Anomalous Primes and the Elliptic Korselt Criterion

Liljana Babinkostova[1], Jackson Bahr[2], Yujin Kim[3], Eric Neyman[4], Gregory Taylor[5]

[1]Boise State University, [2]Carnegie Mellon University, [3]Columbia University, [4]Princeton University, [5]The College of William & Mary

Motivation

With applications to coding theory, cryptography, and random number generation, developing efficient primality tests stands as one of the central problems of number theory. Gordon's 1987 primality test was the first to use the arithmetic of elliptic curves [1]. In 2012, Silverman generalized Gordon's test and introduced the notion of elliptic Korselt Type I (EK-I) numbers, which satisfy an analog of Korselt's criterion in classical number theory. Understanding EK-I numbers may reveal strengths and weaknesses of elliptic curve primality testing and lead to improvements of these tests. A result in [4] suggests a connection between an elliptic curve's EK-I numbers and its anomalous primes, which are of special interest in many areas of mathematics. Our research goal is to investigate these two classes of numbers and the connections between them.

Elliptic Carmichael Numbers

An **elliptic curve** E over a field K is the set

$$E(K) = \{(x, y) \in K^2 \colon y^2 = x^3 + ax + b\} \cup \{\infty\}$$

where K does not have characteristic 2 or 3 and $4a^3 + 27b^2 \neq 0$.

- The points of $E(K)$ form an abelian group.
- The order $\#E(\mathbb{F}_q) = q + 1 - a_q$, where $|a_q| \leq 2\sqrt{q}$, as shown in [2].
- Elliptic curve groups can be defined over $\mathbb{Z}/n\mathbb{Z}$ for n composite by using the Chinese Remainder Theorem.
- If p is prime and E is an elliptic curve, then for a point $\mathcal{P} \in E(\mathbb{Z}/p\mathbb{Z})$,

$$(p + 1 - a_p)\mathcal{P} = \infty.$$

An **elliptic Carmichael number** for a curve E is a composite n such that

$$(n + 1 - a_n)\mathcal{P} = \infty$$

for every $\mathcal{P} \in E(\mathbb{Z}/n\mathbb{Z})$, where a_n is the n^{th} coefficient of the L-series of E.

- Elliptic Carmichael numbers on E satisfy a necessary condition for primality at every point on E despite not being prime.

The Elliptic Korselt Criterion

For an elliptic curve E, a positive integer n is called **elliptic Korselt Type I (EK-I)** if it has at least two distinct prime factors and for each prime factor p,

$$p + 1 - a_p \mid n + 1 - a_n \text{ and}$$

$$\operatorname{ord}_p(a_n - 1) \geq \operatorname{ord}_p(n) - \begin{cases} 1 & \text{if } a_p \not\equiv 1 \pmod{p} \\ 0 & \text{otherwise} \end{cases}$$

where $\operatorname{ord}_p(n)$ denotes the exponent of the largest power of p dividing n.

- If n is an EK-I number for an elliptic curve E, then n is an elliptic Carmichael number for E [4, Proposition 11].

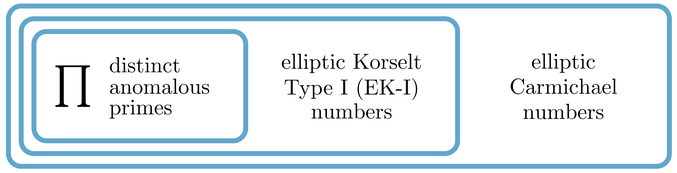
If $\#E(\mathbb{Z}/p\mathbb{Z}) = p$, then E is called an **anomalous curve** and p is called an **anomalous prime** for the curve $E(\mathbb{Z}/p\mathbb{Z})$.

Products of Anomalous Primes are EK-I Numbers

Theorem. Let E be an elliptic curve and $p_1, \ldots, p_m$ be distinct anomalous primes for E. Then $\prod_{i=1}^{m} p_i$ is an elliptic Korselt Type I number for E.

Restrictions on EK-I Numbers

The previous theorem and a result from [4] imply the following inclusions:



Conversely, we establish deterministic and probabilistic results for when EK-I numbers are products of anomalous primes.

A Restriction on EK-I Numbers

Theorem. Let E be an elliptic curve and $n = p_1 p_2 \ldots p_m$ be an elliptic Korselt Type I number for E such that $p_1 < p_2 < \cdots < p_m$. If

$$4^m < p_1 p_2 \ldots p_{m-1} < \frac{\sqrt{p_m}}{4^m},$$

then p_i is anomalous for E for all $1 \leq i \leq m$.

The following results suggest that even if the conditions above are not satisfied, the primes p and q are nevertheless almost certainly anomalous.

Order Divisibility Conjecture

Conjecture. For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a randomly chosen elliptic curve such that $\#E(\mathbb{Z}/p\mathbb{Z})$ and $\#E(\mathbb{Z}/q\mathbb{Z})$ divide $n + 1 - a_n$. Then

$$\lim_{N \to \infty} \Pr[\#E(\mathbb{Z}/n\mathbb{Z}) = n + 1 - a_n] = 1.$$

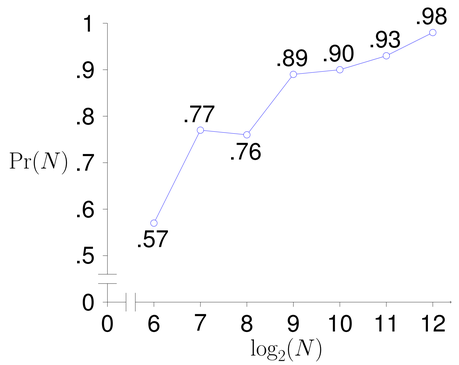


Figure 1: $\Pr(N)$, the probability above as a function of N, with sample size 100 for each N.

A Probabilistic Restriction on EK-I Numbers

Theorem. For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a randomly chosen elliptic curve for which n is an elliptic Korselt Type I number. Assuming the Order Divisibility Conjecture, we have

$$\lim_{N \to \infty} \Pr[p \text{ and } q \text{ are anomalous primes for } E] = 1.$$

Bachet Anomalous Numbers

We call a prime power p^r a **Bachet anomalous number** if there exists an elliptic curve E of the form $y^2 = x^3 + B$ such that $\#E(\mathbb{F}_{p^r}) = p^r$.

Characterizing Bachet Anomalous Numbers

Theorem. Let p denote a prime and r denote a positive integer. Then

- Every Bachet anomalous number p^r is a difference of consecutive cubes.
- Every difference of consecutive cubes of the form p^r, where $r = 1$ or 2, is Bachet anomalous.
- For $r \geq 3$, assuming that $p^r = (n+1)^3 - n^3$ has no integer solutions (a special case of the Tidjeman-Zagier conjecture), no number of the form p^r is Bachet anomalous.

The fact that products of anomalous primes for a curve are EK-I numbers lets us establish the following theorem as a corollary of [3, Theorem 1.2]:

The Infinitude of EK-I Numbers

Theorem. Assuming the Hardy-Littlewood Conjecture, there are infinitely many elliptic Korselt Type I numbers for the curve $E : y^2 = x^3 + B$, where $B \in \mathbb{Z}$ is neither a square nor a cube in $\mathbb{Q}(\sqrt{-3})$ and $B \neq 80d^6$ for any $d \in \mathbb{Z}[(1 + \sqrt{-3})/2]$.

Future Work

- Extend the probabilistic restriction on EK-I numbers to $n = p_1 \ldots p_m$.
- Examine whether the probabilistic result holds if the space of curves is restricted to curves $y^2 = x^3 + B$.
- Investigate which elliptic Carmichael numbers are EK-I numbers. This will more directly connect anomalous primes and Carmichael numbers.
- Investigate the relations between other notions of pseudoprimes (e.g. Euler elliptic pseudoprimes) and anomalous primes.

References

[1] D. Gordon, *Pseudoprimes on elliptic curves*, J. M. DeKoninck and C. Levesque, eds. Number Theory, **Proc. Internat. Number Theory Conf., Laval 1987**, de Gruyter, New York, (1989) 291–305.

[2] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper. I, II & III*, **Crelle's Journal** Vol. 175, (1936) 193–208.

[3] H. Qin, *Anomalous primes of the elliptic curve* $E_D : y^2 = x^3 + D$, **Proceedings of the London Mathematical Society** Vol. 3:112, (2016) 415–453.

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

Acknowledgments

This material is based on work supported by the National Science Foundation under Grant No. DMS-1359425 and by Boise State University. We would like to thank Dr. Lawrence Washington for his insight and advice.