Open image computations for elliptic curves over number fields

ANTS XVI, July 15th 2024

David Zywina

Cornell University

Elliptic curves

Fix a number field K and an algebraic closure $\overline{K}$.

Let E be an elliptic curve defined over K.

For each integer $n \geq 1$, let $E[n]$ be the n-torsion subgroup of $E(\overline{K})$. We have a group isomorphism

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$$

Since E is defined over K, the absolute Galois group

$$\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$$

acts on $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and respects the group structure. We can express this action as a Galois representation

$$\rho_{E,n} \colon \mathrm{Gal}_K \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

For each $n \geq 1$, we have a Galois representation

$$\rho_{E,n} \colon \mathrm{Gal}_K \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

that encodes the Galois action on $E[n]$.
Combining these together, we obtain a single Galois representation

$$\rho_E \colon \mathrm{Gal}_K \to \mathrm{GL}_2(\widehat{\mathbb{Z}}),$$

where $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$, that encodes the Galois action on all the torsion points of E.

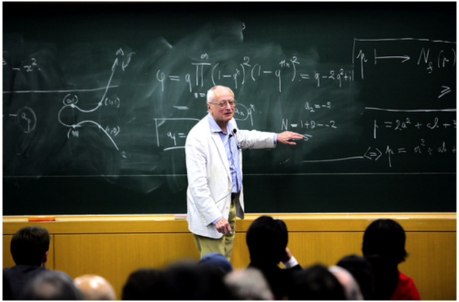
The representation ρ_E is continuous with respect to the profinite topology.

Serre's open image theorem

An elliptic curve E over a number field K gives rise to a representation

$$\rho_E\colon \operatorname{Gal}_K \to \operatorname{GL}_2(\widehat{\mathbb{Z}});$$

define its image $G_E := \rho_E(\operatorname{Gal}_K) \subseteq \operatorname{GL}_2(\widehat{\mathbb{Z}})$.



Source: Wikimedia Commons

Theorem (Serre, 1972)

Let E/K be a non-CM elliptic curve. Then G_E is an open subgroup of $\operatorname{GL}_2(\widehat{\mathbb{Z}})$. Equivalently, $[\operatorname{GL}_2(\widehat{\mathbb{Z}}) : G_E]$ is finite.

Unfortunately, Serre's proof is usually non-effective.

Problem:

Given a non-CM elliptic curve E over a number field K, compute the open group G_E up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

For some $N \geq 1$, G_E contains the kernel of the reduction modulo N map

$$\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

The minimal N is the level of G_E.
So G_E can be explictly described, once known, via its level N and its image in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

When $K = \mathbb{Q}$, the problem has already been solved.

Theorem (Z.)

There is an algorithm to compute G_E, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, for any non-CM elliptic curve $E/\mathbb{Q}$.

The algorithm has been implemented in `Magma` and is efficient! For the non-CM $E/\mathbb{Q}$ of conductor at most 500000, I can compute the groups G_E in around 8 hours. (On average, ≈ 0.01 seconds per curve.)

The original aim of the paper being discussed was to study the computation of G_E when $K \neq \mathbb{Q}$ and to determine whether an algorithm is feasible.

We will focus on computing the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E]$ in the talk.

LMFDB example

For non-CM $E/\mathbb{Q}$ of conductor at most 500000, the images are available via the LMFDB (lmfdb.org). Consider the elliptic curve $E/\mathbb{Q}$ given by

$$y^2 + y = x^3 - x^2 - 7820x - 263580.$$

This curve has conductor 11 and has LMFDB label `11.a1`.

The image $H := \rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ of the adelic Galois representation has level $550 = 2 \cdot 5^2 \cdot 11$, index 1200, genus 37, and generators

$$\begin{pmatrix} 336 & 145 \\ 515 & 216 \end{pmatrix}, \begin{pmatrix} 38 & 41 \\ 191 & 539 \end{pmatrix}, \begin{pmatrix} 1 & 50 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 50 & 1 \end{pmatrix}, \begin{pmatrix} 440 & 9 \\ 127 & 213 \end{pmatrix}, \begin{pmatrix} 501 & 50 \\ 500 & 51 \end{pmatrix}.$$

Input positive integer m to see the generators of the reduction of H to $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$: 100 submit

The reduction of H has index 120 in $\mathrm{GL}_2(\mathbb{Z}/100\mathbb{Z})$ and is generated by

$$\begin{pmatrix} 36 & 45 \\ 15 & 16 \end{pmatrix}, \begin{pmatrix} 38 & 41 \\ 41 & 39 \end{pmatrix}, \begin{pmatrix} 40 & 9 \\ 27 & 13 \end{pmatrix}, \begin{pmatrix} 1 & 50 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 50 & 1 \end{pmatrix}, \begin{pmatrix} 51 & 50 \\ 50 & 51 \end{pmatrix}, \begin{pmatrix} 51 & 0 \\ 0 & 1 \end{pmatrix}.$$

Constraint on $\det(G_E)$

By considering Weil pairings, we always have

$$\det \circ \rho_E = \chi_{\mathrm{cyc}}|_{\mathrm{Gal}_K},$$

where $\chi_{\mathrm{cyc}} \colon \mathrm{Gal}_{\mathbb{Q}} \to \widehat{\mathbb{Z}}^{\times}$ is the cyclotomic character. In particular,

$$\det(G_E) = \det(\rho_E(\mathrm{Gal}_K)) = \chi_{\mathrm{cyc}}(\mathrm{Gal}_K).$$

Therefore,

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\widehat{\mathbb{Z}}^{\times} : \chi_{\mathrm{cyc}}(\mathrm{Gal}_K)] \cdot [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})].$$

So we should focus our attention on the index $[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})]$ and the group $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

A single slide on modular curves

Let $\mathcal{G}$ be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that contains $-I$. Let $L \subseteq \overline{\mathbb{Q}}$ be the minimal number field for which $\chi_{\mathrm{cyc}}(\mathrm{Gal}_L) = \det(\mathcal{G})$. Associated to $\mathcal{G}$ is a modular curve $X_\mathcal{G}$:

There is a nice curve $X_\mathcal{G}$ defined over L with a morphism

$$\pi_\mathcal{G} \colon X_\mathcal{G} \to \mathbb{P}^1_L = \mathbb{A}^1_L \cup \{\infty\}$$

such that the following are equivalent for any non-CM E/K:

- G_E is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $\mathcal{G}$,
- $L \subseteq K$ and the j-invariant j_E of E lies in $\pi_\mathcal{G}(X_\mathcal{G}(K)) \subseteq K \cup \{\infty\}$.

I have implemented an algorithm in `Magma` for computing explicit models of $X_\mathcal{G}$ when $\det(\mathcal{G}) = \widehat{\mathbb{Z}}^\times$ ($L = \mathbb{Q}$). I am beginning to extend it to arbitrary $\mathcal{G}$.

For later: we define the genus of $\mathcal{G}$ to be the genus of $X_\mathcal{G}$.

Main result

Theorem (Z.)

Let K be a number field. There is a finite set $J_K \subseteq K$ such that for any non-CM elliptic curve E over K with

- *j-invariant $j_E \notin J_K$,*
- *$\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell > 19$,*

we can compute the group G_E, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E]$.

- Conjecturally we can remove the assumption that $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ holds for all $\ell > 19$ by extending the finite set J_K (Serre uniformity problem).
- What underlies the algorithm is the precomputation of *finitely many* modular curves (that do not depend on K).
- The set J_K will be very difficult to work out (its finiteness uses Faltings' theorem). However given a $j \in K$, one can determine whether or not $j \notin J_K$.

Key idea

- The group G_E is hard to study and there are too many possibilities!
- The idea is to instead find a slightly larger group $G_E \subseteq \mathcal{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ so that we have an equality

$$[G_E, G_E] = [\mathcal{G}, \mathcal{G}]$$

of commutator subgroups.

We then have inclusions

$$[\mathcal{G}, \mathcal{G}] = [G_E, G_E] \subseteq G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}).$$

So the group $\mathcal{G}$ will limit the possibilities for $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.
- When $K = \mathbb{Q}$, a miracle happens and we have

$$[\mathcal{G}, \mathcal{G}] = G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$$

(miracle = Kronecker–Weber theorem); this is why this case is much easier!

Agreeable closure

Consider a non-CM elliptic curve E/K with $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell > 19$.

We say that a subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is agreeable if:

- $\mathcal{G}$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$,
- $\mathcal{G}$ contains the scalars $\widehat{\mathbb{Z}}^\times I$,
- any prime dividing the level of $\mathcal{G}$ also divides the level of the commutator subgroup $[\mathcal{G}, \mathcal{G}] \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

We have $G_E \subseteq \mathcal{G}_E$ for a unique minimal agreeable subgroup $\mathcal{G}_E \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$.
We call $\mathcal{G}_E$ the agreeable closure of G_E. We indeed have $[G_E, G_E] = [\mathcal{G}_E, \mathcal{G}_E]$.

Moreover, the level of $\mathcal{G}_E$ is not divisible by $\ell > 19$; this is very restrictive!
(The level of G_E can be divisible by primes $\ell > 19$.)

Now consider only agreeable subgroups $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ whose level is not divisible by a prime $\ell > 19$.

- For each $\mathcal{G}$, there are only finitely many maximal agreeable subgroups. The paper gives a classification and an effective way to compute them!
- Starting with $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, taking maximal agreeable subgroups, and repeating..., we will eventually obtain only groups $\mathcal{G}$ of genus at least 2.
- So there is a finite set $\mathcal{A}_1$ consisting of all agreeable subgroups, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, of genus 0 and 1. A large portion of the paper is dedicated to their explicit computation: there are 11960 groups in $\mathcal{A}_1$; 3682 of genus 0 and 8278 of genus 1.
- There is another finite set $\mathcal{A}_2$ of all minimal agreeable subgroups with genus at least 2 up to conjugacy. This set has also been explicitly described.

Fix a number field K and an elliptic curves E/K with $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell > 19$. We have $G_E \subseteq \mathcal{G}_E$. There are two possibilities:

- $\mathcal{G}_E$ is conjugate to a unique $\mathcal{G} \in \mathcal{A}_1$,
- $\mathcal{G}_E$ is conjugate to a subgroup of some $\mathcal{G} \in \mathcal{A}_2$, and hence j_E lies in the set

$$J_K := \bigcup_{\mathcal{G} \in \mathcal{A}_2^*} \pi_{\mathcal{G}}(X_{\mathcal{G}}(K)) \subseteq K \cup \{\infty\}$$

which is finite by Faltings' theorem.

So after the computation of a *finite number* of modular curves (not depending on K or E), we can check if $j_E \in J_K$, and if $j_E \notin J_K$ we can compute $\mathcal{G}_E$.

Aside: there are tens of thousands of modular curves to deal with; this is a large but reasonable task.

Now suppose we have E/K and we known the group $\mathcal{G} := \mathcal{G}_E$.
As already observed, we have inclusions

$$[\mathcal{G}, \mathcal{G}] \subseteq G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}).$$

In particular, we have

$$[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})] \leq [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\mathcal{G}, \mathcal{G}]].$$

We can compute $[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\mathcal{G}, \mathcal{G}]]$ for all $\mathcal{G} \in \mathcal{A}_1$ to get new bounds...

Theorem (Z.)

Let K be a number field. There is a finite set $J_K \subseteq K$ such that for any non-CM elliptic curve E over K with

- $j_E \notin J_K$, *and*
- $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ *for all primes* $\ell > 19$,

we have

$$[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})] \leq \begin{cases} 1382400, & \\ 172800 & \text{if } K \cap \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}, \\ 30000 & \text{if } K \cap \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}) = \mathbb{Q}, \\ 7200 & \text{if } K \cap \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}) = \mathbb{Q}, \\ 1536 & \text{if } K = \mathbb{Q}. \end{cases}$$

Idea for computing $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$

For a non-CM E/K, suppose $\mathcal{G}_E = \mathcal{G} \in \mathcal{A}_1$.
Consider an open subgroup B of $\mathcal{G}$ with $B \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \supseteq [\mathcal{G}, \mathcal{G}]$. The group B is normal in $\mathcal{G}$ and $\mathcal{G}/B$ is finite abelian. Define the character

$$\alpha\colon \mathrm{Gal}_K \xrightarrow{\rho_E} G_E \subseteq \mathcal{G} \to \mathcal{G}/B.$$

We take B with $B \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ minimal so that $\alpha(\mathrm{Gal}(\overline{K}/K^{\mathrm{cyc}})) = 1$.
(These can be worked out using a finite number of precomputed modular curves.)
We will have

$$G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = B \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}).$$

Idea for computing G_E

In the previous slide, there was a character $\alpha\colon \mathrm{Gal}_K \to \mathcal{G}/B$ with $\alpha(\mathrm{Gal}(\overline{K}/K^{\mathrm{cyc}})) = 1$. There is a unique homomorphism

$$\gamma\colon \chi_{\mathrm{cyc}}(\mathrm{Gal}_K) \to \mathcal{G}/B$$

satisfying $\alpha(\sigma) = \gamma(\chi_{\mathrm{cyc}}(\sigma)^{-1})$ for all $\sigma \in \mathrm{Gal}_K$. We have

$$G_E = \{g \in \mathcal{G} : \det g \in \chi_{\mathrm{cyc}}(\mathrm{Gal}_K),\ g \cdot B = \gamma(\det g)\}.$$

Concluding remark: Our approach to computing the groups G_E, for non-CM E/K excluding a finite number of j-invariants, is to show that they are of a very special form (moreover, we are putting them in "families").

This is progress towards "Mazur's Program B" which asks for a classification of the possible groups $G_E = \rho_E(\mathrm{Gal}_K)$ for each K.

Extra slides on modular curves

Let $\mathcal{G}$ be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that contains $-I$. The group gives rise to a modular curve $X_{\mathcal{G}}$ defined over a number field L.
We will now give some ideas on how to compute a model of $X_{\mathcal{G}}$.

Our approach to compute models is via modular forms. Fix an integer $N \geq 1$. For an integer $k \geq 0$, consider

$$M_k(\Gamma(N), \mathbb{Q}(\zeta_N));$$

the space of weight k modular forms on $\Gamma(N)$ with q-expansion having coefficients in $\mathbb{Q}(\zeta_N)$.
There is a right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ such that

- $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts via the natural $\mathrm{SL}_2(\mathbb{Z})$-action,
- $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ acts by acting on Fourier coefficients via $\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, where $\sigma_d(\zeta_N) = \zeta_N^d$.

For our group $\mathcal{G}$, let N be the level of $\mathcal{G}$ and let $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the image of $\mathcal{G}$ modulo N. For each $k \geq 0$, we define the L-vector space

$$M_{k,\mathcal{G}} := M_k(\Gamma(N), \mathbb{Q}(\zeta_N))^G.$$

We have $L = \mathbb{Q}(\zeta_N)^{\det G}$ and

$$M_{k,\mathcal{G}} \otimes_L \mathbb{C} = M_k(\Gamma_{\mathcal{G}}),$$

where $\Gamma_{\mathcal{G}}$ is the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices whose image modulo N lies in G. Here is an ad hoc definition of $X_{\mathcal{G}}/L$:

$$X_{\mathcal{G}} = \mathrm{Proj}\left(\bigoplus_{k\geq 0} M_{k,\mathcal{G}}\right).$$

(We have $X_{\mathcal{G}}(\mathbb{C}) \cong \Gamma_{\mathcal{G}}\backslash\mathbb{H}^*$, and $\pi_{\mathcal{G}}$ corresponds to the quotient map $\Gamma_{\mathcal{G}}\backslash\mathbb{H}^* \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$.)

$$X_{\mathcal{G}} = \operatorname{Proj}\left(\bigoplus_{k\geq 0} M_{k,\mathcal{G}}\right).$$

- Take $k \in \{2, 4, 6\}$ minimal so that $M_{k,\mathcal{G}}$ gives an embedding of $X_{\mathcal{G}}$ into projective space.
- We can compute explicit generators of the L-vector space $M_{k,\mathcal{G}}$ by using sums and products of weight 1 Eisenstein series on $\Gamma(N)$.
- By consider vanishing conditions at cusps, find a relatively small subspace V of $M_{k,\mathcal{G}}$ so that Riemann–Roch ensures an embedding

$$X_{\mathcal{G}} \hookrightarrow \mathbb{P}(V)$$

  defined over L.
- Look for enough relations to cut out the image using q-expansions.

Modular curve example

Let $\mathcal{G}$ be the open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level 13 whose image modulo 13 is

$$G := \langle \left(\begin{smallmatrix} 1 & 2 \\ 4 & 1 \end{smallmatrix}\right) \rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/13\mathbb{Z}).$$

We have $G \cong \mathbb{F}_{13^2}^\times$. Since $\det(\mathcal{G}) = \widehat{\mathbb{Z}}^\times$, the modular curve $X_\mathcal{G}$ is defined over $\mathbb{Q}$. The following is code to compute a model of $X_\mathcal{G}$:

```
> M:=CreateModularCurveRec(13,[[1,2,4,1]]);
> M`genus;
8
> time X:=FindModelOfXG(M,15);
Time: 2.040[r]
```

The model computed in this case is the canonical model $X_\mathcal{G} \hookrightarrow \mathbb{P}^7_\mathbb{Q}$. The curve is cut out by several homogeneous polynomials in $\mathbb{Q}[x_1, \ldots, x_8]$ of degree 2.

```
[
    -x[1]^2 - x[1]*x[2] - x[1]*x[3] + x[1]*x[4] + x[1]*x[5] + x[2]^2 + 2*x[2]*x[3] + x[2]*x[6] - x[2]*x[7] + 2*x[2]*x[8] + x[3]^2 +
        x[3]*x[4] - x[3]*x[5] + x[3]*x[7] + 2*x[3]*x[8] + x[4]^2 - x[4]*x[6] + 2*x[4]*x[7] + x[5]*x[7] - 2*x[5]*x[8] + x[6]*x[7] -
        x[6]*x[8],
    -x[1]*x[2] - x[1]*x[3] + x[1]*x[4] + x[1]*x[5] - x[1]*x[6] + x[2]^2 + x[2]*x[3] - x[2]*x[4] - x[2]*x[5] + x[2]*x[6] + x[2]*x[8]
        + x[3]^2 - x[3]*x[4] - x[3]*x[5] + x[3]*x[6] - x[3]*x[7] + 2*x[3]*x[8] + x[4]*x[5] - x[4]*x[6] + x[4]*x[7] - 2*x[4]*x[8] -
        x[5]*x[8] + x[6]*x[8],
    -x[1]^2 + x[1]*x[2] + x[1]*x[3] + x[1]*x[4] - x[1]*x[6] + 2*x[1]*x[8] - x[2]^2 - x[2]*x[3] - x[2]*x[7] - 2*x[2]*x[8] - x[3]*x[4]
        + x[3]*x[6] - x[3]*x[7] - x[4]^2 + x[4]*x[5] + x[4]*x[6] - x[5]*x[6] + x[5]*x[7] - x[5]*x[8] - x[6]*x[7] + x[6]*x[8] -
        x[7]*x[8] - x[8]^2,
    -x[1]^2 - 2*x[1]*x[5] - x[1]*x[7] + x[1]*x[8] + x[2]*x[3] - x[2]*x[4] + 2*x[2]*x[6] - 3*x[2]*x[7] + x[2]*x[8] + x[3]^2 +
        2*x[3]*x[4] + x[3]*x[8] + x[4]^2 + x[4]*x[5] + x[4]*x[6] + x[4]*x[8] - x[5]^2 - x[5]*x[6] - x[6]^2 + x[6]*x[7] - x[6]*x[8] -
        x[7]^2 - x[7]*x[8],
    -x[1]*x[3] + x[1]*x[6] - x[1]*x[7] + x[1]*x[8] + x[3]^2 + 2*x[3]*x[4] - x[3]*x[5] - x[3]*x[7] + 3*x[3]*x[8] + x[4]^2 - x[4]*x[5]
        - x[4]*x[6] + x[4]*x[7] + x[5]^2 - x[5]*x[6] + x[5]*x[7] + x[6]^2 - x[6]*x[7] + x[7]*x[8] + x[8]^2,
    -x[1]*x[2] + 2*x[1]*x[4] + x[1]*x[6] + x[1]*x[7] + 2*x[2]*x[3] + 3*x[2]*x[4] - 2*x[2]*x[5] - x[2]*x[6] + x[3]*x[4] - 2*x[3]*x[5]
        - x[3]*x[6] - x[3]*x[8] + x[4]^2 - 2*x[4]*x[5] - 2*x[4]*x[6] + x[4]*x[7] + x[4]*x[8] + x[5]^2 + 2*x[5]*x[6] - x[5]*x[7] +
        x[6]^2 + x[6]*x[7],
    x[1]^2 + x[1]*x[2] + x[1]*x[5] + 2*x[1]*x[7] - 3*x[1]*x[8] + 2*x[2]^2 - 3*x[2]*x[4] - x[2]*x[5] + 2*x[2]*x[7] - 2*x[2]*x[8] -
        x[3]^2 - x[3]*x[4] - x[3]*x[5] + x[3]*x[7] - 2*x[3]*x[8] + x[4]^2 + x[4]*x[5] - x[4]*x[8] - x[5]*x[8],
    -x[1]*x[2] + x[1]*x[5] - x[1]*x[7] + 2*x[1]*x[8] + x[2]^2 - x[2]*x[3] - x[2]*x[4] - 2*x[2]*x[6] + x[2]*x[7] + 2*x[2]*x[8] +
        x[3]*x[5] - x[3]*x[7] + 2*x[3]*x[8] - x[4]^2 + 2*x[4]*x[5] + 2*x[4]*x[6] - x[4]*x[7] - x[4]*x[8] - x[5]^2 - x[5]*x[6] -
        x[5]*x[7] - 2*x[6]*x[7],
    -x[1]^2 - x[1]*x[2] - x[1]*x[3] - x[1]*x[5] - x[1]*x[6] - x[1]*x[7] + x[2]*x[3] + x[2]*x[5] + 2*x[2]*x[6] - x[2]*x[7] +
        x[2]*x[8] + x[3]^2 + 2*x[3]*x[5] + x[3]*x[6] + x[3]*x[7] + 2*x[3]*x[8] + x[4]^2 + x[4]*x[5] - 2*x[4]*x[6] + 2*x[4]*x[7] -
        x[5]^2 + x[5]*x[6] - x[5]*x[7] + 2*x[5]*x[8] + x[6]*x[7] + 2*x[6]*x[8],
    -x[1]^2 + 3*x[1]*x[4] + x[1]*x[5] - 3*x[1]*x[6] + x[1]*x[7] + x[1]*x[8] + x[2]*x[4] + x[2]*x[5] - x[2]*x[6] + x[2]*x[7] +
        x[2]*x[8] + x[3]^2 - x[3]*x[5] - 2*x[4]^2 + x[4]*x[6] - x[4]*x[8] - x[5]^2 - x[5]*x[7] - 2*x[5]*x[8] - x[6]*x[7] - x[7]*x[8]
        - x[8]^2,
    -x[1]^2 + 2*x[1]*x[2] + x[1]*x[3] + x[1]*x[5] - x[1]*x[6] + x[2]^2 - 2*x[2]*x[4] + x[2]*x[7] - x[3]*x[5] + 2*x[3]*x[7] - x[4]^2
        + x[4]*x[5] + 3*x[4]*x[6] - 2*x[4]*x[7] + 2*x[4]*x[8] - x[5]^2 - x[5]*x[6] - x[5]*x[7] - 3*x[5]*x[8] - x[6]^2 + x[6]*x[7] -
        2*x[6]*x[8] - 2*x[7]^2 + x[7]*x[8] + x[8]^2,
    -x[1]*x[2] - x[1]*x[3] + x[1]*x[4] + x[1]*x[5] - 2*x[1]*x[6] + x[1]*x[7] - 2*x[1]*x[8] - 2*x[2]*x[3] - 2*x[2]*x[4] + x[2]*x[5] -
        x[2]*x[7] - x[2]*x[8] + 2*x[3]*x[4] + x[3]*x[5] - x[3]*x[6] + x[3]*x[7] - x[3]*x[8] + x[4]^2 + x[4]*x[5] + x[4]*x[6] -
        x[5]^2 - x[5]*x[6] - x[5]*x[8] - x[6]^2 + x[6]*x[7] - x[6]*x[8] - x[7]^2 - x[7]*x[8],
    -x[1]^2 + x[1]*x[3] + 2*x[1]*x[4] + x[1]*x[5] + 2*x[1]*x[6] + x[1]*x[7] + x[2]*x[3] + x[2]*x[5] + 3*x[2]*x[6] + 2*x[2]*x[7] -
        2*x[2]*x[8] - x[3]^2 - 2*x[3]*x[5] + 2*x[3]*x[6] + x[3]*x[7] - 2*x[4]*x[6] + 2*x[4]*x[7] + x[4]*x[8] - x[5]*x[6] - x[5]*x[8]
        + x[6]^2 - x[6]*x[7] + x[6]*x[8] + x[7]*x[8],
    x[1]^2 + x[1]*x[2] + x[1]*x[4] + 3*x[1]*x[5] - 3*x[1]*x[6] + 2*x[1]*x[7] - x[2]^2 + 2*x[2]*x[3] - x[2]*x[5] - x[2]*x[7] -
        x[2]*x[8] + x[3]^2 - 2*x[3]*x[4] - 2*x[3]*x[6] + x[3]*x[7] - x[4]*x[6] - x[4]*x[7] - x[4]*x[8] - x[5]*x[6] - x[5]*x[8] -
        x[6]^2 + x[6]*x[7],
    2*x[1]^2 + 4*x[1]*x[3] + 3*x[1]*x[4] + 3*x[1]*x[7] - x[2]^2 - x[2]*x[4] - x[2]*x[5] + 3*x[2]*x[6] - 2*x[2]*x[7] - x[2]*x[8] +
        4*x[3]^2 + 3*x[3]*x[4] + 3*x[3]*x[6] + x[3]*x[7] + x[4]^2 + x[4]*x[5] + x[4]*x[7] + x[4]*x[8] + x[5]^2 + x[5]*x[6] +
        x[6]*x[7] - x[6]*x[8] + x[7]*x[8] + x[8]^2
]
```

Modular example continued

The model computed in this case is the canonical model $X_{\mathcal{G}} \hookrightarrow \mathbb{P}^7_{\mathbb{Q}}$. The curve is cut out by several homogeneous polynomials in $\mathbb{Q}[x_1, \ldots, x_8]$ of degree 2.

- These equations are very nice! (seriously)
- All of the coefficients are integers with absolute value at most 4.
- We also gave more equations than needed; they actually give a model for $X_{\mathcal{G}}$ as a smooth projective curve over $\operatorname{Spec} \mathbb{Z}[1/13]$.