How often is $\#E(\mathbb{F}_p)$ squarefree?

S. Akhtari, C. David, H. Hahn & L. Thompson

Counting points on elliptic curves

Squarefree values of $\#E(\mathbb{F}_p)$

An upper bound for π_E^{SF}

Generalizations and average results

How often is $\#E(\mathbb{F}_p)$ squarefree?

S. Akhtari, C. David, H. Hahn & L. Thompson

January 12, 2013

Definitions

Definition

An *elliptic curve* is a curve given by an equation of the form

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

where $a, b \in \mathbb{Q}$ and $\Delta := -16(4a^3 + 27b^2)$ is nonzero.

We can represent the set of points on an elliptic curve as

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

where $\mathcal{O}$ is the point at infinity.

So, $\#E(\mathbb{Q}) = 1 + \#(\text{rational solutions to } y^2 = x^3 + ax + b)$.

Counting points on $E/\mathbb{F}_p$

How often is $\#E(\mathbb{F}_p)$ squarefree?

S. Akhtari, C. David, H. Hahn & L. Thompson

Counting points on elliptic curves

Squarefree values of $\#E(\mathbb{F}_p)$

An upper bound for π_E^{SF}

Generalizations and average results

We can reduce $E/\mathbb{Q}$ to a curve over $\mathbb{F}_p$:

$$E(\mathbb{F}_p) := \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 \equiv x^3 + ax + b \pmod{p}\} \cup \{\mathcal{O}\}.$$

Example: Consider $E : y^2 = x^3 + 2x + 1$ over $\mathbb{F}_5$.

x	$x^3 + 2x + 1 \pmod{5}$	y
0	1	1, 4
1	4	2, 3
2	3	–
3	4	2, 3
4	3	–

$\therefore \#E(\mathbb{F}_5) = 2 + 2 + 2 + 1 = 7.$

Counting points on $E/\mathbb{F}_p$

We can reduce $E/\mathbb{Q}$ to a curve over $\mathbb{F}_p$:

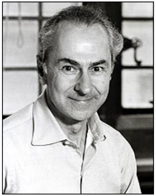
$$E(\mathbb{F}_p) := \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 \equiv x^3 + ax + b \mod p\} \cup \{\mathcal{O}\}.$$

Remark

$\#E(\mathbb{F}_p) = p + 1 - a_p(E)$, where $|a_p(E)| \leq 2\sqrt{p}$.

There are a number of theorems (and open conjectures!) concerning how often $\#E(\mathbb{F}_p)$ takes on certain values.

Fixed integer values of $a_p(E)$



Conjecture (Lang-Trotter, 1976)

Let $\pi_{E,t} := \#\{p \leq X : a_p(E) = t\}$. If E is a non-CM elliptic curve or if $t \neq 0$, then

$$\pi_{E,t}(X) \sim C_{E,t} \cdot \frac{\sqrt{X}}{\log X}$$

.

Prime values of $p+1-a_p(E)$

Conjecture (Koblitz, 1988)

Let $\pi_{E,\text{prime}} := \#\{p \le X : \#E(\mathbb{F}_p)$ is prime$\}$. Then

$$\pi_{E,\text{prime}}(X) \sim C_{E,\text{prime}} \cdot \frac{X}{(\log X)^2}.$$

Counting points on elliptic curves

Squarefree values of $\#E(\mathbb{F}_p)$

An upper bound for π_E^{SF}

Generalizations and average results

Squarefree values of $p + 1 - a_p(E)$

- When E is a CM curve, Cojocaru obtained the correct proportion of primes p for which $p + 1 - a_p(E)$ is squarefree.

Squarefree values of $p+1-a_p(E)$

How often is $\#E(\mathbb{F}_p)$ squarefree?

S. Akhtari, C. David, H. Hahn & L. Thompson

Counting points on elliptic curves

Squarefree values of $\#E(\mathbb{F}_p)$

An upper bound for π_E^{SF}

Generalizations and average results

- When E is a CM curve, Cojocaru obtained the correct proportion of primes p for which $p+1-a_p(E)$ is squarefree.
- When E is a non-CM curve, Cojocaru showed how to obtain the correct proportion by assuming the GRH, Pair Correlation Conjecture and Artin Holomorphy Conjecture.

An (unconditional) conjecture for non-CM curves

Conjecture

Let E be a non-CM elliptic curve defined over $\mathbb{Q}$. Let $\pi_E^{SF} = \#\{p \leq X : p + 1 - a_p$ is squarefree$\}$. As $X \to \infty$, we have

$$\pi_E^{SF}(X) \sim C_E^{SF} \pi(X),$$

where C_E^{SF} is the predicted constant.

An (unconditional) upper bound

Theorem (Akhtari, David, Hahn, T., 2012)

Let E be a non-CM elliptic curve defined over $\mathbb{Q}$. For X sufficiently large (depending on E), and any $\varepsilon > 0$, we have

$$\pi_E^{SF}(X) \leq C_E^{SF}\, \pi(X) \left(1 + O\left(\frac{1}{(\log\log X)^{1-\varepsilon}}\right)\right).$$

Key Lemmas

Lemma (Effective Chebotarev Density Theorem)

Let $K = \mathbb{Q}(E[n])$, *and* C *a union of conjucacy classes in* $\mathrm{Gal}(K/\mathbb{Q})$. *For all* X *such that* $\log X \gg_E n^{12}(\log n)^2$, *we have*

$$\pi_{C,K}(X) = \frac{|C|}{|\mathrm{Gal}(K/\mathbb{Q})|}\pi(X) + O\left(X \exp\left(-\frac{A}{n^2}\sqrt{\log X}\right)\right),$$

where A *is an absolute constant.*

Proof Sketch

Let

$$P(z) := \prod_{\ell \leq z} \ell$$

and let $G_E(n)$ be a particular subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$. Let

$$\Omega_E(P(z)^2) := \left\{ g \in G_E(P(z)^2) \mid \ell^2 \nmid (\det g + 1 - \operatorname{tr} g), \ \forall \ell \leq z \right\}.$$

Proof Sketch

Let

$$P(z) := \prod_{\ell \leq z} \ell$$

and let $G_E(n)$ be a particular subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$. Let

$$\Omega_E(P(z)^2) := \left\{ g \in G_E(P(z)^2) \mid \ell^2 \nmid (\det g + 1 - \operatorname{tr} g),\ \forall \ell \leq z \right\}.$$

By the Effective CDT, we have

$$\begin{aligned} \pi_E^{SF}(X) &\leq \#\{p \leq X : \ell^2 \nmid p + 1 - a_p(E),\ \forall \ell \leq z\} \\ &= \pi(X) \cdot \left| \frac{\Omega_E(P(z)^2)}{G_E(P(z)^2)} \right| + O(X \exp(-\frac{A}{P(z)^4}\sqrt{\log X})), \end{aligned}$$

for X sufficiently large.

Proof Sketch

Let

$$C_E(n) = \{g \in G_E(n) : \det g + 1 - \operatorname{tr} g \equiv 0 \pmod{n}\}.$$

Proof Sketch

Let

$$C_E(n) = \{g \in G_E(n) : \det g + 1 - \mathrm{tr}\ g \equiv 0 \pmod{n}\}.$$

Using the Möbius function to detect squares, we have

$$\begin{aligned} \frac{|\Omega_E(P(z)^2)|}{|G_E(P(z)^2)|} &= \sum_{n \mid P(z)} \mu(n) \frac{|C_E(n^2)|}{|G_E(n^2)|} \\ &= C_E^{SF} + O\left(\sum_{n \geq z} \frac{|C_E(n^2)|}{|G_E(n^2)|} \right). \end{aligned}$$

Proof Sketch

Use a matrix-counting argument to bound

$$\sum_{n \geq z} \frac{|C_E(n^2)|}{|G_E(n^2)|} \ll_E \frac{1}{z^{1-\varepsilon}}.$$

Proof Sketch

Use a matrix-counting argument to bound

$$\sum_{n \geq z} \frac{|C_E(n^2)|}{|G_E(n^2)|} \ll_E \frac{1}{z^{1-\varepsilon}}.$$

Choose the largest possible z so that the error term is still smaller than the main term. This yields

$$\pi_E^{SF} \leq C_E^{SF} \cdot \pi(X) \left(1 + O_E\left(\frac{1}{(\log\log X)^{1-\varepsilon}}\right)\right).$$

A generalization

Instead of just looking at $p+1-a_p(E)$, we could examine other sequences of values associated with the reduction of E over $\mathbb{F}_p$.

A generalization

Instead of just looking at $p+1-a_p(E)$, we could examine other sequences of values associated with the reduction of E over $\mathbb{F}_p$.

Example How often is $a_p(E)^2 - 4p$ squarefree?

A generalization

Instead of just looking at $p + 1 - a_p(E)$, we could examine other sequences of values associated with the reduction of E over $\mathbb{F}_p$.

Example How often is $a_p(E)^2 - 4p$ squarefree?

We can show that our upper bound for π_E^{SF} holds when $p + 1 - a_p(E)$ is replaced with $a_p(E)^2 - 4p$.

A generalization

Instead of just looking at $p+1-a_p(E)$, we could examine other sequences of values associated with the reduction of E over $\mathbb{F}_p$.

Example How often is $a_p(E)^2 - 4p$ squarefree?

We can show that our upper bound for π_E^{SF} holds when $p+1-a_p(E)$ is replaced with $a_p(E)^2-4p$.

In fact, our upper bound holds for any sequence

$$\{f_p(E) := f(a_p(E), p) : p \text{ prime}\}!$$

An average conjecture

Let

$$\pi_{E,f}^{SF} := \#\{p \leq X : f_p(E) \text{ squarefree}\}.$$

Conjecture

Let E be a non-CM elliptic curve defined over $\mathbb{Q}$. As $X \to \infty$, we have

$$\frac{1}{|\mathcal{C}(A,B)|} \sum_{E \in \mathcal{C}(A,B)} \pi_{E,f}^{SF}(X) \sim C_f^{SF}\, \pi(X),$$

where

$$C_f^{SF} := \prod_{\ell} \left(1 - \frac{|C_f(\ell^2)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z})|} \right).$$

An average result

We provide some evidence for this conjecture:

Theorem (Akhtari, David, Hahn, T., 2012)

Let $f_p(E) = p + 1 - a_p(E)$ or $a_p(E)^2 - 4p$. As $A, B \to \infty$, we have

$$\frac{1}{|\mathcal{C}(A,B)|} \sum_{E \in \mathcal{C}(A,B)} C_{E,f}^{SF} \sim C_f^{SF}.$$

Thank you!