Simple things we don't know

Nick Katz

March 26, 2015

Let A/K be an abelian variety of dimension $g \geq 1$ over a number field. Throughtout this talk, we assume that A has big monodromy, in the sense that for some ℓ (equivalently, every ℓ) the image of the ℓ-adic representation

$$\rho_\ell : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GSp}(2g, \mathbb{Q}_\ell)$$

is open.

Examples.

1. $g = 1$ and $j(E) \notin \mathcal{O}_K$ (Serre).
2. Jacobians of hyper elliptic curves $y^2 = f(x)$ with f of degree $n = 2g+1$ or $2g+2$, having Galois group S_n or A_n (Zarhin).
3. Concrete examples: $f(x) = x^n - x - 1$ (Osada) has S_n, and $\sum_{i=1}^n x^i/i!$ has A_n if $4|n$ and S_n otherwise (Schur)

If A has good reduction at $\mathfrak{p}$ then

$$\det\left(1 - T\mathrm{Frob}_\mathfrak{p} \middle| H^1(A_{\bar{K}}, \mathbb{Q}_\ell)\right)$$

has $\mathbb{Z}$-coefficients with reciprocal roots α satisfying $|\alpha| = \sqrt{N\mathfrak{p}}$. Renormalize to get

$$\det(1 - T\sqrt{N\mathfrak{p}}\Theta_\mathfrak{p}).$$

Then $\det(1 - T\Theta_\mathfrak{p})$ is the (reversed) characteristic polynomial of a unique conjugacy class $\Theta_\mathfrak{p}$ in the compact symplectic group $\mathrm{USp}(2g)$.

Expectations

1. Sato-Tate: $\{\Theta_{\mathfrak{p}}\}_{\text{good } \mathfrak{p}}$ are equi-distributed in the space of conjugacy classes of $\mathrm{USp}(2g)$ for its 'Haar measure'. This is known for $g = 1$ when K is totally real.

   Further Sato-Tate-like expectation: if L/K is a finite Galois extension, this equidistribution should still hold for Frobenii of primes lying in a fixed conjugacy class of $\mathrm{Gal}(L/K)$. For example, consider primes in arithmetic progressions.

   This is known for $g = 1$, K totally real, L/K solvable.

2. Also expected
$$\{\mathfrak{p} : A \pmod{\mathfrak{p}} \text{ ordinary } \}$$
has density one. Known for $g = 1$ (Serre) and for $g = 2$ (Sawin).

Now consider the case of an A of dimension $g = 2$. For a degree one prime $\mathfrak{p}$, the characteristic polynomial of Frob_p has the form
$$1 - aT + bT^2 + -paT^3 + p^2T^4,$$
and $A(\mathrm{mod}\ \mathfrak{p})$ is ordinary if and only if $p \not| b$.

Question 1 *Evaluate jumping behavior of Neron-Severi rank as* $\mathfrak{p}$ *varies:*
$$\mathrm{NS}(A \pmod{\mathfrak{p}}) \subset H^2(A \pmod{\mathfrak{p}}) = \bigwedge^2 H^1(A \pmod{\mathfrak{p}}).$$

In the case $g = 2$, expectation based on analysis of roots of characteristic polynomial: To have $\rho(A) > 2$ at a prime of degree one, i.e., more than two eigenvalues p in $\Lambda^2 H^1$, the characteristic polynomial
$$1 - aT + bT^2 + -paT^3 + p^2T^4$$
must be a square, in which case it is the square of
$$1 - (a/2)T + pT^2,$$
and this happens if and only if
$$b = 2p + a^2/4.$$
The probability of this equality of integers of size $O(p)$ is about $1/p$, which leads to the idea that $\rho(A) > 2$ happens $\sim \log\log X$ times for primes $\mathfrak{p}$ with $N\mathfrak{p} < X$.

Question 2 *Still in genus $g = 2$. Evaluate jumping behavior of geometric Neron-Severi rank as $\mathfrak{p}$ varies::*

$$\{\mathfrak{p} : \rho((A \pmod{\mathfrak{p}})_{\overline{\mathbb{F}_p}}) > 2\}.$$

Having an eigenvalue $-p$ at a degree one prime $\mathfrak{p}$ is equivalent to having $a_{\mathfrak{p}} = 0$, i.e. it forces the characteristic polynomial to be of the form

$$1 + bT^2 + p^2T^4.$$

So we are back in usual Lang-Trotter territory: we expect $a_{\mathfrak{p}} = 0$ to happen

$$\sim \frac{\sqrt{X}}{\log X}$$

times for primes $\mathfrak{p}$ with $N\mathfrak{p} < X$.

The tyranny of split primes: Take $K/\mathbb{Q}$ Galois and A/K satisfies Sato-Tate. Assume that for non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, the variety A^σ is not geometrically isogenous to A. There are straightforward examples, e.g., for elliptic curves j has prime p in its denominator but each $j^\sigma, \sigma \neq 1$ does not have p.

Question 3 *Using only the primes*

$$\{\mathfrak{p} : \mathrm{Frob}_{\mathfrak{p}} \textit{ has given conjugacy class in } \mathrm{Gal}(K/\mathbb{Q})\},$$

do we still have the Sato-Tate distribution?

Example. Take $E/\mathbb{Q}(i)$ in Legendre form

$$y^2 = x(x-1)(x-\pi)$$

with π a gaussian prime such that $(\pi) \neq (\bar{\pi})$. For instance $\pi = 1+2i, 1+4i$, $2+3i$, etc. Are the primes $\{p \equiv 3 (\mathrm{mod}\ 4)\}$ OK for Sato-Tate? Numerical experiments suggest that this is so.

Now $\#E(\mathbb{F}_{p^2}) \equiv 0 (\mathrm{mod}\ 4)$ yields

$$N\mathfrak{p} + 1 - a_{\mathfrak{p}} \equiv 0 \pmod{4}.$$

But $N\mathfrak{p} \equiv 1 (\text{mod } 4)$ for any gaussian prime, so $a_{\mathfrak{p}} \equiv 2 (\text{mod } 4)$.In particular, $a_{\mathfrak{p}}$ is nonzero. So at any split prime, this curve is ordinary. If p is $\equiv 3 (\text{mod } 4)$, the supersingular possibilities are, a priori,

$$a_{\mathfrak{p}} \in \{-2p, -p, 0, p, 2p\}.$$

All but $-2p$ and $2p$ are excluded by the mod 4 congruence condition.
Assuming now that Sato-Tate holds for primes which are one mod four, the (heuristic) probability of being supersingular, i.e. of having $a_{\mathfrak{p}}$ at one of the extreme edges of possibilities, is $O(\frac{1}{p\sqrt{p}})$ which is summable. So it is plausible that this sort of Legendre curve over $\mathbb{Q}(i)$ has only finitely many supersingular primes.

Numerical experiments:

1. for $\pi = 2 + 3i$ or for $\pi = 1 + 4i$, there are no supersingular primes up to 3×10^7;

2. for $\pi = 2i$ we find 600959, 957119, and 88271039 as the only supersingular primes up to 10^9

Much remains to be done.