The distribution of Elkies primes

Alexandre Benoist (University of Luxembourg)

Joint work with Jean Kieffer (CNRS Nancy)

C2 days, Pornichet - April 1, 2025

Elliptic curves over finite fields

Let $\mathbb{F}_q$ be a finite field of characteristic $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$.
Let E be an elliptic curve over $\mathbb{F}_q$ given by a Weierstrass equation

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

Elliptic curves over finite fields

Let $\mathbb{F}_q$ be a finite field of characteristic $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$.
Let E be an elliptic curve over $\mathbb{F}_q$ given by a Weierstrass equation

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

The endomorphism of Frobenius of E is:

$$\phi_q : \begin{cases} E \to E \\ (x, y) \mapsto (x^q, y^q). \end{cases}$$

Elliptic curves over finite fields

Let $\mathbb{F}_q$ be a finite field of characteristic $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$.
Let E be an elliptic curve over $\mathbb{F}_q$ given by a Weierstrass equation

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

The endomorphism of Frobenius of E is:

$$\phi_q : \begin{cases} E \to E \\ (x, y) \mapsto (x^q, y^q). \end{cases}$$

There is an integer t_E, called trace of Frobenius of E, such that

$$\phi_q^2 - t_E \phi_q + q = 0.$$

Elliptic curves over finite fields

Let $\mathbb{F}_q$ be a finite field of characteristic $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$.
Let E be an elliptic curve over $\mathbb{F}_q$ given by a Weierstrass equation

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

The endomorphism of Frobenius of E is:

$$\phi_q : \begin{cases} E \to E \\ (x, y) \mapsto (x^q, y^q). \end{cases}$$

There is an integer t_E, called trace of Frobenius of E, such that

$$\phi_q^2 - t_E \phi_q + q = 0.$$

We have $\#E(\mathbb{F}_q) = q + 1 - t_E$. Hasse bound : $|t_E| \leq 2\sqrt{q}$.

Schoof's algorithm

Motivation: point-counting problem.
Let E be an elliptic curve over $\mathbb{F}_q$.

- Schoof's algorithm (1985): compute t_E modulo small primes $\ell \leq \ell_{max}$ such that

$$\prod_{\ell \leq \ell_{max}} \ell > 4\sqrt{q}$$

and use the Chinese Remainder Theorem.

Schoof's algorithm

Motivation: point-counting problem.
Let E be an elliptic curve over $\mathbb{F}_q$.

- Schoof's algorithm (1985): compute t_E modulo small primes $\ell \leq \ell_{max}$ such that
$$\prod_{\ell \leq \ell_{max}} \ell > 4\sqrt{q}$$
and use the Chinese Remainder Theorem.
- For a prime ℓ, the ℓ-torsion subgroup of E is
$$E[\ell] = \{P \in E(\overline{\mathbb{F}_q}) \ : \ [\ell]P = O_E\}.$$
- The trace of ϕ_q seen as an endomorphism of $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ is t_E mod ℓ.

Schoof's algorithm

Motivation: point-counting problem.
Let E be an elliptic curve over $\mathbb{F}_q$.

- Schoof's algorithm (1985): compute t_E modulo small primes $\ell \leq \ell_{max}$ such that

$$\prod_{\ell \leq \ell_{max}} \ell > 4\sqrt{q}$$

  and use the Chinese Remainder Theorem.
- For a prime ℓ, the ℓ-torsion subgroup of E is

$$E[\ell] = \{P \in E(\overline{\mathbb{F}_q}) \ : \ [\ell]P = O_E\}.$$

- The trace of ϕ_q seen as an endomorphism of $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ is t_E mod ℓ.
- Time complexity: $\widetilde{O}(\log(q)^5)$.

The SEA algorithm and Elkies primes

The SEA algorithm (90s) : $t_E \bmod \ell$ can be computed faster if there is a subgroup $K \subset E[\ell]$ of order ℓ defined over $\mathbb{F}_q$. Such a subgroup exists if and only if $t_E^2 - 4q$ is a square modulo ℓ.

The SEA algorithm and Elkies primes

The SEA algorithm (90s) : t_E mod ℓ can be computed faster if there is a subgroup $K \subset E[\ell]$ of order ℓ defined over $\mathbb{F}_q$. Such a subgroup exists if and only if $t_E^2 - 4q$ is a square modulo ℓ.

Definition

A prime $\ell \neq \mathrm{char}(\mathbb{F}_q)$ is said to be Elkies for E if and only if

$$\left(\frac{t_E^2 - 4q}{\ell}\right) = 0 \text{ or } 1.$$

Otherwise, it is said to be Atkin.

Heuristic: The number of Elkies and Atkin primes is approximately the same. If true, the complexity of the SEA algorithm is $\widetilde{O}(\log(q)^4)$.

Setting

Let E be a non-CM elliptic curve defined over $\mathbb{Q}$.

- For $P > 0$, we write $\mathcal{P}_{\mathbb{Q}}(P, 2P)$ for the set of primes of good reduction for E in $[P, 2P]$
- For $p \in \mathcal{P}_{\mathbb{Q}}(P, 2P)$, let E_p be the reduction of E modulo p, and t_p its trace of Frobenius
- For $L > 0$, let $N_e(p, L)$ be the number of Elkies primes for E_p in $[L, 2L]$
- π is the prime-counting function

Setting

Let E be a non-CM elliptic curve defined over $\mathbb{Q}$.

- For $P > 0$, we write $\mathcal{P}_{\mathbb{Q}}(P, 2P)$ for the set of primes of good reduction for E in $[P, 2P]$
- For $p \in \mathcal{P}_{\mathbb{Q}}(P, 2P)$, let E_p be the reduction of E modulo p, and t_p its trace of Frobenius
- For $L > 0$, let $N_e(p, L)$ be the number of Elkies primes for E_p in $[L, 2L]$
- π is the prime-counting function
- Shparlinski and Sutherland (2015): in average, $N_e(p, L)$ is close to $\frac{\pi(2L)-\pi(L)}{2}$.

Simple model to predict the distribution of Elkies primes

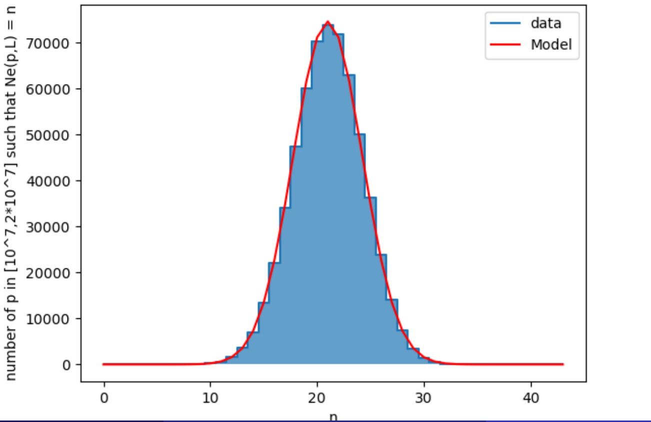
- $t_p^2 - 4p$ has a probability $\frac{1}{2}$ to be a square modulo ℓ, independently of t_p and ℓ.
- For $p \in \mathcal{P}_{\mathbb{Q}}(P, 2P)$, let $X_p := \# \left\{ \ell \in [L, 2L] \;:\; \left(\frac{t_p^2 - 4p}{\ell} \right) = 0 \text{ or } 1 \right\}$.

Simple model to predict the distribution of Elkies primes

- $t_p^2 - 4p$ has a probability $\frac{1}{2}$ to be a square modulo ℓ, independently of t_p and ℓ.
- For $p \in \mathcal{P}_{\mathbb{Q}}(P, 2P)$, let $X_p := \#\left\{\ell \in [L, 2L] \,:\, \left(\frac{t_p^2-4p}{\ell}\right) = 0 \text{ or } 1\right\}$.
- In the model, $X_p \sim B(\pi(2L) - \pi(L), \frac{1}{2})$. Then $\mathbb{E}(X_p) = \frac{\pi(2L)-\pi(L)}{2}$ and $\sigma(X_p) = \frac{\sqrt{\pi(2L)-\pi(L)}}{2}$.

Numerical experiments

The distribution of Elkies primes seems to converge to a Gaussian distribution whose mean value is $\frac{\pi(2L)-\pi(L)}{2}$ and standard deviation $\frac{\sqrt{\pi(2L)-\pi(L)}}{2}$ (graph with $P = 10^7; L = 250; E : y^2 + y = x^3 - x^2$).



Convergence to a Gaussian distribution

We equip $\mathcal{P}_{\mathbb{Q}}(P, 2P)$ with a uniform probability measure $\mathbb{P}_P$.

$$\mu = \frac{\pi(2L) - \pi(L)}{2}, \ \sigma = \frac{\sqrt{\pi(2L) - \pi(L)}}{2}, \ Y_{P,L}(p) = \frac{N_e(p, L) - \mu}{\sigma}.$$

Let $\psi : \mathbb{R}_{>0} \to \mathbb{R}$ be a function such that $\frac{\psi(x)}{x^n} \xrightarrow[x \to +\infty]{} +\infty$ for every $n \in \mathbb{N}$.

Theorem (B.-Kieffer)

Assuming the Generalized Riemann Hypothesis (GRH), the sequence $(Y_{\psi(L),L})$ converges weakly to a standard Gaussian distribution with mean value 0 and variance 1.

Elkies primes in higher dimension

Let $A/\mathbb{F}_q$ be a polarized abelian variety of dimension g with real multiplication by an order $\mathcal{O}$ in a totally real number field K of degree d. For a prime ideal $\mathfrak{l} \subset \mathcal{O}$ and $\mathfrak{l}|\ell$, we define the $\mathfrak{l}$-torsion subgroup $A[\mathfrak{l}] \subset A[\ell]$ as

$$A[\mathfrak{l}] = \bigcap_{f \in \mathfrak{l}} \ker(f) = \{x \in A[\ell] : f(x) = 0 \text{ for every } f \in \mathfrak{l}\}.$$

Definition (Elkies prime)

A prime ideal $\mathfrak{l}$ of $\mathcal{O}$ is said to be Elkies if there exists an $\mathbb{F}_q$-rational subgroup of $A[\mathfrak{l}]$ that is maximal isotropic for the Weil pairing e_ℓ and stable under $\mathcal{O}$.

Setting

Assume GRH.

- $\mathcal{O}$: an order in a totally real number field K of degree d
- A: polarized a.v. of dimension $g \geq 1$ over a number field F with RM by $\mathcal{O}$
- $\mathcal{P}_K(L, 2L)$: set of prime ideals $\mathfrak{l}$ of K such that $N_{K/\mathbb{Q}}(\mathfrak{l}) \in [L, 2L]$
- $\mathcal{P}_F(P, 2P)$: set of prime ideals $\mathfrak{p}$ of F of good reduction for A such that $N_{F/\mathbb{Q}}(\mathfrak{p}) \in [P, 2P]$
- $N_e(\mathfrak{p}, L)$: number of Elkies primes $\mathfrak{l} \in \mathcal{P}_K(L, 2L)$ for $A_\mathfrak{p}$
- Σ_h: set of unordered partitions of the integer $h = g/d$
- $\alpha_h = \sum_{(d_1,\ldots,d_r)\in\Sigma_h} \frac{1}{2^r} \cdot \prod_{i=1}^{r} \frac{1}{d_i} \cdot \prod_{k=1}^{h} \frac{1}{\#\{j : d_j = k\}!}$

The main result

Theorem (B.-Kieffer)

Under GRH and certain assumptions on the Galois representation of A, as $L, P \to \infty$ with $P \gg L^n$ for every positive integer n, the function

$$\begin{array}{rccc} X_{P,L}: & \mathcal{P}_F(P,2P) & \longrightarrow & \mathbb{R} \\ & \mathfrak{p} & \longmapsto & \dfrac{N_e(\mathfrak{p}, L) - \alpha_h \cdot \#\mathcal{P}_K(L,2L)}{\sqrt{\alpha_h(1-\alpha_h) \cdot \#\mathcal{P}_K(L,2L)}} \end{array}$$

converges in distribution to the standard Gaussian distribution with mean value 0 and variance 1.

h	1	2	3	4	5
α_h (exact value)	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{5}{16}$	$\frac{35}{128}$	$\frac{63}{256}$
α_h (approximate value)	0.5	0.375	0.3125	0.2734	0.2461

Table: Values of α_h

Questions ?

Thank you !