Introduction to Galois Representations
Applications

NATO ASI, Ohrid 2014

Arithmetic of Hyperelliptic Curves

August 25 - September 5, 2014

Ohrid, the former Yugoslav Republic of Macedonia,

Francesco Pappalardi
Dipartimento di Matematica e Fisica
Università Roma Tre

Plan for today

Topics

- Short summery of Tuesday's Lecture
- Facts about Elliptic curves over finite fields
- Serre's Cyclicity Conjecture
- Lang–Trotter Conjecture for fixed traces
- Lang–Trotter Conjecture for primitive points
- Artin primitive roots Conjecture

Elliptic curves

WEIERSTRASS EQUATION: $E : Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{Z};$

DISCRIMINANT OF E: $\Delta_E = 4a^3 - 27b^2$

- $\Delta_E = (\alpha_1 - \alpha_2)^2(\alpha_3 - \alpha_2)^2(\alpha_3 - \alpha_1)^2$
  ($\alpha_1, \alpha_2, \alpha_3$ roots of $X^3 + aX + b$);
- $\Delta_E = 0 \iff X^3 + aX + b$ has a double root!

Definition

if $\Delta_E \neq 0 \implies E$ is called ELLIPTIC CURVE

Group of Rational Points

If $K/\mathbb{Q}$ is an extension. Then

$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$$

The n-torsion subgroups

If $n \in \mathbb{N}$ $\qquad E[n] := \{P \in E(\overline{\mathbb{Q}}) \mid nP = \infty\}$

- $E[n] \subset E(\overline{\mathbb{Q}}) \cong \overline{\mathbb{Q}}/\mathbb{Z} \times \overline{\mathbb{Q}}/\mathbb{Z}$ is a subgroup
- $E[n] \cong C_n \oplus C_n$
- $E[2] = \{(\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0), \infty\}$
  ($\alpha_1, \alpha_2, \alpha_3$ roots of $x^3 + ax + b$)
- $E[3]$ is the set of inflection points
- If n is odd, $P = (\alpha, \beta) \in E[n] \implies \psi_n(\alpha) = 0$,
  ψ_n is n–division polynomials ($\partial\psi_n = (n^2 - 1)/2$ if n odd)
- $E : y^3 = x^3 - 2x \implies E[2] = \{(0, 0), (\sqrt{2}, 0), (-\sqrt{2}, 0), \infty\}$

Representation on n-torsion points

The n–torsion field: $$\mathbb{Q}(E[n]) = \bigcap_{K^2 \supset E[n]\setminus\{\infty\}} K$$

- $\mathbb{Q}(E[n])$ is Galois over $\mathbb{Q}$
- $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \subseteq \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$

$$\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

$$\sigma \mapsto \{(x,y) \mapsto (\sigma(x),\sigma(y))\}$$

Injective representation

Theorem (Serre)

If $E/\mathbb{Q}$ is not CM. Then $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$ only for finitely many ℓ.

Conjecture ($\ell \leq 37$)

Reducing modulo primes

Facts about elliptic curves over finite fields

- p prime, $p \nmid \Delta_E$
- $E(\mathbb{F}_p) = \{(X,Y) \in \mathbb{F}_p^2 \mid Y^2 = X^3 + aX + b\} \cup \{\infty\}$
- $E(\mathbb{F}_p) \cong C_k \oplus C_{nk}$ for some $k \mid p-1$
- $k = 1$ above iff $E(\mathbb{F}_p)$ is cyclic
- $\#E(\mathbb{F}_p) = p + 1 - a_p$ (a_p is the TRACE OF FROBENIUS)
- HASSE BOUND: $|a_p| \leq 2\sqrt{p}$;
- $\Psi_p : E(\overline{\mathbb{F}_p}) \to E(\overline{\mathbb{F}_p}), (x,y) \mapsto (x^p, y^p)$
  it is an endomorphism of $E/\mathbb{F}_p$
- $\Psi_p \in \mathrm{End}(E)$ satisfies $T^2 - a_pT + p$
- $\mathbb{Z}[\Psi_p] \subset \mathrm{End}(E)$
- If the equality hold above, we say that E is *ordinary* at p. Otherwise we say that it is *supersingular*
- $E/\mathbb{F}_p$ is supersingular $\iff E[p] = \{\infty\}$
  $\iff a_p = 0$

Serre's Cyclicity Conjecture

Let $E/\mathbb{Q}$ and set

$$\pi_E^{\text{cyclic}}(x) = \#\{p \le x : E(\mathbb{F}_p) \text{ is cyclic}\}.$$

Conjecture (Serre)

The following asymptotic formula holds

$$\pi_E^{\text{cyclic}}(x) \sim \delta_E^{\text{cyclic}} \frac{x}{\log x} \qquad x \to \infty$$

where

$$\delta_E^{\text{cyclic}} = \sum_{n=1}^{\infty} \frac{\mu(n)}{\# \operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})}$$

- Since $E(\mathbb{F}_p) \cong C_k \oplus C_{kn}$
  and $E[\ell] \cong C_\ell \oplus C_\ell$ for all $\ell \neq p$
  $E(\mathbb{F}_p)$ is cyclic iff $E[\ell] \not\subseteq E(\mathbb{F}_p) \forall \ell$ prime $\ell \neq p$
- So we may rewrite
  $$\pi_E^{\text{cyclic}}(x) = \#\{p \le x : E[\ell] \not\subseteq E(\mathbb{F}_p) \forall \ell \text{ prime }, \ell \neq p\}.$$

Serre's Cyclicity Conjecture

We can apply inclusion exclusion principle:

$$\begin{aligned}\pi_E^{\text{cyclic}}(x) = &\quad \#\{p \leq x : E[\ell] \not\subseteq E(\mathbb{F}_p) \forall \ell \text{ prime }, \ell \neq p\} \\ = &\quad \pi(x) - \sum_{\ell \text{ prime}} \pi_{E,\ell}(x) + \sum_{\ell_1,\ell_2 \text{ primes}} \pi_{E,\ell_1\ell_2}(x) - \cdots\end{aligned}$$

where $\pi(x) := \#\{p \leq x\}$ and if $k \in \mathbb{N}$,

$$\pi_{E,k}(x) := \#\{p \leq x : E[k] \subseteq E(\mathbb{F}_p)\}$$

Hence, if μ is the Möbius function, then

$$\pi_E^{\text{cyclic}}(x) = \sum_{k \in \mathbb{N}} \mu(k) \pi_{E,k}(x)$$

We will study $\pi_{E,k}(x)$ by mean of the Chebotarev density Theorem.

Chebotarev Density Theorem (from tuesday)

If $K/\mathbb{Q}$ be Galois and p is prime unramified in K, the *Artin Symbol*

$$\left[\frac{K/\mathbb{Q}}{p}\right] := \left\{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \begin{array}{l} \exists \mathfrak{p} \text{ prime of } K \text{ above } p \text{ s.t.} \\ \sigma\alpha \equiv \alpha^{N\mathfrak{p}} \bmod \mathfrak{p}\ \forall \alpha \in \mathcal{O} \end{array} \right\}$$

Note that $\left[\frac{K/\mathbb{Q}}{p}\right] = \{id\}$ then p splits completely in $K/\mathbb{Q}$
(i.e $p\mathcal{O} \subset \mathcal{O}$ is the product of $[K : \mathbb{Q}]$ prime ideals)

Theorem (Chebotarev Density Theorem)

Let $K/\mathbb{Q}$ be finite and Galois, and let $\mathcal{C} \subset \mathrm{Gal}(K/\mathbb{Q})$ be a union of conjugation classes. Then the density of the primes p such that $\left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}$ equals $\frac{\#\mathcal{C}}{\#\,\mathrm{Gal}(K/\mathbb{Q})}$.
In particular, if $\mathcal{C} = \{\mathrm{id}\}$, then the density of the primes p such that $\left[\frac{K/\mathbb{Q}}{p}\right] = \{\mathrm{id}\}$ equals $\frac{1}{\#\,\mathrm{Gal}(K/\mathbb{Q})}$.

If $K = \mathbb{Q}(E[n])$, then

$$E[n] \subset E(\mathbb{F}_p) \iff \left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right] = \{\mathrm{id}\}$$

Chebotarev Density Theorem and Serre's Cyclicity Conj.

If $K = \mathbb{Q}(E[n])$, then

$$E[n] \subset E(\mathbb{F}_p) \iff \left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right] = \{\mathrm{id}\}$$

Also recall that $\pi_{E,k}(x) := \#\{p \leq x : E[k] \subseteq E(\mathbb{F}_p)\}$

$$\begin{aligned}\pi_E^{\text{cyclic}}(x) &= \sum_{k\in\mathbb{N}} \mu(k)\pi_{E,k}(x) \\ &= \sum_{k\in\mathbb{N}} \mu(k)\# \left\{p \leq x : \left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right] = \{\mathrm{id}\}\right\}\end{aligned}$$

To proceed we need a quantitative versions of the Chebotarev Density Theorem. Let

$$\pi_{\mathcal{C}/\mathcal{G}}(x) := \# \left\{p \leq x : \left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}\right\}.$$

The quantitative Chebotarev Density Theorem

Let

$$\pi_{\mathcal{C}/\mathcal{G}}(x) := \#\left\{p \le x : \left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}\right\}.$$

Theorem (Chebotarev, Lagarias, Odlyzko, Serre, Murty, Saradha)

The Generalized Riemann Hypothesis implies

$$\pi_{\mathcal{C}/\mathcal{G}}(x) = \frac{\#\mathcal{C}}{\#\mathcal{G}} \int_2^x \frac{dt}{\log t} + O\left(\sqrt{\#\mathcal{C}}\sqrt{x}\log(xM\#\mathcal{G})\right)$$

where M is the product of primes numbers that ramify in $K/\mathbb{Q}$.

In the case of $K = \mathbb{Q}(E[k])$ and k is square free, the above specializes to

$$\pi_{E,k}(x) = \frac{1}{\#\,\mathrm{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})} \int_2^x \frac{dt}{\log t} + O\left(\sqrt{x}\log(xk)\right)$$

In the case of $K = \mathbb{Q}(E[k])$ and k is square free, the above specializes to

$$\pi_{E,k}(x) = \frac{1}{\#\,\mathrm{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})} \int_2^x \frac{dt}{\log t} + O\left(\sqrt{x}\log(xk)\right)$$

Hence

$$\pi_E^{\text{cyclic}}(x) = \sum_{k\in\mathbb{N}} \frac{\mu(k)}{\#\,\mathrm{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})} \int_2^x \frac{dt}{\log t} + \mathrm{ERROR}$$

The error can be estimated by standard analytic number theory
Finally

$$\delta_E^{\text{cyclic}} = \sum_{k=1}^{\infty} \frac{\mu(k)}{\#\,\mathrm{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})}.$$

The state of the Art on Serre's Cyclicity Conjecture

- Serre (1976): *GRH* $\Rightarrow \pi_E^{\text{cyclic}}(x) \sim \delta_E^{\text{cyclic}} \frac{x}{\log x}$
- Murty (1979): $E/\mathbb{Q}$ *CM* $\Rightarrow \pi_E^{\text{cyclic}}(x) \sim \delta_E^{\text{cyclic}} \frac{x}{\log x}$
- Gupta & Murty (1990): $\pi_E^{\text{cyclic}}(x) \gg \frac{x}{(\log x)^2}$ iff $E[2] \not\subseteq E[\mathbb{Q}]$
- Cojocaru (2003): *Simple proof and explicit error term for CM curves*
- Cojocaru & Murty (2004): *improved error terms depending on GRH*
- Serre: δ_E^{cyclic} is a rational multiple of

$$C = \prod_\ell \left(1 - \frac{1}{\ell(\ell-1)^2(\ell+1)}\right) = 0.81375190610681571\cdots$$

- Lenstra, Moree & Stevenhagen (2013): *If $E/\mathbb{Q}$ is a Serre curve then:*

$$\delta_E^{\text{cyclic}} = C \times \left(1 + \prod_{\ell \mid 2\,\text{disc}(\mathbb{Q}(\sqrt{\Delta_E}))} \frac{-1}{(\ell^2-1)(\ell^2-\ell)-1}\right)$$

Lang Trotter Conjecture for trace of Frobenius

Let $E/\mathbb{Q}$, $r \in \mathbb{Z}$ and set

$$\pi_E^r(x) = \#\{p \le x : p \nmid \Delta_E \text{ and } \#\overline{E}(\mathbb{F}_p) = p + 1 - r\}$$

Conjecture (Lang – Trotter (1970))

If either $r \neq 0$ or if E has no CM, then the following asymptotic formula holds

$$\pi_E^r(x) \sim C_{E,r} \frac{\sqrt{x}}{\log x} \qquad x \to \infty$$

where $C_{E,r}$ is the *Lang–Trotter constant*

$$C_{E,r} = \frac{2}{\pi} \frac{m_E \# \operatorname{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})_{\mathrm{tr}=r}}{\# \operatorname{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})} \times \prod_{\ell \nmid m_E} \frac{\ell \# \operatorname{GL}_2(\mathbb{F}_\ell)_{\mathrm{tr}=r}}{\# \operatorname{GL}_2(\mathbb{F}_\ell)}$$

and m_E is the *Serre's conductor* of E

- If E is a Serre's curve, then $m_E = [2, \operatorname{disc}(\mathbb{Q}(\sqrt{\Delta_E}))]$
- $\# \operatorname{GL}_2(\mathbb{F}_\ell)_{\mathrm{tr}=r} = \begin{cases} \ell^2(\ell-1) & \text{if } r = 0 \\ \ell(\ell^2 - \ell - 1) & \text{otherwise.} \end{cases}$

Lang Trotter Conjecture for trace of Frobenius

An application of ℓ–adic representations and of the Chebotarev density Theorem

Theorem (Serre)

Assume that $E/\mathbb{Q}$ is not CM or that $r \neq 0$ and that the Generalized Riemann Hypothesis holds. Then

$$\pi_E^r(x) \ll \begin{cases} x^{7/8}(\log x)^{-1/2} & \text{if } r \neq 0 \\ x^{3/4} & \text{if } r = 0. \end{cases}$$

- If $E/\mathbb{Q}$ is CM and $r = 0$. It is classical

$$\pi_E^0(x) \sim \frac{1}{2}\frac{x}{\log x} \qquad x \to \infty$$

- Murty, Murty and Sharadha: If $r \neq 0$, on GRH, $\pi_E^r(x) \ll x^{4/5}/(\log x)^{-1/5}$
- Elkies $\pi_E^0(x) \to \infty \quad x \to \infty$
- Elkies & Murty: GRH $\Longrightarrow \pi_E^0(x) \gg \log\log x$
- Average Versions later

Lang Trotter Conjecture for trace of Frobenius

Unvonditional Stetements

- *J. P. Serre (1981)*,

$$\pi_{E,r}(x) \ll \begin{cases} \frac{x(\log\log x)^2}{\log^2 x} & \text{if } r \neq 0 \\ x^{3/4} & \text{if } r = 0 \text{ and } E \text{ not CM} \end{cases}$$

- *N. Elkies, E. Fouvry, R. Murty (1996)*

$$\pi_{E,0}(x) \gg \log\log\log x / (\log\log\log\log x)^{1+\epsilon}$$

Chebotarev Density Theorem and Serre's Theorem on fixed traces

Let ℓ be sufficiently large such that

$$\mathcal{G} = \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$$

Set $\mathcal{C} = \mathrm{GL}_2(\mathbb{F}_\ell)_{\mathrm{tr}=r} = \{\sigma \in \mathrm{GL}_2(\mathbb{F}_\ell) : \mathrm{tr}\,\sigma = t\}$
So that

$$\#\,\mathrm{GL}_2(\mathbb{F}_\ell) = (\ell^2-1)(\ell^2-\ell)$$

and

$$\#\,\mathrm{GL}_2(\mathbb{F}_\ell)_{\mathrm{tr}=r} = \begin{cases} \ell^2(\ell-1) & \text{if } r=0 \\ \ell(\ell^2-\ell-1) & \text{otherwise.} \end{cases}$$

Then by Chebotarev Density Theorem on GRH,

$$\pi_{\mathcal{C}/\mathcal{G}}(x) = \frac{\#\mathcal{C}}{\#\mathcal{G}}\int_2^x \frac{dt}{\log t} + O\left(\sqrt{\#\mathcal{C}}\sqrt{x}\log(xM\#\mathcal{G})\right)$$
$$\ll \frac{1}{\ell}\frac{x}{\log x} + \ell^{3/2}\sqrt{x}\log(x\ell)$$

Chebotarev Density Theorem and Serre's Theorem on fixed traces

Finally recall (from tuesday) that if Φ_p is the Frobenius endomorphism,

$$\#E(\mathbb{F}_p) = p + 1 - r \quad \Longleftrightarrow \quad \mathrm{Tr}(\Phi_p) \equiv r$$

Hence for all ℓ sufficiently large,

$$\begin{aligned} \pi_E^r(x) &= \#\{p \le x : p \nmid \Delta_E \text{ and } \#E(\mathbb{F}_p) = p + 1 - r\} \\ &\le \#\{p \le x : p \nmid \Delta_E \text{ and } \mathrm{Tr}(\Phi_p) \equiv r \bmod p\} \\ &= \pi_{\mathcal{C}/\mathcal{G}}(x) \\ &\ll \frac{1}{\ell} \frac{x}{\log x} + \ell^{3/2} \sqrt{x} \log(x\ell) \end{aligned}$$

It is enough to choose $\ell = x^{1/5} (\log x)^{-4/5}$
To conclude that

$$\pi_E^r(x) \ll x^{4/5} (\log x)^{-1/5}$$

Average Lang Trotter Conjecture

Theorem (David, F. P. (1997))

Let

$$\mathcal{C}_x = \{E : Y^2 = X^3 + aX + b \ : 4a^3 + 27b^2 \neq 0 \text{ and } |a|, |b| \leq x \log x\}$$

Then

$$\frac{1}{|\mathcal{C}_x|} \sum_{E \in \mathcal{C}_x} \pi_{E,r}(x) \sim c_r \frac{\sqrt{x}}{\log x} \text{ as } x \to \infty$$

where

$$c_r = \frac{2}{\pi} \prod_l \frac{\ell |\operatorname{GL}_2(\mathbb{F}_\ell)^{\mathrm{tr}=r}|}{|\operatorname{GL}_2(\mathbb{F}_\ell)|}.$$

Theorem (N. Jones (2004))

Let

$$\mathcal{C}_x^{\text{Serre}} := \{E \in \mathcal{C}_x : E \text{ is a Serre curve}\}$$

Then

$$\lim_{x \to \infty} \frac{|\mathcal{C}_x^{\text{Serre}}|}{|\mathcal{C}_x|} = 1$$

In this sense almost all elliptic curves are Serre's curves

The General Lang–Trotter Conjecture

Definition (*General Lang–Trotter function*)

Let $K/\mathbb{Q}$ be a number field, Let E/K be an elliptic curve and set $f \mid [K:\mathbb{Q}]$. Define

$$\pi_E^{r,f}(x) = \#\{p \leq x \mid \deg_K(p) = f,\ \exists \mathfrak{p}|p, a_E(\mathfrak{p}) = r\}$$

Conjecture (The General Lang-Trotter Conjecture for Fixed Trace)

$\exists c_{E,r,f} \in \mathbb{R}^{\geq 0}$ such that

$$\pi_E^{r,f}(x) \sim c_{E,r,f} \begin{cases} \frac{x}{\log x} & \text{if } E \text{ has CM and } r = 0 \\ \frac{\sqrt{x}}{\log x} & \text{if } f = 1 \\ \log\log x & \text{if } f = 2 \\ 1 & \text{otherwise.} \end{cases}$$

Example. $K = \mathbb{Q}(i)$: $\pi^{r,1}$ counts split primes $\equiv 1 \bmod 4$;
$\pi^{r,2}$ counts inert primes $\equiv 3 \bmod 4$

Another Average result

Theorem (C. David & F.P. (2004))

Let $K = \mathbb{Q}(i)$, $r \in \mathbb{Z}$, $r \neq 0$ *and for* $\alpha, \beta \in \mathbb{Z}[i]$, *set* $E_{\alpha,\beta} : Y^2 = X^3 + \alpha X + \beta$. *Further let*

$$\mathcal{C}_x = \left\{ E_{\alpha,\beta} : \left| \begin{array}{l} \alpha = a_1 + a_2 i, \beta = b_1 + b_2 i \in \mathbf{Z}[i], \\ 4\alpha^3 - 27\beta^2 \neq 0 \\ \max\{|a_1|, |a_2|, |b_1|, |b_2|\} < x \log x \end{array} \right. \right\}$$

Then

$$\frac{1}{|\mathcal{C}_x|} \sum_{E \in \mathcal{C}_x} \pi_E^{r,2}(x) \sim c_r \log\log x.$$

where

$$c_r = \frac{1}{3\pi} \prod_{\ell > 2} \frac{\ell(\ell - 1 - \left(\frac{-r^2}{\ell}\right))}{(\ell - 1)(\ell - (-1\ell))}$$

Extended to the Average of the General Lang-Trotter function by Kevin James and Ethan Smith in 2011

Sketch of proof. 1/4

Definition (Kronecker–Hurwitz class numbers)

Let $d \in \mathbb{Z}$, $d \equiv 0, 1 \bmod 4$. Then

$$H(d) = 2 \sum_{f^2 | d} \frac{h\left(\frac{d}{f^2}\right)}{w\left(\frac{d}{f^2}\right)}$$

where

- $h(D) =$ class number
- $w(D)$ is number of units in $\mathbb{Z}[D + \sqrt{D}] \subset \mathbb{Q}(\sqrt{d})$

Theorem (Deuring's Theorem)

Let $q = p^n$, r odd (simplicity) with $r^2 - 4q < 0$.

$$\#\left\{ \begin{array}{l} \mathbb{F}_q - \textit{isomorphism classes of } E/\mathbb{F}_q \\ \textit{with } a_q(E) = r \end{array} \right\} = H(r^2 - 4q).$$

Sketch of proof. 2/4

Step 1: switch the order of summation

$$\begin{aligned}\frac{1}{|\mathcal{C}_x|}\sum_{E\in\mathcal{C}_x}\pi_{E,r}(x) &= \frac{1}{|\mathcal{C}_x|}\sum_{E\in\mathcal{C}_x}\sum_{\substack{p\le x\\ a_p(E)=r}} 1\\ &= \sum_{p\le x}\frac{|\{E\in\mathcal{C}_x : a_p(E)=r\}|}{|\mathcal{C}_x|}\\ &= \frac{1}{2}\sum_{p\le x}\frac{H(r^2-4p)}{p}+O(1)\end{aligned}$$

Theorem (Dirichlet Class Number Formula)

Let $\chi_d(n)=\left(\frac{d}{n}\right)$ and let $L(s,\chi_d)$ be the Dirichlet L–function. Then the class number

$$h(d)=\frac{\omega(d)|d|^{1/2}}{2\pi}L(1,\chi_d)$$

Next we use the definition of the Kronecker–Hurwitz class number

Sketch of proof. 3/4

Step 2. applying the class number formula

Let $d = (r^2 - 4p)/f^2$. Then

$$\frac{1}{2}\sum_{p\leq x}\frac{H(r^2-4p)}{p} = \frac{2}{\pi}\sum_{\substack{f\leq 2x\\(f,2r)=1}}\frac{1}{f}\sum_{\substack{p\leq x\\4p\equiv r^2 \bmod f^2}}\frac{L(1,\chi_d)}{p} + O(1)$$

So the problem is reduced to a special L–function value average. Analytic tools become relevant!!

Theorem (Barban–Davenport–Harberstam Theorem)

Let φ be the Euler function. Then for $1 \leq Q \leq x$ and $\forall c > 0$,

$$\sum_{q\leq Q}\sum_{a \bmod q}\left|\sum_{\substack{p\leq x\\p\equiv a \bmod q}}\log p - \frac{x}{\varphi(q)}\right|^2 \ll Qx\log x + \frac{x^2}{\log^c x}$$

Sketch of proof. 4/4

Lemma (Crucial analytic Lemma)

$\forall c > 0,$

$$\sum_{\substack{f\leq 2x\\ (f,2r)=1}} \frac{1}{f} \sum_{\substack{p\leq x\\ 4p\equiv r^2 \bmod f^2}} L(1,\chi_d)\log p = k_r x + O\left(\frac{x}{\log^c x}\right)$$

where

$$k_r = \frac{2}{3}\prod_{\ell>2} \frac{\ell - 1 - \left(\frac{-r^2}{\ell}\right)}{(\ell-1)(\ell - \left(\frac{-1}{\ell}\right))}$$

The rest is classical analytic number theory...

Lang Trotter Conjecture for Primitive points

Definition

Let $E/\mathbb{Q}$ and let $P \in E(\mathbb{Q})$ be of infinite order. P is called *primitive* for a prime p if the reduction $P \bmod p$ is a generator for $E(\mathbb{F}_p)$.

$$\langle P \bmod p \rangle = E(\mathbb{F}_p)$$

Set

$$\pi_{E,P}(x) = \#\{p \leq x : p \nmid \Delta_E \text{ and } P \text{ is primitive for } p\}$$

Conjecture (Lang–Trotter for primitive points (1976))

The following asymptotic formula holds

$$\pi_{E,P}(x) \sim \delta_{E,P} \frac{x}{\log x} \qquad x \to \infty.$$

with

$$\delta_{E,P} = \sum_{n=1}^{\infty} \mu(n) \frac{\#\mathcal{C}_{P,n}}{\# \operatorname{Gal}(\mathbb{Q}(E[n], n^{-1}P)/\mathbb{Q})}$$

where $\mathbb{Q}(E[n], n^{-1}P)$ is the extension of $\mathbb{Q}(E[n])$ of the coordinates of the points $Q \in E(\bar{\mathbb{Q}})$ such that $nQ = P$ and $\mathcal{C}_{P,n}$ is a union of conjugacy classes in $\operatorname{Gal}(\mathbb{Q}(E[n], n^{-1}P)/\mathbb{Q})$.

Statement of the Artin Conjecture

Conjecture (Artin Conjecture (1927))

Let $a \in \mathbb{Q} \setminus \{0, 1, -1\}$ and set

$$P_a(x) := \{p \leq x : \ a \text{ is a primitive root } \mod p\}.$$

Then there exists $\delta_a \in \mathbb{Q}^{\geq 0}$ such that

$$P_a(x) \sim \delta_a \prod_{\ell} \left(1 - \frac{1}{\ell(\ell-1)}\right) \times \pi(x)$$

Theorem (Hooley 1965)

Let $a \in \mathbb{Q} \setminus \{-1, 0, 1\}$ and assume GRH for all the Dedekind ζ–functions $\mathbb{Q}[e^{2\pi i/m}, a^{1/m}], m \in \mathbb{N}$. Then the Artin Conjecture holds:

$$P_a(x) = \delta_a \frac{x}{\log x} + O\left(\frac{x \log \log x}{\log^2 x}\right).$$

Lang–Trotter Conjecture, Serre's Cyclicity & Artin

three "sister" conjectures

Conjecture (Lang Trotter primitive points Conjecture(1977))

Let $P \in E(\mathbb{Q}) \setminus \mathrm{Tors}(E(\mathbb{Q}))$. $\exists \alpha_{E,P} \in \mathbb{Q}^{\geq 0}$ s.t.

$$\frac{\#\{p \leq x : p \nmid \Delta_E, E(\mathbb{F}_p^*) = \langle P \bmod p \rangle\}}{\pi(x)} \sim \alpha_{E,P} \prod_\ell \left(1 - \frac{\ell^3 - \ell - 1}{\ell^2(\ell-1)^2(\ell+1)}\right)$$

Conjecture (Serre's Cyclicity Conjecture (1976))

$\exists \gamma_{E,P} \in \mathbb{Q}^{\geq 0}$ s.t.

$$\frac{\#\{p \leq x : p \nmid \Delta_E, E(\mathbb{F}_p^*) \text{ is cyclic}\}}{\pi(x)} \sim \gamma_{E,P} \prod_\ell \left(1 - \frac{1}{(\ell^2-1)(\ell^2-\ell)}\right)$$

Conjecture (Artin Conjecture (1927))

Let $a \in \mathbb{Q} \setminus \{0, 1, -1\}$, $\exists \delta_a \in \mathbb{Q}^{\geq 0}$ s. t.

$$\frac{\#\{p \leq x : \ a \text{ primitive root } \bmod p\}}{\pi(x)} \sim \delta_a \prod_\ell \left(1 - \frac{1}{\ell(\ell-1)}\right)$$

Naive Densities

- The Artin Constant (primitive roots naive density)

$$A = \prod_{\ell} \left(1 - \frac{1}{\ell(\ell-1)}\right) = 0.3739558136192028\cdots$$

- The Lang Trotter first Constant (LTC naive density)

$$B = \prod_{\ell} \left(1 - \frac{\ell^3 - \ell - 1}{\ell^2(\ell-1)^2(\ell+1)}\right) = 0.4401473667920578 6\cdots$$

- The Serre's Constant (EC cyclicity naive density)
$C = \prod_\ell \left(1 - \frac{1}{\ell(\ell-1)^2(\ell+1)}\right) = 0.8137519061068157 1\cdots$

Comparison between empirical data: AC vs LTC vs SCC

Artin Conjecture

q	$P_q(2^{25})/\pi(2^{25})$	$A - P_q(2^{25})/\pi(2^{25})$
2	$0.37395508\cdots$	$0.0000007\cdots$
3	$0.37388094\cdots$	$0.0000748\cdots$
7	$0.37409997\cdots$	$-0.0001441\cdots$
11	$0.37422450\cdots$	$-0.0002686\cdots$
19	$0.37400887\cdots$	$-0.0000530\cdots$
23	$0.37402147\cdots$	$-0.0000656\cdots$
31	$0.37422208\cdots$	$-0.0002662\cdots$

Lang–Trotter Conjecture   Serre Cyclicity Conjecture

$$\pi_{E,P}(x) = \#\{p \le x : \langle P \bmod p\rangle = E(\mathbb{F}_p^*)\}$$

$$\pi_E^{\mathrm{cycl}}(x) = \#\{p \le x : E(\mathbb{F}_p^*) \text{ is cyclic}\}$$

SERRE'S CURVES OF RANK 1 (no torsion, Galois surjective $\forall \ell$)

E	$\frac{\pi_{E,P}(2^{25})}{\pi(2^{25})}$	$\alpha_{E,P}B - \frac{\pi_{E,P}(2^{25})}{\pi(2^{25})}$
37.a1	$0.44017485\cdots$	$-0.000027\cdots$
43.a1	$0.44034784\cdots$	$-0.000200\cdots$
53.a1	$0.44020198\cdots$	$-0.000054\cdots$
57.a1	$0.44016176\cdots$	$-0.000014\cdots$
58.a1	$0.44012203\cdots$	$0.000025\cdots$
61.a1	$0.44034299\cdots$	$-0.000195\cdots$
77.a1	$0.43964812\cdots$	$0.000499\cdots$
79.a1	$0.44043021\cdots$	$-0.000282\cdots$

E	$\frac{\pi_E^{\mathrm{cycl}}(2^{25})}{\pi(2^{25})}$	$\gamma_E C - \frac{\pi_E^{\mathrm{cycl}}(2^{25})}{\pi(2^{25})}$
37.a1	$0.81383047\cdots$	$-0.000078\cdots$
43.a1	$0.81363907\cdots$	$0.000112\cdots$
53.a1	$0.81389250\cdots$	$-0.000140\cdots$
57.a1	$0.81387263\cdots$	$-0.000120\cdots$
58.a1	$0.81374131\cdots$	$0.000010\cdots$
61.a1	$0.81397584\cdots$	$-0.000223\cdots$
77.a1	$0.81380285\cdots$	$-0.000050\cdots$
79.a1	$0.81392157\cdots$	$-0.000169\cdots$

Further Reading...

- COJOCARU, ALINA CARMEN, *Cyclicity pf CM Elliptic Curves modulo p* Trans. of the AMS **355**, 7, (2003) 2651–2662.
- DAVID, CHANTAL; PAPPALARDI, FRANCESCO, *Average Frobenius Distribution of Elliptic Curves*, Internat. Math. Res. Notices **4** (1999) 165–183.
- GUPTA, RAJIV; MURTY M. RAM, *Primitive points on elliptic curves*, Compositio Mathematica **58**, n. 1 (1986), 13–44.
- GUPTA, RAJIV; MURTY M. RAM, *Cyclicity and generation of points mod p on elliptic curves*, Inventiones mathematicae **101** 1 (1990) 225–235
- LANG, SERGE; TROTTER, HALE, Frobenius distributions in GL_2-extensions. Lecture Notes in Mathematics, Vol. 504. *Springer-Verlag*, Berlin–New York, 1976
- LANG, SERGE; TROTTER, HALE, *Primitive points on elliptic curves*. Bull. Amer. Math. Soc. **83** (1977), no. 2, 289–292.
- MURTY, M. RAM; MURTY, V. KUMAR; SARADHA, N., *Modular Forms and the Chebotarev Density Theorem,* American Journal of Mathematics, **110**, No. 2 (1988), 253–281
- SERRE, JEAN-PIERRE, Abelian ℓ-adic representations and elliptic curves. With the collaboration of Willem Kuyk and John Labute. Second edition. Advanced Book Classics. Addison-Wesley Publishing Company, *Advanced Book Program*, Redwood City, CA, 1989.
- SERRE, JEAN-PIERRE, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. (French) Invent. Math. **15** (1972), no. 4, 259–331.
- SERRE, JEAN-PIERRE, *Quelques applications du théorème de densité de Chebotarev*. (French) Inst. Hautes Études Sci. Publ. Math. No. **54** (1981), 323–401.