Nick Katz

6-28-08

Lang-Trotter revisited, and lower bounds for Frobenius traces:

Let $E/\mathbb{Q}$ be an elliptic curve with good red. outside Δ.

For $p \nmid \Delta$, $\#E(\mathbb{F}_p) = p+1-a(p)$.

We know via Hasse that

$$|a(p)| \leq 2\sqrt{p}.$$

Lang-Trotter try to predict: Given $A \in \mathbb{Z}$, is $A = a(p)$ for infinitely many p?

Congruence obstruction:

$X_1(11)$ has a rational pt. of order 5.

$\forall\, p \neq 11$, $p+1 \equiv a(p) \pmod 5$.

Can $a(p) = 1$? Not very often!

$\forall\, N \geq 2$, "mod N" rep. $\rho_N : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/N\mathbb{Z})$

$$\begin{tikzcd} Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[r] \arrow[d, two heads] & GL_2(\mathbb{Z}/N\mathbb{Z}) \\ \pi_1(\mathbb{Z}[1/N\Delta]) \arrow[ur, "\rho_N"'] & \\ \mathrm{Frob}_p \arrow[r, mapsto] & \rho_N(\mathrm{Frob}_p) \end{tikzcd}$$

$\mathrm{Frob}_p \in \pi_1(\mathbb{Z}[1/N\Delta])$, $p \nmid N\Delta$. (arith)

$tr(\rho_N(\mathrm{Frob}_p)) \equiv a(p) \pmod N$

$det(\rho_N(\mathrm{Frob}_p)) \equiv p \pmod N$.

$\mathrm{Image}(\rho_N) \subset GL_2(\mathbb{Z}/N\mathbb{Z})$.

If $A \bmod N$ is not the trace of an elt. of this image, then at most finitely many primes p can have $a(p) \equiv A \pmod N$. In this case we say there is a "congruence construction at N."

Weak Lang-Trotter conj: Given $E/\mathbb{Q}$, given $A \in \mathbb{Z}$, then $\exists$ ∞'ly many p with $a(p) = A$ iff A has no congruence obstruction.

Known cases:

$A = 0$, $E/\mathbb{Q}$ — CM: $a(p)=0$ w/ density $1/2$

— non CM: $a(p)=0$ ∞'ly many p (Elkies)

E/K = # field. LT $\Rightarrow$ $\exists$ ∞'ly many $\wp$ w/ $a(\wp)=2$.

$E: y^2 = x^3 - x$

$a(p)=2 \Leftrightarrow p = 1+16n^2$ (conj. to be prime ∞'ly often!)

The natural next step since we cannot make progress over $\mathbb{Q}$ is to look at the functional field case.

E/K K - fctn field of proj. smooth. geom. conn. curve $X/\mathbb{F}_q$.

This spreads out to $\mathcal{E}/V$, $V \subset X$ dense open set.

For a closed pt $\wp \in V$, $\mathbb{F}_\wp$

$\#E(\mathbb{F}_\wp) = N\wp + 1 - a(\wp)$. Still have $|a(\wp)| \le 2\sqrt{N\wp}$.

(Bombieri): via Baker - Wustholz if $E/\mathbb{F}_q$ (i.e. coefficient are constant in f.f. case) if s.s., then $q^{n/2} \mid a(q^n) \Rightarrow a(q^n)=0$ or $|a(q^n)| \ge q^{n/2}$. If ordinary, then $|a(q^n)| \to \infty$.

From this, clearly it won't work in this case. It is also no good if E/V has a constant j-invariant.

Assume E/V has a nonconstant j. Shrink V so that E/V is ordinary (throw out finitely many points, which is fine b/c j is nonconstant.) Now at least can't prove it is false.

$\forall N \ge 2$, prime to $p = \mathrm{char}(\mathbb{F}_q)$, have a mod N rep.

for p^ν, there is a 1-dim rep.

$$\rho_{p^\nu} : \pi_1(\mathcal{V}) \longrightarrow (\mathbb{Z}/p^\nu)^\times$$

If $N\wp \geq p^\nu$, $\rho_{p^\nu}(\mathrm{Frob}_\wp) \equiv a(\wp) \mod p^\nu$.

At least in this case one can cook up some examples.

$N \geq 3$ prime to p, $\mathbb{F}_q$, $q \equiv 1 \pmod N$.

$\mathcal{M}_{\Gamma(N)}$ lives over $\mathbb{Z}[\frac{1}{N}, \zeta_N]$ to start. If we fix

an N^{th} root of unity in $\mathbb{F}_q$, then we have

$\mathcal{M}_{\Gamma(N)} \otimes \mathbb{F}_q$.

$N \geq 4$ prime to p.

$\mathcal{M}_{\Gamma_1(N)} \otimes \mathbb{F}_q$ over $\mathbb{Z}[\frac{1}{N}]$ take universal curve...

Given $A \equiv a(\wp)$, then $a(\wp) \equiv 1 + \underbrace{N\wp}_{\text{power of } q} \pmod N$.

So the only conceivable A : $\exists$ power q^{k_0} of q s.t. (need k_0 to be prime to $\varphi(N)$) Say $q \equiv 1 \pmod N$.

$$A \equiv 1 + q^{k_0} \pmod N.$$

Suppose we are given A, $p \nmid A$, and $|A| \leq 2\sqrt{q}$. (general now)

<u>Honda:</u> $\exists\, E/\mathbb{F}_q$ with $a(q) = A$.

$$x^2 - Ax + q \text{ is char. poly. of } F.$$

<u>Deligne:</u> As $p \nmid A$, $\exists$ such an E s.t. $E(\mathbb{F}_q)$ is cyclic.

Choose $k \gg 0$ s.t. $q^{k_0} \equiv q^k \pmod N$, then $|A| \leq 2\sqrt{q^k}$.

We also have $A \equiv 1 + q^k \pmod N \Rightarrow \exists\, E/\mathbb{F}_{q^k}$ - pt of order N and $a(q^k) = A$. But we needed a closed pt! To get this, take $k = \ell$ a prime. Then $E/\mathbb{F}_{q^\ell}$ that gives A. The only obstruction to being a closed pt is if it came from $E_0/\mathbb{F}_q$. This cannot happen though from Bombieri above.