WIKIPEDIA

Modular curve

In number theory and algebraic geometry, a **modular curve** $Y(\Gamma)$ is a Riemann surface, or the corresponding algebraic curve, constructed as a quotient of the complex upper half-plane **H** by the action of a congruence subgroup Γ of the modular group of integral 2×2 matrices SL(2, **Z**). The term modular curve can also be used to refer to the **compactified modular curves** $X(\Gamma)$ which are compactifications obtained by adding finitely many points (called the **cusps of Γ**) to this quotient (via an action on the **extended complex upper-half plane**). The points of a modular curve parametrize isomorphism classes of elliptic curves, together with some additional structure depending on the group Γ. This interpretation allows one to give a purely algebraic definition of modular curves, without reference to complex numbers, and, moreover, prove that modular curves are defined either over the field of rational numbers **Q** or a cyclotomic field $\mathbf{Q}(\zeta_n)$. The latter fact and its generalizations are of fundamental importance in number theory.

Contents

Analytic definition

The modular group SL(2, **Z**) acts on the upper half-plane by fractional linear transformations. The analytic definition of a modular curve involves a choice of a congruence subgroup Γ of SL(2, **Z**), i.e. a subgroup containing the principal congruence subgroup of level N $\Gamma(N)$, for some positive integer N, where

$$\Gamma(N)=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}:\ a\equiv d\equiv 1 \mod N \text{ and } b,c\equiv 0 \mod N\right\}.$$

The minimal such N is called the **level of Γ**. A complex structure can be put on the quotient Γ**H** to obtain a noncompact Riemann surface commonly denoted $Y(\Gamma)$.

Compactified modular curves

A common compactification of $Y(\Gamma)$ is obtained by adding finitely many points called the cusps of Γ. Specifically, this is done by considering the action of Γ on the **extended complex upper-half plane** **H*** = **H** ∪ **Q** ∪ {∞}. We introduce a topology on **H*** by taking as a basis:

- any open subset of **H**,

- for all $r > 0$, the set $\{\infty\} \cup \{\tau \in \mathbf{H} \mid \operatorname{Im}(\tau) > r\}$
- for all coprime integers a, c and all $r > 0$, the image of $\{\infty\} \cup \{\tau \in \mathbf{H} \mid \operatorname{Im}(\tau) > r\}$ under the action of

  $$\begin{pmatrix} a & -m \\ c & n \end{pmatrix}$$

  where m, n are integers such that $an + cm = 1$.

This turns **H*** into a topological space which is a subset of the Riemann sphere $\mathbf{P}^1(\mathbf{C})$. The group Γ acts on the subset **Q** ∪ {∞}, breaking it up into finitely many orbits called the **cusps of Γ**. If Γ acts transitively on **Q** ∪ {∞}, the space Γ\**H*** becomes the Alexandroff compactification of Γ\H. Once again, a complex structure can be put on the quotient Γ\**H*** turning it into a Riemann surface denoted *X*(Γ) which is now compact. This space is a compactification of *Y*(Γ).[1]

Examples

The most common examples are the curves *X*(*N*), $X_0(N)$, and $X_1(N)$ associated with the subgroups Γ(*N*), $\Gamma_0(N)$, and $\Gamma_1(N)$.

The modular curve *X*(5) has genus 0: it is the Riemann sphere with 12 cusps located at the vertices of a regular icosahedron. The covering *X*(5) → *X*(1) is realized by the action of the icosahedral group on the Riemann sphere. This group is a simple group of order 60 isomorphic to A_5 and PSL(2, 5).

The modular curve *X*(7) is the Klein quartic of genus 3 with 24 cusps. It can be interpreted as a surface with three handles tiled by 24 heptagons, with a cusp at the center of each face. These tilings can be understood via dessins d'enfants and Belyi functions – the cusps are the points lying over ∞ (red dots), while the vertices and centers of the edges (black and white dots) are the points lying over 0 and 1. The Galois group of the covering *X*(7) → *X*(1) is a simple group of order 168 isomorphic to PSL(2, 7).

There is an explicit classical model for $X_0(N)$, the classical modular curve; this is sometimes called *the* modular curve. The definition of Γ(*N*) can be restated as follows: it is the subgroup of the modular group which is the kernel of the reduction modulo *N*. Then $\Gamma_0(N)$ is the larger subgroup of matrices which are upper triangular modulo *N*:

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv 0 \mod N \right\},$$

and $\Gamma_1(N)$ is the intermediate group defined by:

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a \equiv d \equiv 1 \mod N, c \equiv 0 \mod N \right\}.$$

These curves have a direct interpretation as moduli spaces for elliptic curves with *level structure* and for this reason they play an important role in arithmetic geometry. The level *N* modular curve *X*(*N*) is the moduli space for elliptic curves with a basis for the *N*-torsion. For $X_0(N)$ and $X_1(N)$, the level structure is, respectively, a cyclic subgroup of order *N* and a point of order *N*. These curves have been studied in great detail, and in particular, it is known that $X_0(N)$ can be defined over **Q**.

The equations defining modular curves are the best-known examples of modular equations. The "best models" can be very different from those taken directly from elliptic function theory. Hecke operators may be studied geometrically, as correspondences connecting pairs of modular curves.

Remark: quotients of **H** that *are* compact do occur for Fuchsian groups Γ other than subgroups of the modular group; a class of them constructed from quaternion algebras is also of interest in number theory.

Genus

The covering $X(N) \to X(1)$ is Galois, with Galois group SL(2, N)/{1, −1}, which is equal to PSL(2, N) if N is prime. Applying the Riemann–Hurwitz formula and Gauss–Bonnet theorem, one can calculate the genus of $X(N)$. For a prime level $p \geq 5$,

$$-\pi\chi(X(p)) = |G| \cdot D,$$

where $\chi = 2 - 2g$ is the Euler characteristic, $|G| = (p+1)p(p-1)/2$ is the order of the group PSL(2, p), and $D = \pi - \pi/2 - \pi/3 - \pi/p$ is the angular defect of the spherical (2,3,p) triangle. This results in a formula

$$g = \tfrac{1}{24}(p+2)(p-3)(p-5).$$

Thus $X(5)$ has genus 0, $X(7)$ has genus 3, and $X(11)$ has genus 26. For $p = 2$ or 3, one must additionally take into account the ramification, that is, the presence of order p elements in PSL(2, **Z**), and the fact that PSL(2, 2) has order 6, rather than 3. There is a more complicated formula for the genus of the modular curve $X(N)$ of any level N that involves divisors of N.

Genus zero

In general a **modular function field** is a function field of a modular curve (or, occasionally, of some other moduli space that turns out to be an irreducible variety). Genus zero means such a function field has a single transcendental function as generator: for example the j-function generates the function field of $X(1)$ = PSL(2, **Z**)**H***. The traditional name for such a generator, which is unique up to a Möbius transformation and can be appropriately normalized, is a **Hauptmodul** (**main** or **principal modular function**).

The spaces $X_1(n)$ have genus zero for n = 1, ..., 10 and n = 12. Since each of these curves is defined over **Q** and has a **Q**-rational point, it follows that there are infinitely many rational points on each such curve, and hence infinitely many elliptic curves defined over **Q** with n-torsion for these values of n. The converse statement, that only these values of n can occur, is Mazur's torsion theorem.

Relation with the Monster group

Modular curves of genus 0, which are quite rare, turned out to be of major importance in relation with the monstrous moonshine conjectures. First several coefficients of q-expansions of their Hauptmoduln were computed already in the 19th century, but it came as a shock that the same large integers show up as dimensions of representations of the largest sporadic simple group Monster.

Another connection is that the modular curve corresponding to the normalizer $\Gamma_0(p)^+$ of $\Gamma_0(p)$ in SL(2, **R**) has genus zero if and only if p is 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59 or 71, and these are precisely the prime factors of the order of the monster group. The result about $\Gamma_0(p)^+$ is due to Jean-Pierre

Serre, Andrew Ogg and John G. Thompson in the 1970s, and the subsequent observation relating it to the monster group is due to Ogg, who wrote up a paper offering a bottle of Jack Daniel's whiskey to anyone who could explain this fact, which was a starting point for the theory of monstrous moonshine.[2]

The relation runs very deep and, as demonstrated by Richard Borcherds, it also involves generalized Kac–Moody algebras. Work in this area underlined the importance of modular *functions* that are meromorphic and can have poles at the cusps, as opposed to modular *forms*, that are holomorphic everywhere, including the cusps, and had been the main objects of study for the better part of the 20th century.

See also

- Manin–Drinfeld theorem
- Moduli stack of elliptic curves
- Modularity theorem
- Shimura variety, a generalization of modular curves to higher dimensions

References

1. Serre, Jean-Pierre (1977), *Cours d'arithmétique*, Le Mathématicien, vol. 2 (2nd ed.), Presses Universitaires de France
2. Ogg (1974)

- Steven D. Galbraith - Equations For Modular Curves (https://www.math.auckland.ac.nz/~sgal018/thesis.pdf)

- Shimura, Goro (1994) [1971], *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, ISBN 978-0-691-08092-5, MR 1291394 (https://www.ams.org/mathscinet-getitem?mr=1291394), Kanô Memorial Lectures, **1**
- Panchishkin, A.A.; Parshin, A.N., "Modular curve" (https://encyclopediaofmath.org/wiki/Modular_curve), *Encyclopaedia of Mathematics*, ISBN 1-4020-0609-8
- Ogg, Andrew P. (1974), "Automorphismes de courbes modulaires" (http://archive.numdam.org/ARCHIVE/SDPP/SDPP_1974-1975__16_1/SDPP_1974-1975__16_1_A4_0/SDPP_1974-1975__16_1_A4_0.pdf) (PDF), *Seminaire Delange-Pisot-Poitou. Theorie des nombres, tome 16, no. 1 (1974–1975), exp. no. 7* (in French), MR 0417184 (https://www.ams.org/mathscinet-getitem?mr=0417184)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Modular_curve&oldid=1020712571"

This page was last edited on 30 April 2021, at 16:44 (UTC).