Point counting formulae on universal elliptic curves

Jin, J.

J. Jin

Point counting formulae on universal elliptic curves

Master's thesis, December 19, 2011.

Thesis advisor: prof. dr. S.J. Edixhoven

Mathematisch Instituut, Universiteit Leiden

CONTENTS

Introduction

The main problem of this thesis is the following.

For which universal elliptic curves *with a point of* universal order n *does there exist an* elementary *formula (in terms of q) for the number of $\mathbb{F}_q$-rational points?*

Loosely speaking, a *universal elliptic curve* with a point of *universal order n* assigns to every field k in which n is invertible, the family of all elliptic curves E (given in Weierstrass form) over k such that the point $(0 : 0 : 1)$ is in E, and is of order n in E. (And the number of $\mathbb{F}_q$-rational points is then the sum of the number of $\mathbb{F}_q$-rational points of each of the elliptic curves over $\mathbb{F}_q$.)

We say that a function in terms of the prime power $q = p^i$ is an *elementary formula* if we can express it as the sum of a polynomial in q (where Dirichlet characters may occur in the coefficients) and an expression in the coefficients of a certain type of cusp forms of weight 3 and level n, called cusp forms with *complex multiplication*, or *CM-forms*. The idea behind this is that the coefficients of this type of cusp form can be expressed in a somewhat simple manner, and that cusp forms that are not linear combinations of CM-forms ('non-CM-forms') cannot be expressed in a simple way.

The (conjectured) answer to this problem is that the universal elliptic curves that do admit an elementary formula for the number of $\mathbb{F}_q$-rational points, are exactly those corresponding to $n \leq 8$.

Summary. In Chapter 1, we give an explicit description of the multiplication-by-n for elliptic curves over an arbitrary ring, and study its kernel. In Chapter 2, we use this description to (correctly) define universal elliptic curves with a point of universal order n, for $n \geq 4$, and give some generalities about modular curves and modular forms. In Chapter 3, we give explicit formulae for the number of $\mathbb{F}_q$-rational points on universal elliptic curves with a point of universal order n, for some small $n \geq 4$. In Chapter 4, we then define Hecke characters, give some properties, and then define what it means for a universal elliptic curve with a point of universal order n to be elementary. We also try to determine which universal elliptic curves are elementary.

1 Elliptic curves over rings

The main goal in this chapter is to describe the multiplication-by-n map on elliptic curves over rings in a fully explicit way. This has already been done for elliptic curves over fields, see for example [7], but the description given there does not directly generalise to elliptic curves over rings; as we will see later, the description given there will only work for a family of points of elliptic curves over rings that in general will be far too restrictive. The description that we will give is 'essentially the same' one, except this description does generalise to elliptic curves over more general rings.

1.1 Definitions

Rings, from now on, will always be associative, commutative and will always contain a multiplicative unit element.

Definition 1.1.1. Let S be a scheme. An *elliptic curve* E over S is a smooth projective morphism $E \longrightarrow S$, of which the geometric fibres are connected curves of genus 1, together with a section $0\colon S \longrightarrow E$.

Remark 1.1.2. Let R be a ring, let E be an elliptic curve over R with an embedding into $\mathbb{P}^2_R$, and let S be an R-algebra. Note that one can identify $E_R(S)$ with a subset of the set of isomorphism classes[1] of 4-tuples $(\mathcal{L}, s_0, s_1, s_2)$ of an invertible $\mathcal{O}_S$-module, and three global sections generating it, by identifying $P \in E_R(S)$ with the (isomorphism class of the) 4-tuple

$$\Big(P^*\big(\mathcal{O}_{\mathcal{E}}(1)\big), P^*x, P^*y, P^*z\Big).$$

If $\mathcal{L} = \mathcal{O}_S$, then we will denote the 4-tuple $(\mathcal{L}, s_0, s_1, s_2)$ by $(s_0 : s_1 : s_2)$.

Example 1.1.3. Let R be a ring, and let $W \in R[x, y, z]$ be a Weierstrass equation, i.e. W is of the form

$$y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3, \qquad a_1, a_2, a_3, a_4, a_6 \in R.$$

Define $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$ and

$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2.$$

Then the *discriminant* $\Delta \in R$ of W is $-b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$.

Let $S = \operatorname{Spec} R$, and let $E = \operatorname{Proj} R[x, y, z]/(W)$. We embed E into $\mathbb{P}^2_R$ as the closed subscheme of $\mathbb{P}^2_R$ given by the equation W. Then the natural morphism $f\colon E \longrightarrow S$ is projective, and smooth if and only if the discriminant Δ is invertible in R. In that case, all geometric fibres of f are connected curves of genus 1. Then E/S, together with the section 0 given by the point $(0 : 1 : 0) \in E(R)$, is an elliptic curve.

[1] An isomorphism of two such 4-tuples $(\mathcal{L}, s_0, s_1, s_2)$ and $(\mathcal{M}, t_0, t_1, t_2)$ is an isomorphism $\mathcal{L} \longrightarrow \mathcal{M}$ sending s_i to t_i for all $i \in \{0, 1, 2\}$.

Let us call elliptic curves of the above type *Weierstrass curves*. Then we can characterize elliptic curves as S-schemes that are (Zariski-) locally Weierstrass on the base. Locally, the corresponding Weierstrass equation (say over a ring R) is unique up to $x \mapsto \alpha^2 x + az$, $y \mapsto \alpha^3 y + bx + cz$, for $\alpha \in R^\times$, and $a, b, c \in R$. See [9, Ch. 2] for details.

Furthermore, elliptic curves have a natural abelian scheme structure. Again, see [9, Ch. 2] for details.

1.2 The multiplication-by-n map

Let $\mathcal{R} = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$, let

$$\mathcal{W} = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 \in \mathcal{R}[x, y, z],$$

and let $\Delta \in \mathcal{R}$ denote its discriminant. Then consider the elliptic curve $\mathcal{E} = \operatorname{Proj} \mathcal{R}_\Delta[x, y, z]/(W)$ over the ring $\mathcal{R}_\Delta = \mathcal{R}[\frac{1}{\Delta}]$. The elliptic curve $\mathcal{E}/\mathcal{R}_\Delta$ is the *universal* Weierstrass curve, i.e. we have the following.

Lemma 1.2.1. *Let E be a Weierstrass curve over a ring R. Then there exists a unique morphism $f\colon \operatorname{Spec} R \longrightarrow \operatorname{Spec} \mathcal{R}_\Delta$ such that E/R is the base change of $\mathcal{E}/\mathcal{R}_\Delta$ by f, and such that this base change is compatible with the embeddings $E \longrightarrow \mathbb{P}^2_R$ and $\mathcal{E} \longrightarrow \mathbb{P}_{\mathcal{R}^2_\Delta}$.*

Proof. Let R be a ring, and let E/R be a Weierstrass curve, with equation

$$W = y^2z + a_1'xyz + a_3'yz^2 - x^3 - a_2'x^2z - a_4'xz^2 - a_6'z^3,$$

where for all i, $a_i' \in R$. Then the ring morphism $\mathcal{R}_\Delta \longrightarrow R$ given by $a_i \mapsto a_i'$ for all i, is the unique morphism making E/R the base change of $\mathcal{E}/\mathcal{R}_\Delta$; the morphism $\mathcal{R}_\Delta \longrightarrow R$ makes E/R the base change of $\mathcal{E}/\mathcal{R}_\Delta$ if and only if the morphism $\mathcal{R}_\Delta[x, y, z] \longrightarrow R[x, y, z]$ (see the following diagram) induced by it maps $\mathcal{W}$ to W.

$$\begin{array}{ccc} E & \longrightarrow & \mathcal{E} \\ \downarrow & & \downarrow \\ \mathbb{P}^2_R & \longrightarrow & \mathbb{P}^2_{\mathcal{R}_\Delta} \\ \downarrow & & \downarrow \\ \operatorname{Spec} R & \longrightarrow & \operatorname{Spec} \mathcal{R}_\Delta \end{array}$$

□

In the situation in the proof above, we say that E is the Weierstrass curve *corresponding to the morphism* $\mathcal{R}_\Delta \longrightarrow R$, or simply *corresponding to* R if it is clear from the context what the morphism $\mathcal{R}_\Delta \longrightarrow R$ is.

Let n be an integer. We want to analyse multiplication by n on the $\mathcal{R}_\Delta$-valued points of E. To this end, let $[n]_\mathcal{E}\colon \mathcal{E} \longrightarrow \mathcal{E}$ denote the multiplication-by-n morphism. We have the following.

Proposition 1.2.2. *For all $n \in \mathbb{Z}$, $[n]_{\mathcal{E}}^*(\mathcal{O}_{\mathcal{E}}(1)) \cong \mathcal{O}_{\mathcal{E}}(n^2)$.*

To prove this proposition, we use the following result on abelian schemes.

Theorem 1.2.3 (Theorem of the Cube, [10, Thm. IV.3.3])**.** *Let S be a scheme, let A be an abelian scheme over S, and let T be an S-scheme. Then for all $a_1, a_2, a_3 \in A_S(T)$, and all invertible sheaves $\mathcal{L}$ on A, the invertible sheaf $\bigotimes_{I \subseteq \{1,2,3\}} (\sum_{i \in I} a_i)^* \mathcal{L}^{(-1)^{\#I}}$ is trivial.*

As a special case of this, we have the following.

Corollary 1.2.4. *Let A/S be an abelian scheme, and let $n_1, n_2, n_3 \in \mathbb{Z}$. For all integers $m \in \mathbb{Z}$, let $[m]_A \colon A \longrightarrow A$ denote the multiplication-by-m map on A. Then for every invertible sheaf $\mathcal{L}$ on A, the invertible sheaf $\bigotimes_{I \subseteq \{1,2,3\}} [\sum_{i \in I} n_i]_A^* \mathcal{L}^{(-1)^{\#I}}$ is trivial.*

Proof of Proposition 1.2.2. We first prove that $[-1]_{\mathcal{E}}^* \mathcal{O}_{\mathcal{E}}(1) \cong \mathcal{O}_{\mathcal{E}}(1)$. To this end, let I denote the ideal sheaf of the zero section. Since the zero section is given by the point $(0:1:0)$, it follows that the sequence of $\mathcal{O}_{\mathcal{E}}$-modules

$$\mathcal{O}_{\mathcal{E}}(-1) \times \mathcal{O}_{\mathcal{E}}(-1) \xrightarrow{(\cdot x, \cdot z)} \mathcal{O}_{\mathcal{E}} \xrightarrow{0^\#} 0_* \mathcal{O}_{\mathcal{R}_\Delta}$$

is exact, so $I = x\mathcal{O}_{\mathcal{E}}(-1) + z\mathcal{O}_{\mathcal{E}}(-1)$.

Then note that

$$I^3 = (y^2 + a_1xy + a_3yz)z\mathcal{O}_{\mathcal{E}}(-3) + x^2z\mathcal{O}_{\mathcal{E}}(-3) + xz^2\mathcal{O}_{\mathcal{E}}(-3) + z^3\mathcal{O}_{\mathcal{E}}(-3) \subseteq z\mathcal{O}_{\mathcal{E}}(-1).$$

Note that every homogeneous polynomial in $\mathcal{R}_\Delta[x,y,z]$ of degree at least 3 lies in the $\mathcal{R}_\Delta[x,y,z]$-ideal generated by $y^2 + a_1xy + a_3yz$, x^2, xz, z^2, since every such polynomial can be written as the sum of a multiple of the first generator, and a homogeneous polynomial that is linear in y, which can be generated by x^2, xz, z^2 since we assumed its degree was at least 3. So locally on open subsets, the inclusion above is an equality. Hence $I^3 = z\mathcal{O}_{\mathcal{E}}(-1)$, so $I^3 \cong I^{\otimes 3}$ is isomorphic to $\mathcal{O}_{\mathcal{E}}(-1)$ as an $\mathcal{O}_{\mathcal{E}}$-module. (It also follows that I is invertible.) We deduce that $I^{\otimes -3} \cong \mathcal{O}_{\mathcal{E}}(1)$. Now note that since $[-1]_{\mathcal{E}}$ fixes the zero section, it follows that $[-1]_{\mathcal{E}}^* I = I$, and hence also that $[-1]_{\mathcal{E}}^* \mathcal{O}_{\mathcal{E}}(1) \cong \mathcal{O}_{\mathcal{E}}(1)$.

Hence it follows that $[-n]_{\mathcal{E}}^* \mathcal{O}_{\mathcal{E}}(1) = [n]_{\mathcal{E}}^* [-1]_{\mathcal{E}}^* \mathcal{O}_{\mathcal{E}}(1) \cong [n]_{\mathcal{E}}^* \mathcal{O}_{\mathcal{E}}(1)$, so it suffices to prove our claim for non-negative n. We do this by induction.

Since $0 = (0:1:0)$, we have $[0]_{\mathcal{E}}^* \mathcal{O}_{\mathcal{E}}(1) \cong \mathcal{O}_{\mathcal{E}}$. Also note that $[1]_{\mathcal{E}}$ is the identity on $\mathcal{E}$, hence given by the identity on $\mathcal{R}_\Delta[x,y,z]/(\mathcal{W})$, so $[1]_{\mathcal{E}}^* \mathcal{O}_{\mathcal{E}}(1) = \mathcal{O}_{\mathcal{E}}(1)$.

To see that $[2]_{\mathcal{E}}^*(\mathcal{O}_{\mathcal{E}}(1)) \cong \mathcal{O}_{\mathcal{E}}(4)$, apply Corollary 1.2.4 with $\mathcal{L} = \mathcal{O}_{\mathcal{E}}(1)$, $n_1 = n_2 = 1$, $n_3 = -1$. Then for $n \geq 3$, our claim follows by induction by applying Corollary 1.2.4 with $\mathcal{L} = \mathcal{O}_{\mathcal{E}}(1)$, $n_1 = n - 2$, $n_2 = n_3 = 1$. □

From now on, we fix, for every $n \in \mathbb{Z}$, an isomorphism $[n]_{\mathcal{E}}^*(\mathcal{O}_{\mathcal{E}}(1)) \longrightarrow \mathcal{O}_{\mathcal{E}}(n^2)$, and identify these two invertible $\mathcal{O}_{\mathcal{E}}$-modules using this isomorphism.

By Proposition 1.2.2, it follows that since $x, y, z \in \Gamma(\mathcal{E}, \mathcal{O}_{\mathcal{E}}(1)) = \big(\mathcal{R}_\Delta[x,y,z]/(\mathcal{W})\big)_1$ generate $\mathcal{O}_{\mathcal{E}}(1)$, the global sections $\alpha_n = [n]_{\mathcal{E}}^* x, \beta_n = [n]_{\mathcal{E}}^* y, \gamma_n = [n]_{\mathcal{E}}^* z$ generate $[n]_{\mathcal{E}}^* \mathcal{O}_{\mathcal{E}}(1) = \mathcal{O}_{\mathcal{E}}(n^2)$. We view these global sections as homogeneous elements of degree n^2 in $\mathcal{R}_\Delta[x,y,z]/(\mathcal{W})$. Note that, if we had chosen a different isomorphism $[n]_{\mathcal{E}}^*\big(\mathcal{O}_{\mathcal{E}}(1)\big) \longrightarrow \mathcal{O}_{\mathcal{E}}(n^2)$, the triple $(\alpha_n', \beta_n', \gamma_n')$ obtained that way will be equal to $(\epsilon\alpha_n, \epsilon\beta_n, \epsilon\gamma_n)$ for some $\epsilon \in \mathcal{R}_\Delta^\times$.

Now we can express using Remark 1.1.2, for any $\mathcal{R}_\Delta$-algebra R, multiplication by n on R-valued points of $\mathcal{E}$ as follows.

Proposition 1.2.5. *Let n be an integer, and let R be an $\mathcal{R}_\Delta$-algebra. Let $P = (\mathcal{L}, s_0, s_1, s_2) \in \mathcal{E}_{\mathcal{R}_\Delta}(R)$. Then*

$$nP = \big(\mathcal{L}^{\otimes n^2}, \alpha_n(s_0,s_1,s_2), \beta_n(s_0,s_1,s_2), \gamma_n(s_0,s_1,s_2)\big)$$

Proof. Let $P = (\mathcal{L}, s_0, s_1, s_2) \in \mathcal{E}_{\mathcal{R}_\Delta}(R)$. Then we have $nP = [n]_{\mathcal{E}} P$, hence

$$\begin{aligned}
(nP)^*\big(\mathcal{O}_{\mathcal{E}}(1)\big) &= P^*[n]_{\mathcal{E}}^*\big(\mathcal{O}_{\mathcal{E}}(1)\big) = P^*\big(\mathcal{O}_{\mathcal{E}}(n^2)\big) = \mathcal{L}^{\otimes n^2}, \\
(nP)^* x &= P^*[n]_{\mathcal{E}}^* x = P^*\alpha_n = \alpha_n(s_0,s_1,s_2), \\
(nP)^* y &= P^*[n]_{\mathcal{E}}^* y = P^*\beta_n = \beta_n(s_0,s_1,s_2), \\
(nP)^* z &= P^*[n]_{\mathcal{E}}^* z = P^*\gamma_n = \gamma_n(s_0,s_1,s_2),
\end{aligned}$$

which is as desired. □

We can generalise this result as follows.

Corollary 1.2.6. *Let R be a ring, and let E/R be a Weierstrass curve. Let n be an integer, and let S be an R-algebra. Let $P = (\mathcal{L}, s_0, s_1, s_2) \in E_R(S)$. Then R is naturally an $\mathcal{R}_\Delta$-algebra, and*

$$nP = \big(\mathcal{L}^{\otimes n^2}, \alpha_n(s_0,s_1,s_2), \beta_n(s_0,s_1,s_2), \gamma_n(s_0,s_1,s_2)\big)$$

Proof of Corollary 1.2.6. Note that by Lemma 1.2.1, every Weierstrass curve E over a ring R gives R the structure of an $\mathcal{R}_\Delta$-algebra such that E becomes the Weierstrass curve corresponding to R.

Let f denote the morphism $E \longrightarrow \mathcal{E}$ obtained by the base change of Lemma 1.2.1. Then note that f commutes with multiplication by n; if $[n]_E \colon E \longrightarrow E$ denotes the multiplication-by-n morphism on E, then $f[n]_E = [n]_{\mathcal{E}} f$.

Now note that $f^*\big(\mathcal{O}_{\mathcal{E}}(1)\big) = \mathcal{O}_E(1)$, and that $f^*x = x, f^*y = y, f^*z = z$. Now it follows from Proposition 1.2.2 that $[n]_E^*\big(\mathcal{O}_E(1)\big) = f^*\big(\mathcal{O}_{\mathcal{E}}(n^2)\big) = \mathcal{O}_E(n^2)$, and that $[n]_E^* x = \alpha_n, [n]_E^* y = \beta_n, [n]_E^* z = \gamma_n$. Hence by the same argument used in the proof of Proposition 1.2.5, it follows that for all S-valued points $P = (\mathcal{L}, s_0, s_1, s_2) \in E_R(S)$,

$$nP = \big(\mathcal{L}^{\otimes n^2}, \alpha_n(s_0,s_1,s_2), \beta_n(s_0,s_1,s_2), \gamma_n(s_0,s_1,s_2)\big).$$ □

1.3 Division polynomials

In this section, we express, for all $n \in \mathbb{Z}$, the elements $\alpha_n, \beta_n, \gamma_n \in \left(\mathcal{R}_\Delta[x,y,z]/(\mathcal{W})\right)_{n^2}$ in terms of the so-called *division polynomials* (cf. [7, Ch. 3]). This is desirable, since one can give an explicit description of the division polynomials in terms of a recurrence relation, see Proposition 1.3.1.

Let K be an algebraic closure of the fraction field of $\mathcal{R}_\Delta$, and consider the elliptic curve E over K defined by $\mathcal{W}$. Let n be an integer, and denote the multiplication-by-n map on E by $[n]_E$. By Corollary 1.2.6, it follows that $[n]_E$ is given by

$$(a : b : c) \mapsto \big(\alpha_n(a,b,c) : \beta_n(a,b,c) : \gamma_n(a,b,c)\big).$$

Hence we have the following identities of rational functions on E.

$$\frac{\alpha_n}{\gamma_n} = [n]_E^* \frac{x}{z}, \qquad\qquad \frac{\beta_n}{\gamma_n} = [n]_E^* \frac{y}{z}.$$

Let X, Y denote the rational functions $\frac{x}{z}, \frac{y}{z}$, respectively. Then $\Gamma(E - \{0\}, \mathcal{O}_E)$ is generated by X, Y, and in fact equal to $K[X,Y]/(W)$, where

$$W = z^{-3}\mathcal{W} = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6.$$

Also note that the function field $K(E)$ of E consists of the fractions $\frac{f_1}{f_2}$, where the elements $f_1, f_2 \in K[x,y,z]/(\mathcal{W})$ are homogeneous of the same degree, and $f_2 \neq 0$.

For $F \in K(E) - \{0\}$, we define its *leading coefficient* ΛF as follows. Let $\mathrm{ord}_0 F$ denote the order of F at 0. Then $\left(\frac{x}{y}\right)^{-\mathrm{ord}_0 F} F$ is a rational function that has neither a pole nor a zero at 0, since $\frac{x}{y}$ has a simple zero at 0. Hence $\left(\frac{x}{y}\right)^{-\mathrm{ord}_0 F} F$ has a well-defined non-zero value at 0. We define ΛF to be this value.

Now define for all $n \in \mathbb{Z} - \{0\}$, the *division polynomial* $\Psi_n \in K[X,Y]/(W)$ as the rational function with divisor $\sum_{P \in E[n]-\{0\}} \langle P \rangle - (n^2-1)\langle 0 \rangle$ and leading coefficient n. (Such a rational function exists, since $\sum_{P \in E[n]-\{0\}} P = 0$, and since $\#E[n] = n^2$.) Additionally, we define $\Psi_0 = 0$. By comparing divisors, it follows that Ψ_n is the unique polynomial (with Y-degree at most 1) with leading coefficient n satisfying

$$\Psi_n^2 = \begin{cases} n^2 \prod_{P \in E[n]-\{0\}} \big(X - X(P)\big) & \text{if } n \text{ is odd,} \\ \frac{1}{4} n^2 (2Y + a_1X + a_3)^2 \prod_{P \in E[n]-E[2]} \big(X - X(P)\big) & \text{if } n \text{ is even.} \end{cases}$$

We collect some properties of division polynomials in the following propositions. For their proofs, see [7, Ch. 3] ([3, Ch. 1] for Proposition 1.3.2.d). (Note, [7] uses the notation $g_n = \alpha_n/\gamma_n, h_n = \beta_n/\gamma_n$.)

Proposition 1.3.1 ([7, Prop. 3.53])**.** *Let b_2, b_4, b_6, b_8 be as in Example 1.1.3. Then the sequence $(\Psi_n)_{n \in \mathbb{Z}}$ is the unique sequence in $K[X,Y]/(W)$ satisfying the following recurrence relation.*

- $\Psi_1 = 1$;
- $\Psi_2 = 2Y + a_1X + a_3$;

- $\Psi_3 = 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8$;
- $\Psi_4 = \Psi_2\big(2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2)\big)$;
- *For all* $m, n \in \mathbb{Z}$, $\Psi_{m+n}\Psi_{m-n} = \Psi_{m+1}\Psi_{m-1}\Psi_n^2 - \Psi_{n+1}\Psi_{n-1}\Psi_m^2$.

Now define for all $n \in \mathbb{Z}$, $\Phi_n, \Omega_n \in K(E)$ as follows.

$$\Phi_n = X\Psi_n^2 - \Psi_{n-1}\Psi_{n+1} \qquad \Omega_n = \begin{cases} 1 & \text{if } n = 0 \\ \frac{1}{2\Psi_n}\big(\Psi_{2n} - \Psi_n^2(a_1\Phi_n + a_3\Psi_n^2)\big) & \text{otherwise} \end{cases}$$

Proposition 1.3.2 ([7, Cor. 3.54, Prop. 3.55], [3, Lem. 1.7.11])**.** *Let* $n \in \mathbb{Z}$.

(a) $\Psi_n \in \mathcal{R}_\Delta[X, Y]/(W)$,
(b) $\Phi_n \in \mathcal{R}_\Delta[X, Y]/(W)$, $ord_0\Phi_n = -2n^2$, $\Lambda\Phi_n = 1$,
(c) $\Omega_n \in \mathcal{R}_\Delta[X, Y]/(W)$, $ord_0\Omega_n = -3n^2$, $\Lambda\Omega_n = 1$,
(d) Ψ_n, Φ_n *generate the unit ideal in* $\mathcal{R}_\Delta[X, Y]/(W)$,

Proposition 1.3.3. *Let* $n \in \mathbb{Z} - \{0\}$, *and let* d *be a divisor of* n. *Then* Ψ_n/Ψ_d, Ψ_d *generate the unit ideal in* $\mathcal{R}_{n\Delta}[X, Y]/(W)$.

The strategy will be the same as in [3, Lem. 1.7.11]; we note that both Ψ_n^2/Ψ_d^2, Ψ_d^2 are elements of $\mathcal{R}_\Delta[X]$, and determine what the irreducible divisors of $\mathrm{Res}(\Psi_n^2/\Psi_d^2, \Psi_d^2)$ are, from which the result will follow.

Lemma 1.3.4. *Let* $\pi \in \mathcal{R}_\Delta$ *be irreducible, let* $n \in \mathbb{Z} - \{0\}$, *and let* $d \neq n$ *be a divisor of* n. *Then* $\pi \mid \mathrm{Res}(\Psi_n^2/\Psi_d^2, \Psi_d^2)$ *if and only if* $\pi \mid n$.

Proof. Note that Ψ_n^2/Ψ_d^2, Ψ_d^2 do not have common factors in $K[X]$, since by definition, Ψ_n^2 and Ψ_d^2 have order 2 at every point of $E(K)[n] - \{0\}$ and $E(K)[d] - \{0\}$, respectively. It follows that $r = \mathrm{Res}\left(\Psi_n^2/\Psi_d^2, \Psi_d^2\right) \neq 0$ in $\mathcal{R}_\Delta$.

Now let π be an irreducible divisor of r in $\mathcal{R}_\Delta$ not dividing n. Then there is an algebraically closed field k in which n is invertible, and an elliptic curve E' over k, such that $\pi = 0$ (so consequently, $r = 0$). Let E be the corresponding elliptic curve. Then Ψ_n^2/Ψ_d^2, Ψ_d^2 have a common factor in $k[X]$. But since n is invertible, we have $\mathrm{ord}_0\Psi_n = n^2 - 1$, $\mathrm{ord}_0\Psi_d = d^2 - 1$ over k. So on one hand, we know that Ψ_n must have $n^2 - 1$ zeroes in total (counted with multiplicities), and on the other hand, $\Psi_n(P) = 0$ for all $P \in E[n] - \{0\}$. Hence it follows that all of the zeroes of Ψ_n (and hence also all of those of Ψ_d) must be simple. This is a contradiction. □

Proof of Proposition 1.3.3. By a basic property of resultants, there exist $s, t \in K[X]$ such that $s\Psi_n^2/\Psi_d^2 + t\Psi_d^2 = \mathrm{Res}(\Psi_n^2/\Psi_d^2, \Psi_d^2)$. Since n is a unit in $\mathcal{R}_{n\Delta}$, and by Lemma 1.3.4, it follows that Ψ_n^2/Ψ_d^2, Ψ_d^2 generate the unit ideal in $\mathcal{R}_{n\Delta}[X, Y]/(W)$. Hence Ψ_n/Ψ_d, Ψ_d also generate the unit ideal in $\mathcal{R}_{n\Delta}[X, Y]/(W)$. □

Proposition 1.3.5 ([7, Prop. 3.55]). *If $n \neq 0$, then we have the following identities in the fraction field of $\mathcal{R}_\Delta[X,Y]/(W)$.*

$$\frac{\alpha_n}{\gamma_n} = \frac{\Phi_n}{\Psi_n^2} \qquad\qquad \frac{\beta_n}{\gamma_n} = \frac{\Omega_n}{\Psi_n^3}.$$

This motivates the following. Define $A_n = \Phi_n\Psi_n$, $B_n = \Omega_n$, $C_n = \Psi_n^3$. We would like to conclude, using Proposition 1.3.5 that α_n, β_n, γ_n are the homogenisations of A_n, B_n, C_n. This doesn't work directly, as there isn't even a unique way to homogenise A_n, B_n, C_n; these elements in $\mathcal{R}_\Delta[X,Y]/(W)$ are only defined up to a multiple of W. Moreover, the way these polynomials were defined would make the degree of A_n, B_n, C_n too high, namely roughly $\frac{3}{2}n^2$, instead of n^2. This problem is solved by choosing $A_n', B_n', C_n' \in \mathcal{R}_\Delta[X,Y]$ in the unique way such that their X-degree is at most 2, and such that in $\mathcal{R}_\Delta[X,Y]/(W)$, we have $A_n = A_n'$, $B_n = B_n'$, $C_n = C_n'$. This is possible since W is monic in X of degree 3.

Lemma 1.3.6. *The total degrees of A_n', B_n', C_n' are n^2, n^2, n^2-1, respectively.*

Proof. First, we note that the set $\{X^iY^j : i \in \{0,1,2\},\ j \geq 0\}$ has the property that its orders are pairwise distinct, and that these are by definition the only monomials occurring in A_n', B_n', C_n' with non-zero coefficient. Let X^iY^j be a monomial occurring in A_n' with non-zero coefficient. Then $2i+3j \leq -\mathrm{ord}_0 A_n' = 3n^2-1$. Hence $j < n^2$. If $j = n^2-1$, then $i \leq 1$. Hence it follows that $i+j \leq n^2$. Since $\mathrm{ord}_0 A_n' = -3n^2+1$, it follows that XY^{n^2-1} occurs in A_n' with non-zero coefficient. So the total degree of A_n' is n^2. The other results follow similarly. □

By Lemma 1.3.6, we now can define the elements $\alpha_n', \beta_n', \gamma_n' \in \left(\mathcal{R}_\Delta[x,y,z]/(\mathcal{W})\right)_{n^2}$ as $\alpha_n' = z^{n^2}A_n'$, $\beta_n' = z^{n^2}B_n'$, $\gamma_n' = z^{n^2}C_n'$. (Or equivalently, α_n', β_n' are the homogenisations of A_n', B_n', respectively, and γ_n' is z times the homogenisation of C_n'.)

Lemma 1.3.7. *Let $n \in \mathbb{Z} - \{0\}$. Then, in the fraction field of $\mathcal{R}_\Delta[X,Y]/(W)$, we have the following identities.*

$$\frac{\alpha_n'}{\alpha_n} = \frac{\beta_n'}{\beta_n} = \frac{\gamma_n'}{\gamma_n}.$$

Proof. Note that since $n \neq 0$, the map $[n]_E$ is surjective. Hence none of the polynomials α_n, β_n, γ_n can be equal to zero (since that would imply that the image of $[n]_E$ is finite). Hence the desired identity follows from 1.3.2. □

Hence we can define for $n \in \mathbb{Z}$, the rational function θ_n as the rational function $\frac{\beta_n'}{\beta_n}$. Then Proposition 1.2.5, Corollary 1.2.6, and Lemma 1.3.7 imply that, to prove that α_n', β_n', γ_n' define multiplication by n on any Weierstrass curve over any ring R, it suffices to prove the following lemma.

Lemma 1.3.8. *For all $n \in \mathbb{Z}$, $\theta_n \in \mathcal{R}_\Delta^\times = \{\pm\Delta^i : i \in \mathbb{Z}\}$.*

Proof. For $n = 0$, there is nothing to prove. Hence suppose that $n \neq 0$.

We first show that θ_n is in the fraction field of $\mathcal{R}_\Delta$ and let by Lemma 1.3.7, f denote the rational function $\frac{\alpha'_n}{\alpha_n} = \frac{\beta'_n}{\beta_n} = \frac{\gamma'_n}{\gamma_n}$. Note that for all $P \in E(K)$, by Corollary 1.2.6, we have in K^3, $\big(\alpha_n(P), \beta_n(P), \gamma_n(P)\big) \neq (0,0,0)$, so f cannot have poles. Hence f cannot have zeroes either, from which it follows that $f \in K^\times$. Now note that since W is monic in X, $\mathcal{R}_\Delta[X,Y]/(W)$ is a free $\mathcal{R}_\Delta$-module. Since $\theta_n \in K^\times$, θ_n arises as the ratio of coefficients of β'_n and β_n with respect to a basis of $\mathcal{R}_\Delta[X,Y]/(W)$. Hence θ_n is in the fraction field of $\mathcal{R}_\Delta$.

The next step is to prove that $\theta_n \in \mathcal{R}_\Delta$. By the above (and because $\mathcal{R}_\Delta$ is a unique factorisation domain), we can write θ_n as a quotient $\frac{f}{g}$ of $f, g \in \mathcal{R}_\Delta$, $g \neq 0$, in a minimal way. Then g divides all of α_n, β_n, γ_n. Note that by Proposition 1.2.5, on the universal Weierstrass curve $\mathcal{E}$, for $P = (0:1:0) \in \mathcal{E}_{\mathcal{R}_\Delta}(\mathcal{R}_\Delta)$, we have $\big(\alpha_n(P) : \beta_n(P) : \gamma_n(P)\big) = (0:1:0)$. It follows that in β_n, the coefficient of y^{n^2} is a unit. Since g divides β_n, it follows that g is a unit, so $\theta_n \in \mathcal{R}_\Delta$.

Finally, we show that $\theta_n \in \mathcal{R}_\Delta^\times$. Note that θ_n divides β'_n by definition, and that the $\mathcal{R}_\Delta$-module $\mathcal{R}_\Delta[x,y,z]/(\mathcal{W})$ is free, since $\mathcal{W}$ is monic in x. We deduce that θ_n must divide every coefficient of β'_n. But 1 occurs as the coefficient of y^{n^2} in β'_n, since $\Lambda\Omega_n = 1$. We deduce that $\theta_n \in \mathcal{R}_\Delta^\times$, as desired. □

From this lemma, we deduce a fully explicit version of 1.2.6.

Theorem 1.3.9. *Let R be a ring, and let E/R be a Weierstrass curve. Let n be an integer, and let S be an R-algebra. Let $P = (\mathcal{L}, s_0, s_1, s_2) \in E_R(S)$. Then R is naturally an $\mathcal{R}_\Delta$-algebra, and*

$$nP = \big(\mathcal{L}^{\otimes n^2}, \alpha'_n(s_0,s_1,s_2), \beta'_n(s_0,s_1,s_2), \gamma'_n(s_0,s_1,s_2)\big).$$

Remark 1.3.10. Note that choosing homogenizations of different representatives of A_n, B_n, C_n in $\mathcal{R}_\Delta[x,y,z]/(\mathcal{W})$ will change the polynomials obtained by a (not necessarily common) power of z. So in that case (for example if we homogenise A_n, B_n, C_n directly), the above corollary will continue to hold for all $P \in E_R(S)$ of the form $(a:b:1)$. In other words, if $P \in E_R(S)$ is given by $(a:b:1)$, then nP is given by $\big((\Phi_n\Psi_n)(a,b) : \Omega_n(a,b) : \Psi_n^3(a,b)\big)$.

Example 1.3.11. Note that $\alpha'_{-1} = -x$, $\beta'_{-1} = y + a_1x + a_3z$, $\gamma'_{-1} = -z$, which generalises the fact that for elliptic curves over fields, P and $-P$ have the same X-coordinate.

Because the general formulas for α'_n, β'_n, γ'_n become very large very quickly (for $n = 4$, one would need several pages already!), we give a special case as an additional example.

Example 1.3.12. Let R be any ring in which 6 is invertible, and consider the elliptic curve E over R given by $y^2z = x^3 + z^3$. Then for small n, the polynomials α'_n, β'_n, γ'_n are given in Table 1.

One can see from these tables that if we take $R = \mathbb{F}_5$ for example, that for all $P \in E(\mathbb{F}_5)$, $5P = -P$, since for all $a \in \mathbb{F}_5$, $a^5 = a$, and since the map $a \mapsto a^3$ on $\mathbb{F}_5$ is a bijection. (Though obviously there are better ways to prove that $E(\mathbb{F}_5)$ is annihilated by 6.)

n	α'_n
-1	$-x$
0	0
1	x
2	$2xy^3 - 18xyz^2$
3	$3xy^8 - 288xy^6z^2 - 162xy^4z^4 + 1944xy^2z^6 - 729xz^8$
4	$4xy^{15} - 2124xy^{13}z^2 - 19116xy^{11}z^4 + 415044xy^9z^6 - 761076xy^7z^8$ $+ 1023516xy^5z^{10} - 1495908xy^3z^{12} + 708588xyz^{14}$
5	$5xy^{24} - 10080xy^{22}z^2 - 428490xy^{20}z^4 + 26292600xy^{18}z^6 - 70340481xy^{16}z^8$ $+ 631745568xy^{14}z^{10} - 4527798588xy^{12}z^{12} + 10098796176xy^{10}z^{14}$ $- 9589852845xy^8z^{16} + 1836660096xy^6z^{18} + 4390765542xy^4z^{20}$ $- 3099363912xy^2z^{22} + 387420489xz^{24}$

n	β'_n
-1	y
0	1
1	y
2	$y^4 + 18y^2z^2 - 27z^4$
3	$y^9 + 216y^7z^2 - 2430y^5z^4 + 3888y^3z^6 - 2187yz^8$
4	$y^{16} + 1224y^{14}z^2 - 67284y^{12}z^4 + 328536y^{10}z^6 - 1115370y^8z^8 + 367416y^6z^{10}$ $+ 1338444y^4z^{12} - 1417176y^2z^{14} + 531441z^{16}$
5	$y^{25} + 4680y^{23}z^2 - 936090y^{21}z^4 + 10983600y^{19}z^6 - 151723125y^{17}z^8$ $- 508608720y^{15}z^{10} + 3545695620y^{13}z^{12} - 12131026560y^{11}z^{14}$ $+ 27834222375y^9z^{16} - 37307158200y^7z^{18} + 27119434230y^5z^{20}$ $- 10331213040y^3z^{22} + 1937102445yz^{24}$

n	γ'_n
-1	$-z$
0	0
1	z
2	$8y^3z$
3	$27y^8z + 216y^6z^3 + 486y^4z^5 - 729z^9$
4	$64y^{15}z + 3456y^{13}z^3 + 57024y^{11}z^5 + 186624y^9z^7 - 1539648y^7z^9$ $+ 2519424y^5z^{11} - 1259712y^3z^{13}$
5	$125y^{24}z + 27000y^{22}z^3 + 1842750y^{20}z^5 + 32076000y^{18}z^7 - 497487825y^{16}z^9$ $+ 1976173200y^{14}z^{11} - 2206464300y^{12}z^{13} - 2125764000y^{10}z^{15}$ $+ 3993779115y^8z^{17} + 573956280y^6z^{19} - 2152336050y^4z^{21} + 387420489z^{25}$

TABLE 1. Values of α'_n, β'_n, γ'_n for the elliptic curve given by $y^2z = x^3 + z^3$.

1.4 Torsion points

Throughout this section, R will denote a ring, and E will denote a Weierstrass curve over R. Let S be an R-algebra. We would like to consider, for all $n \in \mathbb{Z}$ non-zero, the subgroup $E_R(S)[n]$.

Proposition 1.4.1. *Let S be an R-algebra, and let $n \in \mathbb{Z}$. Let $P \in E_R(S)$ be a point of the form $(a : b : 1)$. Then $nP = 0$ if and only if $\Psi_n(P) = \Psi_n(a, b) = 0$.*

Proof. If $\Psi_n(P) = 0$, then Remark 1.3.10 immediately implies that $nP = 0$. So now suppose that $nP = 0$. Then by Remark 1.3.10, $\Psi_n(P)^3 = 0$ and $\Phi_n(P)\Psi_n(P) = 0$. From the first equality, it follows that $\Psi_n(P)$ is nilpotent. Hence by 1.3.2.d, it follows that $\Phi_n(P)$ must be a unit. Now the second equality implies that $\Psi_n(P) = 0$. □

Let S be an R-algebra, and let T be an S-algebra. Then we have a morphism $E_R(S) \longrightarrow E_R(T)$ of groups obtained by base change to T. Hence every point $P \in E_R(S)$ induces a point $P_T \in E_R(T)$. If S and T are both fields, then it follows that this morphism is injective, so it preserves orders of points. In general, this need not be the case.

Example 1.4.2. Consider the elliptic curve E over $\mathbb{Z}/125\mathbb{Z}$ given by the Weierstrass equation $y^2z = x^3 + z^3$. Then we have a point $(5 : 1 : 0) \in E_{\mathbb{Z}/125\mathbb{Z}}(\mathbb{Z}/125\mathbb{Z})$ of order 25 (by Table 1, $5(5 : 1 : 0) = (25 : 1 : 0) \neq 0$, and $25(5 : 1 : 0) = 5(25 : 1 : 0) = 0$), that is mapped to $0 \in E_{\mathbb{Z}/125\mathbb{Z}}(\mathbb{F}_5)$ via the quotient map $\mathbb{Z}/125\mathbb{Z} \longrightarrow \mathbb{F}_5$.

We would like to know of which torsion points in $E_R(S)$ the order is preserved by the group morphism $E_R(S) \longrightarrow E_R(T)$ induced by $S \longrightarrow T$ for all non-zero S-algebras T. For this, we will use the following definition.

Definition 1.4.3. Let n be a non-zero integer. Let S be an R-algebra. A point P in $E_R(S)$ is *of universal order n* if $nP = 0$, and P is of order n in all fibres of $E_S \longrightarrow \operatorname{Spec} S$.

Note that a point of universal order n has order n in $E_R(S)$, if $S \neq 0$. Also note that for any non-zero S-algebra T, every fibre of $E_T \longrightarrow \operatorname{Spec} T$ arises as the base change of a fibre of $E_S \longrightarrow \operatorname{Spec} S$ with $\operatorname{Spec} T \longrightarrow \operatorname{Spec} S$. Hence the map $E_R(S) \longrightarrow E_R(T)$ induced by T preserves orders of points of some universal order. Conversely, if $P \in E_R(S)$ is a point of order n such that for all non-zero S-algebras T, the image of P under the map $E_R(S) \longrightarrow E_R(T)$ is also of order n, then it holds in particular for all fibres of $E_S \longrightarrow \operatorname{Spec} S$, so P is of universal order n. Hence the points of some universal order are indeed exactly the torsion points in $E_R(S)$ of which the order is preserved by the group morphism $E_R(S) \longrightarrow E_R(T)$ induced by $S \longrightarrow T$ for all non-zero S-algebras T, justifying our terminology.

We describe the points $P \in E_R(S)[n]$ that are of universal order n more explicitly.

Lemma 1.4.4. *Let n be a non-zero integer. Let $\mathcal{L}$ be a line bundle on $\operatorname{Spec} R$, and let $s \in \Gamma(\operatorname{Spec} R, \mathcal{L})$. Then s generates $\mathcal{L}$ if and only if for all fields k, and all morphisms $f\colon \operatorname{Spec} k \longrightarrow \operatorname{Spec} R$, we have $f^*s \neq 0$.*

Proof. If s generates $\mathcal{L}$, then $\mathcal{O}_R \cong \mathcal{L}$ (via multiplication by s). Under this isomorphism, for every $f\colon \operatorname{Spec} k \longrightarrow \operatorname{Spec} R$, where k is a field, $f^*s = f^*1 = 1$.

Now suppose that s does not generate $\mathcal{L}$, then there is a point P in $\operatorname{Spec} R$ such that $s \in \mathfrak{m}_P \mathcal{L}_P$. Then for the morphism $\operatorname{Spec} \kappa(P) \xrightarrow{f} \operatorname{Spec} R$, we have $f^*s = 0$. □

Lemma 1.4.5. *Let S be an R-algebra, and let $P \in E_R(S)$. Let $n \in \mathbb{Z} - \{0\}$. Then $nP \neq 0$ in every fibre of $E_S \longrightarrow \operatorname{Spec} S$ if and only if P is of the form $(a : b : 1)$ and $\Psi_n(P) \in S^\times$.*

Proof. First suppose that $P = (\mathcal{L}, s_0, s_1, s_2) \in E_R(S)$ is such that nP is non-zero in any fibre of $E_S \longrightarrow \operatorname{Spec} S$. Then in particular, $P \neq 0$ in any fibre of $E_S \longrightarrow \operatorname{Spec} S$. By Lemma 1.4.4, this implies that s_2 generates $\mathcal{L}$, hence $\mathcal{L} \cong \mathcal{O}_S$, and $s_2 \in S^\times$ under this isomorphism. We deduce that P is of the form $(a : b : 1)$.

Then by Proposition 1.4.1 and Lemma 1.4.4, it follows that since $nP \neq 0$ in any fibre of $E_S \longrightarrow \operatorname{Spec} S$, we must have $\Psi_n(P) \in S^\times$.

For the converse, note that if $P \in E_R(S)$ is of the form $(a : b : 1)$ and $\Psi_n(P) \in S^\times$, then by Proposition 1.4.1 and Lemma 1.4.4, both P and nP are non-zero in all fibres of $E_S \longrightarrow \operatorname{Spec} S$. □

Theorem 1.4.6. *Let S be an R-algebra, and let $P \in E_R(S)$. Let $n \in \mathbb{Z} - \{-1, 0, 1\}$. Then P is of universal order n if and only if P is of the form $(a : b : 1)$, $\Psi_n(P) = 0$, and $\Psi_d(P) \in S^\times$ for all divisors $d < n$ of n.*

Proof. Follows directly from Lemma 1.4.5. □

Now we define polynomials $F_n \in \mathcal{R}_\Delta[X, Y]/(W)$ as follows.

$$\begin{aligned} F_0 &= \Psi_0 = 0, \\ F_1 &= \Psi_1 = 1, \\ F_n &= \Psi_n \prod_{d \mid n, d \neq n} F_d^{-1}, \qquad \text{for } n \geq 2. \end{aligned}$$

The first values of F_n are given in Table 2, where b_2, b_4, b_6, b_8 are as in Example 1.1.3.

n	F_n
0	0
1	1
2	$2Y + a_1X + a_3$
3	$3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8$
4	$2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2)$

TABLE 2. The first values of F_n.

We have the following immediate consequence of Theorem 1.4.6.

Corollary 1.4.7. *Let S be an R-algebra, and let $P \in E_R(S)$. Let $n \in \mathbb{Z}_{>1}$. If P is of universal order n, then P is of the form $(a : b : 1)$, and $F_n(P) = 0$.*

Example 1.4.8. The converse need not be true in general. Let $R = \mathbb{Z}/4\mathbb{Z}$, and let E be the elliptic curve over R given by the Weierstrass equation $y^2z + xyz + yz^2 - x^3 + x^2z + xz^2$. Then $b_2 = -3$, $b_4 = -1$, $b_6 = 1$, $b_8 = -1$, and E has discriminant 17, which is invertible in R.

Consider the point $P = (3 : 1 : 1) \in E_R(R)$. Then $F_4(P) = 0$, and $2P \neq 0$, since $-y - x - z \neq y$ in $\mathbb{Z}/4\mathbb{Z}$. Hence P is of order 4 in $E_R(R)$. But its induced point $P_{\mathbb{F}_2} \in E_R(\mathbb{F}_2)$ is given by the point $P_{\mathbb{F}_2} = (1 : 1 : 1) \in E_R(\mathbb{F}_2)$, which is of order 2. Hence P is not a point of any universal order.

We do have the following partial converse.

Theorem 1.4.9. *Let S be an R-algebra, and let $P \in E_R(S)$. Let $n > 1$ be an integer, and suppose that n is invertible in R. Then P is of universal order n if and only if P is of the form $(a : b : 1)$, and $F_n(P) = 0$.*

Since Ψ_n/Ψ_d, Ψ_d are multiples of F_n, Ψ_d, respectively, we have the following consequence of Proposition 1.3.3.

Corollary 1.4.10. *Let $n \in \mathbb{Z}_{>0}$, and suppose that n is invertible in R. Then F_n and Ψ_d generate the unit ideal in $R[X, Y]/(W)$.*

Proof of Theorem 1.4.9. If $P \in E_R(S)$ is of universal order n, then by Corollary 1.4.7, P is of the form $(a : b : 1)$, and $F_n(P) = 0$.

Suppose that $P \in E_R(S)$ is of the form $(a : b : 1)$, and $F_n(P) = 0$. Then by Corollary 1.4.10, it follows that for all positive $d \mid n$ with $d \neq n$, $\Psi_d(P) \in S^\times$. Hence by Theorem 1.4.6, it follows that P is a point of universal order n. □

2 Algebraic models of the modular curve $Y_1(N)$

2.1 Modular curves and modular forms

We give a definition of modular curves (in particular the modular curve $Y_1(N)$) and modular forms, cf. [5, Ch. 1].

Let $\mathcal{L} = \{(\tau_1, \tau_2) \in \mathbb{C}^2 : \tau_1\mathbb{R} + \tau_2\mathbb{R} = \mathbb{C},\ \mathrm{im}\,\frac{\tau_2}{\tau_1} > 0\}$. Then the group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{L}$ via $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(\tau_1, \tau_2) = (c\tau_2 + d\tau_1, a\tau_2 + b\tau_1)$. So the orbits of $\mathcal{L}$ are exactly the sets $\mathcal{B}_\Lambda$ of all positively oriented $\mathbb{Z}$-bases of a lattice $\Lambda \subseteq \mathbb{C}$.

Note that this group action commutes with scaling, so we get a group action on $\mathcal{L}$ modulo scaling. Since every element of $\mathcal{L}$ can be scaled uniquely to one of the form $(1, \tau)$, with τ in the complex upper half plane $\mathbb{H}$, we get the $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathbb{H}$ given by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau = \frac{a\tau+b}{c\tau+d}$.

Definition 2.1.1. The *modular curve* Y is the (topological) quotient space of $\mathbb{H}$ under the $\mathrm{SL}_2(\mathbb{Z})$-action given by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau = \frac{a\tau+b}{c\tau+d}$.

From the way we defined the action on $\mathbb{H}$, it is clear that Y corresponds bijectively to isomorphism classes of elliptic curves over $\mathbb{C}$, where $\tau \in Y$ corresponds to the elliptic curve given by the lattice $\mathbb{Z} + \mathbb{Z}\tau \subseteq \mathbb{C}$.

Definition 2.1.2. Let N be a positive integer. Then the *principal congruence subgroup* $\Gamma(N)$ of *level* N is the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, d \equiv 1 \pmod N$, $b, c \equiv 0 \pmod N$. Any subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that contains a principal congruence subgroup is called a *congruence subgroup*.

So in particular, $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. We give some more examples of important congruence subgroups.

Example 2.1.3. Let N be a positive integer. Then the subgroup $\Gamma_1(N)$ of $\mathrm{SL}_2(\mathbb{Z})$ consisting of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, d \equiv 1 \pmod N$ and $c \equiv 0 \pmod N$ is a congruence subgroup, and so is the subgroup $\Gamma_0(N)$ of $\mathrm{SL}_2(\mathbb{Z})$ consisting of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $c \equiv 0 \pmod N$.

Definition 2.1.4. Let Γ be a congruence subgroup. Then the *modular curve corresponding to* Γ is the (topological) quotient space of $\mathbb{H}$ under the Γ-action given by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau = \frac{a\tau+b}{c\tau+d}$. In the special cases in which $\Gamma = \Gamma_0(N)$ or $\Gamma = \Gamma_1(N)$ for some positive integer N, we denote this modular curve by $Y_0(N)$ and $Y_1(N)$, respectively.

We now define modular forms. Let $\mathcal{M}(\mathbb{H})$ denote the set of all meromorphic functions $\mathbb{H} \longrightarrow \mathbb{C}$, and let k be an integer. Then for any element $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $f \in \mathcal{M}(\mathbb{H})$, define $\gamma_k^* f \in \mathcal{M}(\mathbb{H})$ as the function $\tau \mapsto (c\tau + d)^{-k} f(\gamma\tau)$. This gives for every integer k an $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathcal{M}(\mathbb{H})$, by the description of the $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathcal{L}$ modulo scaling given earlier.

Definition 2.1.5. Let k be an integer, and let Γ be a congruence subgroup. Then $f \in \mathcal{M}(\mathbb{H})$ is called *weakly modular of weight k with respect to* Γ if f is invariant under the Γ-action corresponding to k.

Let k be an integer, let Γ be a congruence subgroup, and let f be a weakly modular of weight k with respect to Γ. Since for some minimal positive integer h, we have $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$, it follows that f is periodic with period h. Let D be the complex open unit disk, and let $\epsilon\colon \mathbb{H} \longrightarrow D$ be map given by $\tau \mapsto e^{2\pi i\tau/h}$. Then there exists a unique meromorphic $g\colon D - \{0\} \longrightarrow \mathbb{C}$ such that $f = g\epsilon$. We say that f is *holomorphic at* ∞ if g is holomorphic at 0. If f is holomorphic and holomorphic at ∞, then g is holomorphic as well. So in this case, via the Taylor expansion of g at 0, f obtains a *q-expansion* $\sum_{n\geq 0} a_n(f)q^n$, where $q = e^{2\pi i\tau/h}$.

Definition 2.1.6. Let k be an integer, and let Γ be a congruence subgroup. Then $f \in \mathcal{M}(\mathbb{H})$ is a *modular form of weight k with respect to* Γ if f is holomorphic, and invariant under the Γ-action corresponding to k, and if for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma_k^* f$ is holomorphic at ∞.

Definition 2.1.7. Let k be an integer, and let Γ be a congruence subgroup. Then $f \in \mathcal{M}(\mathbb{H})$ is a *cusp form of weight k with respect to* Γ if it is a modular form of weight k with respect to Γ, and for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we have $a_0(\gamma_k^* f) = 0$ in the q-expansion of $\gamma_k^* f$.

We denote the sets of modular forms and cusp forms of weight k with respect to Γ respectively by $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$. Note that $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$ have a natural structure of a $\mathbb{C}$-vector space.

We will be especially interested in the case where $\Gamma = \Gamma_1(N)$, for $N \geq 4$, and where $k = 3$. In this case, we have an explicit formula for the dimensions of the space $\mathcal{S}_k(\Gamma)$.

Proposition 2.1.8 ([5, Fig. 3.4])**.** *Let N be a positive integer. Then* $\dim \mathcal{S}_3\big(\Gamma_1(N)\big) = 0$ *if* $N \leq 4$*, and otherwise,*

$$\dim \mathcal{S}_3\big(\Gamma_1(N)\big) = \tfrac{1}{12}N^2 \prod_{p \mid N} \big(1 - \tfrac{1}{p^2}\big) - \tfrac{1}{4} \sum_{d \mid N} \phi(d)\phi\big(\tfrac{N}{d}\big),$$

where p ranges over all the prime divisors of N, d ranges over all the positive divisors of N, and ϕ denotes the Euler totient function.

For future reference, we list $\dim \mathcal{S}_3\big(\Gamma_1(N)\big)$ for small values of N in Table 3.

N	1	2	3	4	5	6	7	8	9	10
$\dim \mathcal{S}_3\big(\Gamma_1(N)\big)$	0	0	0	0	0	0	1	1	2	4

TABLE 3. Dimension of $\mathcal{S}_3\big(\Gamma_1(N)\big)$ for small values of N

2.2 The modular curve $Y_1(N)$

The remainder of this chapter will be dedicated to give an algebraic description of $Y_1(N)$. To do this, we give a bijective correspondence between $Y_1(N)$ and the set of all isomorphism classes of pairs (E, P) of an elliptic curve E over $\mathbb{C}$, and a point $P \in E(\mathbb{C})$ of order N.

We study the $\Gamma_1(N)$-orbits of $\mathcal{L}$. Let $(\tau_1, \tau_2) \in \mathcal{L}$, and let $\Lambda = \tau_1\mathbb{Z} + \tau_2\mathbb{Z}$. Then $\Gamma_1(N)(\tau_1, \tau_2)$ is the set of positively oriented $\mathbb{Z}$-bases (τ_1', τ_2') such that $\frac{1}{N}(\tau_1 - \tau_1') \in \Lambda$. Hence every $\Gamma_1(N)$-orbit of $\mathcal{L}$ corresponds bijectively with a lattice Λ in $\mathbb{C}$, together with a point $P \in \mathbb{C}/\Lambda$ of

order N, (where (τ_1, τ_2) corresponds to the lattice $\Lambda = \mathbb{Z}\tau_1 + \mathbb{Z}\tau_2$, together with the point $\frac{1}{N}\tau_1 \in \mathbb{C}/\Lambda$). Modulo scaling, this gives us the desired correspondence.

So to construct a model of $Y_1(N)$, one would like to parametrize the isomorphism classes of pairs (E, P) of an elliptic curve E and a point $P \in E(\mathbb{C})$ of order N. We have the following. (See also [1]).

Proposition 2.2.1. *For every pair (E, P) of an elliptic curve E over $\mathbb{C}$ with a point P on E such that $2P \neq 0$ and $3P \neq 0$, there are unique $\sigma, \tau \in \mathbb{C}$ such that (E, P) is isomorphic to $\big(E_{\sigma,\tau}, (0:0:1)\big)$, where*

$$E_{\sigma,\tau} \colon y^2z + \sigma xyz + \tau yz^2 = x^3 + \tau x^2 z.$$

Moreover, the isomorphism $(E, P) \longrightarrow \big(E_{\sigma,\tau}, (0:0:1)\big)$ is unique.

Proof. Write E in some Weierstrass form.

$$E \colon y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

First note that any isomorphism between elliptic curves in Weierstrass form is of the form $(x : y : z) \mapsto (\alpha^2 x + az : \alpha^3 y + bx + cz : z)$, with $\alpha \in \mathbb{C}^\times$, $a, b, c \in \mathbb{C}$, hence can be written uniquely as a composition of a translation, a map of the form $(x : y : z) \mapsto (x : y + bx : z)$, and a scaling.

Note that P is not the point at infinity, so there is a unique translation sending P to $(0 : 0 : 1)$, making $a_6 = 0$. Since $2P \neq 0$, the line given by $x = 0$ is not a tangent of E at P, so $a_3 \neq 0$. Hence there is a unique map of the form $(x : y : z) \mapsto (x : y + bx : z)$ sending the tangent T of E at P to the line given by $y = 0$, making $a_4 = 0$. Finally, since $3P \neq 0$, the line given by $y + a_1x + a_3z = 0$ is not an inflexion, so $a_2 \neq 0$. Hence there is a unique scaling making a_2 and a_3 equal.

The result follows. □

Let $\Delta = -t^3\big(16t^2 + (8s^2 - 36s + 27)t + (s-1)s^3\big) \in \mathbb{Z}[s, t]$. Then for all $\sigma, \tau \in \mathbb{C}$, $\Delta(\sigma, \tau)$ is the discriminant of the cubic curve $E_{\sigma,\tau}$.

We wish to find the set of $(\sigma, \tau) \in \mathbb{C}^2$ such that $\Delta(\sigma, \tau) \neq 0$, and the point $(0 : 0 : 1)$ in $E_{\sigma,\tau}$ is of a given order N. Define $\psi_n \in \mathbb{Z}[s, t]$ as the value of the division polynomial Ψ_n (as defined in Section 1.3) at $(0, 0)$, with $a_1 = s$, $a_2 = a_3 = t$, $a_4 = a_6 = 0$. So these ψ_n satisfy the recurrence relation given in Proposition 1.3.1. By Proposition 1.4.1, $\psi_n = 0$ if and only if $n(0 : 0 : 1) = 0$.

Since $\Delta(\sigma, \tau)$ is required to be non-zero, this property still holds if we replace ψ_n with ψ'_n, where ψ'_n is obtained from ψ_n by removing all of its common factors with Δ. In fact, by [1, Thm. 3.4], $\psi'_n = t^{-\lfloor n^2/3 \rfloor}\psi_n$. Hence we can define polynomials $F_n \in \mathbb{Z}[s, t]$ recursively via the relation $\prod_{d \mid n} F_d = \psi'_n$, for all positive integers n. Note that these differ only by a power of t from the F_n given in Section 1.4. By Theorem 1.4.9 these polynomials have the following property.

Theorem 2.2.2. *Let N be a positive integer, and let $\sigma, \tau \in \mathbb{C}$ with $\Delta(\sigma, \tau) \neq 0$. Then $(0 : 0 : 1) \in E_{\sigma,\tau}$ is of order N if and only if $F_N(\sigma, \tau) = 0$.*

N	g	F_N
1	0	1
2	0	1
3	0	1
4	0	$s-1$
5	0	$s-1-t$
6	0	$s^2-3s+2+t$
7	0	$(s-1)^3-(s-1)t+t^2$
8	0	$(s-1)^2(t+1)-3(s-1)t+2t^2$
9	0	$(s-2)(s-1)^4+(s-1)^3(t+1)-3(s-1)^2t+3(s-1)t^2-t^3$
10	0	$(s-1)^5+(s-1)^4t-3(s-1)^3t+(s-1)^2(3t^2+t)-2(s-1)t^2+t^3$
11	1	$(s-1)^7t-(s-1)^6(3t+1)+3(s-1)^5t(t+2)-9(s-1)^4t^2$ $+(s-1)^3t^2(4t-1)+3(s-1)^2t^3-3(s-1)t^4+t^5$

TABLE 4. The first values of F_N.

The first values of F_N and the genera of $Y_1(N)$ are listed in Table 4, cf. [1, Tab. 1]. (Note that [1] uses the notation $f = t, g = s - 1$.)

In this way, we obtain models $Y_1(N)_{\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[s,t,1/\Delta]/(F_N)$ of $Y_1(N)$ over $\mathbb{Z}$, for all $N \geq 4$.

2.3 Universal elliptic curves

We now define, for all integers N, what a universal elliptic curve with a point of universal order N is. Then we will show that it exists if $N \geq 4$, by giving an explicit description.

Definition 2.3.1. For a positive integer N, a *universal elliptic curve with a point of universal order N* (or simply *universal elliptic curve* if it is clear from the context what N is,) is an elliptic curve $\mathcal{E}$ over a $\mathbb{Z}[1/N]$-scheme $\mathcal{S}$, together with a point $\mathcal{P} \in \mathcal{E}(\mathcal{S})$ of universal order N, with the property that any elliptic curve E/S with S a $\mathbb{Z}[1/N]$-scheme, together with a point $P \in E(S)$ of universal order N, arises by a unique base change of $\mathcal{E}/\mathcal{S}$ compatible with P and $\mathcal{P}$.

Let $X = \operatorname{Proj} \mathbb{Z}[x,y,z] \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} \mathbb{Z}[s,t]$. Let $\mathcal{W} = y^2z + sxyz + tyz^2 - x^3 - tx^2z$. Consider, for $N \geq 4$, the closed subscheme E_N of X defined by $\mathcal{W}$ and F_N. Then we have a morphism $\phi\colon E_N \longrightarrow Y_1(N)_{\mathbb{Z}}$, of which all the fibres are elliptic curves, since the discriminant $\Delta = -t^3\big(16t^2 + (8s^2 - 36s + 27)t + (s-1)s^3\big)$ is invertible. After base change to $\operatorname{Spec} \mathbb{Z}[1/N]$, we obtain a morphism $\mathcal{E}_N \longrightarrow Y_1(N)_{\mathbb{Z}[1/N]}$. Let $\mathcal{P} = (0:0:1) \in \mathcal{E}_N\big(Y_1(N)_{\mathbb{Z}[1/N]}\big)$.

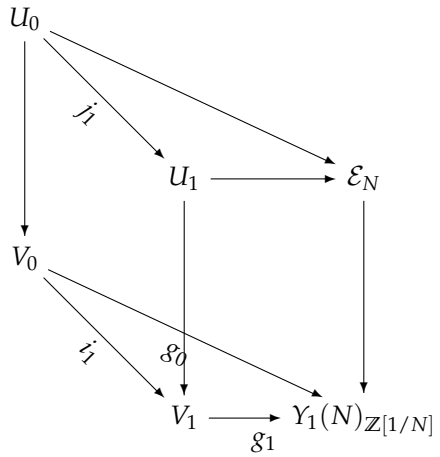
Proposition 2.3.2. *For $N \geq 4$, the pair $\big(\mathcal{E}_N/Y_1(N)_{\mathbb{Z}[1/N]}, \mathcal{P}\big)$ defined above is a* universal elliptic curve *with a point of universal order N.*

We first describe the pair $\big(\mathcal{E}_N/Y_1(N)_{\mathbb{Z}[1/N]}, \mathcal{P}\big)$ more explicitly. Note that $Y_1(N)_{\mathbb{Z}[1/N]} = \operatorname{Spec} \Gamma$, where $\Gamma = \mathbb{Z}[s,t,1/N,1/\Delta]/(F_N)$. Then we also have $\mathcal{E}_N = \operatorname{Proj} \Gamma[x,y,z]/(\mathcal{W})$. Then we note that the point $\mathcal{P} = (0:0:1)$ is indeed of universal order N in $\mathcal{E}_N$, by Theorem 1.4.9.

The following lemma allows us to view the problem locally on the base.

Lemma 2.3.3. *Let E/S be an elliptic curve, and let $\{W_i\}$ be an affine open cover of S that is a basis for the topology of S. Assume that for all i, $f^{-1}[W_i]/W_i$ arises from a unique base change of $\mathcal{E}_N/Y_1(N)_{\mathbb{Z}[1/N]}$, compatible with $P|_{W_i}$ and $\mathcal{P}$. Then E/S also arises from a unique base change of $\mathcal{E}_N/Y_1(N)_{\mathbb{Z}[1/N]}$, compatible with $P|_{W_i}$ and $\mathcal{P}$.*

Proof. Let E/S and $\{W_i\}$ be as in the proposition. Let $V_1, V_2 \in \{W_i\}$ be two of these affine open subsets of S, and let $V_0 \subseteq V_1 \cap V_2$ be another affine open subset of S in $\{W_i\}$. For $j = 0, 1, 2$, let $U_j = f^{-1}[V_j]$ and let g_j denote the unique morphism $V_j \longrightarrow Y_1(N)_{\mathbb{Z}[1/N]}$ making U_j the fibred product of $\mathcal{E}_N$ and V_j over $Y_1(N)_{\mathbb{Z}[1/N]}$. Consider the following diagram, where i_1, j_1 are open immersions.



We want to show that $g_0 = g_1 \circ i_1$. Note that the squares containing g_0 or g_1 are Cartesian by assumption, and that the square containing i_1 is Cartesian since i_1 and j_1 are open immersions, and since U_0 and U_1 are inverse images of V_0 and V_1 under f. It follows that the square containing $g_1 \circ i_1$ is also Cartesian. By assumption, U_0/V_0 arises from a *unique* base change of $\mathcal{E}_N/Y_1(N)_{\mathbb{Z}[1/N]}$. Hence $g_0 = g_1 \circ i_1$. The same argument now also shows that $g_0 = g_2 \circ i_2$, where $i_2 \colon U_0 \longrightarrow U_2$ is the open immersion. From this, we deduce that g_1 and g_2 agree on V_0.

Hence we can glue the morphisms $W_i \longrightarrow Y_1(N)_{\mathbb{Z}[1/N]}$ to a unique morphism from S to $Y_1(N)_{\mathbb{Z}[1/N]}$, such that $E = \mathcal{E}_N \times_{Y_1(N)_{\mathbb{Z}[1/N]}} Y_1(N)_{\mathbb{Z}[1/N]}$, which is compatible with P and $\mathcal{P}$. □

Proof of Proposition 2.3.2. Let $f \colon E \longrightarrow S$ be an arbitrary elliptic curve, where S is a $\mathbb{Z}[1/N]$-scheme, and let $P \in E(S)$ be of universal order N. To show that E/S arises from a unique base change of $\mathcal{E}_N/Y_1(N)_{\mathbb{Z}[1/N]}$ compatible with P and $\mathcal{P}$, it suffices by Lemma 2.3.3 to show this locally on affine open subsets of the base.

Now note that E/S is locally (on the base) Weierstrass, i.e. S admits an affine open cover $\{W_i\}$ such that $f^{-1}[W_i]/W_i$ is a Weierstrass curve. Since for all principal opens U of W_i, $f^{-1}[U]/U$ is again a Weierstrass curve, we may also assume that $\{W_i\}$ is a basis for the topology of S.

So it suffices to show that for a ring R, and a Weierstrass equation W, the Weierstrass curve $E' = \operatorname{Proj} R[x,y,z]/(W)$ over $S' = \operatorname{Spec} R$, together with a point $P \in E'(S')$ of universal order N, arises from a unique base change of $\mathcal{E}_N/Y_1(N)_{\mathbb{Z}[1/N]}$, compatible with P and $\mathcal{P}$. So let R, W, E', S', P be as above. Then by an argument similar to the one used to prove Proposition 2.2.1 (using Lemma 1.4.5 to guarantee that certain elements are invertible), there is a unique Weierstrass equation W' of the form

$$y^2z + s'xyz + t'yz^2 - x^3 - t'x^2z, \qquad s' \in R,\ t' \in R^\times,$$

such that (E', P) is uniquely isomorphic to $E'' = \operatorname{Proj} R[x,y,z]/(W')$, together with the point $P' = (0:0:1)$. This determines a morphism

$$\mathbb{Z}[s,t,1/N,1/\Delta] \longrightarrow R,\ s \mapsto s',\ t \mapsto t'.$$

Since $(0:0:1)$ is of universal order N in $E''(R)$, by Theorem 1.4.9, it follows that $F_N(s',t') = 0$. Hence we get a morphism $\Gamma \longrightarrow R$, $s \mapsto s'$, $t \mapsto t'$, such that E'/R arises from base change by this (by construction unique) morphism.

It follows that $\mathcal{E}_N/Y_1(N)_{\mathbb{Z}[1/N]}$, together with the point $\mathcal{P}$, is indeed a universal elliptic curve. □

3 Formulae for the number of $\mathbb{F}_q$-rational points on $\mathcal{E}_N$

We give formulae for the number of $\mathbb{F}_q$-rational points on $\mathcal{E}_N$ for small N. Since these formulae will tend to contain Kronecker symbols, we define them first, and list some basic properties without proof. See for example [13] for more details.

3.1 The Kronecker symbol

Definition 3.1.1. Let p be an odd prime, and let a be an integer. Then the *Legendre symbol* $\left(\frac{a}{p}\right)$ is the integer in $\{-1, 0, 1\}$ such that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Or equivalently, $\left(\frac{a}{p}\right)$ is equal to 1 if a is a quadratic residue modulo p, to 0 if it is divisible by p, and to -1 if it is a non-quadratic residue modulo p.

We can extend the Legendre symbol $\left(\frac{a}{n}\right)$ to all positive odd n in a multiplicative way, and the result is called the *Jacobi symbol*. The Jacobi symbol has the following properties.

Proposition 3.1.2. *Let a and b be two integers, and let m, n be coprime odd numbers. Then the following holds.*

(1) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$,
(2) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$,
(3) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$,
(4) $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{(n-1)(m-1)/4}$.

Finally, we can further extend the Jacobi symbol to all integers n, by defining for $a \in \mathbb{Z}$,

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & 2 \mid a, \\ \left(\frac{2}{a}\right) & 2 \nmid a, \end{cases}$$
$$\left(\frac{a}{-1}\right) = \operatorname{sgn} a,$$

and extending multiplicatively. The result is called the *Kronecker symbol*. This Kronecker symbol has the following property.

Proposition 3.1.3. *Let $a, b \in \mathbb{Z}$ be two integers, and let q be a prime power. Then the polynomial $x^2 + ax + b$ splits into two distinct factors over $\mathbb{F}_q$ if and only if $\left(\frac{\Delta}{q}\right) = 1$, where $\Delta = a^2 - 4b$ is the discriminant of $x^2 + ax + b$.*

We now give formulae for $\#E_N(\mathbb{F}_q)$ for prime powers q coprime to N.

3.2 Formula for $N = 4$

Proposition 3.2.1. *Let q be a power of an odd prime. Then $\#\mathcal{E}_4(\mathbb{F}_q) = q^2 - q - 1 + \left(\frac{-1}{q}\right)$.*

Proof. Recall that $F_4 = s - 1$, so $\mathcal{E}_4$ is given by the equation $y^2z + xyz + tyz^2 = x^3 + tx^2z$, under the condition that $\Delta = -t^4(16t - 1) \neq 0$. This holds if and only if $t \neq 0$ and $t \neq \frac{1}{16}$.

First, we calculate $\#E_4(\mathbb{F}_q)$, where E_4 is the closed subscheme of $\operatorname{Proj}\mathbb{Z}[x,y,z]\times\operatorname{Spec}\mathbb{Z}[s,t]$ defined by the equation $y^2z+xyz+tyz^2=x^3+tx^2z$; we will deal with the singular $\mathbb{F}_q$-fibres later.

We dehomogenize the equation for E_4, to get the affine equation $y^2+xy+ty=x^3+tx^2$. We rewrite this as $t(y-x^2)=x^3-y^2-xy$. We solve this linear equation in t for all $(x,y)\in\mathbb{F}_q^2$. Let $(x,y)\in\mathbb{F}_q^2$. Then there is a unique solution for t if and only if $y-x^2\neq 0$, q solutions for t if and only if $y-x^2=0$ and $x^3-y^2-xy=0$, and no solutions otherwise. Note that there are q^2-q pairs satisfying $y-x^2\neq 0$. Now suppose that $y-x^2=0$ and $y^2+xy-x^3=0$. Then $xy-x^3=0$, implying that $y^2=0$. We deduce that $(0,0)$ is the unique pair satisfying $y-x^2=0$ and $x^3-y^2-xy=0$. Hence the equation $y^2+xy+ty=x^3+tx^2$ has $q^2-q+q=q^2$ solutions. Adding the q points of infinity (one for every $t\in\mathbb{F}_q$) yields $\#E_4(\mathbb{F}_q)=q^2+q$.

Now note that the singular cubic curve $y^2z+xyz=x^3$ given by $t=0$ has a double point with rational tangents, hence its number of $\mathbb{F}_q$-rational points is q. Consider the singular cubic curve $y^2z+xyz+\frac{1}{16}yz^2=x^3+\frac{1}{16}x^2z$ given by $t=\frac{1}{16}$. After translating the point $(-\frac{1}{8}:\frac{1}{32}:1)$ to $(0:0:1)$, its equation becomes $(y^2+xy+\frac{5}{16}x^2)z=x^3$. Note that the quadratic form in the left hand side has discriminant $-\frac{1}{4}$, which is non-zero, and is a square if and only if -1 is a square in $\mathbb{F}_q$. Hence the singular point is a double point, and has rational tangents if and only if $\left(\frac{-1}{q}\right)=1$. It follows that the number of $\mathbb{F}_q$-rational points of the singular cubic curve $y^2z+xyz+\frac{1}{16}yz^2=x^3+\frac{1}{16}x^2z$ is $q+1-\left(\frac{-1}{q}\right)$.

We deduce that $\#\mathcal{E}_4(\mathbb{F}_q)=q^2-q-1+\left(\frac{-1}{q}\right)$. □

3.3 Formula for $N=5$

Proposition 3.3.1. *Let q be a prime power coprime to 5. Then*

$$\#\mathcal{E}_5(\mathbb{F}_q)=q^2+1-\left(1+\left(\tfrac{5}{q}\right)\right)q-\psi(q),$$

where $\psi=\sum_\chi\chi(-1)^{-1}\chi$, where χ ranges over all the characters modulo 5. (So $\psi(q)=4$ if and only if $q\equiv 4 \pmod 5$, and $\psi(q)=0$ otherwise.)

Proof. Recall that $F_5=s-t-1$. Hence $\mathcal{E}_5$ is given by the equation $y^2z+(t+1)xyz+tyz^2=x^3+tx^2z$, under the condition that $\Delta=-t^5(t^2+11t-1)\neq 0$. This holds if and only if $t\neq 0$ and $t^2+11t-1\neq 0$.

First, we calculate $\#E_5(\mathbb{F}_q)$, where E_5 is the closed subscheme of $\operatorname{Proj}\mathbb{Z}[x,y,z]\times\operatorname{Spec}\mathbb{Z}[s,t]$ defined by the equation $y^2z+sxyz+tyz^2=x^3+tx^2z$ and F_5; we will deal with the singular $\mathbb{F}_q$-fibres later.

Dehomogenizing the equation for E_5 gives us the affine equation $y^2+(t+1)xy+ty=x^3+tx^2$. We rewrite this as $(xy+y-x^2)t=x^3-y^2-xy$. We solve this linear equation in t for all $(x,y)\in\mathbb{F}_q^2$. Let $(x,y)\in\mathbb{F}_q^2$. Then there is a unique solution for t if and only if $xy+y-x^2\neq 0$, q solutions for t if and only if $xy+y-x^2=0$ and $x^3-y^2-xy=0$, and no solutions otherwise. Note that $xy+y-x^2\neq 0$ if and only if $x=-1$ or $y\neq\frac{x^2}{x+1}$ with $x\neq -1$. Hence q^2-q+1 pairs

satisfy this condition. Now suppose that $xy + y - x^2 = 0$ and $x^3 - y^2 - xy = 0$. Then $x^3 - xy = x^2y$, so $y(x^2 - y) = 0$. If $y = 0$, then also $x = 0$. If $x^2 - y = 0$, then as in Proposition 3.2.1, it follows that $x = 0$ and $y = 0$. Hence $(0,0)$ is the unique pair satisfying $xy + y - x^2 = 0$ and $x^3 - y^2 - xy = 0$. Hence the equation $y^2 + (t+1)xy + ty = x^3 + tx^2$ has $q^2 - q + 1 + q = q^2 + 1$ solutions. Adding the q points of infinity yields $\#E_5(\mathbb{F}_q) = q^2 + q + 1$.

Now note that the singular cubic curve $y^2z + xyz = x^3$ given by $t = 0$ has a double point with rational tangents, hence its number of $\mathbb{F}_q$-rational points is q. Hence if $t^2 + 11t - 1 = 0$ has no $\mathbb{F}_q$-rational solutions, then $\#\mathcal{E}_5(\mathbb{F}_q) = q^2 + 1$. This happens if and only if either q is an odd power of 2, or 5 is not a square in $\mathbb{F}_q$, i.e. if and only if $\left(\frac{5}{q}\right) \neq 1$. (By quadratic reciprocity, this holds if and only if $q \equiv 2, 3 \pmod 5$.)

Now suppose that $q \equiv 1, 4 \pmod 5$, let $\alpha \in \mathbb{F}_q$ be a root of $t^2 + 11t - 1 = 0$, and consider the singular cubic curve $E_s\colon y^2z + (\alpha+1)xyz + \alpha yz^2 = x^3 + \alpha x^2 z$. Note that the singular point is $(\frac{3}{5}\alpha - \frac{1}{5} : \frac{13}{5}\alpha - \frac{1}{5} : 1) \neq (0:0:1)$. Hence $(0:0:1) \in E_s^{\mathrm{sm}}(\mathbb{F}_q)$ is of order 5, so $\#E_s(\mathbb{F}_q) \equiv 1 \pmod 5$. We use this later on.

After translating the point $(\frac{3}{5}\alpha - \frac{1}{5} : \frac{13}{5}\alpha - \frac{1}{5} : 1)$ to $(0:0:1)$, the equation becomes $\big(y^2 + (\alpha+1)xy + (-\frac{14}{5}\alpha + \frac{3}{5})x^2\big)z = x^3$. Since the discriminant of the quadratic form in the left hand side is non-zero, it follows that the singular point is a double point. Hence $\#E_s(\mathbb{F}_q) \in \{q, q+2\}$. Since we also know that $\#E_s(\mathbb{F}_q) \equiv 1 \pmod 5$, it follows that if $q \equiv 1 \pmod 5$, then $\#E_s(\mathbb{F}_q) = q$, and if $q \equiv 4 \pmod 5$, then $\#E_s(\mathbb{F}_q) = q + 2$. So if we let $\psi = \sum_\chi \chi(-1)^{-1}\chi$, where χ ranges over all the characters modulo 5, then it follows that $\#E_s(\mathbb{F}_q) = q + \frac{1}{2}\psi(q)$.

Note that the argument above does not depend on the choice of α, so $\#\mathcal{E}_5(\mathbb{F}_q) = q^2 + 1 - 2\#E_s(\mathbb{F}_q) = q^2 + 1 - 2\big(q + \frac{1}{2}\psi(q)\big)$, if $q \equiv 1, 4 \pmod 5$. Together with the result for $q \equiv 2, 3 \pmod 5$, the desired result follows. □

3.4 Formula for $N = 6$

Proposition 3.4.1. *Let q be a prime power coprime to 6. Then $\#\mathcal{E}_6(\mathbb{F}_q) = q^2 - 2q + 2\big(\frac{-3}{q}\big) - 1$.*

Proof. Recall that $F_6 = (s-1)(s-2) + t$. Hence $\mathcal{E}_6$ is given by the equation

$$y^2z + sxyz - (s-1)(s-2)yz^2 = x^3 - (s-1)(s-2)x^2z$$

under the condition that $\Delta = -(s-1)^6(s-2)^3(9s-10) \neq 0$. Equivalently, under the condition that $s \neq 1$, $s \neq 2$ and $s \neq \frac{10}{9}$.

First, in the equation for $\mathcal{E}_6$, we scale x by a factor $s-1$, and y by a factor $(s-1)^2$, to obtain an equation

$$(s-1)y^2z + sxyz - (s-2)yz^2 = x^3 - (s-2)x^2z.$$

Let $X(\mathbb{F}_q) \subseteq \mathbb{P}^2_{\mathbb{F}_q} \times \mathbb{A}^1_{\mathbb{F}_q}$ denote the surface defined by this equation, and let $X'(\mathbb{F}_q)$ denote the part of $X(\mathbb{F}_q)$ where $s \notin \{1, 2, \frac{10}{9}\}$. Note that $\#\mathcal{E}_6(\mathbb{F}_q) = \#X'(\mathbb{F}_q)$.

We now dehomogenize the equation for X' to get the affine equation $(s-1)y^2+sxy-(s-2)y=x^3-(s-2)x^2$, which we can rewrite as

$$(y^2+xy-y+x^2)s=x^3+2x^2+y^2-2y. \tag{1}$$

First, we determine the number of pairs $(x,y)\in\mathbb{F}_q^2$ with $y^2+xy-y+x^2=0$ (*). Note that if we fix $x\in\mathbb{F}_q$, that then (*) has 2 solutions if and only if $(x-1)-4x^2=(x+1)(-3x+1)\in\mathbb{F}_q^{\times 2}$. Or equivalently, if and only if $x\neq -1$ and $\frac{-3x+1}{x+1}=\frac{4}{x+1}-3\in\mathbb{F}_q^{\times 2}$. Since the map $f\colon \mathbb{F}_q-\{-1,\frac{1}{3}\}\longrightarrow \mathbb{F}_q-\{-3,0\}$ given by $x\mapsto\frac{4}{x+1}-3$ is a bijection, it follows that $f(x)\in\mathbb{F}_q^{\times 2}$ for $\frac{1}{2}\big(q-2-\big(\frac{-3}{q}\big)\big)$ of the x in $\mathbb{F}_q$. Also note that (*) has 1 solution for fixed x if and only if $x=-1$ or $x=\frac{1}{3}$. Hence $q-\big(\frac{-3}{q}\big)$ pairs in $\mathbb{F}_q^2$ satisfy (*).

Next, we determine the pairs $(x,y)\in\mathbb{F}_q^2$ for which both (*) and $x^3+2x^2+y^2-2y=0$ (**) hold. Let $(x,y)\in\mathbb{F}_q^2$ be such a pair. Then $y^2+x^2=(-x+1)y$, implying that $x^3+x^2-(x+1)y=0$. Hence either $x=-1$, or $y=x^2$. In the former case, it follows that $y=1$. In the latter case, (*) becomes $x^4+x^3=0$, implying that either $x=-1$ or $x=0$, the latter implying that $y=0$. Hence the only pairs (x,y) satisfying (*) and (**) are $(0,0)$ and $(-1,1)$.

Note that the curve $Y\colon xyz+yz^2=x^3+x^2z$ given by $s=1$ has 1 point at infinity that is $\mathbb{F}_q$-rational, namely $(0:1:0)$. Also note that the number of affine $\mathbb{F}_q$-rational points is $2q-1$, since $xy+y=x^3+x^2$ if and only if $x=-1$ or $y=x^2$. Hence $\#Y(\mathbb{F}_q)=2q$. Also note that the curve $E'\colon y^2z+2xyz=x^3$ given by $s=0$ has a double point $(0:0:1)$ with rational tangents, hence $\#E'(\mathbb{F}_q)=q$. Finally, the curve $E''\colon \frac{1}{9}y^2z+\frac{10}{9}xyz+\frac{8}{9}yz^2=x^3+\frac{8}{9}x^2z$ given by $s=\frac{10}{9}$ has singular point $(\frac{-4}{3}:\frac{8}{3}:1)$. Translating this point to $(0:0:1)$, the equation for E'' becomes $\frac{1}{9}y^2z+\frac{10}{9}xyz+\frac{28}{9}yz^2=x^3$. Hence $(0:0:1)$ is a double point, which has $\mathbb{F}_q$-rational tangents if and only if $\frac{-12}{9}\in\mathbb{F}_q^{\times 2}$. Hence $\#E''(\mathbb{F}_q)=q+1-\big(\frac{-3}{q}\big)$.

Now the pairs $(x,y)\in\mathbb{F}_q^2$ for which (*) does not hold, yield $q^2-q+\big(\frac{-3}{q}\big)$ solutions of (1), and the ones for which both (*) and (**) hold, yield $2q$ solutions. Adding the q points of infinity, it follows that $\#X(\mathbb{F}_q)=q^2+2q+\big(\frac{-3}{q}\big)$. Combining this with the results for Y, E' and E'' above, it follows that

$$\#\mathcal{E}_6(\mathbb{F}_q)=\#X'(\mathbb{F}_q)=q^2-2q+2\big(\tfrac{-3}{q}\big)-1,$$

as desired. □

3.5 Discussion of formulae for higher N, empirically

The formulae for $\#\mathcal{E}_N(\mathbb{F}_q)$ for $N=7,8,9$ given below, are obtained empirically, using Sage [12]; we will elaborate on what we mean exactly by 'empirically' later.

First consider the case $N = 7$. For all $p \neq 7$ prime, and all $n \geq 0$, define a_{p^n} recursively as follows.

$$
\begin{aligned}
a_1 &= 2, \\
a_p &= \begin{cases} \alpha^2 + \overline{\alpha}^2 & \text{if } p \equiv 1,2,4 \pmod 7 \text{ and } p = \mathrm{N}(\alpha) \text{ for some } \alpha \in \mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{-7}\right], \\ 0 & \text{if } p \equiv 3,5,6 \pmod 7. \end{cases} \\
a_{p^n} &= \begin{cases} a_p a_{p^{n-1}} - p^2 a_{p^{n-2}} & \text{if } p \equiv 1,2,4 \pmod 7,\ n \geq 2, \\ p^2 a_{p^{n-2}} & \text{if } p \equiv 3,5,6 \pmod 7,\ n \geq 2. \end{cases}
\end{aligned}
$$

Furthermore, let $\psi = \sum_\chi \chi(-1)^{-1}\chi$, where χ ranges over all characters modulo 7, and let ψ' be the sum of all characters χ modulo 7 such that $\chi(-1) = 1$. (So $\psi(k) = 6$ if $k \equiv -1 \pmod 7$, and $\psi(k) = 0$ otherwise, and $\psi'(k) = 3$ if $k \equiv 1, -1 \pmod 7$, and $\psi'(k) = 0$ otherwise.) Then the formula for $\#\mathcal{E}_7(\mathbb{F}_q)$ is given by $q^2 + 1 + a_q - \big(1 + \psi(q)\big)q - \psi'(q)$.

Now consider the case $N = 8$. Then for all $p \neq 2$ prime, and all $n \geq 0$, define a_{p^n} recursively as follows.

$$
\begin{aligned}
a_1 &= 2, \\
a_p &= \begin{cases} \alpha^2 + \overline{\alpha}^2 & \text{if } p \equiv 1,3 \pmod 8 \text{ and } p = \mathrm{N}(\alpha) \text{ for some } \alpha \in \mathbb{Z}\left[\sqrt{-2}\right], \\ 0 & \text{if } p \equiv 5,7 \pmod 8. \end{cases} \\
a_{p^n} &= \begin{cases} a_p a_{p^{n-1}} - p^2 a_{p^{n-2}} & \text{if } p \equiv 1,3 \pmod 8,\ n \geq 2, \\ p^2 a_{p^{n-2}} & \text{if } p \equiv 5,7 \pmod 8,\ n \geq 2. \end{cases}
\end{aligned}
$$

Also let $\psi = \sum_\chi \chi(-1)^{-1}\chi$, where χ ranges over all characters modulo 8, and let ψ' be the sum of all characters χ modulo 8 with $\chi(-1) = 1$. (So $\psi(k) = 4$ if $k \equiv -1 \pmod 8$, and $\psi(k) = 0$ otherwise, and $\psi'(k) = 2$ if $k \equiv 1, -1 \pmod 8$, and $\psi'(k) = 0$ otherwise.) Then the formula for $\#\mathcal{E}_8(\mathbb{F}_q)$ is given by $q^2 - q + \left(\frac{-1}{q}\right) + a_q - \big(1 + \psi(q)\big)q - \psi'(q)$.

Note that we have, for all primes p coprime with N, $a_p = a_p(f)$, where f is the unique normalised cusp form in $\mathcal{S}_3\big(\Gamma_1(N)\big)$.

For $N = 9$, let α be an algebraic integer satisfying $\alpha^2 + 3\alpha + 3$. Then note that $-\alpha - 1$ is a primitive 6-th root of unity. Let ρ denote the character such that $\rho(2) = -\alpha - 1$. Let $f \in \mathcal{S}_3\big(\Gamma_1(9)\big)$ be the cusp form with q-expansion $f = q + \alpha q^2 + O(q^3)$, and let $\overline{f}$ be its conjugate (f and $\overline{f}$ are the two *newforms* in $\mathcal{S}_3\big(\Gamma_1(9)\big)$, see [5]). Define a_q for q a prime power coprime to 3 by the following recursion.

$$
\begin{aligned}
a_1 &= 2, \\
a_p &= a_p(f), \\
a_{p^n} &= a_p a_{p^{n-1}} - p^2 \rho(p) a_{p^{n-2}}. \qquad (n \geq 2)
\end{aligned}
$$

Let ψ_0 be the sum of all characters χ modulo 9 with $\chi(4) = 1$, and let ψ_1 be the sum of those with $\chi(-1) = 1$. In other words,

$$\psi_0(k) = \begin{cases} 2 & \text{if } k \equiv 1 \pmod 3, \\ 0 & \text{otherwise} \end{cases} \qquad \psi_1(k) = \begin{cases} 3 & \text{if } k \equiv 1, -1 \pmod 9, \\ 0 & \text{otherwise} \end{cases}$$

Also let $\psi' = \sum_\chi \chi(-1)^{-1}\chi$, where χ ranges over all the characters modulo 9 (so $\psi'(k) = 6$ if $k \equiv -1 \pmod 9$, and $\psi'(k) = 0$ otherwise). Then the formula for $N = 9$ is given by $q^2 + 1 + a_q + \overline{a_q} - \big(1 + \psi_0(q) + \psi_1(q)\big)q - \psi'(q)$. Though, this expression still depends on the coefficients of f, for which there is no 'simple' formula to compute these. In that sense, it is not a satisfactory formula.

Looking at these formulae, the following question rises: what do cusp forms of weight 3 have to do with universal elliptic curves? We explain this without going into much detail (it's summarised in [6, Ch. 2], and one can find the details in [4], [11], [2]).

Via the *Lefschetz trace formula*, one can relate $\#\mathcal{E}_N(\mathbb{F}_q)$ to the trace of the Frobenius map on the *cohomology groups* $\mathrm{H}^i(\mathcal{E}_N, \mathbb{F}_l)$ (which are $\mathbb{F}_l$-vector spaces), for all primes l coprime to qN. Of main interest are the groups $\mathrm{H}^2(\mathcal{E}_N, \mathbb{F}_l)$. (The rest will give a contribution which is polynomial in q, with possibly Dirichlet characters occurring in the coefficients.) These turn out to be related to the space $\mathcal{S}_3\big(\Gamma_1(N)\big)$ as a whole, and the Frobenius action on the $\mathrm{H}^2(\mathcal{E}_N, \mathbb{F}_l)$ turns out to be related to the action of the *diamond* and *Hecke operators* on $\mathcal{S}_3\big(\Gamma_1(N)\big)$, and hence to all the normalised eigenforms of $\mathcal{S}_3\big(\Gamma_1(N)\big)$. This gives reason to suspect that the formula for $\#\mathcal{E}_N(\mathbb{F}_q)$ involves the $a_q(f)$ of all the normalised eigenforms in $\mathcal{S}_3\big(\Gamma_1(N)\big)$. (Now we can also explain what we meant by 'empirically' obtaining the formulae for $N = 7, 8, 9$; we calculated enough values of $\#\mathcal{E}_N(\mathbb{F}_q)$ to conclude that if the formula is of the suspected form, then it must be the formula that we have given.

For $N = 7, 8$, all of the cusp forms that occur in the corresponding formulae are of a special kind; they come from *Hecke characters* (which we will define in the next chapter) of imaginary quadratic number fields, which allows for a simple description of the modular coefficients (unlike the cusp form that occurs if $N = 9$; there is no 'elementary' way to express its coefficients). Hence we want to call $\mathcal{S}_3\big(\Gamma_1(N)\big)$ *elementary* if all cusp forms $f \in \mathcal{S}_3\big(\Gamma_1(N)\big)$ are linear combinations of those coming from Hecke characters; in this case, as discussed above, the formula for $\mathcal{E}_N$ will be expected to be 'elementary' as well.

4 Algebraic Hecke characters

We fix our notation: K will in this chapter always denote a number field, and:

- μ_K denotes the set of roots of unity in K;
- V_K denotes the set of primes of K;
- V_K^∞ denotes the set of finite primes of K;
- Σ_K denotes the set of embeddings $K \longrightarrow \mathbb{C}$;
- $\mathcal{O}_K$ denotes the ring of integers of K;
- for $v \in V_K$, K_v (and $\mathcal{O}_v$ if $v \in V_K^\infty$) denote(s) the completions of K (and $\mathcal{O}_K$) with respect to v, respectively.

4.1 Adèles and Idèles

Definition 4.1.1. The *ring of adèles* $\mathbb{A}_K$ of K is the restricted product $\prod'_{v \in V_K} K_v$, i.e. $\mathbb{A}_K$ is the subset of $(x_v)_{v \in V_K} \in \prod_{v \in V_K} K_v$ such that for all but finitely many $v \in V_K^\infty$, we have $x_v \in \mathcal{O}_v$.

We denote by $\mathbb{A}_K^\infty$ the factor $\prod'_{v \in V_K^\infty} K_v$ of $\mathbb{A}_K$ (the *group of finite adèles* of K) and by $K_\mathbb{R}$ the factor $\mathbb{R} \otimes K = \prod_{v \in V_K - V_K^\infty} K_v$ of $\mathbb{A}_K$ (the *archimedean factor* of $\mathbb{A}_K$).

Example 4.1.2. Let $x \in K$. Then we can write $x = \frac{a}{b}$, with $a \in \mathcal{O}_K$, $b \in \mathcal{O}_K - \{0\}$. Then $b \notin v$ for all but finitely many $v \in V_K^\infty$, so $x \in \mathcal{O}_v$ for all but finitely many $v \in V_K^\infty$. Hence $(x)_{v \in V_K}$ defines an element of $\mathbb{A}_K$.

We can embed $K_\mathbb{R}$ in $\prod_{\sigma \in \Sigma_K} \mathbb{C}$ as follows. Let $v \in V_K - V_K^\infty$. If $K_v = \mathbb{R}$, then v corresponds to one (real) embedding of K, and we take the usual embedding $K_v \longrightarrow \mathbb{C}$. If $K_v = \mathbb{C}$, then v corresponds to two conjugate embeddings of K, and we take the embedding $K_v \longrightarrow \mathbb{C}^2$, $x \mapsto (x, \overline{x})$. Taking the product of these embeddings, we obtain an embedding $K_\mathbb{R} \longrightarrow \prod_{\sigma \in \Sigma_K} \mathbb{C}$, with image $\left\{(x_\sigma)_{\sigma \in \Sigma_K} : \forall \sigma \in \Sigma_K,\ x_{\overline{\sigma}} = \overline{x_\sigma}\right\}$. This embedding will be useful at times.

Note that by Example 4.1.2, it follows that we can view K as a subset of $\mathbb{A}_K$ via the diagonal embedding. Then $\mathbb{A}_K$ has a natural $\mathbb{Q}$-algebra structure, and we make it into a topological $\mathbb{Q}$-algebra by saying that a local basis of $0 \in \mathbb{A}_K$ is given by the natural local basis of 0 in $\prod_{v \in V_K} \mathcal{O}_v \times K_\mathbb{R} \subseteq \mathbb{A}_K$, with the product topology. As a topological space, $\mathbb{A}_K$ is Hausdorff and locally compact, and as a subspace, $K \subseteq \mathbb{A}_K$ is discrete and co-compact.

Definition 4.1.3. The *group of idèles* $\mathbb{A}_K^\times$ is the multiplicative group of the ring of adèles of K. The *group of finite idèles* $\mathbb{A}_K^{\infty\times}$ of K is the multiplicative group of the group of finite adèles of K, and the *archimedean factor* of $\mathbb{A}_K^\times$ is the multiplicative group of the archimedean factor of $\mathbb{A}_K$.

We make $\mathbb{A}_K^\times$ into a topological group by viewing it as the closed subset

$$\{(x, y) \in \mathbb{A}_K \times \mathbb{A}_K : xy = 1\}$$

of $\mathbb{A}_K \times \mathbb{A}_K$, and then giving $\mathbb{A}_K^\times$ the induced topology. Hence a local basis of 1 in $\mathbb{A}_K^\times$ is given by the natural local basis of 1 in $\prod_{v \in V_K} \mathcal{O}_v^\times \times K_\mathbb{R}^\times \subseteq \mathbb{A}_K^\times$, with the product topology. Note that this local basis, when restricted to $\mathbb{A}_K^{\infty\times}$, consists of compact open subgroups of $\mathbb{A}_K^{\infty\times}$. Also note that we view $K^\times$ as a subspace of $\mathbb{A}_K^\times$ via the diagonal embedding, and that $K^\times$ is discrete.

4.2 Algebraic Hecke characters

Definition 4.2.1. Let $n\colon \Sigma_K \longrightarrow \mathbb{Z}$ be a function. Then an *algebraic Hecke character* of K of *type* n is a continuous character $\chi\colon \mathbb{A}_K^\times \longrightarrow \mathbb{C}^\times$ that is trivial on $K^\times$, and after restricting to the connected component of the archimedean factor $K_{\mathbb{R}}^\times$ of $\mathbb{A}_K^\times$, is given by

$$K_{\mathbb{R}}^\times \longrightarrow \mathbb{C}^\times\colon (x_\sigma)_{\sigma\in\Sigma_K} \mapsto \prod_{\sigma\in\Sigma_K} x_\sigma^{n(\sigma)}.$$

Note that the map $\mathbb{Z}^{\Sigma_K} \longrightarrow \mathrm{Hom}(K_{\mathbb{R}}^\times, \mathbb{C}^\times)$ given by $n \mapsto \left(x \mapsto \prod_{\sigma\in\Sigma_K} x_\sigma^{n(\sigma)}\right)$ is injective, so any algebraic Hecke character can only have one type.

Example 4.2.2. Let K be any number field, then the trivial character $\chi_0\colon \mathbb{A}_K^\times \longrightarrow \mathbb{C}^\times$ is an algebraic Hecke character of type 0.

Let $n\colon \Sigma_K \longrightarrow \mathbb{Z}$ be a function, and let χ be an algebraic Hecke character over K of type n. Then for all primes $v \in V_K$, define $\chi_v\colon K_v^\times \longrightarrow \mathbb{C}^\times$ as the composition of χ with the injection to the factor $K_v^\times$ of $\mathbb{A}_K^\times$. So χ_v is continuous. We want to express χ in terms of the χ_v.

To do this, first we introduce for notational convenience, for all $v \in V_K^\infty$, subgroups $G_v(n)$ of $\mathcal{O}_v^\times$ for $n \geq 0$. Define $G_v(0) = \mathcal{O}_v^\times$, and for $n \geq 1$, define $G_v(n) = 1 + v^n$. Then we have the following:

Lemma 4.2.3. *Let $n\colon \Sigma_K \longrightarrow \mathbb{Z}$ be a function, and let χ be an algebraic Hecke character over K of type n. Then for all finite primes $v \in V_K^\infty$, there is a minimal non-negative integer $f_\chi(v)$ such that $G_v\big(f_\chi(v)\big) \subseteq \ker \chi_v$, and $f_\chi(v) = 0$ for all but finitely many $v \in V_K^\infty$.*

Proof. Let $U \subseteq \mathbb{C}^\times$ be the open disk with center 1 and radius 1. Let ψ be the restriction of χ to $\mathbb{A}_K^{\infty\times}$. Then $\psi^{-1}[U]$ is open, so it contains (by our choice of local basis) an open subgroup $V = \prod_{v\in V_K^\infty} G_v(i_v)$ of $\mathbb{A}_K^{\infty\times}$, where for all v, i_v is a non-negative integer that is zero for all but finitely many v. Since the only subgroup of $\mathbb{C}^\times$ that is contained in U, is the trivial one, it follows that $V \subseteq \ker \psi$. Hence there exist minimal non-negative integers $f_\chi(v)$ such that $\prod_{v\in V_K^\infty} G_v\big(f_\chi(v)\big) \subseteq \ker \psi$, and such that $f_\chi(v) = 0$ for all but finitely many v. □

It follows that for any $x \in \mathbb{A}_K^\infty$, the product $\prod_{v\in V_K} \chi_v(x_v)$ is well-defined. So now we can express χ in terms of the χ_v.

Proposition 4.2.4. *Let $n\colon \Sigma_K \longrightarrow \mathbb{Z}$ be a function, and let χ be an algebraic Hecke character over K of type n. Then for all $x \in \mathbb{A}_K^\times$, we have*

$$\chi(x) = \prod_{v\in V_K} \chi_v(x_v)$$

Proof. Let $x \in \mathbb{A}_K^\times$. Let S be the (by the above finite) set of finite primes v such that $\chi_v(x_v) \neq 1$. Then $x = \prod_{v\in S} x_v$, for some $x_v \in K_v^\times$ (for all $v \in S$). Hence

$$\begin{aligned}\chi(x) &= \prod_{v\in S} \chi(x_v) \\ &= \prod_{v\in V_K} \chi_v(x_v),\end{aligned}$$

which is as desired. □

By Lemma 4.2.3, the following is well-defined:

Definition 4.2.5. Let $n\colon \Sigma_K \longrightarrow \mathbb{Z}$ be a function, and let χ be an algebraic Hecke character over K of type n. Let for $v \in V_K^\infty$, $f_\chi(v)$ be the minimal non-negative number such that $G_v\big(f_\chi(v)\big) \subseteq \ker \chi_v$. Then the *conductor* $\mathfrak{f}_\chi$ of χ is the $\mathcal{O}_K$-ideal $\prod_{v\in V_K^\infty} v^{f_\chi(v)}$.

Note that, as a partial converse of Proposition 4.2.4, if for each prime v, we have a continuous character $\chi_v\colon K_v^\times \longrightarrow \mathbb{C}^\times$, such that $\chi_v[\mathcal{O}_v^\times] = 1$ for all but finitely many finite v, then the map $\chi\colon \mathbb{A}_K^\times \longrightarrow \mathbb{C}^\times$ sending x to $\prod_{v\in V_K} \chi_v(x_v)$ is a continuous character. This gives a convenient way to describe algebraic Hecke characters.

Example 4.2.6. Let K be any number field, and consider, for all finite primes v, the continuous map $\chi_v\colon K_v \longrightarrow \mathbb{C}^\times\colon x_v \mapsto (\mathrm{N}\, v)^{-\mathrm{ord}_v x}$, and, for all embeddings σ, the continuous map $\chi_\sigma\colon x_\sigma \mapsto x_\sigma$. First note that $\chi_v[\mathcal{O}_v^\times] = 1$ for all finite v, so the map $\chi\colon \mathbb{A}_K^\times \longrightarrow \mathbb{C}^\times$ given by $\chi(x) = \prod_{v\in V_K} \chi_v(x_v)$ is continuous. Then by the product formula, χ is trivial on $K^\times$. Hence χ is an algebraic Hecke character, the *adelic norm* on K, and its type n is given by $n(\sigma) = 1$ for all $\sigma \in \Sigma_K$.

Example 4.2.7. Let $K = \mathbb{Q}(\sqrt{-7})$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-7})]$, its class group is trivial, and $\mu_K = \langle -1\rangle$. View K as a subfield of $\mathbb{C}^\times$ under a certain embedding σ, and note that $\Sigma_K = \{\sigma, \overline{\sigma}\}$. Let for all $v \in V_K^\infty$, $\pi_v \in \mathcal{O}_K$ be a generator of v, and define the continuous map $\chi_v\colon K_v^\times \longrightarrow \mathbb{C}^\times\colon x_v \mapsto \pi_v^{-2\mathrm{ord}_v(x_v)}$. Note that $\chi_v[\mathcal{O}_v^\times] = 1$. Also define $\chi_\sigma\colon x_\sigma \mapsto x_\sigma^2$, and $\chi_{\overline{\sigma}}\colon x_{\overline{\sigma}} \mapsto 1$. Then $\chi\colon \mathbb{A}_K^\times \longrightarrow \mathbb{C}^\times$ given by $\chi(x) = \prod_{v\in V_K} \chi_v(x_v)$ is a continuous character. Moreover, for all $x \in K^\times$, x^2 can be uniquely written as $\prod_{v\in V_K} \pi_v^{2e_v}$. So $\mathrm{ord}_v(x^2) = 2e_v$ for all $v \in V_K$. Hence $\chi(x) = 1$. So χ is indeed an algebraic Hecke character, and its conductor is $\mathcal{O}_K$.

The next result shows that certain types of algebraic Hecke characters cannot occur, if we restrict the conductor.

Lemma 4.2.8. *Let $n\colon \Sigma_K \longrightarrow \mathbb{Z}$ be a function, and let χ be an algebraic Hecke character over K of type n. Let m be such that $\mu_K = \langle \zeta_m\rangle$, let ν_χ be the least common multiple of all the exponents of $\mathcal{O}_v^\times/1 + v^{f_\chi(v)}$, where v ranges over all the finite primes of K. Also let, for every embedding σ, $a(\sigma) \in (\mathbb{Z}/m\mathbb{Z})^\times$ be such that $\sigma(\zeta_m) = e^{\frac{2\pi i}{m} a(\sigma)}$. Then $\frac{m}{\gcd(m,\nu_\chi)}$ divides $\sum_{\sigma\in\Sigma_K} a(\sigma)n(\sigma)$ in $\mathbb{Z}/m\mathbb{Z}$.*

Proof. Consider $z = \prod_{v \in V_K^\infty} \chi_v(\zeta_m)$. On one hand, z is an m-th root of unity in $\mathbb{C}^\times$, since all χ_v are characters, and on the other hand, the order of each $\chi_v(\zeta_m)$ is a divisor of ν_χ, so z must be a ν_χ-th root of unity in $\mathbb{C}^\times$ as well. Hence, if we write $g = \gcd(m, \nu_\chi)$, then z is a g-th root of unity in $\mathbb{C}^\times$. But now note that

$$z^{-1} = \prod_{\sigma \in \Sigma_K} \sigma(\zeta_m)^{n(\sigma)} = e^{\frac{2\pi i}{m} \sum_{\sigma \in \Sigma_K} a(\sigma) n(\sigma)},$$

so $\frac{m}{g}$ divides $\sum_{\sigma \in \Sigma_K} a(\sigma) n(\sigma)$. □

Example 4.2.9. Let $K = \mathbb{Q}(\zeta_6)$. Then $\mu_K = \langle \zeta_6 \rangle$, and the two complex embeddings are given by σ and $\overline{\sigma}$. (Where $\sigma(\zeta_6) = e^{\frac{1}{3}\pi i}$.) Let χ be an algebraic Hecke character of type n. Then if $\mathfrak{f}_\chi = (1 + \zeta_6)$, then $\nu_\chi = 2$. So 3 divides $n(\sigma) - n(\overline{\sigma})$. Hence for example, there exist no algebraic Hecke characters of type $(2, 0)$ over K with conductor $(1 + \zeta_6)$.

We now consider algebraic Hecke characters with conductor $\mathcal{O}_K$. These turn out to be related to the class group of K.

Proposition 4.2.10. *The groups* $\mathbb{A}_K^{\infty\times} / K^\times \prod_{v \in V_K^\infty} \mathcal{O}_v^\times$ *and* $\operatorname{Cl} K$ *are isomorphic.*

Proof. Let $\mathcal{I}$ denote the set of fractional ideals of $\mathcal{O}_K$. Let for all $v \in V_K^\infty$, π_v be a uniformiser of $\mathcal{O}_v$. Since for all $(x_v)_v \in \mathbb{A}_K^{\infty\times}$, we have for all but finitely many $v \in V_K^\infty$ that $\operatorname{ord}_v(x_v) = 0$. Hence we can consider the group morphism

$$\phi \colon \mathbb{A}_K^{\infty\times} \longrightarrow \mathcal{I},\ (x_v)_v \mapsto \prod_{v \in V_K^\infty} v^{\operatorname{ord}_v(x_v)}.$$

Note that $\ker \phi = \prod_{v \in V_K^\infty} \mathcal{O}_v^\times$. Also, by definition (and by unique ideal factorisation), $\phi[K^\times]$ is the set of principal fractional ideals of $\mathcal{O}_K$. Finally, by unique ideal factorisation, it follows that ϕ is surjective. Hence by the Isomorphism Theorem, this gives an isomorphism $\mathbb{A}_K^{\infty\times} / K^\times \prod_{v \in V_K^\infty} \mathcal{O}_v^\times \longrightarrow \operatorname{Cl} K$. □

Remark 4.2.11. A direct consequence is that every algebraic Hecke character of K with conductor $\mathcal{O}_K$, gives rise to a unique group morphism $\operatorname{Cl} K \longrightarrow \mathbb{C}^\times$. Since $\#\operatorname{Hom}(\operatorname{Cl} K, \mathbb{C}^\times) = \#\operatorname{Cl} K$, we obtain an upper bound for the number of algebraic Hecke characters of K with conductor $\mathcal{O}_K$. In the case that K is an imaginary quadratic number field, every element of $\operatorname{Cl} K$ contains an integral ideal of norm at most $\frac{4}{\pi}|\Delta_K|^{1/2}$ (a result which can be found in most books on algebraic number theory, see e.g. [13, Prop. 5.4.7]). Note that in a imaginary quadratic number field, there are at most 2 primes of $\mathcal{O}_K$ lying over a rational prime p. Hence it follows that there are at most $d(n)$ distinct integral ideals of norm n, where $d(n)$ denotes the number of divisors of n. Since $d(n) \leq \frac{1}{2}n$ for $n \geq 4$, we obtain, by summing over all the possible norms, an upper bound $\frac{4}{\pi^2}|\Delta_K|^{1/2}\left(|\Delta_K|^{1/2} + 1\right) + 2$ for $\#\operatorname{Cl} K$, hence also for the number of algebraic Hecke characters with conductor $\mathcal{O}_K$.

4.3 The group of Hecke characters

Let χ, ψ be two algebraic Hecke characters of types n_χ and n_ψ, respectively. Then $\chi \cdot \psi$, χ^{-1} are again algebraic Hecke characters, of types $n_\chi + n_\psi$ and $-n_\chi$, respectively. Hence the set $\mathcal{H}_K$ of all algebraic Hecke characters over K has a natural abelian group structure, and we have a group homomorphism $n_- \colon \mathcal{H}_K \longrightarrow \mathbb{Z}^{\Sigma_K}$ sending an algebraic Hecke character to its type. Now let $\mathcal{H}_K(n)$ denote the set of all algebraic Hecke characters of type n. Then note that $\mathcal{H}_K(n)$ is a coset of the subgroup $\mathcal{H}_K(0)$. Since $\mathcal{H}_K(0)$ is the kernel of n_-, it follows that we have an injective group homomorphism $\mathcal{H}_K/\mathcal{H}_K(0) \longrightarrow \mathbb{Z}^{\Sigma_K}$, hence that $\mathcal{H}_K/\mathcal{H}_K(0)$ is free. We deduce that there is an isomorphism $\mathcal{H}_K \cong \mathcal{H}_K(0) \times \big(\mathcal{H}_K/\mathcal{H}_K(0)\big)$.

Now let $K \subseteq L$ be a finite field extension. Then, for all finite primes v of K and all primes w of L lying over v, we have a (continuous) norm map $N_{L_w/K_v} \colon L_w^\times \longrightarrow K_v^\times$, which maps $\mathcal{O}_w^\times$ into $\mathcal{O}_v^\times$. We also have a continuous map $L_{\mathbb{R}} \longrightarrow K_{\mathbb{R}}$ sending $(x_\tau)_{\tau\in\Sigma_L}$ to $(x_\sigma)_{\sigma\in\Sigma_K}$, where $x_\sigma = \prod_\tau x_\tau$, τ ranging over the extensions of σ. This gives a continuous group homomorphism $N_{L/K} \colon \mathbb{A}_L^\times \longrightarrow \mathbb{A}_K^\times$, that maps $L^\times$ to $K^\times$.

Proposition 4.3.1. *The map $\Psi_{L/K} \colon \mathcal{H}_K \longrightarrow \mathcal{H}_L$ given by $\chi \mapsto \chi \,\mathrm{N}_{L/K}$ is a group homomorphism.*

Proof. Let $\chi \in \mathcal{H}_K$. Then $\chi\,\mathrm{N}_{L/K}$ is a continuous character, which is trivial on $L^\times$. So by the observation above for the map $L_{\mathbb{R}} \longrightarrow K_{\mathbb{R}}$, it follows that $\chi\,\mathrm{N}_{L/K} \in \mathcal{H}_L$. Now it follows from the multiplicativity of all the maps involved, that $\Psi_{L/K}$ is indeed a group homomorphism. □

4.4 Hecke characters, cusp forms and elementary universal elliptic curves

Suppose that K is an imaginary quadratic number field, and let χ be an algebraic Hecke character of K of type $(2,0)$, with conductor $\mathfrak{f}_\chi$. Then we can construct a q-series as follows. Let $v \in V_K^\infty$ be coprime to $\mathfrak{f}_\chi$, then χ_v is trivial on $\mathcal{O}_K^\times$. Let π_v be a uniformiser of $\mathcal{O}_v$. Then note that $\chi_v(\pi_v)$ is independent of the choice of the uniformiser. Then define $s_\chi = \sum_v \chi_v(\pi_v) q^{\mathrm{N}\,v}$, where v ranges over all finite primes coprime to $\mathfrak{f}$.

Theorem 4.4.1 (Hecke, [8])**.** *Let χ be an algebraic Hecke character of an imaginary quadratic number field K of type $(2,0)$. Then the q-series s_χ defines a cusp form in $\mathcal{S}_3\big(\Gamma_1(|\Delta_K|\,\mathrm{N}\,\mathfrak{f}_\chi)\big)$.*

Cusp forms of the form s_χ will be called cusp forms with *complex multiplication*, or *CM-forms* for short. Let n be a positive integer. We now define the subspace $\mathcal{S}_3^{\mathrm{CM}}\big(\Gamma_1(n)\big) \subseteq \mathcal{S}_3\big(\Gamma_1(n)\big)$ as the subspace generated by the CM-forms.

We define $\mathcal{S}_3\big(\Gamma_1(n)\big)$ to be *elementary* if

$$\mathcal{S}_3^{\mathrm{CM}}\big(\Gamma_1(n)\big) = \mathcal{S}_3\big(\Gamma_1(n)\big);$$

by the discussion in Section 3.5, we suspect that $\mathcal{S}_3\big(\Gamma_1(n)\big)$ is elementary if and only if there exists a 'simple' formula for $\#\mathcal{E}_n(\mathbb{F}_q)$.

Proposition 4.4.2. *For all positive integers $n \leq 8$, $\mathcal{S}_3\big(\Gamma_1(n)\big)$ is elementary.*

Proof. We use Table 3. For $n \leq 6$, $\mathcal{S}_3(\Gamma_1(n))$ is trivial, so $\mathcal{S}_3(\Gamma_1(n))$ is automatically elementary. If $n = 7$, then the result follows from Example 4.2.7, since the discriminant of $\mathbb{Q}(\sqrt{-7})$ is -7. The same construction works for $\mathbb{Q}(\sqrt{-2})$, which has discriminant -8 and class number 1, so $\mathcal{S}_3(\Gamma_1(8))$ is elementary as well. □

Conjecture 4.4.3. *For all positive integers $n \geq 9$, $\mathcal{S}_3(\Gamma_1(n))$ is not elementary.*

We at least show that for an infinite family of positive integers n, $\mathcal{S}_3(\Gamma_1(n))$ is not elementary.

Note that $\mathcal{S}_3(\Gamma_1(9))$ is not elementary. First, note that the only imaginary quadratic number field of discriminant dividing 9 is $K = \mathbb{Q}(\zeta_6)$ of discriminant -3. By $\dim \mathcal{S}_3(\Gamma_1(3)) = 0$, it follows that there doesn't exist an algebraic Hecke character of K with conductor $\mathcal{O}_K$ and type $(2,0)$. By Example 4.2.9, it also follows that there doesn't exist an algebraic Hecke character of K with conductor $(1+\zeta_6)$ (nor does there exist one with conductor $(1+\zeta_6^{-1})$, the conjugate of $(1+\zeta_6)$). Hence there is no algebraic Hecke character of K with conductor having norm dividing 3; so $\mathcal{S}_3(\Gamma_1(9))$ is not elementary, since $\dim \mathcal{S}_3(\Gamma_1(9)) = 2$ by Table 3.

Since there are no imaginary quadratic number fields of discriminant dividing 10, and since we have $\dim \mathcal{S}_3(\Gamma_1(10)) = 4$ by Table 3 it follows that $\mathcal{S}_3(\Gamma_1(10))$ is not elementary either.

Proposition 4.4.4. *For all primes $p \geq 13$ with $p \equiv 1 \pmod 4$, $\mathcal{S}_3(\Gamma_1(p))$ and $\mathcal{S}_3(\Gamma_1(2p))$ are not elementary.*

Proof. First note that by Proposition 2.1.8, we have

$$\begin{aligned}
\dim \mathcal{S}_3(\Gamma_1(p)) &= \tfrac{1}{12}(p^2-1) - \tfrac{1}{2}(p-1), \\
&= \tfrac{1}{12}(p-1)(p-5), \\
&\geq 8, \\
\dim \mathcal{S}_3(\Gamma_1(2p)) &= \tfrac{1}{4}(p^2-1) - (p-1), \\
&= \tfrac{1}{4}(p-1)(p-3), \\
&\geq 30.
\end{aligned}$$

Since $p \equiv 1 \pmod 4$, there is no imaginary quadratic number field with discriminant (dividing) $2p$, so in that case, $\dim \mathcal{S}_3^{\mathrm{CM}}(\Gamma_1(p)) = \dim \mathcal{S}_3^{\mathrm{CM}}(\Gamma_1(2p)) = 0$, so $\mathcal{S}_3(\Gamma_1(p))$ and $\mathcal{S}_3(\Gamma_1(2p))$ are not elementary. □

Proposition 4.4.5. *For all primes $p \geq 11$ with $p \equiv 3 \pmod 4$, $\mathcal{S}_3(\Gamma_1(p))$ is not elementary.*

Proof. Similarly as in the previous proposition, we have

$$\dim \mathcal{S}_3(\Gamma_1(p)) = \tfrac{1}{12}(p-1)(p-5).$$

In particular, $\dim \mathcal{S}_3(\Gamma_1(11)) = 5$. Note that all algebraic Hecke characters giving rise to a cusp form in $\mathcal{S}_3^{\mathrm{CM}}(\Gamma_1(11))$, must be algebraic Hecke characters of $K = \mathbb{Q}(\sqrt{-11})$ with conductor $\mathcal{O}_K$. Since $\#\operatorname{Cl} K = 1$, it follows by Remark 4.2.11, that $\dim \mathcal{S}_3^{\mathrm{CM}}(\Gamma_1(11)) \leq 1$. In fact, since

$\mu_K = \{\pm 1\}$, the same construction as in Example 4.2.7 works, so actually $\dim \mathcal{S}_3^{\mathrm{CM}}\big(\Gamma_1(11)\big) = 1$. Hence $\mathcal{S}_3\big(\Gamma_1(11)\big)$ is not elementary.

Now suppose that $p \geq 19$. Note that all algebraic Hecke characters giving rise to a cusp form in $\mathcal{S}_3^{\mathrm{CM}}\big(\Gamma_1(p)\big)$, must be algebraic Hecke characters of $K = \mathbb{Q}\big(\sqrt{-p}\big)$ with conductor $\mathcal{O}_K$. By Remark 4.2.11, there are at most $\frac{4}{\pi^2}\sqrt{p}\big(\sqrt{p}+1\big)+2$ of those, so $\dim \mathcal{S}_3^{\mathrm{CM}}\big(\Gamma_1(p)\big) \leq \frac{4}{\pi}\sqrt{p}$. Now note that $\frac{1}{12}(p-1)(p-5) > \frac{4}{\pi^2}\sqrt{p}\big(\sqrt{p}+1\big)+2$. (One way to see this, is by evaluating both sides at $p = 19$, and then comparing the derivatives with respect to p of both sides, for $p \geq 19$.) Hence $\mathcal{S}_3\big(\Gamma_1(p)\big)$ is not elementary. $\square$

References

[1] H. Baaziz. Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points. *Math. Comp.*, 79(272), October 2010.

[2] P. Bayer and J. Neukirch. On automorphic forms and Hodge theory. *Math. Ann.*, 257(2), 1981.

[3] I. Connell. Elliptic curve handbook, February 1999. `http://www.ucm.es/BUCM/mat/doc8354.pdf`.

[4] P. Deligne. Formes modulaires et représentations l-adiques. *Séminaire N. Bourbaki*, 355, February 1969.

[5] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer, 2005.

[6] S. J. Edixhoven, J.-M. Couveignes, R. de Jong, J. Bosman, and F. Merkl. *Computational aspects of modular forms and Galois representations*, volume 176 of *Ann. Math. Studies*. Princeton University Press, 2011.

[7] A. Enge. *Elliptic curves and their applications to cryptography - an introduction*. Kluwer, 1999.

[8] E. Hecke. *Mathematische Werke*. Vandenhoeck & Ruprecht, 1983.

[9] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Ann. Math. Studies*. Princeton University Press, 1985.

[10] M. Raynaud. *Faisceaux amples sur les schémas en groupes et les espaces homogènes*, volume 119 of *Lecture Notes in Mathematics*. Springer-Verlag, 1970.

[11] A. J. Scholl. Motives for modular forms. *Invent. Math.*, 100(2), 1990.

[12] W. A. Stein et al. *Sage Mathematics Software (Version 4.7.2)*. The Sage Development Team, 2011. `http://www.sagemath.org`.

[13] E. Weiss. *Algebraic number theory*. McGraw-Hill Book Co., Inc., 1963.