The average Lang Trotter Conjecture for imaginary quadratic fields

Francesco Pappalardi

Chennai - January, 2002

Notations.

- ELLIPTIC CURVE: $E : Y^2 = X^3 + aX + b$
  $(a, b \in \mathbb{Z}, \quad -\Delta_E = 4a^3 + 27b^2 \neq 0)$;

- $E(\mathbb{F}_p) = \{(X, Y) \in \mathbb{F}_p^2 \mid Y^2 = X^3 + aX + b\}$;

- TRACE OF FROBENIUS: $a_p(E) = p - \#E(\mathbb{F}_p)$;

- HASSE BOUND: $|a_p(E)| \leq 2\sqrt{p}$;

- LANG TROTTER FUNCTION: $r \in \mathbb{Z}$

$$\pi_E^r(x) = \#\{p \leq x \mid a_p(E) = r\}.$$

The Lang Trotter Conjecture

If $r \neq 0$ or E not CM,

$$\pi_E^r(x) \sim C_{E,r} \frac{\sqrt{x}}{\log x}, \quad C_{E,r} \geq 0.$$

$$\mathrm{Prob}(a_p(E) = r) \approx \frac{1}{2\sqrt{p}} \quad \Longrightarrow \quad \pi_E^r(x) \approx \sum_{p \leq x} \frac{1}{2\sqrt{p}} \sim \frac{\sqrt{x}}{\log x}.$$

State of the Art.

- *M. Deuring (1941):* If E has CM $\pi_{E,0}(x) \sim \frac{1}{2}\frac{x}{\log x}$;
- *J. P. Serre (1981), Elkies, Kaneko, K. Murty, R. Murty, N. Saradha, Wan (1988):*

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

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

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

(Stronger results on GRH)

Average Lang Trotter Conjecture

E. Fouvry, R. Murty (1996), C. David, F. P. (1997)

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

Then

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

where

$$c_r = \frac{2}{\pi} \prod_{l|r} \left(1 - \frac{1}{l^2}\right)^{-1} \prod_{l \nmid r} \frac{l(l^2 - l - 1)}{(l-1)(l^2-1)} = \frac{2}{\pi} \prod_{l} \frac{l|\operatorname{GL}_2(\mathbb{F}_l)^{\operatorname{Tr}=r}|}{|\operatorname{GL}_2(\mathbb{F}_l)|}.$$

Representation on n-torsion points.

For $n \in \mathbb{N}$

- $E[n] = \{P \in E(\mathbb{C}) \mid nP = \mathcal{O}\} \subset E(\mathbb{C})$ *(n-torsion subgroup);*
- $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$;
- $\mathbb{Q}(E[n]) = \bigcap_{\mathbb{K}^2 \supset E[n] \setminus \{\mathcal{O}\}} \mathbb{K}$; *($\mathbb{Q}(E[n])$ Galois over $\mathbb{Q}$);*
- $\mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$;

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

$$\sigma \mapsto \{(x_1, x_2) \mapsto (\sigma(x_1), \sigma(x_2))\}.$$

injective representation.

Theorem.(Serre) *If E not* CM, $\mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{F}_l)$ *except finitely many l.*

Chebotarev Density Thm. & Lang–Trotter Conj.

- p ramifies in $\mathbb{Q}(E[l]) \iff p|l\Delta_E$;
- $p \nmid l\Delta_E$, $\sigma_p \subset \mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q})$ (Frobenius conjugacy class);
- $\mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q}) \subseteq \mathrm{GL}_2(\mathbb{F}_l)$,
  σ_p has characteristic polynomial $T^2 - a_p(E)T + p$.
- $a_p(E) \equiv \mathrm{Tr}(\sigma_p) \bmod l$;
- $\pi_{E,r}(x) \leq \#\{p \leq x \mid a_p(E) \equiv r (\mathrm{mod} l)\}$;
- Chebotarev Density Theorem, $l \gg 0$,

$$\mathrm{Prob}(a_p(E) \equiv r \bmod l) \sim \frac{|\mathrm{GL}_2(\mathbb{F}_l)^{\mathrm{Tr}=r}|}{|\mathrm{GL}_2(\mathbb{F}_l)|}.$$

Lang–Trotter Constant

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

$\exists m_{E,r} \in \mathbb{N}$ s.t.

$$C_{E,r} = \frac{2}{\pi} \frac{m_{E,r} |\mathrm{Gal}(\mathbb{Q}(E[m_{E,r}])/\mathbb{Q})^{\mathrm{Tr}=r}|}{|\mathrm{Gal}(\mathbb{Q}(E[m_{E,r}])/\mathbb{Q})|} \prod_{l \nmid m_{E,r}} \frac{l |\,\mathrm{GL}_2(\mathbb{F}_l)^{\mathrm{Tr}=r}|}{|\,\mathrm{GL}_2(\mathbb{F}_l)|}.$$

More Notations.

- $\mathbb{K}$ finite Galois $/\mathbb{Q}$;
- E elliptic curve defined over $\mathcal{O}_{\mathbb{K}}$;
- Δ_E discriminant ideal of $E/\mathcal{O}_{\mathbb{K}}$;
- $p \in \mathbb{Z}$ unramified in $\mathbb{K}/\mathbb{Q}, p \nmid N(\Delta_E)$;
- $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$, $\mathfrak{p} \mid p$;
- $E_{\mathfrak{p}}$ reduction of E over $\mathcal{O}_{\mathbb{K}}/(\mathfrak{p})$;
- $E_{\mathfrak{p}}(\mathcal{O}_{\mathbb{K}}/(\mathfrak{p})) = N(\mathfrak{p}) + 1 - a_E(\mathfrak{p})$;
- Hasse bound $|a_E(\mathfrak{p})| \leq 2\sqrt{N(\mathfrak{p})}$;
- degree of p: $N(\mathfrak{p}) = p^{\deg_{\mathbb{K}}(p)}$.

A Variation of Lang–Trotter Conjecture

$f \mid [\mathbb{K}:\mathbb{Q}]$. *General Lang–Trotter function:*

$$\pi_E^{r,f}(x) = \#\left\{p \leq x \mid \deg_{\mathbb{K}}(p) = f,\ a_E(\mathfrak{p}) = r\right\}.$$

CONJECTURE: $\exists c_{E,r,f} \in \mathbb{R}^{\geq 0}$ *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. $\mathbb{K} = \mathbb{Q}(i)$: $\pi^{r,1} \leftrightarrow$ split primes $\equiv 1 \bmod 4$;
$\pi^{r,2} \leftrightarrow$ inert primes $\equiv 3 \bmod 4$

Statement of Today's Result

Theorem. (C. David & F. Pappalardi) $\mathbb{K} = \mathbb{Q}(i)$, $r \in \mathbb{Z}$, $r \neq 0$

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

Then

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

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

Sketch of proof. 1/8

Deuring's Thm. $q = p^n$, r *odd (simplicity), s.t.* $r^2 - 4q > 0$.

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

Kronecker class numbers: $H(r^2 - 4p^2) = 2 \sum_{f^2 \mid r^2 - 4p^2} \frac{h(\frac{r^2-4p^2}{f^2})}{w(\frac{r^2-4p^2}{f^2})}$.

$h(D) = $ class number, $w(D) = $ #units in $\mathbb{Z}[D + \sqrt{D}] \subset \mathbb{Q}(\sqrt{r^2 - 4p^2})$.

Step 1:
$$\frac{1}{|\mathcal{C}_x|} \sum_{E \in \mathcal{C}_x} \pi_E^{r,2}(x) = \frac{1}{2} \sum_{\substack{p \le x \\ p \equiv 3 \bmod 4}} \frac{H(r^2 - 4p^2)}{p^2} + O(1).$$

Sketch of proof. 2/8

Given $f^2 | r^2 - 4p^2$,

- $d = (r^2 - 4p^2)/f^2$ $(\equiv 1 \bmod 4)$;
- $\chi_d(n) = \left(\frac{d}{n}\right)$;
- $L(s, \chi_d)$ Dirichlet L–function;
- $h(d) = \frac{\omega(d)|d|^{1/2}}{2\pi} L(1, \chi_d)$ (class number formula).

Step 2.

$$\frac{1}{2} \sum_{\substack{p \le x \\ p \equiv 3 \bmod 4}} \frac{H(r^2 - 4p^2)}{p^2} = \frac{2}{\pi} \sum_{\substack{f \le 2x \\ (f,2r)=1}} \frac{1}{f} \sum_{\substack{p \le x \\ p \equiv 3 \bmod 4 \\ 4p^2 \equiv r^2 \bmod f^2}} \frac{L(1, \chi_d)}{p^2} + O(1).$$

Sketch of proof. 3/8

Lemma A. [Analytic] Let $d = (r^2 - 4p^2)/f^2$, $\forall c > 0$,

$$\sum_{\substack{f \le 2x \\ (f,2r)=1}} \frac{1}{f} \sum_{\substack{p \le x \\ p \equiv 3 \bmod 4 \\ 4p^2 \equiv r^2 \bmod f^2}} L(1, \chi_d) \log p = k_r x + O\left(\frac{x}{\log^c x}\right).$$

where

$$k_r = \sum_{f=1}^{\infty} \frac{1}{f} \sum_{n=1}^{\infty} \frac{1}{n\varphi(4nf^2)} \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \frac{a}{n} \quad \# \quad b \in (\mathbb{Z}/4nf^2\mathbb{Z})^* \quad \begin{matrix} b \equiv 3 \bmod 4, \\ 4b^2 \equiv r^2 - af^2(4nf^2) \end{matrix}.$$

Lemma B. [Euler product] With above notations,

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

Sketch of proof. 4/8

Start from

$$L(1,\chi_d) = \sum_{n\in\mathbb{N}} \frac{d}{n}\frac{1}{n} = \sum_{n\in\mathbb{N}} \frac{d}{n}\frac{e^{-n/U}}{n} + O\left(\frac{|d|^{3/16+\epsilon}}{U^{1/2}}\right)$$

follows from

$$\sum_{n\in\mathbb{N}} \frac{d}{n}\frac{e^{-n/U}}{n} = L(1,\chi_d) + \int_{\Re(s)=-\frac{1}{2}} L(s+1,\chi_d)\Gamma(s+1)\frac{U^s}{s}ds$$

applying Burgess, $L(1/2+it,\chi_d) \ll |t|^2|d|^{3/16+\epsilon}$ and obtain

$$\sum_{\substack{f\leq 2x\\(f,2r)=1}} \frac{1}{f} \sum_{\substack{p\leq x\\ p\equiv 3 \bmod 4\\ 4p^2\equiv r^2 \bmod f^2}} L(1,\chi_d)\log p = \sum_{\substack{f\leq 2x,\\ n\in\mathbb{N}\\ (f,2r)=1}} \frac{e^{-\frac{n}{U}}}{nf} \sum_{\substack{p\leq x\\ p\equiv 3 \bmod 4\\ 4p^2\equiv r^2 \bmod f^2}} \frac{d}{n} \log p + O\left(\frac{x^{11/8+\epsilon}}{U^{1/2}}\right)$$

Sketch of proof. 5/8

$$\sum_{\substack{f\le 2x\\(f,2r)=1}}\frac{1}{f}\sum_{\substack{p\le x\\p\equiv 3 \bmod 4\\4p^2\equiv r^2 \bmod f^2}} L(1,\chi_d)\log p = \sum_{\substack{f\le V,\\ n\le U\log U\\(f,2r)=1}}\frac{e^{-\frac{n}{U}}}{nf}\sum_{\substack{p\le x\\p\equiv 3 \bmod 4\\4p^2\equiv r^2 \bmod f^2}}\left(\frac{d}{n}\right)\log p+O\left(\frac{x}{\log^c x}\right)$$

where $U=x^{1-\epsilon}$. Easy to deal with $f>V=(\log x)^a, n>U\log U$.

Since $\left(\frac{d}{n}\right)$ character modulo $4n$

$$\sum_{\substack{p\le x\\p\equiv 3 \bmod 4\\4p^2\equiv r^2 \bmod f^2}}\left(\frac{d}{n}\right)\log p = \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{p\le x,\ p\equiv 3 \bmod 4\\(r^2-4p^2)/f^2\equiv a \bmod 4n}}\log p$$

$$= \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*}\left(\frac{a}{n}\right)\sum_{\substack{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^*\\b\equiv 3 \bmod 4\\4b^2\equiv r^2-af^2 \bmod 4nf^2}}\psi_1(x,4nf^2,b)$$

where as usual $\psi_1(x,4nf^2,b)=\sum_{2\le p\le x,\ p\equiv b \bmod 4nf^2}\log p$

Sketch of proof. 6/8

Write $E_1(x, 4nf^2, b) = \psi_1(x, 4nf^2, b) - \frac{x}{\varphi(4nf^2)}$,

$$C_r(a,n,f) = \left\{ b \in (\mathbb{Z}/4nf^2\mathbb{Z})^* \;\middle|\; \begin{array}{c} b \equiv 3 \bmod 4, \\ 4b^2 \equiv r^2 - af^2 \bmod 4nf^2 \end{array} \right\}.$$

Then

$$\sum_{\substack{p \le x \\ p \equiv 3 \bmod 4 \\ 4p^2 \equiv r^2 \bmod f^2}} \left(\frac{d}{n}\right) \log p = x \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) \frac{\#C_r(a,n,f)}{\varphi(4nf^2)} + \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \left(\frac{a}{n}\right) \sum_{\substack{b \in (\mathbb{Z}/4nf^2\mathbb{Z})^* \\ b \equiv 3 \bmod 4 \\ 4b^2 \equiv r^2 - af^2 \bmod 4nf^2}} E_1(x, 4nf^2, b)$$

Sketch of proof. 7/8

$$\text{Error term} = \sum_{\substack{f\le V,\\ n\le U\log U\\ (f,2r)=1}} \frac{e^{-\frac{n}{U}}}{nf} \sum_{a\in(\mathbb{Z}/4n\mathbb{Z})^*} \frac{a}{n} \sum_{b\in C_r(a,n,f)} E_1(x,4nf^2,b) \le$$

$$\le \sum_{\substack{f\le V\\ (f,2r)=1}} \frac{1}{f} \sum_{n\le U\log U} \frac{e^{-n/U}}{n} \sum_{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^*} |E_1(x,4nf^2,b)| \le$$

$$\le \sum_{f\le V} \frac{1}{f} \left(\sum_{n\le U\log U} \frac{\varphi(4nf^2)}{n^2} \right)^{1/2} \left(\sum_{n\le U\log U} \sum_{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^*} E_1(x,4nf^2,b)^2 \right)^{1/2}$$

$$\ll \sqrt{\log U} \sum_{f\le V} f \left(\sum_{m\le 4V^2U\log U} \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^*} E_1(x,m,b)^2 \right)^{1/2}.$$

Proof. 8/8

(Barban, Davenport, Halberstam Theorem) for $x > Q \geq x/\log^k x$

$$\sum_{m \leq Q} \sum_{b \in (\mathbb{Z}/m\mathbb{Z})^*} E_1(x,m,b)^2 \ll Qx \log x$$

$$\text{Error Term} \ll \frac{x}{\log^c x}.$$

Main Term:

$$x \sum_{\substack{f \leq V, \\ n \leq U \log U \\ (f,2r)=1}} \frac{e^{-\frac{n}{U}}}{nf} \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \frac{a}{n} \frac{\#C_r(a,n,f)}{\varphi(4nf^2)} =$$

$$= x \sum_{\substack{f,n \in \mathbb{N} \\ (f,2r)=1}} \frac{1}{nf\varphi(4nf^2)} \sum_{a \in (\mathbb{Z}/4n\mathbb{Z})^*} \frac{a}{n} \#C_r(a,n,f) + O\left(\frac{x}{\log^c x}\right)$$

QED

Question.

Given

- $h(T) = a_0 + a_1 T + \cdots + a_k T^k \in \mathbb{Z}[T]$;
- $m \in \mathbb{N}$;
- p prime, $m \mid f(p)$;
- Set $\chi(n) = \left(\frac{f(p)/m}{n}\right)$.

$$\sum_{\substack{p \le x \\ m \mid f(p)}} L(1,\chi) \log p = \delta_{f,m} x + O\left(\frac{x}{m^{\epsilon} \log^c x}\right)?$$

Note: if $\deg h \le 2$ *then done!*

Interesting Example. $h(T) = r^2 - 4x^T$;

Application to average number of elliptic curves over $\mathbb{F}_{p^k}$ $(k \ge 3)$.