Asymptotic Bounds for Extended Elliptic Pseudoprimes

Liljana Babinkostova, Dylan Fillmore, Philip Lamkin, Alice Lin, Calvin Yost-Wolff

Boise State University, University of South Carolina, Carnegie Mellon University, Princeton University, Massachusetts Institute of Technology

Motivation

The problem of distinguishing prime numbers from composite numbers is fundamental in mathematics. Primality tests have become increasingly important in the secure transmission of data in today's society. A composite number that passes a primality test is known as a *pseudoprime*. A pseudoprime that passes such a test for any base is known as a *Carmichael number*. This research analyzes pseudoprimes and Carmichael numbers that arise from elliptic curves, introduced in [1] and [3]. Some of our results provide improvements and corrections of bounds given in [2] for the probability that N is an S-Carmichael number for a random elliptic curve.

Preliminaries

Elliptic Curves

An **elliptic curve** $E/\mathbb{Q}: y^2 = x^3 + Ax + B$ is defined as the set

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

where $\Delta := 4A^3 + 27B^2 \neq 0$.

The L-function of an elliptic curve $E/\mathbb{Q}$ is

$$L(E, s) := \prod_p \left(1 - a_p p^{-s} + 1_E(p) p^{1-2s}\right)^{-1} = \sum_{n \geq 1} \frac{a_n}{n^s}.$$

Size of L-series Coefficients

Let $E/\mathbb{Q}$ be an elliptic curve with L-series $\sum_{n\geq 1} a_n/n^s$. Let $d(n)$ denote the number of divisors of n. Then for all positive integers n,

$$|a_n| < d(n)\sqrt{n}.$$

This bound is tight and corrects the misconception that $|a_n| \leq 2^{\omega(n)}\sqrt{n}$.

S-Pseudoprimes and Carmichael Numbers

Let N be a composite integer, $E/\mathbb{Q}$ be an elliptic curve with good reduction at every prime $p \mid N$, and P be a point on $E(\mathbb{Z}/N\mathbb{Z})$. Let $N+1-a_N = 2^s t$ where t is odd.

- N is an **S-pseudoprime** [3] for (E, P) if
$$(N + 1 - a_N)P \equiv (0 : 1 : 0) \bmod N.$$
- N is a **strong S-pseudoprime** [1] for (E, P) if either
  - $tP \equiv (0 : 1 : 0) \bmod N$ or
  - $(2^r t)P \equiv (x : 0 : 1) \bmod N$ for some $0 \leq r \leq s - 1$.

A composite number N is a **(strong) S-Carmichael number** [1, 3] for an elliptic curve E if N is a (strong) S-pseudoprime for all points on $E(\mathbb{Z}/N\mathbb{Z})$.

S-Carmichael Probabilities

N Squarefree with at Most k Prime Factors

If N is squarefree and the product of at most k primes, the probability that N is an S-Carmichael number for a randomly chosen curve with good reduction at all $p \mid N$ is

$$O\left(\frac{1}{N^{\frac{1}{2k}-\epsilon}}\right).$$

We prove the bounds given above and below by limiting the number of possible values of a_p for which $\exp(E(\mathbb{Z}/p\mathbb{Z})) \mid (N+1-a_N)$, as well as using our bound on the size of L-series coefficients and other analytic number theory techniques.

N with Sufficiently Large Prime Factor

Let N be a composite integer, with a prime factor $q \mid\mid N$, and $q > \log(N)^{f(N)}$ for some function f. The probability that N is an S-Carmichael number for a randomly chosen curve with good reduction at all $p \mid N$ is

$$O\left(\frac{\log^3(f(N))}{f(N)} + \frac{(\log\log\log N)^3}{f(N)}\right).$$

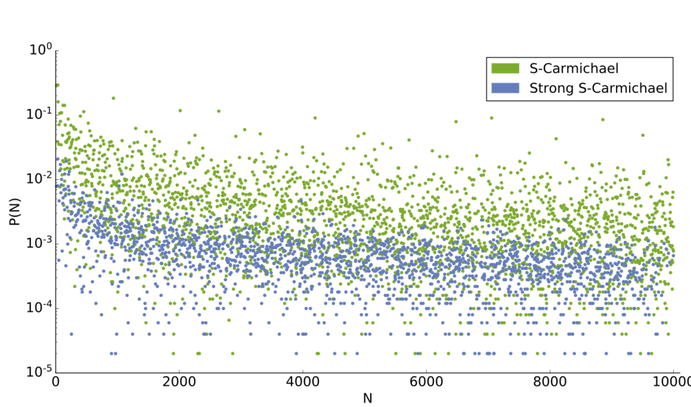

Figure 1. The proportion of elliptic curves $E/\mathbb{Q}$ for which N is a (strong) S-Carmichael number.

Random N in Interval $[x, 2x]$

The probability that a composite integer N chosen uniformly at random from the interval $[x, 2x]$ is a S-Carmichael number for a randomly chosen curve with good reduction at all $p \mid N$ is

$$O\left((\log x)^{-o(\log\log\log x)}\right).$$

Strong S-Carmichael Probabilities

Frequency of Strong S-Pseudoprime Points

Let N be an odd positive integer with distinct primes $q_1, q_2 \mid N$. The probability that N is a strong S-pseudoprime at a random point P on a randomly chosen curve with good reduction at all $p \mid N$ is at most

$$\frac{17q_1q_2 + 2q_1 + 2q_2 + 4}{32q_1q_2}.$$

Finding an upper bound for the probability that a composite integer passes the strong S-pseudoprime test at a random point is important for primality tests.

Characterization of Strong S-Carmichael Numbers

Let N be an odd composite integer. Then N is an strong S-Carmichael number for a curve E if and only if N is an S-Carmichael number for E and a_p is odd for all odd primes $p \mid N$.

Since $(1 + 1/p)/3$ of all cubic polynomials are irreducible over $\mathbb{F}_p$, a_p is odd for approximately $1/3$ of all elliptic curves.

Bound Based on Parity of a_p

Let N be an odd composite integer. The probability that N is a strong S-Carmichael number for a randomly chosen curve with good reduction at all $p \mid N$ is

$$O\left(\frac{\log\omega(N)}{3^{\omega(N)}}\right)$$

where $\omega(N)$ denotes the number of distinct prime divisors of N.

We can expand upon this bound by limiting the probability odd values of a_p satisfy $\exp(E(\mathbb{Z}/p\mathbb{Z})) \mid (N + 1 - a_N)$.

Strong S-Carmichael Probability

Let N be an odd composite squarefree integer with $\omega(N) \leq \frac{\log(N)}{(\log\log N)^2}$. The probability that N is a strong S-Carmichael number for a randomly chosen curve E with good reduction at all $p \mid N$ is

$$O\left(\frac{\log\omega(N)\,(\log\log\log N)^3}{3^{\omega(N)}\log\log N}\right).$$

Note that the condition on $\omega(n)$ happens asymptotically with probability 1 since $\omega(n)$ for $n \leq x$ is normally distributed with mean $\log\log x$ and standard deviation $\sqrt{\log\log x}$.

Acknowledgements

This research, conducted at the Complexity Across Disciplines Research Experience for Undergraduates site, was supported by National Science Foundation REU site Grant DMS-1659872 and by Boise State University.

References

[1] L. Babinkostova, A. Hernandez-Espiet and H.J. Kim, *On Types of Elliptic Pseudoprimes*, (2017) (arXiv:1710.05264)

[2] J. Schlage-Puchta. The non-existence of universal Carmichael numbers. *From Arithmetic to Zeta-Functions*, Springer, Cham, (2016) 435–453.

[3] J.H. Silverman, *Elliptic Carmichael Numbers and Elliptic Korselt Criteria*, Acta Arithmetica, Vol. 155:3, (2012) 233–246.

Future Work

- Prove that the probability that a random composite integer $N \in [x, 2x]$ is an S-Carmichael number for a random curve E is $O(x^{-c})$ for some $c > 0$.
- Find the distribution of a_{p^k}, where p is a prime and $k > 1$, over elliptic curves.
- Construct large composite integers N which are S-Carmichael numbers with high probability.