UNIVERSITÀ
DEGLI STUDI
DI MILANO

UNIVERSITÄT
DUISBURG
ESSEN
Offen im Denken

Università degli Studi di Milano

Universität Duisburg-Essen

Master Thesis

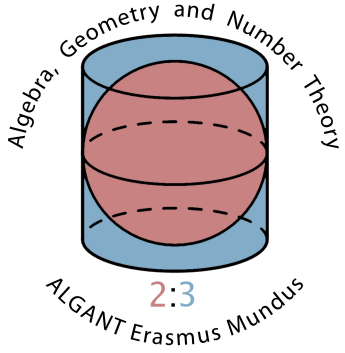
presented by

Giada Grossi

Heegner points and a p-adic Gross–Zagier formula

advisor

Prof. Dr. Massimo Bertolini



Academic year 2015/2016

Fakültat für Mathematik
Universität Duisburg-Essen
Thea-Leymann-Str. 9
45141 Essen

Contents

Introduction

One of the most interesting results proved in the last 20 years is the *modularity theorem* for elliptic curves defined over the rationals, which associates to every such a curve E of conductor N a weight 2 newform of level N. In particular this gives rise to the *modular parametrization*

$$\phi_N : X_0(N) \to E,$$

where $X_0(N)$ is the modular curve of level N. One of the most important arithmetic applications of this arises through the theory of complex multiplication. Fixed a quadratic imaginary field K satisfying certain assumptions, one can indeed construct some special points on E, called *Heegner points*, defined over the class fields of K. They turn out to be very useful tools to get different kind of information about E.

In order to better understand this theory, **Chapter 0** gives a brief overview about elliptic curves, following mainly [Sil09]. After recalling the basic definitions and results, the theory of complex multiplication is summarized, following [Shi71], in order to have the characterization of the class fields of a quadratic imaginary field needed for the construction of the Heegner points. Finally we recall also the definition and properties of the L-function associated to an elliptic curve over $\mathbb{Q}$, that is a key tool to understand the connection with the theory of modular forms.

Chapter 1 reviews first of all the classical definitions of modular forms and p-adic modular forms and then illustrates, following [Kat72], how these can be seen as particular functions on *marked elliptic curves*. After introducing some operators, that will be useful in the following chapters, we define the L-function associated to a newform f with rational coefficients and finally present the result of Eichler-Shimura, which associates to f an elliptic curve over $\mathbb{Q}$, and the modularity theorem, which does the converse. To conclude we then define, fixed a quadratic imaginary field K satisfying the Heegner hypothesis and an elliptic curve E over $\mathbb{Q}$, the Heegner point $P_K \in E(K)$.

Such a point P_K, and in particular its being of infinite order or not, gives information about the L-function of E over K. Indeed the Gross–Zagier formula relates the Néron-Tate height of P_K to the first derivative of such a function evaluated at the central critical point $s = 1$. In **Chapter 2** we illustrate a particular case of the main theorem proved in [BDP], as it is presented in chapter 1.3 of [BCD+14], that is a p-adic analogue of the Gross–Zagier formula. If f is the newform associated to E, one can indeed construct the *anticyclotomic p-adic L-function attached to f and K* interpolating the L-functions of f over K twisted by certain Hecke characters. The main theorem relates the value of this function in a point outside the domain of interpolation to the p-adic logarithm of P_K.

Both in the case of the Gross–Zagier formula and in the case of the p-adic analogue we presented, to determine whether the considered function vanishes at the relevant critical point is equivalent to determine if the Heegner point P_K has infinite order. Using thus this kind of question as a motivation for studying the behaviour of such special points, we

present in **Chapter 3** two explicit examples: the first one, explaining some results about Heegner points proved in [Gro86], is an example of Heegner point of infinite order; the second, following [Zag84], is an example of trivial Heegner point.

The construction of the point $P_K \in E(K)$ can be generalized to get, as we were saying at the beginning, a collection of points $P_n \in E(K_n)$, where K_n is the class field of K of conductor n. In the **Appendix** we present this construction and give a sketch, following [Gro91], of how to use these points to prove Kolyvagin's theorem: if P_K is of infinite order, then the rank of $E(K)$ is equal to 1 and the Tate-Shafarevich group $Ш(E/K)$ is finite.

Chapter 0

Elliptic Curves

0.1 A brief overview

We start by recalling some definitions and basic results about the theory of elliptic curves, following mainly [Sil09].

Definition 0.1.1. An *elliptic curve* is a pair (E, O), where E is a nonsingular curve of genus one and $O \in E$. We say that the elliptic curve is defined over K, written E/K, if E is defined over K and $O \in E(K)$.

Using Riemann-Roch theorem, one can show quite easily that every elliptic curve is isomorphic to a plane curve (in $\mathbb{P}^2$) given by the Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{1}$$

with $a_i \in K$ and with the point O corresponding to $[0:1:0]$. Moreover curve given by such an equation is an elliptic curve. In the case of $char(K) \neq 2, 3$ the equation above simplifies further and can be written in the form

$$Y^2 = 4X^3 + AX + B. \tag{2}$$

One defines also the two quantities

$$\Delta = -16(4A^3 + 27B^2) \text{ and } j = -1728\frac{(4A)^3}{\Delta}.$$

One has the following

Theorem 0.1.2. *a) A curve given by the equation (2)*

(i) is nonsingular (and so an elliptic curve) if and only if $\Delta \neq 0$;

(ii) has a node if and only if $\Delta = 0$ and $A \neq 0$;

(iii) has a cusp if and only if $\Delta = A = 0$.

b) Two elliptic curves are isomorphic over $\bar{K}$ if and only if they have the same j-invariant.

c) Given $j_0 \in \bar{K}$ there exists an elliptic curve defined over $K(j_0)$ whose j-invariant is equal to j_0.

Proof. See [Sil09] proposition 1.4, chapter III. □

Using the characterization above, one defines, geometrically, a group law on E in the following way:

> if $P, Q \in E$, we consider L to be the line through P and Q, if $P = Q$ we consider the tangent line to E in P. Let R be the third point of intersection of L with E. We define $P + Q$ to be the third point of intersection of the line through O and R with E.

This operation turns E into a commutative algebraic hroup with identity element given by O and inverse denoted by $-$. Indeed one can prove the following:

Theorem 0.1.3. *Let E/K be an elliptic curve. Writing explicit equations for the group law above defined, one gets:*

$$\begin{aligned} +\,&: E \times E \to E \qquad \text{and} \quad -\,: E \to E \\ &(P, Q) \mapsto P + Q \qquad\qquad P \mapsto -P. \end{aligned}$$

These maps define two morphisms.

Proof. See [Sil09] theorem 3.6, chapter III. □

One next defines which are the maps between elliptic curves.

Definition 0.1.4. If E_1, E_2 are two elliptic curves, an *isogeny* from E_1 to E_2 is a morphism $\varphi : E_1 \to E_2$ such that $\varphi(O) = O$.

Definition 0.1.5. If E is an elliptic curve, we define the endomorphism ring $\mathrm{End}(E)$ of E to be the ring of all isogenies from E to E.

Using then the group isomorphism between an elliptic curve E and the group of degree zero divisors on E modulo principal divisors

$$\begin{aligned} E &\xrightarrow{\simeq} \mathrm{Pic}^0(E) \\ P &\mapsto [P - O], \end{aligned}$$

one gets the following

Theorem 0.1.6. *An isogeny defines a group homomorphism with respect to the group law on the elliptic curves. Concretely, if $\varphi : E_1 \to E_2$ is an isogeny, then*

$$\varphi(P + Q) = \varphi(P) + \varphi(Q) \quad \textit{for all } P, Q \in E_1.$$

Proof. If φ is the zero-isogeny there is nothing to prove. If φ is not the zero-isogeny, we can use the fact that φ is a finite map, we get a homomorphism

$$\begin{aligned} \varphi_* &: \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2) \\ &[\sum n_i P_i] \mapsto [\sum n_i \varphi(P_i)]. \end{aligned}$$

Using $\varphi(O) = O$ we get a commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\simeq} & \mathrm{Pic}^0(E_1) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi_*} \\ E_2 & \xrightarrow{\simeq} & \mathrm{Pic}^0(E_2), \end{array}$$

where the horizontal maps are defined as we have just seen. Since these two and φ_* are group homomorphism and the lower arrow is injective, we get that φ is a group homomorphism. □

Example 0.1.7. For each $m \in \mathbb{Z}$ one can define the multiplication by m isogeny by setting, if $m > 0$

$$\begin{aligned}[m] :& E \to E \\ & P \mapsto \underbrace{P + P + \cdots + P}_{m\text{-times}}\end{aligned}$$

and if $m < 0$ we simply set $[m](P) = [-m](-P)$. Clearly if $m = 0$ we define $[0]$ to be the zero-isogeny.

We also define the m-torsion subgroup of E to be the kernel of this isongeny, i.e.

$$E[m] := \{P \in E \text{ s.t. } [m](P) = O\},$$

one can prove that if $char(K) = 0$ or $p = char(K) \not| m$, then $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. See [Sil09] corollary 6.4, chapter III.

Using the above example, we can define an injective map

$$\begin{aligned}[\ ] :& \mathbb{Z} \to \mathrm{End}(E) \\ & m \mapsto [m].\end{aligned}$$

One can then prove the following

Theorem 0.1.8. *The endomorphism ring of an elliptic curve E/K is either $\mathbb{Z}$, or an order in an imaginary quadratic field, or an order in a quaternion algebra. If $char(K) = 0$, only the first two cases are possible.*

Proof. See [Sil09] corollary 9.4, chapter III. □

We will be interested in the case $char(K) = 0$ and we will see how to prove this theorem in the easier case of $K = \mathbb{C}$. We say that

Definition 0.1.9. E/K has CM by a quadratic imaginary field L if its endomorphism ring is strictly larger than $\mathbb{Z}$ and it is an order in L.

Another object which will be useful is the invariant differential or Néron differential of an elliptic curve E/K. It is the canonical choice of a generator for Ω_E which has some nice properties that we recall now briefly.

Definition 0.1.10. Let E/K defined by the equation (1). *The invariant differential or Néron differential* of E is

$$\omega_E = \frac{dx}{2y + a_1 x + a_3}.$$

It is called *invariant differential* in light of the following

Proposition 0.1.11. *For every $Q \in E$, let $\tau_Q : E \to E$ be the translation by Q map. Then*

$$\tau_Q^* \omega_E = \omega_E.$$

Proof. See [Sil09] proposition 5.1, chapter III. □

Moreover we have

Theorem 0.1.12. *Let E and E' be elliptic curves and $\varphi, \phi : E' \to E$ two isogenies. Then*

$$(\varphi + \phi)^* \omega_E = \varphi^* \omega_E + \phi^* \omega_E.$$

Proof. See [Sil09] theorem 5.2, chapter III. □

As corollary from this, one gets that $[m]^* \omega_E = m\omega_E$ for every $m \in \mathbb{Z}$.

0.1.1 Elliptic curves over $\mathbb{C}$

The theory of elliptic curves over the field of complex numbers $\mathbb{C}$ becomes much easier, since it is equivalent (in a categorial sense) to the one of lattices in $\mathbb{C}$ or, equivalently again, to the one of complex tori. We recall briefly how this works, for a more detailed analysis see [Sil09], chapter VI.

Consider Λ a lattice in $\mathbb{C}$ and $\mathbb{C}/\Lambda$ the corresponding complex torus. It is a complex Lie group. What one shows is that it is isomorphic, as complex Lie group, to an elliptic curve $E/\mathbb{C}$. To do this we need the following

Definition 0.1.13. The *Eisenstein series of weight 2k* associated to Λ is

$$G_{2k}(\Lambda) = \sum_{0 \neq \omega \in \Lambda} \omega^{-2k}.$$

The *Weierstrass $\wp$-function* associated to Λ is

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

One can prove that G_{2k} is absolutely convergent for $k > 1$ and that $\wp$ is an even elliptic function with a double pole with residue 0 at each lattice point and no other poles. Moreover for every $z \in \mathbb{Z} \setminus \Lambda$, $\wp$ and its derivative $\wp'$ satisfy the relation

$$\wp'(z)^2 = \wp(z)^3 - 60G_4(\Lambda)\wp(z) - 140G_6(\Lambda). \tag{3}$$

After defining $g_2 = g_2(\Lambda) := 60G_4(\Lambda)$ and $g_3 = g_3(\Lambda) := 140G_6(\Lambda)$, using the properties of the Weierstrass $\wp$-function associated to Λ, one can prove the following key result:

Theorem 0.1.14. *With the previous notation $\Delta(\Lambda) := g_2^3 - 27g_3^2$ is non zero thus*

$$E : y^2 = 4x^2 - g_2 x - g_3$$

is an elliptic curve over $\mathbb{C}$. Moreover the map

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\mapsto [\wp(z) : \wp'(z) : 1] \end{aligned}$$

defines an isomorphism of complex Lie groups.

Proof. See [Sil09] proposition 3.6, chapter VI. □

To proceed, one consider then two lattices Λ_1, Λ_2 and the elliptic curves E_1, E_2 associated to the complex tori $\mathbb{C}/\Lambda_1$, $\mathbb{C}/\Lambda_2$, in the sense of the previous theorem. Every $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$ gives rise to a well defined holomorphic map

$$\begin{aligned} \phi_\alpha : \mathbb{C}/\Lambda_1 &\to \mathbb{C}/\Lambda_2 \\ z &\mapsto \alpha z \end{aligned}$$

Using this association and the previous theorem one gets the following

Theorem 0.1.15. *There are bijections*

$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \longleftrightarrow \left\{ \begin{array}{l} \textit{holomorphic maps} \\ \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ \textit{such that } \phi(0) = 0 \end{array} \right\} \longleftrightarrow \{\textit{isogenies } \phi : E_1 \to E_2\},$$

where the first bijection assigns, with the above notation, $\alpha \mapsto \phi_\alpha$ *and the second one is induced by the isomorphism defined in the previous theorem.*

Proof. See [Sil09] theorem 4.1, chapter VI. □

A natural question which arises at this point is whether every elliptic curve over $\mathbb{C}$ is isomorphic to a complex torus or not. In other words, starting from an elliptic curve given by the equation (2), can we find a lattice Λ such that $g_2(\Lambda) = -A$ and $g_3(\Lambda) = -B$ so that $\mathbb{C}/\Lambda$ and E are isomorphic as complex Lie groups? The answer is positive and moreover this lattice is unique up to homothety. This follows by the Uniformization Theorem, which can be proved using the theory of modular forms, that we will see later.

Theorem 0.1.16 (Uniformization theorem)**.** *For every* $A, B \in \mathbb{C}$ *such that* $4A^3 - 27B^2 \neq 0$*, there exists a unique lattice* $\Lambda \subset \mathbb{C}$ *such that* $g_2(\Lambda) = -A$ *and* $g_3(\Lambda) = -B$*.*

This way we obtain what we were saying at the beginning of this discussion: the category of elliptic curve over $\mathbb{C}$, with morphisms given by the isogenies, and the category of complex tori of dimension 1, with morphisms complex analytic maps sending 0 to 0, are equivalent. In particular for $E/\mathbb{C}$ isomorphic to $\mathbb{C}/\Lambda$ we have

$$\mathrm{End}(A) \simeq \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}.$$

Going back to the definition of complex multiplication and using the above results, we can now prove theorem 0.1.8 in the case of elliptic curves over $\mathbb{C}$.

Theorem 0.1.17. *Let* $E/\mathbb{C}$ *be an elliptic curve and* $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ *be the corresponding lattice. Then one of the following is true*

i) $\mathrm{End}(E) \simeq \mathbb{Z}$*,*

ii) The field $K := \mathbb{Q}(\omega_1/\omega_2)$ *is an imaginary quadratic field and* $\mathrm{End}(E)$ *is isomorphic to an order in* K*.*

Proof. Let $\tau := \omega_1/\omega_2$ and suppose it is in $\mathfrak{H}$, the complex upper half plane (ω_1, ω_2 are a $\mathbb{R}$-basis of $\mathbb{C}$, so either ω_1/ω_2 or ω_2/ω_1 are in $\mathfrak{H}$). Multiplying Λ by $1/\omega_1$ we get that Λ is homothetic to $\mathbb{Z} \oplus \mathbb{Z}\tau$, so we can replace Λ by $\mathbb{Z} \oplus \mathbb{Z}\tau$. Let $A = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$. Take $\alpha \in A$, then there exist integers a, b, c, d such that $\alpha = a + b\tau, \alpha\tau = c + d\tau$. This means that α is an eigenvalue for the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

(with respect to the eigenvector $(1, \tau)$). So it satisfies its characteristic polynomial, which is a monic polynomial with coefficients in $\mathbb{Z}$, hence α is integral over $\mathbb{Z}$ and $A \supset \mathbb{Z}$ is integral. If $A \supsetneq \mathbb{Z}$, take $\alpha \in A \setminus \mathbb{Z}$, write it as before (now with $b \neq 0$) . Substituting $\alpha = a + b\tau$ in $\alpha\tau = c + d\tau$ we get

$$b\tau^2 - (a - d)\tau + c = 0.$$

So $K = \mathbb{Q}(\tau)$ is a quadratic extension of $\mathbb{Q}$ and it is imaginary (otherwise $\tau \in \mathbb{R}$). Since $\mathcal{O}_K$, the ring of integers of K, is free as $\mathbb{Z}$ module and A is a $\mathbb{Z}$-submodule of $\mathcal{O}_K$, A is also free and of rank 2 (containing strictly $\mathbb{Z}$), so we are done. □

0.1.2 Elliptic curves over finite fields

Consider now an elliptic curve E/K, where K is a field of characteristic p (suppose $p \neq 2, 3$). We can define the curve $E^{(q)}/K$ by raising all the coefficients of the equation for E to the q-th power. Using theorem 0.1.2 and the fact that $\Delta(E^{(q)}) = \Delta(E)^q$, we have that $E^{(q)}/K$ is again an elliptic curve over K.

We are now interested in the case $K = \mathbb{F}_q$ the finite field with $q = p^r$ elements. In this case clearly $E^{(q)} = E$ and we can then define the endomorphism of E

$$\pi_q : [x : y : z] \mapsto [x^q : y^q : z^q] \tag{4}$$

Definition 0.1.18. The endomorphism given by (4) is called the *Frobenius endomorphism* of E.

Remark 0.1.19. Notice that the set of points fixed by π_q is exactly $E(\mathbb{F}_q)$.

Using the previous remark and some properties of the Frobenius endomorphism, one proves

Theorem 0.1.20 (Hasse)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve over the finite field $\mathbb{F}_q$, then*

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

Proof. See [Sil09] theorem 1.1, chapter V. □

Being in characteristic different from zero it can happen that the endomorphism ring of an elliptic curve $E/\mathbb{F}_q$ is neither $\mathbb{Z}$ nor an order in a quadratic imaginary field, i.e. it is an order in a quaternion algebra. This is a quite unusual and rare case, which is the reason of the use of the word *supersingular* in the following definition.

Definition 0.1.21. An elliptic curve $E/\mathbb{F}_q$ is called *supersingular* if its endomorphism ring is an order in a quaternion algebra.

For a more detailed discussion we refer to [Sil09], V.3-V.4. We restrict ourself to state a couple of theorems. The first one clarifies what we meant by saying that such elliptic curves are rare.

Theorem 0.1.22. *Fix a finite field $\mathbb{F}_q$ of characteristic p. There is only a finite number of supersingular elliptic curves (up to $\bar{\mathbb{F}}_q$-isomorphism).*

Proof. This descends from [Sil09], theorem 4.1.c, chapter V. □

Theorem 0.1.23. *Let $\mathbb{F}_q$ be a finite field of characteristic p and $E/\mathbb{F}_q$ an elliptic curve which is not supersingular. Then for every $r \geq 1$*

$$E[p^r] = \mathbb{Z}/p^r\mathbb{Z}.$$

Proof. See [Sil09], theorem 3.1, chapter V. □

0.1.3 A general definition

Following [Kat72], chapter 1, we now give a more general definition of elliptic curve over a scheme S, that will be useful later.

Definition 0.1.24. An *elliptic curve over a scheme* S is the datum of a proper smooth morphism $\pi : E \to S$, whose geometric fibres are connected curves of genus 1, together with a section $s : S \to E$.

Remark 0.1.25. Notice that taking $S = \mathrm{Spec}(K)$, for K a field, we get back our definition of elliptic curve over K. Indeed, since $\mathrm{Spec}(K)$ consists in a point, E is the only geometric fibre of $\pi : E \to \mathrm{Spec}(K)$ and it is a connected smooth curve of genus 1. Moreover the section corresponds to the K-point O of our previous definition.

0.1.4 Reduction modulo a prime

For this section we consider E an elliptic curve over a number field K. We start by using the language of (0.1.3) since it makes everything easier. Let $\mathcal{O}_K$ be the ring of integers of K, $\mathfrak{p}$ a prime ideal and $v = v_{\mathfrak{p}}$ the associated valuation. Consider K_v the completion of K at v. In particular E is an elliptic curve over K_v. K_v is a local field with ring of integers $\mathcal{O}_v$, a DVR with maximal ideal $\mathfrak{m}_v = (\pi_v)$ and residue field $k_v = \mathcal{O}_v/\mathfrak{m}_v$.

Definition 0.1.26. An elliptic curve as above *has good reduction at* $\mathfrak{p}$ if there exists an elliptic curve E' over $\mathrm{Spec}(\mathcal{O}_v)$ such that the fibre over the generic point is isomorphic to E (over $\mathrm{Spec}(K_v)$), so that we have the following cartesian diagram

$$\begin{array}{ccc} E & \longrightarrow & E' \\ \downarrow & & \downarrow \\ \mathrm{Spec}(K_v) & \longrightarrow & \mathrm{Spec}(\mathcal{O}_v). \end{array}$$

We denote with $\tilde{E}$ the fibre over the special point; $\tilde{E}$ is an elliptic curve over the finite field k_v, since the base change of a proper smooth morphism is again proper and smooth.

In this case we get a map, called the reduction map, from the the K_v-points of E to the k_v-points of $\tilde{E}$. Indeed to $\varphi : \mathrm{Spec}(K_v) \to E \in E(K_v)$ we can associate a morphism $\varphi' : \mathrm{Spec}(K_v) \to \tilde{E}$ so that we get the following commutative diagram

$$\begin{array}{ccc} \mathrm{Spec}(K_v) & \xrightarrow{\varphi'} & \tilde{E} \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathcal{O}_v) & \longrightarrow & \mathrm{Spec}(k_v). \end{array}$$

Since the right arrow is proper for the assumption of good reduction, the valuative criterion tells us that there exists a unique lift of φ' to $\mathrm{Spec}(\mathcal{O}_K)$. Then

$$\tilde{\varphi} : \mathrm{Spec}(k_v) \to \mathrm{Spec}(\mathcal{O}_v) \xrightarrow{\varphi'} \tilde{E}$$

gives us the desired k_v-point of $\tilde{E}$. We denote with

$$red : E(K_v) \to \tilde{E}(k_v)$$

the map which associates $\tilde{\varphi}$ to φ. Notice that we can restrict it to a map $E(K) \to \tilde{E}(k_v)$.

Remark 0.1.27. Following [Sil09], chapter VII.2-3, the same operation can be done in a more *concrete* way by considering a Weierstrass equation for E/K. One then can reduce, by multiplying for sufficiently large power of π_v, to have such an equation defined over $\mathcal{O}_v$. The minimal Weiestrass equation for E at v is the one for which $v(\Delta)$ is the minimum with respect to the condition of the coefficients being in $\mathcal{O}_v$. Assume that E is given by this equation. The $\tilde{E}$ of above is given by the curve over k_v whose coefficients are the reduction modulo $\mathfrak{m}_v$ of the coefficients of E. One then sees that E has good reduction modulo $\mathfrak{p}$ if and only if $v(\Delta) \neq 0$. By this one can also see that E has good reduction at $\mathfrak{p}$ for all but finitely many $\mathfrak{p}$. We say that E has *multiplicative* reduction if $\tilde{E}$ has a node, *additive* reduction if it has a cusp. Moreover, in the case of good reduction, the reduction map is given by noticing that every $P = [x : y : z] \in E(K_v)$ can be taken with coordinates in $\mathcal{O}_v$ and almost one coordinate in $\mathcal{O}_v^\times$. Then one take the reduction modulo $\mathfrak{m}_v$ of every coordinate and get $\tilde{P} = [\tilde{x} : \tilde{y} : \tilde{z}] \in \tilde{E}(k_v)$.

If $\mathfrak{p}$ is a prime lying above the rational prime p and of residual degree f, the field k_v is a finite field of cardinality p^f. If E/K has good reduction at $\mathfrak{p}$, one can then ask if the reduction modulo $\mathfrak{p}$ of E is supersingular or not. With the previous notation we give the following

Definition 0.1.28. An elliptic curve E/K is said to be *supersingular at* $\mathfrak{p}$ if $\tilde{E}$ is supersingular. Otherwise it is said to be *ordinary at* $\mathfrak{p}$.

In the case of elliptic curves with CM the answer to our problem is given by the following

Theorem 0.1.29. *Let E be an elliptic curve over the number field K such that it has complex multiplication by L a quadratic imaginary field. Suppose that E has good reduction at $\mathfrak{p}$, a prime of K lying above p. Then*

$$E \text{ is ordinary at } \mathfrak{p} \Leftrightarrow p \text{ splits completely in } L.$$

Proof. See [Lan87], theorem 12, chapter 13, §4. □

0.2 The formal group logarithm

In this section we recall briefly how to associate to an elliptic curve over a local field a formal group and a formal logarithm, following [Sil09] chapter IV. The case we will be interested in later will be the one of an elliptic curve over $\mathbb{Q}$. As before, we can view it as an elliptic curve over $\mathbb{Q}_p$, the field of p-adic numbers, for every p prime and then use this theory.

We start with general definitions and properties.

Definition 0.2.1. A *formal group $\mathcal{F}$ over a ring R* is a power series $F(X, Y) \in R[[X, Y]]$ such that

(a) $F(X, Y) = X + Y +$ (terms of degree ≥ 2);

(b) (associativity) $F(X, F(Y, Z)) = F(F(X, Y), Z)$;

(c) (commutativity) $F(X, Y) = F(Y, X)$;

(d) (inverse) there is a unique $i(T) \in R[[T]]$ such that $F(T, i(T)) = 0$;

(e) $F(X, 0) = X$ and $F(0, Y) = Y$.

$F(X,Y)$ is the *formal group law of* $\mathcal{F}$.

Definition 0.2.2. If $(\mathcal{F},F)$ and $(\mathcal{G},G)$ are two formal groups defined over R, a *homomorphism from* $\mathcal{F}$ *to* $\mathcal{G}$ defined over R is a power series $f \in R[[T]]$ such that $f(F(X,Y)) = G(f(X),f(Y))$.

Definition 0.2.3. An *invariant differential* on a formal group $\mathcal{F}$ over R is a differential form $\omega(T)dT \in R[[T]]dT$ such that $\omega(F(T,S)) = \omega(T)$.

The condition in the above definition tells us that the power series defining an invariant differential satisfies $P(F(T,S))F_X(T,S) = P(T)$, where F_X is the partial derivative of F with respect to X. It is *normalized* if $P(0) = 1$. Then one can show that there exists a unique normalized differential on $\mathcal{F}/R$ and it is given by $\omega = F_X(0,T)^{-1}dT$. Every invariant differential is of the form $a\omega$ for $a \in R$.

Example 0.2.4. The easiest example is the one of the *formal additive group*, denoted by $\hat{\mathbb{G}}_a$, defined by $F(X,Y) = X + Y$. In this case the invariant differential is $\omega = dT$.

Now we proceed with the definition of the formal logarithm.

Definition 0.2.5. Let R be a torsion-free ring and $K = R \otimes \mathbb{Q}$. If $\mathcal{F}/R$ is a formal group and $\omega(T) = (1 + c_1T + c_2T^2 + \dots)dT$ is the normalized invariant differential, the *formal logarithm of* $\mathcal{F}/R$ is the power series

$$log_{\mathcal{F}}(T) = \int \omega(T) = T + \frac{c_1}{2}T^2 + \frac{c_2}{3}T^3 + \cdots \in K[[T]].$$

Remark 0.2.6. Notice that one can also define the formal logarithm associated to a *non-normalized* differential in a similar way, writing $log_{\omega(T)} = \int \omega(T)$. One chooses the normalized one so that the power series admits an inverse in $R[[T]]$, since the coefficient of T is invertible. We call *formal exponential of* $\mathcal{F}/R$ the unique power series $exp_{\mathcal{F}}(T) \in R[[T]]$ such that

$$log_{\mathcal{F}}(exp_{\mathcal{F}}(T)) = exp_{\mathcal{F}}(log_{\mathcal{F}}(T)) = T.$$

An easy fact that follows right from the definition is the following

Proposition 0.2.7. *Let* $\mathcal{F}$ *and* $\mathcal{G}$ *be two formal groups over* R *and* f *a formal group homomorphism. If* ω *is the normalized invariant differential of* $\mathcal{G}$ *we have*

$$log_{f^*\omega}(T) = log_{\omega}(f(T)),$$

where $f^*\omega(T) = \omega(f(T))$.

Proof. We just write $log_{f^*\omega}(T) = \int \omega(f(T)) = log_{\omega}(f(T))$. □

Proposition 0.2.8. *If* R *is a torsion-free ring and* $\mathcal{F}/R$ *is a formal group. Then*

$$log_{\mathcal{F}} : \mathcal{F} \to \hat{\mathbb{G}}_a$$

is an isomorphism of formal groups over $K = R \otimes \mathbb{Q}$.

Proof. Let $\omega(T)$ be the normalized invariant differential so that $\omega(F(T,S)) = \omega(T)$. Integrating with respect to T gives us $log_{\mathcal{F}}F(T,S) = \log_{\mathcal{F}}(T) + C(S)$ for some $C(S) \in K[[S]]$. Taking $T = 0$ gives us $C(S) = \log_{\mathcal{F}}(S)$ so that $log_{\mathcal{F}}$ is a homomorphism (recall the definition of the formal group $\hat{\mathbb{G}}_a$ from example 0.2.4). Moreover there exists an inverse, $\exp_{\mathcal{F}}$, so it is an isomorphism of formal groups. □

Remark 0.2.9. One can associate to a formal group a group, in the case in which R is a complete local ring. We will be interested in the case of $R = \mathcal{O}_v$ so that $\mathrm{Frac}(R) = R \otimes \mathbb{Q} = K_v$ is the completion of a number field with respect to the valuation v. To associate a group to $\mathcal{F}/R$, one considers the set $\mathfrak{m}$, the maximal ideal of R, with the group operations

$$\begin{aligned} x +_{\mathcal{F}} y &= F(x, y) \\ -_{\mathcal{F}} x &= i(x) \end{aligned}$$

for $x, y \in \mathfrak{m}$. Since R is a complete ring, the power series $F(x, y), i(x)$ converge in R. In the case of $\mathcal{F} = \hat{\mathbb{G}}_a$, the associated group is simply $\mathfrak{m}$ with the usual group law.

The formal group of an elliptic curve. Let E/K be an elliptic curve. We want to associate to it a formal group and, consequently a formal logarithm. The idea is to investigate its structure and the group law close to the origin. Let (x, y) be the affine coordinates of E. We make a change of variables

$$z = -x/y \text{ and } w = -1/y, \tag{5}$$

so that the origin O of E is now the point $(0, 0)$. Now the Weierstrass equation for E gets the form

$$w = f(z, w) \in K[z, w].$$

By substituting this equation into itself one gets a power series in z of the form

$$w(z) = z^3(1 + A_1 z + A_2 z^2 + \dots) \in K[[z]].$$

This can be done thanks to the Hensel lemma applied to the complete ring $K[[z]]$ to find a solution of $F(w) = f(z, w) - w$, so that the power series above is the unique one satisfying $w(z) = f(z, w(z))$. Then using (5) one can derive the Laurent series $x(z), y(z) \in K((z))$. If we further assume that E has equation whose coefficients are in R, the ring of integers of a local field K, we get an injective map

$$\begin{aligned} \mathfrak{m} &\to E(K) \\ z &\mapsto (x(z), y(z)), \end{aligned}$$

since the power series $x(z), y(z)$ converge for any $z \in \mathfrak{m}$, the maximal ideal of R. The image of this map is given by the points (x, y) with $x^{-1} \in \mathfrak{m}$.

Finally one finds the power series formally giving the addition law on E by following the definition, i.e. by considering the line between two points $(z_1, w(z_1)), (z_2, w(z_2))$, taking the intersection with E, and so on. Similarly for the inverse. For a more detailed discussion see [Sil09], IV.1. So one gets two power series

$$F(z_1, z_2) \in K[[z_1, z_2]] \text{ and } i(z) \in K[[z]]$$

giving the formal addition law and the formal inverse. From the properties of the addition law on E one gets

$$\begin{aligned} F(z_1, z_2) &= F(z_2, z_1) \\ F(z_1, F(z_2, z_3)) &= F(F(z_1, z_2), z_3) \\ F(z, i(z)) &= F(i(z), z). \end{aligned}$$

The explicit equation for F and some computations show that F satisfies also the remaining properties of definition 0.2.1. We denote with $\hat{E}$ the formal group associated to E, which is defined over R, if the coefficients defining E are in R.

Moreover, if we consider the expansion of the invariant differential for E we get that $\omega(z) \in K[[z]]dz$ is the formal normalized invariant differential, so that we can associate to E/K the formal logarithm $log_{\hat{E}}$. In particular we will be interested in considering an elliptic curve $E/\mathbb{Q}$. For every prime p it is in particular an elliptic curve over $\mathbb{Q}_p$. Assuming that the coefficients of its equation are in $R = \mathbb{Z}_p$ the ring of p-adic integers, we get a map as above

$$p\mathbb{Z}_p \to E(\mathbb{Q}_p),$$

with an inverse defined on the points whose first coordinate has p-adic norm strictly bigger than 1. On such points we then define

$$\log_p : P \mapsto \log_p(P) \in \mathbb{Q}_p,$$

using the inverse given above and the formal logarithm associated to the normalized invariant differential of $\hat{E}$ seen as formal group over $\mathbb{Z}_p$. Using proposition 0.2.8 and remark 0.2.9 we get that $\log_p$ is an isomorphism to $\mathbb{Q}_p$.

The formal group associated to an elliptic curve is very useful to prove some properties of the elliptic curve itself. One can for example prove that the group associated to the formal group $\hat{E}$ with respect to $\mathbb{Z}_p$ is isomorphic to the kernel of the reduction modulo p map defined above and get the following important exact sequence

$$0 \to \hat{E}(p\mathbb{Z}_p) \to E(\mathbb{Q}_p) \xrightarrow{red_p} \tilde{E}(\mathbb{F}_p) \to 0.$$

0.3 Main theorem of Complex Multiplication

We briefly state here the main theorem of complex multiplication for elliptic curves as presented in chapter V of [Shi71] and list the most interesting consequences.

Before starting we need to define the *multiplication* of a $\mathbb{Z}$-lattice in a quadratic imaginary field K by an idèle $x \in \mathbb{A}_K^\times$. If $\mathfrak{a} \subset K$ is a $\mathbb{Z}$-lattice, one has that, for p a rational prime, $\mathfrak{a}_p := \mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Z}_p \subset K_p = K \otimes_{\mathbb{Q}} \mathbb{Q}$ is a $\mathbb{Z}_p$-lattice and $\mathfrak{a}$ is *determined by the* $\mathfrak{a}_p$'s, in the sense that $\mathfrak{a} = \mathfrak{b}$ if and only if $\mathfrak{a}_p = \mathfrak{b}_p$ for every p. Moreover we have the following

Lemma 0.3.1. *Given two lattices $\mathfrak{a}, \mathfrak{b}$, one has $\mathfrak{a}_p = \mathfrak{b}_p$ for almost all p. Conversely if $\mathfrak{a}$ is a lattice as above and for every prime p we are given a $\mathbb{Z}_p$-lattice $\mathfrak{c}_p$ such that $\mathfrak{a}_p = \mathfrak{c}_p$ for almost all p, then there exists a unique lattice $\mathfrak{b}$ such that $\mathfrak{b}_p = \mathfrak{c}_p$ for every p.*

Using $\mathbb{A}_K^\times = K \otimes \mathbb{A}_{\mathbb{Q}}^\times$ we can talk about the p-th component of $x \in \mathbb{A}_K^\times$, we denote it with $x_p \in K_p^\times$. Since $\mathfrak{a}_p = x_p\mathfrak{a}_p$ for almost all p, we can use the conversely part of the above lemma to show that there exists a unique lattice, denoted with $x\mathfrak{a}$, such that $(x\mathfrak{a})_p = x_p\mathfrak{a}_p$ for every p. Finally using the isomorphisms $K/\mathfrak{a} \simeq \bigoplus_p K_p/\mathfrak{a}_p$ and $K/x\mathfrak{a} \simeq \bigoplus_p K_p/x_p\mathfrak{a}_p$, we have a well defined isomorphism

$$K/\mathfrak{a} \xrightarrow{\cdot x} K/x\mathfrak{a}.$$

We also recall that class field theory gives us a surjective map

$$\begin{aligned} rec: \ & \mathbb{A}_K^\times \to Gal(K^{ab}/K) \\ & s \mapsto [s, K], \end{aligned}$$

where K^{ab} is the maximal abelian extension of K.

Theorem 0.3.2 (Main theorem of complex multiplication). *Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by an order $\mathcal{O}$ in K and denote with $\mathfrak{a}$ the $\mathbb{Z}$-lattice in K such that we have in isomorphism $\xi : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$. Let $\sigma \in Aut(\mathbb{C}/K)$ and $s \in \mathbb{A}_K^\times$ such that $[s, K] = \sigma_{|K^{ab}}$. Then there exists a unique isomorphism $\xi' : \mathbb{C}/s^{-1}\mathfrak{a} \to E^\sigma(\mathbb{C})$ such that the following diagram commutes*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\xi} & E_{tors}(\mathbb{C}) \\ \downarrow{\scriptstyle \cdot s^{-1}} & & \downarrow{\scriptstyle \sigma} \\ K/s^{-1}\mathfrak{a} & \xrightarrow{\xi'} & E^\sigma_{tors}(\mathbb{C}). \end{array}$$

One of the most interesting applications of this theorem is the description of the class fields of a quadratic imaginary field K. We sum up these results in the two following theorems.

Theorem 0.3.3. *Let $\mathcal{O}$ be an order in a quadratic imaginary field K. If $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal, we denote with $j(\mathfrak{a})$ the j-invariant of elliptic curve $\mathbb{C}/\mathfrak{a}$. Then we have*

(i) $Gal(K(j(\mathfrak{a}))/K)$ is isomorphic to $\mathrm{Pic}(\mathcal{O})$ and if σ corresponds to the class of the ideal $\mathfrak{b}$, $j(\mathfrak{a})^\sigma = j(\mathfrak{b}^{-1}\mathfrak{a})$.

(ii) If $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ are a complete set of representatives for $\mathrm{Pic}(\mathcal{O})$, then $j(\mathfrak{a}_1), \dots, j(\mathfrak{a}_n)$ is a complete set of conjugates of $j(\mathfrak{a})$ over $\mathbb{Q}$ and over K.

Theorem 0.3.4. *If K is a quadratic imaginary field, let E be any elliptic curve with complex multiplication my the maximal order in K, so that $E \simeq \mathbb{C}/\mathfrak{a}$, for some fractional ideal $\mathfrak{a}$. Then*

1) the ray class field K_m of conductor m is $K_m = K(j(\mathfrak{a}), E[m])$. In particular the Hilbert class field H_K is $H_K = K(j(\mathfrak{a}))$.

2) $K^{ab} = K(j(\mathfrak{a}), E_{tors})$.

Moreover, if $\mathcal{O}$ is the order of conductor $m \in \mathbb{Z}$, we also have that $K_m = K(j(\mathcal{O}))$.

Remark 0.3.5. Recall that H_K is the maximal unramified abelian extension of K and that the Artin map gives an isomorphism

$$\begin{aligned} Art : \mathrm{Pic}(\mathcal{O}_K) &\to Gal(H_K/K) \\ [\mathfrak{b}] &\mapsto \left(\frac{H_K/K}{\mathfrak{b}}\right). \end{aligned}$$

We can now say more: if the class of $\mathfrak{b}$ is equal to $Art^{-1}(\sigma)$, i.e. $\sigma = \left(\frac{H_K/K}{\mathfrak{b}}\right)$, then we have $j(\mathfrak{a})^\sigma = j(\mathfrak{b}^{-1}\mathfrak{a})$.

0.4 The L-function of an elliptic curve over $\mathbb{Q}$

Following [Dar04], chapter 1.4, we give the definition of the L-function associated to an elliptic curve over $\mathbb{Q}$.

Let $E/\mathbb{Q}$ be an elliptic curve. We have seen that for every prime p we can look at the reduction of E modulo p. Following the notation of remark 0.1.27, when E has bad reduction at p we have two cases: $\tilde{E}$ has a cusp (*additive* reduction) or it has a node (*multiplicative* reduction). In the second case we further distinguish two cases: if $\tilde{E}$ has a node and the

tangent lines in the node have rational coefficients we say that E has *split multiplicative* reduction at p, otherwise it has *non-split multiplicative* reduction at p.

The next step is to define an integer a_p for every prime p. We do it in the following way:

$$a_p = \begin{cases} 0 & \text{if } E \text{ has additive reduction at } p \\ 1 & \text{if } E \text{ has split multiplicative reduction at } p \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p \\ -N_p + p + 1 & \text{if } E \text{ has good reduction at } p, \end{cases}$$

where $N_p = \#\tilde{E}(\mathbb{F}_p)$ in the case of good reduction.

We make the extra assumption that for $p = 2$ or 3 E has not additive reduction at p, to semplify the following

Definition 0.4.1. The *conductor* N of the elliptic curve E is defined by $N := \prod_p p^{ord_p(N)}$, where

$$a_p = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has multiplicative reduction at } p \\ 2 & \text{otherwise.} \end{cases}$$

Finally the L-function of E is defined by

$$L(E,s) = \sum a_n n^{-s} := \prod_{p \not| N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N} (1 - a_p p^{-s})^{-1}.$$

Theorem 0.4.2. *The L-series above defined converges absolutely in the right half-plane* $Re(s) > 3/2$.

Proof. We need to prove the convergence of the infinite product

$$\prod_{p \text{ of good red}} (1 - a_p p^{-s} + p^{1-2s}),$$

since $L(E,s)$ is obtained by multiplication of it by a finite product. It converges absolutely if and only if

$$\sum_{p \text{ of good red}} |-a_p p^{-s} + p^{1-2s}| < +\infty.$$

Using theorem 0.1.20 with $q = p$ we get that $|a_p| < 2\sqrt{p}$. Thus

$$\begin{aligned} \sum_{p \text{ of good red}} |-a_p p^{-s} + p^{1-2s}| &\leq \sum_{p \text{ of good red}} 2|p^{-s+\frac{1}{2}}| + |p^{1-2s}| \\ &\leq \sum_{p \text{ prime}} 2|p^{-s+\frac{1}{2}}| + |p^{1-2s}| \leq \sum_{p \text{ prime}} p^{Re(-s+\frac{1}{2})}(1 + 2p^{Re(-s+\frac{1}{2})}) \\ &\leq \sum_{p \text{ prime}} p^{Re(-s+\frac{1}{2})} < \sum_n n^{Re(-s+\frac{1}{2})}, \end{aligned}$$

which converges if $\mathrm{Re}(s) > 3/2$. □

We will see later that, thanks to the work started by A. Wiles, one can prove the following

Theorem 0.4.3. *The L-function $L(E,s)$ extends to an entire function on $\mathbb{C}$ and has a functional equation of the form*

$$\Lambda(E,s) = -\varepsilon_E \Lambda(E, 2-s), \quad \textit{with } \varepsilon_E = \pm 1,$$

where $\Lambda(E,s) := (2\pi)^{-s}\Gamma(s)N^{s/2}L(E,s)$, with $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt$ the usual Γ-function.

Remark 0.4.4. Notice that from the functional equation one gets, deriving n-times,

$$\Lambda^{(n)}(E,s) = (-1)^{n+\frac{\varepsilon+1}{2}}\Lambda^{(n)}(E,2-s).$$

In particular evaluating it in $s=1$, one finds

- if $\varepsilon_E = 1$, $L^{(n)}(E,1) = 0$ for every n even;
- if $\varepsilon_E = -1$, $L^{(n)}(E,1) = 0$ for every n odd.

Hence in the first case $L(E,s)$ vanishes with odd order at 1, in the second with even order. Moreover the Birch and Swinnerton-Dyer conjecture asserts that this order of vanishing (called the *analytic rank*) is equal to the rank of the abelian group $E(\mathbb{Q})$, which is finite thanks to Mordell-Weil theorem.

Chapter 1

Modular Forms, Modularity Theorem and Heegner Points

In this chapter we give an overview of the classical theory of modular forms and p-adic modular forms, following Serre's approach, in particular [Ser73] for the first ones and [Ser72] for the second ones. We also try to understand the more general approach introduced by Katz in [Kat72]. In the final part we connect the theory of modular forms with the one of elliptic curves, illustrating the Modularity Theorem and the construction of Heegner points on an elliptic curve over the rationals.

1.1 Modular forms

We start by fixing some notations. Consider $\mathrm{SL}_2(\mathbb{Z})$, the standard modular group. For every $N \geq 1$ we have the following congruence subgroups

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1, c \equiv 0 \pmod{N} \right\}.$$

They both have finite index in $\mathrm{SL}_2(\mathbb{Z})$. From now on we denote with Γ one of the above groups. One can consider more in general a subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, requiring that it has finite index. We also denote with $\mathfrak{H}$ the complex upper half plane.

Definition 1.1.1. A *weakly modular function of weight $k \in \mathbb{Z}$ with respect to* Γ is a function f such that

(i) f is meromorphic on $\mathfrak{H}$,

(ii) $f(\gamma\tau) = (c\tau + d)^{-k} f(\tau)$, for every $\tau \in \mathfrak{H}$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and where $\gamma\tau = \frac{a\tau+b}{c\tau+d}$.

Remark 1.1.2. Since $\gamma = -I \in \Gamma$ for every Γ, condition (ii) tells us that a modular function of odd weight is identically zero. So we have non trivial modular functions only for k even.

We consider, set-theoretically, $\Gamma \setminus \mathfrak{H}^*$, where $\mathfrak{H}^* = \mathfrak{H} \sqcup \mathbb{P}^1_{\mathbb{Q}} = \mathfrak{H} \sqcup \mathbb{Q} \sqcup \{\infty\}$, and Γ acts on $\mathfrak{H}^*$ in the following way: if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, then

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}, \text{ for } \tau \in \mathfrak{H},$$

$$\gamma[x:y] = [ax+by : cx+dy], \text{ for } [x:y] \in \mathbb{P}^1_{\mathbb{Q}}.$$

We will come back later to this quotient space. We are now interested in the cusps, i.e. in the set $\Gamma \setminus \mathbb{P}^1_{\mathbb{Q}}$. First of all we need to show

Lemma 1.1.3. *The set of cusps is finite.*

Proof. It is easy to see that $\mathrm{SL}_2(\mathbb{Z})\setminus\mathbb{P}^1_{\mathbb{Q}} = \{\infty\}$ and also that Γ is a subgroup of finite index of $\mathrm{SL}_2(\mathbb{Z})$, write $\gamma_1, \ldots, \gamma_m$ for a set of representatives. For every point $P \in \mathbb{P}^1_{\mathbb{Q}}$ take $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma P = \infty$ and γ_i such that $\gamma = \gamma' \cdot \gamma_i$, with $\gamma' \in \Gamma$. So we have $P = \gamma'(\gamma_i\infty)$ and the set of cusps is the set $\{[\gamma_i\infty], i = 1, \ldots, m\}$ and so is finite. □

Now the idea is the following: in the simplest case of $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, a modular function f is invariant by translation for every $n \in \mathbb{Z}$ since $f(\tau+n) = f(\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\tau) = f(\tau)$ for every τ. Thus we can write $f(\tau) = f^*(q)$ with $q = e^{2\pi i\tau}$, in a suitable neighbourhood of $q = 0$. We will require some conditions on f^* in order to define the modular function f to be a modular form.

We want to consider something like the above f^* for every cusp $[s] \in \Gamma \setminus \mathfrak{H}^*$. Take $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma s = \infty$ and let Γ_s be the stabilizer of s in Γ. We have that

$$\gamma \cdot \Gamma_x \cdot \gamma^{-1}\infty = \infty.$$

Since we have that $\gamma\infty = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\infty = \infty$ if and only if $c = 0$ we get that

$$\gamma \cdot \Gamma_x \cdot \gamma^{-1} \subset \{\pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, n \in \mathbb{Z}\}.$$

Let h be the smallest positive integer n occurring in this way, we get

$$\gamma \cdot \Gamma_x \cdot \gamma^{-1} \subset \{\pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m, m \in \mathbb{Z}\}.$$

It is easy to see that this number h is the index of $\gamma \cdot \Gamma_x \cdot \gamma^{-1}$ and it is independent on the choice of the representative s of the cusp.

Taking f as in definition 1.1.1, we define $f_s(\tau) = f(\gamma^{-1}\tau)(c\tau+d)^{-k}$, where $\gamma^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then one can show that f_s is a weakly modular function of weight k with respect to the subgroup $\gamma \cdot \Gamma_x \cdot \gamma^{-1}$. In particular it is invariant with respect to the translation by h and we then have $f_s(\tau) = f_s^*(q^{1/h})$ with $q = e^{2\pi i\tau}$.

Definition 1.1.4. A weakly modular function of weight k with respect to Γ is meromorphic (respectively holomorphic) at a cusp $[s]$ if f_s^* is meromorphic (respectively holomorphic) at 0.

If f satisfies the condition of the above definition, we can then consider the q expansion

$$f_s(\tau) = \sum_{n=r}^{+\infty} a_n q^{n/h}, \tag{1.1}$$

where $r \in \mathbb{Z}$ and, again, $q = e^{2\pi i\tau}$.

We are finally ready to give the definition of modular function and modular form.

Definition 1.1.5. A weakly modular function of weight k with respect to Γ is said to be a *modular function* if it is meromorphic at every cusp; we write $f \in F_k(\Gamma)$. If it is holomorphic on $\mathfrak{H}$ and at every cusp, it is said to be a *modular form*; we write $f \in M_k(\Gamma)$. If moreover it vanishes at every cusp (i.e. $r \geq 1$ in (1.1) for every cusp), then it is said to be a *cusp form*; we write $f \in S_k(\Gamma)$.

Remark 1.1.6. One can replace Γ with any discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ such that $\Gamma \setminus \mathfrak{H}^*$, which has a natural structure of Riemann surface, is compact. Such a Γ is called *Fuchsian group of the first kind*. One defines then in the same way *automorphic functions* and *automorphic form* for Γ, so that for Γ a congruence subgroup we exactly have modular functions and modular forms.

Modular forms on $\mathbf{SL}_2(\mathbb{Z})$. To make some examples, we restrict to the simplest case of modular forms over $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

First of all we state an important theorem. We denote with $ord_\tau f$ the order, as meromorphic function, of the modular function f in τ. Notice that for every $\gamma \in \Gamma$, $ord_\tau f = ord_{\gamma\tau} f$. Moreover the order in ∞ is the order of f^* in 0. We have

Theorem 1.1.7. *Let f be a modular function of weight k, not identically zero. One has:*

$$ord_\infty f + \frac{1}{2} ord_i f + \frac{1}{3} ord_\rho f + \sum_{\tau \in \Gamma \setminus \mathfrak{H}} ord_\tau f = \frac{k}{12},$$

where the last sum is taken over $\tau \neq i, \rho$ and $\rho = e^{2\pi i/3}$.

Proof. See [Ser73] theorem 3, chapter 2, §3. □

Example 1.1.8 (Eisenstein series)**.** The first example is given by

$$G_k(\tau) := \sum_{(m,n) \neq (0,0)} \frac{1}{(m\tau + n)^k},$$

when m, n run over the integers. Then one can prove that this is a modular form of weight k for every $k > 2$ even. Moreover it is not a cusp form as $G_k(\infty) = G_k^*(0) = 2\zeta(k)$, where ζ is the Riemann zeta function. See [Ser73], chapter 2 proposition 4,§2 and proposition 8, §4. One can also prove (see proposition 8, chapter 2,§4) that the q-expansion of G_k is given by

$$G_k(q) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n, \tag{1.2}$$

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

Notice that $G_k(\tau)$ is the Eisenstein series of weight k associated to the lattice $\mathbb{Z} + \mathbb{Z}\tau$ in (0.1.13). And following that notation we define $g_2(\tau) := 60G_4(\tau), g_3(\tau) = 140G_6(\tau)$, which are modular forms of weight 4 and 6 respectively.

Example 1.1.9 (Δ-function)**.** We define

$$\Delta(\tau) := g_2(\tau)^3 - 27 g_3(\tau)^2.$$

It is a modular form of weight 12 and since for every τ it is the discriminant of the elliptic curve associated to the lattice $\mathbb{Z} + \mathbb{Z}\tau$ (times a non zero factor), it is non-vanishing on all $\mathfrak{H}$. Then, using theorem 1.1.7, we find that Δ has a simple zero at ∞ and in particular it is a cusp form.

Example 1.1.10 (j-function)**.** We define

$$j(\tau) := \frac{1728 \cdot g_2(\tau)^3}{\Delta(\tau)}.$$

It is a modular function of weight 0, with a simple pole at ∞. In particular it defines a function $j : \Gamma \setminus \mathfrak{H} \to \mathbb{C}$. Using again theorem 1.1.7, it is easy to prove that the weight 12 modular form $1728g_2^3 - \lambda\Delta$ has a unique zero for every $\lambda \in \mathbb{C}$, i.e. $j : \Gamma \setminus \mathfrak{H} \to \mathbb{C}$ is bijective. This gives us the fact that every elliptic curve over $\mathbb{C}$, uniquely determined up to isomorphism by its j-invariant j_E, is isomorphic to the elliptic curve associated to the lattice $\mathbb{Z} \oplus \mathbb{Z}\tau$ where $\tau \in \mathfrak{H}$ is such that $j([\tau]) = j_E$. From this one gets also easily a proof of theorem 0.1.16.

1.1.1 The modular curve

We give a brief overview of the definition and properties of the modular curves. For more details we refer to the notes [Mil12] or to chapter 1.5 of [DS05].

For $\Gamma = \mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(1)$, one can define on $X_0(1) := \Gamma \setminus \mathfrak{H}^*$ the structure of a compact Riemann surface, and using j of (1.1.10), find an analytic isomorphism $j : X_0(1) \to \mathbb{P}^1_{\mathbb{C}}$. Moreover the field of meromorphic functions on $X_0(1)$ is given by the modular functions of weight 0 $F_0(\Gamma)$, which is given by the space of rational functions in j, $\mathbb{C}(j)$. Using the bijection above and denoting with $Y_0(1) = \Gamma \setminus \mathfrak{H} \subset X_0(1)$ one also shows that there is a bijection

$$\begin{aligned} Y_0(1) &\longleftrightarrow \{\text{isomorphism classes of elliptic curves}/\mathbb{C}\} \\ \tau &\longmapsto [\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau]. \end{aligned}$$

Moreover for any field $L \subset \mathbb{C}$, an isomorphism class $[E]$ of an elliptic curve over $\mathbb{C}$ defines under the above bijection a L-rational point of $Y_0(1)$ (i.e. a L-rational point of $\mathbb{P}^1_{\mathbb{C}}$) if and only if there is a representative for $[E]$ defined over L.

One can do the same for $\Gamma = \Gamma_0(N)$ or $\Gamma = \Gamma_1(N)$, obtaining a Riemann surface $\Gamma \setminus \mathfrak{H}^*$, denoted with $X_0(N)$ and $X_1(N)$ respectively. As above we have an isomorphism with an algebraic curve. We call $C'(N)$ and $C(N)$ respectively the model of this curve over $\mathbb{Q}$. We also have bijections

$$\begin{aligned} Y_0(N) &\longleftrightarrow \left\{ \begin{array}{c} (E, S) : E \text{ elliptic curve over } \mathbb{C}, \\ S \text{ is a cyclic subgroup of } E \\ \text{of order } N \end{array} \right\} / \approx \\ \tau &\longmapsto [\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau, \langle \frac{1}{N} \rangle] \end{aligned}$$

and

$$\begin{aligned} Y_1(N) &\longleftrightarrow \left\{ \begin{array}{c} (E, t) : E \text{ elliptic curve over } \mathbb{C}, \\ t \text{ is a point of } E \text{ of order } N \end{array} \right\} / \approx \\ \tau &\longmapsto [\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau, \frac{1}{N}]. \end{aligned}$$

In both cases $Y_i(N)$ is $X_i(N)$ without the cusps, i.e $Y_i(N) = \Gamma \setminus \mathfrak{H}$ and the equivalence relations on the right sets are given by isomorphisms of elliptic curves preserving the given structure (of the cyclic group or of the point respectively).

Also in this case, the isomorphism with $C'(N)$ and $C(N)$ respectively together with the above bijections "acts well with respect to subfields": an isomorphism class $[(E, C)]$ (or

$[(E,t)]$) defines a L-rational point of $Y_i(N)$ if and only if there is a representative for the pair defined over L. As above a point on $Y_i(N)$ is L-rational if it corresponds to an L-rational point of $C'(N)$ and $C(N)$ respectively. We can summarize this in the following

Remark 1.1.11. Denote with $(C')^0(N)(\mathbb{C})$ and $C^0(N)(\mathbb{C})$ the subsets of $C'(N)(\mathbb{C})$ and $C(N)(\mathbb{C})$ respectively corresponding to $Y_0(N)$ and $Y_1(N)$. These are solutions of the moduli problems of elliptic curves with cyclic subgroups (respectively, points) of order N over $\mathbb{C}$. Actually this is still a solution over any field of characteristic not dividing N.

1.1.2 The geometric definition of modular form

As we were saying above, we want to give, following Katz, a more geometric definition of modular form. To do this we restrict to the case of $\Gamma = \Gamma_1(N)$ and we follow the notation of the preliminaries' chapter of [BDP].

First of all recall the general definition given in (0.1.24). We want to define for such an elliptic curve what does it means "to have a point of order N".

Definition 1.1.12. An *elliptic curve with* Γ*-level structure over a ring* R is a pair (E,t) where

i) $E \to \operatorname{Spec} R$ is an elliptic curve over $\operatorname{Spec} R$ as in (0.1.24);

ii) $t : \mathbb{Z}/N\mathbb{Z} \to E$ is a closed immersion of group schemes over $\operatorname{Spec} R$.

Moreover a *marked elliptic curve with* Γ*-level structure* is a triple (E,t,ω), where ω is a global section of Ω^1_E over $\operatorname{Spec} R$.

An isomorphism of elliptic curves with Γ-level structure (resp. of marked elliptic curves) is clearly defined as an R-isomorphism between elliptic curves which is compatible with the closed immersions (and with the chosen differentials).

Define $\tilde{Ell}(\Gamma, R)$ to be the set of isomorphism classes of marked elliptic curves with Γ-level structure.

Definition 1.1.13. A *weakly holomorphic algebraic modular form of weight* k *on* Γ *defined over* $\mathbb{C}$ is a rule which to every isomorphism class of triples $(E,t,\omega) \in \tilde{Ell}(\Gamma, R)$, for R a $\mathbb{C}$-algebra, associates an element $f(E,t,\omega) \in R$ such that

i) (Compatibility with base change). For every $j : R \to R'$ homomorphism of $\mathbb{C}$-algebras

$$f((E,t,\omega) \otimes_j R') = j(f(E,t,\omega)).$$

ii) (Weight k). For all $\lambda \in R^\times$

$$f(E,t,\lambda\omega) = \lambda^{-k} f(E,t,\omega).$$

Now let us consider the Tate curve $\mathbb{G}_m/q^{\mathbb{Z}}$ with some level N structure t defined over the $\mathbb{C}$-algebra $\mathbb{C}((q^{1/h}))$, for some $h \mid N$. Let $\omega_{can} := \frac{du}{u}$, where u is the usual parameter on $\mathbb{G}_m/q^{\mathbb{Z}}$.

Definition 1.1.14. A weakly holomorphic modular form f is an *algebraic modular form on* Γ *over* $\mathbb{C}$ if

$$f(Tate(q), t, \omega_{can}) \in \mathbb{C}[[q^{1/h}]], \text{ for all } t.$$

If these values are in $q^{1/h}\mathbb{C}[[q^{1/h}]]$, f is called a *cusp form*.

The *q-expansions* of f are the finitely many Laurent series obtained by varying the level N structure on the Tate curve.

Now consider $\mathcal{E}$ the universal elliptic curve with level N-structure. Consider $C = C(N)$ and $C^0 = C^0(N)$ the modular curves of level N over $\mathbb{Q}$. C^0 is a moduli scheme for the moduli problem "elliptic curves with level N structure", so we consider the map

$$\pi : \mathcal{E} \to C^0.$$

$\mathcal{E}$ is an elliptic curve over the scheme C^0 in the sense of (0.1.24). Then consider $\Omega^1_{\mathcal{E}/C^0}$ the sheaf of differential on $\mathcal{E}/C^0$, we define via π a sheaf on C^0 by

$$\underline{\omega} := \pi_* \Omega^1_{\mathcal{E}/C^0}.$$

Then one can view a (weakly holomorphic) modular form f as global section of the sheaf $\underline{\omega}^k$ by setting

$$f(E,t) = f(E,t,\omega)\omega^k, \tag{1.3}$$

where ω is a generator of Ω^1_E over $\operatorname{Spec} R$. Thanks to the weight k-condition in the definition, this expression does not depend on the choice of ω. We identify a point of C^0 as a pair (E,t) as in definition 1.1.12. Working on $\mathbb{C}$ and viewing $\underline{\omega}^k$ as analytic sheaf over $C^0(\mathbb{C})$, f is a holomorphic section and it gives rise to a holomorphic function on $\mathfrak{H}$ setting

$$f(\tau) := f(\mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z}, \frac{1}{N}, 2\pi i dw),$$

where w is the standard coordinate on $\mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z}$. This function obeys to the transformation rule

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau),$$

with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$, thanks again to the weight-k condition in the definition. This gives us the correspondence between the more general definition of modular form and the basic one. Moreover the Laurent series of f correspond to the q-expansions of f, seen as holomorphic function on the upper half plane, at the cusps. Clearly, in the other direction, if f is a modular form in the classical sense, since every elliptic curve over $\mathbb{C}$ is isomorphic to a complex torus and the associated lattice is homothetic to $\mathbb{Z} \oplus \mathbb{Z}\tau$ for some $\tau \in \mathfrak{H}$, we put

$$f(\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau, \frac{1}{N}, dw) := f(\tau). \tag{1.4}$$

1.1.3 The Shimura-Maas derivative operator

Another key object we want to introduce and that we will use later is the Shimura-Maas derivative operator, which acts on modular forms. Even if one can work with the geometric definition of modular form and give a more general definition of this operator, we define it by the way it acts on modular forms, seen in the classical definition we gave. We follow for this [BCD+14], 1.2.

Definition 1.1.15. Let f be a modular form of weight k with respect to a congruence subgroup Γ. Then the action of the *Shimura-Maas derivative operator* δ_k is defined as follows

$$\delta_k f(\tau) = \frac{1}{2\pi i}\left(\frac{d}{d\tau} + \frac{k}{\tau - \bar{\tau}}\right) f(\tau), \text{ for every } \tau \in \mathfrak{H}.$$

The first thing we notice is that $\delta_k f$ can be no more holomorphic. What is true, fixing the congruence subgroup Γ, is the following

Lemma 1.1.16. *δ_k sends modular forms of weight k to modular functions of weight $k+2$.*

Proof. Consider $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, we have

$$d(\gamma\tau) = d\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{ac\tau + ad - bc - ac\tau}{(c\tau+d)^2} d\tau = \frac{1}{(c\tau+d)^2} d\tau;$$
$$\gamma\tau - \overline{\gamma\tau} = \frac{a\tau+b}{c\tau+d} - \frac{a\bar{\tau}+b}{c\bar{\tau}+d} = \frac{\tau-\bar{\tau}}{(c\bar{\tau}+d)(c\tau+d)}.$$

Then with some calculations we compute:

$$\begin{aligned}
\delta_k f(\gamma\tau) &= \frac{1}{2\pi i}\left(\frac{d}{d(\gamma\tau)} + \frac{k}{\gamma\tau - \overline{\gamma\tau}}\right) f(\gamma\tau) \\
&= \frac{1}{2\pi i}\left((c\tau+d)^2 \frac{d}{d\tau} + (c\bar{\tau}+d)(c\tau+d)\frac{k}{\tau-\bar{\tau}}\right)(c\tau+d)^k f(\tau) \\
&= \frac{1}{2\pi i}\left((c\tau+d)^{k+2}\frac{d}{d\tau} f(\tau) + ck(c\tau+d)^{k+1} f(\tau) + (c\bar{\tau}+d)(c\tau+d)^{k+1}\frac{k}{\tau-\bar{\tau}} f(\tau)\right) \\
&= \frac{1}{2\pi i}\left((c\tau+d)^{k+2}\frac{d}{d\tau} f(\tau) + (c\tau+d)^{k+1} f(\tau)\left(ck + \frac{k(c\bar{\tau}+d)}{\tau-\bar{\tau}}\right)\right) \\
&= \frac{1}{2\pi i}\left((c\tau+d)^{k+2}\frac{d}{d\tau} f(\tau) + (c\tau+d)^{k+2}\frac{k}{\tau-\bar{\tau}} f(\tau)\right) \\
&= (c\tau+d)^{k+2}\delta_k f(\tau).
\end{aligned}$$

□

Moreover for r positive integer, one can define

$$\delta_k^r := \delta_{k+2r-2} \circ \cdots \circ \delta_{k+2} \circ \delta_k,$$

which sends modular forms of weight k to real analytic modular form of weight $k+2r$. This is just an iterated application of the above lemma.

One can naturally define

Definition 1.1.17. A *nearly holomorphic modular form of weight k on Γ* is a linear combination

$$f = \sum_{i=1}^{t} \delta_{k-2j_i}^{j_i} f_i,$$

where the f_i are modular forms of weight $k-2j_i$ on Γ.

Remark 1.1.18. As for modular forms, it makes sense to evaluate a nearly holomorphic modular form f on $\Gamma_1(N)$ in triples (E, t, ω) as above, with E elliptic curve over $\mathbb{C}$, by setting

$$f(\mathbb{C}/\mathbb{Z}\oplus\mathbb{Z}\tau, \frac{1}{N}, dw) := f(\tau).$$

1.2 p-adic modular forms

Let p be an odd prime number. As above we first quickly recall the classical definition of p-adic modular form, following Serre [Ser72], and then give the geometric one, as given in [Kat72].

Let $f = \sum_{n=0}^{+\infty} a_n q^n \in \mathbb{Q}_p[[t]]$. The p-adic valuation of f is defined as

$$v_p(f) := \inf_{n\geq 0}\{v_p(a_n)\}.$$

Definition 1.2.1. An element $f \in \mathbb{Q}_p[[t]]$ is said to be a *p-adic modular form on* Γ if there exists a sequence $\{f_k\}_k \subset \mathbb{Q}[[t]]$ such that f_k is the q-expansion at ∞ of a classical modular form on Γ and f_k tends p-adically to f, i.e.

$$\sup_{n\geq 0} |a_{n,k} - a_n|_p \xrightarrow[k\to+\infty]{} 0, \text{ i.e. } v_p(f_k - f) \xrightarrow[k\to+\infty]{} +\infty.$$

The *weight of a p-adic modular form* is defined to be the p-adic limit of the weights of the f_k's. It is an element of the weight space $W := \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$. One can show that this definition does not depend on the sequence $\{f_k\}_k$.

Notice that, in particular, the q-expansion of a classical modular form of weight k with rational coefficients is a p-adic modular form of weight k.

Example 1.2.2 (p-adic Eisenstein series)**.** The idea is to take the limit of families of Eisenstein series. We notice the q-expansion of G_k (1.2) has not rational coefficients. So we consider the classical modular forms of weight k

$$E_k(\tau) := \frac{(k-1)!}{(-1)^{(}k/2)\pi^k 2^{k+1}} \cdot G_k(\tau).$$

One can show that its q-expansion is given by

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

where $B_k \in \mathbb{Q}$ is the k-th Bernoulli number. We then define

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

Notice that since $p \nmid d$, $d \in \mathbb{Z}_p^\times$ and thus the exponential d^{k-1} makes sense. For $k \in 2W \setminus \{0\}$, take a sequence of $k_i \in 2\mathbb{Z}$ such that $k_i \to +\infty$ in the usual sense and $k_i \to k$ p-adically. Then one has

$$\sigma_{k_i-1}(n) \to \sigma_{k-1}^{(p)}(n)$$

in $\mathbb{Z}_p$ and uniformly in n. Now consider E_{k_i}. Then one can show that this family converges to the p-adic modular form of weight k

$$E_k^{(p)} = a_0 + \sum_{n=1}^{\infty} \sigma_{k-1}^{(p)}(n) q^n,$$

where $a_0 = \lim(-B_{k_i}/2k_i)$. It is called the p-adic Eisenstein series of weight k. See [Ser72] 1.5, corollary 2 and 1.6 for more details.

Notice that this gives us also the p-adic Eisenstein series of weight 2, even if a classical Eisenstein series of weight 2 does not exist.

1.2.1 The geometric definition of p-adic modular form

We follow, as before, the notations of the preliminaries' chapter of [BDP]. Let $\mathbb{C}_p$ the completion of the algebraic closure of $\mathbb{Q}_p$.

Definition 1.2.3. A *p-adic modular form of weight k on Γ defined over $\mathbb{C}_p$* is a rule which to every isomorphism class of triples $(E,t,\omega) \in \tilde{Ell}(\Gamma,R)$, with E ordinary at p and for R a $\mathbb{C}_p$-algebra, associates an element $f(E,t,\omega) \in R$ such that

i) (Compatibility with base change). For every $j : R \to R'$ homomorphism of $\mathbb{C}_p$-algebras

$$f((E,t,\omega) \otimes_j R') = j(f(E,t,\omega)).$$

ii) (Weight k). For all $\lambda \in R^\times$

$$f(E,t,\lambda\omega) = \lambda^{-k} f(E,t,\omega).$$

iii) (Behaviour at cusps). For all level N structure t on the Tate elliptic curve defined on $\mathbb{C}_p((q^{1/h}))$,

$$f(Tate(q),t,\omega_{can}) \in \mathbb{C}_p[[q^{1/h}]].$$

As in the case of classical modular form, we would like to see p-adic modular forms as sections of a suitable rigid analytic line bundle. One can not hope to define, in a similar way as before, a line bundle on $C(\mathbb{C}_p)$, since we are considering only "points" of the form (E,t,ω) with E not supersingular. So we need to *remove something*. First of all assume that $p \nmid N$, then C extends to a smooth proper model $\mathcal{C}$ over $\operatorname{Spec}\mathbb{Z}_p$. Then we can consider the natural reduction map

$$red_p : C(\mathbb{C}_p) \to C_{\mathbb{F}_p}(\bar{\mathbb{F}}_p),$$

with $C_{\mathbb{F}_p} := \mathcal{C} \times_{\mathbb{Z}_p} \mathbb{F}_p$. Recall that theorem 0.1.22 tells us that there are only finitely many (isomorphism classes of) supersingular elliptic curves over $\bar{\mathbb{F}}_p$. They correspond to finitely many points $\{P_1,\dots,P_t\}$ in $C_{\mathbb{F}_p}(\bar{\mathbb{F}}_p)$. Define $D(P_j)$ the residue disc attached to P_j to be the set of points of $C(\mathbb{C}_p)$ which have the same image as P_j under red_p. It is conformal to the unit disc in $\mathbb{C}_p$. The union of all these $D(P_j)$ corresponds to all elliptic curves whose reduction modulo p is supersingular. It is then natural to define

$$\mathcal{A} := C(\mathbb{C}_p) \setminus (D(P_1) \cup \cdots \cup D(P_t)),$$

this is called the *ordinary locus* of $C(\mathbb{C}_p)$. Now, as before, one can consider a sheaf $\underline{\omega}$ on $\mathcal{A}$ and, arguing as in (1.3), view a p-adic modular form as a section of $\underline{\omega}^k$ over $\mathcal{A} \subset C(\mathbb{C}_p)$.

1.2.2 The operators U and V

Following Serre's approach, we quickly recall the definition of two operators on the space of p-adic modular forms. Let f be a p-adic modular form of weight k

$$f = \sum a_n q^n.$$

We then define

$$Uf := \sum a_{pn} q^n \quad and \quad Vf := \sum a_n q^{pn}.$$

This definition are meaningful in light of the following

Proposition 1.2.4. *With the above notation and assumptions, Uf and Vf are p-adic modular forms of weight k.*

Proof. See [Ser72], théorème 4, §2. □

We can introduce another operator, which will turn out to be very useful, combining this two. We then consider $UV - VU$. The following lemma makes clear how it acts.

Lemma 1.2.5. *If f is a p-adic modular form as above,*

$$(UV - VU)f = \sum_{p|\not n} a_n q^n.$$

Proof. We just compute VUf and UVf. First we get

$$VUf = V(\sum a_{pn} q^n) = \sum a_{pn} q^{pn} = \sum_{p|n} a_n q^n.$$

Then we compute

$$UVf = U(\sum a_n q^{pn}) = \sum a_n q^n = f.$$

Putting together these computations we get the thesis. □

As always, this operators can be described also geometrically, in a way that is compatible with the approach we have presented.

1.2.3 The lifting of the Frobenius morphism

Following the above notation, we choose a rigid analytic isomorphism

$$h_j : D(P_j) \to \{z \in \mathbb{C}_p : ord_p(x) \geq 0\},$$

for every $j = 1, \ldots, t$. For every $\epsilon \in \mathbb{R}_{>0}$, we have the *wide open neighbourhood of* $\mathcal{A}$ which is defined by

$$\mathcal{W}_\epsilon := \mathcal{A} \cup \bigcup_{j=1}^{t} \{x \in D(P_j) : ord_p(h_j(x)) < \epsilon\}.$$

So $\mathcal{W}_\epsilon$ is obtained by adjoining to $\mathcal{A}$ t open annulli of width ϵ around the boundaries of the deleted residue discs $D(P_j)$.

Now we consider $U_{\mathbb{F}_p} := C_{\mathbb{F}_p} \setminus \{P_1, \ldots, P_t\}$. We denote with σ the Frobenius automorphism of $\mathbb{F}_p$. There exists a canonical morphism $\phi : U_{\mathbb{F}_p} \to U^\sigma_{\mathbb{F}_p} = U_{\mathbb{F}_p} \times_\sigma \mathbb{F}_p$ such that for every $f \in \mathcal{O}_{C_{\mathbb{F}_p}}(U_{\mathbb{F}_p})$, $\phi^* f^\sigma = f^p$. We assume that $\{P_1, \ldots, P_t\}$ is stable under ϕ. One can then show that there exists a morphism

$$\Phi : \mathcal{A} \to \mathcal{A}$$

which is a lifting in characteristic zero of ϕ.

This can be extended to a morphism $\Phi : \mathcal{W}_\epsilon \to \mathcal{W}_{\epsilon'}$, for suitable $0 < \epsilon < \epsilon'$ and induces a linear map

$$\Phi : \Omega^1(\mathcal{W}_{\epsilon'}) \to \Omega^1(\mathcal{W}_\epsilon).$$

In particular if we start with a p-adic modular form f and associate to it the differential $\omega_f = \sum a_n q^n dq/q$, i.e. a section of Ω^1 over $\mathcal{A}$, we can obtain an explicit description of the action. Indeed we have

$$\Phi \omega_f = p \omega_{Vf}.$$

1.2.4 The Coleman primitive

For this section we refer to the third chapter of [BDP], considering the case $r = 0$.

As above, we can associate to f, a p-adic modular form of weight k, the analytic section ω_f of Ω^1 over $\mathcal{A}$.

We denote with ∇ the rigid analytic integrable connection

$$\nabla : \mathcal{O} \to \Omega^1.$$

For a more precise definition of it we refer to [BDP]. One shows that, starting with a rigid analytic section of $\mathcal{O}$ on some wide open neighbourhood $\mathcal{W}$ and considering its q-expansion, the action of ∇ is given by taking the derivative with respect to q, so that $\nabla(\sum a_n q^n) = (\sum n \cdot a_n q^{n-1})dq$.

Definition 1.2.6. The *Coleman primitive* F_f of ω_f is the locally analytic section of $\mathcal{O}$ over C such that $\nabla F_f = \omega_f$ and F_f vanishes at infinity.

One proves that such a section exists and that, moreover, one can obtain a p-adic modular form of weight zero applying an operator to it. We will state a theorem (theorem 3.15 in [BDP]), which is proved in [Col94], sections 10 and 11.

Theorem 1.2.7. *Let $\omega = \omega_f$ be the global rigid section of Ω^1 over C as before. There exists a polynomial $P \in \mathbb{C}_p[x]$ and a locally analytic section F_ω of $\mathcal{O}$ over C such that*

(i) $\nabla F_\omega = \omega$;

(ii) $P(\Phi)(F_\omega)$ *is a rigid analytic section of $\mathcal{O}$ on some open neighbourhood $\mathcal{W}$.*

Remark 1.2.8. Notice that the theorem doesn't give us only the existence of the Coleman primitive, but also tells us that, after applying $P(\Phi)$, we get a p-adic modular form of weight 0.

1.2.5 The Atkin-Serre operator

We now introduce another operator, which acts on p-adic modular forms. As before, even if one can work with the geometric definition, we define it by the way it acts on p-adic modular forms as in Serre's definition.

Let now $g = \sum_{n=0}^{+\infty} b_n q^n$ be a p-adic modular form of weight k on Γ.

Definition 1.2.9. The *Atkin-Serre operator* d acts on a p-adic modular form g as follows

$$dg = q\frac{d}{dq}\sum_{n=0}^{+\infty} b_n q^n = \sum_{n=1}^{+\infty} n b_n q^n.$$

This is again a p-adic modular form and its weight is $k+2$. To see this, we first analyse the behaviour of the d-operator on classical modular forms (with rational coefficients). Let f be such a modular form of weight k, with q-expansion at ∞ given by $f = \sum_{n=0}^{\infty} a_n q^n$, with $q = e^{2\pi i z}$ for $z \in \mathfrak{H}$. Let us call $\theta = \frac{1}{2\pi i}\frac{d}{dz}$. Then we have

$$\theta f = \frac{1}{2\pi i}\frac{df}{dz} = \frac{1}{2\pi i}\sum_{n=0}^{\infty}(2\pi i) n a_n q^n = \sum_{n=0}^{\infty} n a_n q^n = df.$$

Now consider the Eisenstein series of weight 2: $P = 1 - 24\sum \sigma_1(n) q^n$. This is not a modular form in the usual sense, but we have that $P(-\frac{1}{z}) = z^2 P(z) + \frac{12z}{2\pi i}$. We have the following

Lemma 1.2.10. *If f is a modular form of weight k, then*

$$\theta f - \frac{k}{12} Pf$$

is a modular form of weight $k+2$.

Proof. Assuming for semplicity that $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, we only need to check that $(\theta f - \frac{k}{12}Pf)(-\frac{1}{z}) = z^{k+2}(\theta f - \frac{k}{12}Pf)(z)$. To do this we use $P(-\frac{1}{z}) = z^2 P(z) + \frac{12z}{2\pi i}$ and we differentiate with respect to z the equality $f(-\frac{1}{z}) = z^k f(z)$, which holds since f is a modular form of weight k. From the latter we get

$$\frac{df}{dz} = \left(\frac{kz^{k+1}}{1 - z^{k+2}} \right) f.$$

Then, substituting this into

$$(\theta f - \frac{k}{12}Pf)(-\frac{1}{z}) = \frac{1}{2\pi i}\frac{df}{dz}\left(-\frac{1}{z}\right) - \frac{k}{12} z^{k+2} P(z) f(z) - \frac{k}{12}\frac{12}{2\pi i} z^{k+1} f(z),$$

one gets the thesis. □

From the lemma it easily follows what we stated before.

Proposition 1.2.11. *The Atkin-Serre operator d sends p-adic modular forms of weight k to p-adic modular forms of weight $k+2$.*

Proof. If g is a p-adic modular form of weight k, we can find a family $\{g_i\}_i$ of classical modular forms with rational coefficients such that the q-expansions of the g_i's converge p-adically to g, each g_i is of weight k_i and k is the limit of the k_i's. One can easily see that the $dg_i = \theta g_i$ converge to dg. The lemma tells us that $dg_i = \frac{k_i}{12} P g_i + h_i$ where h_i is a modular form of weight $k_i + 2$. Since Pg_i is a p-adic modular form of weight $k_i + 2$, we have that dg is the limit of modular forms of weight $k_i + 2$, hence is a p-adic modular form of weight $k + 2$. □

There is a key result which connects this operator and the Shimura-Maas derivative operator. If f is a classical modular form of weight k on Γ with rational coefficients, we can apply to it both the Shimura-Maas derivative operator and the Atkin-Serre operator, viewing f as p-adic modular form for the latter. We obtain very different objects, but, using the geometric definitions we gave, we can evaluate both of them in triples of the form (E, t, ω), where E is an elliptic curve with Γ-level structure and E is ordinary at p. Using a more geometric description of these operators, one can prove the following surprising

Theorem 1.2.12. *Let f be a classical modular form of weight k on Γ with rational coefficients and $r \geq 0$ an integer. Consider (E, t, ω) an elliptic curve with Γ-level structure, such that E is ordinary at p and E* ***has complex multiplication****, then we have*

$$\delta_k^r f(E, t, \omega) = d^r(E, t, \omega).$$

1.3 Modularity theorem and Heegner points

We conclude this chapter with the statement of modularity theorem; we will also see how to use it to construct some special points on elliptic curves defined over the rationals. Our main references are the notes [Dar04], chapter 2.

1.3.1 The L-function attached to a newform

Even if the following definitions and constructions can be given in general for modular forms of weight k on Γ, we restrict our attention to the case of cusp forms of weight 2 on $\Gamma_0(N)$. We will denote $S_k(N) := S_k(\Gamma_0(N)) \subset M_k(N) := M_k(\Gamma_0(N))$.

Hecke operators. The complex vector space $M_k(N)$ is equipped with the Hecke operators T_p for p prime, which act on an element $f \in M_k(N)$ in the following way:

$$T_p f(\tau) = \begin{cases} \frac{1}{p}\sum_{i=0}^{p-1} f\left(\frac{\tau+i}{p}\right) + pf(p\tau) & \text{if } p \not| N \\ \frac{1}{p}\sum_{i=0}^{p-1} f\left(\frac{\tau+i}{p}\right) & \text{if } p \mid N. \end{cases}$$

It sends modular forms in modular form and cusp forms in cusp forms. The action of T_p on the q-expansions of f at ∞ is given by

$$T_p f = \begin{cases} \sum_{p|n} a_n q^{n/p} + p\sum a_n q^{pn} & \text{if } p \not| N \\ \sum_{p|n} a_n q^{n/p} & \text{if } p \mid N. \end{cases}$$

One then define the Hecke operator T_n for n positive integer by equating the coefficient of n^{-s} in the formal identity

$$\sum_{n=1}^{+\infty} T_n n^{-s} := \prod_{p \not| N} (1 - T_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N} (1 - T_p p^{-s})^{-1}. \tag{1.5}$$

We denote with $\mathbb{T}$ the commutative subalgebra of $\mathrm{End}_{\mathbb{C}}(M_k(N))$ generated over $\mathbb{Z}$ by the T_n's. One also has that the following properties hold:

(i) $T_n \cdot T_m = T_{nm}$ if $(n, m) = 1$;

(i) $T_p \cdot T_{p^n} = T_{p^{n+1}} + p^{2k-1} T_{p^{n-1}}$ for p prime and $n \geq 2$,

where k is the weight of the modular forms in which the operators are acting.

Definition 1.3.1. An *eigenform* of weight k is a modular form such that there exists a ring homomorphism $\lambda : \mathbb{T} \to \mathbb{C}$ so that for every n, $T_n f = \lambda(T_n) f$. It is normalized if the coefficient a_1 of the q-expansion is equal to 1.

Looking at the action on q-expansions and using the above properties one has that, for an eigenform f with Fourier coefficients a_n

(i) $a_n \cdot a_m = a_{nm}$ if $(n, m) = 1$;

(i) $a_p \cdot a_{p^n} = a_{p^{n+1}} + p^{2k-1} a_{p^{n-1}}$ for p prime and $n \geq 2$;

(iii) $a_n = a_1 \lambda(T_n)$.

We now look at the case of $S_2(N)$. We say that $f \in S_2(N)$ is an *oldform* if it is a linear combination of functions of the form $g(d'\tau)$, with $g \in S_2(N/d)$ and $d' \mid d > 1$. The *new subspace* of $S_2(N)$, denoted with $S_2^{\mathrm{new}}(N)$, is the orthogonal complement of the space of oldforms with respect to the Petersson scalar product on $S_2(N)$, defined by

$$\langle f_1, f_2 \rangle = \int_{\Gamma \backslash \mathfrak{H}} f_1(\tau) f_2(\tau) dx dy.$$

Finally, we give the following

Definition 1.3.2. A *newform of level* N is a normalized eigenform which lays in $S_2^{\text{new}}(N)$.

To a newform f of level N we want to attach an L-series. Consider $f = \sum_{n=1}^{+\infty} a_n q^n$ the q-expansion at ∞. We define

$$L(f,s) := \sum_{n=1}^{\infty} a_n n^{-s}.$$

By applying λ associated to f to (1.5) and noticing that $a_n = \lambda(T_n)$ one can see that such a function admits the Euler product factorization

$$L(f,s) = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N} (1 - a_p p^{-s})^{-1}.$$

Moreover there is the following important

Theorem 1.3.3. *The L-function $L(f,s)$ extends to an entire function on $\mathbb{C}$ and has a functional equation of the form*

$$\Lambda(f,s) = \pm \Lambda(f, 2-s),$$

where $\Lambda(f,s) := (2\pi)^{-s}\Gamma(s)N^{s/2}L(f,s)$, with $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt$ the usual Γ-function.

Remark 1.3.4 (Atkin-Lehner involution)**.** One can prove that the rule

$$w_N(f)(\tau) := \frac{1}{N\tau^2} f(-\frac{1}{N\tau}), \quad \text{for every } \tau \in \mathfrak{H},$$

where f is a newform of level N, is an involution on the space of newforms of level N, commuting with the Hecke operators. In fact $\mathbb{T}$ is generated by $\{T_p,\ p \nmid N\}$ and by w_N. One also has

$$w_N(f) = \varepsilon_f f, \quad \text{where } \varepsilon_f = \pm 1.$$

With this notation the functional equation of the above theorem can be written more precisely as

$$\Lambda(f,s) = -\varepsilon_f \Lambda(f, 2-s).$$

The fact that such L-functions have properties similar to the ones of L-functions attached to elliptic curve suggests a connection between this two theories. We explain the biggest results about this in the following section.

1.3.2 Eichler-Shimura theory and Modularity theorem

From a newform to an elliptic curve. This direction of the connection we were talking about is due to the work of Shimura and Eichler. Indeed they proved the following

Theorem 1.3.5. *If f is a newform of level N with rational Fourier coefficients, there exists an elliptic curve E_f over $\mathbb{Q}$ such that*

$$L(E_f, s) = L(f, s).$$

In particular we want to describe how the elliptic curve E_f is obtained. One can consider the ring homomorphism associated to f

$$\lambda_f : \mathbb{T} \to \mathbb{Z},$$

defined on the generators of the Hecke algebra of level N by $\lambda_f(T_p) = a_p(f)$ and $\lambda_f(w_N) = \varepsilon_f$. Take then the ideal $I_f := \ker(\lambda_f)$. Consider the Jacobian $J_0(N)$ of the curve $X_0(N)$ (where by abuse of notation we denote with $X_0(N)$ also the associated curve $C'(N)$); it is an abelian variety of dimension equal to the genus of $X_0(N)$. The Hecke algebra can be viewed as a subring of the endomorphism ring of $J_0(N)$. Thus one defines E_f to be the quotient of $J_0(N)$ by the subvariety $I_f J_0(N)$.

Moreover, since we have a canonical morphism from $X_0(N)$ to its Jacobian, sending a point P to the degree zero divisor $(P) - (\infty)$, composing with the natural projection $\pi : J_0(N) \to E_f$, we get

$$\phi_N : X_0(N) \to E_f,$$

which is called the *modular parametrization*. One often denotes with φ_N the projection morphism from $J_0(N)$ to E_f.

Remark 1.3.6. Notice that since $\lambda_f(T_p - a_p) = \lambda_f(w_N - \varepsilon_f) = 0$, for every (class of) degree zero divisor d, one has $\varphi_N(T_p d) = a_p d$ and $\varphi_N(w_N d) = \varepsilon_f d$.

The converse. Thanks to the work started by Wiles in the 1990's, it is now proved also the converse, in the case of elliptic curves over the rationals.

Theorem 1.3.7. *If E is an elliptic curve over $\mathbb{Q}$ of conductor N, there exists a newform $f \in S_2(N)$ such that*

$$L(E, s) = L(f, s).$$

Furthermore, E is isogenous to the elliptic curve E_f obtained with the Eichler-Shimura construction.

From this theorem, together with theorem 1.3.3, we obtain theorem 0.4.3. We also get a modular parametrization

$$\phi_N : X_0(N) \to E,$$

obtained by the one associated to E_f and composing with the isogeny $E_f \to E$.

1.3.3 Heegner points

We finally give the construction of Heegner points. Let K be a quadratic imaginary field and N an integer. We assume

Heegner hypothesis. There exists an ideal $\mathfrak{n} \subset \mathcal{O}_K$ satisfying $\mathcal{O}_K/\mathfrak{n} = \mathbb{Z}/N\mathbb{Z}$.

What one can require for instance is that every prime dividing N splits in K. Indeed

Lemma 1.3.8. *If K is a quadratic imaginary field in which every prime p dividing N splits, then K satisfies the Heegner hypothesis, i.e. there exists an ideal of norm N. More precisely, if N is divided by m distinct rational primes, there are 2^m such ideal.*

Proof. For every p dividing N write $(p) = \mathfrak{p}_{1,p}\mathfrak{p}_{2,p}$, for $\mathfrak{p}_{1,p}, \mathfrak{p}_{2,p}$ integral primes of K. Let $N = \prod_{p|N} p^{n_p}$, then

$$\mathfrak{n} = \prod_{p|N} \mathfrak{p}_{i_p,p}^{n_p},$$

for $i_p \in \{1, 2\}$, is an ideal of norm N. We have 2^m possibilities for such ideals and they are all the possible ones thanks to the unique prime ideals factorization in the Dedekind ring $\mathcal{O}_K$ and to the multiplicativity of the norm. □

To proceed we notice that, using the bijections in (0.1.15) and

$$\mathrm{End}(\mathbb{C}/\Lambda) \simeq \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\},$$

the lattices associated to elliptic curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$ are given by rank 2 $\mathbb{Z}$-submodules of K, hence fractional ideals. So we have

$$\begin{aligned} \mathrm{Pic}(\mathcal{O}_K) &\xrightarrow{1:1} \{\text{elliptic curves}/\mathbb{C} \text{ with CM by } \mathcal{O}_K\}/\approx \\ [\mathfrak{a}] &\longmapsto [\mathbb{C}/\mathfrak{a}]. \end{aligned}$$

Moreover, given $\mathfrak{n}$ as above, we also get a map

$$\begin{aligned} \mathrm{Pic}(\mathcal{O}_K) &\longrightarrow Y_0(N)(\mathbb{C}) \\ [\mathfrak{a}] &\longmapsto [\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{n}^{-1}\mathfrak{a}], \end{aligned}$$

where we view $Y_0(N)(\mathbb{C}) = \Gamma_0(N) \setminus \mathfrak{H}$ as the moduli space classifying either, as before, the pairs (E, C) with E elliptic curve over $\mathbb{C}$ and C cyclic subgroup of order N up to isomorphism (preserving the subgroups), or, equivalently, the isogenies $\varphi : E_1 \to E_2$ with kernel a cyclic subgroup of order N.

Now consider E an elliptic curve over $\mathbb{Q}$ of conductor N. Consider the modular parametrization defined above:

$$\phi_N : X_0(N)(\mathbb{C}) \to E(\mathbb{C}).$$

Collecting everything we can associate to every element $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_K)$ of the class group a point $P_{[\mathfrak{a}]} \in E(\mathbb{C})$, which actually turns out to be in $E(H_K)$, where H_K is the Hilbert class field of K. Indeed in the isomorphism class of the elliptic curve $\mathbb{C}/\mathfrak{n}$, together with the corresponding subgroup, there is a representative defined over $K(j(\mathfrak{a})) = H_K$, and thus the considered point on $Y_0(N)$ is an H_K-point. Using the group law on E we define

$$P_K := \sum_{[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_K)} P_{[\mathfrak{a}]}.$$

Recall, using theorems 0.3.3 and 0.3.4, that if $[\mathfrak{a}_1], \ldots, [\mathfrak{a}_h]$ are representative of $\mathrm{Pic}(\mathcal{O}_K)$, $H_K = K(j([\mathfrak{a}_i]))$ and $j([\mathfrak{a}_1]), \ldots, j([\mathfrak{a}_h])$ are a complete set of conjugates over K. We also have that the Artin map gives an isomorphism

$$Art : \mathrm{Pic}(\mathcal{O}_K) \to Gal(H_K/K) \tag{1.6}$$

So taking $\sigma \in Gal(H_K/K)$, as shown in remark 0.3.5, one finds, letting $Art^{-1}(\sigma) = [\mathfrak{b}]$, that ${P_{[\mathfrak{a}]}}^{\sigma} = P_{[\mathfrak{b}]^{-1}[\mathfrak{a}]}$, hence we get

$${P_K}^{\sigma} = \sum_{[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_K)} {P_{[\mathfrak{a}]}}^{\sigma} = \sum_{[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_K)} P_{[\mathfrak{b}]^{-1} \cdot [\mathfrak{a}]} = P_K,$$

hence $P_K \in E(K)$.

Remark 1.3.9. Notice that one could do the same by choosing points which correspond to elliptic curves with complex multiplication by an order $\mathcal{O}_n$ in $\mathcal{O}_K$, using the Picard group of $\mathcal{O}_n$. So for every $n \not| 2Ndisc(K)$, we consider such a point y_n which turns out to be in $E(K_n)$, where K_n is the ring class field of K associated to $\mathcal{O}_n$. Such a collection of points $\{y_n \in E(K_n)\}$ satisfies the axioms

AX 1. $\mathrm{Tr}_{K_{pn}/K_n}(y_{pn}) = \mathcal{L}_p y_n$ for every $p \nmid 2Ndisc(K)$,

AX 2. $y_{pn} \equiv Fr_\delta^{-1} y_n \pmod{\omega}$, for every ω, δ prime ideals of K_{pn}, K respectively, such that $\omega \mid \delta \mid p$,

where $\mathcal{L}_p = a_p = p + 1 - N_p$, with the notation of (0.4), if p remains prime in K and $\mathcal{L}_p = a_p - Fr_{\delta_1} - Fr_{\delta_2}$ if $(p) = \delta_1\delta_2$ splits in K. We denoted with Fr_δ the Frobenius element with respect to δ.

Such a collection of points is called an *Euler system of Heegner points*. See the Appendix to have some ideas of how one can use them to get information about the elliptic curve E.

Remark 1.3.10. To conclude we want to emphasize why we required that K satisfies the Heegner hypothesis. It is clear that this is fundamental to construct the Heegner points on E, since we explicitly used the existence of an ideal of norm N. It is proved that if, more generally, the sign of the functional equation of $L(E/K, s)$ is equal to -1 then there exists a non-trivial Heegner system of points $y_n \in E(K_n)$, satisfying the required properties, so that, for example, one can apply the same constructions and reasoning presented in the appendix.

One can not hope to build the points y_n starting from the modular curve and using the modular parametrization if the Heegner hypothesis is not satisfied. Let's suppose for example that the conductor N is divisible by p an inert prime in K and that there exists an ideal of norm N/p in K. One could then define a point x on $X_0(N/p)$ and lift it to $X_0(N)$. One has that the trace of this point on $J_0(N)$ is equal to the sum of all the lifts and it therefore comes from the old part of $J_0(N)$, which is contained in the kernel of the modular parametrization. We therefore would get that the trace of $\varphi_N(x)$ is equal to 0. This construction hence does not yield any point on E defined over ring class fields of conductor prime to p.

If E is a semistable elliptic curve of conductor N and the sign of the functional equation of $L(E/K, s)$ is equal to -1, the natural construction is done with Shimura curves. If every inert prime dividing N, divides it exactly, the construction of Heegner points using Shimura curves and a generalization of the results of [BDP], removing the Heegner hypothesis, is presented in [Bro13].

Chapter 2

A p-adic Gross–Zagier formula

In this chapter we illustrate a particular case of the main theorem proved in [BDP], as it is presented in chapter 1.3 of [BCD+14].

2.1 Motivation

Let E be an elliptic curve over $\mathbb{Q}$ and K a quadratic imaginary field satisfying the Heegner hypothesis. Consider $L(E/K, s)$, the L-function associated to E, which can be defined in a way that is similar to the one used to define $L(E, s)$. It actually turns out that $L(E/K, s)$ is a multiple of $L(E, s)$. Let us denote with $\hat{h}$, the Néron-Tate height on E. We have the following

Proposition 2.1.1. *For $P \in E(\bar{Q})$, $\hat{h}(P) = 0$ if and only if $P \in E(\bar{\mathbb{Q}})_{tors}$.*

Proof. See [Sil09] theorem 9.3.d, chapter VIII. □

The main result proved in [GZ86] relates the first derivative of the function $L(E/K, s)$ evaluated at $s = 1$ to the Néron-Tate height of P_K, the Heegner point defined at the end of the previous chapter. Namely

Theorem 2.1.2 (the Gross–Zagier formula)**.** *With the above assumptions and notations*

$$L'(E/K, 1) = c_{E,K} \cdot \hat{h}(P_K),$$

where $c_{E,K}$ is a non zero constant depending on E and on K.

Using the above proposition, we get an immediate

Corollary 2.1.3. *$L'(E/K, 1) = 0 \iff P_K$ is torsion in $E(K)$.*

If $L'(E/K, 1) \neq 0$, then, from the above corollary, we have that the rank of $E(K)$ as abelian group is certainly greater or equal then 1. Surprisingly, this is enough for saying that it is actually equal to 1. To show this one uses another deep result proved by Kolyvagin in [Kol90]. He proved that we also have an upper bound for the rank using the theory of *Euler systems*. See the appendix *A* to have some ideas of how the proof of a similar and slightly weaker result goes.

Theorem 2.1.4 (Kolyvagin)**.** *If P_K is of infinite order, then $E(K)$ has rank 1 and the Tate-Shafarevic group $Ш(E/K)$ is finite.*

And so we get, as we were saying,

Corollary 2.1.5. *If $L'(E/K,1) \neq 0$ then the rank of $E(K)$ is 1.*

What we want to do is to state (and prove) a result which is similar to the theorem of Gross and Zagier and which replaces the first derivative of the L-function with a p-adic L-function associated to f, the newform attached to E, and the height of P_K with (the square of) the formal group logarithm on E evaluated in P_K.

2.2 The hypotheses

We now fix the notation and the hypothesis of the setting we are working in.

Consider K to be a quadratic imaginary field with odd discriminant $D < 0$, assuming for simplicity that its class number is one and that it has trivial group of units. We will also consider a prime p which splits in K, i.e. $(p) = \mathfrak{p}\bar{\mathfrak{p}}$. Assume also that K satisfies the *Heegner hypothesis*. Following the notation of before we denote with $\mathfrak{n}$ a fixed integral ideal such that

$$\mathcal{O}_K/\mathfrak{n} = \mathbb{Z}/N\mathbb{Z}.$$

Notice that, being the discriminant odd, we are in the case

$$K = \mathbb{Q}(\sqrt{D}) \text{ and } \mathcal{O}_K = \mathbb{Z}[\tfrac{1+\sqrt{D}}{2}].$$

Assume that we can write the ideal $\mathfrak{n}$ in the form

$$\mathfrak{n} = \mathbb{Z}N \oplus \mathbb{Z}\frac{b+\sqrt{D}}{2},$$

for some $b \in \mathbb{Z}$. Now write

$$\tau_{\mathfrak{n}} = \tfrac{b+\sqrt{D}}{2N} \in \mathfrak{H}.$$

We want to specialize the construction we gave in (1.3.3) for our situation. There exists a unique (up to sign) element α of norm N such that $(\alpha) = \mathfrak{n}$, as $\mathcal{O}_K$-module. It is of norm N, so we have that $\pm N = \alpha \cdot \bar{\alpha}$. We now consider the $\mathbb{Z}$-module $\mathbb{Z} \oplus \mathbb{Z}\tau_{\mathfrak{n}}$. We have

$$\mathbb{Z} \oplus \mathbb{Z}\tau_{\mathfrak{n}} = \frac{1}{N} \cdot \mathfrak{n} = \frac{1}{\alpha \cdot \bar{\alpha}} \cdot (\alpha) = (\bar{\alpha}^{-1}) = \bar{\mathfrak{n}}^{-1}$$

We want to consider the pair $(\mathbb{C}/\bar{\mathfrak{n}}^{-1}, 1/N)$, where, by abuse of notation, we write $1/N$ for the cyclic subgroup of order N generated by this element. We start by proving the following:

Lemma 2.2.1. *With the notation above and under the moduli interpretation of $X_0(N)$, we have*

$$[(\mathbb{C}/\bar{\mathfrak{n}}^{-1}, \frac{1}{N})] \in X_0(N)(K_{\mathfrak{n}}),$$

where $K_{\mathfrak{n}}$ is the ray class field of K of conductor $\mathfrak{n}$. More precisely, there exists a model A of the elliptic curve corresponding to $\mathbb{C}/\bar{\mathfrak{n}}^{-1}$ defined over $K \subset K_{\mathfrak{n}}$ and the corresponding point $t_{\mathfrak{n}}$ is defined over $K_{\mathfrak{n}}$.

Proof. The elliptic curve $E/\mathbb{C}$ corresponding to the given complex torus has a model A defined over $K(j(E)) = H_K$, the Hilbert class field of K. Using the isomorphism (1.6) and

the fact that $\mathrm{Pic}(\mathcal{O}_K)$ is trivial under our assumptions, we have that $H_K = K$. Moreover we notice that $1/N$ is a $\mathfrak{n}$-torsion point of E. Indeed using the previous notations we get

$$\mathfrak{n} \cdot \frac{1}{N} = (\alpha) \cdot \frac{1}{\alpha\bar{\alpha}} \subset \bar{\mathfrak{n}}^{-1}.$$

Using the characterization of theorem 0.3.4, we have $K_\mathfrak{n} = H_K(E[\mathfrak{n}]) = K(E[\mathfrak{n}])$ and we get that $(\mathbb{C}/\bar{\mathfrak{n}}^{-1}, 1/N) \xrightarrow{\simeq} (A, t_\mathfrak{n})$ where A is an elliptic curve defined over K and $t_\mathfrak{n}$ is defined over $K_\mathfrak{n}$. □

Since we will be interested in evaluating a modular form in such a point, we need to choose a differential. So let ω_A be the Néron differential associated to A, as in definition 0.1.10. We can assume that A, and hence ω_A, are actually defined over $\mathcal{O}_K$. We get the isomorphism of marked elliptic curves

$$(A, t_\mathfrak{n}, \omega_A) \xrightarrow{\simeq} (\mathbb{C}/\bar{\mathfrak{n}}^{-1}, \frac{1}{N}, \bar{\alpha}\Omega_K dz),$$

where the isomorphism is the inverse of the one used in the proof of the above lemma and Ω_K is a complex number uniquely determined (up to sign, since $\mathcal{O}_K = \{\pm 1\}$) once ω_A has been chosen.

So for f modular form of weight k on $\Gamma_0(N)$, using (1.4) and the weight k condition, we have

$$f(A, t_\mathfrak{n}, \omega_A) = f(\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau_\mathfrak{n}, \frac{1}{N}, \Omega_K\bar{\alpha}dz) = (\Omega_K\bar{\alpha})^{-k} f(\tau_\mathfrak{n}). \tag{2.1}$$

Remark 2.2.2. Notice that, since A is an elliptic curve with complex multiplication by K and p splits in K, we can apply theorem 0.1.29 to prove that A is ordinary at p. We can then apply theorem 1.2.12 to say that, for every r, we have

$$\delta_k^r f(A, t_\mathfrak{n}, \omega_A) = d^r(A, t_\mathfrak{n}, \omega_A), \tag{2.2}$$

where δ_k^r and d^r are Shimura-Maas operator and Atkin-Serre operator respectively.

2.3 The anticyclotomic p-adic L-function

We now define a key object that, as we will see, will play the same role as the first derivative of the L function associated to an elliptic curve in the Gross–Zagier formula.

2.3.1 Waldspurger's formula

Waldspurger's formula relates the the value $\delta_k^r f(A, t_\mathfrak{n}, \omega_A)$ with the L-function of f twisted over K by certain unramified Hecke characters of K.

Recall that an Hecke character of K is a continuous homomorphism $\phi : \mathbb{A}_K^\times \to \mathbb{C}^\times$, where $\mathbb{A}_K^\times$ is the idèle group of K. Recall also that, using

$$\begin{aligned} \mathbb{A}_K^\times &\longrightarrow \{\text{fractional ideals of } K\} \\ a &\longmapsto \prod \mathfrak{p}^{ord_{v_\mathfrak{p}}(a)}, \end{aligned}$$

where $v_\mathfrak{p}$ is the non archimedean valuation associated to $\mathfrak{p}$, we can view ϕ as a multiplicative function on the fractional ideal of K.

Let f be a newform of weight k on $\Gamma_0(N)$, we then give the following

Definition 2.3.1. The *L-function of f over K twisted by the Hecke character ϕ* is defined, for $s \in \mathbb{C}$ in some right-half plane, by the Euler product

$$L(f, K, \phi, s) = \prod_{\mathfrak{l} \text{ prime}} [(1 - \alpha_{N\mathfrak{l}} \cdot \phi(\mathfrak{l}) \cdot N\mathfrak{l}^{-s})(1 - \beta_{N\mathfrak{l}} \cdot \phi(\mathfrak{l}) \cdot N\mathfrak{l}^{-s})]^{-1},$$

where, if the q-expansion of f at ∞ is given by $f = \sum_n a_n(f)q^n$ and $x^2 - a_l(f)x + l^{k-1}$ is the Hecke polynomial for f at the rational prime l, $\alpha_l(f)$ and $\beta_l(f)$ are its roots. Then if $N\mathfrak{l} = l^t$, $\alpha_{N\mathfrak{l}} := \alpha_l(f)^t$ and $\beta_{N\mathfrak{l}} := \beta_l(f)^t$.

One can show that $L(f, K, \phi, s)$ admits an analytic continuation to the entire complex plane. Now consider k_1, k_2 integers with the same parity and define the Hecke character of K by

$$\phi_{k_1,k_2}((\alpha)) = \alpha^{k_1}\alpha^{-k_2}.$$

It is defined on the fractional ideal of K, that are all principal by our assumptions. We have that

Lemma 2.3.2. *ϕ_{k_1,k_2} as defined above is an Hecke character.*

Proof. The map is clearly continuous. It is also well defined thanks to the fact that k_1, k_2 have the same parity. Indeed $k_1 - k_2$ is even and if $(\alpha) = (\beta)$ then $\alpha = u \cdot \beta$ for some $u \in \mathcal{O}_K^\times$. But we assumed that $\mathcal{O}_K^\times = \{\pm 1\}$, so we have $\phi_{k_1,k_2}((\alpha)) = \alpha^{k_1}\alpha^{-k_2} = u^{k_1-k_2}\beta^{k_1}\beta^{-k_2} = \phi_{k_1,k_2}((\beta))$. □

Now we define, for $k_1 - k_2 \in 2\mathbb{Z}$

$$L(f, K, k_1, k_2) := L(f, K, \phi_{k_1,k_2}^{-1}, 0).$$

Waldspurger's formula relates the value of this function in $(k + r, -r)$ to the value of $\delta_k^r f$ in our special point. Notice that k is even (it is the weight of f) and so $k + 2r \in 2\mathbb{Z}$ and we are in the case of the definition above.

Theorem 2.3.3 (Waldspurger's formula)**.** *With the notations and assumptions of this chapter, we have*

$$(\delta_k^r f(A, t_{\mathfrak{n}}, \omega_A))^2 = 1/2 \cdot (2\pi/\sqrt{D})^{k+2r-1} r!(k + r - 1)! \cdot \frac{L(f, K, k + r, -r)}{(2\pi i \cdot \overline{\alpha}\Omega_K)^{2(k+2r)}}.$$

2.3.2 The anticyclotomic p-adic L-function attached to f and K

Using Waldspurger's formula we want to construct a p-adic analytic function which interpolates the L-function we have just defined. We are assuming that $p = \mathfrak{p}\overline{\mathfrak{p}}$ is a prime which splits in K and does not divide N. Recall that, if the q-expansion of f at ∞ is given by $f = \sum_{n=1}^{\infty} a_n(f)q^n$, we have

$$d^r f = \sum_{n=1}^{\infty} n^r a_n(f) q^n,$$

where d^r is the Atkin-Serre operator.

The coefficients of q^n when $p|n$ do not extend to a p-adic analytic function of $r \in W = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$. What one can do is to consider the *p-depletion* of f:

$$f^{[p]}(\tau) := f(\tau) - a_p(f)f(p\tau) + p^{k+1}f(p^2\tau).$$

Proposition 2.3.4. *The q expansion of the p-depletion of f is $f^{[p]} = \sum_{p\nmid n} a_n(f)q^n$.*

Remark 2.3.5. Notice that, if we prove the proposition, then we have, as we wanted,

$$d^r f^{[p]} = \sum_{p\nmid n} n^r a_n(f) q^n. \tag{2.3}$$

Proof. Recall that f is a newform, in particular a normalized eigenform, so we have

(i) $a_1 = 1$;

(ii) if $(n,m) = 1$, $a_{nm} = a_n a_m$;

(iii) for p prime and $i \geq 2$, $a_{p^i} = a_p a_{p^{i-1}} - p^{k-1} a_{p^{i-2}}$,

where we write a_n for $a_n(f)$. Moreover, using $q = e^{2\pi i \tau}$ we get, letting $g(\tau) = f(p\tau)$ and $h(\tau) = f(p^2\tau)$,

$$g(q) = \sum_{n=1}^{\infty} n^r a_n q^{pn} = \sum_{p|n} a_{\frac{n}{p}} q^n \quad \text{and} \quad h(q) = \sum_{p^2|n} a_{\frac{n}{p^2}} q^n$$

Using (ii) we have that if $p \parallel n$ (i.e. $p \mid n$ but $p^2 \nmid n$), then $a_n = a_p a_{\frac{n}{p}}$. So we find

$$f^{[p]}(q) = \sum_{n=1}^{\infty} a_n q^n - \sum_{p|n} a_p a_{\frac{n}{p}} q^n + p^{k+1} \sum_{p^2|n} a_{\frac{n}{p^2}} q^n = \sum_{p\nmid n} a_n q^n + \sum_{p^2|n} (a_n - a_p a_{\frac{n}{p}} + p^{k-1} a_{\frac{n}{p^2}}) q^n.$$

Now, using (ii) and (iii) and writing $n = p^i m$ with $p \nmid m$, we get that the second sum in the last term above is zero. Indeed $a_n = a_m a_{p^i} = a_m(a_p a_{p^{i-1}} - p^{k-1} a_{p^{i-2}}) = a_p a_{\frac{n}{p}} - p^{k-1} a_{\frac{n}{p^2}}$. □

Remark 2.3.6. Notice that $f^{[p]}$ is a priori a modular form of weight k on $\Gamma_0(p^2N)$ since $g(\tau) = f(p\tau)$ and $h(\tau) = f(p^2\tau)$ are modular forms on $\Gamma_0(pN)$ and $\Gamma_0(p^2N)$ respectively and $\Gamma_0(N) \cap \Gamma_0(pN) \cap \Gamma_0(p^2N) = \Gamma_0(p^2N)$. Hence $d^r f^{[p]}$ is a p-adic modular form of weight $k + 2r$ on $\Gamma_0(p^2N)$.

We would like to evaluate $d^r f^{[p]}$ in $(A, t_{\mathfrak{n}}, \omega_A)$. To do this we need to work a bit, since, like we noticed in the above remark, $d^r f^{[p]}$ is not a p-adic modular form on $\Gamma_0(N)$. We can consider the natural projection

$$\pi : X_0(p^2N) \to X_0(N).$$

This is given by sending the pair (E, C), where C is a cyclic subgroup of order p^2N, to the pair (E, C'), where C' is the cyclic subgroup of C of order N, which exists unique since p and N are coprime. The following proposition will be important for our discussion:

Proposition 2.3.7. *π admits a section s from the ordinary locus of $X_0(N)$, $\mathcal{A}_N$, to the ordinary locus of $X_0(p^2N)$, $\mathcal{A}_{p^2N}$.*

Remark 2.3.8. Using this proposition we can then give sense to the evaluation of $f^{[p]}$ in $(A, t_{\mathfrak{n}}, \omega_A)$ by setting

$$d^r f^{[p]}(A, t_{\mathfrak{n}}, \omega_A) := d^r f^{[p]}(s(A, t_{\mathfrak{n}}, \omega_A)) \tag{2.4}$$

Proof. We just define how to associate to a point of $Y_0(N) \cap \mathcal{A}_N$ a point of $Y_0(p^2N) \cap \mathcal{A}_{p^2N}$, not considering the cusps. This will be enough for us. So we consider $(E, C) \in Y_0(N)$, with E elliptic curve over $\mathbb{C}_p$ ordinary at p and C a cyclic subroup of order N, say generated by t. We can moreover suppose that E is defined over the ring of integers of $\mathbb{C}_p$. The reduction modulo p of E, say $\tilde{E}$ is ordinary, thus, applying theorem 0.1.23, $\tilde{E}[p^2] = \mathbb{Z}/p^2\mathbb{Z}$. Moreover, using (0.1.7), $E[p^2] = (\mathbb{Z}/p^2\mathbb{Z})^2$, then the kernel of the map

$$E[p^2] \to \tilde{E}[p^2]$$

is a cyclic subgroup of E of order p^2. Take u to be its generator, we can then define

$$s : (E, \langle t \rangle) \mapsto (E, \langle ut \rangle),$$

which gives us the desired section. □

Using this construction we want to give an explicit computation of $d^r f^{[p]}(A, t_\mathfrak{n}, \omega_A)$ in terms of $d^r f(A, t_\mathfrak{n}, \omega_A)$. In particular we have the following:

Proposition 2.3.9. *With the above notations and assumptions, we have*

$$d^r f^{[p]}(A, t_\mathfrak{n}, \omega_A) = (1 - a_p(f)\beta^r \bar{\beta}^{-k-r} + \beta^{k+2r-1}\bar{\beta}^{-k-2r-1}) d^r f(A, t_\mathfrak{n}, \omega_A), \tag{2.5}$$

where β is a generator of $\mathfrak{p}$.

Proof. First of all, letting again $g(\tau) = f(p\tau)$ and $h(\tau) = f(p^2\tau)$, we have

$$d^r f^{[p]} = d^r f - a_p p^r d^r g + p^{k-1} p^{2r} h. \tag{2.6}$$

Now recall that $[(A, t_\mathfrak{n}, \omega_A)] = [(\mathbb{C}/\bar{\mathfrak{n}}^{-1}, 1/N, \bar{\alpha}\Omega_K dz)]$, where $(\alpha) = \mathfrak{n}$. The torsion part of $\mathbb{C}/\bar{\mathfrak{n}}^{-1}$ is given by $K/\bar{\mathfrak{n}}^{-1}$ and in particular we can deduce, using $(p) = \mathfrak{p} \cdot \bar{\mathfrak{p}}$ in K,

$$\mathbb{C}/\bar{\mathfrak{n}}^{-1}[p^2] = \mathbb{C}/\bar{\mathfrak{n}}^{-1}[\mathfrak{p}^2] \times \mathbb{C}/\bar{\mathfrak{n}}^{-1}[\bar{\mathfrak{p}}^2].$$

After fixing an embedding $K \hookrightarrow \bar{\mathbb{Q}}_p$, we can assume that the cyclic subgroup of order p^2 is given by the $\mathfrak{p}^2$-torsion part of $\mathbb{C}/\bar{\mathfrak{n}}^{-1}$. Let β a generator of $\mathfrak{p}$ as $\mathcal{O}_K$ module. It is an element of norm p so that $p = \beta\bar{\beta}$. Then the $\mathfrak{p}^2$-torsion subgroup is generated by $u = 1/\beta^2 = \bar{\beta}^2/p^2$. So we get

$$s(A, t_\mathfrak{n}, \omega_A) = s(\mathbb{C}/\bar{\mathfrak{n}}^{-1}, 1/N, \bar{\alpha}\Omega_K dz) = (\mathbb{C}/\bar{\mathfrak{n}}^{-1}, \bar{\beta}^2/p^2N, \bar{\alpha}\Omega_K dz).$$

Now notice that $\mathfrak{p}^2\mathfrak{n} = \mathbb{Z}Np^2 \oplus \mathbb{Z}\frac{b+\sqrt{D}}{2}$, since the r.h.s. term is an ideal of norm p^2N and it does not contain (p^2). So we get, letting again $\tau_\mathfrak{n} = \frac{b+\sqrt{D}}{2N}$,

$$\mathbb{Z} \oplus \mathbb{Z}\frac{1}{p^2}\tau_\mathfrak{n} = \frac{1}{p^2N}\mathfrak{p}^2\mathfrak{n} = \bar{\mathfrak{p}}^{-2}\mathfrak{n}^{-1}.$$

Hence we find an isomorphism of marked elliptic curves

$$(\mathbb{C}/\bar{\mathfrak{n}}^{-1}, \bar{\beta}^2/p^2N, \bar{\alpha}\Omega_K dz) \xrightarrow{\cdot\bar{\beta}^{-2}} (\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\frac{1}{p^2}\tau_\mathfrak{n}, \frac{1}{p^2N}, \bar{\beta}^{-2}\bar{\alpha}\Omega_K dz).$$

Using (2.6), we want to evaluate f, g, h in this point. In particular we want to compute

$$d^r f^{[p]}(\mathbb{C}/\mathbb{Z}\oplus\mathbb{Z}\frac{1}{p^2}\tau_\mathfrak{n}, \frac{1}{p^2N}, \bar{\beta}^{-2}\bar{\alpha}\Omega_K dz) = (\bar{\beta}^{-2}\bar{\alpha}\Omega_K)^{-(k+2r)} \left(d^r f(\frac{1}{p^2}\tau_\mathfrak{n}) - a_p p^r d^r f(\frac{1}{p}\tau_\mathfrak{n}) + p^{k-1+2r} d^r f(\tau_\mathfrak{n}) \right).$$

But we have

$$\frac{1}{p^2}\tau_{\mathfrak{n}} \leftrightarrow [(\mathbb{C}/\bar{\mathfrak{p}}^{-2}\mathfrak{n}^{-1}, \frac{1}{N}, dz)] = [(\mathbb{C}/\mathfrak{n}^{-1}, \frac{1}{N}, \bar{\beta}^2 dz)]$$
$$\frac{1}{p}\tau_{\mathfrak{n}} \leftrightarrow [(\mathbb{C}/\bar{\mathfrak{p}}^{-1}\mathfrak{n}^{-1}, \frac{1}{N}, dz)] = [(\mathbb{C}/\mathfrak{n}^{-1}, \frac{1}{N}, \bar{\beta} dz)],$$

where we used as we did many times the multiplication by $\bar{\beta}^2$ and $\bar{\beta}$ respectively and the fact that the cyclic group generated by $\bar{\beta}/N$ or $\bar{\beta}^2/N$ is the same as the one generated by $1/N$ since $\bar{\mathfrak{p}}$ and N are coprime. So what we get at the end is

$$d^r f^{[p]}(\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\frac{1}{p^2}\tau_{\mathfrak{n}}, \frac{1}{p^2 N}, \bar{\beta}^{-2}\bar{\alpha}\Omega_K dz) = (\bar{\beta}^{-2}\bar{\alpha}\Omega_K)^{-(k+2r)} d^r f(\mathbb{C}/\mathfrak{n}^{-1}, \frac{1}{N}, dz) \cdot$$
$$\cdot (\bar{\beta}^{-2(k+2r)} - a_p \bar{\beta}^{-(k+2r)} + p^{k-1+2r}) =$$
$$= (1 - a_p \bar{\beta}^{-(k+2r)} + p^{k-1+2r}\bar{\beta}^{-2(k+2r)}) d^r f(\mathbb{C}/\mathfrak{n}^{-1}, \frac{1}{N}, \bar{\alpha}\Omega_K dz)$$

Using $\beta\bar{\beta} = p$ and substituting we get

$$d^r f^{[p]}(\mathbb{C}/\mathfrak{n}^{-1}, \frac{1}{N}, \bar{\alpha}\Omega_K dz) = (1 - a_p(f)\beta^r \bar{\beta}^{-k-r} + \beta^{k+2r-1}\bar{\beta}^{-k-2r-1}) d^r f(\mathbb{C}/\mathfrak{n}^{-1}, \frac{1}{N}, \bar{\alpha}\Omega_K dz)$$

ane hence the thesis. □

Then, since (2.3) tells us that the function sending $r \mapsto n^r a_n(f^{[p]})$ extends to a p-adic analytic function on $W = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$, up to multiplying by a p-adic period $\Omega_p \in \mathbb{C}_p^\times$, (2.5) extends to a p-adic analytic function on W. More precisely, in a similar way we did for the complex period Ω_K with respect to the differential dz, we consider the canonical differential dt/t on the formal multiplicative group $\hat{\mathbb{G}}_m$. We then fix an isomorphism

$$i : \hat{A} \to \hat{\mathbb{G}}_m,$$

where $\hat{A}$ is the formal completion of A defined over the ring of integers of $\mathbb{C}_p$ along its identity section. Then letting $\omega_{can} := i^*(dt/t)$, the p-adic period $\Omega_p \in \mathbb{C}_p^*$ is defined by

$$\omega_A = \Omega_p \cdot \omega_{can}.$$

Now we define

$$L_p(f, K, k+r, -r) := \Omega_p^{2(k+2r)} \times d^r f^{[p]}(A, t_{\mathfrak{n}}, \omega_A)^2 \tag{2.7}$$

to be the *anticyclotomic p-adic L-function attached to f and K*. Then, using (2.2) and Waldspurger's formula, one gets that $L_p(f, K, k+r, -r)$ interpolates the values of $L(f, K, k+r, -r)$ for $r \geq 0$ integer (up to multiplication of some factors coming from the Waldspurger's formula).

2.4 The Coleman primitive of f and Heegner points

Before getting to the theorem, we need to see some results concerning the Coleman primitive associated to f, seen as p-adic modular form of weight k, as in (1.2.4), and its value in our special point (A, t, ω).

Following [BDP] we consider the operator $UV - VU$, that we defined in (1.2.2). This operator will play the role of $P(\Phi)$ in theorem 1.2.7. This makes sense, since using lemma 1.2.5 together with the fact that $\Phi f = pVf$ we have the following

Lemma 2.4.1. *$UV - VU$ is a polynomial in the variable Φ.*

Proof. To show this we use proposition 2.3.4. We can rephrase it by saying that

$$(1 - \frac{1}{p}a_p\Phi + p^{k-3}\Phi^2)f = \sum_{p\not|n} a_n q^n.$$

Lemma 1.2.5 gives us $1 - \frac{1}{p}a_p\Phi + p^{k-3}\Phi^2 = UV - VU$, so we are done. □

Assuming the fact that $UV - UV = P(\Phi)$ satisfies the conditions of theorem 1.2.7, with $P = 1 - \frac{1}{p}a_p x + p^{k-3}x^2$, we denote with $F_f^{[p]}$ the locally analytic section obtained by applying $UV - VU$ to the Coleman primitive F_f. What we get is, in fact, a p-adic modular form. To see this we use proposition 3.24 of [BDP], which becomes much easier for us since $j = r = 0$.

Proposition 2.4.2. *If f is as above a p-adic modular form,*

$$d(F_f^{[p]}) = f^{[p]},$$

where d is the Atkin-Serre operator.

Proof. To prove this we use the fact that the q-expansion of F_f is given by $F_f = \sum a_n/n\ q^n$ so that $F_f^{[p]} = \sum_{p\not|n} a_n/n\ q^n$. Recalling that the Atkin-Serre operator acts as $q\ d/dq$ we find

$$d(F_f^{[p]}) = q\frac{d}{dq}\sum_{p\not|n}\frac{a_n}{n}q^n = \sum_{p\not|n} a_n q^n$$

and so the thesis. □

Remark 2.4.3. In particular this theorem implies that, using the explicit description of the action of ∇ on q-expansions, $\nabla F_f^{[p]} = f^{[p]}dq/q = \omega_{f^{[p]}}$ and so we have that $F_f^{[p]} = (UV - VU)F_f = F_{f^{[p]}}$ is the Coleman primitive of $\omega_{f^{[p]}}$ and theorem 1.2.7 tells us that it is a rigid analytic section of $\mathcal{O}$ on some open neighbourhood $\mathcal{W}$.

We conclude this section by stating another key result we will need in the proof of the theorem. In paragraph 3.7 of [BDP] it is shown how the p-adic Abel-Jacobi map, introduced in 3.4, and the Coleman primitive of f are related to each other. In the case of $r = 0$ the Heegner cycles are just Heegner points and the p-adic Abel-Jacobi map is characterized by

$$\begin{aligned} AJ : \{\text{Heegner points}\} &\to \Omega^1(\mathcal{A})^\vee \\ P &\mapsto (\omega \mapsto \log_\omega(P)) \end{aligned}$$

In particular lemma 3.22 of [BDP] gives us, in our case with $j = r = 0$ and with $\varphi = id$,

Lemma 2.4.4. *Let (A, t, ω) a marked elliptic curve of level N with complex multiplication by a quadratic imaginary field where p splits. Consider f a p-adic modular form of level N and let P be the Heegner point corresponding to (A, t, ω). We have*

$$\log_{\omega_f}(P) = F_f(A, t, \omega),$$

where F_f is the Coleman primitive of ω_f.

2.5 The theorem

We finally get to the theorem. In our setting f is attached to a rational elliptic curve E of conductor N in the sense of theorem 1.3.7. Thus f is a newform on $\Gamma_0(N)$ and of weight 2.

Consider $J_0(N)$ the Jacobian variety of the modular curve $X_0(N)$ and let $P_K \in J_0(N)(K)$ be the class of the degree 0 divisor $(A, t_{\mathfrak{n}}) - (\infty)$. Consider the map

$$\varphi_N : J_0(N) \to E$$

arising from f and let ω_E be the regular differential on E such that $\varphi_N^*(\omega_E) = \omega_f := (2\pi i) f(\tau) d\tau$. Define $P_{K,f} := \varphi_N(P_K)$.

Theorem 2.5.1. *Let f, N and E be as above and consider p a rational prime not dividing N. Let K be a quadratic imaginary field satisfying the assumptions of this chapter. Denote with $\log_p$ the formal group logarithm on E associated with the regular differential ω_E defined above. Then*

$$L_p(f, K, 1, 1) = \left(\frac{1 - a_p(f) + p}{p}\right)^2 \log_p(P_{K,f})^2.$$

Proof. The key fact we are using to prove the theorem is the existence of the Coleman primitive. In our setting, with $k = 2, r = -1$ in (2.7), we have

$$L_p(f, K, 1, 1) = d^{-1} f^{[p]}(A, t_{\mathfrak{n}}, \omega_A)^2.$$

Denote with $F^{[p]} := d^{-1} f^{[p]} = \sum_{p \nmid n} a_n(f)/nq^n$. Then we have seen that

$$dF^{[p]} = \sum_{p \nmid n} a_n(f) q^n dq/q = \omega_{f^{[p]}}.$$

We have that $F^{[p]} = F_{f^{[p]}}$ is the Coleman primitive of $\omega_{f^{[p]}}$.

Now consider F_f the Coleman primitive of ω_f. Similarly we get that $F_f = d^{-1} f$. Moreover applying lemma 2.4.4 and theorem 0.2.7 together with the hypothesis that $\varphi_E^*(\omega_E) = \omega_f$ we get

$$F_f(A, t_{\mathfrak{n}}, \omega_A) = \log_{\omega_f}(P) = \int \omega_f(P_K) = \int \omega_E(\varphi_N(P_K)) = \int \omega_E(P_{K,f}) = \log_p(P_{K,f}).$$

We then rewrite (2.5) in our special situation, using $\beta\bar{\beta} = p$, and get

$$\begin{aligned} d^{-1} f^{[p]}(A, t_{\mathfrak{n}}, \omega_A) &= (1 - a_p(f)\beta^{-1}\bar{\beta}^{-1} + \beta^{-1}\bar{\beta}^{-1}) d^{-1} f(A, t_{\mathfrak{n}}, \omega_A) \\ &= (1 - a_p(f)p^{-1} + p^{-1}) d^{-1} f(A, t_{\mathfrak{n}}, \omega_A) \\ &= \left(\frac{1 - a_p(f) + p}{p}\right) d^{-1} f(A, t_{\mathfrak{n}}, \omega_A). \end{aligned}$$

Putting everything together we conclude. Indeed

$$\begin{aligned} L_p(f, K, 1, 1) = d^{-1} f^{[p]}(A, t_{\mathfrak{n}}, \omega_A)^2 &= \left(\frac{1 - a_p(f) + p}{p}\right)^2 d^{-1} f(A, t_{\mathfrak{n}}, \omega_A)^2 \\ &= \left(\frac{1 - a_p(f) + p}{p}\right)^2 F_f(A, t_{\mathfrak{n}}, \omega_A)^2 \\ &= \left(\frac{1 - a_p(f) + p}{p}\right)^2 \log_p(P_{K,f})^2. \end{aligned}$$

□

Following the ideas of (2.1), we can get a corollary of the main theorem, just as we did for corollary 2.1.5 after the Gross–Zagier formula, applying Kolyvagin's theorem 2.1.4. To do this we recall the following

Proposition 2.5.2. *Let $P \in E(K)$. P is a torsion point if and only if $\log_p(P) = 0$.*

So we get, as an easy corollary of the theorem above

Corollary 2.5.3. *With the notations and assumptions as in theorem 2.5.1,*

$$L_p(f, K, 1, 1) \neq 0 \Leftrightarrow P_{K,f} \text{ has infinite order.}$$

Proof. We just need to check that the coefficient on the right hand side of the formula in theorem 2.5.1 is different from zero. Then we can apply the previous proposition and the result follows. But recall that $a_p(f) = a_p$, the p-th coefficient of the L-function associated to E. Since E has good reduction at p ($(N, p) = 1$), we have $a_p = -N_p + p + 1$, where N_p is the number of $\mathbb{F}_p$-points of the reduction of E modulo p and it is strictly greater than 0. Thus $1 - a_p(f) + p \neq 0$. □

Then the main theorem, together with Kolyvagin's result gives us

Corollary 2.5.4. *With the notations and assumptions as in theorem 2.5.1, if $L_p(f, K, 1, 1) \neq 0$ then the rank of $E(K)$ is 1.*

Chapter 3

Examples and applications

The aim of this chapter is to present some concrete examples of how to use the p-adic Gross–Zagier formula we proved, and in particular corollary 2.5.3, to verify if the p-adic L-function vanishes or not in $r = -1$. To do this we will need to deal with the Heegner point associated to K and to look at his order, using some results of Gross and Zagier, and we will see at work both the p-adic and the classical Gross–Zagier formulas. We start by proving some general results, to get more into the theory of Heegner points.

3.1 Example 1: $L_p(f, K, 1, 1) \neq 0$

3.1.1 Gross' criterion

We start by presenting a result, proved by Gross in [Gro86], which will give us an easy sufficient condition for a Heegner point to be of infinite order.

We first need to understand what we hinted in (1.3.2): we want to see Hecke operators, having fixed the level N, as endomorphisms of the Jacobian of the corresponding modular curve. Indeed, using correspondences, we will give a second definition of Hecke operators following [Maz77] and see that the definition given in (1.3.1) can be recovered from it. Then we introduce the concept of Eisenstein prime, again following [Maz77], in order to understand Gross' construction.

Atkin-Lehner involution. We consider the matrix $g_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. It induces an involution on $X_0(N)$, seen as quotient $\Gamma_0(N) \setminus \mathfrak{H}^*$, obtained by $[\tau] \to [g_N\tau] = [-1/N\tau]$. This is easy to see since $g_N(g_N\tau) = g_N(-1/N\tau) = \tau$. Moreover if $[\tau] = [\tau']$, we have $\tau' = \frac{a\tau+b}{c\tau+d}$ with $ad - bc = 1$ and $c \equiv 0 \pmod{N}$. Then

$$g_N\tau' = \frac{-c\tau - d}{Na\tau + Nb} = \begin{pmatrix} d & \frac{c}{N} \\ -Nb & a \end{pmatrix} \left(-\frac{1}{N\tau}\right) = \begin{pmatrix} d & \frac{c}{N} \\ -Nb & a \end{pmatrix} g_n\tau.$$

Since the last matrix is again in $\Gamma_0(N)$, the map is well defined. We also notice that it interchanges the two cusps ∞ and 0. One gets an induced map

$$\begin{aligned} w_N : H^0(X_0(N), \Omega^1) &\to H^0(X_0(N), \Omega^1) \\ f(\tau)d\tau &\mapsto f\left(-\frac{1}{N\tau}\right)\frac{1}{N\tau^2}d\tau. \end{aligned}$$

Recalling that we have a bijection

$$\begin{array}{c} S_2(N) \to H^0(X_0(N), \Omega^1) \\ f(\tau) \longmapsto f(\tau)d\tau, \end{array} \tag{3.1}$$

we then obtain the Atkin-Lehner involution defined on newforms in remark 1.3.4.

Under the moduli interpretation of the modular curve, one actually has that the multiplication by g_N corresponds to

$$(E, C) \mapsto (E/C, E[N]/C), \tag{3.2}$$

where, as always, E is an elliptic curve over $\mathbb{C}$ and C a cyclic subgroup of order N. We denoted with $E[N]$ the N-torsion part of E. To check this, one uses the fact that $\tau \in \mathfrak{H}$ corresponds to $(E, C) = (\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau, 1/N)$, so that $g_N\tau$ corresponds to $(\mathbb{C}/\mathbb{Z} + \mathbb{Z}(-1/N\tau), 1/N)$. Then we have

$$(E/C, E[N]/C) = (\mathbb{C}/\mathbb{Z}1/N + \mathbb{Z}\tau, \tau/N) \xrightarrow{\simeq} (\mathbb{C}/\mathbb{Z} + \mathbb{Z}(-1/N\tau), 1/N),$$

where the last is an isomorphism of marked elliptic curves induced by the multiplication by $-1/\tau$.

Hecke operators as correspondences. To define a correspondence for two curves C_1, C_2, one needs to choose another curve D and two finite morphism α, β in the following way

$$\begin{array}{ccc} & D & \\ {\scriptstyle\alpha}\swarrow & & \searrow{\scriptstyle\beta} \\ C_1 & & C_2. \end{array}$$

The correspondence is the induced map on the Jacobians sending

$$(x) \mapsto \sum_{y \in \alpha^{-1}(x)} (\beta(y)).$$

We will be interested in the case where $C_1 = C_2 =: C$. We then have two natural maps

$$\alpha^* : H^0(C, \Omega^1) \to H^0(D, \Omega^1), \quad \beta_* : H^0(D, \Omega^1) \to H^0(C, \Omega^1).$$

Composing them, we get

$$\beta_* \circ \alpha^* : H^0(C, \Omega^1) \to H^0(C, \Omega^1).$$

Now consider $C = X_0(N)$ as above. We define T_l, for l rational prime not dividing N, to be the correspondence associated to the diagram

$$\begin{array}{ccc} & X_0(lN) & \\ {\scriptstyle\alpha}\swarrow & & \searrow{\scriptstyle\beta} \\ X_0(N) & & X_0(N). \end{array}$$

We now define α and β first as holomorphic maps between Riemann surfaces, then we will see, as we did for w_N, the corresponding interpretation using the moduli spaces structure.

Since $\Gamma_0(lN) \subset \Gamma_0(N)$, we take α to be the natural projection

$$\alpha : \Gamma_0(lN) \setminus \mathfrak{H}^* \to \Gamma_0(N) \setminus \mathfrak{H}^*.$$

It is clear that, in this case, $\alpha : (E, C_l \oplus C_N) \mapsto (E, C_N)$, where E is an elliptic curve over $\mathbb{C}$, and we used the fact that, thanks to the coprimality, every cyclic subgroup of order lN is the direct sum of a cyclic subgroup of order l, C_l, and a cyclic subgroup of order N, C_N.

To define β, we notice that the map $\tau \to l\tau$ defines an isomorphism

$$\Gamma_0(lN) \setminus \mathfrak{H}^* \xrightarrow{\simeq} \gamma\Gamma_0(lN)\gamma^{-1} \setminus \mathfrak{H}^*,$$

with $\gamma = \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}$. Notice that

$$\gamma\Gamma_0(lN)\gamma^{-1} = \Gamma' := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : b \equiv 0 \pmod{l}\ , c \equiv 0 \pmod{N}\}.$$

It is then clear that $\gamma\Gamma_0(lN)\gamma^{-1} \subset \Gamma_0(N)$ and as above we obtain a natural projection. We define β to be the composition of the two:

$$\beta : \Gamma_0(lN) \setminus \mathfrak{H}^* \xrightarrow{\simeq} \Gamma' \setminus \mathfrak{H}^* \to \Gamma_0(N) \setminus \mathfrak{H}^*.$$

In this case one obtains, with the above notation that $\beta : (E, C_l \oplus C_N) \mapsto (E/C_l, C_l \oplus C_N/C_l)$.

Finally we get the description of the correspondence T_l on the Jacobian of $X_0(N)$

$$T_l : (E, C_N) \mapsto \sum_H (E/H, H \oplus C_N/H),$$

where the sum is taken over all cyclic subgroups H of E of order l.

What we claim now is that, using the bijection (3.1), we can recover with the map $\beta_* \circ \alpha^*$ the description of T_l on cusp forms of weight 2. Since α^* is simply the inclusion $S_2(N) \subset S_2(Nl)$ we need to work on β_*. One has

$$\beta_* : f(\tau)d\tau \mapsto \sum_{\substack{\tau' \text{ s.t.} \\ \beta([\tau'])=[\tau]}} f(\tau')d(\tau')$$

Since we know that multiplication by l is an isomorphism between $\Gamma_0(lN) \setminus \mathfrak{H}^*$ and $\Gamma' \setminus \mathfrak{H}^*$, we only need to compute a set of representatives for the quotient $\Gamma_0(N)/\Gamma'$. It is easy to see that this is given by the $l+1$ matrices

$$\gamma_j := \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}, \quad j = 0, \ldots, l-1 \text{ and } \quad \gamma_l = \begin{pmatrix} ml & n \\ N & 1 \end{pmatrix}, \text{ with } m, n \in \mathbb{Z} \text{ s.t. } ml - nN = 1.$$

We finally get

Proposition 3.1.1. *If f is a cusp form of weight 2 and level N, $\beta_* \circ \alpha^*(f) = T_l f$, as defined in (1.3.1).*

Proof. It is now only a simple computation, using the above discussion. Indeed we have, for a differential form $f(\tau)d\tau$ for $X_0(N)$,

$$\begin{aligned}\beta_* \circ \alpha^*(f(\tau)d\tau) = \beta_*(f(\tau)d\tau) &= \sum_{j=0}^{l} f\left(\frac{\gamma_j\tau}{l}\right) d\left(\frac{\gamma_j\tau}{l}\right) \\ &= \frac{1}{l}\sum_{j=0}^{l-1} f\left(\frac{\tau+j}{l}\right) d\tau + f\left(\begin{pmatrix} m & n \\ N & l \end{pmatrix} l\tau\right) \frac{l}{(lN\tau+l)^2} d\tau \\ &= \frac{1}{l}\sum_{j=0}^{l-1} f\left(\frac{\tau+j}{l}\right) d\tau + lf(l\tau)d\tau,\end{aligned}$$

where for the last equality we used the fact that, thanks to the bijection (3.1), f is a cusp form of weight 2. Invoking again that bijection and using the above computation we conclude. □

From now on we denote with J the Jacobian of the modular curve $X_0(N)$. We further assume that N is prime. We can give the following definitions.

Definition 3.1.2. The *Hecke algebra* $\mathbb{T}$ is the subring of $\mathrm{End}(J)$ generated by the Hecke operators T_l for l prime different from N and by the involution w_N.

Definition 3.1.3. The *Eisenstein ideal* $\mathfrak{I} \subset \mathbb{T}$ is the ideal generated by $1 + l - T_l$ for $l \neq N$ and by $1 + w_N$.

One can prove that, letting $m :=\gcd(N-1, 12)$ and $n = (N-1)/m$, the quotient $\mathbb{T}/\mathfrak{I}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, as shown in proposition 9.7 of [Maz77].

Definition 3.1.4. An *Eisenstein prime* is a prime ideal $\mathfrak{P} \subset \mathbb{T}$ in the support of the Eisenstein ideal, i.e. such that $\mathfrak{P} \subset \mathfrak{I}$.

Using $\mathbb{T}/\mathfrak{I} \simeq \mathbb{Z}/n\mathbb{Z}$, we see that the Eisenstein primes are in one to one correspondence with the primes p dividing n, so that such an ideal is in the form $\mathfrak{P} = (\mathfrak{I}, p)$ and $\mathbb{T}/\mathfrak{P} \simeq \mathbb{Z}/p\mathbb{Z}$.

We now consider the completion of $\mathbb{T}$ at an Eisenstein prime $\mathfrak{P} = (\mathfrak{I}, p)$: $\mathbb{T}_\mathfrak{P} := \varprojlim \mathbb{T}/\mathfrak{P}^m$; it is, for what we said above, a $\mathbb{Z}_p$ module. We then define

$$\gamma_\mathfrak{P} := \ker(\mathbb{T} \to \mathbb{T}_\mathfrak{P}) = \bigcap_m \mathfrak{P}^m.$$

We now prove an easy lemma we will need later

Lemma 3.1.5. *$1 + w_N \in \gamma_\mathfrak{P}$ if p is an odd prime and $\mathfrak{P} = (\mathfrak{I}, p)$.*

Proof. The key fact we are using is that w_N is an involution. One then finds

$$\begin{gathered}(1+w_N)^2 = 2 + 2w_N = 2(1+w_N); \\ (1+w_N)^3 = (1+w_N)(1+w_N)^2 = 4(1+w_N); \\ \cdots \\ (1+w_N)^i = 2^{i-1}(1+w_N) \\ \cdots\end{gathered}$$

Moreover, since p is odd, for every i there exists $m_i, n_i \in \mathbb{Z}$ such that $m_i p^{i-1} + n_i 2^{i-1} = 1$. We obtain $n_i(1+w_N)^i + m_i p^{i-1}(1+w_N) = n_i 2^{i-1}(1+w_N) + m_i p^{i-1}(1+w_N) = (1+w_N) \in (p, \mathfrak{I})^i$, since $(1+w_N)^i, p^{i-1}(1+w_N) \in (p, \mathfrak{I})^i$. So we have $(1+w_N) \in \bigcap_i \mathfrak{P}^i$ and we are done. □

Denote with $\gamma_{\mathfrak{P}} \cdot J \subset J$ the sub-abelian variety generated by the images $\alpha \cdot J$ for $\alpha \in \gamma_{\mathfrak{P}}$.

Definition 3.1.6. The *p-Eisenstein quotient of* J is the quotient abelian variety $\tilde{J}^{(p)}$

$$0 \to \gamma_{\mathfrak{P}} \cdot J \to J \to \tilde{J}^{(p)} \to 0.$$

Letting as above $m :=\gcd(N-1, 12)$ and $n = (N-1)/m$, we now consider the meromorphic function on $X_0(N)$

$$f(z) := \left(\frac{\Delta(z)}{\Delta(Nz)}\right)^{1/m}.$$

To recover its q-expansion at ∞ we need the following

Lemma 3.1.7. *The q-expansion of* $\Delta \in S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ *can be written as*

$$\Delta(\tau) = (2\pi)^{12} q \prod_{n \geq 1} (1-q^n)^{24},$$

with $q = e^{2\pi i \tau}$.

Proof. See [Kna92], corollary 8.9, chapter VIII. □

It is now easy to write

$$f(q) = ((2\pi)^{12} q \prod_{n \geq 1} (1-q^n)^{24})^{1/m} ((2\pi)^{12} q^N \prod_{n \geq 1} (1-q^{Nn})^{24})^{-1/m}.$$

We can conclude that f has a pole of order $\frac{N-1}{m} = n$ at ∞ and, since $\mathrm{div}(f)$ is of degree zero and the only other possible zero/pole of f can be at the other cusp $z = 0$ (being $\Delta \neq 0$ for every $z \in \mathfrak{H}$), we must have

$$\mathrm{div}(f) = n(0) - n(\infty).$$

What Gross does, is to consider a homomorphism from the group of degree zero divisors, defined over a fixed subfield F of $\mathbb{C}$ and coprime with the cusps (0) and (∞), to F^*. It is defined by

$$\delta : \sum a_i(x_i) \mapsto \prod f(x_i)^{a_i} \in F^*.$$

Using Weil reciprocity, we find that, on principal divisors, $\delta((g)) = f((g)) = g((f)) = (g(0)/g(\infty))^n$, thus δ induces a homomorphism

$$\delta : J(F) \to F^*/F^{*n} \simeq F^* \otimes \mathbb{Z}/n\mathbb{Z}.$$

Using the isomorphism $\mathbb{T}/\mathfrak{I} \simeq \mathbb{Z}/n\mathbb{Z}$ and the fact that the Eisenstein ideal annihilates the divisor $(0) - (\infty)$ one finds that δ is a homomorphism of Hecke modules and that δ is trivial on $\mathfrak{I}J(F)$. If we consider a prime p dividing n and the corresponding Eisenstein prime $\mathfrak{P}$ we then get that δ induces a homomorphism

$$\delta_p : J(F) \otimes \mathbb{T}_{\mathfrak{P}}/\mathfrak{I}\mathbb{T}_{\mathfrak{P}} \to F^* \otimes \mathbb{Z}_p/n\mathbb{Z}_p.$$

Lemma 3.1.8. *If* $e \in J(F)$ *is such that* $\delta_p(e) \neq 0$, *then* $e \neq 0$ *in* $J(F) \otimes \mathfrak{P}$. *If* e *is not* $\mathfrak{P}$ *-primary torsion, its projection* $e^{(p)}$ *to* $\tilde{J}^{(p)}$ *has infinite order.*

Proof. If $e = 0$, then $\delta_p(e) = 0$, so the first assertion is trivial. For the second one, following Gross, write $k_{\mathfrak{P}} = \mathbb{T}_{\mathfrak{P}} \otimes \mathbb{Q}_p$. One can prove that the projection induces an isomorphism $J(F) \otimes_{\mathbb{T}} k_{\mathfrak{P}} \simeq \tilde{J}^{(p)}(F) \otimes_{\mathbb{T}} k_{\mathfrak{P}}$. We can translate the fact that e is not $\mathfrak{P}$-primary torsion with the condition $e \otimes 1 \neq 0$ in $J(F) \otimes_{\mathbb{T}} k_{\mathfrak{P}}$; hence its projection has infinite order on $\tilde{J}^{(p)}$. □

We now focus on the case where $F = K$ a quadratic imaginary field and the prime $N = \mathfrak{n}\cdot\bar{\mathfrak{n}}$ splits in K. Let p be a odd prime and h the class number of K. Consider the Heegner point $P_K := \sum_{[\mathfrak{a}]\in \mathrm{Pic}(\mathcal{O}_K)} P_{[\mathfrak{a}]} - h(\infty) \in J(K)$, where we recall that $P_{[\mathfrak{a}]}$ correspond to the pair $(\mathbb{C}/\mathfrak{a}, \mathfrak{n}^{-1}\mathfrak{a}/\mathfrak{a})$, we denote this pair with $([\mathfrak{a}], \mathfrak{n})$. This divisor class has some cuspidal support, so we consider

$$e := P_K - \overline{P_K} = \sum_{[\mathfrak{a}]\in \mathrm{Pic}(\mathcal{O}_K)} P_{[\mathfrak{a}]} - \sum_{[\mathfrak{a}]\in \mathrm{Pic}(\mathcal{O}_K)} \overline{P_{[\mathfrak{a}]}}.$$

It is not hard to see that $\overline{P_{[\mathfrak{a}]}}$ corresponds to the pair $([\mathfrak{a}]^{-1}, \bar{\mathfrak{n}})$. Moreover using that, if $E = \mathbb{C}/\mathfrak{a}$ has complex multiplication then $E[N] = E[\mathfrak{n}] \times E[\bar{\mathfrak{n}}] = \mathfrak{n}^{-1}\mathfrak{a}/\mathfrak{a} \times \bar{\mathfrak{n}}^{-1}\mathfrak{a}/\mathfrak{a}$ and using the characterization of the action of w_N on $X_0(N)$ given in (3.2), we find

$$([\mathfrak{a}], \mathfrak{n}) \xrightarrow{w_N} ([\mathfrak{n}^{-1}\mathfrak{a}], \bar{\mathfrak{n}}).$$

Applying this, one gets

$$w_N\Big(\sum_{[\mathfrak{a}]\in Pic(\mathcal{O}_K)} P_{[\mathfrak{a}]}\Big) = \sum_{[\mathfrak{a}]\in Pic(\mathcal{O}_K)} ([\mathfrak{n}^{-1}\mathfrak{a}], \bar{\mathfrak{n}}) = \sum_{[\mathfrak{b}]\in Pic(\mathcal{O}_K)} ([\mathfrak{b}]^{-1}, \bar{\mathfrak{n}}) = \sum_{[\mathfrak{b}]\in Pic(\mathcal{O}_K)} \overline{P_{[\mathfrak{b}]}}.$$

Lemma 3.1.9. *With the above notations, $e^{(p)} = 2P_K^{(p)}$.*

Proof. We have to prove that the difference $e - 2P_K \in \gamma_{\mathfrak{P}} \cdot J$. First of all notice that we can write it as

$$2P_K - e = P_K + \overline{P_K} = \sum_{[\mathfrak{a}]} P_{[\mathfrak{a}]} + \sum_{[\mathfrak{a}]} \overline{P_{[\mathfrak{a}]}} - 2h(\infty).$$

Now we want to compute the image of P_K under $1+w_N$, which is an element of $\gamma_{\mathfrak{P}}$, as proved in lemma 3.1.5. We use what we said in the discussion above.

$$1+w_N(P_K) = 1+w_N\left(\sum_{[\mathfrak{a}]} P_{[\mathfrak{a}]} - h(\infty)\right) = \sum_{[\mathfrak{a}]} P_{[\mathfrak{a}]} - h(\infty) + \sum_{[\mathfrak{a}]} \overline{P_{[\mathfrak{a}]}} - h(0) = 2P_K - e + (h(\infty) - h(0)).$$

We are almost done. Indeed if $h(\infty)-h(0)$ was a principal divisor, then $1+w_N(P_K) = 2P_K - e$ in $J(K)$ and we would get $e-2P_K \in \gamma_{\mathfrak{P}}\cdot J$. But this is true because we can proceed in a similar way as before, letting $g(z) := (\Delta(Nz)/\Delta(z))^{h/(N-1)}$ and we find $(g) = h(\infty) - h(0)$. □

Consider now the ring $A = \mathcal{O}_K[N^{-1}]$ and let h_A be the order of $\mathrm{Pic}(A)$. One has $h = h_A \cdot O(\mathfrak{n})$, where $O(\mathfrak{n})$ is the order of $[\mathfrak{n}]$ in $\mathrm{Pic}(\mathcal{O}_K)$. This can be seen, for example using the exact sequence of abelian groups

$$\mathbb{Z} \to \mathrm{Pic}(\mathcal{O}_K) \to \mathrm{Pic}(A) \to 1,$$

obtained as in proposition 6.5 of [Har77]. In particular the first map is given by $1 \mapsto [\mathfrak{n}]$ and we then obtain the desired relation between the cardinalities.

The theorem we want to prove asserts that $\delta_p(e) \neq 0$ if and only if $ord_p(h_A) < ord_p(n)$. Before stating it in details and proving it, we notice that, from the definition of δ and e, we have

$$\delta_p(e) \equiv \left(\prod_{[\mathfrak{a}]\in \mathrm{Pic}(\mathcal{O}_K)} \frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{n}\mathfrak{a})} \cdot \frac{\Delta(\bar{\mathfrak{n}}\bar{\mathfrak{a}})}{\Delta(\bar{\mathfrak{a}})}\right)^{1/m} \pmod{K^{*n}}, \tag{3.3}$$

where the Δ function is now seen as function on lattices in $\mathbb{C}$. We need to work a bit on this, since the complex numbers of the form $\frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{n}\mathfrak{a})}$ have some nice properties we will need in

the proof. We then make a small digression, following more or less the first paragraphs of chapter IV of [DE66], changing a bit the notation.

Consider H_p to be the set of matrices of integer coprime coefficients and determinant p a prime number. A set of representative of H_p modulo the action of $\mathrm{SL}_2(\mathbb{Z})$ is given by the $p+1$ matrices

$$M_j := \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}, \quad j = 0, \dots, p-1 \text{ and } \gamma_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

For any $M \in H_p$ we define $\varphi_M(\omega_1, \omega_2) := \frac{\Delta(\omega_1,\omega_2)}{p^{12}\Delta(M(\omega_1,\omega_2))}$, where again Δ is seen as function on lattices, i.e. $\Delta(\omega_1, \omega_2) = \omega_2^{-12}\Delta(\omega_1/\omega_2)$, assuming $\omega_1/\omega_2 \in \mathfrak{H}$. This is a homogeneous function of degree 0 in ω_1, ω_2 and it depends only on the class of M in $H_p/\mathrm{SL}_2(\mathbb{Z})$. We then obtain $p+1$ homogeneous functions $\varphi_0, \dots, \varphi_p$, where $\varphi_i := \varphi_{M_i}$. The action of $\mathrm{SL}_2(\mathbb{Z})$ permutes these functions among themselves. Using lemma 3.1.7, we write $\Delta(\omega_1, \omega_2) = (2\pi/\omega_2)^{12} q(1 + B(q))$, where $q = e^{2\pi i \omega_1/\omega_2}$ and $B(q)$ is a power series with integral rational coefficient such that $B(0) = 0$. We can then write for $i = 0, \dots, p-1$

$$\varphi_i(\omega_1, \omega_2) = \zeta_p^{-j} q^{1-1/p}(1 + B(\zeta_p^j q^{1/p-1}))^{-1}(1 + B(q)),$$

where $\zeta_p = e^{2\pi i/p}$. And clearly $\varphi_p(\omega_1, \omega_2) = p^{-12}q^{1-p}(1 + B(pq))^{-1}(1 + B(q))$. From this we see that a symmetric function in the φ_i's can only have the singularity of a pole at ∞ and thus is a polynomial in the variable j, where j is the usual j-function. We find then

$$\phi_p(t) := \prod_{i=0}^{p} (t - p^{-12}\varphi_i(\omega_1, \omega_2)) \in \mathbb{C}(j)[t];$$

we moreover see that the coefficients are actually algebraic integers.

Lemma 3.1.10. *Let $\mathfrak{a}$ be a fractional ideal of the quadratic imaginary field K and (α_1, α_2) a $\mathbb{Z}$-basis such that $\alpha_1/\alpha_2 \in \mathfrak{H}$. For any $M \in H_p$, $\varphi_M(\alpha_1, \alpha_2)$ is an integer in the Hilbert class field H_K of K and the ideal $(\varphi_M(\alpha_1, \alpha_2))$ divides (p^{-12}).*

Proof. Recalling the fact that $j(\mathfrak{a})$ is an algebraic integer (generating H_K over K), we have that $\varphi_M(\alpha_1, \alpha_2) = \varphi_j(\alpha_1, \alpha_2)$ for some j and it satisfies $\phi_p(t, j(\mathfrak{a}))$, which is a monic polynomial with algebraic coefficients, hence it is an algebraic integer.

Moreover, using the above computations, the q-expansion of $\prod \varphi_i(\omega_1, \omega_2)$ starts with the constant term $\prod \zeta_p^{-j} p^{-12} = (-1)^{p-1} p^{-12}$. The second part then follows. □

We finally get the result we need

Proposition 3.1.11. *Let $\mathfrak{a}, \alpha_1, \alpha_2, K$ be as in the lemma. Let p be a prime which splits in K. Write $(p) = \mathfrak{p} \cdot \bar{\mathfrak{p}}$. Let $P \in H_p$ such that $P(\alpha_1, \alpha_2)$ is a $\mathbb{Z}$-basis for $\mathfrak{p} \cdot \mathfrak{a}$. Then*

$$(\varphi_P(\alpha_1, \alpha_2)) = \bar{\mathfrak{p}}^{-12},$$

and then we deduce that $\left(\frac{\Delta(\alpha_1,\alpha_2)}{\Delta(P(\alpha_1,\alpha_2))}\right) = p^{12}\bar{\mathfrak{p}}^{-12} = \mathfrak{p}^{12}$.

Proof. Let f be a positive integer such that $\mathfrak{p}^f = (\alpha)$, for $\alpha \in K$, with $\alpha\bar{\alpha} = p^f$. We can find elements $P_1 = P, P_2, \dots, P_f \in H_p$ such that $P_i P_{i-1} \cdots P_1(\alpha_1, \alpha_2)$ is a basis of $\mathfrak{p}^i \cdot \mathfrak{a}$; in particular $P_f \cdots P_1(\alpha_1, \alpha_2) = (\alpha\alpha_1, \alpha\alpha_2)$. Now let

$$\lambda_i = \varphi_{P_i}(P_{i-1} \cdots P_1(\alpha_1, \alpha_2)) = \frac{\Delta(P_{i-1} \cdots P_1(\alpha_1, \alpha_2))}{p^{12}\Delta(P_i \cdots P_1(\alpha_1, \alpha_2))}.$$

We then find

$$\left(\prod_{i=1}^{f}\lambda_i\right)=\left(\frac{\Delta(\alpha_1,\alpha_2)}{p^{12f}\Delta(P_f\cdots P_1(\alpha_1,\alpha_2))}\right)=\left(\frac{\Delta(\alpha_1,\alpha_2)}{p^{12f}\Delta(\alpha\alpha_1,\alpha\alpha_2)}\right)=\left(\alpha^{12}p^{-12f}\right)=(\bar{\alpha}^{-12})=\bar{\mathfrak{p}}^{-12}.$$

The previous lemma tells us that λ_i is an algebraic integer and we have shown that (λ_i) divides $\bar{\mathfrak{p}}^{-12}$. The lemma also tells us that (λ_i) divides $(p^{-12})=\mathfrak{p}^{-12}\bar{\mathfrak{p}}^{-12}$. We then get that, for every i, $(\lambda_i)=\bar{\mathfrak{p}}^{-12}$. In particular we have $(\varphi_P(\alpha_1,\alpha_2))=\bar{\mathfrak{p}}^{-12}$. □

We can now proceed to the statement and proof of the result of Gross' article.

Theorem 3.1.12. *Let $p>3$ be a prime such that $p\mid n$. With the previous notations, one has*

$$\delta_p(e)\neq 0 \quad \textit{if and only if} \quad ord_p(h_A)<ord_p(n).$$

In this case $P_K^{(p)}$ has infinite order in $J^{(p)}(K)$ (and then P_K has infinite order in $J(K)$).

Proof. Using the above proposition and (3.3) we have that $\delta_p(e)$ is congruent to an element of K^* which generates the ideal $(\mathfrak{n}\bar{\mathfrak{n}}^{-1})^{12h/m}$. Let $\alpha\in K^*$ be a generator of the principal ideal $(\mathfrak{n}\bar{\mathfrak{n}}^{-1})^{O(\mathfrak{n})}$, we can then write

$$\delta_p(e)\equiv\zeta\alpha,$$

where ζ is a unit of K, i.e. a root of unity in K^*.

We claim that α is not a p-th power in K^*. Indeed, if otherwise $\alpha=x^p$, for $x\in K^*$ we would find, using $[\mathfrak{n}\cdot\bar{\mathfrak{n}}^{-1}]=[\mathfrak{n}^2]$,

$$[(x^p)]=[(\mathfrak{n}\cdot\bar{\mathfrak{n}}^{-1})^{O(\mathfrak{n})}]=[\mathfrak{n}^{2O(\mathfrak{n})}]=[(y^2)],$$

where $y\in\mathbb{K}^*$ is a generator of the principal ideal $\mathfrak{n}^{O(\mathfrak{n})}$. So we would find $z\in K^*$ such that $y^2=zx^p$ and this is not possible since $p\neq 2$. Since $(12/m,p)=1$, we also have that $\alpha^{12/m}$ is not a p-th power.

It is easy to see that ζ is a p-th power. Indeed the possible values of ζ, being K a quadratic imaginary field, are $\pm1,\pm i,\zeta_6^j$ for, $j=1,\dots,5$. We have $-1=(-1)^p$ and we also can write $i=i^p$ if $p\equiv 1 \pmod 4$ or $i=(-i)^p$ if $p\equiv 3 \pmod 4$; moreover using $(p,6)=1$ we can find k,l such that $1=6l+pk$ and then $\zeta_6=(\zeta_6^k)^p$. Notice that this discussion also implies that ζ is a p^k-th power for every k. We then have that $\delta_p(e)$ is a p^k-th power if and only if $h_A\equiv 0 \pmod{p^k}$. We can then conclude that $\delta_p(e)\neq 0$ in $K^*/K^{*n}\otimes\mathbb{Z}_p$ if and only if $\mathrm{ord}_p(h_A)<\mathrm{ord}_p(n)$.

If this is the case and if we prove that e is not $\mathfrak{P}$-primary torsion, we can apply lemma 3.1.8 to conclude that $e^{(p)}=2P_K^{(p)}$ has infinite order and so has $P_K^{(p)}$. Using the fact that $\bar{e}=-e$, we would find, if e was $\mathfrak{P}$-primary torsion, a non trivial element in the minus space for complex conjugation of $J[\mathfrak{P}](K)$, which is not possible because of the determination of the $\mathfrak{P}$ primary torsion part of J given by Mazur, $J[\mathfrak{P}]=\mathbb{Z}/p\mathbb{Z}\oplus\mu_p$ □

3.1.2 A Heegner point of infinite order

We now want to give an example of how to apply this result. First we need to fix an elliptic curve. We want to consider the modular curve $X_0(11)$, which will turn out to be an elliptic curve itself. This way the modular parametrization will simply be the identity and we will also have a concrete description of the associated newform. We proceed by steps.

Step 1: The modular curve $X_0(11)$

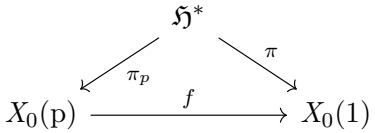
We first prove a general result which will help us showing that $X_0(11)$ is actually an elliptic curve.

Proposition 3.1.13. *Let p be a rational prime such that $p \equiv -1$ (mod 12), then the genus of the modular curve $X_0(p)$ is $\frac{p+1}{12}$.*

Proof. Let

$$f : X_0(\mathrm{p}) \to X_0(1)$$

be the natural projection induced by $\Gamma_0(\mathrm{p}) \subset \Gamma = \mathrm{SL}_2(\mathbb{Z})$. We have the commutative diagram



where π_p, π are the natural projections. We start by proving the following

Lemma 3.1.14. *f is a morphism of Riemann surfaces of degree $p+1$. Moreover*

i. $\#\{x \in X_0(\mathrm{p}) \,|f(x) = \pi(i)\} = \frac{p+1}{2}$ *and for every such element $mult_x(f) = e_x(f) = 2$,*

ii. $\#\{x \in X_0(\mathrm{p}) \,|f(x) = \pi(\rho)\} = \frac{p+1}{3}$ *and for every such element $e_x(f) = 3$,*

iii. $e_0(f) = p$,

iv. $e_\tau(f) = 1$, *otherwise.*

Proof of the lemma. We will prove that f is a morphism of Riemann surfaces showing that for every complex chart (U_p, ϕ_{U_p}) of $X_0(\mathrm{p})$ and for every complex chart (U, ϕ_U) of $X_0(1)$ such that $U_p \cap f^{-1}(U) \neq \emptyset$, $\phi_U \circ f \circ \phi_{U_p}^{-1}$ is holomorphic. Doing this we will discover also the ramification point and the multiplicity.
We know that for every $x \in X_0(\mathrm{p})$ (respectively $x \in X_0(1)$), if $Stab_{\Gamma_0(\mathrm{p})}(x) = \{\pm 1\}$ (respectively $Stab_\Gamma(x) = \{\pm 1\}$) a local chart is given by π_p^{-1} (respectively π^{-1}) restricted to a suitable neighbourhood. Moreover we know that this is always possible if $\pi_p^{-1}(x) \neq \rho, i, \infty, 0$, so in such a neighbourhood of x we find that $\phi_U \circ f \circ \phi_{U_p}^{-1}$ is the identity. So it is holomorphic and the multiplicity of x is equal to 1.
We now consider the case $x = \pi_p(\phi_j^{-1}(i))$, where $\phi_j = T^{-j}S$. Recalling that $\Gamma = \coprod_{j=0}^{p} \Phi_j \cdot \Gamma_0(\mathrm{p})$ and that $F(p) = \bigcup_{j=0}^{p} \Phi_j^{-1}(F(1))$ is a fundamental domain for $Y_0(\mathrm{p})$, we see that this are all the points of $X_0(\mathrm{p})$ such that $f(x) = \pi(i)$. Now we use the following fact, which is not hard to prove: there exists $\gamma \in \Gamma_0(\mathrm{p})$ such that $\gamma\phi_k^{-1}(i) = \phi_j^{-1}(i)$ if and only if $kj \equiv -1($ mod $p)$ or $j = 0, k = p$. Noticing that $p \equiv_{12} -1$ implies $p \equiv_4 3$, we have that $j^2 \not\equiv_p -1$ and so $\gamma\phi_j^{-1}(i) \neq \phi_j^{-1}(i)$ for every j, hence their stabilizer in $\Gamma_0(\mathrm{p})$ is trivial and the charts are given locally by π_p^{-1}. Moreover since $\pi_p(\phi_0^{-1}(i)) = \pi_p(\phi_p^{-1}(i))$ and $\pi_p(\phi_j^{-1}(i)) = \pi_p(\phi_k^{-1}(i))$ for $\frac{p-1}{2}$ distinct couples, we have exactly $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ elements in $X_0(\mathrm{p})$ that are mapped to $\pi(i)$. Using the definition of the chart in the neighbourhood of $\pi(i) \in X_0(1)$ we have that in this case

$$\phi_U \circ f \circ \phi_{U_p}^{-1} : \tau \longmapsto \left(\frac{\tau - i}{\tau + i}\right)^2.$$

Hence, being $\frac{\tau-i}{\tau+i}$ a biholomorphism restricted to our suitable neighbourhood, and characterizing the multiplicity as "local numbers of preimages", we have that $e_x(f) = 2$ for every $x \in f^{-1}(\pi(i))$. This also gives us

$$\deg f = \sum_{x \in f^{-1}(\pi(i))} e_x(f) = 2 \cdot \frac{p+1}{2} = p+1.$$

Now we can use the same reasoning applied to the case $x = \pi_p(\phi_j^{-1}(\rho))$. Here we have $\phi_j \gamma \phi_k^{-1} = ST, (ST)^2$, for the characterization of the stabilizer in Γ. Hence, in particular, $Stab_{\Gamma_0(\mathrm{p})}(\phi_j^{-1}(\rho))$ is non trivial if and only if $j(1-j) \equiv 1$ or $j(j+1) \equiv_p -1$ (this is, as above, a not too hard computation). So we are looking for solutions in $\mathbb{F}_p$ of $X^2 - X + 1 = 0$ and of $X^2 + X + 1 = 0$. The solutions would be in the form

$$\frac{1 \pm \sqrt{-3}}{2}, \frac{-1 \pm \sqrt{-3}}{2},$$

so if we show that -3 is not a square modulo p (i.e. $\left(\frac{-3}{p}\right) = -1$), we have proved $Stab_{\Gamma_0(\mathrm{p})}(\phi_j^{-1}(\rho))$ is trivial. But now we use the properties of Legendre symbol and the fact that $p \equiv_4 3$ and we get

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

Now, applying the reciprocity law and $p \equiv_4 3$, we have

$$\left(\frac{3}{p}\right) = (-1)^{\frac{2(p-1)}{4}} \left(\frac{p}{3}\right) = -\left(\frac{p}{3}\right)$$

since $p \equiv_3 2$ (using again $p \equiv_{12} -1$) is not a square.
So as before we have, using π_p^{-1} as chart around $\pi_p(\phi_j^{-1}(\rho))$ and the usual one around $\pi(\rho)$

$$\phi_U \circ f \circ \phi_{U_p}^{-1} : \tau \longmapsto \left(\frac{\tau - \rho}{\tau - \overline{\rho}}\right)^3.$$

As before, this tells us that $e_x(f) = 3$ for every x such that $f(x) = \pi(\rho)$. To count the preimages of $\pi(\rho)$ (i.e. the cardinality of $\Gamma_0(\mathrm{p}) \cdot \{\phi_j^{-1}(\rho)\}_{j=0}^p$) we use that we already know that the degree of f is $p+1$, so:

$$p+1 = \sum_{x \in f^{-1}(\pi(\rho))} e_x(f) = 3 \cdot \#\{f^{-1}(\pi(\rho))\}$$

and we get $\#\{f^{-1}(\pi(\rho))\} = \frac{p+1}{3}$. Now notice that $f^{-1}(\pi(\infty)) = \{\pi_p(\infty), \pi_p(0)\}$. Since $Stab_\Gamma(\infty) = Stab_{\Gamma_0(\mathrm{p})}(\infty) =< T >$, the charts around $\pi(\infty)$ and around $\pi_p(\infty)$ are defined in the same way and hence $\phi_U \circ f \circ \phi_{U_p}^{-1}$ is the identity. So $\pi_p(\infty)$ is unramified and the formula about the degree tells us

$$p+1 = \sum_{x \in f^{-1}(\pi(\infty))} e_x(f) = 1 + e_{\pi_p(0)}(f)$$

and we get $e_{\pi_p(0)}(f) = p$.
If we want to be precise and show holomorphicity at $\pi_p(0)$, we know that the chart around $\pi_p(0)$ is given by $\pi_p(\tau) \mapsto e^{\frac{2\pi i}{h}\gamma(\tau)} =: q_\tau$ (for some γ and h) and hence

$$\phi_U \circ f \circ \phi_{U_p}^{-1} : q \longmapsto \pi(\tau) = \pi(\gamma(\tau)) \mapsto e^{2\pi i \gamma(\tau)} = q^h$$

is holomorphic and h must be p. □

To compute the genus we want to apply Hurwitz formula. We need to calculate the index of ramification:

$$\begin{aligned} r_f &= \sum_{x \in X_0(\mathrm{p})} (e_x(f) - 1) = \sum_{x \in f^{-1}(\pi(\rho))} 2 + \sum_{x \in f^{-1}(\pi(i))} 1 \; + \; (p-1) \\ &= \frac{p+1}{3} \cdot 2 + \frac{p+1}{2} + p - 1 = \frac{13p+1}{6} \end{aligned}$$

Now using $2 - 2g = \deg f(2 - 2g(X_0(1))) - r_f$ and $g(X_0(1)) = 0$, we have

$$g = \left(2 - 2(p+1) + \frac{13p+1}{6}\right)\frac{1}{2} = \frac{p+1}{12}.$$

□

Applying the proposition for $p = 11$, which clearly satisfies the hypothesis, we get that the genus of $X_0(11)$ is 1. So, since it is a nonsingular curve of genus one, it is an elliptic curve over $\mathbb{Q}$. Moreover since the jacobian of an elliptic curve is isomorphic to the elliptic curve itself, the modular parametrization is the identity.

One can find in different ways an explicit equation for such an elliptic curve, see for example [Wes]. Moreover it has conductor 11 and it can be shown, see [Cre97] p.110, that $X_0(11)(\mathbb{Q})$ has rank 0.

Step 2: The newform associated to $X_0(11)$

To find the newform associated to $X_0(11)$ we first recall bijection (3.1)

$$S_2(N) \xrightarrow{1:1} \Omega^1(X_0(N)).$$

So, applying proposition 3.1.13, one gets $\dim_{\mathbb{C}}(S_2(11)) = g(X_0(11)) = 1$, so that $S_2(11) \neq \{0\}$. Let s be any non-zero weight 2 cusp form of level 11. We will use it in order to find an explicit generator (as $\mathbb{C}$-vector space) of $S_2(11)$.

To do this we first look for a cusp form of weight 24 and level 11. Let $\Delta(z) \in S_{12}(SL_2(\mathbb{Z}))$ be the discriminant function. Denote with Δ_{11} the function defined on $\mathfrak{H}$ by $\Delta_{11}(z) := \Delta(11 \cdot z)$ and set $h_{11} := \Delta \cdot \Delta_{11} \in S_{24}(11)$. One can easily see, looking at the q-expansion, that h_{11} has a zero of order 12 at ∞. Moreover one computes the order of h_{11} at $\mathbf{0}$, the other cusp, finding that h_{11} has a zero of order 12 in $\mathbf{0}$.

Now take $0 \neq s \in S_2(\Gamma_0(11))$ and consider $f := \frac{s^{12}}{h_{11}}$ as a meromorphic function on $X_0(11)$. Since s is holomorphic and has two zeroes of order greater or equal then 12 in $\pi_{11}(0)$ and $\pi_{11}(\infty)$, f is holomorphic (remind that h_{11} has no zeroes different from $\pi_{11}(0)$ and $\pi_{11}(\infty)$ and that their order is equal to 12). Being $X_0(11)$ a compact Riemann surface, this implies $f = \lambda \in \mathbb{C}^*$ constant. So we can write $\sqrt[12]{h_{11}} = \frac{1}{\sqrt[12]{\lambda}} \cdot s$. We denote with h the cusp form $\sqrt[12]{h_{11}}$ multiplied by a suitable constant, so that the coefficient of q in the q-expansion at infinity is 1. We then have $S_2(\Gamma_0(11)) = \mathbb{C} \cdot h$.

Since the modularity theorem ensures that there exists a newform associated to $X_0(11)$, it must be h: indeed every other cusp form of weight 2 can not be normalized since it is a multiple of h.

Notice in particular that, from the construction, we get that $h(\tau) \neq 0$ for every $\tau \in \mathfrak{H}$. We can also present the q-expansion of h, using lemma 3.1.7.

Proposition 3.1.15. *The q-expansion at infinity of $h \in S_2(\Gamma_0(11))$ is*

$$h(\tau) = q \prod_{n \geq 1} (1-q^n)^2 (1-q^{11n})^2.$$

Proof. From the lemma we can recover the q-expansion at infinity of Δ_{11}. We get

$$\Delta_{11}(\tau) = \Delta(\tau)\Delta(11\tau) = (2\pi)^{24} q^{12} \prod_{n \geq 1} (1-q^n)^{24} (1-q^{11n})^{24}.$$

To conclude, one just recall that h was defined as the 12-th root of this cusp form, multiplied by a scalar so that it is normalized. □

Step 3: the field K

Another ingredient we need to apply our theorem is a quadratic imaginary field K satisfying the Heegner hypothesis and all our assumptions; we moreover need to choose a prime p such that $p \neq 11$ and p splits in K. Summarizing we want the following facts to be verified:

1. 11 splits or ramifies in K and then there exists an ideal $\mathfrak{n}$ in $\mathcal{O}_K$ of norm 11;
2. the discriminant D of K is odd;
3. $\mathrm{Pic}(\mathcal{O}_K)$ is trivial;
4. $\mathcal{O}_K^\times = \{\pm 1\}$;
5. $p \neq 11$ is a rational prime which splits in K.

The only quadratic imaginary fields whose group of units is bigger than $\{\pm 1\}$ are $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. Moreover there are only a finite number of quadratic imaginary fields, among the remaining ones, whose class group is trivial; they are in the form $\mathbb{Q}(\sqrt{D})$ with

$$D \in \{-2, -7, -11, -19, -43, -67, -163\}.$$

In order to have odd discriminant, we need to pick one of the odd D, since they are all congruent to 1 modulo 4. One can see that 11 is inert in $\mathbb{Q}(\sqrt{-7})$. We proceed with the next one and then claim

Claim. $K = \mathbb{Q}(\sqrt{-11})$ together with $p = 5$ satisfies the hypotheses 1. to 5. above.

Proof. We have already discussed points 2. to 4. Moreover since 11 divides the discriminant, it ramifies in K and there exists a unique ideal of norm 11. Now we check that 3 splits in K. The minimal polynomial of the ring of integers is $X^2 - X + 3$. We have $X^2 - X + 3 = X(X-1) \pmod 3$ and thus 3 splits in K. □

Step 4: the Heegner point P_K

As we said before, in this case the modular parametrization is just the identity, so, with the notation introduced in (2.5), we have that $P_{K,h} = P_K$.

What we want to do is to show that $L_3(h, K, 1, 1) \neq 0$, and applying the results above, it will be enough to prove that P_K is a point of infinite order (and, then that the rank of

$X_0(11)(K)$ is 1). But we can now apply theorem 3.1.12, with $N = 11$ and $p = 5$. Indeed in this case $h_A = 1$ and $gcd(N-1, 12) = 2$ so that $n = 5$. Then we have

$$ord_5(h_A) = 0 < ord_5(n) = 1$$

and we get that P_K has infinite order as we wanted.

Remark 3.1.16. The hypothesis that the class group of K is trivial has been used only to explicit some computations concerning the Coleman primitive and the p-adic L-function. Removing this restrictive hypothesis and using an analogue of theorem 3.1.12 one has plenty of examples where the Heegner point is of infinite order. It is indeed enough to take an elliptic curve with prime conductor N and fix a prime p dividing $n = (N-1)/gcd(N-1, 12)$, so that $ord_5(n) > 0$. We can then take any imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$ where N, p split, i.e. such that

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

and with class number h such that $p \not| h = c \cdot h_A$. This is enough because this way we have that p does not divide h_A and $ord_p(h_A) = 0$.

3.2 Example 2: $L_p(f, K, 1, 1) = 0$

On the other side now, following [Zag84] and using the classical Gross–Zagier formula, we want to give an example of an elliptic curve of rank 3 with trivial Heegner point. In order to do so we need a brief discussion about the L-series $L(E/K, s)$ of an elliptic curve $E/\mathbb{Q}$ associated to a quadratic imaginary field K.

3.2.1 The L-function $L(E/K, s)$

Let K be a quadratic imaginary field with square free discriminant $-D > 0$, so that $K = \mathbb{Q}(\sqrt{D})$ and let E be an elliptic curve defined over $\mathbb{Q}$, say given by $E : y^2 = x^3 + ax + b$.

Definition 3.2.1. The *quadratic twist of E by K* is the elliptic curve E^D over $\mathbb{Q}$ given by the equation $Dy^2 = x^3 + ax + b$.

Remark 3.2.2. Such an elliptic curve is named twist of E since E^D becomes isomorphic to E over $\bar{\mathbb{Q}}$, even already over K. It is indeed enough to take the isomorphism

$$E^D(K) \to E(K)$$
$$(x, y) \mapsto (\sqrt{D}x, y)$$

Let $L(E^D, s)$ be the L-function associated to $E^D/\mathbb{Q}$ and $L(E, s)$ the one associated to $E/\mathbb{Q}$. One has

$$L(E/K, s) = L(E, s) \cdot L(E^D, s).$$

From this and using the remark 0.4.4, one gets

Lemma 3.2.3. *With the above notations*

- *if* $\varepsilon_E = 1$, $L'(E/K, 1) = L'(E, 1) \cdot L(E^D, 1)$
- *if* $\varepsilon_E = -1$, $L'(E/K, 1) = L(E, 1) \cdot L'(E^D, 1)$

Example 3.2.4. We have that, for $E = X_0(11)$, $\varepsilon_E = -1$. Indeed $X_0(11)$ is a semistable elliptic curve, since it has bad reduction only of split multiplicative type (and only at $p = 11$). In this case the sign of the functional equation of $L(E, s)$ is given by $(-1)^{s+1}$ where s is the number of primes of split multiplicative reduction, in this case $s = 1$ and thus $-\varepsilon_E = 1$. Recalling that the Heegner point P_K chosen as before is of infinite order, the Gross–Zagier formula tells us that $L'(E/K, 1) \neq 0$. Thus the above lemma tells us that $L(E, 1) \neq 0$, thus the analytic rank of E is equal to zero which is equal to the rank of $E(\mathbb{Q})$, as asserted by the Birch and Swinnerton-Dyer conjecture.

Clearly also $L(E/K, s)$ satisfies a functional equation $\Lambda(E/K, s) = \pm\Lambda(E/K, 2-s)$ for a suitable $\Lambda(E/K, s)$. Another interesting fact is that the sign of this functional equation can be computed explicitly.

Theorem 3.2.5. *If E is an elliptic curve over $\mathbb{Q}$ of conductor N and K is a quadratic imaginary field the sign of the functional equation of $L(E/K, s)$ is given by $(-1)^{\#S_{E,K}}$, where*

$$\#S_{E,K} = \{\lambda \text{ prime of } K : \lambda | l | N \text{ and } E \text{ has split multiplicative reduction at the prime } l\} \cup \{\infty\}.$$

Corollary 3.2.6. *If K is a quadratic imaginary field where every prime dividing the conductor N splits, the sign of the functional equation of $L(E/K, s)$ is -1 and in particular, with the above notation, $\varepsilon_E \cdot \varepsilon_{E^D} = -1$.*

Proof. The set $\{\lambda$ prime of $K : \lambda | l | N$ and E has split multiplicative reduction at the prime $l\}$ has even cardinality, since for every prime l dividing the conductor we find two primes λ_1, λ_2 in K dividing N. Thus $\#S_{E,K}$ is odd and we apply the theorem. □

3.2.2 A trivial Heegner point

We know consider the elliptic curve E given by $y^2 = x^3 + 10x^2 - 20x + 8$. It has conductor $N = 37$. Next consider $K = \mathbb{Q}(\sqrt{-139})$, since $-139 \equiv 1 \pmod 4$, it has odd discriminant. Moreover N splits in K since $-139 \equiv 9 \pmod{37}$ and hence it is a square; write $(37) = \mathfrak{n}\bar{\mathfrak{n}}$. Since $\mathcal{O}_K = \mathbb{Z}[x]$ where $x = (1 + \sqrt{-139})/2$ has minimal polynomial $X^2 - X + 35$, and $X^2 - X + 35 = (X - 2)(X - 1) \pmod{37}$, we can write $\mathfrak{n} = (x - 2, 37), \bar{\mathfrak{n}} = (x - 1, 37)$. Thus K satisfies the Heegner hypothesis. We then do the following

Claim. The class group of K is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ and it is generated by a prime ideal of norm 5.

Proof. We proceed in the standard way, computing the Minkowsky bound, which is less than 8. The generators of the class group are then the (classes of the) prime ideals dividing $2, 3, 5, 7$. We have $\mathcal{O}_K = \mathbb{Z}[x]$ where x has minimal polynomial $X^2 - X + 35$. It is irreducible both modulo 2 and 3, thus they are inert and trivial in the class group. Modulo 5 and 7 we have $X^2 - X + 35 \equiv X(X - 1)$, thus $5\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ and $7\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$, with $\mathfrak{p} = (5, x), \bar{\mathfrak{p}} = (5, x - 1), \mathfrak{q} = (7, x), \bar{\mathfrak{q}} = (7, x - 1)$. An easy computation on the norms shows that they are all non principal. Moreover the norm of x is 35 and thus $(35) = \mathfrak{p}\mathfrak{q}$, so that $[\mathfrak{q}] = [\mathfrak{p}]^{-1}$. If we show that $\mathfrak{p}^3$ is principal we are done, since this implies that its order is 3 and it is a generator of the class group. It is enough to take $9 + x$, whose norm is 125, it is contained in $\bar{\mathfrak{p}}$, but not in $\mathfrak{p}$, thus $(9 + x) = \bar{\mathfrak{p}}^3$, so that $[\mathfrak{p}] = [\bar{\mathfrak{p}}]^{-3} = 1$. □

We now want to find three points z_i in $\mathfrak{H}$ corresponding to the three points on $X_0(37)$ associated to the three isomorphism classes of elliptic curves with complex multiplication by the maximal order in K. Consider, letting $y = \sqrt{-139}$,

$$\tau_1 = \frac{-3+y}{2} = x-2, \quad \tau_2 = \frac{71+y}{2} = x+35, \quad \tau_3 = \frac{-151+y}{2} = x-76$$

and the three lattices

$$\Lambda_1 = 37\mathbb{Z} \oplus \tau_1\mathbb{Z}, \quad \Lambda_2 = 37\cdot 5\mathbb{Z} \oplus \tau_2\mathbb{Z}, \quad \Lambda_1 = 37\cdot 5\mathbb{Z} \oplus \tau_3\mathbb{Z}.$$

They are integral ideals of K of norm, respectively, $37, 37\cdot 5, 37\cdot 5$. In particular notice that $\Lambda_1 = \mathfrak{n}$ and, since $\tau_2 = (x-2)+37 = x+7\cdot 5$, Λ_2 is contained in $\mathfrak{n}$ and in $\mathfrak{p}$, thus $\Lambda_2 = \mathfrak{p}\mathfrak{n}$; similarly $\tau_3 = (x-2)-37\cdot 2 = (x-1)-15\cdot 5$, Λ_3 is contained in $\mathfrak{n}$ and in $\bar{\mathfrak{p}}$, thus $\Lambda_3 = \bar{\mathfrak{p}}\mathfrak{n}$. In this way $(\mathbb{C}/\Lambda_1 \to \mathbb{C}/\mathcal{O}_K), (\mathbb{C}/\Lambda_2 \to \mathbb{C}/\mathfrak{p}), (\mathbb{C}/\Lambda_3 \to \mathbb{C}/\bar{\mathfrak{p}})$ are the three representatives of the cyclic isogenies of order 37 of elliptic curves with complex multiplication by $\mathcal{O}_K$. The corresponding points in $\mathfrak{H}$ are

$$z_1 = \tau_1/37, \quad z_2 = \tau_2/(37\cdot 5), \quad z_3 = \tau_3/(37\cdot 5)$$

Looking at the modular curve $X_0(37)$ as quotient $\Gamma_0(37)\setminus\mathfrak{H}^*$, the Heegner point P_K is given by the class of the degree zero divisor

$$(z_1)+(z_2)+(z_3)-3(\infty).$$

Claim. P_K is trivial in $J_0(37)(K)$ and thus the corresponding Heegner point on E is trivial.

Proof. To prove this we need to show that the divisor $(z_1)+(z_2)+(z_3)-3(\infty)$ is principal. We consider the following matrices in $\mathrm{SL}_2(\mathbb{Z})$

$$A_1 = \begin{pmatrix} -3 & -1 \\ 1 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} -77 & -31 \\ 5 & 2 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 34 & -7 \\ 5 & -1 \end{pmatrix}.$$

Some computations show that for $i = 1,2,3$, one has $37z_i = A_i z_i$ and $(c_i z_i + d_i) = z_1$ for every i, where c_i, d_i are the entries of the second row of A_i. Letting $\alpha := z_1^{-1}$, we then define, for every $\tau \in \mathfrak{H}$

$$g(\tau) := \sqrt[12]{\frac{\Delta(\tau)}{\Delta(37\tau)}} - \alpha.$$

This is a meromorphic function on $\Gamma_0(37)\setminus\mathfrak{H}^*$. We find, for every i

$$g(z_i) = \sqrt[12]{\frac{\Delta(z_i)}{\Delta(37z_i)}} - \alpha = \sqrt[12]{\frac{\Delta(z_i)}{\Delta(A_i z_i)}} - \alpha = \sqrt[12]{(cz_i+d_i)^{-12}} - \alpha = 0.$$

As we did many times, using the q-expansion of Δ at ∞ we find that g has a pole of order 3 at ∞, thus $(g) = (z_1)+(z_2)+(z_3)-3(\infty)$ and we are done. □

What we can now conclude is that, as we wanted, if f is the newform associated to E and p is any prime splitting in K and different from 37, then $L_p(f,K,1,1) = 0$. Notice that Tchebotarev density theorem tells us that there are infinitely many such primes.

Remark 3.2.7. All these computations about the triviality of the Heegner point can actually allow us to conclude more, using the classical Gross–Zagier formula. Applying it we indeed have the vanishing also of the the classical L function: $L(E/K, 1) = 0$. Arguing as before, since E has split multiplicative reduction only at $p = 37$, we get $\varepsilon_E = -1$. We then know that $\varepsilon_{E^{-139}} = 1$. Moreover applying lemma 3.2.3 and that, in fact, $L(E, 1) \neq 0$, one finds that $L'(E^{-139}, 1) = 0$, so that the next possible order of non-vanishing of this function is 3. Indeed $L^{(3)}(E^{-139}, 1) \neq 0$ and we found an elliptic curve of analytic rank 3 (that is easily seen to have also algebraic rank equal to 3, compatibly with the Birch and Swinnerton-Dyer conjecture).

Notice, to conclude, that the interesting point of the Gross–Zagier formula and also of the p-adic analogue we presented here is that they are *closed* formulae where on one side we have something hard to understand (the value of the first derivative of $L(E/K, s)$ in 1 in the first case, the p-adic L-function evaluated in a point outside the domain of interpolation in the second one) and on the other side we have much more understandable quantities. Indeed as we showed in this last chapter dealing with Heegner points it is, somehow, very concrete. One can also notice that the values $L(E/K, 1)$ and $L_p(K, f, 1, 1)$ can be approximated computationally. In the first case one uses the fact that the L-function is the Mellin transform of the associated newform and for the p-adic version one has some computational tools as well, as showed for example in [Lau14]. However approximation can be helpful to prove that something is different from zero, while proving that it is exactly equal to zero can not be done without the help of such closed formulae. Indeed, since we don't have a Gross–Zagier analogue for the third derivative of the L-function, it is not yet known an example of elliptic curve of analytic rank strictly bigger than 3, even if it easy to find elliptic curves of algebraic rank bigger than 3. The approximation methods in these cases show that $L^{(3)}(E, 1)$ is close to zero, but one can not prove it is actually equal to zero.

Appendix A

Euler system of Heegner points for bounding Selmer groups

In this appendix we want to give some ideas of how, given an elliptic curve E over $\mathbb{Q}$ of conductor N and a quadratic imaginary field K, one can use the construction of Heegner points as in (1.3.9) to bound a Selmer group of the E. We will further assume that K satisfies the Heegner hypothesis, assuming that all prime factors of N split in K.

A.1 A weaker version of Kolyvagin's result

We denote with P_K the Heegner point on $E(K)$. Recall the result of Kolyvagin we stated in theorem 2.1.4:

Theorem A.1.1. *If P_K is of infinite order, then*

(1) $E(K)$ has rank 1,

(2) the Tate-Shafarevic group $Ш(E/K)$ is finite.

Following [Gro91], we will sketch briefly how to prove a slightly weaker result, namely

Theorem A.1.2. *If p is an odd prime such that $Gal(\mathbb{Q}(E_p)/\mathbb{Q}) = GL_2(\mathbb{Z}/p\mathbb{Z})$ and p does not divide P_K in $E(K)$. Then*

(1) $E(K)$ has rank 1,

(2) the p-torsion subgroup of the Tate-Shafarevic group $Ш(E/K)_p$ is trivial.

To justify the assumptions on p in the above theorem we say that, first of all, it has been proved by Mazur that if E is semi-stable (and this is the case since N is square-free), the Galois group of $\mathbb{Q}(E_p)/\mathbb{Q}$ is isomorphic to $GL_2(\mathbb{Z}/p\mathbb{Z})$ for all $p \geq 11$. Moreover the Mordell-Weil theorem tells us that $E(K)$ is finitely generated, hence if P_K has infinite order, then it is not divisible by p in $E(K)$ for almost every p. So we can prove the first part of theorem A.1.1 taking one of these primes and applying theorem A.1.2.

We consider the usual exact sequence of $\mathbb{Z}/p\mathbb{Z}$-modules

$$0 \to E(K)/pE(K) \xrightarrow{\delta} \mathrm{Sel}(E/K)_p \to Ш(E/K)_p \to 0.$$

Theorem A.1.2 is a corollary of the following

Theorem A.1.3. *If p is an odd prime such that $Gal(\mathbb{Q}(E_p)/\mathbb{Q}) = GL_2(\mathbb{Z}/p\mathbb{Z})$ and p does not divide P_K in $E(K)$, then the p-Selmer group $\mathrm{Sel}(E/K)_p$ is cyclic generated by δP_K*

Indeed using the above exact sequence we get that the subgroup $E(K)/pE(K)$ is again cyclic and it is generated by P_K. Thus $Ш(E/K)_p = 0$ and, using the fact that $E(K)$ contains no p-torsion (otherwise $\mathbb{Q}(E_p) \cap K = K$ and this contradicts our hypothesis on the Galois group, whose cardinality is p^2 and is not divisible by 2), we have also that the rank of $E(K)$ is equal to one.

A.2 Heegner points and cohomology classes

We review the construction of the Euler system of Heegner points on E, proving only some of their properties and showing how to build up some cohomology classes attached to them.

As in the previous chapters, we denote with $\mathfrak{n}$ the ideal of $\mathcal{O}_K$ of norm N, which exists thanks to Heegner hypothesis. For every $n \geq 1$ square-free and coprime with N, p as in the above theorems and denoting with D the discriminant of K, let $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ be the order of conductor n. The ideal $\mathfrak{n}_n = \mathfrak{n} \cap \mathcal{O}_n$ satisfies $\mathcal{O}_n/\mathfrak{n}_n \simeq \mathbb{Z}/N\mathbb{Z}$. As we did for $n = 1$, we then can define a point x_n on $X_0(N)$, defined over $K(j(\mathcal{O}_n)) = K_n$ (theorem 0.3.4). Using the modular parametrization we define $y_n := \phi_N(x_n)$; notice that $P_K = Tr_{K_1/K} y_1$, where $K_1 = H$ the Hilbert class field of K.

Denote with τ the complex conjugation.

Claim. The complex conjugation τ acts on $Gal(K_n/K)$ by

$$\tau\sigma\tau^{-1} = \sigma^{-1}. \tag{A.1}$$

Proof. Since σ fixes K and we have the characterization $K_n = K(j(\mathcal{O}_n))$, we just need to check that $\tau\sigma(j(\mathcal{O}_n)) = \sigma^{-1}\tau(j(\mathcal{O}_n))$. We use theorem 0.3.3: if σ corresponds to (the class) of the $\mathcal{O}_n$-proper ideal $\mathfrak{b}$, then $\sigma(j(\mathcal{O}_n)) = j(\mathfrak{b}^{-1})$. For any lattice Λ, it is easy to see that $g_2(\bar{\Lambda}) = \overline{g_2(\Lambda)}$ and the same for g_3; thus $\overline{j(\mathfrak{a})} = j(\bar{\mathfrak{a}})$ for any proper $\mathcal{O}_n$-ideal $\mathfrak{a}$. Since in $\mathrm{Pic}(\mathcal{O}_n)$ one has $[\bar{\mathfrak{a}}] = [\mathfrak{a}^{-1}]$, we get that $\overline{j(\mathfrak{a})} = j(\mathfrak{a}^{-1})$. In particular $\overline{(j(\mathcal{O}_n))} = j(\mathcal{O}_n)$. We then conclude that $\sigma(j(\mathcal{O}_n)) = \overline{j(\mathfrak{b}^{-1})} = j(\mathfrak{b}) = \sigma^{-1}(j(\mathcal{O}_n)) = \sigma^{-1}(\overline{(j(\mathcal{O}_n))})$. □

Now take any integer n as above and any prime l dividing it and consider the extension $K(E_p)/\mathbb{Q}$, which has index $2p^2$. Using the assumptions on n, one shows that l is unramified for $K(E_p)/\mathbb{Q}$, so we have a well defined conjugacy class $\mathrm{Frob}(l)$ in $Gal(K(E_p)/\mathbb{Q})$. We further require that

$$\mathrm{Frob}(l) = \mathrm{Frob}(\infty), \tag{A.2}$$

where $\mathrm{Frob}(\infty)$ is the conjugacy class of τ. Tchebotarev density theorem implies that there are infinitely many such l and so infinitely many n satisfy our assumptions.

Since (A.2) implies that $\mathrm{Frob}(l)$ in $K/\mathbb{Q}$ is equal to τ, every such l is inert in K, we denote with λ its unique prime factor and with F_λ the residue field at λ, which has l^2 elements. Since the characteristic polynomial of $\mathrm{Frob}(l)$ acting on E_p is $x^2 - a_l + l$ and the one of τ is $x^2 - 1$, one has, equating the coefficients,

$$a_l \equiv l + 1 \equiv 0 \pmod{p}. \tag{A.3}$$

Now write $n = \prod l$ and let $G_n = Gal(K_n/K_1)$ so that we have $G_n \simeq \prod G_l$. We have that $G_l \simeq F_\lambda^\times / F_l^\times$ is cyclic of order $l+1$ and we fix a generator σ_l and let

$$Tr_l := \sum_{\sigma \in G_l} \sigma = \sum_{i=1}^{l+1} \sigma_l^i \in \mathbb{Z}[G_l],$$

$$D_l := \sum_{i=1}^{l} i \cdot \sigma_l^i \in \mathbb{Z}[G_l].$$

Lemma A.2.1. *We have the following equality in $\mathbb{Z}[G_l]$:*

$$(\sigma_l - 1) \cdot D_l = l + 1 - Tr_l.$$

Proof. It is just an easy computation. Indeed we have

$$(\sigma_l - 1) \cdot D_l = (\sigma_l - 1) \cdot \sum_{i=1}^{l} i \cdot \sigma_l^i = \sum_{i=2}^{l+1} (i-1)\sigma_l^i - \sum_{i=1}^{l} i \cdot \sigma_l^i = -Tr_l + l\sigma_l^{l+1} + \sigma_l^{l+1} = -Tr_l + l + 1.$$

□

We finally define D_n to be $D_n = \prod D_l \in \mathbb{Z}[G_n]$.

As we were anticipating in (1.3.9), our collection of points y_n is an Euler system. Indeed

Proposition A.2.2. *The collection $\{y_n\}_n$ as above satisfies the axioms of an Euler system. Namely, if $n = l \cdot m$, then*

AX 1. $Tr_l\ y_n = a_l \cdot y_m$ *in* $E(K_m)$,

AX 2. each prime factor λ_n of l in K_n divides a unique prime λ_m of K_m and $y_n \equiv \mathrm{Frob}(\lambda_m)(y_m)$ (mod λ_n).

Proof. We will only sketch the proof of the first property and refer to Gross' article (proposition 3.7) for the proof of the second one.

From the description of T_l that we gave in (3.1.1), one can check that $Tr_l\ x_n = T_l(x_m)$ as divisors on $X_0(N)$. We then use what we observed in remark 1.3.6 and get

$$Tr_l\ y_n = \varphi_N(Tr_l\ x_n) = \varphi_N(T_l(x_m)) = a_l \cdot \varphi_N(x_m) = a_l \cdot y_m.$$

□

The first important result, that will allow us to build up the desired cohomology classes, is the following

Proposition A.2.3. *The class of the point $D_n y_n$ in $E(K_n)/pE(K_n)$ is fixed by the action of G_n.*

Proof. It suffices to show that the class of $D_n y_n$ is fixed by σ_l for every l dividing n, since these elements generate G_n. We thus need to show that $(\sigma_l - 1)D_n y_n \in pE(K_n)$. Writing $n = l \cdot m$, we have, by definition $D_n = D_l \cdot D_m$ and applying lemma A.2.1 we get that

$$(\sigma_l - 1)D_n y_n = (\sigma_l - 1)D_l \cdot D_m y_n = (l+1)D_m y_n - D_m(Tr_l\ y_l).$$

We now use (A.3) and the first part of proposition A.2.2 to conclude. □

Let now $\mathcal{G}_n := Gal(K_n/K)$, we then have an exact sequence

$$0 \to G_n \to \mathcal{G}_n \to Gal(K_1/K) \to 0.$$

Let S be a set of coset representatives for G_n in $\mathcal{G}_n$, define then

$$P_n := \sum_{\sigma \in S} \sigma(D_n y_n) \in E(K_n) \tag{A.4}$$

An easy corollary of proposition A.2.3 is that the class of P_n in $E(K_n)/pE(K_n)$ is fixed by $\mathcal{G}_n$, in other words (the class of) P_n lies in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$. Moreover the class of P_n is independent on the choice of S. Notice further that $P_1 = Tr_{K_1/K}(y_1) = P_K$.

Now take the Galois cohomology of the exact sequence $0 \to E_p \to E \xrightarrow{\cdot p} E \to 0$, we get the following diagram with exact rows and columns

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & H^1(K_n/K, E_p(K_n)) & & H^1(K_n/K, E(K_n))_p & & \\
 & & & & \downarrow \mathrm{Inf} & & \downarrow \mathrm{Inf} & & \\
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E_p) & \longrightarrow & H^1(K, E)_p & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \\
0 & \longrightarrow & (E(K_n)/pE(K_n))^{\mathcal{G}_n} & \xrightarrow{\delta_n} & H^1(K_n, E_p)^{\mathcal{G}_n} & \longrightarrow & H^1(K_n, E)_p^{\mathcal{G}_n} & \longrightarrow & 0
\end{array} \tag{A.5}$$

First of all we say that one can prove (see lemma 4.3 of [Gro91]) that our assumptions on p force $E_p(K_n)$ to be trivial. This implies that $H^1(K_n/K, E_p(K_n)) = H^2(K_n/K, E_p(K_n)) = 0$ and so we get that the left restriction map in the above diagram is actually an isomorphism. Using this we define the Kolyvagin's cohomology class $c(n)$ to be the unique element in $H^1(K, E_p)$ such that

$$\mathrm{Res}\, c(n) = \delta_n(P_n).$$

We also let $d(n)$ be the image of $c(n)$ in $H^1(K, E)_p$. We have that $\mathrm{Res}\, d(n)$ is equal to the image of $\delta_n(P_n)$ in $H^1(K_n, E_p)^{\mathcal{G}_n}$ by the commutativity of the diagram, and the exactness tells us that thus $\mathrm{Res}\, d(n) = 0$, so there exists a unique element $\tilde{d}(n) \in H^1(K_n/K, E(K_n))_p$ such that

$$\mathrm{Inf}\, \tilde{d}(n) = d(n).$$

From the definition of $c(n), d(n), \tilde{d}(n)$ and using again the above diagram, it is immediate to prove the following

Proposition A.2.4. *(i) The class $c(n)$ is trivial if and only if $P_n \in pE(K_n)$.*

(ii) The class $d(n)$ is trivial (and so it is $\tilde{d}(n)$) if and only if $P_n \in pE(K_n) + E(K)$.

Remark A.2.5. We can give an explicit description of the cohomology class $c(n)$. Indeed one has

$$\begin{aligned} \delta_n(P_n) : & Gal(\bar{\mathbb{Q}}/K_n) \to E_p(\bar{Q}) \\ & \sigma \mapsto \sigma(\frac{1}{p} P_n) - \frac{1}{p} P_n, \end{aligned}$$

where $\frac{1}{p}P_n$ is a fixed p-th root of P_n in $E(\bar{Q})$. And one shows that

$$\begin{aligned}\delta_n(P_n) :&Gal(\bar{\mathbb{Q}}/K) \to E_p(\bar{Q})\\ &\sigma \mapsto \sigma(\frac{1}{p}P_n) - \frac{1}{p}P_n - \frac{(\sigma-1)P_n}{p},\end{aligned}$$

where $\frac{(\sigma-1)P_n}{p}$ is the unique p-th root of $(\sigma-1)P_n$ in $E(K_n)$, which exists since, being $E_p(K_n)$ trivial, multiplication by p gives an automorphism of $E(K_n)$.

A.2.1 Some properties of the cohomology classes $c(n), d(n)$

We want first of all investigate the behaviour of $c(n), d(n)$ under the action of complex conjugation τ, we will show in particular that they lay in an eigenspace for τ. To do this, we first need to discuss the action of τ on the points $y_n \in E(K_n)$ (notice that this makes sense since clearly τ acts on K_n). From now on we will denote with ε the eigenvalue of w_N on the newform f associated to E.

Lemma A.2.6. *We have $y_n^\tau = \varepsilon \cdot y_n^{\sigma'} + (torsion)$ in $E(K_n)$ for some $\sigma' \in \mathcal{G}_n = Gal(K_n/K)$.*

Proof. The reasoning we presented in the proof of (A.1) can be applied to show that if x_n is the point on $X_0(N)$ corresponding to the elliptic curve with associated lattice $\mathfrak{a}$, using the ideal $\mathfrak{n}$ to build up the corresponding cyclic subgroup, x_n^τ corresponds to the pair $(\mathfrak{a}^{-1}, \bar{\mathfrak{n}})$. Moreover the description that we gave of w_N in terms of an endomorphism of $J_0(N)$, tells us that such a point is equal to $w_N(y)$, where y corresponds to the pair $(\mathfrak{a}^{-1} \cdot \mathfrak{n}, \mathfrak{n})$. Finally, using the description of the action of $\mathcal{G}_n = Gal(K_n/K) \simeq \mathrm{Pic}(\mathcal{O}_n)$ in terms of ideals as in theorem 0.3.3, gives us $x_n^\tau = w_N(x_n^{\sigma'})$, where σ' corresponds to the element $[\mathfrak{a}]$. We then have

$$(x_n - \infty)^\tau = w_N(x_n^{\sigma'}) - (\infty) - w_N\infty + w_N\infty = w_N(x_n - \infty)^{\sigma'} + (0) - (\infty).$$

As we did many times, we can realize $m((0)-(\infty))$ as the divisor of a meromorphic function on $X_0(N)$ for an appropriate m, so that $(0)-(\infty)$ is a torsion point. We then apply φ_N on both sides and to conclude we apply what we observed in remark 1.3.6, namely

$$y_n^\tau = \varphi_N((x_n - \infty)^\tau) = \varphi_N(w_N(x_n - \infty)^{\sigma'}) + (torsion) = \varepsilon \cdot y_n^{\sigma'} + (torsion).$$

□

Using this lemma, we get to the following

Proposition A.2.7. *Let $f_n := \#\{l \text{ prime: } l \mid n\}$ and $\varepsilon_n := \varepsilon \cdot (-1)^{f_n}$. The class of P_n, $c(n)$ and $d(n)$ lie in the ε_n-eigenspace for τ in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$, $H^1(K, E_p)$ and $H^1(K, E)_p$ respectively.*

Proof. Since the diagram (A.5) commutes with the action of τ, it is enough to prove that the class of P_n lies in the ε_n-eigenspace for τ in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$. Using the definition of P_n and the relation (A.1), we find that $\tau P_n = \sum_{\sigma \in S} \tau\sigma D_n y_n = \sum_{\sigma \in S} \sigma^{-1}\tau D_n y_n$. Now consider D_l for $l \mid n$. We have, using again (A.1)

$$\begin{aligned}\tau D_l + \sigma_l D_l \tau &= \sum_{i=1}^{l} i\tau\sigma_l^i + \sum_{i=1}^{l} i\sigma_l^{i+1}\tau = \sum_{i=1}^{l} i\sigma_l^{l+1-i}\tau + \sum_{i=2}^{l+1}(i-1)\sigma_l^i\tau\\ &= \sum_{i=1}^{l}(l+1-i)\sigma_l^i\tau + \sum_{i=2}^{l+1}(i-1)\sigma_l^i\tau = l\sigma_l\tau + l\tau + l\sum_{i=2}^{l}\sigma_l^i\tau = l \cdot Tr_l \cdot \tau = l \cdot Tr_l.\end{aligned}$$

Using the first part of theorem A.2.2 together with (A.3) we get

$$\tau P_n \equiv (-1)^{f_n} \cdot \prod_{l|n} \sigma_l \cdot \sum_{\sigma \in S} \sigma^{-1} D_n y_n \pmod{pE(K_n)}.$$

Now, applying the above lemma, together with the fact that $E_p(K_n) = 0$ we find that

$$\tau P_n \equiv \varepsilon_n \cdot \prod_{l|n} \sigma_l \cdot \sigma' \cdot \sum_{\sigma \in S} \sigma^{-1} D_n y_n \pmod{pE(K_n)},$$

for some $\sigma' \in \mathcal{G}_n$. Using proposition A.2.3 and the fact that $\{\sigma^{-1}\}_{\sigma \in S}$ is another set of coset representatives for G_n in $\mathcal{G}_n$, we get that $\sum_{\sigma \in S} \sigma^{-1} D_n y_n \equiv P_n$. Moreover the class of P_n is fixed by $\mathcal{G}_n$ so we can conclude $\tau P_n \equiv \varepsilon_n \cdot P_n$. □

Another question one could ask is whether the class $c(n)$ lies in the Selmer group $\mathrm{Sel}(E/K)_p$ or not. Recall the definition of this group

$$\mathrm{Sel}(E/K)_p = \ker\left(H^1(K, E_p) \to \prod_v H^1(K_v, E)_p \right),$$

where the product is taken over all places v of K and K_v denotes the compeltion of K at v. Moreover the map is given by the collections of the maps obtained from the composition of $H^1(K, E_p) \to H^1(K, E)_p$ followed by the restriction $H^1(K, E)_p \to H^1(K_v, E)_p$, whose image of an element d we will denote with d_v. Thus asking for $c(n)$ to be in $\mathrm{Sel}(E/K)_p$ is equivalent to ask for $d(n)_v$ to be trivial for every place v. What one can prove is the following

Proposition A.2.8. *(1) $d(n)_v$ is trivial at the archimedean place $v = \infty$ and at all finite places v such that $v \nmid n$.*

(2) If $n = l \cdot m$ and $(l) = \lambda$ in K, then $d(n)_\lambda$ is trivial if and only if $P_m \in pE(K_\lambda)$.

Proof. See proposition 6.2 of [Gro91]. □

A.3 A useful pairing

In this section we present a collection of results that will be used to prove the main theorem. For the proofs of the following statements and the construction of the pairing one need to look at Weil pairing and use Tate duality. We refer to sections 7-8-9 of [Gro91] for more details. We decided not to go too much into it since we just want to give an idea of how, using cohomology classes $c(n)$ and these results, one can obtain the bounding on the Selmer group.

One has a non-degenerate pairing of $\mathbb{Z}/p\mathbb{Z}$-vector spaces respecting the $\pm$-eigenspaces for complex conjugation τ

$$\langle\ ,\ \rangle : E(K_\lambda)/pE(K_\lambda) \times H^1(K_\lambda, E)_p \to \mathbb{Z}/p\mathbb{Z},$$

where K_λ is the completion of K at a prime λ. Using this one can prove, with the notation of the previous section, the following

Proposition A.3.1. *If $d \in H^1(K, E_p)^\pm$ is such that $d_v = 0$ for every $v \neq \lambda$ but $d_\lambda \neq 0$ for λ an inert prime of K, then for every $s \in \mathrm{Sel}(E/K)_p^\pm \subset H^1(K, E_p)^\pm$ we have $s_\lambda = 0$ in $H^1(K_\lambda, E_p)^\pm$.*

We now define $L := K(E_p)$ and $\mathcal{G} := Gak(L/K)$. One has

Proposition A.3.2. *There is a pairing* $[\ ,\ ] : H^1(K, E_p) \times Gal(\bar{\mathbb{Q}}/L) \to E_p(L)$ *such that*

(i) $[s^\sigma, \rho^\sigma] = [s, \rho^\sigma] = [s, \rho]^\sigma$, *for ever* $s \in H^1(K, E_p), \rho \in Gal(\bar{\mathbb{Q}}/L)$ *and* $\sigma \in \mathcal{G}$.

(ii) If $[s, \rho] = 0$ *for every* $\rho \in Gal(\bar{\mathbb{Q}}/L)$, *then* $s = 0$.

Moreover for every finite subgroup $S \subset H^1(K, E_p)$, *denote with* $Gal_S(\bar{\mathbb{Q}}/L) = \{\rho \in Gal(\bar{\mathbb{Q}}/L) : [s, \rho] = 0$ *for every* $s \in S\}$ *and with* L_S *the field fixed by* $Gal_S(\bar{\mathbb{Q}}/L)$. *Then we obtain a non-degenerate induce pairing*

$$[\ ,\ ] : S \times Gal(L_S/L) \to E_p(L).$$

Such a pairing induces isomorphisms $Gal(L_S/L) \simeq \mathrm{Hom}(S, E_p(L)$ *and* $S \simeq \mathrm{Hom}_{\mathcal{G}}(Gal(L_S/L), E_p(L))$.

We want to apply the second part of the above proposition to $S = \mathrm{Sel}(E/K)_p$. We write $M = L_S$ and $H = Gal(M/L)$. We assume that P_K is not divisible by p in $E(K)$ so that $\delta P_K \in \mathrm{Sel}(E/K)_p$ is different from zero. We moreover define I to be the subgroup of H which fixes the subfield $L(\frac{1}{p}P_K)$ of M, so that $Gal(M/L(\frac{1}{p}P_K)) = I$. We denote with H^+ and I^+ the $+1$-eigenspace for τ, which acts by conjugation on H and I. One has

Proposition A.3.3. *(1)* $H^+ = \{(\tau h)^2 : h \in H\}$, $I^+ = \{(\tau i)^2 : i \in H\}$ *and* $H^+/I^+ \simeq \mathbb{Z}/p\mathbb{Z}$.

(2) Let $s \in \mathrm{Sel}(E/K)_p^{\pm}$. *The following are equivalent*

(a) $[s, \rho] = 0$ *for all* $\rho \in H$
(b) $[s, \rho] = 0$ *for all* $\rho \in H^+$
(c) $[s, \rho] = 0$ *for all* $\rho \in H^+ \setminus I^+$
(d) $s = 0$.

Now we want to consider a prime λ of K not dividing Np, so that λ is unramified in M/K and further assume that λ splits completely in L/K. Let λ_M be a prime factor of λ in M. We let

$$\rho := \left(\frac{M/K}{\lambda_M}\right) \tag{A.6}$$

be the Frobenius element corresponding to λ_M. It actually lies in $H = Gal(M/L)$, since its restriction to L is the Frobenius with respect to the extension L/K, where λ splits completely, thus it is the identity.

Proposition A.3.4. *Let* $s \in \mathrm{Sel}(E/K)_p$ *and let* $\rho \in H$ *and* λ *as above. Then*

$$[s, \rho] = 0 \quad \Leftrightarrow \quad s_\lambda = 0 \text{ in } \ H^1(K_\lambda, E_p).$$

Moreover, fixed a prime λ as above, we have

Lemma A.3.5. *Let* λ *be as above have and let* P *be a* K*-point which is not divisible by* p *in* $E(K)$. *Then the following are equivalent*

(a) λ *splits completely in* $L(\frac{1}{p}P)$,

(b) P *is divisible by* p *in* $E(K_\lambda)$, *i.e.* $\frac{1}{p}P \in E(K_\lambda)$.

Proof. Since λ splits completely in L/K, we have that, for every place $w \mid \lambda$, $L_w = K_\lambda$. Now first notice that $L(\frac{1}{p}P) = L(Q)$, where Q is such that $pQ = P$, since L contains all p-torsion points of E. Now, saying that Q is defined over $K_\lambda = L_w$ (for every $w \mid \lambda$) is equivalent to say that $L_w(Q) = L_w$, i.e. every prime w of L dividing λ splits completely in $L(Q) = L(\frac{1}{p}P)$; equivalently λ splits completely in $L(\frac{1}{p}P)$. □

A.4 Proof of theorem A.1.3

Recall that in order to prove theorem A.1.2 it is enough to prove A.1.3, which asserts that, under our assumptions on p and P_K, the p-Selmer group is cyclic and generated by δP_K. One has the direct sum decomposition in eigenspaces with respect to τ

$$\mathrm{Sel}(E/K)_p = \mathrm{Sel}(E/K)_p^+ \oplus \mathrm{Sel}(E/K)_p^-.$$

We therefore prove the following theorem, that gives us the desired result.

Theorem A.4.1. $\mathrm{Sel}(E/K)_p^{-\varepsilon} = 0$ *and* $\mathrm{Sel}(E/K)_p^{\varepsilon} \simeq \mathbb{Z}/p\mathbb{Z} \cdot \delta P_K$.

Proof. **Step 1.** We first prove that $\mathrm{Sel}(E/K)_p^{-\varepsilon} = 0$.

Take $s \in \mathrm{Sel}(E/K)_p^{-\varepsilon}$; applying proposition A.3.3, we get that $s = 0$ if and only if $[s, \rho'] = 0$ for all $\rho' \in H^+ \setminus I^+$. We can then write such a ρ' as $(\tau h)^2$ for $h \in H$.

Now consider l a rational prime unramified in $M/\mathbb{Q}$ and whose prime factor λ_M is such that the Frobenius of λ_M in $Gal(M/\mathbb{Q})$ is equal to τh. Such a prime exists thanks to Tchebotarev density theorem. One can show that $(l) = \lambda$ is inert in K and λ splits completely in L. Since $\rho = (\tau h)^2 = \rho'$, where ρ is as in (A.6), by proposition A.3.4, $[s, \rho'] = 0$ if and only if $s_\lambda = 0$.

We now finally consider the cohomology classes $c(l)$ and $d(l)$. Proposition A.2.7 tells us that they both lie in the $-\varepsilon$-eigenspaces for τ and proposition A.2.8 (1) tells us that $d(n)_v$ is trivial for all places $v \neq \lambda$. Using (2) of the same proposition we get that $d(n)_\lambda$ is trivial if and only if $P_1 = P_K \in pE(K_\lambda)$ and lemma A.3.5 tells us that this holds if and only if λ splits completely in $L(\frac{1}{p}P_K)$, using our hypothesis that P_K is not divisible by p in $E(K)$. But if λ split completely in $L(\frac{1}{p}P_K)$, then $\rho_{|L(\frac{1}{p}P_K)}$ would be equal to the identity, i.e. $\rho' \in I^+ = I \cap H^+$, but we were considering $\rho' \in H^+ \setminus I^+$, so we get $d(l)_\lambda \neq 0$.

Now we apply proposition A.3.1 to $d = d(l)$, which satisfies the assumptions, and get $s_\lambda = 0$, so we are done.

Step 2. We now prove, using the first step, a useful lemma.

Lemma A.4.2. *Let l, λ_M, λ, h as in the Step 1. The following are equivalent:*

(a) $c(l) = 0$

(b) $c(l) \in \mathrm{Sel}(E/K)_p$

(c) P_l *is divisible by* p *in* $E(K_l)$

(d) $d(l) = 0$

(e) $d(l)_\lambda = 0$

(f) $P_1 = P_K$ *is divisible by* p *in* $E(K_\lambda)$

(g) $h^\tau h \in I^+$.

Proof (of lemma A.4.2). As above $c(l)$ and $d(l)$ lie in the $-\varepsilon$-eigenspaces for τ. Using $\mathrm{Sel}(E/K)_p^{-\varepsilon} = 0$ we get $(a) \Leftrightarrow (b)$ and we have $(a) \Leftrightarrow (c)$ for the first part of proposition A.2.4. Moreover $\mathrm{Sel}(E/K)_p^{-\varepsilon} = 0$ implies $(E(K)/pE(K))^{-\varepsilon} = 0$, thus $c(l) = 0$ if and only if $d(l) = 0$. Moreover, as we have shown above, $d(l)_v = 0$ for all $v \neq \lambda$ thus $d(l) \in Ш(E/K)_p^{-\varepsilon}$ if and only if $d(l)_\lambda = 0$. Since $Ш(E/K)_p^{-\varepsilon} = 0$, we get $(d) \Leftrightarrow (e)$. Again we have $(e) \Leftrightarrow (f)$ thanks to proposition A.2.8. Finally $h^\tau h = \tau^{-1} h \tau h = (\tau h)^2 = \rho$, thus $h^\tau h \in I^+$ if and only if λ splits completely in $L(\frac{1}{p}P_K)$. So lemma A.3.5 gives $(f) \Leftrightarrow (g)$. □

Step 3. To conclude, we now prove that $\mathrm{Sel}(E/K)_p^{\varepsilon} \simeq \mathbb{Z}/p\mathbb{Z} \cdot \delta P_K$.

Take $s \in \mathrm{Sel}(E/K)_p^{\varepsilon}$. We want to show that $[s, \rho'] = 0$ for every $\rho' \in I$, so that, using proposition A.3.2 and the first part of proposition A.3.3, we get $s \in \mathrm{Hom}_{\mathcal{G}}(H/I, E_p) \simeq \mathbb{Z}/p\mathbb{Z} \cdot \delta P_K$. An analogous of proposition A.3.3 tells us that it is enough to check $[s, \rho'] = 0$ for every $\rho' \in I^+$. Take such a ρ' and write it in the form $\rho' = (\tau i)^2$, for $i \in I$.

Now consider a rational prime l' such that $c(l') \neq 0$. We make full use of the lemma of the previous step to construct such a prime: it is indeed enough to take l' such that its Frobenius in $M/\mathbb{Q}$ is conjugate to τh, for $h \in H$ such that $h^{\tau+1} \notin I^+$. The same lemma tells us that $c(l') \notin \mathrm{Sel}(E/K)_p$. We consider then $L' := L_{c(l')}$, the subextension of $\bar{\mathbb{Q}}/L$ fixed by $Gal(\bar{\mathbb{Q}}/L) = \{\sigma : [c(l'), \sigma] = 0\}$. Since $M = L_{\mathrm{Sel}(E/K)_p}$ and $c(l') \notin \mathrm{Sel}(E/K)_p$, the extensions M/L and L'/L are disjoint.

Using the description of $c(l')$ given in remark A.2.5 one can show that $L' = L(\frac{1}{p}P_{l'})$. Then we get, applying lemma A.3.5, that a prime $(l) = \lambda$ of K splitting completely in L splits completely in L' if and only if $P_{l'} \in pE(K_\lambda)$.

Now take a prime l such that its Frobenius in $M/\mathbb{Q}$ is conjugate to τi and its Frobenius in $L'/\mathbb{Q}$ its conjugate to τj in $L'/\mathbb{Q}$, with $j \in Gal(L'/L)$ such that $j^{\tau+1} \neq 1$. We used here the fact that $L' \cap M = L$ to find a prime satisfying both conditions. We want to proceed as before: we would like to apply proposition A.3.1 to $d = d(ll')$ to prove $s_\lambda = 0$; this would give us $[s, \rho'] = 0$, thanks to proposition A.3.4.

We now check that $d(ll')$ satisfies the assumptions of proposition A.3.1. If $v \neq \lambda, \lambda'$, then $d(ll')_v = 0$ for the first part of proposition A.2.8. If $v = \lambda'$, being $i \in I$, using the lemma of Step 2, we get $c(l) = 0$ and $P_l \in pE(K_l)$ and applying the second part of proposition A.2.8, we get $d(ll')_{\lambda'} = 0$. If also $d(ll')_\lambda = 0$ then, for the same reasoning, $P_{l'} \in pE(K_\lambda)$ and this holds, as we concluded above, if and only if λ splits completely in L', i.e. if and only if $(\tau j)^2 = j^{\tau+1} = 1$, which is not true thanks to the assumption on j. □

Bibliography

[BCD+14] M. Bertolini, F. Castella, H Darmon, S. Dasgupta, K. Prasanna, and V. Rotger. p-adic L-functions and euler systems: a tale in two trilogies. In *Automorphic Forms and Galois Representations, I.* Cambridge University Press, 2014. LMS, Lecture note series **414**.

[BDP] M. Bertolini, H. Darmon, and K. Prasanna. Generalized heegner cycles and p-adic rankin L-series. *Duke Math. J., Vol.* ***162****, No. 6.*

[Bro13] E.H. Brooks. Generalized Heegner cycles, Shimura curves, and special values of p-adic L-functions, 2013. PhD thesis available at dept.math.lsa.umich.edu/research/number_theory/theses/hunter_brooks.pdf.

[Col94] R.F. Coleman. A p-adic shimura isomorphism and p-adic periods of modular forms. In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture.* Contemp. Math, American Math. Society **165**, 1994.

[Cre97] J.E. Cremona. Algorithms for modular elliptic curves. *Cambridge University Press*, 1997.

[Dar04] H Darmon. Rational points on modular elliptic curves, 2004. CBMS Regional Conference Series in Mathematics.

[DE66] A. Dold and B. Eckmann, editors. *Seminar on Complex Multiplication.* Springer, 1966. Lecture Notes in Math. **21**.

[DS05] F. Diamond and J. Shurman. *A first course in modular forms.* Springer, 2005. Graduate Texts in Mathematics **228**.

[Gro86] B.H. Gross. Heegners points on $X_0(N)$. *Rankin, R.A. (ed): Modular forms*, pages 87–106, 1986.

[Gro91] B.H. Gross. Kolyvagin's work on modular elliptic curves. In J. Coates and M. J. Taylor, editors, *L-functions and arithmetic.* Cambridge University press, 1991. LMS, Lecture note series **153**.

[GZ86] B.H. Gross and D.B. Zagier. Heegners points and derivatives of L-series. *Inv. Math.*, 1986.

[Har77] R. Hartshorne. *Algebraic geometry.* Springer, 1977. Graduate Texts in Mathematics **52**.

[Kat72] N.M. Katz. p-adic properties of modular schemes and modular forms. In P. Deligne and W. Kuyk, editors, *Modular Functions of One Variable III.* Springer, 1972. International Summer School on Modular Functions.

[Kna92] A. Knapp. *Elliptic curves.* Princeton university press, 1992. Mathematical Notes **40**.

[Kol90] V.A. Kolyvagin. Euler systems. In P. Deligne and W. Kuyk, editors, *The grothendieck festschrift, Vol II.* Progr. in Math. **87**, 1990.

[Lan87] S. Lang. *Elliptic functions.* Springer, 2 edition, 1987. Graduate Texts in Mathematics **112**.

[Lau14] A. Lauder. Efficient computation of rankin p-adic L-functions. In Boeckle G. and Wiese G., editors, *Proceedings of a Summer School and Conference, Heidelberg, August/September 2011*, pages 181–200. Springer Verlag, 2014.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Publications mathématiques de l'I.H.É.S.,* ***47***, pages 33–186, 1977.

[Mil12] James S. Milne. Modular function and modular forms, 2012. Available at www.jmilne.org/math/CourseNotes/MF.pdf.

[Ser72] J.-P. Serre. Formes modulaires et fonctions zêta p-adiques. In P. Deligne and W. Kuyk, editors, *Modular Functions of One Variable III.* Springer, 1972. International Summer School on Modular Functions.

[Ser73] J.-P. Serre. *A course in arithmetic.* Springer, 1973. Graduate Texts in Mathematics **7**.

[Shi71] G. Shimura. *Introduction to the arithmetic theory of automorphic functions.* Princeton university press, 1971.

[Sil09] J.H. Silverman. *The arithmetic of elliptic curves.* Springer, 2 edition, 2009. Graduate Texts in Mathematics **106**.

[Wes] T. Weston. The modular curves $X_0(11)$ and $X_1(11)$. Available at people.math.umass.edu/~weston/ep.html.

[Zag84] D.B. Zagier. L-series of elliptic curves, the Birch-Swinnerton-Dyer conjecture, and the class number problem of Gauss. *Notices AMS* ***31***, pages 739–743, 1984.

Versicherung an Eides Statt

Ich, Giada Grossi; via San Matteo, 11, 24042 Capriate S.G. (Italy); Matrikelnummer: 3039434, versichere an Eides Statt durch meine Unterschrift, dass ich die vorstehende Arbeit selbstständig und ohne fremde Hilfe angefertigt und alle Stellen, die ich wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen habe, als solche kenntlich gemacht habe, mich auch keiner anderen als der angegebenen Literatur oder sonstiger Hilfsmittel bedient habe.

Ich versichere an Eides Statt, dass ich die vorgenannten Angaben nach bestemWissen und Gewissen gemacht habe und dass die Angaben der Wahrheit entsprechen und ich nichts verschwiegen habe.

Die Strafbarkeit einer falschen eidesstattlichen Versicherung ist mir bekannt, namentlich die Strafandrohung gemäß §156 StGB bis zu drei Jahren Freiheitsstrafe oder Geldstrafe bei vorsätzlicher Begehung der Tat bzw. gemäß §163 Abs. 1 StGB bis zu einem Jahr Freiheitsstrafe oder Geldstrafe bei fahrlässiger Begehung.

Ort, Datum	Unterschrift (Giada Grossi)