The Modular Curve $X_0(N)$

Lloyd Elliott

In previous discussions, it was shown that $X_0(1)$ is analytically isomorphic to $\mathbb{H}/SL_2(\mathbb{Z})$. Here, $X_0(1)$ is the set of isomorphism classes of elliptic curves over $\mathbb{C}$, and $\mathbb{H}$ is the upper half plane, and a matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ acts on $\tau \in \mathbb{H}$ by $A\tau = \frac{a\tau+b}{c\tau+d}$. This analytic isomorphism is given by $\Psi E = \tau$, where $E \simeq [1,\tau] = \{\alpha + \beta\tau : \alpha, \beta \in \mathbb{Z}\}$. In previous discussions, it was shown that every elliptic curves over $\mathbb{C}$ is isomorphic to a unique curve of the form $[1,\tau]$, and that $[1,\tau] = [1, A\tau]$ for all $A \in SL_2(\mathbb{Z})$. So, Ψ is well defined, and bijective. This fully descibes isomorphism classes of elliptic curves. In order to extend this description to isogenies from one elliptic curve to another, it suffices to look at pairs (E, C), where E is an elliptic curve, and C is a cyclic subgroup of order N. For, non trivial isogenies have finite kernels [Silverman, III.4.9]. Thus, the kernel is finitely generated, and can be expressed as a direct sum of cyclic groups. So, the problem of classifying all isogenies between elliptic curves reduces to the problem of classifying elliptic curves and cyclic subgroups of every order. Let $X_0(N)$ be isomorphism classes of pairs of elliptic curves and cyclic subgroups of order N.

Theorem 1. *Every isomorphism class in $X_0(N)$ contains a pair of the form (E, C) with $E = [1,\tau]$ and $C = [\frac{1}{N}, \tau]$.*

Proof. Say $E \simeq [\alpha, \beta]$. Then, C is cyclic, so there is a point $\delta \in E$ such that $C \simeq \mathbb{Z}$-span$\{\delta\}$ in E. So, $N\delta \in E$. Consider the line in $\mathbb{H}$ connecting δ to the origin. Let x be the point of $[\alpha, \beta]$ with smallest non zero magnitude on this line (x exists, as C is finite). Then, $\frac{x}{N}$ generates C. For, if $M\delta$ is any element of C, then by subtracting x an appropriate number of times, $M\delta$ is equivalent to tx, where $0 \leq t < 1$. Then, $NM\delta \in E$, so $Ntx \in E$. Thus, $tx = \frac{A}{N}$ for some $0 \leq A < N$. Thus, $[\alpha, \beta]$ is isomorphic to $\frac{1}{Nx}[\alpha, \beta]$, and $1 \in \frac{1}{Nx}[\alpha, \beta]$ is the smallest non negative real number in $\frac{1}{Nx}[\alpha, \beta]$. Also, this multiplication sends $\mathbb{Z}$-span$\{\delta\}$ to $\mathbb{Z}$-span$\{\frac{1}{N}\}$. By previous discussions, if $1 \in [\alpha, \beta]$, then there is a $\tau \in \mathbb{H}$ such that $[\alpha, \beta]$ is isomorphic to $[1, \tau]$. So, (E, C) is isomorphic to $([1, \tau], [\frac{1}{N}, \tau])$. $\square$

There is a map from $\pi_N \colon X_0(1) \to X_0(N)$, given by forgetting about the additional information provided by C. This map is well defined, for if (E_1, C^1) and (E_2, C^2) are two pairs of elliptic curves and cyclic subgroups of order N, then they are in the same equivalence class if and only if there is an isomorphism $\phi\colon E_1 \to E_2$ such that $\phi C^1 = C^2$. So, E_1 is isomorphic to E_2, and thus $\pi_N(E_1, C^1) = E_1 = E_2 = \pi_N(E_2, C^2)$ in $X_0(1)$. Also, this map is surjective, for if an elliptic curve $E \in X_0(1)$ is given, E is isomorphic to an elliptic curve of the form $[1, \tau]$, and thus $\pi_N([1, \tau], [\frac{1}{N}, \tau]) = E$.

Define $\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : c \equiv 0(\text{mod } m)\}$. It will be shown that $\mathbb{H}/\Gamma_0(N) \simeq X_0(N)$. The set $\Gamma_0(N)$ is a subgroup of $SL(\mathbb{Z})$. Consider $\mathbb{H}/SL_2(\mathbb{Z})$ as orbits of $SL_2(\mathbb{Z})$ acting on $\mathbb{H}$. Then, for every $\tau \in \mathbb{H}$, and for every coset $\Gamma_0(N)A$ of $\Gamma_0(N)$, $\Gamma_0(N)A\tau$ is a subset of $SL_2(\mathbb{Z})\tau$. So, there is a map $q\colon \mathbb{H}/\Gamma_0(\mathbb{Z}) \to \mathbb{H}/SL_2(\mathbb{Z})$, by sending $\Gamma_0(N)\tau$ to $SL_2(\mathbb{Z})\tau$. By the orbit stabiliser theorem, this is a $[SL_2(\mathbb{Z}) : \Gamma_0(N)]$ to one covering of $\mathbb{H}/SL_2(\mathbb{Z})$.

Theorem 2. *The function $j(\tau)$ is invariant under the action of $SL_2(\mathbb{Z})$. Also, $j(\tau)$ and $j(N\tau)$ are invariant under the action of $\Gamma_0(N)$.*

Proof. If $\sigma \in SL_2(\mathbb{Z})$, then $j(\tau) = \frac{1728 g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2}$, and because g_2, g_3 are modular functions of weight 2 and 3 respectively, $j(\sigma\tau) = j(\tau)$. Also, $\Gamma_0(N) \subset SL_2(\mathbb{Z})$, so $j(\tau)$ is clearly $\Gamma_0(N)$ invariant. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, and $\gamma' = \left(\begin{smallmatrix} a & Nb \\ \frac{c}{N} & d \end{smallmatrix}\right)$, then $j(N\gamma\tau) = j(\gamma' N\tau) = j(N\tau)$. So, $j(N\tau)$ is $\Gamma_0(N)$ invariant. □

If $\gamma \in \Gamma_0(N)$, and (E, C) is an elliptic curve along with a cyclic subgroup of order N, then the pair is isomorphic to $([1, \tau], [\frac{1}{N}, \tau])$ for some $\tau \in \mathbb{H}$. Also, $(\gamma E, \gamma C)$ is isomorphic to $([1, \gamma\tau], [\frac{1}{N}, \gamma\tau])$. But, $[\frac{1}{N}, \tau]$ is isomorphc to $N[\frac{1}{N}, \tau]$, so $[\frac{1}{N}, \gamma\tau]$ is isomorphic to $[1, \gamma N\tau]$. So, by the above theorem, the j invariant of $[1, \tau]$ is the same as that of $[1, \gamma\tau]$, and that of $[\frac{1}{N}, \tau]$ is the same as that of $[\frac{1}{N}, \gamma\tau]$. Thus, $X_0(N)$ is invariant under the action of $\Gamma_0(N)$.

Thus, the map $\omega\colon X_0(N) \to \mathbb{H}/\Gamma_0(N)$ that sends (E, C) to τ, where (E, C) is isomorphic to $([1, \tau], [\frac{1}{N}, \tau])$, is well defined.

This information can be summarised by the following diagram. Later, it will be shown that this diagram commutes, and that the horizontal arrows are analytic isomorphisms:

$$\begin{tikzcd}
X_0(N) \arrow[r, "\omega"] \arrow[d, "\pi_N"'] & \mathbb{H}/\Gamma_0(N) \arrow[d, "q"'] \\
X_0(1) \arrow[r, "\psi"] & \mathbb{H}/SL_2(\mathbb{Z})
\end{tikzcd}$$

Consider the set $C(N) = \{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) : \gcd(a,b,d) = 1, |ad| = N, 0 < a, 0 \leq b < d \}$.

Theorem 3. *There is a bijection between cosets of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$, and elements of $C(N)$.*

Proof. Let $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in C(N)$ and $\sigma_0 = \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right) \in C(N)$. It will be shown that the set $\sigma_0^{-1} SL_2(\mathbb{Z}) \sigma \cap SL_2(\mathbb{Z})$ is a coset of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$. Elements in this set are of the form $\left(\begin{smallmatrix} \frac{a'a}{N} & \frac{a^{P}rimeb+b'd}{N} \\ c'a & c'b+d'd \end{smallmatrix}\right)$ where $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Clearly, every such matrix has determinant 1, for determinant is multiplicative. So, to deminstrate that there is an element in this set, it is enough to find $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$ such that $\frac{a'a}{N}$ and $\frac{a'b+b'd}{N}$ integers, and a', b' coprime. For, then c', d' can be chosen so that $a'd' - b'c' = 1$, and thus, the matrix product is in $SL_2(\mathbb{Z})$.

Say $x = \frac{a'a}{N} = 1$, so $a' = d$, and $g = (a,b)$. Then, $\frac{a'b+b'd}{N} = \frac{xb+b'}{a}$. For this to be an integer, a must divide $b + b'$ so write $ka = b + b'$. But, $(\frac{a}{g}, \frac{b}{g}) = 1$, so by Dirichlet's theorem on primes in arithmetic progressions, there exists an integer k such that $\frac{b'}{g} = k\frac{a}{g} - \frac{b}{g}$ is a prime greater than d. Then, $\frac{b+b'}{a} = k$, an integer. Also, $\frac{a'a}{N} = 1$ is an integer. Finally, $(a', b') = (d, ka - b) = 1$. For, assume $h > 0$ and $h|d$ and $h|ka - b = g\frac{ka-b}{g}$. Then, $\frac{ka-b}{g}$ is a prime greater than d, and $h < d$ so $h \not| \frac{ka-b}{g}$. Thus, $h|g$ and $h|d$ implies $h = 1$, for $(a,b,d) = 1$ implies $(g,d) = 1$. This demonstrates the existance of an element $X \in \sigma_0^{-1} SL_2(\mathbb{Z}) \sigma \cap SL_2(\mathbb{Z})$.

Consider the set $\sigma_0^{-1} SL_2(\mathbb{Z}) \sigma_0 \cap SL_2(\mathbb{Z})$. This set is $\{ \left(\begin{smallmatrix} a' & Nb' \\ \frac{c'}{N} & d' \end{smallmatrix}\right) : \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \} \cap SL_2(\mathbb{Z}) = \{ \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : N|c' \} = \Gamma_0(N)$. So, for any element $\sigma \in C(N)$, choose X as above, then there is an element $Z \in SL_2(\mathbb{Z})$ such that $\sigma_0^{-1} Z \sigma = X$. So, $\Gamma_0 X = \sigma_0^{-1} SL_2(\mathbb{Z}) \sigma_0 Z \sigma \cap SL_2(\mathbb{Z}) = \sigma_0^{-1} SL_2(\mathbb{Z}) Z \sigma_0 \sigma \cap SL_2(\mathbb{Z})$. Thus, for every element $\sigma \in C(N)$, $\sigma_0^{-1} SL_2(\mathbb{Z}) \sigma \cap SL_2(\mathbb{Z})$ is a coset of Γ_0 in $SL_2(\mathbb{Z})$.

If $X = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, then there is a $\sigma \in C(N)$ with $X \in \sigma_0 SL_2(\mathbb{Z}) \sigma \cap SL_2(\mathbb{Z})$ if and only if $\sigma^{-1} x^{-1} \sigma_0^{-1} \in SL_2(\mathbb{Z})$. That is, if $B = \left(\begin{smallmatrix} \frac{ad'-bc'}{N} & a'b-ab' \\ -\frac{c'}{a} & \frac{NA'}{a} \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Say $a = (c', N)$, then $a|c'$ and $a|Na'$. So, $-\frac{c'}{a}$ and $\frac{Na'}{a}$ are integers. Also, $(\frac{c'}{a}, \frac{N}{a}) = 1$, so there are integers α, b such that $\frac{N}{a}\alpha + \frac{c'}{a}b = d'$. Thus, $\alpha = \frac{ad'-c'b}{N}$ is an integer. Furthermore, if $\alpha' = \alpha + k\frac{c'}{a}$, then the choice $b = \frac{ad'-N\alpha'}{c'} = \frac{ad'-N\alpha}{c'} + kd$ also yields an integer. Thus, there is a unique choice of b such that $0 \leq b < d$. Thus, if $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, then B has integer entries and determinant 1, and $X \in \sigma_0^{-1} SL_2(\mathbb{Z}) \sigma \cap SL_2(\mathbb{Z})$. This choice has $(a,b,d) = 1$, for if $(a,b,d) = \delta > 1$ then $\delta|d$ so $\delta|da'$, and $\delta|a$, $\delta|b$ implies $\delta|a'b - ab'$, which is a contradiction, as $B \in SL_2(\mathbb{Z})$, so $(\frac{Na'}{a}, a'b - ab') = 1$. Thus, every element of $SL_2(\mathbb{Z})$ appears in a coset of the form $\sigma_0^{-1} SL_2(\mathbb{Z}) \sigma \cap SL_2(\mathbb{Z})$. This selection of σ is unique given X. For, $a|c'$, $a|Na'$ is necessary. Also, if $\frac{N}{a}$, $\frac{c'}{a}$ have a common factor, then it also divides d' for any choice of d. But, $(c', d') = 1$. So, $a = (N, c')$. Also, b is determined by the choice of a.

If $\left(\begin{smallmatrix} w & x \\ Ny & z \end{smallmatrix}\right) \in \Gamma_0$, then the above construction is invariant under multiplication on the left by G. That is, X and GX both yield the same element of $C(N)$. For, by computing the coordinants of $\sigma^{-1}(GX)^{-1}\sigma_0^{-1}$, the above construction applied to GX yields $a = (N, Nya' + zc')$ and $b = \frac{a(Nyb'+zd')-N\beta}{Nya'+zc'}$. But, $(N, z) = 1$, so $(N, Nya' + zc') = (N, c')$. Write $c' = ta$, and then $Nya' + zc' = ra$ implies that $dya' + zt = r$. Then, $(N, r) = 1$, for otherwise $(N, z) > 1$, and $\frac{r}{z} = t(\text{mod } d)$. So, $b = \frac{Nyb'+zd'-b\beta}{r} = \frac{z}{r}d'(\text{mod } d) = \frac{d'}{t}(\text{mod d})$. But, the choice for b arising from X is $\frac{ad'-N\alpha}{c'} + kd = \frac{d'-d}{t} + kd = \frac{d'}{t}(\text{mod } d)$. Thus, the choice of b the same for both X and GX. So, every element of $SL_2(\mathbb{Z})$ is in a coset coming from an element of $C(N)$, and two elements are in the same coset if and only if the corresponding elements of $C(N)$ are the same. Thus, there is a bijection between cosets of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$, and elements of $C(N)$.

$\square$

Theorem 4. *If L' is a cyclic sublattice of $L = [1, \tau]$ of order N, then there is a unique matrix $\sigma \in C(N)$ such that $L' = d[1, \sigma\tau]$. Also, if $\sigma \in C(N)$, then $d[1, \sigma\tau]$ is a cyclic sublattice of $[1, \tau]$ of order N.*

Proof. If $L' \subset L = [1, \tau]$, then $L' = [a\tau + b, c\tau + d]$. In this case, $[L : L'] = |ad - bc| = N$. This will be shown by appealing to the theory of $\mathbb{Z}$-modules. If $M = \mathbb{Z}^2$, and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, and $A' = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, then $\det A = M$. Also, if $M = [e_1, e_2]$, where e_1, e_2 are standard basis vectors, then $AM = [ae_1 + be_2, ce_1 + de_2]$, and $(\det A)M = [(ad - bc)e_1, (ad - bc)e_2]$. If $x \in (\det A)M$, and $x = \alpha(ad - bc)e_1 + \beta(ad - bc)e_2$, then $x = (\alpha d - \beta c)(ae_1 + be_2) + (\beta a - \alpha b)(ce_1 + de_2)$. So, $x \in AM$.

Also, $M/A'M \simeq AM/(\det A)M$ as $\mathbb{Z}$-modules. This isomorphism is given by multiplication by A and A^{-1}, for $AA' = \det A$.

The sequence $0 \to AM/(\det A)M \to M/(\det A)M \to M/AM \to 0$ is exact. For, $AM \subset M$ implies $AM/(\det A)M \subset M/(\det A)M$. Also, as shown above $\det(A)M \subset AM$, so he map $M/(\det A)M \to M/AM$ is a quotient with kernel $AM/(\det A)M$. It is clearly surjective, for if $x + AM \in M/AM$, then $x + (\det A)M$ is mapped to $x + AM$. So, by this short exact sequence, $(M/(\det A)M)/(AM/(\det A)M) = M/AM$. This implies that $|M/(\det A)M| = |M/AM||AM/(\det A)M$. But, $|M/(\det A)M| = (\det A)^2$. The last equality can be seen because $M/(\det A)M = \{\alpha e_1 + \beta e_2 : (\det A)e_1 = (\det A)e_2 = 0\}$, so there are $(\det A)^2$ ways to choose α and β. Finally, $M/AM \simeq M/A'M$, for if $\theta = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and $x + AM \in M/AM$, then $\theta(x + AM) = \theta x + A'M$. And, θ^{-1} exists with integer coefficients. So, $|M/A'M| = |M/AM|$. Combining this with the expression gained from the short exact sequence yields

$|M/AM| = \det A$. Thus, $[L : L'] = N$.

To show $\gcd(a, b, c, d) = 1$, a theorem of finite Abelian groups says that such a group G is not cyclic if and only if there is a subgroup of the form $(\mathbb{Z}/d\mathbb{Z})^2$. So, if D divides all of a, b, c, d, then write $A = DA'$. Then, $A'M/DA'M = (\mathbb{Z}/D\mathbb{Z})^2$. But, $A'M \subset M$ implies $A'M/DA'M \subset M/AM$, so M/AM is not cyclic. Conversely, if M/AM is not cyclic, then there is $M'|M'/AM \simeq (\mathbb{Z}/D\mathbb{Z})^2$. So, $M' = \mathbb{Z}\text{-span}\{x, y\}$ for some x, y such that $Dx \in AM, Dy \in AM$. This implies $DM' \subset AM$, and thus there is A' such that $A'DM' = AM$. Then, $A = DA'$, and so D divides $\gcd(a, b, c, d)$.

If $L' \subset [1, \tau]$ is cyclic and of finite index, and $[L : L'] = N$, then let d b the smallest positive integer in $L' \cap \mathbb{Z}$. This exists, because $[L : L']$ is finite. Then, $1 \in \frac{L'}{d}$, and $\frac{L'}{d}$ is a lattice. By previous discussions, $\frac{L'}{d} = [1, \tau']$. But, $d\tau' \in L'$, so $d\tau' = a\tau + b$, so $L' = [d, a\tau + b] = [d, a\tau + (b + kd)]$. These integers can be chosen so that $0 < a$, and $0 \leq b < d$. From the first paragraph, $|ad| = N, c = 0, (a, b, d) = 1$. For uniqueness, say $L' = [d, a'\tau + d']$, then $|ad| = |a'd|$, and $a' > 0$, so $a = a'$. Also, if $b' = b$, for $0 \leq b', b < d$, so if $b' \neq b$, then $(a\tau - b') - (a\tau - b) = b' - b$ is in L', but then $|b - b'| < d$, which contradicts the minimality of d. □

Thus, the map $q \colon X_0(N) \to X_0(1)$ is a covering of degree $|C(N)|$, and ramifies only when the automorphism class of E is non trivial. But, the map $q \colon \mathbb{H}/\Gamma_0(N) \to \mathbb{H}/SL_2(\mathbb{Z})$ is also a covering of degree $|C(N)|$. Also, if the map $\Psi : X_0(1) \to \mathbb{H}/SL_2(\mathbb{Z})$ gives the analytic isomorphism from $X_0(1)$ to $\mathbb{H}/SL_2(\mathbb{Z})$ discussed in the first paragraph, then Ψ is a covering of degree one. The map $\pi_N \colon X_0(N) \to X_0(1)$ composed with the map $\Psi \colon X_0(1) \to \mathbb{H}/SL_2(\mathbb{Z})$ is the same as the map $\omega \colon X_0(N) \to \mathbb{H}/\Gamma_0(N)$ composed with the map $q \colon \mathbb{H}/\Gamma_0(N) \to \mathbb{H}/SL_2(\mathbb{Z})$ (that is, $\Psi\pi_N = q\omega$.) For, if $(E, C) \simeq ([1, \tau], [\frac{1}{N}, \tau]) \in X_0(N)$, then $\Psi\pi_N(E, C) = \Psi E = SL_2(\mathbb{Z})\tau$. Also, $q\omega(E, C) = q\Gamma_0(N)\tau = SL_2(\mathbb{Z}\tau)$. The degree of the covering $q\omega$ is $|C(N)|$, so the degree of the covering $\Psi\omega$ is also $|C(N)|$. But, degree of coverings is multiplicative, so the degree of the covering ω is one. Also, q, π_N and Ψ are all analytic, so ω is also analytic. Thus, $X_0(N)$ is analytically isomorphic to $\mathbb{H}/\Gamma_0(\mathbb{Z})$.