Shimura Varieties: Problem sheet 1

Modular Curves

8 October 2014

1. **A fundamental domain for** $\mathrm{SL}_2(\mathbb{Z})$

   Prove that
   $$\mathcal{F} = \{\tau \in \mathcal{H} \mid -\tfrac{1}{2} < \operatorname{Re}\tau < \tfrac{1}{2}, |\tau| > 1\}$$
   is a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$.

   Recall the definition of a **fundamental domain**: $\mathcal{F} \subset \mathcal{H}$ is a fundamental domain for $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ if it is a connected open set, no two points of $\mathcal{F}$ lie in the same Γ-orbit, and every Γ-orbit in $\mathcal{H}$ contains at least one point of the closure of $\mathcal{F}$.

   Outline of proof:

   (a) If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then $\operatorname{Im}(\gamma\tau) = \operatorname{Im}(\tau)/\left|c\tau + d\right|^2$.

   (b) Deduce that every $\mathrm{SL}_2(\mathbb{Z})$-orbit contains an element τ such that $\operatorname{Im}\tau$ is greater than or equal to $\operatorname{Im}\tau'$ for any other τ' in the same orbit.

   (c) We can replace the above τ by $\tau+b$ for some $b \in \mathbb{Z}$, such that $-\frac{1}{2} \leq \operatorname{Re}(\tau+b) \leq \frac{1}{2}$. Then show that $|\tau + b| \geq 1$.

   (d) Show that if τ and τ' are both in $\mathcal{F}$ and they lie in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit, then $\tau = \tau'$.

2. **Riemann surface structure on the compactified modular curve** $X(\Gamma)$

   Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be any congruence subgroup.

   (a) Show that the action of Γ on $\mathcal{H}$ is **properly discontinuous** i.e. for all $\tau_1, \tau_2 \in \mathcal{H}$, there exist neighbourhoods U_1 of τ_1 and U_2 of τ_2 such that, for all $\gamma \in \Gamma$,
   $$\gamma(U_1) \cap U_2 \neq \emptyset \Rightarrow \gamma(\tau_1) = \tau_2.$$

   (b) Show that if S is any Hausdorff space and G is any discrete group acting properly discontinuously on S, then the quotient topological space $G\backslash S$ is Hausdorff.

   (c) Let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Define a topology on $\mathcal{H}^*$, generated by the topology on $\mathcal{H}$ together with the following open sets:

   - $\{\tau \mid \operatorname{Im}\tau > R\} \cup \{\infty\}$ for each $R \in \mathbb{R}$;
   - sets of the form $D \cup \{x\}$ for $x \in \mathbb{Q}$, where D is a disc in $\mathcal{H}$ tangent to the real line at x.

Prove that $\mathcal{H}^*$ is Hausdorff and that the action of Γ on $\mathcal{H}$ extends to a properly discontinuous action on $\mathcal{H}^*$.

(d) Define $X(\Gamma)$ to be the quotient topological space $\Gamma\backslash\mathcal{H}^*$. Define a **cusp** of $X(\Gamma)$ to be an element of $\Gamma\backslash\mathbb{P}^1(\mathbb{Q})$. Prove that $X(\Gamma)$ has finitely many cusps, and that $X(\Gamma)$ is compact.

(e) We say that $P \in Y(\Gamma)$ is an **elliptic point** for Γ if there is some $\tau \in \mathcal{H}$ lifting P and some $\gamma \in \Gamma - \{\pm 1\}$ such that $\gamma\tau = \tau$. The **order** of the elliptic point P is the order of the group

$$\mathrm{Stab}_\Gamma(\tau)/(\Gamma \cap \{\pm 1\}).$$

Determine the elliptic points in $Y(1)$ and their orders. Deduce that every modular curve $Y(\Gamma)$ has finitely many elliptic points, and that their orders can only be 2 or 3.

(f) Show that if $P \in Y(\Gamma)$ is not an elliptic point and $\tau \in \mathcal{H}$ lifts P, then there is a neighbourhood U of τ such that $\pi_{|U}$ is a homeomorphism from U to an open subset of $Y(\Gamma)$.

(g) Let $P \in Y(\Gamma)$ be an elliptic point of order n and $\tau \in \mathcal{H}$ a point lifting P. Choose $\delta \in \mathrm{SL}_2(\mathbb{C})$ mapping $\tau \mapsto 0$ and $\bar{\tau} \mapsto \infty$. Show that δ conjugates $\mathrm{Stab}_\Gamma(\tau)/(\Gamma \cap \{\pm 1\})$ to the group of rotations generated by $e^{2\pi i/n}$.
Show that there are open neighbourhoods U of τ in $\mathcal{H}$, D, D' of 0 in $\mathbb{C}$ and U' of P in $Y(\Gamma$ such that $\pi_{|U}$ factors as follows, with ϕ being a homeomorphism:

$$U \xrightarrow{\delta} D \xrightarrow{z \mapsto z^n} D' \xrightarrow{\phi} U'$$

ϕ^{-1} gives us a chart on a neighbourhood of P.

(h) Let $P \in X(\Gamma)$ be a cusp and $x \in \mathbb{P}^1(\mathbb{Q})$ point lifting P. Choose $\delta \in \mathrm{SL}_2(\mathbb{Z})$ such that $\delta P = \infty$. Show that δ conjugates $\mathrm{Stab}_\Gamma(P)/(\Gamma \cap \{\pm 1\})$ to the group of translations generated by $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ for some integer h.
Show that we can define a chart on a neighbourhood of P by a method similar to the above, using $z \mapsto e^{2\pi i z/h}$ in place of $z \mapsto z^n$.

(i) Show that all the charts on $X(\Gamma)$ defined above are compatible.

3. **Genus of modular curves**

Let p be a prime number, and let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be any congruence subgroup.

(a) Use the Riemann–Hurwitz formula for the natural map $X(\Gamma) \to X(1)$ to prove the following formula for the genus of $X(\Gamma)$:

$$g(X(\Gamma)) = 1 + \frac{n}{12} - \frac{e_2}{4} - \frac{e_3}{3} - \frac{e_\infty}{2}$$

where $n = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]/[\{\pm 1\} : \Gamma \cap \{\pm 1\}] = \deg(X(\Gamma) \to X(1))$, e_2 and e_3 are the numbers of elliptic points of order 2 and 3 respectively on $X(\Gamma)$, and e_∞ is the number of cusps on $X(\Gamma)$.

(b) Show that $X_0(p)$ has two cusps and that the degree of $X_0(p) \to X(1)$ is $p+1$.

(c) Deduce that $X_0(N)$ has genus 0 for $N = 2, 3, 5, 7, 13$ (you don't need to do any more calculations: remember that the genus and the e_i are nonnegative integers).

(d) Show that if the number of elliptic points of order 2 on $X_0(p)$ is

- 0 if $p \equiv 3 \mod 4$;
- 2 if $p \equiv 1 \mod 4$;
- 1 if $p = 2$.

(e) Show that the number of elliptic points of order 3 on $X_0(p)$ is

- 0 if $p \equiv 2 \mod 3$;
- 2 if $p \equiv 1 \mod 3$;
- 1 if $p = 3$.

(This is similar to counting elliptic points of order 2 but more tedious so you might skip it.)

(f) Calculate the genus of $X_0(11)$ and $X_0(17)$.

(g) Count the cusps on $X_0(N)$ and calculate the degree of $X_0(N) \to X(1)$ for composite N, or at least for all $N \leq 10$, and deduce that $X_0(N)$ has genus zero for all $N \leq 10$.

(h) (Optional extra – a lot of work) Compute the genus of $X_1(p)$ or maybe even $X(p)$. Note that there are no elliptic points on $X_1(p)$ for $p \geq 5$ and on $X(p)$ for $p \geq 2$.

4. **The j-function as a modular function**

The purpose of this exercise is to show that the elliptic curve $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ really does have j-invariant $j(\tau)$, where j is the unique $\mathrm{SL}_2(\mathbb{Z})$-invariant holomorphic function satisfying $j(i) = 1728$ and $j(e^{2\pi i/3}) = 0$ and such that the induced function on $X(1)$ is meromorphic at the cusp.

(a) For any integer $k \geq 3$, define the **Eisenstein series**

$$G_k(\tau) = \sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}} \frac{1}{(m+n\tau)^k}.$$

Prove that G_k converges absolutely and uniformly on compact subsets of $\mathcal{H}$, and hence defines a holomorphic function on $\mathcal{H}$. (For $k = 2$, the series converges but not absolutely.) Note that when k is odd, the series sums to zero.

(b) Prove that for $k \geq 3$, G_k satisfies

$$G_k(\gamma\tau) = (c\tau + d)^k G_k(\tau)$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$. A meromorphic function on $\mathcal{H}$ satisfying this condition is said to be **weakly modular of weight k**.

(c) Prove that as $G_k(\tau)$ is bounded on $\{\tau \in \mathcal{H} \mid \operatorname{Im} \tau > C\}$ for some constant $C > 0$. A weakly modular function which is holomorphic on $\mathcal{H}$ and satisfies this boundedness condition is called a **modular form**. (You may often see the definition of modular form given with a stronger condition at ∞, but the next point implies that the apparently stronger definition is equivalent.)

(d) Since G_k is invariant under translations by $\mathbb{Z}$, it factors as

$$G_k(\tau) = F(e^{2\pi i \tau})$$

for some function F which is holomorphic on a disc punctured at the origin. The condition from the (c) shows that F is bounded on a neighbourhood of 0, and hence extends to a holomorphic function at 0.

You can interpret this disc with coordinate $q = e^{2\pi i \tau}$ as a coordinate chart around the cusp on $X(1)$. However this does not show that G_k induces a holomorphic function on $X(1)$ because it is not $\mathrm{SL}_2(\mathbb{Z})$-invariant (and in any case $X(1)$ has no non-constant holomorphic functions). It is possible to interpret modular forms as meromorphic differential forms on $X(1)$, but that is beyond the scope of these exercises.

(e) One can use the Weierstrass $\wp$-function to define an isomorphism between $\mathbb{C}/\Lambda_\tau$ and the elliptic curve with Weierstrass equation

$$E_\tau \colon Y^2 Z = 4X^3 - g_2(\tau) X Z^2 - g_3(\tau) Z^3.$$

where $g_2 = 60 G_4$ and $g_3 = 140 G_6$. (Note that the $4X^3$ is a different normalisation from that used in lectures.)

Show that the j-invariant of E_τ is

$$J(\tau) = 1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2}.$$

(f) Show that $G_6(i) = G_4(e^{2\pi i/3}) = 0$ using the fact that i and $e^{2\pi i/3}$ have non-trivial stabilisers in $\mathrm{SL}_2(\mathbb{Z})$. Use the fact that the discriminant of E_τ is non-zero to deduce that $G_4(i) \neq 0$ and $G_6(e^{2\pi i/3}) \neq 0$. Substituting in the above formula, deduce that

$$J(i) = 1728, \quad J(e^{2\pi i/3}) = 0.$$

(g) Since G_4 and G_6 extend to meromorphic functions on a neighbourhood of ∞ in $\mathcal{H}^*$, J does likewise. Hence J induces a meromorphic function on $X(1)$. Conclude that $J = j$.

Because J is a holomorphic function of degree 1 on $Y(1)$, it has a pole of order 1 at the cusp. It is possible to calculate the Laurent series of G_{2k} at ∞, and use this to obtain the Laurent series of J. This begins

$$J = \frac{1}{q} + 744 + 196884q + \cdots$$

where q is the local coordinate $e^{2\pi i\tau}$. One justification for the 1728 which appears in the definition of j is that the pole has residue 1 and the Laurent series has integer coefficients.

5. **Modular polynomials**

For $N \geq 2$, define $j_N\colon \mathcal{H} \to \mathbb{C}$ by $j_N(\tau) = j(N\tau)$.

In this exercise we will construct the modular polynomial $\Phi_N(X, Y)$, a symmetric polynomial in $\mathbb{C}[X, Y]$ such that $\Phi_N(j, j_N) = 0$. The curve defined by Φ_N in $\mathbb{A}^2$ is birational to $X_0(N)$.

(a) Show that j_N is $\Gamma_0(N)$-invariant, and so induces a meromorphic function on $X_0(N)$.

(b) Let $\gamma_1, \dots, \gamma_r$ be a set of representatives for $\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z})$, and define $f_i = j_N \circ \gamma_i\colon \mathbb{H} \to \mathbb{C}$.

Observe that for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the set of functions $\{f_1 \circ \gamma, \dots, f_r \circ \gamma\}$ is a permutation of $\{f_1, \dots, f_r\}$. Deduce that any symmetric polynomial in the f_i is $\mathrm{SL}_2(\mathbb{Z})$-invariant and so lies in $\mathbb{C}(j)$. Hence

$$P_N(Y) = \prod_{i=1}^{r} (Y - f_i)$$

is a polynomial with coefficients in $\mathbb{C}(j)$, which vanishes at j_N.

(c) Consider any polynomial $P \in \mathbb{C}(j)[T]$. Observe that $P(j_N)$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant, and deduce that $P(j_N) = P(f_i)$ for all i. In particular, if j_N is a root of P, then all the f_i are roots of P.

(d) Show that the functions $f_1, \dots, f_r$ are distinct.

(e) Deduce that P_N is the minimum polynomial of j_N over the field $\mathbb{C}(j)$. Observe that $\deg P_N = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = \deg(X_0(N) \to X(1))$ and deduce that the field of meromorphic functions on $X_0(N)$ is $\mathbb{C}(j, j_N)$.

(f) The coefficients of P_N are holomorphic functions on $\mathcal{H}$, so they lie not just in $\mathbb{C}(j)$ but in $\mathbb{C}[j]$. Hence, if we replace j by X in P_N, we get a two variable polynomial $\Phi_N \in \mathbb{C}[X, Y]$ such that $\Phi_N(j, j_N) = 0$.

(g) By considering $\Phi_N(j(-1/N\tau), j(-1/\tau))$, show that Φ_N is symmetric in X and Y.

Using the fact that the q-expansion of j has integer coefficients, one can show that the coefficients of Φ_N are also integers. Furthermore, using the q-expansion of j it is in principle possible to calculate Φ_N for any given N. However its coefficients grow very fast so even with a computer, this is only feasible for very small N.

The plane curve $C_N = \{(x, y) \in \mathbb{C}^2 \mid \Phi_N(x, y) = 0\}$ has function field $\mathbb{C}(j, j_N)$, the same as the function field of $Y_0(N)$, so these curves are birationally equivalent.

However these curves are not isomorphic because $Y_0(N)$ is smooth while C_N is singular (you can prove this by noting that if C_N were smooth, Plücker's formula would give the wrong genus for $X_0(N)$).

Can you give an explanation in terms of moduli for why C_N and $Y_0(N)$ are not isomorphic?

Every function field of a curve has a unique smooth projective model, so we could construct $X_0(N)$ as an algebraic curve over $\mathbb{Q}$ by blowing up the singularities of a compactification of C_N.