Modular curves, Chen type isogeny and many points

Pietro Mercuri
a joint work with V. Dose, G. Lido and C. Stirpe

Sapienza Università di Roma

ANTS XVI
July 16, 2024

Modular curves, Chen type isogeny...

Let X_H be the modular curve corresponding to a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that, for every prime $p|n$ and $p^e||n$, H mod p^e is conjugate to one of the following subgroups:

$$\underset{\text{Borel}}{\left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}};\quad \underset{\text{split Cartan}}{\left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\}};\quad \underset{\text{normalizer split Cartan}}{\left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix},\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}\right\}};$$

$$\underbrace{\underset{\text{non-split Cartan}}{\left\{\begin{pmatrix} a & b\xi \\ b & a \end{pmatrix}\right\}};\underset{\text{normalizer non-split Cartan}}{\left\{\begin{pmatrix} a & b\xi \\ b & a \end{pmatrix},\begin{pmatrix} a & b\xi \\ -b & -a \end{pmatrix}\right\}}}_{p \text{ odd and } \xi \bmod p^e \text{ non-square}};\underbrace{\underset{\text{non-split Cartan}}{\left\{\begin{pmatrix} a & b \\ b & a+b \end{pmatrix}\right\}};\underset{\text{normalizer non-split Cartan}}{\left\{\begin{pmatrix} a & b \\ b & a+b \end{pmatrix},\begin{pmatrix} a & a-b \\ b & -a \end{pmatrix}\right\}}}_{p=2}.$$

Let W be a subgroup of $\mathrm{Aut}(X_H)$, then

$$\mathrm{Jac}(X_H/W) \sim \prod_{d|n^2 \text{ with some conditions}} \left(J_0^{\mathrm{new}}(d)/W_d\right)^{m_d},$$

where $J_0^{\mathrm{new}}(d)$ is the new part of the Jacobian of the classical Borel modular curve $X_0(d)$, $m_d \in \mathbb{Z}_{\geq 1}$ and W_d is a subgroup of the Atkin-Lehner operators of $X_0(d)$ depending on W and d.

...and many points

There is the Hasse-Weil-Serre upper bound for the number of points of a smooth, projective, absolutely irreducible algebraic curve X over a finite field $\mathbb{F}_q$ of genus g, with $q = p^k$ and p prime; it is

$$|\#X(\mathbb{F}_q) - q - 1| \leq g\lfloor 2\sqrt{q} \rfloor.$$

In particular cases sharper upper bounds can be given. On the website manypoints.org there are tables collecting, for a given pair genus-finite field $(g, \mathbb{F}_q)$, the best curve with "many points", meaning that it has at least $\left\lfloor \frac{U(g,\mathbb{F}_q)-1-q}{\sqrt{2}} \right\rfloor + 1 + q$ points, where $U(g, \mathbb{F}_q)$ is the lowest upper bound for the given pair $(g, \mathbb{F}_q)$.

Let $[f]$ be the Galois-orbit of the newform f appearing in the decomposition of $J_0^{\text{new}}(d)$. Using Fourier coefficients $a_p(h)$, for $h \in [f]$, contained in LMFDB and computing numerically the roots α_h, β_h of the polynomial $x^2 - a_p(h)x + p = 0$, we have a fast algorithm to compute

$$\#(X_H/W)(\mathbb{F}_{p^k}) = p^k + 1 - \sum_{[f]} m_d \sum_{h\in[f]} (\alpha_h^k + \beta_h^k).$$

We analysed 14800 curves in around 4 hours and we found 112 improvements (+88 matches of previous best results) over 2950 slots in the table on manypoints website.