Arithmetic of elliptic curves and modular forms

Hossein Movasati

June 2, 2008

Contents

Chapter 0

Introduction

Modular forms and elliptic curves are firmly rooted in the fertil grounds of number theory. As a proof of the mentioned fact and as an introduction to the present text we mention the followings: For p prime, the Fermat last theorem ask for a non-trivial integer solution for the Diophantine equation

$$a^p + b^p + c^p = 0$$

For a hypothetical solution $(A, B, C) = (a^p, b^p, c^p)$ of the Fermat equation, Gerhart Frey considered the elliptic curve

$$E_{A,B,C} : y^2 = x(x - A)(x + B)$$

From this one construct a modular form $f_{A,B,C}$ and a Galois representation with certain properties and then one proves that such objects does not exist. During this passage one encounters the Modularity conjecture which claims that every elliptic curve over $\mathbb{Q}$ is modular. Roughly speaking this means that every elliptic curve over $\mathbb{Q}$ appears in the Jacobian of of a modular curve of level N. Another formulation of modularity property is by using L functions which generalizes the famous Riemann zeta function

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Riemann hypothesis claims that all the non-trivial zeros of ζ lies on $\Re(s) = \frac{1}{2}$ and it has strong consequences on the growth of prime number. For the L functions associated to elliptic curves one has the Birch-Swinnerton Dyer conjecture which predicts the rank of an elliptic curve to be the order of vanishing of the corresponding L-function at $s = 1$.

It is assumed that the reader has a basic knowledge in algebraic geometry of curves and complex analysis in one variable.

Chapter 1

Elliptic curves in Weierstrass form

Throughout the present text we work with a field k of arbitrary characteristic and not necessarily algebraically closed. By $\bar{k}$ we mean the algebraic closure of k. The main examples that we have in mind are

$$\mathsf{k} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p := \frac{\mathbb{Z}}{\mathbb{Z}/p\mathbb{Z}}$$

a number field and function field. A number field k is a field that contains $\mathbb{Q}$ and has finite dimension, when considered as a vector space over $\mathbb{Q}$. A function field $\mathsf{k}(t_1, t_2, \ldots, t_s)$ over a field k is the field of rational functions $\frac{a(t_1,t_2,\cdots,t_s)}{b(t_1,t_2,\ldots,t_s)}$, where a and b are polynomials in indeterminates $t_1, t_2, \ldots, t_s$ and with coefficients in $t_1, t_2, \ldots, t_s$. Later, we will also use the field of p-adic numbers.

1.1 Curves

Let k be a field and $\mathsf{k}[x, y]$ be the space of polynomial in two variables x, y and with coefficients in k. The n dimensional affine space over k is by definition

$$\mathbb{A}^n(\mathsf{k}) = \mathsf{k} \times \mathsf{k} \times \cdots \times \mathsf{k}, \ n \text{ times}$$

and the projective n dimensional space is

$$\mathbb{P}^n(\mathsf{k}) := \mathbb{A}^{n+1}(\mathsf{k}) - \{(0, 0, \cdots, 0)\}/\sim$$

$$a \sim b \text{ if and only if } \exists \lambda \in \mathsf{k}, a = \lambda b$$

We will consider the following inclusion

$$\mathbb{A}^n(\mathsf{k}) \to \mathbb{P}^n(\mathsf{k}), \ (x_1, x_2, \cdots, x_n) \mapsto [x_1; x_2; \cdots; x_n; 1]$$

and call $\mathbb{P}^n$ the compactification of $\mathbb{A}^n$. The projective space at infinity is defined to be

$$\mathbb{P}^{n-1}_\infty(\mathsf{k}) = \mathbb{P}^n(\mathsf{k}) - \mathbb{A}^n(\mathsf{k}) = \{[x_1; x_2; \cdots; x_n; x_{n+1}] \mid x_{n+1} = 0\}.$$

For simplicity, in the case $n = 1, 2$ and 3 we use x, (x, y) and (x, y, z) instead of $x_1, x_2, \ldots$.

Any polynomial $f \in \mathsf{k}[x, y]$ defines an affine curve

$$C(\mathsf{k}) := \{(x, y) \in \mathsf{k}^2 \mid f(x, y) = 0\}.$$

The most famous Diophantine curve is give by $f = x^n + y^n - 1$. We denote it by F_n.

Remark 1.1. The set $C(\mathsf{k})$ may be empty, for instance take $\mathsf{k} = \mathbb{Q},\ f = x^2 + y^2 + 1$. This means that the identification of a curve with its points in some field is not a good treatment of curves. One of the starting points of the theory of schemes is this simple observation.

For $f \in \mathsf{k}[x, y]$ we define the homogenization of f

$$F(x, y, z) = z^d f(\frac{x}{z}, \frac{y}{z}),\ d := \deg(f).$$

F defines a projective plane curve in $\mathbb{P}^2(\mathsf{k})$:

$$\bar{C}(\mathsf{k}) := \{[x; y; z] \in \mathbb{P}^2(\mathsf{k}) \mid F(x, y, z) = 0\}.$$

Note that

$$\forall c \in \mathsf{k}, (x, y, z) \in \mathsf{k}^3,\ F(cx, cy, cz) = c^d F(x, y, z).$$

One has the injection

$$C(\mathsf{k}) \to \bar{C}(\mathsf{k}),\ (x, y) \mapsto [x; y; 1]$$

and for this reason one sometimes says that $\bar{C}(\mathsf{k})$ is the compactification of $C(\mathsf{k})$. Let g be the las homogeneous piece of the polynomial f. By definition it is a homogeneous polynomial of degree d. The points in

$$\bar{C}(\mathsf{k}) - C(\mathsf{k}) = \{[x; y] \in \mathbb{P}^1_\infty \mid g(x, y) = 0\}$$

are called the points at infinity of $C(\mathsf{k})$. The set of points at infinity of $\bar{F}_n$ is empty if n is even and it is $\{[1; -1]\}$ if n is odd.

Remark 1.2. From now on we use the notation C or $\{f = 0\}$ instead of $C(\mathsf{k})$. We are also going to use the notion of an arbitrary curve over k form algebraic geometry of schemes. Roughly speaking, a curve C over k means C over $\bar{k}$ and the ingredient polynomials of C are defined over k. The reader who is not familiar with those general objects may follow the text for affine and projective curves as above. The set $C(\mathsf{k})$ is now the set of k-rational points of C.

Definition 1.1. We say that an affine curve C is singular if there is a point $(a, b) \in \bar{\mathsf{k}}^2$ such that

$$f(a, b) = f_x(a, b) = f_y(a, b) = 0.$$

where f_x is the derivation of f with respect to x and so on. Using other charts of $\mathbb{P}^2$ one can define a singular point of a projective curve.

Exercise 1.1. Give an algorithm with the input $f \in \mathsf{k}[x, y]$ and the output Δ which is a polynomial in the coefficients of f such that

$$\{f = 0\} \text{ is singular } \Leftrightarrow \Delta = 0.$$

Let C be a smooth projective curve of degree d in $\mathbb{P}^2$, i.e. its defining polynomial is of degree d. Its genus is by definition

$$g(C) := \frac{(d-1)(d-2)}{2}$$

The main objective of the Diophantine theory is to describe the set $C(\mathbb{Q})$ for the curves defined over $\mathbb{Q}$. The most famous example is the Fermat curve given by the polynomial $f = x^n + y^n - 1$. The machinery of algebraic geometry is very useful to distinguish between various types of Diophantine equations. For instance, one can describe the rational points of genus zero curves. Genus one curves are called elliptic curves and the study of their rational points is the objective of the present text. For higher genus we have a conjecture of Mordell around 1922 which is proved by Faltings in 1982:

A non-singular projective curve of genus> 1 and defined over $\mathbb{Q}$ has only finitely many $\mathbb{Q}$-rational points.

In fact, the above theorem is true even for number fields. For instance the above theorem says that the Fermat curve F_n has a finite number of $\mathbb{Q}$-rational points. However, it does not say something about the nature of $F_n(\mathbb{Q})$. Mordell's conjecture for function fields was proved by Y. Manin in 1963, see [12] .

Exercise 1.2. Collect information on rational points of quadratic polynomials of degree two and in two variables.

1.2 Elliptic curves

We are ready to give the definition of an elliptic curve:

Definition 1.2. An elliptic curve over k is a pair (E, p), where E is a genus one complete smooth curve and p is p is a k-rational point of E.

Therefore, by definition an elliptic curve over k has at least a k-rational point. A smooth projective curve of degree 3 is therefore an elliptic curve if it has a k-rational point. For instance, the Fermat curve

$$F_3 : x^3 + y^3 = z^3$$

is an elliptic curve over $\mathbb{Q}$. It has $\mathbb{Q}$-rational points $[0, 1, 1]$ and $[1, 0, 1]$. However

$$E : 3x^3 + 4y^3 + 5z^3 = 0$$

has not $\mathbb{Q}$-rational points and so it is not an elliptic curve defined over $\mathbb{Q}$. It is an interesting fact to mention that $E(\mathbb{Q}_p)$ for all prime p and $E(\mathbb{R})$ are not empty. This example is due to Selmer (see [3, 20]).

1.3 Elliptic curves in Weierstrass form

An elliptic curve in the Weierstrass form E is the affine curve given by the polynomial

$$E_{t_2,t_3} : y^2 - 4x^3 + t_2 x + t_3,\ t_2, t_3 \in \mathsf{k},$$
$$\Delta := t_2^3 - 27t_3^2 \neq 0,\ \mathrm{char}(\mathsf{k}) \neq 2, 3$$

In homogeneous coordinates it is written in the form

$$zy^2 - 4x^3 + t_2 xz^2 + t_3 z^3 = 0.$$

It has only one point at infinity, namely $[0; 1; 0]$, which is considered as the marked point in the definition of an elliptic curve. It is in fact a smooth point of $\bar{E}$ which is tangent to the projective line at infinity of order 3 and $[0; 1; 0]$ is the only intersection point of the line at infinity with $\bar{E}$. If $\mathrm{char}(\mathsf{k}) = 2, 3$ then the curve E_{t_2,t_3} is always singular and it can be easily shown that $\Delta = 0$ if and only if the corresponding curve is singular.

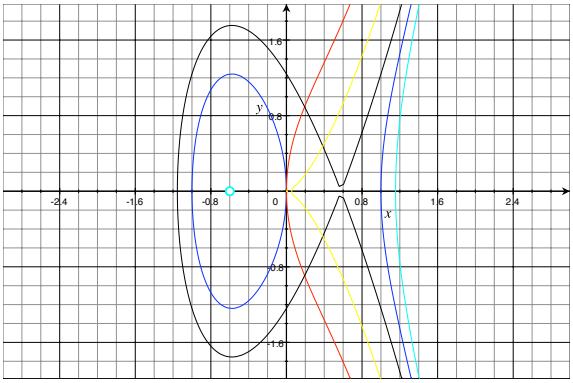

Figure 1.1: Elliptic curves: $y^2 - 4x^3 + t_2x + t_3 = 0$

1.4 Real geometry of elliptic curves

For a projective smooth curve C defined over $\mathbb{R}$ the set $C(\mathbb{R})$ has many connected components, all of them topologically isomorphic to a circle. We call each of them an oval.

For an elliptic curve E defined over $\mathbb{R}$ we want to analyze the topology of $E(\mathbb{R})$. For simplicity (in fact because of Proposition 1.2 which will be presented later) we assume that $E = E_{t_2,t_3}$ is in the Weierstrass form. For $(t_2, t_3) \in \mathbb{R}^2$ let $\Delta = t_2^3 - 27t_3^2$ be the discriminant of the elliptic curve E. We have:

1. If $\Delta > 0$ then $E(\mathbb{R})$ has two connected components, one is a closed path in $\mathbb{R}^2$, which we call it an affine oval, and the other a closed path in $\mathbb{P}^2(\mathbb{R})$. We call it a projective oval.

2. If $\Delta < 0$ then $E(\mathbb{R})$ has only one component which is a projective oval.

3. If $\Delta = 0$ and $t_3 < 0$ then $E(\mathbb{R})$ is an α-shaped path in $\mathbb{R}^2$ (∞-shaped path in $\mathbb{P}^2(\mathbb{R})$). In this case, we say that E has a real nodal singularity.

4. If $\Delta = 0$ and $t_3 > 0$ then $E(\mathbb{R})$ is a union of a point and a projective oval. In this case, we say that E has a complex nodal singularity.

5. If $t_2 = t_3 = 0$ then $E(\mathbb{R})$ look likes a broken line in $\mathbb{R}^2$. In this case, we say that E has a cuspidal singularity.

Note that $E(\mathbb{R})$ intersects the line at infinity only at $[0; 1; 0]$. To see/prove all the topological statements above, it is enough to take an example in each class and draw the corresponding $E(\mathbb{R})$. Note that in the (t_2, t_3)-space each set defined by the above items is connected and the topology of $E(\mathbb{R})$ does not change in each item (see Figure 1.1 and 1.7, the correspondence between the values of t_2, t_3 and $E_{t_2,t_3}(\mathbb{R})$ are done by colours).

1.5 Complex geometry of elliptic curves

Let C be a smooth projective curve of genus g over a subfield k of $\mathbb{C}$. It can be shown that $C(\mathbb{C})$ is a compact (Riemann) surface with $g(C)$ wholes (a sphere with g handles).

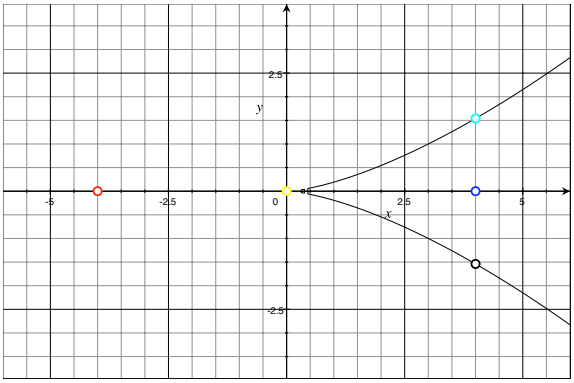

Figure 1.2: The curve $t_2^3 - 27t_3^2 = 0$ and points $(t_2, t_3) = (\pm 4, 0), (4, \pm\frac{8}{3\sqrt{3}})$

Exercise 1.3. Give a proof of the above statement using the followings. 2. Any compact Riemann surface is diffeomorphic to a sphere with some handles. 2. Riemann-Hurwitz formula.

In genus one case, therefore, the set $C(\mathbb{C})$ is torus.

Exercise 1.4. For a smooth elliptic curve E over $\mathbb{R}$ and in the Weierstrass form describe the real curves $E(\mathbb{R})$ inside the torus (Hint: Use the Riemann-Hurwitz formula).

1.6 Congruent numbers

A natural number n is said to be congruent if it is the area of a right triangle whose sides have rational length. In other words we are looking for the Diophantine equation:

$$C_n : x^2 + y^2 = z^2,\ n = \frac{1}{2}xy$$

in $\mathbb{Q}$, where x, y and z are the sides of the triangle. Consider the affine curve $C_n/\mathbb{Q}$ in $\mathbb{A}^3$ defined by the above equations. It intersects the projective space at infinity in 4 points:

$$[x; y; z; w] = [0; \pm 1; 1; 0],\ [\pm 1; 0; 1; 0].$$

Let

$$C : y^2 = x^4 - n^2,\ E_n : y^2 = x^3 - n^2 x.$$

We have morphisms

$$C_n \to C,\ (x, y, z) \mapsto (\frac{z}{2}, \frac{x^2 - y^2}{4})$$

and

$$C \to E_n,\ (x, y) \mapsto (x^2, xy)$$

defined over $\mathbb{Q}$.

Proposition 1.1. *A necessary and sufficient condition for the point $(x, y) \in E_n(\mathbb{Q})$ be in the image of $C_n(\mathbb{Q}) \to E_n(\mathbb{Q})$ is that*

1. *x to be a square and that*

2. its denominator be divisible by two

3. and its numerator has no common factor with n.

The proof is simple and is left to the reader (see [9]).

Exercise 1.5. Let $\bar{C}_n$ be the projectivization of C_n in $\mathbb{P}^3$. Is $\bar{C}_n$ smooth? If yes determine its genus.

Exercise 1.6. Ex. 1,2,3,4 of Koblitz, page 5.

1.7 The group law in elliptic curves

Let C be a smooth cubic curve in $\mathbb{P}^2$. Let also $P, Q \in C(\mathsf{k})$ and L be the line in $\mathbb{P}^2$ connecting two points P and Q. If $P = Q$ then L is the tangent line to C at P. The line L is defined over k and it is easy to verify that the third intersection $R := PQ$ of $C(\bar{k})$ with $L(\bar{k})$ is also in $C(\mathsf{k})$. Fix a point $O \in C(\mathsf{k})$ and call it the zero element of $C(\mathsf{k})$. Define

$$P + Q = O(PQ)$$

For instance, for an elliptic curve in the weierstrass form take $O = [0; 1; 0]$ the point at infinity. By definition $O + O = O$.

Theorem 1.1. *The above construction turns $C(\mathsf{k})$ into a commutative group.*

Proof. The only non-trivial piece of the proof is the associativity property of $+$:

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

The proof constitute of three pieces:

1. Let $P_i = [x_i; y_i; z_i]$ be 8 points in $\mathbb{P}^2(\bar{k})$ such that the vectors $(x_i^3, \cdots, z_i^3) \in \bar{\mathsf{k}}^{10}$of monomials of degree 3 in x_i, y_i, z_i are linearly independent. A cubic polynomial F passing through all P_i's corresponds to a vector $a \in \bar{\mathsf{k}}^{10}$ such that $P_i \cdot a = 0$ and so the space of such cubic polynomials is two dimensional. This means that there is two cubic polynomial F and G such that any other cubic polynomial passing through P_i's is of the form $\lambda F + \mu G$ and so it crosses a ninth point too.

2. We apply the first part to the eight points $O, P, Q, R, PQ, QR, P + Q, Q + R$ and conclude that $(P + Q)R = P(Q + R)$. Note that from these 8 points it crosses there cubic polynomials: C, the product of lines through $(0, PQ, P+Q)$, (R, Q, QR), $(P(Q+R), P, Q+R)$ and the product of the lines $(0, QR, Q + R)$, (PQ, Q, P), $(P + Q, R, (P + Q)R)$:

$$\begin{pmatrix} P+Q & PQ & O \\ R & Q & QR \\ (P+Q)R, P(Q+R) & P & Q+R \end{pmatrix}$$

(each column or row corresponds to aline).

3. The morphisms $C \times C \times C \to C, (P, Q, R) \mapsto (P + Q) + R, P + (Q + R)$ coincides in a Zariski open subset and so they are equal. □

Exercise 1.7. ([22] p. 60) On the elliptic curve

$$E : y^2 = x^3 + 17$$

over $\mathbb{Q}$. We have points

$$P_1 = (-2, 3),\ P_2 = (-1, 4),\ P_3 = (2, 5),\ P_4 = (4, 9),\ P_5 = (8, 23) P_6 = (43, 282)$$

$$P_7 = (52, 375),\ P_8 = (5234, 378661)$$

verify:

$$P_5 = 2P_1,\ P_4 = P_1 - P_3,\ 3P_1 - P_3 = P_7,$$

Prove that $E(\mathbb{Q})$ is freely generated by P_1 and P_3 and there are only 16 integral points $\pm P_i,\ i = 1, 2, \ldots, 8$ (see [19]).

Exercise 1.8. [9], p. 35, Problem 4b: For the elliptic curve $E_n : y^2 = x^3 - n^2 x$ find an explicit formula for the x coordinates of inflection points.

Exercise 1.9. [9], p. 36, Problem 7: How many elements of $E_n(\mathbb{R})$ or of order $2, 3$ and 4? Describe geometrically where these points are located.

Exercise 1.10. [9], p. 36, Problem 9: For an elliptic curve over $\mathbb{R}$ prove that $E(\mathbb{R})$ (as a group) is isomorphic to $\mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercise 1.11. [9], p. 36, Problem 11:

1.8 Weierstrass form revised

In this section we prove that any elliptic curve can be realized as a certain curve in $\mathbb{P}^2$. The following proposition is proved in [22], III, Proposition 3.1.

Proposition 1.2. *Let E be an elliptic curve over a field k. There exist functions $x, y \in \mathsf{k}(E)$ such that the map*

$$E \to \mathbb{P}^2,\ a \mapsto [x(a); y(a); 1]$$

give an isomorphism of E/k onto a curve given by

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,\ a_1, \cdots, \ldots, a_6 \in \mathsf{k}$$

sending O to $[0; 1; 0]$. If further $\mathrm{char}(\mathsf{k}) \neq 2, 3$ we can assume that the image curve is given by

$$y^2 = 4x^3 - t_2 x - t_3,\ t_2, t_3 \in \mathsf{k}, t_2^3 - 27t_3^2 \neq 0.$$

We call x and y the weierstrass coordinates of of E.

Proof. For a divisor D on a curve $C/\bar{k}$ define the linear system

$$\mathcal{L}(D) = \{f \in \bar{k}(C),\ f \neq 0 \mid div(f) + D \geq 0\} \cup \{0\}$$

and

$$l(D) = \dim_{\bar{k}}(\mathcal{L}(D)).$$

We know by Riemann-Roch theorem that

$$l(D) - l(K - D) = \deg(D) - g + 1,$$

where K is the canonical divisor of C. We have $\deg(K) = 2g-2$ and so for $\deg(D) > 2g-2$, equivalently $\deg(K - D) < 0$, we have

$$l(D) = \deg(D) - g + 1.$$

For $g = 1$ and $D = nO$ we get $l(D) = n$. For $n = 2$ we can choose $x, y \in \mathsf{k}(E)$ such that $1, x$ form a basis of $\mathcal{L}(2O)$ and $1, x, y$ form a basis of $\mathcal{L}(3O)$ (discuss the fact that we can choose x and y with coefficients in k). The function x (resp. y) has a pole of order 2 (resp. 3) at O. Now $\mathcal{L}(6O)$ has dimension 6 and $1, x, y, x^2, xy, y^2, x^3 \in \mathcal{L}(6O)$. It follows that there is a relation

$$ay^2 + a_1xy + a_3y = bx^3 + a_2x^2 + a_4x + a_6,\ a_1, \cdots, \ldots, a_6, a, b \in \mathsf{k}.$$

(discuss the fact that the coefficients are in k). Note that $ab \neq 0$, otherwise every term would have a different pole order at O and so all the coefficients would vanish. Multiplying x, y with some constants and dividing the whole equation with another constant, we get the desired equation. The map induced by x and y is the desired map (check the details).

If $\mathrm{char}(\mathsf{k}) \neq 2, 3$ we make the change of variables $x' = x, y' = y - \frac{a_3x}{2}$ and we eliminate xy term. A change of variables $x' = x - \frac{a_2}{3},\ y' = y - \frac{a_3}{2}$ will eliminate x^2 and y terms. In order to obtain the coefficient 4 of x^3 we replace y with $\frac{1}{2}y$.

□

Now we can state what is the moduli of elliptic curves.

Proposition 1.3. *Assume that* $\mathrm{char}(\mathsf{k}) \neq 2, 3$. *Two elliptic curves* E_{t_2,t_3} *and* $E_{t_2',t_3'}$ *are isomorphic if and only if there exists* $\lambda \in \mathsf{k},\ \lambda \neq 0$ *such that*

$$t_2' = \lambda^2 t_2,\ t_3' = \lambda^6 t_3$$

The isomorphism is given by

$$(x, y) \mapsto (\lambda^4 x, \lambda^3 y).$$

Proof. Let (x, y) and (x', y') be two sets of Weierstrass coordinate functions on an elliptic curve E_{t_2,t_3}. It follows that $\{1, x\}$ and $\{1, x'\}$ are both bases of $\mathcal{L}(2O)$, and similarly $\{1, x, y\}$ and $\{1, x', y'\}$ are both bases for $\mathcal{L}(3O)$. Writing x', y' in terms of x, y and substituting in the equation of $E_{t_2',t_3'}$ we get the first affirmation of the proposition. The second affirmation is easy to check.

□

Combining Proposition 1.2 and Proposition 1.3 we conclude that the moduli space of elliptic curves over a field of characteristic $\neq 2, 3$ is

$$\mathcal{M}_1(\mathsf{k}) := \left(\mathbb{A}^2(\mathsf{k}) - \{(t_2, t_3) \mid t_2^3 - 27t_3^2 = 0\}\right) / \sim$$

where

$$(t_2, t_3) \sim (t_2', t_3') \text{ if and only if } \exists \lambda \in \mathsf{k},\ \lambda \neq 0,\ (t_2', t_3') = (\lambda^4 t_2, \lambda^6 t_6).$$

If k is algebraically closed then this is the set of k-rational points of the weighted projective space $\mathbb{P}^{2,3}(\mathsf{k})$ mines a point induced in $\mathbb{P}^{2,3}$ by $\Delta = 0$. In this case the j-invariant of elliptic curves

$$j : \mathcal{M}_1(\mathsf{k}) \to \mathbb{A}(\mathsf{k}),\ j[t_2; t_3] = \frac{1728 t_2^3}{t_2^3 - 27 t_3^2}$$

is an isomorphism and so the moduli of elliptic curves over k is $\mathbb{A}^1(\mathsf{k})$. However, note that if k is not algebraically closed then j has non-trivial fibers. For instance, all the elliptic curves

$$y^2 = x^3 - t_3,\ t_3 \in \mathbb{Q}$$

are isomorphic over $\bar{\mathbb{Q}}$ but not over $\mathbb{Q}$.

If $j_0 \neq 0, 1728$ consider the elliptic curve:

$$E_{j_0} : y^2 + xy = x^3 - \frac{36}{j_0 - 1728} x - \frac{1}{j_0 - 1728}.$$

It satisfies $j(E) = j_0$.

Exercise 1.12. Write the following elliptic curves in the Weierstrass form:

$$y^2 = x^4 - 1,\ O = [0; 1; 0]$$

$$x^3 + y^3 = 1,\ O = [0; 1; 1]$$

1.9 Finite fields

A finite field, as its name indicates, is a field with finite cardinality. By definition of a field and finiteness property, the characteristic of a finite field is a prime number $p > 1$. Finite fields are completely classified as follows:

1. The order of a finite field of characteristic p is p^n for some $n \in \mathbb{N}$.
2. There is a unique (up to isomorphism of fields) finite field with $p^n,\ n \in \mathbb{N}$ elements.
3. For a prime number the finite field with cardinality p is simply the quotient
$$\mathbb{F}_p := \frac{\mathbb{Z}}{p\mathbb{Z}}.$$
4. For $q = p^n,\ n \in \mathbb{N}$ the finite field with cardinality p^n is denoted by $\mathbb{F}_q$. It is the spliting field of the polynomial $x^q - x$ over $\mathbb{F}_p$.
5. Every finite integral domain is a field and in particular
6. Let $f(T)$ be a monic irreducible polynomial of degree n in $\mathbb{F}_p[T]$. Then the quotient $\mathbb{F}_q[T]/\langle f \rangle$ is a finite field with p^n elements.
7. Let $f(x, y) \in \mathbb{F}_p[x, y]$ be a polynomial and I be a non zero prime ideal of $R := \mathbb{F}_p[x, y]/\langle f \rangle$. Then the quotient R/I is a finite field.

For more on finite fields the reader is referred to [6].

1.10 Elliptic curves over finite fields

In this section we want to analyze the torsion points of

$$E_n : y^2 = x^3 - n^2 x$$

By definition of the group structure of E_n we know that

$$O, (0,0), (0, \pm n)$$

are 2-torsions of E_n. Following the lines of [9] p. 44 Proposition 4, we want to prove:

Proposition 1.4. *We have*

$$E_n(\mathbb{Q})_{tors} = \{O, (0,0), (0, \pm n)\}$$

and so $\#E_n(\mathbb{Q})_{tors} = 4$.

Proof. Let us first give the strategy of the proof. Let $E/\mathbb{Q}$ be an a elliptic curve in the Weierstrass form and let $p > 2$ be a prime number which does not divide the discriminant of E. By a linear change of variable $(x, y) \mapsto (a^2 x, a^3 y)$ we can assume that the ingredient coefficients of E are in $\mathbb{Z}$. Let $\bar{E}/\mathbb{F}_p$ be the elliptic curve obtained from E by considering the coefficients of E modulo p. The main ingredient of the proof is the reduction map

$$E(\mathbb{Q}) \to \bar{E}(\mathbb{F}_p),$$

which is a group homomorphism. Note that by our assumption on p, $\bar{E}/\mathbb{F}_p$ is not singular. This is an injection of $E(\mathbb{Q})_{tors}$ inside $E(\mathbb{F}_p)$ for all but finitely many p and so for such primes $m := \#E(\mathbb{Q})_{tors}$ divides $\#E(\mathbb{F}_p)$. In fact, we have not yet proved that $E(\mathbb{Q})_{tors}$ is finite (a corollary of Mordell-Weil theorem). Therefore, we take a finite subgroup G of $\#E(\mathbb{Q})_{tors}$ and prove that the reduction map restricted to G is an injection and so $m := \#G$ divides $\#E(\mathbb{F}_p)$. From another side, we prove that for $E = E_n$:

$$\#E_n(\mathbb{F}_p) = p + 1, \ \forall p \text{ prime } p \equiv -1 \bmod 4 \tag{1.1}$$

Therefore, for all but finitely many primes $p \equiv -1 \bmod 4$ we have $p \equiv -1 \bmod m$. This implies that $m = 4$. Therefore, every finite subgroup of $E(\mathbb{Q})_{tors}$ is of order 4. Since all the elements of $E(\mathbb{Q})_{tors}$ are torsion, we conclude that $\#E_n(\mathbb{Q})_{tors} = 4$.

Now let us prove that the reduction map induces an injection in a finite subgroup G of $E(\mathbb{Q})_{tors}$. Two points $P = [x; y; z], Q = [x'; y'; z'] \in E(\mathbb{Q})$ are the same after reduction if and only if

$$xy' - x'y, xz' - x'z, yz' - y'z \tag{1.2}$$

are zero modulo p. For all pairs P, Q in G, the number of numbers (1.2) is finite and so there are finitely many primes dividing at least one of them. For all other primes p, we have the injection of G in $E(\mathbb{F}_p)$ by the reduction map. The proof of (1.1) is done in the next proposition. □

Proposition 1.5. *Let* $q = p^f, \ p \not| 2n$. *Suppose that* $q \equiv -1$ *mod* 4. *Then there are* $q + 1$ $\mathbb{F}_q$ *points on the elliptic curve* $E_n : y^2 = x^3 - n^2 x$.

Proof. Consider the map

$$f : \mathbb{F}_q \to \mathbb{F}_q,\ f(x) = x^3 - n^2 x$$

f is an odd function, i.e. $f(-x) = -f(x)$, and -1 is not in its image (this follows from the hypothesis on p). It follows that the index of the multiplicative group $\mathbb{F}_q^2 - \{0\}$ in $\mathbb{F}_q - \{0\}$ is two and so for all $x \in \mathbb{F}_q - \{0\}$ exactly one of x or $-x$ is square and so for all $x \in \mathbb{F}_q - \{0, n, -n\}$ exactly one of $f(x)$ or $f(-x)$ is square. Each such a pair $(x, y),\ y = f(x)$ gives us two points $(x, y),\ (x, -y) \in E_n(\mathbb{F}_q)$ and so in total we have $3 + 2\frac{q-1}{2}$ points in $E_n(\mathbb{F}_q)$. □

Proposition 1.6. *The natural number n is congruent if and only if $E_n(\mathbb{Q})$ has non-zero rank.*

Proof. If n is a congruent number then by Proposition 1.1, E_n has $\mathbb{Q}$-rational point with x-coordinate in $(\mathbb{Q}^+)^2$. The x coordinates of 2-torsion points in the affine chart x, y are $0, \pm n$. The fact that n is square free and Proposition 1.4 implies that such a rational point is of infinite order.

Conversely, suppose that P is a rational point of infinite order in E_n. Then by Exercise 1.13, the One can □

Exercise 1.13. ([9], p. 35, Ex. 2c) If P is a point not of order 2 in $E_n(\mathbb{Q})$, then the x-coordinate of $2P$ is a square of rational number having an even denominator. By Proposition 1.1, $2P$ comes from a point in $C_n(\mathbb{Q})$ and hence n is a congruent number.

Exercise 1.14. ([9], p. 49-50) Ex. 4,5,6, 7,9.

1.11 Mordell-Weil Theorem

We have seen that for an elliptic curve over $\mathbb{Q}$ the set $E(\mathbb{Q})$ is an abelian group and so

$$E(\mathbb{Q})/E(\mathbb{Q})_{tors}$$

where

$$E(\mathbb{Q})_{tors} := \{x \in E(\mathbb{Q}) \mid nx = 0, \quad \text{for some } n \in \mathbb{N}\},$$

is a freely generated $\mathbb{Z}$-module.

Theorem 1.2. *For an elliptic curve E over a number field k the group $E(\mathsf{k})$ of k-rational points is finitely generated abelian group.*

The above theorem for $\mathsf{k} = \mathbb{Q}$ was proved by Mordell. Its generalization for an arbitrary number field was proved by André Weil and it is known as the Mordell-Weil theorem. For the proof see [10, 5].

Let us take $\mathsf{k} = \mathbb{Q}$. The above theorem implies that the set of torsion points $E(\mathbb{Q})_{tors}$ of $E(\mathbb{Q})$ is finite and there is a number $r \in \mathbb{N}$ such that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}.$$

The non-negative integer r is called the rank of $E(\mathbb{Q})$.

1.12 Zeta functions of elliptic curves over finite fields

Let V be an affine or projective variety defined over $\mathbb{F}_q$. The zeta function of V is defined to be the formal power series in T:

$$Z(V,T) = \exp(\sum_{r=1}^{\infty} \frac{\#V(\mathbb{F}_{q^r})}{r} T^r)$$

Theorem 1.3. *Let E be an elliptic curve defined over $\mathbb{F}_p$. Then*

$$Z(E,T) = \frac{1 + 2a_E T + pT^2}{(1-T)(1-pT)}. \tag{1.3}$$

where a_E is an integer depending only on E. Moreover, the Riemann hypothesis holds for E, i.e. the only zeros of

$$\zeta(C,s) := Z(E, q^{-s})$$

are in the line $\Re(s) = \frac{1}{2}$.

Let

$$1 - 2a_E T + qT^2 = (1-\alpha T)(1-\beta T)$$

and so

$$\alpha + \beta = 2a_E,\ \alpha\beta = q \tag{1.4}$$

Note that α and β are algebraic integers:

$$\alpha, \beta = a_E \pm \sqrt{a_E^2 - q}.$$

We take the logarithmic derivative of both sides of (1.3) and one easily finds the equalities

$$\#E(\mathbb{F}_{p^r}) = p^r + 1 - \alpha^r - \beta^r,\ r = 1, 2, 3, \ldots$$

For $r = 1$ we obtain

$$\#E(\mathbb{F}_p) = p + 1 - 2a_E$$

We conclude that for elliptic curves over a finite field $\mathbb{F}_q$ the number of $\mathbb{F}_q$-rational points determine the number of $\mathbb{F}_{q^r}$-rational points.

Concerning the Riemann hypothesis, we note that it is equivalent to the inequality:

$$|\#E(\mathbb{F}_p) - p - 1| < 2\sqrt{p}. \tag{1.5}$$

The Riemann hypothesis holds if and only if $|\alpha| = |\beta| = p^{\frac{1}{2}}$. If these equalities happen then

$$|\#E(\mathbb{F}_p) - p - 1| = |2a_E| = |\alpha + \beta| < 2\sqrt{p}.$$

(the equality cannot occur because p is prime). Conversely, if (1.5) happens then $a_E^2 - p < 0$ and so the roots of the polynomial $1 - 2a_E T + qT^2$ are complex conjugate, $\beta = \bar{\alpha}$ and so $|\alpha| = |\beta| = p^{\frac{1}{2}}$.

The general reuslt as in (1.3) was conjectured by André Weil [25] and was proved by P. Deligne (see for instance [8] for an exposition of Deligne results).

Let us now state the result for the elliptic curve E_n related to the congruent numbers. The Legendre symbol is defined for integers a and positive odd primes p by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \text{ divides } a \\ 1 & \text{for some } x \in \mathbb{Z},\ a \equiv x^2 \bmod p \\ -1 & \text{otherwise} \end{cases}$$

Proposition 1.7. *In the zeta function of $E_n : y^2 = x^3 - n^2x$ defined over $\mathbb{F}_p$, p a prime $p \not| 2n$, we have:*

$$\alpha = \begin{cases} i\sqrt{p} & \text{if } p \equiv 3(\ mod\ 4) \text{ in this case } a_{E_n} = 0 \\ 2k + \left(\frac{n}{p}\right) + 2ki & \text{if } p \equiv 1(\ mod\ 4) \text{ in this case } a_{E_n} = 2k + \left(\frac{n}{p}\right) \end{cases}$$

In the second case k is determined by the fact that $\alpha\bar{\alpha} = p$

Exercise 1.15. ([16], Ex. 19.12) Let E be the elliptic curve

$$E : y^2 = x^3 - 4x^2 + 16$$

Consider also the formal power series given by

$$F(q) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + \cdots$$

1. Compute $N_p = \#E(\mathbb{F}_p)$ for all primes $3 \leq p \leq 13$.
2. Calculate the coefficient of M_n of q^n in $F(q)$ for $n \leq 13$.
3. Compute the sum $M_p + N_p$ for p prime $p \leq 13$.
4. Formulate a conjecture on the sum $M_p + n_p$. Can you prove it?.

1.13 Nagell-Lutz Theorem

In this section we state Nagell-Lutz theorem which gives a finite set of of possibilities for a torsion point of an elliptic curve.

Theorem 1.4. *(Nagell-Lutz Theorem) Let E be an elliptic curve with the Weierstrass equation:*

$$y^2 = x^3 + t_2x + t_3, \quad t_2, t_3 \in \mathbb{Z}, \Delta := 4t_2^3 + 27t_3^2 \neq 0.$$

Then for all non-zero torsion points $P = (a, b) \in E(\mathbb{Q})$ we have:

1. *The coordinates of P are in $\mathbb{Z}$, i.e. $a, b \in \mathbb{Z}$.*
2. *If P is of order greater than 2, then $b^2 \quad$ divides $\quad \Delta$.*
3. *If P is of order 2 then $b = 0$ and $a^3 + t_2a + t_3 = 0$.*

A proof can be found in [22], p. 221 or in [23] p.56.

Exercise 1.16. *[16], Exercise 8.11. For four of the following elliptic curves compute the torsion subgroup.*

$$y^2 = x^3 + 2, \ \cdots$$

See the reference above for the list of elliptic curves.

1.14 Mazur theorem

Theorem 1.5. *(Mazur, [13, 14]) Let E be an elliptic curve over $\mathbb{Q}$. Then the torsion subgroup $E(\mathbb{Q})_{tors}$ is one of the following fifteen groups:*

$$\mathbb{Z}/N\mathbb{Z},\ 1 \leq N \leq 10, \quad or\ N = 12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z},\ 1 \leq N \leq 4$$

Note that the above theorem implies that for an elliptic curve over $\mathbb{Q}$ we have always:

$$\#(E(\mathbb{Q})_{tors}) \leq 16.$$

It is natural to conjecture that: If E is an elliptic curve over a number field k, the order of the torsion subgroup of $E(\mathsf{k})$ is bounded by a constant which depends only on the degree of k over $\mathbb{Q}$. This is known uniform boundedness conjecture (UBC). It is proved by S. Kamienny in [7] for all quadratic fields and by L. Merel in [15] for all number fields.

For the proof of all the statements above one needs the notion of modular curves $X_0(N)$ and modular forms which will be introduced in the forthcoming chapters.

1.15 Riemann zeta function

In this section we are going to study the first of all Zeta function, namely Riemann zeta function:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Proposition 1.8. *The series $\zeta(s)$ converges for all $s \in \mathbb{C}$ with $\Re(s) > 1$ and*

$$\zeta(s) = \prod_{p} \frac{1}{(1 - p^{-s})}.$$

where p runs over all primes.

Proof. We have $|n^{-s}| = n^{\Re s}$ and so it is enough to prove the proposition for $s \in \mathbb{R}, s > 1$. We have

$$\sum_{n=2}^{\infty} \frac{1}{n^s} \leq \int_1^{\infty} x^{-s} = \frac{x^{-s+1}}{-s+1} \mid_1^{+\infty} = \frac{1}{s-1} \quad \text{if } s > 1$$

Again we assume that s is a real number bigger than 1. We have $p^{-s} < 1$ and so

$$(1 - p^{-s}) = \sum_{m=0}^{\infty} p^{-ms}.$$

By unique factorization theorem

$$\prod_{p \leq N} (1 - p^{-s})^{-1} = \sum_{n \leq N} n^{-s} + R_N(s).$$

Clearly

$$R_N(s) \leq \sum_{n=N+1}^{\infty} n^{-s}.$$

Since $\zeta(s)$ converges we have $R_N(s) \to 0$ as $N \to \infty$ and the result follows. □

There are many generalizations of the Riemann Zeta function. One of them is already used in §1.12. Bellow we explain how the zeta functions of a curve over a finite field is a generalization of the Riemann zeta function.

Consider a plane affine curve $C : f(x, y) = 0,\ f \in F_p(x, y)$ defined over the field $\mathbb{F}_p$. In analogy with the Riemann zeta function we define

$$\zeta(C, s) = \prod_{\mathfrak{p}} \frac{1}{(1 - (\mathbb{N}\mathfrak{p})^{-s})}. \tag{1.6}$$

where $\mathfrak{p}$ runs over all non-zero prime ideals of $\mathbb{F}_p[C] := \mathbb{F}_p[x, y]/\langle f(x, y)\rangle$. Here $\mathbb{N}\mathfrak{p}$ is the order of the quotient $\mathbb{F}_p[\mathbb{C}]/\mathfrak{p}$. Since such a quotient is a finite integral domain it is a field and hence it has p^n elements. We define $\deg(\mathfrak{p}) := n$. This allows us to redefine the zeta function as follows:

$$Z(C, T) = \prod_{\mathfrak{p}} \frac{1}{(1 - T^{\deg(\mathfrak{p})})}.$$

with $\zeta(C, s) = Z(C, p^{-s})$.

Proposition 1.9. *Let C be a curve ove the finite field $\mathbb{F}_p$. We have*

$$Z(C, T) = \exp(\sum_{r=1}^{\infty} \frac{\#C(\mathbb{F}_{p^r})}{r} T^r)$$

For a proof see [16] p. 90.

Exercise 1.17. Calculate the zeta functions of $\mathbb{A}^1$ and $\mathbb{P}^1$.

Exercise 1.18. Calculate the zeta function of degenerated elliptic curves:

$$y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 = 0.$$

1.16 Dedekind Zeta function

In this section we give a summary of Dedekind Zeta functions. Let k be anumber field and $\mathcal{O}_\mathsf{k}$ be its ring of integers.

Theorem 1.6. *The integer ring of a number field is a Dedekind domain, i.e every ideal $a \subset \mathcal{O}_\mathsf{k}$ in a unique way can be written*

$$\mathfrak{a} = \mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2} \cdots \mathfrak{p}_s^{\alpha_s},$$

where $\alpha_1, \ldots, \alpha_s \in \mathbb{N}_0$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are prime ideals.

A character χ on $\mathcal{O}_\mathsf{k}$ is a map from the set of non-zero ideals of $\mathcal{O}_\mathsf{k}$ to $\mathbb{C}$ such that it is multiplicative:

$$\chi(\mathfrak{a}_1\mathfrak{a}_2) = \chi(\mathfrak{a}_1)\chi(\mathfrak{a}_2).$$

We mainly use the Character $\chi \equiv 1$. Formally, the Dedekind Zeta function is defined in the following way:

$$\zeta_\mathsf{k}(s) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\mathbb{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})\mathbb{N}(\mathfrak{p})^{-s}},\ \mathbb{N}(\mathfrak{a}) = \#(\mathcal{O}_\mathsf{k}/\mathfrak{a}),$$

where the sum is running in non-zero ideals of $\mathcal{O}_\mathsf{k}$ and the product is running in the prime ideals of $\mathcal{O}_\mathsf{k}$.

Exercise 1.19. Discuss the convergence of the Dedekind Zeta function (put $\chi \equiv 1$).

Exercise 1.20. Discuss the fact that the integer ring of a number field is not necessarily a unique factorization domain/principal ideal domain. Give examples of irreducible but not prime elements. Hint $\mathbb{Q}(\sqrt{-5})$

$$2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

$$\langle 6\rangle = \langle 2, 1+\sqrt{-5}\rangle\langle 2, 1-\sqrt{-5}\rangle\langle 3, 1+\sqrt{-5}\rangle\langle 3, 1-\sqrt{-5}\rangle$$

Exercise 1.21. The ring of Gaussian integers is $\mathbb{Z}[i]$. Prove that the prime ideals of $\mathbb{Z}[i]$ are of two types:

$$\mathfrak{p} = \langle p\rangle, \quad \text{if} p \equiv 3(4), \ = \langle a+ib\rangle, \quad \text{if } a^2 = b^2 = p \equiv 1(4).$$

In the second case we say that p splits in $\mathbb{Z}[i]$. Show that the only units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$. Show also that the only ideal which ramifies is $\mathfrak{p} = \langle 1+i\rangle$, i.e. $\mathfrak{p}^2 = \langle p\rangle$.

1.17 Discriminant revised

Definition 1.3. Let us be given a polynomial $f \in \mathbb{Z}[t][x, y, \ldots]$, where $t = (t_1, t_2, \ldots, t_s)$ is a multi parameter and $(x, y, \ldots)$ a multi variable. The discriminant of f is an element $\Delta \in \mathbb{Z}[t]$ such that

$$\Delta = fa_1 + f_x a_2 + f_y a_3 + \cdots, \quad \text{for some } a_1, a_2, \ldots \in \mathbb{Z}[t][x, y, \ldots]$$

and no factor of Δ satisfy the mentioned property.

Exercise 1.22. The discriminant exists and is unique up to multiplication by $\pm$.

We have calculated the discriminant of

$$f = y^2 - x^3 - t_4 x - t_6 - t_2 x^2 + t_1 xy + t_3 y. \tag{1.7}$$

$$\begin{aligned}
\Delta = {} & (t_1^6 t_6 - t_1^5 t_3 t_4 + t_1^4 t_2 t_3^2 + 12 t_1^4 t_2 t_6 - t_1^4 t_4^2 - 8 t_1^3 t_2 t_3 t_4 - t_1^3 t_3^3 - 36 t_1^3 t_3 t_6 + 8 t_1^2 t_2^2 t_3^2 + 48 t_1^2 t_2^2 t_6 - 8 t_1^2 t_2 t_4^2 \\
& + 30 t_1^2 t_3^2 t_4 - 72 t_1^2 t_4 t_6 - 16 t_1 t_2^2 t_3 t_4 - 36 t_1 t_2 t_3^3 - 144 t_1 t_2 t_3 t_6 + 96 t_1 t_3 t_4^2 + 16 t_2^3 t_3^2 + 64 t_2^3 t_6 - 16 t_2^2 t_4^2 \\
& - 72 t_2 t_3^2 t_4 - 288 t_2 t_4 t_6 + 27 t_3^4 + 216 t_3^2 t_6 + 64 t_4^3 + 432 t_6^2).
\end{aligned}$$

$$\begin{aligned}
a_1 = {} & 432x^3 - 432y^2 + (-432t_1)xy + (432t_2)x^2 + (-432t_3)y + (432t_4)x + (-t_1^6 - 12t_1^4 t_2 + 36 t_1^3 t_3 - 48 t_1^2 t_2^2 \\
& + 72 t_1^2 t_4 + 144 t_1 t_2 t_3 - 64 t_2^3 + 288 t_2 t_4 - 216 t_3^2 - 432 t_6)
\end{aligned}$$

$$\begin{aligned}
a_2 = {} & -144x^4 + (-48t_1^2 - 192t_2)x^3 + (-t_1^4 - 8t_1^2 t_2 - 120 t_1 t_3 - 16 t_2^2 - 240 t_4)x^2 + (-t_1^5)y + (6t_1^4 t_2 - 20 t_1^3 t_3 + \\
& 24 t_1^2 t_2^2 - 40 t_1^2 t_4 - 80 t_1 t_2 t_3 + 32 t_2^3 - 160 t_2 t_4)x + (t_1^4 t_4 + 4 t_1^3 t_2 t_3 + 8 t_1^2 t_2 t_4 - 16 t_1^2 t_3^2 \\
& + 8 t_1 t_2^2 t_3 - 64 t_1 t_3 t_4 + 16 t_2^2 t_4 - 64 t_4^2).
\end{aligned}$$

$$\begin{aligned}
a_3 = {} & -432x^3 y + 216y^3 + (-144t_1)x^4 + (324t_1)xy^2 + (54t_1^2 - 432t_2)x^2 y + (-3t_1^3 - 120 t_1 t_2 - 216 t_3)x^3 + \\
& (324t_3)y^2 + (108 t_1 t_3 - 432 t_4)xy + (-t_1^5 + 4t_1^3 t_2 - 21 t_1^2 t_3 + 8 t_1 t_2^2 - 96 t_1 t_4 - 216 t_2 t_3)x^2 + (t_1^6 + 6 t_1^4 t_2 - 18 t_1^3 t_3 + 24 t_1^2 t_2^2 \\
& - 36 t_1^2 t_4 - 72 t_1 t_2 t_3 + 32 t_2^3 - 144 t_2 t_4 + 162 t_3^2)y + (-t_1^5 t_2 + t_1^4 t_3 + 2 t_1^3 t_4 + 4 t_1^2 t_2 t_3 + 8 t_1 t_2 t_4 - 27 t_1 t_3^2 - 216 t_3 t_4)x \\
& + (-t_1^5 t_4 + t_1^4 t_2 t_3 - 4 t_1^3 t_2 t_4 - t_1^3 t_3^2 + 8 t_1^2 t_2^2 t_3 + 14 t_1^2 t_3 t_4 - 8 t_1 t_2^2 t_4 - 36 t_1 t_2 t_3^2 + 32 t_1 t_4^2 + 16 t_2^3 t_3 - 72 t_2 t_3 t_4 + 27 t_3^3);
\end{aligned}$$

This modulo 2 is:

$$\Delta = t_1^4 t_2 t_3^2 + t_1^5 t_3 t_4 + t_1^6 t_6 + t_1^3 t_3^3 + t_1^4 t_4^2 + t_3^4$$

$$a_1 = t_1^6, \ a_2 = t_1^4 x^2 + t_1^5 y + t_1^4 t_4$$

$$a_3 = t_1^5x^2 + t_1^3x^3 + t_1^6y + t_1^5t_2x + t_1^4t_3x + t_1^2t_3x^2 + t_1^4t_2t_3 + t_1^5t_4 + t_1^3t_3^2 + t_1t_3^2x + t_3^3$$

For the case

$$f = y^2 - x^3 - t_4x - t_6 - t_2x^2. \tag{1.8}$$

we have

$$\Delta = 2(4t_2^3t_6 - t_2^2t_4^2 - 18t_2t_4t_6 + 4t_4^3 + 27t_6^2);$$
$$a_1 = 2(27x^3 - 27y^2 + (27t_2)x^2 + (27t_4)x + (-4t_2^3 + 18t_2t_4 - 27t_6));$$
$$a_2 = 2(-9x^4 + (-12t_2)x^3 + (-t_2^2 - 15t_4)x^2 + (2t_2^3 - 10t_2t_4)x + (t_2^2t_4 - 4t_4^2));$$
$$a_3 = -54x^3y + 27y^3 + (-54t_2)x^2y + (-54t_4)xy + (4t_2^3 - 18t_2t_4)y;$$

Modulo 3 this is:

$$\Delta = t_2^2t_4^2 - t_2^3t_6 - t_4^3$$
$$a_1 = t_2^3,\ a_2 = t_2^2x^2 + t_2^3x + t_2t_4x - t_2^2t_4 + t_4^2,\ a_3 = t_2^3y.$$

For

$$f = y^2 - x^3 - t_4x - t_6; \tag{1.9}$$

we have

$$\Delta = 2(4t_4^3 + 27t_6^2),\ a_1 = 2(27x^3 - 27y^2 + (27t_4)x + (-27t_6)),$$
$$a_2 = 2(-9x^4 + (-15t_4)x^2 + (-4t_4^2)),\ a_3 = -54x^3y + 27y^3 + (-54t_4)xy.$$

Remark 1.3. The reader may has noticed that by this slight modification of the definition of discriminant if we take an elliptic curve (1.9) with all t_i in $\mathbb{Z}$, it is singular reduced mode p if and only if $p \mid \Delta$.

1.18 One dimensional algebraic groups

We follow [16] p. 23. When elliptic curves degenerate we find the following algebraic groups:

1. The additive group $\mathbb{G}_a := (\mathbb{A}^1(\mathsf{k}), +)$.
2. The multiplicative group $\mathbb{G}_m := (\mathbb{A}(\mathsf{k}), \cdot)$.
3. Twisted multiplicative group $\mathbb{G}_m[a]$.

Exercise 1.23.

$$\mathbb{G}_m[a] \cong \mathbb{G}_m[ac^2],\ a, c \in \mathsf{k} - 0,$$

Exercise 1.24.

$$\mathbb{G}_m[a](\mathbb{F}_q) = q + 1.$$

By Bezout theorem a cubic curve E in $\mathbb{P}^2$ has a unique singular point (if there are two singularities then the line connecting that points meets the curve in 4 points counted with multiplicities). The singular point is defined over k because it is fixed under the action of the Galois group $Gal(\bar{\mathsf{k}}/\mathsf{k})$. Let S be the singular point of of E and

$$E^{ns}(\mathsf{k}) := E(\mathsf{k})\backslash\{S\}.$$

The same definition of group law for elliptic curves applies for E^{ns} and it turns out that E^{ns} as a group and:

Exercise 1.25. If the elliptic curve E is given by the Weierstrass form

$$y^2 = x^3 + t_4 x + t_6,\ t_2, t_3 \in \mathsf{k}, \Delta = 2(4t_4^3 + 27t_6^2) = 0.$$

then E^{ns} is isomorphic to the three one dimensional group described above:

$$E^{ns}(\mathsf{k}) \cong \mathbb{G}_m(\mathsf{k}) \text{ or } \mathbb{G}_m[c](\mathsf{k}),\ \text{or } \mathbb{G}_a(\mathsf{k})$$

mentioned in the lectures. Does we need $\mathrm{char}(\mathsf{k}) \neq 2, 3$?

Exercise 1.26. For $\mathrm{char}(\mathsf{k}) = 3$ (resp. $\mathrm{char}(\mathsf{k}) = 2$) we have to consider the case (1.8) (resp. (1.9)). Discuss the reduction modulo 2 and 3 in such cases.

1.19 Reduction of elliptic curves

We take an elliptic curve in the Weierstrass form

$$y^2 = x^3 + t_4 x + t_6,\ t_2, t_3 \in \mathbb{Q}, \Delta := 2(4t_4^3 + 27t_6^2) \neq 0.$$

and by change of coordinates $(x, y) \mapsto (c^2 x, c^3 y),\ c \in \mathbb{Q}$ we assume that $|\Delta|$ is minimal. For p prime different from 2 and 3 we have the curve $E/\mathbb{F}_p$ and the reduction map

$$E(\mathbb{Q}) \to E(\mathbb{F}_p).$$

1. Good reduction. If p does not divide Δ then $E/\mathbb{F}_p$ is an elliptic curve.
2. Cuspidal reduction/additive reduction. The reduced curve $E/\mathbb{F}_p$ has a cusp as a singularity and so its non-singular part is an additive group. If $\mathrm{char}(\mathsf{k}) \neq 2, 3$ this case happens if and only if $p \mid \Delta$, and $p \mid 2t_4 t_6$.
3. Nodal reduction/split multiplicative. The reduced curve $E^{ns}/\mathbb{F}_p$ is a multiplicative group.
4. Nodal reduction/nonsplit multiplicative. The reduced curve $E^{ns}/\mathbb{F}_p$ is a twisted multiplicative group.

Exercise 1.27. Reduction moulo 3 of the above elliptic curve in Weierstrass form is singular if and only if $t_4 = 0$. In the singular case it is always a cusp. In reduction modulo 2 the elliptic curve $E/\mathbb{F}_2$ is always singular and its singular point is $S = (t_4, t_6)$. Find the four groups $E^{ns}(\mathbb{F}_2)$ corresponding to the four choice of (t_4, t_6).

Exercise 1.28. Let $E/\mathbb{Q} : y^2 + y = x^3 - x^2 + 2x - 2$. Show that 1. the primes of bad reduction for E are $p = 5$ and 7. 2. The reduction at $p = 5$ is additive, while the reduction at $p = 7$ is multiplicative. 3. $N_{E/\mathbb{Q}} = 175$.

1.20 Zeta functions of curves over $\mathbb{Q}$

We follow [16] p. 102. The non-complete zeta function of a smooth curve $E : f(x, y) = 0,\ f \in \mathbb{Z}[x, y]$ is defined to be

$$\zeta_S(E, s) = \prod_{p \notin S} \zeta(E/\mathbb{F}_p, s).$$

where S is a finite number of prime numbers such that $E/\mathbb{F}_p$ is singular.

Exercise 1.29. Can you justify the definition of the zeta function of a variety over $\mathbb{Q}$ by interpreting it as a Euler product, the one similar to (1.6).

In the case of elliptic curves it is natural to define

$$L_S(E,s) := \prod_{p \notin S} \frac{1}{1 + (\#(E(\mathbb{F}_p)) - p - 1)p^s + p^{1-2s}}$$

and so we have

$$\zeta_S(E,s) = \frac{\zeta_S(s)\zeta_S(s-1)}{L_S(E,s)}$$

Proposition 1.10. *The product $\zeta_S(E,s)$ and hence $L_S(E,s)$ converges for $\Re(s) > \frac{3}{2}$*

Proof. It is direct consequence of the Riemann hypothesis for elliptic curves over finite fields and the convergence of the Riemann zeta function(see [16] p.102). □

We we want to define the complete L function by adding bad prime numbers $p \in S$. We define

$$L_p(T) = \begin{cases} 1 + (\#(E(\mathbb{F}_p)) - p - 1)T + pT^2 & p \text{ good} \\ 1 - T & \text{modulo } p \text{ we have split multiplicative reduction} \\ 1 + T & \text{modulo } p \text{ we have non-split multiplicative reduction} \\ 1 & \text{modulo } p \text{ we have additive reduction} \end{cases}$$

We have defined this in such a way that

$$L_p(p^{-1}) = \frac{\#E^{ns}(\mathbb{F}_p)}{p}$$

Now we define the L-function of an elliptic curve E over $\mathbb{Q}$:

$$L(E,s) = \prod_p \frac{1}{L_p(p^{-s})}.$$

1.21 Hasse-Weil conjecture

The conductor of an elliptic curve over $\mathbb{Q}$ is defined to be

$$N_{E/\mathbb{Q}} = \prod_{p \text{ bad}} p^{f_p}$$

where $f_p = 1$ if E has multiplicative reduction at p, $f_p = 2$ if $p \not| 2,3$ and E has additive reduction at p. For the case in which we have additive reduction modulo $p = 2,3$ we have $f_p \geq 2$, $f_p \in \mathbb{N}$ and f_p depends on wild ramification in the action of the inertia group at of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the Tate module of E.

Exercise 1.30. Discuss the case $p = 2,3$ in the above definition. [16] is also talking about a formula of Ogg $f_p = ord_p\Delta + 1 - m_p$ using Néron models. Can you obtain some information on this.

Define

$$\Lambda(E,s) := N_{E/\mathbb{Q}}^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(E,s)$$

Theorem 1.7. *(Hasse-Weil conjecture for elliptic curves) The function $\Lambda(E,s)$ can be analytically continued to a meromorphic function on the whole $\mathbb{C}$ and it satisfies the functional equation*

$$\Lambda(E,s) = \pm\Lambda(E,2-s).$$

This theorem was first proved for CM elliptic curves by Deuring 1951/1952. It is proved in its generality by the works of Eichler and Shimura, Wiles, Taylor, Diamond and others.

1.22 Birch Swinnerton-Dyer conjecture

For the functional equation of L the value $s=1$ is in the middle, i.e. it is the fixed point of $s \mapsto 2-s$.

Conjecture 1.1. (BSD conjecture) For an elliptic curve E over $\mathbb{Q}$, the function $L(E,s)$ is holomorphic at $s=1$ and its order of vanishing at $s=1$ is the rank of the elliptic curve E.

A weak form of this conjecture is not also proved:

Conjecture 1.2. (weak BSD conjecture) $L(E,1)=0$ if and only if E has infinitely many rational points.

For papers on BSD conjecture see [4, 1, 2, 24, 11] [21], [17].

1.23 Congruent numbers

The bad prime numbers for the elliptic curve $E_n : y^2 = x^3 - nx$ are those which divide $2n$. For $p \mid 2n,\ p \neq 2$ or $p=2,\ 2|n$ we have an additive reduction. For $p=2$ and $p \not| n$ we have apparently a multiplicative reduction: $y^2 = x^3 + x$. The singular point in this case is $S=(1,0)$ and $E^{ns}(\mathbb{F}_2) = \{O,(0,0)\}$ which is isomorphic to $(\mathbb{A}(\mathbb{F}_2),+)$ and so it is additive.

The conductor of E_n is:

$$N_{E_n/\mathbb{Q}} = \begin{cases} 2^4 n^2 & \text{if } n \text{ is even} \\ 2^5 n^2 & \text{if } n \text{ is odd} \end{cases}$$

In Theorem 1.7 the root number $\pm$ is determined in the following way:

$$\begin{cases} +1 & \text{if } n \equiv 1,2,3 \ (8) \\ -1 & \text{if } n \equiv 5,6,7 \ (8) \end{cases}$$

Reformulating Proposition 1.7 and using Exercise 1.21 we have:

$$(1-T)(1-pT)Z(E_n/\mathbb{F}_p,T) = \prod_{\mathfrak{p}|\langle p\rangle} (1-(\alpha_{\mathfrak{p}}T)^{\deg(\mathfrak{p})})$$

where

$$\alpha_{\mathfrak{p}} = \begin{cases} i\sqrt{p} & \text{if } \mathfrak{p} = \langle p\rangle \\ a+ib & \text{if } p \text{ splits, where } a+ib \text{ is the unique generator of } \mathfrak{p} \\ & \text{which is congruent to } (\frac{n}{p}) \bmod 2+2i. \\ 0 & p \mid 2n \end{cases}$$

The L function of E_n is

$$L(E_n, s) = \prod_{\mathfrak{p} \subset \mathbb{Z}[i] \text{ prime}} (1 - (\alpha_{\mathfrak{p}})^{\deg(\mathfrak{p})} (\mathbb{N}\mathfrak{p})^{-s})^{-1}$$

Now $\mathbb{Z}[i]$ is a Dedekind domain and so we can define a unique map χ from the ideals of $\mathbb{Z}[i]$ to $\mathbb{C}$ such that $\chi_n(\mathfrak{p}) = \alpha_{\mathfrak{p}}^{\deg(\mathfrak{p})}$. Therefore

$$L(E_n, s) = \prod_{\mathfrak{p} \subset \mathbb{Z}[i] \text{ prime}} (1 - \chi(\mathfrak{p})(\mathbb{N}\mathfrak{p})^{-s})^{-1} = \sum_{\mathfrak{a} \subset \mathbb{Z}[i]} \chi_n(\mathfrak{a})(\mathbb{N}\mathfrak{a})^{-s}$$

where the sum is taken over all non-zero ideals.

1.24 p-adic numbers

By definition a p-adic integer is an element in the inverse limit of

$$\cdots \to \mathbb{Z}/p^3\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}.$$

One can show that a p-adic integer is identified with a formal series

$$a_1 p + a_2 p^2 + a_3 p^3 + \cdots, \ a_i \in \{0, 1, 2, \ldots, p-1\}.$$

The set of p-adic integers is denoted by $\mathbb{Z}_p$:

$$\mathbb{Z}_p := \lim_{\infty \leftarrow n} \mathbb{Z}/\mathbb{Z}p^n.$$

$\mathbb{Z}_p$ is a ring without zero divisor, i.e. if $ab = 0, a, b \in \mathbb{Z}_p$ then either $a = 0$ or $b = 0$. The field $\mathbb{Q}_p$ of p-adic numbers is the quotient field of $\mathbb{Z}_p$. The ring $\mathbb{Z}$ of integers is a subring of $\mathbb{Z}_p$ in a natural way and so $\mathbb{Q}_p$ is a field extension of $\mathbb{Q}$, $\mathbb{Q} \subset \mathbb{Q}_p$.

Exercise 1.31. Show that the Diphantine equation $x^3 + y^3 - 3 = 0$ has not a solution in $\mathbb{Q}_3$ and hence it has not a solution in $\mathbb{Q}$.

There is another way to define p-adic numbers. Any non-zero rational number a can be expressed in the form $a = p^r \frac{m}{n}$ with $m, n \in \mathbb{Z}$ and not divisable by p. We define

$$\mathrm{ord}_p(a) := r, \ |a|_p := \frac{1}{p^r}, \ |0|_p := 0$$

We have

1. $$|a|_p = 0 \text{ if and only if } a = 0$$

2. $$|ab|_p = |a|_p |b|_p, \ a, b \in \mathbb{Q}.$$

3. $$|a + b|_p \leq \max\{|a|_p, |b|_p\} \text{ and so } \leq |a|_p + |b|_p$$

Therefore,

$$d_p(a,b) := |a-b|_p$$

is a metric on $\mathbb{Q}$. The field $\mathbb{Q}_p$ of p-adic numbers is the completion of $\mathbb{Q}$ with respect to d_p. We have a cononical matric, call it again d_p, on $\mathbb{Q}_p$ which extends the previous one on $\mathbb{Q} \subset \mathbb{Q}_p$ (this inclusion is given by sending $a \in \mathbb{Q}$ to the constant Cauchy sequence $a, a, \ldots$). The same construction with the usual norm of $\mathbb{Q}$, i.e. $d(a,b) = |a-b|$ yields to the field of real numbers $\mathbb{R}$.

Exercise 1.32. Prove that the two definitions of $\mathbb{Q}_p$ presented above are equivalent. Prove also

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\} = \text{ the closure of } \mathbb{Z} \text{ in } \mathbb{Q}_p$$

Chapter 2

Modular forms

The objective of this chapter is to introduce modular forms and their relations with elliptic curves.

2.1 Elliptic integrals

We follow partially [22] Chapter VI §1.

Let us take $t_2, t_3 \in \mathbb{C}$ in such a way that the polynomial $f(x) := 4x^3 - t_2 x - t_3$ has three distinct roots. In other words $27t_2^3 - t_3^2 \neq 0$. During the history the mathematicians understood that the elliptic integral

$$\int_I \frac{dx}{\sqrt{4x^3 - t_2 x - t_3}},$$

where I is a path connecting two roots of f, for generic numbers t_2, t_3 is a new integral and cannot be calculated by previusly known numbers. For simplicity one can take t_2 and t_3 real numbers in such a way that f has three real roots. Then one can take I the interval between two roots of f. One can write them, up to ± 1, in a modern way as

$$\int_\delta \frac{dx}{y},\ \delta \in H_1(E_t, \mathbb{Z})$$

where $E_t : y^2 = 4x^3 - t_2 x - t_3$ is an elliptic curve (see the introduction of [18]).

Exercise 2.1. Justify the topological cycle $\delta \in H_1(E_t, \mathbb{Z})$ described in the course.

Exercise 2.2. By algebraic geometric methods show that $\frac{dx}{y}$ restricted to E_t has no poles even at infinity.

2.2 Weierstrass uniformization theorem

We follow partially [22] Chapter VI §3. A lattice Λ in $\mathbb{C}$ is a $\mathbb{Z}$-submodule of $\mathbb{Z}$ generated by two $\mathbb{R}$-linear independent elements ω_1 and ω_2 in $\mathbb{C}$. Without loss of generality we can assume that $\Im(\frac{\omega_1}{\omega_2}) > 0$. For a lattice $\Lambda \subset \mathbb{C}$ the Weierstrass $\wp$-function is

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda,\ \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

and the Eisenstein series of weight $2k$ are

$$G_{2k}(\Lambda) = \sum_{\omega\in\Lambda,\ \omega\neq 0} \frac{1}{\omega^{2k}}$$

Proposition 2.1. *Let $\Lambda \subset \mathbb{C}$ be a lattice. The Eenstein series G_{2k} is absolutely convergent for all $k > 1$. The Weierstrass $\wp$-function converges absolutely and uniformely on every compact subset of $\mathbb{C} - \Lambda$.*

Proof. See Theorem 3.1 of [22]. □

Exercise 2.3. Show that $\sum_{\omega\in\Lambda,\ \omega\neq 0} \frac{1}{(z-\omega)^2}$ does not converge.

Let $\mathcal{L}$ be the space of lattices $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$.

Exercise 2.4. Show that $\mathcal{L}$ has a natural structure of a complex manifold. More precisely, show that $\mathcal{L}$ can be obtained by a quotient of a complex manifold by $\mathrm{SL}(2,\mathbb{Z})$.

Theorem 2.1. *(Weierstrass uniformization theorem) Let*

$$E_t : y^2 = 4x^3 - t_2 x - t_3,\ t_2^3 - 27t_3^2 \neq 0.$$

The map given by

$$\mathsf{p} : \mathbb{C}^2\backslash\{t_2^3 - 27t_3^2 = 0\} \to \mathcal{L}$$

$$(t_2, t_3) \mapsto \int_{H_1(E_t,\mathbb{Z})} \frac{dx}{y}$$

is well-defined and it is a biholomorphism which satisfies

$$\mathsf{p}(t_2\lambda^{-4}, t_3\lambda^{-6}) = \lambda\mathsf{p}(t_2, t_3).$$

Its inverse is given by the Eisenstein series:

$$\Lambda \to (g_2(\Lambda), g_3(\Lambda))$$

where

$$g_2 := 60G_4,\ g_3 = -140G_6$$

Moreover, for a fixed t_2, t_3 the Abel map given by

$$E_t \to \mathbb{C}/\Lambda,\ a \mapsto \int_a^\infty \frac{dx}{y}$$

is a biholomorphism and homomorphism of groups and its inverse is given by

$$z \mapsto [\wp(z,\Lambda); \wp'(z,\Lambda); 1],$$

where $\Lambda = \mathsf{p}(t)$.

Exercise 2.5. Ex. 6.2, 6.4,6.6,6.7,6.14 of [22].

2.3 Picard-Lefschetz theory

We consider again the familly of elliptic curves

$$E_t : y^2 = 4x^3 - t_2 x - t_3,\ t_2^3 - 27t_3^2 \neq 0.$$

Let us put

$$T := \mathbb{C}^2 - \{(t_2, t_3) \in \mathbb{C}^2 \mid t_2^3 - 27t_3^2 = 0\}$$

By Ehresmann's theorem the fibration $E_t, t \in T$ is a C^∞ bundle over T, i.e. it is locally trivial. This is the basic stone for the Picard-Lefschetz theory (see for instance [**?**] and the references there). It gives us the following linear action:

$$\pi_1(T, b) \times H_1(E_b, \mathbb{Z}) \to H_1(E_b, \mathbb{Z})$$

where $b \in T$ is a fixed point In order to calculate it we proceed as follows: First we choose two cycles $\delta_1, \delta_2 \in H_1(E_b, \mathbb{Z})$. For the fixed parameter $t_2 \neq 0$, define the function f in the following way:

$$f : \mathbb{C}^2 \to \mathbb{C},\ (x, y) \mapsto -y^2 + 4x^3 - t_2 x.$$

The function f has two critical values given by $\tilde{t}_3,\ \check{t}_3 = \pm\sqrt{\frac{t_2^3}{27}}$. In a regular fiber $E_t = f^{-1}(t_3)$ of f one can take two cycles δ_1 and δ_2 such that $\langle \delta_1, \delta_2 \rangle = 1$ and δ_1 (resp. δ_2) vanishes along a straight line connecting t_3 to $\tilde{t}_3$ (resp. $\check{t}_3$). The corresponding anti-clockwise monodromy around the critical value $\tilde{t}_3$ (resp $\check{t}_3$) can be computed using the Picard-Lefschetz formula:

$$\delta_1 \mapsto \delta_1,\ \delta_2 \mapsto \delta_2 + \delta_1 \text{ (resp. } \delta_1 \mapsto \delta_1 - \delta_2,\ \delta_2 \mapsto \delta_2).$$

It is not hard to see that the canonical map $\pi_1(\mathbb{C}\backslash\{\tilde{t}_3, \check{t}_3\}, b) \to \pi_1(T, t)$ induced by inclusion is an isomorphism of groups and so the image of the monodromy group written in the basis δ_1 and δ_2 is:

$$\langle A_1, A_2 \rangle = \mathrm{SL}(2, \mathbb{Z}), \quad \text{where } A_1 := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ A_2 := \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Note that $g_1 := A_2^{-1}A_1^{-1}A_2^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $g_2 := A_1^{-1}A_2^{-1} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ and $\mathrm{SL}(2, \mathbb{Z}) = \langle g_1, g_2 \mid g_1^2 = g_2^3 = -I \rangle$, where I is the identity 2×2 matrix.

Exercise 2.6. Discuss the Picard-Lefschetz theory as above for the Legendre family of elliptic curves:

$$y^2 = x(x-1)(x-\lambda)$$

2.4 Schwarz function

Let us take the Legendre family of elliptic curves and consider the Schwarz function

$$\lambda \mapsto \frac{\int_{\delta_1} \frac{dx}{y}}{\int_{\delta_2} \frac{dx}{y}} \in \mathbb{H}$$

It is multivalued beacuse of the choice of δ_1, δ_2. In order to get a one valued function we restrict λ to $\mathbb{H}$ and choose cycles $\delta_i,\ i = 1, 2$ such that the projection of δ_1 (resp. δ_2)

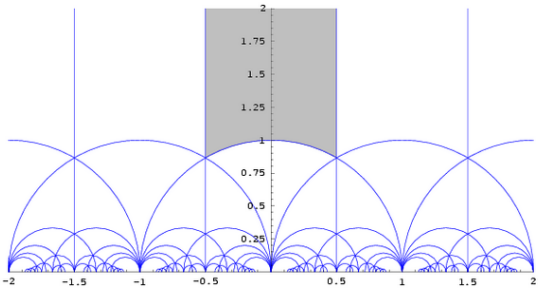

Figure 2.1: Fundamental domain

to the x-palne is a cycle around 0 (resp. 1)and λ. In this way the Shwarz function is a biholomorphisim. Its analytic continuations around $\lambda = 0, 1$ corresponds to the Picard-Lefschetz transformation of δ_1 and δ_2.

Exercise 2.7. Show that the image of the Schwarz function is the region depicted in 2.1[1]. The analytic continuations of the Schwarz map gives us the trianglization of $\mathbb{H}$.

2.5 CM elliptic curves

Recall that $\mathcal{L}$ is a complex manifold whose points are lattices $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. In fact one can reinterpret it as follows:

Exercise 2.8. $\mathcal{L}$ is the moduli of triples (E, ω, p), where E is a Riemann surface of genus one, $p \in E$, and ω is a holomorphic differential form on E. The canonical action of $a \in \mathbb{C}^*$ on $\mathcal{L}$ corresponds to the multiplication of ω with a^{-1}.

Definition 2.1. The endomorphisim group of an elliptic curve $E = E_\Lambda$ is the set of all holomorphic maps $E_\Lambda \to E_\Lambda$ which are in addition homomorphisims of groups. It is in one to one correspondance with

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\}$$

We have $\mathbb{Z} \subset \mathrm{End}(E)$ and we say that E is CM if the inclusion is strict.

Later, we will encounter two spcial CM elliptic curves as follows:

Exercise 2.9. Classify all elliptic curves E with $\alpha \in \mathrm{End}(E)$ which is not multiplication by ± 1 and is an isomorphism. More precisely show that we have only two such elliptic curve

$$E = E_{\langle z,1\rangle},\ z = i, \frac{-1 + i\sqrt{3}}{2}.$$

Exercise 2.10. Ex. 8,9,10,12 of Koblitz.

[1]Reproduced from Wikipedia

2.6 Full modular forms

Let us consider a point $z \in \mathbb{H}$ and the lattice $\langle 1, z\rangle \subset \mathbb{C}$. The Eisenstein series restricted to such a lattice gives us the following series

$$G_{2k}(z) := \sum_{(n,m)\in\mathbb{Z}^2-\{(0,0)\}} \frac{1}{(nz+m)^{2k}},\ k = 2, 3, \dots$$

which we call them again Eisenstein series. It is easy to show that G_{2k} is a modular form of weight $2k$ for the group $\mathrm{SL}(2,\mathbb{Z})$:

Definition 2.2. A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called a modular form of weight k for the group $\mathrm{SL}(2,\mathbb{Z})$ (full modular form of weight k) if

1. f has a finite growth at infinity, i.e.

$$\lim_{\Im z\to\infty} f(z) = a_\infty \in \mathbb{C} \tag{2.1}$$

2. f satisfies

$$(cz+d)^{-k} f(\frac{az+b}{cz+d}) = f(z),\ \forall,\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}),\ z \in \mathbb{H}.$$

The group $\mathrm{SL}(2,\mathbb{R})$ acts on $\mathbb{H}$ in a canonical way:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z := \frac{az+b}{cz+d},\quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}),\ z \in \mathbb{H}$$

The fundamental domain of the action of $\mathrm{SL}(2,\mathbb{Z})$ is depicted in Figure 2.1. It is useful to define the slash operator on holomorphic functions f in $\mathbb{H}$:

$$f|_k(z) := (cz+d)^{-k} f(\frac{az+b}{cz+d}),\quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}),\ z \in \mathbb{H}.$$

Exercise 2.11. Modular forms of weight k are in one to one correspondance with holomorphic functions f on $\mathcal{L}$ such that

1. For all $\Lambda \in \mathcal{L}$ and $a \in \mathbb{C}^*$, $f(a\Lambda) = a^{-k} f(\Lambda)$.
2. $f(\langle z, 1\rangle)$ has finite growth at infinity as in (2.1).

2.7 Fourier series

Since for a full modular form we have $f(z+1) = f(z)$ we can write the Laurant series of f in $e^{2\pi i z}$:

$$f(z) = \sum_{i=0}^{\infty} a_i q^i,\ q := e^{2\pi i z}$$

This is called the Fourier series (q-expansion) of f.

Proposition 2.2. *Let $k > 2$ be an even integer. The q-expansion of G_k is as follows:*

$$G_k = 2\zeta(k)(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n),\ q := e^{2\pi iz}$$

where the Bernoulli numbers B_k are defined by:

$$\frac{x}{e^x - 1} = \sum_{k=1}^{\infty} B_k \frac{x^k}{k!} = 1 + \frac{\frac{-1}{2}}{1!}x + \frac{\frac{1}{6}}{2!}x^2 + \frac{\frac{-1}{30}}{4!}x^4 + \frac{\frac{1}{42}}{6!}x^6 + \frac{\frac{1}{32}}{8!}x^8 + \frac{\frac{5}{66}}{10!}x^{10} + \cdots$$

and

$$\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}$$

Proof. [9], p. 110. □

It is sometimes usefull to define the normalized Eisenstein series:

$$E_k = \frac{1}{2}\sum_{n,m\in\mathbb{Z},\ (n,m)=1} \frac{1}{(nz+m)^k} = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$$

2.8 The algebra of modular forms

Let us denote by $\mathrm{M}_k := \mathrm{M}_k(\mathrm{SL}(2,\mathbb{Z}))$ the vector space of full modular forms of weight k. The set

$$\mathrm{M} = \oplus_{k\in\mathbb{Z}}\mathrm{M}_k$$

form a graded $\mathbb{C}$-algebra.

Proposition 2.3. *The $\mathbb{C}$-algebra* M *is freely generated by the Eisenstein series $G_k,\ k = 4, 6$.*

Proof. The proposition follows from the Weierstrass uniformization theorem as follows: Let us consider the map

$$\mathbb{H} \to \mathbb{C}^2,\ z \mapsto \mathsf{p}^{-1}(\langle z, 1\rangle)$$

It factores through $\mathbb{H} \to \mathbb{D} - \{0\},\ z \mapsto e^{2\pi iz}$ and so using Proposition 2.2 we obtain the holomorphic map

$$\alpha : \mathbb{D} \to \mathbb{C}^2,\ \alpha(q) = (60G_4(q), -140G_6(q)).$$

Moreover, we can check that $\alpha(0)$ is a regular point of $\Delta = 0$ and the image of α at $\alpha(0)$ is transeverse to $\Delta = 0$.

We consider a modular form as a holomorphic function on $\mathcal{L}$ as it is asked in Exercise 2.11. Pulling back f by the period map p we get a holomorphic function g in $T := \mathbb{C}^2 - \{\Delta = 0\}$ which satisfies

$$g(\lambda^{-4}t_2, \lambda^{-6}t_3) = \lambda g(t_2, t_3)$$

and g restricted to the image of α is holomorphic in $\alpha(0)$. Conversely, a holomorphic function g in T with these properties corresponds to a modular form f. It follows that g is holomorphic in all points of $\Delta = 0$ and so it extends to a holomorphic function in $\mathbb{C}^2$. Writting the taylor series of f with homoheneous pieces in $\mathbb{C}[t_2, t_3],\ \deg(t_2) = 4,\ \deg(t_6) = 6$ we conclude that g is homogeneous polynomial of degree k in the mentioned ring. □

2.9 The discriminant

Recall that

$$\zeta(4) = \frac{\pi^4}{90},\ \zeta(6) = \frac{\pi^6}{945},$$

We define

$$\Delta := t_2^3 - 27t_3^2 = g_2^3 - 27g_3^2 = (2\zeta(4)60E_4)^3 - 27(2\zeta(6)140)^2E_6^2 = \frac{(2\pi)^{12}}{1728}(E_4^3 - E_6^2)$$

and we have

$$(2\pi)^{-12}\Delta = \frac{1}{1728}(E_4^3 - E_6^2) = (\sum_{n=1}^{\infty}\tau(n)q^n = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 + \cdots = q\prod_{n=1}^{\infty}(1-q^n)^{24}$$

$\tau(n)$ is called the Ramanujan function of n.

Exercise 2.12. Exercise 4, p. 123 of Koblitz. The third part of the exercise says that

$$\tau(n) \equiv \sigma_{11}(n)(\text{ mod } 691)$$

Also Ex. 3

2.10 The j function

We have

$$j = 1728\frac{t_2^3}{t_2^3 - 27t_3^2} = 1728\frac{E_4^3}{E_4^3 - E_6^2} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

There is so called Monstrous Moonshine conjecture, proved by Brocherd, relating the coefficients of the q-expansion of j with the minimal dimensions needed to represent monster groups.

2.11 Hecke operators

So far, we have interpreted modular forms as functions in theree spaces: the Poicaré upper half plan $\mathbb{H}$, the space $\mathcal{L}$ of lattices and the affine space $\mathbb{A}^2_{\mathbb{C}}$ representing the parameters t_2 and t_3. In this section for each natural number n we want to define the Hecke operator

$$T_n : \mathrm{M}_k \to \mathrm{M}_k$$

which is a linear map. It is given by one of the following equivalent definitions:

1. For $f : \mathbb{H} \to \mathbb{C}$ a modular form of weight k we have

$$T_n(f) = \sum_{i=1}^{s} f|_k A_i,$$

where $\{[A_1], [A_2], \cdots [A_s]\} = \mathrm{SL}(2,\mathbb{Z})/\mathbb{M}at_n(2,\mathbb{Z})$.

2. For $f : \mathcal{L} \to \mathbb{C}$ a modular form of weight k we have
$$T_n(f)(\Lambda) = \sum_{\Lambda'} f(\Lambda'),$$
where Λ' runs through all sublattices $\Lambda' \subset \Lambda$ of index n. This means that $\#(\Lambda/\Lambda') = n$.

3. For f a homogeneous polynomial of degree k in $\mathbb{C}[t_t, t_3]$, $\deg(t_2) = 4$, $\deg(t_3) = 6$ we have
$$T_n(f)(t_2, t_3) = \sum_{t'} f(t'),$$
where $t' = (t'_2, t'_3)$ runs through all parameters for which there is an isogeny $\alpha : E_{t'} \to E_t$ such that $\alpha^*(\frac{dx}{y}) = \frac{dx}{y}$ and $\deg(\alpha) = n$.

Exercise 2.13. Prove the equivalence of the above definitions.

Exercise 2.14. Prove that each equivalence class in $\mathrm{SL}(2,\mathbb{Z})/\mathbb{M}at_n(2,\mathbb{Z})$ is represented exactly by one of the matrices
$$\begin{pmatrix} d & b \\ 0 & \frac{n}{d} \end{pmatrix},\ d|n,\ 0 \le b < \frac{n}{d}.$$

Exercise 2.15. Can you show by algebraic geometric methods that for fixed $t \in \mathbb{C}^2 \backslash \{\Delta = 0\}$ the set of parameters t' with
$$\alpha : E_{t'} \to E_t, \alpha^* \frac{dx}{y} = \frac{dx}{y},\ \deg(\alpha) = n$$
is finite.

Let A be an element in the group generated by $\mathrm{GL}_+(2,\mathbb{R})$ and $\{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \mid \lambda \in \mathbb{C}^*\} \cong \mathbb{C}^*$. Let also $\omega = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathcal{P}$. Then
$$A\omega \in \mathcal{P}.$$
Using the map p in Weierstrass uniformization theorem, we can translate the above process to the (t_2, t_3)-space. Namely, for each $t \in \mathbb{C}^2 - \{\Delta = 0\}$ and a basis of the homology $\delta_1, \delta_2 \in H_1(E_t, \mathbb{Z})$ with $\langle \delta_1, \delta_2 \rangle = 1$ and A as above we have a local holomorphic map $t \mapsto \alpha(t)$. If we choose another basis of $H_1(E_t, \mathbb{Z})$ obtained by the previous one by an element $B \in \mathrm{SL}(2,\mathbb{Z})$, then we have a new period matrix $AB\omega$. This is equal to $A\omega$ in $\mathcal{L}$ if and only if
$$ABA^{-1} \in \mathrm{SL}(2,\mathbb{Z}).$$
We conclude that if we choose representatives for the quotient
$$(A \cdot \mathrm{SL}(2,\mathbb{Z}) \cdot A^{-1} \cap \mathrm{SL}(2,\mathbb{Z}))\backslash(A \cdot \mathrm{SL}(2,\mathbb{Z}) \cdot A^{-1}) = \{[A_i] \mid i = 1, 2, \ldots, s\}$$
then to each A_i we have associated a local map $\alpha_i(t)$.

Exercise 2.16. Let $A_i = AS_iA^{-1},\ S_i \in \mathrm{SL}(2,\mathbb{Z})$. Show that
$$\mathrm{SL}(2,\mathbb{Z})/\mathbb{M}at_n(2,\mathbb{Z}) = \{[AS_i] \mid i = 1, 2, \ldots, s\}$$
and vice-versa.

Exercise 2.17. For two natural numbers $n.m$ and Hecke operators $T_n, T_m \in \mathrm{M}_k \to \mathrm{M}_k$ prove that

$$T_n \circ T_m = \sum_{d|(n,m)} d^{k-1} T_{\frac{nm}{d^2}}.$$

The above formula is summarized in the following formal equality:

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_p (1 - T_p p^{-s} + p^{k-1-2s})^{-1}$$

Let f be a modular form with the Fourier expansion:

$$f(z) = \sum_{n=0}^{\infty} a_n q^n, \ q = e^{2i\pi z}.$$

For $m \in \mathbb{N}$, we have $T_m f(z) = \sum\limits_{n=0}^{\infty} b_n q^n$, where

$$b_n = \sum_{d|\gcd(m,n)} d^{k-1} a_{mn/d^2}.$$

Exercise 2.18. Let $n \in \mathbb{N}$. Are there polynomials $p_{n,i}(t_2, t_3), \ i = 2, 3$ such that $p_n := (p_{n,2}, p_{n,3})$ leaves $\Delta = 0$ invariant and

$$T_n(f)(t) = f(p_n^{-1}(t)), \ f \in \mathrm{M}_k,$$

where $f(X) = \sum_{x \in X} f(x)$.

2.12 Groups

We have seen that $\mathrm{SL}(2, \mathbb{Z})$ appears as the monodromy group of the Weierstrass familly of elliptic curves. In this section we work with subgroups of $\mathrm{SL}(2, \mathbb{Z})$. Let N be a positive integer number. Define

$$\Gamma(N) := \{A \in \mathrm{SL}(2, \mathbb{Z}) \mid A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ (\mathrm{mod}\ N)\}$$

It is the kernel of the canonical homomorphism of groups $\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$. A subgroup $\Gamma \subset \mathrm{SL}(2, \mathbb{Z})$ is called a congruence subgroup of level N if it contains $\Gamma(N)$. Our main examples are

$$\Gamma_1(N) := \{A \in \mathrm{SL}(2, \mathbb{Z}) \mid A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \ (\mathrm{mod}\ N)\}$$

$$\Gamma_1(N) := \{A \in \mathrm{SL}(2, \mathbb{Z}) \mid A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \ (\mathrm{mod}\ N)\}$$

Let $\Lambda \subset \mathbb{C}$ be a lattice. The N-torsion subgroup of the complex elliptic curve $E = \mathbb{C}/\Lambda$ is

$$E[N] := \{p \in E \mid np = 0\} = (\frac{1}{N}\Lambda)/\Lambda.$$

and

$$\mu_N := \{e^{\frac{2\pi ik}{N}} \mid k \in \mathbb{Z}\}.$$

The Weil pairing

$$e_N : E[N] \times E(N) \to \mu_N$$

is defined as follows: let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2,\ \Im(\frac{\omega_1}{\omega_2}) > 0$. For $p, q \in E[N]$ write

$$\begin{pmatrix} p \\ q \end{pmatrix} = A \begin{pmatrix} \frac{\omega_1}{N} \\ \frac{\omega_2}{N} \end{pmatrix},\ A \in \mathrm{SL}(2, \mathbb{Z}).$$

Define

$$e_N(p, q) = e^{\frac{2\pi i \det(A)}{N}}$$

Exercise 2.19. Prove that the above definition is well-defined.

Proposition 2.4. *Let*

$$Y_0(N) := \Gamma_0(N)\backslash\mathbb{H},\ Y_1(N) := \Gamma_1(N)\backslash\mathbb{H},\ Y(N) := \Gamma(N)\backslash\mathbb{H}.$$

1. *The set $Y_0(N)$ is the moduli space of pairs (E, C), where E is a complex elliptic curve and C is a cyclic subgroup of E of order N.*
2. *The set $Y_1(N)$ is the moduli space of pairs (E, p), where E is a complex elliptic curve and p is a point of E of order N.*
3. *The set $Y(N)$ is the moduli space of pairs $(E, (p, q))$, where E is a complex elliptic curve and (p, q) is a pair of points of E that generates the N-torsion subgroup of E with Weil pairing $e_N(p, q) = e^{\frac{2\pi i}{N}}$.*

The item 2 is proved in the lectures.

Exercise 2.20. Prove 1 and 3 above.

Bibliography

[1] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[2] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[3] J. W. S. Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, 41:193–291, 1966.

[4] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.

[5] Dale Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[6] Nathan Jacobson. *Basic algebra. I.* W. H. Freeman and Company, New York, second edition, 1985.

[7] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992.

[8] Nicholas M. Katz. An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields. In *Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974)*, pages 275–305. Amer. Math. Soc., Providence, R.I., 1976.

[9] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[10] Serge Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1978.

[11] Serge Lang. Sur la conjecture de Birch-Swinnerton-Dyer (d'après J. Coates et A. Wiles). In *Séminaire Bourbaki, 29e année (1976/77)*, volume 677 of *Lecture Notes in Math.*, pages Exp. 503, pp. 189–200. Springer, Berlin, 1978.

[12] Ju. I. Manin. Rational points on algebraic curves over function fields. *Izv. Akad. Nauk SSSR Ser. Mat.*, 27:1395–1440, 1963.

[13] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[14] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[15] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[16] J. S. Milne. Elliptic curves. *Lecture notes,* `www.jmilne.org`, 1996.

[17] L. J. Mordell. *Diophantine equations*. Pure and Applied Mathematics, Vol. 30. Academic Press, London, 1969.

[18] Hossein Movasati. Moduli of polarized hodge structures. *Bull. Bras. Math. Soc.*, 39(1):81–107, 2008.

[19] Trygve Nagell. Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre. Technical report, Skr. Norske Vid.-Akad., Oslo 1935, No.1, 1-25 , 1935.

[20] Ernst S. Selmer. The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 85:203–362 (1 plate), 1951.

[21] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.

[22] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[23] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[24] J. B. Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Invent. Math.*, 72(2):323–334, 1983.

[25] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.