PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 17–21

Valerio Dose

Automorphisms of non-split Cartan modular curves

written by Mohammed Anwar

Modular curves are algebraic curves whose points (more precisely all but finitely many of them) parametrize families of elliptic curves. Classically modular curves are constructed as (compactifications of) quotients of the upper half plane under the action of subgroups of $\mathrm{SL}_2(\mathbb{Z})$. The general set up is as follows:

- $\mathfrak{h} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$
- H a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$
- $\Gamma_H = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \bmod N \text{ belongs to } H\}$

Then Γ acts on $\mathfrak{h}$ by fractional linear transformations:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \quad \gamma(\tau) = \frac{a\tau + b}{c\tau + d}$$

and the action can be extended to $\mathfrak{h} \cup \mathbb{Q} \cup \{\infty\}$. The space of orbits $\mathfrak{h} \cup \mathbb{Q} \cup \{\infty\}/\Gamma_H$ can be given the structure of Riemann surface and is denoted by X_H and is called the *modular curve* associated to H. The point of X_H coming from $\mathbb{Q} \cup \{\infty\}$ are called the *cusps (or cuspidal points)* of X_H.

To connect the above definition to elliptic curves recall that to every $\tau \in \mathfrak{h}$ is associated a complex torus E_τ, (thus an elliptic curve over $\mathbb{C}$), defined by $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$. Moreover any two such complex tori E_τ and $E_{\tau'}$ are isomorphic if and only if are in the same orbit under $\mathrm{SL}_2(\mathbb{Z})$. This gives the modular interpretation of X_Γ, (here $\Gamma = \mathrm{SL}_2(\mathbb{Z})$) as parametrizing isomorphism classes of elliptic curves. For general Γ_H one has to consider the following set up:

- E is an elliptic curve over $\mathbb{C}$, and $E[N]$ denotes the subgroup of N-torsion points.
- $\varphi : E[N] \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ is an isomorphism.
- Two pair (E, φ) and (E', φ') are equivalent if and only if there exist an isomorphism $f : E \to E'$, such that $M \circ \varphi = \varphi' \circ f$, for some $M \in H$.

Then, the non cuspidal points of X_H parametrize equivalence class of pairs (E, φ). A crucial fact is that the compact Rieman surfaces X_H can be given a structure of projective algebraic curve defined over the cyclotomic field $\mathbb{Q}(\zeta_N)$. Moreover if $\det : H \to \mathbb{Z}/NZ^*$ is surjective than X_H is actually defined over $\mathbb{Q}$.

One interesting problem is to study the group of automorphisms of X_H. Recall that $\mathrm{SL}_2(\mathbb{R})/\{\pm Id\}$ is the automorphisms group of $\mathfrak{h}$, acting upon $\mathfrak{h}$ by fractional linear transformations. If $N(\Gamma_H)$ denotes the the normaliser of Γ_H in $\mathrm{SL}_2(\mathbb{R})$, then an element η of $N(\Gamma_H)$ define an automorphism of $\mathfrak{h}/\Gamma_H$ and it can be shown that η extends to an automorphism of X_H. Set $B(X_H) = N(\Gamma_H)/\Gamma_H \subset \mathrm{Aut}(X_H)$, the elements of $B(X_H)$ are called *modular automorphisms*. A non-modular automorphism is called *exceptional*

Question 1 *When the genus of X_H is at least 2 is every automorphism of X_H modular?*

Beside being an interesting question on its own the above question is also related to Serre's Uniformity conjecture as follows: In [7] J.P.

Serre proved the following result (here and in the sequel CM stands for complex multiplication)

Theorem 2 *Let E be an elliptic curve over $\mathbb{Q}$. If E is without CM then there exist a constant C_E such that for every prime number $p > C_E$ the Galois representation modulo p attached to E is surjective.*

Serre asked whether the constant C_E could be made independent of E:

Question 3 (Serre's uniformity problem) *Does there exist a number C_0 such that for every elliptic curve without CM and every $p > C_0$ the Galois representations modulo p attached to E is surjective?*

It widely believed that one can take $C_0 = 37$, (see, e.g. [1]). Since the maximal subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ are:

- Exceptional subgroups, i.e. those whose image in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is isomorphic to $\mathcal{A}_4$, $\mathcal{S}_4$, or $\mathcal{A}_5$.
- Borel subgroups.
- Normalizers of split Cartan subgroups.
- Normalizers of non-split Cartan subgroups.

Thus, to solve Serre's uniformity problem, one has to prove that for sufficiently large p the image of the Galois representation is not contained in any of the above subgroups. Serre settled the exceptional subgroups, while the case of Borel subgroups follows from work of Mazur [6] on rational isogenies of prime degree. Much more recently Bilu and Parent solved Serre's problem in the split Cartan case. Thus the only remaining case is the non-split Cartan.

The connection to points on modular goes as follows: Let H be a (maximal) subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, then a rational point on X_H is associated to a pair (E, φ), where

- E is an elliptic curve defined over $\mathbb{Q}$;

- $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the p-torsion to as subgroup of H;
- the image of the Galois representation modulo p attached to E is contained in H.

We refer the interested reader to [5] for details.
Thus elliptic curves without CM, for which the associate Galois representation modulo p is not surjective correspond to (non CM) rational points on the modular curve X_H (for some maximal subgroup H of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$), which are not cusps. Such a rational point could be constructed as the mage of a cuspidal point via an exceptional automorphism of X_H.

Let C be a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and C^+ its normalizer. The associated modular curves are denoted by $X_{ns}(p)$ and $X_{ns}^+(p)$ respectively. C has index 2 in C^+ and there exists a degree two morphism $X_{ns}(p) \to X_{ns}^+(p)$ and a modular involution w of $X_{ns}^+(p)$, such that $X_{ns}^+(p) = X_{ns}(p)/\langle w\rangle$. Moreover $B\left(X_{ns}(p)\right) = \langle w\rangle$ and $B\left(X_{ns}^+(p)\right)$ is trivial. It is expected that for large p all the automorphism of $X_{ns}(p)$ are modular. The following are some recent result on regarding the automorphism group of $X_{ns}(p)$

Theorem 4 ([2]) *The automorphism group of $X_{ns}(11)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2Z$.*

Theorem 5 ([3])

1) For $p \geq 37$ all the automorphisms of $X_{ns}(p)$ preserve the cusps.

2) If $p \equiv 1 \bmod 12$ and $p \neq 13$, then

$$\mathrm{Aut}(X_{ns}(p)) = \langle w\rangle = B\left(X_{ns}(p)\right)$$

Theorem 6 ([4]) *If $13 \leq p \leq 31$, then*

1) $\mathrm{Aut}(X_{ns}^+(p))$ *is trivial.*

2) $\mathrm{Aut}(X_{ns}(p)) = \langle w\rangle$

References

[1] Y. Bilu and P. Parent *Serre's uniformity problem in the split Cartan case*, Ann. of Math. 2 Vol 173 (2011), pp. 569-584.

[2] V. Dose, J. Fernández, J. González and R. Schoof,*The automorphism group of the non-split Cartan modular curve of level 11*, J. Algebra, 417 (2014) p.95-102.

[3] V. Dose, *On the automorphisms of the non-split cartan modular curves of prime level*, arXiv:1503.05165.

[4] J. González *Constraints on the automorphism group of a curve*, arXiv:1503.05691.

[5] B. Mazur *Rational points on modular curves*, in Modular functions of one variable V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 107-148; Lecture Notes in Math. 601, Springer, Berlin, 1977.

[6] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. 44 (1978), pp. 129-162.

[7] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* Invent. Math., vol. 15 (1972), pp. 259-331.

Mohammed Anwar
Dipartimento di Matematica e Fisica
Università Roma Tre
L.go San Leonardo Murialdo 1
00146 Roma, Italy.
email: anwar@mat.uniroma3.it