GENUS OF MODULAR CURVES

LALIT JAIN

1. Introduction

In previous lectures we have developed the theory of modular curves as quotients of the upper half plane by congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. In this essay we will compute the genus for the curves $\mathrm{X}_0(N)$ for $N = 2, 3, 5, 7$ and 13, i.e. all N such that $N - 1|24$.

Recall that

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv 0 \bmod N \right\}$$

is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and that

$$\mathrm{X}_0(N) \cong \frac{\mathrm{H}^*}{\Gamma_0(N)}$$

Recall from Lloyd's talk that the points of $\mathrm{X}_0(N)$ consist of isomorphism classes of pairs of the form (E, C) where E is an elliptic curve and C is a cyclic subgroup of E of size N. Since $\Gamma_0(N)$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ there is a natural map $\phi : \mathrm{X}_0(N) \to \mathrm{X}_0(1)$ which maps each point corresponding to (E, C) to the point on $\Gamma_0(N)$ corresponding to E. This map is a covering of $\mathrm{X}_0(1)$ by $\mathrm{X}_0(N)$ of degree $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$. For N prime $E[N] \cong \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^2$ thus there are $N+1$ cyclic subgroups of order N in the elliptic curve E. So unless there is an automorphism $\psi : (E, C) \to (E, C')$ which maps the cyclic subgroup C to the cyclic subgroup C', (E, C) and (E, C') correspond to different points of $\mathrm{X}_0(N)$. From this we can also see that for N prime, $[\mathrm{X}_0(N) : \mathrm{X}_0(1)] = N + 1$.

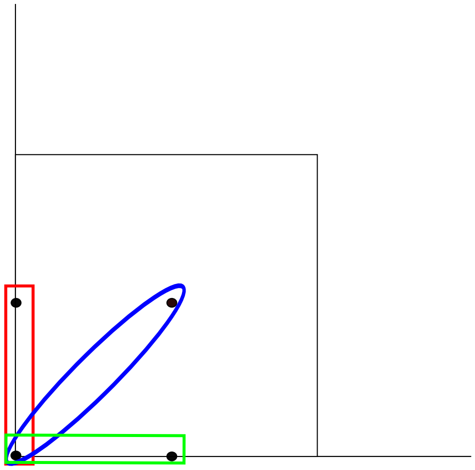
Thus we see that ramification of ϕ will occur at points of $\mathrm{X}_0(N)$ (orbits) which contain pairs (E, C) for which there is a non trivial automorphism. Note that isomorphic elliptic curves have the same j invariant, so from our classification of automorphisms this can only occur for elliptic curves with identified isomorphic cyclic subgroups that have j invariant $1728, 0$, and ∞. Once we find these ramification degrees we can use the following to compute genus:

Theorem 1.1 (Riemann-Hurwitz). *If $f : X \to Y$ is a surjective analytic function between Riemann surfaces, then*

$$2g_X - 2 = deg(f)(2g_Y - 2) + \sum_{P \in X} (e(P) - 1)$$

where g_X is the genus of X and g_Y is the genus of Y.

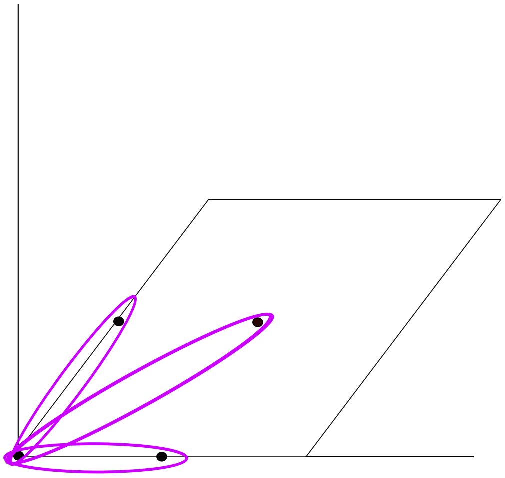
Of course in our case we take $Y = \mathrm{X}_0(1)$ which is isomorphic to $\mathbb{C}$ under j, so it has genus 0. Now let us apply this theorem when $N = 2$. In this case the curve with $j = 1728$ correspond to the lattice below



We can easily check that in the case of $j = 1728$ that the subgroups marked by boxes are mapped to each other by an element of the automorphism group while the oval is distinct.

Thus these correspond to two unique points on the modular curve $\mathrm{X}_0(2)$, one of the points (corresponding to the pair (E, C) where C represents the boxes and $j(E) = 1728$) ramifies twice and the other point ramifies once under ϕ.

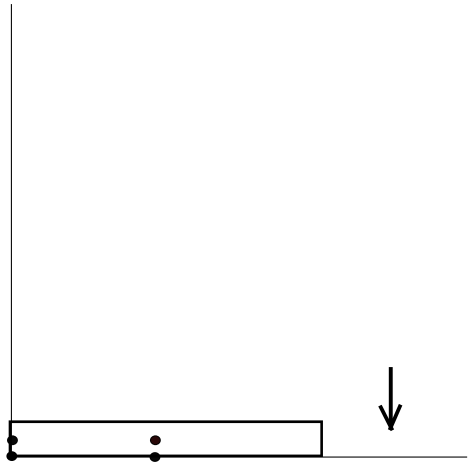
Similarily in the case of $j = 0$ we can easily see that all the cyclic subgroups of size to are the same under $\mathrm{Aut}(E)$. Thus this corresponds to a point with ramification index 3.



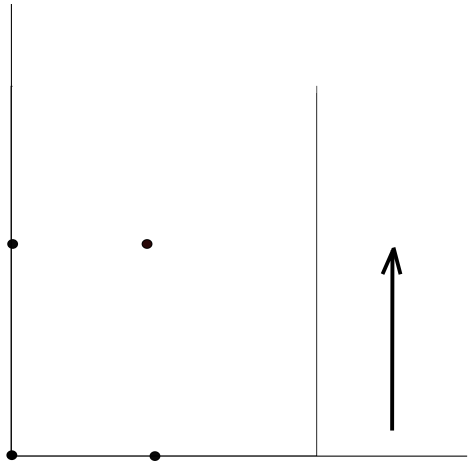
This leaves the case of when $j = \infty$. Of course there is no elliptic curves which correspond to a j invariant of infinity, but these correspond to the cusps of $\Gamma_0(N)$. Before we proceed we state the following lemma

Lemma 1.2. *If N is prime $X_0(N)$ consists of two cusps,* $[0, 1]$ *and* $[1, 0]$ *in* $\mathbb{P}^1(\mathbb{Q})$.

These two cusps correspond respectively to the orbits of $\mathbb{Q}$ and the point at infinity, $[1, 0]$. First consider the orbit of $\mathbb{Q}$. In the limit we can picture these 'curves' as having arbritrarily small height as illustrated below. As this height goes to 0, the 2 cyclic subgroups which lie off the imaginary axis will become identified, and thus we have a point of ramification 2.



In the case of $[1, 0]$ we have a 'curve' with arbritarily large height. In this case it is clear that there is only one identified cyclic subgroup, the one on the real axis. In the limit the other subgroups will not be cyclic. Thus this gives a point which ramifies once.



Now to compute the genus we employ Riemann Hurwitz

$$2g-2 = 3 \cdot -2 + \underbrace{2-1+1-1}_{j=1728} + \underbrace{3-1}_{j=0} + \underbrace{2-1+1-1}_{j=\infty} = -2$$

so $g = 0$.

Now we consider an alternative way to find the genus and ramification points. We begin by defining the Dekekind η function

$$\eta(\tau) = q^{1/24} \prod_{i \geq 1} (1 - q^i)$$

where $q = \exp(2\pi i \tau)$. Define

$$j_2(\tau) = \frac{\eta(\tau)^{24}}{\eta(2\tau)^{24}}.$$

We can easily show that j_2 is a modular function of weight 0 for $\Gamma_0(2)$. Now j defines a map on $\mathrm{X}_0(2)$ and since j_2 is a Hauptmodul we know that j must be a rational function of j_2. Namely

$$j = \frac{(j_2 + 256)^3}{j_2^2}.$$

Note that this is enough information to determine the ramification points of ϕ. For $j = 0$, this corresponds to $j_2 = -256$ ramifying three times. When $j = \infty$, $j_2 = 0$ which ramifies twice or $j_2 = \infty$ ramifying once. When $j = 1728$, we can use the fact that

$$j - 1728 = \frac{(j_2 + 64)(j_2 - 512)^2}{j_2^2}$$

to see that this corresponds to points on $\mathrm{X}_0(2)$ with $j_2 = 64$ ramifying once (the blue oval above), and $j_2 = 512$ ramifying twice (the rectangles).

In general for $N - 1|24$ we have that

$$j_N = \frac{\eta(\tau)^{24/(N-1)}}{\eta(N\tau)^{24/(N-1)}}$$

is an analytic isomorphism from $\mathrm{X}_0(N)$ to $\mathbb{C}$. Furthermore it is a Hauptmodul[1] so j as a function on $\mathrm{X}_0(N)$ can be written as a rational function in j_2. Now from the lemma and a geometric argument analogous to the one above, $\mathrm{X}_0(N)$ will have two cusps, one of them will correspond to $j_2 = 0$ and will have ramification N, and the other will correspond to $j_2 = \infty$ and will have ramification 1. Thus we know that

$$j = \frac{P(j_N)}{j_N^N}$$

where j_N is a polynomial of degree $N+1$. To determine the polynomial, recall that we have the following expansion for j,

$$j = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n)q^n = \frac{(j_2 + 256)^3}{j_2^2}.$$

We can use this expression to solve for the coefficients of $P(z)$. For example when $N = 3$

$$P(j_N) = j_N^4 + bj_N^3 + cj_N^2 + dj_N + e$$

and

$$(j_N^4 + bj_N^3 + cj_N^2 + dj_N + e) - j_N^3 \cdot j = 0.$$

Expanding and equating coefficients of powers of q gives the result. A Maple file has been attached explaining how to carry out this computation. Note that all we have to check when equating powers of q is the negative Laurent terms since the modular curves are compact Riemann surfaces and thus any non constant function must have a pole. In the case of $N = 3$ the method given above gives

$$j = \frac{(j_3 + 27)(j_3 + 243)^3}{j_3^3}.$$

[1] A Hauptmodul is simply an analytic isomorphism from the upper half plane quotiented by some congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ such that each modular function on the resulting surface can be written as a rational function of the hauptmodul. In addition the Hauptmodul is always chosen so that it's Laurent expansion is of the form $\frac{1}{q} + \sum_{i=1}^{\infty} c_n q^n$.

Thus when $j = 0$ we have a point of ramification 1 and a point which ramifies thrice. The following table summarizes the ramification points for ϕ for $N = 2, 3, 5, 7, 13$. The statement k to 1 is the ramification index of a particular point with the given j value of that column.

N	j	Ramification		
		$j = 1728$	$j = 0$	$j = \infty$
2	$\frac{(j_2+256)^3}{j_2^2}$	2 to 1	3 to 1	2 to 1
		1 to 1		1 to 1
3	$\frac{(j_3+27)(j_3+243)^3}{j_3^3}$	2 to 1	3 to 1	3 to 1
		2 to 1	1 to 1	1 to 1
5	$\frac{(j_5^2+250j_5+5^5)^3}{j_5^5}$	2 to 1	3 to 1	5 to 1
		1 to 1	3 to 1	1 to 1
		1 to 1		
		2 to 1		
7	$\frac{(j_7^2+13j_7+49)(j_7^2+245j_7+7^4)^3}{j_7^7}$	2 to 1	3 to 1	7 to 1
		2 to 1	3 to 1	1 to 1
		2 to 1	1 to 1	
		2 to 1	1 to 1	
13	$\frac{(j_{13}^2+5j_{13}+13)(j_{13}^4+247j_{13}^3+3380j_{13}^2+15379j_{13}+13^4)^3}{j_{13}^13}$	Six 2 to 1	Four 3 to 1	13 to 1
		Two 1 to 1	Two 1 to 1	1 to 1

To demonstrate how we can use Riemann Hurwitz given this type of data consider the case of $N = 7$,

$$2g - 2 = -2 \cdot \underbrace{8}_{\deg \phi} + \underbrace{1 + 1 + 1 + 1}_{j=1728} + \underbrace{2 + 2}_{j=0} + \underbrace{6}_{j=\infty} = -2$$

which implies that the genus of $\mathrm{X}_0(7)$ is 0.

References

[1] Joseph H. Silverman. The Arithmetic of Elliptic Curves.
[2] David A. Cox. Primes of the Form $x^2 + ny^2$.
[3] D.A. Buell and J.T. Teitelbaum Computational Perspectives on Number Theory.