Almost prime orders of CM elliptic curves modulo p.

Jorge Jimenez Urroz

Banff, 21 May 2008

Introduction

Let $E/\mathbb{Q}$ be an elliptic curve given by

$$y^2 = x^3 + ax + b.$$

Introduction

Let $E/\mathbb{Q}$ be an elliptic curve given by

$$y^2 = x^3 + ax + b.$$

Then,

$$E(\mathbb{Q}) \simeq E_{\text{tors}}(\mathbb{Q}) \otimes \mathbb{Z}^{r(E)}.$$

Introduction

Let $E/\mathbb{Q}$ be an elliptic curve given by

$$y^2 = x^3 + ax + b.$$

Then,

$$E(\mathbb{Q}) \simeq E_{\text{tors}}(\mathbb{Q}) \otimes \mathbb{Z}^{r(E)}.$$

Moreover, for any given prime $p \nmid 6N(E)$

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \otimes \mathbb{Z}/d_p e_p\mathbb{Z}$$

Questions

- When is $E(\mathbb{F}_p)$ cyclic?

Questions

- When is $E(\mathbb{F}_p)$ cyclic?

- Given $E/\mathbb{Q}$ with $r(E) \geq 1$, $P \in E(\mathbb{Q})/E_{\text{tors}}(\mathbb{Q})$,

  When $< P \bmod p >= E(\mathbb{F}_p)$?

Questions

- When is $E(\mathbb{F}_p)$ cyclic?
- Given $E/\mathbb{Q}$ with $r(E) \geq 1$, $P \in E(\mathbb{Q})/E_{\text{tors}}(\mathbb{Q})$,

  When $< P \bmod p >= E(\mathbb{F}_p)$?
- When $|E(\mathbb{F}_p)|$ is prime?

Cyclicity

Conjecture: (Borosh-Moreno-Porta) Let $E/\mathbb{Q}$ be an elliptic curve. There exist a constant C_E such that

$$\Pi_E(x) = \#\{p \le x \,:\, E(\mathbb{F}_p) \text{ is cyclic}\} \sim C_E \frac{x}{\log x}.$$

Cyclicity

Conjecture: (Borosh-Moreno-Porta) Let $E/\mathbb{Q}$ be an elliptic curve. There exist a constant C_E such that

$$\Pi_E(x) = \#\{p \le x \;:\; E(\mathbb{F}_p) \text{ is cyclic}\} \sim C_E \frac{x}{\log x}.$$

- Proved by Serre in 1976 under GRH, with an explicit constant C_E, which is non zero precisely when $[\mathbb{Q}(E[2]) : \mathbb{Q}] > 1$.

Cyclicity

Conjecture: (Borosh-Moreno-Porta) Let $E/\mathbb{Q}$ be an elliptic curve. There exist a constant C_E such that

$$\Pi_E(x) = \#\{p \le x \,:\, E(\mathbb{F}_p) \text{ is cyclic}\} \sim C_E \frac{x}{\log x}.$$

- Proved by Serre in 1976 under GRH, with an explicit constant C_E, which is non zero precisely when $[\mathbb{Q}(E[2]) : \mathbb{Q}] > 1$.
- In 1979 Murty prove the conjecture unconditionally for CM curves.

Primitive points

Conjecture: (Lang-Trotter, 1976) Given $E/\mathbb{Q}$ with $r(E) > 1$, $P \in E(\mathbb{Q})$ free, there exist $C_{E,P}$ such that if

$$A_{E,P}(x) = \{p \leq x \ :< P \bmod p >= E(\mathbb{F}_p)\},$$

then

$$|A_{E,P}(x)| \sim C_{E,P} \frac{x}{\log x}.$$

Primitive points

Given $E/\mathbb{Q}$ with CM by O_K, $r(E) \geq 1$, $P \in E(\mathbb{Q})$ free, let

$$\Pi_{E,P}^{\text{split}}(x) = \#\{p \in A_{E,P}(x) \; : \; p \text{ splits in } O_K\}.$$

Primitive points

Given $E/\mathbb{Q}$ with CM by O_K, $r(E) \geq 1$, $P \in E(\mathbb{Q})$ free, let

$$\Pi_{E,P}^{\text{split}}(x) = \#\{p \in A_{E,P}(x) \; : \; p \text{ splits in } O_K\}.$$

Theorem: (Gupta-Murty, 1987) Under GRH we have

$$\Pi_{E,P}^{\text{split}}(x) \sim C_{E,P} \frac{x}{\log x}$$

Remark: The constant $C_{E,P}$ is positive whenever $2, 3$ are inert or $K = \mathbb{Q}(\sqrt{-11})$.

Primitive points

Theorem: (Gupta-Murty, 1987) Whenever $r(E) \geq 6$, there is a finite explicit set, $S \in E(\mathbb{Q})$ such that $|A_{E,P}(x)| \to \infty$ unconditionally for some $P \in S$.

Primitive points

Theorem: (Gupta-Murty, 1987) Whenever $r(E) \geq 6$, there is a finite explicit set, $S \in E(\mathbb{Q})$ such that $|A_{E,P}(x)| \to \infty$ unconditionally for some $P \in S$.

Theorem: (Gupta-Murty, 1987)

$$\#\{p \leq x : \; p \text{ splits }, |< P \bmod p >| < x^{\frac{1}{2}-\epsilon}\} = o(x)$$

$$\#\{q \leq x : \; q \text{ inert }, |< P \bmod q >| < x^{\frac{1}{3}-\epsilon}\} = o(x)$$

Prime Order

Conjecture: (Koblitz, 1988) Let $E/\mathbb{Q}$ be an elliptic curve not isogenus to one with nontrivial $\mathbb{Q}$ torsion. Then,

$$\Pi_E^{\text{prime}}(x) = \#\{p \leq x : |E(\mathbb{F}_p)| \text{ is prime}\} \sim C_E \frac{x}{\log^2 x}.$$

Remark: It is not known a single example of curve for which the conjecture is true. Why?

Prime Order

Conjecture: (Koblitz, 1988) Let $E/\mathbb{Q}$ be an elliptic curve not isogenus to one with nontrivial $\mathbb{Q}$ torsion. Then,

$$\Pi_E^{\text{prime}}(x) = \#\{p \le x : |E(\mathbb{F}_p)| \text{ is prime}\} \sim C_E \frac{x}{\log^2 x}.$$

Remark: It is not known a single example of curve for which the conjecture is true. Why?
Consider the CM case.

$$|E(\mathbb{F}_p)| = N(\pi_p - 1), \quad \pi_p \in O_K,$$

Hence, $\pi_p = 1 + \tilde{\pi}_p$, is the twin prime conjecture in the ring O_K.

Prime Order, known results.

Theorem:(Balog-Cojocaru-David, Preprint)

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\Pi_E^{\text{prime}}(x)\sim C\frac{x}{\log^2 x}.$$

Prime Order, known results.

Theorem:(Balog-Cojocaru-David, Preprint)

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\Pi_E^{\text{prime}}(x)\sim C\frac{x}{\log^2 x}.$$

Find the smallest n such that

$\#\{p\leq x\ :\ |E(\mathbb{F}_p)|=P_n\}\gg\frac{x}{\log^2 x}$

Prime Order, known results.

Theorem:(Balog-Cojocaru-David, Preprint)

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\Pi_E^{\text{prime}}(x)\sim C\frac{x}{\log^2 x}.$$

Find the smallest n such that
$\#\{p\leq x\ :\ |E(\mathbb{F}_p)|=P_n\}\gg\frac{x}{\log^2 x}$

- (Miri-Murty) , GRH, non CM, $n\leq 16$.

Prime Order, known results.

Theorem:(Balog-Cojocaru-David, Preprint)

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\Pi_E^{\text{prime}}(x)\sim C\frac{x}{\log^2 x}.$$

Find the smallest n such that
$\#\{p\le x\ :\ |E(\mathbb{F}_p)|=P_n\}\gg\frac{x}{\log^2 x}$

- (Miri-Murty) , GRH, non CM, $n\le 16$.
- (Steuding-Weng), GRH, $n\le 9$, and $n\le 4$ if CM.

Prime Order, known results.

Theorem:(Balog-Cojocaru-David, Preprint)

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\Pi_E^{\text{prime}}(x)\sim C\frac{x}{\log^2 x}.$$

Find the smallest n such that
$\#\{p\le x\ :\ |E(\mathbb{F}_p)|=P_n\}\gg\frac{x}{\log^2 x}$

- (Miri-Murty) , GRH, non CM, $n\le 16$.
- (Steuding-Weng), GRH, $n\le 9$, and $n\le 4$ if CM.
- (Cojocaru), CM $n\le 5$

Prime Order, known results.

Theorem:(Balog-Cojocaru-David, Preprint)

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\Pi_E^{\text{prime}}(x)\sim C\frac{x}{\log^2 x}.$$

Find the smallest n such that
$\#\{p\le x\ :\ |E(\mathbb{F}_p)|=P_n\}\gg\frac{x}{\log^2 x}$

- (Miri-Murty) , GRH, non CM, $n\le 16$.
- (Steuding-Weng), GRH, $n\le 9$, and $n\le 4$ if CM.
- (Cojocaru), CM $n\le 5$
- (Iwaniec-Jiménez Urroz), $n\le 2$ for $y^2=x^3-x$.

Almost prime orders.

Theorem: (Jiménez Urroz) Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by O_K. Then,

$$\#\{p \le x, p \text{ splits } : \frac{1}{d_E}|E(\mathbb{F}_p)| = P_2\} \gg \frac{x}{\log^2 x}$$

Almost prime orders.

Theorem: (Jiménez Urroz) Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by O_K. Then,

$$\#\{p \le x, p \text{ splits } : \frac{1}{d_E}|E(\mathbb{F}_p)| = P_2\} \gg \frac{x}{\log^2 x}$$

Remark: The method allow us to improve on primitive points in the following way.

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by O_K with $r(E) \ge 1$, and $P \in E(\mathbb{Q})$ free. Then

$$\#\{q \le x : q \text{ inert }, | < P \bmod q > | > x^{0.44}\} \gg \frac{x}{\log^2 x}$$

Proof of the remark.

The Theorem gives an explicit constant such that

$$\#\{p \leq x, : \frac{1}{d_E}|E(\mathbb{F}_p)| = P_2\} \gg \frac{x}{\log^2 x}$$

Proof of the remark.

The Theorem gives an explicit constant such that

$$\#\{p \leq x, : \frac{1}{d_E}|E(\mathbb{F}_p)| = P_2\} \gg \frac{x}{\log^2 x}$$

We know that

$$\#\{q \leq x \ : \ | < P \bmod q > | < x^{1/3}\} = o(x).$$

Proof of the remark.

The Theorem gives an explicit constant such that

$$\#\{p \le x, : \frac{1}{d_E}|E(\mathbb{F}_p)| = P_2\} \gg \frac{x}{\log^2 x}$$

We know that

$$\#\{q \le x \ : \ | < P \bmod q > | < x^{1/3}\} = o(x).$$

By sieve, find β such that

$$\#\{p \le x, : q||E(\mathbb{F}_p)|, x^{1/3} < q < x^{\beta}\} < (C - \epsilon)\frac{x}{\log^2 x}.$$

For inert primes use results of Cai and Wu for the best constant in the twin prime conjecture.

The constant d_E

D	(g_4, g_6)	d_E
-4	$(-g^4, 0), (4g^4, 0)$	8
-4	$(m^2, 0), (-m^2, 0)$	4
-4	$(m, 0)$	2
-8	$(-30g^2, -56g^3)$	2
-3	$(0, g^6), (0, -27g^6)$	12
-3	$(0, m^3)$	4
-3	$(0, m^2), (0, -27m^2)$	3
-3	$(0, m)$	1
-7	$(-140g^2, -784g^3)$	4
$-D \geq 11$	(g_4, g_6)	1

The constant d_E

Corollary: Any $E/\mathbb{Q}$ with CM curve by $K = \mathbb{Q}(\sqrt{-D})$, $D \geq 11$ does not have rational torsion.

The constant d_E

Corollary: Any $E/\mathbb{Q}$ with CM curve by $K = \mathbb{Q}(\sqrt{-D})$, $D \geq 11$ does not have rational torsion.

Proof: Note that for any prime $\lambda \in O_K$, $|(O_K/\lambda O_K)^*| \geq 3$ and use Čebotarev density theorem.

Proof of Main Theorem

Based on the formula

$$|E(\mathbb{F}_p)| = N(\pi_p - 1),$$

for some explicit π_p above p in O_K. Recently Rubin and Silverberg have given a general formula, valid in particular for any CM curve over $\mathbb{Q}$.

Consider the sequence

$$\mathcal{A}(x) = \left\{ a = N\left(\frac{\pi_p - 1}{\delta_E}\right),\ \pi \in \mathcal{P}(x) \right\}.$$

The problem is a typical sieve problem.

Proof of Main Theorem

Use the weighted sum

$$\sum_{\substack{a \in \mathcal{A}(x) \\ (a, P(z)Q(z)p_K)=1}} \left\{ 1 - \sum_{\substack{p_0 | a \\ z < p_0 \leq y}} \frac{1}{2} - \sum_{\substack{a = p_1 p_2 p_3 \\ z < p_3 \leq y < p_2 < p_1}} \frac{1}{2} \right\}$$

Proof of Main Theorem

Use the weighted sum

$$\sum_{\substack{a \in \mathcal{A}(x) \\ (a, P(z)Q(z)p_K)=1}} \left\{ 1 - \sum_{\substack{p_0 | a \\ z < p_0 \leq y}} \frac{1}{2} - \sum_{\substack{a = p_1 p_2 p_3 \\ z < p_3 \leq y < p_2 < p_1}} \frac{1}{2} \right\}$$

To control the error term, we need a Bombieri-Vinogradov type theorem in two different contexts, first in the ring O_K, and then for elements

$$\omega = \delta_E \pi_1 \pi_2 \pi_3 .$$

Finally, one key ingredient is remove the inert primes from the sequence before sieving in order to increase the level of distribution of the sequence.