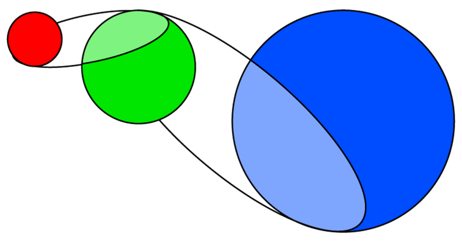
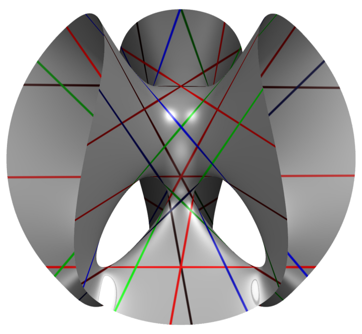
# Young Women in Algebraic Geometry





# Models for Modular Curves

Iva Kodrnja

Advisor : Prof. Dr. Goran Muić

University of Zagreb

## Introduction

In this poster I present a method for obtaining defining equations for modular curves. This method is from my mentor Goran Muić. Modular curves are objects which have the structure of compact Riemann surfaces. They are mapped to the projective plane and represented as irreducible projective curves. The method uses modular forms to create a map into the projective plane. Modular curves are defined, as well as modular forms and one example of a model of $X_0(p)$, with $p$ prime, is given.

## Fuchsian groups and Riemann surfaces

### Action of Fuchsian groups on the upper half plane

The domain

$$\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im} z > 0\}$$

is called the *upper half plane*. We observe it as a model for hyperbolic geometry, with the following metric:

$$ds = \frac{\sqrt{(dx)^2 + (dy)^2}}{y}, \quad z = x + iy.$$

A discrete subgroup of $SL_2(\mathbb{R})$ is called a *Fuchsian group*.

Let $\Gamma$ be a fixed Fuchsian group. An element $\alpha \in \Gamma$ acts on the upper half plane by *linear fractional transformations*

$$\alpha.z = \frac{az+b}{cz+d}, \quad \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

The mapping $z \to \alpha.z$ is an automorphism of the upper half plane for $\alpha \in GL_2^+(\mathbb{R})$. If we denote by $\imath(\alpha)$ this automorphism, then the mapping

$$\imath : GL_2^+(\mathbb{R}) \to Aut(\mathbb{H})$$

induces an isomorphism

$$GL_2^+(\mathbb{R})/\mathbb{R}^x \simeq SL_2(\mathbb{R})/\{\pm 1\} \simeq Aut(\mathbb{H}).$$

Let us denote by $\mathbb{H}^*$ the extended upper half plane $\mathbb{H} \cup \mathbb{R} \cup \{\infty\}$. On the quotient space $\Gamma \backslash \mathbb{H}^* = \{\Gamma.z : z \in \mathbb{H}^*\}$ of $\mathbb{H}^*$ by the action of $\Gamma$ a complex structure (a complex coordinate system) can be defined. Thus this set is a Riemann surface and we denote it by $\mathfrak{R}_\Gamma$. The equivalence classes of the action of $\Gamma$ on the set $\mathbb{R} \cup \{\infty\}$ are called *cusps* of that Fuchsian group.

Definition of a Riemann surface

Let $X$ be a connected topological space. For every $x \in X$ there is an open neighbourhood $V \subseteq X$ and a homeomorphism $t$ that maps $V$ onto a connected complex domain. The set $V$ is called a *coordinate neighbourhood* and the map $t$ is called a *local chart*. A collection $\{(V_\alpha, t_\alpha)\}$ is called a *coordinate system* or an *atlas* if the sets $V_\alpha$ cover $X$ and the charts are pairwise compatible - if $V_\alpha \cap V_\beta \neq \emptyset$, then $t_\beta t_\alpha^{-1}$ is a holomorphic mapping in the complex plane. On the set of all coordinate systems we can define an ordering in a natural way. We call $X$ a *Riemann surface* if a maximal coordinate system is given.

### Modular Groups

The group $\Gamma(1) = SL_2(\mathbb{Z})$ and its subgroups of finite index are called *modular groups*. All modular groups are Fuchsian groups. For a positive integer $N$, we define the *principal congruence subgroup* $\Gamma(N)$ by

$$\Gamma(N) = \left\{ \gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\}.$$

A modular group containing a principal congruence subgroup is called a *congruence modular group*. An example is the group $\Gamma_0(N)$ defined by

$$\Gamma_0(N) = \left\{ \gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\}.$$

## Modular Curves

The quotient space of a modular group is called a *modular curve* and it has the structure of a compact Riemann surface. We denote by $X(1)$ the modular curve obtained by the action of $\Gamma(1)$. It is a curve of genus 0 and is birationally equivalent to the projective line. The curve $X_0(N)$ obtained by the group action of $\Gamma_0(N)$ is referred to as the *classical modular curve*. It is important in the theory of elliptic curves because of the theorem of modularity which says that all elliptic curves are rational images of classical modular curves. Smallest $N$ such that an elliptic curve is the image of $X_0(N)$ is called the conductor of the curve. The curve $X(1)$ parametrizes isomorphism classes of elliptic curves, while the curve $X_0(N)$ prametrizes isomorphism classes of elliptic curves with subgroups of order $N$. The genus $g$ of the modular curve $\mathfrak{R}_\Gamma$ can be calculated from the formula:

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

where $\mu$ is the index of the subgroup $\Gamma$ with regards to the group $\Gamma(1)$, $\nu_2$ and $\nu_3$ are numbers of elliptic points of order 2 ad 3 in $\Gamma$ and $\nu_\infty$ is the number of cusps of $\Gamma$.

## Modular forms

### Definition of a modular form

Let $\Gamma$ be a modular group and $k$ an integer. If $f : \mathbb{H} \to \mathbb{C}$ is a meromorphic function that satisfies the transformation formula

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, z \in \mathbb{H}$$

then we say that f is *weakly modular of weight $k$ for* $\Gamma$. The group $\Gamma(1) = SL_2(\mathbb{Z})$ is generated by two elements $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, so any weakly modular function on $\Gamma(1)$ must satisfy $f(z+1) = f(z)$ i.e. it is a periodic function. Therefore, it has a Fourier expansion of the following form in a neighbourhood of the origin

$$f(q) = \sum_{n=m}^{\infty} a_n q^n, \quad q = e^{2\pi i z}.$$

If $a_n = 0$ for $n < 0$, we say that $f$ is *holomorphic at* $\infty$. The expression $f(q)$ is called the *Fourier expansion of* $f$. We define the *weight $k$ operator* $|[\gamma]_k$ on functions from $\mathbb{H}$ to $\mathbb{C}$ by

$$(f|[\gamma]_k)(z) = (cz+d)^{-k} f(\frac{az+b}{cz+d}), \quad z \in \mathbb{H}.$$

We say that the function $f : \mathbb{H} \to \mathbb{C}$ is a *modular form of weight $k$ for the group* $\Gamma$ if

1. $f$ if holomorphic on $\mathbb{H}$
2. $f$ is weakly modular of weight $k$ for $\Gamma$
3. $f|[\alpha]_k$ is holomorphic at $\infty$ for all $\alpha \in \Gamma(1)$.

The space of modular forms of weight $k$ on the modular group $\Gamma$, denoted by $M_k(\Gamma)$, is a finite dimensional $\mathbb{C}-$vector space. The space of all modular forms $\sum_k M_k(\Gamma)$ is a graded ring. Modular forms of weight $k$ on $\Gamma$ are differentials of degree $k/2$ on the Riemann surface $\mathfrak{R}_\Gamma$.

## Models for modular curves

### Compact Riemann surfaces

The theory of compact Riemann surfaces is equivalent to the theory of projective algebraic curves - compact Riemann surfaces are algebraic objects. The compact Riemann surface $X$ has its field of meromorphic functions $\mathcal{M}(X)$ which we know is non-empty from the Riemann-Roch theorem. Here is how we see its canonical structure as a projective curve whose set of rational functions is exactly $\mathcal{M}(X)$. We take a Zariski open set $U \subseteq X$ (complement of a finite set) and define regular functions on $U$ to be functions in $\mathcal{M}(X)$ that don't have poles in $U$. In this way we get a projective curve. The map $U \to \mathbb{C}[U]$ is the sheaf of regular functions on $X$. For this reason, we can construct embeddings from compact Riemann surfaces to projective space. The image of such embedding is called *projective model* of the given Riemann surface and it is an irreducible projective curve $C$. The field of rational functions on $C$ is isomorphic to the field of meromorphic functions on the Riemann surface. The homogeneous polynomials defining $C$ are often referred to as defining equations of the corresponding Riemann surface.

### Holomorphic map to the projective plane

Let $\Gamma$ be a modular group. We take three linearly independent modular forms $f, g, h$ of the even weight $k \geq 4$ and construct the map $\mathfrak{R}_\Gamma \to \mathbb{P}^2$

$$\mathfrak{a} \to [f(z) : g(z) : h(z)].$$

Denote the image curve by $C(f,g,h)$ and the degree of the map by $d(f,g,h)$. The degree of the map is defined as the degree of extension of the field of rational functions on $\mathcal{C}(f,g,h)$ over the field of rational functions on $\mathfrak{R}_\Gamma$. The following formula is valid:

$$d(f,g,h) \deg C(f,g,h) = \dim M_k(\Gamma) + g(\Gamma) - 1 - \sum_{\mathbf{a} \in \mathfrak{R}_\Gamma} \min\left(D_f(\mathbf{a}), D_g(\mathbf{a}), D_h(\mathbf{a})\right),$$

where $g(\Gamma)$ is the genus of $\mathfrak{R}_\Gamma$ and $D_f, D_g, D_h$ are integral divisors attached to the modular forms $f, g, h$. This formula enables us to calculate the degree of the map. We developed an algorithm that calculates the degree of the curve $C(f,g,h)$ (and its defining polynomial). There are also methods to calculate the attached integral divisors of modular forms, and there are formulas for the dimension of the vector space of modular forms of weight $k$ and the genus.

If the degree of the map equals 1 i.e. the map is a birational equivalence, then we have a model for the modular curve $\mathfrak{R}_\Gamma$.

## Example

There are many methods for finding models for the classical modular curve $X_0(N)$. This curve has its canonical model - its field of meromorphic functions is generated by the modular $j$ function and the function $j(N\cdot)$. The classic equation of the curve is the modular polynomial $\phi_N$, which is the minimal polynomial of $j(N\cdot)$ over $\mathbb{C}(j)$. But this model has many disadvantages - the polynomial $\phi_N$ is very difficult to compute and has enormous coefficients. That was the reason for the search for other models. Using the described method we can get the following model for the classic modular curve using the Ramanujan Delta function

$$\Delta(z) = q + \sum_{n=2}^{\infty} \tau(n) q^n \in M_{12}(\Gamma_0(N))$$

and Eisenstein series of weight 4

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \in M_4(\Gamma_0(N))$$

to construct a map

$$\mathfrak{a} = \pi(z) \to \left[\Delta(z) : E_4^3(z) : \Delta(Nz)\right].$$

When $N$ is a prime number, this map is birational equivalence, and the degree of the resulting curve equals $\psi(N) = N \prod_{p|N} (1 + 1/p)$.

### References

- L. J. P. Kilford, *Modular forms - A classical and computational introduction*, Imperial College Press, 2008;
- R. Miranda, *Algebraic Curves and Riemann Surfaces*, American Mathematical Society, 1995;
- T. Miyake, *Modular Forms*, Springer-Verlag, 2008;
- G. Muić, *On degrees and birationality of the maps $X_0(N) \to \mathbb{P}^2$ constructed via modular forms*, preprint.

2015 Faculty of Civil Engineering, Zagreb, Croatia

ikodrnja@grad.hr