Complex multiplication

Course taught by: Henri Darmon

Notes taken by: Francesc Gispert

9th December 2020

Contents

1 Overview

The topic of the course is complex multiplication, a beautiful theory developed in the 19–th century with many arithmetic applications. This theory tells us something about the values of certain modular functions at certain points.

Definition 1. A *modular function* is a holomorphic function $f\colon \mathfrak{H} \to \mathbb{C}$ satisfying that

$$f\Big(\frac{az+b}{cz+d}\Big) = f(z) \quad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \text{ and } z \in \mathbb{C},$$

where

- $\mathfrak{H}$ is the Poincaré upper half-plane $\{\, z \in \mathbb{C} : \mathrm{Im}(z) > 0 \,\}$, and
- Γ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Remark. We will only use the following congruence subgroups:

$$\begin{aligned} \Gamma_0(N) &= \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \text{ mod } N \Big\}, \\ \Gamma_1(N) &= \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \text{ mod } N \Big\}, \\ \Gamma(N) &= \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ mod } N \Big\}. \end{aligned}$$

Also, sometimes we consider modular functions having values in $\mathbb{P}^1(\mathbb{C})$ (i.e., with poles) or even in $E(\mathbb{C})$ for some elliptic curve E.

Example 2. The following are examples of modular functions:

(1) The j–invariant $j\colon\ \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \to \mathbb{C}$ is an analytic isomorphism and generates the ring of modular functions on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$.

(2) The λ–function $\lambda\colon \Gamma(2)\backslash\mathfrak{H} \to \mathbb{C} \setminus \{\,0, 1\,\}$ is an analytic isomorphism related to j by

$$j = 256\frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

It also satisfies the equations

$$\lambda = 16\frac{\eta(z/2)^8\,\eta(2z)^{16}}{\eta(z)^{24}} \quad \text{and} \quad 1 - \lambda = \frac{\eta(z/2)^{16}\,\eta(2z)^8}{\eta(z)^{24}},$$

where

$$\eta(z) = q^{1/24}\prod_{n\geq 1}(1 - q^n) \quad \text{if } q = e^{2\pi i z} \quad \text{(Dedekind eta function)}.$$

(The q–expansion of $\eta(z)$ together with the previous formulae for λ and $1-\lambda$ show that, indeed, λ does not take the values 0 or 1.)

(3) The Siegel units: we have a modular function $U_N\colon \Gamma_0(N)\backslash\mathfrak{H} \to \mathbb{C}^\times$ given by

$$U_N = \frac{\Delta(Nz)}{\Delta(z)}, \quad \text{where } \Delta(z) = \eta(z)^{24}.$$

(4) Modular parametrizations: every elliptic curve $E/\mathbb{Q}$ of conductor N admits a non-constant analytic map $\Phi_E\colon \Gamma_0(N)\backslash\mathfrak{H} \to E(\mathbb{C})$ (modularity theorem).

1.1 The main theorem

Definition 3. A *CM point* of $\mathfrak{H}$ is a point $\tau \in \mathfrak{H}$ which satisfies a quadratic equation over $\mathbb{Q}$, so that $\tau = a + b\sqrt{d}$ for some $a, b, d \in \mathbb{Q}$ with $d < 0$ and $b > 0$.

Theorem 4. *Let $\tau \in \mathfrak{H} \cap \mathbb{Q}(\sqrt{d})$ (for some $d < 0$) and let f be a modular function. If the q–expansion of f has coefficients in $\mathbb{Q}$, then $f(\tau)$ is algebraic and is defined over an abelian extension of* $\mathbb{Q}(\sqrt{d})$.

This theorem suggests that we might be able to generate almost all abelian extensions of a quadratic imaginary fields (i.e., explicit class fields) from the values of modular functions.

Example 5. The CM values of $j(z)$ are called *singular moduli.* Consider a quadratic imaginary field K with $D = \operatorname{disc}(K)$, $D < 0$, and class number $h(K) = 1$. Then the CM point

$$\tau_D = \frac{D + \sqrt{D}}{2}$$

satisfies that $j(\tau_D) \in \mathbb{Z}$.

Table 1 shows all these singular moduli. One can observe several patterns: all the numbers in the second column are perfect cubes and have many small prime factors but not all (no 7 or 13); in contrast the numbers in the third column are *almost* perfect squares (except for a factor of D) and includes the prime 7 but no 5. This kind of patterns were explained by the work of Gross and Zagier.

Writing

$$(j(\tau_D), j(\tau_D) - 1728) = (x^3, Dy^2),$$

we obtain an integral solution to the equation

$$x^3 - Dy^2 = 1728.$$

D	$j(\tau_D)$	$j(\tau_D) - 1728$
-3	0	$-2^6 3^3$
-4	$2^6 3^3$	0
-7	$-3^3 5^3$	$-3^6 7$
-8	$2^6 5^3$	$2^7 7^2$
-11	-2^{15}	$-2^6 7^2 11$
-19	$-2^{15} 3^3$	$-2^6 3^6 19$
-43	$-2^{18} 3^3 5^3$	$-2^6 3^8 7^2 43$
-67	$-2^{15} 3^3 5^3 11^3$	$-2^6 3^6 7^2 31^2 67$
-163	$-2^{18} 3^3 5^3 23^3 29^3$	$-2^6 3^6 7^2 11^2 19^2 127^2 163$

Table 1: Singular moduli for quadratic imaginary fields with class number 1.

These kind of numbers seem to *contradict* the ABC conjecture. Of course this is not really the case because we only have a finite number of quadratic imaginary fields with class number 1.

Example 6. In the spirit of the last observation in the previous example, Granville and Stark proved that a strong version of the ABC conjecture implies that $h(D)$ grows asymptotically like

$$\frac{\sqrt{|D|}}{\log(|D|)}$$

as $D \to -\infty$. In particular, the Dirichlet L–function $L(\chi_D, s)$ has no Siegel zeros.

1.2 More applications

Let D be a negative discriminant as before. We have the following associated data:

(1) a quadratic order $\mathscr{O}_D = \mathbb{Z}[(D + \sqrt{D})/2]$;

(2) the class group $\mathrm{Cl}(D) = \mathrm{Pic}(\mathscr{O}_D)$, and

(3) a ring class field H_D such that, if $K = \mathbb{Q}(\sqrt{D})$,

$$\mathrm{Gal}(H_D/K) = \mathrm{Cl}(D)$$

by class field theory. Furthermore, if we write $D = D_0 c^2$, where D_0 is a fundamental discriminant (square-free) and c is the conductor of the order, then H_D is unramified outside c.

Proposition 7. *If f is a modular function for some group Γ with rational q–expansion, then $f(\tau_D)$ is defined over an abelian extension L of H_D satisfying that*

(1) *L is unramified outside the level N of Γ and*

(2) $[L : H_D] \leq [\mathrm{SL}_2(Z) : \Gamma]$.

Proposition 8. *In the situation of proposition 7, if $f(\mathfrak{H})$ is contained in $V(\mathbb{C})$ for an algebraic variety V (such as $\mathbb{A}^1$, $\mathbb{A}^1 \setminus \{ 1 \}$ or an elliptic curve E), then*

$$f(\tau_D) \in V(\mathscr{O}_L[N^{-1}]).$$

Example 9.

(1) $j(\tau_D) \in \mathscr{O}_L$.

(2) $\lambda(\tau_D)$ is a solution to

$$(x^2 - x + 1)^3 - 2^{-8} j(\tau_D) x^2 (x-1)^2 = 0$$

and so $\lambda(\tau_D) \in \mathscr{O}_L[1/2]^\times$. Exercise: $1 - \lambda(\tau_D) \in \mathscr{O}_L[1/2]^\times$. The pair $(\lambda(\tau_D), 1 - \lambda(\tau_D))$ is then a solution to the 2–unit equation in L.

(3) $U_N(\tau_D) \in \mathscr{O}_L[1/N]^\times$ (and often even $U_N(\tau_D) \in \mathscr{O}_L^\times$). These units are called *elliptic units*. There is an interesting analogy summarized in table 2.

$\mathbb{Q}$	K (imaginary quadratic)
Circular units $1 - \zeta_N$	Elliptic units $U_N(\tau_D)$
Class number formula: $L'(\chi, 1) \leftrightarrow \log(1 - \zeta_N)$ for an even Dirichlet character χ	Kronecker limit formula: $L'(\psi, 1) \leftrightarrow \log(U_N(\tau_D))$ for a finite-order Hecke character ψ
Work of Thaine, Rubin (Iwasawa main conjecture)	Work of Coates–Wiles, Rubin (Iwasawa main conjecture)

Table 2: Analogy between the theory over $\mathbb{Q}$ and over K.

Theorem 10 (Coates–Wiles, Rubin). *Let $A/\mathbb{Q}$ be an elliptic curve with CM. If the Hasse–Weil L–function of A satisfies that $L(A, 1) \neq 0$, then $A(\mathbb{Q}) < \infty$ (Coates–Wiles) and $Ш(A/\mathbb{Q}) < \infty$ (Rubin).*

Remarkably, CM theory has applications towards the proof of the BSD conjecture for general elliptic curves (not just those with CM). Consider an elliptic curve $E/\mathbb{Q}$ and a modular parametrization $\Phi_E \colon \Gamma_0(N)/\mathfrak{H} \to E(\mathbb{C})$. Choosing an appropriate D, we get $\Phi_E(\tau_D) \in E(H_D)$. Define

$$P_D = \sum_{\mathrm{disc}(\tau) = D} \Phi_E(\tau) \in E(K).$$

Theorem 11 (Gross–Zagier). *In the situation above and if D is perfect square modulo N, then*

$$L'(E,1) \sim \mathrm{ht}_{\mathrm{NT}}(P_D).$$

In particular, P_D has infinite order precisely when $L'(E,1) \neq 0$.

Theorem 12 (Kolyvagin). *If P_D has infinite order, then $E(K)$ is generated by P_D and $Ш(E/K) < \infty$.*

Corollary 13. *If* $\mathrm{ord}_{s=1}(L(E,s)) \leq 1$, *then*

$$\mathrm{rank}(E(\mathbb{Q})) = \mathrm{ord}_{s=1}(L(E,s)) \quad \textit{and} \quad Ш(E/\mathbb{Q}) < \infty.$$

These are essentially the best known results towards a proof of the BSD conjecture, and they would not be available without the theory of complex multiplication.

1.3 Topics of this course

1.3.1 Basic theory and elementary applications

We are going to introduce the geometric ideas that justify the apparently *miraculous* fact that values of certain analytic functions turn out to be algebraic or integral. More precisely:

- The analytic space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ as the points $Y(\mathbb{C})$ of an algebraic curve Y that is a moduli space of elliptic curves over $\mathbb{Q}$. Models of Y over $\mathbb{Q}$ and $\mathbb{Z}$.
- Correspondence between the CM points $\tau \in \mathfrak{H}$ and elliptic curves "with extra endomorphisms" (i.e., with CM).
- Given a CM point $\tau \in \mathfrak{H}$ and $K = \mathbb{Q}(\tau)$, we study the value $j(\tau) \in K^{\mathrm{ab}}$.
- Factorization of Gross–Zagier for differences of singular moduli.
- Heegner and Stark's classification of negative discriminants $D < 0$ with class number $h(D) = 1$.
- The work of Granville–Stark on the ABC conjecture and Siegel zeros.

1.3.2 Generalizations

The most natural and fruitful ideas to generalize CM theory come from the work of Shimura–Taniyama. The theory of elliptic curves with CM is a particular case of the theory of abelian varieties with CM (already considered by Hilbert and developed by Blumenthal and other mathematicians until the culmination of Shimura and Taniyama). However, we will not cover this topic but only focus on the question of why explicit class field theory is accessible for CM fields.

Consider a CM field K, that is a totally imaginary quadratic extension of a totally real field F. The group of units

$$\mathscr{O}_{K/F}^{\times} = \{\, u \in \mathscr{O}_K^{\times} : \mathrm{N}_{K/F}(u) = 1 \,\}$$

is finite and we can study it by means of class field theory. In general, class field theory provides a description of the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ in terms of an idèle class group and it turns out that one can get a good understanding of explicit class field theory if this description does not involve a group of units.

In contrast, the simplest non-accessible case is that of a real quadratic field K. In that case, there is a fundamental unit (Dirichlet's theorem) that appears as a solution to Pell's equation. This unit appears as an obstruction to the explicit description of all abelian extensions of K. A general approach that one can follow to remedy this is to generalize the analytic statements without the geometric proofs. In our setting, the naive statement that we would like to have is that, given a modular function f and a point $\tau \in \mathfrak{H} \cap K$, the value $f(\tau)$ lies in K^{ab}. However, this statement cannot be true because $\mathfrak{H} \cap K = \emptyset$.

One possibility is to consider a geodesic on $\mathfrak{H}$ going from τ to its conjugate τ'. The subgroup of $\mathrm{SL}_2(\mathbb{Z})$ which leaves this geodesic invariant is isomorphic to $\mathbb{Z}$ up to torsion and so admits a generator corresponding in some sense to the fundamental unit of $\mathscr{O}_K$. There is work of Kaneko, Zagier and Duke–Imamoḡlu–Tóth in this direction.

Another possibility is to replace $\mathfrak{H}$ with a non-archimedean analogue: given a prime number p, the p–adic upper half-plane is $\mathfrak{H}_p = \mathbb{P}^1(\mathbb{C}_p) \setminus \mathbb{P}^1(\mathbb{Q}_p)$. The reason to consider this space is that $K \cap \mathfrak{H}_p \neq \emptyset$ if p is either inert or ramified in K. There is a theory of p–adic uniformization of certain curves which allows one to have a variant of the theory of complex multiplication. Thus, the second theme of the course will be p–adic variants of CM theory.

This part will be less complete and self-contained and we will treat the following topics:

- Shimura curves, which are moduli spaces of "fake elliptic curves". These are analogues of modular curves and are attached to quaternion algebras.
- Jacquet–Langlands theory relating modular forms and some kind of differentials on Shimura curves: if $E/\mathbb{Q}$ is an elliptic curve satisfying certain conditions, there is a modular parametrization $X \to E$ from a Shimura curve X.
- Cerednik–Drinfeld theory: given a Shimura curve X, for certain p one can identify $X(\mathbb{C}_p) \cong \Gamma\backslash\mathfrak{H}_p$ for some arithmetic subgroup Γ of $\mathrm{SL}_2(\mathbb{Q}_p)$.

One can then develop a variant of CM theory by studying the points in a Shimura variety that correspond to fake elliptic curves with extra endomorphisms. Then these points are defined over abelian extensions.

We will also talk about certain computational aspects:

- Algorithmic aspects (work of Greenberg and of Negrini).
- Gross–Zagier factorizations (work of Giampietro).

Unfortunately, one gets no immediate insights into the theory of real multiplication just from this theory. The problem is that the special points on $\Gamma\backslash\mathfrak{H}_p$ arise from tori $K^\times \subset B^\times$, where B is a definite quaternion algebra (so the quadratic fields are automatically imaginary). Instead, we would like to obtain Γ from an indefinite quaternion algebra.

1.3.3 RM theory

We may consider $\Gamma = \mathrm{SL}_2(\mathbb{Z}[p^{-1}])$ acting on $\mathfrak{H}_p$, but this action is not discrete. That is, writing $\mathscr{A}$ for the ring of (rigid) analytic functions on $\mathfrak{H}_p$ and $\mathscr{M}$ for the ring of meromorphic functions on $\mathfrak{H}_p$, we obtain that $\mathrm{H}^0(\Gamma,\mathscr{A}) = \mathrm{H}^0(\Gamma,\mathscr{M}) = \mathbb{C}_p$. To obtain an interesting theory, one has to look at higher cohomology groups. The next objects that one might consider are

$$\mathrm{H}^1(\Gamma,\mathscr{A}) \text{ or } \mathrm{H}^1(\Gamma,\mathscr{A}^\times),$$
$$\mathrm{H}^1(\Gamma,\mathscr{M}) \text{ or } \mathrm{H}^1(\Gamma,\mathscr{M}^\times).$$

Theorem 14 (Darmon–Vonk).

(1) $\mathrm{H}^1(\Gamma,\mathscr{A}) = \mathrm{H}^1(\Gamma,\mathscr{M}) = 0.$

(2) *The group* $\mathrm{H}^1(\Gamma,\mathscr{M}^\times)$ *is not finitely generated.*

(3) *Consider a rigid meromorphic cocycle* $J\colon \Gamma \to \mathscr{M}^\times$, *which represents a class in* $\mathrm{H}^1(\Gamma,\mathscr{M}^\times)$. *If*

$$J\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right) = 1,$$

then for every $\gamma \in \Gamma$ *the function* $J(\gamma)$ *has its zeros and poles in the set* $\mathfrak{H}_p^{\mathrm{RM}}$ *of RM points (i.e., points of* $\mathfrak{H}_p$ *that satisfy a quadratic equation with rational coefficients and generate a real quadratic field).*

The basic idea is that there should be an RM theory in which rigid meromorphic cocycles play the same role as modular functions in CM theory.

If $J\colon \Gamma \to \mathscr{M}^\times$ is a rigid meromorphic cocycle and $\tau \in \mathfrak{H}_p \cap K$ for a quadratic field K with $\mathrm{disc}(K) > 0$, then $\mathrm{Stab}_\Gamma(\tau) \cong \mathbb{Z}$ up to torsion and we can choose a generator γ_τ of this free part. It turns out that the eigenvalues of γ_τ are essentially powers of the fundamental unit of K.

Definition 15. The value of J at τ is

$$J[\tau] = J(\gamma_\tau)(\tau) \in \mathbb{C}_p \cup \{\infty\}.$$

(This value is well-defined because there is a canonical choice of γ_τ.)

Conjecture 16. *The rigid meromorphic cocycle J has a* field of definition H_J *such that* $[H_J : \mathbb{Q}] < \infty$ *and*

$$J[\tau] \in H_J \cdot H_\tau$$

for all $\tau \in \mathfrak{H}_p^{\mathrm{RM}}$, where H_τ is an abelian extension of $\mathbb{Q}(\tau)$.

These RM values of rigid meromorphic cocycles seem to behave like CM values of modular functions. For example, there are conjectural Gross–Zagier factorizations. We might also comment about some modular generating series of RM values from the work of Darmon–Pozzi–Vonk.

Theorem 17 (modular parametrizations). *For every elliptic curve E of conductor p, there exists a non-trivial $J_E \in \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}[p^{-1}]), \mathscr{A}^\times / q_E^{\mathbb{Z}})$, where q_E is the Tate period of E. In particular,*

$$J_E[\tau] \in \mathbb{C}_p^\times / q_E^{\mathbb{Z}} = E(\mathbb{C}_p).$$

Conjecture 18. *In the situation of theorem 17, $J_E[\tau] \in E(K^{\mathrm{ab}})$, where $K = \mathbb{Q}(\tau)$.*

2 Modular forms

Our goal is to define modular forms as some sort of "functions" on spaces parametrizing elliptic curves.

2.1 Framed elliptic curves

Definition 19. An *elliptic curve* over a field K is a smooth proper algebraic curve E of genus 1 over K equipped with a rational point $\mathcal{O} \in E(K)$ (the origin or identity element for the group law).

Theorem 20 (Riemann–Roch). *The space $\Omega^1_{E/K}$ of regular differentials on E over K has dimension* 1.

Definition 21. A *framed elliptic curve* is a pair (E, ω) where E is an elliptic curve over a field K and ω is a K–basis of $\Omega^1_{E/K}$.

Theorem 22 (classification of framed elliptic curves). *Let K be a field in which* 6 *is invertible and let (E, ω) be a framed elliptic curve over K. There exists a unique pair of functions $x, y \in \mathscr{O}_E(E \setminus \{ \mathcal{O} \})$ satisfying the following conditions:*

(1) $\operatorname{ord}_{\mathcal{O}}(x) = -2$ *and* $\operatorname{ord}_{\mathcal{O}}(y) = -3$*;*

(2) *x and y satisfy an equation of the form*

$$y^2 = x^3 + g_4 x + g_6$$

for some $g_4, g_6 \in K$ with the property that $\Delta = 4g_4^3 + 27g_6^2 \in K^\times$, and

(3) $\omega = \dfrac{dx}{y}$.

Remark. One can get an analogous result working with framed elliptic curves over a ring R (that might not be a field) such that $6 \in R^\times$.

Definition 23. We say that two framed elliptic curves (E, ω) and (E', ω') over a field K are *isomorphic* if there exists an isomorphism of elliptic curves $\varphi\colon E \to E'$ over K with the property that $\varphi^*(\omega') = \omega$.

Remark. In particular, $\operatorname{Aut}_K(E, \omega) = \{ 1 \}$, in contrast to what happens when we only consider (not framed) elliptic curves, in which case we have at least 2 automorphisms. This fact will be important when we consider moduli spaces.

2.2 Modular forms

Definition 24. A *weakly holomorphic modular form* (or *weak modular form*) over a field K is a rule

$$(E, \omega)/R \mapsto f(E, \omega),$$

assigning to each framed elliptic curve (E, ω) over a K–algebra R a scalar value $f(E, \omega) \in R$, with the following properties:

(1) $f(E, \omega)$ depends only on the isomorphism class of the framed elliptic curve $(E, \omega)/R$, and

(2) it is compatible with base change in the sense that, given a morphism $\varphi \colon R_1 \to R_2$ of K–algebras and a framed elliptic curve $(E, \omega)/R_1$,

$$f\big(\varphi^*(E, \omega)\big) = f\big((E, \omega) \otimes_{R_1, \varphi} R_2\big) = \varphi\big(f(E, \omega)\big).$$

We say that f has *weight* $k \in \mathbb{Z}$ if it satisfies that

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

for all framed elliptic curves (E, ω) over K–algebras and all $\lambda \in R^\times$.

Example 25.

(1) The rule g_4 that assigns to each (E, ω) the coefficient g_4 appearing in the canonical equation (as in theorem 22) is a (weak) modular form over $\mathbb{Z}[1/6]$ of weight 4. Similarly, the rule g_6 that assigns to each (E, ω) the coefficient g_6 appearing in the canonical equation (as in theorem 22) is a (weak) modular form over $\mathbb{Z}[1/6]$ of weight 6. Indeed, to pass from (E, ω) to $(E, \lambda\omega)$, one must apply the change of variables

$$(x, y) \mapsto (\lambda^{-2}x, \lambda^{-3}y)$$

in the canonical equations arising from theorem 22.

(2) Any homogeneous polynomial in g_4 and g_6 of degree k (where g_4 has degree 4 and g_6 has degree 6) is a (weak) modular form of weight k.

(3) $\Delta = 4g_4^3 + 27g_6^2$ is a (weak) modular form of weight 12. By definition, for every framed elliptic curve (E, ω) over a ring R in which 6 is invertible, $\Delta(E, \omega) \in R^\times$.

(4) If $F(X, Y)$ is a homogeneous polynomial of degree of the form $k + 12m$ for some $k, m \in \mathbb{Z}_{\geq 0}$, then

$$\frac{F(g_4, g_6)}{\Delta^m}$$

is a weak modular form of weight k.

(5) $j = g_4^3/\Delta$ is a weak modular form of weight 0; that is, a weak modular function.

Fact 26. *The space* $\mathrm{WMF}(R)$ *of weak modular forms over a ring R in which* 6 *is invertible is a graded ring isomorphic to* $R[g_4, g_6, \Delta^{-1}]$ *(where g_4, g_6 and Δ have degrees* 4, 6 *and* 12*, respectively).*

Definition 27. For every ring R with $6 \in R^\times$, we define

$$\mathrm{Ell}^+(R) = \{ \text{Isomorphism classes of framed elliptic curves } (E, \omega)/R \}.$$

Remark. Theorem 22 shows that there is a natural bijection between $\mathrm{Ell}^+(R)$ and $\mathrm{Hom}_{\mathbb{Z}[1/6]\text{–Alg}}(\mathbb{Z}[1/6][g_4, g_6, \Delta^{-1}], R)$. In fact, Ell^+ is a functor representable by $\mathrm{Spec}(\mathbb{Z}[1/6][g_4, g_6, \Delta^{-1}])$.

2.2.1 Analytic theory

Next we work over $R = \mathbb{C}$. In this situation, one can check that $\mathrm{Ell}^+(\mathbb{C})$ corresponds to the space $\mathcal{L}$ of lattices in $\mathbb{C}$. Indeed, to each framed elliptic curve $(E, \omega)/\mathbb{C}$ we can assign the period lattice

$$\left\{ \int_\gamma \omega : \gamma \in \mathrm{H}_1(E(\mathbb{C}), \mathbb{Z}) \right\}$$

and to each lattice Λ we assign (the isomorphism class of) the framed elliptic curve

$$(\mathbb{C}/\Lambda, 2\pi i\, dz).$$

Using this interpretation of $\mathrm{Ell}^+(\mathbb{C})$, we can give a more concrete definition of weak modular forms over $\mathbb{C}$.

Definition 28. A *weak modular form* over $\mathbb{C}$ of weight k is a function $f\colon \mathcal{L} \to \mathbb{C}$ with the property that

$$f(\lambda\Lambda) = \lambda^{-k} f(\Lambda) \text{ for all } \lambda \in \mathbb{C}^\times \text{ and all } \Lambda \in \mathcal{L}.$$

In order to understand these weak modular forms, one needs to study the space $\mathcal{L}$ of lattices.

Lemma 29. $\mathbb{C}^\times$ *acts on $\mathcal{L}$ by multiplication and there is a canonical bijection*

$$\mathcal{L}/\mathbb{C}^\times \cong \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}.$$

Idea of the proof. Given $\Lambda \in \mathcal{L}$, we can choose an $\mathbb{R}$–basis (ω_1, ω_2) of Λ with the property that $\omega_1/\omega_2 \in \mathfrak{H}$. One checks that different bases differ by a matrix in $\mathrm{SL}_2(\mathbb{Z})$. □

Now we can redefine weak modular forms analytically. If f is a weak modular form over $\mathbb{C}$ (of some weight k), we define

$$f(\tau) = f(\mathbb{Z}\tau \oplus \mathbb{Z}) = f\big(\mathbb{C}/(\mathbb{Z}\tau \oplus \mathbb{Z}), 2\pi i\, dz\big),$$

which is an analytic function on $\mathfrak{H}$. Furthermore,

$$\begin{aligned} f\Big(\frac{a\tau+b}{c\tau+d}\Big) &= f\Big(\mathbb{Z}\frac{a\tau+b}{c\tau+d} \oplus \mathbb{Z}\Big) = f\big((c\tau+d)^{-1}\big(\mathbb{Z}(a\tau+d) \oplus \mathbb{Z}(c\tau+d)\big)\big) \\ &= (c\tau+d)^k f\big(\mathbb{Z}(a\tau+b) \oplus \mathbb{Z}(c\tau+d)\big) = (c\tau+d)^k f(\tau). \end{aligned}$$

In this way, we recover the usual analytic definition of weakly holomorphic modular forms.

2.2.2 The Tate curve

The map $e^{2\pi i\,\cdot}$ induces an isomorphism

$$\big(\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau), 2\pi i\, dz\big) \cong \Big(\mathbb{C}^\times/q^{\mathbb{Z}}, \frac{dt}{t}\Big),$$

where $q = e^{2\pi i\tau}$ and $t = e^{2\pi i z}$. One should think of τ as a variable on $\mathfrak{H}$ and of q as a variable on the (punctured) unit disc.

Proposition 30. *The framed elliptic curve $\big(\mathbb{C}^\times/q^{\mathbb{Z}}, dt/t\big)$ is described by an affine equation*

$$E_q \colon y^2 = x^3 + g_4(q)x + g_6(q)$$

with invariant differential

$$\omega_q = \frac{dx}{y},$$

where

$$\begin{aligned} g_4(q) &\equiv \frac{1}{240} + \sum_{n=1}^{\infty} \sigma_3(n)q^n \mod \mathbb{Z}[1/6]^\times, \\ g_6(q) &\equiv \frac{-1}{504} + \sum_{n=1}^{\infty} \sigma_5(n)q^n \mod \mathbb{Z}[1/6]^\times, \\ \sigma_k(n) &= \sum_{d|n} d^k. \end{aligned}$$

Remark. We may make a change of variables to avoid the factors 2 and 3 in the denominators and obtain an equation

$$E_q \colon y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

with coefficients in $\mathbb{Z}[\![q]\!]$. The discriminant of E_q is given by

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24},$$

which makes sense as a formal series in $\mathbb{Z}(\!(q)\!)^{\times}$.

Definition 31. The framed elliptic curve $(E_q, \omega_q)/\mathbb{Z}(\!(q)\!)$ given by the equations in proposition 30 is called the *Tate curve*.

Remark. By abuse of notation, given a ring R, we write (E_q, ω_q) (or $(E_q, \omega_q)/R(\!(q)\!)$) also for the base change of $(E_q, \omega_q)/\mathbb{Z}(\!(q)\!)$ to $R(\!(q)\!)$.

Definition 32. The *q–expansion* of a weak modular form f over a ring R is

$$f\big((E_q, \omega_q)/R(\!(q)\!)\big) \in R(\!(q)\!).$$

Definition 33. A *(holomorphic) modular form* is a weakly modular form f over a ring R whose q–expansion $f(E_q, \omega_q)$ lies in $R[\![q]\!]$ (not just in $R(\!(q)\!)$). We write $\mathrm{MF}(R)$ for the space of modular forms over R.

Remark. Suppose that $6 \in R^{\times}$. The identification $\mathrm{WMF}(R) = R[g_4, g_6, \Delta^{-1}]$ restricts to $\mathrm{MF}(R) = R[g_4, g_6]$.

3 Elliptic curves with complex multiplication

3.1 Endomorphisms of elliptic curves

Let E be an elliptic curve over a field k. Let $\mathrm{End}_k(E)$ denote the ring of endomorphisms of E/k (i.e., morphisms $E \to E$ of algebraic curves over k mapping $\mathcal{O}$ to $\mathcal{O}$). In $\mathrm{End}_k(E)$ there is a sum induced by the (commutative) group law of E and a multiplication given by composition.

The ring $\mathrm{End}_k(E)$ is equipped with a canonical anti-involution that sends an isogeny ϕ to its dual ϕ^*. The fact that this operation is an anti-involution means that $(\phi^*)^* = \phi$ and $(\phi \circ \psi)^* = \psi^* \circ \phi^*$. Recall that $\phi \circ \phi^* = \phi^* \circ \phi = [\deg(\phi)]$.

Fix an algebraic closure $\overline{k}$ of k. One can prove that $\mathrm{End}_{\overline{k}}(E)$ is a free $\mathbb{Z}$–module of rank ≤ 4. Indeed, $\mathrm{End}_{\overline{k}}(E)$ is $\mathbb{Z}$–torsion-free because

$$n\phi = 0 \implies n^2 \deg(\phi) = \deg(n\phi) = 0 \implies \deg(\phi) = 0 \implies \phi = 0.$$

Moreover, $\mathrm{End}_{\overline{k}}(E)$ is free of rank ≤ 4 over $\mathbb{Z}$ because, given a prime $\ell \neq \mathrm{char}(k)$, $\mathrm{End}_{\overline{k}}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ acts faithfully on $\mathrm{T}_\ell(E)(\overline{k}) \cong \mathbb{Z}_\ell^2$.

Proposition 34. *In the situation above, there are only the following possibilities:*

(1) $\mathrm{End}_{\overline{k}}(E) = \mathbb{Z}$,

(2) $\mathrm{End}_{\overline{k}}(E)$ *is an order in a quadratic imaginary field or*

(3) $\mathrm{char}(k) = p > 0$ *and* $\mathrm{End}_{\overline{k}}(E)$ *is an order in the quaternion algebra ramified at p and at ∞.*

The proof of this result can be found in Silverman's books on elliptic curves.

3.1.1 The theory over $\mathbb{C}$

Lemma 35. *Let E be an elliptic curve over $\mathbb{C}$. Then* $\mathrm{End}_{\mathbb{C}}(E)$ *is either $\mathbb{Z}$ or a quadratic imaginary order.*

Proof. Consider an isogeny $\phi\colon E \to E$ and regard it as an analytic function $\phi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ by means of the complex uniformization of E. Then

$$\phi(z+\omega) - \phi(z) \in \Lambda \quad \text{for all } z \in \mathbb{C} \text{ and } \omega \in \Lambda.$$

In particular, if we fix $\omega \in \Lambda$ and view this as a function of $z \in \mathbb{C}$,

$$\phi'(z+\omega) - \phi'(z) = 0.$$

Therefore, ϕ' takes all its values on a fundamental parallelogram, which is compact in $\mathbb{C}$, and so must be bounded. Liouville's theorem implies that $\phi'(z)$ is constant and so, using that $\phi(\Lambda) \subset \Lambda$, there exists $\alpha \in \mathbb{C}$ such that ϕ is of the form

$$\phi(z) = \alpha \cdot z \quad \text{for all } z \in \mathbb{C}/\Lambda.$$

In conclusion, every endomorphism of E acts as a scalar on $\Omega^1_{E/\mathbb{C}}$.

In fact, we may identify

$$\mathrm{End}_{\mathbb{C}}(E) = \{\, \alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda \,\}.$$

Hence, $\mathrm{End}_{\mathbb{C}}(E)$ is a discrete subring of $\mathbb{C}$ (because it preserves a lattice) and so must be either $\mathbb{Z}$ or a quadratic imaginary order. □

Remark. The ring $\mathrm{End}_{\mathbb{C}}(E)$ acts faithfully both on $\mathrm{H}_1(E(\mathbb{C}), \mathbb{Z})$ and on $\Omega^1_{E/\mathbb{C}}$ (that can be regarded inside $\mathrm{H}^1_{\mathrm{dR}}(E/\mathbb{C})$). These actions provide embeddings of $\mathrm{End}_{\mathbb{C}}(E)$ into $\mathrm{M}_2(\mathbb{Z})$ and into $\mathbb{C}$, respectively.

Definition 36. We say that an elliptic curve $E/\mathbb{C}$ has *complex multiplication* or *CM* if $\mathrm{End}_{\mathbb{C}}(E)$ is an order in a quadratic imaginary field.

Remark. Quadratic orders are uniquely determined by their *discriminant*. Every discriminant can be decomposed as $D = D_0c^2$, where D_0 is a fundamental discriminant: the discriminant of a maximal order (the ring of integers in a quadratic imaginary field). A fundamental discriminant D_0 must be

- of the form $2^t m$ for m odd and square-free and $0 \leq t \leq 3$, and
- $D_0 \equiv 0$ or $1 \bmod 4$.

3.2 Complex multiplication by $\mathscr{O}$

Let $\mathscr{O}$ be an order in a quadratic imaginary field K. (Sometimes we will assume that $\mathscr{O}$ is the ring of integers $\mathscr{O}_K$ to simplify the exposition). We write D for the discriminant of $\mathscr{O}$ and consider the class group $\mathrm{Cl}(D) = \mathrm{Cl}(\mathscr{O})$, which is the group of invertible fractional ideal classes of $\mathscr{O}$ (the precise definitions become somewhat more complicated if $\mathscr{O}$ is not a maximal order). Let k be a field with a fixed inclusion $\mathscr{O} \hookrightarrow k$.

Definition 37. We define $\mathrm{CM}_k(\mathscr{O})$ to be the set of $\bar{k}$–isomorphism classes of elliptic curves E/k equipped with an isomorphism $\mathscr{O} \cong \mathrm{End}_k(E)$ with the property that, for every $\alpha \in \mathscr{O}$ (that we identify with an element in $\mathrm{End}_k(E)$), the induced morphism $\alpha^* \colon \Omega^1_{E/k} \to \Omega^1_{E/k}$ is given by $\alpha^*(\omega) = \alpha\omega$.

Remark. Given an elliptic curve E/k with CM by $\mathscr{O}$, there could be two ways to define $\mathscr{O} \cong \mathrm{End}_k(E)$ (as we can always compose with $[-1]$). The last condition pins down one of the two isomorphisms.

Proposition 38. *The set* $\mathrm{CM}_{\mathbb{C}}(\mathscr{O})$ *is finite and has the same number of elements as* $\mathrm{Cl}(\mathscr{O})$.

Proof. We use the correspondence between elliptic curves $E/\mathbb{C}$ and lattices Λ in $\mathbb{C}$ up to homothety. If E has CM by $\mathscr{O}$, then Λ is a projective module over $\mathscr{O}$ and there are $h = |\mathrm{Cl}(\mathscr{O})|$ homothety classes of such modules. □

Remark. We can use the complex uniformization of elliptic curves to describe $\mathrm{CM}_{\mathbb{C}}(\mathscr{O})$ as the set of $\tau \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ that satisfy a quadratic equation

$$a\tau^2 + b\tau + c = 0$$

with a, b, c coprime integers such that $D = b^2 - 4ac$ (i.e., they are zeros of a primitive binary quadratic form of the given discriminant D). We fix representatives $\tau_1, \dots, \tau_h$ of $\mathrm{CM}_{\mathbb{C}}(\mathscr{O})$.

Proposition 39. *If* $E/\mathbb{C}$ *has CM by* $\mathscr{O}$*, then* $j(E)$ *is algebraic and generates a field of degree* $\leq h = |\mathrm{Cl}(\mathscr{O})|$ *over* $\mathbb{Q}$.

Proof. The group $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ acts on $\mathrm{CM}_{\mathbb{C}}(\mathscr{O})$. Indeed, given $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ and $\phi \in \mathrm{End}_{\mathbb{Q}}(E)$, we have $\phi^\sigma \in \mathrm{End}_{\mathbb{Q}}(E^\sigma)$. Thus, $\phi \mapsto \phi^\sigma$ gives an identification $\mathrm{End}_{\mathbb{Q}}(E) \cong \mathrm{End}_{\mathbb{Q}}(E^\sigma)$.

Therefore, $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ permutes the j–invariants $j(\tau_1), \dots, j(\tau_h)$ of the elliptic curves in $\mathrm{CM}_{\mathbb{C}}(\mathscr{O})$. In particular, $j(E)$ is the zero of a polynomial of degree $\leq h$.□

Let L be the field generated by $j(\tau_1), \dots, j(\tau_h)$ over the quadratic imaginary field $K = \mathrm{Frac}(\mathscr{O})$. We fix an embedding $L \hookrightarrow \mathbb{C}$. By proposition 39, we obtain that $\mathrm{CM}_L(\mathscr{O}) \cong \mathrm{CM}_{\mathbb{C}}(\mathscr{O})$. Our next goal is to relate $\mathrm{Cl}(\mathscr{O})$ and $\mathrm{CM}_L(\mathscr{O})$ (which are finite sets of the same size) algebraically (without relying on the complex uniformization of elliptic curves).

3.3 The action of $\mathrm{Cl}(\mathscr{O})$ on $\mathrm{CM}_L(\mathscr{O})$

We continue with the notation from section 3.2. Let us assume that $\mathscr{O}$ is a maximal ideal for simplicity.

Definition 40. Let $\mathfrak{a}$ be a fractional ideal of $\mathscr{O}$. We define

$$\mathfrak{a} * E = \mathrm{Hom}_{\mathscr{O}}(\mathfrak{a}, E).$$

Fix an elliptic curve E/L with CM by $\mathscr{O}$. Since E/L is an algebraic group and $\mathrm{End}_L(E) \cong \mathscr{O}$, we may identify E with the functor

$$\mathrm{Hom}_{L\text{–Alg}}(\,\cdot\,, E)\colon L\text{–Alg} \to \mathscr{O}\text{–Mod}.$$

Given $[\mathfrak{a}] \in \mathrm{Cl}(\mathscr{O})$, we interpret $\mathrm{Hom}_{\mathscr{O}}(\mathfrak{a}, E)$ again as a functor L–Alg $\to \mathscr{O}$–Mod and try to see next that it is represented by another elliptic curve in $\mathrm{CM}_L(\mathscr{O})$.

We may assume, up to multiplication by a scalar in $\mathscr{O}$, that $\mathfrak{a}$ is an ideal of $\mathscr{O}$ (not just an integral ideal). In that case, there is a short exact sequence

$$0 \longrightarrow \mathfrak{a} \longrightarrow \mathscr{O} \longrightarrow \mathscr{O}/\mathfrak{a} \longrightarrow 0$$

of $\mathscr{O}$–modules to which we can apply $\mathrm{Hom}_{\mathscr{O}}(\,\cdot\,, E)$ to obtain another short exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathscr{O}}(\mathscr{O}/\mathfrak{a}, E) \longrightarrow \mathrm{Hom}_{\mathscr{O}}(\mathscr{O}, E) \longrightarrow \mathrm{Hom}_{\mathscr{O}}(\mathfrak{a}, E) \longrightarrow 0.$$

We can interpret the last exact sequence as the definition of the algebraic group $\mathrm{Hom}_{\mathscr{O}}(\mathfrak{a}, E)$:

$$\begin{aligned} \mathrm{Hom}_{\mathscr{O}}(\mathscr{O}/\mathfrak{a}, E) &\longrightarrow E \\ f &\longmapsto f(1) \end{aligned} \qquad \text{and} \qquad \begin{aligned} \mathrm{Hom}_{\mathscr{O}}(\mathscr{O}, E) &\longrightarrow E \\ f &\longmapsto f(1) \end{aligned}$$

allow us to identify

$$\mathrm{Hom}_{\mathscr{O}}(\mathscr{O}/\mathfrak{a}, E) = E[\mathfrak{a}] \quad \text{and} \quad \mathrm{Hom}_{\mathscr{O}}(\mathscr{O}, E) = E$$

and so $\mathfrak{a} * E = \mathrm{Hom}_{\mathscr{O}}(\mathfrak{a}, E)$ must be the (isomorphism class of the) elliptic curve $E/E[\mathfrak{a}]$. That is, we obtain a short exact sequence

$$0 \longrightarrow E[\mathfrak{a}] \longrightarrow E \longrightarrow \mathfrak{a} * E \longrightarrow 0$$

and so we have an isogeny $\varphi_{\mathfrak{a}}\colon E \to \mathfrak{a} * E$ with $\mathrm{Ker}(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}]$. In particular, if $\mathfrak{a}$ is a principal ideal generated by $\alpha \in \mathscr{O}$, then $\varphi_a = \alpha\colon E \to E$ (and $\mathfrak{a} * E = E$). All in all, we defined an action of $\mathrm{Cl}(\mathscr{O})$ on $\mathrm{CM}_L(\mathscr{O})$.

Working over $\mathbb{C}$, the elliptic curve $E/\mathbb{C}$ corresponds to a lattice Λ giving rise to a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \Lambda \arrow[r] & \mathbb{C} \arrow[r] & E(\mathbb{C}) \arrow[r] & 0. \end{tikzcd}$$

After applying $\mathrm{Hom}_{\mathscr{O}}(\mathfrak{a}, \cdot\,)$, we obtain a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_{\mathscr{O}}(\mathfrak{a},\Lambda) \arrow[r] \arrow[d, equal] & \mathrm{Hom}_{\mathscr{O}}(\mathfrak{a},\mathbb{C}) \arrow[r] \arrow[d, equal] & \mathrm{Hom}_{\mathscr{O}}(\mathfrak{a},E(\mathbb{C})) \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & \mathfrak{a}^{-1}\Lambda \arrow[r] & \mathbb{C} \arrow[r] & (\mathfrak{a} * E)(\mathbb{C}) \arrow[r] & 0 \end{tikzcd}$$

and so $\mathfrak{a} * E$ corresponds to $\mathbb{C}/(\mathfrak{a}^{-1}\Lambda)$. In particular, the action of $\mathrm{Cl}(\mathscr{O})$ on $\mathrm{CM}_{\mathbb{C}}(\mathscr{O})$ is simply transitive.

Corollary 41. *The set $\mathrm{CM}_L(\mathscr{O})$ is a principal $\mathrm{Cl}(\mathscr{O})$–set with an action of $\mathrm{Gal}(L/K)$.*

Proposition 42. *The natural actions of $\mathrm{Gal}(L/K)$ and of $\mathrm{Cl}(\mathscr{O})$ on $\mathrm{CM}_L(\mathscr{O})$ commute.*

Proof. Take $\mathfrak{a} \in \mathrm{Cl}(\mathscr{O})$ and $\sigma \in \mathrm{Gal}(L/K)$. We want to prove that (with the notation from before) $\mathrm{Hom}_{\mathscr{O}}(\mathfrak{a}, E)^{\sigma} = \mathrm{Hom}_{\mathscr{O}}(\mathfrak{a}, E^{\sigma})$. We use the short exact sequences characterizing these algebraic groups. Namely, $\mathfrak{a} * E$ is defined by the sequence

$$\begin{tikzcd} 0 \arrow[r] & E[\mathfrak{a}] \arrow[r] & E \arrow[r] & \mathfrak{a} * E \arrow[r] & 0. \end{tikzcd}$$

After applying σ to it, we obtain another short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & E[\mathfrak{a}]^{\sigma} \arrow[r] & E^{\sigma} \arrow[r] & (\mathfrak{a} * E)^{\sigma} \arrow[r] & 0. \end{tikzcd}$$

But $E[\mathfrak{a}]^{\sigma} = E^{\sigma}[\mathfrak{a}]$ because σ acts trivially on K. Therefore, the last short exact sequence is that which characterizes $\mathfrak{a} * (E^{\sigma})$ and we conclude that

$$(\mathfrak{a} * E)^{\sigma} = \mathfrak{a} * (E^{\sigma}). \qquad \square$$

Lemma 43. *Let G be a group and let X be a principal G–set (with a left action of G). Let $x_0 \in X$. If X is also equipped with a commuting right action of another group Γ, there is a homomorphism $r\colon \Gamma \to G$ defined as follows: for every $\sigma \in \Gamma$, $r(\sigma)$ is the unique element of G such that*

$$x_0^{\sigma} = r(\sigma) * x_0.$$

Proof. The existence and uniqueness of $r(\sigma)$ with the property that $x_0^{\sigma} = r(\sigma) * x_0$ follow from the fact that X is principal as a G–set.

To see that r is a group homomorphism, take $\sigma, \tau \in \Gamma$ and compute

$$x_0^{\sigma\tau} = (x_0^{\sigma})^{\tau} = \big(r(\sigma) * x_0\big)^{\tau} = r(\sigma) * x_0^{\tau} = r(\sigma) * (r(\tau) * x_0) = \big(r(\sigma)r(\tau)\big) * x_0.$$

Therefore, $r(\sigma\tau) = r(\sigma)r(\tau)$. □

Remark. The homomorphism $r \colon \Gamma \to G$ depends on the choice of $x_0 \in X$, but replacing x_0 with $h * x_0$ conjugates r by h.

Corollary 44. *Let $E \in \mathrm{CM}_L(\mathscr{O})$. There is a homomorphism $r \colon \operatorname{Gal}(L/K) \to \operatorname{Cl}(\mathscr{O})$ (independent of E) characterized by*

$$E^{\sigma} = r(\sigma) * E.$$

Recall that $L = K(j(\tau_1), \dots, j(\tau_h))$ and so r is injective. In particular, L is an abelian extension of K of degree $\leq h$. But observe that we have yet to prove that r is surjective.

3.3.1 The effect of r on Frobenius elements

Let S be the set of prime ideals $\mathfrak{p}$ of $\mathscr{O} = \mathscr{O}_K$ satisfying one of the following properties:

(1) $\mathfrak{p}$ is ramified in L/K,

(2) some of the elements $j(\tau_1), \dots, j(\tau_h)$ fails to be integral at $\mathfrak{p}$ or

(3) the natural map $\{ j(\tau_1), \dots, j(\tau_h) \} \to \mathscr{O}_L/\mathfrak{P}$ is not injective for some prime ideal $\mathfrak{P}$ of $\mathscr{O}_L$ lying over $\mathfrak{p}$ or, equivalently,

$$\mathfrak{p} \mid \mathrm{N}_{L/K}\Big(\prod_{k<l} (j(\tau_k) - j(\tau_l))\Big).$$

Proposition 45. *Let $\mathfrak{p}$ be a prime ideal of $\mathscr{O}_K$ such that $\mathfrak{p} \notin S$ and let $\sigma_{\mathfrak{p}} \in \operatorname{Gal}(L/K)$ be the Frobenius element at $\mathfrak{p}$. Then $r(\sigma_{\mathfrak{p}}) = \mathfrak{p}$.*

Proof. Let $E \in \mathrm{CM}_L(\mathscr{O}_K)$. Recall that we have an isogeny $\varphi_{\mathfrak{p}} \colon E \to \mathfrak{p} * E$, defined over $\mathscr{O}_L$, with $\operatorname{Ker}(\varphi_{\mathfrak{p}}) = E[\mathfrak{p}]$. We consider its reduction modulo $\mathfrak{P}$ (for a prime $\mathfrak{P}$ of $\mathscr{O}_L$ lying over $\mathfrak{p}$), $\overline{\varphi}_{\mathfrak{p}} \colon \overline{E} \to \mathfrak{p} * \overline{E}$.

- Case 1: $p\mathscr{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ with $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Then $\varphi_{\mathfrak{p}}$ is an isogeny of degree p and we claim that $\overline{\varphi}_{\mathfrak{p}}$ is (purely) inseparable. Indeed, we can choose an ideal $\mathfrak{a}$ such that $\mathfrak{a}\mathfrak{p} = \alpha\mathscr{O}_K$ for some $\alpha \in \mathscr{O}_K$ and $p \nmid \mathrm{N}(\mathfrak{a})$. Then the composition

$$\overline{E} \xrightarrow{\overline{\varphi}_{\mathfrak{p}}} \mathfrak{p} * \overline{E} \xrightarrow{\overline{\varphi}_{\mathfrak{a}}} \mathfrak{a} * \mathfrak{p} * \overline{E} \cong \overline{E}$$

is inseparable (as it induces multiplication by α on differentials) and this is only possible if the first arrow is inseparable. On the other hand, there is a unique inseparable isogeny of degree p (up to isomorphisms) which is the p–th power Frobenius. Therefore, $j(\mathfrak{p} * \overline{E}) = j(\overline{E}^{(p)})$. By the last condition on the set S, we conclude that $\mathfrak{p} * E = E^{\sigma_{\mathfrak{p}}}$.

- Case 2: $p\mathcal{O}_K = \mathfrak{p}^2$. We can apply the same argument as above.
- Case 3: $p\mathcal{O}_K$ is a prime ideal. In that case, φ_p is the multiplication-by-p morphism. On the other hand, E must have supersingular reduction at $\mathfrak{P}$ and so, on $\overline{E}$, the endomorphism $[p]$ differs from the p^2–th power Frobenius morphism by an isomorphism. □

3.4 Elliptic curves over finite fields

Let E be an elliptic curve over a finite field k with $q = p^f$ elements. We have a (relative) Frobenius morphism

$$\phi_p \colon E \to E^{(p)}$$

given on coordinates by $\phi_p(x, y) = (x^p, y^p)$. One can check that ϕ is a purely inseparable isogeny of degree p and so admits a dual isogeny

$$\phi_p^* \colon E^{(p)} \to E.$$

Write $E[p]$ for the kernel of the multiplication-by-p morphism $[p] \colon E \to E$, regarded as a finite flat group scheme over k. Since $[p] = \phi_p^* \circ \phi_p$ and ϕ_p is purely inseparable, $\mathrm{Ker}(\phi)$ is a connected group scheme and so $E[p]$ can have at most p points (over an algebraic closure $\overline{k}$):

$$\text{either } E[p](\overline{k}) = 0 \text{ or } E[p](\overline{k}) \cong \mathbb{Z}/p\mathbb{Z}.$$

Observe that $E^{(p^f)} = E$ and so $\phi_p^f \in \mathrm{End}_k(E)$. Often (more precisely, when E is ordinary) this endomorphism ϕ_p^f is not in $\mathbb{Z}$ (i.e., is not multiplication by an integer).

Theorem 46. *Let E be an elliptic curve over k as above. The following conditions are equivalent:*

(1) $E[p](\overline{k}) = 0$ *and* $[p] \colon E \to E$ *is purely inseparable;*

(2) $\mathrm{End}_{\overline{k}}(E)$ *is an order in a quaternion algebra B such that*

$$B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \mathrm{M}_2(\mathbb{Q}_\ell) \text{ for all primes } \ell \neq p$$

and

$$B \otimes_{\mathbb{Q}} \mathbb{Q}_p \text{ and } B \otimes_{\mathbb{Q}} \mathbb{R} \text{ are division algebras.}$$

If these conditions hold, $j(E) \in \mathbb{F}_{p^2}$.

Definition 47. We say that an elliptic curve E/k is *supersingular* if it satisfies the equivalent conditions of theorem 46; otherwise, we say that E/k is *ordinary*.

Theorem 48. *If E/k is an ordinary elliptic curve, then*

(1) *$E[p](\overline{k}) \cong \mathbb{Z}/p\mathbb{Z}$ and $\phi_p^* \colon E^{(p)} \to E$ is separable, and*

(2) *the ring $\mathrm{End}_{\overline{k}}(E)$ is a quadratic imaginary order.*

3.4.1 Reduction of elliptic curves with CM

Let $\mathscr{O}$ be an order in a quadratic imaginary field K and let $L = K(j(\tau_1), \dots, j(\tau_h))$ for a set of representatives $\tau_1, \dots, \tau_h$ of the classes in $\mathrm{CM}_{\mathbb{C}}(\mathscr{O})$. Write k for the residue field of L.

Proposition 49. *Let E be an elliptic curve over L and let $\mathfrak{P}$ be a prime ideal of $\mathscr{O}_L$ at which E has good reduction. Write $\overline{E}$ for the reduction of E modulo $\mathfrak{P}$. The canonical morphism*

$$\mathrm{End}_L(E) \to \mathrm{End}_k(\overline{E})$$

is injective.

Proof. If $\phi \in \mathrm{End}_L(E)$ lies in the kernel of the reduction, then ϕ induces the 0 morphism on $\overline{E}[\ell^n](\overline{k})$ for every prime $\ell \neq p$ and every $n \geq 1$. But reduction modulo $\mathfrak{P}$ induces an isomorphism $E[\ell^n](\overline{L}) \cong \overline{E}[\ell^n](\overline{k})$, so $\phi|_{E[\ell^n](\overline{L})} = 0$. As the kernel of a non-trivial isogeny is finite, this is only possible if $\phi = 0$. □

Theorem 50. *Let $E \in \mathrm{CM}_L(\mathscr{O}_K)$ and let $\mathfrak{P}$ be a prime ideal of $\mathscr{O}_L$ at which E has good reduction. Let $\mathfrak{p}$ (resp. p) denote the prime of $\mathscr{O}_K$ (resp. $\mathbb{Z}$) below $\mathfrak{P}$.*

(1) *If p splits in K, then E has ordinary reduction at $\mathfrak{P}$.*

(2) *If p is inert or ramified in K, then the E has supersingular reduction at $\mathfrak{P}$.*

Proof. First suppose that p splits in K and write $p\mathscr{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. The isogeny

$$\varphi_{\overline{\mathfrak{p}}} \colon E \to \overline{\mathfrak{p}} * E$$

with kernel $E[\overline{\mathfrak{p}}]$ introduced in section 3.3 is a separable morphism modulo $\mathfrak{P}$. Indeed, we can choose an ideal $\mathfrak{a} \subset \mathscr{O}_K$ such that $\mathfrak{a}\overline{\mathfrak{p}} = \alpha\mathscr{O}_K$ with $\mathfrak{p} \nmid \alpha$. Then the composition

$$\alpha\colon E \xrightarrow{\varphi_{\overline{\mathfrak{p}}}} \overline{\mathfrak{p}} * E \xrightarrow{\varphi_{\mathfrak{a}}} \mathfrak{a}\overline{\mathfrak{p}} * E \cong E$$

induces a map on differentials given by $\alpha^*(\omega) = \alpha\omega$, which is $\neq 0 \bmod \mathfrak{P}$. Thus, the reduction of $\varphi_{\overline{\mathfrak{p}}}$ must be separable (of degree p) and $E[\overline{\mathfrak{p}}](\overline{k}) \cong \mathbb{Z}/p\mathbb{Z}$. In particular, the reduction $\overline{E}$ has $\overline{k}$–rational points of order p, which means that $\overline{E}$ is ordinary.

Conversely, suppose that $\overline{E}$ is ordinary. For every $n \in \mathbb{Z}_{\geq 1}$, consider the restriction

$$\mathrm{End}_{\overline{k}}(\overline{E}) \to \mathrm{End}\big(\overline{E}[p^n](\overline{k})\big).$$

We know that $\overline{E}[p^n](\overline{k}) \cong \mathbb{Z}/p^n\mathbb{Z}$ and taking the projective limit over n we obtain an injective morphism

$$\mathrm{End}_{\overline{k}}(\overline{E}) \hookrightarrow \mathrm{End}\big(\mathrm{T}_p(E)(\overline{k})\big) \cong \mathrm{End}\big(\mathbb{Z}_p\big) \cong \mathbb{Z}_p$$

(the injectivity follows because a non-trivial isogeny cannot have infinitely many points in the kernel). Therefore, we obtain

$$\mathscr{O}_K \cong \mathrm{End}_L(E) \hookrightarrow \mathrm{End}_k(\overline{E}) \hookrightarrow \mathbb{Z}_p$$

and this is only possible if p splits in K. □

3.5 Class field theory

Let K be a number field with ring of integers $\mathscr{O}_K$. Let $\mathfrak{c}$ be an ideal of $\mathscr{O}_K$. We define $I(\mathfrak{c})$ to be the set of fractional ideals I of $\mathscr{O}_K$ such that $(I, \mathfrak{c}) = 1$ and $P(\mathfrak{c})$ to be the subset of principal fractional ideals (α) of $\mathscr{O}_K$ such that $\alpha \equiv 1 \bmod \mathfrak{c}$.

Main theorem of class field theory. *There is an abelian extension $H_\mathfrak{c}$ of K equipped with an isomorphism*

$$\mathrm{rec} = \mathrm{rec}_\mathfrak{c}\colon I(\mathfrak{c})/P(\mathfrak{c}) \to \mathrm{Gal}(H_\mathfrak{c}/K)$$

satisfying the following properties:

(1) *the extension $H_\mathfrak{c}/K$ is unramified away from $\mathfrak{c}$, and*

(2) $\mathrm{rec}(\mathfrak{p}) = \sigma_\mathfrak{p}$ *for all prime ideals $\mathfrak{p} \subset \mathscr{O}_K$ such that $\mathfrak{p} \nmid \mathfrak{c}$ (where $\sigma_\mathfrak{p}$ denotes the Frobenius at $\mathfrak{p}$).*

The abelian extension $H_{\mathfrak{c}}$, called the ray class field of K of conductor $\mathfrak{c}$, *is uniquely determined by these properties.*

Remark. When $\mathfrak{c} = 1$, the field $H = H_1$ is the *Hilbert class field of K*: the maximal unramified abelian extension of K, which satisfies that $\mathrm{Gal}(H/K) \cong \mathrm{Cl}(K)$.

Theorem 51. *If K is a quadratic imaginary field, the extension $L = K(j(E_1), \ldots, j(E_h))$ generated by the j–invariants of the elliptic curves $\{ E_1, \ldots, E_h \} = \mathrm{CM}_{\mathbb{C}}(\mathscr{O}_K)$ is the Hilbert class field of K.*

Proof. Recall that we constructed

$$r\colon \mathrm{Gal}(L/K) \to \mathrm{Cl}(\mathscr{O}_K)$$

characterized by $r(\sigma_{\mathfrak{p}}) = \mathfrak{p}$ for all prime ideals $\mathfrak{p}$ of $\mathscr{O}_K$ outside a finite set S. Therefore, r must be the inverse of rec. □

3.6 Galois action on torsion points

Let $\mathscr{O}_K$ be the ring of integers of a quadratic imaginary field K and consider $\mathrm{CM}_{\mathbb{C}}(\mathscr{O}_K) = \{ E_1, \ldots, E_h \}$. We saw that the values $j(E_1), \ldots, j(E_h)$ are defined over the Hilbert class field H of K. Thus, we can fix $E \in \mathrm{CM}_H(\mathscr{O}_K)$. Our next goal is to study the action of $\mathrm{Gal}(\overline{H}/H)$ on the torsion points of E.

Let $\mathfrak{c}$ be an ideal of $\mathscr{O}_K$. Then $E[\mathfrak{c}](\overline{H})$ is a free $(\mathscr{O}_K/\mathfrak{c})$–module of rank 1 with an action of $\mathrm{Gal}(\overline{H}/H)$. We write

$$\rho_{E,\mathfrak{c}}\colon \mathrm{Gal}(\overline{H}/H) \to \mathrm{Aut}_{\mathscr{O}_K/\mathfrak{c}}(E[\mathfrak{c}](\overline{H}))$$

for the corresponding representation.

Corollary 52. *In the situation above, the representation $\rho_{E,\mathfrak{c}}$ has abelian image.*

Proof. We have

$$\mathrm{Aut}_{\mathscr{O}_K/\mathfrak{c}}(E[\mathfrak{c}](\overline{H})) \cong (\mathscr{O}_K/\mathfrak{c})^\times,$$

which is clearly abelian. □

Proposition 53. *The field $L_{\mathfrak{c}}$ cut out by $\rho_{E,\mathfrak{c}}$ is the ray class field $H_{\mathfrak{c}}$ of conductor $\mathfrak{c}$.*

Proof. We have a short exact sequence

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(H_{\mathfrak{c}}/H) \arrow[r] \arrow[d, phantom, "\wr\|"] & \mathrm{Gal}(H_{\mathfrak{c}}/K) \arrow[r] \arrow[d, phantom, "\wr\|"] & \mathrm{Gal}(H/K) \arrow[r] \arrow[d, phantom, "\wr\|"] & 1 \\
1 \arrow[r] & P(1)/P(\mathfrak{c}) \arrow[r] & I(\mathfrak{c})/P(\mathfrak{c}) \arrow[r] & I(1)/P(1) \arrow[r] & 1
\end{tikzcd}$$

and so, by looking at generators,

$$\mathrm{Gal}(H_{\mathfrak{c}}/H) \cong P(1)/P(\mathfrak{c}) \cong (\mathscr{O}_K/\mathfrak{c})^\times/\mathscr{O}_K^\times.$$

Define $\mathrm{CM}_{L_{\mathfrak{c}}}(\mathscr{O}_K, \mathfrak{c})$ to be the set of isomorphism classes of pairs (E, P), where E is an elliptic curve defined over $L_{\mathfrak{c}}$ with CM by $\mathscr{O}_K$ and P is a generator of $E[\mathfrak{c}](L_{\mathfrak{c}})$. This set is endowed with an action of $I(\mathfrak{c})/P(\mathfrak{c})$ given by

$$\mathfrak{a} * (E, P) = (\mathfrak{a} * E, \varphi_{\mathfrak{a}}(P)),$$

where $\varphi_{\mathfrak{a}} \colon E \to \mathfrak{a} * E$ is the canonical isogeny associated with $\mathfrak{a}$ as described in section 3.3. The actions of $I(\mathfrak{c})/P(\mathfrak{c})$ and of $\mathrm{Gal}(\overline{H}/H)$ on $\mathrm{CM}_{L_{\mathfrak{c}}}(\mathscr{O}_K, \mathfrak{c})$ commute. Therefore, by lemma 43, we obtain an isomorphism

$$r \colon \mathrm{Gal}(L_{\mathfrak{c}}/K) \to I(\mathfrak{c})/P(\mathfrak{c}).$$

On principal ideals, we have

$$r^{-1}(\alpha\mathscr{O}_K)(E, P) = (E, \varphi_\alpha(P)) = (E, \alpha P).$$

By a density argument, we see that r must be the inverse of the reciprocity map $\mathrm{rec}_{\mathfrak{c}}$. In conclusion, $L_{\mathfrak{c}} = H_{\mathfrak{c}}$ by the main theorem of class field theory. □

Corollary 54. *The values $j(\tau_1), \ldots, j(\tau_h)$ together with the coordinates of all the torsion points of $E_1, \ldots, E_h$ generate the maximal abelian extension of K.*

3.7 Integrality

Let K be a finite extension of $\mathbb{Q}_p$ and let E be an elliptic curve over K. Let $\mathscr{O}_K$ be the ring of integers of K and let $\mathfrak{p}$ denote its maximal ideal. By hypothesis, $j(E) \in K$.

Suppose that $\mathrm{ord}_{\mathfrak{p}}(j(E)) < 0$. Recall that the q–expansion of j is of the form

$$j(q) = \frac{1}{q}\Big(1 + 744q + 196884q^2 + \cdots\Big) \in \mathbb{Z}((q))^\times$$

and so we can express

$$\begin{aligned} q &= \frac{1}{j}\Big(1 + 744q + \cdots\Big) = \frac{1}{j}\Big(1 + 744\frac{1}{j}(1 + 744q + \cdots) + \cdots\Big) \\ &= \frac{1}{j} + a_2\frac{1}{j^2} + a_3\frac{1}{j^3} + \cdots \in \mathbb{Z}[\![j^{-1}]\!] \end{aligned}$$

Write $j_E = j(E)$ and

$$q_E = \frac{1}{j_E} + a_2\frac{1}{j_E^2} + a_3\frac{1}{j_E^3} + \cdots \in \mathfrak{p},$$

which is the Tate period of E/K. The ring homomorphism

$$\begin{aligned} \varphi_{q_E} \colon \mathbb{Z}((q)) &\longrightarrow K \\ q &\longmapsto q_E \end{aligned}$$

induces an isomorphism $E_q \otimes_{\mathbb{Z}((q)),\varphi_{q_E}} K \cong E$ (i.e., allows us to view E in terms of the Tate curve E_q). In particular, $E(\overline{K}) \cong \overline{K}^\times/q_E^{\mathbb{Z}}$. If E has split multiplicative reduction, such isomorphism is even defined over K.

Theorem 55. *In the situation above, consider a prime number ℓ. If $j(E) \notin \mathscr{O}_K$, the representation*

$$\mathrm{Gal}(\overline{K}/K) \hookrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}(\mathrm{T}_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$$

is not abelian.

Proof. We may assume, up to replacing K with a quadratic extension, that the isomorphism $E(\overline{K}) \cong \overline{K}^\times/q_E^{\mathbb{Z}}$ is compatible with the action of $\mathrm{Gal}(\overline{K}/K)$. Then

$$E[\ell^n](\overline{K}) = \left(\overline{K}^\times/q_E^{\mathbb{Z}}\right)[\ell^n] = \{\, \zeta_{\ell^n}^a q_E^{b/\ell^n} : a, b \in \mathbb{Z}/\ell^n\mathbb{Z} \,\}.$$

Therefore, the field generated by the ℓ^n–torsion points of E is $K(\zeta_{\ell^n}, q_E^{1/\ell^n})$, which is not abelian over K if $n \gg 0$ (e.g., using Kummer theory). □

Corollary 56. *Let K be a quadratic imaginary field and let H be its Hilbert class field. If E is an elliptic curve with CM by $\mathscr{O}_K$, then $j(E) \in \mathscr{O}_H$.*

Proof. Suppose that there exists a prime ideal $\mathfrak{p}$ of $\mathscr{O}_H$ at which $j(E)$ is not integral. We can take the base change of E from H to $H_\mathfrak{p}$ and apply the previous theorem to conclude that the image of the decomposition group at $\mathfrak{p}$ under the representation $\mathrm{Gal}(\overline{H}/H) \to \mathrm{T}_\ell(E)(\overline{H})$ is not abelian, thus contradicting corollary 52. □

3.8 The class number 1 problem (revisited)

Theorem 57. *Let $D \in \mathbb{Z}_{<0}$ be a fundamental discriminant and let $K = \mathbb{Q}(\sqrt{D})$. If the class number of K is $h = 1$, then*

$$j\left(\frac{D + \sqrt{D}}{2}\right) \in \mathbb{Z}$$

and, in fact, this value is a perfect cube.

Proof. Let E be the elliptic curve over $\mathbb{C}$ corresponding to the point

$$\tau = \frac{D+\sqrt{D}}{2} \in \mathfrak{H}.$$

One checks that $q = e^{2\pi i\tau} \in \mathbb{R}$ and so $j(q) \in \mathbb{R}$. Therefore, $j(E) \in \mathcal{O}_K \cap \mathbb{R} = \mathbb{Z}$. The fact that this value is a perfect cube can be proved using the theory of modular curves of higher levels. □

Definition 58. Let E be an elliptic curve over a field L and let $N \in \mathbb{Z}_{\geq 1}$. A *full level N structure on E* is a basis (P_1, P_2) of $E[N](L)$ as a $(\mathbb{Z}/N\mathbb{Z})$–module.

Remark. Using the Weil pairing $\langle\, \cdot\, , \,\cdot\, \rangle$ of E, the level structure (P_1, P_2) provides a primitive N–th root of unity $\langle P_1, P_2 \rangle$ in L.

Fix a primitive N–th root of unity $\zeta_N \in \overline{\mathbb{Q}}$. Consider the functor

$$\Gamma(N)\colon \mathbb{Q}(\zeta_N)\text{–Alg} \to \text{Set}$$

that sends a $\mathbb{Q}(\zeta_N)$–algebra L to the set of $\overline{L}$–isomorphism classes (E, P_1, P_2), where E/L is an elliptic curve with full level N structure (P_1, P_2) such that $\langle P_1, P_2 \rangle = \zeta_N$.

Proposition 59. *If $N > 2$, the functor $\Gamma(N)$ from the previous paragraph is represented by a smooth affine curve $Y(N)$ over $\mathbb{Q}(\zeta_N)$ that is geometrically connected.*

We will prove that we can express $\operatorname{Spec}(\mathbb{Q}[j^{1/3}])$ as a quotient of $Y(3)$ and that will allow us to conclude the proof of theorem 57.

3.9 Modular curves

Let $N \in \mathbb{Z}_{\geq 1}$ and fix a primitive N–th root ζ_N of 1. The modular curve $Y(N)$ (of full level N) is an affine curve over $\mathbb{Q}(\zeta_N)$ whose L–rational points, for an extension $L/\mathbb{Q}(\zeta_N)$, correspond to the $\overline{L}$–isomorphism classes of triples (E, P_1, P_2), where E is an elliptic curve over L and P_1, P_2 form a basis of $E[N](L)$ and satisfy that $\langle P_1, P_2 \rangle = \zeta_N$.

Proposition 60. *If $N \geq 3$, the map*

$$(E, P_1, P_2) \mapsto E$$

defines a Galois covering $Y(N) \to Y(1)$ with Galois group $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$*.*

Proof. An automorphism of $Y(N)$ over $Y(1)$ must be of the form

$$(E, P_1, P_2) \mapsto (E, aP_1 + bP_2, cP_1 + dP_2)$$

for some

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

because

$$\langle aP_1 + bP_2, cP_1 + dP_2 \rangle = \langle P_1, P_2 \rangle^{ad-bc} = \zeta_N.$$

In fact, since $(E, P_1, P_2) \cong (E, -P_1, -P_2)$ via the automorphism $[-1]$, we obtain an isomorphism $\mathrm{Aut}(Y(N)/Y(1)) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\} = \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$. □

From now on, assume for simplicity that N is prime. We will see that the base change $Y(N)_{\overline{\mathbb{Q}}} \to Y(1)_{\overline{\mathbb{Q}}}$ has the same Galois group.

The maximal subgroups of $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ are:

- the exceptional subgroups A_4, S_4 and A_5,
- the Borel subgroup of upper triangular matrices and
- the normalizer H of a Cartan subgroup C, which satisfies that $[H : C] = 2$ and can be
  - either the normalizer

    $$H = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \right\}$$

    of the split Cartan subgroup

    $$C = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\},$$

  - or the normalizer H of the non-split Cartan subgroup $C = \mathbb{F}_{N^2}^\times$ inside $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Now we have to produce elliptic curves $E/\overline{\mathbb{Q}}$ with automorphisms of $E[N](\overline{\mathbb{Q}})$ not contained in any of the proper subgroups of $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$.

Let E be a Tate elliptic curve defined over a number field L, with $j(E) \notin \mathscr{O}_{L_\mathfrak{P}}$ for some prime $\mathfrak{P}$ of $\mathscr{O}_L$. If $N \nmid -\mathrm{ord}_\mathfrak{P}(j(E)) = \mathrm{ord}_\mathfrak{P}(q_E)$, then the image of the representation

$$\rho_{E,N} \colon \mathrm{Gal}(\overline{L}/L) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

given by $E[N](\overline{L})$ contains an element of order N, namely

$$\begin{cases} \zeta_N \mapsto \zeta_N, \\ q_E^{1/N} \mapsto \zeta_N q_E^{1/N}. \end{cases}$$

Therefore, (at least for $N > 5$) $\mathrm{Gal}(Y(N)/Y(1))$ cannot be contained in an exceptional group or in the normalizer of a Cartan subgroup because the orders of those groups are not divisible by N.

To rule out the Borel, let E be an elliptic curve with CM by $\mathscr{O}_K$ with N inert in K. We may assume that E is defined over the Hilbert class field H of K. By class field theory, $\rho_{E,N}(\mathrm{Gal}(\overline{H}/H))$ is contained in a non-split Cartan subgroup $\mathbb{F}_{N^2}^\times$ (as $E[N](\overline{H})$ is a vector space over $\mathscr{O}_K/N\mathscr{O}_K = \mathbb{F}_{N^2}$) and cannot be contained in the Borel subgroup.

Alternatively, we can work over $\mathbb{C}$. The points of $Y(N)_\mathbb{C}$ correspond to the quotient $\Gamma(N)\backslash\mathfrak{H}$ via

$$\tau \mapsto \Big(\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau), \frac{1}{N}, \frac{\tau}{N}\Big)$$

and then the covering is given by the natural projection $\Gamma(N)\backslash\mathfrak{H} \twoheadrightarrow \Gamma(1)\backslash\mathfrak{H}$.

Given a subgroup H of $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$, we have the quotient $Y_H(N) = Y(N)/H$ attached to H. The element $j(E)$ of $Y(1)$ lifts to an L–rational point on $Y_H(N)$ if and only if the representation $\rho_{E,N}\colon \mathrm{Gal}(\overline{L}/L) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ has image contained in a conjugate of H.

For example, for $N = 3$, the group $\mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z})$ can be identified with A_4 (viewing the elements of the group as permutations on $\mathbb{P}^1(\mathbb{F}_3)$). Consider its 2–Sylow subgroup $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so that $Y_H(3)$ is a cyclic Galois cover of $Y(1)$ with Galois group $\mathbb{Z}/3\mathbb{Z}$.

Proposition 61. *In the situation from the previous paragraph,*

$$Y_H(3) = \mathrm{Spec}\big(\mathbb{Q}(\zeta_3)(j^{1/3})\big).$$

Proof. By Kummer theory, the function field F of $Y_H(3)$ has to be of the form $\mathbb{Q}(\zeta_3)(j)(?^{1/3})$ for some element $? \in \mathbb{Q}(\zeta_3)(j)$. But this extension is ramified precisely at $j = \infty$ and $j = 0$. That is, the polynomial $X^3 - ?$ has zeros or poles only at $j = 0$ and $j = \infty$. Thus, at least over $\mathbb{C}$ we see that $F_\mathbb{C} = \mathbb{C}(j)(j^{1/3})$. A descent argument implies that $F = \mathbb{Q}(\zeta_3)(j^{1/3})$. □

Corollary 62. *Let E/L be an elliptic curve. The value $j(E)$ is a cube in L if and only if $\rho_{E,3}(\mathrm{Gal}(\overline{L}/L))$ contains no element of order* 3.

Proof of theorem 57 (continuation). If $E/\mathbb{C}$ has CM by a maximal order $\mathscr{O}_K$ with class number $h(\mathscr{O}_K) = 1$ and discriminant D, then D must be prime.

- If $3 \mid D$, then $D = -3$ and $j(E) = 0$.
- If $3 \nmid D$, then 3 is either split or inert in K and $\rho_{E,3}(G_\mathbb{Q})$ is contained in the normalizer of a Cartan subgroup, either split or inert. That is,

$$\rho_{E,3}(G_\mathbb{Q}) \subseteq \begin{cases} \{\pm 1\} \ltimes \Big((\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times\Big) & \text{if 3 splits,} \\ \{\pm 1\} \ltimes \mathbb{F}_9^\times & \text{if 3 is inert.} \end{cases}$$

The orders of these groups are not divisible by 3.
Hence $j(E)$ is a cube by corollary 62. □

Remark. The condition that D is a fundamental discriminant is important. For example, for $D = -12$, we have the order

$$\mathscr{O} = \mathscr{O}_D = \mathbb{Z}[\sqrt{-3}] \subsetneq \mathbb{Z}\Big[\frac{1+\sqrt{-3}}{2}\Big]$$

and $j(\sqrt{-3}) = 2^4 3^3 5^3$ fails to be a cube.

Definition 63. We define $Y_{\mathrm{ns}}^+(N)$ to be the modular curve $Y_H(N)$ for the normalizer H of a non-split Cartan subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Theorem 64. *Let D be a fundamental discriminant of class number* 1. *If $D > 4N$, then*

$$j\Big(\frac{D+\sqrt{-D}}{2}\Big)$$

lifts to a rational point on $Y_{\mathrm{ns}}^+(N)/\mathbb{Q}$.

Therefore, one can study the class number 1 problem by classifying the integral points on $X_{\mathrm{ns}}^+(N)$. This has been done

- for $N = 24$ by Heegner and Stark;
- for $N = 7$ and 9 by Kenku;
- for $N = 5$ by I. Chen (after a suggestion of Siegel);
- for $N = 16, 20$ and 21 by Baran;
- for $N = 13$ by Balakrishnan, Dogra, Müller, Tuitman and Vonk.

More generally, for an elliptic curve E with CM by an order $\mathscr{O} = \mathscr{O}_D$, the j–invariant $j(E)$ lifts to $Y_0(\ell) = Y_{\mathrm{Borel}}(\ell)$ if ℓ splits as a product $\lambda\overline{\lambda}$ with $\overline{\lambda} \neq \lambda$ in $K = \mathbb{Q}(\sqrt{D})$: we obtain a point $(E, E[\lambda]) \in Y_0(\ell)(H)$, where H is the Hilbert class field of K. Such points are called Heegner points on $Y_0(\ell)$ and they can be used to obtain rational points on elliptic curves. Moreover, on $Y_0(\ell)$ there are interesting units such as

$$U_N(z) = \frac{\Delta(z)}{\Delta(\ell z)}$$

whose values at Heegner points give units in $\mathcal{O}_H[1/\ell]^\times$.

3.10 Factorizations of singular moduli

Let D_1 and D_2 be two distinct (negative) fundamental discriminants. Define

$$J(D_1, D_2) = \prod_{\substack{\operatorname{disc}(\tau_1)=D_1 \\ \operatorname{disc}(\tau_2)=D_2}} (j(\tau_1) - j(\tau_2)),$$

where the product is over the points $\tau_1, \tau_2 \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ such that $\operatorname{disc}(\tau_1) = D_1$ and $\operatorname{disc}(\tau_2) = D_2$. This quantity is in fact in $\mathbb{Z}$ because of its Galois invariance.

Theorem 65 (Gross–Zagier). *Let ℓ be a prime number. If $\ell \mid J(D_1, D_2)$, then*

(1) $\left(\frac{D_1}{\ell}\right) \neq 1 \neq \left(\frac{D_2}{\ell}\right)$ *and*

(2) *ℓ divides a positive integer of the form*

$$\frac{D_1 D_2 - x^2}{4} \quad \text{with } x \in \mathbb{Z}.$$

Remark. The prime numbers appearing in the second column of table 1 are all $\equiv 0$ or 2 mod 3. We can justify that fact using the first part of the theorem as follows: we can express

$$j(\tau_D) = j(\tau_D) - j\Big(\frac{3+\sqrt{3}}{2}\Big)$$

and this difference can only be divisible by the primes that are either inert or ramified in $\mathbb{Q}(\sqrt{3})$. One can also check that the bound on the prime numbers in terms of the discriminant given by the second part of the theorem is satisfied.

Proof. For $i = 1$ or 2, let $\mathcal{O}_{D_i}$ be the (maximal) order of discriminant D_i and let H_i be the corresponding Hilbert class field. Since $\ell \mid J(D_1, D_2)$, we can pick a prime ideal λ of $\mathcal{O}_{H_1 H_2}$ lying over ℓ and such that $\lambda \mid (j(\tau_1) - j(\tau_2))$ for some τ_1 and τ_2 appearing in the definition of $J(D_1, D_2)$. Let $E_1/\mathcal{O}_{H_1}$ and $E_2/\mathcal{O}_{H_2}$ be the elliptic curves associated with τ_1 and τ_2, respectively. Observe that both E_1 and E_2 have good reduction at λ and let $\overline{E}_i$ denote the reduction of E_i modulo λ.

(1) Suppose, for the sake of contradiction, that

$$\left(\frac{D_1}{\ell}\right) = 1.$$

By theorem 50, E_1 has ordinary reduction at λ and so

$$\mathrm{End}_{\overline{\mathbb{F}}_\ell}(\overline{E}_1) \cong \mathrm{End}_{\overline{\mathbb{Q}}}(E_1) \cong \mathscr{O}_{D_1}.$$

But, as $j(\tau_1) \equiv j(\tau_2) \bmod \lambda$, we deduce that $\overline{E}_1 \cong \overline{E}_2$. Therefore, we obtain an inclusion

$$\mathscr{O}_{D_2} \cong \mathrm{End}_{\overline{\mathbb{Q}}}(E_2) \hookrightarrow \mathrm{End}_{\overline{\mathbb{F}}_\ell}(\overline{E}_2) \cong \mathscr{O}_{D_1},$$

which is impossible because $D_1 \neq D_2$ and both are fundamental discriminants.

In conclusion, both E_1 and E_2 must have supersingular reduction at every prime dividing $J(D_1, D_2)$.

(2) We argue again using how endomorphisms of CM elliptic curves behave under reductions. By the arguments in the previous part, there exist an order R in a quaternion algebra ramified at ℓ and ∞ (isomorphic to $\mathrm{End}_{\overline{\mathbb{F}}_\ell}(\overline{E}_i)$ for $i = 1$ and 2) and inclusions

$$\mathscr{O}_{D_1} \hookrightarrow R \hookleftarrow \mathscr{O}_{D_2}$$

(cf. proposition 49). Now we can find conditions that such an order R must satisfy in order to contain both $\mathscr{O}_{D_1}$ and $\mathscr{O}_{D_2}$. The theorem will follow from the next proposition. □

Proposition 66. *Let R be an order in a quaternion algebra ramified exactly at ℓ and ∞. If R contains both $\mathscr{O}_{D_1}$ and $\mathscr{O}_{D_2}$, then ℓ divides*

$$\frac{D_1 D_2 - x^2}{4} > 0 \quad \textit{for some } x \in \mathbb{Z}.$$

Proof. Let B be the quaternion algebra ramified exactly at ℓ and at ∞. That is,

$$B \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathrm{M}_2(\mathbb{Q}_p) \text{ for every prime } p \neq \ell,$$

$B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}$ and $B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is a division algebra over $\mathbb{Q}_\ell$. We may assume that R is its maximal order. Consider the pairing

$$\langle x, y \rangle = \mathrm{Tr}(x\overline{y}),$$

which satisfies that

(1) $\langle \cdot , \cdot \rangle$ is bilinear and positive definite and

(2) if e_1, e_2, e_3, e_4 is a $\mathbb{Z}$–basis of R, then

$$\det(R) = \det\big(\langle e_i, e_j\rangle\big) = \ell^2.$$

Let $\varphi_i \colon \mathscr{O}_{D_i} \hookrightarrow R$ denote the given inclusions and write $\delta_1 = \varphi_1(\sqrt{D_1})$ and $\delta_2 = \varphi_2(\sqrt{D_2})$. Consider the lattice $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\delta_1 \oplus \mathbb{Z}\delta_2 \oplus \mathbb{Z}\delta_1\delta_2$ inside R. We have $\det(\Lambda) = [R : \Lambda]^2 \det(R)$. The pairing $\langle \cdot\,, \cdot \rangle$ on Λ is determined by the pairing matrix

$$\begin{aligned} M &= \begin{pmatrix} \langle 1,1\rangle & \langle 1,\delta_1\rangle & \langle 1,\delta_2\rangle & \langle 1,\delta_1\delta_2\rangle \\ \langle \delta_1,1\rangle & \langle \delta_1,\delta_1\rangle & \langle \delta_1,\delta_2\rangle & \langle \delta_1,\delta_1\delta_2\rangle \\ \langle \delta_2,1\rangle & \langle \delta_2,\delta_1\rangle & \langle \delta_2,\delta_2\rangle & \langle \delta_2,\delta_1\delta_2\rangle \\ \langle \delta_1\delta_2,1\rangle & \langle \delta_1\delta_2,\delta_1\rangle & \langle \delta_1\delta_2,\delta_2\rangle & \langle \delta_1\delta_2,\delta_1\delta_2\rangle \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 & 0 & x \\ 0 & -2D_1 & -x & 0 \\ 0 & -x & -2D_2 & 0 \\ x & 0 & 0 & 2D_1D_2 \end{pmatrix}, \end{aligned}$$

where we defined $x = \operatorname{Tr}(\delta_1\delta_2)$. Hence,

$$\det(\Lambda) = \det(M) = (4D_1D_2 - x^2)^2.$$

On the other hand, to obtain the determinant of $\widetilde{\Lambda} = \varphi_1(\mathscr{O}_{D_1})\varphi_2(\mathscr{O}_{D_2})$ we observe that $\widetilde{\Lambda}$ is generated in the same way as Λ but replacing D_i with $(1 + D_i)/2$. In particular, $[\Lambda : \widetilde{\Lambda}] = 16$ and so

$$\det(\widetilde{\Lambda}) = \left(\frac{D_1D_2 - x^2}{4}\right)^2$$

All in all,

$$\ell^2 = \det(R) \mid \det(\widetilde{\Lambda}) = \left(\frac{D_1D_2 - x^2}{4}\right)^2.$$

The fact that $D_1D_2 - x^2$ is positive follows from Cauchy–Schwartz's inequality:

$$\langle \delta_1, \delta_2\rangle^2 \leq \langle \delta_1, \delta_1\rangle\langle \delta_2, \delta_2\rangle. \qquad \square$$

4 Complex multiplication on Shimura curves

The course will now shift to more analytic aspects of the theory. Next, we are going to study p–adic variants of singular moduli based on CM points on Shimura curves.

4.1 Quaternion algebras

Definition 67. A *quaternion algebra* over a field k is a central simple algebra of dimension 4 over k.

Example 68. The algebra of matrices $\mathrm{M}_2(k)$ is a quaternion algebra. In fact, for every quaternion algebra B over k, $B \otimes_k \overline{k} \cong \mathrm{M}_2(\overline{k})$ (as algebras over the algebraic closure $\overline{k}$).

Example 69. Over $\mathbb{Q}$, we have Hamilton's quaternions $\mathbb{H} = \mathbb{Q}(i, j, k)$, where $i^2 = j^2 = k^2 = -1$ and $ij = k = -ji$, $jk = i = -kj$ and $ki = j = -ik$.

Let B be a quaternion algebra over k and take $\alpha \in B \setminus k$. Then $K = k(\alpha)$ is a quadratic algebra over k. If K is a quadratic field extension of k, we can regard B as a right K–module with a left action of B itself and in this way we obtain an embedding of B in $\mathrm{M}_2(K)$. Moreover, we can pick $j \in B$ such that $B = K \oplus Kj$ (eigenspace decomposition for the B–action) with $\delta = j^2 \in k$ and $j\alpha = \overline{\alpha}j$. We sometimes write $B = (K, \delta)$, as this quaternion algebra is determined by K and the image of δ in $k^\times / \mathrm{N}_{K/k}(K^\times)$.

4.1.1 Classification over $\mathbb{Q}$

To classify quaternion algebras over $\mathbb{Q}$, we first look at the local situation.

(1) Over $\mathbb{R}$, there are only two (isomorphism classes of) quaternion algebras: $\mathrm{M}_2(\mathbb{R})$ and $\mathbb{H} = (\mathbb{C}, -1)$.

(2) Similarly, for a prime number ℓ, there are two (isomorphism classes of) quaternion algebras over $\mathbb{Q}_\ell$: $\mathrm{M}_2(\mathbb{Q}_\ell)$ and a division algebra D over $\mathbb{Q}_\ell$.

Definition 70. We say that a quaternion algebra B over $\mathbb{Q}$ is *split* at a place v if $B \otimes_{\mathbb{Q}} \mathbb{Q}_v \cong \mathrm{M}_2(\mathbb{Q}_v)$; otherwise, we say that B is *ramified* at v.

Theorem 71. *Let B be a quaternion algebra over $\mathbb{Q}$ and let $\mathrm{Ram}(B)$ be the set of places of $\mathbb{Q}$ at which B becomes a division algebra (after base change). The set $\mathrm{Ram}(B)$ is finite with even cardinality and determines B up to isomorphism. Conversely, for every finite set S of places of $\mathbb{Q}$ with even cardinality, there exists a quaternion algebra B_S over $\mathbb{Q}$ such that $\mathrm{Ram}(B_S) = S$.*

Example 72. Let $S = \{\infty, p\}$. Then we can construct $B_S = \mathrm{End}_{\mathbb{F}_p}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ for a supersingular elliptic curve E over the finite field $\mathbb{F}_{p^2}$.

Remark. The Brauer group of a field k classifies the central simple algebras over k and the 2–torsion corresponds to (isomorphism classes of) quaternion algebras. Theorem 71 can be reinterpreted as the short exact sequence

$$0 \longrightarrow \mathrm{Br}(\mathbb{Q})_2 \longrightarrow \bigoplus_v \mathrm{Br}(\mathbb{Q}_v)_2 \xrightarrow{\Sigma} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

Definition 73. A quaternion algebra B over $\mathbb{Q}$ is called *definite* if $\infty \in \mathrm{Ram}(B)$; otherwise, B is called *indefinite*.

Definition 74. An *order* in a quaternion algebra B over $\mathbb{Q}$ is a subring R of B which is a free $\mathbb{Z}$–module of rank 4.

Example 75.

(1) The ring $\mathrm{M}_2(\mathbb{Z})$ (or a conjugate of it) is an order in $\mathrm{M}_2(\mathbb{Q})$. Similarly, given $N \in \mathbb{Z}_{\geq 1}$,

$$M_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, d \in \mathbb{Z} \text{ and } c \in N\mathbb{Z} \right\}$$

is an order in $\mathrm{M}_2(\mathbb{Q})$.

(2) In the hamiltonian quaternion algebra $B = \mathbb{Q}(i, j, k)$, we have orders such as $\mathbb{Z}[i, j, k]$ and $\mathbb{Z}[i, j, k, (1 + i + j + k)/2]$ (maximal).

More generally, we are going to use $\mathbb{Z}[N^{-1}]$–orders for $N \in \mathbb{Z}_{\geq 1}$ (i.e., subrings that are free $\mathbb{Z}[N^{-1}]$–modules of rank 4).

Lemma 76. *Let R be an order in a quaternion algebra B over $\mathbb{Q}$. If B is definite, then $R^\times$ is finite.*

Proof. The group $R^\times$ is a discrete subgroup of $(B \otimes_{\mathbb{Q}} \mathbb{R})_1^\times$, which is a compact group. Therefore, $R^\times$ must be finite. □

Remark. If B is indefinite, we can just say that $R^\times$ is a discrete subgroup of $\mathrm{GL}_2(\mathbb{R})$, but not finite in general.

4.2 Shimura curves

Let S be a finite set of places of $\mathbb{Q}$. Suppose that S has an odd number of elements and that $\infty \in S$. There is no quaternion algebra ramified exactly at S. However, we can pick $v \in S$ and get a quaternion algebra $B_{S\setminus\{v\}}$. Let $R_{S,v}$ be a maximal $\mathbb{Z}\left[\frac{1}{v}\right]$–order in $B_{S\setminus\{v\}}$ if v is finite or a maximal $\mathbb{Z}$–order in $B_{S\setminus\{\infty\}}$ if $v = \infty$. Define

$$\Gamma_{S,v} = \left(R_{S,v}^{\times}\right)_1 = \{\, \alpha \in R_{S,v}^{\times} : \alpha\overline{\alpha} = 1 \,\}.$$

We can fix an isomorphism $\iota_v \colon B_{S\setminus\{v\}} \otimes_{\mathbb{Q}} \mathbb{Q}_v \to \mathrm{M}_2(\mathbb{Q}_v)$ that allows us to regard $\Gamma_{S,v} \subseteq \mathrm{SL}_2(\mathbb{Q}_v)$. In particular, $\Gamma_{S,\infty} \subseteq \mathrm{SL}_2(\mathbb{R})$ acts discretely on the upper half-plane $\mathfrak{H}$ by Möbius transformations. Analogously, for every $p \in S \setminus \{\,\infty\,\}$, $\Gamma_{S,p}$ acts discretely on $\mathfrak{H}_p = \mathbb{P}^1(\mathbb{C}_p) \setminus \mathbb{P}^1(\mathbb{Q}_p)$ and it turns out that $\Gamma_{S,p}\backslash\mathfrak{H}_p$ is a rigid analytic curve.

Theorem 77 (Cerednik–Drinfeld). *Let S be a finite set of places of $\mathbb{Q}$ of odd cardinality and containing ∞. There is a curve X_S over $\mathbb{Q}$ satisfying that*

(1) $X_S(\mathbb{C}) \cong \Gamma_{S,\infty}\backslash\mathfrak{H}$ *and*

(2) $X_S(\mathbb{C}_p) \cong \Gamma_{S,p}\backslash\mathfrak{H}_p$ *for every* $p \in S \setminus \{\,\infty\,\}$.

Remark. If $S = \{\,\infty\,\}$, then $\Gamma_{S,\infty} = \mathrm{SL}_2(\mathbb{Z})$ and so we obtain a generalization of the modular curve (of level 1).

4.3 Uniformization of Shimura curves

Keep the notation from section 4.2. We want to make some comments on the idea of the proof of theorem 77.

Observe that there is an equivalence between elliptic curves E over $\mathbb{Q}$ and abelian surfaces A endowed with a morphism $\iota\colon\ \mathrm{M}_2(\mathbb{Z}) \to \mathrm{End}(A)$ given by

$$E \mapsto E \times E \quad \text{and} \quad A \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} A.$$

We can use this equivalence to generalize the moduli interpretation of modular curves as follows: given a field L, we define $X_S(L)$ to be the set of isomorphism classes of abelian surfaces A/L endowed with a morphism $\iota\colon R_{S,\infty} \to \mathrm{End}(A)$.

We would like to understand X_S over $\mathbb{Q}_p$ when $p \in S \setminus \{\,\infty\,\}$.

Fact 78. *If A is an abelian surface over $\overline{\mathbb{F}}_p$ with quaternionic multiplication by $R_{S,\infty}$, then A is isomorphic to a product $E \times E$, where E is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. Moreover, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{R_{S,\infty}(A)}$ is contained in the centralizer of $B_{S\setminus\{\infty\}}$ in $\mathrm{M}_2(B_{p\infty})$.*

4.4 The p–adic upper half-plane

Consider the p–adic upper half-plane $\mathcal{H}_p = \mathfrak{H}_p = \mathbb{P}^1(\mathbb{C}_p) \setminus \mathbb{P}^1(\mathbb{Q}_p)$. More generally, we may view it as a functor that sends a complete field extension L of $\mathbb{Q}_p$ to $\mathcal{H}_p(L) = \mathbb{P}^1(L) \setminus \mathbb{P}^1(\mathbb{Q}_p)$. (Most of the time, it will suffice to work with $L = \widehat{\mathbb{Q}}_p^{\mathrm{ur}}$, the completion of the maximal unramified extension of $\mathbb{Q}_p$.) It turns out that $\mathcal{H}_p$ is represented by a rigid analytic space endowed with an action of $\mathrm{SL}_2(\mathbb{Q}_p)$. Let us try to understand its affinoids.

4.4.1 Some basic subspaces

Observe that we can write points as follows:

$$\mathbb{P}^1(\mathbb{C}_p) = \mathbb{P}^1(\mathscr{O}_{\mathbb{C}_p}) = \{\, z = [z_1, z_2] : z_1, z_2 \in \mathscr{O}_{\mathbb{C}_p} \text{ and } (z_1, z_2) = 1 \,\}.$$

Thus, we can consider the reduction modulo p

$$\mathrm{red}\colon \mathbb{P}^1(\mathbb{C}_p) \to \mathbb{P}^1(\overline{\mathbb{F}}_p).$$

The region

$$\mathcal{A}^* = \mathrm{red}^{-1}\big(\mathbb{P}^1(\overline{\mathbb{F}}_p) \setminus \mathbb{P}^1(\mathbb{F}_p)\big)$$

is called *the standard affinoid of* $\mathfrak{H}_p$. We get an induced action of $\mathrm{SL}_2(\mathbb{Z}_p)$ on $\mathcal{A}^*$ and we find other affinoids as the translates of $\mathcal{A}^*$ by elements of $\mathrm{SL}_2(\mathbb{Q}_p)$. However, that will not be enough to see all affinoids.

We will need to use the following annuli. For $t \in \{\, 0, 1, \dots, p-1 \,\}$, set

$$\mathcal{W}_t = \{\, z \in \mathbb{C}_p : p^{-1} < |z - t|_p < 1 \,\}.$$

Similarly, define

$$\mathcal{W}_\infty = \{\, z \in \mathbb{C}_p : 1 < |z|_p < p \,\}.$$

Then we obtain a wide open subspace $\mathcal{W}^* = \mathcal{A}^* \cup \mathcal{W}_0 \cup \cdots \cup \mathcal{W}_{p-1} \cup \mathcal{W}_\infty$.

4.4.2 The action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on $\mathcal{A}^*$ and $\mathcal{W}^*$

This action has the following properties:

(1) $\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Q}_p)}(\mathcal{A}^*) = \mathrm{PGL}_2(\mathbb{Z}_p)$;

(2) $\mathrm{PGL}_2(\mathbb{Z}_p)$ permutes the annuli $(\mathcal{W}_t)_{t \in \mathbb{P}^1(\mathbb{F}_p)}$ by acting in the obvious way on the subindices, and

(3) we obtain a covering
$$\mathcal{H}_p = \bigcup_{\gamma \in \mathrm{GL}_2(\mathbb{Q}_p)} \gamma \mathcal{W}^*.$$

4.4.3 The Bruhat–Tits tree

Definition 79. The *Bruhat–Tits tree $\mathcal{T}$ of* $\mathrm{PGL}_2(\mathbb{Q}_p)$ is the graph whose vertices are in bijection with similarity classes of $\mathbb{Z}_p$–lattices in $\mathbb{Q}_p^2$ and whose edges join (vertices corresponding to) lattices Λ_1 and Λ_2 such that

$$p\Lambda_2 \subsetneq \Lambda_1 \subsetneq \Lambda_2.$$

Write $\mathcal{T}_0$ for the set of vertices of $\mathcal{T}$ and $\mathcal{T}_1$ for the set of (unoriented) edges of $\mathcal{T}$.

Let us describe $\mathcal{T}$ locally. Consider the standard vertex $v^* = [\mathbb{Z}_p^2]$. The edges containing v^* can be labelled as $e_0, \dots, e_{p-1}, e_\infty$ and one can define an action of the group $\mathrm{PGL}_2(\mathbb{Q}_p)$ acts on $\mathcal{T}$ with the following properties:

(1) $\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Q}_p)}(v^*) = \mathrm{PGL}_2(\mathbb{Z}_p)$;

(2) $\mathrm{PGL}_2(\mathbb{Z}_p)$ permutes $(e_t)_{t \in \mathbb{P}^1(\mathbb{F}_p)}$ by acting on the subindices in the obvious way, and

(3) $\mathcal{T}_0 = \{\, \gamma v^* : \gamma \in \mathrm{PGL}_2(\mathbb{Q}_p) \,\}$ and $\mathcal{T}_1 = \{\, \gamma e_t : \gamma \in \mathrm{PGL}_2(\mathbb{Q}_p), t \in \mathbb{P}^1(\mathbb{F}_p) \,\}$.

Proposition 80. *There is a unique map*

$$r \colon \mathcal{H}_p \to \mathcal{T},$$

called the reduction map, *with the following properties: for every $z \in \mathcal{H}_p$,*

(1) *$r(z) = v^*$ if and only if $z \in \mathcal{A}^*$;*

(2) *$r(z) = e_j$ if and only if $z \in \mathcal{W}_j$ (here, $j \in \mathbb{P}^1(\mathbb{F}_p)$), and*

(3) *$r(\gamma z) = \gamma r(z)$ for all $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$.*

Definition 81. A subgraph Σ of $\mathcal{T}$ is called *closed* if, for every edge (v_1, v_2) in Σ, the vertices v_1 and v_2 are also in Σ.

Definition 82. An *affinoid subset* of $\mathcal{H}_p$ is a subset of the form $r^{-1}(\Sigma)$ for some finite closed subgraph Σ of $\mathcal{T}$.

Remark. These affinoids are actually the ones that one gets on the upper half-plane over $\widehat{\mathbb{Q}}_p^{\mathrm{ur}}$ (there are more if one adds ramification).

4.4.4 Rigid analytic and meromorphic functions

Definition 83. A function $f\colon \mathcal{H}_p \to \mathbb{C}_p$ is *rigid analytic* if, for every affinoid $\mathcal{A}$ of $\mathcal{H}_p$, the restriction $f|_{\mathcal{A}}$ is a uniform limit of rational functions with poles only in $\mathbb{P}^1(\mathbb{C}_p) \setminus \mathcal{A}$.

Definition 84. The *distance* between two points $x = [x_1, x_2]$ and $y = [y_1, y_2]$ of $\mathbb{P}^1(\mathbb{C}_p)$ is

$$d(x,y) = \left| \det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} \right|_p .$$

Remark. The action of $\mathrm{GL}_2(\mathbb{Z}_p)$ preserves distances.

For $z \in \mathcal{H}_p$, we have

$$d(z, \mathbb{P}^1(\mathbb{Q}_p)) = \min\{\, d(z,t) : t \in \mathbb{P}^1(\mathbb{Q}_p) \,\} > 0.$$

We define for each $N \in \mathbb{Z}_{\geq 1}$ the affinoid

$$\mathcal{H}_p^{\leq N} = \{\, z \in \mathcal{H}_p : d(z, \mathbb{P}^1(\mathbb{Q}_p)) \geq p^{-N} \,\}.$$

This corresponds to the part of $\mathcal{T}$ that is at distance $\leq N$ (edges) from v^*. It is easy to see that

$$\mathcal{H}_p = \bigcup_{N \geq 1} \mathcal{H}_p^{\leq N}.$$

Each $\mathcal{H}_p^{\leq N}$ is obtained by removing $(p+1)p^{N-1}$ residue discs of radius p^{-N} centred at the points of $\mathbb{P}^1(\mathbb{Z}/p^N\mathbb{Z})$.

Since the affinoids $\mathcal{H}_p^{\leq N}$ for $N \in \mathbb{Z}_{\geq 1}$ form an admissible covering of $\mathcal{H}_p$, we can rephrase the definition of rigid analytic functions on $\mathcal{H}_p$ using only these affinoids (cf. definition 83).

Definition 85. A *rigid meromorphic function* on $\mathcal{H}_p$ is a quotient of rigid analytic functions on $\mathcal{H}_p$.

Our main goal now is to produce Γ–invariant rigid analytic (or meromorphic) functions, where $\Gamma = \Gamma_{S,p} = (R_{S,p}^\times)_1$ as in section 4.2. To simplify the notation, we also write $R = R_{S,p}$ and $B = B_{S \setminus \{p\}}$ (recall that R is the maximal $\mathbb{Z}[p^{-1}]$–order in B). Keep that notation for the following sections.

4.4.5 The action of Γ on $\mathcal{H}_p$

Let v be a vertex of $\mathcal{T}$. The "vertex stabilizer"

$$R_v = \{\, x \in R : xv = v \,\} \cup \{\, 0 \,\}$$

is a maximal $\mathbb{Z}$–order in R, as it is formed of those elements that preserve a lattice. But recall that $B_{S\setminus\{p\}}$ is a definite quaternion algebra (i.e., $B_{S\setminus\{p\}} \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}$). A consequence of this will be:

Lemma 86. *Let $v \in \mathcal{T}_0$. The stabilizer* $\mathrm{Stab}_\Gamma(v)$ *is a finite set.*

Proof. It is easy to see that $\mathrm{Stab}_\Gamma(v) = (R_v^\times)_1$. But R_v is a maximal $\mathbb{Z}$–order in the quaternion algebra B and so lemma 76 implies the result. □

Lemma 87. *Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be two affinoids in $\mathcal{H}_p$. The set*

$$\{\, \gamma \in \Gamma : \gamma\mathcal{A}_1 \cap \mathcal{A}_2 \neq \emptyset \,\}$$

is finite.

Proof. Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be the two finite subgraphs of $\mathcal{T}$ corresponding to $\mathcal{A}_1$ and $\mathcal{A}_2$ (i.e., $r(\mathcal{A}_i) = \mathcal{G}_i$ for $i = 1$ or 2). We can express

$$\begin{aligned}\{\, \gamma \in \Gamma : \gamma\mathcal{A}_1 \cap \mathcal{A}_2 \neq \emptyset \,\} &= \{\, \gamma \in \Gamma : \gamma\mathcal{G}_1 \cap \mathcal{G}_2 \neq \emptyset \,\} \\ &= \bigcup_{\substack{v_1 \in \mathcal{G}_1 \cap \mathcal{T}_0 \\ v_2 \in \mathcal{G}_2 \cap \mathcal{T}_0}} \{\, \gamma \in \Gamma : \gamma v_1 = v_2 \,\}.\end{aligned}$$

But each of the latter sets (for v_1 and v_2) is finite. The result follows from this because $\mathcal{G}_1 \times \mathcal{G}_2$ is also finite. □

4.4.6 The Weil symbol

Given $\mathcal{D} \in \mathrm{Div}^0(\mathbb{P}^1(\mathbb{C}_p))$, we can take a rational function $f_{\mathcal{D}}$ satisfying that $\mathrm{div}(f_{\mathcal{D}}) = \mathcal{D}$; this $f_{\mathcal{D}}$ is unique up to multiplication by constants.

Definition 88. The *Weil symbol* attached to two divisors $\mathcal{D}_1, \mathcal{D}_2 \in \mathrm{Div}^0(\mathbb{P}^1(\mathbb{C}_p))$ with disjoint supports is

$$[\mathcal{D}_1; \mathcal{D}_2] = f_{\mathcal{D}_1}(\mathcal{D}_2),$$

where functions on $\mathbb{P}^1(\mathbb{C}_p)$ are extended to $\mathrm{Div}^0(\mathbb{P}^1(\mathbb{C}_p))$ by multiplicativity.

Proposition 89. *The Weil symbol satisfies the following properties:*

(1) *It is bilinear: for every $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3 \in \mathrm{Div}^0(\mathbb{P}^1(\mathbb{C}_p))$,*

$$[\mathcal{D}_1 + \mathcal{D}_2; \mathcal{D}_3] = [\mathcal{D}_1; \mathcal{D}_3] \cdot [\mathcal{D}_2; \mathcal{D}_3]$$

and

$$[\mathcal{D}_1; \mathcal{D}_2 + \mathcal{D}_3] = [\mathcal{D}_1; \mathcal{D}_2] \cdot [\mathcal{D}_1; \mathcal{D}_3].$$

(2) *It is symmetric: for every $\mathcal{D}_1, \mathcal{D}_2 \in \mathrm{Div}^0(\mathbb{P}^1(\mathbb{C}_p))$,*

$$[\mathcal{D}_1; \mathcal{D}_2] = [\mathcal{D}_2; \mathcal{D}_1] \quad \textit{(Weil reciprocity).}$$

(3) *It is $\mathrm{SL}_2(\mathbb{Q}_p)$–equivariant: for every $\mathcal{D}_1, \mathcal{D}_2 \in \mathrm{Div}^0(\mathbb{P}^1(\mathbb{C}_p))$ and $\gamma \in \mathrm{SL}_2(\mathbb{Q}_p)$,*

$$[\gamma\mathcal{D}_1; \gamma\mathcal{D}_2] = [\mathcal{D}_1; \mathcal{D}_2].$$

(4) *For (distinct) points $x_1, x_2, y_1, y_2 \in \mathbb{P}^1(\mathbb{C}_p)$,*

$$[(x_1) - (x_2); (y_1) - (y_2)] = \frac{(x_1 - y_1)(x_2 - y_2)}{(x_1 - y_2)(x_2 - y_1)} \quad \textit{(cross-ratio).}$$

Lemma 90. *Let $\mathcal{D}_1, \mathcal{D}_2 \in \mathrm{Div}^0(\mathbb{P}^1(\mathbb{C}_p))$ and let $N \in \mathbb{Z}_{\geq 1}$. If there is $t \in \mathbb{P}^1(\mathbb{Q}_p)$ such that $d(x,t) \leq p^{-2N}$ for all $x \in \mathrm{Supp}(\mathcal{D}_1)$ and $d(y,t) \geq p^{-N}$ for all $y \in \mathrm{Supp}(\mathcal{D}_2)$, then*

$$\big|[\mathcal{D}_1; \mathcal{D}_2] - 1\big|_p \leq p^{-N}.$$

Proof. Since $\mathrm{SL}_2(\mathbb{Z}_p)$ acts transitively on $\mathbb{P}^1(\mathbb{Q}_p)$ and preserves distances, we may assume that $t = 0$. Moreover, by bilinearity, we may assume that $\mathcal{D}_1 = (x_1) - (x_2)$ and $\mathcal{D}_2 = (y_1) - (y_2)$. In this simplified situation,

$$[\mathcal{D}_1; \mathcal{D}_2] = \frac{(x_1 - y_1)(x_2 - y_2)}{(x_1 - y_2)(x_2 - y_1)} \equiv 1 \mod p^N$$

by the conditions on the valuations of the x_i and the y_i. □

Corollary 91. *Let $\mathcal{D}_1, \mathcal{D}_2 \in \mathrm{Div}^0(\mathcal{H}_p)$. The infinite product*

$$[\mathcal{D}_1; \mathcal{D}_2]_\Gamma = \prod_{\gamma \in \Gamma} [\mathcal{D}_1; \gamma\mathcal{D}_2]$$

converges absolutely.

Proof. Choose $N \in \mathbb{Z}_{\geq 1}$ large enough so that $\mathrm{Supp}(\mathcal{D}_1)$ and $\mathrm{Supp}(\mathcal{D}_2)$ are both in

$\mathcal{H}_p^{\leq N}$. By lemma 87,

$$\gamma\mathcal{H}_p^{\leq N} \cap \mathcal{H}_p^{\leq 2N} = \emptyset \quad \text{for all but finitely many } \gamma \in \Gamma.$$

For such γ, the connected space $\gamma\mathcal{H}_p^{\leq N}$ must be contained in one of the residue discs of radius p^{-2N} excluded in $\mathcal{H}_p^{\leq 2N}$, which implies that there is $t_\gamma \in \mathbb{P}^1(\mathbb{Q}_p)$ (a "centre" of such disc) with the property that

$$d(\gamma z, t_\gamma) \leq p^{-2N} \quad \text{and} \quad d(z, t_\gamma) \geq p^{-N}$$

for all $z \in \mathcal{H}_p^{\leq N}$. In particular,

$$d(z, t_\gamma) \geq p^{-N} \quad \text{for all } z \in \operatorname{Supp}(\mathcal{D}_1)$$

and

$$d(z, t_\gamma) \leq p^{-2N} \quad \text{for all } z \in \operatorname{Supp}(\gamma\mathcal{D}_2).$$

Therefore, we can apply lemma 90 to $\mathcal{D}_1$ and $\gamma\mathcal{D}_2$ using t_γ and deduce that

$$[\mathcal{D}_1; \gamma\mathcal{D}_2] \equiv 1 \mod p^N \mathscr{O}_{\mathbb{C}_p}.$$

Since these congruences hold for all but finitely many $\gamma \in \Gamma$, the product becomes finite modulo p^N. All in all, $[\mathcal{D}_1; \mathcal{D}_2]_\Gamma$ converges absolutely in the p–adic topology. □

Definition 92. Consider $\mathcal{D}_1, \mathcal{D}_2 \in \operatorname{Div}^0(\mathcal{H}_p)$ that have supports with disjoint Γ–orbits. The Γ–*Weil symbol attached to* $\mathcal{D}_1$ *and* $\mathcal{D}_2$ is the value $[\mathcal{D}_1; \mathcal{D}_2]_\Gamma$ defined in corollary 91.

4.4.7 The p–adic period pairing

Given $\gamma_1, \gamma_2 \in \Gamma$, we define

$$\langle \gamma_1, \gamma_2 \rangle = [(\gamma_1 z_1) - (z_1); (\gamma_2 z_2) - (z_2)]_\Gamma,$$

where the "base points" $z_1, z_2 \in \mathcal{H}_p$ are chosen arbitrarily.

Proposition 93. *Let* $\gamma_1, \gamma_2 \in \Gamma$. *The value* $\langle \gamma_1, \gamma_2 \rangle$ *is independent of the choice of* z_1 *and* z_2.

Proof. Take two points $z, z' \in \mathcal{H}_p$ and let $\mathcal{D} \in \mathrm{Div}^0(\mathcal{H}_p)$ and $\gamma \in \Gamma$. By the bilinearity and the Γ–invariance of the Γ–Weil symbol,

$$\frac{[(\gamma z) - (z); \mathcal{D}]_\Gamma}{[(\gamma z') - (z'); \mathcal{D}]_\Gamma} = \frac{[(\gamma z) - (\gamma z'); \mathcal{D}]_\Gamma}{[(z) - (z'); \mathcal{D}]_\Gamma} = \frac{[(z) - (z'); \mathcal{D}]_\Gamma}{[(z) - (z'); \mathcal{D}]_\Gamma} = 1.$$

Applying this result twice concludes the proof. □

Proposition 94. *The period pairing $\langle \cdot , \cdot \rangle$ takes values in $\mathbb{Q}_p^\times$.*

Proof. We can embed $B \otimes_\mathbb{Q} \mathbb{Q}_p$ into $\mathrm{M}_2(\mathbb{Q}_p)$ and so Γ into $\mathrm{SL}_2(\mathbb{Q}_p)$. For every $\gamma_1, \gamma_2 \in \Gamma$ and every $\sigma \in \mathrm{Aut}(\mathbb{C}_p/\mathbb{Q}_p)$,

$$\langle \gamma_1, \gamma_2 \rangle^\sigma = [\gamma_1(z_1^\sigma) - (z_1^\sigma); \gamma_2(z_2^\sigma) - (z_2^\sigma)]_\Gamma = \langle \gamma_1, \gamma_2 \rangle$$

by proposition 93. □

Proposition 95. *The period pairing $\langle \cdot , \cdot \rangle$ is a homomorphism in each variable.*

Proof. Take $\gamma_1, \gamma_2, \gamma_3 \in \Gamma$. Let $z, z' \in \mathcal{H}_p$. We can compute

$$\begin{aligned} \langle \gamma_1\gamma_2, \gamma_3 \rangle &= [(\gamma_1\gamma_2 z) - (z); (\gamma_3 z') - (z')]_\Gamma \\ &= [(\gamma_1\gamma_2 z) - (\gamma_2 z); (\gamma_3 z') - (z')]_\Gamma \cdot [(\gamma_2 z) - (z); (\gamma_3 z') - (z')]_\Gamma \\ &= \langle \gamma_1, \gamma_3 \rangle \cdot \langle \gamma_2, \gamma_3 \rangle \end{aligned}$$

and similarly for the second variable. □

All in all, $\langle \cdot , \cdot \rangle$ induces a symmetric bilinear pairing

$$\langle \cdot , \cdot \rangle \colon \Gamma^{\mathrm{ab}} \times \Gamma^{\mathrm{ab}} \longrightarrow \mathbb{Q}_p^\times.$$

Theorem 96. *The function*

$$-\mathrm{v}_p(\langle \cdot , \cdot \rangle) \colon \Gamma^{\mathrm{ab}} \times \Gamma^{\mathrm{ab}} \longrightarrow \mathbb{Z}$$

modulo torsion is positive definite in the sense that, for every $\gamma \in \Gamma$,

$$\mathrm{v}_p(\langle \gamma, \gamma \rangle) \leq 0$$

with equality if and only if γ is in the torsion subgroup of Γ^{ab}.

Corollary 97. *The period pairing* $\langle\,\cdot\,,\,\cdot\,\rangle$ *induces a map* $j\colon \Gamma \to \mathrm{Hom}(\Gamma, \mathbb{Q}_p^\times)$ *such that the kernel of*

$$\mathrm{v}_p(j(\,\cdot\,))\colon \Gamma^{\mathrm{ab}} \longrightarrow \mathrm{Hom}(\Gamma, \mathbb{Z})$$

is precisely the torsion subgroup of Γ^{ab}.

We will see that the quotient $\mathrm{Hom}(\Gamma, \mathbb{Q}_p^\times)/j(\Gamma)$ can be identified with $J_S(\mathbb{Q}_p)$, where $J_S = \mathrm{Jac}(\Gamma\backslash\mathcal{H}_p)$.

4.4.8 p–adic θ–functions

Next we would like to produce rigid meromorphic functions on $\Gamma\backslash\mathcal{H}_p$ having prescribed zeros and poles given by $\Delta \in \mathrm{Div}^0(\Gamma\backslash\mathcal{H}_p)$. To do that, take a lift $\mathcal{D} \in \mathrm{Div}^0(\mathcal{H}_p)$ of Δ.

Definition 98. The *p–adic θ–function associated with $\mathcal{D}$* is the function

$$\theta_{\mathcal{D}}(z) = [(z) - (\eta); \mathcal{D}]_\Gamma,$$

where $\eta \in \mathcal{H}_p$ is an arbitrary base point.

Proposition 99. *Let* $\mathcal{D} \in \mathrm{Div}^0(\mathcal{H}_p)$.

(1) *The function* $\theta_{\mathcal{D}}$ *is a rigid meromorphic function on* $\mathcal{H}_p$.

(2) *The function* $\theta_{\mathcal{D}}$ *is* Γ*–invariant up to multiplication by scalars, in the sense that there exists* $c_{\mathcal{D}}\colon \Gamma \to \mathbb{C}_p^\times$ *with the property that*

$$\theta_{\mathcal{D}}(\gamma z) = c_{\mathcal{D}}(\gamma) \cdot \theta_{\mathcal{D}}(z) \quad \textit{for all } \gamma \in \Gamma \textit{ and } z \in \mathcal{H}_p.$$

Proof. Using the properties of the Γ–Weil symbol, we can compute

$$\begin{aligned}\theta_{\mathcal{D}}(\gamma z) &= [(\gamma z) - (\eta); \mathcal{D}]_\Gamma = [(z) - (\gamma^{-1}\eta); \mathcal{D}]_\Gamma \\ &= [(z) - (\eta); \mathcal{D}]_\Gamma \cdot [(\eta) - (\gamma^{-1}\eta); \mathcal{D}]_\Gamma = \theta_{\mathcal{D}}(z) \cdot [(\gamma\eta) - (\eta); \mathcal{D}]_\Gamma\end{aligned}$$

and so we can define $c_{\mathcal{D}}(\gamma) = [(\gamma\eta) - (\eta); \mathcal{D}]_\Gamma$. Moreover, this expression does not depend on the choice of $\eta \in \mathcal{H}_p$. □

Definition 100. Let $\mathcal{D} \in \mathrm{Div}^0(\mathcal{H}_p)$. The function $c_{\mathcal{D}}\colon \Gamma \to \mathbb{C}_p^\times$ defined by proposition 99 is called the *factor of automorphy associated with* $\theta_{\mathcal{D}}$.

Theorem 101. *Let* $\mathcal{D} \in \mathrm{Div}^0(\mathcal{H}_p)$ *and let* $\Delta \in \mathrm{Div}^0(\Gamma\backslash\mathcal{H}_p)$ *be its image. If the factor of automorphy* $c_{\mathcal{D}}$ *belongs to* $j(\Gamma)$, *where* j *is the map from corollary 97 induced by the period pairing, then there exists a rigid meromorphic function* $F_\Delta\colon \Gamma\backslash\mathcal{H}_p \to \mathbb{P}^1(\mathbb{C}_p)$ *such that* $\mathrm{div}(F_\Delta) = \Delta$.

Proof. Since $c_{\mathcal{D}} \in j(\Gamma)$, there exists $\alpha \in \Gamma$ such that

$$c_{\mathcal{D}}(\gamma) = \langle \gamma, \alpha \rangle = [(\gamma\eta) - (\eta); (\alpha\eta') - (\eta')]_{\Gamma}.$$

After replacing $\mathcal{D}$ with $\mathcal{D} - \big((\alpha\eta') - (\eta')\big)$ (which gives another lift of Δ), we may assume that $c_{\mathcal{D}}(\gamma) = 1$ for all $\gamma \in \Gamma$. But in that case the function $\theta_{\mathcal{D}}$ is Γ–invariant and so descends to a function on $\Gamma\backslash\mathcal{H}_p$ that we call F_Δ. By the definition of

$$F_\Delta(z) = [(z) - (\eta); \mathcal{D}]_\Gamma$$

as an infinite product, one checks that $\operatorname{div}(F_\Delta) = \Delta$. □

In general, for $\mathcal{D} \in \operatorname{Div}^0(\mathcal{H}_p)$ lifting $\Delta \in \operatorname{Div}^0(\Gamma\backslash\mathcal{H}_p)$, the image of $c_{\mathcal{D}}$ in $\operatorname{Hom}(\Gamma, \mathbb{C}_p^\times)/j(\Gamma)$ encodes the image of the divisor Δ in the jacobian $J_S(\mathbb{C}_p)$ (where $J_S = \operatorname{Jac}(\Gamma\backslash\mathcal{H}_p)$).

4.4.9 Cohomological formulation

Let $\mathscr{M}^\times$ denote the multiplicative group of non-zero rigid meromorphic functions on $\mathcal{H}_p$. Observe that $\mathscr{M}^\times$ is a Γ–module with the action given by

$$(\gamma f)(z) = f(\gamma^{-1}z).$$

Given $\mathcal{D} \in \operatorname{Div}^0(\mathcal{H}_p)$, we defined $\theta_{\mathcal{D}} \in \mathrm{H}^0(\Gamma, \mathscr{M}^\times/\mathbb{C}_p^\times)$. Taking cohomology of the short exact sequence

$$0 \longrightarrow \mathbb{C}_p^\times \longrightarrow \mathscr{M}^\times \longrightarrow \mathscr{M}^\times/\mathbb{C}_p^\times \longrightarrow 0,$$

we obtain an exact sequence

$$0 \longrightarrow \mathbb{C}_p^\times \longrightarrow \mathrm{H}^0(\Gamma, \mathscr{M}^\times) \longrightarrow \mathrm{H}^0(\Gamma, \mathscr{M}^\times/\mathbb{C}_p^\times) \longrightarrow \mathrm{H}^1(\Gamma, \mathbb{C}_p^\times) = \operatorname{Hom}(\Gamma, \mathbb{C}_p^\times)$$

The automorphy factor $c_{\mathcal{D}}$ represents the obstruction to lifting $\theta_{\mathcal{D}}$ to an element in $\mathrm{H}^0(\Gamma, \mathscr{M}^\times)$.

4.5 CM points on X_S

Let S and X_S be as in theorem 77. For every field $L/\mathbb{Q}$, the points in $X_S(L)$ correspond to isomorphism classes of abelian surfaces A over L endowed with a morphism $\iota \colon R_\infty \hookrightarrow \operatorname{End}(A)$, where R_∞ is the maximal order in $B_{S\backslash\{\infty\}}$.

Definition 102. A quaternionic abelian surface A is called *special* if

$$\mathrm{End}_{R_\infty}(A) \neq \mathbb{Z}.$$

Theorem 103. *Let A be an abelian surface defined over a field L of characteristic 0 endowed with an embedding $\iota \colon R_\infty \hookrightarrow \mathrm{End}(A)$. If $E = \mathrm{End}_{R_\infty}(A) \neq \mathbb{Z}$, then E is an order in a quadratic imaginary field K in which all places $\ell \in S$ are non-split (i.e., the discriminant D of K satisfies that*

$$\left(\frac{D}{\ell}\right) \neq 1 \quad \text{if } \ell \text{ is finite}$$

and $D < 0$ for the condition at ∞).

Sketch of the proof. To shorten notation, write $M_0 = \mathrm{End}(A)$ and $M = M_0 \otimes_{\mathbb{Z}} \mathbb{Q}$. The algebra M contains $B_{S\setminus\{\infty\}} \otimes_{\mathbb{Q}} K$, where $K = \mathrm{End}_{R_\infty}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ and so we deduce that $\dim_{\mathbb{Q}}(M) \geq 4 \dim_{\mathbb{Q}}(K)$. Since M acts faithfully on $\mathrm{H}_1(A(\mathbb{C}), \mathbb{Q})$ and M_0 preserves a lattice $\mathrm{H}_1(A(\mathbb{C}), \mathbb{Z})$, we have

$$\mathrm{rank}_{\mathbb{Z}}(M_0) = \dim_{\mathbb{Q}}(M) = \dim_{\mathbb{R}}(M \otimes_{\mathbb{Q}} \mathbb{R}).$$

But $M \otimes_{\mathbb{Q}} \mathbb{R}$ can be embedded in $\mathrm{M}_2(\mathbb{C})$ via its action on $\Omega^1(A/\mathbb{C})$. Therefore, $\dim_{\mathbb{R}}(M \otimes_{\mathbb{Q}} R) \leq 8$ and $\dim_{\mathbb{Q}}(K) \leq 2$, which implies that K is a quadratic field. Finally, from

$$\mathrm{M}_2(K \otimes_{\mathbb{Q}} \mathbb{R}) \cong B_{S\setminus\{\infty\}} \otimes_{\mathbb{Q}} K \otimes_{\mathbb{Q}} \mathbb{R} \hookrightarrow M \otimes_{\mathbb{Q}} \mathbb{R} \hookrightarrow \mathrm{M}_2(\mathbb{C})$$

we deduce that $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{C}$, which means that K is quadratic imaginary. All the inequalities above are in fact equalities.

The quadratic imaginary field K splits $B_{S\setminus\{\infty\}}$ because

$$K = \mathrm{End}_{R_\infty}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \subseteq \mathrm{End}_{R_\infty}\big(\mathrm{H}_1(A(\mathbb{C}), \mathbb{Z})\big) \otimes_{\mathbb{Z}} \mathbb{Q}$$

and the latter is the normalizer of R_∞ in $\mathrm{End}\big(\mathrm{H}_1(A(\mathbb{C}), \mathbb{Z})\big) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathrm{M}_4(\mathbb{Q})$, which is just $B_{S\setminus\{\infty\}}$. That is to say, $K \subseteq B_{S\setminus\{\infty\}}$. Therefore, the subalgebra $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ of the division algebra $B_{S\setminus\{\infty\}} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a field for every place $p \in S \setminus \{\infty\}$. □

Let $\mathscr{O}$ be the order of discriminant $D < 0$ in a quadratic imaginary field K. We define $\mathrm{CM}(\mathscr{O})$ to be the set of CM points of discriminant D in $X_S(K^{\mathrm{ab}})$. (Combining the actions of K and $B_{S\setminus\{\infty\}}$, one can prove that the CM points on X_S

are isogenous to products of two CM elliptic curves and so must be defined over an abelian extension of K.)

4.5.1 Description over $\mathbb{C}$

Let $\Gamma = (R_{S,\infty}^{\times})_1$. We want to view $\mathrm{CM}(\mathscr{O})$ inside $X_S(\mathbb{C}) = \Gamma \backslash \mathfrak{h}$. The points in $\mathrm{CM}(\mathscr{O})$ are in bijection with classes of embeddings $\psi \colon \mathscr{O} \hookrightarrow R_{S,\infty}$; let τ_ψ be the unique fixed point of $\mathfrak{h}$ under the action of $\psi(K^\times)$. Then

$$\mathrm{CM}(\mathscr{O}) = \{\, \tau_\psi \in \Gamma \backslash \mathfrak{h} : \psi \colon \mathscr{O} \hookrightarrow R_{S,\infty} \,\}.$$

4.5.2 Description over $\mathbb{C}_p$

Let $\Gamma = (R_{S,p}^{\times})_1$. We want to view $\mathrm{CM}(\mathscr{O})$ inside $X_S(\mathbb{C}_p) = \Gamma \backslash \mathcal{H}_p$. The elements of $\mathrm{CM}(\mathscr{O})$ are indexed by embeddings $\psi \colon \mathscr{O} \hookrightarrow R_{S,p}$ and now the action of $\psi(K^\times)$ on $\mathcal{H}_p$ has two fixed points τ_ψ and $\overline{\tau}_\psi$.

By theorem 101, a divisor $\Delta \in \mathrm{Div}^0(\mathrm{CM}(\mathscr{O})) \subset \mathrm{Div}^0(\Gamma \backslash \mathcal{H}_p)$ is principal if it admits a lift $\mathcal{D} \in \mathrm{Div}^0(\mathcal{H}_p)$ such that

$$c_{\mathcal{D}}(\gamma) = [(\gamma\eta) - (\eta); \mathcal{D}]_\Gamma = 1 \quad \text{for all } \gamma \in \Gamma.$$

Proposition 104. *Let $\mathcal{D}_1, \mathcal{D}_2 \in \mathrm{Div}^0(\mathcal{H}_p)$ and suppose that these two divisors are supported on $\mathrm{CM}(\mathscr{O}_1)$ and $\mathrm{CM}(\mathscr{O}_2)$, where $\mathscr{O}_1$ and $\mathscr{O}_2$ are two orders of discriminants D_1 and D_2 giving rise to ring class fields H_{D_1} and H_{D_2}, respectively. If $\mathcal{D}_1$ is principal (i.e., $c_{\mathcal{D}_1} = 1$), then $[\mathcal{D}_1; \mathcal{D}_2]_\Gamma \in H_{D_1} H_{D_2}$.*

4.5.3 Concluding remarks

In conclusion, given a finite set S of places of $\mathbb{Q}$ of odd cardinality and containing ∞, we have a Shimura curve X_S containing a supply of CM points leading to extensions of singular moduli and their differences and of Heegner points on elliptic curves. Moreover, for $S = \{\infty\}$, we recover the theory over the j–line $X(1)$.

Associated with a finite set S of places of $\mathbb{Q}$, we have the following objects:

- If S has even cardinality and $\infty \in S$, then we get a definite quaternion algebra (ramified exactly at the places in S).
- If S has even cardinality and $\infty \notin S$, then we get an indefinite quaternion algebra (ramified exactly at the places in S).
- If S has odd cardinality and $\infty \in S$, then we get a Shimura curve X_S.

- If S has odd cardinality and $\infty \notin S$, it is not clear what kind of object we should consider. However, it should contain some “real multiplication” points because we do not add a restriction to the sign of the discriminant of quadratic fields.

5 RM theory

The key example of this theory will be the case of $S = \{ p \}$. Then we only need to study the action of $\Gamma_{S,p} \cong \mathrm{SL}_2(\mathbb{Z}[p^{-1}])$ on the p–adic upper half-plane $\mathcal{H}_p$. This has been studied by Darmon and Vonk. (A more general quaternionic setting has recently been studied by Guitart, Masdeu and Xarles.) From now on, write $\Gamma = \mathrm{SL}_2(\mathbb{Z}[p^{-1}])$. One of the main results of this theory is the following:

Theorem 105. *Let $\mathscr{A}^\times$ (resp. $\mathscr{M}^\times$) be the multiplicative group of non-zero rigid analytic (resp. rigid meromorphic) functions on $\mathcal{H}_p$.*

(1) *The vector space $\mathrm{H}^1(\Gamma, \mathscr{A}^\times/\mathbb{C}_p^\times) \otimes_{\mathbb{Z}} \mathbb{Q}$ is finite-dimensional and the Hecke action on it factors through the algebra $\mathbb{T}_2(\Gamma_0(p)) \subset \mathrm{End}\big(M_2(\Gamma_0(p))\big)$.*

(2) *The vector space $\mathrm{H}^1(\Gamma, \mathscr{M}^\times) \otimes_{\mathbb{Z}} \mathbb{Q}$ is infinite-dimensional and has no finite-dimensional Hecke-stable subspaces.*

We keep this notation in the following subsections.

5.1 p–adic integration on $\Gamma\backslash\mathcal{H}_p$

We revert to the setting where Γ acts discretely on $\mathcal{H}_p$. Let $\mathcal{T}$ denote the Bruhat–Tits tree of $\mathcal{H}_p$ (cf. section 4.4.3). We assume that $\Gamma\backslash\mathcal{T}$ is a finite graph and that, for every edge e and every vertex v, $\mathrm{Stab}_\Gamma(e) = \mathrm{Stab}_\Gamma(v) = 1$.

5.1.1 Rigid differentials on $\Gamma\backslash\mathcal{H}_p$

Modifying the constructions from section 4.4.8, we can define a map

$$\begin{aligned}\Theta\colon \Gamma &\longrightarrow \mathrm{H}^0(\Gamma, \mathscr{A}^\times/\mathbb{C}_p^\times)\\ \gamma &\longmapsto \Theta_\gamma\end{aligned}$$

given by

$$\Theta_\gamma(z) = [(z) - (\eta); (\gamma\xi) - (\xi)]_\Gamma,$$

where η and ξ are arbitrary base points on $\mathcal{H}_p$. Consider the logarithmic derivative $\mathrm{dlog}\colon \mathscr{A}^\times/\mathbb{C}_p^\times \to \Omega^1(\mathcal{H}_p)$ given by

$$f \mapsto \frac{df}{f}.$$

We obtain by composition a morphism (of groups) $j \colon \Gamma^{\mathrm{ab}} \to \Omega^1(\Gamma\backslash\mathcal{H}_p)$ defined by

$$j(\gamma) = \mathrm{dlog}\big(\Theta_\gamma(z)\big) = \frac{d\Theta_\gamma(z)}{\Theta_\gamma(z)}.$$

On the other hand, we can use the period pairing $\langle \cdot\,, \cdot \rangle \colon \Gamma^{\mathrm{ab}} \times \Gamma^{\mathrm{ab}} \to \mathbb{Q}_p^\times$ and theorem 96 to identify $\Gamma^{\mathrm{ab}} \otimes_{\mathbb{Z}} \mathbb{Q}$ with its dual. We will want to define

$$\int_\gamma \omega = \langle \gamma, j^{-1}(\omega) \rangle \in \mathbb{C}_p,$$

which will make sense later once we prove that the map j induces an isomorphism $\Gamma^{\mathrm{ab}} \otimes_{\mathbb{Z}} \mathbb{C}_p \cong \Omega^1(\Gamma\backslash\mathcal{H}_p)$ of $\mathbb{C}_p$–vector spaces.

5.1.2 The residue map

Let v be a vertex of the Bruhat–Tits tree $\mathcal{T}$. For every oriented edge e in $\mathcal{T}$, we write $s(e)$ and $t(e)$ for the source and the target vertices, respectively, of e. Consider

$$\mathcal{A}_v = r^{-1}(v) = \mathbb{P}^1(\mathbb{C}_p) \setminus \Bigg(\bigcup_{s(e)=v} D_e \Bigg),$$

where $r \colon \mathcal{H}_p \to \mathcal{T}$ is the reduction map and D_e denotes the residue disc corresponding to the edge e. Given $\omega \in \Omega^1(\mathcal{H}_p)$, we write $\omega_v = \omega|_{\mathcal{A}_v}$. If α is a rational differential on $\mathbb{P}^1(\mathbb{C}_p)$ that is regular on $\mathcal{A}_v$, then we can define

$$\mathrm{Res}_e(\alpha) = \mathrm{Res}_{D_e}(\alpha) = \sum_{x \in D_e} \mathrm{Res}_x(\alpha).$$

Now, writing

$$\omega_v = \lim_{j\to\infty} \alpha_j \qquad \text{for rational differentials } \alpha_j \text{ as above}$$

(the limit being with respect to the supremum norm of $\mathcal{A}_v$), we want to define

$$\mathrm{Res}_e(\omega) = \lim_{j\to\infty} \mathrm{Res}_e(\alpha_j).$$

One checks that this limit is well-defined. (To prove that it does not depend on the choice of the α_j, one can use that, for $t_1, t_2 \in B(t, p^{-N})$,

$$\left| \frac{1}{z-t_1} - \frac{1}{z-t_2} \right|_p \leq p^{n-N} \qquad \text{for all } z \in \mathcal{H}_p^{\leq n}.)$$

Let $\vec{\mathcal{T}}_1$ denote the set of oriented edges of $\mathcal{T}$. Given $\omega \in \Omega^1(\mathcal{H}_p)$, we define the *residue of* ω to be the map $c_\omega \colon \vec{\mathcal{T}}_1 \to \mathbb{C}_p$ given by $c_\omega(e) = \mathrm{Res}_e(\omega)$.

Proposition 106. *The function $c_\omega \colon \vec{\mathcal{T}}_1 \to \mathbb{C}_p$ satisfies the following properties:*

(1) *for every $e \in \vec{\mathcal{T}}_1$ with inverse edge $\bar{e}$, $c_\omega(\bar{e}) = -c_\omega(e)$, and*

(2) *for every $v \in \mathcal{T}_0$,*

$$\sum_{s(e)=v} c_\omega(e) = 0.$$

Proof. It follows by the residue theorem (for rational differentials on $\mathbb{P}^1(\mathbb{C}_p)$). For example, for the second part, we get that

$$\sum_{s(e)=v} \mathrm{Res}_{D_e}(\alpha_j) = \sum_{x \in \mathbb{P}^1(\mathbb{C}_p)} \mathrm{Res}_x(\alpha_j) = 0$$

because α_j is regular outside the residue discs D_e appearing in the first sum. □

Definition 107. A function $c \colon \vec{\mathcal{T}}_1 \to \mathbb{C}_p$ is called a *harmonic cocycle* if it satisfies conditions (1) and (2) of proposition 106. We write $C_{\text{har}}(\mathcal{T})$ for the space of harmonic cocycles on $\mathcal{T}$.

Lemma 108. *Let $\omega \in \Omega^1(\Gamma \backslash \mathcal{H}_p)$. The harmonic cocycle c_ω has the property that*

$$c_\omega(\gamma e) = c_\omega(e) \quad \textit{for all } \gamma \in \Gamma \textit{ and all } e \in \vec{\mathcal{T}}_1.$$

That is, $c_\omega \in C_{\text{har}}(\mathcal{T})^\Gamma$.

Corollary 109. *The image of c_ω is contained in a bounded subset of $\mathbb{C}_p$.*

Theorem 110. *The residue map*

$$\begin{aligned} \mathrm{Res} \colon \Omega^1(\Gamma \backslash \mathcal{H}_p) &\longrightarrow C_{\text{har}}(\mathcal{T})^\Gamma \\ \omega &\longmapsto c_\omega \end{aligned}$$

is surjective.

Proof. We produce an explicit (left) inverse. To do so, we first pass from harmonic cocycles to boundary measures. Observe that $\{ D_e \cap \mathbb{P}^1(\mathbb{Q}_p) \ : \ e \in \vec{\mathcal{T}}_1 \}$ is a collection of compact open balls in $\mathbb{P}^1(\mathbb{Q}_p)$ which is a basis of the topology of $\mathbb{P}^1(\mathbb{Q}_p)$. Given $c \in C_{\text{har}}(\mathcal{T})^\Gamma$, we define a measure μ by requiring that

$$\mu(D_e \cap \mathbb{P}^1(\mathbb{Q}_p)) = c(e).$$

(The fact that such μ is a measure and not just a distribution follows from corollary 109.)

Our objective is to construct $\omega \in \Omega^1(\Gamma \backslash \mathcal{H}_p)$ such that $c_\omega = c$; we will do it by means of the p–adic Poisson transform:

$$\omega(z) = \left(\int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{d\mu(t)}{z-t} \right) dz.$$

We claim that $\mathrm{Res}_e(\omega) = c(e)$.

Given $z \in \mathcal{H}_p$,

$$t \mapsto \frac{1}{z-t}$$

defines a continuous $\mathbb{C}_p$–valued function on $\mathbb{P}^1(\mathbb{Q}_p)$. But, dividing $\mathbb{P}^1(\mathbb{Q}_p)$ into residue discs of radius p^{-N} for $N \in \mathbb{Z}_{\geq 0}$, the differential ω can be expressed as a limit of Riemann sums

$$\omega_N = \sum_{j \in \mathbb{P}^1(\mathbb{Z}/p^N\mathbb{Z})} \frac{dz}{z-j} \cdot \mu(D_{e_j}) = \sum_{j \in \mathbb{P}^1(\mathbb{Z}/p^N\mathbb{Z})} \frac{c(e_j)}{z-j} dz,$$

where e_j is the edge of $\mathcal{T}$ corresponding to the ball $B(j, p^{-N})$. These ω_N are rational differentials which converge to ω uniformly on affinoids. One can check (exercise) that

$$\mathrm{Res}_e(\omega_N) \xrightarrow[N \to \infty]{} c(e)$$

for every $e \in \vec{\mathcal{T}}_1$. □

With the same notation as in the proof of theorem 110, one checks that ω is Γ–invariant if c is. Indeed,

$$\frac{1}{\gamma(z) - \gamma(t)} = \frac{(cz+d)^2}{z-t} + u(z)(cz+d)^2 \quad \text{if } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and so

$$\frac{d(\gamma(z))}{\gamma(z) - \gamma(t)} = \frac{dz}{z-t} + u(z)\, dz.$$

Since $u(z)\, dz$ does not depend on t, after integrating we deduce that

$$\left(\int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{d\mu(t)}{\gamma(z) - t} \right) d\gamma(z) = \left(\int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{d\mu(t)}{\gamma(z) - \gamma(t)} \right) d\gamma(z) = \left(\int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{d\mu(t)}{z-t} \right) dz,$$

which is to say that $\gamma^*(\omega) = \omega$.

Theorem 111 (Drinfeld–Manin). *The residue map*

$$\mathrm{Res}\colon \Omega^1(\Gamma\backslash\mathcal{H}_p) \longrightarrow C_{\mathrm{har}}(\mathcal{T})^\Gamma$$

is an isomorphism.

Sketch of the proof. By theorem 110, it suffices to compare dimensions. Using the rigid GAGA principle, we can express

$$\dim\bigl(\Omega^1(\Gamma\backslash\mathcal{H}_p)\bigr) = g(\Gamma\backslash\mathcal{H}_p),$$

where g is the genus. Thus, by the surjectivity of Res, $\dim\bigl(C_{\mathrm{har}}(\mathcal{T})^\Gamma\bigr) \leq g(\Gamma\backslash\mathcal{H}_p)$.

We will need some basic facts about the action of $\mathrm{SL}_2(\mathbb{Q}_p)$ on $\mathcal{T}$.

- Given $v \in \mathcal{T}_0$ and $\gamma \in \mathrm{SL}_2(\mathbb{Q}_p)$, the distance $d(v, \gamma(v))$ is an even integer.
- Given two $\mathbb{Z}_p$–lattices Λ_1 and Λ_2 with generalized index $[\Lambda_1 : \Lambda_2] \in p^{\mathbb{Z}}$, we have $[\Lambda_1 : \Lambda_2] = [\Lambda_1 : \gamma\Lambda_2]$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Q}_p)$.
- Let v^* be the standard vertex corresponding to $[\mathbb{Z}_p^2]$. We say that a vertex $v \in \mathcal{T}_0$ is *even* (resp. *odd*) if $d(v, v^*)$ is even (resp. odd). We can decompose $\mathcal{T}_0 = \mathcal{T}_0^+ \sqcup \mathcal{T}_0^-$, where $\mathcal{T}_0^+$ consists of the even vertices and $\mathcal{T}_0^-$ consists of the odd vertices.

Consequently, the quotient $\Gamma\backslash\mathcal{T}$ is a bipartite graph.

There is an exact sequence

$$0 \longrightarrow C_{\mathrm{har}}(\mathcal{T})^\Gamma \xrightarrow{i} \mathrm{Map}(\Gamma\backslash\mathcal{T}_1, \mathbb{C}_p) \xrightarrow{j} \mathrm{Map}(\Gamma\backslash\mathcal{T}_0, \mathbb{C}_p) \longrightarrow W \longrightarrow 0$$

(where W is just the cokernel of j) defined as follows:

- $i(c)(e) = c(\vec{e})$, where $\vec{e}$ is the oriented version of e going from an even to an odd vertex, and
- $j(f)(v) = \sum\limits_{v\in e} f(e)$ where the sum runs over the edges e containing v.

Now we can check that $\dim(W) \geq 1$ because

$$\sum_{v \text{ even}} j(f)(v) = \sum_{v \text{ odd}} j(f)(v)$$

(i.e., there is a non-trivial relation on $\mathrm{Im}(j)$). But, writing $V = |\Gamma\backslash\mathcal{T}_0|$ and $E = |\Gamma\backslash\mathcal{T}_1|$, we conclude that

$$\dim C_{\mathrm{har}}(\mathcal{T}) = E - V + \dim(W) \geq E - V + 1 = g(\Gamma\backslash\mathcal{T}),$$

and one can prove that $g(\Gamma\backslash\mathcal{H}_p) = g(\Gamma\backslash\mathcal{T})$. □

We have seen two approaches to constructing elements of $\Omega^1(\Gamma\backslash\mathcal{H}_p)$:

(1) We have a morphism $j\colon \Gamma^{\mathrm{ab}} \to \Omega^1(\Gamma\backslash\mathcal{H}_p)$ defined by

$$j(\gamma) = \mathrm{dlog}\big(\Theta_\gamma(z)\big).$$

(2) We have a map $C_{\mathrm{har}}(\Gamma\backslash\mathcal{T})^\Gamma \to \Omega^1(\Gamma\backslash\mathcal{H}_p)$ given by the p–adic Poisson transform of measures (i.e., the inverse of Res above).

Remark. Since the last approach gives a very explicit description of differentials in $\Omega^1(\Gamma\backslash\mathcal{H}_p)$, we can find line integrals explicitly too:

$$\begin{aligned}\int_{\tau_1}^{\tau_2} \omega(z) = \int_{\tau_1}^{\tau_2}\left(\int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{d\mu(t)}{z-t}\right) dz = \int_{\mathbb{P}^1(\mathbb{Q}_p)}\left(\int_{\tau_1}^{\tau_2} \frac{dz}{z-t}\right) d\mu(t)\\ = \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{\tau_2 - t}{\tau_1 - t}\right) d\mu(t).\end{aligned}$$

5.2 Rigid analytic and meromorphic cocycles

Consider $\Gamma = \mathrm{SL}_2(\mathbb{Z}[p^{-1}])$. Let $\mathscr{A}^\times$ (resp. $\mathscr{M}^\times$) denote the multiplicative group of analytic (resp. meromorphic) functions on $\mathcal{H}_p$.

Definition 112.

(1) A *rigid analytic cocycle* is a class in $\mathrm{H}^1(\Gamma, \mathscr{A}^\times)$.

(2) A *rigid analytic θ–cocycle* is a class in $\mathrm{H}^1(\Gamma, \mathscr{A}^\times/\mathbb{C}_p^\times)$.

(3) A *rigid meromorphic cocycle* is a class in $\mathrm{H}^1(\Gamma, \mathscr{M}^\times)$.

Definition 113. An *RM point* is a point $\tau \in \mathcal{H}_p$ such that $\mathbb{Q}(\tau)$ is a real quadratic field. Then $\mathrm{Stab}_\Gamma(\tau) \cong \gamma_\tau^{\mathbb{Z}}$ modulo torsion (where γ_τ denotes a generator). Given a rigid meromorphic cocycle J, we define the *RM value*

$$J[\tau] = J(\gamma_\tau)(\tau).$$

These RM values $J[\tau]$ are conjectured to be defined over class fields of $\mathbb{Q}(\tau)$. There should be the following analogy:

	RM values	CM values
Analytic cocycles	Gross–Stark points	Elliptic units
θ–cocycles	Stark–Heegner points	Heegner points
Meromorphic cocycles	“Singular moduli”	Singular moduli

Example 114. The *tautological cocycle* $J_{\mathrm{triv}}\colon \Gamma \to \mathscr{A}^\times$ is defined by

$$J_{\mathrm{triv}}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)(z) = cz + d \quad \text{for } z \in \mathcal{H}_p.$$

Given an RM point $\tau \in \mathcal{H}_p$, we can compute the corresponding RM value using a generator of $\mathrm{Stab}_\Gamma(\tau)$. That is a matrix for which $(\tau, 1)$ is an eigenvector or, equivalently, satisfying that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \tau \\ 1 \end{pmatrix} = (c\tau + d)\begin{pmatrix} \frac{a\tau+b}{c\tau+d} \\ 1 \end{pmatrix} = (c\tau + d)\begin{pmatrix} \tau \\ 1 \end{pmatrix},$$

so $c\tau + d$ is an eigenvalue or, equivalently, a fundamental unit of the real quadratic order $\mathscr{O}_\tau$ associated with τ. This tautological cocycle is an example of an *Eisenstein cocycle*: for every prime $\ell \neq p$, the Hecke operator T_ℓ acts by

$$\mathrm{T}_\ell(J_{\mathrm{triv}}) = J_{\mathrm{triv}}^{\ell+1}.$$

5.2.1 The cohomology of Γ

Theorem 115. *Let* $\Gamma = \mathrm{SL}_2(\mathbb{Z}[p^{-1}])$.
(1) $\mathrm{H}^1(\Gamma, \mathbb{Q}) = 0$.
(2) $\mathrm{H}^2(\Gamma, \mathbb{Q}) = \mathrm{H}^1(\Gamma_0(p), \mathbb{Q})$.

We follow a proof of Ihara and Serre using the Bruhat–Tits tree $\mathcal{T}$ of $\mathcal{H}_p$. Let $\mathcal{T}_0^+$ (resp. $\mathcal{T}_0^-$) denote the set of even (resp. odd) vertices of $\mathcal{T}$ and let $\vec{\mathcal{T}}_1^+$ (resp. $\vec{\mathcal{T}}_1^-$) denote the set of oriented edges of $\mathcal{T}$ having even (resp. odd) source vertex.

Lemma 116. *The group* Γ *acts transitively on each of the sets* $\mathcal{T}_0^+$, $\mathcal{T}_0^-$, $\vec{\mathcal{T}}_1^+$, $\vec{\mathcal{T}}_1^-$ *and* $\mathcal{T}_1$.

Proof. Let Λ_1 and Λ_2 be two $\mathbb{Z}_p$–lattices in $\mathbb{Q}_p^2$. There exists $\gamma \in \mathrm{GL}_2(\mathbb{Q}_p)/\mathbb{Q}_p^\times$ such that $\gamma\Lambda_1 = \Lambda_2$. To pass to Γ, we use that $[\mathrm{PGL}_2(\mathbb{Q}_p) : \mathrm{PSL}_2(\mathbb{Q}_p)] = 4$ (assuming $p > 2$) and there is a homomorphism $\mathrm{PGL}_2(\mathbb{Q}_p)/\,\mathrm{PSL}_2(\mathbb{Q}_p) \to \mathbb{Z}/2\mathbb{Z}$ given by

$$\gamma \mapsto \mathrm{v}_p(\det(\gamma)).$$

We have seen that $\mathrm{PGL}_2(\mathbb{Q}_p)$ acts transitively on $\mathcal{T}_0$ and one checks that the matrices γ that interchange the sets $\mathcal{T}_0^+$ and $\mathcal{T}_0^-$ are precisely the ones satisfying that $\mathrm{v}_p(\det(\gamma)) \equiv 1 \bmod 2$. Thus, $\mathrm{PSL}_2(\mathbb{Q}_p)$ acts on $\mathcal{T}_0$ with the two orbits $\mathcal{T}_0^+$ and $\mathcal{T}_0^-$ and then we can use that Γ is dense in $\mathrm{SL}_2(\mathbb{Q}_p)$ to deduce the same result for Γ. The statement for edges can be proved similarly. □

By lemma 116, the quotient graph $\Gamma\backslash\mathcal{T}$ has two vertices joined by an edge. We use as representatives the standard vertex v^* and the standard edge e^* going from v^* to another vertex $v^{*,\prime}$ (corresponding to the lattice $p\mathbb{Z}_p \oplus \mathbb{Z}_p$). We have $\mathrm{Stab}_\Gamma(v^*) = \mathrm{SL}_2(\mathbb{Z})$ and

$$\mathrm{Stab}_\Gamma(v^{*,\prime}) = \mathrm{SL}_2(\mathbb{Z})' = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, d \in \mathbb{Z}, b \in \frac{1}{p}\mathbb{Z}, c \in p\mathbb{Z} \right\}.$$

Therefore, $\mathrm{Stab}_\Gamma(e^*) = \mathrm{Stab}_\Gamma(v^*) \cap \mathrm{Stab}_\Gamma(v^{*,\prime}) = \Gamma_0(p)$.

For every Γ–module M, there is a short exact sequence

$$0 \longrightarrow M \xrightarrow{i} \mathrm{Map}(\mathcal{T}_0, M) \xrightarrow{d} \mathrm{Map}(\mathcal{T}_1, M) \longrightarrow 0$$

given by $i(m)(v) = m$ and $d(f)(e) = f(v^+) - f(v^-)$, where v^+ and v^- are the even and odd vertices of e, respectively. The corresponding long exact sequence of cohomology is

$$\begin{aligned} 0 \longrightarrow M^\Gamma \longrightarrow \mathrm{Map}(\mathcal{T}_0, M)^\Gamma \longrightarrow \mathrm{Map}(\mathcal{T}_1, M)^\Gamma \xrightarrow{\delta} \mathrm{H}^1(\Gamma, M) - \\ \to \mathrm{H}^1(\Gamma, \mathrm{Map}(\mathcal{T}_0, M)) \longrightarrow \mathrm{H}^1(\Gamma, \mathrm{Map}(\mathcal{T}_1, M)) \xrightarrow{\delta} \mathrm{H}^2(\Gamma, M) - \\ \to \mathrm{H}^2(\Gamma, \mathrm{Map}(\mathcal{T}_0, M)) \longrightarrow \cdots \end{aligned}$$

By lemma 116, we can express

$$\mathrm{Map}(\mathcal{T}_0, M) = \mathrm{Ind}^\Gamma_{\mathrm{SL}_2(\mathbb{Z})}(M) \oplus \mathrm{Ind}^\Gamma_{\mathrm{SL}_2(\mathbb{Z})'}(M)$$

and

$$\mathrm{Map}(\mathcal{T}_1, M) = \mathrm{Ind}^\Gamma_{\Gamma_0(p)}(M).$$

Using Shapiro's lemma, we can rewrite the long exact sequence as

$$\begin{aligned} 0 \longrightarrow M^\Gamma \longrightarrow M^{\mathrm{SL}_2(\mathbb{Z})} \oplus M^{\mathrm{SL}_2(\mathbb{Z})'} \longrightarrow M^{\Gamma_0(p)} \xrightarrow{\delta} \mathrm{H}^1(\Gamma, M) - \\ \to \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}), M) \oplus \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z})', M) \longrightarrow \mathrm{H}^1(\Gamma_0(p), M) \xrightarrow{\delta} \mathrm{H}^2(\Gamma, M) - \\ \to \mathrm{H}^2(\mathrm{SL}_2(\mathbb{Z}), M) \oplus \mathrm{H}^2(\mathrm{SL}_2(\mathbb{Z})', M) \longrightarrow \cdots \end{aligned}$$

- If $M = \mathbb{Q}$, from the surjectivity of $\mathbb{Q}^{\mathrm{SL}_2(\mathbb{Z})} \oplus \mathbb{Q}^{\mathrm{SL}_2(\mathbb{Z})'} \to \mathbb{Q}^{\Gamma_0(p)}$ and the fact that $\mathrm{H}^i(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q}) = 0 = \mathrm{H}^i(\mathrm{SL}_2(\mathbb{Z})', \mathbb{Q})$ for $i = 1$ or 2, we deduce that $\mathrm{H}^1(\Gamma, \mathbb{Q}) = 0$ and $\delta\colon \mathrm{H}^1(\Gamma_0(p), \mathbb{Q}) \to \mathrm{H}^2(\Gamma, \mathbb{Q})$ is an isomorphism.
- If $M = \mathbb{Z}$, we obtain an injective morphism $\delta\colon \mathrm{H}^1(\Gamma_0(p), \mathbb{Z}) \to \mathrm{H}^2(\Gamma, \mathbb{Z})$ with finite cokernel.

5.3 The Dedekind–Rademacher cocycle

We consider certain Eisenstein series of weight 2 and level $\Gamma_0(p)$, which can be constructed as follows. From the modular discriminant

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24} \quad \text{(of weight 12 and level } \mathrm{SL}_2(\mathbb{Z})\text{)},$$

we construct a modular unit

$$U_p = \frac{\Delta(q^p)}{\Delta(q)}$$

on $Y_0(p)$. Then we define an Eisenstein series $E_2^{(p)}$ (that we identify with a differential form on $Y_0(p)$) by

$$E_2^{(p)}(z)\,dz = \mathrm{dlog}(U_p) = \left((p-1) + 24\sum_{n=1}^{\infty}\sigma^{(p)}(n)q^n\right)\frac{dq}{q},$$

where

$$\sigma^{(p)}(n) = \sum_{p\nmid d|n} d.$$

Conceptually, we view U_p as a morphism $Y_0(p) \to \mathbb{G}_\mathrm{m}$ and then $E_2^{(p)}(z)\,dz$ is the pull-back of $\frac{dz}{z}$. Define $\varphi_{\mathrm{DR}}\colon \Gamma_0(p) \to \mathbb{Z}$ by

$$\varphi_{\mathrm{DR}}(\gamma) = \frac{1}{2\pi i}\int_{z_0}^{\gamma(z_0)} E_2^{(p)}(z)\,dz$$

for some base point $z_0 \in \mathcal{H}_p$. One checks that $\varphi_{\mathrm{DR}} \in \mathrm{H}^1(\Gamma_0(p),\mathbb{Z})$. Now take $\alpha_{\mathrm{DR}} = \delta(\varphi_{\mathrm{DR}}) \in \mathrm{H}^2(\Gamma,\mathbb{Z})$. We view $p^{\alpha_{\mathrm{DR}}} \in \mathrm{H}^2(\Gamma, p^{\mathbb{Z}})$ inside $\mathrm{H}^2(\Gamma,\mathbb{C}_p^\times)$.

Theorem 117. *The natural image of $p^{\alpha_{\mathrm{DR}}}$ in $\mathrm{H}^2(\Gamma,\mathscr{A}^\times)$ is trivial.*

Corollary 118. *There exists a 1–cochain $J_{\mathrm{DR}} \in \mathrm{C}^1(\Gamma,\mathscr{A}^\times)$ characterized by*

$$\gamma_1 J_{\mathrm{DR}}(\gamma_2)\cdot J_{\mathrm{DR}}(\gamma_1\gamma_2)^{-1}\cdot J_{\mathrm{DR}}(\gamma_1) = p^{\alpha_{\mathrm{DR}}(\gamma_1,\gamma_2)}$$

for all $\gamma_1,\gamma_2 \in \Gamma$.

Definition 119. The *Dedekind–Rademacher cocycle* is the image of the 1–cocycle J_{DR} from corollary 118 in $\mathrm{H}^1(\Gamma,\mathscr{A}^\times/p^{\mathbb{Z}})$. (This class is not uniquely defined, but its image in $\mathrm{H}^1(\Gamma,\mathscr{A}^\times/p^{\mathbb{Z}})\otimes_{\mathbb{Z}}\mathbb{Q}$ is).

Remark. The RM values of J_{DR}, defined in $\mathbb{C}_p^\times/p^{\mathbb{Z}}$, are analogues of elliptic units.

5.3.1 Siegel units

Let $\mathscr{O}_{\mathcal{H}}^{\times}$ denote the non-zero complex analytic functions on the upper half-plane $\mathcal{H} = \mathfrak{h}$, which is endowed with a right action of $\mathrm{SL}_2(\mathbb{Q})$ given by

$$(h|\gamma)(z) = h(\gamma z).$$

Consider $(\alpha, \beta) \in (\mathbb{Q}/\mathbb{Z})^2$ with $\alpha \neq 0$ or $\beta \neq 0$ and let N be the order of (α, β) in this group.

Proposition 120. *There exists $g_{\alpha,\beta} \in \mathscr{O}_{Y(N)}^{\times} \otimes_{\mathbb{Z}} \mathbb{Q}$ with*

$$g_{\alpha,\beta} = -q^{w} \cdot \prod_{n \geq 1} \left(1 - q^{n+\alpha} e^{2\pi i \beta}\right) \cdot \prod_{n \geq 1} \left(1 - q^{n-\alpha} e^{-2\pi i \beta}\right),$$

where

$$w = \frac{1}{12} - \frac{\alpha}{2} + \frac{\alpha}{2N}$$

and we choose the representatives of α and β in the interval $[0, 1)$.

There is a right action of $\mathrm{SL}_2(\mathbb{Z})$ on the set $\{ g_v : v \in (\mathbb{Q}/\mathbb{Z})^2 \setminus \{ 0 \} \}$ given by

$$g_v | \gamma = g_{v\gamma} \quad \text{(where we view } v \text{ as a row vector).}$$

One gets the following norm-compatibility relations:

$$\prod_{n\alpha' = \alpha} g_{\alpha',\beta}(z) = g_{\alpha,\beta}\left(\frac{z}{n}\right)$$

and

$$\prod_{n\beta' = \beta} g_{\alpha,\beta'}(z) = g_{\alpha,\beta}(nz).$$

5.3.2 The Siegel distribution

Let $\mathbb{X}_0 = (\mathbb{Z}_p^2)'$ denote the primitive vectors in $\mathbb{Z}_p^2$ (i.e., such that one of the two coordinates is in $\mathbb{Z}_p^{\times}$) and let $\mathbb{X} = \mathbb{Q}_p^2 \setminus \{ 0 \}$. We can express

$$\mathbb{X} = \bigsqcup_{j \in \mathbb{Z}} p^j \mathbb{X}_0.$$

Let $\mathrm{LC}(\mathbb{X}_0, \mathbb{Z})$ be the space of locally constant $\mathbb{Z}$–valued functions on $\mathbb{X}_0$ and consider a right Γ–module A.

Definition 121. An *A–valued distribution on* $\mathbb{X}_0$ is a homomorphism (of groups) $\mu\colon \operatorname{LC}(\mathbb{X}_0, \mathbb{Z}) \to A$. We write $\mathbb{D}(\mathbb{X}_0, A)$ for the space of such distributions.

Remark. There is an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{D}(\mathbb{X}_0, A)$ characterized by

$$(\mu|\gamma)(U) = \big(\mu(U\gamma^{-1})\big)\big|\gamma$$

for all compact open subsets U of $\mathbb{X}_0$.

Since we want to get Γ–modules but $\Gamma = \mathrm{SL}_2(\mathbb{Z}[p^{-1}])$ does not preserve primitive vectors, we next consider distributions on $\mathbb{X}$. Since $\mathbb{X}$ (as opposed to $\mathbb{X}_0$) is not compact, we need to work with locally constant functions that are compactly supported. Apart from this, the definition of distributions on $\mathbb{X}$ is analogous to definition 121.

Definition 122. A distribution μ on $\mathbb{X}$ is called *p–invariant* if $\mu(pU) = \mu(U)$ for all compact open subsets of $\mathbb{X}$. We write $\mathbb{D}(\mathbb{X}, A)$ for the module of p–invariant A–valued distributions on $\mathbb{X}$.

Remark. Since
$$\mathbb{X} = \bigsqcup_{j \in \mathbb{Z}} p^j \mathbb{X}_0,$$
we identify p–invariant distributions on $\mathbb{X}$ with distributions on $\mathbb{X}_0$ via restriction. Thus, we obtain an $\mathrm{SL}_2(\mathbb{Z})$–equivariant isomorphism $\mathbb{D}(\mathbb{X}, A) \cong \mathbb{D}(\mathbb{X}_0, A)$. But, on $\mathbb{D}(\mathbb{X}, A)$, the action of $\mathrm{SL}_2(\mathbb{Z})$ extends to an action of Γ.

Given a locally constant compactly supported function $f(x, y)$ on $\mathbb{X}$ and a distribution $\mu \in \mathbb{D}(\mathbb{X}, A)$, we have

$$\int_{\mathbb{X}} f(x, y)\, d(\mu|\gamma) = \left(\int_{\mathbb{X}} f\big((x, y)\gamma\big)\, d\mu\right)\bigg|\gamma.$$

Definition 123. The *Siegel distribution* is the unique $\mu_{\mathrm{Sie}} \in \mathbb{D}(\mathbb{X}, \mathscr{O}_{\mathcal{H}}^{\times})$ such that

$$\mu_{\mathrm{Sie}}\big((a, b) + p^N \mathbb{Z}_p^2\big) = g_{a/p^N, b/p^N}^{12} \in \mathscr{O}_{\mathcal{H}}^{\times}$$

for all $(a, b) \in \mathbb{Z}^2$ and all $N \in \mathbb{Z}_{\geq 1}$.

Remark. It seems that Henri thought that the exponent 12 was enough to "kill denominators" (i.e., get rid of the $\otimes_{\mathbb{Z}} \mathbb{Q}$) in proposition 120. However, David Loeffler pointed out that the exponents should be unbounded (depending on N).

See section 5.3.3 below for the necessary corrections. Then one can check from the norm-compatibility relations that the formula above (once suitably modified) defines an element $\mu_{\mathrm{Sie}} \in \mathbb{D}(\mathbb{X}, \mathscr{O}_{\mathcal{H}}^{\times})$.

Theorem 124. *The distribution μ_{Sie} is Γ–invariant.*

Proof. If $\alpha = \frac{a}{p^N}$ and $\beta = \frac{b}{p^N}$, we define $U_{\alpha,\beta} = (a, b) + p^N\mathbb{Z}_p^2$. For $T \in \mathrm{SL}_2(\mathbb{Z})$, it is clear that

$$\mu_{\mathrm{Sie}}(U_{\alpha,\beta}|T) = \mu_{\mathrm{Sie}}(U_{\alpha,\beta})|T.$$

Thus, it suffices to show the same relation for

$$T = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix},$$

as Γ is contained in the group generated by $\mathrm{SL}_2(\mathbb{Z})$ and T. But we can express

$$\begin{aligned} U_{\alpha,\beta}|T = U_{p\alpha,\beta} &= (pa + p^{N+1}\mathbb{Z}_p) \times (b + p^N\mathbb{Z}_p) \\ &= \bigcup_{b' \equiv b \mod p^N} (pa + p^{N+1}\mathbb{Z}_p) \times (b' + p^{N+1}\mathbb{Z}_p) = \bigcup_{p\beta'=\beta} U_{\alpha,\beta'}. \end{aligned}$$

Therefore, using the norm-compatibility relations,

$$\mu_{\mathrm{Sie}}(U_{\alpha,\beta}|T) = \prod_{p\beta'=\beta} g_{\alpha,\beta'}^{12}(z) = g_{\alpha,\beta}^{12}(pz) = g_{\alpha,\beta}^{12}|T = \mu_{\mathrm{Sie}}(U_{\alpha,\beta})|T.$$

□

Lemma 125.

(1) $\mu_{\mathrm{Sie}}(\mathbb{X}_0) \equiv 1 \bmod p^{\mathbb{Z}}$.

(2) $\mu_{\mathrm{Sie}}(p\mathbb{Z}_p \times \mathbb{Z}_p^{\times}) = \dfrac{\Delta(q^p)}{\Delta(q)}$.

Idea of the proof.

(1) $\mu_{\mathrm{Sie}}(\mathbb{X}_0)$ is a unit on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$, but those are all constants.

(2) We can compute

$$\mu_{\mathrm{Sie}}(p\mathbb{Z}_p \times \mathbb{Z}_p^{\times}) = \prod_{i=1}^{p-1} \mu_{\mathrm{Sie}}\big((0,1) + p\mathbb{Z}_p^2\big) = \prod_{i=1}^{p-1} g_{0,i/p}^{12}(z) = p^{12}\frac{\Delta(q^p)}{\Delta(q)}.$$

□

5.3.3 A correction on Siegel units

Consider the theta function $\theta(\tau,z)$ (for $\tau \in \mathcal{H}$ fixed and $z \in \mathbb{C}$ variable), which is "almost" an elliptic function in the sense that

$$\theta(\tau,z+1)=\theta(\tau,z) \quad \text{and} \quad \theta(\tau,z+\tau)=e^{-\pi i(\tau+2z)}\theta(\tau,z).$$

The only zeros of $\theta(\tau,\,\cdot\,)$ are the points $z \in \mathbb{Z}\oplus\mathbb{Z}\tau$. Let $c \in \mathbb{Z}$ such that $(6,c)=1$. We define a variant of θ (depending on c) as follows:

$${}_c\theta(\tau,z)=\frac{(\theta(\tau,z))^{c^2}}{\theta(\tau,cz)}.$$

This function still satisfies that

$${}_c\theta(\tau,z+\lambda)={}_c\theta(\tau,z) \quad \text{for all } \lambda \in \mathbb{Z}\oplus\mathbb{Z}\tau.$$

By definition, if E is the elliptic curve over $\mathbb{C}$ corresponding to $\mathbb{C}/(\mathbb{Z}\oplus\mathbb{Z}\tau)$, we have $\operatorname{div}({}_c\theta(\tau,\,\cdot\,))=c^2(0)-E[c]$. Now we can define modified Siegel units

$${}_cg_{\alpha,\beta}(\tau)={}_c\theta(\tau,\alpha+\tau\beta)\in\mathscr{O}_{Y(N)}^{\times} \quad \text{whenever } (c,N)=1.$$

These units are related to the ones defined in section 5.3.1 by

$${}_cg_{\alpha,\beta}(\tau)=\frac{g_{\alpha,\beta}^{c^2}(\tau)}{g_{c\alpha,c\beta}(\tau)}.$$

The correct characterization of $\mu_{\mathrm{Sie}} \in \mathbb{D}(\mathbb{X}_0,\mathscr{O}_{\mathcal{H}}^{\times})^{\mathrm{SL}_2(\mathbb{Z})}$ is

$$\mu_{\mathrm{Sie}}\big((a,b)+p^N\mathbb{Z}_p\big)={}_cg_{\alpha,\beta}(\tau) \quad \text{for } \alpha=\frac{a}{p^N} \text{ and } \beta=\frac{b}{p^N}.$$

As explained in section 5.3.2, we obtain in this way $\mu_{\mathrm{Sie}} \in \mathbb{D}(\mathbb{X},\mathscr{O}_{\mathcal{H}}^{\times})^{\Gamma}$ with the property that

$$\mu_{\mathrm{Sie}}(\mathbb{X}_0)\in p^{\mathbb{Z}} \quad \text{and} \quad \mu_{\mathrm{Sie}}(p\mathbb{Z}_p\times\mathbb{Z}_p^{\times})=\left(p\frac{\Delta(q^p)}{\Delta(q)}\right)^{(c^2-1)/24}$$

From now on, we assume that $p>5$ and we can take $c=5$ (to forget about the exponent in the last formula).

5.3.4 The cocycle valued in distributions

Let A denote a Γ–module.

Lemma 126. *Let $\mu \in \mathbb{D}(\mathbb{X}, A)$. For every $\mathbb{Z}_p$–lattice $\Lambda \subseteq \mathbb{Q}_p^2$, the subset Λ_{prim} of primitive vectors in Λ is compact and*

$$\mu(\Lambda_{\text{prim}}) = \mu(\mathbb{X}_0).$$

Proof. Choose $N \in \mathbb{Z}_{\geq 0}$ such that $p^N\mathbb{Z}_p^2 \subseteq \Lambda \subseteq p^{-N}\mathbb{Z}_p^2$. For every $v \in \Lambda_{\text{prim}}$, there is $j \in [-N, N]$ such that $p^j v \in \mathbb{X}_0$. That is, we can decompose

$$\Lambda_{\text{prim}} = p^{m_1}U_1 \sqcup \cdots \sqcup p^{m_t}U_t$$

with $-N \leq m_i \leq N$ and

$$\mathbb{X}_0 = (\mathbb{Z}_p^2)_{\text{prim}} = U_1 \sqcup \cdots \sqcup U_t.$$

Therefore,

$$\mu(\Lambda_{\text{prim}}) = \mu(U_1) + \cdots + \mu(U_t) = \mu(\mathbb{X}_0). \qquad \square$$

Lemma 127. *The rule $A \mapsto \mathbb{D}(\mathbb{X}, A)$ is an exact functor on Γ–modules.*

Proof. Left as an exercise. The key issue is right exactness. $\square$

From the short exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathscr{O}_{\mathcal{H}} \xrightarrow{f \mapsto e^{2\pi i f}} \mathscr{O}_{\mathcal{H}}^{\times} \longrightarrow 1$$

of Γ–modules, we obtain by lemma 127 a short exact sequence

$$0 \longrightarrow \mathbb{D}(\mathbb{X}, \mathbb{Z}) \longrightarrow \mathbb{D}(\mathbb{X}, \mathscr{O}_{\mathcal{H}}) \longrightarrow \mathbb{D}(\mathbb{X}, \mathscr{O}_{\mathcal{H}}^{\times}) \longrightarrow 1$$

from which, taking cohomology, we get a connecting homomorphism

$$\delta\colon \mathrm{H}^0(\Gamma, \mathbb{D}(\mathbb{X}, \mathscr{O}_{\mathcal{H}}^{\times})) \to \mathrm{H}^1(\Gamma, \mathbb{D}(\mathbb{X}, \mathbb{Z})).$$

We define a *Dedekind–Rademacher cocycle valued on distributions*

$$\mu_{\text{DR}} = \delta(\mu_{\text{Sie}}) \in \mathrm{H}^1(\Gamma, \mathbb{D}(\mathbb{X}, \mathbb{Z})).$$

Writing

$$\widetilde{\mu}_{\mathrm{Sie}} = \frac{1}{2\pi i}\log(\mu_{\mathrm{Sie}}),$$

we can express

$$\mu_{\mathrm{DR}}(\gamma) = \widetilde{\mu}_{\mathrm{Sie}}|\gamma^{-1} - \widetilde{\mu}_{\mathrm{Sie}}.$$

Lemma 128.

(1) $\mu_{\mathrm{DR}}(\gamma)(\mathbb{X}_0) = 0$ *for all* $\gamma \in \Gamma$.

(2) $\mu_{\mathrm{DR}}(\gamma)(p\mathbb{Z}_p \times \mathbb{Z}_p^\times) = \varphi_{\mathrm{DR}}(\gamma)$ *for all* $\gamma \in \Gamma_0(p)$.

Proof. By the last formula for μ_{DR},

$$\mu_{\mathrm{DR}}(\gamma)(\mathbb{X}_0) = (\widetilde{\mu}_{\mathrm{Sie}}|\gamma^{-1})(\mathbb{X}_0) = \widetilde{\mu}_{\mathrm{Sie}}(\mathbb{X}_0) = \widetilde{\mu}_{\mathrm{Sie}}(\mathbb{X}_0\gamma)|\gamma^{-1} - \widetilde{\mu}_{\mathrm{Sie}}(\mathbb{X}_0) = 0$$

because $\widetilde{\mu}_{\mathrm{Sie}}(\mathbb{X}_0\gamma) = \widetilde{\mu}_{\mathrm{Sie}}(\mathbb{X}_0)$. Similarly, but using also that

$$\mu_{\mathrm{Sie}}(p\mathbb{Z}_p \times \mathbb{Z}_p^\times) = p\frac{\Delta(pz)}{\Delta(z)}$$

and so

$$\widetilde{\mu}_{\mathrm{Sie}}(p\mathbb{Z}_p \times \mathbb{Z}_p^\times) = \frac{\log(p)}{2\pi i} + \frac{1}{2\pi i}\log\left(\frac{\Delta(pz)}{\Delta(z)}\right),$$

we check that for every $\gamma \in \Gamma_0(p)$, which preserves $p\mathbb{Z}_p \times \mathbb{Z}_p^\times$,

$$\mu_{\mathrm{DR}}(\gamma) = \frac{1}{2\pi i}\int_{z_0}^{\gamma(z_0)} \mathrm{dlog}\left(\frac{\Delta(pz)}{\Delta(z)}\right) = \varphi_{\mathrm{DR}}(\gamma).$$

□

5.3.5 The multiplicative Poisson transform

Given $\mu \in \mathbb{D}(\mathbb{X}, \mathbb{Z})$ and a compactly supported function f on $\mathbb{X}$ with values in $\mathbb{C}_p$, we define

$$\int_{\mathbb{X}} f\, d\mu(x,y) = \lim \sum_{\alpha \in I} f(x_\alpha, y_\alpha)\mu(U_\alpha),$$

where the limit is taken over finer and finer coverings

$$\mathbb{X} = \bigsqcup_{\alpha \in I} U_\alpha$$

and $(x_\alpha, y_\alpha) \in U_\alpha$.

We have a multiplicative version of these integrals: given $\mu \in \mathbb{D}(\mathbb{X}, \mathbb{Z})$ and a compactly supported function $f\colon \mathbb{X} \to \mathbb{C}_p^\times$, we define

$$\mathop{\times\!\!\!\!\!\!\int}_{\mathbb{X}} f\, d\mu = \lim \prod_{\alpha \in I} f(x_\alpha, y_\alpha)^{\mu(U_\alpha)},$$

where the limit is taken over coverings as above.

Definition 129. Define the subset $\mathbb{D}_0(\mathbb{X}, \mathbb{Z})$ of $\mu \in \mathbb{D}(\mathbb{X}, \mathbb{Z})$ such that $\mu(\mathbb{X}_0) = 0$ (or, equivalently, $\mu(\Lambda_{\mathrm{prim}}) = 0$ for all $\mathbb{Z}_p$–lattices Λ of $\mathbb{Q}_p^2$). The *multiplicative Poisson transform* of $\mu \in \mathbb{D}_0(\mathbb{X}, \mathbb{Z})$ is the analytic function $J(\mu) \in \mathscr{A}^\times$ defined by

$$J(\mu)(\tau) = \mathop{\times\!\!\!\!\!\!\int}_{\mathbb{X}_0} (x\tau + y)\, d\mu(x, y).$$

Definition 129 gives rise to a $\mathrm{SL}_2(\mathbb{Z})$–equivariant function $J\colon \mathbb{D}_0(\mathbb{X}, \mathbb{Z}) \to \mathscr{A}^\times$. In fact, J becomes even Γ–equivariant modulo $p^{\mathbb{Z}}$. That is, regard

$$J\colon \mathbb{D}_0(\mathbb{X}, \mathbb{Z}) \to \mathscr{A}^\times / p^{\mathbb{Z}}$$

and observe that, for $\gamma \in \Gamma$,

$$J(\mu|\gamma)(\tau) = \mathop{\times\!\!\!\!\!\!\int}_{\mathbb{X}_0} (x\tau + y)\, d(\mu|\gamma)(x, y) = \mathop{\times\!\!\!\!\!\!\int}_{\mathbb{X}_0\gamma^{-1}} (x(\gamma\tau) + y)\, d\mu(x, y).$$

Decomposing

$$\mathbb{X}_0\gamma^{-1} = p^{m_1}U_1 \sqcup \cdots \sqcup p^{m_t}U_t$$

with $\mathbb{X}_0 = U_1 \sqcup \cdots \sqcup U_t$ as in lemma 126, we can write

$$\begin{aligned} J(\mu|\gamma)(\tau) &= \prod_{j=1}^{t} \mathop{\times\!\!\!\!\!\!\int}_{p^{m_j}U_j} (x(\gamma\tau) + y)\, d\mu(x, y) \equiv \prod_{j=1}^{t} \mathop{\times\!\!\!\!\!\!\int}_{U_j} (x(\gamma\tau) + y)\, d\mu(x, y) \\ &= \mathop{\times\!\!\!\!\!\!\int}_{\mathbb{X}_0} (x(\gamma\tau) + y)\, d\mu(x, y) = J(\mu)(\gamma\tau) \mod^\times p^{\mathbb{Z}}. \end{aligned}$$

Therefore,

$$J(\mu|\gamma)(\tau) = J(\mu)(\gamma\tau) = \big(J(\mu)|\gamma\big)(\tau).$$

5.3.6 Proof of corollary 118

Definition 130. We define

$$J_{\mathrm{DR}} = J(\mu_{\mathrm{DR}}) \in \mathrm{H}^1(\Gamma, \mathscr{A}^\times / p^{\mathbb{Z}}).$$

We have to check that the J_{DR} from definition 130 satisfies corollary 118.

Namely, we have morphisms

$$\begin{tikzcd}
\mathrm{H}^1(\Gamma, \mathscr{A}^\times/p^{\mathbb{Z}}) \arrow[r] & \mathrm{H}^2(\Gamma, p^{\mathbb{Z}}) & \mathrm{H}^1(\Gamma_0(p), p^{\mathbb{Z}}) \arrow[l, "\cong"'] \\
J_{\mathrm{DR}} \arrow[r, mapsto, dashed] & p^{\alpha_{\mathrm{DR}}} & p^{\varphi_{\mathrm{DR}}} \arrow[l, mapsto]
\end{tikzcd}$$

and, letting $\eta\colon \mathrm{H}^1(\Gamma, \mathscr{A}^\times/p^{\mathbb{Z}}) \to \mathrm{H}^1(\Gamma_0(p), p^{\mathbb{Z}})$ denote the composition, we have to check that $\eta(J_{\mathrm{DR}}) = p^{\varphi_{\mathrm{DR}}}$. To do so, we give an explicit description of the (inverse) morphism $\mathrm{H}^2(\Gamma, \mathbb{Z}) \to \mathrm{H}^1(\Gamma_0(p), \mathbb{Z})$. Given $\alpha \in \mathrm{Z}^2(\Gamma, \mathbb{Z})$, we consider the restrictions $\alpha|_{\mathrm{SL}_2(\mathbb{Z})} = d\kappa$ and $\alpha|_{\mathrm{SL}_2(\mathbb{Z})'} = d\kappa'$, where $\kappa \in \mathrm{C}^1(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$ and $\kappa' \in \mathrm{C}^1(\mathrm{SL}_2(\mathbb{Z})', \mathbb{Z})$. Since $\Gamma_0(p) = \mathrm{SL}_2(\mathbb{Z}) \cap \mathrm{SL}_2(\mathbb{Z})'$, we obtain

$$(\kappa - \kappa')|_{\Gamma_0(p)} \in \mathrm{H}^1(\Gamma_0(p), \mathbb{Z}).$$

Next, we want to describe $\eta(J_{\mathrm{DR}})$. Take two lifts $I_{\mathrm{DR}} \in \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}), \mathscr{A}^\times)$ and $I'_{\mathrm{DR}} \in \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z})', \mathscr{A}^\times)$ of J_{DR}. We can express

$$\eta(J_{\mathrm{DR}}) = \left.\frac{I_{\mathrm{DR}}}{I'_{\mathrm{DR}}}\right|_{\Gamma_0(p)},$$

so it remains to describe I_{DR} and I'_{DR} on $\Gamma_0(p)$. But

$$I_{\mathrm{DR}}(\gamma)(\tau) = \times\!\!\!\!\!\!\int_{\mathbb{X}_0} (x\tau + y)\, d\mu_{\mathrm{DR}}(x, y)$$

and

$$I'_{\mathrm{DR}}(\gamma)(\tau) = \times\!\!\!\!\!\!\int_{\mathbb{X}'_0} (x\tau + y)\, d\mu_{\mathrm{DR}}(x, y) \quad (\text{where } \mathbb{X}'_0 = (p\mathbb{Z}_p \times \mathbb{Z}_p)_{\mathrm{prim}}).$$

Now the key point is that $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{X}_0$ and $\mathrm{SL}_2(\mathbb{Z})'$ acts on $\mathbb{X}'_0$ and, using that

$$\mathbb{X}_0 \cap \mathbb{X}'_0 = p\mathbb{Z}_p \times \mathbb{Z}_p^\times, \quad \mathbb{X}_0 \setminus \mathbb{X}'_0 = \mathbb{Z}_p^\times \times \mathbb{Z}_p, \quad \mathbb{X}'_0 \setminus \mathbb{X}_0 = p(\mathbb{Z}_p^\times \times \mathbb{Z}_p),$$

we can express

$$\begin{aligned}
\frac{I_{\mathrm{DR}}(\gamma)(\tau)}{I'_{\mathrm{DR}}(\gamma)(\tau)} &= \frac{\times\!\!\!\!\!\!\int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p} (x\tau + y)\, d\mu_{\mathrm{DR}}(x, y)}{\times\!\!\!\!\!\!\int_{p(\mathbb{Z}_p^\times \times \mathbb{Z}_p)} (x\tau + y)\, d\mu_{\mathrm{DR}}(x, y)} \\
&= \times\!\!\!\!\!\!\int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p} p\, d\mu_{\mathrm{DR}}(\gamma) = p^{\varphi_{\mathrm{DR}}(\gamma)}
\end{aligned}$$

as desired.

Conjecture 131. *Let $\tau \in \mathcal{H}_p$ be an RM point of fundamental discriminant D such that $p \nmid D$. Let H denote the Hilbert class field of $\mathbb{Q}(\tau)$. The RM value $J_{\mathrm{DR}}[\tau]$ belongs to $(\mathscr{O}_H[p^{-1}])^\times$.*

This conjecture has not been proved yet, but we have partial results in this direction:

Theorem 132. *In the setting of conjecture 131, we have*

$$J_{\mathrm{DR}}[\tau] \in (\mathscr{O}_H[p^{-1}])^\times \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Remark. There are two approaches to prove this kind of results: one by Dasgupta and Kakde using a tame refinement of the Gross–Stark conjectures and another by Darmon, Pozzi and Vonk using modular generating series. We will see the latter.

5.4 Elliptic cocycles

The main idea now is to replace $E_2^{(p)}$ with some cusp form of weight 2 and level $\Gamma_0(p)$. Let E be an elliptic curve over $\mathbb{Q}$ of conductor p, which by modularity corresponds to $f_E \in S_2(\Gamma_0(p))$. We obtain a homomorphism $\varphi_E \colon \Gamma_0(p) \to \mathbb{C}$ defined by

$$\varphi_E(\gamma) = \int_{z_0}^{\gamma(z_0)} 2\pi i f_E(z)\, dz$$

(for some base point $z_0 \in \mathcal{H}$), whose image is "essentially" the period lattice of E. At least we can get periods $\Omega_E^+, \Omega_E^- \in \mathbb{R}$ such that $\Omega_E^+\mathbb{Z} \oplus i\Omega_E^-\mathbb{Z}$ contains the image of φ_E. We define two $\mathbb{Z}$–valued morphisms

$$\varphi_E^+ = \frac{1}{\Omega_E^+} \operatorname{Re}(\varphi_E) \quad \text{and} \quad \varphi_E^- = \frac{1}{\Omega_E^-} \operatorname{Im}(\varphi_E).$$

In this way, we obtain $\alpha_E^+, \alpha_E^- \in \mathrm{H}^2(\Gamma, \mathbb{Z})$ (exactly as we defined α_{DR} from φ_{DR} in section 5.3, using $\delta \colon \mathrm{H}^1(\Gamma_0(p), \mathbb{Z}) \hookrightarrow \mathrm{H}^2(\Gamma, \mathbb{Z})$).

Theorem 133. *In the situation above, there exists $q \in p\mathbb{Z}_p$ (depending on E) satisfying that*

(1) *the cohomology class $q^{\alpha_E^\pm} \in \mathrm{H}^2(\Gamma, q^{\mathbb{Z}})$ becomes trivial in $\mathrm{H}^2(\Gamma, \mathscr{A}^\times)$ and*
(2) *the Tate curve $\mathbb{G}_{\mathrm{m}}/q^{\mathbb{Z}}$ is isogenous to E over $\mathbb{Q}_p$.*

Corollary 134. *There exist* 1*–cochains* $J_E^+, J_E^- \in \mathrm{C}^1(\Gamma, \mathscr{A}^\times)$ *such that*

$$\gamma_1 J_E^\pm(\gamma_2) \cdot J_E^\pm(\gamma_1\gamma_2)^{-1} \cdot J_E^\pm(\gamma_1) = q^{\alpha_E^\pm(\gamma_1,\gamma_2)}$$

for all $\gamma_1, \gamma_2 \in \Gamma$.

Definition 135. The classes J_E^+ and J_E^- of $\mathrm{H}^1(\Gamma, \mathscr{A}^\times/q^{\mathbb{Z}})$ given by corollary 134 are called the *even* and *odd*, respectively, *rigid analytic θ–cocycles associated with E*.

Let τ be an RM point with fundamental discriminant D such that $p \nmid D$. From these two cocycles, we obtain the RM values $J_E^\pm[\tau] \in \mathbb{C}_p^\times/q^{\mathbb{Z}}$ that we can view inside $E(\mathbb{C}_p)$.

Conjecture 136. *Let* H *(resp.* H^+*) be the Hilbert class field (resp. the narrow Hilbert class field) of* $\mathbb{Q}(\tau)$.

(1) *The value* $J_E^+[\tau]$ *belongs to* $E(H)$.

(2) *The value* $J_E^-[\tau]$ *belongs to* $E(H^+)$ *and, in fact, to the* (-1)*–eigenspace of complex conjugation.*

These RM values would (conjecturally) provide a large supply of $\overline{\mathbb{Q}}$–rational points of E called *Stark–Heegner points*.

5.4.1 Modular symbols

The homomorphisms $\varphi_E^\pm$ from section 5.4 can be described by *modular symbols*, which are functions $m_E\colon \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \to \mathbb{Z}$ satisfying that

$$m_E(r,s) = -m_E(s,r) \quad \text{and} \quad m_E(r,s) + m_E(s,t) = m_E(r,t)$$

for all $r, s, t \in \mathbb{P}^1(\mathbb{Q})$. For example, let us focus on φ_E^+. We define

$$m_E(r,s) = \frac{1}{\Omega_E^+} \mathrm{Re}\left(\int_r^s 2\pi i f_E(z)\, dz \right) \in \mathbb{Z}$$

(we might have to slightly modify the period Ω_E^+ to obtain a $\mathbb{Z}$–valued function) and then

$$\varphi_E^+(\gamma) = m_E(r, \gamma(r)) \quad \text{for any } r \in \mathbb{P}^1(\mathbb{Q}).$$

Let $\mathrm{MS}(\mathbb{Z})$ denote the $\mathbb{Z}$–module of $\mathbb{Z}$–valued modular symbols for Γ. Another way to express the last equation is saying that φ_E^+ (and similarly φ_E^-) is in the image of a "connecting homomorphism"

$$\delta\colon \mathrm{MS}(\mathbb{Z})^{\Gamma_0(p)} \to \mathrm{H}^1(\Gamma_0(p), \mathbb{Z}).$$

5.4.2 The construction of $J_E^{\pm}$

Consider again the Bruhat–Tits tree $\mathcal{T}$ and recall how Γ acts on its vertices and edges from lemma 116.

Lemma 137. *There exists a collection $(m_e)_{e\in\vec{\mathcal{T}}_1}$ of modular symbols $m_e \in \mathrm{MS}(\mathbb{Z})$ such that, for every $r, s \in \mathbb{P}^1(\mathbb{Q})$,*

(1) *$m_{e^*}(r,s) = m_E(r,s)$,*

(2) *$m_{\gamma(e)}(\gamma(r),\gamma(s)) = m_e(r,s)$ for all $\gamma \in \Gamma$ and*

(3) *$m_{\bar{e}}(r,s) = -m_e(r,s)$.*

Proof. Since Γ acts transitively on unordered edges, these three properties determine completely the collection $(m_e)_{e\in\vec{\mathcal{T}}_1}$ so long as they do not give rise to "contradictions". But m_E is invariant under $\mathrm{Stab}_\Gamma(e^*) = \Gamma_0(p)$. □

As in section 5.4.1, we continue to focus on the + versions of all cocycles. Fix $r, s \in \mathbb{P}^1(\mathbb{Q})$. One can check that the map $e \mapsto m_e(r,s)$ is a harmonic cocycle on $\mathcal{T}$ and, by (the proof of) theorem 110, we obtain a measure $\mu(r,s)$ on $\mathbb{P}^1(\mathbb{Q}_p)$ with Poisson transform

$$F_E(r,s)(z) = \int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{d(\mu(r,s))(t)}{z-t}.$$

Varying r and s, we obtain $F_E \in \mathrm{MS}(\mathscr{A}_2)^\Gamma$, where $\mathscr{A}_2$ is the group of rigid analytic functions on $\mathcal{H}_p$ with an action of Γ of weight 2 given by

$$(F|\gamma)(z) = (cz+d)^{-2}\, F\Big(\frac{az+b}{cz+d}\Big) \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

Our goal is to define cocycles with values in $\mathscr{A}^\times/\mathbb{C}_p^\times$, so we just need to find "preimages" under $\mathrm{dlog}\colon \mathscr{A}^\times/\mathbb{C}_p^\times \to \mathscr{A}_2\, dz$. We already did that in section 5.3.5. Thus, we define

$$J_E^+(r,s)(z) = \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{d(\mu_E(r,s))(t)}{z-t},$$

which gives rise to $J_E^+ \in \mathrm{MS}(\mathscr{A}^\times/\mathbb{C}_p^\times)^\Gamma$.

It remains to prove that J_E^+ lifts to a class in $\mathrm{MS}(\mathscr{A}^\times/q^{\mathbb{Z}})^\Gamma$. If J_E^+ lifts to $\mathrm{MS}(\mathscr{A}^\times/G)^\Gamma$, where G denotes any subgroup of $\mathbb{C}_p^\times$, then we should be able to write

$$J_E^+(\gamma(r),\gamma(s))(\gamma(z)) \equiv J_E^+(r,s)(z) \bmod^\times G$$

for all $r, s \in \mathbb{P}^1(\mathbb{Q})$ and all $\gamma \in \Gamma$. (Of course, the previous equation is not well defined because $J_E^+ \in \mathrm{MS}(\mathscr{A}^\times/\mathbb{C}_p^\times)^\Gamma$.) In particular, taking $(r,s) = (0,\infty)$ and

$$\gamma = \begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix} \in \Gamma,$$

we would have

$$J_E^+(0,\infty)(p^2 z) \equiv J_E^+(0,\infty)(z) \bmod^\times G.$$

This motivates the need to study the period

$$Q = \frac{J_E(0,\infty)(p^2 z)}{J_E(0,\infty)(z)} \in \mathbb{Q}_p^\times$$

(well-defined).

Lemma 138. *In the situation above,*

(1) $\mathrm{v}_p(Q) = \frac{1}{\Omega_E^+} L(E,1)$ *and*

(2) $\log_p(Q) = L_p'(E,1)$ *(where $L_p(E,\,\cdot\,)$ is the Mazur–Swinnerton-Dyer p–adic L–function of E).*

Idea of the proof. The first claim is a direct calculation using the definition of $L(E,\,\cdot\,)$ as a Mellin transform (i.e., an integral). The second claim follows from the theorem of Greenberg–Stevens (proving a conjecture of Mazur–Tate–Teitelbaum) which states that

$$\Omega_E^+ \frac{L_p'(E,1)}{L(E,1)} = \frac{\log_p(q_E)}{\mathrm{v}_p(q_E)}.$$

Greenberg and Stevens proved this formula using deformations of Galois representations along a Hida family. □

5.5 Lifting obstructions

Recall that when we had a discrete action of Γ on $\mathcal{H}_p$ we could construct a map $\mathrm{AJ}\colon \mathrm{Div}^0(\mathcal{H}_P) \to \mathrm{H}^1(\Gamma, \mathbb{C}_p^\times)$ given by

$$\mathrm{AJ}(\mathcal{D})(\gamma) = [\mathcal{D}; (\gamma z) - (z)]_\Gamma$$

(see section 4.4.9). More precisely, $\mathrm{AJ}(\mathcal{D})$ is the "lifting obstruction" of a class $\theta_{\mathcal{D}}(z) \in \mathrm{H}^0(\Gamma, \mathscr{M}^\times/\mathbb{C}_p^\times)$.

We can imitate this construction for the action of $\Gamma = \mathrm{SL}_2(\mathbb{Z}[p^{-1}])$ on the RM points of $\mathcal{H}_p$ after shifting the cohomological degree by 1. Consider an RM point $\tau \in \mathcal{H}_p$ with fundamental discriminant D such that $p \nmid D$. We will define a meromorphic θ–cocycle $J_\tau \in \mathrm{H}^1(\Gamma, \mathscr{M}^\times/\mathbb{C}_p^\times)$ and $\mathrm{AJ}(\tau) = \delta(J_\tau) \in \mathrm{H}^2(\Gamma, \mathbb{C}_p^\times)$.

Our next goal is to define the rigid meromorphic θ–cocycle $J_\tau \in \mathrm{H}^1(\Gamma, \mathscr{M}^\times/\mathbb{C}_p^\times)$ "having poles and zeros at $\Gamma\tau$". By assumption, the point $\tau \in \mathcal{H}_p$ satisfies an equation

$$a\tau^2 + b\tau + c = 0 \quad \text{with } a, b, c \in \mathbb{Z}$$

and $D = \mathrm{disc}(\tau) = b^2 - 4ac > 0$. We assume moreover that

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

5.5.1 Discrete divisors

Consider the p–adic upper half-plane $\mathcal{H}_p$ and its Bruhat–Tits tree $\mathcal{T} = (\mathcal{T}_0, \mathcal{T}_1)$. Let red: $\mathcal{H}_p \to \mathcal{T}$ denote the reduction map from proposition 80.

Recall that a formal divisor

$$\mathcal{D} = \sum_{x \in \mathcal{H}_p} m_x(x)$$

is *discrete* if, for every affinoid $\mathcal{A} \subset \mathcal{H}_p$, the formal sum

$$\mathcal{D} \cap \mathcal{A} = \sum_{x \in \mathcal{A}} m_x(x)$$

is a genuine divisor (i.e., a finite sum). We say that $\mathcal{D}$ *has degree* 0 if $\mathcal{D} \cap \mathcal{A}$ has for all affinoids $\mathcal{A} \subset \mathcal{H}_p$. In particular, when we have a group Γ acting discretely over $\mathcal{H}_p$, then

$$\mathcal{D}_\tau = \sum_{w \in \Gamma\tau} (w)$$

is a discrete divisor. However, the Ihara group $\Gamma = \mathrm{SL}_2(\mathbb{Z}[p^{-1}])$ does not act discretely on $\mathcal{H}_p$ and

$$\mathcal{D}_\tau = \sum_{w \in \Gamma\tau} (w)$$

is *not* discrete because (for example, assuming that $\mathrm{red}(\tau) = v^*$)

$$\mathcal{D}_\tau \cap \mathrm{red}^{-1}(v^*) = \sum_{w \in \mathrm{SL}_2(\mathbb{Z})\tau} (w)$$

is not a finite sum.

We will construct a discrete divisor as follows. Fix $r, s \in \mathbb{P}^1(\mathbb{Q})$. For every RM point $w \in \mathcal{H}_p$, let w' denote its conjugate. Write $(w, w') \cdot (r, s)$ for the topological intersection number of the geodesic from w to w' and the geodesic from r to s on the archimedean upper half-plane $\mathcal{H}$, which is a number in $\{0, \pm 1\}$. We define

$$\mathcal{D}_\tau = \sum_{w \in \Gamma\tau} \big[(w, w') \cdot (r, s)\big](w).$$

Proposition 139. *The divisor $\mathcal{D}_\tau(r,s)$ defined above is a discrete divisor of degree* 0.

Proof. Since $p \nmid D$, we can express

$$\Gamma\tau = \bigcup_{v \in \mathcal{T}_0} \big((\Gamma\tau) \cap \mathrm{red}^{-1}(v)\big).$$

Given $v \in \mathcal{T}_0$, set $\mathcal{A}_v = \mathrm{red}^{-1}(v)$. It suffices to show that $\mathcal{D}_\tau(r,s) \cap \mathcal{A}_v$ is a divisor of degree 0. By definition,

$$\mathcal{D}_\tau(r,s) \cap \mathcal{A}_v = \sum_{w \in \Gamma\tau \cap \mathcal{A}_v} \big[(w, w') \cdot (r, s)\big](w)$$

and, up to replacing τ with another representative of $\Gamma\tau$, we may assume that $\mathrm{red}(\tau) = v$. As $\Gamma_v = \mathrm{Stab}_\Gamma(v)$ is conjugate to $\mathrm{SL}_2(\mathbb{Z})$,

$$\mathcal{D}_\tau(r,s) \cap \mathcal{A}_v = \sum_{w \in \Gamma_v\tau} \big[(w, w') \cdot (r, s)\big](w) = \sum_{\gamma \in \Gamma_v / \gamma_\tau^{\mathbb{Z}}} \big[(\gamma\tau, \gamma\tau') \cdot (r, s)\big](\gamma\tau),$$

where γ_τ is a generator of $\mathrm{Stab}_{\Gamma_v}(\tau)$. Assume that, for every point z_0 (other than the endpoints) of the geodesic (τ, τ') in $\mathcal{H}$,

$$\gamma_\tau^{\infty} z_0 = \tau' \quad \text{and} \quad \gamma_\tau^{-\infty} z_0 = \tau$$

(i.e., τ is a repulsive fixed point and τ' is an attractive fixed point), so that we can decompose

$$(\tau, \tau') = \sum_{j \in \mathbb{Z}} (\gamma_\tau^j z_0, \gamma_\tau^{j+1} z_0).$$

Then

$$\begin{aligned} \mathcal{D}_\tau(r,s) &= \sum_{\gamma \in \Gamma_v / \gamma_\tau^{\mathbb{Z}}} \sum_{j \in \mathbb{Z}} \big[(\gamma\gamma_\tau^j z_0, \gamma\gamma_\tau^{j+1} z_0) \cdot (r,s)\big](\gamma\tau) \\ &= \sum_{\gamma \in \Gamma_v} \big[(\gamma z_0, \gamma\gamma_\tau z_0) \cdot (r,s)\big](\gamma\tau). \end{aligned}$$

But

$$\sum_{\gamma \in \Gamma_v} (\gamma z_0, \gamma\gamma_\tau z_0) \cdot (r,s)$$

is the topological intersection number of the projections of $(z_0, \gamma_\tau z_0)$ and (r,s) onto $\Gamma_v\backslash\mathcal{H}$. Therefore, $\mathcal{D}_\tau(r,s) \cap \mathcal{A}_v$ is a divisor and it has degree 0 because $\Gamma_v\backslash\mathcal{H}$ has genus 0. □

Let $\mathrm{Div}^{0,\dagger}(\mathcal{H}_p)$ be the group of discrete divisors of degree 0 on $\mathcal{H}_p$. Observe that the map

$$(r,s) \mapsto \mathcal{D}_\tau(r,s)$$

defines an element $\mathcal{D}_\tau \in \mathrm{MS}(\mathrm{Div}^{0,\dagger}(\mathcal{H}_p))^\Gamma$. Moreover, for a fixed $v \in \mathcal{T}_0$, the map

$$(r,s) \mapsto \deg\big(\mathcal{D}_\tau(r,s) \cap \mathcal{A}_v\big)$$

defines an element of $\mathrm{MS}(\mathbb{Z})^{\Gamma_v}$. We define

$$J_\tau(r,s)(z) = [(z) - (\eta); \mathcal{D}_\tau(r,s)] = \lim_{\mathcal{A}\to\mathcal{H}_p} [(z) - (\eta); \mathcal{D}_\tau(r,s) \cap \mathcal{A}]$$

(for some base point $\eta \in \mathcal{H}_p$), where the limit is taken over affinoids $\mathcal{A}$ of an increasing admissible covering of $\mathcal{H}_p$ and converges absolutely. One can check that $J_\tau(r,s) \in \mathscr{M}^\times$ and so $J_\tau \in \mathrm{MS}(\mathscr{M}^\times)$. Moreover, for every $\gamma \in \Gamma$,

$$\begin{aligned} J_\tau(\gamma r, \gamma s)(\gamma z) &= [(\gamma z) - (\eta); \mathcal{D}_\tau(\gamma r, \gamma s)] = [(\gamma z) - (\eta); \gamma\mathcal{D}_\tau(r,s)] \\ &= [(z) - (\gamma^{-1}\eta); \mathcal{D}_\tau(r,s)] = J_\tau(r,s)(z) \cdot [(\eta) - (\gamma^{-1}\eta); \mathcal{D}_\tau(r,s)], \end{aligned}$$

whence we can view $J_\tau \in \mathrm{MS}(\mathscr{M}^\times/\mathbb{C}_p^\times)^\Gamma$ or $J_\tau \in \mathrm{H}^1_{\mathrm{par}}(\Gamma, \mathscr{M}^\times/\mathbb{C}_p^\times)$.

5.5.2 Stark–Heegner points as lifting obstructions

Consider the composition

$$\begin{tikzcd} \mathrm{H}^1_{\mathrm{par}}(\Gamma_0(p), \mathbb{Z}) \arrow[r, dashed, "i"] \arrow[d] & \mathrm{H}^1_{\mathrm{par}}(\Gamma_0(p), \mathbb{C}_p^\times) \arrow[d, "\cong"] \\ \mathrm{H}^1_{\mathrm{par}}(\Gamma, \mathscr{A}^\times/\mathbb{C}_p^\times) \arrow[r, hook] & \mathrm{H}^2_{\mathrm{par}}(\Gamma, \mathbb{C}_p^\times) \end{tikzcd}$$

and define the *period lattice*

$$\Lambda = i\big(\mathrm{H}^1_{\mathrm{par}}(\Gamma_0(p), \mathbb{Z})\big) \subseteq \mathrm{H}^1(\Gamma_0(p), \mathbb{C}_p^\times),$$

which is a discrete lattice.

Conjecture 140. *The rigid analytic torus* $\mathrm{H}^2(\Gamma, \mathbb{C}_p^\times)/\Lambda$ *is isogenous to* $J_0(p)^2$ *over* $\mathbb{Q}_{p^2}$*, where* $J_0(p)$ *is the jacobian of* $X_0(p)$*.*

Consider the connecting homomorphism

$$\delta\colon \mathrm{H}^1(\Gamma, \mathscr{M}^\times/\mathbb{C}_p^\times) \to \mathrm{H}^2(\Gamma, \mathbb{C}_p^\times).$$

Then $\delta(J_\tau)$ should map to a point in $J_0(p)(H)^2 \otimes_{\mathbb{Z}} \mathbb{Q}$, where H is the Hilbert class field of $\mathbb{Q}(\tau)$.

When we had a group Γ acting discretely on $\mathcal{H}_p$ (in section 4), we had a diagram

$$\begin{tikzcd}
 & \mathrm{H}^0(\Gamma, \mathscr{A}^\times/\mathbb{C}_p^\times) \arrow[r, "\delta"] \arrow[d, hook] & \Lambda \arrow[d, hook] \\
\mathrm{H}^0(\Gamma, \mathscr{M}^\times) \arrow[r] \arrow[d, "\mathrm{div}"] & \mathrm{H}^0(\Gamma, \mathscr{M}^\times/\mathbb{C}_p^\times) \arrow[r, "\delta"] \arrow[d, "\mathrm{div}"] & \mathrm{H}^1(\Gamma, \mathbb{C}_p^\times) \arrow[d] \\
P(X_\Gamma) \arrow[r, hook] & \mathrm{Div}^{0,\dagger}(\mathcal{H}_p)^\Gamma \arrow[r] & \mathrm{Jac}(X)(\mathbb{C}_p)
\end{tikzcd}$$

in which the last column gives the obstructions to lift elements in the middle column. (Here, $P(X_\Gamma)$ means the principal divisors on X_Γ.)

Now, for $\Gamma = \mathrm{SL}_2(\mathbb{Z}[p^{-1}])$, we have an analogous diagram

$$\begin{tikzcd}
 & \mathrm{H}^1(\Gamma, \mathscr{A}^\times/\mathbb{C}_p^\times) \arrow[r] \arrow[d, hook] & \Lambda \arrow[d, hook] \\
\mathrm{H}^1(\Gamma, \mathscr{M}^\times) \arrow[r] \arrow[d] & \mathrm{H}^1(\Gamma, \mathscr{M}^\times/\mathbb{C}_p^\times) \arrow[r, "\delta"] \arrow[d] & \mathrm{H}^2(\Gamma, \mathbb{C}_p^\times) \arrow[d] \\
P \arrow[r, hook] & \mathrm{H}^1(\Gamma, \mathrm{Div}^{0,\dagger}(\mathcal{H}_p^{\mathrm{RM}})) \arrow[r] & \mathrm{Jac}(X_0(p))^2
\end{tikzcd}$$

(where the last vertical arrow is conjectural).

5.5.3 Real quadratic singular moduli

In the category of groups modulo torsion, we have an exact sequence

$$0 \longrightarrow \mathrm{H}^1(\Gamma, \mathscr{M}^\times) \longrightarrow \mathrm{H}^1(\Gamma, \mathscr{M}^\times/\mathbb{C}_p^\times) \longrightarrow \mathrm{H}^2(\Gamma, \mathbb{C}_p^\times)$$

and the middle group (which contains the $(J_\tau)_{\tau \in \mathcal{H}_p^{\mathrm{RM}}}$) is huge but the last one is not that big because every element is annihilated by Hecke operators in $\mathbb{T}_2(\Gamma_0(p))$.

In particular, if $p \in \{2, 3, 5, 7, 13\}$ (or, equivalently, $X_0(p)$ has genus 0), then $\mathrm{H}^2_{\mathrm{par}}(\Gamma, \mathbb{C}_p^\times)$ is finite and, up to torsion, every J_τ lifts to $\mathrm{H}^1(\Gamma, \mathscr{M}^\times)$.

Definition 141. The *real quadratic singular moduli associated with* τ_1 *and* τ_2 is the value $J_p(\tau_1, \tau_2) = J_{\tau_1}[\tau_2] \in \mathbb{C}_p^\times$.

Consider two RM points τ_1 and τ_2 in $\mathcal{H}_p$ with discriminants D_1 and D_2 such that $p \nmid D_1D_2$ and $(D_1, D_2) = 1$. The real quadratic singular moduli $J_p(\tau_1, \tau_2)$ from definition 141 should "behave like" the singular moduli $J_\infty(\tau_1, \tau_2) = j(\tau_1) - j(\tau_2)$ when τ_1 and τ_2 are CM points of $\mathcal{H}$ (see theorem 65). More precisely:

Conjecture 142. *The value* $J_p(\tau_1, \tau_2)$ *is defined in the compositum* H_1H_2 *of the Hilbert class fields* H_1 *and* H_2 *of* $\mathbb{Q}(\tau_1)$ *and* $\mathbb{Q}(\tau_2)$*, respectively.*

Conjecture 143. *Let* $\mathfrak{q}$ *be a prime ideal of* $\mathscr{O}_{H_1H_2}$ *lying over* $q \in \mathbb{Z}$*. If* $\mathfrak{q} \mid J_p(\tau_1, \tau_2)$*, then*

(1) $\left(\frac{D_1}{q}\right) \neq 1 \neq \left(\frac{D_2}{q}\right)$ *and*

(2) q *divides a positive integer of the form*

$$\frac{D_1D_2 - m^2}{4p} \quad \textit{(for some } m \in \mathbb{Z}\textit{).}$$

5.6 Algebraicity statements

Unlike the situation for Stark–Heegner points, the algebraicity of RM values of the forms $J_{\mathrm{DR}}[\tau]$ or $J_{\tau_1}[\tau_2]$ is somewhat tractable.

5.6.1 Gross–Zagier revisited

Theorem 144 (Gross–Zagier). *Let* τ_1 *and* τ_2 *be two CM points of discriminants* D_1 *and* D_2*, respectively, such that* $(D_1, D_2) = 1$*. We have a factorization*

$$\mathrm{N}_{H_1H_2/\mathbb{Q}}\big(j(\tau_1) - j(\tau_2)\big) = \prod_q q^{m_q},$$

where the product runs over the primes q *dividing a positive integer of the form*

$$\frac{D_1D_2 - n^2}{4} \quad \textit{with } n \in \mathbb{Z}$$

and such that

$$\left(\frac{D_1}{q}\right) \neq 1 \neq \left(\frac{D_2}{q}\right).$$

Gross and Zagier gave two proofs of this theorem: the "algebraic proof" that we saw in section 3.10 and an "analytic proof" which adapts better to the RM setting. We now explain the latter.

Let $D = D_1 D_2 > 0$ and set $F = \mathbb{Q}(\sqrt{D})$ (real quadratic field). Consider $L = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$, which is a biquadratic extension of $\mathbb{Q}$ containing F. The quadratic extension L/F is unramified and so is contained in the narrow Hilbert class field of F. We obtain a character

$$\psi = \psi_{D_1,D_2} \colon \mathrm{Cl}^+(F) \to \mathrm{Gal}(L/F) \cong \{\pm 1\},$$

known as the *genus character* attached to D_1 and D_2.

Fix an embedding $F \hookrightarrow \mathbb{R}$. Consider the Hilbert modular Eisenstein series

$$E_{k,\psi}(z, z') = \sum_{\mathfrak{a} \in \mathrm{Cl}^+(F)} \psi(\mathfrak{a}) \, \mathrm{N}(\mathfrak{a})^k \sum_{(m,n) \in \mathfrak{a}^2 / \mathscr{O}_F^\times} \frac{1}{(mz+n)^k (m'z'+n')^k},$$

where m' and n' are the conjugates of m and n, respectively, and $z, z' \in \mathfrak{h}$. There is an action of $\mathrm{SL}_2(\mathscr{O}_F)$ on $\mathfrak{h} \times \mathfrak{h}$ with respect to which $E_{k,\psi}$ is "almost invariant":

$$E_{k,\psi}\Big(\frac{az+b}{cz+d}, \frac{a'z'+b'}{c'z'+d'}\Big) = (cz+d)^k (c'z'+d')^k E_{k,\psi}(z,z').$$

We will also use the non-holomorphic but real-analytic versions

$$\begin{aligned} E_{k,s,\psi}(z,z') = &\sum_{\mathfrak{a} \in \mathrm{Cl}^+(F)} \psi(\mathfrak{a}) \, \mathrm{N}(\mathfrak{a})^k \cdot \\ &\cdot \sum_{(m,n) \in \mathfrak{a}^2 / \mathscr{O}_F^\times} \frac{1}{(mz+n)^k (m'z'+n')^k} \frac{\mathrm{Im}(z)^s \, \mathrm{Im}(z')^s}{|mz+n|^{2s} |m'z'+n'|^{2s}} \end{aligned}$$

for s in some right half-plane of $\mathbb{C}$. One can extend the definition to other values of s by analytic continuation.

Fact 145. *The function $E_{1,s,\psi}$ vanishes at $s = 0$.*

Set $G_s(\psi) = E_{1,s,\psi}(z,z) \in M_2(\mathrm{SL}_2(\mathbb{Z}))^{\mathrm{an}}$ (i.e., this diagonal restriction transforms like a modular form of weight 2 but is only real-analytic). By fact 145, $G_0(\psi) = 0$. Then we are interested in

$$G_0'(\psi) = \left[\frac{d}{ds} G_s(\psi)\right]\bigg|_{s=0} \in M_2(\mathrm{SL}_2(\mathbb{Z}))^{\mathrm{an}}.$$

Consider the holomorphic projection

$$\pi_{\mathrm{hol}} \colon M_2(\mathrm{SL}_2(\mathbb{Z}))^{\mathrm{an}} \to M_2(\mathrm{SL}_2(\mathbb{Z})) = 0.$$

From the definition of $E_{1,s,\psi}(z,z)$, one gets a q–expansion

$$\pi_{\mathrm{hol}}(G_0'(\psi)) = \sum_{n\geq 0} a_n q^n.$$

The main calculation in Gross–Zagier's article shows that

$$a_1 = \log\left|\mathrm{N}_{H_1H_2/\mathbb{Q}}\big(j(\tau_1) - j(\tau_2)\big)\right| - \sum_q m_q \log(q),$$

where the sum runs over the primes appearing in theorem 144. Then theorem 144 follows from the fact that $a_1 = 0$.

5.6.2 A p–adic analogue

Next we want to adapt the proof explained in section 5.6.1 to the RM setting using p–adic analytic methods. Let $F = \mathbb{Q}(\sqrt{D})$ be a real quadratic field and suppose that the prime p is inert in F. Let ψ be an odd character of the class group of F.

The q–expansion of the Hilbert modular Eisenstein series from section 5.6.1 is

$$E_{k,\psi} = L(F,\psi,1-k) + 4 \sum_{\nu\in\mathfrak{d}_+^{-1}} \sigma_{k-1,\psi}(\nu\mathfrak{d}) e^{2\pi i(\nu z + \nu' z')},$$

where $\mathfrak{d}^{-1}$ is the inverse different of F, $\mathfrak{d}_+^{-1}$ consists of the totally positive elements of $\mathfrak{d}^{-1}$ and

$$\sigma_{k-1,\psi}(\alpha) = \sum_{I|(\alpha)} \psi(I)\,\mathrm{N}(I)^{k-1}.$$

These functions are formed from algebraic quantities. To obtain a p–adically interpolable function, we consider the p–stabilization

$$E_{k,\psi}^{(p)} = E_{k,\psi}(z,z') - E_{k,\psi}(pz,pz') = L_p(F,\psi,1-k) + 4 \sum_{\nu\in\mathfrak{d}_+^{-1}} \sigma_{k-1}^{(p)}(\nu\mathfrak{d}) e^{2\pi i(\nu z + \nu' z')},$$

where

$$\sigma_{k-1}^{(p)}(\alpha) = \sum_{p\nmid I|(\alpha)} \psi(I)\,\mathrm{N}(I)^{k-1}.$$

Now the functions vary analytically in k. We can set

$$G_k(\psi) = E^{(p)}_{k,\psi}(z,z) \in M_{2k}(\Gamma_0(p))$$

and this yields a p–adic family of modular forms. In particular, $G_1(\psi) = 0$ in $M_2(\Gamma_0(p))$ and we can work with

$$G_1'(\psi) = \left[\frac{d}{ds} G_s(\psi)\right]\Bigg|_{s=1} \in M_2^{p-\mathrm{adic}}(\mathrm{SL}_2(\mathbb{Z})).$$

In this case, we have to use the ordinary projection

$$\pi_{\mathrm{ord}} = \lim_{n\to\infty} \mathrm{U}_p^{n!} \colon M_2^{p-\mathrm{adic}}(\mathrm{SL}_2(\mathbb{Z})) \to M_2(\Gamma_0(p)).$$

Theorem 146 (Darmon–Pozzi–Vonk). *Consider the q–expansion*

$$\pi_{\mathrm{ord}}(G_1'(\psi)) = \sum_{n\geq 0} a_n q^n \in M_2(\Gamma_0(p)).$$

There is a rigid analytic θ–cocycle J_W, called the winding cocycle, *such that*

$$a_1 = \sum_{\mathrm{disc}(\tau)=D} \psi(\tau)\log\big(J_W[\tau]J_W[\tau']\big),$$

where the sum runs over the RM points $\tau \in \Gamma\backslash\mathcal{H}_p$ of discriminant D.

5.6.3 The winding cocycle

The geodesic path $(0,\infty)$ from 0 to $i\infty$ on $\mathfrak{h}$ (or its projection) is called the *winding element* of $\mathrm{H}_1(X_0(p), \mathrm{cusps}, \mathbb{Z})$. By Poincaré duality, we view the winding element in $\mathrm{H}^1(\Gamma_0(p), \mathbb{Z})$; the winding cocycle J_W will be its image in $\mathrm{H}^1(\Gamma, \mathscr{A}^\times/\mathbb{C}_p^\times)$.

Let $\Gamma = \mathrm{SL}_2(\mathbb{Z}[p^{-1}])$. We can decompose

$$\Gamma(0,\infty) = \Sigma = \bigsqcup_{i\geq 0} \Sigma_i,$$

where

$$\Sigma_i = \left\{ \left(\frac{a}{b}, \frac{c}{d}\right) : ad - bc = \pm p^i \right\}$$

(writing all fractions in lowest terms). Choose base points $\eta_p \in \mathcal{H}_p$ and $\eta_\infty \in \mathcal{H}$.

We define $J_W \colon \Gamma \to \mathscr{A}^\times/\mathbb{C}_p^\times$ by

$$J_W(\gamma)(z) = \prod_{(r,s)\in\Sigma} [(z)-(\eta_p);(r)-(s)]^{(r,s)\cdot(\eta_\infty,\gamma\eta_\infty)}$$
$$= \prod_{i=0}^{\infty} \prod_{(r,s)\in\Sigma_i} [(z)-(\eta_p);(r)-(s)]^{(r,s)\cdot(\eta_\infty,\gamma\eta_\infty)}$$

for all $\gamma \in \Gamma$ and $z \in \mathcal{H}_p$. One checks that the products in the last expression converge absolutely. Unlike the cocycles J_{DR} or J_E, the winding cocycle J_W is not a Hecke eigenclass (but it is simpler geometrically!).

Theorem 147. *We have the q–expansion*

$$\pi_{\mathrm{ord}}(G_1'(\psi)) = L_p'(F,\psi,0) + 4\sum_{n\geq 1} \log_p\big(\mathrm{T}_n\, J_W[\Delta_\psi]\big)q^n,$$

where we evaluate $\mathrm{T}_n\, J_W$ *at the divisor on* $\Gamma\backslash\mathcal{H}_P$

$$\Delta_\psi = \sum_{\mathrm{disc}(\tau)=D} \psi(\tau)\cdot\big((\tau)+(\tau')\big)$$

(the last sum runs over the RM points $\tau \in \Gamma\backslash\mathcal{H}_p$ *of discriminant D).*

Theorem 147, which is proofed with a direct computation, is a more general version of theorem 146. To imitate the last part of section 5.6.1, we need another description of J_W.

Lemma 148. *We can express*

$$J_W = \frac{2}{p-1}J_{\mathrm{DR}} + \sum_{f \text{ eigen.}} L_{\mathrm{alg}}(f,1)J_f^-,$$

where the sum runs over the (normalized) cuspidal eigenforms f *of weight* 2 *and level* $\Gamma_0(p)$ *and* $L_{\mathrm{alg}}(f,1)$ *is a quotient of* $L(f,1)$ *by a real period.*

Idea of the proof. One can show that

$$(0,\infty) = \frac{2}{p-1}\varphi_{\mathrm{DR}} + \sum_{f\ \mathrm{eigen.}} L_{\mathrm{alg}}(f,1)\varphi_f^-.$$

The L–values appear as path integrals. □

Corollary 149. *We have a linear combination*

$$\pi_{\mathrm{ord}}(G_1'(\psi)) = \frac{-4}{p-1}\log_p\big(J_{\mathrm{DR}}[\Delta_\psi]\big)E_2^{(p)} + \sum_{f \textit{ eigen.}} L_{\mathrm{alg}}(f,1)\log_p\big(J_f^-[\Delta_\psi]\big)f.$$

Comparing the constant coefficients of the q–expansions, we see that

$$L_p'(F,\psi,0) = \log_p\big(J_{\mathrm{DR}}[\Delta_\psi]\big) \quad \text{(Kronecker limit formula).}$$

5.6.4 CM theory of Shimura–Taniyama

Let F be a totally real field with $[F:\mathbb{Q}] = d > 1$. Consider the discrete action of $\mathrm{SL}_2(\mathscr{O}_F)$ on $\mathfrak{h}^d = \mathfrak{h} \times \overset{(d)}{\cdots} \times \mathfrak{h}$. We can interpret $\mathrm{SL}_2(\mathscr{O}_F)\backslash\mathfrak{h}^d$ as the $\mathbb{C}$–points of a Hilbert modular surface X, which is a moduli space of abelian varieties A endowed with an embedding $\mathscr{O}_F \hookrightarrow \mathrm{End}(A)$. There are a number of *special points* on X corresponding to abelian varieties A with an embedding $\mathscr{O}_K \hookrightarrow \mathrm{End}(A)$ for a CM extension K/F.

Fact 150. *Given a Hilbert modular function ϕ and a special point x of X (corresponding to a CM field K), the value $\phi(x)$ lies in a class field of a* reflex field *of K.*

One can also study this kind of values via rigid cocycles. Let $\mathfrak{p}$ be a prime ideal of $\mathscr{O}_F$ and let $\Gamma = \mathrm{SL}_2(\mathscr{O}_F[\mathfrak{p}^{-1}])$. The action of Γ on the $\mathfrak{p}$–adic "upper half-plane" $\mathcal{H}_\mathfrak{p}$ is not discrete, but we can define *special points* to be the $\tau \in \mathcal{H}_\mathfrak{p}$ such that

(1) $F(\tau)$ is a totally real quadratic extension of F and

(2) $\mathrm{Stab}_\Gamma(\tau) \cong \mathbb{Z}^d$ up to torsion.

Then one can attach to each special point τ a cocycle $J_\tau \in \mathrm{H}^d(\Gamma, \mathscr{M}^\times/\mathbb{C}_p^\times)$ and one can study the lifting obstructions. It turns out that $\mathrm{H}^{d+1}(\Gamma, \mathbb{C}_p^\times)$ gives (conjecturally) a p–adic uniformization of an abelian variety. Eventually, there should be some analogue of the Gross–Zagier theory in this setting.

A Student presentations

The notes that I took of the student presentations are quite worse than the rest for a number of reasons, including my inability to take decent notes of talks based on slides. The following pages do not do justice to the quality of the actual presentations. The interested reader should watch the recordings instead.

A.1 Proof of theorem 22 (Jhan-Cyuan Syu)

Theorem 151 (Riemann–Roch). *Let C be a smooth projective algebraic curve over a field K. Fix an algebraic closure $\overline{K}$ of K. For every $D \in \operatorname{Div}(C)$,*

$$\ell(D) - \ell(\mathcal{K} - D) = \deg(D) - g + 1,$$

where

(1) *$\ell(D)$ is the dimension of the $\overline{K}$–vector space*

$$\mathcal{L}(D) = \{ f \in \overline{K}(C)^\times : \operatorname{div}(f) \geq -D \},$$

(2) *$\mathcal{K}$ is a canonical divisor of C and*

(3) *g is the genus of C.*

We are going to apply theorem 151 to an elliptic curve E/K to prove theorem 22.

Step 1. Construction of $x, y \in K(E)$.

Applying Riemann–Roch's theorem with the divisors

- $D = 0$: $\ell(0) - \ell(\mathcal{K}) = \deg(0)$ and so $\ell(\mathcal{K}) = 1$;
- $D = \mathcal{K}$: $\ell(\mathcal{K}) - \ell(0) = \deg(\mathcal{K})$ and so $\deg(\mathcal{K}) = 0$;
- $D = n[\mathcal{O}]$ for some $n \in \mathbb{Z}_{\geq 1}$: $\ell(n[\mathcal{O}]) - \ell(\mathcal{K} - n[\mathcal{O}]) = \deg(n[\mathcal{O}])$ and so $\ell(n[\mathcal{O}]) = n$ because $\deg(\mathcal{K} - n[\mathcal{O}]) < 0$.

We have seen that $\mathcal{L}(n[\mathcal{O}])$ has dimension n over $\overline{K}$. Next we claim that we can take a $\overline{K}$–basis of $\mathcal{L}(n[\mathcal{O}])$ formed of elements in $K(E)$ (i.e., of rational functions over K, not just over $\overline{K}$).

To descend from $\overline{K}$ to K, we consider the Galois action of G_K on $\mathcal{L}(n[\mathcal{O}])$. Take $v \in \mathcal{L}(n[\mathcal{O}])$. By continuity of the Galois action, $\operatorname{Stab}_{G_K}(v)$ is an open subgroup of G_K. Therefore, the action of G_K on v factors through $\operatorname{Gal}(L/K)$ for some finite Galois extension L/K. Write $\operatorname{Gal}(L/K) = \{ \sigma_1, \ldots, \sigma_m \}$ and take a

K–basis $v_1, \dots, v_m$ of L. Define

$$\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{pmatrix} = \begin{pmatrix} v_1^{\sigma_1} & v_1^{\sigma_2} & \cdots & v_1^{\sigma_m} \\ v_2^{\sigma_1} & v_2^{\sigma_2} & \cdots & v_2^{\sigma_m} \\ \vdots & \vdots & \ddots & \vdots \\ v_m^{\sigma_1} & v_m^{\sigma_2} & \cdots & v_m^{\sigma_m} \end{pmatrix} \cdot \begin{pmatrix} v^{\sigma_1} \\ v^{\sigma_2} \\ \vdots \\ v^{\sigma_m} \end{pmatrix}.$$

It is clear that $\mathrm{Gal}(L/K)$ acts trivially on each w_i, which means that $w_i \in K(E)$. Moreover, the matrix above is invertible and so v can be expressed as an L–linear combination of the w_i. Applying this argument to each element of a $\overline{K}$–basis of $\mathcal{L}(n[\mathcal{O}])$, we obtain generators of $\mathcal{L}(n[\mathcal{O}])$ that are already defined over K.

Now take $x, y \in K(E)$ such that

$$\mathcal{L}(2[\mathcal{O}]) = \overline{K} \cdot 1 \oplus \overline{K} \cdot x \quad \text{and} \quad \mathcal{L}(3[\mathcal{O}]) = \overline{K} \cdot 1 \oplus \overline{K} \cdot x \oplus \overline{K} \cdot y.$$

Step 2. Properties of x and y.

Since $x \notin \mathcal{L}([\mathcal{O}])$ and $y \notin \mathcal{L}(2[\mathcal{O}])$, we deduce from the definition of $\mathcal{L}(\,\cdot\,)$ that

$$\mathrm{ord}_{\mathcal{O}}(x) = -2 \quad \text{and} \quad \mathrm{ord}_{\mathcal{O}}(y) = -3$$

and there are no other poles.

In $\mathcal{L}(6[\mathcal{O}])$ we have the seven elements 1, x, y, x^2, xy, x^3 and y^2 which must satisfy a non-trivial relation, say

$$a_1 + a_2 x + a_3 y + a_4 x^2 + a_5 xy + a_6 x^3 + a_7 y^2 = 0 \quad \text{with } a_6, a_7 \neq 0.$$

The change of coordinates

$$(x, y) \mapsto (-a_6 a_7 x, a_6^2 a_7)$$

allows us to rewrite the equation as

$$y_2 + A_1 xy + A_3 y = x^3 + A_2 x^2 + A_4 x + A_6.$$

Since $2 \in K^\times$, after the change of coordinates

$$(x, y) \mapsto \Big(x, \frac{1}{2}(y - A_1 x - A_3)\Big)$$

we obtain an equation of the form

$$y^2 = 4x^3 + B_2x^2 + B_4x + B_6.$$

Finally, since $6 \in K^\times$, we can apply the change of coordinates

$$(x, y) \mapsto \Big(\frac{x - 3B_2}{36}, \frac{y}{108}\Big)$$

to obtain an equation of the form

$$y^2 = x^3 + c_4x + c_6.$$

The canonical equation $y^2 = x^3 + g_4x + g_6$ is obtained by rescaling

$$(x, y) \mapsto (\lambda^{-2}x, \lambda^{-3}y) \quad \text{for suitable } \lambda \in K^\times$$

so that

$$\omega = \frac{dx}{y}.$$

A.2 The ring of weak modular forms (Martí Roset)

Let R be a base ring with $6 \in R^\times$. We want to identify $\mathrm{WMF}(R) = R[g_4, g_6, \Delta^{-1}]$. To that aim, we are going to use theorem 22 (or rather, its generalization for rings in which 6 is invertible):

Theorem 22 (classification of framed elliptic curves). *Let K be a field in which 6 is invertible and let (E, ω) be a framed elliptic curve over K. There exists a unique pair of functions $x, y \in \mathscr{O}_E(E \setminus \{\, \mathcal{O}\, \})$ satisfying the following conditions:*

(1) $\mathrm{ord}_{\mathcal{O}}(x) = -2$ *and* $\mathrm{ord}_{\mathcal{O}}(y) = -3$*;*

(2) *x and y satisfy an equation of the form*

$$y^2 = x^3 + g_4x + g_6$$

for some $g_4, g_6 \in K$ with the property that $\Delta = 4g_4^3 + 27g_6^2 \in K^\times$, and

(3) $\omega = \dfrac{dx}{y}$.

From the unicity statement, we see that g_4 and g_6 define weak modular forms over R and the weak modular form $\Delta = 4g_4^3 + 27g_6^2$ has to be invertible. Our goal is to prove the following result:

Proposition 152. *The space* $\mathrm{WMF}(R)$ *is the R–algebra $R_0[g_4, g_6, \Delta^{-1}]$.*

The strategy to prove proposition 152 will be to identify $f \in \mathrm{WMF}(R)$ with its value at a *universal* framed elliptic curve over $R[g_4, g_6, \Delta^{-1}]$. (Here, universal means that every framed elliptic curve over an R–algebra can be obtained as a base change of it.)

Consider the functor $\mathrm{Ell}_R^+ \colon R\text{–Alg} \to \mathrm{Set}$ that sends an R–algebra S to the set $\mathrm{Ell}_R^+(S)$ of framed elliptic curves over S. A morphism of R–algebras $S \to S'$ is sent to the map $\mathrm{Ell}_R^+(S) \to \mathrm{Ell}_R^+(S')$ given by base change of framed elliptic curves by $S \to S'$.

Lemma 153. *The functor* Ell_R^+ *is represented by* $R[g_4, g_6, \Delta^{-1}]$ *(we view this ring abstractly as* $R[X, Y, 1/(4X^2 + 27Y^3)]$*).*

Proof. Let S be an R–algebra. By theorem 22, we can define a map

$$\begin{aligned} \mathrm{Ell}_{R_0}^+(R) &\longrightarrow \mathrm{Hom}_{R_0\text{–Alg}}\big(R_0[g_4, g_6, \Delta^{-1}], R\big) \\ (E, \omega)/R &\longmapsto \big(\psi = \psi_{(E,\omega)} \colon R_0[g_4, g_6, \Delta^{-1}] \to R\big) \end{aligned}$$

characterized by $\psi(g_4) = g_4(E, \omega)$ and $\psi(g_6) = g_6(E, \omega)$.

- Surjectivity. Given ψ, we can recover the framed elliptic curve by means of the equation
$$y^2 = x^3 + \psi(g_4)x + \psi(g_6).$$
- Injectivity. The isomorphism class of (E, ω) is completely determined by $g_4(E, \omega) = \psi(g_4)$ and $g_6(E, \omega) = \psi(g_6)$. □

Using lemma 153, we can redefine weak modular forms as follows. A weak modular form f over R is a rule assigning a value $f(S, \psi) \in S$ to every pair consisting of an R–algebra S and a morphism $\psi \colon R[g_4, g_6, \Delta^{-1}] \to S$ of R–algebras in a way that is compatible with base change: given $\varphi \colon S \to S'$,

$$f(S', \varphi \circ \psi) = \varphi(f(S, \psi)).$$

Proof of proposition 152. Let $f \in \mathrm{WMF}(R)$. Consider the *universal* morphism of R–algebras $\mathrm{id} \colon R[g_4, g_6, \Delta^{-1}] \to R[g_4, g_6, \Delta^{-1}]$. Then $f\big(R[g_4, g_6, \Delta^{-1}], \mathrm{id}\big)$ is an element $P = P(g_4, g_6, \Delta^{-1}) \in R[g_4, g_6, \Delta^{-1}]$. We claim that we can identify f with P. Indeed, for every pair $(S, \psi \colon R[g_4, g_6, \Delta^{-1}] \to S)$ as above,

$$\begin{aligned} f(S, \psi) &= f(S, \psi \circ \mathrm{id}) = \psi(f(S, \mathrm{id})) = \psi(P(g_4, g_6, \Delta^{-1})) \\ &= P(\psi(g_4), \psi(g_6), \psi(\Delta)^{-1}) = P(g_4(S, \psi), g_6(S, \psi), \Delta^{-1}(S, \psi)). \end{aligned}$$

Remark. A weak modular form is a natural transformation from Ell_R^+ to the forgetful functor R–Alg $\to$ Set and this proof is an application of Yoneda's lemma.

Alternatively, one can give an analytic proof of proposition 152.

Proposition 154. *Let f be a non-zero holomorphic modular form over $\mathbb{C}$ of weight k. Then*

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\,\mathrm{ord}_i(f) + \frac{1}{3}\,\mathrm{ord}_{e^{2\pi i/3}}(f) + \sum_{x \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*} \mathrm{ord}_x(f) = \frac{k}{12}.$$

Idea of the proof. This formula can be proved applying the residue theorem to the logarithmic derivative of f on a certain contour close to the boundary of a fundamental domain. □

Proposition 155. *The space of holomorphic modular forms over $\mathbb{C}$ is $\mathbb{C}[g_4, g_6]$.*

Sketch of the proof. Let f be a modular form of weight k. We argue by induction on k that $f \in \mathbb{C}[g_4, g_6]$. By the valence formula, the cases $k \leq 2$ are trivial. For $k \geq 4$, we can choose $a, b \in \mathbb{Z}_{\geq 0}$ such that $4a + 6b = k$. We can choose $\lambda \in \mathbb{C}$ such that $f - \lambda g_4^a g_6^b$ is a cusp form of weight k and then we apply the induction hypothesis to $h = (f - \lambda g_4^a g_6^b)/\Delta$. □

Remark. Proposition 155 can be refined using the q–expansion principle to obtain a presentation for $\mathrm{MF}(R)$ for any subring R of $\mathbb{C}$ with $6 \in R^\times$. Then by base change one may pass to any general ring in which 6 is invertible.

A.3 The class number one problem (Dhruva Kelkar)

Let $K = \mathbb{Q}(\sqrt{n})$ for some square-free $n \in \mathbb{Z} \setminus \{0, 1\}$. Write

$$D_K = \begin{cases} n & \text{if } n \equiv 1 \mod 4 \\ 4n & \text{if } n \equiv 2 \text{ or } 3 \mod 4 \end{cases}$$

for the discriminant of K. The maximal order in K is its ring of integers, which admits a basis of the form $1, w_K$ with

$$w_K = \frac{D_K + \sqrt{D_K}}{2}.$$

Every other order $\mathcal{O}$ is of the form $\mathbb{Z} + \mathfrak{f} w_K \mathbb{Z}$ for some $\mathfrak{f} \in \mathbb{Z}_{\geq 1}$ called the *conductor* of $\mathcal{O}$.

Proposition 156. *The class numbers $h(\mathscr{O})$ of $\mathscr{O}$ and $h(\mathscr{O}_K)$ of $\mathscr{O}_K$ are related by*

$$h(\mathscr{O}) = \frac{h(\mathscr{O}_K)\mathfrak{f}}{[\mathscr{O}_K^\times : \mathscr{O}^\times]} \prod_{p|\mathfrak{f}} \left(1 - \left(\frac{D_K}{p}\right) \cdot \frac{1}{p}\right),$$

where

$$\left(\frac{D_K}{p}\right)$$

denotes the Legendre symbol.

Our goal is to obtain all orders of class number 1. Write D for the discriminant of the order $\mathscr{O}$ and $h(D) = h(\mathscr{O})$ for its class number.

The theory of binary quadratic forms yields the following results:

Proposition 157. *Let $n \in \mathbb{Z}_{\geq 1}$. The class number $h(-4n)$ is 1 if and only if*

$$n \in \{1, 2, 3, 4, 7\}.$$

Proposition 158. *Let $n \in \mathbb{Z}_{\geq 1}$. If n has at least two odd prime factors, the class number $h(-n)$ is even.*

Using these two results, our problem is reduced to the study of $h(-p)$ for p prime. More precisely, we have to determine when $h(-p) = 1$.

Next, we can deal with the case $p \equiv 7 \bmod 8$: taking

$$\mathscr{O}_K = \mathbb{Z} + \frac{1 + \sqrt{-p}}{2}\mathbb{Z} \quad \text{and} \quad \mathscr{O} = \mathbb{Z} + \sqrt{-p}\mathbb{Z},$$

one checks with proposition 156 that $h(-p) = h(-4p)$ and proposition 157 gives us the complete list of possibilities.

Finally, the most interesting case is $p \equiv 3 \bmod 8$. The theory of complex multiplication implies that the ring class field of conductor $\mathscr{O}$ is generated by $j(\mathfrak{a})$ for any invertible fractional ideal $\mathfrak{a}$ of $\mathscr{O}$. One can define a cubic root $\gamma_2(z)$ of $j(z)$ and Weber's functions $f(z)$, $f_1(z)$ and $f_2(z)$ and prove several algebraic relations between them. The problem is thus reduced to certain diophantine equations using integral values of modular functions.

A.4 Endomorphisms of elliptic curves over finite fields (Cédric Dion)

Let K be a field and let E_1 and E_2 be two elliptic curves over K. An isogeny $\psi \colon E_1 \to E_2$ corresponds to a morphism of fields $\psi^* \colon K(E_2) \hookrightarrow K(E_1)$ via which we can see $K(E_1)$ as a finite extension of $\psi^*(K(E_2))$.

Definition 159. The isogeny $\psi\colon E_1 \to E_2$ is called *separable* (resp. *inseparable*) if it induces a separable (resp. inseparable) extension $K(E_1)/\psi^*(K(E_2))$ of fields. We define the *degree* (resp. *separable degree*, *inseparable degree*) of ψ to be the degree (resp. separable degree, inseparable degree) of $K(E_1)/\psi^*(K(E_2))$.

Proposition 160. *Given an isogeny $\psi\colon E_1 \to E_2$, the kernel of ψ has exactly $\deg_s(\psi)$ $\overline{K}$–rational points.*

From now on, suppose that K has characteristic $p > 0$. Let $q = p^f$ for some $f \in \mathbb{Z}_{\geq 1}$. For every elliptic curve E/K, we can define the (relative) q–th power Frobenius morphism

$$\phi_q\colon E \to E^{(q)}.$$

Proposition 161. *In the situation above, the isogeny ϕ_q is purely inseparable of degree q.*

Corollary 162. *In the situation above, either $E[p](\overline{K}) = 0$ or $E[p](\overline{K}) \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof. We can count the number of p–torsion points of E as follows:

$$|E[p](\overline{K})| = |\mathrm{Ker}([p])(\overline{K})| = \deg_s[p] = \deg_s(\phi_p^* \circ \phi_p) = \deg_s \phi_p^*.$$

The last degree divides p, so it is either 1 or p. □

Finally, we want to prove theorem 46. In fact, we prove the following version of the theorem:

Theorem 163. *Let E/K be an elliptic curve. The following assertions are equivalent:*

(1) *$E[p](\overline{K}) = 0$;*
(2) *$[p]\colon E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$, and*
(3) *$\mathrm{End}_{\overline{K}}(E)$ is an order in a quaternion algebra.*

Proof. The proof of corollary 162 shows that $E[p](\overline{K}) = 0$ if and only if ϕ_p^* (and so $[p]$) is purely inseparable. In that case, $\phi_p^*\colon E^{(p)} \to E$ has to factor through $\phi_p\colon E^{(p)} \to E^{(p^2)}$, which is only possible if $E^{(p^2)} \cong E$. Therefore,

$$j(E)^{p^2} = j(E)$$

and we conclude that $j(E) \in \mathbb{F}_{p^2}$.

Next, let us prove that (2) implies (3). Suppose, for the sake of contradiction, that $\mathrm{End}_{\overline{K}}(E)$ is either $\mathbb{Z}$ or an order in a quadratic imaginary field. Choose a prime

$\ell \neq p$ such that, for every E' isogenous to E, ℓ is a prime in $\mathrm{End}_{\overline{K}}(E')$. We can take a compatible sequence of cyclic subgroups C_n of E of order $\mathbb{Z}/\ell^n\mathbb{Z}$, which induce isogenous curves $E_n = E/C_n$. Since there are only finitely many such curves (up to isomorphism), there exist $m, n \in \mathbb{Z}_{\geq 1}$ such that $E_{m+n} \cong E_m$. Thus, we obtain an endomorphism $E_m \to E_{m+n} \cong E_m$ whose kernel is cyclic of order ℓ^n. In particular, it has degree ℓ^n and, as ℓ is prime in $\mathrm{End}_{\overline{K}}(E_m)$, it must differ from $[\ell^{n/2}]$ by a unit. But $[\ell^{n/2}]$ is not cyclic and we get the desired contradiction.

For the converse, assume that $[p]$ is not purely inseparable. Then from the identification $\mathrm{T}_p(E)(\overline{K}) \cong \mathbb{Z}_p$ we obtain an injection

$$\mathrm{End}_{\overline{K}}(E) \hookrightarrow \mathrm{End}_{\mathbb{Z}_p}(\mathrm{T}_p(E)(\overline{K})) \cong \mathbb{Z}_p,$$

which is impossible if $\mathrm{End}_{\overline{K}}(E)$ is an order in a quaternion algebra (as it would not be abelian). □

Theorem 164. *Let E/K be an ordinary elliptic curve. Then $E[p](\overline{K}) \cong \mathbb{Z}/p\mathbb{Z}$. Also, if $j(E) \in \overline{\mathbb{F}}_p$, then* $\mathrm{End}_{\overline{K}}(E)$ *is an order in a quadratic imaginary field.*

Proof. The first proof is clear from the proof of corollary 162. For the second part, assume that $j(E)$ is algebraic over $\mathbb{F}_p$ and consider $E'/\mathbb{F}_q$, for $q = p^f$, isomorphic to E over $\overline{K}$. We consider the q–th power Frobenius $\phi_q \in \mathrm{End}_{\overline{K}}(E')$. and show that it cannot be multiplication by an integer. Indeed, if it were, we would have $\phi_q = [\pm p^{f/2}]$. But then we would have $E[p^{r/2}](\overline{K}) = 0$, which is not the case. □

A.5 Pell's equation (Antoine Giard)

Let $K = \mathbb{Q}(\sqrt{(D)})$ for a fundamental discriminant $D < -4$. We write $\zeta_K(s)$ for the Dedekind zeta function of K and, more generally, $\zeta_K(s, A)$ for the partial zeta functions associated with subsets A of ideals of $\mathscr{O}_K$. Define the character

$$\chi_D(\mathfrak{p}) = \left(\frac{D}{\mathrm{N}(\mathfrak{p})}\right)$$

(using the Kronecker symbol).

Let d be a square-free positive integer. We want to study the solutions to Pell's equation

$$x^2 - dy^2 = \pm 1.$$

By Dirichlet's unit theorem, there is a fundamental unit ε_d for $\mathbb{Q}(\sqrt{d})$.

Recall that Riemann's zeta function $\zeta(s)$ satisfies that

$$\lim_{s\to 1}\Big(\zeta(s) - \frac{1}{s-1}\Big) = \gamma$$

(where γ is Euler's constant). There is an analogue of this formula for K:

Theorem 165 (Kronecker's limit formula). *Let $A \in \mathrm{Cl}(\mathscr{O}_K)$. Then*

$$\lim_{s\to 1}\left(\zeta_K(s,A) - \frac{\pi}{\sqrt{-D}(s-1)}\right) = \frac{\pi}{\sqrt{-D}}\Big(2\gamma - \log(-D) - 2\log(g(\tau_A))\Big),$$

where

$$g(z) = \sqrt{\frac{2}{\sqrt{-D}}\,\mathrm{Im}(z)\cdot|\eta(z)|^2}$$

and τ_A is the CM point corresponding to A^{-1}.

Next, we want to study the L–function $L_K(s,\chi)$ for certain characters χ. Decompose $D = D_1D_2$ and define the genus character

$$\chi_{D_1D_2}(\mathfrak{p}) = \begin{cases} \Big(\dfrac{D_1}{\mathrm{N}(\mathfrak{p})}\Big) & \text{if } \mathfrak{p}\nmid D, \\ \Big(\dfrac{D_i}{\mathrm{N}(\mathfrak{p})}\Big) \neq 0 & \text{if } \mathfrak{p} \mid D. \end{cases}$$

(in the second case, we choose the $i \in 1,2$ that makes the Kronecker symbol $\neq 0$).

Theorem 166 (Kronecker). *We have a decomposition*

$$L_K(s,\chi_{D_1D_2}) = L(s,\chi_{D_1})L(s,\chi_{D_2}).$$

Assume that $\chi_{D_1D_2} \neq 1$. Using Kronecker's limit formula, we can express

$$L_K(1,\chi_{D_1D_2}) = \sum_{A\in\mathrm{Cl}(D)} \chi_{D_1D_2}(A)\zeta_K(1,A) = \frac{-2\pi}{\sqrt{-D}}\sum_{A\in\mathrm{Cl}(D)}\chi_{D_1D_2}(A)\log(g(\tau_A)).$$

Suppose that $D_1 > 0$ and $D_2 < 0$. The class number formula gives

$$L(1,\chi_{D_1}) = \frac{2h(D_1)\log(\varepsilon_{D_1})}{\sqrt{D_1}} \quad \text{and} \quad L(1,\chi_{D_2}) = \frac{2\pi h(D_2)}{\omega_{D_2}\sqrt{-D_2}}$$

and so, combining everything,

$$\frac{2h(D_1)h(D_2)}{\omega_{D_2}}\log(\varepsilon_{D_1}) = -\sum_{A\in\mathrm{Cl}(D)}\chi_{D_1D_2}(A)\log(g(\tau_A)).$$

Theorem 167. *We have*

$$\varepsilon_{D_1}^{2h(D_1)h(D_2)/\omega_{D_2}} = \prod_{A\in \mathrm{Cl}(D)} (g(\tau_A))^{-\chi_{D_1D_2}(A)}.$$

Remark. In this way, we have described a solution to Pell's equation in terms of modular forms.

Theorem 168 (Chowla–Selberg). *We have*

$$\prod_{A\in \mathrm{Cl}(D)} g(\tau_A) = \Big(\frac{1}{4\pi\sqrt{-D}}\Big)^{\frac{h(D)}{2}} \prod_{i=1}^{-D} \Gamma\Big(\frac{i}{-D}\Big)\frac{\omega_D\chi_D(i)}{4}.$$

A.6 The work of Granville–Stark (Christian Táfula)

Let D be a (negative) fundamental discriminant and let $\mathrm{Cl}(D)$ and $h(D)$ denote the class group and the class number, respectively, of the corresponding quadratic imaginary field $K = \mathbb{Q}(\sqrt{D})$.

Let $\tau \in \mathfrak{H}$. Recall that τ is called a CM point if

$$A\tau^2 + B\tau + C = 0$$

for some pairwise coprime $A, B, C \in \mathbb{Z}$ with $A > 0$. Thus, τ corresponds to a binary quadratic form

$$Ax^2 + Bxy + Cy^2.$$

In particular, the set of Heegner points Λ_D, consisting of CM points in a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ with discriminant D, is in bijection with the set of reduced primitive binary quadratic forms of discriminant D. In particular,

$$\tau_D = \begin{cases} \dfrac{\sqrt{D}}{2} & \text{if } D \equiv 0 \mod 4 \\ \dfrac{-1+\sqrt{D}}{2} & \text{if } D \equiv 1 \mod 4 \end{cases}$$

corresponds to the principal form given by

$$(A, B, C) = \begin{cases} \Big(1, 0, -\dfrac{D}{4}\Big) & \text{if } D \equiv 0 \mod 4 \\ \Big(1, 1, \dfrac{1-D}{4}\Big) & \text{if } D \equiv 1 \mod 4 \end{cases}$$

(note that this definition of τ_D is different from the usual).

Recall that $H = H_D = \mathbb{Q}(\sqrt{D}, j(\tau_D))$ is the Hilbert class field of K and that the values

$$\{ j(\tau) : \tau \in \Lambda_D \}$$

are the Galois conjugates of $j(\tau_D)$.

We saw in examples 5 and 6 that we can find study the solutions of the form $(j(\tau_D), j(\tau_D) - 1728) = (x^3, Dy^2)$ to the equation $x^3 - Dy^2 = 1728$ to give lower bounds for $h(D)$ using that the ABC conjecture predicts that there are few such solutions.

Conjecture 169. *Let $a, b, c \in \mathbb{Z}$. Suppose that $a + b = c$ and that the numbers a, b and c are pairwise coprime. For every $\varepsilon > 0$, there exists a constant $C_\varepsilon > 0$ such that*

$$\max\{ |a|, |b|, |c| \} < C_\varepsilon \cdot \left(\prod_{p|abc} p \right)^{1+\varepsilon}.$$

Heilbronn proved that $h(D) \to \infty$ as $D \to -\infty$, so there are two natural kinds of problems: listing values of $h(D)$ for small values of $|D|$ (e.g., the class number one problem) and estimating the asymptotic growth of $h(D)$. The main (classical) result in this direction is Siegel's estimate

$$\frac{h(D)}{\sqrt{|D|}} \gg_\varepsilon |D|^{-\varepsilon}$$

(unconditional but ineffective).

Granville and Stark proved that, assuming a certain uniform formulation of the ABC conjecture, there are no Siegel zeros for $\zeta_K(s)$. To do so, they studied solutions to the equation $x^3 - y^2 = 1728$ of the form $(j(\tau_D), j(\tau_D) - 1728) = (x^3, y^2)$. If x and y were integers, the ABC conjecture with $a = x^3$, $b = -y^2$ and $c = 1728$ would imply that

$$\log\bigl(\max\{ |x|^3, |y|^2 \}\bigr) < \frac{5}{6}(1+\varepsilon) log\bigl(\max\{ |x|^3, |y|^2 \}\bigr) + T_\varepsilon$$

for some $T_\varepsilon \in O_\varepsilon(1)$ or, equivalently,

$$\log\bigl(\max\{ |x|^3, |y|^2 \}\bigr) < (6 + \varepsilon')T'_\varepsilon.$$

To formalize this, one has to use the ABC conjecture for number fields: given a number field K and $\varepsilon > 0$, there exists a constant $C(K, \varepsilon) > 0$ such that, for every triple $a, b, c \in K$ with $a + b + c = 0$,

$$\operatorname{ht}([a : b : c]) < (1 + \varepsilon)\big(\mathcal{N}_K([a : b : c]) + \log(\operatorname{rd}_K)\big) + C(K, \varepsilon),$$

where ht denotes the (naive) height in $\mathbb{P}^2(K)$, $\mathcal{N}_K$ denotes the log-conductor and rd_K is the root-discriminant of K. Then, writing $\widetilde{H}_D = H_D(x, y)$, we obtain that

$$\operatorname{ht}(j(\tau_D)) < 6\big((1 + \varepsilon)\log(\operatorname{rd}_{\widetilde{H}_D}) + C(\widetilde{H}_D, \varepsilon)\big).$$

A "factorization" argument using modular functions shows that $\operatorname{rd}_{\widetilde{H}_D} \leq 6\sqrt{D}$, and the uniform form of the ABC conjecture allows us to use a constant $C(\varepsilon)$ independent of the field.

Lemma 170 (Granville–Stark). *The uniform ABC conjecture implies that*

$$\operatorname{ht}(j(\tau_D)) \leq \big(3 + o(1)\big)\log(|D|)$$

as $D \to -\infty$.

Theorem 171 (Granville–Stark). *The uniform ABC conjecture implies that*

$$h(D) \geq \left(\frac{\pi}{3} + o(1)\right)\frac{\sqrt{|D|}}{\log(|D|)}\sum_{\tau \in \Lambda_D}\frac{1}{A}$$

as $D \to -\infty$, where the index of summation $\tau \in \Lambda_D$ corresponds to a reduced binary quadratic form (A, B, C).

Consider the Dedekind zeta function

$$\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathscr{O}_K}\frac{1}{\mathrm{N}(\mathfrak{a})^s} = \frac{c_{-1}}{s - 1} + c_0 + O(s - 1) \quad \text{for } s \to 1.$$

Conjecture 172. *There exists $\delta > 0$ such that*

$$\zeta_K(\beta) \neq 0 \quad \textit{whenever } 1 - \frac{\delta}{\log(|D|)} \leq \beta < 1.$$

Using theorem 171 and the class number formula, one checks (assuming the uniform ABC conjecture) that

$$\zeta_K(\beta) \leq -\left(\frac{1}{\delta} + o(1)\right)\sum_{\tau \in \Lambda_D}\frac{1}{A} + c_0(D) + o(1).$$

Then one can use Kronecker's limit formula to control the term $c_0(D)$:

$$c_0(D) = \frac{\pi^2}{6} \sum_{\tau \in \Lambda_D} \frac{1}{A} - \frac{\pi}{\sqrt{|D|}} \sum_{\tau \in \Lambda_D} \log\left(\frac{\sqrt{|D|}}{2A}\right) + O\left(\frac{h(D)}{\sqrt{|D|}}\right).$$

After some algebraic manipulation and using Duke's theorem on the equidistribution of Λ_D, one can prove that conjecture 172 is equivalent to the estimate

$$h(D) \gg \frac{\sqrt{|D|}}{\log(|D|)} \sum_{\tau \in \Lambda_D} \frac{1}{A}.$$

A.7 Factorization of singular moduli (Arihant Jain)

In the previous lecture, we saw some results about the primes that appear in the factorization of

$$\prod_{\substack{\mathrm{disc}(\tau_1)=D_1 \\ \mathrm{disc}(\tau_2)=D_2}} (j(\tau_1) - j(\tau_2))$$

for two (distinct) fundamental discriminants D_1 and D_2. Now we are going to study something about their multiplicities. More precisely, we are going to work with

$$J(D_1, D_2) = \prod_{\substack{\mathrm{disc}(\tau_1)=D_1 \\ \mathrm{disc}(\tau_2)=D_2}} (j(\tau_1) - j(\tau_2))^{\frac{4}{w_1 w_2}},$$

where w_i is the number of units in the ring of integers of $\mathbb{Q}(\sqrt{D_i})$ (in particular, if $D_i < -4$, then $w_i = 2$).

Given a prime number ℓ such that

$$\left(\frac{D_1 D_2}{\ell}\right) \neq -1,$$

we define

$$\varepsilon(\ell) = \begin{cases} \left(\frac{D_1}{\ell}\right) & \text{if } \ell \nmid D_1, \\ \left(\frac{D_2}{\ell}\right) & \text{if } \ell \nmid D_2. \end{cases}$$

More generally, if $n \in \mathbb{Z}_{\geq 1}$ has a prime factorization

$$n = \prod_i \ell_i^{a_i}$$

with each ℓ_i satisfying the condition from before, we define

$$\varepsilon(n) = \prod_i \varepsilon(\ell_i)^{a_i}.$$

Theorem 173 (Gross–Zagier). *Let $D = D_1 D_2$. Then*

$$J(D_1, D_2)^2 = \pm \prod_{|x|<\sqrt{D}} \prod_{n \mid \frac{D-x^2}{4}} n^{-\varepsilon(n)}.$$

A.8 Evaluation of p–adic theta functions (Isabella Negrini)

For every $n \in \mathbb{Z}_{\geq 1}$, choose representatives P_n for $\mathbb{P}^1(\mathbb{Q}_p)$ modulo p^n. For example, we can take

$$P_n = \{\, [a, 1] : a \in \mathbb{Z}_p / p^n \mathbb{Z}_p \,\} \cup \{\, [1, b] : b \in p\mathbb{Z}_p / p^n \mathbb{Z}_p \,\}.$$

Define

$$\Omega_n = \mathbb{P}^1(\mathbb{C}_p) \setminus \left(\bigcup_{x \in P_n} B(x, n) \right),$$

where $B(x, n)$ denotes the closed ball of radius p^n centred at x, and

$$\Omega_n^- = \mathbb{P}^1(\mathbb{C}_p) \setminus \left(\bigcup_{x \in P_n} B^-(x, n) \right),$$

where $B^-(x, n)$ denotes the open ball of radius p^n centred at x. By definition,

$$\mathcal{H}_p = \bigcup_{n \geq 1} \Omega_n = \bigcup_{n \geq 1} \Omega_n^-.$$

We will describe these subsets of $\mathcal{H}_p$ by means of the Bruhat–Tits tree $\mathcal{T}$. Observe that, given a vertex v_0, the vertices at distance n from v_0 are in bijection with $\mathbb{P}^1(\mathbb{Z}_p / p^n \mathbb{Z}_p)$. We take v_0 to be the standard vertex corresponding to $[\mathbb{Z}_p^2]$ and set

$$v_1 = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} v_0.$$

The edge e_0 joining v_0 and v_1 is called the standard edge and satisfies that

$$\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Q}_p)}(e_0) = \left\{ \gamma \in \mathrm{PGL}_2(\mathbb{Z}_p) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod p \right\}.$$

Definition 174. The *ends of $\mathcal{T}$* are the equivalence classes of infinite paths on $\mathcal{T}$

without backtracking under the equivalence relation defined as follows: two infinite paths are equivalent if they only differ by finite segments. Let $\mathrm{Ends}(\mathcal{T})$ denote the set of ends.

We endow $\mathrm{Ends}(\mathcal{T})$ with the topology which has as a basis the subsets

$$U(e) = \{ \text{Ends of } \mathcal{T} \text{ starting with } e \}$$

for all oriented edges e of $\mathcal{T}$. One can define a $\mathrm{PGL}_2(\mathbb{Q}_p)$–equivariant homeomorphism $\mathrm{Ends}(\mathcal{T}) \cong \mathbb{P}^1(\mathbb{Q}_p)$.

Let $r\colon \mathcal{H}_p \to \mathcal{T}$ denote the reduction map. Observe that $\mathcal{A}^* = r^{-1}(v_0)$ and $\mathcal{W}_0 = r^{-1}(e_0)$ and that Ω_n^- is the preimage of the subtrees of $\mathcal{T}$ made of points at distance at most $n-1$ from v_0. More generally, we can obtain affinoids as preimages of vertices and annuli as preimages of edges.

Theorem 175 (Mumford).

(1) *Let Γ be a discrete subgroup of $\mathrm{SL}_2(\mathbb{Q}_p)$. If $\Gamma\backslash\mathcal{H}_p$ is compact, then it is an algebraic curve over $\mathbb{Q}_p$.*

(2) *Conversely, if X is an algebraic curve over $\mathbb{Q}_p$ with totally degenerate reduction, then there exists a discrete subgroup Γ of $\mathrm{SL}_2(\mathbb{Q}_p)$ such that X is isomorphic to $\Gamma\backslash\mathcal{H}_p$.*

Let $B = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ be Hamilton's quaternions and consider the order

$$R = \mathbb{Z}\Big[i, j, k, \frac{1+i+j+k}{2}\Big].$$

We have an isomorphism $\iota_p\colon B \otimes_{\mathbb{Q}} \mathbb{Q}_p \to \mathrm{M}_2(\mathbb{Q}_p)$ and define

$$\Gamma = \iota_p\left(R\Big[\frac{1}{p}\Big]_1^\times \right) \subseteq \mathrm{SL}_2(\mathbb{Q}_p).$$

Definition 176. Let $a, b, z \in \mathcal{H}_p$. The *theta function $\theta(a,b;z)$* is defined by

$$\theta(a,b;z) = \prod_{\gamma\in\Gamma} \frac{z-\gamma a}{z-\gamma b}.$$

Definition 177. For every $n \in \mathbb{Z}_{\geq 0}$, we define

$$\Gamma_n = \left\{ \iota_p\Big(\frac{x}{p^n}\Big) : x \in R,\ \mathrm{N}(x) = p^{2n} \right\}$$

and

$$\phi_n(a,b;z) = \prod_{\gamma\in\Gamma_n\setminus\Gamma_{n-1}} \frac{z-\gamma a}{z-\gamma b}.$$

Proposition 178. *The product $\theta(a,b;z)$ converges for all $a,b,z \in \mathcal{H}_p$. It defines a meromorphic function of z with zeros at $\{\, \gamma a : \gamma \in \Gamma \,\}$ and poles at $\{\, \gamma b : \gamma \in \Gamma \,\}$.*

One way to compute $\theta(a,b;z)$ could be to approximate it with

$$\prod_{i=0}^{n} \phi_i(a,b;z) \qquad \text{for } n \gg 0.$$

However, this is not efficient (the order of Γ_n grows exponentially). To do it better, one can express the quaternions of norm p^n in terms of those of norm p.

Proposition 179. *A primitive quaternion of norm p^n factors uniquely (up to units) as a product of quaternions of norm p.*

One can also separate the quaternions according to where they send the standard affinoid. In the end, θ can be given by a collection of power series with different centres.

A.9 Quaternion algebras over $\mathbb{Q}$ (Siva Sankar Nair)

Definition 180. Let F be a field of characteristic $\neq 2$. A *quaternion algebra over F* is a central F–algebra B satisfying one of the following equivalent conditions:

(1) B is simple and has dimension 4 over K;

(2) there are a quadratic separable F–algebra K with an embedding $K \hookrightarrow B$ and elements $\beta \in B$ and $b \in F^\times$ such that $B = K \oplus K\beta$, $\beta^2 = b$ and $\beta\alpha = \overline{\alpha}\beta$ for all $\alpha \in K$;

(3) there are elements $i, j \in B$ that generate B as an F–algebra and satisfy that $i^2 = a$, $j^2 = b$ and $ij = -ji$ for some $a, b \in F^\times$, and

(4) B is simple, strictly larger than F and finite-dimensional over F and there is an F–linear anti-involution such that $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} \in F$ and $\mathrm{N}(\alpha) = \alpha \cdot \overline{\alpha} \in F$ for all $\alpha \in B$.

We write

$$B = (K,b)/F = \left(\frac{a,b}{F}\right).$$

Example 181. Let $a, b \in F^\times$. If one of a or b is a square in F, then

$$\left(\frac{a,b}{F}\right) \cong \mathrm{M}_2(F)$$

via

$$i \mapsto \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \quad \text{and} \quad j \mapsto \begin{pmatrix} \sqrt{b} & 0 \\ 0 & -\sqrt{b} \end{pmatrix}.$$

Given a quaternion algebra B/F, there is a symmetric bilinear form

$$\langle \cdot\,, \cdot \rangle \colon B \times B \to F$$

given by $\langle \alpha, \beta \rangle = \mathrm{Tr}(\alpha\overline{\beta})$. One checks that $\langle \alpha, \alpha \rangle = 2\,\mathrm{N}(\alpha)$. Let $\mathscr{O}$ be an order in B. We define

$$\mathrm{disc}(\mathscr{O}) = \left|\det\left(\langle e_i, e_j \rangle\right)_{ij}\right|,$$

where e_1, e_2, e_3, e_4 is a $\mathbb{Z}$–basis of $\mathscr{O}$.

Example 182. Take

$$B = \left(\frac{a, b}{\mathbb{Q}}\right) \quad \text{with } a, b \in \mathbb{Z}.$$

For $\mathscr{O} = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$, we have $\mathrm{disc}(\mathscr{O}) = (4ab)^2$

One can compute maximal orders in $B/\mathbb{Q}$ with the following algorithm:

(1) Take any order $\mathscr{O}'$ of B and find all primes p such that $\mathscr{O}'_p$ is not maximal in $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$.

(2) For such a prime p, depending on the Legendre symbol

$$\left(\frac{a}{p}\right)$$

(and on the parity of p), we adjoin elements satisfying certain congruence conditions modulo p to make an order that is maximal at p.

A.10 Coleman integration (Ting-Han Huang)

We want to define line integrals for a rigid analytic function f on the p–adic upper half-plane $\mathcal{H}_p$.

Given an affinoid X, we write $A(X)$ for the corresponding affinoid algebra and $\Omega(X)$ for the module of rigid analytic differentials on X. There is the canonical map $d \colon A(X) \to \Omega(X)$.

Definition 183. Let X be an affinoid and let $\widetilde{X}$ denote its reduction to characteristic p. An endomorphism $\phi \colon X \to X$ is called a *Frobenius endomorphism* if its reduction $\widetilde{\phi}$ is the Frobenius endomorphism of $\widetilde{X}$.

Theorem 184 (Coleman). *Let K be a complete subfield of $\mathbb{C}_p$ and let X be a connected affinoid over K with good reduction $\widetilde{X}$. Let ω be a closed 1–form on X and let ϕ be the Frobenius endomorphism. If there exists $P(T) \in \mathbb{C}_p[T]$ whose roots are not roots of unity and such that*

$$P(\phi^*)\omega \in dA(X),$$

then there exists a locally analytic function f_ω on $X(\mathbb{C}_p)$, unique up to additive constant, such that

(1) *$df_\omega = \omega$ and*

(2) *$P(\phi^*)f_\omega \in A(X)$.*

Remark. The Coleman primitive f_ω is independent of the choice of P and ϕ.

Take $X = \mathbb{G}_{\mathrm{m}}(\mathscr{O}_{\mathbb{C}_p}) = \{ z \in \mathbb{C}_p : |z|_p = 1 \}$. We can fix a branch of the p–adic logarithm $\log\colon \mathbb{C}_p^\times \to \mathbb{C}_p$, characterized by

$$\frac{d}{dz}\log(z) = \frac{1}{z}.$$

Given $\omega \in \Omega(X)$, we can integrate ω locally and thus obtain a locally analytic function F on X such that $dF = \omega$. Two such primitives differ by a locally constant function, but we would like integration to be defined up to a (global) constant.

Lemma 185. *Let X be an affinoid with a Frobenius endomorphism ϕ. If f is a locally constant function on X such that $\phi^* f = af$ for some $a \in \mathbb{C}_p$ that is not a root of unity, then $f = 0$.*

For our simple choice of X, we can take ϕ to be the map $z \mapsto z^p$. Then

$$\phi^*\Big(\frac{dz}{z}\Big) = p\frac{dz}{z}$$

and we obtain a Coleman primitive $F(z)$ such that

$$\phi^* F(z) = pF(z).$$

This is the usual p–adic logarithm.

A.11 Calculation of singular moduli on Shimura curves (Sofia Giampietro)

Let S be an odd set of places of $\mathbb{Q}$ containing ∞. Let B_p be the quaternion algebra ramified at the places in $S \setminus \{ p \}$. Let $R_{S,p}$ be the maximal $\mathbb{Z}[p^{-1}]$–order in B_p and consider $\Gamma_p = (R_{S,p}^\times)_1$ embedded inside $\mathrm{SL}_2(\mathbb{Q}_p)$. We have a Shimura curve X_S such that $X_S(\mathbb{C}_p) = \Gamma_p \backslash \mathcal{H}_p$.

For a quadratic order $\mathscr{O}$ of discriminant D, the elements of $\mathrm{CM}(\mathscr{O}) \subseteq X_S(\mathbb{C}_p)$ are in bijection with optimal embeddings of $\mathscr{O}[p^{-1}]$ into $R_{S,p}$.

Fix two quadratic discriminants D_1 and D_2. Take conjugate pairs (τ_i, τ_i') of CM points of discriminants D_i and define

$$\mathcal{D}_i = (\tau_i) - (\tau_i') \in \mathrm{Div}^0(\mathcal{H}_p).$$

We want to compute $[\mathcal{D}_1; \mathcal{D}_2]_{\Gamma_p}$ in some particular cases. Recall that, if $\mathcal{D}_1$ is principal, then this quantity is defined in the compositum $H_{D_1} H_{D_2}$, where H_{D_i} denotes the ring class field corresponding to the order $\mathscr{O}_i$ of discriminant D_i.

We can express

$$[\mathcal{D}_1; \mathcal{D}_2]_{\Gamma_p} = \prod_{\gamma \in \Gamma_p} \frac{(\tau_1 - \gamma\tau_2)(\tau_1' - \gamma\tau_2')}{(\tau_1 - \gamma\tau_2')(\tau_1' - \gamma\tau_2)} = \frac{\theta_{\mathcal{D}_2}(\tau_1)}{\theta_{\mathcal{D}_2}(\tau_1')}.$$

Assume that X_S has genus 0, so that $c_{\mathcal{D}_1}$ is trivial. This happens only for the sets of places $S = \{2, 3, \infty\}$, $\{2, 5, \infty\}$ or $\{2, 11, \infty\}$. Write $J_p(\tau_1, \tau_2) = [\mathcal{D}_1; \mathcal{D}_2]_{\Gamma_p}$.

The θ–functions can be computed separating the elements of Γ_p according to their p–adic valuation and using a recursive algorithm in terms of factorizations in B_p that works under the assumption that B_p has class number 1.

A.12 Heegner points (Reginald Lybbert)

Let K be a quadratic imaginary field. Recall that, if $\mathrm{CM}_{\mathbb{C}}(\mathscr{O}_K) = \{\tau_1, \dots, \tau_h\}$, then $H = K(j(\tau_1), \dots, j(\tau_h))$ is the Hilbert class field of K.

Let E be an elliptic curve over $\mathbb{Q}$. The modularity theorem provides a modular parametrization

$$\phi_E \colon X_0(N) \longrightarrow E,$$

where N is the conductor of E. Analytically, this map can be defined as follows:

$$\phi_E(\tau) = \big(\wp(z_\tau), \wp'(z_\tau)\big)$$

where, if f_E is the modular form of level $\Gamma_0(N)$ corresponding to E, then

$$z_\tau = 2\pi i \int_{i\infty}^{\tau} f_E(z)\,dz = \sum_{n \geq 1} \frac{a_n(f_E)}{n} q^n, \quad \text{where } q = e^{2\pi i \tau}.$$

For a CM point $\tau \in \mathfrak{h}$, we consider the order

$$\mathscr{O}_\tau^{(N)} = \left\{ \gamma \in \mathrm{M}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \text{ and } \gamma\tau = \tau \right\} \cup \{ 0 \}.$$

Theorem 186. *Let $\tau \in \mathfrak{h} \cap K$ and let H be the ray class field attached to $\mathscr{O}_\tau^{(N)}$. Then $\phi_E(\tau) \in E(H)$.*

In particular, one can use this result to compute some rational points of E over (hopefully) "small" fields. In fact, we can even obtain points in $E(K)$ as follows:

- for each class $[a] \in \mathrm{Gal}(H/K)$, we can find some $\tau_\mathfrak{a}$ such that $\mathscr{O}_{\tau_\mathfrak{a}}^{(N)} \cong \mathfrak{a}$;
- thus, $\phi_E(\tau_\mathfrak{a}) \in E(H)$, and
- summing over all such elements, we obtain

$$P_K = \sum_{\mathfrak{a} \in \mathrm{Cl}(K)} \phi_E(\tau_\mathfrak{a}) \in E(K).$$

Theorem 187 (Gross–Zagier). *Let P_K be the* Heegner point *defined above. Then*

$$L'(1,E) = \frac{32\pi^2 \|f_E\|^2}{|\mathscr{O}_K^\times|^2 \sqrt{|D_K|} \deg(\phi_E)} h_E(P_K),$$

where h_E denotes the Néron–Tate height.

A.13 The Chowla–Selberg formula (Subham Roy)

Let $\mathscr{O}$ be an order of discriminant D in a quadratic imaginary field K. Write $\mathfrak{Z}_D$ for the set of CM points of discriminant D in $\mathfrak{h}$. For each $\tau \in \mathfrak{Z}_D$, there exists a period Ω_τ (depending only on τ) such that, for every modular form f of weight k and level $\mathrm{SL}_2(\mathbb{Z})$ defined over $\overline{\mathbb{Q}}$, $f(\tau) \in \Omega_\tau^k \cdot \overline{\mathbb{Q}}$. In fact, we can deduce the following more general result:

Proposition 188. *Let K be a quadratic imaginary field. There exists a period $\Omega_K \in \mathbb{C}^\times$ with the property that, for every $\tau \in \mathfrak{h} \cap K$ and every modular form f of weight $k \in \mathbb{Z}$ and level $\mathrm{SL}_2(\mathbb{Z})$ defined over $\overline{\mathbb{Q}}$,*

$$f(\tau) \in \Omega_K^k \cdot \overline{\mathbb{Q}}.$$

We apply this result to $F(z) = \mathrm{Im}(z)|\eta(z)|^4$ and to all the CM points $\tau \in \mathfrak{Z}_D$, where $D = \mathrm{disc}(K)$.

Theorem 189 (Chowla–Selberg). *In the situation above,*

$$\prod_{\tau \in \mathrm{SL}_2(\mathbb{Z})\backslash \mathfrak{Z}_D} \Big(4\pi\sqrt{|D|}F(\tau)\Big)^{2/w} = \prod_{m=1}^{|D|-1} \Gamma\Big(\frac{m}{|D|}\Big)^{\chi_D(m)},$$

where $w = |\mathscr{O}_K^\times|$ and χ_D is the quadratic character associated with K.

Using this formula, one checks that the period Ω_K can be chosen to be

$$\Omega_K = \frac{1}{\sqrt{2\pi|D|}}\Bigg(\prod_{m=1}^{|D|-1} \Gamma\Big(\frac{m}{|D|}\Big)^{\chi_D(m)}\Bigg)^{w/4h(D)}.$$