The distribution of Elkies primes for reductions of abelian varieties

Alexandre Benoist - Jean Kieffer

University of Luxembourg - Université de Lorraine, CNRS, Inria, LORIA

The distribution of Elkies primes for elliptic curves

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The number of $\mathbb{F}_q$-rational points of E is

$$\#E(\mathbb{F}_q) = q + 1 - t_E,$$

where t_E is an integer called the trace of Frobenius of E. It satisfies $|t_E| \leq 4\sqrt{q}$.

The SEA algorithm

- Compute $t_E \bmod \ell$ for small primes $\ell \leq \ell_{\max}$ such that
$$\prod_{\ell \leq \ell_{max}} \ell > 4\sqrt{q}.$$
- The trace of the endomorphism of Frobenius of E, seen as an endomorphism of $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$, is $t_E \bmod \ell$. It is faster to compute it if there is a subgroup $K \subset E[\ell]$ of order ℓ defined over $\mathbb{F}_q$.

A subgroup $K \subset E[\ell]$ of order ℓ defined over $\mathbb{F}_q$ exists if $t_E^2 - 4q$ is a square modulo ℓ.

Elkies primes (elliptic curves)

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 $\widetilde{O}(\log(q)^4)$.

Shparlinski and Sutherland have shown that this heuristic is true on average for the two following families:

- the set of elliptic curves defined over the same finite field $\mathbb{F}_q$, for large values of q,
- **the reductions modulo primes of good reduction of a non-CM elliptic curve E 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 $L > 0$, let $N_e(p, L)$ be the number of Elkies primes for $E \bmod p$ in $[L, 2L]$.

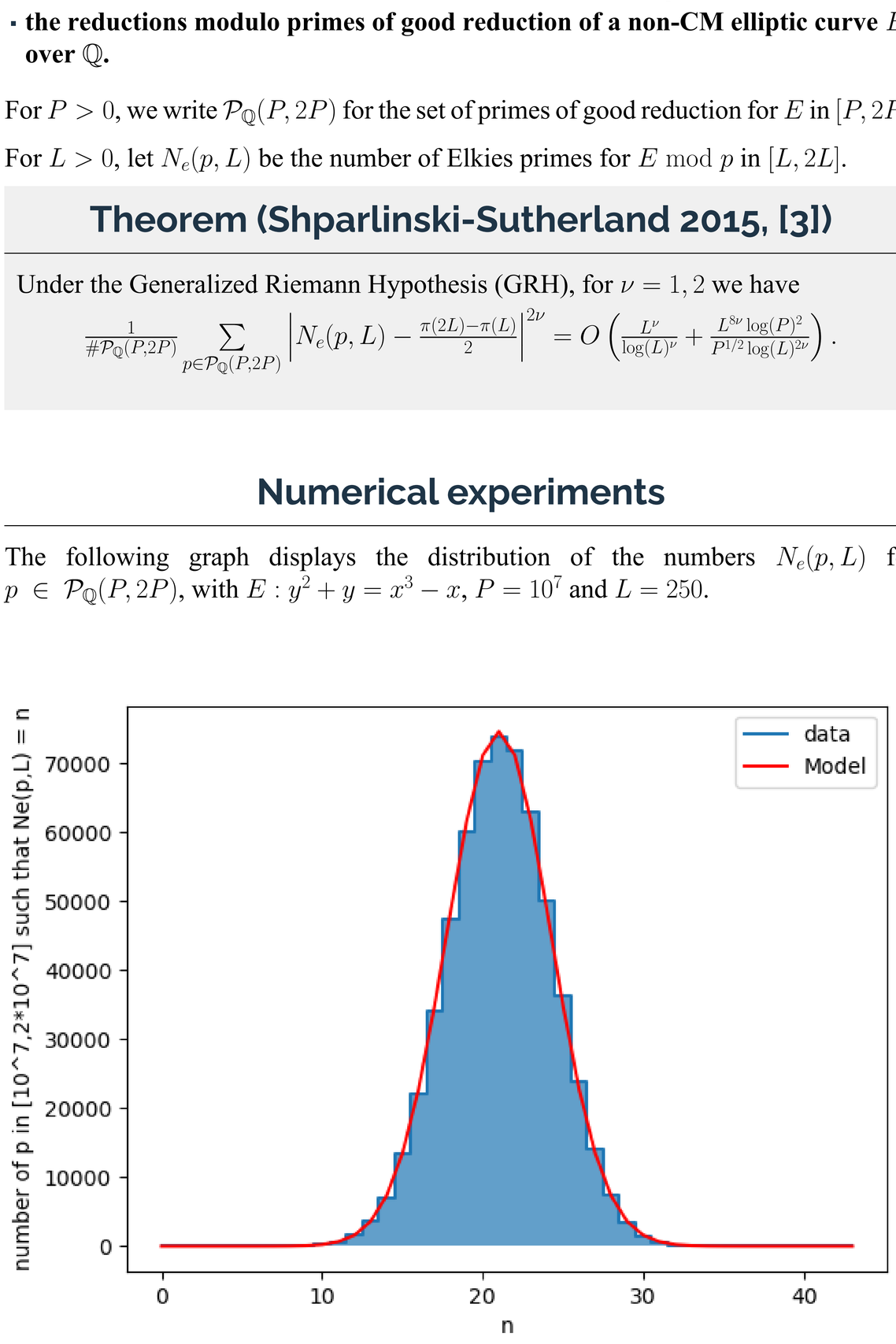
Theorem (Shparlinski-Sutherland 2015, [3])

Under the Generalized Riemann Hypothesis (GRH), for $\nu = 1, 2$ we have

$$\frac{1}{\#\mathcal{P}_{\mathbb{Q}}(P,2P)} \sum_{p \in \mathcal{P}_{\mathbb{Q}}(P,2P)} \left| N_e(p, L) - \frac{\pi(2L) - \pi(L)}{2} \right|^{2\nu} = O\left(\frac{L^\nu}{\log(L)^\nu} + \frac{L^{8\nu} \log(P)^2}{P^{1/2} \log(L)^{2\nu}} \right).$$

Numerical experiments

The following graph displays the distribution of the numbers $N_e(p, L)$ for $p \in \mathcal{P}_{\mathbb{Q}}(P, 2P)$, with $E : y^2 + y = x^3 - x$, $P = 10^7$ and $L = 250$.



Generalizing 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

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

Elkies primes (abelian varieties)

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 and stable under the action of $\mathcal{O}$.

The main result

Let A be a polarized abelian variety of dimension $g \geq 1$ over $\mathbb{Q}$ with real multiplication by an order $\mathcal{O}$ in a totally real number field K of degree d. Let $h = g/d$.

We write $\widehat{\mathbb{Z}}_{\geq n} = \prod_{\ell \text{ prime},\, \ell \geq n} \mathbb{Z}_\ell$. The ℓ-adic Galois representations

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSp}_{2h}(\mathcal{O} \otimes \mathbb{Z}_\ell)$$

attached to A can be combined into a global representation

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

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

Let $N_e(p, L)$ the number of Elkies primes of norm contained in $[L, 2L]$ for $A \bmod p$.

Theorem

Under GRH, if A has large Galois image, as $L, P \to \infty$ with $P \gg L^n$ for every positive integer n, there is a constant $\alpha_h > 0$ such that the function

$$\begin{aligned} X_{P,L} : \mathcal{P}_{\mathbb{Q}}(P, 2P) &\longrightarrow \mathbb{R} \\ p &\longmapsto \frac{N_e(p, L) - \alpha_h \cdot (\pi(2L) - \pi(L))}{\sqrt{\alpha_h(1 - \alpha_h) \cdot (\pi(2L) - \pi(L))}} \end{aligned}$$

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

Strategy of the proof

- General strategy: 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 $A \bmod p$ in terms of the action of Frobenius on $(A \bmod p)[\mathfrak{l}]$ and a Frobenius element at p of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
- The density of primes such that a given prime $\mathfrak{l}$ is Elkies for A is given by the Chebotarev density theorem. We can compute it if the Galois representation attached to A is large: it is equal to α_h.

Conclusion

Asymptotically, the distribution of Elkies primes for reductions of abelian varieties defined over a number field is Gaussian. This leads to a result about the time complexity of the SEA algorithm in higher dimension.

References

[1] A. Benoist and J. Kieffer. *The asymptotic distribution of Elkies primes for reductions of abelian varieties is Gaussian*. Res. number theory 11, 65 (2025).

[2] I. E. Shparlinski and A. V. Sutherland. *On the distribution of Atkin and Elkies primes*. Found. Comput. Math. 14 (2014), pp. 285-297.

[3] I. E. Shparlinski and A. V. Sutherland. *On the distribution of Atkin and Elkies primes for reductions of elliptic curves on average*. LMS J. Comput. Math. 18.1 (2015), pp. 308-322.