On the distribution of Elkies primes for abelian varieties

Alexandre Benoist (University of Luxembourg)

Joint work with Jean Kieffer (CNRS Nancy)

Journées arithmétiques, Luxembourg - June 30, 2025

Elliptic curves over finite fields

Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field.

Definition (Elkies prime)

A prime $\ell \neq \mathrm{char}(\mathbb{F}_q)$ is said to be Elkies for E if and only if there exist an elliptic curve E' and an isogeny $\varphi : E \to E'$ of degree ℓ defined over $\mathbb{F}_q$. Otherwise it is said to be Atkin.

Elliptic curves over finite fields

Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field.

Definition (Elkies prime)

A prime $\ell \neq \mathrm{char}(\mathbb{F}_q)$ is said to be Elkies for E if and only if there exist an elliptic curve E' and an isogeny $\varphi : E \to E'$ of degree ℓ defined over $\mathbb{F}_q$. Otherwise it is said to be Atkin.

The characteristic polynomial of Frobenius of E is $X^2 - tX + q$ where $t = q + 1 - \#E(\mathbb{F}_q)$.
The prime ℓ is Elkies for E if and only if

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

Elliptic curves over finite fields

Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field.

Definition (Elkies prime)

A prime $\ell \neq \mathrm{char}(\mathbb{F}_q)$ is said to be Elkies for E if and only if there exist an elliptic curve E' and an isogeny $\varphi : E \to E'$ of degree ℓ defined over $\mathbb{F}_q$. Otherwise it is said to be Atkin.

The characteristic polynomial of Frobenius of E is $X^2 - tX + q$ where $t = q + 1 - \#E(\mathbb{F}_q)$.
The prime ℓ is Elkies for E if and only if

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

Heuristic: The number of Elkies and Atkin primes is approximately the same.

Results about the distribution of Elkies primes

Shparlinski and Sutherland proved that the number of Elkies and Atkin primes is approximately the same **on average** for these two families:

- all elliptic curves defined over a fixed finite field $\mathbb{F}_q$
- the reductions modulo p of a given non-CM elliptic curve $E/\mathbb{Q}$.

Results about the distribution of Elkies primes

Shparlinski and Sutherland proved that the number of Elkies and Atkin primes is approximately the same **on average** for these two families:

- all elliptic curves defined over a fixed finite field $\mathbb{F}_q$
- the reductions modulo p of a given non-CM elliptic curve $E/\mathbb{Q}$.

We now consider a non-CM elliptic curve $E/\mathbb{Q}$.

Goal

For a prime p of good reduction for E, we denote by E_p the reduction of E modulo p.

- For $L > 0$, let $N_e(p, L)$ be the number of Elkies primes for E_p in the interval $[L, 2L]$. We have $0 \leq N_e(p, L) \leq \pi(2L) - \pi(L)$ and we expect

$$N_e(p, L) \approx \frac{\pi(2L) - \pi(L)}{2}.$$

- We want to study the distribution of these numbers for primes p in an interval of the form $[P, 2P]$.

Simple model to predict the distribution of Elkies primes

For a prime p of good reduction for E, we denote by t_p the trace of Frobenius of E_p.

- Naive assumption: $t_p^2 - 4p$ has a probability $\frac{1}{2}$ to be a square modulo ℓ, independently of t_p and ℓ.
- Let $X_p := \# \left\{ \ell \in [L, 2L] \ : \ \left(\frac{t_p^2 - 4p}{\ell} \right) = 0 \text{ or } 1 \right\}.$

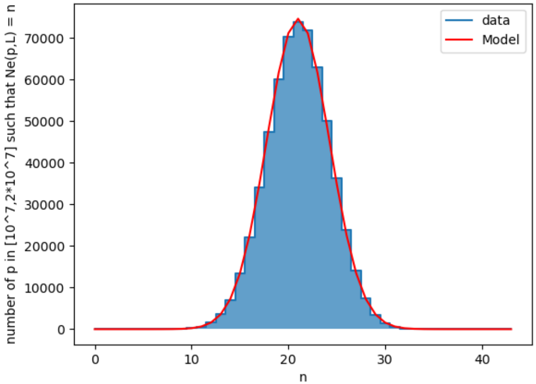
Simple model to predict the distribution of Elkies primes

For a prime p of good reduction for E, we denote by t_p the trace of Frobenius of E_p.

- Naive assumption: $t_p^2 - 4p$ has a probability $\frac{1}{2}$ to be a square modulo ℓ, independently of t_p and ℓ.
- 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 the numbers $N_e(p, L)$ seems to converge to a Gaussian distribution whose mean value is $\mu = \frac{\pi(2L)-\pi(L)}{2}$ and standard deviation $\sigma = \frac{\sqrt{\pi(2L)-\pi(L)}}{2}$ (graph with $P = 10^7$; $L = 250$; $E : y^2 + y = x^3 - x^2$).



Convergence to a Gaussian distribution

For $p \in [P, 2P]$, we set

$$X_{P,L}(p) = \frac{N_e(p, L) - \mu}{\sigma}.$$

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 $(X_{\psi(L),L})$ converges weakly to the standard Gaussian distribution with mean value 0 and variance 1 as $L \to +\infty$.

Elkies primes in higher dimension

Let $A/\mathbb{F}_q$ be a polarized abelian variety of dimension g with real multiplication (RM) 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 for A 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 $\mathcal{O}$.

Goal

Let A be a polarized abelian variety defined over a number field F with RM by $\mathcal{O}$.

- For a prime $\mathfrak{p}$ of good reduction for A, we denote by $A_{\mathfrak{p}}$ the reduction of A modulo $\mathfrak{p}$. The reduction $A_{\mathfrak{p}}$ also has RM by $\mathcal{O}$.
- For $L > 0$, let $N_e(\mathfrak{p}, L)$ be the number of Elkies primes for $A_{\mathfrak{p}}$ of norm in $[L, 2L]$.
- We want to study the distribution of these numbers for primes $\mathfrak{p}$ whose norm is in an interval of the form $[P, 2P]$.

The main result

Let c_L be the number of primes $\mathfrak{l}$ of $\mathcal{O}$ whose norm is contained in $[L, 2L]$ and $h = g/d$. For $\mathfrak{p}$ of norm in $[P, 2P]$, let $X_{P,L}(\mathfrak{p}) = \frac{N_e(\mathfrak{p},L) - \alpha_h \cdot c_L}{\sqrt{\alpha_h(1-\alpha_h) \cdot c_L}}$, where α_h is a constant.

Theorem (B.-Kieffer)

Assume GRH. If A has "large Galois image", then the sequence $(X_{\psi(L),L})$ converges weakly to the standard Gaussian distribution with mean value 0 and variance 1 as $L \to +\infty$.

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

Large Galois images

Let $G_F = \mathrm{Gal}(\overline{F}/F)$. We write $\widehat{\mathbb{Z}}_{\geq n} = \prod_{\ell \text{ prime}, \ell \geq n} \mathbb{Z}_\ell$. The ℓ-adic Galois representations $\rho_\ell : G_F \to \mathrm{GSp}_{2h}(\mathcal{O} \otimes \mathbb{Z}_\ell)$ attached to A can be combined into a global representation

$$\widehat{\rho}_n = G_F \to \mathrm{GSp}_{2h}(\mathcal{O} \otimes \widehat{\mathbb{Z}}_{\geq n}).$$

Definition (Large Galois image)

We say that A has large Galois image if for some $n \geq 1$, the image of $\widehat{\rho}_n$ contains $\mathrm{Sp}_{2h}(\mathcal{O} \otimes \widehat{\mathbb{Z}}_{\geq n})$.

Elkies primes, Frobenius elements and the Chebotarev density theorem

- Strategy of the proof: show that the moments $\mathbb{E}(X_{P,L}^k)$ converge to the moments of the Gaussian distribution with mean value 0 and variance 1.

Elkies primes, Frobenius elements and the Chebotarev density theorem

- Strategy of the proof: show that the moments $\mathbb{E}(X_{P,L}^k)$ converge to the moments of the Gaussian distribution with mean value 0 and variance 1.
- For a prime ideal $\mathfrak{l}$ of $\mathcal{O}$, we could characterize the fact that $\mathfrak{l}$ is Elkies for $A_\mathfrak{p}$ in terms of the action of Frobenius on $A_\mathfrak{p}[\mathfrak{l}]$ and a Frobenius element at $\mathfrak{p}$ of G_F.

Elkies primes, Frobenius elements and the Chebotarev density theorem

- Strategy of the proof: show that the moments $\mathbb{E}(X_{P,L}^k)$ converge to the moments of the Gaussian distribution with mean value 0 and variance 1.
- For a prime ideal $\mathfrak{l}$ of $\mathcal{O}$, we could characterize the fact that $\mathfrak{l}$ is Elkies for $A_\mathfrak{p}$ in terms of the action of Frobenius on $A_\mathfrak{p}[\mathfrak{l}]$ and a Frobenius element at $\mathfrak{p}$ of G_F.
- The density of primes $\mathfrak{p}$ such that a given prime $\mathfrak{l}$ is Elkies for $A_\mathfrak{p}$ is given by the Chebotarev density theorem. We can compute it if A has large Galois image.

Elkies primes, Frobenius elements and the Chebotarev density theorem

- Strategy of the proof: show that the moments $\mathbb{E}(X_{P,L}^k)$ converge to the moments of the Gaussian distribution with mean value 0 and variance 1.
- For a prime ideal $\mathfrak{l}$ of $\mathcal{O}$, we could characterize the fact that $\mathfrak{l}$ is Elkies for $A_\mathfrak{p}$ in terms of the action of Frobenius on $A_\mathfrak{p}[\mathfrak{l}]$ and a Frobenius element at $\mathfrak{p}$ of G_F.
- The density of primes $\mathfrak{p}$ such that a given prime $\mathfrak{l}$ is Elkies for $A_\mathfrak{p}$ is given by the Chebotarev density theorem. We can compute it if A has large Galois image.

Elkies primes, Frobenius elements and the Chebotarev density theorem

- Strategy of the proof: show that the moments $\mathbb{E}(X_{P,L}^k)$ converge to the moments of the Gaussian distribution with mean value 0 and variance 1.
- For a prime ideal $\mathfrak{l}$ of $\mathcal{O}$, we could characterize the fact that $\mathfrak{l}$ is Elkies for $A_\mathfrak{p}$ in terms of the action of Frobenius on $A_\mathfrak{p}[\mathfrak{l}]$ and a Frobenius element at $\mathfrak{p}$ of G_F.
- The density of primes $\mathfrak{p}$ such that a given prime $\mathfrak{l}$ is Elkies for $A_\mathfrak{p}$ is given by the Chebotarev density theorem. We can compute it if A has large Galois image.

Thank you !