1.4 Points on modular curves parameterize elliptic curves with extra structure

The classical theory of the Weierstass $\wp$-function sets up a bijection between isomorphism classes of elliptic curves over $\mathbf{C}$ and isomorphism classes of one-dimensional complex tori $\mathbf{C}/\Lambda$. Here Λ is a lattice in $\mathbf{C}$, i.e., a free abelian group $\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ of rank 2 such that $\mathbf{R}\omega_1 + \mathbf{R}\omega_2 = \mathbf{C}$.

Any homomorphism φ of complex tori $\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ is determined by a $\mathbf{C}$-linear map $T : \mathbf{C} \to \mathbf{C}$ that sends Λ_1 into Λ_2.

Lemma 1.4.1. *Suppose $\varphi : \mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ is nonzero. Then the kernel of φ is isomorphic to $\Lambda_2/T(\Lambda_1)$.*

Lemma 1.4.2. *Two complex tori $\mathbf{C}/\Lambda_1$ and $\mathbf{C}/\Lambda_2$ are isomorphic if and only if there is a complex number α such that $\alpha\Lambda_1 = \Lambda_2$.*

Proof. Any $\mathbf{C}$-linear map $\mathbf{C} \to \mathbf{C}$ is multiplication by a scalar $\alpha \in \mathbf{C}$. □

Suppose $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ is a lattice in $\mathbf{C}$, and let $\tau = \omega_1/\omega_2$. Then $\Lambda_\tau = \mathbf{Z}\tau + \mathbf{Z}$ defines an elliptic curve that is isomorphic to the elliptic curve determined by Λ. By replacing ω_1 by $-\omega_1$, if necessary, we may assume that $\tau \in \mathfrak{h}$. Thus every elliptic curve is of the form $E_\tau = \mathbf{C}/\Lambda_\tau$ for some $\tau \in \mathfrak{h}$ and each $\tau \in \mathfrak{h}$ determines an elliptic curve.

Proposition 1.4.3. *Suppose $\tau, \tau' \in \mathfrak{h}$. Then $E_\tau \cong E_{\tau'}$ if and only if there exists $g \in \mathrm{SL}_2(\mathbf{Z})$ such that $\tau = g(\tau')$. Thus the set of isomorphism classes of elliptic curves over $\mathbf{C}$ is in natural bijection with the orbit space $\mathrm{SL}_2(\mathbf{Z})\backslash\mathfrak{h}$.*

Proof. Suppose $E_\tau \cong E_{\tau'}$. Then there exists $\alpha \in \mathbf{C}$ such that $\alpha\Lambda_\tau = \Lambda_{\tau'}$, so $\alpha\tau = a\tau' + b$ and $\alpha 1 = c\tau' + d$ for some $a, b, c, d \in \mathbf{Z}$. The matrix $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has determinant ± 1 since $a\tau' + b$ and $c\tau' + d$ form a basis for $\mathbf{Z}\tau + \mathbf{Z}$; this determinant is positive because $g(\tau') = \tau$ and $\tau, \tau' \in \mathfrak{h}$. Thus $\det(g) = 1$, so $g \in \mathrm{SL}_2(\mathbf{Z})$.

Conversely, suppose $\tau, \tau' \in \mathfrak{h}$ and $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ is such that

$$\tau = g(\tau') = \frac{a\tau' + b}{c\tau' + d}.$$

Let $\alpha = c\tau' + d$, so $\alpha\tau = a\tau' + b$. Since $\det(g) = 1$, the scalar α defines an isomorphism from Λ_τ to $\Lambda_{\tau'}$, so $E_\tau \cong E'_\tau$, as claimed. □

Let $E = \mathbf{C}/\Lambda$ be an elliptic curve over $\mathbf{C}$ and N a positive integer. Using Lemma 2.4.1, we see that

$$E[N] := \{x \in E \,:\, Nx = 0\} \cong \left(\frac{1}{N}\Lambda\right)/\Lambda \cong (\mathbf{Z}/N\mathbf{Z})^2.$$

If $\Lambda = \Lambda_\tau = \mathbf{Z}\tau + \mathbf{Z}$, this means that τ/N and $1/N$ are a basis for $E[N]$.

Suppose $\tau \in \mathfrak{h}$ and recall that $E_\tau = \mathbf{C}/\Lambda_\tau = \mathbf{C}/(\mathbf{Z}\tau + \mathbf{Z})$. To τ, we associate three "level N structures". First, let C_τ be the subgroup of E_τ generated by $1/N$. Second, let P_τ be the point of order N in E_τ defined by $1/N \in \Lambda_\tau$. Third, let Q_τ be the point of order N in E_τ defined by τ/N, and consider the basis (P_τ, Q_τ) for $E[N]$.

In order to describe the third level structure, we introduce the *Weil pairing*

$$e : E[N] \times E[N] \to \mathbf{Z}/N\mathbf{Z}$$

as follows. If $E = \mathbf{C}/(\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2)$ with $\omega_1/\omega_2 \in \mathfrak{h}$, and $P = a\omega_1/N + b\omega_2/N$, $Q = c\omega_1/N + d\omega_2/N$, then

$$e(P, Q) = ad - bc \in \mathbf{Z}/N\mathbf{Z}.$$

Notice that $e(P_\tau, Q_\tau) = -1 \in \mathbf{Z}/N\mathbf{Z}$. Also if $\mathbf{C}/\Lambda \cong \mathbf{C}/\Lambda'$ via multiplication by α, and $P, Q \in (\mathbf{C}/\Lambda)[N]$, then $e(\alpha(P), \alpha(Q)) = e(P, Q)$.

Theorem 1.4.4. *Let N be a positive integer.*

1. *The non-cuspidal points on $X_0(N)$ correspond to isomorphism classes of pairs (E, C) where C is a cyclic subgroup of E of order N. (Two pairs (E, C), (E', C') are isomorphic if there is an isomorphism $\varphi : E \to E'$ such that $\varphi(C) = C'$.)*

2. *The non-cuspidal points on $X_1(N)$ correspond to pairs (E, P) where P is a point on E of exact order N. (Two pairs (E, P) and (E', P') isomorphic if there is an isomorphism $\varphi : E \to E'$ such that $\varphi(P) = P'$.)*

3. *The non-cuspidal points on $X(N)$ correspond to triples (E, P, Q) where P, Q are a basis for $E[N]$ such that $e(P, Q) = -1 \in \mathbf{Z}/N\mathbf{Z}$. (Triples (E, P, Q) and (E, P', Q') are isomorphic if there is an isomorphism $\varphi : E \to E'$ such that $\varphi(P) = P'$ and $\varphi(Q) = Q'$.)*

This theorem follows from Propositions 2.4.5 and 2.4.7 below.

Proposition 1.4.5. *Let E be an elliptic curve over $\mathbf{C}$. If C is a cyclic subgroup of E of order N, then there exists $\tau \in \mathfrak{h}$ such that (E, C) is isomorphic to (E_τ, C_τ). If P is a point on E of order N, then there exists $\tau \in \mathbf{C}$ such that (E, P) is isomorphic to (E_τ, P_τ). If P, Q is a basis for $E[N]$ and $e(P, Q) = -1 \in \mathbf{Z}/N\mathbf{Z}$, then there exists $\tau \in \mathbf{C}$ such that (E, P, Q) is isomorphic to (E_τ, P_τ, Q_τ).*

Proof. Write $E = \mathbf{C}/\Lambda$ with $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ and $\omega_1/\omega_2 \in \mathfrak{h}$.

Suppose $P = a\omega_1/N + b\omega_2/N$ is a point of order N. Then $\gcd(a, b, N) = 1$, otherwise P would have order strictly less than N, a contradiction. Thus we can modify a and b by adding multiples of N to them (this follows from the fact that $\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ is surjective), so that $P = a\omega_1/N + b\omega_2/N$ and $\gcd(a, b) = 1$. There exists $c, d \in \mathbf{Z}$ such that $ad - bc = 1$, so $\omega_1' = a\omega_1 + b\omega_2$ and $\omega_2' = c\omega_1 + d\omega_2$ form a basis for Λ, and C is generated by $P = \omega_1'/N$. If necessary, replace ω_2' by $-\omega_2'$ so that $\tau = \omega_2'/\omega_1' \in \mathfrak{h}$. Then (E, P) is isomorphic to (E_τ, P_τ). Also, if C is the subgroup generated by P, then (E, C) is isomorphic to (E_τ, C_τ).

Suppose $P = a\omega_1/N + b\omega_2/N$ and $Q = c\omega_1/N + d\omega_2/N$ are a basis for $E[N]$ with $e(P, Q) = -1$. Then the matrix $\left(\begin{smallmatrix} a & b \\ -c & -d \end{smallmatrix}\right)$ has determinant 1 modulo N, so because the map $\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ is surjective, we can replace a, b, c, d by integers which are equivalent to them modulo N (so P and Q are unchanged) and so that $ad - bc = -1$. Thus $\omega_1' = a\omega_1 + b\omega_2$ and $\omega_2' = c\omega_1 + d\omega_2$ form a basis for Λ. Let

$$\tau = \omega_2'/\omega_1' = \frac{c\frac{\omega_1}{\omega_2} + d}{a\frac{\omega_1}{\omega_2} + b}.$$

Then $\tau \in \mathfrak{h}$ since $\omega_1/\omega_2 \in \mathfrak{h}$ and $\left(\begin{smallmatrix} c & d \\ a & b \end{smallmatrix}\right)$ has determinant $+1$. Finally, division by ω_1' defines an isomorphism $E \to E_\tau$ that sends P to $1/N$ and Q to τ/N. $\square$

Remark 1.4.6. Part 3 of Theorem 2.4 in Chapter 11 of Husemöller's book on elliptic curves is **wrong**, since he neglects the Weil pairing condition. Also the first paragraph of his proof of the theorem is incomplete.

The following proposition completes the proof of Theorem 2.4.4.

Proposition 1.4.7. *Suppose $\tau, \tau' \in \mathfrak{h}$. Then (E_τ, C_τ) is isomorphic $(E_{\tau'}, C_{\tau'})$ if and only if there exists $g \in \Gamma_0(N)$ such that $g(\tau) = \tau'$. Also, (E_τ, P_τ) is isomorphic $(E_{\tau'}, P_{\tau'})$ if and only if there exists $g \in \Gamma_1(N)$ such that $g(\tau) = \tau'$. Finally, (E_τ, P_τ, Q_τ) is isomorphic $(E_{\tau'}, P_{\tau'}, Q_{\tau'})$ if and only if there exists $g \in \Gamma(N)$ such that $g(\tau) = \tau'$.*

Proof. We prove only the first assertion, since the others are proved in a similar way. Suppose (E_τ, C_τ) is isomorphic to (E'_τ, C'_τ). Then there is $\lambda \in \mathbf{C}$ such that $\lambda\Lambda_\tau = \Lambda_{\tau'}$. Thus $\lambda\tau = a\tau' + b$ and $\lambda 1 = c\tau' + d$ with $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ (as we saw in the proof of Proposition 2.4.3). Dividing the second equation by N we get $\lambda\frac{1}{N} = \frac{c}{N}\tau' + \frac{d}{N}$, which lies in $\Lambda_{\tau'} = \mathbf{Z}\tau' + \frac{1}{N}\mathbf{Z}$, by hypothesis. Thus $c \equiv 0 \pmod{N}$, so $g \in \Gamma_0(N)$, as claimed. For the converse, note that if $N \mid c$, then $\frac{c}{N}\tau' + \frac{d}{N} \in \Lambda_{\tau'}$. $\square$

1.5 The Genus of $X(N)$

Let N be a positive integer. The aim of this section is to establish some facts about modular curves associated to congruence subgroups and compute the genus of $X(N)$. Similar methods can be used to compute the genus of $X_0(N)$ and $X_1(N)$ (for $X_0(N)$ see [3, §1.6] and for $X_1(N)$ see [1, §9.1]).

The groups $\Gamma_0(1)$, $\Gamma_1(1)$, and $\Gamma(1)$ are all equal to $\mathrm{SL}_2(\mathbf{Z})$, so $X_0(1) = X_1(1) = X(1) = \mathbf{P}^1$. Since $\mathbf{P}^1$ has genus 0, we know the genus for each of these three cases. For general N we obtain the genus by determining the ramification of the corresponding cover of $\mathbf{P}^1$ and applying the Hurwitz formula, which we assume the reader is familiar with, but which we now recall.

Suppose $f : X \to Y$ is a surjective morphism of Riemann surfaces of degree d. For each point $x \in X$, let e_x be the ramification exponent at x, so $e_x = 1$ precisely when f is unramified at x, which is the case for all but finitely many x. (There is a point over $y \in Y$ that is ramified if and only if the cardinality of $f^{-1}(y)$ is less than the degree of f.) Let $g(X)$ and $g(Y)$ denote the genera of X and Y, respectively.

Theorem 1.5.1 (Hurwitz Formula). *Let $f : X \to Y$ be as above. Then*

$$2g(X) - 2 = d(2g(Y) - 2) + \sum_{x \in X} (e_x - 1).$$

If $X \to Y$ is Galois, so the e_x in the fiber over each fixed $y \in Y$ are all equal, then this formula becomes

$$2g(X) - 2 = d\left(2g(Y) - 2 + \sum_{y \in Y}\left(1 - \frac{1}{e_y}\right)\right).$$

Let X be one of the modular curves $X_0(N)$, $X_1(N)$, or $X(N)$ corresponding to a congruence subgroup Γ, and let $Y = X(1) = \mathbf{P}^1$. There is a natural map $f : X \to Y$ got by sending the equivalence class of τ modulo the congruence subgroup Γ to the equivalence class of τ modulo $\mathrm{SL}_2(\mathbf{Z})$. This is "the" map $X \to \mathbf{P}^1$ that we mean everywhere below.

Because $\mathrm{PSL}_2(\mathbf{Z})$ acts faithfully on $\mathfrak{h}$, the degree of f is the index in $\mathrm{PSL}_2(\mathbf{Z})$ of the image of Γ in $\mathrm{PSL}_2(\mathbf{Z})$ (see Exercise X). Using that the map $\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ is surjective, we can compute these indices (Exercise X), and obtain the following lemma:

Proposition 1.5.2. *Suppose $N > 2$. The degree of the map $X_0(N) \to \mathbf{P}^1$ is $N\prod_{p|N}(1 + 1/p)$. The degree of the map $X_1(N) \to \mathbf{P}^1$ is $\frac{1}{2}N^2\prod_{p|N}(1 - 1/p^2)$. The degree of the map from $X(N) \to \mathbf{P}^1$ is $\frac{1}{2}N^3\prod_{p|N}(1 - 1/p^2)$. If $N = 2$, then the degrees are 3, 3, and 6, respectively.*

Proof. This follows from the discussion above, Exercise X about indices of congruence subgroups in $\mathrm{SL}_2(\mathbf{Z})$, and the observation that for $N > 2$ the groups $\Gamma(N)$ and $\Gamma_1(N)$ do not contain -1 and the group $\Gamma_0(N)$ does. □

Proposition 1.5.3. *Let X be $X_0(N)$, $X_1(N)$ or $X(N)$. Then the map $X \to \mathbf{P}^1$ is ramified at most over ∞ and the two points corresponding to elliptic curves with extra automorphisms (i.e., the two elliptic curves with j-invariants 0 and 1728).*

Proof. Since we have a tower $X(N) \to X_1(N) \to X_0(N) \to \mathbf{P}^1$, it suffices to prove the assertion for $X = X(N)$. Since we do not claim that there is no ramification over ∞, we may restrict to $Y(N)$. By Theorem 2.4.4, the points on $Y(N)$ correspond to isomorphism classes of triples (E, P, Q), where E is an elliptic curve over $\mathbf{C}$ and P, Q are a basis for $E[N]$. The map from $Y(N)$ to $\mathbf{P}^1$ sends the isomorphism class of (E, P, Q) to the isomorphism class of E. The equivalence class of (E, P, Q) also contains $(E, -P, -Q)$, since $-1 : E \to E$ is an isomorphism. The only way the fiber over E can have cardinality smaller than the degree is if there is an extra equivalence $(E, P, Q) \to (E, \varphi(P), \varphi(Q))$ with φ an automorphism of E not equal to ± 1. The theory of CM elliptic curves shows that there are only two isomorphism classes of elliptic curves E with automorphisms other than ± 1, and these are the ones with j-invariant 0 and 1728. This proves the proposition. □

Theorem 1.5.4. *For $N > 2$, the genus of $X(N)$ is*

$$g(X(N)) = 1 + \frac{N^2(N-6)}{24}\prod_{p|N}\left(1 - \frac{1}{p^2}\right).$$

For $N = 1, 2$, the genus is 0.

Thus if $g_N = g(X(N))$, then $g_1 = g_2 = g_3 = g_4 = g_5 = 0$, $g_6 = 1$, $g_7 = 3$, $g_8 = 5$, $g_9 = 10$, $g_{389} = 2414816$, and $g_{2003} = 333832500$.

Proof. Since $X(N)$ is a Galois covering of $X(1) = \mathbf{P}^1$, the ramification indices e_x are all the same for x over a fixed point $y \in \mathbf{P}^1$; we denote this common index by e_y. The fiber over the curve with j-invariant 0 has size one-third of the degree, since the automorphism group of the elliptic curve with j-invariant 0 has order 6, so the group of automorphisms modulo ± 1 has order three, hence $e_0 = 3$. Similarly, the fiber over the curve with j-invariant 1728 has size half the degree, since the automorphism group of the elliptic curve with j-invariant 1728 is cyclic of order 4, so $e_{1728} = 2$.

To compute the ramification degree e_∞ we use the orbit stabilizer theorem. The fiber of $X(N) \to X(1)$ over ∞ is exactly the set of $\Gamma(N)$ equivalence classes of cusps, which is $\Gamma(N)\infty, \Gamma(N)g_2\infty, \ldots, \Gamma(N)g_r\infty$, where $g_1 = 1, g_2, \ldots, g_r$ are coset representatives for $\Gamma(N)$ in $\mathrm{SL}_2(\mathbf{Z})$. By the orbit-stabilizer theorem, the number of cusps equals $\#(\Gamma(1)/\Gamma(N))/\#S$, where S is the stabilizer of $\Gamma(N)\infty$ in $\Gamma(1)/\Gamma(N) \cong \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. Thus S is the subgroup $\{\pm\left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right) : 0 \leq n < N-1\}$, which has order $2N$. Since the degree of $X(N) \to X(1)$ equals $\#(\Gamma(1)/\Gamma(N))/2$, the number of cusps is the degree divided by N. Thus $e_\infty = N$.

The Hurwitz formula for $X(N) \to X(1)$ with $e_0 = 3$, $e_{1728} = 2$, and $e_\infty = N$, is

$$2g(X(N)) - 2 = d\left(0 - 2 + \left(1 - \frac{1}{3} + 1 - \frac{1}{2} + 1 - \frac{1}{N}\right)\right),$$

where d is the degree of $X(N) \to X(1)$. Solving for $g(X(N))$ we obtain

$$2g(X) - 2 = d\left(1 - \frac{5}{6} - \frac{1}{N}\right) = d\left(\frac{N-6}{6N}\right),$$

so

$$g(X) = 1 + \frac{d}{2}\left(\frac{N-6}{6N}\right) = \frac{d}{12N}(N-6) + 1.$$

Substituting the formula for d from Proposition 2.5.2 yields the claimed formula. $\square$

References

[1] F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem, Providence, RI, 1995, pp. 39–133.

[2] J-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.

[3] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.