Explicit Arithmetic of Modular Curves

Samir Siksek

Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom
E-mail address: s.siksek@warwick.ac.uk

Abstract. These are my notes for a course I gave at the *Institut Henri Poincaré* (29 April–3 May 2019) and at *CMI-HIMR Summer School in Computational Number Theory*, Bristol (17–21 June 2019). I would like to than Philippe Michaud-Rodgers for catching many misprints in a previous version.

Please proceed with extreme caution. These notes are extremely rough, written from the top of my head without checking of references and probably contain serious errors. At some point a more polished and complete version will eventually appear on my homepage.

CHAPTER 1

References

Theoretical:

- P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.
- B. Mazur, *Rational points on modular curves*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), 1977, pp. 107–148. Lecture Notes in Math., Vol. 601.
- F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

Explicit: Many many papers, by Derickx, Sutherland, Zywina, Najman, ...

- Steven Galbraith, *Equations for Modular Curves*, DPhil Thesis, Oxford, 1996.
- J. Rouse and D. Zureick-Brown, *Elliptic curves over* $\mathbb{Q}$ *and* 2*-adic images of Galois*, Research in Number Theory, Volume 1, Issue 1, 2015.

Magma packages for "modular forms", "modular symbols", "modular abelian varieties", "small modular curves". Versions of the first three are available in SAGE, but unfortunately not the last one. If you would like to experiment with Magma but don't have a license you can use the Magma online calculator:

http://magma.maths.usyd.edu.au/calc/

Descriptions of the packages mentioned above can be found at:

http://magma.maths.usyd.edu.au/magma/handbook/part/17

CHAPTER 2

Galois Properties of Torsion of Elliptic Curves

The key goal of the subject is to understand the Galois properties of torsion subgroups of elliptic curves, or put slightly differently, the possible images of Galois representations of elliptic curves. We shall introduce Galois representations of elliptic curves from scratch. We assume familiarity with elliptic curves, roughly to the level of Silverman's book [**22**]. Much of the material in this chapter can in fact be found in Silverman's book, but we rewrite it in fashion that emphasizes Galois representations.

1. Definition and First Examples

Notation:

K	a perfect field
G_K	$= \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K
N	a positive integer, if $\mathrm{char}(K) > 0$ then want $\mathrm{char}(K) \nmid N$.
E	an elliptic curve defined over K.

Recall

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z} \tag{1}$$

and so $E[N]$ has rank 2 as a $\mathbb{Z}/N\mathbb{Z}$-module [1]. However, $E[N] \subset E(\overline{K})$ and is stable under the action of G_K. We therefore obtain a representation

$$\overline{\rho}_{E,N} \ : \ G_K \to \mathrm{Aut}(E[N])$$

where $\mathrm{Aut}(E[N])$ is the automorphism group of $E[N]$. This is known as the **mod N Galois representation** attached to E. An automorphism of $E[N]$ is the same as an $\mathbb{Z}/N\mathbb{Z}$-linear isomorphism $E[N] \to E[N]$. Choosing an basis for $E[N]$ we can identify $\overline{\rho}_{E,N}$ as a representation

$$\overline{\rho}_{E,p} \ : \ G_K \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Since $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is finite, we know that the kernel $\ker(\overline{\rho})$ is normal of finite index. Moreover,

$$\sigma \in \ker(\overline{\rho}) \iff P^\sigma = P \text{ for all } P \in E[N].$$

Thus

$$\ker(\overline{\rho}) = G_{K(E[N])}.$$

[1] If $K \subseteq \mathbb{C}$ then we may see this as follows. Recall that there is some $\tau \in \mathbb{H}$ (the upper half-plane) and a complex analytic isomorphism

$$E(\mathbb{C}) \cong \frac{\mathbb{C}}{\mathbb{Z} + \tau\mathbb{Z}}.$$

Thus $E(\mathbb{C}) \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ from which (1) follows.

Hence

$$\overline{\rho}(G_K) \;\cong\; G_K/G_{K(E[N])} \;\cong\; \mathrm{Gal}(K(E[N])/K).$$

2. An Example: $\overline{\rho}_{E,2}$

In simple examples we can sometimes guess what the image $\overline{\rho}(G_K)$ has to be. The simplest case is when $N = 2$. Here we are supposing $\mathrm{char}(K) \neq 2$. We can write

$$E \;:\; Y^2 = f(X), \qquad f(X) = X^3 + aX^2 + bX + c \in K[X], \quad \Delta(f) \neq 0.$$

Recall that the points of order 2 are $(\theta_i, 0)$ where θ_1, θ_2, θ_3 are the roots of f. Write $P_i = (\theta_i, 0)$. Then P_1, P_2 is a basis for $E[2] = \{0, P_1, P_2, P_3\}$ and $P_3 = P_1 + P_2$. Observe that

$$K(E[2]) = K(\theta_1, \theta_2, \theta_3), \qquad \mathrm{Gal}(K(E[2])/K) = \mathrm{Gal}(f).$$

- If θ_1, θ_2, $\theta_3 \in K$, then $\overline{\rho} = 1$ (the trivial homomorphism).
- Suppose $\theta_1 \in K$, $\theta_2 \notin K$ and so $\theta_3 \notin K$. We can write $f(X) = (X - \theta_1)(X^2 + uX + v)$ where u, $v \in K$, and $d = u^2 - 4v \in K^* \setminus (K^*)^2$. Thus θ_2, θ_3 are the two roots of the irreducible quadratic factor $X^2 + uX + v$, and $K(E[2]) = K(\theta_2) = K(\theta_3) = K(\sqrt{d})$. We shall write $\overline{\rho}_{E,2}$ with respect to the basis P_1, P_2. Let $\sigma \in G_K$. If $\sigma(\sqrt{d}) = \sqrt{d}$ then

  $$\sigma(P_1) = P_1, \quad \sigma(P_2) = P_2, \qquad \overline{\rho}(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$$

  If $\sigma(\sqrt{d}) = -\sqrt{d}$ then σ swaps θ_2, θ_3, so

$$\sigma(P_1) = P_1, \quad \sigma(P_2) = P_3 = P_1 + P_2, \qquad \overline{\rho}(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2).$$

  Note that

$$\overline{\rho}(G_K) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\} \cong \mathbb{Z}/2\mathbb{Z} \cong \mathrm{Gal}(K(\sqrt{d})/K) = \mathrm{Gal}(K(E[2])/K).$$

- Suppose f is irreducible, but $\Delta(f) \in (K^*)^2$. Then $\mathrm{Gal}(f) \cong A_3$. Let $\sigma \in G_K$. Then σ acts on $(\theta_1, \theta_2, \theta_3)$ via one of the three permutations id, $(1,2,3)$, $(1,3,2) \in A_3$.

$$(\theta_1, \theta_2, \theta_3)^\sigma = (\theta_1, \theta_2, \theta_3) \implies P_1^\sigma = P_1, \quad P_2^\sigma = P_1 \implies \overline{\rho}(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$(\theta_1, \theta_2, \theta_3)^\sigma = (\theta_2, \theta_3, \theta_1) \implies P_1^\sigma = P_2, \quad P_2^\sigma = P_3 = P_1 + P_2 \implies \overline{\rho}(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$(\theta_1, \theta_2, \theta_3)^\sigma = (\theta_3, \theta_1, \theta_2) \implies P_1^\sigma = P_3 = P_1 + 2, \quad P_2^\sigma = P_1 \implies \overline{\rho}(\sigma) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

  Thus

$$\overline{\rho}(G_K) \;=\; \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\} \cong \mathbb{Z}/3\mathbb{Z} \cong \mathrm{Gal}(K(E[2])/K).$$

- Suppose f is irreducible and $\Delta(f) \notin K^{*2}$. Thus $\mathrm{Gal}(K(E[2]/K) = \mathrm{Gal}(f) = S_3$. Thus $\overline{\rho}(G_K)$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ that is isomorphic to S_3. But $\#S_3 = \#\,\mathrm{GL}_2(\mathbb{F}_2) = 6$. Hence $\overline{\rho}$ is surjective and we also arrive at the conclusion that $S_3 \cong \mathrm{GL}_2(\mathbb{F}_2)$. It's easy to write the matrix $\overline{\rho}(\sigma)$ in terms of the action of σ on θ_1, θ_2, θ_3.

Important Remark. The image $\overline{\rho}(G_K) \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ depends on a choice of basis for $E[N]$. If we change basis then we conjugate $\overline{\rho}$ by the change of basis matrix, which is an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. So the image is really only well defined up to conjugation.

3. The mod N-Cyclotomic Character

Let ζ_N be a primitive N-th root of 1. Define **the mod N-cyclotomic character** $\chi_N : G_{\mathbb{Q}} \to (\mathbb{Z}/N\mathbb{Z})^*$ as follows. For $\sigma \in G_{\mathbb{Q}}$ we see that ζ_N^σ is also a primitive N-root of unity and so $\zeta_N^\sigma = \zeta_N^{a_\sigma}$ where a_σ is an integer, coprime to N, and whose value is defined only modulo N, i.e. $a_\sigma \in (\mathbb{Z}/N\mathbb{Z})^*$. We let $\chi_N(\sigma) = a_\sigma$. To summarise,

$$\chi_N : G_K \to (\mathbb{Z}/N\mathbb{Z})^*, \qquad \zeta_N^\sigma = \zeta_N^{\chi_N(\sigma)}.$$

THEOREM 1. *Let K be a number field.*

(i) *If $\tau \in G_K$ denotes any complex conjugation*[2]*, then $\chi_N(\tau) = -1$.*

(ii) *Let $\lambda \neq N$ be finite place of K, and let $I_\lambda \subset G_K$ denote an inertia subgroup at λ. Then $\chi_N(I_\lambda) = 1$ (we say that χ_N is **unramified** at λ). Moreover, if $\sigma_\lambda \in G_K$ denotes a Frobenius element at λ, then*

$$\chi_N(\sigma_\lambda) \equiv \mathrm{Norm}_{K/\mathbb{Q}}(\lambda) \pmod{N}.$$

PROOF. Part (i) is clear as complex conjugation takes ζ_N to ζ_N^{-1}.

We turn to (ii). Corresponding to I_λ is a prime $\mu \mid \lambda$ of $\overline{K}$ (changing μ conjugates I_λ and so leaves the desired result unaffected). By definition of inertia,

$$\zeta_N^\sigma \equiv \zeta_N \pmod{\mu}$$

for all $\sigma \in I_\lambda$. Recall that the difference of two distinct N-th roots of 1 divides N. As $\lambda \neq N$ we have $\mu \nmid N$. Thus $\zeta_N^\sigma = \zeta_N$. But $\zeta_N^\sigma = \zeta_N^{\chi_N(\sigma)}$ by definition of χ_N. It follow that $\zeta_N^{\chi_N(\sigma)} = \zeta_N$ and $\chi_N(\sigma) = 1$ for all $\sigma \in I_\lambda$.

Now let σ_λ be a Frobenius element corresponding to λ. Then

$$\zeta_N^{\sigma_\lambda} \equiv \zeta_N^{\mathrm{Norm}_{K/\mathbb{Q}}(\lambda)} \pmod{\mu}$$

by definition of Frobenius. As above $\zeta_N^{\sigma_\lambda} = \zeta_N^{\mathrm{Norm}_{K/\mathbb{Q}}(\lambda)}$. Hence $\chi_N(\sigma_\lambda) \equiv \mathrm{Norm}_{K/\mathbb{Q}}(\lambda) \pmod{N}$. □

THEOREM 2. $\det \overline{\rho}_{E,N} = \chi_N$.

PROOF. Recall that the Weil pairing

$$e_N : E[N] \times E[N] \to \mu_N = \langle \zeta_N \rangle$$

is bilinear, alternating[3], non-degenerate and Galois invariant.

---

[2]Let us explain what complex conjugation is. Let K be a number field and let $\iota_\infty : K \hookrightarrow \mathbb{R}$ be a real embedding of K. Let $\iota : \overline{K} \hookrightarrow \mathbb{C}$ be an embedding extending ι_∞. Let $c : \mathbb{C} \to \mathbb{C}$ denote complex conjugation. Then $\iota^{-1} \circ c \circ \iota$ is an element of G_K which we call a **complex conjugation**. Of course if K is totally complex then it does not have any complex conjugations. You can check that the conjugacy classes of complex conjugations inside G_K are in bijection with the real embeddings of K

[3]As a reminder, **alternating** means $e_N(S,S) = 1$ for all $S \in E[N]$. This implies that e_N is **skew-symmetric**: $e_N(T,S) = e_N(S,T)^{-1}$. To see this note

$$1 = e_N(S+T, S+T) = e_N(S,S)e_N(S,T)e_N(T,S)e_N(T,T) = e_N(S,T)e_N(T,S).$$

As e_N is non-degenerate, we may choose a basis S, T for $E[N]$ such that $e_N(S,T) = \zeta_N$. Let $\sigma \in G_K$. Write

$$\overline{\rho}_{E,N}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Thus

$$S^\sigma = aS + cT, \qquad T^\sigma = bS + dT.$$

Then

$$\begin{aligned}
\zeta_N^{\chi_N(\sigma)} &= \zeta_N^\sigma && \text{by definition of } \chi_N \\
&= e_N(S,T)^\sigma && \text{by choice of } S,\ T \\
&= e_N(S^\sigma, T^\sigma) && \text{by Galois invariance of } e_N \\
&= e_N(aS+cT, bS+dT) \\
&= e_N(S,S)^{ac} e_N(S,T)^{ad} e_N(T,S)^{bc} e_N(T,T)^{cd} && \text{by bilinearity of } e_N \\
&= e_N(S,T)^{ad-bc} && \text{as } e_N \text{ is alternating} \\
&= \zeta_N^{ad-bc} && \text{again by choice of } S,\ T.
\end{aligned}$$

Hence $\chi_N(\sigma) = ad - bc = \det \overline{\rho}_{E,N}(\sigma)$ completing the proof. □

When K is a number field we say that a representation $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is **odd** if for every complex conjugation $\tau \in G_K$ we have $\det(\overline{\rho}(\tau)) = -1$.

Corollary 3.1. *Let E be an elliptic curve over a number field K. Then $\overline{\rho}_{E,N}$ is odd.*

Proof. This follows from Theorems 1 and 2. □

Of course if K is totally complex, then the corollary is vacuous.

4. Torsion and Isogenies

Theorem 3. *The following are equivalent:*

(a) *E has a K-rational point of order N;*

(b) $\overline{\rho}_{E,N} \sim \begin{pmatrix} 1 & * \\ 0 & \chi_N \end{pmatrix}$.

(c) *$\overline{\rho}_{E,N}(G_K)$ is conjugate inside $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of*

$$B_1(N) := \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} : b \in \mathbb{Z}/N\mathbb{Z},\ d \in (\mathbb{Z}/N\mathbb{Z})^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Proof. (a) $\Longrightarrow$ (b). Suppose E has a K-rational point P of order N. Let $Q \in E[N]$ so that P, Q is a $\mathbb{Z}/N\mathbb{Z}$-basis for $E[N]$. Then for all $\sigma \in G_K$, we have

$$\sigma(P) = P, \qquad \sigma(Q) = b_\sigma P + d_\sigma Q.$$

Hence

$$\overline{\rho}_{E,N}(\sigma) = \begin{pmatrix} 1 & b_\sigma \\ 0 & d_\sigma \end{pmatrix}$$

for all $\sigma \in G_K$. However, by Theorem 2,

$$d_\sigma = \det \overline{\rho}_{E,N}(\sigma) = \chi_N(\sigma)$$

Thus (b) holds.

(b) $\Longrightarrow$ (c). This is clear.

(c) $\Longrightarrow$ (a). Suppose (c). Then we can choose a basis P, Q so that the image $\overline{\rho}_{E,N}(G_K)$ is contained in $B_1(N)$. Note that

$$P^\sigma = P, \qquad Q^\sigma = b_\sigma P + d_\sigma Q$$

for all $\sigma \in G_K$ (where b_σ, $d_\sigma \in \mathbb{Z}/N\mathbb{Z}$). As P is fixed by G_K it follows that $P \in E(K)$. Since P, Q is a basis, P must have exact order N, proving (a). □

THEOREM 4. *The following are equivalent:*

(a) *E has a cyclic K-rational N-isogeny;*

(b) *$\overline{\rho}_{E,N} \sim \begin{pmatrix} \phi & * \\ 0 & \psi \end{pmatrix}$, where ϕ, $\psi : G_K \to (\mathbb{Z}/N\mathbb{Z})^*$ are characters satisfying $\phi\psi = \chi_N$.*

(c) *$\overline{\rho}_{E,N}(G_K)$ is conjugate inside $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of*

$$B_0(N) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : b \in \mathbb{Z}/N\mathbb{Z}, \quad a,\ d \in (\mathbb{Z}/N\mathbb{Z})^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

PROOF. (a) $\Longrightarrow$ (b). Suppose E has a cyclic K-rational N-isogeny $\theta : E \to E$. The $\ker(\theta)$ is cyclic of order N and thus $\ker(\theta) = \langle P \rangle$ where P is an element of $E[N]$ of order N. As θ is defined over K, the group $\langle P \rangle$ is K-rational (i.e. it is stable under the action of G_K). Let $Q \in E[N]$ be such that P, Q is a basis. Then for all $\sigma \in G_K$, we have

$$P^\sigma = a_\sigma P, \qquad Q^\sigma = b_\sigma P + d_\sigma Q.$$

Hence

$$\overline{\rho}_{E,N}(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ 0 & d_\sigma \end{pmatrix}$$

for all $\sigma \in G_K$. Let ϕ, $\psi : G_K \to (\mathbb{Z}/N\mathbb{Z})^*$ be given by $\phi(\sigma) = a_\sigma$, $\psi(\sigma) = d_\sigma$. We leave to the reader the task of checking that ϕ, ψ must be characters, and completing the remainder of the proof. □

5. Quadratic Twisting

LEMMA 5.1. *Let $d \in K^*$. Suppose $\mathrm{char}(K) \neq 2$. Let E' be the quadratic twist of E by d. Let $\psi : G_K \to \{1, -1\}$ be the quadratic character defined by $\sqrt{d}^\sigma = \psi(\sigma) \cdot \sqrt{d}$. Then $\overline{\rho}_{E,N} \sim \psi \cdot \overline{\rho}_{E',N}$.*

PROOF. As $\mathrm{char}(K) \neq 2$, the curves E, E' have models

$$E \ : \ Y^2 \ = \ X^3 + aX^2 + bX + c, \qquad E' \ : \ Y^2 \ = \ X^3 + daX^2 + d^2bX + d^3c.$$

The map

$$\phi : E(\overline{K}) \to E'(\overline{K}), \qquad \phi(x, y) \ = \ \left(\frac{x}{d},\ \frac{y}{d\sqrt{d}} \right)$$

is an isomorphism of abelian groups, and thus induces an isomorphism $\phi : E[N] \to E'[N]$. Let $P = (x, y) \in E[N]$. Note that $\pm P = (x, \pm y)$. Thus,

$$\phi(P)^\sigma \ = \ \left(\frac{x^\sigma}{d},\ \frac{y^\sigma}{d\sqrt{d}^\sigma} \right) \ = \ \left(\frac{x^\sigma}{d},\ \psi(\sigma) \cdot \frac{y^\sigma}{d\sqrt{d}} \right) \ = \ \psi(\sigma) \cdot \left(\frac{x^\sigma}{d},\ \frac{y^\sigma}{d\sqrt{d}} \right) \ = \ \psi(\sigma) \cdot \phi(P^\sigma).$$

Now let P, Q be a basis for $E[N]$, and we take $\phi(P)$, $\phi(Q)$ as a basis for $E'[N]$. With respect to these bases it is now an easy exercise to show that $\overline{\rho}_{E,N} = \psi \cdot \overline{\rho}_{E',N}$. □

THEOREM 5. *Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Suppose that $\overline{\rho}_{E,N}(G_K)$ is contained in H. Let E' be a quadratic twist by some $d \in K^*$. If $-I \in H$, then $\overline{\rho}_{E',N}(G_K)$ is contained in a conjugate of H.*

PROOF. This follows immediately from Lemma 5.1. □

COROLLARY 5.2. *If E has a cyclic K-rational N isogeny, then so does any quadratic twist.*

For $N \geq 3$, if E is an elliptic curve with a K-rational point of order N then a non-trivial quadratic twist will not have a point of order N, but it will have an N-isogeny.

EXERCISE 6. Suppose E has a K-rational 3-isogeny. Show that there is a quadratic twist E' that has a point of order 3.

6. Local Properties of mod N Representations of Elliptic Curves

Let K be a number field and λ be a prime of K. Let E be an elliptic curve defined over K. We say that $\overline{\rho}_{E,N}$ is **unramified** at λ if $\overline{\rho}_{E,N}(I_\lambda) = 1$, where $I_\lambda \subseteq G_K$ denotes an inertia subgroup at λ.

THEOREM 7. *Suppose $\lambda \nmid N$ is a prime of good reduction for E. Then $\overline{\rho}_{E,N}$ is unramified at λ.*

PROOF. The choice of inertia subgroup I_λ corresponds to a choice of prime μ of $\overline{K}$ above λ. As E has good reduction at μ and $\mu \nmid N$, the reduction modulo μ map

$$E[N] \to E(\overline{\mathbb{F}}_\lambda), \qquad Q \mapsto \tilde{Q} \pmod{\mu} \tag{2}$$

is injective. Let $\sigma \in I_\lambda$. Then for all $Q \in E[N]$ we have that $\widetilde{Q^\sigma} = \tilde{Q}$ by definition of inertia. By the injectivity of (2) we have $Q^\sigma = Q$. Thus $\overline{\rho}_{E,N}(\sigma) = 1$ which completes the proof. □

7. The mod N representation of a Tate curve

Another very instructive computation is the mod N representation of a Tate curve. The standard reference for Tate curves is Silverman's advanced textbook [**23**, Chapter V] In this section K is a field complete with respect to a non-archimedean valuation $|\cdot|$ (e.g. $K = \mathbb{Q}_p$). Let $q \in K^*$ satisfy $|q| < 1$. Define

$$s_k(q) := \sum_{n \geq 1} \frac{n^k q^n}{1 - q^n}, \qquad a_4(q) := -s_3(q), \qquad a_5(q) := -\frac{5s_3(q) + 7s_5(q)}{12}.$$

These converge in K. Define the **Tate curve** with parameter q by

$$E_q : \qquad Y^2 + XY = X^3 + a_4(q)X + a_6(q).$$

This is an elliptic curve over K with discriminant

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

and j-invariant

$$j = \frac{1}{q} + 744 + 196884q^2 + \cdots.$$

EXAMPLE 8. If $E/\mathbb{Q}_p$ has split multiplicative reduction, then $E \cong E_q$ for some choice of $q \in \mathbb{Q}_p$ (i.e. E is a Tate curve). If $E/\mathbb{Q}_p$ has potentially multiplicative reduction (i.e. $|j(E)|_p > 1$) then E is the quadratic twist of some Tate curve E_q by $-c_4(E)/c_6(E)$ where c_4, c_6 has their usual meanings.

THEOREM 9 (Tate). *There is an analytic isomorphism*

$$\phi \,:\, E_q(\overline{K}) \to \overline{K}^*/q^{\mathbb{Z}}\,,$$

which is compatible with the action of G_K.

COROLLARY 7.1. *Let $E = E_q$ be a Tate curve as above. Then*

$$\overline{\rho}_{E,N} \sim \begin{pmatrix} \chi_N & * \\ 0 & 1 \end{pmatrix}.$$

PROOF. Note that ϕ induces an isomorphism

$$\phi \,:\, E[N] \to \left(\overline{K}^*/q^{\mathbb{Z}}\right)[N]$$

that is compatible with the action of G_K. A basis for the group on the right is ζ_N, $q^{1/N}$. Let $\sigma \in G_K$. Then

$$\sigma(\zeta_N) = \zeta_N^{\chi_N(\sigma)}, \qquad \sigma(q^{1/N}) = \zeta_N^{a_\sigma}\, q^{1/N}$$

for some a_σ. Let $P = \phi^{-1}(\zeta_N)$, $Q = \phi^{-1}(q^{1/N})$. Then P, Q is a basis for $E[N]$ and, as ϕ is compatible with the G_K-action

$$P^\sigma = \chi_N(\sigma) \cdot P, \qquad Q^\sigma = a_\sigma \cdot P + Q.$$

Hence, with respect to this basis,

$$\overline{\rho}_{E,N}(\sigma) = \begin{pmatrix} \chi_N(\sigma) & a_\sigma \\ 0 & 1 \end{pmatrix}.$$

□

EXAMPLE 10. Let $E/\mathbb{Q}$ have split multiplicative reduction at p. Let $G_p \subset G_{\mathbb{Q}}$ be the decomposition group at p; this is simply $G_{\mathbb{Q}_p}$. As E is a Tate curve when considered over $\mathbb{Q}_p$, we see from the above that

$$\overline{\rho}_{E,N}|_{G_p} \sim \begin{pmatrix} \chi_N & * \\ 0 & 1 \end{pmatrix}.$$

More generally, let $E/\mathbb{Q}$ have potentially multiplicative reduction at p. Let $\psi : G_p \to \{\pm 1\}$ be the character satisfying $\sigma(\sqrt{-c_4/c_6}) = \psi(\sigma) \cdot \sqrt{-c_4/c_6}$. Then

$$\overline{\rho}_{E,N}|_{G_p} \sim \psi \cdot \begin{pmatrix} \chi_N & * \\ 0 & 1 \end{pmatrix}.$$

8. Serre's Uniformity Conjecture

CONJECTURE (Serre's Uniformity Conjecture). *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $p > 37$. Then $\overline{\rho}_{E,p}$ is surjective.*

Recall that $\det \circ \overline{\rho}_{E,p} = \chi_p$ and that this is surjective on $G_{\mathbb{Q}}$. Thus the conjecture is equivalent to $\mathrm{SL}_2(\mathbb{F}_p) \subset \overline{\rho}_{E,p}(G_{\mathbb{Q}})$ for all $p > 37$. It is useful to know Dickson's classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$.

THEOREM 11 (Dickson). *Let H be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ not containing $\mathrm{SL}_2(\mathbb{F}_p)$. Then (up to conjugation)*

(i) *either* $H \subseteq B_0(p) := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$ *(Borel subgroup)*
(ii) *or* $H \subseteq N_s^+(p) := \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, \begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix} : \alpha, \beta \in \mathbb{F}_p^* \right\}$ *(normalizer of split Cartan)*
(iii) *or* $H \subseteq N_{ns}^+(p)$ *(normalizer of non-split Cartan)*[4]
(iv) *or the image of* H *in* $\mathrm{PGL}_2(\mathbb{F}_p)$ *is isomorphic to* A_4, S_4 *or* A_5 *(these are called the exceptional subgroups of* $\mathrm{GL}_2(\mathbb{F}_p)$*).*

EXERCISE 12. Suppose $E/\mathbb{Q}_p$ has potentially multiplicative reduction at p. Show for $p \geq 11$ that $\overline{\rho}_{E,p}(G_p)$ is not exceptional. (Hint: show that it contains an element whose order is too large to fit inside the exceptional subgroups.)

In fact Serre showed that $\overline{\rho}_{E,p}(G_p)$ is too large to fit inside the exceptional subgroups for $p \geq 11$.

THEOREM 13 (Serre). *Let* $p \geq 11$ *and* $E/\mathbb{Q}$ *be an elliptic curve. Then* $\overline{\rho}_{E,p}(G_{\mathbb{Q}})$ *is not exceptional.*

[4] $N_{ns}^+(p)$ can be conjugated inside $\mathrm{GL}_2(\mathbb{F}_{p^2})$ to

$$\left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix}, \begin{pmatrix} 0 & \alpha \\ \alpha^p & 0 \end{pmatrix} : \alpha \in \mathbb{F}_p^{2*} \right\}.$$

CHAPTER 3

Modular Curves

1. Vague Objective

Given a field K, a positive integer N, and a subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we want to understand the set of all elliptic curves E/K such that $\overline{\rho}_{E,N}(G_K)$ is conjugate to a subgroup of H. Provided H satisfies certain technical assumptions, such elliptic curves give rise to (non-cuspidal) K-points on X_H, where X_H is the modular curve associated to H. By understanding $X_H(K)$ we can give a complete description of the set of elliptic curves E/K such that $\overline{\rho}_{E,N}(G_K)$ is conjugate to a subgroup of H.

We suppose prior acquaintance with the modular curves $X(1)$, $X_1(N)$, $X_0(N)$ at least as Riemann surfaces, as well as the interpretation of their complex points in terms of isomorphism classes of elliptic curves with extra level structure, as explained for example in the excellent book of Diamond and Shurman [**7**]. However, we briefly recall the definitions and summarise the basic facts.

2. The Modular Curve $X(1)$

If you've done a first course on modular forms then you will have seen the construction of $X(1)$ as Riemann surface. Let

$$\mathbb{H} \;:=\; \{x+yi \;:\; x,\; y \in \mathbb{R},\; y>0\}$$

be the upper half-plane, and

$$\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$$

the extended upper half-plane. The moduli interpretation of the complex points of $X(1)$ (as well as $X_1(N)$ and $X_0(N)$) makes use of the theory of elliptic functions. Recall, that given any $\tau \in \mathbb{H}$, there is an elliptic curve $E_\tau/\mathbb{C}$ such that $E_\tau(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\cdot\tau)$. Every elliptic curve over $\mathbb{C}$ is isomorphic to E_τ for some τ. Moreover $E_{\tau_1} \cong E_{\tau_2}$ if and only if $\tau_1 = \gamma(\tau_2)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Therefore we have a bijection

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \leftrightarrow \{\text{isom classes of elliptic curves } E/\mathbb{C}\}, \qquad \mathrm{SL}_2(\mathbb{Z})\cdot\tau \mapsto [\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)];$$

On the right hand-side of the correspondence we are identifying E_τ with $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$. here the square brackets denotes isomorphism class. In other words the points of the Riemann surface $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ are in one-one correspondence with isomorphism classes of elliptic curves over $\mathbb{C}$. The Riemann surface $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is non-compact; its compactification is $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$, which is a compact Riemann surface of genus 0. The points of $\mathbb{P}^1(\mathbb{Q}) \subset \mathbb{H}^*$ form one orbit under the action of $\mathrm{SL}_2(\mathbb{Z})$, so the compactification has only one extra point, called the cusp at infinity ∞. Any compact Riemann surface can be identified as the set of complex points on an

algebraic curve of the same genus. In this we case we denote the algebraic curve by $X(1) = \mathbb{P}^1$. The standard identification is via the modular j-function

$$j \,:\, \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^* \to X(1)(\mathbb{C})\,, \qquad \mathrm{SL}_2(\mathbb{Z})\cdot\tau \mapsto j(\tau) \;=\; \frac{1}{q} + 744 + 196884q^2 + \cdots\,,$$

where

$$q := \begin{cases} \exp(2\pi i\tau) & \tau \in \mathbb{H} \\ 0 & \tau \in \mathbb{P}^1(\mathbb{Q}). \end{cases}$$

Note that under this identification, the cusp $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{P}^1(\mathbb{Q})$ corresponds to the point $\infty \in X(1)(\mathbb{C})$. Let $Y(1) := X(1) \setminus \infty \cong \mathbb{A}^1$. To summarize, there is a one-one correspondence between isomorphism classes of elliptic curves $E/\mathbb{C}$ and points $j \in Y(1)(\mathbb{C})$. But more is true: the value $j \in Y(1)(\mathbb{C})$ corresponding to $E/\mathbb{C}$ is none other than the familiar j-invariant $j(E)$.

Now let K be any field. The correspondence between isomorphism classes of $E/\overline{K}$ and points in $Y(1)(\overline{K})$, sending E to its j-invariant E, remains valid. But what if we're working over K and not $\overline{K}$? What do points in $j \in Y(1)(K)$ correspond to? They correspond to classes of elliptic curves defined over K which are isomorphic over $\overline{K}$. Now if E, E' are defined over K and isomorphic over $\overline{K}$, then they are quadratic twists, **except possibly if they have j-invariants** 0**,** 1728. So we have the following $1-1$ correspondence:

$$\{\text{elliptic curves over } K \text{ with } j\text{-invariant} \neq 0,\, 1728\}/\sim \;\Longleftrightarrow\; j \in X(1)(K)\backslash\{0, 1728, \infty\}$$

where $\sim$ denotes quadratic twisting.

3. The modular curves $X_1(N)$, $X_0(N)$

We fix $N \geq 1$. Let

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

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

We are interested in isomorphism classes of pairs (E, P) where $E/\mathbb{C}$ is an elliptic curve and P is a point of order N on E. By an isomorphism of pairs (E_1, P_1), (E_2, P_2) we mean an isomorphism $\phi : E_1 \to E_2$ such that $\phi(P_1) = P_2$. We write $[(E, P)]$ for the isomorphism class of the pair (E, P). One checks that given (E, P) with E an elliptic curve over $\mathbb{C}$, then there is some $\tau \in \mathbb{H}$ such that $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\cdot\tau)$ and this isomorphism take P to $1/N + (\mathbb{Z} + \mathbb{Z}\tau) \in \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ (we'll henceforth denote the coset $1/N + (\mathbb{Z} + \mathbb{Z}\tau)$ by $1/N$). Thus we may identify $[(E, P)]$ with $[(\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau), 1/N)]$. Moreover τ_1, τ_2 yield isomorphic pairs $(\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau_1), 1/N)$, $(\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau_2), 1/N)$ if and only if there is some $\gamma \in \Gamma_1(N)$ such that $\tau_1 = \gamma(\tau_2)$. Thus we have a one-one correspondence

$$\Gamma_1(N)\backslash\mathbb{H} \leftrightarrow \{\text{isom classes of pairs } (E/\mathbb{C}, P)\}, \qquad \Gamma_1(N)\cdot\tau \mapsto [(\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau), 1/N)].$$

We are also interested in isomorphism classes of pairs (E, C) where $E/\mathbb{C}$ is an elliptic curve and C is a cyclic subgroup of order N on E. By an isomorphism of pairs (E_1, C_1), (E_2, C_2) we mean an isomorphism $\phi : E_1 \to E_2$ such that $\phi(C_1) = C_2$,

and again we write $[(E, C)]$ for the isomorphism class of the pair (E, C). Arguing similarly as before we obtain a one-one correspondence

$$\Gamma_0(N)\backslash\mathbb{H} \leftrightarrow \{\text{isom classes of pairs } (E/\mathbb{C}, C)\}, \qquad \Gamma_0(N)\cdot\tau \mapsto [(\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau), \langle 1/N\rangle)].$$

Miracle: there are (open) curves $Y_1(N)$, $Y_0(N)$ defined over $\mathbb{Q}$, such that

$$Y_1(N)(\mathbb{C}) \cong \Gamma_1(N)\backslash\mathbb{H}, \qquad Y_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathbb{H},$$

The completions $X(1)$, $X_1(N)$, $X_0(N)$ satisfy

$$X_1(N)(\mathbb{C}) \cong \Gamma_1(N)\backslash\mathbb{H}^*, \qquad X_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathbb{H}^*,$$

We call $X_1(N) \setminus Y_1(N)$, $X_0(N) \setminus Y_0(N)$ the sets of cusps of $X_1(N)$, $X_0(N)$ respectively.

Fact. A point $Q \in Y_1(N)(\overline{K})$ parametrises an isomorphism class of pairs $[(E, P)]$ where $E/\overline{K}$ and P is a point of order N. We shall write $Q = [(E, P)] \in Y_1(N)(\overline{K})$ (in other words we identify the point Q of Y_1 with the pair it represents). Moreover, this is parametrisation is compatible with the action of G_K. Thus $Q^\sigma = [(E, P)]^\sigma$ where $[(E, P)]^\sigma$ is simply defined as (E^σ, P^σ).

Question. Let $Q = [(E, P)] \in Y_1(N)(\overline{K})$ as above. If E is defined over K, and P is a K-rational point of order N, then $Q^\sigma = [(E, P)]^\sigma = [(E, P)] = Q$ for all $\sigma \in G_K$, and thus $Q \in Y_1(K)$. **Does the converse necessarily hold? If $Q \in Y_1(N)(K)$, is there necessarily some E defined over K, and P that is a K-rational point order N such that $Q = [(E, P)]$?**

Example 14. Let $N = 3$ and

$$E \ : \ Y^2 = X^3 + 2.$$

Let $P = (0, \sqrt{2})$. We consider $Q = [(E, P)] \in Y_1(N)(\overline{\mathbb{Q}})$. We claim that $Q \in Y_1(N)(\mathbb{Q})$. For this we want to show that for any $\sigma \in G_\mathbb{Q}$, (E^σ, P^σ) is isomorphic to (E, P) In fact $E^\sigma = E$ as E is defined over $\mathbb{Q}$. Moreover $P^\sigma = \pm P$. If $P^\sigma = P$ then the two pairs are equal. If $P^\sigma = -P$, then we take $\phi : E \to E$ to be the isomorphism $R \mapsto -R$. This shows that $[(E, P)] = [(E, P^\sigma)]$. Hence $Q \in Y_1(N)(\mathbb{Q})$ as claimed.

In this case the above question has an affirmative answer. Let

$$E' \ : \ Y^2 = X^3 + 1$$

and let

$$\psi \ : \ E \to E', \qquad (X, Y) \mapsto \left(\frac{X}{\sqrt[2]{2}}, \frac{Y}{\sqrt[3]{2}}\right).$$

Let $P' = (0, 1) = \psi(P)$ which is a rational point of order 3 on E'. Then ψ is an isomorphism of pairs $(E, P) \cong (E', P')$. So $Q = [(E', P')]$ and we have answered the above question affirmatively in this case.

Example 15. We take $N = 3$, and

$$E \ : \ Y^2 = X^3 + 1.$$

The third division polynomial for E is $\psi_3(E)(X) = 3X(X^3 + 4)$. Thus $P = (\sqrt[3]{-4}, \sqrt{-3})$ is a point of order 3. Let $Q = [(E, P)] \in Y_1(\overline{\mathbb{Q}})$. We will show that Q is a rational point. If $\sigma \in G_\mathbb{Q}$ then

$$\sigma(P) = (\zeta_3^a \sqrt[3]{-4}, \pm\sqrt{-3}).$$

But $\mathrm{Aut}(E) \cong \mathbb{Z}/6\mathbb{Z}$ generated by

$$\phi : E \to E, \qquad \phi(X, Y) = (\zeta_3 X, -Y).$$

Thus

$$\sigma(P) = \phi^b(P)$$

for some b. Hence $[(E,P)]^\sigma = [(E, P^\sigma)] = [(E,P)]$. Therefore $[(E,P)] \in Y_1(3)(\mathbb{Q})$.

Note that any $E'/\mathbb{Q}$ belonging to the $\overline{\mathbb{Q}}$-isomorphism class of E has the form

$$E' \ : \ Y^2 = X^3 + D$$

where $D \in \mathbb{Z}$ is non-zero. There is an obvious isomorphism

$$\psi \ : \ E \to E', \qquad \psi(X, Y) = (\sqrt[3]{D}X, \sqrt{D}Y).$$

We want a value of D such that $\psi(P) \in E'(\mathbb{Q})$, or equivalently

$$\sqrt[3]{D} \cdot \sqrt[3]{-4} \in \mathbb{Q}, \qquad \sqrt{D} \cdot \sqrt{-3} \in \mathbb{Q}.$$

We can take $D = -27 \times 16$. Thus the answer to the above question is affirmative in this case too!

4. The Modular Curve X_H

We want to generalise the above constructions to an arbitrary group $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

4.1. Level Structure. We call an isomorphism $\alpha : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ a **level N structure on** E. Note that a level N-structure simply corresponds to a choice of basis: $P_1 = \alpha^{-1}(e_1)$, $P_2 = \alpha^{-1}(e_2)$ where $e_1 = (1,0)$, $e_2 = (0,1)$.

Definition 1. We call pairs (E_1, α_1) and (E_2, α_2) **H-isomorphic**, and write

$$(E_1, \alpha_1) \sim_H (E_2, \alpha_2)$$

if there is an isomorphism $\phi : E_1 \to E_2$ and an element $h \in H$ such that

$$\alpha_1 \ = \ h \circ \alpha_2 \circ \phi.$$

Here we think of $h \in H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as an isomorphism $h : (\mathbb{Z}/N\mathbb{Z})^2 \to (\mathbb{Z}/N\mathbb{Z})^2$.

Exercise 16. Show that H-isomorphism is an equivalence relation.

We denote the H-isomorphism class of the pair (E, α) by $[(E, \alpha)]_H$.

Exercise 17. Let $H = B_1(N)$. Show that $(E_1, \alpha_1) \sim_H (E_2, \alpha_2)$ if and only if there is an isomorphism $\phi : E_1 \to E_2$ such that $\phi(P_1) = P_2$, where

$$P_1 = \alpha_1^{-1}(1,0), \qquad P_2 = \alpha_2^{-1}(1,0),$$

are respectively points of order N on E_1, E_2.

Exercise 18. Let $H = B_0(N)$. Show that $(E_1, \alpha_1) \sim_H (E_2, \alpha_2)$ if and only if there is an isomorphism $\phi : E_1 \to E_2$ such that $\phi(\langle P_1 \rangle) = \langle P_2 \rangle$, where P_1, P_2 are as above.

4.2. The congruence subgroup associated to H. Given a subgroup $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ it is possible to define an associated Riemann surface in the following way. Let

$$H_0 := \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cap H, \qquad \Gamma_H := \{A \in \mathrm{SL}_2(\mathbb{Z}) \ : \ (A \mod N) \in H_0\}.$$

Note that

$$\Gamma_H \ \supseteq \ \Gamma(N) \ := \ \{A \in \mathrm{SL}_2(\mathbb{Z}) \ : \ A \equiv I \pmod N\}.$$

Therefore Γ_H is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Exercise 19. Show that

$$\Gamma_{B_0(N)} = \Gamma_0(N), \qquad \Gamma_{B_1(N)} = \Gamma_1(N).$$

Given $\tau \in \mathbb{H}$ we will write α_τ for the level N structure on $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ that satisfies

$$\alpha_\tau(1/N) = (1, 0), \qquad \alpha_\tau(\tau/N) = (0, 1).$$

One checks the following

- if E is an elliptic curve over $\mathbb{C}$ and α is a level N-structure then there exists $\tau \in \mathbb{H}$ such that $E = E_\tau$ and the isomorphism $E_\tau(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ identifies α with α_τ. Thus we can think of (E, α) as $(\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \alpha_\tau)$.
- τ_1, τ_2 lead to H-isomorphic pairs $(\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau_1), \alpha_{\tau_1})$, $(\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau_2), \alpha_{\tau_2})$ if and only if $\tau_1 = \gamma(\tau_2)$ for some $\gamma \in \Gamma_H$.

We conclude that there is a one-one correspondence

$$\Gamma_H\backslash\mathbb{H} \leftrightarrow \{H\text{-isom classes } (E/\mathbb{C}, \alpha)\}, \qquad \Gamma_H \cdot \tau \mapsto [(\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \alpha_\tau)]_H \, .$$

5. The curve X_H

As before there are algebraic curves $X_H \supset Y_H$, with X_H complete and Y_H open such that

$$Y_H(\mathbb{C}) \cong \Gamma_H\backslash\mathbb{H}, \qquad X_H(\mathbb{C}) \cong \Gamma_H\backslash\mathbb{H}^*,$$

where the isomorphisms are isomorphisms of Riemann surfaces. Moreover, $\Gamma_H\backslash\mathbb{H}^*$ is compact.

Recall that there is an isomorphism

$$\chi_N \ : \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z})^*.$$

Now $\det(H)$ is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ and so we can identify it with a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. So it makes sense to speak of the fixed field

$$L_H \ := \ \mathbb{Q}(\zeta_N)^{\det(H)}.$$

Theorem 20. *The modular curve X_H has a model defined over L_H.*

Note, since $\Gamma_H \subset \mathrm{SL}_2(\mathbb{Z})$ we have a natural surjective morphism of Riemann surfaces

$$\Gamma_H\backslash\mathbb{H}^* \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*, \qquad \Gamma_H \cdot \tau \to \mathrm{SL}_2(\mathbb{Z}) \cdot \tau.$$

This induces a non-constant morphism of curves $X_H \to X(1)$, again defined over L_H, which we denote by j (on complex points it factors through the earlier j-map $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^* \to X(1)(\mathbb{C})$).

Assumption: we shall henceforth impose the condition $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$. Thus X_H is defined over $\mathbb{Q}$, and so is the $j : X_H \to X(1)$. The cusps of X_H is the set $j^{-1}(\infty)$, and we have $Y_H := X_H \setminus j^{-1}(\infty)$.

Now let K be a perfect field, which has characteristic 0, or such that $\mathrm{char}(K) \nmid N$. A point $Q \in Y_H(\overline{K})$ represents an H-isomorphism class of pairs $[(E,\alpha)]_H$ where E is an elliptic curve defined over $\overline{K}$ and α is a mod N level structure on E; we identify Q with $[(E,\alpha)]_H$ and so write $Q = [(E,\alpha)]_H$.

LEMMA 5.1. *Let $Q = [(E,\alpha)]_H \in Y_H(\overline{K})$. Let $E'/\overline{K}$ be an elliptic curve that is isomorphic to E. Then there is some isomorphism $\alpha' : E'[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ such that $Q = [(E',\alpha')]_H$.*

What the lemma is saying is that for any point Q on Y_H I can replace E by any isomorphic E' and obtain the same point Q provided I suitably choose the mod N level structure on E'.

PROOF. Let $\phi : E \to E'$ be an isomorphism. Let $\alpha' = \alpha \circ \phi^{-1}$. Observe that $\alpha = I \circ \alpha' \circ \phi$ where I is the identity element in H. Thus $(E,\alpha) \sim_H (E',\alpha')$. □

6. Galois action and rationality

There is an action of G_K on the pairs (E,α)

$$(E,\alpha)^\sigma \ := \ (E^\sigma, \alpha \circ \sigma^{-1}).$$

This action is compatible with action of G_K on $Y_H(\overline{K})$. In other words, if $Q = [(E,\alpha)]_H$ then $Q^\sigma = [(E^\sigma, \alpha \circ \sigma^{-1})]_H$.

LEMMA 6.1. *Let $Q \in Y_H(\overline{K})$. Then $Q \in Y_H(K)$ if and only if $Q = [(E,\alpha)]_H$ for some E/K, and some level N structure $\alpha : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ such that for all $\sigma \in G_K$, there is an $\phi_\sigma \in \mathrm{Aut}_{\overline{K}}(E)$ and $h_\sigma \in H$ satisfying*

$$\alpha = h_\sigma \circ \alpha \circ \sigma^{-1} \circ \phi_\sigma. \tag{3}$$

PROOF. $\Longleftarrow$ Condition (3) implies $(E,\alpha) \sim_H (E, \alpha \circ \sigma^{-1})$. Thus $Q^\sigma = Q$ for all $\sigma \in G_K$ and so $Q \in Y_H(K)$.

$\Longrightarrow$ Suppose $Q \in Y_H(K)$ and write $Q = [(E,\alpha)]_H$. Note that $E \cong E^\sigma$ for all $\sigma \in G_K$. Thus the j-invariant $j(E)$ belongs to K. It follows that E is isomorphic to some elliptic curve defined over K. By Lemma 5.1 we are allowed to suppose that E is in fact defined over K. Since $Q^\sigma = Q$ for all $\sigma \in G_K$ we have $(E,\alpha) \sim_H (E, \alpha \circ \sigma^{-1})$. Now (3) follows from the definition of $\sim_H$. □

6.1. The case $-I \in H$.

THEOREM 21. *Let $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Suppose*

- $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$;
- $-I \in H$.

Then X_H, Y_H are defined over $\mathbb{Q}$ (in fact they have models defined over $\mathrm{Spec}(\mathbb{Z}[1/N])$).

(i) *Every $Q \in Y_H(K)$ is supported on some E/K (this means that there is some E/K and an isomorphism $\alpha : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ such that $Q = [(E,\alpha)]_H$).*

(ii) *If $Q \in Y_H(K)$ and $j(Q) \neq 0$, 1728, then $Q = [(E,\alpha)]_H$ such that E is defined over K and $\overline{\rho}_{E,N}(G_K) \subset H$ (up to conjugation). Conversely, if there is E is defined over K and $\overline{\rho}_{E,N}(G_K) \subset H$ (up to conjugation) then $[(E,\alpha)] \in Y_H(K)$ for a suitable α.*

(iii) *If $Q \in Y_H(K)$ and $j(Q) \neq 0$, 1728, and $Q = [(E, \alpha)]_H$ as above, then $Q = [(E', \alpha')]$ for any quadratic twist E'/K defined over K, and for suitable α'.*

PROOF. Let's fill in some of the details for (ii) using Lemma 6.1. Note that $j(Q) = j(E)$. As this $\neq 0$, 1728, the automorphism group $\mathrm{Aut}(E) = \{1, -1\}$. Thus $\phi_\sigma = \pm 1$ and in particular commutes with all other maps. Thus (3) can be rewritten as

$$\alpha \circ \sigma = (\phi_\sigma h_\sigma) \circ \alpha.$$

This can be rewritten as

$$\overline{\rho}_{E,N}(\sigma) \ = \ \phi_\sigma h_\sigma$$

once we have taken $\alpha^{-1}(1, 0)$, $\alpha^{-1}(0, 1)$ as basis for $E[N]$. Note that $\phi_\sigma h_\sigma = \pm h_\sigma \in H$. Thus $\overline{\rho}_{E,N}(G_K) \subseteq H$ as required. Since quadratic twisting multiplies the $\overline{\rho}_{E,N}$ by a character taking values in ± 1, replacing E by a quadratic twist does not change the property $\overline{\rho}_{E,N}(G_K) \subseteq H$. □

Note, if $-I \in H$, then a rational point on Y_H corresponds to an infinite family of quadratic twists (away from j-invariants 0, 1728). Therefore Y_H is a 'coarse moduli space'.

7. The case $-I \notin H$

THEOREM 22. *Let $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Suppose*

- $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$;
- $-I \notin H$.

Then X_H, Y_H are defined over $\mathbb{Q}$ (in fact they have models defined over $\mathrm{Spec}(\mathbb{Z}[1/N])$).

(i) *Every $Q \in Y_H(K)$ is supported on some E/K (this means that there is some E/K and an isomorphism $\alpha : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ such that $Q = [(E, \alpha)]_H$).*

(ii) *If $Q \in Y_H(K)$ and $j(Q) \neq 0$, 1728, then $Q = [(E, \alpha)]_H$ such that E is defined over K and $\overline{\rho}_{E,N}(G_K) \subset H$ (up to conjugation). Conversely, if there is E is defined over K and $\overline{\rho}_{E,N}(G_K) \subset H$ (up to conjugation) then $[(E, \alpha)] \in Y_H(K)$ for a suitable α.*

(iii) *If $Q \in Y_H(K)$ and $j(Q) \neq 0$, 1728, and $Q = [(E, \alpha)]_H$ as above, then E is unique.*

PROOF. Again let's fill in some of the details for (ii) using Lemma 6.1. As before $\phi_\sigma \in \{\pm 1\}$ and

$$\overline{\rho}_{E,N}(\sigma) \ = \ \phi_\sigma h_\sigma$$

once we have taken $\alpha^{-1}(1, 0)$, $\alpha^{-1}(0, 1)$ as basis for $E[N]$. Let $H' = \langle H, -I \rangle \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Since $-I$ commutes with the elements of H, we have that H is a normal subgroup of H' of index 2. Now consider the map

$$\psi : G_K \to \frac{H'}{H} \cong \{\pm I\}, \qquad \psi(\sigma) = \overline{\rho}(\sigma) \cdot H = \psi_\sigma.$$

Since $\overline{\rho}$ is a homomorphism, the map ψ is also a homomorphism and so a quadratic character, or trivial. If ψ is trivial then $\overline{\rho}_{E,N}(G_K) \subset H$. Otherwise ψ is a quadratic character, and by Galois theory its kernel fixes a quadratic extension $K(\sqrt{d})$ of K. Now $\overline{\rho}_{E_d,N} = \psi \cdot \overline{\rho}_{E,N}$, and thus $\overline{\rho}_{E_d,N}(\sigma) = h_\sigma \in H$. Therefore replace E by E_d

and adjusting the level structure α gives $Q = [(E, \alpha)]_H$ with E defined over K and $\overline{\rho}_{E,N}(G_K) \subset H$. □

Note that away from j-invariants 0, 1728, the modular curve Y_H is a 'fine moduli space', by which we mean that a rational point is supported on a unique elliptic curve. Indeed, let

$$U := X_H \setminus j^{-1}\{0, 1728, \infty\}.$$

There is an elliptic surface

$$\mathcal{E} \to U$$

which we think of as a family of (smooth) elliptic curves parametrized by the points of U, and we write $\mathcal{E}_Q$ for the fibre above $Q \in U$. If $Q \in U(K)$ then $\mathcal{E}_Q$ is defined over K. Moreover, the image $\overline{\rho}_{\mathcal{E}_Q,N}(G_K)$ is contained in a subgroup conjugate to H, and $Q = [(E, \alpha)]_H$ for a suitable α. Conversely, if E/K is an elliptic curve with $j(E) \neq 0$, 1728 and $\overline{\rho}_{\mathcal{E}}(G_K)$ is conjugate to a subgroup of H then there is some $Q \in U(K)$ (possibly non-unique) such that $E \cong \mathcal{E}_Q$. The family $\mathcal{E}$ is called the **universal elliptic curve over** X_H.

8. Modular Curves corresponding to subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

Let p be an odd prime. In Dickson's classification we met groups $B_0(p)$, $C_s^+(p)$, $C_{ns}^+(p)$, and those with images isomorphic to A_4, S_4, A_5 in $\mathrm{PGL}_2(\mathbb{F}_p)$ (the case A_5 only arises for $p \equiv \pm 1 \pmod 5$). Corresponding to these six subgroups, there are six modular curves $X_0(p)$, $X_s^+(p)$, $X_{ns}^+(p)$, $X_{A_4}(p)$, $X_{S_4}(p)$ and $X_{A_5}(p)$ (again the last case is only for $p \equiv \pm 1 \pmod 5$). To prove Serre's uniformity conjecture, it is enough to show that the rational points on each of these curves are either CM or cuspidal for $p > 37$. In fact this has been accomplished for all these families except $X_{ns}^+(p)$.

Theorem 23 (Serre). *If $p \geq 11$ then $X(\mathbb{Q}_p) = \emptyset$ for $X = X_{A_4}(p)$, $X_{S_4}(p)$, $X_{A_5}(p)$.*

Theorem 24 (Mazur). *If $p > 37$ then $X_0(p)(\mathbb{Q}) \subset \{$cusps, cm points$\}$.*

Theorem 25 (Bilu, Parent and Rebolledo). *If $p > 13$ then $X_s^+(p)(\mathbb{Q}) \subset \{$cusps, cm points$\}$.*

Theorem 26 (Balakrishnan, Dogra, Müller, Tuitman, Vonk). *$X_s^+(13)(\mathbb{Q})$ and $X_{ns}^+(13)(\mathbb{Q})$ consist of cusps and CM points.*

The question of rational points on $X_{ns}^+(p)$ is a famous open problem.

CHAPTER 4

A Naive Approach to Equations for $X_1(N)$

1. Mazur's Theorem on Torsion

THEOREM 27 (Mazur). *Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the groups*

$$\begin{cases} \mathbb{Z}/N\mathbb{Z} & (N = 1, 2, \ldots, 10, 12), \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & (N = 1, 2, 3, 4). \end{cases}$$

The main part of the proof of this great theorem is to show that for $p \geq 11$ prime, there are no elliptic curves $E/\mathbb{Q}$ with a rational point of order p. This is equivalent to the following theorem.

THEOREM 28 (Mazur). *$X_1(p)(\mathbb{Q})$ consists entirely of cusps for $p \geq 11$ prime.*

2. Tate Form

LEMMA 2.1. *Let E/K be an elliptic curve and $P \in E(K)$ such that P, $2P$, $3P \neq 0$. Then there is a change of coordinates (defined over K) so that E becomes the model*

$$E_{u,v} \ : \ Y^2 + uXY + vY = X^3 + vX^2\,, \qquad P = (0,0), \tag{4}$$

where u, $v \in K$.

PROOF. This is an easy exercise. Since $P \neq 0$ it belongs to the affine plane in any Weierstrass model for E. Simply shifting P to $(0,0)$ ensures that E has the form

$$E \ : \ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X.$$

Now the condition $2P \neq 0$ ensures that $a_3 \neq 0$. Now rotate the (X,Y)-plane so that the tangent at $(0,0)$ is the X-axis (for this you will need $a_3 \neq 0$), and then stretch so that $a_2 = a_3$ (this is where you will use the fact that $3P \neq 0$). □

The model $E_{u,v}$ is called the **Tate form** for E. It can be used (rather painfully) to give a model for $X_1(p)$ for small values of p.

3. $X_1(5)$

In the Tate form (4) you can check that $5P = 0$ if and only if $u = v + 1$. If you want to do this computation, it is easiest to rewrite $5P = 0$ as $3P = -2P$. This in fact tells us that $X_1(5) \cong \mathbb{P}^1$. The parameter v is a parameter on $X_1(5) \cong \mathbb{P}^1$ and corresponding to this is the elliptic curve

$$E_v \ : \ Y^2 + (v+1)XY + vY = X^3 + vX^2.$$

The point $(0,0)$ is a point of order 5 on E_v. We have almost completed our task of classifying all elliptic curves over K with a rational point of order 5. We must check

whether the model E_v is smooth (and therefore really defines an elliptic curve) or singular. The discriminant of the model is

$$\Delta(E_v) \;=\; -v^5 \cdot (v^2 + 11v - 1).$$

Thus the values $v = 0$, $v = (-11 \pm 5\sqrt{5})/2$ do not correspond to elliptic curves. What about $v = \infty \in \mathbb{P}^1(\mathbb{Q})$. Here it is easier to work with the j-invariant of E_v:

$$j(E_v) \;=\; \frac{(v^4 + 12v^3 + 14v^2 - 12v + 1)^3}{-v^5 \cdot (v^2 + 11v - 1)}\,.$$

so that when $v = \infty$ we have $j(E_v) = \infty$ so E_v is not an elliptic curve. The values $\{\infty, 0, (-11 \pm 5\sqrt{5})/2\}$ are the cusps of $X_1(5)$. The curve E_v is called the **universal elliptic curve over** $X_1(5)$.

4. $X_1(11)$

Repeating the above calculation with 11 instead of 5 it is possible to show that $X_1(11)$ is the elliptic curve `11A3` with Weierstrass model

$$X_1(11) \;:\; s^2 - s = t^3 - t.$$

The universal elliptic curve over $X_1(11)$ is

$$E_{s,t} \;:\; Y^2 + (st + t - s^2)XY + s(s-1)(s-t)t^2Y \;=\; X^3 + s(s-1)(s-t)tX^2\,.$$

Thus an elliptic curve E/K with a K-rational point over order 11 is isomorphic to $E_{s,t}$ for some $(s,t) \in X_1(11)(K)$ where the point of order 11 becomes the point $(0,0)$ on the model $E_{s,t}$. The converse is true if we avoid the cusps; if $(s,t) \in X_1(11)(K)$ is a non-cuspidal point then $E_{s,t}$ is an elliptic curve defined over K with $(0,0)$ a point of order 11.

The Mordell–Weil group of $X_1(11)/\mathbb{Q}$ is

$$X_1(11)(\mathbb{Q}) \;=\; \{0,\ (0,0),\ (0,1),\ (1,0),\ (1,1)\} \;\cong\; \mathbb{Z}/5\mathbb{Z}.$$

It turns out that $X_1(11)$ has 10 cusps, and the five rational points are among the 10 cusps. Thus there are no elliptic curves $E/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order 11. The other cusps are given by the equations

$$t^5 - 18t^4 + 35t^3 - 16t^2 - 2t + 1 = 0, \qquad s = \frac{-3t^4 + 52t^3 - 74t^2 + 17t + 10}{11},$$

which give five cusps defined over $\mathbb{Q}(\zeta_{11})^+$.

CHAPTER 5

Jacobians of Curves

It is convenient for now to talk about general curves. Let X be a curve over a field K, and let $g = g(X)$ be the genus. Functorially associated to X is its Jacobian $J = J_X$ which is an abelian variety defined over K of dimension g. Jacobians give us a way of studying K-points on X. If $X(K) \neq \emptyset$ and $g \geq 1$ then we have an embedding $X(K) \hookrightarrow J(K)$, and the set $J(K)$ is an abelian group. If we understand $J(K)$ as an abelian group we might hope to say something about $X(K)$. Unfortunately it is in general very hard to write down equations for J. The best computational approach to J is via divisors.

1. Divisors

Let X be a curve over k. A divisor D on X is a formal linear combination

$$D = \sum_{i=1}^{n} a_i P_i, \qquad a_i \in \mathbb{Z}, \quad P_i \in X(\overline{K}).$$

We define the **degree** of D to be $\sum a_i$. We say that D is **rational** if it is invariant under $G_K := \mathrm{Gal}(\overline{K}/K)$.

Example 29. Let

$$X \ : \ y^2 = x(x^2+1)(x^3+1).$$

This is a genus 2 curve defined over $\mathbb{Q}$. Let

$$D_1 = 2 \cdot (0,0) + (1,2), \quad D_2 = (i,0) - (-i,0), \quad D_3 = (i,0) + (-i,0) - 2 \cdot (1,2).$$

These are divisors and their degrees are

$$\deg(D_1) = 3, \qquad \deg(D_2) = 0, \qquad \deg(D_3) = 0.$$

Observe that any $\sigma \in G_{\mathbb{Q}}$ sends i to itself (e.g. σ is the identity) or changes its sign (e.g. σ is complex conjugation). Thus D_1 is rational, D_3 is rational, but D_2 is **not** rational, since complex conjugation negates it.

The **divisor group** of X/K, denoted by $\mathrm{Div}(X/K)$ is the set of rational divisors of X/K. This is obviously an abelian group with addition defined in the obvious formal way. The **degree** 0 **subgroup of the divisor group** is the subgroup

$$\mathrm{Div}^0(X/K) := \{D \in \mathrm{Div}(X/K) \ : \ \deg(D) = 0\}.$$

This is an abelian group.

Example 30. We continue Example 29. In the example $D_3 \in \mathrm{Div}^0(X/\mathbb{Q})$, but $D_1,\ D_2 \notin \mathrm{Div}^0(X/\mathbb{Q})$.

2. Principal Divisors

Let X be a curve defined over a field K. Let $K(X)$ be the function field of X, and let $f \in K(X)^*$. If $P \in X(\overline{K})$ then there is $\upsilon_P(f) \in \mathbb{Z}$ which measures the **order of vanishing** of f at P. Define

$$\operatorname{div}(f) = \sum_{P \in X(\overline{K})} \upsilon_P(f) \cdot P.$$

A divisor of the form $\operatorname{div}(f)$ is called a **principal divisor**.

LEMMA 2.1. *If $f \in K(X)^*$ then $\operatorname{div}(f) \in \operatorname{Div}^0(X/K)$.*

EXAMPLE 31. Let $f = \frac{x^2-7}{x^3}$ on $\mathbb{P}^1/\mathbb{Q}$. Then

$$\operatorname{div}(f) = -3 \cdot (0) + (\sqrt{7}) + (-\sqrt{7}) + \infty.$$

Intuitively, if x is large, then $f \sim 1/x$ which explains why it vanishes to order 1 at ∞. Observe that $\operatorname{div}(f) \in \operatorname{Div}^0(\mathbb{P}^1/\mathbb{Q})$.

3. The Picard Group

It follows from Fact 2.1 that

$$\operatorname{Princ}(X/K) := \{\operatorname{div}(f) : f \in k(X)^*\}$$

is contained in $\operatorname{Div}^0(X/K)$. This is called the **subgroup of principal divisors**. It is easy to show that it is a subgroup using the properties

$$\operatorname{div}(1) = 0, \qquad \operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g), \qquad \operatorname{div}(1/f) = -\operatorname{div}(f),$$

that follow from the definition of div. We define the **Picard group** of X/K as

$$\operatorname{Pic}^0(X/K) := \frac{\operatorname{Div}^0(X/K)}{\operatorname{Princ}(X/K)}.$$

The following two theorems are standard consequences of the Riemann–Roch Theorem (See [**22**, Chapters II and III]).

THEOREM 32.

$$\operatorname{Pic}^0(\mathbb{P}^1/K) = 0.$$

THEOREM 33. *Let*

$$E \ : \ y^2 = x^3 + Ax + B, \qquad A, B \in K, \quad 4A^3 + 27B^2 \neq 0.$$

be an elliptic curve over K. Then

$$E(k) \cong \operatorname{Pic}^0(E/K), \qquad P \mapsto [P - \infty]. \tag{5}$$

In (5), the group operation on $E(K)$ is the usual one defined by secants and tangents.

If X is a curve that isn't an elliptic curve, what is the correct object to replace $X(K)$ in the isomorphism (5)?

4. Jacobians

Let X/K be a curve of genus g. We don't define the **Jacobian** J_X of X, but mention that it is a g-dimensional abelian variety defined over K that is 'functorially associated' to X. An elliptic curve E is its own Jacobian $J_E = E$.

THEOREM 34. *(Mordell–Weil Theorem) If K is a number field then $J_C(K)$ is a finitely generated abelian group.*

The proof uses descent and heights and is similar to the proof of the Mordell–Weil Theorem for elliptic curves. We can often compute $J_X(K)$ in practice, but there is no algorithm guaranteed to work.

THEOREM 35. *Let X be a curve with $X(K) \neq \emptyset$. Then*

$$J_X(K) \cong \mathrm{Pic}^0(X/K).$$

For more on this theorem see [**19**, Section 3]. We usually use elements of $\mathrm{Pic}^0(X/K)$ to represent elements of $J_X(K)$.

EXAMPLE 36. We continue Example 29. Let

$$X \ : \ y^2 = x(x^2+1)(x^2+3).$$

This is a curve of genus 2 defined over $\mathbb{Q}$. It has one rational point at infinity which we denote by ∞ (and which we see on a smooth model in a projective plane with appropriate weights). The curve X has genus 2. Using descent it is possible to show that

$$J_X(\mathbb{Q}) = \frac{\mathbb{Z}}{2\mathbb{Z}} \cdot [(0,0) - \infty] \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \cdot [(i,0) + (-i,0) - 2\infty].$$

It is easy to check that

$$[(0,0) - \infty] + [(i,0) + (-i,0) - 2\infty] = [(\sqrt{-3},0) + (-\sqrt{-3},0) - 2\infty];$$

to check this the reader should write down a function on X whose divisor is

$$(0,0) + (i,0) + (-i,0) - (\sqrt{-3},0) - (-\sqrt{-3},0) - \infty.$$

DEFINITION 2. Let X/K be a curve of genus ≥ 1. Let $P_0 \in X(K)$. The **Abel–Jacobi** map associated to P_0 is the embedding

$$\iota \ : \ X \hookrightarrow J_X, \qquad P \to [P - P_0].$$

LEMMA 4.1. *If X has genus ≥ 1 and $P_0 \in X(K)$ then $\iota(X(K)) \subseteq J_X(k)$. If moreover $J_X(K)$ is finite (and we know it) we can compute $X(K)$.*

5. Torsion Subgroups

Let $\mathcal{A}$ be an abelian variety over a number field K. The Mordell–Weil theorem applies to abelian varieties too and tells us that $\mathcal{A}(K)$ is a finitely generated abelian group. In particular, the torsion subgroup $\mathcal{A}(K)_{\mathrm{tors}}$ is finite.

Let $\mathfrak{p}$ be a prime of K that is of good reduction for $\mathcal{A}$. Then we have a natural homomorphism

$$\mathrm{red}_{\mathfrak{p}} \ : \ \mathcal{A}(K) \to \mathcal{A}(\mathbb{F}_{\mathfrak{p}})$$

that takes a point $P \in \mathcal{A}(K)$ and reduces it modulo $\mathfrak{p}$. The following is a standard type of result; see [**13**, Appendix].

THEOREM 37 (Katz). *With notation as above (in particular $\mathfrak{p}$ is a prime of good reduction for $\mathcal{A}$), let p be the rational prime below $\mathfrak{p}$ and write $e(\mathfrak{p}/p)$ for the ramification degree. Suppose $e(\mathfrak{p}/p) < p-1$. Then $\mathrm{red}_{\mathfrak{p}}$ is injective when restricted to the torsion subgroup $\mathcal{A}(K)_{\mathrm{tors}}$.*

The following is immediate.

COROLLARY 5.1. *Let $\mathcal{A}$ be an abelian variety over $\mathbb{Q}$. Let $p \geq 3$ be a prime of good reduction. Then red_p is injective when restricted to the torsion subgroup $\mathcal{A}(\mathbb{Q})_{\mathrm{tors}}$.*

CHAPTER 6

Jacobians of Modular curves and Eichler–Shimura

Return to our setting: H is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$ and $-I \in H$. Write J_H for the Jacobian of X_H. These in fact have models over $\mathrm{Spec}(\mathbb{Z}[1/N])$ so they good reduction away from N.

Recall that we defined a congruence subgroup Γ_H associated to H.

$$H_0 := \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cap H, \qquad \Gamma_H := \{A \in \mathrm{SL}_2(\mathbb{Z}) \ : \ (A \mod N) \in H_0\}.$$

There is an isomorphism

$$S_2(\Gamma_H) \cong \Omega(X_H), \qquad f(q) \mapsto f(q)\frac{dq}{q},$$

where $S_2(\Gamma_H)$ is space of weight 2 cuspforms for the group Γ_H and $\Omega(X_H)$ is the space of regular differentials on X_H. In particular,

$$\mathrm{genus}(X_H) \ := \ \dim(\Omega(X_H)) \ = \ \dim(S_2(\Gamma_H)).$$

There is an action of the Hecke algebra on $S_2(\Gamma_H)$. Let $f_1, \ldots, f_n$ be representatives of Galois orbits of Hecke eigenforms. Eichler–Shimura associate an abelian variety $\mathcal{A}_f/\mathbb{Q}$ to each eigenform $f \in \{f_1, \ldots, f_n\}$. Let K_f be the Hecke eigenvalue field of f. Then

$$[K_f : \mathbb{Q}] = \dim(\mathcal{A}_f).$$

Moreover, $\mathrm{End}_{\mathbb{Q}}(\mathcal{A}_f)$ is an order in K_f (we say that $\mathcal{A}_f$ is of GL_2-type).

THEOREM 38. $\mathrm{rank}(\mathcal{A}_f(\mathbb{Q}))$ *is a multiple of* $[K_f : \mathbb{Q}]$.

Finally,

$$J_H \ \sim \ \mathcal{A}_{f_1} \times \mathcal{A}_{f_2} \times \cdots \times \mathcal{A}_{f_n},$$

where $\sim$ denotes isogeny over $\mathbb{Q}$.

Now let $g \in \{f_1, \ldots, f_n\}$, let K_g be the Hecke eigenvalue field of g, and let $\sigma_1, \ldots, \sigma_d : K_g \hookrightarrow \mathbb{C}$ be the embeddings of $\mathbb{C}$ (here $d = [K_g : \mathbb{Q}] = \dim(\mathcal{A}_g)$). Let $g_i = \sigma(g)$ be the conjugates of g. Then we have an equality of L-function.

$$L(\mathcal{A}_g, s) = \prod_{i=1}^{d} L(g_i, s).$$

We have the following famous theorem, which is a version of weak BSD for modular Jacobians.

THEOREM 39 (Kolyvagin and Logachev). *Suppose* $\mathcal{A}_g$ *is a factor of* $J_0(M)$ *for some* M.

(i) *If* $\mathrm{ord}_{s=1}(L(g_i, s)) = 0$ *for some* i *then* $\mathrm{ord}_{s=1}(L(g_i, s)) = 0$ *for all* i *and* $\mathrm{rank}(\mathcal{A}_g(\mathbb{Q})) = 0$.

(ii) *If* $\mathrm{ord}_{s=1}(L(g_i, s)) = 1$ *for some* i *then* $\mathrm{ord}_{s=1}(L(g_i, s)) = 1$ *for all* i *and* $\mathrm{rank}(\mathcal{A}_g(\mathbb{Q})) = \dim(\mathcal{A}_g) = [K_g : \mathbb{Q}]$.

In fact, $L(\mathcal{A}_g, 1)/\Omega_g$ is a rational number, where Ω_g is integral of the Néron differential over $\mathcal{A}_g(\mathbb{R})$. The modular symbols algorithm [**5**] can in fact compute $L(\mathcal{A}_g, 1)/\Omega_g$ exactly, so we have a way of testing if $L(\mathcal{A}_g, s)$ vanishes or not at $s = 1$. Values $L^{(r)}(\mathcal{A}_g, 1)$ can only be computed numerically for $r \geq 1$.

EXAMPLE 40. Let us consider $X_0(43)$ and its Jacobian $J_0(43)$. The modular symbols algorithm (implemented in `Magma` and in `SAGE`) allows us to compute the eigenforms belonging to $S_2(\Gamma_0(43))$; see [**25**] for details. These are

$$\begin{aligned} f &= q - 2q^2 - 2q^3 + 2q^4 - 4q^5 + \cdots \\ g_1 &= q + \sqrt{2} \cdot q^2 - \sqrt{2} \cdot q^3 + (2 - \sqrt{2}) \cdot q^5 + \cdots \\ g_2 &= q - \sqrt{2} \cdot q^2 + \sqrt{2} \cdot q^3 + (2 + \sqrt{2}) \cdot q^5 + \cdots \end{aligned}$$

The Hecke eigenvalue field for f is $\mathbb{Q}$. The eigenform f corresponds to a dimension 1 abelian variety, which is the elliptic curve 43A1 with Weierstrass model

$$\mathcal{A}_f \ : \ y^2 + y = x^3 + x^2.$$

Note that g_1, g_2 form a single Galois orbit, with Hecke eigenvalue field $\mathbb{Q}(\sqrt{2})$ of degree 2. The abelian variety $\mathcal{A}_{g_1} = \mathcal{A}_{g_2}$ has dimension 2. There is probably no easy way of giving equations for it. It might not even be a Jacobian. Moreover,

$$J_0(43) \sim \mathcal{A}_f \times \mathcal{A}_{g_1}$$

has dimension 3 and so $X_0(43)$ has genus 3. What can we say about the Mordell–Weil group $J_0(43)(\mathbb{Q})$?

In fact

$$\frac{L(\mathcal{A}_f, 1)}{\Omega_{\mathcal{A}_f}} = 0, \qquad \frac{L(\mathcal{A}_{g_1}, 1)}{\Omega_{\mathcal{A}_g}} = \frac{2}{7}.$$

So we know that $\mathcal{A}_{g_1}(\mathbb{Q})$ has rank 0 from the Kolyvagin–Logachev theorem. What about $\mathcal{A}_f(\mathbb{Q})$? We find that

$$L'(f, 1) = 0.34352\ldots$$

so by the Kolyvagin–Logachev theorem, $\mathcal{A}_f(\mathbb{Q})$ has rank 1. Hence $J_0(43)(\mathbb{Q})$ has rank 1.

EXAMPLE 41. Let's consider $J_0(31)$ instead. There is only one Galois orbit of eigenforms of weight 2 for $\Gamma_0(31)$:

$$\begin{aligned} f_1 &= q + \alpha q^2 - 2\alpha q^3 + (\alpha - 1)q^4 + q^5 + \cdots, \qquad \alpha = \frac{1 + \sqrt{5}}{2} \\ f_2 &= q + \beta q^2 - 2\beta q^3 + (\beta - 1)q^4 + q^5 + \cdots, \qquad \beta = \frac{1 - \sqrt{5}}{2}. \end{aligned}$$

Thus $J_0(31)$ is a simple 2-dimensional abelian variety. We find that $L(J_0(31))/\Omega = 2/5$, so $J_0(31)(\mathbb{Q})$ has rank 0.

Let's use this fact to show that there are no elliptic curves over $\mathbb{Q}$ with a point of order 31. We consider this commutative diagram.

$$\begin{array}{ccccc} X_1(31)(\mathbb{Q}) & \xrightarrow{\pi} & X_0(31)(\mathbb{Q}) & \longrightarrow & X(1)(\mathbb{Q}) \\ \downarrow & & \downarrow & & \downarrow \\ X_1(31)(\mathbb{F}_3) & \longrightarrow & X_0(31)(\mathbb{F}_3) & \longrightarrow & X(1)(\mathbb{F}_3). \end{array}$$

Suppose $E/\mathbb{Q}$ has a $\mathbb{Q}$-rational point of order 31. This gives rise to a non-cuspidal rational point $P \in X_1(31)(\mathbb{Q})$. Suppose that E has good reduction at 3. Then, by the injectivity of torsion, $E(\mathbb{F}_3)$ has a point of order 31, which is impossible because $\#E(\mathbb{F}_3) \leq 7$ by the Hasse–Weil bounds. So E cannot have good reduction at 3. Let's instead suppose that E has potentially good reduction at 3 (in particular $\mathrm{ord}_3(j(E)) \geq 0$). We consider the filtration

$$E(\mathbb{Q}_3) \supset E_0(\mathbb{Q}_3) \supset E_1(\mathbb{Q}_3) \supset E_2(\mathbb{Q}_3) \cdots$$

In fact, we know from the theory of the formal group that $E_1(\mathbb{Q}_3) \cong \mathbb{Z}_3$ which has no torsion. Moreover,

$$[E(\mathbb{Q}_3) : E_0(\mathbb{Q}_3)] \leq 4, \qquad [E_0(\mathbb{Q}_3) : E_1(\mathbb{Q}_3)] = \#E_{ns}(\mathbb{F}_3) = 3$$

as E has additive reduction. We see that $E(\mathbb{Q}_3)$ does not have 31 torsion and we have a contradiction.

Hence E has potentially multiplicative reduction at 3. This means that $\mathrm{ord}_3(j(E)) < 0$. Hence the image of P in $X(1)(\mathbb{F}_3)$ is the cusp. Let $Q = \pi(P) \in X_0(31)(\mathbb{Q})$. Then $Q \equiv c \pmod 3$ where c is one of the two cusps on $X_0(31)$ (both of these are rational points). Now consider $[Q - c] \in J_0(31)(\mathbb{Q})$. This is a torsion point since $J_0(31)(\mathbb{Q})$ has rank 0. But its reduction $\widetilde{[Q-c]} = 0 \in J_0(31)(\mathbb{F}_3)$ as $Q \equiv c \pmod 3$. By the injectivity of torsion in reduction (Corollary 5.1) we conclude $[Q-c] = 0$ in $J_0(31)(\mathbb{Q})$. So $Q = c$ (you can use Riemann–Roch to show that if two points on a curve of genus ≥ 1 are linearly equivalent then they must be equal). That is Q is a cusp on $X_0(31)$ and so P is a cusp of $X_1(31)$ giving a contradiction.

Note that we worked with $X_0(31)$ and $J_0(31)$. We only needed the fact that the point comes from $X_1(31)$ to make sure it reduces to a cusp modulo 3. In fact if Q is any rational point on $X_0(31)$ that reduces to a cusp modulo any prime $p \neq 2, 31$ then Q must equal that cusp, by the above argument. We have excluded 2 because we need injectivity of torsion when reducing mod p. We have excluded 31 because $X_0(31)$ has bad reduction at 31. But we can conclude that if $Q \in X_0(31)(\mathbb{Q})$ then $j(Q) \in \mathbb{Z}[1/62]$, so the problem of determining the rational points on $X_0(31)$ is essentially reduced to a problem about integral points.

But it is much easier if we knew the whole Mordell–Weil group. We shall make use of the following theorem.

THEOREM 42 (Mazur). *Let p be a prime. Then*

$$J_0(p)(\mathbb{Q})_{\mathrm{tors}} \;=\; (\mathbb{Z}/d_p\mathbb{Z}) \cdot [c_1 - c_2], \qquad d_p = \text{numerator}\left(\frac{p-1}{12}\right)$$

where c_1, c_2 are the two cusps of $X_0(p)$.

In our case

$$J_0(31)(\mathbb{Q}) = \frac{\mathbb{Z}}{5\mathbb{Z}} \cdot [c_1 - c_2].$$

Now let $Q \in X_0(31)(\mathbb{Q})$. Then $[Q - c_2] = n \cdot [c_1 - c_2]$ for $n = 0, 1, 2, 3, 4$. Thus for one of these values of n, we have $Q \sim n \cdot c_1 + (1 - n) \cdot c_2$. If $n = 0$ then $Q = c_2$ and $n = 1$ then $Q = c_1$. What about the other 3 values of n? Write $D_n = c_1 + (1 - n)c_2$. Then $Q \sim D_n$ which means that $Q = D_n + \mathrm{div}(f)$ where $f \in \mathbb{Q}(X_0(31))^*$. Note that f belongs to the Riemann–Roch space $L(D_n)$. In fact it is possible to compute Riemann–Roch spaces if we have a model for the curve

(for example using an algorithm of Hess that is implemented in `Magma`). A model for $X_0(31)$ was worked out by Galbraith:

$$X_0(31) \quad : \quad y^2 = \underbrace{x^6 - 8x^5 + 6x^4 + 18x^3 - 11x^2 - 14x - 3}_{h}.$$

Here c_1, c_2 are the two points at ∞ on this model. We find that $\dim(L(D_n)) = 1$, 1, 0, 0, 0 for $n = 0, 1, 2, 3, 4$ respectively. Thus we know that there is no point $Q \sim D_n$ for $n = 2$, 3, 4. We conclude that $X_0(31)(\mathbb{Q}) = \{c_1,\ c_2\}$. In particular, there are no elliptic curves over $\mathbb{Q}$ with a 31-isogeny.

Now let's be more ambitious and look at quadratic points. Here we're following a recent paper of Bruin and Najman [**2**]. Let $Q \in X_0(31)(K)$ where K is any quadratic field. Let Q^σ be its Galois conjugate. Now $Q + Q^\sigma$ is a $\mathbb{Q}$-rational divisor of degree 2, and $Q + Q^\sigma - c_1 - c_2$ is a $\mathbb{Q}$-rational divisor of degree 0. In particular, $[Q + Q^\sigma - c_1 - c_2] \in J_0(31)(\mathbb{Q})$ and so

$$Q + Q^\sigma - c_1 - c_2 \sim n(c_1 - c_2)$$

where $0 \leq n \leq 4$. So

$$Q + Q^\sigma = (n+1)c_1 + (1-n)c_2 + \mathrm{div}(f)$$

where $f \in L((n+1)c_1 + (1-n)c_2)$. For $n = 0, 1, 2, 3, 4$ the dimensions of $L((n+1)c_1 + (1-n)c_2)$ are 2, 1, 1, 1, 1. Let's deal with $1 \leq n \leq 4$ first. In each of these cases, $L((n+1)c_1 + (1-n)c_2) = \mathbb{Q} \cdot g_n$ for some non-zero function g_n. And so there is a unique possibility for $Q + Q^\sigma$, namely: $Q + Q^\sigma = (n+1)c_1 + (1-n)c_2 + \mathrm{div}(g_n)$. We obtain

n	$Q + Q^\sigma$
1	$2c_1$
2	$\left(\frac{-1+\sqrt{-3}}{2}, \frac{11+\sqrt{-3}}{2}\right) + \left(\frac{-1-\sqrt{-3}}{2}, \frac{11-\sqrt{-3}}{2}\right)$
3	$\left(\frac{-1+\sqrt{-3}}{2}, -\frac{11+\sqrt{-3}}{2}\right) + \left(\frac{-1-\sqrt{-3}}{2}, -\frac{11-\sqrt{-3}}{2}\right)$
4	$2c_2$

Next we consider, $n = 0$. Then

$$L(c_1 + c_2) = \mathbb{Q} \oplus \mathbb{Q} \cdot x.$$

If we take $f \in \mathbb{Q}$, then $\mathrm{div}(f) = 0$ and so $Q + Q^\sigma = c_1 + c_2$. Suppose $f \notin \mathbb{Q}$. Then it is proportional to $x - u$ for $u \in \mathbb{Q}$, and so $\mathrm{div}(f) = \mathrm{div}(x - u)$. But

$$\mathrm{div}(x - u) \ = \ (u, \sqrt{h(u)}) + (u, -\sqrt{h(u)}) - c_1 - c_2.$$

Hence $Q + Q^\sigma = (u, \sqrt{h(u)}) + (u, -\sqrt{h(u)})$. Note that $h(u)$ is not a square for any $u \in \mathbb{Q}$, since we've already shown that the only two rational points are at infinity. In particular, $Q = (u, \sqrt{h(u)})$, $Q^\sigma = (u, -\sqrt{h(u)})$ so that Q and Q^σ are interchanged by the hyperelliptic involution. Ogg has shown that for $X_0(31)$ that the hyperelliptic involution is w_{31}, the Atkin-Lehner involution. What does w_{31} do? Recall that a point on $X_0(31)$ represents a pair (E, C) where E is an elliptic curve and C is a cyclic subgroup of order 31. Now

$$w_{31}(E, C) \ = \ (E/C, E[31]/C)\,;$$

here E/C is the isogenous elliptic curve. So in our case $Q = [(E, C)]$ and E^σ is isomorphic to E/C. Hence this infinite family of elliptic curves over quadratic fields are quadratic $\mathbb{Q}$-curves (i.e. isogenous to their conjugate).

CHAPTER 7

Sketch of Mazur's Theorem for $X_1(p)$

DEFINITION 3. A morphism of schemes $\theta : X \to Y$ over $\mathrm{Spec}(\mathbb{Z}[1/p])$ is a **formal immersion** at $x \in X(\mathbb{Q})$ if the induced map

$$\hat{\mathcal{O}}_{Y,f(x)} \to \hat{\mathcal{O}}_{X,x}$$

is surjective.

Remark. Let $q \neq p$ be a prime. Let

$$\mathrm{Res}_q(x) \ := \ \{x' \in X(\mathbb{Q}_q) \ : \ x' \equiv x \pmod{q}\}$$

which is called the q-adic residue disc of x. If θ is a formal immersion at x then the map

$$\theta \ : \ \mathrm{Res}_q(x) \to Y(\mathbb{Q}_q)$$

is an injection.

PROPOSITION 0.1. *In the above, suppose $Y = \mathcal{A}$ is an abelian variety such that $\mathcal{A}(\mathbb{Q})$ has rank 0. Suppose θ is a formal immersion at x. Then*

$$X(\mathbb{Q}) \cap \mathrm{Res}_q(x) \ = \ \{x\}$$

for all primes $q \notin \{2, p\}$.

PROOF. Let $x' \in X(\mathbb{Q}) \cap \mathrm{Res}_q(x)$. Then $x' \equiv x \pmod{q}$. Thus $\theta(x') - \theta(x)$ is an element of $\mathcal{A}(\mathbb{Q})$ that reduces to 0 modulo q. But $\mathcal{A}(\mathbb{Q})$ is torsion. By the injectivity of torsion $\theta(x') - \theta(x) = 0$. Thus $\theta(x') = \theta(x)$. However, as θ is a formal immersion at x, and x' belong to $\mathrm{Res}_q(x)$ we have $x = x'$. □

We now sketch a proof of Mazur's Theorem for $X_1(p)$. Suppose $z \in X_1(p)(\mathbb{Q})$. We want to show that z is in fact a cusp. Suppose it is not. Then it represents a pair $[(E, P)]$ where E is an elliptic curve defined over $\mathbb{Q}$ and P is a rational point of order p. We take $q = 3$. Now in the example we can show (because p is large) that E has potentially multiplicative reduction at 3. Let $y = \pi(z)$ where $\pi : X_1(p) \to X_0(p)$ is the degeneracy map. In particular y reduces to one of the cusps on X_0. The Atkin-Lehner involution swaps the cusps. Thus we can suppose that y reduces to the infinity cusp on X_0 which we denote by ∞. To complete the argument we need some large quotient of J that has rank 0. We let $J_e(p)$ be the largest quotient of J that has analytic rank 0. This **Merel's winding quotient**. We know by Kolyvagin–Logachev that this has rank 0. We take θ to be the map $X_0(p) \to J_0(p) \to J_e(p)$. Now we need the highly non-trivial fact that this is a formal immersion at ∞. Now

$$y \in \mathrm{Res}_3(\infty) \cap X_0(3)(\mathbb{Q}).$$

Hence by the above proposition $y = \infty$. Thus z is a cusp.

An important remark: The proofs of Mazur's theorem for $X_0(p)$, Merel's Uniform Boundedness theorem and the theorem of Bilu, Parent and Rebolledo for $X_s^+(p)$ all crucially depend on the existence of a rank 0 quotient of the modular Jacobian. However, for $X_{ns}^+(p)$ it is known that every factor of the Jacobian has odd analytic rank, and so assuming BSD has non-zero rank. This is the reason why Serre's uniformity conjecture is still an open problem.

CHAPTER 8

Equations for Modular Curves

We'll mostly follow the method of Galbraith [**10**] for writing down equations for (a couple of) modular curves.

Let X/K be a curve of genus $g \geq 2$. Let $\Omega(X)$ be the space of regular differentials. This is a K-vector space of dimension g. Let $\omega_1, \ldots, \omega_g$ be a K-basis for $\Omega(X)$. The **canonical map** is the map

$$\phi : X \to \mathbb{P}^{g-1}, \qquad P \mapsto (\omega_1(P) : \cdots : \omega_g(P)).$$

Recall that the ratio of any two differentials ω_1, ω_2 is actually a function on X, so the map makes sense.

Example 43. Consider a genus 2 curve

$$X \ : \ y^2 = a_6 x^6 + \cdots + a_0, \qquad a_i \in K.$$

Here the polynomial on the right hand-side is separable. A basis for $\Omega(X)$ is $\omega_1 = dx/y$ and $\omega_2 = xdx/y$. Note that $\omega_2/\omega_1 = x$. Thus

$$\phi : X \to \mathbb{P}^1, \qquad P \mapsto (1 : x(P)).$$

In particular, the image of ϕ is $\mathbb{P}^1$, and so ϕ is **not** an isomorphism, but is 2 to 1.

Let's instead look at a genus 3 curve

$$X \ : \ y^2 = a_8 x^8 + \cdots + a_0, \qquad a_i \in K.$$

A basis for $\Omega(X)$ is $\omega_1 = dx/y$, $\omega_2 = xdx/y$, $\omega_3 = x^2 dx/y$. Thus

$$\phi : X \to \mathbb{P}^2, \qquad \phi(x, y) = (1 : x : x^2).$$

If we choose coordinates $(u_1 : u_2 : u_3)$ for $\mathbb{P}^2$ then the image is the conic $u_1 u_3 = u_2^2$.

More generally, a hyperelliptic curve of genus g can be written as

$$X \ : \ y^2 = a_{2g+2} x^{2g+2} + \cdots + a_0, \qquad a_i \in K.$$

Here the polynomial again needs to be separable to obtain genus g. A basis for $\Omega(X)$ is

$$\frac{dx}{y}, \ \frac{xdx}{y}, \ldots, \ \frac{x^{g-1}dx}{y}.$$

Check that the image of the canonical map is isomorphic to $\mathbb{P}^1$.

Theorem 44. *Let X be a curve of genus ≥ 2. The canonical map is an embedding if and only if X is non-hyperelliptic. In this case $\phi(X)$ has degree $2g-2$.*

We'll focus on modular curves where the genus is ≥ 2. Recall the isomorphism

$$S_2(\Gamma_H) \cong \Omega(X_H), \qquad f(q) \mapsto f(q)\frac{dq}{q}.$$

Let $f_1, \dots, f_g$ be a basis for $S_2(\Gamma_H)$. Then the canonical map is given by

$$\phi = (f_1(q)dq/q : f_2(q)dq/q : \cdots : f_g(q)dq/q) = (f_1(q) : \cdots : f_g(q)).$$

1. $X_0(30)$ and $X_0(45)$

Let's look first at $X_0(30)$. A basis for $S_2(\Gamma_0(30))$ is

$$\begin{aligned} f_1 &= q - q^4 - q^6 - 2q^7 + q^9 + O(q^{10}), \\ f_2 &= q^2 - q^4 - q^6 - q^8 + O(q^{10}), \\ f_3 &= q^3 + q^4 - q^5 - q^6 - 2q^7 - 2q^8 + O(q^{10}). \end{aligned}$$

Thus $X_0(30)$ has genus 3. A genus 3 curve is either hyperelliptic or plane quartic. We want to know whether $X_0(30)$ is hyperelliptic or a plane quartic. We compute the image of the canonical embedding. If it is hyperelliptic, then the image must be a conic. Note that the basis f_1, f_2, f_2 is not necessarily the same as the basis dx/y, xdx/y, x^2dx/y for the hyperelliptic model, if $X_0(30)$ is indeed hyperelliptic; the two bases will be related by an invertible matrix. Thus if $X_0(30)$ is hyperelliptic then the image we obtain from f_1, f_2, f_3 will the result of some invertible linear transformation applied to the conic $u_1u_3 - u_2^2$, and so will be a conic.

The degree 2 monomials in f_1, f_2, f_3 are

$$\begin{aligned} f_1^2 &= q^2 - 2q^5 - 2q^7 - 3q^8 + 4q^{10} + O(q^{11}) \\ f_2^2 &= q^4 - 2q^6 - q^8 + O(q^{12}) \\ f_3^2 &= q^6 + 2q^7 - q^8 - 4q^9 - 5q^{10} - 6q^{11} + q^{12} + O(q^{13}) \\ f_1f_2 &= q^3 - q^5 - q^6 - q^7 - 3q^9 + 2q^{10} + O(q^{11}) \\ f_1f_3 &= q^4 + q^5 - q^6 - 2q^7 - 3q^8 - 2q^9 - 2q^{10} + O(q^{11}) \\ f_2f_3 &= q^5 + q^6 - 2q^7 - 2q^8 - 2q^9 - 2q^{10} + 2q^{11} + O(q^{12}). \end{aligned}$$

The image is a conic if and only if there is a non-trivial linear combination of these six expressions that is identically 0. Thus we are looking for $a_1, \dots, a_6$ (not all zero) such that

$$a_1f_1^2 + a_2f_2^2 + a_3f_3^2 + a_4f_1f_2 + a_5f_1f_3 + a_6f_2f_3 = 0.$$

Looking at the coefficient of q^2 we immediately see that $a_1 = 0$. And at the coefficient of q^3 that $a_4 = 0$. Moreover,

$$a_2 + a_5 = 0, \qquad a_5 + a_6 = 0, \qquad -2a_2 + a_3 - a_5 + a_6 = 0$$

from the coefficients of q^4, q^5, q^6. There is only one solution (up to scaling) which is

$$a_2 = 1, \quad a_3 = 0, \quad a_5 = -1, \quad a_6 = 1.$$

Thus $f_2^2 - f_1f_3 + f_2f_3 = 0 + O(q^7)$. In fact we can check that $f_2^2 - f_1f_3 + f_2f_3 = 0 + O(q^{100})$. But do we know that $f_2^2 - f_1f_3 + f_2f_3 = 0$ exactly? For this we need the Sturm bound.

THEOREM 45 (Sturm). *Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of index m. Let $f \in S_k(\Gamma)$ and suppose $\mathrm{ord}_q(f) > km/12$. Then $f = 0$.*

We let $f = f_2^2 - f_1 f_3 + f_2 f_3$. Since f_1, f_2, f_3 are cusp forms for $\Gamma_0(30)$ of weight 2, f is a cusp form of weight $k = 4$. Thus Recall the formula for the index of $\Gamma_0(N)$:

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} (1 + 1/p).$$

In our case $N = 30$ and

$$m = 30(1 + 1/2)(1 + 1/3)(1 + 1/5) = 72.$$

Note $km/12 = 4 \times 72/12 = 36$. Since $\mathrm{ord}_q(f) \geq 100$ we know from Sturm that $f = 0$. Hence $X_0(30)$ is hyperelliptic. We'll return to writing down equations for $X_0(30)$ later.

We repeat the computation for $X_0(45)$. A basis for $S_2(\Gamma_0(45))$ is

$$\begin{aligned} g_1 &= q - q^4 + O(q^{10}), \\ g_2 &= q^2 - q^5 - 3q^8 + O(q^{10}), \\ g_3 &= q^3 - q^6 - q^9 + O(q^{10}). \end{aligned}$$

Thus $X_0(45)$ has genus 3 and is either hyperelliptic or the canonical image has degree 4 and is therefore a plane quartic. Again we look for $a_1, \ldots, a_6$ such that

$$a_1 g_1^2 + a_2 g_2^2 + a_3 g_3^2 + a_4 g_1 g_2 + a_5 g_1 g_3 + a_6 g_2 g_3 = 0.$$

By solving the resulting system of linear equations from the coefficients of $q^2, \ldots, q^{10}$ we find that all the $a_i = 0$. Thus the image is not a conic, and so $X_0(45)$ is a plane quartic. Next we look at all monomials of degree 4 in g_1, g_2, g_3. There are 10 of these, and we are looking a for a linear combination which is 0. By solving the system resulting from the coefficients of lots of q^j up to q^{20} we find a unique solution (up to scaling). This unique solution gives us our degree 4 model:

$$X_0(45) \ : \ x_0^3 x_2 - x_0^2 x_1^2 + x_0 x_1 x_2^2 - x_1^3 x_2 - 5 x_2^4 \qquad \subset \mathbb{P}^2.$$

Did we need to check up to the Sturm bound? Not this time! We have already proved that $X_0(45)$ is not hyperelliptic. So we know that the canonical image is a quartic. We solved for this quartic and found only one solution, so that must be the correct quartic.

We return to $X_0(30)$. We've worked out that this is hyperelliptic and so has a model

$$y^2 = h(x), \qquad h = a_8 x^8 + \cdots + a_0.$$

This model is not unique. If (u, v) is any point on this model, we then we can change the model to move this point to infinity:

$$x' = \frac{1}{x - u}, \qquad y' = \frac{y}{(x - u)^4}.$$

The new model has the form

$$y'^2 = v^2 x'^8 + \cdots .$$

If $v = 0$ (i.e. the original point was a Weierstrass point) then we would end up with $y'^2 =$ degree 7 but otherwise it is $y'^2 =$ degree 8. Now the infinity cusp c_∞ is a point on $X_0(30)$. Let's move c_∞ to infinity on the hyperelliptic model. **Question: Do we obtain a degree 7 model or a degree 8 model?**

EXERCISE 46. (i) Let

$$X \ : \ y^2 = a_{2g+2}x^{2g+2} + \cdots + a_0$$

be a curve of genus g where $a_{2g+2} \neq 0$. Let ∞_+ be one of the two points at infinity. Show that

$$\mathrm{ord}_{\infty_+}\left(\frac{dx}{y}\right) = g-1, \quad \mathrm{ord}_{\infty_+}\left(\frac{xdx}{y}\right) = g-2, \ldots, \mathrm{ord}_{\infty_+}\left(\frac{x^{g-1}dx}{y}\right) = 0.$$

(ii) Let

$$X \ : \ y^2 = a_{2g+1}x^{2g+1} + \cdots + a_0$$

be a curve of genus g (here necessarily $a_{2g+1} \neq 0$ otherwise the genus would be smaller than g). Let ∞ be the unique point at infinity. Show that

$$\mathrm{ord}_{\infty}\left(\frac{dx}{y}\right) = 2(g-1), \quad \mathrm{ord}_{\infty}\left(\frac{xdx}{y}\right) = 2(g-2), \ldots, \mathrm{ord}_{\infty}\left(\frac{x^{g-1}dx}{y}\right) = 0.$$

We can now answer the question. We have the q-expansions of f_1, f_2, f_3. What you need to know is that q is a uniformizer at c_∞ (i.e. the order of vanishing of q at c_∞ is 1). From the q-expansions

$$\mathrm{ord}_{c_\infty}\left(f_1(q)\frac{dq}{q}\right) = 0, \qquad \mathrm{ord}_{c_\infty}\left(f_2(q)\frac{dq}{q}\right) = 1, \qquad \mathrm{ord}_{c_\infty}\left(f_3(q)\frac{dq}{q}\right) = 2.$$

Any regular differential has to be a linear combination of f_1dq/q, f_2dq/q, f_3dq/q. Thus there is no non-zero regular differential that has valuation 4 at c_∞. However, in the degree 7 model dx/y is a regular differential that has valuation 4. The answer to our question is that we obtain a degree 8 model. (In slightly technical language c_∞ is not a Weierstrass point.) Replacing y by $-y$ we can suppose that $c_\infty = \infty_+$. But

$$\mathrm{ord}_{\infty_+}\left(\frac{dx}{y}\right) = 2, \qquad \mathrm{ord}_{\infty_+}\left(x\frac{dx}{y}\right) = 1, \qquad \mathrm{ord}_{\infty_+}\left(x^2\frac{dx}{y}\right) = 0.$$

From the valuations

$$\begin{aligned}
\frac{dx}{y} &= \alpha_3 \cdot f_3(q)\frac{dq}{q}, \\
\frac{xdx}{y} &= \beta_2\frac{f_2(q)dq}{q} + \beta_3\frac{f_3(q)dq}{q}, \\
\frac{x^2dx}{y} &= \gamma_1\frac{f_1(q)dq}{q} + \gamma_2\frac{f_2(q)dq}{q} + \gamma_3\frac{f_3(q)dq}{q},
\end{aligned}$$

where α_3, β_2 and $\gamma_1 \neq 0$. The change of hyperelliptic model

$$x \mapsto rx, \qquad y \mapsto sy$$

keeps the points at infinity where they are but have the following effect on the differentials:

$$\frac{dx}{y} \mapsto (r/s)\frac{dx}{y}, \qquad \frac{xdx}{y} \mapsto (r^2/s)\frac{dx}{y}, \qquad \ldots$$

Thus we can make $\alpha_3 = 1$ and $\beta_2 = 1$. Moreover the change of model

$$x \mapsto x + t, \qquad y \mapsto y.$$

has the effect

$$\frac{dx}{y} \mapsto \frac{dx}{y}, \qquad \frac{xdx}{y} \mapsto \frac{xdx}{y} + t\frac{dx}{y}.$$

So we can suppose $\beta_3 = 0$. i.e.

$$\frac{dx}{y} = f_3(q)\frac{dq}{q}, \qquad \frac{xdx}{y} = f_2(q)\frac{dq}{q}.$$

Hence

$$x = f_2(q)/f_3(q) = \frac{1}{q} - 1 + q - q^2 + 2q^3 - 2q^4 + 2q^5 - 3q^6 + 5q^7 - 5q^8 + 5q^9 + \cdots .$$

$$y = \frac{dx}{dq} \cdot \frac{q}{f_3(q)} = -\frac{1}{q^4} + \frac{1}{q^3} - \frac{1}{q^2} - \frac{1}{q} + 5 - 15q + 29q^2 - 60q^3 + 118q^4 - 210q^5 + 346q^6 - 573q^7 + 929q^8 - 1454q^9 + \cdots .$$

Recall that we want a model of the form

$$y^2 = a_8x^8 + a_7x^7 + \cdots + a_0$$

where a_8 is non-zero. By comparing the coefficients of q^{-8} on both sides we see that $a_8 = 1$. Now

$$y^2 - x^8 = \frac{6}{q^7} - \frac{33}{q^6} + \cdots$$

so $a_7 = 6$. Also

$$y^2 - x^8 - 6x^7 = \frac{9}{q^6} - \frac{48}{q^5} + \cdots$$

so $a_6 = 9$. Continuing in this fashion we arrive at

$$y^2 - x^8 - 6x^7 - 9x^6 - 6x^5 + 4x^4 + 6x^3 - 9x^2 + 6x - 1 = O(q^{100}).$$

Therefore, a model for $X_0(30)$ is

$$X_0(30) \ : \ y^2 \ = \ x^8 + 6x^7 + 9x^6 + 6x^5 - 4x^4 - 6x^3 + 9x^2 - 6x + 1.$$

CHAPTER 9

Some Open Problems

There are deep and difficult open problems such as determination of the rational points on $X_{ns}^{+}(p)$. However, here we mention open problems that might be easier. Historically $X_0(p)$ and $X_1(p)$ have received much more attention than other modular curves.

1. Mazur's Vertical Uniformity Problem

Given an elliptic curve $E/\mathbb{Q}$, we can for each prime p construct a family of representations

$$\overline{\rho}_{E,p^r} \ : \ G_{\mathbb{Q}} \to \mathrm{GL}(E[p^r]) \cong \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}).$$

The Tate module $T_p(E)$ is defined as the inverse limit

$$T_p(E) \ := \ \lim_{\leftarrow} E[p^r] \ \cong \ \mathbb{Z}_p^2.$$

Putting all the $\overline{\rho}_{E,p^r}$ together we obtain a representation

$$\rho_{E,p} \ : \ G_{\mathbb{Q}} \to \mathrm{GL}(T_p(E)) \cong \mathrm{GL}_2(\mathbb{Z}_p).$$

The following question is due to Mazur, and known as the **Vertical Uniformity Problem**.

Problem: Determine all possible $\rho_{E,p}(G_{\mathbb{Q}})$ as E ranges over all elliptic curve $E/\mathbb{Q}$ without CM, and p over all primes.

This was in fact solved by Rouse and Zureick-Brown [**20**] for $p = 2$, who found a total of 1208 possibilities for $\rho_{E,2}(G_{\mathbb{Q}})$. This involved the study of rational points on 727 modular curves. However the question is still open for all other values of p. If one accepts Serre's Uniformity Conjecture then one needs to solve Mazur's Vertical Uniformity Problem for $3 \leq p \leq 37$.

2. Torsion on Modular Jacobians

Write $C_0(H)$ be the subgroup of $J_H(\overline{\mathbb{Q}})$ generated by classes of differences of cusps. Let $C_0(H)(\mathbb{Q}) := C_0(H) \cap J_H(\overline{\mathbb{Q}})$. The group $C_0(H)$ is known as the **cuspidal subgroup**, and $C_0(H)(\mathbb{Q})$ as the **rational cuspidal subgroup**. For the following theorem see [**15**], [**8**], [**9**].

THEOREM 47 (Manin–Drinfel'd). *$C_0(H) \subset J_H(\overline{\mathbb{Q}})_{\mathrm{tors}}$, and $C_0(H)(\mathbb{Q}) \subset J_H(\mathbb{Q})_{\mathrm{tors}}$.*

Mazur's Theorem 42 says that the rational cuspidal subgroup is equal to the torsion subgroup for $J_0(p)$ (p prime). We do not know if this is necessarily true for other families of modular curves.

CONJECTURE (Generalized Ogg Conjecture). *Write $C_0(N)(\mathbb{Q})$ for the rational cuspidal subgroup of $J_0(N)$. Then $J_0(N)(\mathbb{Q})_{\mathrm{tors}} = C_0(N)(\mathbb{Q})$.*

This is called the "generalized Ogg conjecture" because Theorem 42 for $J_0(p)$ was a conjecture of Ogg before it was proved by Mazur. As far as I can see there is not a lot of evidence for the generalized Ogg conjecture, and it might be worth searching for counterexamples!

More generally, it would be interesting to have some results on the torsion subgroups for $J_1(p)$, $J_{\mathrm{ns}}^+(p)$, $J_{\mathrm{s}}^+(p)$, $J_{A_4}(p)$, $J_{S_4}(p)$, $J_{A_5}(p)$, ...

3. Chen's Isogeny

Chen has shown that

$$J_{ns}^+(p) \sim (J_0(p^2)/w_{p^2})^{\mathrm{new}}, \qquad J_s^+(p) \sim J_0(p) \times (J_0(p^2)/w_{p^2})^{\mathrm{new}}.$$

It would be interesting to know the degrees of these isogenies. Are there analogous isogenies for $J_{A_4}(p)$, $J_{S_4}(p)$, $J_{A_5}(p)$?

Bibliography

[1] W. Bosma, J. Cannon and C. Playoust, The Magma Algebra System I: The User Language, *J. Symb. Comp.* **24** (1997), 235–265. (See also `http://magma.maths.usyd.edu.au/magma/`)

[2] P. Bruin and F. Najman, *Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields*, LMS J. Comput. Math. **18** (2015), no. 1, 578–602. 41

[3] G. Cornell and J. H. Silverman (editors), *Arithmetic Geometry*, Springer-Verlag, 1986.

[4] G. Cornell, J. H. Silverman and G. Stevens (editors), *Modular Forms and Fermat's Last Theorem*, Springer-Verlag, 1997.

[5] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992. 6

[6] M. Derickx, *Torsion points on elliptic curves over number fields of small degree*, PhD thesis, Leiden University, 2016.

[7] F. Diamond and J. Shurman, *A First Course on Modular Forms*, GTM **228**, Springer, 2005. 1

[8] V. G. Drinfel'd, *Two theorems on modular curves* (Russian), Funkcional. Anal. i Priložen. 7 (1973), no. 2, 83–84. 2

[9] R. Elkik, *Le théorème de Manin-Drinfel'd*, Astérisque **183** (1990), 59–67. 2

[10] S. D. Galbraith, *Equations for Modular Curves*, DPhil thesis, University of Oxford, 1996. 8

[11] F. Hess, *Computing Riemann–Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445.

[12] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math., **109** (1992), no. 2 221-229

[13] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502. 5

[14] V. A. Kolyvagin and D. Yu. Logachëv, *Finiteness of the Shafarevich–Tate group and the group of rational points for some modular abelian varieties* (Russian), Algebra i Analiz **1** (1989), no. 5, 171–196; translation in Leningrad Math. J. **1** (1990), no. 5, 1229–1253.

[15] Ju. I. Manin, *Parabolic points and zeta functions of modular curves* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66. 2

[16] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. No. **47** (1977), 33–186.

[17] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), no. 2, 129–162.

[18] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math.**124** (1996), no. 1-3, 437–449.

[19] B. Poonen and E. F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. 4

[20]

[21] J. Rouse and D. Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Research in Number Theory, Volume 1, Issue 1, 2015. 1

[22] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer, 1986. 2, 3

[23] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer, 1994. 7

[24] W. A. Stein, *Explicit approaches to modular abelian varieties*, University of California at Berkeley PhD thesis, 2000.

[25] W. A. Stein, *Modular Forms: A Computational Approach*, American Mathematical Society, 2007. 40

[26] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), 245–277.