# مقدّمه الى المنحنيات الاهليليجيه
# و التخمين حسب لانگ و تروتر

فرانچسكو پاپالاردي

بيروت ٢١ ذي الهجّرة ١٤٢٢

# What is an Elliptic curve?

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

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

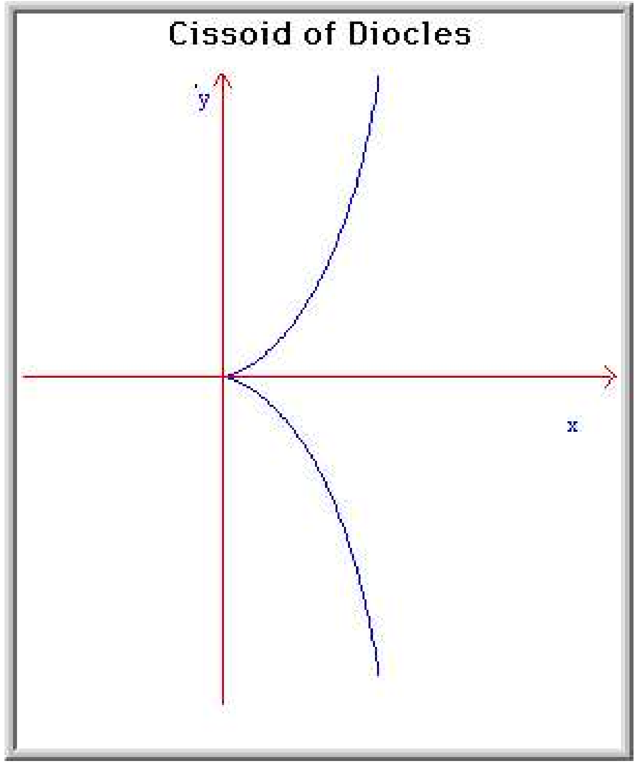
**Note:**

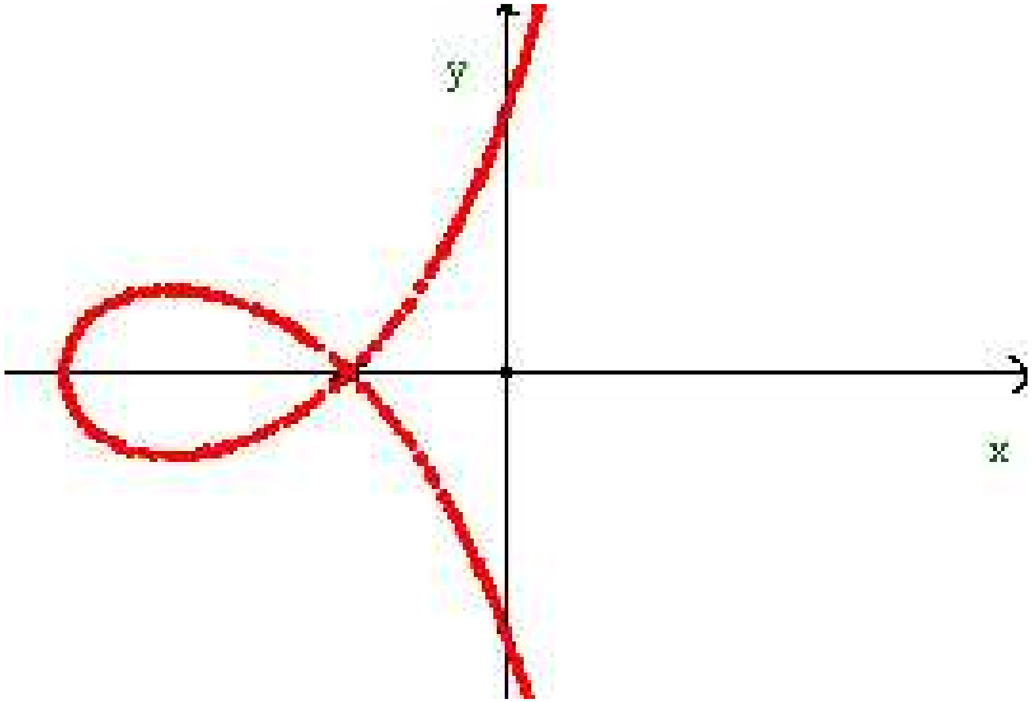
- $\Delta_E = (\alpha_1 - \alpha_2)^2(\alpha_3 - \alpha_2)^2(\alpha_3 - \alpha_1)^2$
  $(\alpha_1,\ \alpha_2,\ \alpha_3$ *roots of* $X^3 + aX + b);$
- $\Delta_E = 0 \iff X^3 + aX + b$ has a double root!

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

## Pictures of Cubic Equations: (2/4)

**Singular case** (i.e. $\Delta_E = 0$),

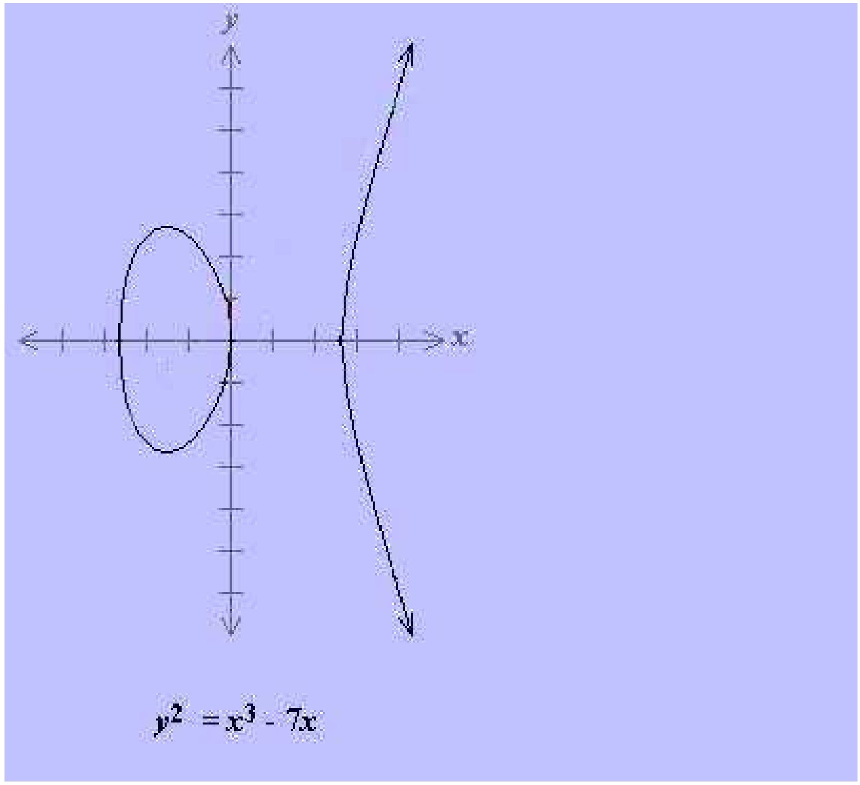


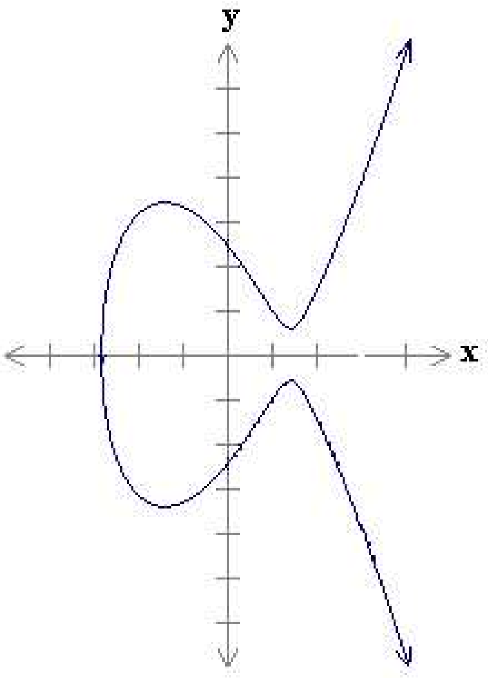




$(0,0)$ has 1 double tangent, 2 distinct tangents.

# Pictures of Cubic Equations: (1/2)

**Non singular case** (i.e. $\Delta_E \neq 0$),



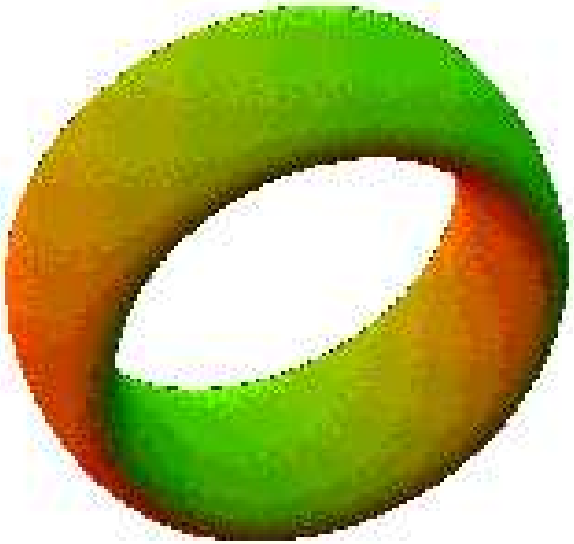

$X^3 + aX + b$ has 3 real roots

1 real root

# Elliptic curve over $\mathbb{C}$

**Complex points:**

$E(\mathbb{C}) =$

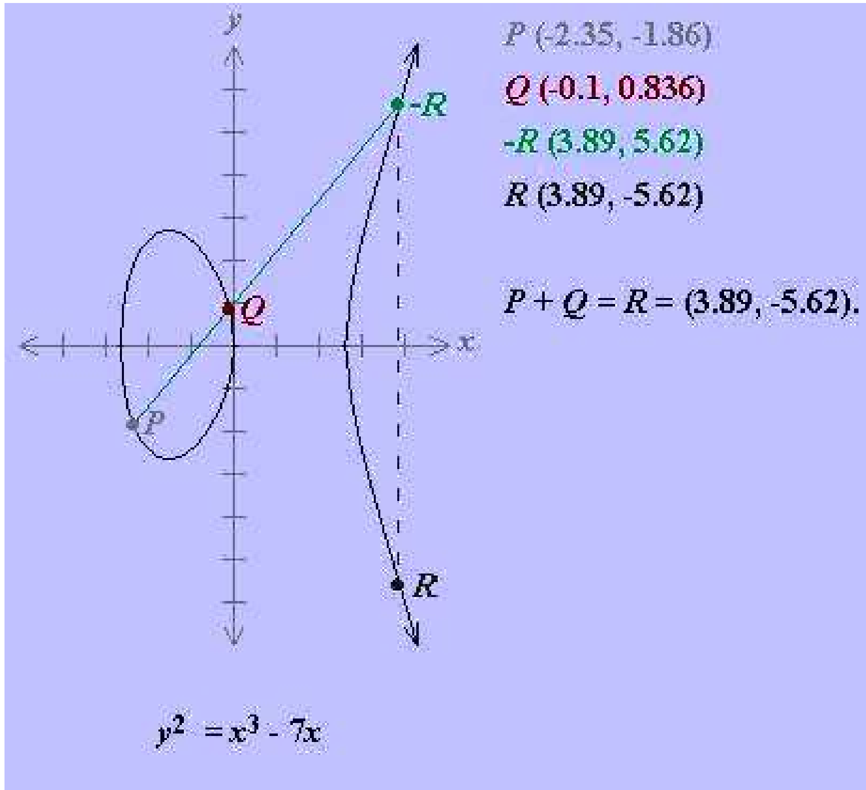


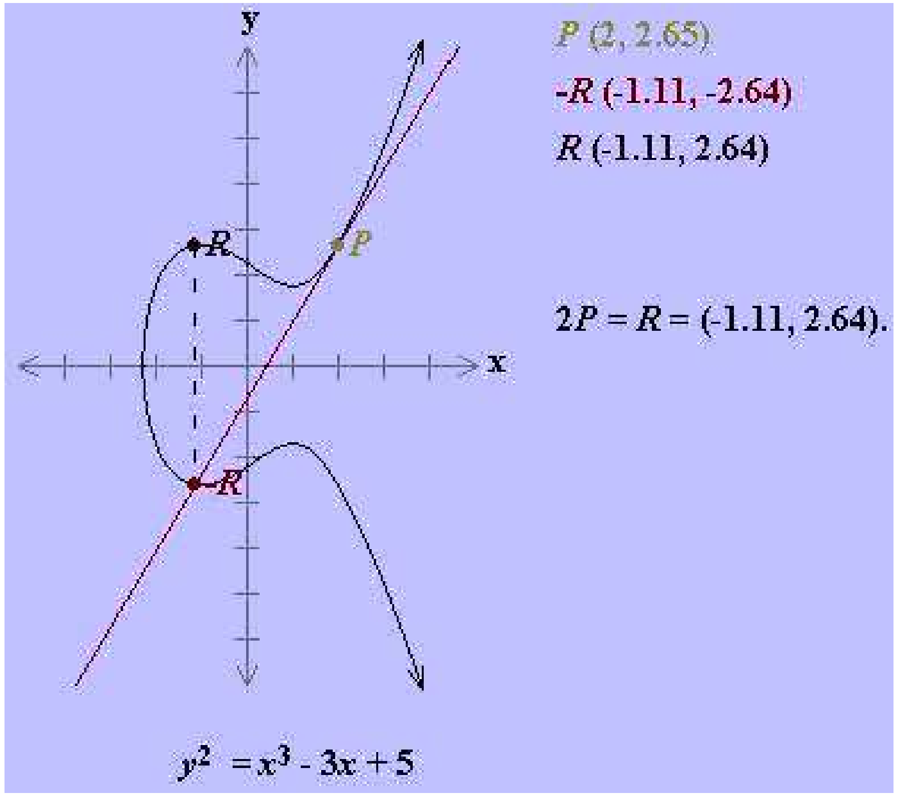
$\cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$

*An abelian group!!*

# Addition Law on Elliptic Curves

*"The line through any two points of an elliptic curve always meets the curve in exactly another point"*




$P \oplus Q \oplus R = \varnothing \iff P, Q, R$ are on the same line

## Group law with other words

$\mathbb{K} \supseteq \mathbb{Q}$ is a field, $\mathcal{O}$ a "*point at infinity*" (top of $y$-axis)

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

For $P_1, P_2 \in E(\mathbb{K})$

$$r(P_1, P_2) = \text{straight line in } \mathbb{C}^2 \text{ from } P_1 \text{ to } P_2,$$

Convention:

$r(P_1, P_1)$ = tangent line to $E(\mathbb{C})$ at $P_1$;

$r(P_1, \mathcal{O})$= vertical line at $P_1$;

$r(\mathcal{O}, \mathcal{O}) = \{\mathcal{O}\}$.

$$E(\mathbb{C}) \bigcap r(P_1, P_2) = \{P_1, P_2, P_3\} \quad \& \quad P_3 \in E(\mathbb{K}).$$

GROUP STRUCTURE ON $E(\mathbb{K})$ $\boxed{P_1 \oplus P_2 \oplus P_3 = \mathcal{O}}$

## Multiplication formulas 1/2.

$P = (x_1, y_1)$, $Q = (x_2, y_2) \in E(\mathbb{Q})$

- $P \oplus Q = (\lambda^2 - x_1 - x_2, (2x_1 + x_2 - \lambda^2)\lambda - y_2)$ where

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

If $P = (x, y) \in E(\mathbb{Q})$

- $P \oplus P = [2]P = (\frac{(3x+a)^2}{4y^2} - 2x, (x - \frac{(3x+a)^2}{4y^2} - 2x)\frac{3x^2+a}{2y} - y)$

## Multiplication formulas 2/2.

If $P = (x, y) \in E(\mathbb{Q})$ (or in $E(\mathbb{K})$),

$$[n]P = \begin{cases} \left(x - 4y^2 \frac{f_{n+1}f_{n-1}}{f_n^2}, y\frac{f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2}{f_n^3}\right) & \text{if } n \text{ is odd} \\ \left(x - \frac{f_{n+1}f_{n-1}}{4y^2 f_n^2}, \frac{f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2}{16y^3 f_n^3}\right) & \text{if } n \text{ is even} \end{cases}$$

$f_n \in \mathbb{Z}[x]$ called $n$–*division polynomials*

$$f_0 = 0, \quad f_1 = 1, \quad f_2 = 1, \quad f_3 = 3x^4 + 6ax^2 + 12bx - a^2,$$

$$f_4 = 2(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),$$

$$f_{2m+1} = \begin{cases} f_{m+2}f_m^3 - (4x^3 + 4ax + 4b)f_{m-1}f_{m+1}^3 & \text{if } m \text{ is odd, } m \geq 3 \\ (4x^3 + 4ax + 4b)^2 f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3 & \text{if } m \text{ is even, } m \geq 2 \end{cases}$$

$$f_{2m} = \left(f_{m+2}f_{m-1}^2 - f_{m-2}f_{m+1}^2\right) f_m, \qquad m > 2$$

# What kind of group is $E(\mathbb{Q})$?

$\mathbb{K}$ finite field extension of $\mathbb{Q}$.

**Theorem (Mordell Weil).** *$E(\mathbb{K})$ is a finitely generated Abelian group.* □

$$\Longrightarrow \boxed{E(\mathbb{K}) \cong \mathbb{Z}^r \oplus \mathrm{Tor}(E(\mathbb{K}))}$$

- $r = \mathrm{rank}(E(\mathbb{K}))$
- $\mathrm{Tor}(E(\mathbb{K})) = \{P \in E(\mathbb{K}) \mid [n]P = \mathcal{O},\ \exists n \in \mathbb{N}\}.$ (finite)

**Theorem (Mazur).**

$$\mathrm{Tor}(E(\mathbb{Q})) \cong \begin{cases} \mathbb{Z}/N\mathbb{Z},\ \ N = 1, 2, \ldots, 10 & \textit{or} \\ \mathbb{Z}/12\mathbb{Z} & \textit{or} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, N = 1, \ldots, 4. \end{cases}$$

# Records!

**S. Fermigier (1996)**

$$E : y^2 = x^3 - 12186281750382032063222317965030959123x+$$
$$+4995627314275003346233751126834109716556367836229944 78$$

$$\mathrm{rank}(E(\mathbb{Q})) \geq 22$$

$$E : y^2 = x^3 - 1386747x + 368636886$$

$$\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$$

## $n$-torsion subgroups.

$n \in \mathbb{N}$ $$E[n] = \{P \in E(\mathbb{C}) \mid nP = \mathcal{O}\}.$$

- $E[n] \subset E(\mathbb{C}) \cong \mathbb{C}/\mathbb{Z} \times \mathbb{C}/\mathbb{Z}$;
- $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
- $E[2] = \{(\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0), \mathcal{O}\}$ $(\alpha_1, \alpha_2, \alpha_3$ roots of $x^3 + ax + b)$.
- $E[3]$ is the set of inflection points;
- If $P = (\alpha, \beta) \in E[n] \implies f_n(\alpha) = 0$, $f_n$ is $n$–division polynomials $(\partial f_n = (n^2 - 1)/2$ if $n$ odd$)$.

$$E : y^3 = x^3 - 2x \Longrightarrow E[2] = \{(0,0), (\sqrt{2}, 0), (-\sqrt{2}, 0), \mathcal{O}\}.$$

# Representation on $n$-torsion points

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

- $\mathbb{Q}(E[n])$ is the splitting field of $f_n$ (division polynomials)
- $\mathbb{Q}(E[n])$ 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).** $\mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q}) \neq \mathrm{GL}_2(\mathbb{F}_l)$ only for finitely many $l$. **Conjecture.** $E$ not CM $\Longrightarrow \quad l \leq 41$

## Reducing modulo primes

- $p$ prime, $p \nmid \Delta_E$;
- $E_p = \{(X, Y) \in \mathbb{F}_p^2 \mid Y^2 = X^3 + aX + b\} \cup \{\mathcal{O}\}$;
- $E_p$ is a finite group (excellent for Cryptography);
- $\#E_p = p + 1 - a_p(E)$ ($a_p(E)$ is the Trace of Frobenius);
- Hasse bound: $|a_p(E)| \leq 2\sqrt{p}$;
- Lang Trotter function: $r \in \mathbb{Z}$, $E$ elliptic curve

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

- The Lang Trotter Conjecture: if $r \in \mathbb{Z} \setminus \{0\}$,

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

## Computing the $\#E_p$

Extremely important for

1. Cryptography;
2. Lenstra's Factoring Algorithm.

Two efficient Algorithms to compute $a_p(E)$:

- Schoof's algorithm (1984) **SEA**;

  *good for large characteristics (p large)*

- Satoh's algorithm (2000).

  *good for very small characteristics*

# SEA Record.

Date: Fri, 27 Jan 1995 08:31:06 EST

to: Number Theory List <NMBRTHRY@NDSUVM1.BITNET>

From: Francois Morain <morainpolytechnique.fr> (with R. Lercier )

Subject: $\#E_{10^{499}+153}$

The number of points on $Y^2 = X^3 + 4589 * X + 91228$ modulo $p = 10^{499} + 153$ is $p + 1 - t$ where $t$ is

5531712505360656916297653020318487459872397403254686568065996317
0112741379929457444426115606162586501422237972934053155035899388
8032237207379679849162325347608624510817409606791818935212167258
0436106733206830434953965949226510594406908149864694178969.

The algorithm is the Schoof-Elkies-Atkin algorithm.

Total time was the equivalent of 4200 hours (including 2900 hours for $X^p$) on a DEC 3000 - M300X (running with DEC OSF/1 V3.0) on several DEC alpha's of different types/processors.

# Computing $a_p$! Record with Satoh

$$E : y^2 + xy = x^3 + a_6 \text{ over } \mathbb{F}_{2^{8009}} = \mathbb{F}_2[x]/(x^{8009} + x^{3159} + 1)$$

$$a_6 = 0x3F636F6420707520737277746168570$$

is ASCII encoding (ISO-8859-1) of:

`What's up doc?`

$$E_{2^{8009}} = 2^{8009} + 1 - a_q$$

$a_q = -$17378149685594750502663500286963595380822933538157005646462119394089505686350478329402199506511963606403774445812182470625610137509222778589927985938237550881351222845270754344880422783035045363031828999342995504854485827143123555492592521801602146297652260480619999262960763361539904566574812040349729572481861270581173700193287323971397603133330712119203114012493671611026134429999234346261809470788338123957569235406267517774312808492870478992705390275752742617858435029461809834041469208533041196458220109508446398689194968075677256945577617529809841962758062023088140569701683784391173249003421959273604438212331467792983817285353774705442794273977446148471220998599947677749428708057483893707967448370865437766774878223251230907188543743371846062602461954573022985733585945296159149982779473118032339677677469399798074962839080605378520850947719776739982522235914473325897684462049958915633164608595632215687149327930873471961114801333048429224220685255589456315042900333035718583585795982719859853933656740181710300520394197995947070862975337672119759738829977044161535194629382784749657469972262477586456885200921027091523639543300481998246149254354076621958725963487702977031745623495061636260095

2001. **New record** over $\mathbb{F}_{2^{16001}}$ due to *R. Harley and J. F. Mestre*

# Lang Trotter Conjecture:

$$\pi_E^r(x) = \#\{p \le x \mid a_p(E) = r\} \sim C_{E,r} \frac{\sqrt{x}}{\log x}$$

$C_{E,r}$ is defined in terms of the $E[m]$'s

$$C_{E,r} = \lim_{m \to \infty}^{\times} \frac{2}{\pi} \frac{m|\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})^{\mathrm{Tr}=r}|}{|\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})|}$$

**Consequence of Serre's Theorem:** $\exists m_{E,r} \in \mathbb{N}$ such that

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

## State of the Art on the Lang–Trotter Conjecture

- *$M.$ *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*

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

*where*

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

# 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);
- $\mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q}) \subseteq \mathrm{GL}_2(\mathbb{F}_l)$,
  $\sigma_p$ has characteristic polynomial $T^2 - a_p(E)T + p$;
- $a_p(E) \equiv \mathrm{Tr}(\sigma_p) \bmod l$;
- $\pi_{E,r}(x) \leq \#\{p \leq x \mid a_p(E) \equiv r (\bmod l)\}$;
- Chebotarev Density Theorem, $l \gg 0$,
  $$\mathrm{Prob}(a_p(E) \equiv r \bmod l) \sim \frac{|\mathrm{GL}_2(\mathbb{F}_l)^{\mathrm{Tr}=r}|}{|\mathrm{GL}_2(\mathbb{F}_l)|}.$$

## More Notations

- $\mathbb{K}$ finite Galois $/\mathbb{Q}$;
- $E$ elliptic curve defined over $\mathcal{O}_{\mathbb{K}}$;
- $\Delta_E$ 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:*

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

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) $\mathbb{K}=\mathbb{Q}(i)$, $r\in\mathbb{Z}$, $r\neq 0$

$$\mathcal{C}_x=\left\{E:Y^2=X^3+\alpha X+\beta \;\middle|\; \begin{array}{l}\alpha=a_1+a_2i,\beta=b_1+b_2i\in\mathbf{Z}[i],\\ 4\alpha^3-27\beta^2\neq 0\\ \max\{|a_1|,|a_2|,|b_1|,|b_2|\}<x\log x\end{array}\right\}$$

*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. 1/3

**Deuring's Theorem** $q = p^n$, $r$ *odd (simplicity) with* $r^2 - 4q > 0$.

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

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

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

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

## Sketch of proof. 2/3

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. 3/3

**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,

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