

Motivation

Cryptosystems in ubiquitous commercial use base their security on the difficulty of factoring. Deployment of these schemes necessitate reliable, efficient methods of recognizing the primality of a number. A number that passes a probabilistic test, but is in fact composite is known as a *pseudoprime*. A pseudoprime that passes such test for any base is known as a *Carmichael* number. The focus of this research is analysis of types of pseudoprimes that arise from elliptic curves and from group structures derived from Lucas sequences [2]. We extend the Korselt criterion presented in [3] for two important classes of elliptic pseudoprimes and deduce some of their properties. Furthermore, we solve a standing conjecture of [1] and thus characterize a class of pseudoprimes in [3] via anomalous elliptic curves.

Elliptic Pseudoprimes

Elliptic Curves over the Rationals

An elliptic curve $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ over \mathbb{Q} 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

$$L(E, s) := \prod_p (1 - a_p(E)p^{-s} + 1_E(p)p^{1-2s})^{-1} = \sum_N \frac{a_N}{N^s}.$$

Elliptic Pseudoprimes

Let $N > 0$ be a composite integer, E/\mathbb{Q} be an elliptic curve with good reduction at every prime dividing N , and $\mathcal{P} \in E$. Then, N is an elliptic pseudoprime [3] for (E, \mathcal{P}) if $(N + 1 - a_N)\mathcal{P} \equiv \mathcal{O} \pmod{N}$.

Moreover, N is an **Euler elliptic pseudoprime** for (E, \mathcal{P}) if

$$\left(\frac{N+1-a_N}{2}\right)\mathcal{P} \equiv \begin{cases} \mathcal{O} \pmod{N} & \text{if } \mathcal{P} = 2\mathcal{Q} \text{ for some } \mathcal{Q} \in E(\mathbb{Z}/N\mathbb{Z}) \\ \text{a 2-torsion point} & \text{otherwise.} \end{cases}$$

Writing $N+1-a_N = 2^s t$ where t is odd, N is a **strong elliptic pseudoprime** for (E, \mathcal{P}) if

- $t\mathcal{P} \equiv \mathcal{O} \pmod{N}$, or
- $(2^r t)\mathcal{P} \equiv (x, 0) \pmod{N}$ for some $x \in \mathbb{Z}/N\mathbb{Z}$ and integer $0 \leq r < s$.

Strong to Euler Elliptic Carmichael Numbers

Let E/\mathbb{Q} be an elliptic curve. If $N + 1 - a_N$ is even and N is a strong elliptic pseudoprime for (E, \mathcal{P}) for every $\mathcal{P} \in E$, then N is an Euler elliptic pseudoprime for (E, \mathcal{P}) for every $\mathcal{P} \in E$.

Future Work

Elliptic Korselt Criteria

Korselt Criteria for Euler and Strong Elliptic Carmichael Numbers

Let $\epsilon_{N,p}(E)$ be the exponent of $E(\mathbb{Z}/p^{\text{ord}_p(N)}\mathbb{Z})$. Then, N is an Euler elliptic Carmichael number if and only if, for every prime p dividing N ,

$$2\epsilon_{N,p} \mid (N + 1 - a_N).$$

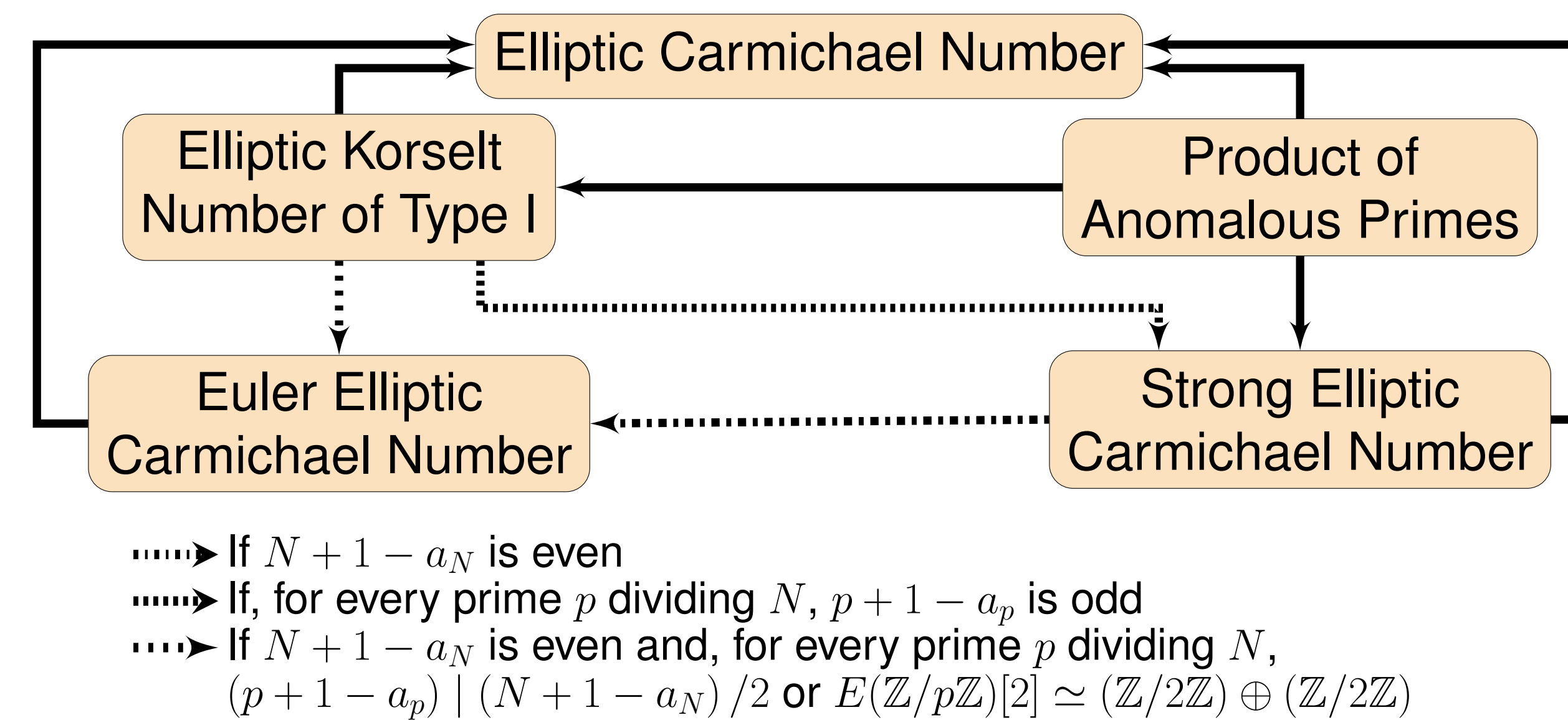
If t is the largest odd divisor of $(N + 1 - a_N)$, then N is a strong elliptic Carmichael number if and only if, for every prime p dividing N ,

$$\epsilon_{N,p} \mid t.$$

An integer $N > 0$ is an **elliptic Korselt number of Type I** [3] for E if N has at least two distinct prime factors, and, for every prime p dividing N ,

- E has a good reduction at p ,
- $(p + 1 - a_p) \mid (N + 1 - a_N)$, and
- $\text{ord}_p(a_N - 1) \geq \text{ord}_p(N) - \begin{cases} 1 & \text{if } a_p \not\equiv 1 \pmod{p} \\ 0 & \text{if } a_p \equiv 1 \pmod{p}. \end{cases}$

A prime p is **anomalous** for an elliptic curve E/\mathbb{Q} if $\#E(\mathbb{Z}/p\mathbb{Z}) = p$.



Anomalous Prime Factors vs. Elliptic Korselt Number of Type I

Let $M \geq 7$ be an integer, $5 \leq p, q \leq M$ be randomly chosen distinct primes, $N = pq$, and E/\mathbb{Q} be a randomly chosen elliptic curve with good reduction at p and q . For all $\epsilon > 0$,

$$\Pr[a_p = a_q = 1] = \Omega(1/M^{1+\epsilon}) \text{ and } \Pr[(p + 1 - a_p), (q + 1 - a_q) \mid (N + 1 - a_N)] = O(1/M^{5/4-\epsilon}).$$

Density of E with $\#E(\mathbb{Z}/N\mathbb{Z}) = N + 1 - a_N$ Given a Condition

Let M, N, E, p , and q be as above. If $(p + 1 - a_p), (q + 1 - a_q) \mid (N + 1 - a_N)$, then

$$\lim_{M \rightarrow \infty} \Pr[(p + 1 - a_p)(q + 1 - a_q) = N + 1 - a_N] = 1.$$

References

- [1] L. Babinkostova et al., *Anomalous Primes and the Elliptic Korselt Criterion*, arXiv:1608.02317, (2016).
- [2] R. Baillie and S. S. Wagstaff, *Lucas Pseudoprimes*, *Math. of Comp.* Vol. 3, (1980) 1391–1417.
- [3] J.H. Silverman, *Elliptic Carmichael Numbers and Elliptic Korselt Criteria*, *Acta Arithmetica* Vol. 155:3, (2012) 233–246.

Lucas Pseudoprimes

Lucas Groups

Let D, N be coprime integers. The Lucas group $\mathcal{L}_{\mathbb{Z}/N\mathbb{Z}}$ is defined on

$$\mathcal{L}_{\mathbb{Z}/N\mathbb{Z}} = \{(x, y) \in (\mathbb{Z}/N\mathbb{Z})^2 \mid x^2 - Dy^2 \equiv 1 \pmod{N}\}.$$

Algebraic Structure of Lucas Groups

If p is a prime and D is an integer coprime to p , then $\mathcal{L}_{\mathbb{Z}/p\mathbb{Z}}$ is a cyclic group of order $p^{e-1}(p - (D/p))$.

Lucas Pseudoprimes

Let D, N be coprime integers, $N > 0$, and $\mathcal{P} \in \mathcal{L}_{\mathbb{Z}/N\mathbb{Z}}$. Then, N is a Lucas pseudoprime for (D, \mathcal{P}) if $(N - (D/N))\mathcal{P} = \mathcal{O}$.

Moreover, N is an **Euler Lucas pseudoprime** for (D, \mathcal{P}) if

$$\left(\frac{N - (D/N)}{2}\right)\mathcal{P} = \begin{cases} \mathcal{O} & \text{if } \mathcal{P} = 2\mathcal{Q} \text{ for some } \mathcal{Q} \in \mathcal{L}_{\mathbb{Z}/N\mathbb{Z}} \\ (-1, 0) & \text{otherwise.} \end{cases}$$

Writing $(N - (D/N)) = 2^s t$ where t is odd, N is a **strong Lucas pseudoprime** for (D, \mathcal{P}) if

- $t\mathcal{P} = \mathcal{O}$, or
- $(2^r t)\mathcal{P} = (-1, 0)$ for some integer $0 \leq r < s$.

n	lpsp	L -psp(D, \mathcal{P})	elpsp	E -lpsp(D, \mathcal{P})	slpsp	S -lpsp(D, \mathcal{P})
10^2	1	1	0	1	0	1
10^3	6	9	2	6	0	6
10^4	21	29	9	21	2	22
10^5	91	124	50	91	14	98
10^6	279	395	155	279	41	302

Table 1: Number of pseudoprimes less than n for $(5, (47, 21))$

The Nonexistence of Certain Pseudoprimes

Let $\mathcal{L}_{\mathbb{Z}/N\mathbb{Z}}$ be a lucas group. Then there are no numbers that are Euler Lucas or strong Lucas numbers for every $\mathcal{P} \in \mathcal{L}_{\mathbb{Z}/N\mathbb{Z}}$.

Korselt Criterion for Lucas Pseudoprimes

An integer N is a Lucas pseudoprime for every $\mathcal{P} \in \mathcal{L}_{\mathbb{Z}/N\mathbb{Z}}$ if and only if N is squarefree and, for every prime p dividing N , $(p - (D/p))$ divides $(N - (D/N))$.

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.

- Find the number of points in each setting for which N is a pseudoprime.
- Find the density when N is the product of three or more primes.
- Identify when N is both a strong and an Euler Lucas pseudoprime.