Applications to Cryptography of the Construction of Curves from Modular Invariants

Jesse Franklin

University of Vermont

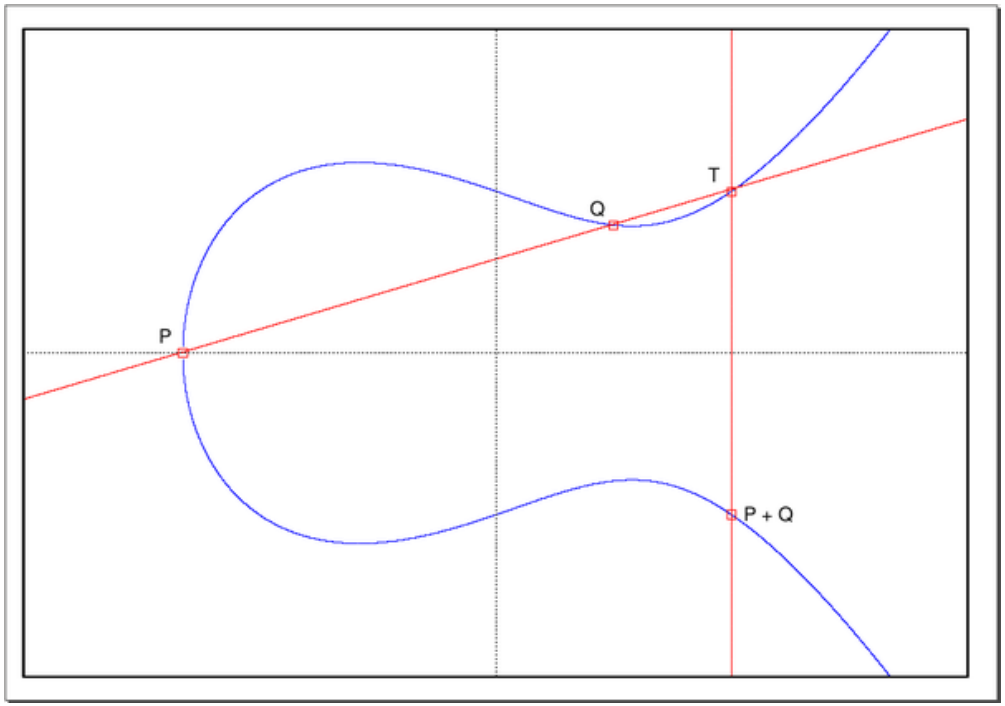
July 19, 2021

Our application to cyrptography

We wish to compute, via modular invariants, certain characteristics of a moduli space of elliptic curves with a known number of points. Currently the best method for computing these elliptic curves is by writing down an arbitrary elliptic curve equation and checking by hand whether it has the right number of points. The use of such curves is instrumental in cryptographic applications, but this discussion focuses only on the technique we will use to parameterize such elliptic curves.

Modular curves: moduli spaces of elliptic curves with extra information

The important part of elliptic curve theory for cyrptography is the group structure on an elliptic curve depicted in the figure:



A modular curve is a moduli (parameter) space of equivalence classes of elliptic curves equipped with some amount of information about this group law.

What is a modular curve?

The action of the group $SL_2(\mathbb{Z}) = \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, \ \det\gamma = 1\}$ on the upper half of the complex plane $\mathcal{H} = \{z \in \mathbb{C} : \Im z \geq 0\}$ quotients $\mathcal{H}$ into crudely speaking, a g-holed torus whose points are classes of elliptic curves which share the same group structure. In particular the congruence subgroup

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv 0 \pmod{N}\} \subset SL_2(\mathbb{Z})$$

is a covering space whose points are elliptic curves with a known number of points. This is the space we wish on which we wish to compute modular invariants.

Modular forms

For $k \in \mathbb{Z}$, a function $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight k if

1. f is holomorphic on $\mathcal{H}$ and at ∞
   and
2. for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and $z \in \mathcal{H}$ we have that

$$f(\gamma z) = f(\frac{az+b}{cz+d}) = (cz+d)^k f(z).$$

Modular forms are a graded ring $\mathcal{M}(SL_2(\mathbb{Z})) = \oplus_1^\infty \mathcal{M}_k(SL_2(\mathbb{Z}))$ with an ideal of forms called cusp forms denoted $\mathcal{S}(SL_2(\mathbb{Z}))$ with the analogous graded structure, and these definitions extend to congruence subgroups in the obvious way.
If $f \in \mathcal{M}_k(\Gamma)$ is a modular form of weight k for $\Gamma \subset SL_2(\mathbb{Z})$ a congruence subgroup, f has a Fourier expansion

$$f(z) = \sum_{\mathbb{N}} a_n(f) e^{2\pi i z}$$

and we say f is a cusp form if $a_0 = 0$.

Modular invariants part 1

To write a canonical basis for the space of cusp forms is in general a hard problem, but the solution to which gives modular invariants which let parameterize a space of the kind of elliptic curves we are concerned with.
We do this with the use of Hecke operators T_p on the space of cusp forms in the following way:
for $f(z) = \sum_{\mathbb{N}} a_n e^{2\pi i z} \in \mathcal{M}_k(\Gamma_0(N))$, define

$$T_p f(z) = \sum_{\mathbb{N}} (a_{pn} + p^{k-1} a_{n/p}) e^{2\pi i z}.$$

Hecke operators are themselves a ring $\mathbb{T}(k, N)$, act on the space of cusp forms $S_k(\Gamma_0(N))$, and with some arithmetic we have an isomorphism of algebras

$$\mathbb{T}(k, N) \otimes \mathbb{Q} \cong S_k(\Gamma_0(N), \mathbb{Q}).$$

Modular Invariants part 2

We can use Sage to compute not only the Hecke algebra, characteristic polynomials for operators $T_n \in \mathbb{T}(k, N)$ but also whether those polynomials are irreducible. We use this for the follow construction:
With an isomorphism of fields

$$\mathbb{T}(k, N) \cong S_k(\Gamma_0(N), \mathbb{Q}) \cong \mathbb{Q}[T_n]/(a(x)),$$

where $T_n \in \mathbb{T}(k, N)$ generates the Hecke algebra and $a(x)$ is its associated, irreducible, characteristic polynomial, we can compute the Galois group over $\mathbb{Q}$ of this field extension.

Modular Invariants part 3: Galois

With the Eichler-Shimura relation, which gives us a correspondence between Hecke operators and Galois representations, and the identification above we get:

1. a finite Galois extension of $\mathbb{Q}$ with a basis (i.e. a friendly number field)
2. elements of the Galois as matrices over that basis and
3. the trace of the Galois representation for interesting Galois elements

That allows us to determine the Hecke operator's eigenvalues and therefore the modular invariants of this operator. For really big primes p we care about those T_p for cryptography.