THE KLEIN QUARTIC

Most of this is based off of Noam Elkies' article on the Klein quartic, "The Klein Quartic in Number Theory".

1. The Klein quartic as a Riemann surface

The Klein quartic X is a projective curve in $\mathbf{P}^2(\mathbf{C})$ cut out by

$$x^3y + y^3z + z^3x = 0.$$

This is a compact Riemann surface of genus three, and in fact has 168 automorphisms.

Let's quickly think about these automorphisms. First, there are two obvious types of automorphisms:

- We can cyclically permute the variables, so there is a copy of $\mathbf{Z}/3\mathbf{Z}$ in $\mathrm{Aut}(\mathrm{X})$ generated by an element A.
- A bit less obvious: fix a primitive 7th root of unit ζ. Then applying

  $$\mathrm{B} = \begin{pmatrix} \zeta^4 & & \\ & \zeta^2 & \\ & & \zeta \end{pmatrix}$$

  to the vector (x, y, z) we obtain an order seven automorphism.

These first two generators satisfy $\mathrm{B}^4 = \mathrm{ABA}^{-1}$. Thus they generate a semidirect product of $\mathbf{Z}/3\mathbf{Z}$ and $\mathbf{Z}/7\mathbf{Z}$ of order 21.

There is also a highly non-obvious involution on X, given by applying

$$\mathrm{C} = -\frac{1}{\sqrt{-7}} \begin{pmatrix} \zeta - \zeta^6 & \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 \\ \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 & \zeta - \zeta^6 \\ \zeta^4 - \zeta^3 & \zeta - \zeta^6 & \zeta^2 - \zeta^5 \end{pmatrix}.$$

Modulo the scaling factor, this is the Fourier transform on the space of odd functions $\mathbf{F}_7 \to \mathbf{C}$.

The group of automorphisms generated by $\langle \mathrm{A}, \mathrm{B}, \mathrm{C} \rangle$ is now actually quite large, as all the 49 elements

$$\mathrm{B}^a \mathrm{C} \mathrm{B}^b$$

for $a, b \in [0, 6]$ are in fact distinct automorphisms. In fact, this gives an explicit presentation of the unique simple group of order 168, $\mathrm{PSL}_2(\mathbf{F}_7)$.

This is the largest possible number of automorphisms for this genus, meeting the Hurwitz bound.

Proposition 1.1. Let X be a compact Riemann surface of genus $g \geq 2$. Then the group $\mathrm{Aut}(X)$ of orientation-preserving conformal automorphisms has order at most
$$|\mathrm{Aut}(X)| \leq 84(g-1).$$

Sketch. Take X and set $G = \mathrm{Aut}(X)$. The orbit space X/G has an induced complex structure from X, which in fact makes X/G a Riemann surface. The map
$$X \to X/G$$
is a branched covering, with finitely many ramification points (say k of them).

Let g' be the genus of X/G. Riemann-Hurwitz tells us
$$2g - 2 = |G| \cdot \left(2g_0 - 2 + \sum_{i \leq k} 1 - \frac{1}{e_i}\right).$$

The ramification indices at a ramification point are the orders of the stabilizers of that orbit. The number of preimages f_i of a ramification point then satisfies $e_i f_i = |G|$ by orbit-stabliizer.

We now need some casework. If $g_0 \geq 2$, then we get $2g - 2 \geq 2|G|$ so $|G| \leq g - 1$ and cannot be very large. In particular, the upper bound will want $g_0 = 0$. Also, if we have many ramification points (say ≥ 5) even if $g_0 = 0$ then we again get a good bound $|G| \leq 4(g-1)$.

One can argue the least number of ramification points is 3 (χ cannot be negative, so if $k \leq 2$ there is no hope of making $-2 + \sum_{i \leq k} 1 - \frac{1}{e_i}$ positive), and then minimizing $3 - \frac{1}{e_1} - \frac{1}{e_2} - \frac{1}{e_3}$ we see the minimum is at $(2, 3, 7)$. The corresponding bound is
$$2g - 2 \geq |G| \cdot \left(\frac{1}{42}\right)$$
so $84(g-1) \geq |G|$. □

A conceptual argument can also be given as follows. By uniformization, we can see X is covered by $\mathbb{H}$. The conformal maps on X are induced by orientation-preserving automorphisms of $\mathbb{H}$, so we want to maximize these. By Gauss-Bonnet, we see from the fact that there is no boundary and that the surface is hyperbolic that
$$\mathrm{Area}(X) = -2\pi\chi(X) = 4\pi(g-1).$$

We imagine X as coming from folding up a subset of $\mathbb{H}$ using the covering map, and that this subset is tiled from a fundamental domain D by applying automorphisms on $\mathbb{H}$. To get the most automorphisms, we want D to be as small as possible. If D is a triangle with angles π/e_i, then we wish to minimize

$$\mathrm{Area(D)} = \pi\left(1 - \sum \frac{1}{e_i}\right).$$

This is achieved for $(2, 3, 7)$, giving

$$\mathrm{Area(X)}/\mathrm{Area(D)} \leq 168(g-1).$$

This overcounts by a factor of two, because on X some of the automorphisms can be orientation-reversing. If we account for this, we get the actual bound.

In fact, this fact about maximality of automorphisms uniquely characterizes the Klein quartic.

> THEOREM 1.2. There is a unique genus 3 Riemann surface X with 168 automorphisms. We can equivalently characterize such an X by it admitting a branched cover
>
> $$\mathrm{X} \to \mathbf{P}^1$$
>
> which is ramified at three points with indices 2,3, and 7.

2. As a modular curve

The previous criterion gives us an easy way to check if a curve is the Klein quartic over $\mathbf{C}$. However, in defining X we actually did so over $\mathbf{Q}$.

Modular curves are constructed as quotients of the upper half plane $\mathbb{H}$ by congruence subgroups. Namely, taking the usual action of linear fractional transformations

$$z \mapsto \frac{az+b}{cz+d}$$

we obtain an action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathbb{H}$. A subgroup $\Gamma \leq \mathrm{PSL}_2(\mathbf{Z})$ is called a *congruence subgroup* if it contains $\Gamma(N)$ for some N, the subgroup

$$\Gamma(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : a \equiv d \equiv 1 \pmod N, b, c \equiv 0 \pmod N\}.$$

Or, more simply, the kernel of the surjective map

$$\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}).$$

We can use the chinese remainder theorem to see the map is surjective, so $\mathrm{SL}_2(\mathbf{Z})/\Gamma(N) \simeq \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ which easily lets us compute the index.

DEFINITION 2.1. The affine modular curve $\mathrm{Y}(N)$ is the quotient $\mathbb{H}/\Gamma(N)$. The compactified modular curve is

$$\mathrm{X}(N) := \mathbb{H}^*/\Gamma(N)$$

where we add the cusps $\mathbf{Q} \cup \infty = \mathbf{P}^1(\mathbf{Q})$ to $\mathbb{H}$.

EXAMPLE 2.2. The curve $\mathrm{X}(1)$ is $\mathbf{CP}^1$.

Observe that $\mathrm{Aut}(\mathrm{X})$ is a simple group of order 168, so in particular it is isomorphic to $\mathrm{PSL}_2(\mathbf{F}_7)$. The previous discussion shows that

$$\Gamma(1)/\Gamma(7) \simeq \mathrm{SL}_2(\mathbf{F}_7).$$

Observing the matrices $\pm\mathrm{I}$ induce the same automorphism, this shows that over $\mathbf{C}$ the modular curve $\mathrm{X}(7)$ has an action by $\mathrm{G} = \mathrm{PSL}_2(\mathbf{F}_7)$.

COROLLARY 2.3. Over $\mathbf{C}$, the Klein quartic is isomorphic to $\mathrm{X}(7)$ as a Riemann surface.

Proof. We actually have several ways to do this at this point. It is easy to check that $\mathrm{X}(7)$ has at least 168 distinct automorphism, so by our previous results we just need to show it has genus 3.

The covering

$$\mathrm{X}(7) \to \mathrm{X}(1) \simeq \mathbf{P}^1$$

is Galois, with Galois group $\mathrm{G} = \mathrm{PSL}_2(\mathbf{F}_7)$. Applying Riemann-Hurwitz,

$$\chi(\mathrm{X}(7)) = 168\chi(\mathbf{P}^1) - \sum_p (e_p - 1)$$

where the sum is over the ramification points $p \in \mathrm{X}$. Since the cover is Galois, the ramification indices of preimages of a point in $\mathbf{P}^1$ are the same. Using the standard description of a fundamental domain for $\mathrm{X}(1)$, the potential ramification points are $[i]$, $[\rho]$ (ρ is $e^{2\pi i/3}$) and $[\infty]$. The ramification indices here are $2, 3$, and 7 respectively, computed by the size of stabilizer of the G-action at that point.

Note that just the ramification computation is enough to see we get X. $\square$

In fact, this isomorphism even descends over $\mathbf{Q}$ when we use the $\mathbf{Q}$-scheme $x^3y + y^3z + z^3x = 0$ for X.

THEOREM 2.4. Over $\mathbf{Q}$, the modular curve $\mathrm{X}(7)$ parameterizes elliptic curves with level N structure, i.e. an isomorphism

$$\mathrm{E}[N] \simeq \mathbf{Z}/7\mathbf{Z} \times \mu_7$$

as Galois modules.

REMARK 2.5. This is a special feature over $\mathbf{Q}$ that we need to think about the Galois action. The Weil pairing identifies $\Lambda^2\mathrm{E}[N] \simeq \mu_N$, so we actually have many choices of level structure. This is the one which is the simplest guess, and matches up with the Klein quartic.

THEOREM 2.6. Over $\mathbf{Q}$, $\mathrm{X}(7)$ is isomorphic to $x^3y + y^3z + z^3x = 0$.

The basic idea is that we can find some explicit weight 2 modular forms for $\Gamma(7)$, or functions f so that

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 f(\tau)$$

for matrices in $\Gamma(7)$. Equivalently, $f(\tau)\mathrm{d}\tau$ is $\Gamma(7)$-invariant, so these will correspond to sections in $\mathrm{H}^0(\mathrm{X}(7), \Omega^1)$ (or differential forms). In particular, we find three such global sections which generate Ω^1, which then defines a map

$$\mathrm{X}(7) \to \mathbf{P}^2.$$

The modular forms $x(\tau), y(\tau)$ and $z(\tau)$ satisfy exactly the relation of the Klein quartic, and moreover we can check this is an embedding. It turns out this strategy also descends to $\mathbf{Q}$.

Explicitly, these modular forms take the form

$$\sum_{\beta \in \mathbf{Z}[\frac{-1+\sqrt{-7}}{2}]} \mathrm{Re}(\beta) q^{\beta\bar{\beta}/7}$$

where $q = e^{2\pi i \tau}$ and the sum runs over β congruent modulo $\sqrt{-7}$ to one of $1, 2, 4$.

REMARK 2.7. To really descend to $\mathbf{Q}$ we need to check the moduli problem matches. To do this one can write down a generic elliptic curve attached to a non-cusp point $(x : y : z)$ on X, and then compute the Galois module $\mathrm{E}[7]$ for this curve and deduce it is $\mathbf{Z}/7\mathbf{Z} \times \mu_7$.

3. HEEGNER NUMBERS

The Stark-Heegner theorem is the following result.

THEOREM 3.1. The only imaginary quadratic fields $\mathbf{Q}(\sqrt{-D})$ whose rings of integers are PIDs occur when
$$D = 3, 4, 7, 8, 11, 19, 43, 67, 163.$$

The basic idea of the argument is that the existence of such D implies the existence of a special elliptic curve. This follows from the theory of complex multiplication, which I'll summarize briefly.

DEFINITION 3.2. Let $\mathrm{E}/\mathbf{C}$ be an elliptic curve. Then E has CM if the endomorphism ring $\mathrm{End}(\mathbf{Z})$ is larger than $\mathbf{Z}$.

LEMMA 3.3. Let $E/\mathbf{C}$ be an elliptic curve. Then $\mathrm{End}(E) \neq \mathbf{Z}$ if and only if $\mathrm{End}^0(E) = K/\mathbf{Q}$ is an imaginary quadratic field. In this case, $\mathrm{End}(E) = \mathcal{O} \subset K$ is an order in K.

Proof. We may write $\mathrm{End}(E) = \{\lambda \in \mathbf{C} : \lambda(\Lambda) \subseteq \Lambda\}$. Now assuming $\Lambda = \omega_1\mathbf{Z} \oplus \omega_2\mathbf{Z}$, to have $\lambda(\Lambda) \subset \Lambda$ means that $\lambda\omega_1 = a\omega_1 + b\omega_2$ and $\lambda\omega_2 = c\omega_1 + d\omega_2$ for $a, b, c, d \in \mathbf{Z}$. Then if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, using the regular action we have $z = \omega_1/\omega_2$ which satisfies
$$z = \frac{\lambda\omega_1}{\lambda\omega_2} = \gamma \cdot z.$$

If $\lambda \notin \mathbf{Z}$, or E has CM, then b and c are nonzero, so $\mathbf{Q}(z)$ is an imaginary quadratic field by using the (quadratic) relation $z = \gamma \cdot z$. From the realizations of $\mathrm{End}(E)$ and $\mathrm{End}^0(E)$ in terms of Λ, we see $\mathrm{End}^0(E) = \mathbf{Q}(z) = K$ is an imaginary quadratic field. It is clear $\mathrm{End}(E)$ needs to be an order in K, since it is a ring which is a full and finitely generated $\mathbf{Z}$-submodule of K. □

Elliptic curves with CM can always be defined over $\bar{\mathbf{Q}}$, even K^{ab}.

In fact, the set of isomorphism classes over $\bar{\mathbf{Q}}$ of elliptic curves with CM by a particular order $\mathcal{O}$ is the same as the class group of that order.

THEOREM 3.4. Let $\mathrm{E}/\mathbf{C}$ be an elliptic curve with CM by $\mathcal{O}_K$. Then $[\mathbf{Q}(j(\mathrm{E})) : \mathbf{Q}] \leq |\mathrm{Cl}(\mathcal{O}_K)|$.

Proof. Since E has CM we can define it over $\bar{\mathbf{Q}}$. Write down the Weierstrass form of E, and apply any automorphism σ of $\bar{\mathbf{Q}}$ and note

$$j(\mathrm{E}^\sigma) = j(\mathrm{E})^\sigma.$$

This also induces an equivalence $\mathrm{End}(\mathrm{E}) \simeq \mathrm{End}(\mathrm{E}^\sigma)$, so we again get an elliptic curve with CM. But there are at most $|\mathrm{Cl}(\mathcal{O}_K)|$ such isomorphism classes, so $j(\mathrm{E})^\sigma$ can take on at most $|\mathrm{Cl}(\mathcal{O}_K)|$ different values. This implies it is algebraic and also bounds the degree of $\mathbf{Q}(j(\mathrm{E}))$. □

In particular, the relevant fact for us is that we can always construct an elliptic curve with CM by $\mathcal{O}_K$, and in the situation that K has class number one then there is a unique such curve up to $\bar{\mathbf{Q}}$-isomorphism and $j(\mathrm{E}) \in \mathbf{Q}$. In fact $j(\mathrm{E})$ must be an integer, as all j-invariants of CM elliptic curves are algebraic integers.

Idea. Reduce the class number one problem to finding points of a modular curve with integral j invariant.

We will need more conditions to actually make the number of such points finite.

Consider an imaginary quadratic field $K = \mathbf{Q}(\sqrt{-D})$, and assume it has class number one. Then if $D > 28$, the prime 7 will actually remain prime. Otherwise, there is a prime (α) above 7 (it is principal by the class number assumption) and $\mathbf{N}(\alpha) = 7$. But when D is large there cannot be a $\sqrt{-D}$ or $\frac{1+\sqrt{-D}}{2}$ component, which forces α to be an integer which is impossible given the norm condition.

Thus, we may assume 7 is inert.

> Lemma 3.5. If $D > 28$ and $K = \mathbf{Q}(\sqrt{-D})$ has class number one, there is an elliptic curve over $\mathbf{Q}$ with CM by $\mathcal{O}_K$ (which is unique up to $\bar{\mathbf{Q}}$-isomorphism). The action of $\mathcal{O}_K$ on E[7] gives it the structure of a 1-dimensional vector space over $\mathbf{F}_{49}$ (which respects the $\mathrm{G}_{\mathbf{Q}}$-action).

Proof. By the class number one condition, we know there must exist a unique isomorphism class over $\bar{\mathbf{Q}}$ of elliptic curves with CM by $\mathcal{O}_K$. Moreover, the j-invariant is an integer, so there is an elliptic curve over $\mathbf{Q}$ which lands in this isomorphism class over $\bar{\mathbf{Q}}$ (you can write a curve in Weierstrass form from the specified j-invariant, which completely classifies the isomorphism class over $\bar{\mathbf{Q}}$).

For the second statement, on E[7] the $\mathcal{O}_K$-action by endomorphisms becomes an action of $\mathcal{O}_K/7 \simeq \mathbf{F}_{49}$ (note that 7 in End(E) actually corresponds to the multiplication by 7 endomorphism). But this is now a field, giving it a vector space structure. These endomorphisms must also respect the Galois action. □

This extra structure on E[7] is exactly what we need, and where the Klein quartic will come into play. The Klein quartic gives us explicit equations to describe X(7). We will need a variant of X(7) to capture this slightly different version of level structure.

> Definition 3.6. The 2-Sylow subgroup of $\mathrm{PSL}_2(\mathbf{F}_7)$ is isomorphic to the 8-element dihedral group D_8, so we will denote it by this.
>
> Let X denote the Klein quartic, and set $\mathrm{X}_{\mathrm{ns}}(7) := \mathrm{X}/\mathrm{D}_8$.

> Theorem 3.7. The curve $\mathrm{X}_{\mathrm{ns}}(7)$ is defined over $\mathbf{Q}$ and parameterizes elliptic curves such that the Galois action E[7] is contained in the normalizer of a nonsplit Cartan in $\mathrm{GL}_2(\mathbf{F}_7)$. A non-split Cartan subgroup is a subgroup of the form
>
> $$\mathrm{H} = \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} : a^2 - \epsilon b^2 \neq 0 \right\}$$
>
> where $\epsilon \in \mathbf{F}_7^\times$ is a nonsquare. Mapping to $\mathrm{PGL}_2(\mathbf{F}_7)$, this gives you a dihedral group (which is the relation).

To set up the next part of the argument, we will consider the following diagram.

$$\begin{tikzcd}
\mathrm{X} \arrow[r, "\simeq"] \arrow[d] & \mathrm{X}(7) \arrow[dd] \\
\mathrm{X}/S_4 \arrow[d] & \\
\mathrm{X}/D_8 \arrow[r, "\simeq"] \arrow[d] & \mathrm{X}_{\mathrm{ns}}(7) \arrow[d] \\
\mathrm{X}/\mathrm{PSL}_2(\mathbf{F}_7) \arrow[r, "\simeq"] & \mathrm{X}(1) = \mathbf{P}^1
\end{tikzcd}$$

On the right hand side, the maps forget level structure with the map to X(1) being the j-invariant. The idea is that we will produce points of $\mathrm{X}_n(7)$ with integral j-invariant, and then translate across this diagram to turn this into a diophantine equation with finitely many solutions.

The easiest step is to write down the map $j : \mathrm{X} \to \mathrm{X}(1) \simeq \mathbf{P}^1$ in terms of the coordinates x, y, z as a rational function of degree 168 (there is a simpler way to express it in terms of certain invariant polynomials coming from the representation theory of $\mathrm{PSL}_2(\mathbf{F}_7)$).

Our goal is to give an explicit rational parameter ϕ for X/D_8 along with the j map, so that we can write j in terms of this parameter and ask for rational solutions so $j \in \mathbf{Z}$.

This is done by first describing the genus zero curve X/S_4 as rationally parameterized by an explicit coordinate ψ on X. The j-function can also be explicitly given, describing the map $\mathrm{X}/S_4 \to \mathrm{X}/\mathrm{PSL}_2(\mathbf{F}_7) \simeq \mathrm{X}(1) = \mathbf{P}^1$. To do this one writes down the j function on $\mathrm{X}/\mathrm{PSL}_2(\mathbf{F}_7)$ as a degree 168 rational function, and then write j as a rational function of the coordinate ψ on X/S_4.

Then, we can describe X/D_8 as a degree 3 cover of X/S_4 (it will in fact be genus 0 again). This gives it a coordinate ϕ where we can write $\psi \in \mathbf{Q}(\phi)$. In total, we obtain in all its horrible glory that

$$j = 12^3 + 56^2\frac{(\phi-3)(2\phi^4 - 14\phi^3 + 21\phi^2 + 28\phi + 7)P^2(\phi)}{(\phi^3 - 7\phi^2 + 7\phi + 7)^7}$$

where $P(\phi) = (\phi^4 - 14\phi^2 + 56\phi + 21)(\phi^4 - 7\phi^3 + 14\phi^2 - 7\phi + 7)$.

THEOREM 3.8. The only imaginary quadratic fields $\mathbf{Q}(\sqrt{-D})$ whose rings of integers are PIDs occur when

$$D = 3, 4, 7, 8, 11, 19, 43, 67, 163.$$

Proof. As we have seen, once $D > 28$ we may assume 7 is inert and then produce an elliptic curve E with CM by $\mathcal{O}_K$ defined over $\mathbf{Q}$ with integer j-invariant. Moreover, we found that the Galois action on E[7] is compatible with a $\mathbf{F}_{49}$-vector space structure, which restricts us to $\mathbf{F}_{49}$-linear maps. This means that E gives a rational point of $\mathrm{X}_{\mathrm{ns}}(7)$ (in particular a $\mathbf{Z}[1/7]$-point which does not give cusps for $p \neq 7$) such that the j-invariant is an integer.

Now we can use the massive formula from earlier to solve the problem. Put $\phi = \frac{m}{n}$ with gcd one. Writing

$$j = \frac{A(m,n)}{B(m,n)}$$

we find that $\gcd(A(m,n), B(m,n)) | 56^7$ given $(m,n) = 1$. In particular,

$$(m^3 - 7m^2n + 7mn^2 + 7n^3) | 56.$$

It is now possible to find all possible solutions (m,n). Essentially, m/n needs to be a good rational approximation on the order of n^3 of a root α of $\phi^3 - 7\phi^2 + 7\phi + 7$, as $m^3 - 7m^2n + 7mn^2 + 7n^3$ is forced to be small. Any bound

$$|\alpha - m/n| > C_\alpha n^{-C'_\alpha}$$

where $C'_\alpha < 3$ suffices, and many exist (in this case 0.099 and 7/3). $\square$