Orders of reductions of elliptic curves with many and few prime factors

Lee Troupe

University of Georgia

August 14, 2015
Motivation

Classical problem: Understand arithmetic functions from a statistical point of view.
Motivation

Classical problem: Understand arithmetic functions from a statistical point of view.

Theorem (Hardy, Ramanujan 1917)

The normal order of $\omega(n)$ is $\log \log n$; in fact, for any $\epsilon > 0$,

$$|\omega(n) - \log \log n| < (\log \log n)^{1/2+\epsilon}$$

for all $n$ not belonging to a certain set of asymptotic density zero.
The Erdős - Kac theorem

Theorem (Erdős, Kac 1940)

The quantity

\[ \frac{\omega(n) - \log \log n}{\sqrt{\log \log n}} \]

has normal probability distribution; that is,

\[ \lim_{x \to \infty} \frac{1}{x} \# \{ n \leq x : a \leq \frac{\omega(n) - \log \log n}{\sqrt{\log \log n}} \leq b \} = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} \, dt. \]
Extreme values of $\omega(n)$

Fix $\gamma > 1$ and let $N_\gamma(x) = \#\{n \leq x : \omega(n) > \gamma \log \log x\}$. 

Theorem (Delange, 1979)

As $x \to \infty$, $N_\gamma(x) = C_\gamma \cdot x \left(\log x\right)^{1+\gamma \log \gamma - \gamma \sqrt{\log \log x} \left(1 + O\left(1/\log \log x\right)\right)}$. 

The above theorem appears in a paper of Erd˝ os and Nicolas (to whom Delange communicated the result). Its proof relies on a formula utilized by Selberg to improve upon work of Sathe (1953-1954).
Extreme values of $\omega(n)$

Fix $\gamma > 1$ and let $N_\gamma(x) = \#\{n \leq x : \omega(n) > \gamma \log \log x\}$.

Theorem (Delange, 1979)

As $x \to \infty$,

$$N_\gamma(x) = C_\gamma \cdot \frac{x}{(\log x)^{1+\gamma \log \gamma - \gamma \sqrt{\log \log x}}} \left(1 + O\left(\frac{1}{\log \log x}\right)\right).$$

The above theorem appears in a paper of Erdős and Nicolas (to whom Delange communicated the result). Its proof relies on a formula utilized by Selberg to improve upon work of Sathe (1953-1954).
Titchmarsh (1931) asked (and answered, on GRH): What is the average behavior of $\tau(p + a)$?

More generally: What can we say about arithmetic functions applied to a sequence indexed by primes, rather than all of $\mathbb{N}$?
Titchmarsh (1931) asked (and answered, on GRH): What is the average behavior of $\tau(p + a)$?
More generally: What can we say about arithmetic functions applied to a sequence indexed by primes, rather than all of $\mathbb{N}$?

For shifted primes $p - 1$:

- The normal order of $\omega(p - 1)$ is $\log \log p$ (Erdős, 1935)
- There is an analogue of the Erdős - Kac theorem (Halberstam, 1956)
Let $E/\mathbb{Q}$ be an elliptic curve. If $p$ is a prime of good reduction, then

$$E(\mathbb{F}_p) \cong \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z}$$

for uniquely determined integers $d_p$ and $e_p$ where $d_p | e_p$. The behavior of $d_p$ and $e_p$ as $p$ varies over primes of good reduction has been studied by a number of authors.
Let $E/\mathbb{Q}$ be an elliptic curve. If $p$ is a prime of good reduction, then

$$E(\mathbb{F}_p) \cong \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z}$$

for uniquely determined integers $d_p$ and $e_p$ where $d_p | e_p$. The behavior of $d_p$ and $e_p$ as $p$ varies over primes of good reduction has been studied by a number of authors.

One also has

$$\#E(\mathbb{F}_p) = p + 1 - a_p,$$

where $|a_p| < 2\sqrt{p}$.

What can we say about the arithmetical behavior of $\#E(\mathbb{F}_p)$, as $p$ varies?
The normal order of $\omega(\#E(\mathbb{F}_p))$

Theorem (Cojocaru, 2005)

Let $E/\mathbb{Q}$ be an elliptic curve. Assume GRH if $E$ does not have CM. Then $\omega(\#E(\mathbb{F}_p))$ has normal order $\log \log p$; in fact, we have

$$|\omega(\#E(\mathbb{F}_p)) - \log \log p| < (\log \log p)^{1/2+\epsilon}$$

for all $p \leq x$ except for a set of primes of relative density zero.
Erdős - Kac for elliptic curves

Theorem (Liu, 2006)

Let $E/\mathbb{Q}$ be an elliptic curve. Assume GRH if $E$ does not have CM. Then

$$\frac{1}{\pi(x)} \# \{ p \leq x : a \leq \frac{\omega(#E(F_p)) - \log \log p}{\sqrt{\log \log p}} \leq b \} \rightarrow \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} \, dt$$

as $x \to \infty$, where the above set is restricted to primes $p$ of good reduction for $E$. 

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

Theorem (T, 2015)

Let $E/\mathbb{Q}$ be an elliptic curve with CM. For $\gamma > 1$ fixed,

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma \log \log x\} = \frac{x}{(\log x)^{2+\gamma \log \gamma - \gamma + o(1)}}$$

as $x \to \infty$.

The same statement can be proved for $\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) < \gamma \log \log x\}$ when $0 < \gamma < 1$. 
Extreme values of $\omega(#E(\mathbb{F}_p))$

Theorem (T, 2015)

Let $E/\mathbb{Q}$ be an elliptic curve with CM. For $\gamma > 1$ fixed,

$$\#\{p \leq x : \omega(#E(\mathbb{F}_p)) > \gamma \log \log x\} = \frac{x}{(\log x)^{2+\gamma \log \gamma - \gamma + o(1)}}$$

as $x \to \infty$.

The same statement can be proved for

$$\#\{p \leq x : \omega(#E(\mathbb{F}_p)) < \gamma \log \log x\} \text{ when } 0 < \gamma < 1.$$

More precisely: We bound $\#\{p \leq x : \omega(#E(\mathbb{F}_p)) > \gamma \log \log x\}$ from above and below by an expression of the shape

$$\frac{x}{(\log x)^{2+\gamma \log \gamma - \gamma + o(1)}}.$$

* From now on, we focus on the curve $E : y^2 = x^3 - x$, and we restrict to primes $p$ of good ordinary reduction for $E$. 
Fix $\gamma > 1$. To prove

$$\# \{ p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma \log \log x \} \ll_{\gamma} \frac{x}{(\log x)^{2+\gamma \log \gamma - \gamma + o(1)}},$$

we follow the argument employed by Erdős to prove a normal order result for $\omega(p - 1)$ for $p$ prime.
Upper bound

Fix $\gamma > 1$. To prove

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma \log \log x\} \ll \gamma \frac{x}{(\log x)^{2+\gamma \log \gamma - \gamma + o(1)}},$$

we follow the argument employed by Erdős to prove a normal order result for $\omega(p - 1)$ for $p$ prime.

Key Idea (following Hardy and Ramanujan): Bound the size of the set

$$M_k := \{p \leq x : \omega(\#E(\mathbb{F}_p)) = k\}$$

from above in terms of $k$. Then sum on $k > \gamma \log \log x$. 
Upper bound

Lemma

Let \( x \geq 3 \) and let \( P(n) \) denote the largest prime factor of \( n \). All but a negligible amount of natural numbers \( n \leq x \) possess both of the following properties:

(i) \( P(n) > x^{1/6 \log \log x} \)

(ii) \( P(n)^2 \nmid n \).

Define

\[ N_k := \#\{ p \leq x : \#E(\mathbb{F}_p) \text{ satisfies (i), (ii) and } \omega(\#E(\mathbb{F}_p)) = k \} \].

Then

\[
N_k \leq \sum_{a \leq x^{1-1/6 \log \log x}} \sum_{\omega(a)=k-1} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{4} \\ a \mid \#E(\mathbb{F}_p) \\ \#E(\mathbb{F}_p)/a \text{ prime}}} 1.
\]
Divisors of $\#E(\mathbb{F}_p)$

For primes $p \leq x$ with $p \equiv 1 \pmod{4}$, we have

$$\#E(\mathbb{F}_p) = p + 1 - (\pi + \overline{\pi}) = (\pi - 1)(\overline{\pi} - 1),$$

where $\pi \in \mathbb{Z}[i]$ is chosen so that $p = \pi\overline{\pi}$ and $\pi \equiv 1 \pmod{(1+i)^3}$.
Divisors of $\#E(\mathbb{F}_p)$

For primes $p \leq x$ with $p \equiv 1 \pmod{4}$, we have

$$\#E(\mathbb{F}_p) = p + 1 - (\pi + \bar{\pi}) = (\pi - 1)(\bar{\pi} - 1),$$

where $\pi \in \mathbb{Z}[i]$ is chosen so that $p = \pi \bar{\pi}$ and $\pi \equiv 1 \pmod{(1+i)^3}$. Thus, $a \mid \#E(\mathbb{F}_p) \iff a \mid \|\pi - 1\|$. 

The inner sum can be estimated using Brun's pure sieve in the Gaussian integers.
Divisors of $\#E(\mathbb{F}_p)$

For primes $p \leq x$ with $p \equiv 1 \pmod{4}$, we have

$$\#E(\mathbb{F}_p) = p + 1 - (\pi + \overline{\pi}) = (\pi - 1)(\overline{\pi} - 1),$$

where $\pi \in \mathbb{Z}[i]$ is chosen so that $p = \pi \overline{\pi}$ and $\pi \equiv 1 \pmod{(1+i)^3}$. Thus, $a \mid \#E(\mathbb{F}_p) \iff a \mid \|\pi - 1\|$. So,

$$N_k \leq \frac{1}{2} \sum_{a \leq x^{1-1/6 \log \log x}} \sum_{\omega(a)=k-1} \sum_{\pi: \|\pi\| \leq x} \sum_{\pi \equiv 1 \pmod{(1+i)^3}} 1,$$

where the inner sum is restricted to $\pi$ lying over $p \equiv 1 \pmod{4}$. The inner sum can be estimated using Brun’s pure sieve in the Gaussian integers.
Lower bound

We want to show, for $\gamma > 1$ fixed,

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma \log \log x\} \geq \frac{x}{(\log x)^{2+\gamma \log \gamma-\gamma+o(1)}}.$$ 

Again we have $\#E(\mathbb{F}_p) = \|\pi - 1\|$, where $p = \pi \overline{\pi}$ and $\pi \equiv 1 \pmod{(1+i)^3}$.

Fix $\sigma \in \mathbb{Z}[i]$ with $\|\sigma\| \leq x^{1/10}$ and $\omega(\|\sigma\|) = k > \gamma \log \log x$. We count primes $\pi \in \mathbb{Z}[i]$ satisfying $\sigma(1+i)^3 \mid (\pi - 1)$ such that $\|\pi\| \leq x$ and $\sigma \mid \pi - 1$. 
Lower bound

We want to show, for $\gamma > 1$ fixed,

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma \log \log x\} \geq \frac{x}{(\log x)^2 + \gamma \log \gamma \log \gamma + \gamma + o(1)}.$$  

Again we have $\#E(\mathbb{F}_p) = \|\pi - 1\|$, where $p = \pi \overline{\pi}$ and $\pi \equiv 1 \pmod{(1+i)^3}$.

Fix $\sigma \in \mathbb{Z}[i]$ with $\|\sigma\| \leq x^{1/10}$ and $\omega(\|\sigma\|) = k > \gamma \log \log x$.

We count primes $\pi \in \mathbb{Z}[i]$ satisfying $\sigma(1+i)^3 \mid (\pi - 1)$ such that $\|\pi\| \leq x$ and $\sigma \mid \pi - 1$.

All such $\pi$ have $\omega(\|\pi - 1\|) \geq k$.

A sharp-enough lower bound follows upon summing carefully over $\sigma$ and choosing $k = \min\{n > \gamma \log \log x\}$. 

Summing carefully over $\sigma$

We expect, by the prime number theorem, that the number of $\pi$ with $\|\pi\| \leq x$ and $\sigma \mid \pi - 1$ should be

$$\frac{x}{\Phi(\sigma) \log x}.$$
Summing carefully over $\sigma$

We expect, by the prime number theorem, that the number of $\pi$ with $\|\pi\| \leq x$ and $\sigma \mid \pi - 1$ should be

$$\frac{x}{\Phi(\sigma) \log x}.$$

Bombieri-Vinogradov in $\mathbb{Z}[i]$: This is correct, on average.
Summing carefully over $\sigma$

We expect, by the prime number theorem, that the number of $\pi$ with $\|\pi\| \leq x$ and $\sigma | \pi - 1$ should be

\[ \frac{x}{\Phi(\sigma) \log x}. \]

Bombieri-Vinogradov in $\mathbb{Z}[i]$: This is correct, on average.

We need a lower bound for

\[ \sum_{\|\sigma\| < x^{1/10}, \omega(\|\sigma\|) = k} \frac{1}{\Phi(\sigma)}. \]
Summing carefully over \( \sigma \)

Lemma

Let \( y_1, y_2, \ldots, y_M \) be nonnegative real numbers. For each \( d \in \mathbb{N}, d \leq M \), let \( \eta_d \) denote the \( d \)th elementary symmetric function of the \( y_i \)'s; that is,

\[
\eta_d = \sum_{1 \leq i_1 < \cdots < i_d \leq M} y_{i_1} y_{i_2} \cdots y_{i_d}.
\]

Then, for each \( d \),

\[
\eta_d \geq \frac{1}{d!} \eta_1^d \left( 1 - \binom{d}{2} \frac{1}{\eta_1^2} \sum_{i=1}^M y_i^2 \right).
\]
Lower bound: $0 < \gamma < 1$

We want to show, for $0 < \gamma < 1$ fixed,

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) < \gamma \log \log x\} \geq \frac{x}{(\log x)^{2+\gamma \log \gamma - \gamma + o(1)}}.$$  

Fix $\sigma \in \mathbb{Z}[i]$ with $\|\sigma\| \leq x^{1/10}$ and $\omega(\|\sigma\|) = k < \gamma \log \log x$. We count primes $\pi \in \mathbb{Z}[i]$ such that $\|\pi\| \leq x$ and $\sigma \mid \pi - 1$. 
Lower bound: $0 < \gamma < 1$

We want to show, for $0 < \gamma < 1$ fixed,

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) < \gamma \log \log x\} \geq \frac{x}{(\log x)^{2+\gamma \log \gamma - \gamma + o(1)}}.$$  

Fix $\sigma \in \mathbb{Z}[i]$ with $\|\sigma\| \leq x^{1/10}$ and $\omega(\|\sigma\|) = k < \gamma \log \log x$. We count primes $\pi \in \mathbb{Z}[i]$ such that $\|\pi\| \leq x$ and $\sigma | \pi - 1$.

First step: Remove those $\pi$ with $(\pi - 1)/\sigma$ having a small prime factor ($< x^{1/100 \log \log x}$, say).
Lower bound: $0 < \gamma < 1$

We want to show, for $0 < \gamma < 1$ fixed,

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) < \gamma \log \log x \} \geq \frac{x}{(\log x)^{2+\gamma \log \gamma - \gamma + o(1)}}.$$  

Fix $\sigma \in \mathbb{Z}[i]$ with $\|\sigma\| \leq x^{1/10}$ and $\omega(\|\sigma\|) = k < \gamma \log \log x$. We count primes $\pi \in \mathbb{Z}[i]$ such that $\|\pi\| \leq x$ and $\sigma | \pi - 1$.

First step: Remove those $\pi$ with $(\pi - 1)/\sigma$ having a small prime factor ($< x^{1/100 \log \log x}$, say).

Claim: We can safely discard those $\pi$ such that $(\pi - 1)/\sigma$ satisfies

$$\omega\left(\left\|\frac{\pi - 1}{\sigma}\right\|\right) > \frac{1}{\log_4 x} (\log \log x).$$

Choose $k = \max\{n < \gamma \log \log x\} - \frac{1}{\log_4 x} (\log \log x)$. 