Schiermonnikoog, Gerard 60. 2010/09/22 ①

0. About Gerard: Compositio: Ben and Frans have already said that, and it is in a letter in Expt. volume
I learned Arakelov theory from Gerard's course with Robin de Jong.

1. Cubics and $\Delta = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n$.

smooth compactification of 10-fold fiber pr. of univ. ell. curve.

$\mathbb{C}\cdot\Delta = S_{12}(Sl_2(\mathbb{Z})) \subset H^{11,0}(\overline{E^{10}_{\mathbb{C}}})$

So: $\tau(p)$ "occurs in" point counting of $\overline{E}^{10}(\mathbb{F}_p)$.

Aim: to make a precise and as simple as possible statement of this kind (no level structure, no stacks, ...).

Thm. For $n\geq 0$ let $\mathcal{C}_n$ be the scheme of smooth cubic curves in $\mathbb{P}^2$ with n given points. Then $\exists$ $f_0,\ldots,f_{10}$ in $\mathbb{Z}[x]$ s.t.

$\forall\ \mathbb{F}_q$: $\#\mathcal{C}_n(\mathbb{F}_q) = f_n(q)\cdot \#PGl_3(\mathbb{F}_q)$ if $n<10$.

$\forall\ p$: $\#\mathcal{C}_{10}(\mathbb{F}_p) = (f_{10}(p) - \tau(p))\cdot \#PGl_3(\mathbb{F}_p)$ (where $\mathcal{O}(1)|_C \cong \mathcal{O}_C(P_0+2P_1)$)

$(C,P_1,\ldots,P_n) \mapsto ((C,P_0),P_1,\ldots,P_n)$

Proof. $PGl_3(\mathbb{F}_q) \circlearrowright \mathcal{C}_n(\mathbb{F}_q)$ is equiv. to $\mathcal{E}_n(\mathbb{F}_q)$, ~~the~~ where $\mathcal{E}_n$ is the stack of elliptic curves with n given points.

Then Deligne, Behrend: $\#\mathcal{E}_n(\mathbb{F}_q)$ has the required property, $= \sum_x \frac{1}{\#\mathrm{Aut}(x)}$.

because $S_k(Sl_2(\mathbb{Z})) = \begin{cases} 0 & \text{for } k<12 \\ \mathbb{C}\cdot\Delta & \text{for } k=12. \end{cases}$ ⊠

Some ~~more detail~~ explanation of this:

$$\begin{array}{c} \mathcal{E}_1^n \\ \downarrow \pi \\ \mathcal{M}_{1,1} \end{array}$$

Gerard & Jonas gave us these for

$\#\mathcal{E}_1^n(\mathbb{F}_q) = \mathrm{trace}(F_q^*, H_c^\cdot(\mathcal{E}^n_{\overline{\mathbb{F}}_q,et}, \mathbb{Q}_\ell)) =$

rank 2 loc. syst.

$= \mathrm{trace}(F_q^*, H_c^\cdot(\mathcal{M}_{1,1}, \underbrace{R^\cdot\pi_*\mathbb{Q}_\ell})) \,,\ = (H^0 \oplus H^1 \oplus H^2)^{\otimes n}$

$H^0 = \mathbb{Q}_\ell$, $H^2 = \mathbb{Q}_\ell(1)$

Δ shows up in $\mathrm{Sym}^{10}(H^1)$, contributes ~~…~~ $-\tau(p)$.

Conclusion: $\dim \mathbb{Q}[x,y,z]_3 = 10$ implies that for $k<12$: $S_k(Sl_2(\mathbb{Z})) = 0$.

2. Couveignes's method of numerically inverting the Abel-Jacobi map.

Context:
$$\begin{tikzcd}
 & X^{(g)} \arrow[dr] & \\
X^g \arrow[ur] \arrow[rr, "\varphi"] & & J = \mathbb{C}^g/\Lambda
\end{tikzcd}$$
$X = X_1(l)(\mathbb{C})$, l not fixed.

$P \in X^g$, $P \longmapsto [P_1 + \dots + P_g - g\cdot O] = \sum_{j=1}^{g} \int_O^{P_j} \omega$

$x \in J$ – of order l

$\Omega^1(X) = \bigoplus_{j=1}^{g} \mathbb{C}\cdot\omega_j$ normalised newforms.

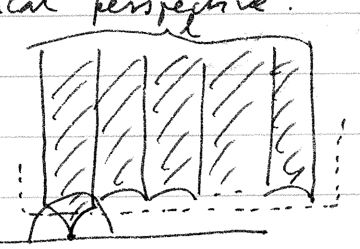
$\omega_j = \sum_{n\geq 1} a_n(\omega_j)\cdot q^n \cdot \frac{dq}{q}$ with $a_1(\omega_j) = 1$.

Assume that $\exists!\, D_x \in X^{(g)}$ s.t. $[D_x - g\cdot O] = x$.

Problem: approximate D_x with a given accuracy, deterministically in polynomial time.

Let us look at $X^g \xrightarrow{\varphi} J$ from a numerical perspective.

- Fundamental domain, e.g. for $\Gamma_0(l)^*$:
  X is covered by open disks around the cusps
  $\omega_1, \dots, \omega_g$ given by power series with suitably bounded coeff.



  $H_1(X,\mathbb{Z}) \xrightarrow{\sim} \Lambda \subset \mathbb{C}^g$ and φ can be well approximated.

- First, practical method. Pick $P \in X^g$, compute $\varphi(P)$ and try to lift the straight line in J from $\varphi(P)$ to x. Works in practice i.e. for small l (Johan Bosman), but we do not know how to prove that it always works. (problem with distance to the bad locus).

- Couveignes's method. Idea 1: just try to find P s.t. $\varphi(P)$ is close to x; for x as we have, height bounds from Arakelov theory are applied to show that $P_1 + \dots + P_g$ is close enough to D_x. The new problem can be solved for any x!
  Idea 2. Take $R_1, R_1', \dots, R_{2g}, R_{2g}'$ s.t. R_j very close to R_j', let $b_j := [R_j' - R_j]$, such that $\det(b_1, \dots, b_{2g})$ w.r.t. st. $\mathbb{R}$-basis of $\mathbb{C}^g$ not too small. Compute $\lambda_1, \dots, \lambda_{2g} \in \mathbb{R}$ s.t. $x = \lambda_1 b_1 + \dots + \lambda_{2g} b_{2g}$, put $n_j := \lfloor \lambda_j + \frac{1}{2} \rfloor$. Note: the $|n_j|$ are big!
  Then $\varphi(\sum_j n_j(R_j' - R_j))$ is close to x.
  numerically Reduce the divisors $(\sum_j n_j R_j' - \sum_j n_j \cdot O)$ $(\sum_j n_j R_j - \sum_{n_j} O)$ to one of the form $P_1 + \dots + P_g - g\cdot O$;

weight 4 cuspforms; ell. deg r.g.

Basic operation: $0 \neq s \in \Gamma(X, \mathcal{L}(-A-B))$, $C := \mathrm{div}(s)$

then $C = \mathcal{L} - A - B$ in $\mathrm{Pic}(X)$

$0 \neq t \in \Gamma(X, \mathcal{L}(-C - g \cdot O))$, $D := \mathrm{div}(t)$

then $D = \mathcal{L} - C - g \cdot O = \cancel{\mathcal{L}} - \cancel{\mathcal{L}} + A + B - g \cdot O$ in $\mathrm{Pic}(X)$.

Ingredient: compute zeros of power series, with required prec. in pol. time.

Fast exponentiation: error remains small.

3. Peter Bruin's thesis. (defended Sept. 1)

$\mathbb{Z}$-Hecke algebra $S_k(\Gamma_1(n))$; 2. square free

Main result: $\exists$ probabilistic alg. that given $\mathbb{T}(n,k) \xrightarrow{f} \mathbb{F} \supset \mathbb{F}_\ell$, computes $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ in time polynomial in $n, k, \#\mathbb{F}$.

(assume GRH)

Schoof type applications ~~consequences~~: $T_p \in \mathbb{T}(n,k)$ can be computed in time pol. in $n, k, \log p$. Very nice application to $\left(\sum_{n \in \mathbb{Z}} q^{n^2}\right)^{2k}$.

Ingredients:
- better control of Arakelov Green functions.
- more flexibility with origin-divisor: $x \sim D_x - d_x \cdot O$, $d_x \leq g$. (I cheated about this, earlier in this talk).
- computations in $J(\mathbb{F}_q)$ done using Khuri-Makdisi's general methods (nicer than the plane models of X used by Couveignes).

involves a lot of work; not at all a straightforward généralisation of previous work.