Shimura curves

In the 60s, Shimura studied certain algebraic curves as analogues of classical modular curves in order to construct class fields of totally real number fields. These curves were later coined "Shimura curves" and vastly generalized by Deligne. We will take a tour of the rich geometry and arithmetic of Shimura curves. Along the way, we may encounter tessellations of disks, quaternion algebras, abelian surfaces, elliptic curves with CM, Hurwitz curves ... and the answer to life, the universe and everything.

This is a note I prepared for my first Trivial Notions talk at Harvard, Fall 2011. Our main sources are [1], [2], [3], [4] and [5].

[-] **Contents**

Briefly speaking, Shimura curves are simply one-dimensional Shimura varieties. I have accomplished my trivial notion task because I have told you a trivial notion. But obviously it does not help much if you do not know what the term Shimura varieties means. It only takes 5 chapters in Milne's notes in order to define them — not too bad — but initially Shimura invented them really because they are natural analogues of classical modular curves.

Review of Modular Curves ▲

Let $\mathcal{H}$ be the upper half plane. Then $\Gamma(1)=SL_2(\mathbb{Z})\subseteq SL_2(\mathbb{R})$ acts on $\mathcal{H}$ by Mobius transformations. For each complex number $z\in\mathcal{H}$, we can associate an elliptic curve $E_z=\mathbb{C}/\langle 1,z\rangle$. The endomorphism ring is given by $\mathrm{End}(E_z)\subseteq\{\alpha\in\mathbb{C}:\alpha\cdot\langle 1,z\rangle=\langle 1,z\rangle\}$, which is either $\mathbb{Z}$ or an order in some imaginary quadratic field $\mathbb{Q}(\tau)/\mathbb{Q}$. The latter case is rarer and is given the name *complex multiplication* (CM). Two such elliptic curves E_z and $E_{z'}$ are isomorphic if and only if z,z' lie in the same $\Gamma(1)$-orbit. Hence we have the following bijection.

Proposition 1 There is a natural bijection

$$\Gamma(1)\backslash\mathcal{H}\longleftrightarrow\{\text{elliptic curves } E/\mathbb{C}\}/\text{isomorphism}.$$

$\Gamma(1)\backslash\mathcal{H}$ can be identified with the fundamental set

$$\Omega=\{|z|>1,-1/2\le\mathrm{Re}\,z<1/2\}\cup\{|z|=1,-1/2\le\mathrm{Re}\,z\le 0\}.$$

The elliptic point i and $\rho=e^{2\pi i/3}$ have nontrivial stabilizer of order 2 and 3, which correspond to elliptic curves with complex multiplication by $\mathbb{Z}[i]$ and $\mathbb{Z}[\rho]$ and automorphisms groups of order 4 and 6. $\Gamma(1)\backslash\mathcal{H}$ can be viewed as the Riemann sphere with the north pole missing. By adding the cusp ∞, we get the compactification $X(1)=\Gamma(1)\backslash\mathcal{H}^*$. The cusp has the moduli interpretation as degenerate elliptic curves — nodal cubic curves.

Proposition 2 $X(1)$ is the coarse moduli space of complex elliptic curves and is isomorphic to $\mathbb{P}^1$ via the j-invariant.

Analogously, for the congruence subgroups $\Gamma(N)\subseteq\Gamma_1(N)\subseteq\Gamma_0(N)\subseteq\Gamma(1)$, where

- $\Gamma(N)=\begin{bmatrix}1&0\\0&1\end{bmatrix}\pmod N,$
- $\Gamma_1(N)=\begin{bmatrix}1&*\\0&1\end{bmatrix}\pmod N,$
- $\Gamma_0(N)=\begin{bmatrix}*&*\\0&*\end{bmatrix}\pmod N,$

Links

Chao Li's Homepage
Harvard University
Math Department
maTHμ

we get the compact Riemann surfaces $X(N) \to X_1(N) \to X_0(N) \to X(1)$ after adding cusps to the quotient $\Gamma\backslash\mathcal{H}$. These *classical modular curves*, which date back to Klein and Fricke in the 19th century, also play an important role in the modern proof of Fermat's last theorem. They are coverings of $X(1)$ and are coarse moduli spaces of elliptic curves with additional torsion data:

- $X_0(N)$ parametrizes elliptic curves with a N-cyclic subgroup.
- $X_1(N)$ parametrizes elliptic curves with a point of order N.
- $X(N)$ parametrizes elliptic curves with a basis of the N-torsion points with a fixed Weil pairing.

Due to the moduli interpretation, $X_0(N)$ and $X_1(N)$ both have models over $\mathbb{Q}$. $X_0(N)$ has the function field $\mathbb{Q}(j(\tau), j(N\tau))$, so there is a polynomial $\Phi_n(x,y) \in \mathbb{Q}[x,y]$ such that $\Phi_n(j(\tau), j(N\tau)) = 0$. A remarkable fact is that Φ_n actually has integer coefficients. One can utilize this to show that for an elliptic curve E with CM by $\mathcal{O}_\tau$, where $\mathcal{O}_\tau$ is the ring of integers of $\mathbb{Q}(\tau)$, $j(E)$ is actually an algebraic integer (Gross-Zagier have very explicit formula for these values). Moreover, the theory of complex multiplication shows:

Theorem 1 $j(E)$ is an algebraic integer of degree $h(\tau)$, where $h(\tau)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\tau)$. The Hilbert class filed H of K can be obtained from K by adjoining $j(E)$. The maximal abelian extension of $\mathbb{Q}(\tau)$ can be obtained by adjoining $j(E)$ and the x-coordinates of torsion points of E. Moreover, the action of $\mathrm{Gal}(H/K)$ on $j(E)$ can be described explicitly.

This main theorem of complex multiplication implies an interesting result discovered by Ramanujan: $e^{\pi\sqrt{163}} \approx 744 - j((\sqrt{-163}+1)/2)$ is an "almost integer" as $\mathbb{Q}(\sqrt{-163})$ has class number 1!

Shimura curves

One problem with $\Gamma(1) = SL_2(\mathbb{Z})$ is that its fundamental domain $SL_2(\mathbb{Z})\backslash\mathcal{H}$ is not compact. As a consequence, every subgroup of $SL_2(\mathbb{R})$ commensurable with $SL_2(\mathbb{Z})$ is not cocompact and we have to add cusps to obtain modular curves.

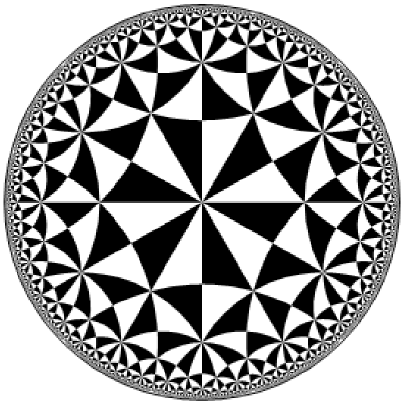
Question Can we find a discrete subgroup Γ of $SL_2(\mathbb{R})$ such that Γ is cocompact?

You have definitely seen many examples from the artwork of M. C. Escher. Using the Poincare disk model for $\mathcal{H}$, we can tessellate $\mathcal{H}$ with infinitely many hyperbolic triangles with geodesic sides.

Example 1 Let Δ be the hyperbolic triangle with angles $\pi/2, \pi/4, \pi/6$. Let σ_j be the $2\pi/j$ rotation with respect to its π/j vertex ($j = 2, 4, 6$). Then the group $G_{2,4,6}$ generated by σ_j acts on $\mathcal{H}$ as automorphisms. Looking at the picture we obtain the representation

$$G_{2,4,6} = \langle \sigma_2, \sigma_4, \sigma_6 : \sigma_2^2 = \sigma_4^4 = \sigma_6^6 = \sigma_2\sigma_4\sigma_6 = 1\rangle.$$

It is called the $(2,4,6)$-triangle group and has the fundamental domain consisting of Δ and one copy of its reflection. Hence $G_{2,4,6}$ is a discrete cocompact subgroup of $SL_2(\mathbb{R})$.



More generally, any triple (n,m,p) satisfying $\frac{1}{n} + \frac{1}{m} + \frac{1}{p} < 1$ gives us a triangle group. It is a cocompact subgroup of $SL_2(\mathbb{R})$ and has exactly three elliptic points of orders n, m, p. From this point view, $SL_2(\mathbb{Z})$ is simply the limiting case $(2,3,\infty)$, where $\pi/2$ and $\pi/3$ are the order 2 and 3 elliptic points and the cusp emerges as the limit π/∞ vertex.

Question Can we obtain cocompact subgroups arithmetically?

By "arithmetically" we mean the way we obtained $\Gamma(1)$ and other congruence subgroups by "taking $\mathbb{Z}$-points" of a matrix group. More precisely,

Definition 1 Let $G\subseteq GL_n$ be an algebraic group over $\mathbb{Q}$. A subgroup of $G(\mathbb{Q})$ is called *arithmetic* if $\Gamma_0\subseteq G(\mathbb{Q})$ is commensurable with $G(\mathbb{Z})$.

Definition 2 A subgroup $\Gamma\subseteq SL_2(\mathbb{R})$ is called *arithmetic* if there exists an algebraic group G over $\mathbb{Q}$ and a surjective homomorphism $\phi: G(\mathbb{R})\rightarrow SL_2(\mathbb{R})$ with compact kernel such that $\Gamma=\phi(\Gamma_0)$, where Γ_0 is an arithmetic subgroup of $G(\mathbb{Q})$.

Roughly speaking, after ignoring compact factors, an arithmetic subgroup of $SL_2(\mathbb{R})$ is simply a subgroup commensurable with $G(\mathbb{Z})$ provided $G(\mathbb{R})=SL_2(\mathbb{R})$. The congruence subgroups of $\Gamma(1)$ are obtained by taking $G=SL_2$. But none of them are cocompact! In order get a cocompact arithmetic subgroup, we need to find some other algebraic group G with $G(\mathbb{R})=SL_2(\mathbb{R})$. Instead of working with the matrix algebra $M_2(\mathbb{Q})$ and $SL_2(\mathbb{Q})$, we need some other $\mathbb{Q}$-algebra structure. One example is given by the quaternion algebra.

Definition 3 A quaternion algebra over k is a central simple k-algebra of dimension 4, namely a 4-dimensional k-algebra with center k and no nontrivial two-sided ideals.

By Wedderburn's theorem, every central simple k algebra is a matrix algebra over a central division k-algebra. All the central division k-algebra are classified by the Brauer group $\mathrm{Br}(k)\cong H^2(\mathrm{Gal}(k^s/k),(k^s)^\times)$. Quaternion algebras are characterized from division k-algebras as those having a quadratic splitting field.

Example 2 Let $(a,b/k)$ is the k-algebra with basis $\{1,i,j,ij\}$ satisfying the relations $i^2=a$, $j^2=b$, $ij=-ji$, where $a,b\in k^\times$. Then $(a,b/k)$ is a quaternion algebra. We can view $i=\begin{bmatrix}\sqrt{a} & 0\\ 0 & -\sqrt{a}\end{bmatrix}$ and $j=\begin{bmatrix}0 & b\\ 1 & 0\end{bmatrix}$. Then $k(\sqrt{a})$ splits $(a,b/k)$ as i,i^2,j,ij are $k(\sqrt{a})$-linear independent. Conversely, every quaternion algebra (including $M_2(k)$) is of the form $(a,b/k)$. One can regard quaternion algebras as a noncommutative way of gluing quadratic fields together. There is a natural involution given by $\overline{x+yi+zj+wij}=x-yi-zj-wij$. The *trace* and *norm* are given by

$$\mathrm{Tr}(\alpha)=\alpha+\overline{\alpha},\quad \mathrm{Nm}(\alpha)=\alpha\overline{\alpha}.$$

Example 3 For $k=\mathbb{R}$, we have the matrix algebra $M_2(\mathbb{R})$ and the Hamilton quaternion $\mathbb{H}=(-1,-1/\mathbb{R})$. As $\mathrm{Br}(\mathbb{R})=H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}),\mathbb{C}^\times)=\mathbb{R}^\times/\mathrm{Nm}(\mathbb{C}^\times)\cong\mathbb{Z}/2\mathbb{Z}$, these are the only two! Moreover, the norm one elements in $M_2(\mathbb{R})$ form $SL_2(\mathbb{R})$ and the norm one elements in $\mathbb{H}$ form a compact group.

Example 4 For k a non-archimedean local field, one big result from local class field theory tells us that $\mathrm{Br}(k)\cong\mathbb{Q}/\mathbb{Z}$ and quaternion algebras are classified by $\mathrm{Br}(k)[2]\cong\mathbb{Z}/2\mathbb{Z}$. Again there is a unique nonsplit quaternion algebra.

Example 5 For k a number field, one big result from global class field theory tells us that $\mathrm{Br}(k)$ sits inside an exact sequence

$$0\rightarrow\mathrm{Br}(k)\rightarrow\oplus_v\mathrm{Br}(k_v)\xrightarrow{\Sigma}\mathbb{Q}/\mathbb{Z}\rightarrow 0$$

and quaternion algebras are classified by $\mathrm{Br}(k)[2]$. So there are many quaternion algebras B over k, each of which is uniquely determined by an even number of nonsplit places. The *discriminant* D_B of B is product of all nonsplit places of B. So for $k=\mathbb{Q}$, any finite set S of finite primes will give a unique rational quaternion algebra, which is split at ∞ if $\#S$ is even and nonsplit at ∞ if $\#S$ is odd. In particular, a quaternion algebras split at every place is just the usual matrix algebra $M_2(k)$.

Now on let B be a rational quaternion algebra split at ∞. We can generalize the procedure of taking $SL_2(\mathbb{Z})$ from $M_2(\mathbb{Z})\subseteq M_2(\mathbb{Q})$ by taking a maximal order (a $\mathbb{Z}$-lattice of rank 4 which also a subring) $\mathcal{O}\subseteq B$ and its norm 1 elements $\mathcal{O}_1^\times\subseteq\mathcal{O}$. Since $\mathcal{O}_1^\times(\mathbb{R})=SL_2(\mathbb{R})$, $\mathcal{O}_1^\times$ is an arithmetic subgroup of $SL_2(\mathbb{R})$. As $\mathcal{O}_1^\times$ has no parabolic elements, we know that $\mathcal{O}_1^\times\backslash\mathcal{H}$ is cocompact. The resulting complex algebraic curve is the counterpart of the classical modular curve $X(1)$.

Definition 4 $\mathcal{O}_1^\times\backslash\mathcal{H}$ is called a *Shimura curve*. We denoted it by $\mathcal{X}(1)$ to show the analogy to $X(1)$.

Moduli interpretation and class fields

Now given any $z\in\mathcal{H}$, we have a rank 4-lattice $\Lambda_z=\mathcal{O}\cdot\langle 1,z\rangle$ in $\mathbb{C}^2$, where we view $\mathcal{O}\subseteq M_2(\mathbb{R})\subseteq M_2(\mathbb{C})$. So we obtain a complex torus $\mathbb{C}^2/\Lambda_z$ with an $\mathcal{O}$-action. It is actually an abelian surface via the Riemann form $(x\langle 1,z\rangle,y\langle 1,z\rangle)=\mathrm{tr}(\mu x\bar{y})$, where $\mu\in\mathcal{O}$ is chosen in the way that $\mu^2+D=0$. A special case is when

$B = M_2(\mathbb{Q})$ and $\mathcal{O} = M_2(\mathbb{Z})$, $\mathbb{C}^2/\Lambda_z$ is just two copies of the elliptic curve $E = \mathbb{C}/\langle 1, z\rangle$. So the same logic should apply and we can check that

Theorem 2 $\mathcal{X}(1)$ is the coarse moduli space of pairs (A, ι), where A is an abelian surface and $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ is an embedding.

In this case we say A is a *QM-surface* (quaternionic multiplication). For a fixed choice of μ, a theorem of Milne implies that if there is an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(A)$, then there is a unique principal polarization λ of A such that the corresponding Rosati involution $\alpha \mapsto \lambda^{-1}\hat{\alpha}\lambda$ on $\mathrm{End}(A)$ coincides with the positive involution $b \mapsto \mu^{-1}\bar{b}\mu$ on $\mathcal{O}$.

Now assume B is nonsplit and let A be a QM-surface.

- If A is simple, then its endomorphism algebra $D = \mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$ is an division algebra. D acts on $\Lambda \otimes \mathbb{Q}$ freely, so D has dimension at most 4. But (A, ι) is QM, so D has dimension at least 4 and $\mathrm{End}^0(A) = B$.
- If A is not simple, then $A \sim E_1 \times E_2$. If E_1, E_2 are not isogenous, then $D = \mathrm{End}^0(E_1) \times \mathrm{End}^0(E_2)$ which cannot contain the quaternion algebra B. Hence $A \sim E^2$ and $D \cong M_2(\mathrm{End}^0(E))$. Since B is nonsplit, we know that $\mathrm{End}^0(E) \not\cong \mathbb{Q}$, hence E is an elliptic curve with CM by a field K which splits B.

So we have proved the following

Proposition 3 If A is a QM-surface. Then either A is simple with $\mathrm{End}^0(A) = B$ or $A \sim E^2$, where E is an elliptic curve with CM by a field which splits B.

In the latter case, the corresponding point on the Shimura curve $\mathcal{X}(1)$ is called a *CM point*. Those are in some sense "degenerate" points on the moduli space of QM-surfaces. One can expect that these CM points could play an important role, since, unlike the modular curves case, we do not have truly degenerate cusps to work with.

Due to the moduli interpretation, $\mathcal{X}(1)$ has a canonical model over $\mathbb{Q}$. More generally, one can define the order $\Gamma(N) \subseteq \Gamma(1) = \mathcal{O}_1^\times$ by imposing a congruence condition $a \equiv 1 \pmod{N}$. The resulting Shimura curve $\mathcal{X}(N)$ has a similar moduli interpretation as QM-surfaces with extra level-N structures, which I do not quite bother writing down here.

Instead of $\mathbb{Q}$, one can also work more generally with a totally real number field F of degree $[F : \mathbb{Q}] = n$ and a quaternion algebra B over F split only at one real place. Then we have an embedding from B to the split factor $M_2(\mathbb{R})$ of $B \otimes_{\mathbb{Q}} \mathbb{R} = M_2(\mathbb{R}) \times \mathbb{H}^{n-1}$. Then norm one element $\mathcal{O}_1^\times$ in the maximal order $\mathcal{O} \subseteq B$ will again form a cocompact arithmetic subgroup of $SL_2(\mathbb{R})$ and the quotient $\mathcal{O}_1^\times \backslash \mathcal{H}$ is a Shimura curve. These curves also have a moduli interpretation as abelian varieties of dimension $2n$ with $\mathcal{O}$-actions, which is more complicated than the $F = \mathbb{Q}$ case. Using the moduli interpretation, Shimura proved that $\mathcal{X}(1)$ has a canonical model $\phi : \mathcal{X}(1) \to V$, where V is a complete algebraic curve over C_F, the maximal abelian extension of F unramified at all finite primes. Shimura then constructed class fields for totally imaginary extension of totally real number fields:

Theorem 3 (Shimura) Let M be a totally imaginary extension of F, which is isomorphic to a quadratic subfield of B over F. Then the Hilbert class field H of M is obtained from $C_F \cdot M$ by adjoining $\phi(z)$ for z a regular fixed point of M on $\mathcal{H}$.

Whatever the word "regular fixed point" means, it can be viewed as an analogue of the value of $j(E)$ in the modular curves case. Moreover, the action of $\mathrm{Gal}(H/M)$ can be described explicitly by the *Shimura reciprocity law*. We shall not go into the excessive details here.

Hurwitz curves ▲

Now let us look at an interesting example of Shimura curves which relates to

Question What is the answer to life, the universe and everything?

Answer 42. It is calculated by an enormous supercomputer in Douglas Adams' *The Hitchhiker's Guide to the Galaxy*. 42 is important also because it is the perfect IMO score and many of you have achieved it.

In the mathematical context, you may have seen this magic number as a bound for the number of automorphisms of a complex algebraic curve X.

Theorem 4 (Hurwitz) If the genus $g(X) \geq 2$, then $\# \operatorname{Aut}(X) \leq 42 \cdot (2g-2)$.

You know the proof if you went to Anand's class and listened carefully. Those curves with equality are called *Hurwitz curves*. Now let me show you how quaternion algebras and Shimura curves could help us in finding Hurwitz curves. Let us get started by finding a volume formula for the fundamental domain of $X = \Gamma \backslash \mathcal{H}$. Suppose M is the half fundamental domain consisting of k elliptic points of orders $e_1, \ldots, e_k$ and g quadruples of sides which are glued together in a way you all know. By the Gauss-Bonnet formula

$$\int_M K dA + \int_{\partial M} k_g ds = 2\pi\chi(M),$$

where K is the Gaussian curvature of M, k_g is the geodesic curvature of ∂M. In our case, $K = -1$, $\int_{\partial M} k_g ds = \sum_{i=1}^k (\pi - \pi/e_i)$ and $\chi(M) = 1 - g$. Therefore,

$$-\frac{1}{2}\operatorname{Vol}(X) + \pi \cdot \sum_{i=1}^k \left(1 - \frac{1}{e_i}\right) = \pi(2g-2),$$

In other words, we recover the Riemann-Hurwitz formula,

$$\frac{1}{2\pi}\operatorname{Vol}(X) = 2g - 2 + \sum_{i=1}^k \left(1 - \frac{1}{e_i}\right).$$

A simple calculation shows that the fundamental domain has the minimal volume $2\pi \cdot \frac{1}{42}$ when $k = 3$, $g = 2$ and $(e_1, e_2, e_3) = (2, 3, 7)$, which corresponds to $\Gamma = G_{2,3,7}$. Suppose $\Gamma' \subseteq \Gamma$ is a normal subgroup, then we know Γ/Γ' acts on $X' = \Gamma' \backslash \mathcal{H}$ as automorphisms and $[\Gamma : \Gamma'] = \operatorname{Vol}(X')/\operatorname{Vol}(X)$. If Γ' furthermore has no elliptic points, then $\operatorname{Vol}(X') = 2\pi \cdot (2g-2)$, hence $\# \operatorname{Aut}(X') \geq \Gamma/\Gamma' = 42 \cdot (2g-2)$ and X' is indeed a Hurwitz curve!

The remarkable thing is that $G_{2,3,7}$ is actually an arithmetic subgroup coming from a quaternion algebra. How can one possibly figure this out? The above volume formula is true for an arbitrary discrete subgroup Γ. But since arithmetic subgroups are defined in an arithmetic way, so one could expect that the arithmetic properties of quaternion algebras would benefit us. This is the case and here is an amazing volume formula worked out by Shimizu [6] using only arithmetic properties.

Theorem 5 (Shimizu) Let $F/\mathbb{Q}$ be a totally real number field of degree F. Then

$$\frac{1}{2\pi}\operatorname{Vol}(\mathcal{X}(1)) = \frac{d_F^{3/2}\zeta_F(2)}{4^{n-1}\pi^{2n}} \prod_{\mathfrak{p} | D_B} (N(\mathfrak{p}) - 1),$$

where d_F is the discriminant of $F/\mathbb{Q}$, D_B is the discriminant of B and ζ_F is the Dedekind zeta function of F.

Example 6 When $F = \mathbb{Q}$, we have a rather simple formula for the volume

$$\frac{1}{2\pi}\operatorname{Vol}(\mathcal{X}(1)) = \frac{1}{6}\prod_{p | D_B}(p-1).$$

Given a quaternion algebra, we can work out the volume of $\mathcal{X}(1)$ with Shimizu's formula in hand (and the zeta function is going to take over the world). Hence we can possibly solve g, k and e_i using the general volume formula. In fact, e_i can also be determined by investigating arithmetics by the work of Eichler. So one can sit down and work hard with quaternion algebras with a hope of finding triangle groups, i.e. those with $k = 3$ and $g = 0$. The complete list of arithmetic triangle groups are determined by Takeuchi [7], [8].

Example 7 The triangle group $G_{2,3,7}$ can be identified the group $\Gamma(1)$ for the cubic totally real field $F = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) = \mathbb{Q}(\cos\frac{2\pi}{7})$ and the quaternion algebras B over F only nonsplit at two real places. As discussed above, any normal subgroup Γ of $\Gamma(1)$ gives us a Hurwitz curve if it has no elliptic points. It turns out that the congruence subgroup $\Gamma(\mathfrak{p})$ has no elliptic points for any ideal $\mathfrak{p}$ of F, hence gives sn infinite family of Hurwitz curves! Even better, the number of automorphisms can be computed as

$$\# \operatorname{Aut} X(\mathfrak{p}) = \omega \cdot (N(\mathfrak{p}) - 1) \cdot N(\mathfrak{p}) \cdot (N(\mathfrak{p}) + 1),$$

where $\omega = 1$ if $\mathfrak{p} = (2)$ and $\omega = 1/2$ otherwise. The first few with small values of genus are listed as follows.

- For the ramified prime over 7, $N(\mathfrak{p}) = 7$. So $\# \operatorname{Aut} X(\mathfrak{p}) = \frac{1}{2} \cdot 6 \cdot 7 \cdot 8 = 168$, $g(X(\mathfrak{p})) = 3$ and $\operatorname{Aut} X(\mathfrak{p}) \cong PSL_2(\mathbb{F}_7)$.. It is known as the *Klein quartic* with the model $x^3y + y^3z + z^3x = 0$.

- For the inert prime over 2, $N(\mathfrak{p}) = 8$. So $\# \operatorname{Aut} X(\mathfrak{p}) = 7 \cdot 8 \cdot 9 = 504$, $g(X(\mathfrak{p})) = 7$ and $\operatorname{Aut} X(\mathfrak{p}) \cong PSL_2(\mathbb{F}_8)$. It is known as the *Fricke-Macbeath curve*.
- For the three unramified primes over 13, $N(\mathfrak{p}) = 13$. So we have three curves with $\# \operatorname{Aut} X(\mathfrak{p}) = \frac{1}{2} \cdot 12 \cdot 13 \cdot 14 = 1092$, $g(X(\mathfrak{p})) = 14$ and $\operatorname{Aut} X(\mathfrak{p}) \cong PSL_2(\mathbb{F}_{13})$. These were unkown before Shimura and are called the *first Hurwitz triplet*.

The above five are actually the first five smallest genus Hurwitz curves. The next one is of genus 17, which is non-arithmetic. The next arithmetic one is of genus 118 given by the inert prime above 3.

References

[1] Clark, P.L., *Rational points on Atkin-Lehner quotients of Shimura curves,* Harvard University Cambridge, Massachusetts, 2003.

[2] Shimura, G., *Construction of class fields and zeta functions of algebraic curves,* The Annals of Mathematics **85** (1967), no.1, 58--159.

[3] Voight, J., *Shimura curve computations,* Arithmetic geometry **8** (2006), 103--113.

[4] Elkies, N., *Shimura curve computations,* Algorithmic number theory (1998), 1--47.

[5] Elkies, N.D., *The Klein quartic in number theory,* The Eightfold Way, edited by S. Lévy (1999), 51--102.

[6] Shimizu, H., *On zeta functions of quaternion algebras,* The Annals of Mathematics **81** (1965), no.1, 166--193.

[7] Takeuchi, Kisao, *Commensurability classes of arithmetic triangle groups,* J. Fac. Sci. Univ. Tokyo Sect. IA Math. **24** (1977), no.1, 201--212.

[8] Takeuchi, Kisao, *Arithmetic triangle groups,* J. Math. Soc. Japan **29** (1977), no.1, 91--106.