Explicit Arithmetic of Modular Curves
Lecture IV: Equations for Modular Curves

Samir Siksek (Warwick/IHÉS/IHP)

20 June 2019
Canonical Map

- $K$ field
- $X$ curve of genus $g \geq 2$
- $\Omega(X)$ space of regular differentials on $X/K$
  
  this is a $K$-vector space of dimension $g$.

Let $\omega_1, \ldots, \omega_g$ be a $K$-basis for $\Omega(X)$.

The **canonical map** is the map

$$\phi : X \to \mathbb{P}^{g-1}, \quad P \mapsto (\omega_1(P) : \cdots : \omega_g(P)).$$

**What does this mean?** Let $f \in K(X) \setminus K$. Then every differential $\omega$ can
be written as $\omega = hdf$ where $h \in K(X)$. So I can write $\omega_i = h_idf$, and then

$$\phi(P) = (h_1(P) : \cdots : h_g(P)).$$
Canonical Map for Hyperelliptic Curves

Consider a genus 2 curve

\[ X : y^2 = a_6 x^6 + \cdots + a_0, \quad a_i \in K, \quad \Delta(f) \neq 0. \]

A basis for \( \Omega(X) \) is

\[ \omega_1 = \frac{dx}{y}, \quad \omega_2 = \frac{x dx}{y}. \]

Note that \( \omega_2/\omega_1 = x \). Thus

\[ \phi : X \to \mathbb{P}^1, \quad P \mapsto (1 : x(P)). \]

Thus \( \phi(X) = \mathbb{P}^1. \)

\[ \therefore \quad \phi \text{ is not an isomorphism but is 2 to 1.} \]
Canonical Map for Genus 3 Hyperelliptic

\[ X : y^2 = a_8 x^8 + \cdots + a_0, \quad a_i \in K, \quad \Delta(f) \neq 0. \]

A basis for \( \Omega(X) \) is

\[ \omega_1 = \frac{dx}{y}, \quad \omega_2 = \frac{xdx}{y}, \quad \omega_3 = \frac{x^2 dx}{y}. \]

\[ \phi : X \to \mathbb{P}^2, \quad \phi(x, y) = (1 : x : x^2). \]

If we choose coordinates \((u_1 : u_2 : u_3)\) for \( \mathbb{P}^2 \) then the image is the conic

\[ \phi(X) = C : u_1 u_3 = u_2^2 \subset \mathbb{P}^2. \]

\[ \therefore \phi : X \to \phi(X) \text{ is not an isomorphism but it is 2 to 1.} \]
A hyperelliptic curve of genus $g$ can be written as

$$X : y^2 = a_{2g+2}x^{2g+2} + \cdots + a_0, \quad a_i \in K, \quad \Delta(f) \neq 0.$$ 

A basis for $\Omega(X)$ is

$$\frac{dx}{y}, \quad \frac{x\,dx}{y}, \quad \ldots, \quad \frac{x^{g-1}\,dx}{y}.$$ 

Check that $\phi : X \to \phi(X) \cong \mathbb{P}^1$ is 2 to 1.
Theorem

Let $X$ be a curve of genus $\geq 2$.

- If $X$ is hyperelliptic then $\phi(X) \cong \mathbb{P}^1$ and the canonical map $\phi : X \to \phi(X)$ is 2 to 1.
- If $X$ is non-hyperelliptic then $\phi : X \to \mathbb{P}^{g-1}$ is an embedding (so $X$ is isomorphic to $\phi(X)$). Moreover $\phi(X)$ is a curve of degree $2g - 2$.

We focus on modular curves where the genus is $\geq 2$.

Recall the isomorphism

$$S_2(\Gamma_H) \cong \Omega(X_H), \quad f(q) \mapsto f(q) \frac{dq}{q}.$$ 

Let $f_1, \ldots, f_g$ be a basis for $S_2(\Gamma_H)$.

The canonical map is given by

$$\phi : X_H \to \mathbb{P}^{g-1}$$

$$\phi = (f_1(q) \frac{dq}{q} : \cdots : f_g(q) \frac{dq}{q}) = (f_1(q) : \cdots : f_g(q)).$$
Example $X_0(30)$

A basis for $S_2(\Gamma_0(30))$ is

\[ f_1 = q - q^4 - q^6 - 2q^7 + q^9 + O(q^{10}), \]
\[ f_2 = q^2 - q^4 - q^6 - q^8 + O(q^{10}), \]
\[ f_3 = q^3 + q^4 - q^5 - q^6 - 2q^7 - 2q^8 + O(q^{10}). \]

\[ \therefore X = X_0(30) \text{ has genus } 3. \]

By theorem,

- either $X$ is hyperelliptic;
- or $X \cong \phi(X)$ is a curve in $\mathbb{P}^{g-1} = \mathbb{P}^2$ which has degree $2g - 2 = 4$; i.e. $\phi(X)$ is a plane quartic curve.

Which is it?
If $X$ is hyperelliptic then $\phi(X)$ is a conic.

(Note in this case that $f_1(q) dq/\ p, \ldots, f_3(q) dq/\ p$ and $dx/y, xdx/y, x^2dx/y$ don't have to be the same basis for $\Omega(X)$. The two bases are related by a linear transformation. So $\phi(X)$ might be a different conic than before.)

$\phi(X) = \text{conic iff } \exists a_1, \ldots, a_6 \ (\text{not all zero}) \ \text{such that}$

$$a_1 f_1^2 + a_2 f_2^2 + a_3 f_3^2 + a_4 f_1 f_2 + a_5 f_1 f_3 + a_6 f_2 f_3 = 0.$$ 

$$f_1^2 = q^2 - 2q^5 - 2q^7 - 3q^8 + 4q^{10} + O(q^{11})$$
$$f_2^2 = q^4 - 2q^6 - q^8 + O(q^{12})$$
$$f_3^2 = q^6 + 2q^7 - q^8 - 4q^9 - 5q^{10} - 6q^{11} + q^{12} + O(q^{13})$$
$$f_1 f_2 = q^3 - q^5 - q^6 - q^7 - 3q^9 + 2q^{10} + O(q^{11})$$
$$f_1 f_3 = q^4 + q^5 - q^6 - 2q^7 - 3q^8 - 2q^9 - 2q^{10} + O(q^{11})$$
$$f_2 f_3 = q^5 + q^6 - 2q^7 - 2q^8 - 2q^9 - 2q^{10} + 2q^{11} + O(q^{12})$$.
\[ \phi(X) = \text{conic iff } \exists a_1, \ldots, a_6 \text{ (not all zero) such that} \]

\[ a_1 f_1^2 + a_2 f_2^2 + a_3 f_3^2 + a_4 f_1 f_2 + a_5 f_1 f_3 + a_6 f_2 f_3 = 0. \]

\[ f_1^2 = q^2 - 2q^5 - 2q^7 - 3q^8 + 4q^{10} + O(q^{11}) \]
\[ f_2^2 = q^4 - 2q^6 - q^8 + O(q^{12}) \]
\[ f_3^2 = q^6 + 2q^7 - q^8 - 4q^9 - 5q^{10} - 6q^{11} + q^{12} + O(q^{13}) \]
\[ f_1 f_2 = q^3 - q^5 - q^6 - q^7 - 3q^9 + 2q^{10} + O(q^{11}) \]
\[ f_1 f_3 = q^4 + q^5 - q^6 - 2q^7 - 3q^8 - 2q^9 - 2q^{10} + O(q^{11}) \]
\[ f_2 f_3 = q^5 + q^6 - 2q^7 - 2q^8 - 2q^9 - 2q^{10} + 2q^{11} + O(q^{12}). \]

- Coefficient of \( q^2 \) \( \implies \ a_1 = 0. \)
- Coefficient of \( q^3 \) \( \implies \ a_4 = 0. \)
- Coefficient of \( q^4, q^5, q^6 \) give

\[ a_2 + a_5 = 0, \quad a_5 + a_6 = 0, \quad -2a_2 + a_3 - a_5 + a_6 = 0 \]
There is only one solution (up to scaling) which is
\[ a_2 = 1, \quad a_3 = 0, \quad a_5 = -1, \quad a_6 = 1. \]

\[ \therefore f_2^2 - f_1 f_3 + f_2 f_3 = 0 + O(q^7). \]

In fact we can check that
\[ f_2^2 - f_1 f_3 + f_2 f_3 = 0 + O(q^{100}). \]

**Question.** Do we know that \( f_2^2 - f_1 f_3 + f_2 f_3 = 0 \) exactly? **If so** then the image is the conic
\[ u_2^2 - u_1 u_3 + u_2 u_3 = 0 \quad \subset \mathbb{P}^2, \]
and \( X \) is hyperelliptic.
In fact we can check that

\[ f_2^2 - f_1 f_3 + f_2 f_3 = 0 + O(q^{100}) \]


**Question.** Do we know that \( f_2^2 - f_1 f_3 + f_2 f_3 = 0 \) exactly? If so then the image is the conic

\[ u_2^2 - u_1 u_3 + u_2 u_3 = 0 \subset \mathbb{P}^2, \]

and \( X \) is hyperelliptic.

---

**Theorem (Sturm)**

Let \( \Gamma \) be a congruence subgroup of \( \text{SL}_2(\mathbb{Z}) \) of index \( m \). Let \( f \in S_k(\Gamma) \) and suppose \( \text{ord}_q(f) > km/12 \). Then \( f = 0 \).
Theorem (Sturm)

Let $\Gamma$ be a congruence subgroup of $\text{SL}_2(\mathbb{Z})$ of index $m$. Let $f \in S_k(\Gamma)$ and suppose $\text{ord}_q(f) > km/12$. Then $f = 0$.

Let $f = f_2^2 - f_1 f_3 + f_2 f_3$.

$f_1, f_2, f_3$ are cusp forms for $\Gamma_0(30)$ of weight 2.

$\therefore$ $f$ is a cusp form for $\Gamma_0(30)$ of weight $k = 4$.

\[
[\text{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} (1 + 1/p).
\]

$N = 30 \implies m = 30(1 + 1/2)(1 + 1/3)(1 + 1/5) = 72 \implies \frac{km}{12} = 36$.

Since $\text{ord}_q(f) \geq 100$ we know from Sturm that $f = 0$.

$\therefore X_0(30)$ is hyperelliptic.
\[X_0(45)\]

Repeat \(X_0(45)\). A basis for \(S_2(\Gamma_0(45))\) is

\[g_1 = q - q^4 + O(q^{10}),\]
\[g_2 = q^2 - q^5 - 3q^8 + O(q^{10}),\]
\[g_3 = q^3 - q^6 - q^9 + O(q^{10}).\]

\[\therefore X_0(45)\] has genus 3. \textbf{Is it hyperelliptic?} i.e. \textbf{Is the canonical image a conic?} Again we look for \(a_1, \ldots, a_6\) such that

\[a_1g_1^2 + a_2g_2^2 + a_3g_3^2 + a_4g_1g_2 + a_5g_1g_3 + a_6g_2g_3 = 0.\]

By solving the resulting system of linear equations from the coefficients of \(q^2, \ldots, q^{10}\) we find that all the \(a_i = 0\).

\[\therefore \text{image is not a conic.}\]

\[\therefore \text{image is a plane quartic.}\]
Write down an equation for this plane quartic!

- Look at all 10 monomials of degree 4 in $g_1, g_2, g_3$.
- Want a linear combination which is 0.
- By solving the system resulting from the coefficients of $q^j$ up to $q^{20}$ we find a unique solution (up to scaling).

This unique solution gives us our degree 4 model:

$$X_0(45) : x_0^3 x_2 - x_0^2 x_1^2 + x_0 x_1 x_2^2 - x_1^3 x_2 - 5x_2^4 \subset \mathbb{P}^2.$$ 

Did we need to check up to the Sturm bound? Not this time!

- Already proved that $X_0(45)$ is not hyperelliptic.
- So we know that the canonical image is a quartic.
- We solved for this quartic and found only one solution.
- So that must be the correct quartic.
Return to $X_0(30)$

Know this is hyperelliptic and so has a model

$$y^2 = h(x), \quad h = a_8x^8 + \cdots + a_0.$$

The model is not unique. If $(u, v)$ is any point on this model, we then we can change the model to move this point to infinity:

$$x' = \frac{1}{x - u}, \quad y' = \frac{y}{(x - u)^4}.$$

The new model has the form

$$y'^2 = v^2x'^8 + \cdots.$$

If $v = 0$ (i.e. the original point was a Weierstrass point) then we would end up with $y'^2 = \text{degree 7}$ but otherwise it is $y'^2 = \text{degree 8}$.

Now the infinity cusp $c_\infty$ is a point on $X_0(30)$. Let’s move $c_\infty$ to infinity on the hyperelliptic model. **Question:** Do we obtain a degree 7 model or a degree 8 model?
Exercise.

(i) Let

$$X : y^2 = a_{2g+2}x^{2g+2} + \cdots + a_0$$

be a curve of genus $g$ where $a_{2g+2} \neq 0$. Let $\infty_+$ be one of the two points at infinity. Show that

$$\text{ord}_{\infty_+} \left( \frac{dx}{y} \right) = g - 1, \quad \text{ord}_{\infty_+} \left( \frac{x dx}{y} \right) = g - 2, \ldots,$$

(ii) Let

$$X : y^2 = a_{2g+1}x^{2g+1} + \cdots + a_0$$

be a curve of genus $g$ (here necessarily $a_{2g+1} \neq 0$ otherwise the genus would be smaller than $g$). Let $\infty$ be the unique point at infinity. Show that

$$\text{ord}_{\infty} \left( \frac{dx}{y} \right) = 2(g - 1), \quad \text{ord}_{\infty} \left( \frac{x dx}{y} \right) = 2(g - 2), \ldots,$$
Recall that basis for $S_2(\Gamma_0(30))$ is

\[ f_1 = q - q^4 - q^6 - 2q^7 + q^9 + O(q^{10}), \]
\[ f_2 = q^2 - q^4 - q^6 - q^8 + O(q^{10}), \]
\[ f_3 = q^3 + q^4 - q^5 - q^6 - 2q^7 - 2q^8 + O(q^{10}). \]

\[ \text{ord}_{c_\infty} \left( f_1(q) \frac{dq}{q} \right) = 0, \]
\[ \text{ord}_{c_\infty} \left( f_2(q) \frac{dq}{q} \right) = 1, \]
\[ \text{ord}_{c_\infty} \left( f_3(q) \frac{dq}{q} \right) = 2. \]

\[ \therefore \text{ord}_{c_\infty}(\omega) \leq 2, \quad \forall \omega \in \Omega(X) \setminus \{0\}. \]

But if $c_\infty = \infty$ on $y^2 = \text{degree 7 model}$, then there is some $\omega$ with
\[ \text{ord}_{c_\infty}(\omega) = 4. \]

\[ \therefore \text{When we move } c_\infty \text{ to } \infty \text{ we get a } y^2 = \text{degree 8 model}. \]
Can suppose
$X: y^2 = a_8 x^8 + a_7 x^7 + \cdots + a_0, \quad a_8 \neq 0, \quad c_\infty = \infty_+.$

\[ \text{ord}_{c_\infty} \left( f_1(q) \frac{dq}{q} \right) = 0, \quad \text{ord}_{c_\infty} \left( f_2(q) \frac{dq}{q} \right) = 1, \quad \text{ord}_{c_\infty} \left( f_3(q) \frac{dq}{q} \right) = 2. \]

\[ \text{ord}_{\infty_+} \left( \frac{dx}{y} \right) = 2, \quad \text{ord}_{\infty_+} \left( x \frac{dx}{y} \right) = 1, \quad \text{ord}_{\infty_+} \left( x^2 \frac{dx}{y} \right) = 0. \]

From the valuations

\[
\frac{dx}{y} = \alpha_3 \cdot f_3(q) \frac{dq}{q}, \\
\frac{xdx}{y} = \beta_2 \frac{f_2(q) dq}{q} + \beta_3 \frac{f_3(q) dq}{q}, \\
\frac{x^2 dx}{y} = \gamma_1 \frac{f_1(q) dq}{q} + \gamma_2 \frac{f_2(q) dq}{q} + \gamma_3 \frac{f_3(q) dq}{q},
\]

where $\alpha_3, \beta_2$ and $\gamma_1 \neq 0$. 
\( X : y^2 = a_8 x^8 + a_7 x^7 + \cdots + a_0, \quad a_8 \neq 0, \quad c_\infty = \infty_+ . \)

\[
\begin{align*}
\frac{dx}{y} &= \alpha_3 \cdot f_3(q) \frac{dq}{q}, \\
\frac{xdx}{y} &= \beta_2 \frac{f_2(q) dq}{q} + \beta_3 \frac{f_3(q) dq}{q}, \\
\frac{x^2 dx}{y} &= \gamma_1 \frac{f_1(q) dq}{q} + \gamma_2 \frac{f_2(q) dq}{q} + \gamma_3 \frac{f_3(q) dq}{q},
\end{align*}
\]

The change of hyperelliptic model

\[ x \mapsto rx, \quad y \mapsto sy \]

preserve points at infinity but has the effect

\[
\begin{align*}
\frac{dx}{y} &\mapsto (r/s) \frac{dx}{y}, \\
\frac{xdx}{y} &\mapsto (r^2/s) \frac{xdx}{y}, \quad \ldots
\end{align*}
\]

Thus we can make \( \alpha_3 = 1 \) and \( \beta_2 = 1 \).
\[ X : y^2 = a_8 x^8 + a_7 x^7 + \cdots + a_0, \quad a_8 \neq 0, \quad c_\infty = \infty_+. \]

\[
\frac{dx}{y} = f_3(q) \frac{dq}{q}, \quad \frac{xdx}{y} = \frac{f_2(q) dq}{q} + \beta_3 \frac{f_3(q) dq}{q}, \quad \frac{x^2 dx}{y} = \gamma_1 \frac{f_1(q) dq}{q} + \gamma_2 \frac{f_2(q) dq}{q} + \gamma_3 \frac{f_3(q) dq}{q},
\]

The change of model

\[ x \mapsto x + t, \quad y \mapsto y. \]

preserves the points at infinity and has the effect

\[
\frac{dx}{y} \mapsto \frac{dx}{y}, \quad \frac{xdx}{y} \mapsto \frac{xdx}{y} + t \frac{dx}{y}.
\]

So we can suppose \( \beta_3 = 0. \) i.e.

\[
\frac{dx}{y} = f_3(q) \frac{dq}{q}, \quad \frac{xdx}{y} = f_2(q) \frac{dq}{q}.
\]
\[ X : \ y^2 = a_8 x^8 + a_7 x^7 + \cdots + a_0, \quad a_8 \neq 0, \quad c_{\infty} = \infty_+. \]

\[
\frac{dx}{y} = f_3(q) \frac{dq}{q}, \quad \frac{x dx}{y} = f_2(q) \frac{dq}{q}.
\]

\[ x = f_2(q)/f_3(q) = \frac{1}{q} \frac{1}{1+q-q^2+2q^3-2q^4+2q^5-3q^6+5q^7-5q^8+5q^9+\cdots}. \]

\[ y = \frac{dx}{dq} \cdot \frac{q}{f_3(q)} = -\frac{1}{q^4} + \frac{1}{q^3} - \frac{1}{q^2} - \frac{1}{q} + 5 - 15q + 29q^2 - 60q^3 + 118q^4 - 210q^5 + 346q^6 - 573q^7 + 929q^8 - 1454q^9 + \cdots. \]

By comparing the coefficients of \( q^{-8} \) on both sides we see that \( a_8 = 1. \)
\[ X : y^2 = x^8 + a_7 x^7 + \cdots + a_0, \quad c_\infty = \infty_+. \]

\[ x = \frac{1}{q} - 1 + q - q^2 + 2q^3 - 2q^4 + 2q^5 - 3q^6 + 5q^7 - 5q^8 + 5q^9 + \cdots. \]

\[ y^2 - x^8 = \frac{6}{q^7} - \frac{33}{q^6} + \cdots \]

so \( a_7 = 6 \). Also

\[ y^2 - x^8 - 6x^7 = \frac{9}{q^6} - \frac{48}{q^5} + \cdots \]

so \( a_6 = 9 \). Continuing in this fashion we arrive at

\[ y^2 - x^8 - 6x^7 - 9x^6 - 6x^5 + 4x^4 + 6x^3 - 9x^2 + 6x - 1 = O(q^{100}). \]

Therefore, a model for \( X_0(30) \) is

\[ X_0(30) : y^2 = x^8 + 6x^7 + 9x^6 + 6x^5 - 4x^4 - 6x^3 + 9x^2 - 6x + 1. \]