. In particular the integral closures are unique factorization domains, which will be a useful property later on.

If the endomorphism ring of an elliptic curve E/K is an order in a quaternion algebra then we say E/K is *supersingular*. Notice that by proposition 1.5 we must have $\mathrm{char}(K) > 0$ for any supersingular elliptic curve E/K. Moreover if an elliptic curve is supersingular it does not mean it is singular.

For a CM-curve E with endomorphism ring $\mathbb{Z}[\alpha]$ the dual of an endomorphism $\pi \in \mathbb{Z}[\alpha]$ is given by its complex conjugate $\overline{\pi}$ (see [Sil94, p.97]). Hence the degree of an endomorphism is given by $\pi\overline{\pi}$ and since a CM-curve is defined over a field of characteristic zero we see that any morphism is separable, hence for any $\pi \in \mathbb{Z}[\alpha]$

$$|\ker(\pi)| = \pi\overline{\pi}.$$

In particular $|E[m]| = m^2$ for any $m \in \mathbb{Z}$.

By proposition 1.5 we also see that the endomorphism ring of an arbitrary elliptic curve is a ring extension of $\mathbb{Z}$. Moreover we see that $\mathrm{End}(E)$ is free of rank $1, 2$ or 4 as a $\mathbb{Z}$-algebra. Hence there exist $x_1, ..., x_n \in \mathrm{End}(E)$ that form a $\mathbb{Z}$-basis for $\mathrm{End}(E)$ for some $n \in \{1, 2, 4\}$

$$\mathrm{End}(E) \cong \mathbb{Z}x_1 \oplus \mathbb{Z}x_2 \oplus ... \oplus \mathbb{Z}x_n.$$

Now for any $x \in \mathrm{End}(E)$ we consider the $\mathbb{Z}$-linear multiplication by x map, $M_x : \mathrm{End}(E) \to \mathrm{End}(E), \quad a \mapsto xa$. With a $\mathbb{Z}$-basis as above we can describe this map by an $n \times n$ matrix with coefficients in $\mathbb{Z}$. We define the *norm* and *trace* of an element $x \in \mathrm{End}(E)$ by

$$\mathrm{N}(x) := \det M_x \quad \text{and} \quad \mathrm{Tr}(x) := \mathrm{trace}\ M_x.$$

Both the norm and the trace are independent of the choice of basis. We can also construct the *characteristic polynomial* f^x of $x \in \mathrm{End}(E)$, namely

$$f^x = \det(X\ \mathrm{Id}_{\mathrm{End}(E)} - M_x).$$

This is a monic polynomial of degree n and it has coefficients in $\mathbb{Z}$. Moreover $f^x(x) = 0$ for all $x \in \mathrm{End}(E)$. Notice also that the constant coefficient of f^x equals $(-1)^n\mathrm{N}(x)$ and that the second highest coefficient equals $-\mathrm{Tr}(x)$.

1.4 Frobenius Endomorphism

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_q$ for some prime power $q = p^n$. Because this elliptic curve is defined over a finite field we can define the so called *Frobenius endomorphism*

$$\mathrm{Fr}_q : E \longrightarrow E, \quad (x, y) \longmapsto (x^q, y^q).$$

This map is well-defined since for any $x, y \in \mathbb{F}_q$, we have $x^q = x$ and $(x + y)^q = x^q + y^q + \sum_{i=1}^{q-1} \binom{q}{i} x^i y^{q-i} = x^q + y^q$, because $p \mid \binom{q}{i}$ for all $1 \leq i \leq q - 1$ and $\mathrm{char}(\mathbb{F}_q) = p$. Hence for $(x, y) \in E$ we have

$$\begin{aligned} 0 &= y^2 - x^3 - Ax - B \\ &= (y^2 - x^3 - Ax - B)^q \\ &= (y^q)^2 - (x^q)^3 - A^q x^q - B^q \\ &= (y^q)^2 - (x^q)^3 - Ax^q - B, \end{aligned}$$

where the last equality follows since $A, B \in \mathbb{F}_q$. So $(x^q, y^q) \in E$.

Theorem 1.6. *Let $E/\mathbb{F}_q$ be an elliptic curve, let*

$$\mathrm{Fr}_q : E \to E, \quad (x, y) \mapsto (x^q, y^q),$$

be the Frobenius endomorphism and let

$$a(q) = q + 1 - |E(\mathbb{F}_q)|.$$

a) Let π and $\overline{\pi}$ be the roots of the polynomial $X^2 - a(q)X + q$. Then π and $\overline{\pi}$ are complex conjugates satisfying $|\pi| = |\overline{\pi}| = \sqrt{q}$, and for every $n \geq 1$,

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - \pi^n - \overline{\pi}^n.$$

b) The Frobenius endomorphism satisfies

$$\mathrm{Fr}_q^2 - a(q)\,\mathrm{Fr}_q + q = 0.$$

Proof. See theorem 2.3.1 of [Sil09, p.142]. □

We thus see that the trace and norm of the Frobenius endomorphism are respectively given by

$$\mathrm{Tr}(\mathrm{Fr}_q) = q + 1 - |E(\mathbb{F}_q)| \quad \text{and} \quad \mathrm{N}(\mathrm{Fr}_q) = q.$$

And the characteristic polynomial of Fr_q in $\mathrm{End}(E)$ is given by

$$P(X) = X^2 - a(q)X + q.$$

So Fr_q is a zero $\pi \in \mathrm{End}(E)$ of this polynomial. Moreover $a(q) = \pi + \overline{\pi}$ and $\pi\overline{\pi} = q$.

Note that the polynomial $P(X) = X^2 - a(q)X + q$ has discriminant $a(q)^2 - 4q$. But by the Hasse-Weil bound we have $|a(q)| < 2\sqrt{q}$ for all q. Hence the discriminant of $P(X)$ is negative and therefore is $P(X)$ irreducible in $\mathbb{Z}[X]$. Also note that we have $q = \pi\overline{\pi}$ and the number of points in $E(\mathbb{F}_q)$ is determined by π. So we can compute $|E(\mathbb{F}_q)|$ by finding the correct factorization of q in $\mathrm{End}(E)$. For elliptic curves that arise as reductions of CM-curves we have the following theorem:

Theorem 1.7. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. Let p be a prime such that p splits in K, where K is the field of fractions of $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ and such that E has good reduction modulo p. Then there exists a prime $\pi \in \mathrm{End}_{\overline{\mathbb{Q}}}(E)$ such that $p = \pi\overline{\pi}$ and*

$$|E(\mathbb{F}_p)| = p + 1 - \pi - \overline{\pi}.$$

Furthermore $\mathrm{End}_{\overline{\mathbb{F}_p}}(\overline{E}) \cong \mathrm{End}_{\overline{\mathbb{Q}}}(E)$.

Sketch of the proof. We will not give the full proof of this theorem, since it requires some tools beyond the scope of this thesis. The first important step of the proof is that the reduction modulo p induces a natural map

$$\mathrm{End}_{\overline{\mathbb{Q}}}(E) \longrightarrow \mathrm{End}_{\overline{\mathbb{F}_p}}(\overline{E}).$$

This map preserves the degrees of the endomorphisms. Now if the conditions of the theorem are fulfilled then this map is an isomorphism. So there exists a $\pi \in \mathrm{End}_{\overline{\mathbb{Q}}}(E)$ which maps to Fr_p. Hence π has the same degree as Fr_p, which is p. But over the complex numbers the degree

of π is just its norm. So $N(\pi) = \pi\overline{\pi} = p$ in $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$. The following fact we will use is that for separable endomorphisms the degree equals the cardinality of the kernel. Therefore we see

$$|E(\mathbb{F}_p)| = |\ker(1 - \mathrm{Fr}_p)| = \deg(1 - \mathrm{Fr}_p).$$

If we now again use the fact that the reduction map preserves degrees, we find

$$\begin{aligned} \deg(1 - \mathrm{Fr}_p) &= \deg(1 - \pi) \\ &= (1 - \pi)(1 - \overline{\pi}) \\ &= p + 1 - \pi - \overline{\pi}. \end{aligned}$$

□

This theorem gives a nice way to compute the number of points $E(\mathbb{F}_p)$ of an elliptic curve $E/\mathbb{Q}$ with complex multiplication. At least for primes p of good reduction that split in $\mathrm{End}(E)$. So what happens if a prime ramifies or is inert in $\mathrm{End}(E)$?

1.5 Rationality

In this section we will only consider elliptic curves over fields with characteristic zero. By proposition 1.5 this means that the endomorphism rings of these elliptic curves are orders in imaginary quadratic fields. Let E be an elliptic curve over a field K with $\mathrm{char}(K) = 0$ and let $R \subset \mathbb{C}$ such that $\mathrm{End}(E) \cong R$. Then there exists a unique isomorphism

$$[\cdot] : R \longrightarrow \mathrm{End}(E),$$

such that for any invariant differential $\omega \in \Omega_E$ (see [Sil09])

$$[\alpha]^*\omega = \alpha\omega \quad \text{for all } \alpha \in R.$$

For a proof of this statement see proposition 1.1 of [Sil94, p.97]. From this isomorphism it follows that we can denote every endomorphism by $[\alpha]$ for some unique $\alpha \in R$.

First we will prove the following useful theorem.

Theorem 1.8. *Let E_1 and E_2 be two elliptic curves over a finite field $\mathbb{F}_q$. If there exists an isogeny from E_1 to E_2 defined over $\mathbb{F}_q$ then $|E_1(\mathbb{F}_{q^n})| = |E_2(\mathbb{F}_{q^n})|$ for any $n \geq 1$.*

Proof. Let $\phi : E_1 \longrightarrow E_2$ be an isogeny defined over $\mathbb{F}_q$. And let Fr_q be the Frobenius endomorphism which acts on E_1 and on E_2 since both are defined over $\mathbb{F}_q$. Let $X^2 - aX + q$ be the characteristic polynomial of Fr_q in $\mathrm{End}(E_1)$. Since ϕ is an isogeny defined over $\mathbb{F}_q$ it is given as the quotient of two polynomials in $\mathbb{F}_q$, hence ϕ commutes with Fr_q. Moreover the multiplication by m map also commutes with ϕ since ϕ is a homomorphism of groups. So on the on hand we have

$$\phi((\mathrm{Fr}_q^2 - a\,\mathrm{Fr}_q + q)P) = \phi(0P) = \phi(\mathcal{O}_1) = \mathcal{O}_2,$$

for any $P \in E_1$. But on the other hand we have

$$\phi((\mathrm{Fr}_q^2 - a\,\mathrm{Fr}_q + q)P) = \mathrm{Fr}_q^2\,\phi(P) - a\,\mathrm{Fr}_q\,\phi(P) + q\phi(P) = (\mathrm{Fr}_q^2 - a\,\mathrm{Fr}_q + q)\phi(P).$$

So $(\mathrm{Fr}_q^2 - a\,\mathrm{Fr}_q^2 + q)\phi(P) = 0$ for any $P \in E_1$. The surjectivity of isogenies now implies $\mathrm{Fr}_q^2 - a\,\mathrm{Fr}_q^2 + q = 0$ in $\mathrm{End}(E_2)$. So the characteristic polynomials of Frobenius are the same on both curves. Then by theorem 1.6 it now follows that $|E_1(\mathbb{F}_{q^n})| = |E_2(\mathbb{F}_{q^n})|$ for any $n \geq 1$. □

Remark. The converse of this theorem holds as well. In theorem 1 of [Tat66] Tate proves the following statement from which theorem 1.8 follows.

Theorem 1.9. *Let E_1 and E_2 be two elliptic curves over a finite field k. Then the following two statements are equivalent:*

a) There exists an isogeny from E_1 to E_2 defined over k.

b) E_1 and E_2 have the same number of points defined over k' for every finite extension k' of k.

Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$ such that there exists an isogeny from E_1 tot E_2 that is defined over $\mathbb{Q}$. For primes p such that E_1 and E_2 have good reduction modulo p we see that the isogeny reduces to an isogeny from $E_1(\mathbb{F}_p)$ to $E_1(\mathbb{F}_p)$ defined over $\mathbb{F}_p$. Therefore $|E_1(\mathbb{F}_p)| = |E_2(\mathbb{F}_p)|$ for all primes p such that E_1 and E_2 have good reduction.

Example 1.4. Let $E_1 : y^2 = (x-a)(x^2+ax+b)$ be an elliptic curve over $\mathbb{Q}$ with $a, b \in \mathbb{Z}$ and let $E_2 : y^2 = (x+2a)(x^2-2ax-7a^2-4b)$ be another elliptic curve (see also example 1.1). Then we have the following isogeny

$$\phi : E_1 \longrightarrow E_2, \quad (x,y) \longmapsto \left(x + \frac{2a^2+b}{x-a}, \left(1 - \frac{2a^2+b}{(x-a)^2}\right) y \right).$$

For primes p such that E_1 and E_2 have good reduction modulo p we see by theorem 1.8 that

$$|E_1(\mathbb{F}_p)| = |E_2(\mathbb{F}_p)|.$$

Theorem 1.8 already shows the importance of some rationality questions which arise when trying to find the cardinality of an elliptic curve over a finite field. We will be interested in whether certain isogenies are defined over $\mathbb{Q}$. The following theorem gives a lot of information about the field of definition of isogenies and endomorphisms. Here E^σ is the elliptic curve obtained by applying $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}})$ to the coefficients of E and $[\alpha]_E^\sigma$ is the endomorphism obtained by applying σ to the coordinate functions.

Theorem 1.10. *a) Let $E/\overline{\mathbb{Q}}$ be an elliptic curve with complex multiplication by the ring $R \subset \overline{\mathbb{Q}}$. Then*

$$[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma} \quad \text{for all } \alpha \in R \text{ and } \sigma \in \mathrm{Aut}(\overline{\mathbb{Q}}).$$

b) Let E be an elliptic curve defined over a field $L \subset \mathbb{C}$ with complex multiplication by the quadratic imaginary field $K \subset \mathbb{C}$. Then every endomorphism of E is defined over the compositum LK.

c) Let E_1/L and E_2/L be elliptic curves defined over a field $L \subset \mathbb{C}$. Then there is a finite extension L'/L such that every isogeny from E_1 to E_2 is defined over L'.

Proof. See theorem 2.2 of [Sil94, p.105]. □

Let now $E/\mathbb{Q}$ be an elliptic curve with complex multiplication such that $\left[\sqrt{-d}\right] \in \mathrm{End}(E)$. Then for any $\sigma \in \mathrm{Aut}(\mathbb{C})$, $E^\sigma = E$ since E is defined over $\mathbb{Q}$. Moreover

$$\left[\sqrt{-d}\right]^\sigma = \left[\left(\sqrt{-d}\right)^\sigma\right] = \left[\pm\sqrt{-d}\right],$$

where the sign depends on whether σ fixes $\sqrt{-d}$ or not.

We can now twist the curve E with $\sqrt{-d}$ to obtain the quadratic twist E_{-d}. An isomorphism between these curves is given by

$$\phi : E \longrightarrow E_{-d}, \quad (x, y) \longmapsto (-dx, -d\sqrt{-d}y).$$

This isomorphism is defined over $\mathbb{Q}(\sqrt{-d})$ and since both E_{-d} and E are defined over $\mathbb{Q}$ we find another isomorphism ϕ^σ between these curves for every $\sigma \in \mathrm{Aut}(\mathbb{C})$. By the explicit formulas given for ϕ we see that $\phi^\sigma = \pm\phi$, where the sign depends on whether σ fixes $\sqrt{-d}$ or not. But this means that the isogeny

$$\phi \circ \left[\sqrt{-d}\right] : E \longrightarrow E_{-d},$$

is fixed by $\mathrm{Aut}(\mathbb{C})$. Hence the isogeny $\phi \circ \left[\sqrt{-d}\right]$ is defined over $\mathbb{Q}$. Since the isogeny ϕ is an isomorphism, this proves the following proposition.

Proposition 1.11. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication such that $\left[\sqrt{-d}\right] \in \mathrm{End}(E)$. Then there exists an isogeny defined over $\mathbb{Q}$ from E to the quadratic twist E_{-d}. Moreover the kernel of this isogeny is equal to the kernel of the endomorphism $\left[\sqrt{-d}\right]$.*

We have already found a method to determine the cardinality of $E(\mathbb{F}_p)$ when p splits in $\mathrm{End}(E)$. Of course we are also interested in the cardinality of $E(\mathbb{F}_p)$ for primes p that are inert in $\mathrm{End}(E)$. The following lemma decides whether a prime p splits, ramifies or is inert in a quadratic field extension K of $\mathbb{Q}$.

Lemma 1.12. *Let d be a square free integer, $K = \mathbb{Q}(\sqrt{d})$ and let $\mathcal{O}_K$ be the ring of integers of K. Then for an odd prime $p \in \mathbb{Z}$ we have:*

a) if $\left(\frac{\triangle}{p}\right) = -1$ then p is inert in K,

b) if $\left(\frac{\triangle}{p}\right) = 1$ then p is split in K,

b) if $\left(\frac{\triangle}{p}\right) = 0$ then p is ramified in K,

where $\triangle$ is the discriminant of K.

Proof. First suppose p is an odd prime that is not inert in K. Then

$$\begin{array}{lllll} (p) = \mathbf{p}_1\mathbf{p}_2 & \text{for prime ideals } \mathbf{p}_1 \text{ and } \mathbf{p}_2 & \Longrightarrow & \mathcal{O}_K/\mathbf{p}_1 \cong \mathbb{Z}/p\mathbb{Z} \\ \Longrightarrow & \exists a \in \mathbb{Z} : a \equiv \sqrt{d} \mod \mathbf{p}_1 & \Longrightarrow & a^2 \equiv d \mod \mathbf{p}_1 \\ \Longrightarrow & a^2 \equiv d \mod p & \Longrightarrow & \left(\frac{d}{p}\right) = 1 \text{ or } \left(\frac{d}{p}\right) = 0. \end{array}$$

Now since $\triangle = d$ if $d \equiv 1 \mod 4$ and $\triangle = 4d$ if $d \equiv 2, 3 \mod 4$ we see $\left(\frac{d}{p}\right) = \left(\frac{\triangle}{p}\right)$ for all square free integers d. Hence a) follows from the above.

Now suppose $\left(\frac{\triangle}{p}\right) = \left(\frac{d}{p}\right) = 1$ for an odd prime p. Then

$$\begin{array}{l} \exists a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\} : a^2 \equiv d \mod p \\ \Longrightarrow p \mid a^2 - d = (a - \sqrt{d})(a + \sqrt{d}) \\ \Longrightarrow (p, a - \sqrt{d})(p, a + \sqrt{d}) \subset (p). \end{array}$$

Suppose $(p, a - \sqrt{d}) = (p, a + \sqrt{d})$, then $2a = a - \sqrt{d} + a + \sqrt{d} \in (p, a - \sqrt{d}) \cap \mathbb{Z} = p\mathbb{Z}$. But this contradicts the fact that $p \nmid a$. Hence $(p, a - \sqrt{d})$ and $(p, a + \sqrt{d})$ are two distinct primes lying above p, and since K is a quadratic extension their product must equal (p). So $(p, a - \sqrt{d})(p, a + \sqrt{d}) = (p)$ and p is split in K.

Now suppose $\left(\frac{d}{p}\right) = 0$ for an odd prime p. Then $p \mid d$ so $(p, \sqrt{d})^2 = (p^2, d, p\sqrt{d}) \subset (p)$. But since d is square free we have $\gcd(d, p^2) = p$, hence $(p, \sqrt{d})^2 = p$. Therefore it follows that p is ramified in K if $\left(\frac{d}{p}\right) = 0$. □

We are now ready to prove the following theorem.

Theorem 1.13. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication given by the quadratic imaginary field $K \subset \mathbb{C}$. Let p be an odd prime such that p is inert in K and such that E has good reduction modulo p. Then*

$$|E(\mathbb{F}_p)| = p + 1.$$

Proof. We may assume that $K = \mathbb{Q}(\sqrt{-d})$ for some square free integer $d > 0$. Then there exists an $a \in \mathbb{Z}$ such that $a\sqrt{-d} \in \mathrm{End}(E)$. By proposition 1.11 this implies there exists an isogeny defined over $\mathbb{Q}$ from E to the quadratic twist E_{-da^2}. Hence by theorem 1.8

$$|E(\mathbb{F}_p)| = |E_{-da^2}(\mathbb{F}_p)|,$$

for all primes p of good reduction. Let now $a(p)$ be such that

$$|E(\mathbb{F}_p)| = p + 1 - a(p).$$

Then

$$|E_{-da^2}(\mathbb{F}_p)| = p + 1 - \left(\frac{-d}{p}\right) a(p).$$

In particular

$$\left(\frac{-d}{p}\right) a(p) = a(p),$$

for all primes p of good reduction. But by lemma 1.12

$$\left(\frac{-d}{p}\right) = -1,$$

if p is inert in K. Hence $a(p) = 0$ if p is inert in K and the theorem follows. □

Chapter 2

Cardinality Formulas

In this section we will use theorem 1.7 and theorem 1.13 to find the cardinality $|\overline{E}(\mathbb{F}_p)|$ for some elliptic curves $E/\mathbb{Q}$. We take an elliptic curve $E/\mathbb{Q}$ with complex multiplication by the quadratic imaginary field K such that E has good reduction modulo a prime p. By theorem 1.7 we then have to factor p in $\mathrm{End}(E)$ to find the cardinality of $E(\mathbb{F}_p)$. In particular theorem 1.7 shows us that if a rational prime p splits in K, then there exists a $\pi \in K$ such that $p = \pi\overline{\pi}$ and

$$|E(\mathbb{F}_p)| = p + 1 - \pi - \overline{\pi}.$$

Moreover theorem 1.13 shows us that

$$|E(\mathbb{F}_p)| = p + 1 \qquad \text{if } p \text{ is inert in } K.$$

This factorization is however not uniquely determined by p and the endomorphism ring, since we may for example multiply π with -1 to find another factorization of p. So counting the number of points comes down to finding the correct factorization of the prime p.

Lemma 1.12 gave us conditions to determine whether a prime splits or is inert in a quadratic imaginary field K. So for an elliptic curve $E/\mathbb{Q}$ with complex multiplication given by $K = \mathbb{Q}(\sqrt{-d})$ and any prime p of good reduction we have

$$|E(\mathbb{F}_p)| = p + 1 \quad \text{if} \quad \left(\frac{-d}{p}\right) = -1. \tag{2.1}$$

Proposition 2.1. *Let $E_1 : y^2 = x^3 - x$ be the elliptic curve over $\mathbb{Q}$ with complex multiplication given by $\mathbb{Z}[i]$. Then for any odd prime p*

$$|E_1(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } p \equiv -1 \mod 4, \\ p + 1 - \left(\frac{2}{p}\right) 2x & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2 + y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

Proof. First of all E_1 has discriminant $\triangle(E_1) = 64 = 2^6$, therefore E_1 has good reduction modulo all odd primes. By lemma 1.12 we see that an odd prime $p \in \mathbb{Z}$ splits in $\mathbb{Z}[i]$ if $\left(\frac{-1}{p}\right) = 1$ and is inert if $\left(\frac{-1}{p}\right) = -1$. But

$$\begin{aligned} \left(\frac{-1}{p}\right) &= 1 \iff p \equiv 1 \mod 4 \quad \text{and} \\ \left(\frac{-1}{p}\right) &= -1 \iff p \equiv -1 \mod 4. \end{aligned}$$

So the first case follows from theorem 1.13. We now assume that $p \equiv 1 \mod 4$. Hence p splits in $\mathbb{Z}[i]$. This means that we can write $p = \pi\overline{\pi}$ for some $\pi \in \mathbb{Z}[i]$. Then $\pi = a + bi$ with $a, b \in \mathbb{Z}$ and since $\mathbb{Z}[i]$ is an unique factorization domain any other factorization of p will be given by multiplying π with a unit. Since $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$ we are left with 4 candidates for the correct factorization of p, as in theorem 1.7.

Next we compute the 4^{th}-division polynomial $\psi_4(x)$ of E_1 whose roots are the x-coordinates of the points of $E_1[4] \setminus \{\mathcal{O}\}$. We find

$$\psi_4(x) = 8x(x-1)(x+1)(x^2+1)(x^2-2x-1)(x^2-2x-1),$$

with roots $\{0, \pm 1, \pm i, \pm 1 \pm \sqrt{2}\}$. Moreover if we take $f(x) = x^3 - x$ we find

$$\begin{array}{lcll} f(i) & = & -2i & = & (1-i)^2, \\ f(-i) & = & 2i & = & (1+i)^2, \\ f(1+\sqrt{2}) & = & 6+4\sqrt{2} & = & (2+\sqrt{2})^2, \\ f(1-\sqrt{2}) & = & 6-4\sqrt{2} & = & (2-\sqrt{2})^2, \\ f(-1+\sqrt{2}) & = & -6+4\sqrt{2} & = & (2i-\sqrt{-2})^2, \\ f(-1-\sqrt{2}) & = & -6-4\sqrt{2} & = & (2i+\sqrt{-2})^2, \end{array}$$

and since $f(0) = f(1) = f(-1) = 0$ we have

$$\begin{aligned} E_1[4] \;=\; & \{\mathcal{O}, (0,0), (1,0), (-1,0), (i, \pm(1-i)), (-i, \pm(1+i)), \left(2+\sqrt{2}, \pm(2+\sqrt{2})\right), \\ & \left(2-\sqrt{2}, \pm(2-\sqrt{2})\right), \left(-2+\sqrt{2}, \pm(2i-\sqrt{-2})\right), \left(-2-\sqrt{2}, \pm(2i+\sqrt{-2})\right)\}. \end{aligned}$$

Now notice that since $p \equiv 1 \mod 4$ we have $i = \sqrt{-1} \in \mathbb{F}_p$, which means there exists a square root of -1 in $\mathbb{F}_p$. Hence $\{\mathcal{O}, (0,0), (1,0), (-1,0), (i, \pm(1-i)), (-i, \pm(1+i))\} \subset E_1(\mathbb{F}_p)[4]$. And since $E_1(\mathbb{F}_p)[4]$ is a subgroup of $E_1[4]$ we see that $|E_1(\mathbb{F}_p)[4]| \in \{8, 16\}$, hence 8 divides the order of the subgroup $E_1(\mathbb{F}_p)[4]$. But this means that 8 divides the order of the group $E_1(\mathbb{F}_p)$. By theorem 1.7 it now follows for $p \equiv 1 \mod 4$ that

$$|E_1(\mathbb{F}_p)| = p + 1 - (\pi + \overline{\pi}) = p + 1 - 2a \equiv 0 \mod 8.$$

Hence if $p \equiv 1 \mod 8$ then $a \equiv 1 \mod 4$ and if $p \equiv 5 \mod 8$ then $a \equiv -1 \mod 4$.

Now notice that since $p = \pi\overline{\pi} = a^2 + b^2 \equiv 1 \mod 4$, either a or b has to be odd and they can not be both odd. By the above we see that a has to be odd. Altogether we find

$$|E_1(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } p \equiv -1 \mod 4, \\ p+1-\left(\dfrac{2}{p}\right)2x & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2+y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

Here we have used the following identity

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \mod 8, \\ -1 & \text{if } p \equiv \pm 3 \mod 8. \end{cases}$$

□

Proposition 2.2. *Let $E_2 : y^2 = x^3 - 11x - 14$ be the elliptic curve over $\mathbb{Q}$ with complex multiplication given by $\mathbb{Z}[2i]$. Then for any odd prime p*

$$|E_2(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } p \equiv -1 \mod 4, \\ p+1-\left(\frac{2}{p}\right)2x & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2+y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

Proof. The discriminant of this elliptic curves is given by $\triangle(E_2) = -2^9$, hence E_2 has good reduction modulo all odd primes. Moreover we can write

$$E_1 : y^2 = (x-1)(x^2+x),$$
$$E_2 : y^2 = (x+2)(x^2-2x-7).$$

Therefore by example 1.4 we have the following isogeny

$$\phi : E_1 \longrightarrow E_2, \quad (x,y) \longmapsto (x + \frac{2}{x-1}, \left(1 - \frac{2}{(x-1)^2}\right)y),$$

which is defined over $\mathbb{Q}$. It now follows by theorem 1.8 that

$$|E_1(\mathbb{F}_p)| = |E_2(\mathbb{F}_p)|,$$

for all odd primes p, which completes the proof. □

Proposition 2.3. *Let $E_3 : y^2 = x^3 + 1$ be the elliptic curve over $\mathbb{Q}$ with complex multiplication given by $\mathbb{Z}[\omega]$, where $\omega = \frac{1+\sqrt{-3}}{2}$. Then for any prime $p > 3$*

$$|E_3(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } p \equiv -1 \mod 3, \\ p+1-\left(\frac{x}{3}\right)2x & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2+3y^2. \end{cases}$$

Proof. First of all the discriminant of this curve is given by $\triangle(E_3) = -2^4 3^3$. Hence E_3 has good reduction modulo p for all primes p unequal to 2 and 3. Moreover by lemma 1.12 we see that p is inert in $\mathbb{Z}[\omega]$ if $\left(\frac{-3}{p}\right) = -1$ and p splits if $\left(\frac{-3}{p}\right) = 1$. By the quadratic reciprocity law we now have

$$\left(\frac{-3}{p}\right)\left(\frac{p}{3}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}} = 1.$$

Hence

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 3, \\ -1 & \text{if } p \equiv -1 \mod 3. \end{cases}$$

Which proves the proposition for the case $p \equiv -1 \mod 3$. So now assume $p \equiv 1 \mod 3$. Hence p splits in $\mathbb{Q}(\omega)$ and by theorem 1.7 we can write $p = \pi\overline{\pi}$ for some $\pi \in \mathbb{Z}[\omega]$. Let $\pi = a + b\omega$ be as in theorem 1.7.

Using the *Nagel-Lutz* theorem (see [ST92]) we can calculate the complete torsion subgroup of $E(\mathbb{Q})$, consisting of all points of finite order defined over $\mathbb{Q}$. We find that the torsion of $E(\mathbb{Q})$ is given by $\{(-1,0),(0,-1),(0,1),(2,-3),(2,3),\mathcal{O}\}$. Therefore $E(\mathbb{Q})$ contains a point of order 2 and a point of order 3. We see that by reducing the coordinates modulo p, for $p > 3$ we have

that $E(\mathbb{F}_p)$ contains a point of order 2 and a point of order 3. Hence $6 \mid |E(\mathbb{F}_p)|$ for all primes $p > 3$.

Moreover $p \equiv 1 \mod 3$ is an odd prime, hence $p \equiv 1 \mod 6$. So altogether we find

$$0 \equiv |E(\mathbb{F}_p)| \equiv p + 1 - (\pi + \overline{\pi}) \equiv 2 - 2a - b \mod 6. \tag{2.2}$$

However $\mathbb{Z}[\omega]$ is a unique factorization domain, hence any other factorization of p is given by multiplying π with a unit. We have $\mathbb{Z}[\omega]^\times = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$, which gives us 6 possible candidates for the correct factorization of p. If we can eliminate 5 of them we have determined π (up to conjugation).

By equation 2.2 we have $\pi + \overline{\pi} = 2a + b \equiv 2 \mod 6$. So b has to be even which implies that a has to be odd since $p = \pi\overline{\pi} = a^2 + ab + b^2$ is an odd prime. These congruences give us some restrictions on the factorization of p in the endomorphism ring. All other factorizations of p are found by multiplying π with a unit. Computing the other candidates gives us

$$\begin{aligned}
-\pi &\Rightarrow -\pi - \overline{\pi} \equiv -2 \mod 6, \\
\omega\pi &= a\omega + b\omega^2 = -b + (a - b)\omega, \\
-\omega\pi &= b + (b - a)\omega, \\
\omega^2\pi &= b - a - a\omega, \\
-\omega^2\pi &= a - b + a\omega.
\end{aligned}$$

Since a is odd and b is even we see that the condition $\pi + \overline{\pi} \equiv 2 \mod 6$ determines π up to conjugation. Moreover since b is even we have

$$\pi = a + b\omega = a + \frac{b}{2} + \frac{b}{2}\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}].$$

Hence $p = \pi\overline{\pi} = x^2 + 3y^2$ for some $x, y \in \mathbb{Z}$. But $2x = \pi + \overline{\pi} \equiv 2 \mod 6$ which implies $x \equiv 1 \mod 3$.

Altogether we thus find the following formula, which holds for all primes $p > 3$

$$|E_3(\mathbb{F}_p)| = \begin{cases} p + 1 & \text{if } p \equiv -1 \mod 3, \\ p + 1 - \left(\frac{x}{3}\right) 2x & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2 + 3y^2. \end{cases}$$

□

Proposition 2.4. *Let $E_4 : y^2 = x^3 - 15x + 22$ be the elliptic curve over $\mathbb{Q}$ with complex multiplication given by $\mathbb{Z}[\sqrt{-3}]$. Then for any prime $p > 3$*

$$|E_4(\mathbb{F}_p)| = \begin{cases} p + 1 & \textit{if } p \equiv -1 \mod 3, \\ p + 1 - \left(\frac{x}{3}\right) 2x & \textit{if } p \equiv 1 \mod 3 \textit{ and } p = x^2 + 3y^2. \end{cases}$$

Proof. The discriminant of E_4 is given by $\triangle(E_4) = 2^8 3^3$, hence E_4 has good reduction for all primes $p > 3$. We can now write

$$\begin{aligned}
E_3 &: y^2 = (x + 1)(x^2 - x + 1), \\
E_4 &: y^2 = (x - 2)(x^2 + 2x - 11).
\end{aligned}$$

Therefore by example 1.4 we have the following isogeny

$$\phi : E_3 \longrightarrow E_4, \quad (x, y) \longmapsto (x + \frac{3}{x+1}, \left(1 - \frac{3}{(x+1)^2}\right) y),$$

which is defined over $\mathbb{Q}$. It now follows by theorem 1.8 that

$$|E_3(\mathbb{F}_p)| = |E_4(\mathbb{F}_p)|,$$

for all primes $p \neq 2, 3$, which completes the proof. □

2.1 Multiplication by $\sqrt{-\mathrm{d}}$

For other CM-curves over $\mathbb{Q}$ we need some extra tools to find formulas as the ones in the previous section. So let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. Suppose $d \in \mathbb{Z}_{>0}$ such that $[\sqrt{-d}] \in \mathrm{End}(E)$. We will study the kernel of this endomorphism, which we denote by $E[\sqrt{-d}]$. Since $\mathrm{char}(\mathbb{Q}) = 0$ it follows that

$$|E[\sqrt{-d}]| = \deg([\sqrt{-d}]) = \left(\sqrt{-d}\right)\left(-\sqrt{-d}\right) = d.$$

Now notice that for $P \in E[\sqrt{-d}]$ we have

$$[d](P) = -[\sqrt{-d}][\sqrt{-d}](P) = \mathcal{O}.$$

So $E[\sqrt{-d}]$ is a subgroup of $E[d]$. Therefore the x-coordinates of the points in $E[\sqrt{-d}] \setminus \{\mathcal{O}\}$ are zeros of the d^{th}-division polynomial ψ_d.

Now let $E : y^2 = x^3 + Ax + B$ be a short Weierstrass equation of E for some $A, B \in \mathbb{Q}$ and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then for any $(x, y) \in E$ we have

$$\begin{aligned} 0 = \sigma(0) &= \sigma(y^2 - x^3 - Ax - B) \\ &= \sigma(y)^2 - \sigma(x)^3 - \sigma(A)\sigma(x) - \sigma(B) \\ &= \sigma(y)^2 - \sigma(x)^3 - A\sigma(x) - B, \end{aligned}$$

where the last inequality follows since $A, B \in \mathbb{Q}$. Hence for any $(x, y) \in E(\overline{\mathbb{Q}})$ we see $\sigma((x, y)) = (\sigma(x), \sigma(y)) \in E$, so σ maps $E(\overline{\mathbb{Q}})$ to $E(\overline{\mathbb{Q}})$. Since the addition formulas are defined over $\mathbb{Q}$ we see that σ defines a group isomorphism and therefore $\sigma(E[m]) = E[m]$.

Lemma 2.5. *Let E be an elliptic curve over $\mathbb{Q}$. Then the group $E[\sqrt{-d}]$ is fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.*

Proof. By proposition 1.11 we see that $E[\sqrt{-d}]$ is the kernel of an $\mathbb{Q}$-isogeny from E to its twist E_{-d}. Therefore the lemma immediately follows. □

For any point $(x, y) \in E$ we have $(x, -y) \in E$. Moreover these points are distinct when $y \neq 0$, i.e. when $(x, y) \notin E[2]$. If we take d odd, then $E[2] \cap E[d] = \{\mathcal{O}\}$. Therefore any zero of the d^{th}-division polynomial ψ_d gives us two points of $E[d]$. Moreover $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ fixes $E[\sqrt{-d}]$. Hence if we factor ψ_d over $\mathbb{Q}$ and we find a unique factor of degree $\frac{d-1}{2}$, then the zeros of this factor give us a unique set of $d - 1$ points in $E[d] \setminus \{\mathcal{O}\}$, for which the x-coordinates are fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This means that these points together with $\mathcal{O}$ form the set $E[\sqrt{-d}]$.

$E[\sqrt{-d}]$ is a subgroup with d elements. Hence if d is a prime $E[\sqrt{-d}] \cong \mathbb{Z}/d\mathbb{Z}$. In particular the field $\mathbb{Q}\left(E\left[\sqrt{-d}\right]\right)$, obtained by adding all coordinates of $E\left[\sqrt{-d}\right]$ to $\mathbb{Q}$, has

$$\mathrm{Gal}\left(\mathbb{Q}\left(E\left[\sqrt{-d}\right]\right)/\mathbb{Q}\right) \subset (\mathbb{Z}/d\mathbb{Z})^{\times}.$$

Hence $\mathbb{Q}\left(E\left[\sqrt{-d}\right]\right)$ is an abelian extension of $\mathbb{Q}$.

Theorem 2.6 (Kronecker-Weber)**.** *Let K be an abelian extension of $\mathbb{Q}$. Then there is a positive integer n such that $K \subset \mathbb{Q}(\zeta_n)$, $\zeta_n = e^{2\pi i/n}$.*

Proof. See theorem 4.1 of [Was97, p.319]. □

When we study the proof of the Kronecker-Weber theorem, as stated in [Was97], we find an even stronger result. This proof starts with an abelian extension $K/\mathbb{Q}$ and it constructs the cyclotomic field $\mathbb{Q}(\zeta_n)$, where

$$n = \prod_{p \text{ ramifies}} p^{e_p}.$$

The product is taken over all rational primes that ramify in the extension $K/\mathbb{Q}$. The next and most difficult step of the proof consists of proving that $K \subset \mathbb{Q}(\zeta_n)$.

We have thus seen that n is only divisible by primes that ramify in $K/\mathbb{Q}$. Moreover a prime ramifies in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ if and only if it divides n. It follows that, if we take n to be minimal, the primes ramifying in $\mathbb{Q}(\zeta_n)$ are exactly the primes ramifying in K. We will now assume that we always take n to be minimal when applying the Kronecker-Weber theorem.

Let now d be a prime such that $\left[\sqrt{-d}\right] \in \mathrm{End}(E)$. Then $\mathbb{Q}\left(E\left[\sqrt{-d}\right]\right)/\mathbb{Q}$ is an abelian extension and the Kronecker-Weber theorem implies the existence of a primitive root of unity ζ_n such that $\mathbb{Q}\left(E\left[\sqrt{-d}\right]\right) \subset \mathbb{Q}(\zeta_n)$. But the Galois group of $\mathbb{Q}(\zeta_n)$ is simply $(\mathbb{Z}/n\mathbb{Z})^\times$ and any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is given by $\sigma(\zeta_n) = \zeta_n^a$ for some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Furthermore we see that for a prime p of good reduction σ_p sending ζ_n to ζ_n^p acts exactly as the Frobenius endomorphism Fr_p after reduction modulo p.

Hence if we are able to determine the primitive root of unity ζ_n such that $\mathbb{Q}\left(E\left[\sqrt{-d}\right]\right) \subset \mathbb{Q}(\zeta_n)$, we will be able to determine the action of Frobenius on $E(\overline{\mathbb{F}_p})[\sqrt{-d}]$ by explicit computations in characteristic 0. This means that we will be able to determine residue class of the Frobenius endomorphism modulo $\sqrt{-d}$.

Altogether it follows that if there exists an element $\tilde{\pi} \in \mathrm{End}(E)$ such that

$$\sigma_p : E[\sqrt{-d}] \longrightarrow E[\sqrt{-d}], \quad P \longmapsto \tilde{\pi}P$$

we find $\mathrm{Fr}_p \equiv \tilde{\pi} \mod \sqrt{-d}$ and since $a(p) = \mathrm{Tr}(\mathrm{Fr}_p) = \mathrm{Fr}_p + \overline{\mathrm{Fr}_p}$ we will be able to determine $a(p)$ modulo $\sqrt{-d}$ with this information.

Proposition 2.7. *Let $E_5 : y^2 = x^3 - 270x - 1512$ be the elliptic curve over $\mathbb{Q}$ with complex multiplication given by $\mathbb{Z}[\sqrt{-2}]$. Then for any prime $p > 3$*

$$|E_5(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } p \not\equiv 1,3 \mod 8, \\ p+1-2x & \text{if } p \equiv 1,3 \mod 16 \text{ and } p = x^2+2y^2 \text{ such that } x \equiv 1 \mod 4, \\ p+1-2x & \text{if } p \equiv 9,11 \mod 16 \text{ and } p = x^2+2y^2 \text{ such that } x \equiv 3 \mod 4. \end{cases}$$

Proof. Firstly the discriminant of this curve is equal to $\triangle(E_5) = 272097792 = 2^9 3^{12}$. So E_5 has good reduction modulo all primes $p > 3$. Moreover

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,3 \mod 8 \\ 0 & \text{if } p = 2 \\ -1 & \text{otherwise.} \end{cases}$$

So the first case now follows from equation 2.1.

Next we consider the case $p \equiv 1, 3 \mod 8$. Then p splits in $\mathbb{Q}(\sqrt{-2})$, hence $p = \pi\overline{\pi}$ for some $\pi \in \mathbb{Z}[\sqrt{-2}]$. Now since $\mathbb{Z}[\sqrt{-2}]$ is a unique factorization domain and $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$ we see that the factorization is unique up to the sign of π and $\overline{\pi}$. We have $\pi = a + b\sqrt{-2}$ for some $a, b \in \mathbb{Z}$ and $p = \pi\overline{\pi} = a^2 + 2b^2$. Hence a is odd and we only have to determine the sign of a to find $a(p) = \mathrm{Tr}(\mathrm{Fr}_p) = \pi + \overline{\pi} = 2a$. Therefore it is enough to determine the residue class of a modulo 4.

To determine this residue class we will consider the endomorphism $[2\sqrt{-2}] : E_5 \to E_5$. For a point $P \in E_5[2\sqrt{-2}]$ we see $4P = [\sqrt{-2}][2\sqrt{-2}]P = \mathcal{O}$, hence $E_5[2\sqrt{-2}] \subset E_5[4]$. Moreover $E_5[2] \subset E_5[2\sqrt{-2}]$. But we can compute the x-coordinates of $E_5[2]$ by solving

$$x^3 - 270x - 1512 = (x + 12)(x^2 - 12x - 126) = 0.$$

We find

$$E_5[2] = \{\mathcal{O}, (-12, 0), (6 - 9e^{4\pi i/16} + 9e^{12\pi i/16}, 0), (6 + 9e^{4\pi i/16} - 9e^{12\pi i/16}, 0)\}.$$

We also know that the degree of the endomorphism $[2\sqrt{-2}]$ is 8, hence $|E_5[2\sqrt{-2}]| = 8$. So there are 4 other points in this subgroup, but these points only give us two new x-coordinates since $(x, y) \neq (x, -y)$ for all $(x, y) \in E_5 \setminus E_5[2]$. We compute the 4^{th}-division polynomial

$$\psi_4(x) = 8(x + 12)(x^2 - 12x - 126)(x^2 + 24x - 18)(x^4 - 24x^3 - 756x^2 - 12528x - 77436).$$

Since the group $E_5[2\sqrt{-2}]$ is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we see that the x-coordinates we need are zeros of $x^2 + 24x - 18$. Hence altogether we find

$$\begin{aligned} E_5[2\sqrt{-2}] \setminus E_5[2] \quad = \quad & \{(-12 - 9e^{4\pi i/16} + 9e^{12\pi i/16}, 54e^{6\pi i/16} + 54e^{10\pi i/16}), \\ & (-12 - 9e^{4\pi i/16} + 9e^{12\pi i/16}, -54e^{6\pi i/16} - 54e^{10\pi i/16}), \\ & (-12 + 9e^{4\pi i/16} - 9e^{12\pi i/16}, 54e^{2\pi i/16} + 54e^{14\pi i/16}), \\ & (-12 + 9e^{4\pi i/16} - 9e^{12\pi i/16}, -54e^{2\pi i/16} - 54e^{14\pi i/16})\} \end{aligned}$$

In particular we see that all coordinates of $E[2\sqrt{-2}]$ are elements of the field $\mathbb{Q}(e^{2\pi i/16})$. For any prime $p \neq 2$ we now have $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(e^{2\pi i/16})/\mathbb{Q})$ such that

$$\sigma_p : E_5[2\sqrt{-2}] \longrightarrow E_5[2\sqrt{-2}], \quad e^{2\pi i/16} \longmapsto e^{2p\pi i/16}.$$

Hence σ_p is determined by the residue class of p modulo 16. And since σ_p gets mapped to Fr_p after reduction modulo p we see that acting on $E_5(\overline{\mathbb{F}_p})[2\sqrt{-2}]$ the Frobenius endomorphism only depends on the residue class of p modulo 16. Therefore it follows that for two primes p and q we have

$$\begin{aligned} p \equiv q \mod 16 \quad & \Longrightarrow \quad \mathrm{Fr}_p \equiv \mathrm{Fr}_q \mod 2\sqrt{-2} \\ & \Longrightarrow \quad \tfrac{1}{2}a(p) \equiv \tfrac{1}{2}a(q) \mod 2\sqrt{-2} \\ & \Longrightarrow \quad \tfrac{1}{2}a(p) \equiv \tfrac{1}{2}a(q) \mod 4, \\ & \Longrightarrow \quad a(p) \equiv a(q) \mod 8, \end{aligned}$$

where the second to last implication follows since $a(p), a(q) \in \mathbb{Z}$. This means that we only have to determine $a(p)$ for one p in each residue class modulo 16. By simply counting the number of points on the reduction of E_5 modulo p we find

$$\begin{aligned} a(p) \equiv a(17) &= p + 1 - |E_5(\mathbb{F}_{17})| = 18 - 24 \equiv 2 \mod 8, \text{ if } p \equiv 1 \mod 16, \\ a(p) \equiv a(19) &= p + 1 - |E_5(\mathbb{F}_{19})| = 20 - 18 \equiv 2 \mod 8, \text{ if } p \equiv 3 \mod 16, \\ a(p) \equiv a(41) &= p + 1 - |E_5(\mathbb{F}_{41})| = 42 - 36 \equiv 6 \mod 8, \text{ if } p \equiv 9 \mod 16, \\ a(p) \equiv a(11) &= p + 1 - |E_5(\mathbb{F}_{11})| = 12 - 6 \equiv 6 \mod 8, \text{ if } p \equiv 11 \mod 16. \end{aligned}$$

Therefore we have

$$|E_5(\mathbb{F}_p)| = \begin{cases} p+1-2x & \text{if } p \equiv 1,3 \mod 16 \text{ and } p = x^2+2y^2 \text{ such that } x \equiv 1 \mod 4, \\ p+1-2x & \text{if } p \equiv 9,11 \mod 16 \text{ and } p = x^2+2y^2 \text{ such that } x \equiv 3 \mod 4. \end{cases}$$

□

Remark. The proof above shows that if $\mathbb{Q}(E[\sqrt{-d}]) \subset \mathbb{Q}(\zeta_n)$ for some n^{th}-root of unity ζ_n, then we only have to determine $a(p)$ modulo $\sqrt{-d}$ for one prime in each residue class of $(\mathbb{Z}/n\mathbb{Z})^\times$. Since for two primes $p_1 \equiv p_2 \mod n$ that split in $Q(\mathrm{End}(E))$, we have $\mathrm{Fr}_{p_1} \equiv \mathrm{Fr}_{p_2} \mod \sqrt{-d}$. Note that these endomorphism act on different elliptic curves since Fr_{p_1} acts on the reduction of E modulo p_1 and Fr_{p_2} acts on the reduction of E modulo p_2. However we do have

$$\mathrm{End}_{\overline{\mathbb{F}_{p_1}}}(\overline{E}) \cong \mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong \mathrm{End}_{\overline{\mathbb{F}_{p_2}}}(\overline{E}).$$

So the different Frobenius endomorphisms we are considering in the proof above all lie in isomorphic endomorphism rings.

Proposition 2.8. *Let $E_6 : y^2 = x^3 - 35x - 98$ be the elliptic curve over $\mathbb{Q}$ with complex multiplication given by $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$. Then for any prime $p \neq 2, 7$*

$$|E_6(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } p \not\equiv 1,2,4 \mod 7, \\ p+1-\left(\frac{x}{7}\right)2x & \text{if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2. \end{cases}$$

Proof. The discriminant of E_6 is given by $\triangle(E_6) = -2^{12}7^3$, hence E_6 has good reduction modulo all primes $p \neq 2, 7$. Moreover

$$\left(\frac{-7}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,2,4 \mod 7 \\ 0 & \text{if } p = 7 \\ -1 & \text{otherwise.} \end{cases}$$

So the first case now follows from equation 2.1.

Now let p be a prime that splits in $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$, i.e. $p \equiv 1,2,4 \mod 7$. So we have

$$\pi = \frac{c+d\sqrt{-7}}{2},$$

for some $c, d \in \mathbb{Z}$ of the same parity such that $\pi\overline{\pi} = p$. Moreover the Frobenius endomorphism is given by multiplication by π and therefore $a(p) = p+1-|E_6(\mathbb{F}_p)| = \pi + \overline{\pi} = c$. But since $x^3 - 35x - 98 = (x-7)(x^2+7x+14)$ we see that $(7,0) \in E_6[2]$. Therefore for any prime p of good reduction there exists a point of order 2 in $E(\mathbb{F}_p)$. By group theory it now follows that $2 \mid |E(\mathbb{F}_p)|$, hence $a(p) = c$ is even. This means we can write

$$\pi = a + b\sqrt{-7},$$

for some $a, b \in \mathbb{Z}$ and $p = a^2 + 7b^2$. Moreover $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]^\times = \{\pm 1\}$, hence a and b are unique up to their sign.

To determine the correct sign of a and b we consider the map $[\sqrt{-7}] : E_6 \to E_6$. This map has degree 7 and therefore its kernel $E_6[\sqrt{-7}]$ is a cyclic group of order 7. We now compute the factorization of the 7^{th}-division polynomial

$$\begin{aligned}\psi_7(x) &= 7(x^3+7x^2-21x-91)(x^{21}-7x^{20}-1470x^{19}-44982x^{18}-233583x^{17}\\ &\quad +501809x^{16}+50228920x^{15}+1225220696x^{14}+12432574882x^{13}\\ &\quad +35737295538x^{12}-294580389908x^{11}-2691399230884x^{10}\\ &\quad -8217188522550x^9-44125428998742x^8-657825428058120x^7\\ &\quad -5592520198825448x^6-27801800465550531x^5-88052206971443211x^4\\ &\quad -182466352815263454x^3-246619853810564374x^2-21226041110052562 7x\\ &\quad -100374559224312443).\end{aligned}$$

Since $E_6[\sqrt{-7}]$ is fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we see that the x-coordinates of $E_6[\sqrt{-7}] \setminus \{\mathcal{O}\}$ are zeros of $x^3+7x^2-21x-91$. We find $E_6[\sqrt{-7}] = \langle P \rangle$ with

$$\begin{aligned}P &= \left(-1+4e^{4\pi i/7}+4e^{10\pi i/7}, 8e^{2\pi i/7}-4e^{4\pi i/7}+4e^{10\pi i/7}-8e^{12\pi i/7}\right),\\ 2P &= \left(-1+4e^{2\pi i/7}+4e^{12\pi i/7}, 8+4e^{2\pi i/7}+8e^{4\pi i/7}+16e^{8\pi i/7}+8e^{10\pi i/7}+12e^{12\pi i/7}\right),\\ 3P &= \left(-1+4e^{6\pi i/7}+4e^{8\pi i/7}, -8e^{4\pi i/7}-4e^{6\pi i/7}+4e^{8\pi i/7}+8e^{10\pi i/7}\right),\\ 4P &= \left(-1+4e^{6\pi i/7}+4e^{8\pi i/7}, 8e^{4\pi i/7}+4e^{6\pi i/7}-4e^{8\pi i/7}-8e^{10\pi i/7}\right),\\ 5P &= \left(-1+4e^{2\pi i/7}+4e^{12\pi i/7}, -8-4e^{2\pi i/7}-8e^{4\pi i/7}-16e^{8\pi i/7}-8e^{10\pi i/7}-12e^{12\pi i/7}\right),\\ 6P &= \left(-1+4e^{4\pi i/7}+4e^{10\pi i/7}, -8e^{2\pi i/7}+4e^{4\pi i/7}-4e^{10\pi i/7}+8e^{12\pi i/7}\right),\\ 7P &= \mathcal{O}.\end{aligned}$$

In particular $\mathbb{Q}(E_6[\sqrt{-7}]) \subset \mathbb{Q}(e^{2\pi i/7})$. Therefore we only have to compute $\frac{a(p)}{2} = a$ for one p in each residue class modulo 7 to determine $|E(\mathbb{F}_p)|$ for all primes p of good reduction. However since $E_6[\sqrt{-7}]$ is a cyclic group and $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(e^{2\pi i/7})/\mathbb{Q}) : e^{2\pi i/7} \mapsto e^{2p\pi i/7}$ a group homomorphism we see $\sigma_p(P) = mP$ for some $m \in \mathbb{Z}$. In particular we find

$$\begin{aligned}\sigma_p(P) &= P \quad \text{if } p \equiv 1 \mod 7,\\ \sigma_p(P) &= 4P \quad \text{if } p \equiv 2 \mod 7,\\ \sigma_p(P) &= 2P \quad \text{if } p \equiv 4 \mod 7.\end{aligned}$$

Since σ_p reduces to the Frobenius endomorphism at p, at least on $E[\sqrt{-7}](\mathbb{F}_p)$, we see that

$$\begin{aligned}\pi = a+b\sqrt{-7} \equiv a \equiv 1 \mod \sqrt{-7}, \quad \text{if } p \equiv 1 \mod 7,\\ \pi = a+b\sqrt{-7} \equiv a \equiv 4 \mod \sqrt{-7}, \quad \text{if } p \equiv 2 \mod 7,\\ \pi = a+b\sqrt{-7} \equiv a \equiv 2 \mod \sqrt{-7}, \quad \text{if } p \equiv 4 \mod 7.\end{aligned}$$

It actually follows that $\left(\frac{a}{7}\right) = 1$ in each case. Therefore

$$|E_6(\mathbb{F}_p)| = p+1-\left(\frac{x}{7}\right)2x \quad \text{if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2.$$

Notice that the sign of x is not determined by the conditions above. But since $\left(\frac{-1}{p}\right) = -1$ both choices give the same cardinality. □

Proposition 2.9. *Let $E_7 : y^2 = x^3 - 595x - 5586$ be the elliptic curve over $\mathbb{Q}$ with complex multiplication given by $\mathbb{Z}\left[\sqrt{-7}\right]$. Then for any prime $p \neq 2, 7$*

$$|E_6(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } p \not\equiv 1,2,4 \mod 7,\\ p+1-\left(\frac{x}{7}\right)2x & \text{if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2.\end{cases}$$

Proof. First we determine the discriminant of E_7, which is given by $\triangle(E_7) = 2^{12}7^3$. So E_7 has good reduction modulo all primes $p \neq 2, 7$. We can now write

$$E_6 : y^2 = (x-7)(x^2+7x+14),$$
$$E_7 : y^2 = (x+14)(x^2-14x-399).$$

Therefore by example 1.4 we have the following isogeny

$$\phi : E_6 \longrightarrow E_7, \quad (x,y) \longmapsto (x + \frac{112}{x-7}, \left(1 - \frac{112}{(x-7)^2}\right) y),$$

which is defined over $\mathbb{Q}$. It now follows by theorem 1.8 that

$$|E_6(\mathbb{F}_p)| = |E_7(\mathbb{F}_p)|,$$

for all primes $p \neq 2, 7$, which completes the proof. □

Proposition 2.10. *Let $E_8 : y^2 = x^3 - 480x + 4048$ be the elliptic curve over $\mathbb{Q}$ with complex multiplication given by $\mathbb{Z}\left[\frac{1+3\sqrt{-3}}{2}\right]$. Then for any prime $p > 3$*

$$|E_8(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } p \equiv -1 \mod 3, \\ p+1+\left(\frac{x}{3}\right)x & \text{if } p \equiv 1 \mod 3 \text{ and } 4p = x^2 + 27y^2. \end{cases}$$

Proof. Firstly the discriminant of E_8 is given by $\triangle(E_8) = -2^{12}3^5$, so E_8 has good reduction modulo all primes $p > 3$. Moreover a prime p is inert in $Q(\mathrm{End}(E)) \cong \mathbb{Q}(\sqrt{-3})$ if $p \equiv -1 \mod 3$ and splits if $p \equiv 1 \mod 3$. The first case now follows.

So now assume $p \equiv 1 \mod 3$. Then there exists a

$$\pi = \frac{a + b3\sqrt{-3}}{2} \in \mathbb{Z}\left[\frac{1+3\sqrt{-3}}{2}\right] \subset \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right],$$

such that $4\pi\overline{\pi} = a^2 + 27b^2 = 4p$ and $a = a(p) = \pi + \overline{\pi}$. The ring $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is a unique factorization domain and $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$, where

$$\omega = \frac{1+\sqrt{-3}}{2}.$$

We thus see that the factorization of p is determined up to these units. Now we compute the full torsion subgroup of E_8 over $\mathbb{Q}$. This group is given by

$$\{\mathcal{O}, (12,4), (12,-4)\}.$$

Hence $E_8(\mathbb{F}_p)$ contains a point of order 3 for all primes $p > 3$. Therefore

$$|E_8(\mathbb{F}_p)| = p + 1 - a(p) \equiv 2 - a(p) \equiv 0 \mod 3.$$

Hence $a(p) = a \equiv 2 \mod 3$. From this it follows that $\pm\omega\pi, \pm\omega^2\pi \notin \mathbb{Z}\left[\frac{1+3\sqrt{-3}}{2}\right]$, since

$$\pm\omega\pi = \pm\frac{a - 9b + (a+3b)\sqrt{-3}}{4},$$
$$\pm\omega^2\pi = \pm\frac{-a - 9b + (a-3b)\sqrt{-3}}{4},$$

and $a \pm 3b \equiv 2 \mod 3$. Moreover $-\pi - \bar{\pi} = -a \equiv -2 \mod p$, therefore the factorization of p is determined uniquely by the properties stated above. Altogether we thus find

$$|E_8(\mathbb{F}_p)| = p + 1 + \left(\frac{x}{3}\right) x \quad \text{if } p \equiv 1 \mod 3 \text{ and } 4p = x^2 + 27y^2.$$

□

From E_8 we can create an isogeny to $E : y^2 = x^3 + 16$ with kernel $\{\mathcal{O}, (12, 4), (12, -4)\}$. Namely

$$\phi : E_8 \longrightarrow E : (x, y) \longmapsto \left(\frac{x^3 - 24x^2 + 48x + 1216}{9(x-12)^2}, \frac{x^3 - 36x^2 + 528x - 3008}{27(x-12)^3} y \right).$$

Note that its kernel is given by $\{\mathcal{O}, (12, 4), (12, -4)\}$, hence the degree of this isogeny is 3. Moreover E is a twist of the curve $E_3 : y^2 = x^3 + 1$, it is however not a quadratic twist of E_3. By theorem 1.8 we now see that for all primes p such that both E_8 and E have good reduction

$$|E_8(\mathbb{F}_p)| = |E(\mathbb{F}_p)|.$$

Proposition 2.11. *Let $E_9 : y^2 = x^3 - 9504x + 365904$ be the elliptic curve over $\mathbb{Q}$ with complex multiplication given by $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$. Then for any prime $p \neq 2, 3, 11$*

$$|E_9(\mathbb{F}_p)| = \begin{cases} p + 1 & \text{if } \left(\frac{p}{11}\right) = -1, \\ p + 1 + \left(\frac{x}{11}\right) x & \text{if } \left(\frac{p}{11}\right) = 1 \text{ and } 4p = x^2 + 11y^2. \end{cases}$$

Proof. The discriminant of E_9 is given by $\triangle(E_9) = -2^{12}11^3$, therefore E_9 has good reduction modulo all primes unequal to $2, 3$ and 11. The first case now follows since

$$\left(\frac{p}{11}\right) = \left(\frac{-11}{p}\right) = -1$$

implies that p does not split.

Now assume that p does split in $\mathbb{Q}(\sqrt{-11})$. Then $p \equiv 1, 3, 4, 5, 9 \mod 11$. Moreover $p = \pi\overline{\pi}$ such that $\pi \in \mathrm{End}(E_9)$ and $a(p) = \pi + \overline{\pi}$. Again π is uniquely determined up to its sign, since it is a factor of p in a unique factorization domain with units ± 1. So we only have to determine the correct sign of

$$\pi = \frac{a + b\sqrt{-11}}{2}.$$

For this we consider the endomorphism $[\sqrt{-11}] : E_9 \to E_9$. The degree of this endomorphism is 11 and therefore its kernel $E_9[\sqrt{-11}]$ is a cyclic group of order 11. When we factor the 11^{th}-division polynomial ψ_{11} over $\mathbb{Q}$ we find a unique factor of degree 5 namely

$$x^5 - 264x^4 + 7920x^3 + 1463616x^2 - 92835072x + 1294672896.$$

The zeros of this polynomial are the x-coordinates of $E_9[\sqrt{-11}]$. We compute $E_9[\sqrt{-11}] = \langle P \rangle$, where $P = (x_1, y_1)$ with

$$\begin{aligned} x_1 &= 60 + 36\zeta^2 - 36\zeta^3 + 36\zeta^4 + 36\zeta^7 - 36\zeta^8 + 36\zeta^9, \\ y_1 &= 756 - 432\zeta + 432\zeta^2 + 216\zeta^4 + 216\zeta^7 + 432\zeta^9 - 432\zeta^{10}, \end{aligned}$$

where $\zeta = e^{2\pi i/11}$. Similarly we can compute the coordinates of all points in $E_9[\sqrt{-11}]$, these coordinates all lie in $\mathbb{Q}(e^{2\pi i/11})$. Therefore we can explicitly determine the action of the group homomorphism

$$\sigma_p : E_9[\sqrt{-11}] \longrightarrow E_9[\sqrt{-11}], \quad e^{2\pi i/11} \longmapsto e^{2p\pi i/11},$$

for all primes p. This map is determined by the residue class of p modulo 11. In particular we find

$$\begin{array}{lll} \sigma_p(P) = P & \text{if } p \equiv 1 & \mod 11, \\ \sigma_p(P) = 5P & \text{if } p \equiv 3 & \mod 11, \\ \sigma_p(P) = 9P & \text{if } p \equiv 4 & \mod 11, \\ \sigma_p(P) = 4P & \text{if } p \equiv 5 & \mod 11, \\ \sigma_p(P) = 3P & \text{if } p \equiv 9 & \mod 11. \end{array}$$

Since σ_p reduces to the Frobenius endomorphism at p we now know how Fr_p acts on $E_9[\sqrt{-11}]$. We see that

$$\begin{aligned} \pi &= \frac{a+b\sqrt{-11}}{2} \equiv \frac{a}{2} \equiv 1 \mod \sqrt{-11}, \quad \text{if } p \equiv 1 \mod 11, \\ \pi &= \frac{a+b\sqrt{-11}}{2} \equiv \frac{a}{2} \equiv 5 \mod \sqrt{-11}, \quad \text{if } p \equiv 3 \mod 11, \\ \pi &= \frac{a+b\sqrt{-11}}{2} \equiv \frac{a}{2} \equiv 9 \mod \sqrt{-11}, \quad \text{if } p \equiv 4 \mod 11, \\ \pi &= \frac{a+b\sqrt{-11}}{2} \equiv \frac{a}{2} \equiv 4 \mod \sqrt{-11}, \quad \text{if } p \equiv 5 \mod 11, \\ \pi &= \frac{a+b\sqrt{-11}}{2} \equiv \frac{a}{2} \equiv 3 \mod \sqrt{-11}, \quad \text{if } p \equiv 9 \mod 11. \end{aligned}$$

Hence

$$\begin{array}{llll} a(p) = a \equiv 2 & \mod 11, & \text{if } p \equiv 1 & \mod 11, \\ a(p) = a \equiv 10 & \mod 11, & \text{if } p \equiv 3 & \mod 11, \\ a(p) = a \equiv 7 & \mod 11, & \text{if } p \equiv 4 & \mod 11, \\ a(p) = a \equiv 8 & \mod 11, & \text{if } p \equiv 5 & \mod 11, \\ a(p) = a \equiv 6 & \mod 11, & \text{if } p \equiv 9 & \mod 11, \end{array}$$

In particular we see that

$$\left(\frac{a(p)}{11}\right) = -1,$$

for all primes p that split in $\mathbb{Q}(\sqrt{-11})$. And since $\left(\frac{-1}{11}\right) = -1$ this property determines the sign of a. Altogether we thus find

$$|E_9(\mathbb{F}_p)| = p + 1 + \left(\frac{x}{11}\right) x \ \text{ if } \ \left(\frac{p}{11}\right) = 1 \text{ and } 4p = x^2 + 11y^2.$$

□

2.2 Minimal Models

The division polynomials and abelian extensions of $\mathbb{Q}$ are already getting quite large. An easier method would be to determine the primitive root of unity ζ_n such that $\mathbb{Q}(E[\sqrt{-d}]) \subset \mathbb{Q}(\zeta_n)$ without actually computing the coordinates of the points in $E[\sqrt{-d}]$. Throughout this section we will assume that d is an odd prime. In particular $\mathbb{Q}(E[\sqrt{-d}])/\mathbb{Q}$ is an abelian extension and $\mathbb{Q}(E[\sqrt{-d}]) \subset \mathbb{Q}(\zeta_n)$ for some n that is only divisible by primes ramifying in $\mathbb{Q}(E[\sqrt{-d}])/\mathbb{Q}$.

Definition 2.1. Let E be an elliptic curve defined over a K and $k > 1$ an integer. Then L_k is the smallest field containing all x-coordinates and all y-coordinates of the group $E[k]$ of k-torsion points. The field L_k is called the k^{th}-division field of E.

The following theorem shows that the k^{th}-division field of an elliptic curve E has some properties we will be able to use. Notice also that $\mathbb{Q}(E[\sqrt{-d}]) \subset L_d$ for all d.

Theorem 2.12. *Let E be an elliptic curve defined over a number field K and $k > 1$ an integer. Let L_k be the k^{th}-division field of E and $\mathfrak{p}$ be a prime of good reduction for E with $N(\mathfrak{p})$ relative prime to k. Then $\mathfrak{p}$ is unramified in L_k.*

Proof. This theorem is proven in the paper [DT02] written by W. Duke and Á Tóth. □

Theorem 2.12 is stated in a greater generality than needed. Therefore we state the following corollary which provides precisely the results we need.

Corollary 2.13. *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication by an order R_K in a quadratic imaginary field K. Let d be a prime such that $\sqrt{-d} \in R_K$. Then there exists an $n \in \mathbb{Z}_{\geq 0}$ such that $\mathbb{Q}(E[\sqrt{-d}]) \subset \mathbb{Q}(\zeta_n)$, where n is not divisible by primes $p \neq d$ of good reduction.*

Proof. Since d is a prime, $\mathbb{Q}(E[\sqrt{-d}])/\mathbb{Q}$ is an abelian extension. Hence by the Kronecker-Weber theorem $\mathbb{Q}(E[\sqrt{-d}]) \subset \mathbb{Q}(\zeta_m)$ for some $m \in \mathbb{Z}$ only divisible by primes that ramify in $\mathbb{Q}(E[\sqrt{-d}])/\mathbb{Q}$. Moreover $\mathbb{Q}(E[\sqrt{-d}]) \subset L_d$ and by theorem 2.12 we see that all primes $p \neq d$ of good reduction are unramified in L_d. Hence these primes are also unramified in $\mathbb{Q}(E[\sqrt{-d}])$ and the corollary follows. □

We can also say some things about the degree of the extension $\mathbb{Q}(E[\sqrt{-d}])/\mathbb{Q}$. The following lemma gives a bound for this degree.

Lemma 2.14. *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication. Let d be an odd prime such that $\left[\sqrt{-d}\right] \in \mathrm{End}(E)$. Then*

$$\left[\mathbb{Q}(E[\sqrt{-d}]) : \mathbb{Q}\right] \;\Big|\; d - 1 \,.$$

Proof. $E[\sqrt{-d}]$ is a group of order d. Hence, since d is prime, $E[\sqrt{-d}] \cong \mathbb{Z}/d\mathbb{Z}$. In particular

$$\mathrm{Gal}\left(\mathbb{Q}\left(E\left[\sqrt{-d}\right]\right)/\mathbb{Q}\right) \subset (\mathbb{Z}/d\mathbb{Z})^{\times} \,.$$

And since $\left|(\mathbb{Z}/d\mathbb{Z})^{\times}\right| = d - 1$ the lemma follows. □

The particularly useful part of this lemma is that it shows that the degree of the extension $\mathbb{Q}(E[\sqrt{-d}])/\mathbb{Q}$ is not divisible by any prime $p \geq d$.

An elliptic curve $E/\mathbb{Q}$ has different Weierstrass models, all related by a change of coordinates. If we only consider Weierstrass equation with coefficients in $\mathbb{Z}$, we see that the discriminants of these models are all integers. However these discriminants are not the same. Among all these models there are models such that $\mathrm{ord}_p(\triangle(E))$ is minimal for a prime p. Such a model is called minimal at p.

Proposition 2.15. *For an elliptic curve $E/\mathbb{Q}$ there exists a Weierstrass model with coefficients in $\mathbb{Z}$, which is minimal at p for all primes p. Such a Weierstrass model is called a minimal model of E.*

Proof. See proposition 1.3 of [Sil09, p.186]. □

Taking a minimal model for E will enable us to eliminate as many primes as possible from the integer n such that $E[\sqrt{-d}] \subset \mathbb{Q}(\zeta_n)$. And the smaller the degree of the field extension $\mathbb{Q}(\sqrt{-d})/\mathbb{Q}$ is, the easier it will be to determine the action of Frobenius on $E[\sqrt{-d}]$.

Proposition 2.16. *Let $E_{10} : y^2 = x^3 - 608x - 5776$ be the elliptic curve over $\mathbb{Q}$ with complex multiplication given by $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. Then for any prime $p \neq 2, 19$*

$$|E_{10}(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } \left(\frac{p}{19}\right) = -1, \\ p+1+\left(\frac{x}{19}\right)x & \text{if } \left(\frac{p}{19}\right) = 1 \text{ and } 4p = x^2 + 19y^2. \end{cases}$$

Proof. Let E be the elliptic curve given by the Weierstrass equation

$$E : y^2 + y = x^3 - 38x + 90.$$

Then we find the following isomorphism

$$\phi : E \longrightarrow E_{10}, \quad (x, y) \longmapsto (4x, 8y + 4).$$

The Weierstrass equation of the elliptic curve E is a minimal model for E_{10}. Moreover E has complex multiplication by the integrally closed domain

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right].$$

Therefore we see that for all primes of good reduction

$$|E(\mathbb{F}_p)| = p + 1 \quad \text{if } \left(\frac{p}{19}\right) = -1.$$

So now assume that p is a prime of good reduction for E that splits in the endomorphism ring. Then there exists a $\pi = \frac{1}{2}(a + b\sqrt{-19})$ such that $p = \pi\bar{\pi}$ and $a(p) = \pi + \overline{\pi} = a$. The endomorphism ring is a unique factorization domain with units ± 1. Therefore a factorization of p determines $a(p)$ up to its sign. If we determine the sign of π we will know $a(p)$ and thus the cardinality of $E(\mathbb{F}_p)$.

The discriminant of E is given by $\triangle(E) = -19^3$. Therefore by corollary 2.13 we see that

$$\mathbb{Q}(E[\sqrt{-19}]) \subset \mathbb{Q}(\zeta_{19^n}),$$

for some $n \in \mathbb{Z}_{\geq 0}$. From the theory of cyclotomic fields we know that

$$[\mathbb{Q}(\zeta_{19^n}) : \mathbb{Q}] = 19^{n-1}(19 - 1).$$

But by lemma 2.14 it follows that 19 does not divide $\left[\mathbb{Q}(E[\sqrt{-19}]) : \mathbb{Q}\right]$. Hence

$$\mathbb{Q}(E[\sqrt{-19}]) \subset \mathbb{Q}(\zeta_{19}).$$

But this means that the action of the Frobenius endomorphism Fr_p on $E(\overline{\mathbb{F}_p})[\sqrt{-19}]$ only depends on the residue class of p modulo 19. In particular we see that for all primes p and q,

$$\begin{aligned} p \equiv q \mod 19 &\implies \mathrm{Fr}_p \equiv \mathrm{Fr}_q \mod \sqrt{-19} \\ &\implies a(p) \equiv a(q) \mod \sqrt{-19} \\ &\implies a(p) \equiv a(q) \mod 19. \end{aligned}$$

Computing $a(p)$ for a prime in each residue class modulo 19 now shows that

$$\left(\frac{a(p)}{19}\right) = -1 \quad \text{if } \left(\frac{p}{19}\right) = 1.$$

And since

$$\left(\frac{-1}{19}\right) = -1,$$

these conditions determine the sign of π. Hence

$$|E(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } \left(\frac{p}{19}\right) = -1, \\ p+1+\left(\frac{x}{19}\right)x & \text{if } \left(\frac{p}{19}\right) = 1 \text{ and } 4p = x^2+19y^2, \end{cases}$$

for all primes $p \neq 19$. Now notice that the isomorphism ϕ gives us an isomorphism form $E(\mathbb{F}_p)$ to $E_{10}(\mathbb{F}_p)$ for all primes $p \neq 2$. Therefore the proposition follows. □

Proposition 2.17. *Let $E_{11} : y^2 = x^3 - 13760x - 621264$ be the elliptic curve over $\mathbb{Q}$ with complex multiplication given by $\mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right]$. Then for any prime $p \neq 2, 43$*

$$|E_{11}(\mathbb{F}_p)| = \begin{cases} p+1 & \textit{if } \left(\frac{p}{43}\right) = -1, \\ p+1+\left(\frac{x}{43}\right)x & \textit{if } \left(\frac{p}{43}\right) = 1 \textit{ and } 4p = x^2+43y^2. \end{cases}$$

Proof. Let $E : y^2 + y = x^3 - 860x + 9707$ be a minimal model for E_{11}. Then E has complex multiplication by the integrally closed domain

$$\mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right].$$

Therefore we see that for all primes of good reduction

$$|E(\mathbb{F}_p)| = p+1 \quad \text{if } \left(\frac{p}{43}\right) = -1.$$

So now assume that p is a prime of good reduction for E that splits in the endomorphism ring. Then there exists a $\pi = \frac{1}{2}(a + b\sqrt{-43})$ such that $p = \pi\bar{\pi}$ and $a(p) = \pi + \overline{\pi} = a$. The endomorphism ring is unique factorization domain with units ± 1. Hence a factorization of p determines $a(p)$ up to its sign.

The discriminant of E is given by $\triangle(E) = -43^3$. By corollary 2.13 this implies

$$\mathbb{Q}(E[\sqrt{-43}]) \subset \mathbb{Q}(\zeta_{43^n}),$$

for some $n \in \mathbb{Z}_{\geq 0}$. But by lemma 2.14 it follows that 43 does not divide $\left[\mathbb{Q}(E[\sqrt{-43}]) : \mathbb{Q}\right]$. Hence

$$\mathbb{Q}(E[\sqrt{-43}]) \subset \mathbb{Q}(\zeta_{43}).$$

In particular it follows that $a(p) \equiv a(q) \mod 43$ if $p \equiv q \mod 43$. Computing $a(p)$ for a prime in each residue class modulo 43 shows us that

$$\left(\frac{a(p)}{43}\right) = -1 \quad \text{if } \left(\frac{p}{43}\right) = 1.$$

And since

$$\left(\frac{-1}{43}\right) = -1,$$

these conditions determine the sign of $a(p)$. Hence

$$|E(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } \left(\frac{p}{43}\right) = -1, \\ p+1+\left(\frac{x}{43}\right)x & \text{if } \left(\frac{p}{19}\right) = 1 \text{ and } 4p = x^2 + 43y^2, \end{cases}$$

for all primes $p \neq 19$.

The isomorphism between E and E_{11} is given by

$$\phi : E \longrightarrow E_{11}, \quad (x, y) \longmapsto (4x, 8y + 4).$$

This isomorphism reduces to an isomorphism between $E(\mathbb{F}_p)$ and $E_{11}(\mathbb{F}_p)$ for all primes $p \neq 2, 19$ and thus the proposition follows. □

Proposition 2.18. *Let $E_{12} : y^2 = x^3 - 117920x - 15585808$ be the elliptic curve over $\mathbb{Q}$ with complex multiplication given by $\mathbb{Z}\left[\frac{1+\sqrt{-67}}{2}\right]$. Then for any prime $p \neq 2, 67$*

$$|E_{12}(\mathbb{F}_p)| = \begin{cases} p+1 & \textit{if } \left(\frac{p}{67}\right) = -1, \\ p+1+\left(\frac{x}{67}\right)x & \textit{if } \left(\frac{p}{67}\right) = 1 \textit{ and } 4p = x^2 + 67y^2. \end{cases}$$

Proof. Let $E : y^2 + y = x^3 - 7370x + 243528$ be a minimal model for the elliptic curve E_{12}. Then E has complex multiplication by $\mathbb{Q}(\sqrt{-67})$, therefore the first case follows. The endomorphism ring of E is integrally closed and it is an unique factorization domain with units ± 1. Therefore we only need to determine the correct sign of $a(p)$. The discriminant of E is given by $\triangle(E) = -67^3$. As in the previous propositions we find $\mathbb{Q}(E[\sqrt{-67}]) \subset \mathbb{Q}(\zeta_{67})$. Therefore the residue class of $a(p)$ modulo 67 is determined by the residue class of p modulo 67. Computing $a(p)$ for a prime in each residue class now shows that

$$\left(\frac{a(p)}{67}\right) = -1 \quad \text{if } \left(\frac{p}{67}\right) = 1.$$

And since

$$\left(\frac{-1}{67}\right) = -1,$$

these conditions determine the sign of $a(p)$. The proposition now follows by applying the isomorphism between E and E_{13}. □

Proposition 2.19. *Let* $E_{13} : y^2 = x^3 - 34790720x - 78984748304$ *be the elliptic curve over* $\mathbb{Q}$ *with complex multiplication given by* $\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$. *Then for any prime* $p \neq 2, 163$

$$|E_{13}(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } \left(\frac{p}{163}\right) = -1, \\ p+1+\left(\frac{x}{163}\right)x & \text{if } \left(\frac{p}{163}\right) = 1 \text{ and } 4p = x^2 + 163y^2. \end{cases}$$

Proof. Let $E : y^2 + y = x^3 - 2174420x + 1234136692$ be a minimal model for the elliptic curve E_{13}. Then E has complex multiplication by $\mathbb{Q}(\sqrt{-163})$, therefore the first case follows. The endomorphism ring of E is integrally closed and it is an unique factorization domain with units ± 1. And thus we only need to determine the correct sign of $a(p)$. The discriminant of E is given by $\triangle(E) = -163^3$. As in the previous propositions we find $\mathbb{Q}(E[\sqrt{-163}]) \subset \mathbb{Q}(\zeta_{163})$. Therefore the residue class of $a(p)$ modulo 163 is determined by the residue class of p modulo 163. Computing $a(p)$ for a prime in each residue class now shows that

$$\left(\frac{a(p)}{163}\right) = -1 \quad \text{if } \left(\frac{p}{163}\right) = 1.$$

And since

$$\left(\frac{-1}{163}\right) = -1,$$

these conditions determine the sign of $a(p)$. The proposition now follows by applying the isomorphism between E and E_{13}. □

Chapter 3

Gamma Function

In this chapter we will review some theory about the p-adic gamma function and about Gauss sums. The next chapter will relate these two with the elliptic curves of the previous chapter, leading to certain congruences. From now on we will consider only odd primes p. Let $\mathbf{Q}_p$ be the field of p-adic numbers and let $\mathbf{Z}_p$ be the ring of p-adic integers. Consider the following function

$$f : \mathbb{N} \to \mathbb{Z}, \quad n \mapsto (-1)^n \prod_{1 \leq j < n,\ p \nmid j} j.$$

Lemma 3.1. *Let a and $k \geq 1$ be integers and let p be an odd prime. Then*

$$\prod_{a \leq j < a+p^k,\ p \nmid j} j \equiv -1 \mod p^k.$$

Proof. The factors of this product are precisely the elements of $(\mathbb{Z}/p^k\mathbb{Z})^\times$. We can pair these elements with there inverses, at least when $x \not\equiv x^{-1} \mod p^k$. The remaining factors are all roots of the polynomial $x^2 - 1 = (x-1)(x+1)$ modulo p^k. Clearly ± 1 are roots of this polynomial. For any other root x we must have that $x-1$ and $x+1$ are both zero divisors in $\mathbb{Z}/p^k\mathbb{Z}$, therefore they are divisible by p. Hence $p \mid 2 = (x-1) - (x+1)$, but this contradicts the fact that p is an odd prime. Altogether we thus find

$$\prod_{a \leq j < a+p^k,\ p \nmid j} j \equiv -1 \times 1 \equiv -1 \mod p^k.$$

□

From this lemma it follows that the function $f(n)$ satisfies

$$f(n) \equiv f(n + mp^k) \mod p^k \text{ for all } n, m \in \mathbb{N}.$$

This function is therefore uniformly continuous for the p-adic topology, hence it has a unique continuous extension to $\mathbf{Z}_p$.

Definition 3.1. The p-adic gamma function is the continuous function

$$\Gamma_p : \mathbf{Z}_p \to \mathbf{Z}_p,$$

that extends

$$f(n) = (-1)^n \prod_{1 \leq j < n,\ p \nmid j} j.$$

Theorem 3.2. *For an odd prime p, the p-adic gamma function $\Gamma_p : \mathbf{Z_p} \to \mathbf{Z}_p$ is continuous. Its image is contained in $\mathbf{Z}_p^\times$. Moreover for all $x, y \in \mathbf{Z}_p$:*

a) $\Gamma_p(0) = 1, \Gamma_p(1) = -1, \Gamma_p(2) = 1$ *and* $\Gamma_p(n+1) = (-1)^{n+1} n!$, *for all* $1 \leq n \leq p$,

b) $\Gamma_p(x)\Gamma_p(1-x) = (-1)^{R(x)}$, *where* $1 \leq R(x) \leq p$ *such that* $R(x) \equiv x \mod p$.

Proof. See [Rob00, p.369]. □

3.1 Gauss Sums

We take K to be a field containing a q^{th}-root of unity ζ_q. We call a group homomorphism $\psi : \mathbb{F}_q \to K^\times$ an *additive character* of $\mathbb{F}_q$ and we call a group homomorphism $\chi : \mathbb{F}_q^\times \to K^\times$ a *multiplicative character* of $\mathbb{F}_q$. We extend a multiplicative character χ to $\mathbb{F}_q$ by defining $\chi(0) = 0$. Now we can consider the following sum for any pair (ψ, χ),

$$G(\psi, \chi) = \sum_{x \in \mathbb{F}_q} \psi(x)\chi(x) = \sum_{x \in \mathbb{F}_q^\times} \psi(x)\chi(x),$$

this sum is called the Gauss sum of the pair (ψ, χ). We state the following proposition without a proof. For a proof see [Rob00, p.400].

Proposition 3.3. *Let $\tau : \mathbb{F}_q \to K^\times$ be a nontrivial additive character of the finite field $\mathbb{F}_q$. Then any other additive character ψ has the form $\psi(x) = \tau(ax)$ for some $a \in \mathbb{F}_q$.*

From this proposition it follows that

$$\begin{aligned} G(\psi, \chi) &= \textstyle\sum_{x \in \mathbb{F}_q} \tau(ax)\chi(x) \\ &= \textstyle\sum_{a^{-1}x \in \mathbb{F}_q} \tau(x)\chi(a^{-1}x) \\ &= \chi(a^{-1}) \textstyle\sum_{x \in \mathbb{F}_q} \tau(x)\chi(x) \\ &= \chi(a^{-1})G(\tau, \chi), \end{aligned}$$

for any character $\psi(x) = \tau(ax)$.

Moreover the multiplicative group $\mathbb{F}_q^\times$ is cyclic for any prime power q, i.e. $\mathbb{F}_q^\times = \langle g \rangle$ for some $g \in \mathbb{F}_q^\times$. Now let ω be a multiplicative character of $\mathbb{F}_q$, such that $\omega(g) = \zeta$ for some primitive $\varphi(q)^{th}$-root of unity ζ in K, here $\varphi(q) = |\mathbb{F}_q^\times|$. Then any other $\varphi(q)^{th}$-root of unity is a power of ζ. Therefore any other multiplicative character χ has the form $\chi(x) = \omega(x)^n$ for some $n \in \mathbb{Z}/\varphi(q)\mathbb{Z}$.

Lemma 3.4. *Let p be a prime number. The ring of p-adic integers $\mathbf{Z}_p$ contains exactly $p-1$ distinct $(p-1)^{th}$ roots of unity. Furthermore, every two distinct $(p-1)^{th}$-roots of unity are distinct modulo p.*

Proof. Since $\mathbf{Q}_p$ is a field the function $f(x) = x^{p-1} - 1$ has at most $p-1$ roots in $\mathbf{Q}_p$. Now if we take $a \in \mathbb{Z}$ with $1 \leq a \leq p-1$, then $f(a) \equiv 0 \mod p$. But $f'(a) = (p-1)a^{p-2} \not\equiv 0 \mod p$. By Hensel's lemma (see [Rob00, p.48]) it now follows that there exists a root $x \in \mathbf{Z}_p$ of $f(x)$ such that $x \equiv a \mod p$. Since $1 \leq a \leq p-1$ was arbitrary, there are exactly $p-1$ roots of $f(x)$ in $\mathbf{Z}_p$, moreover they are distinct modulo p. □

From now on we consider the field $\mathbb{F}_p$ for some prime p. By the above lemma we can define the Teichmüller character.

Definition 3.2. The Teichmüller character is the unique multiplicative character

$$\omega : \mathbb{F}_p^\times \to \mathbf{Z}_p^\times,$$

such that $\omega(a) \equiv a \mod p$.

The Teichmüller character ω is a nontrivial multiplicative character of $\mathbb{F}_p$ and since $\omega(g) \equiv g \mod p$ we see that $\omega(g)$ is a primitive $(p-1)^{th}$-root of unity for any generator g of $\mathbb{F}_p^\times$. Therefore we can write any other multiplicative character of $\mathbb{F}_p$ mapping into $\mathbf{Q}_p$ as a power of ω, i.e. ω is a generator of the group of multiplicative characters of $\mathbb{F}_p$. Moreover

$$\omega^s = \omega^t, \text{ if } s \equiv t \mod p-1.$$

Let now π be a root of $x^{p-1} + p$. Then by a proposition of Dwork (see [Rob00, p.394]) there exists a unique p^{th}-root of unity ζ_π, such that

$$\zeta_\pi \equiv 1 + \pi \mod \pi^2.$$

From now on we take $K = \mathbf{Q}_p(\zeta_\pi)$ and we fix the additive character ψ by

$$\psi : \mathbb{F}_p \longrightarrow K, \quad x \longmapsto \zeta_\pi^x.$$

We can now express any Gauss sum as

$$g_a = \sum_{x \in \mathbb{F}_p} \omega(x)^a \psi(x),$$

where ω is the Teichmüller character. Notice that $g_a = g_b$ if $a \equiv b \mod p-1$. Moreover

$$g_0 = \sum_{x \in \mathbb{F}_p^\times} \zeta_\pi^x = \frac{\zeta_\pi^p - 1}{\zeta_\pi - 1} - 1 = -1.$$

From basic theory about characters we know that for any group G and any $g \in G$ not the identity

$$\sum_{\chi \in \tilde{G}} \chi(g) = 0,$$

where $\tilde{G}$ is the group of all characters on G. Therefore the following identity follows

$$\begin{aligned} \sum_{s=0}^{p-2} g_s \omega(y)^{-s} &= \sum_{s=0}^{p-2} \sum_{x \in \mathbb{F}_p} \omega(xy^{-1})^s \psi(x) \\ &= \sum_{x \in \mathbb{F}_p} \psi(x) \sum_{s=0}^{p-2} \omega(xy^{-1})^s \\ &= (p-1)\psi(y). \end{aligned}$$

Hence we see that

$$\psi(y) = \frac{1}{p-1} \sum_{s=0}^{p-2} g_s \omega(y)^{-s}. \tag{3.1}$$

We now have a theorem connecting the Gauss sums to the p-adic gamma function. We will state this theorem in a more simplified setting, for a proof see [Coh07, p.386].

Theorem 3.5 (Gross-Koblitz)**.** *Let $a \in \mathbb{Z}$. The value of the Gauss sum g_a as defined above is explicitly given by*

$$g_a = -\pi^{S_p(a)}\Gamma_p\left(\left\{\frac{a}{1-p}\right\}\right),$$

where $\{x\}$ is the fractional part of x and $S_p(a) = (p-1)\left\{\frac{a}{1-p}\right\}$.

Remark. There is a slight difference in the Gross-Koblitz theorem stated here and the one stated in [Coh07]. This has to do with the fact that Cohen uses the inverse of the Teichmüller character. Moreover if we agree that $(-p)^{\frac{1}{p-1}} = \pi$, then we can write

$$g_a = -(-p)^{s_p(a)}\Gamma_p\left(\left\{\frac{a}{1-p}\right\}\right),$$

where $s_p(a) = \left\{\frac{a}{1-p}\right\}$.

When we now use some identities of the Gamma function from theorem 3.2 we can rewrite some Gauss sums. For example we see by theorem 3.2e) that

$$\Gamma_p(x) = \frac{(-1)^x}{\Gamma_p(1-x)} \quad \text{for all } 1 \leq x \leq p.$$

Moreover in the ring of p-adic integers we have the following identity

$$\sum_{i\geq 0} p^i = \frac{1}{1-p},$$

since $(1-p)\sum_{i\geq 0} p^i = 1$. Using these identities we find for example, for $0 < m < p-1$:

$$\begin{aligned} g_{-m} &= -(-p)^{s_p(-m)}\Gamma_p(\{\tfrac{-m}{1-p}\}) \\ &= -(-p)^{s_p(-m)}\Gamma_p(\tfrac{-m}{1-p}) \\ &= (-1)^m(-p)^{s_p(-m)}\frac{1}{\Gamma_p(1+\frac{m}{1-p})} \\ &= (-1)^m(-p)^{s_p(-m)}\frac{1}{\Gamma_p(1+m\sum_{i=0}^{\infty}p^i)}. \end{aligned}$$

By evaluating both sides for $m = 0$ we see that the equation above also holds for $m = 0$. Namely for $m = 0$ we find

$$g_0 = -1 = (-1)^0(-p)^{s_p(0)}\frac{1}{\Gamma_p(1)}.$$

When we consider this Gauss sum modulo p the first thing we see is that $\Gamma_p(1+m\sum_{i=0}^{\infty}p^i) \equiv \Gamma_p(1+m) \mod p$ by lemma 3.1. Moreover $\Gamma_p(1+m) = -(-1)^m m!$ and therefore we can write

$$g_{-m} \equiv -(-p)^{s_p(-m)}\frac{1}{m!} \mod p \quad \text{for all } 0 \leq m < p-1.$$

Using that $g_a \equiv g_b$ if $a \equiv b \mod p-1$ we also find the following congruences (modulo p).

$$g_{-2m} \equiv \begin{cases} -(-p)^{s_p(-2m)}\dfrac{1}{(2m)!}, & \text{if } 0 \le m < \dfrac{p-1}{2}, \\ -(-p)^{s_p(-2m)}\dfrac{1}{(2m+1-p)!}, & \text{if } \dfrac{p-1}{2} \le m < p-1. \end{cases}$$

$$g_{-3m} \equiv \begin{cases} -(-p)^{s_p(-3m)}\dfrac{1}{(3m)!}, & \text{if } 0 \le m < \dfrac{p-1}{3}, \\ -(-p)^{s_p(-3m)}\dfrac{1}{(3m+1-p)!}, & \text{if } \dfrac{p-1}{3} \le m < \dfrac{2(p-1)}{3}, \\ -(-p)^{s_p(-3m)}\dfrac{1}{(3m+2-2p)!}, & \text{if } \dfrac{2(p-1)}{3} \le m < p-1. \end{cases}$$

$$g_{4m} \equiv \begin{cases} (-p)^{s_p(4m)}(4m)!, & \text{if } 0 < m \le \dfrac{p-1}{4}, \\ (-p)^{s_p(4m)}(4m+1-p)!, & \text{if } \dfrac{p-1}{4} < m \le \dfrac{p-1}{2}, \\ (-p)^{s_p(4m)}(4m+2-2p)!, & \text{if } \dfrac{p-1}{2} < m \le \dfrac{3(p-1)}{4}, \\ (-p)^{s_p(4m)}(4m+3-3p)!, & \text{if } \dfrac{3(p-1)}{4} < m \le p-1. \end{cases}$$

$$g_{3m} \equiv \begin{cases} (-1)^m(-p)^{s_p(3m)}(3m)!, & \text{if } 0 < m \le \dfrac{p-1}{3}, \\ (-1)^m(-p)^{s_p(3m)}(3m+1-p)!, & \text{if } \dfrac{p-1}{3} < m \le \dfrac{2(p-1)}{3}, \\ (-1)^m(-p)^{s_p(3m)}(3m+3-2p)!, & \text{if } \dfrac{2(p-1)}{3} < m \le p-1. \end{cases}$$

$$g_{6m} \equiv \begin{cases} (-p)^{s_p(6m)}(6m)!, & \text{if } 0 < m \le \dfrac{p-1}{6}, \\ (-p)^{s_p(6m)}(6m+1-p)!, & \text{if } \dfrac{p-1}{6} < m \le \dfrac{p-1}{3}, \\ (-p)^{s_p(6m)}(6m+2-2p)!, & \text{if } \dfrac{p-1}{3} < m \le \dfrac{p-1}{2}, \\ (-p)^{s_p(6m)}(6m+3-3p)!, & \text{if } \dfrac{p-1}{2} < m \le \dfrac{2(p-1)}{3}, \\ (-p)^{s_p(6m)}(6m+4-4p)!, & \text{if } \dfrac{2(p-1)}{3} < m \le \dfrac{5(p-1)}{6}, \\ (-p)^{s_p(6m)}(6m+5-5p)!, & \text{if } \dfrac{5(p-1)}{6} < m \le p-1. \end{cases}$$

Chapter 4

Super Congruences

In this chapter we will find a connection between the Gauss sums of the previous chapter and the elliptic curves of chapter 2. For this we use the following theorem

Theorem 4.1. *Let V_λ be the affine variety given by the dehomogenized equation*

$$f_\lambda = 1 + y_1 + y_2 + \cdots + y_d + \lambda y_1^{a_1} \cdots y_d^{a_d} = 0,$$

where $a_i \in \mathbb{Z}$. Then for any prime p

$$|V_\lambda(\mathbb{F}_p^\times)| - |V_0(\mathbb{F}_p^\times)| = \frac{1}{p-1}\left((-1)^d + \frac{1}{p}\sum_{m=1}^{p-2} g_{a_0 m}\cdots g_{a_d m} g_{-m}\omega(\lambda)^m\right),$$

where $a_0 \in \mathbb{Z}$ such that $a_0 + a_1 + a_2 + ... + a_d = 1$ and ω is the Teichmüller character.

Before proving this theorem we prove the following lemma.

Lemma 4.2. *Let V_d be the variety given by the dehomogenized equation*

$$V_d : 1 + y_1 + y_2 + \cdots + y_d = 0.$$

Then $\left|V_d(\mathbb{F}_p^\times)\right| = \frac{1}{p}\left((p-1)^d - (-1)^d\right)$.

Proof. We prove this theorem by induction on the parameter d. For $d = 1$ we find

$$\left|V_1(\mathbb{F}_p^\times)\right| = 1 = \frac{1}{p}\left((p-1)^d - (-1)^d\right),$$

so this lemma holds for $d = 1$. Now suppose that this lemma is true for all $d \leq D$. We take $d = D + 1$. For any choice of $y_1, ..., y_D \in \mathbb{F}_p^\times$ there exists a unique $y_{D+1} \in \mathbb{F}_p$ such that $1 + y_1 + y_2 + \cdots + y_{D+1} = 0$. Moreover $y_{D+1} \in \mathbb{F}_p^\times$ if and only if $1 + y_1 + y_2 + \cdots + y_D \neq 0$. There are $(p-1)^D$ possible choices for $y_1, ..., y_D \in \mathbb{F}_p^\times$, and for $\left|V_D(\mathbb{F}_p^\times)\right|$ of these choices we have $1 + y_1 + y_2 + \cdots + y_D = 0$. Hence

$$\begin{aligned}
\left|V_{D+1}(\mathbb{F}_p^\times)\right| &= (p-1)^D - \left|V_D(\mathbb{F}_p^\times)\right| \\
&= (p-1)^D - \frac{1}{p}\left((p-1)^D - (-1)^D\right) \\
&= \frac{1}{p}\left((p-1)^{D+1} - (-1)^{D+1}\right),
\end{aligned}$$

where the second equality follows from the induction hypotheses. Hence this lemma is also true for $d = D + 1$. □

Proof of theorem 4.1. Let p be a prime and let

$$F_\lambda(t_0, \mathbf{y}) = t_0 + y_1 + y_2 + \cdots + y_d + \lambda t_0^{a_0} y_1^{a_1} \cdots y_d^{a_d} = 0$$

be the homogenized equation of the variety V_λ. Notice that

$$F_\lambda(t_0, \mathbf{y}) = t_0 f_\lambda(\frac{\mathbf{y}}{t_0}).$$

Let now ψ be the additive character

$$\psi : \mathbb{F}_p \longrightarrow \mathbf{Q}_p(\zeta_\pi), \quad x \longmapsto \zeta_\pi^x$$

of the previous chapter. Then we can consider the following sum

$$\begin{aligned} S_p(F) &= \sum_{t_0, y_i \in \mathbb{F}_p^\times} \psi(F_\lambda(t_0, \mathbf{y})) \\ &= \sum_{t_0, y_i \in \mathbb{F}_p^\times} \psi(t_0 f_\lambda(\mathbf{y} t_0^{-1})) \\ &= \sum_{t_0, y_i \in \mathbb{F}_p^\times} \psi(t_0 f_\lambda(\mathbf{y})) \\ &= \left(\sum_{t_0 \in \mathbb{F}_p, y_i \in \mathbb{F}_p^\times} \psi(t_0 f_\lambda(\mathbf{y})) \right) - (p-1)^d. \end{aligned}$$

If we now use the fact that

$$\sum_{x \in \mathbb{F}_p} \psi(x) = 0,$$

we see that

$$\sum_{t_0 \in \mathbb{F}_p} \psi(t_0 f_\lambda(\mathbf{y})) = \begin{cases} p & \text{if } f_\lambda(\mathbf{y}) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore we find the following identity

$$S_p(F) = p|V_\lambda(\mathbb{F}_p^\times)| - (p-1)^d.$$

Hence using the identity above we find

$$p|V_\lambda(\mathbb{F}_p^\times)| = (p-1)^d - (-1)^d + S_p(F) + (-1)^d.$$

Now notice that, by lemma 4.2, $|V_0(\mathbb{F}_p^\times)| = \frac{1}{p}\left((p-1)^d - (-1)^d\right)$. We thus find

$$|V_\lambda(\mathbb{F}_p^\times)| - |V_0(\mathbb{F}_p^\times)| = \frac{1}{p} S_p(F) + \frac{1}{p}(-1)^d. \tag{4.1}$$

We will now compute the sum $S_p(F)$ in a different way. Equation 3.1 of chapter 3 namely gives the following identity

$$\psi(y) = \frac{1}{p-1} \sum_{s=0}^{p-2} g_s \omega(y)^{-s}.$$

In particular we have

$$\begin{aligned} S_p(F) &= \sum_{t_0,y_i\in\mathbb{F}_p^\times} \psi(t_0)\psi(y_1)\cdots\psi(y_d)\psi(\lambda t_0^{a_0}y_1^{a_1}\cdots y_d^{a_d}) \\ &= \frac{1}{(p-1)^{d+2}} \sum_{t_0,y_i\in\mathbb{F}_p^\times} \sum_{s_0,\cdots,s_{d+1}=0}^{p-2} g_{s_0}\cdots g_{s_{d+1}}\omega(t_0)^{-s_0}\omega(y_1)^{-s_1}\cdots\omega(\lambda t_0^{a_0}y_1^{a_1}\cdots y_d^{a_d})^{-s_{d+1}} \\ &= \frac{1}{(p-1)^{d+2}} \sum_{s_0,\cdots,s_{d+1}=0}^{p-2} g_{s_0}\cdots g_{s_{d+1}}\omega(\lambda)^{-s_{d+1}} \sum_{t_0,y_i\in\mathbb{F}_p^\times} \omega(t_0^{s_0+a_0s_{d+1}}y_1^{s_1+a_1s_{d+1}}\cdots y_d^{s_d+a_ds_{d+1}})^{-1}. \end{aligned}$$

But for all j we have

$$\sum_{y_j\in\mathbb{F}_p^\times} \omega(y_j^{s_j+a_js_{d+1}})^{-1} = \begin{cases} p-1 & \text{if } s_j = -a_js_{d+1}, \\ 0 & \text{otherwise.} \end{cases}$$

A similar relation holds for t_0. Therefore we can simplify the expression for $S_p(F)$ as follows

$$\begin{aligned} S_p(F) &= \frac{1}{(p-1)^{d+2}} \sum_{s_{d+1}=0}^{p-2} g_{-a_0s_{d+1}}g_{-a_1s_{d+1}}\cdots g_{-a_ds_{d+1}}g_{s_{d+1}}\omega(\lambda)^{-s_{d+1}}(p-1)^{d+1} \\ &= \frac{1}{p-1}\sum_{m=0}^{p-2} g_{a_0m}\cdots g_{a_dm}g_{-m}\omega(\lambda)^m. \end{aligned}$$

Together with equation 4.1 it now follows that

$$\begin{aligned} |V_\lambda(\mathbb{F}_p^\times)| - |V_0(\mathbb{F}_p^\times)| &= \frac{(-1)^d}{p} + \frac{1}{p(p-1)}\sum_{m=0}^{p-2} g_{a_0m}\cdots g_{a_dm}g_{-m}\omega(\lambda)^m \\ &= \frac{(-1)^d}{p} + \frac{(-1)^d}{p(p-1)} + \frac{1}{p(p-1)}\sum_{m=1}^{p-2} g_{a_0m}\cdots g_{a_dm}g_{-m}\omega(\lambda)^m \\ &= \frac{1}{p-1}\left((-1)^d + \frac{1}{p}\sum_{m=1}^{p-2} g_{a_0m}\cdots g_{a_dm}g_{-m}\omega(\lambda)^m\right). \end{aligned}$$

□

We will rewrite the Gauss sums as in the previous chapter and use some of the formulas found in chapter 2 to obtain certain congruences. Let us first start with the following cubic curve.

4.1 The cubic curve $C_1(t) : y^2 + xy + x^3 + t = 0$

Proposition 4.3. *Let p be a primes and let $C_1(t) : y^2 + xy + x^3 + t = 0$ be an elliptic curve for some $t \in \mathbb{F}_p$. Then,*

$$|C_1(t)(\mathbb{F}_p)| \equiv -\sum_{m=1}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!}t^m \mod p.$$

Before proving this proposition we will state and prove a useful lemma. This lemma can be used to connect the number of points of an elliptic curve over $\mathbb{F}_p$ to the number of points over $\mathbb{F}_p^\times$ in a nice way.

Lemma 4.4. *For all $t \in \mathbb{F}_p$ we have*

$$\#\{x \in \mathbb{F}_p : x^3 \equiv t \mod p\} = \begin{cases} 1 + \omega\left(t^{\frac{p-1}{3}}\right) + \omega\left(t^{\frac{2(p-1)}{3}}\right) & \text{if } p \equiv 1 \mod 3, \\ 1 & \text{if } p \equiv 2 \mod 3, \end{cases}$$

where ω is the Teichmüller character.

Proof. First suppose $p \equiv 1 \mod 3$. The case $t = 0$ is clear so we take $t \neq 0$. The discriminant of $x^2 + x + 1$ equals -3, which is a square modulo p. Therefore the equation $x^2 + x + 1 = 0$ has a solution in $\mathbb{F}_p$, hence $\mathbb{F}_p$ contains a primitive cube root of unity. It follows that if a is a solution of the equation $x^3 \equiv t \mod p$, we can find two other solutions by multiplying a by a primitive cube root of unity. Hence if t is a cube modulo p we find

$$\#\{x \in \mathbb{F}_p : x^3 \equiv t \mod p\} = 3,$$

but on the other hand $t = x^3$ for some $x \in \mathbb{F}_p$ and thus

$$1 + t^{\frac{p-1}{3}} + t^{\frac{2(p-1)}{3}} \equiv 1 + x^{p-1} + x^{2(p-1)} \equiv 3 \mod p.$$

If t is not a cube modulo p then $\#\{x \in \mathbb{F}_p : x^3 \equiv t \mod p\} = 0$, moreover $t \equiv x^a$ for some generator x of $\mathbb{F}_p^\times$ and some $a \in \mathbb{Z}$ not divisible by 3. Hence

$$t^{\frac{p-1}{3}} \equiv x^{\frac{a(p-1)}{3}} \neq 1,$$

since $\frac{a(p-1)}{3}$ is not divisible by $p-1$. But $t^{\frac{p-1}{3}}$ is a root of $x^3 - 1 = (x-1)(x^2+x+1)$, therefore it is a root of $x^2 + x + 1$ and the first case of the lemma follows.

Now suppose $p \equiv 2 \mod 3$. Since we can write $p = 3n + 2$ for some $n \in \mathbb{Z}$ we have

$$x \equiv x^{p-1}x^p \equiv x^{6n+3} \equiv (x^{2n+1})^3 \mod p,$$

for all $x \in \mathbb{F}_p$. Therefore any element of $\mathbb{F}_p$ is a cube and $\#\{x \in \mathbb{F}_p : x^3 \equiv t \mod p\} = 1$ for all t. □

We are now ready to prove proposition 4.3.

Proof of proposition 4.3. Let $V_1(t)$ be the variety given by the dehomogenized equation

$$f_t = 1 + x + y + tx^{-3}y^{-2} = 0.$$

Then for any prime p we have the following map

$$\varphi : V_1(t)(\mathbb{F}_p^\times) \to C_1(t)(\mathbb{F}_p^\times), \qquad (x, y) \mapsto (xy, x^2y).$$

This map is well defined, moreover it is a bijection with inverse

$$\varphi^{-1} : C_1(t)(\mathbb{F}_p^\times) \to V_1(t)(\mathbb{F}_p^\times), \qquad (x, y) \mapsto \left(\frac{y}{x}, \frac{x^2}{y}\right).$$

Hence $|V_1(t)(\mathbb{F}_p^\times)| = |C_1(t)(\mathbb{F}_p^\times)|$ for all primes p. Moreover we see that

$$|C_1(t)(\mathbb{F}_p^\times)| = |C_1(t)(\mathbb{F}_p))| - 1 - \#\{x \in \mathbb{F}_p : x^3 \equiv -t \mod p\} - \#\{y \in \mathbb{F}_p : y^2 \equiv -t \mod p\}.$$

Now notice that $\#\{y \in \mathbb{F}_p : y^2 \equiv -t \mod p\} = 1 + \left(\frac{-t}{p}\right)$. Thus by lemma 4.4 we find

$$|C_1(t)(\mathbb{F}_p))| = \begin{cases} |V_1(t)(\mathbb{F}_p^\times)| + 3 + t^{\frac{p-1}{3}} + t^{\frac{2(p-1)}{3}} + \left(\dfrac{-t}{p}\right) & \text{if } p \equiv 1 \mod 3, \\ |V_1(t)(\mathbb{F}_p^\times)| + 3 + \left(\dfrac{-t}{p}\right) & \text{if } p \equiv 2 \mod 3. \end{cases} \tag{4.2}$$

By theorem 4.1 we have

$$|V_1(t)(\mathbb{F}_p^\times)| - |V_1(0)(\mathbb{F}_p^\times)| = \frac{1}{p-1}\left(1 + \sum_{m=1}^{p-2} P_1(m)\omega(t)^m\right),$$

where $P_1(m) := \dfrac{1}{p} g_{6m} g_{-3m} g_{-2m} g_{-m}$. And for $0 \le m < p-1$ we see that

$$\begin{aligned} S_1(m) &:= s_p(6m) + s_p(-3m) + s_p(-2m) + s_p(-m) \\ &= \left\{\frac{6m}{1-p}\right\} + \left\{\frac{-3m}{1-p}\right\} + \left\{\frac{-2m}{1-p}\right\} + \left\{\frac{-m}{1-p}\right\} \\ &= \frac{6m}{1-p} + \frac{-3m}{1-p} + \frac{-2m}{1-p} + \frac{-m}{1-p} - \left\lfloor\frac{6m}{1-p}\right\rfloor - \left\lfloor\frac{-3m}{1-p}\right\rfloor - \left\lfloor\frac{-2m}{1-p}\right\rfloor - \left\lfloor\frac{-m}{1-p}\right\rfloor \\ &= \left\lceil\frac{6m}{p-1}\right\rceil - \left\lfloor\frac{3m}{p-1}\right\rfloor - \left\lfloor\frac{2m}{p-1}\right\rfloor. \end{aligned}$$

Note that $S_1(m) - 1$ is the exponent of the factor p occurring in each term $P_1(m)$. By the above it now follows that

$$S_1(m) = \begin{cases} 1, & \text{if } 0 < m \le \dfrac{p-1}{6}, \\ 2, & \text{if } \dfrac{p-1}{6} < m < \dfrac{p-1}{3}, \\ 1, & \text{if } m = \dfrac{p-1}{3}, \\ 2, & \text{if } \dfrac{p-1}{3} < m < \dfrac{p-1}{2}, \\ 1, & \text{if } m = \dfrac{p-1}{2}, \\ 2, & \text{if } \dfrac{p-1}{2} < m < \dfrac{2(p-1)}{3}, \\ 1, & \text{if } m = \dfrac{2(p-1)}{3}, \\ 2, & \text{if } \dfrac{2(p-1)}{3} < m \le \dfrac{5(p-1)}{6}, \\ 3, & \text{if } \dfrac{5(p-1)}{6} < m < p-1. \end{cases}$$

Now assume p is a prime such that $p \equiv 1 \mod 3$, i.e. $p \equiv 1 \mod 6$. If we then use the congruences of the previous chapter concerning the Gauss sums, we find the following congruence modulo p

$$P_1(m) \equiv \begin{cases} \dfrac{(6m)!}{(3m)!(2m)!m!} & \text{if } 1 \le m \le \dfrac{p-1}{6}, \\ -\dfrac{1}{\left(\frac{2(p-1)}{3}\right)!\left(\frac{p-1}{3}\right)!} & \text{if } m = \dfrac{p-1}{3}, \\ -\dfrac{1}{\left(\frac{p-1}{2}\right)!\left(\frac{p-1}{2}\right)!} & \text{if } m = \dfrac{p-1}{2}, \\ -\dfrac{1}{\left(\frac{p-1}{3}\right)!\left(\frac{2(p-1)}{3}\right)!} & \text{if } m = \dfrac{2(p-1)}{3}, \\ 0 & \text{otherwise.} \end{cases}$$

A very important identity we have used is the fact that $g_a = g_b$ if $a \equiv b \mod p-1$, in particular $g_{p-1} = g_0 = -1$. Moreover we see that since $p-1$ is even,

$$\left(\frac{2(p-1)}{3}\right)!\left(\frac{p-1}{3}\right)! \equiv -1 \mod p \text{ for all primes } p \equiv 1 \mod 3.$$

The term $\left(\frac{p-1}{2}\right)!\left(\frac{p-1}{2}\right)!$ is the final term we have to consider, it is the product of all quadratic residues modulo p. If a is a quadratic residue modulo p then so is its multiplicative inverse. Hence we can pair all factors in this product with their inverses unless the factor is its own inverse. Therefore we find as in the proof of theorem 3.1

$$\left(\frac{p-1}{2}\right)!\left(\frac{p-1}{2}\right)! \equiv -\left(\frac{-1}{p}\right).$$

Hence altogether we find the following congruence,

$$P_1(m) \equiv \begin{cases} \dfrac{(6m)!}{(3m)!(2m)!m!} & \mod p \text{ if } 1 \le m \le \dfrac{p-1}{6}, \\ -1 & \mod p \text{ if } m = \dfrac{p-1}{3}, \\ -\left(\dfrac{-1}{p}\right) & \mod p \text{ if } m = \dfrac{p-1}{2}, \\ -1 & \mod p \text{ if } m = \dfrac{2(p-1)}{3}, \\ 0 & \mod p \text{ otherwise.} \end{cases}$$

If we now use the fact that $|V_1(0)(\mathbb{F}_p^\times)| = p-2$, we see that for all primes $p \equiv 1 \mod 3$

$$\begin{aligned}
|V_1(t)(\mathbb{F}_p^\times)| &= \frac{1}{p-1}\left(1+\sum_{m=1}^{p-2} P_1(m)\omega(t)^m\right)+p-2 \\
&\equiv -3-\sum_{m=1}^{p-2} P_1(m)t^m && \mod p, \\
&\equiv -3-t^{\frac{p-1}{3}}-t^{\frac{2(p-1)}{3}}-\left(\frac{-1}{p}\right)t^{\frac{p-1}{2}}-\sum_{m=1}^{\frac{p-1}{6}}\frac{(6m)!}{(3m)!(2m)!m!}t^m && \mod p.
\end{aligned}$$

Here we used that $\omega(t) \equiv t \mod p$ for all $t \in \mathbb{F}_p$. Combined with equation 4.2 we see that for all primes $p \equiv 1 \mod 3$,

$$|C_1(t)(\mathbb{F}_p)| \equiv -\sum_{m=1}^{\frac{p-1}{6}}\frac{(6m)!}{(3m)!(2m)!m!}t^m \mod p.$$

Now suppose $p \equiv 2 \mod 3$. Then

$$|V_1(t)(\mathbb{F}_p^\times)| \equiv -3-\left(\frac{-t}{p}\right)-\sum_{m=1}^{\lfloor\frac{p-1}{6}\rfloor}\frac{(6m)!}{(3m)!(2m)!m!}t^m \mod p.$$

This means that for all primes p,

$$|C_1(t)(\mathbb{F}_p))| \equiv -\sum_{m=1}^{p-1}\frac{(6m)!}{(3m)!(2m)!m!}t^m \mod p,$$

where we have used the fact that $\dfrac{(6m)!}{(3m)!(2m)!m!} \equiv 0 \mod p$ for all $m > \frac{p-1}{6}$. □

The following theorem enables us to find even more congruences, when using proposition 4.3.

Theorem 4.5. *Let p be an odd prime and let x be a variable. Then*

$$\left(\sum_{m=0}^{p-1}\frac{(6m)!}{(3m)!(2m)!m!}x^m\right)^2 \equiv \sum_{m=0}^{p-1}\frac{(6m)!}{(3m)!(m!)^3}(x(1-432x))^m \mod p^2.$$

Proof. See theorem 3.1 of [Sun11b]. The proof uses a Wilf-Zeilberger pair. This is a pair of functions that can be used to certify certain combinatorial identities. □

The curve $C_1(t) : y^2+xy+x^3+t=0$ has a parameter t. Its discriminant and j-invariant are given by

$$\triangle(C_1(t)) = -t(432t-1) \quad \text{and} \quad j(C_1(t)) = \frac{-1}{432t^2-t}.$$

We will be interested in the t-values for which $C_1(t)$ is singular or has complex multiplication. For these curves chapters 1 and 2 will give us cardinality formulas and combined with the results above this will lead to certain congruences.

The curve $C_1(t)$ is singular over $\mathbb{Q}$ for $t=0$ and for $t=432^{-1}$. Moreover $t=864^{-1}$ is the only rational t-value for which the curve $C_1(t)$ has complex multiplication. This can be easily seen since there are only finitely many j-invariants such that an elliptic curve over $\mathbb{Q}$ has complex multiplication.

4.1.1 The case $t = 432^{-1}$

For $t = 432^{-1}$ we can apply the following transformation

$$\phi : C_1\left(\frac{1}{432}\right) \longrightarrow C : y^2 = x^3 - x^2, \quad (x, y) \longmapsto \left(\frac{2}{3} - 4x, 8y + 4x\right).$$

Hence by corollary 1.4 we see

$$\left|C_1\left(\frac{1}{432}\right)(\mathbb{F}_p)\right| = p + 1 - \left(\frac{-1}{p}\right),$$

for all primes $p > 3$. Combining this result with proposition 4.3 we find the following congruence for primes $p > 3$

$$-\sum_{m=1}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} 432^{-m} \equiv 1 - \left(\frac{-1}{p}\right) \mod p.$$

Rearranging the terms now gives us

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} 432^{-m} \equiv \left(\frac{-1}{p}\right) \mod p, \tag{4.3}$$

which holds for all primes $p > 3$. Note that for these primes the reduction and transformation are well defined.

This sum is also treated in an article [Sun11c] of Zhi-Wei Sun. In this article some open conjectures on congruences are described. Some of these conjectures are proven already. The following conjecture leads to a congruences concerning the sum mentioned above. However most of the congruences in [Sun11c] hold modulo higher powers of p.

Conjecture 4.6 ([Sun11c, A45])**.** *For any prime $p > 3$ we have*

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} 432^{-m} \equiv \left(\frac{-1}{p}\right) - \frac{25}{9}p^2 E_{p-2} \mod p^3,$$

where E_k are the Euler numbers defined by

$$E_0 = 1 \quad \textit{and} \quad \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} E_{n-2k} = 0 \textit{ for } n \in \mathbb{Z}_{>0}.$$

4.1.2 The case $t = 864^{-1}$

The curve $C_1(864^{-1})$ has j-invariant 1728 and endomorphism ring $\mathbb{Z}[i]$. This curve is not isomorphic to a quadratic twist of any of the curves treated in chapter 2. However we do know that if a prime $p > 3$ is inert in $\mathbb{Z}[i]$, then $\left|C_1(864^{-1})\right| = p + 1$. Therefore the following congruence holds for all primes $p > 3$ congruent to -1 modulo 4,

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} 864^{-m} \equiv 0 \mod p.$$

This sum appears in conjecture B16 of [Sun11c], where a congruence modulo p^2 is conjectured. This conjecture has been proven already. Modulo p this conjecture coincides with the congruences above.

If we now take the square of this sum we find a congruence modulo p^2, since if a number is divisible by p its square must be divisible by p^2. Therefore we can use theorem 4.5 to find

$$\begin{aligned}\sum_{m=0}^{p-1}\frac{(6m)!}{(3m)!(m!)^3}1728^{-m} &\equiv \left(\sum_{m=0}^{p-1}\frac{(6m)!}{(3m)!(2m)!m!}864^{-m}\right)^2 && \mod p^2,\\ &\equiv 0 && \mod p^2,\end{aligned}$$

which holds for all primes $p>3$ congruent to -1 modulo 4.

Again this sum appears in a conjecture stated by Zhi-Wei Sun. This time we have proven a part of the following conjecture.

Conjecture 4.7 ([Sun11c, A29]). *For any prime $p>3$ we have*

$$\sum_{m=0}^{p-1}\frac{(6m)!}{(3m)!(m!)^3}1728^{-m}\equiv\begin{cases}\left(\frac{p}{3}\right)(4x^2-2p) & \mod p^2 \quad \text{if } p\equiv 1 \mod 4 \text{ and}\\ & \quad p=x^2+y^2 \text{ where } x \text{ is odd,}\\ 0 & \mod p^2 \quad \text{if } p\equiv -1 \mod 4.\end{cases}$$

This conjecture has already been solved by Zhi-Wei Sun in [Sun12]. However the tools used in this paper are very different from the ones we used.

4.1.3 The case $t=\left(143748\pm 24948\sqrt{33}\right)^{-1}$

We can also consider some irrational t-values since for some primes p these irrational t-values reduce to elements in $\mathbb{F}_p$. Suppose for example that $p>3$ is a prime such that $\left(\frac{33}{p}\right)=1$. Then the ideal (p) splits in $R=\mathbb{Z}\left[\frac{1+\sqrt{33}}{2}\right]$, where R is the ring of integers of $\mathbb{Q}(\sqrt{33})$. In other words there exist ideals $\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_2\subset R$ such that $(p)=\boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$. Moreover

$$R/\boldsymbol{\lambda}_1\cong\mathbb{F}_p.$$

Hence if we reduce the elliptic curve $C_1\left(\left(143748-24948\sqrt{33}\right)^{-1}\right)$ modulo $\boldsymbol{\lambda}_1$ we obtain an elliptic curve over $\mathbb{F}_p$. This means however that the congruences obtained will not be modulo p but modulo $\boldsymbol{\lambda}_1$.

A short Weierstrass model for $C_1(t)$ is given by

$$C_1'(t): y^2=x^3-\frac{1}{48}x+\frac{1}{864}-t.$$

A transformation from $C_1(t)$ to $C_1'(t)$ is given by

$$\phi: C_1(t)\longrightarrow C_1'(t),\qquad (x,y)\longmapsto\left(\frac{1}{12}-x,y+\frac{1}{2}x\right).$$

Hence for all $t\in\mathbb{F}_p$ and for all primes $p>3$, $|C_1(\mathbb{F}_p)|=|C_1'(\mathbb{F}_p)|$.

The elliptic curve

$$C_1'\left(\left(143748-24948\sqrt{33}\right)^{-1}\right)$$

has j-invariant 66^3 and therefore complex multiplication by $\mathbb{Z}[2i]$. When we twist this elliptic curve with $2\sqrt[4]{33}$ we obtain the curve

$$E_2: y^2=x^3-11x-14.$$

So if $\left(\frac{33}{p}\right) = 1$ we find

$$\left| C_1\left(\left(143748 - 24948\sqrt{33}\right)^{-1}\right)(\mathbb{F}_p)\right| - p + 1 = \left(\frac{\sqrt{33}}{\boldsymbol{\lambda}_1}\right)(|E_2(\mathbb{F}_p)| - p + 1).$$

Here

$$\left(\frac{a}{\boldsymbol{\lambda}_1}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue in } R/\boldsymbol{\lambda}_1, \\ -1 & \text{if } a \text{ is a quadratic nonresidue in } R/\boldsymbol{\lambda}_1, \end{cases}$$

for all $a \in \mathbb{Q}(\sqrt{33})$.

By proposition 2.2 it now follows that, for all odd primes p such that $\left(\frac{33}{p}\right) = 1$,

$$\left| C_1\left(\left(143748 - 24948\sqrt{33}\right)^{-1}\right)(\mathbb{F}_p)\right| = \begin{cases} p+1 & \text{if } p \equiv -1 \mod 4, \\ p+1-\left(\frac{\sqrt{33}}{\boldsymbol{\lambda}_1}\right)2x & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2+y^2, \\ & \text{with } x \equiv 1 \mod 4. \end{cases}$$

Combined with proposition 4.3 the following congruence holds for all odd primes p such that $\left(\frac{33}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in R,

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!}\left(143748 - 24948\sqrt{33}\right)^{-m} \equiv$$

$$\begin{cases} 0 \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv -1 \mod 4, \\ \left(\frac{\sqrt{33}}{\boldsymbol{\lambda}_1}\right)2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2+y^2 \text{ with } x \equiv 1 \mod 4. \end{cases}$$

Notice that when we reduce the elliptic curve modulo the ideal $\boldsymbol{\lambda}_2$ we find similar results. In particular we find

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!}\left(143748 - 24948\sqrt{33}\right)^{-m} \equiv 0 \mod \boldsymbol{\lambda}_2 \qquad \text{if } p \equiv -1 \mod 4.$$

Hence this sum is an element of both $\boldsymbol{\lambda}_1$ and $\boldsymbol{\lambda}_2$. From this it follows that this sum is an element of the ideal (p) and therefore the congruence holds modulo p. Altogether we thus find the following congruence which holds for all odd primes p such that $\left(\frac{33}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in R,

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!}\left(143748 - 24948\sqrt{33}\right)^{-m} \equiv$$

$$\begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 4, \\ \left(\frac{\sqrt{33}}{\boldsymbol{\lambda}_1}\right)2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2+y^2 \text{ with } x \equiv 1 \mod 4. \end{cases}$$

We find a similar result for the case

$$t = \left(143748 + 24948\sqrt{33}\right)^{-1}.$$

Namely for all odd primes p such that $\left(\frac{33}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in R,

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!}\left(143748 + 24948\sqrt{33}\right)^{-m} \equiv$$

$$\begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 4, \\ \left(\frac{-\sqrt{33}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2 + y^2 \text{ with } x \equiv 1 \mod 4. \end{cases}$$

When we now use theorem 4.5 we find the following congruence

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(m!)^3} 66^{-3m} \equiv \begin{cases} 0 \mod p^2 & \text{if } p \equiv -1 \mod 4, \\ 4x^2 \mod p & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2 + y^2, \\ & \text{with } x \equiv 1 \mod 4, \end{cases}$$

which holds for all odd primes p such that $\left(\frac{33}{p}\right) = 1$. This congruence holds modulo p^2 and p since all terms in the sum are rational numbers.

In the next sections we will consider t-values in quadratic extensions of $\mathbb{Q}$ such that the elliptic curve $C_1(t)$ has complex multiplication. Using the same methods we can also find congruences for t-values in other extensions of $\mathbb{Q}$. The important part is that we are able to reduce the elliptic curve to an elliptic curve over the finite field $\mathbb{F}_p$.

4.1.4 The case $t = \left(27000 \pm 11880\sqrt{5}\right)^{-1}$

When we twist the elliptic curve

$$C_1'\left(\left(27000 + 11880\sqrt{5}\right)^{-1}\right) : y^2 = x^3 - \frac{1}{48}x + \frac{11\sqrt{5}}{21600}$$

with $2\sqrt[4]{45}$ we obtain the curve $E_4 : y^2 = x^3 - 15x + 22$. Therefore proposition 2.4 combined with proposition 4.3 implies the following congruence,

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!}\left(27000 + 11880\sqrt{5}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 3, \\ \left(\frac{x}{3}\right)\left(\frac{3\sqrt{5}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2 + 3y^2, \end{cases}$$

which holds for all primes $p > 3$ such that $\left(\frac{5}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Similarly we find that the following congruence holds for all primes $p > 3$ such that $\left(\frac{5}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$,

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!}\left(27000 - 11880\sqrt{5}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 3, \\ \left(\frac{x}{3}\right)\left(\frac{-3\sqrt{5}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2 + 3y^2. \end{cases}$$

If we combine these congruences with theorem 4.5 the following congruence also follows for all primes $p > 3$ such that $\left(\frac{5}{p}\right) = 1$,

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(m!)^3} 54000^{-m} \equiv \begin{cases} 0 \mod p^2 & \text{if } p \equiv -1 \mod 3, \\ 4x^2 \mod p & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2 + 3y^2. \end{cases}$$

4.1.5 The case $\mathrm{t} = \left(4000 - 1120\sqrt{10}\right)^{-1}$

We can do the exact same thing for all other j-invariants that give us complex multiplication. So for the remaining cases we will only state the congruences obtained this way.

The following congruences hold for all primes $p > 3$ such that $\left(\frac{10}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{10}\right]$.

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!}\left(4000 - 1120\sqrt{10}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1, 3 \mod 8, \\ \left(\frac{\sqrt{10}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1, 3 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 1 \mod 4, \\ \left(\frac{\sqrt{10}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 9, 11 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 3 \mod 4. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(m!)^3} 20^{-3m}$$

$$\equiv \begin{cases} 0 \mod p^2 & \text{if } p \not\equiv 1, 3 \mod 8, \\ 4x^2 \mod p & \text{if } p \equiv 1, 3 \mod 8 \text{ and } p = x^2 + 2y^2. \end{cases}$$

4.1.6 The case $\mathrm{t} = 2\left(-3375 + 405\sqrt{105}\right)^{-1}$

The following congruences hold for all primes $p > 3$ such that $\left(\frac{105}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\frac{1+\sqrt{105}}{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} \left(\frac{-3375+405\sqrt{105}}{2}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1,2,4 \mod 7, \\ \left(\dfrac{\sqrt{105}}{\boldsymbol{\lambda}_1}\right)\left(\dfrac{x}{7}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(m!)^3}(-15)^{-3m} \equiv \begin{cases} 0 \mod p^2 & \text{if } p \not\equiv 1,2,4 \mod 7, \\ 4x^2 \mod p & \text{if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2. \end{cases}$$

4.1.7 The case $\mathrm{t} = 2\left(16581375 - 392445\sqrt{1785}\right)^{-1}$

The following congruences hold for all primes $p > 3$ such that $\left(\frac{1785}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\frac{1+\sqrt{1785}}{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} \left(\frac{16581375-392445\sqrt{1785}}{2}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1,2,4 \mod 7, \\ \left(\dfrac{\sqrt{1785}}{\boldsymbol{\lambda}_1}\right)\left(\dfrac{x}{7}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(m!)^3} 255^{-3m} \equiv \begin{cases} 0 \mod p^2 & \text{if } p \not\equiv 1,2,4 \mod 7, \\ 4x^2 \mod p & \text{if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2. \end{cases}$$

4.1.8 The case $\mathrm{t} = \left(-6144000 - 1943040\sqrt{10}\right)^{-1}$

The following congruences hold for all primes $p > 3$ such that $\left(\frac{10}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{10}\right]$.

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} \left(-6144000-1943040\sqrt{10}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 3, \\ -\left(\dfrac{3\sqrt{10}}{\boldsymbol{\lambda}_1}\right)\left(\dfrac{x}{3}\right) x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1 \mod 3 \text{ and } 4p = x^2+27y^2. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(m!)^3}(-12288000)^{-m} \equiv \begin{cases} 0 \mod p^2 & \text{if } p \equiv -1 \mod 3, \\ x^2 \mod p & \text{if } p \equiv 1 \mod 3 \text{ and } 4p = x^2+27y^2. \end{cases}$$

4.1.9 The case $\mathrm{t} = \left(-16384 - 3584\sqrt{22}\right)^{-1}$

The following congruences hold for all primes $p > 3$ such that $\left(\frac{22}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{22}\right]$.

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} \left(-16384 - 3584\sqrt{22}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } \left(\frac{p}{11}\right) = -1, \\ -\left(\frac{\sqrt{22}}{\boldsymbol{\lambda}_1}\right)\left(\frac{x}{11}\right) x \mod \boldsymbol{\lambda}_1 & \text{if } \left(\frac{p}{11}\right) = 1 \text{ and } 4p = x^2 + 11y^2. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(m!)^3}(-32)^{-3m} \equiv \begin{cases} 0 \mod p^2 & \text{if } \left(\frac{p}{11}\right) = -1, \\ x^2 \mod p & \text{if } \left(\frac{p}{11}\right) = 1 \text{ and } 4p = x^2 + 11y^2. \end{cases}$$

4.1.10 The case $\mathrm{t} = \left(-442368 - 41472\sqrt{114}\right)^{-1}$

The following congruences hold for all primes $p > 3$ such that $\left(\frac{114}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{114}\right]$.

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} \left(-442368 - 41472\sqrt{114}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } \left(\frac{p}{19}\right) = -1, \\ -\left(\frac{\sqrt{114}}{\boldsymbol{\lambda}_1}\right)\left(\frac{x}{19}\right) x \mod \boldsymbol{\lambda}_1 & \text{if } \left(\frac{p}{19}\right) = 1 \text{ and } 4p = x^2 + 19y^2. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(m!)^3}(-96)^{-3m} \equiv \begin{cases} 0 \mod p^2 & \text{if } \left(\frac{p}{19}\right) = -1, \\ x^2 \mod p & \text{if } \left(\frac{p}{19}\right) = 1 \text{ and } 4p = x^2 + 19y^2. \end{cases}$$

4.1.11 The case $\mathrm{t} = \left(-442368000 - 17418240\sqrt{645}\right)^{-1}$

The following congruences hold for all primes $p > 3$ such that $\left(\frac{645}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\frac{1+\sqrt{645}}{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} \left(-442368000 - 17418240\sqrt{645}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } \left(\frac{p}{43}\right) = -1, \\ -\left(\frac{2\sqrt{645}}{\boldsymbol{\lambda}_1}\right)\left(\frac{x}{43}\right) x \mod \boldsymbol{\lambda}_1 & \text{if } \left(\frac{p}{43}\right) = 1 \text{ and } 4p = x^2 + 43y^2. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(m!)^3}(-960)^{-3m} \equiv \begin{cases} 0 \mod p^2 & \text{if } \left(\frac{p}{43}\right) = -1, \\ x^2 \mod p & \text{if } \left(\frac{p}{43}\right) = 1 \text{ and } 4p = x^2 + 43y^2. \end{cases}$$

4.1.12 The case $\mathrm{t} = \left(-73598976000 - 494968320\sqrt{22110}\right)^{-1}$

The following congruences hold for all primes $p > 3$ such that $\left(\frac{22110}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{22110}\right]$.

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} \left(-73598976000 - 494968320\sqrt{22110}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } \left(\frac{p}{67}\right) = -1, \\ -\left(\frac{\sqrt{22110}}{\boldsymbol{\lambda}_1}\right)\left(\frac{x}{67}\right) x \mod \boldsymbol{\lambda}_1 & \text{if } \left(\frac{p}{67}\right) = 1 \text{ and } 4p = x^2 + 67y^2. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(m!)^3}(-5280)^{-3m} \equiv \begin{cases} 0 \mod p^2 & \text{if } \left(\frac{p}{67}\right) = -1, \\ x^2 \mod p & \text{if } \left(\frac{p}{67}\right) = 1 \text{ and } 4p = x^2 + 67y^2. \end{cases}$$

4.1.13 The case $\mathrm{t} = \left(-131268706320384000 - 102791891220480\sqrt{1630815}\right)^{-1}$

The following congruences hold for all primes $p > 3$ such that $\left(\frac{1630815}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{1630815}\right]$.

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} \left(-131268706320384000 - 102791891220480\sqrt{1630815}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } \left(\frac{p}{163}\right) = -1, \\ -\left(\frac{2\sqrt{1630815}}{\boldsymbol{\lambda}_1}\right)\left(\frac{x}{163}\right) x \mod \boldsymbol{\lambda}_1 & \text{if } \left(\frac{p}{163}\right) = 1 \text{ and } 4p = x^2 + 163y^2. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(m!)^3}(-640320)^{-3m} \equiv \begin{cases} 0 \mod p^2 & \text{if } \left(\frac{p}{163}\right) = -1, \\ x^2 \mod p & \text{if } \left(\frac{p}{163}\right) = 1 \text{ and } 4p = x^2 + 163y^2. \end{cases}$$

4.2 The cubic curve $\mathrm{C_2(t) : y^2 + xy - ty + x^3 = 0}$

Proposition 4.8. *Let p be a prime and let $C_2(t) : y^2 + xy - ty + x^3 = 0$ be a cubic curve for some $t \in \mathbb{F}_p^\times$. Then for all primes p,*

$$|C_2(t)(\mathbb{F}_p)| \equiv -\sum_{m=1}^{p-1} \frac{(3m)!}{(m!)^3} t^m \mod p.$$

Proof. Let $V_2(t)$ be the variety given by the dehomogenized equation

$$f_t = 1 + x + y - tx^{-1}y^{-1} = 0.$$

Then for any prime p we have the following map

$$\varphi : V_2(t)(\mathbb{F}_p^\times) \to C_2(t)(\mathbb{F}_p^\times), \qquad (x, y) \mapsto \left(-\frac{t}{x}, -\frac{ty}{x}\right).$$

This map is well defined, moreover it is a bijection with inverse

$$\varphi^{-1} : C_2(t)(\mathbb{F}_p^\times) \to V_2(t)(\mathbb{F}_p^\times), \qquad (x, y) \mapsto \left(-\frac{t}{x}, -\frac{y}{x}\right).$$

Hence $|V_2(t)(\mathbb{F}_p^\times)| = |C_2(t)(\mathbb{F}_p^\times)|$ for all primes p. Moreover we see that

$$|C_2(t)(\mathbb{F}_p^\times)| = |C_2(t)(\mathbb{F}_p))| - 3,$$

since $\mathcal{O}, (0,0), (0,t) \in C_2(t)(\mathbb{F}_p)$ are the only points not defined over $\mathbb{F}_p^\times$. By theorem 4.1 we now have

$$|V_2(t)(\mathbb{F}_p^\times)| - |V_2(0)(\mathbb{F}_p^\times)| = \frac{1}{p-1}(1 + \sum_{m=1}^{p-2} P_2(m)\omega(-t)^m),$$

where $P_2(m) := \frac{1}{p} g_{3m} g_{-m}^3$. And for $0 \le m < p-1$ we have

$$\begin{aligned} S_2(m) &:= s_p(3m) + 3s_p(-m) \\ &= \left\{\frac{3m}{1-p}\right\} + 3\left\{\frac{-m}{1-p}\right\} \\ &= \frac{3m}{1-p} + 3\frac{-m}{1-p} - \left\lfloor \frac{3m}{1-p} \right\rfloor - 3\left\lfloor \frac{-m}{1-p} \right\rfloor \\ &= \left\lceil \frac{3m}{p-1} \right\rceil \end{aligned}$$

Hence

$$S_2(m) = \begin{cases} 1, & \text{if } 0 < m \leq \dfrac{p-1}{3}, \\ 2, & \text{if } \dfrac{p-1}{3} < m \leq \dfrac{2(p-1)}{3}, \\ 3, & \text{if } \dfrac{2(p-1)}{3} < m < p-1. \end{cases}$$

The following congruence now follows

$$P_2(m) \equiv \begin{cases} \dfrac{(-1)^m(3m)!}{(m!)^3} & \mod p \text{ if } 0 < m \leq \dfrac{p-1}{3}, \\ 0 & \mod p \text{ otherwise.} \end{cases}$$

Hence altogether we find

$$\begin{aligned} |C_2(t)(\mathbb{F}_p)| &= |V_2(t)(\mathbb{F}_p^\times)| + 3 \\ &= \frac{1}{p-1}\left(1 + \sum_{m=1}^{p-2} P_2(m)\omega(-t)^m\right) + p - 2 + 3 \\ &\equiv -\sum_{m=1}^{\frac{p-1}{3}} \frac{(3m)!}{(m!)^3} t^m \qquad \mod p \\ &\equiv -\sum_{m=1}^{p-1} \frac{(3m)!}{(m!)^3} t^m \qquad \mod p, \end{aligned}$$

where the last congruence follows since $\dfrac{(3m)!}{(m!)^3} \equiv 0 \mod p$ for all $m > \dfrac{p-1}{3}$. □

For this curve we find another theorem, which enables us to transform the sum of proposition 4.8 to another sum. Using the congruence given by this theorem we will be able to prove certain other congruences.

Theorem 4.9. *Let p be an odd prime and let x be a variable. Then*

$$\left(\sum_{m=0}^{p-1} \frac{(3m)!}{(m!)^3} x^m\right)^2 \equiv \sum_{m=0}^{p-1} \frac{(2m)!(3m)!}{(m!)^5} (x(1-27x))^m \mod p^2.$$

Proof. See theorem 2.1 of [Sun11b]. □

The curve $C_2(t) : y^2+xy-ty+x^3 = 0$ has the following discriminant and j-invariant respectively

$$\triangle(C_2(t)) = -t^3(27t-1) \quad \text{and} \quad j(C_2(t)) = \frac{(24t-1)^3}{27t^4 - t^3}.$$

In particular we see that $C_2(t)$ is singular for $t = 27^{-1}$ and for $t = 0$. Moreover we see that $C_2(t)$ has complex multiplication for the following rational t-values:

$$t \in \left\{\frac{1}{24}, \frac{1}{54}, \frac{-1}{216}\right\}.$$

We will also consider t-values that lie in a quadratic extension of $\mathbb{Q}$.

4.2.1 The case $t = 27^{-1}$

We can apply the following transformation for $t = 27^{-1}$

$$\phi : C_2\left(\frac{1}{27}\right) \longrightarrow C : y^2 = x^3 - 3x^2, \quad (x, y) \longmapsto (4 - 36x, 216y + 108x - 4).$$

We now see that the curve $C : y^2 = x^3 - 3x^2$ is obtained from the curve $y^2 = x^3 + x^2$ by twisting with $\sqrt{-3}$. Therefore corollary 1.4 gives us

$$\left|C_2\left(\frac{1}{27}\right)(\mathbb{F}_p)\right| = p + 1 - \left(\frac{-3}{p}\right),$$

for all primes $p > 3$. Combining this result with proposition 4.8 and rearranging the terms gives the following congruence

$$\sum_{m=0}^{p-1} \frac{(3m)!}{(m!)^3} 27^{-m} \equiv \left(\frac{-3}{p}\right) \mod p,$$

for all primes $p > 3$ (see also conjecture A52 of [Sun11c]).

4.2.2 The case $t = 24^{-1}$

The curve $C_2(24^{-1})$ has j-invariant 0 and therefore endomorphism ring $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. This curve is not isomorphic to any of the curves treated in chapter 2. However we do know that if a prime p is inert this endomorphism ring, then $\left|C_2(24^{-1})\right| = p + 1$. Therefore the following congruence holds for all odd primes $p \equiv -1 \mod 3$,

$$\sum_{m=0}^{p-1} \frac{(3m)!}{(m!)^3} 24^{-m} \equiv 0 \mod p.$$

See also conjecture A46 of [Sun11c]. The conjecture coincides with the congruence above if we reduce it modulo p.

We can now use theorem 4.9 to find

$$\begin{aligned} \sum_{m=0}^{p-1} \frac{(2m)!(3m)!}{(m!)^5} (-192)^{-m} &\equiv \left(\sum_{m=0}^{p-1} \frac{(3m)!}{(m!)^3} 24^{-m}\right)^2 && \mod p^2, \\ &\equiv 0 && \mod p^2, \end{aligned}$$

which holds for all odd primes $p \equiv -1 \mod 3$.

4.2.3 The case $t = 54^{-1}$

By substituting other values for the parameter t we find more congruences. Lets start with the curve $C_2(54^{-1})$, this curve has j-invariant 2×30^3 and after a change of variables it can be transformed into the elliptic curve $E_4 : y^2 = x^3 - 15x + 22$. By proposition 2.4 we find, for all primes $p > 3$

$$\left|C_2(54^{-1})(\mathbb{F}_p)\right| = \begin{cases} p + 1 & \text{if } p \equiv -1 \mod 3, \\ p + 1 - \left(\frac{x}{3}\right) 2x & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2 + 3y^2. \end{cases}$$

Combined with proposition 4.8 the following congruence now follows

$$\sum_{m=0}^{p-1} \frac{(3m)!}{(m!)^3} 54^{-m} \equiv \begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 3, \\ \left(\frac{x}{3}\right) 2x \mod p & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2 + 3y^2. \end{cases}$$

By theorem 4.9 we find another congruence namely

$$\sum_{m=0}^{p-1} \frac{(2m)!(3m)!}{(m!)^5} 108^{-m} \equiv \begin{cases} 0 \mod p^2 & \text{if } p \equiv -1 \mod 3, \\ 4x^2 \mod p & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2 + 3y^2. \end{cases}$$

This congruences proves the second case of the following conjecture and it confirms the first case modulo p.

Conjecture 4.10 ([Sun11c, A29])**.** *For any prime $p > 3$ we have*

$$\sum_{m=0}^{p-1} \frac{(2m)!(3m)!}{(m!)^5} 108^{-m} \equiv \begin{cases} 4x^2 - 2p \mod p^2 & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2 + 3y^2, \\ 0 \mod p^2 & \text{if } p \equiv -1 \mod 3. \end{cases}$$

Zhi-Wei Sun has already proven this conjecture in his paper [Sun12].

4.2.4 The case $\mathrm{t} = -216^{-1}$

Now consider the curve $C_2(-216^{-1})$, which has j-invariant -3×160^2. After a change of variables this curve transforms into the elliptic curve $E_8 : y^2 = x^3 - 480x + 4048$. But this means proposition 2.10 gives us

$$\left|C_2(-216^{-1})\left(\mathbb{F}_p\right)\right| = \begin{cases} p+1 & \text{if } p \equiv -1 \mod 3, \\ p + 1 + \left(\frac{x}{3}\right) x & \text{if } p \equiv 1 \mod 3 \text{ and } 4p = x^2 + 27y^2. \end{cases}$$

Combined with proposition 4.8 we now find the following congruence

$$\sum_{m=0}^{p-1} \frac{(3m)!}{(m!)^3} (-216)^{-m} \equiv \begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 3, \\ -\left(\frac{x}{3}\right) x \mod p & \text{if } p \equiv 1 \mod 3 \text{ and } 4p = x^2 + 27y^2. \end{cases}$$

See also conjecture A46 of [Sun11c].

Again we can apply theorem 4.9 to find the following congruence.

$$\sum_{m=0}^{p-1} \frac{(2m)!(3m)!}{(m!)^5} (-192)^{-m} \equiv \begin{cases} 0 \mod p^2 & \text{if } p \equiv -1 \mod 3, \\ x^2 \mod p & \text{if } p \equiv 1 \mod 3 \text{ and } 4p = x^2 + 27y^2. \end{cases}$$

This proves the second case of the following conjecture and it confirms the first case modulo p.

Conjecture 4.11 ([Sun11c, A8])**.** *For any prime $p > 3$ we have*

$$\sum_{m=0}^{p-1} \frac{(2m)!(3m)!}{(m!)^5} (-192)^{-m} \equiv \begin{cases} x^2 - 2p \mod p^2 & \text{if } p \equiv 1 \mod 3 \text{ and } 4p = x^2 + 27y^2, \\ 0 \mod p^2 & \text{if } p \equiv -1 \mod 3. \end{cases}$$

Another proof for the second case of this conjecture can be found in the paper [Sun11b] of Zhi-Hong Sun. Again we see that Zhi-Hong Sun uses a completely different approach.

4.2.5 The case $t = \left(4 + 10\sqrt{-2}\right)^{-1}$

As before we can also consider irrational t-values for which the curve $C_2(t)$ has complex multiplication. We will only consider t-values in a quadratic extension of $\mathbb{Q}$.

A short Weierstrass model for $C_2(t)$ is given by

$$C_2'(t) : y^2 = x^3 + (648t - 27)x + 11664t^2 - 1944 + 54.$$

An isogeny from $C_2(t)$ to $C_2'(t)$ is now given by

$$\phi : C_2(t) \longrightarrow C_2'(t), \qquad (x, y) \longmapsto (3 - 36x, 216y + +108x - 108t)\,.$$

Hence for all $t \in \mathbb{F}_p$ and for all primes $p > 3$, $|C_2(\mathbb{F}_p)| = |C_2'(\mathbb{F}_p)|$.

Suppose $p > 3$ is prime such that $\left(\frac{-2}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{-2}\right]$. Then the curve

$$C_2'\left(\left(4 + 10\sqrt{-2}\right)^{-1}\right)$$

can be reduced modulo $\boldsymbol{\lambda}_1$ and because

$$\mathbb{Z}(\sqrt{-2})/\boldsymbol{\lambda}_1 \cong \mathbb{F}_p$$

we obtain an elliptic curve over $\mathbb{F}_p$. Moreover it has j-invariant 20^3 and therefore complex multiplication by $\mathbb{Z}\left[\sqrt{-2}\right]$. The curve $C_2'\left(\left(4 + 10\sqrt{-2}\right)^{-1}\right)$ is obtained by twisting the curve $E_5 : y^2 = x^3 - 270x - 1512$ with

$$\sqrt{-\frac{1}{3} - \frac{1}{6}\sqrt{-2}} = \frac{1}{6}\sqrt{-12 - 6\sqrt{-2}}.$$

Therefore

$$\left|C_2\left(\left(4 + 10\sqrt{-2}\right)^{-1}\right)(\mathbb{F}_p)\right| - p + 1 = \left(\frac{-12 - 6\sqrt{-2}}{p}\right)(|E_5(\mathbb{F}_p)| - p + 1).$$

Together with proposition 4.8 and 2.7 this leads to the following congruence, which holds for all primes $p > 3$ such that $\left(\frac{-2}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{-2}\right]$,

$$\sum_{m=0}^{p-1} \frac{(3m)!}{(m!)^3}\left(4 + 10\sqrt{-2}\right)^{-m}$$

$$\equiv \begin{cases} \left(\dfrac{-12 - 6\sqrt{-2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1, 3 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 1 \mod 4, \\ \left(\dfrac{-12 - 6\sqrt{-2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 9, 11 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 3 \mod 4. \end{cases}$$

If we now apply theorem 4.9 we find the following congruence, for all primes $p > 3$ such that $\left(\frac{-2}{p}\right) = 1$,

$$\sum_{m=0}^{p-1} \frac{(2m)!(3m)!}{(m!)^5} 8^{-m} \equiv 4x^2 \mod p \qquad \text{where } p = x^2 + 2y^2.$$

4.2.6 The case $\mathrm{t} = \left(32 + 2\sqrt{6}\right)^{-1}$

The following congruences are obtained with the same techniques. For all primes $p > 5$ such that $\left(\frac{6}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{6}\right]$,

$$\sum_{m=0}^{p-1} \frac{(3m)!}{(m!)^3} \left(32 + 2\sqrt{6}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1,3 \mod 8, \\ \left(\dfrac{-4 - 6\sqrt{6}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1,3 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 1 \mod 4, \\ \left(\dfrac{-4 - 6\sqrt{6}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 9,11 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 3 \mod 4. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(2m)!(3m)!}{(m!)^5} \left(3704 - 1456\sqrt{6}\right)^{-m} \equiv \begin{cases} 0 \mod p^2 & \text{if } p \not\equiv 1,3 \mod 8, \\ 4x^2 \mod p & \text{if } p \equiv 1,3 \mod 8 \text{ and } p = x^2 + 2y^2. \end{cases}$$

The last congruence holds modulo $\boldsymbol{\lambda}_1$ according to theorem 4.9. However this congruence also holds modulo $\boldsymbol{\lambda}_2$ in an analogous way and therefore it holds modulo p.

4.2.7 The case $\mathrm{t} = \left(32 + 8\sqrt{-11}\right)^{-1}$

The following congruences hold for all primes $p > 3$ such that $\left(\frac{-11}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$. Note that $\left(\frac{-11}{p}\right) = \left(\frac{p}{11}\right)$ for all odd primes p.

$$\sum_{m=0}^{p-1} \frac{(3m)!}{(m!)^3} \left(32 + 8\sqrt{-11}\right)^{-m}$$

$$\equiv -\left(\frac{726 + 66\sqrt{-11}}{\boldsymbol{\lambda}_1}\right) \left(\frac{x}{11}\right) x \mod \boldsymbol{\lambda}_1 \quad \text{if } \left(\frac{p}{11}\right) = 1 \text{ and } 4p = x^2 + 11y^2.$$

$$\sum_{m=0}^{p-1} \frac{(2m)!(3m)!}{(m!)^5} 64^{-m} \equiv x^2 \mod p \quad \text{if } \left(\frac{p}{11}\right) = 1 \text{ and } 4p = x^2 + 11y^2.$$

4.2.8 The case $\mathrm{t} = \left(4 - 4\sqrt{33}\right)^{-1}$

The following congruences hold for all primes $p > 3$ such that $\left(\frac{33}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\frac{1+\sqrt{33}}{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(3m)!}{(m!)^3} \left(4 - 4\sqrt{33}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } \left(\frac{p}{11}\right) = -1, \\ -\left(\frac{2+66\sqrt{33}}{\boldsymbol{\lambda}_1}\right)\left(\frac{x}{11}\right) x \mod \boldsymbol{\lambda}_1 & \text{if } \left(\frac{p}{11}\right) = 1 \text{ and } 4p = x^2 + 11y^2. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(2m)!(3m)!}{(m!)^5} \left(-16736 + 2912\sqrt{33}\right)^{-m} \equiv \begin{cases} 0 \mod p^2 & \text{if } \left(\frac{p}{11}\right) = -1, \\ x^2 \mod p & \text{if } \left(\frac{p}{11}\right) = 1 \text{ and } 4p = x^2 + 11y^2. \end{cases}$$

4.2.9 The case $\mathrm{t} = \left(18 + 6\sqrt{3}\right)^{-1}$

The elliptic curve

$$C_2'\left(\left(18 + 6\sqrt{3}\right)^{-1}\right)$$

can be reduced to an elliptic curve over $\mathbb{F}_p$ whenever $\left(\frac{3}{p}\right) = 1$. Moreover it has j-invariant 1728 and therefore complex multiplication by $\mathbb{Z}[i]$. Since this elliptic curve has j-invariant 1728 there exist higher order twists. Therefore the results in this case will follow if we apply the techniques of chapter 2. We find the following congruences for primes that are inert in the endomorphism ring. These congruences hold for all primes $p > 3$ such that $\left(\frac{3}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{3}\right]$.

$$\sum_{m=0}^{p-1} \frac{(3m)!}{(m!)^3} \left(18 + 6\sqrt{3}\right)^{-m} \equiv 0 \mod p \qquad \text{if } p \equiv -1 \mod 4.$$

$$\sum_{m=0}^{p-1} \frac{(2m)!(3m)!}{(m!)^5} \left(288 + 168\sqrt{3}\right)^{-m} \equiv 0 \mod p^2 \qquad \text{if } p \equiv -1 \mod 4.$$

4.3 The cubic curve $\mathrm{C_3(t) : y^2 + xy + x^3 + tx = 0}$

Proposition 4.12. *Let p be a prime and let $C_3(t) : y^2 + xy + x^3 + tx = 0$ be a cubic curve for some $t \in \mathbb{F}_p$. Then,*

$$|C_3(t)(\mathbb{F}_p)| \equiv -\sum_{m=1}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} t^m \mod p.$$

Proof. Let $V_3(t)$ be the variety given by the dehomogenized equation

$$f_t = 1 + x + y + tx^{-1}y^{-2} = 0.$$

Then for any prime p we have the following map

$$\varphi : V_3(t)(\mathbb{F}_p^\times) \to C_3(t)(\mathbb{F}_p^\times), \qquad (x, y) \mapsto (xy, xy^2).$$

This map is well defined, moreover it is a bijection with inverse

$$\varphi^{-1} : C_3(t)(\mathbb{F}_p^\times) \to V_3(t)(\mathbb{F}_p^\times), \qquad (x,y) \mapsto \left(\frac{y}{x}, \frac{x^2}{y}\right).$$

Hence $|V_3(t)(\mathbb{F}_p^\times)| = |C_3(t)(\mathbb{F}_p^\times)|$ for all primes p. Moreover we see that

$$|C_3(t)(\mathbb{F}_p^\times)| = |C_3(t)(\mathbb{F}_p))| - 3 - \left(\frac{-t}{p}\right),$$

since $\mathcal{O}, (0,0), (0,\sqrt{t}), (0,-\sqrt{t}) \in C_3(t)(\overline{\mathbb{F}_p})$ are the only points not defined over $\mathbb{F}_p^\times$. By theorem 4.1 we now have

$$|V_3(t)(\mathbb{F}_p^\times)| - |V_3(0)(\mathbb{F}_p^\times)| = \frac{1}{p-1}(1 + \sum_{m=1}^{p-2} P_3(m)\omega(t)^m),$$

where $P_3(m) := \frac{1}{p} g_{4m} g_{-2m} g_{-m}^2$. For $0 \le m < p-1$ we have

$$\begin{aligned} S_3(m) &:= s_p(4m) + s_p(-2m) + 2s_p(-m) \\ &= \frac{4m}{1-p} + \frac{-2m}{1-p} + 2\frac{-m}{1-p} - \left\lfloor \frac{4m}{1-p} \right\rfloor - \left\lfloor \frac{-2m}{1-p} \right\rfloor - 2\left\lfloor \frac{-m}{1-p} \right\rfloor \\ &= \left\lceil \frac{4m}{p-1} \right\rceil - \left\lfloor \frac{2m}{p-1} \right\rfloor \end{aligned}$$

Hence

$$S_3(m) = \begin{cases} 1, & \text{if } 0 < m \le \dfrac{p-1}{4}, \\ 2, & \text{if } \dfrac{p-1}{4} < m < \dfrac{p-1}{2}, \\ 1, & \text{if } m = \dfrac{p-1}{2}, \\ 2, & \text{if } \dfrac{p-1}{2} < m \le \dfrac{3(p-1)}{4}, \\ 3, & \text{if } \dfrac{3(p-1)}{4} < m < p-1. \end{cases}$$

It now follows that

$$P_3(m) \equiv \begin{cases} \dfrac{(4m)!}{(2m)!(m!)^2} & \mod p \text{ if } 0 < m \le \dfrac{p-1}{4}, \\ \dfrac{-1}{(m!)^2} & \mod p \text{ if } m = \dfrac{p-1}{2}, \\ 0 & \mod p \text{ otherwise.} \end{cases}$$

And we have already seen that

$$\left(\frac{p-1}{2}\right)!\left(\frac{p-1}{2}\right)! = -\left(\frac{-1}{p}\right).$$

Therefore it follows that

$$
\begin{aligned}
|C_3(t)(\mathbb{F}_p)| &= |V_3(t)(\mathbb{F}_p^\times)| + 3 + \left(\frac{-t}{p}\right) \\
&= \frac{1}{p-1}\left(1 + \sum_{m=1}^{p-2} P_3(m)\omega(t)^m\right) + p - 2 + 3 + \left(\frac{-t}{p}\right) \\
&\equiv -\sum_{m=1}^{\frac{p-1}{4}} \frac{(4m)!}{(2m)!(m!)^2} t^m - \left(\frac{-1}{p}\right) t^{\frac{p-1}{2}} + \left(\frac{-t}{p}\right) && \mod p \\
&\equiv -\sum_{m=1}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} t^m && \mod p.
\end{aligned}
$$

Where the last congruence follows since

$$\left(\frac{t}{p}\right) \equiv t^{\frac{p-1}{2}} \mod p,$$

and $\dfrac{(4m)!}{(2m)!(m!)^2} \equiv 0 \mod p$ for all $m > \dfrac{p-1}{4}$. □

Theorem 4.13. *Let p be an odd prime and let x be a variable. Then*

$$\left(\sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} x^m\right)^2 \equiv \sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} (x(1-64x))^m \mod p^2.$$

Proof. See theorem 2.4 of [Sun11b]. □

The cubic curve $C_3(t)$ has the following discriminant and j-invariant respectively

$$\triangle(C_3(t)) = -t^2(64t-1) \quad \text{and} \quad j(C_3(t)) = \frac{(48t-1)^3}{64t^3 - t^2}.$$

We thus see that $C_3(t)$ is singular for $t = 64^{-1}$.

There are also other rational values for the parameter t which will give us nice congruences. For

$$t \in \left\{\frac{1}{72}, \frac{1}{576}, \frac{1}{128}, \frac{1}{48}, \frac{1}{72}, -\frac{1}{196}, \frac{1}{63}, \frac{1}{4032}\right\},$$

the elliptic curve $C_3(t)$ has complex multiplication and the point counting formulas of chapter 2 can be used.

4.3.1 The case t = 64^{-1}

After a change of coordinates over $\mathbb{Q}$ we can transform $C_3(64^{-1})$ into the curve $C : y^2 = x^3 - 2x$, which is obtained as a quadratic twist of the curve $y^2 = x^3 + x$ with $\sqrt{-2}$. Therefore corollary 1.4 implies

$$\left|C_2\left(\frac{1}{64}\right)(\mathbb{F}_p)\right| = p + 1 - \left(\frac{-2}{p}\right),$$

for all primes $p > 3$. Combining this results with proposition 4.12 gives us the following congruence

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} 64^{-m} \equiv \left(\frac{-2}{p}\right) \mod p.$$

Mortenson actually proved that this congruence holds modulo p^2 in his paper [Mor03b]. Zhi-Wei Sun stated several conjectures related to this sum in [Sun11c].

4.3.2 The case $t = 72^{-1}$

The curve $C_3(72^{-1})$ has j-invariant 1728 and it has short Weierstrass model $E : y^2 = x^3 - 9x$. This is curve is obtained by twisting the curve $E_1 : y^2 = x^3 - x$ with $\sqrt{3}$. Therefore by proposition 2.1 it follows that

$$\left|C_3(72^{-1})(\mathbb{F}_p)\right| = \begin{cases} p+1 & \text{if } p \equiv -1 \mod 4, \\ p+1-\left(\frac{6}{p}\right)2x & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2+y^2, \text{with } x \equiv 1 \mod 4, \end{cases}$$

for all primes $p > 3$. Combined with proposition 4.12 we thus find the following congruence for all primes $p > 3$,

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} 72^{-m} \equiv \begin{cases} 0 & \mod p \text{ if } p \equiv -1 \mod 4, \\ \left(\frac{6}{p}\right)2x & \mod p \text{ if } p \equiv 1 \mod 4 \text{ and } p = x^2+y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

See also conjecture A47 of [Sun11c]. In this conjecture a congruence modulo p^2 is stated involving the above sum. This congruence confirms conjecture A47 modulo p.

By theorem 4.13 we now find another congruence namely

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} 648^{-m} \equiv \begin{cases} 0 & \mod p^2 \text{ if } p \equiv -1 \mod 4, \\ 4x^2 & \mod p \text{ if } p \equiv 1 \mod 4 \text{ and } p = x^2+y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

This congruence proves one case of the following conjecture stated by Zhi-Hong Sun in his paper [Sun11a].

Conjecture 4.14 ([Sun11a, 2.1])**.** *Let $p > 3$ be a prime. Then*

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} 648^{-m} \equiv \begin{cases} 4x^2 - 2p & \mod p^2 \text{ if } p \equiv 1 \mod 4 \text{ and } p = x^2+y^2 \text{ where } 2 \nmid x, \\ 0 & \mod p^2 \text{ if } p \equiv -1 \mod 4. \end{cases}$$

Zhi-Hong Sun later proved the second case of this conjecture in his paper [Sun11b].

4.3.3 The case $t = 576^{-1}$

The curve $C_3(576^{-1})$ has j-invariant 66^3 and it has short Weierstrass model $E : y^2 = x^3 - 396x + 3024$. This is curve is obtained by twisting the curve $E_2 : y^2 = x^3 - 11x - 14$ with $\sqrt{-6}$. Therefore by proposition 2.2 it follows that

$$\left|C_3(576^{-1})(\mathbb{F}_p)\right| = \begin{cases} p+1 & \text{if } p \equiv -1 \mod 4, \\ p+1-\left(\frac{3}{p}\right)2x & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2+y^2, \text{with } x \equiv 1 \mod 4, \end{cases}$$

for all primes odd primes p. Combined with proposition 4.12 we thus find the following congruence for all odd primes p,

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} 576^{-m} \equiv \begin{cases} 0 & \mod p \text{ if } p \equiv -1 \mod 4, \\ \left(\frac{3}{p}\right) 2x & \mod p \text{ if } p \equiv 1 \mod 4 \text{ and } p = x^2 + y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

4.3.4 The case $t = 128^{-1}$

The curve $C_3(128^{-1})$ has j-invariant 20^3 and it has short Weierstrass model $E : y^2 = x^3 - 270x + 1512$. This is curve is obtained by twisting the curve $E_5 : y^2 = x^3 - 270x - 1512$ with $\sqrt{-1}$. Therefore by proposition 2.7 it follows that

$$\left|C_3(128^{-1})(\mathbb{F}_p)\right| = \begin{cases} p+1 & \text{if } p \not\equiv 1,3 \mod 8, \\ p+1-\left(\frac{-1}{p}\right) 2x & \text{if } p \equiv 1,3 \mod 16 \text{ and } p = x^2 + 2y^2 \\ & \text{such that } x \equiv 1 \mod 4, \\ p+1-\left(\frac{-1}{p}\right) 2x & \text{if } p \equiv 9,11 \mod 16 \text{ and } p = x^2 + 2y^2 \\ & \text{such that } x \equiv 3 \mod 4, \end{cases}$$

for all primes $p > 3$. Combined with proposition 4.12 we thus find the following congruence for all primes $p > 3$,

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} 128^{-m} \equiv \begin{cases} 0 & \mod p \text{ if } p \not\equiv 1,3 \mod 8, \\ \left(\frac{-1}{p}\right) 2x & \mod p \text{ if } p \equiv 1,3 \mod 16 \text{ and } p = x^2 + 2y^2 \\ & \text{such that } x \equiv 1 \mod 4, \\ \left(\frac{-1}{p}\right) 2x & \mod p \text{ if } p \equiv 9,11 \mod 16 \text{ and } p = x^2 + 2y^2 \\ & \text{such that } x \equiv 3 \mod 4. \end{cases}$$

See also conjecture B16 of [Sun11c]. This conjecture is already confirmed and states a more general congruence than the one above.

By theorem 4.13 we now find another congruence namely

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} 256^{-m} \equiv \begin{cases} 0 & \mod p^2 \text{ if } p \not\equiv 1,3 \mod 8, \\ 4x^2 & \mod p \text{ if } p \equiv 1,3 \mod 8 \text{ and } p = x^2 + 2y^2. \end{cases}$$

This congruences proves one case of the following conjecture.

Conjecture 4.15 ([Sun11c, A29])**.** *Let $p > 3$ be a prime. Then*

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} 256^{-m} \equiv \begin{cases} 4x^2 - 2p & \mod p^2 \text{ if } \left(\frac{-2}{p}\right) = 1 \text{ and } p = x^2 + 2y^2, \\ 0 & \mod p^2 \text{ if } \left(\frac{-2}{p}\right) = -1, \text{i.e. if } p \equiv 5,7 \mod 8. \end{cases}$$

Zhi-Wei Sun has already proven this conjecture in his paper [Sun12].

4.3.5 The case $t = 48^{-1}$

The curve $C_3(48^{-1})$ has j-invariant 0 and it has short Weierstrass model $E : y^2 = x^3 - 27$. This is curve is obtained by twisting the curve $E_3 : y^2 = x^3 + 1$ with $\sqrt{-3}$. Therefore by proposition 2.3 it follows that

$$\left|C_3(48^{-1})(\mathbb{F}_p)\right| = \begin{cases} p+1 & \text{if } p \equiv -1 \mod 3, \\ p+1-\left(\frac{-3}{p}\right)\left(\frac{x}{3}\right)2x & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2+3y^2, \end{cases}$$

for all primes $p > 3$. Combined with proposition 4.12 we thus find the following congruence for all primes $p > 3$,

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} 48^{-m} \equiv \begin{cases} 0 & \mod p \text{ if } p \equiv -1 \mod 3, \\ \left(\frac{x}{3}\right)2x & \mod p \text{ if } p \equiv 1 \mod 3 \text{ and } p = x^2+3y^2, \end{cases}$$

where we have used the fact that

$$\left(\frac{-3}{p}\right) = 1 \quad \text{for all primes } p \equiv 1 \mod 3.$$

See also conjecture A48 of [Sun11c], here a more general congruence involving this sum is stated.

By theorem 4.13 we now find another congruence namely

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} (-144)^{-m} \equiv \begin{cases} 0 & \mod p^2 \text{ if } p \equiv -1 \mod 3, \\ 4x^2 & \mod p \text{ if } p \equiv 1 \mod 3 \text{ and } p = x^2+3y^2. \end{cases}$$

This congruence proves one case of the following conjecture.

Conjecture 4.16 ([Sun11a, 2.2])**.** *Let $p > 3$ be a prime. Then*

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} (-144)^{-m} \equiv \begin{cases} 4x^2 - 2p & \mod p^2 \text{ if } p \equiv 1 \mod 3 \text{ and } p = x^2+3y^2, \\ 0 & \mod p^2 \text{ if } p \equiv -1 \mod 3. \end{cases}$$

Zhi-Hong Sun stated this conjecture in his paper [Sun11a] and he later proved the second case of this conjecture in theorem 2.7 of his paper [Sun11b].

4.3.6 The case $t = -192^{-1}$

The curve $C_3(-192^{-1})$ has j-invariant 2×30^3 and it has short Weierstrass model $E : y^2 = x^3 - 5040x + 4752$. This is curve is obtained by twisting the curve $E_4 : y^2 = x^3 - 15x + 22$ with $\sqrt{6}$. Therefore by proposition 2.4 it follows that

$$\left|C_3(-192^{-1})(\mathbb{F}_p)\right| = \begin{cases} p+1 & \text{if } p \equiv -1 \mod 3, \\ p+1-\left(\frac{6}{p}\right)\left(\frac{x}{3}\right)2x & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2+3y^2, \end{cases}$$

for all primes $p > 3$. Combined with proposition 4.12 we thus find the following congruence for all primes $p > 3$,

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} (-192)^{-m} \equiv \begin{cases} 0 & \mod p \text{ if } p \equiv -1 \mod 3, \\ \left(\frac{6}{p}\right)\left(\frac{x}{3}\right)2x & \mod p \text{ if } p \equiv 1 \mod 3 \text{ and } p = x^2+3y^2. \end{cases}$$

This congruence is also treated in conjecture A48 of [Sun11c], where the similarity between the case $t = 48^{-1}$ and the case $t = -192^{-1}$ is noted.

4.3.7 The case $t = 63^{-1}$

The curve $C_3(63^{-1})$ has j-invariant -15^3 and it has short Weierstrass model $E : y^2 = x^3 - 315x - 2646$. This is curve is obtained by twisting the curve $E_6 : y^2 = x^3 - 35x - 98$ with $\sqrt{3}$. Therefore by proposition 2.8 it follows that

$$\left|C_3(63^{-1})(\mathbb{F}_p)\right| = \begin{cases} p+1 & \text{if } p \not\equiv 1,2,4 \mod 7, \\ p+1-\left(\frac{3}{p}\right)\left(\frac{x}{7}\right)2x & \text{if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2, \end{cases}$$

for all primes $p \neq 2, 7$. Combined with proposition 4.12 we thus find the following congruence for all primes $p \neq 2, 7$,

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} 63^{-m} \equiv \begin{cases} 0 & \mod p \text{ if } p \not\equiv 1,2,4 \mod 7, \\ \left(\frac{3}{p}\right)\left(\frac{x}{7}\right)2x & \mod p \text{ if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2. \end{cases}$$

See also conjecture A49 of [Sun11c]. By theorem 4.13 we now find another congruence namely

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} (-3969)^{-m} \equiv \begin{cases} 0 & \mod p^2 \text{ if } p \not\equiv 1,2,4 \mod 7, \\ 4x^2 & \mod p \text{ if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2. \end{cases}$$

This congruence proves one case of the following conjecture stated by Zhi-Hong Sun.

Conjecture 4.17 ([Sun11a, 2.3])**.** *Let $p > 3$ be a prime. Then*

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} (-3969)^{-m} \equiv \begin{cases} 4x^2 - 2p & \mod p^2 \text{ if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2, \\ 0 & \mod p^2 \text{ if } p \equiv 3,5,6 \mod 7. \end{cases}$$

Zhi-Hong Sun has proven the second case of this conjecture in his paper [Sun11b].

4.3.8 The case $t = -4032^{-1}$

The curve $C_3(-4032^{-1})$ has j-invariant 255^3 and it has short Weierstrass model $E : y^2 = x^3 - 1049580x + 413855568$. This is curve is obtained by twisting the curve $E_7 : y^2 = x^3 - 595x - 5586$ with $\sqrt{-42}$. Therefore by proposition 2.9 it follows that

$$\left|C_3(-4032^{-1})(\mathbb{F}_p)\right| = \begin{cases} p+1 & \text{if } p \not\equiv 1,2,4 \mod 7, \\ p+1-\left(\frac{-42}{p}\right)\left(\frac{x}{7}\right)2x & \text{if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2, \end{cases}$$

for all primes $p \neq 2, 7$. Combined with proposition 4.12 we thus find the following congruence for all primes $p \neq 2, 7$,

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} (-4032)^{-m} \equiv \begin{cases} 0 & \mod p \text{ if } p \not\equiv 1,2,4 \mod 7, \\ \left(\frac{-42}{p}\right)\left(\frac{x}{7}\right)2x & \mod p \text{ if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2+7y^2. \end{cases}$$

If we now use the fact that

$$\left(\frac{-7}{p}\right)=\left(\frac{p}{7}\right)=1 \quad \text{if} \quad p\equiv 1,2,4 \mod 7,$$

we see that the following congruence holds for all primes $p\neq 2,7$

$$\sum_{m=0}^{p-1}\frac{(4m)!}{(2m)!(m!)^2}(-4032)^{-m}\equiv\begin{cases}0 & \mod p \ \text{ if } p\not\equiv 1,2,4 \mod 7,\\ \left(\frac{6}{p}\right)\left(\frac{x}{7}\right)2x & \mod p \ \text{ if } p\equiv 1,2,4 \mod 7 \text{ and } p=x^2+7y^2.\end{cases}$$

4.3.9 The case $t=\left(-216-198\sqrt{2}\right)^{-1}$

As in the previous sections we can also find congruences for irrational t-values in a quadratic extension of $\mathbb{Q}$. The following congruences hold for all primes $p\neq 2,3,7$ such that $\left(\frac{2}{p}\right)=1$ and $(p)=\boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{2}\right]$.

$$\sum_{m=0}^{p-1}\frac{(4m)!}{(2m)!(m!)^2}\left(-216-198\sqrt{2}\right)^{-m}$$

$$\equiv\begin{cases}0 \mod p & \text{if } p\equiv -1 \mod 4,\\ \left(\frac{-42-84\sqrt{2}}{\boldsymbol{\lambda}_1}\right)2x \mod \boldsymbol{\lambda}_1 & \text{if } p\equiv 1 \mod 4 \text{ and } p=x^2+y^2, \text{with } x\equiv 1 \mod 4.\end{cases}$$

$$\sum_{m=0}^{p-1}\frac{(4m)!}{(m!)^4}\left(143208-101574\sqrt{2}\right)^{-m}$$

$$\equiv\begin{cases}0 \mod p^2 & \text{if } p\equiv -1 \mod 4,\\ 4x^2 \mod p & \text{if } p\equiv 1 \mod 4 \text{ and } p=x^2+y^2, \text{with } x\equiv 1 \mod 4.\end{cases}$$

4.3.10 The case $t=\left(168+60\sqrt{3}\right)^{-1}$

The following congruences hold for all primes $p\neq 2,3,11$ such that $\left(\frac{3}{p}\right)=1$ and $(p)=\boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{3}\right]$.

$$\sum_{m=0}^{p-1}\frac{(4m)!}{(2m)!(m!)^2}\left(168+60\sqrt{3}\right)^{-m}$$

$$\equiv\begin{cases}0 \mod p & \text{if } p\equiv -1 \mod 3,\\ -\left(\frac{33+66\sqrt{3}}{\boldsymbol{\lambda}_1}\right)\left(\frac{x}{3}\right)2x \mod \boldsymbol{\lambda}_1 & \text{if } p\equiv 1 \mod 3 \text{ and } p=x^2+3y^2.\end{cases}$$

$$\sum_{m=0}^{p-1}\frac{(4m)!}{(m!)^4}\left(26856-15300\sqrt{3}\right)^{-m}\equiv\begin{cases}0 \mod p^2 & \text{if } p\equiv -1 \mod 3,\\ 4x^2 \mod p & \text{if } p\equiv 1 \mod 3 \text{ and } p=x^2+3y^2.\end{cases}$$

4.3.11 The case $\mathrm{t} = \left(8 - 40\sqrt{2}\right)^{-1}$

The following congruences hold for all primes $p \neq 2, 3, 7$ such that $\left(\frac{2}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} \left(8 - 40\sqrt{2}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1, 3 \mod 8, \\ \left(\dfrac{-28 - 42\sqrt{2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1, 3 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 1 \mod 4, \\ \left(\dfrac{-28 - 42\sqrt{2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 9, 11 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 3 \mod 4. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} \left(3656 - 2600\sqrt{2}\right)^{-m} \equiv \begin{cases} 0 \mod p^2 & \text{if } p \not\equiv 1, 3 \mod 8, \\ 4x^2 \mod p & \text{if } p \equiv 1, 3 \mod 8 \text{ and } p = x^2 + 2y^2. \end{cases}$$

4.3.12 The case $\mathrm{t} = 2\left(81 + 45\sqrt{-7}\right)^{-1}$

The following congruences hold for all primes $p > 3$ such that $\left(\frac{-7}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} \left(\frac{81 + 45\sqrt{-7}}{2}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1, 2, 4 \mod 7, \\ \left(\dfrac{-147 - 21\sqrt{-7}}{\boldsymbol{\lambda}_1}\right) \left(\dfrac{x}{7}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1, 2, 4 \mod 7 \text{ and } p = x^2 + 7y^2. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} 81^{-m} \equiv \begin{cases} 0 \mod p^2 & \text{if } p \not\equiv 1, 2, 4 \mod 7, \\ 4x^2 \mod p & \text{if } p \equiv 1, 2, 4 \mod 7 \text{ and } p = x^2 + 7y^2. \end{cases}$$

4.3.13 The case $\mathrm{t} = \left(2088 + 765\sqrt{7}\right)^{-1}$

The following congruences hold for all primes $p \neq 2, 3, 19$ such that $\left(\frac{7}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{7}\right]$.

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} \left(2088 + 765\sqrt{7}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1,2,4 \mod 7, \\ \left(\dfrac{-931 - 1064\sqrt{7}}{\boldsymbol{\lambda}_1}\right)\left(\dfrac{x}{7}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2 + 7y^2. \end{cases}$$

$$\sum_{m=0}^{p-1} \frac{(4m)!}{(m!)^4} \left(8292456 - 3132675\sqrt{7}\right)^{-m} \equiv \begin{cases} 0 \mod p^2 & \text{if } p \not\equiv 1,2,4 \mod 7, \\ 4x^2 \mod p & \text{if } p \equiv 1,2,4 \mod 7 \text{ and } p = x^2 + 7y^2. \end{cases}$$

4.4 The cubic curve $\mathrm{C_4(t) : y^2 = x(x-1)(x-16t)}$

For the cubic curve $C_4(t) : y^2 = x(x-1)(x-16t)$ a different approach will suffice to find the cardinality of $C_4(t)(\mathbb{F}_p)$, at least modulo p. We do not need the theory of Gauss sums in this section, however we do need some other tools such as the following lemma.

Lemma 4.18. *Let p be an odd prime. Then*

$$\sum_{x=1}^{p-1} x^k = \begin{cases} 0 & \text{if } (p-1) \nmid k, \\ p-1 & \text{if } (p-1) \mid k. \end{cases}$$

Proof. Let's consider the polynomial

$$P(X) = X^{p-1} - 1 = (X-1)\sum_{l=0}^{p-2} X^l.$$

Then $P(x) \equiv 0 \mod p$ for all $x \in \mathbb{F}_p^\times$. Therefore

$$\sum_{l=0}^{p-2} x^l \equiv \begin{cases} 0 \mod p & \text{if } x \in \mathbb{F}_p^\times \setminus \{1\}, \\ p-1 \mod p & \text{if } x \equiv 1 \mod p. \end{cases}$$

Let now $y \in \mathbb{F}_p^\times$ and let g be a generator of the group $\mathbb{F}_p^\times$. Then $y = g^k$ for some $0 \le k \le p-2$, hence

$$\sum_{l=0}^{p-2} y^l = \sum_{l=0}^{p-2} (g^l)^k = \sum_{x=1}^{p-1} x^k \equiv \begin{cases} 0 \mod p & \text{if } g^k \in \mathbb{F}_p^\times \setminus \{1\}, \\ p-1 \mod p & \text{if } g^k \equiv 1 \mod p. \end{cases}$$

Since g is a generator of the group $\mathbb{F}_p^\times$ the lemma now follows. □

We are now ready to prove the following proposition.

Proposition 4.19. *Let p be an odd primes and let $C_4(t) : y^2 = x(x-1)(x-16t)$ be a cubic curve for some $t \in \mathbb{F}_p$. Then*

$$|C_4(t)(\mathbb{F}_p)| \equiv 1 - (-1)^{\frac{p-1}{2}} \sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} t^m \mod p.$$

Proof. We can count the number of points in $C_4(t)(\mathbb{F}_p)$ as follows

$$\begin{aligned}
|C_4(t)(\mathbb{F}_p)| &= 1 + \sum_{x\in\mathbb{F}_p} \left(\left(\frac{x(x-1)(x-16t)}{p} \right) + 1 \right) \\
&\equiv p + 1 + \sum_{x\in\mathbb{F}_p} (x(x-1)(x-16t))^{\frac{p-1}{2}} && \mod p, \\
&\equiv 1 + \sum_{x=1}^{p-1} (x(x-1)(x-16t))^{\frac{p-1}{2}} && \mod p.
\end{aligned}$$

Let now $P(x)$ be the polynomial of degree $\dfrac{3(p-1)}{2}$ given by

$$P(x) = (x(x-1)(x-16t))^{\frac{p-1}{2}} = \sum_{k=0}^{\frac{3(p-1)}{2}} a_k x^k.$$

By lemma 4.18 it now follows that

$$\begin{aligned}
|C_4(t)(\mathbb{F}_p)| &\equiv 1 + \sum_{x=1}^{p-1} P(x) && \mod p, \\
&\equiv 1 + (p-1)(a_{p-1} + a_0) && \mod p, \\
&\equiv 1 + (p-1)a_{p-1} && \mod p.
\end{aligned}$$

This means that we have to compute the coefficient a_{p-1} of $P(x)$. We have

$$P(x) = x^{\frac{p-1}{2}} \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} x^k (-1)^{\frac{p-1}{2}-k} \sum_{l=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{l} x^l (-16t)^{\frac{p-1}{2}-l}.$$

Therefore

$$\begin{aligned}
a_{p-1} &= \sum_{k+l=\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} \binom{\frac{p-1}{2}}{l} (-1)^{p-1-k-l} (16t)^{\frac{p-1}{2}-l} \\
&= (-1)^{\frac{p-1}{2}} \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k}^2 (16t)^k.
\end{aligned}$$

The binomial coefficient appearing above can be reduced modulo p as follows

$$\begin{aligned}
\binom{\frac{p-1}{2}}{k}(-4)^k &= \frac{\frac{p-1}{2}\frac{p-3}{2}\cdots\frac{p-2k+1}{2}}{k!}(-4)^k \\
&= \frac{(1-p)(3-p)\cdots(2k-1-p)}{k!}2^k \\
&\equiv \frac{(2k)!}{k!(2\cdot 4\cdot 6\cdots 2k)}2^k && \mod p, \\
&\equiv \frac{(2k)!}{k!k!} && \mod p.
\end{aligned}$$

Altogether we thus find

$$\begin{aligned} |C_4(t)(\mathbb{F}_p)| &\equiv 1 + (-1)^{\frac{p-1}{2}}(p-1)\sum_{k=0}^{\frac{p-1}{2}} \frac{(2k)!^2}{k!^4} t^k \qquad \mod p, \\ &\equiv 1 - (-1)^{\frac{p-1}{2}} \sum_{k=0}^{p-1} \frac{(2k)!^2}{k!^4} t^k \qquad \mod p. \end{aligned}$$

□

The discriminant and j-invariant of $C_4(t)$ are given by, respectively,

$$\triangle(C_4(t)) = 4096t^2(16t-1)^2 \quad \text{and} \quad j(C_4(t)) = \frac{(256t^2-16t+1)^3}{t^2(16t-1)^2}.$$

Hence the cubic curve $C_4(16^{-1})$ is singular. Moreover we can compute the values of t for which $C_4(t)$ is an elliptic curve with complex multiplication. For

$$t \in \left\{ \frac{1}{32}, -\frac{1}{16}, \frac{1}{8} \right\},$$

$C_4(t)$ is an elliptic curve with complex multiplication by $\mathbb{Z}[i]$. For other rational values of t, $C_4(t)$ will not be an elliptic curve with complex multiplication.

4.4.1 The case t $= 16^{-1}$

The curve $C_4(16^{-1}) : y^2 = x(x-1)^2$ is singular. Moreover we have the following change of coordinates

$$\phi : C_4(16^{-1}) \longrightarrow E : y^2 = x^2(x+1), \qquad (x,y) \longmapsto (x-1, y).$$

Therefore by corollary 1.4 $|C_4(16^{-1})| = p$ for all odd primes p. Combining this result with proposition 4.19 gives the following congruence

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} 16^{-m} \equiv (-1)^{\frac{p-1}{2}} \mod p,$$

for all odd primes p. See also conjecture $A33$ of [Sun11c] in which a more general congruence is stated.

4.4.2 The case t $= 8^{-1}$

The cubic curve $C_4(8^{-1})$ is an elliptic curve with j-invariant 1728. Moreover we have the following change of coordinates

$$\phi : C_4(16^{-1}) \longrightarrow E_1 : y^2 = x^3 - x, \qquad (x,y) \longmapsto (x-1, y).$$

Hence $|C_4(8^{-1})(\mathbb{F}_p)| = |E_1(\mathbb{F}_p)|$ for all primes p. By proposition 2.1 it now follows that for any odd prime p

$$|C_4(8^{-1})(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } p \equiv -1 \mod 4, \\ p+1-\left(\frac{2}{p}\right)2x & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2+y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

Combined with proposition 4.19 we find the following congruence after rearranging some terms

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} 8^{-m} \equiv \begin{cases} 0 & \mod p \text{ if } p \equiv -1 \mod 4, \\ \left(\frac{2}{p}\right) 2x & \mod p \text{ if } p \equiv 1 \mod 4 \text{ and } p = x^2 + y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

Here we have used the fact that $(-1)^{\frac{p-1}{2}} = 1$ for all primes $p \equiv 1 \mod 4$. See also conjecture $A35$ of [Sun11c].

4.4.3 The case $t = -16^{-1}$

The curve $C_4(-16^{-1})$ is given by $y^2 = x^3 - x$. Therefore we find, as in the previous example, the following congruence

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} (-16)^{-m} \equiv \begin{cases} 0 & \mod p \text{ if } p \equiv -1 \mod 4, \\ \left(\frac{2}{p}\right) 2x & \mod p \text{ if } p \equiv 1 \mod 4 \text{ and } p = x^2 + y^2, \text{with } x \equiv 1 \mod 4, \end{cases}$$

which holds for all odd primes p.

4.4.4 The case $t = 32^{-1}$

The curve $C_4(32^{-1}) : y^2 = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x$ is an elliptic curve with j-invariant 1728. Moreover we have the following change of coordinates

$$\phi : C_4(32^{-1}) \longrightarrow E : y^2 = x^3 - 4x, \qquad (x, y) \longmapsto (4x - 2, 8y).$$

Hence $|C_4(8^{-1})(\mathbb{F}_p)| = |E(\mathbb{F}_p)|$ for all odd primes p. But E is obtained from $E_1 : y^2 = x^3 - x$ by twisting with $\sqrt{2}$. Hence for all odd primes p

$$|C_4(8^{-1})(\mathbb{F}_p)| = |E(\mathbb{F}_p)| = \begin{cases} p + 1 & \text{if } p \equiv -1 \mod 4, \\ p + 1 - 2x & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2 + y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

Together with proposition 4.19 we find the following congruence for all odd primes p

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} (32)^{-m} \equiv \begin{cases} 0 & \mod p \text{ if } p \equiv -1 \mod 4, \\ 2x & \mod p \text{ if } p \equiv 1 \mod 4 \text{ and } p = x^2 + y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

4.4.5 The case $t = \left(8 - 6\sqrt{2}\right)^{-1}$

Again we can consider the cases were t lies in a quadratic extension of $\mathbb{Q}$. This will lead to several new congruences. The following congruence holds for all primes $p > 3$ such that $\left(\frac{2}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1 \boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(8 - 6\sqrt{2}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 4, \\ \left(\frac{6 + 4\sqrt{2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2 + y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

4.4.6 The case $\mathrm{t} = \left(-256 - 192\sqrt{2}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{2}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(-256 - 192\sqrt{2}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 4, \\ \left(\dfrac{-\sqrt{2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2 + y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

4.4.7 The case $\mathrm{t} = \left(272 + 192\sqrt{2}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{2}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(272 + 192\sqrt{2}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 4, \\ \left(\dfrac{-6 + 4\sqrt{2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1 \mod 4 \text{ and } p = x^2 + y^2, \text{with } x \equiv 1 \mod 4. \end{cases}$$

4.4.8 The case $\mathrm{t} = \left(-32 - 32\sqrt{2}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{2}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(-32 - 32\sqrt{2}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1, 3 \mod 8, \\ \left(\dfrac{-\sqrt{2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1, 3 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 1 \mod 4, \\ \left(\dfrac{-\sqrt{2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 9, 11 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 3 \mod 4. \end{cases}$$

4.4.9 The case $\mathrm{t} = \left(8 - 8\sqrt{2}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{2}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(8 - 8\sqrt{2}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1,3 \mod 8, \\ \left(\dfrac{4+2\sqrt{2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1,3 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 1 \mod 4, \\ \left(\dfrac{4+2\sqrt{2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 9,11 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 3 \mod 4. \end{cases}$$

4.4.10 The case $\mathrm{t} = \left(48 + 32\sqrt{2}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{2}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(48 + 32\sqrt{2}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1,3 \mod 8, \\ \left(\dfrac{-4+2\sqrt{2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1,3 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 1 \mod 4, \\ \left(\dfrac{-4+2\sqrt{2}}{\boldsymbol{\lambda}_1}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 9,11 \mod 16 \text{ and } p = x^2 + 2y^2 \text{ such that } x \equiv 3 \mod 4. \end{cases}$$

4.4.11 The case $\mathrm{t} = \left(128 + 64\sqrt{3}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{3}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{3}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(128 + 64\sqrt{3}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 3, \\ \left(\dfrac{3\sqrt{3}}{\boldsymbol{\lambda}_1}\right)\left(\dfrac{x}{3}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2 + 3y^2. \end{cases}$$

4.4.12 The case $\mathrm{t} = \left(112 + 64\sqrt{3}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{3}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{3}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(112 + 64\sqrt{3}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 3, \\ \left(\dfrac{-9 - 6\sqrt{3}}{\boldsymbol{\lambda}_1}\right)\left(\dfrac{x}{3}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2 + 3y^2. \end{cases}$$

4.4.13 The case $\mathrm{t} = \left(8 + 4\sqrt{3}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{3}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{3}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(8 + 4\sqrt{3}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \equiv -1 \mod 3, \\ \left(\dfrac{9 - 4\sqrt{3}}{\boldsymbol{\lambda}_1}\right)\left(\dfrac{x}{3}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1 \mod 3 \text{ and } p = x^2 + 3y^2. \end{cases}$$

4.4.14 The case $\mathrm{t} = 2\left(31 + 3\sqrt{-7}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{-7}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(\frac{31 + 3\sqrt{-7}}{2}\right)^{-m} \equiv \left(\frac{21 - \sqrt{-7}}{\boldsymbol{\lambda}_1}\right)\left(\frac{x}{7}\right) 2x \mod \boldsymbol{\lambda}_1 \quad \text{where } p = x^2 + 7y^2.$$

4.4.15 The case $\mathrm{t} = 2\left(1 + 3\sqrt{-7}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{-7}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(\frac{1 + 3\sqrt{-7}}{2}\right)^{-m} \equiv \left(\frac{7\sqrt{-7}}{\boldsymbol{\lambda}_1}\right)\left(\frac{x}{7}\right) 2x \mod \boldsymbol{\lambda}_1 \quad \text{where } p = x^2 + 7y^2.$$

4.4.16 The case $\mathrm{t} = \left(8 + 24\sqrt{-7}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{-7}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(8 + 24\sqrt{-7}\right)^{-m} \equiv \left(\frac{-21 - \sqrt{-7}}{\boldsymbol{\lambda}_1}\right) \left(\frac{x}{7}\right) 2x \mod \boldsymbol{\lambda}_1 \quad \text{where } p = x^2 + 7y^2.$$

4.4.17 The case $\mathrm{t} = \left(8 + 3\sqrt{7}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{7}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{7}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(8 + 3\sqrt{7}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1, 2, 4 \mod 7, \\ \left(\dfrac{-147 + 56\sqrt{7}}{\boldsymbol{\lambda}_1}\right) \left(\dfrac{x}{7}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1, 2, 4 \mod 7 \text{ and } p = x^2 + 7y^2. \end{cases}$$

4.4.18 The case $\mathrm{t} = \left(2048 + 768\sqrt{7}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{7}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{7}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(2048 + 768\sqrt{7}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1, 2, 4 \mod 7, \\ \left(\dfrac{-7\sqrt{7}}{\boldsymbol{\lambda}_1}\right) \left(\dfrac{x}{7}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1, 2, 4 \mod 7 \text{ and } p = x^2 + 7y^2. \end{cases}$$

4.4.19 The case $\mathrm{t} = \left(-2032 + 768\sqrt{7}\right)^{-1}$

The following congruence holds for all primes $p > 3$ such that $\left(\frac{7}{p}\right) = 1$ and $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ in $\mathbb{Z}\left[\sqrt{7}\right]$.

$$\sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} \left(-2032 + 768\sqrt{7}\right)^{-m}$$

$$\equiv \begin{cases} 0 \mod p & \text{if } p \not\equiv 1, 2, 4 \mod 7, \\ \left(\dfrac{147 + 56\sqrt{7}}{\boldsymbol{\lambda}_1}\right) \left(\dfrac{x}{7}\right) 2x \mod \boldsymbol{\lambda}_1 & \text{if } p \equiv 1, 2, 4 \mod 7 \text{ and } p = x^2 + 7y^2. \end{cases}$$

Chapter 5

Conjectures

Super congruences are congruences modulo higher powers of primes. However the congruences in the previous chapter are mostly stated modulo the first power of a prime. For this final chapter we have computed some of the hypergeometric sums and verified whether these congruences hold modulo higher powers of these primes. By doing this we were able to state some conjectures concerning these sums. To be able to state these conjectures in some generality we will first establish some notation.

As in the previous chapter we define the following elliptic curves:

$$\begin{aligned} C_1(t): &\quad y^2 + xy + x^3 + t = 0, \\ C_2(t): &\quad y^2 + xy - ty + x^3 = 0, \\ C_3(t): &\quad y^2 + xy + x^3 + tx = 0, \\ C_4(t): &\quad y^2 = x(x-1)(x-16t). \end{aligned}$$

To all of these elliptic curves there is a hypergeometric sum related by propositions 4.3,4.8,4.12 and 4.19. For these sums we use the following notation:

$$\begin{aligned} S_1(t) &= \sum_{m=0}^{p-1} \frac{(6m)!}{(3m)!(2m)!m!} t^m, \\ S_2(t) &= \sum_{m=0}^{p-1} \frac{(3m)!}{(m!)^3} t^m, \\ S_3(t) &= \sum_{m=0}^{p-1} \frac{(4m)!}{(2m)!(m!)^2} t^m, \\ S_4(t) &= \sum_{m=0}^{p-1} \frac{(2m)!^2}{m!^4} t^m. \end{aligned}$$

5.1 Rational t-values

First we start with investigating the rational t-values. In this case all sums are rational and we can consider the congruences modulo rational primes as we did in the previous chapter. Suppose $t \in \mathbb{Q}$ and $1 \leq i \leq 4$ such that $C_i(t)$ is an elliptic curve with complex multiplication by the quadratic imaginary field K.

The evaluation of different sums suggests the following conjecture.

Conjecture 5.1. *Let $t \in \mathbb{Q}$ and $1 \leq i \leq 4$ such that $C_i(t)$ is an elliptic curve with complex multiplication by the quadratic imaginary field K. Suppose that p is a rational prime that is inert in K, then*

$$S_i(t) \equiv 0 \mod p^2.$$

Now suppose that p splits in K, i.e. $p = \pi\overline{\pi}$ where the factorization is chosen as in chapters 2 and 4. Then by the previous chapter we find that

$$S_i(t) \equiv \pm(\pi + \overline{\pi}) \mod p.$$

The previous chapter describes the correct choice of sign. But this congruence implies that

$$S_i(t) \equiv \pm\overline{\pi} \mod \pi.$$

If we study this last congruences we see that a stronger result seems to hold. Namely we find evidence for the following conjecture to be true.

Conjecture 5.2. *Let $t \in \mathbb{Q}$ and $1 \leq i \leq 4$ such that $C_i(t)$ is an elliptic curve with complex multiplication by the quadratic imaginary field K. Suppose that p is a rational prime that splits in K, then*

$$S_i(t) \equiv \pm\overline{\pi} \mod \pi^2 \qquad \text{where } p = \pi\overline{\pi} \text{ in } K.$$

Notice that the super congruences in [Sun11c] concern the same kind of hypergeometric sums as the congruences above. However these sums are reduced modulo powers of rational primes. This leads to different kinds of conjectures, where an extra term is added in comparison to the congruences modulo p.

In [CVH91], Coster and Van Hamme describe advanced tools to solve super congruences for values of Legendre polynomials. In particular they prove the conjectures stated here for the primes p that split in the endomorphism ring in the case that $i = 4$. This article also inspired us to look at these kind of congruences for the other cases resulting in some conjectures.

5.2 Quadratic t-values

We can use the same approach for irrational t-values. As in the previous chapter we start with $t \in L$, where L is some quadratic field extension of $\mathbb{Q}$. So let $t \in L \setminus \mathbb{Q}$ such that $C_i(t)$ has complex multiplication given by the quadratic imaginary field K. As in the previous chapter the elliptic curve $C_i(t)$ must have a twist that is defined over $\mathbb{Q}$ to be able to use the formulas of chapter 2. This condition is equivalent to the condition that K has class number 1 or to the condition that

$$j\left(C_i(t)\right) \in \left\{1728, 66^3, 0, 2 \cdot 30^3, 20^3, -15^3, 255^3, -3 \cdot 160^3, -32^3, -96^3, -960^3, -5280^3, -640320^3\right\}.$$

First suppose that p is a rational prime that splits in L, but is inert in K. Then $(p) = \boldsymbol{\lambda}_1\boldsymbol{\lambda}_2$ for some ideals $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \mathcal{O}_L$, where $\mathcal{O}_L$ is the ring of integers of L. By the previous chapter we then find

$$S_i(t) \equiv 0 \mod p.$$

This congruence does not hold modulo p^2 in general, which was the case for rational t-values.

Now suppose that p splits in K as well, i.e. $p = \pi\overline{\pi}$, where the factorization is chosen as in chapters 2 and 4. We are now working in two different quadratic extension of $\mathbb{Q}$ namely K and L both lying in the composite field LK. If we disregard the exceptional case that $K = L$, we see that the field LK is a quartic extension $\mathbb{Q}$. In this field p splits as $(p) = \boldsymbol{\mu}_1\boldsymbol{\mu}_2\boldsymbol{\mu_3}\boldsymbol{\mu}_4$ for some ideals $\boldsymbol{\mu}_i \subset \mathcal{O}_{LK}$. We choose $\boldsymbol{\mu}_i$ such that $\boldsymbol{\mu}_1\boldsymbol{\mu}_2 = (\pi)$ and $\boldsymbol{\mu}_1\boldsymbol{\mu}_3 = \boldsymbol{\lambda}_1$. The previous chapter now shows that the following congruence holds for all i,

$$S_i(t) \equiv \pm(\pi + \overline{\pi}) \mod \boldsymbol{\lambda}_1.$$

In its turn this congruence implies the following

$$S_i(t) \equiv \pm\overline{\pi} \mod \boldsymbol{\mu}_1.$$

We can numerically study this last congruence by computing the sum $S_i(t)$ for different t-values and for different primes p. When we do this a stronger results seems to be true.

Conjecture 5.3. *Let $t \in L$, where L is a quadratic extension of $\mathbb{Q}$, and let $1 \leq i \leq 4$ such that $C_i(t)$ is an elliptic curve with complex multiplication by the quadratic imaginary field K with class number 1. Suppose that $K \neq L$ and that p is a rational prime that splits in both K and L. Then $(p) = \boldsymbol{\mu}_1\boldsymbol{\mu}_2\boldsymbol{\mu_3}\boldsymbol{\mu}_4$ where we choose the factorization as above. Moreover*

$$S_i(t) \equiv \pm\overline{\pi} \mod \boldsymbol{\mu}_1^2.$$

If we now consider the case that $K = L$ we find a somewhat simpler result.

Conjecture 5.4. *Let $t \in L$ and let $1 \leq i \leq 4$ such that $C_i(t)$ is an elliptic curve with complex multiplication by the quadratic imaginary field K with class number 1. Suppose that $K = L$ and that p is a rational prime that splits in K, i.e. $p = \pi\overline{\pi}$. Then*

$$S_i(t) \equiv \pm\overline{\pi} \mod \pi^2.$$

5.3 Other extensions of $\mathbb{Q}$

Thus far we have only considered t-values in quadratic extensions of $\mathbb{Q}$. There are however other t-values for which the elliptic curves above have complex multiplication. For these t-values we can apply the same methods as before. So let $t \in \overline{\mathbb{Q}}$ such that the elliptic curve $C_i(t)$ has complex multiplication by the quadratic imaginary field K with class number 1. Now suppose that p is a rational prime such that there exists a prime ideal $\boldsymbol{\lambda} \subset \mathbb{Q}(t)$ above p with ideal norm $N(\boldsymbol{\lambda}) = p$. This implies that $\mathbb{Q}(t)/\boldsymbol{\lambda} \cong \mathbb{F}_p$ and that we can embed $\mathbb{Q}(t)$ into the p-adic numbers $\mathbf{Q}_p$. If now p is inert in K we find

$$S_i(t) \equiv 0 \mod \boldsymbol{\lambda},$$

which can be proven with the techniques of the previous chapter.

Now suppose that p splits in K, i.e. $p = \pi\overline{\pi}$ for some $\pi \in K$. Then we can prove that

$$S_i(t) \equiv \pm(\pi + \overline{\pi}) \mod \boldsymbol{\lambda}.$$

Moreover there exists a prime ideal $\boldsymbol{\mu} \subset LK$ lying above the ideals (π) and $\boldsymbol{\lambda}$. From this the following congruence follows

$$S_i(t) \equiv \pm\overline{\pi} \mod \boldsymbol{\mu}.$$

Again we computed the sum $S_i(t)$ for different t-values and different primes p to find evidence for the following conjecture to be true.

Conjecture 5.5. *Let $t \in L$, where L is a finite field extension of $\mathbb{Q}$, and let $1 \leq i \leq 4$ such that $C_i(t)$ is an elliptic curve with complex multiplication by the quadratic imaginary field K with class number 1. Suppose that $K \not\subset L$ and that p is a rational prime that splits in K, i.e. $p = \pi\overline{\pi}$. Suppose moreover that $\boldsymbol{\lambda} \subset L$ is a prime ideal above p with ideal norm $N(\boldsymbol{\lambda}) = p$. Then there exists an ideal $\boldsymbol{\mu} \subset LK$ above (π) and $\boldsymbol{\lambda}$. Moreover*

$$S_i(t) \equiv \pm\overline{\pi} \mod \boldsymbol{\mu}^2.$$

We have thus found very general statements which seem to be true. This thesis provides the techniques to prove these congruences modulo the first power of the primes considered. For some reason these congruences hold modulo higher powers of these primes. To prove these conjectures we will need some extra tools which this thesis does not provide.

5.4 Primes inert in L

Let $t \in L \setminus \mathbb{Q}$ such that $C_i(t)$ has complex multiplication by the quadratic imaginary field K with class number 1. Thus far we have only considered primes p such that there exists an ideal $\boldsymbol{\lambda} \subset L$ of norm $N(\boldsymbol{\lambda}) = p$. In this case we were able to reduce the elliptic curve E to an elliptic curve over $\mathbb{F}_p$. One might wonder what happens when p is inert in L. When this happens we can not use any of the tools in this thesis. We can however compute the hypergeometric sums to find evidence for the following conjecture.

Conjecture 5.6. *Let $t \in L$, where L is a finite field extension of $\mathbb{Q}$, and let $1 \leq i \leq 4$ such that $C_i(t)$ is an elliptic curve with complex multiplication by the quadratic imaginary field K with class number 1. Suppose that p is a prime that is inert in both K and L. Then*

$$S_i(t) \equiv 0 \mod p.$$

Hence when a prime p is inert in both K and L we find a similar congruence. However when a prime p is inert in L but splits in K we do not find any congruences as we did in the case that p splits in L.

5.5 Other j-invariants

The cardinality formulas of chapter 2 rely on the fact that some twist of the CM-curve is defined over $\mathbb{Q}$. This assumption leaves only finitely many j-invariants to consider, since the class number of the CM-field K has to be 1. There are however other elliptic curves with complex multiplication that do not have a twist defined over $\mathbb{Q}$. The j-invariants of these elliptic curves are all algebraic. For these elliptic curves we can not find cardinality formulas as in chapter 2. We can however compute whether the same kind of congruences hold for these j-invariants. We find evidence, by computing these sums for different t-values and different primes, for the following conjecture to be true

Conjecture 5.7. *Let $t \in L$, where L is a finite field extension of $\mathbb{Q}$, and let $1 \leq i \leq 4$ such that $C_i(t)$ is an elliptic curve with complex multiplication by the quadratic imaginary field K. Suppose that p is a rational prime that is inert in K. Suppose moreover that $\boldsymbol{\lambda} \subset L$ is a prime ideal above p with ideal norm $N(\boldsymbol{\lambda}) = p$. Then*

$$S_i(t) \equiv 0 \mod \boldsymbol{\lambda}.$$

This conjecture is more general since it does not assume that K has class number 1. When K has class number 1 we found congruences in the case that p splits as well. These congruences depend on the factorization $p = \pi\overline{\pi}$ in K. If K has a different class number we may not expect to have such a factorization. We were therefore not able to find any congruences in this case.

Bibliography

[BH] I.A. Burhanuddin and M.D. Huang. On computing rational torsion on elliptic curves. http://www.cs.usc.edu/assets/002/82925.pdf.

[BSS00] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.

[Coh07] Henri Cohen. *Number theory. Vol. II. Analytic and modern tools*, volume 240 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[CVH91] M.J. Coster and L. Van Hamme. Supercongruences of atkin and swinnerton-dyer type for legendre polynomials. *J. Number Theory 38*, (3):256–286., 1991.

[DT02] W. Duke and Á. Tóth. The splitting of primes in division fields of elliptic curves. *Experiment. Math.*, 11(4):555–565 (2003), 2002.

[Kna92] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[Mor03a] Eric Mortenson. A supercongruence conjecture of Rodriguez-Villegas for a certain truncated hypergeometric function. *J. Number Theory*, 99(1):139–147, 2003.

[Mor03b] Eric Mortenson. Supercongruences between truncated ${}_2F_1$ hypergeometric functions and their Gaussian analogs. *Trans. Amer. Math. Soc.*, 355(3):987–1007 (electronic), 2003.

[Ono98] Ken Ono. Values of Gaussian hypergeometric series. *Trans. Amer. Math. Soc.*, 350(3):1205–1223, 1998.

[Rob00] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[RS10] K. Rubin and A. Silverberg. Choosing the correct elliptic curve in the CM method. *Math. Comp.*, 79(269):545–561, 2010.

[RV03] Fernando Rodriguez-Villegas. Hypergeometric families of Calabi-Yau manifolds. In *Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001)*, volume 38 of *Fields Inst. Commun.*, pages 223–231. Amer. Math. Soc., Providence, RI, 2003.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[ST92] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[Ste08] P. Stevenhagen. Elliptic curves. http://www.math.leidenuniv.nl/ rvl/elliptic/2011/ec.pdf, 2008.

[Ste12] P. Stevenhagen. Number rings. http://websites.math.leidenuniv.nl/algebra/ant.pdf, 2012.

[Sun11a] Zhi-Hong Sun. Congruences concerning Legendre polynomials. *Proc. Amer. Math. Soc.*, 139(6):1915–1929, 2011.

[Sun11b] Zhi-Hong Sun. Some supercongruences modulo p^2. http://arxiv.org/pdf/1101.1050.pdf, 2011.

[Sun11c] Zhi-Wei Sun. Open conjectures on congruences. http://arxiv.org/pdf/0911.5665.pdf, 2011.

[Sun12] Zhi-Wei Sun. On sums involving products of three binomial coefficients. *Acta Arith.*, 156(2):123–141, 2012.

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.