Elliptic Pseudoprimes
Frequency of Extended Elliptic Pseudoprimes

L. Babinkostova, D. Fillmore, P. Lamkin, A. Lin, and C. Yost-Wolff

2018 REU CAD Symposium
Boise State University
The security of cryptosystems depends on the continued generation of new large prime numbers, which in turn requires ways to test for primality.
Motivation for Primality Tests

- The security of cryptosystems depends on the continued generation of new large prime numbers, which in turn requires ways to test for primality.
- Knowing how often these tests can turn up false positives allows us to design efficient and accurate algorithms.
Motivation for Primality Tests

- The security of cryptosystems depends on the continued generation of new large prime numbers, which in turn requires ways to test for primality.
- Knowing how often these tests can turn up false positives allows us to design efficient and accurate algorithms.
- A composite number which passes a probabilistic test is known as a pseudoprime. The focus of this research is analysis of types of pseudoprimes that arise from elliptic curves.
Motivation for Primality Tests

- The security of cryptosystems depends on the continued generation of new large prime numbers, which in turn requires ways to test for primality.
- Knowing how often these tests can turn up false positives allows us to design efficient and accurate algorithms.
- A composite number which passes a probabilistic test is known as a pseudoprime. The focus of this research is analysis of types of pseudoprimes that arise from elliptic curves.
- We investigate the probability a composite number $N$ is a (strong) S-Carmichael number for a random elliptic curve $E$. 
Fermat’s Little Theorem says that for any prime \( p \) and any base \( b \) relatively prime to \( p \), \( b^{p-1} \equiv 1 \mod p \).
Pseudoprimes

- Fermat’s Little Theorem says that for any prime $p$ and any base $b$ relatively prime to $p$, $b^{p-1} \equiv 1 \mod p$.
- This gives us a Fermat primality test: if $b^{N-1} \not\equiv 1 \mod N$, $N$ can’t be prime.
- But some composite numbers pass this test, and these are called pseudoprimes. If some $N$ passes for all bases $b$ relatively prime to $N$, then $N$ is called a Carmichael number.
Fermat’s Little Theorem says that for any prime $p$ and any base $b$ relatively prime to $p$, $b^{p-1} \equiv 1 \pmod{p}$.

This gives us a Fermat primality test: if $b^{N-1} \not\equiv 1 \pmod{N}$, $N$ can’t be prime.

But some composite numbers pass this test, and these are called pseudoprimes. If some $N$ passes for all bases $b$ relatively prime to $N$, then $N$ is called a Carmichael number.

This test relies on the multiplicative structure of $(\mathbb{Z}/N\mathbb{Z})^\times$. 

Pseudoprimes
Generalizing Pseudoprimes

Can we define pseudoprimes for other finite groups?
Can we define pseudoprimes for other finite groups?

$$(\mathbb{Z}/N\mathbb{Z})^\times$$
Generalizing Pseudoprimes

Can we define pseudoprimes for other finite groups?

$$(\mathbb{Z}/N\mathbb{Z})^* \rightarrow$$
Can we define pseudoprimes for other finite groups?

\[(\mathbb{Z}/N\mathbb{Z})^\times \to E(\mathbb{Z}/N\mathbb{Z})\ldots\]
Definition (Projective Space)

Projective space, \( \mathbb{P}^2(\mathbb{R}) \) is defined as \( \mathbb{R}^3/ \sim \), where \( (a, b, c) \sim (a', b', c') \) if there exists a \( 0 \neq u \in \mathbb{R} \) such that \( (a, b, c) = u(a', b', c') \). We write a point in \( \mathbb{P}^2(\mathbb{R}) \) as \( (a : b : c) \).
**Projective Space**

**Definition (Projective Space)**

Projective space, $\mathbb{P}^2(\mathbb{R})$ is defined as $\mathbb{R}^3/\sim$, where $(a, b, c) \sim (a', b', c')$ if there exists a $0 \neq u \in \mathbb{R}$ such that $(a, b, c) = u(a', b', c')$. We write a point in $\mathbb{P}^2(\mathbb{R})$ as $(a : b : c)$.

**Definition (Elliptic Curve)**

An *elliptic curve* over a ring $R$ is the set of solutions to an equation of the form $y^2z = x^3 + Axz^2 + Bz^3$. These points on the curve form a group under a definition of point addition explained on the next page.
Adding Points on an Elliptic Curve
Adding Points on an Elliptic Curve

Given two points $P$ and $Q$ on an elliptic curve, we can compute $P + Q$. 

Adding Points on an Elliptic Curve

Given two points $P$ and $Q$ on an elliptic curve, we can compute $P + Q$. 
Given two points $P$ and $Q$ on an elliptic curve, we can compute $P + Q$. 
Adding Points on an Elliptic Curve

Given two points $P$ and $Q$ on an elliptic curve, we can compute $P + Q$. 
Adding Points on an Elliptic Curve

Given two points $P$ and $Q$ on an elliptic curve, we can compute $P + Q$. 

![Diagram of adding points on an elliptic curve](image)
Adding Points on an Elliptic Curve

Given two points $P$ and $Q$ on an elliptic curve, we can compute $P + Q$. 

![Diagram of adding points on an elliptic curve]
Adding Points on an Elliptic Curve

Given two points $P$ and $Q$ on an elliptic curve, we can compute $P + Q$. 

![Diagram showing the addition of points on an elliptic curve](image.png)
Elliptic Pseudoprimes

Definition (Gordon, 1989)

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-d})$, and let $P$ be a point of infinite order on $E(\mathbb{Q})$. A composite number $N$ with $\gcd(N, 6\Delta) = 1$ is an $G$-pseudoprime for $(E, P)$ if $(\frac{-d}{N}) = -1$ and

$$(N + 1)P \equiv (0 : 1 : 0) \pmod{N}.$$
Elliptic Pseudoprimes

**Definition (Gordon, 1989)**

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-d})$, and let $P$ be a point of infinite order on $E(\mathbb{Q})$. A composite number $N$ with $\gcd(N, 6\Delta) = 1$ is an *G-pseudoprime* for $(E, P)$ if $(\frac{-d}{N}) = -1$ and

$$(N + 1)P \equiv (0 : 1 : 0) \mod N.$$
Elliptic Pseudoprimes

Definition (Gordon, 1989)

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-d})$, and let $P$ be a point of infinite order on $E(\mathbb{Q})$. A composite number $N$ with $\gcd(N, 6\Delta) = 1$ is an $G$-pseudoprime for $(E, P)$ if $(\frac{-d}{N}) = -1$ and $(N + 1)P \equiv (0 : 1 : 0) \mod N$.

Definition (Gordon, 1989)

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-d})$, and let $P$ be a point of infinite order on $E(\mathbb{Q})$. Let $N$ be a composite integer, and write $N + 1 = 2^s t$ with $t$ odd. Then $N$ is an strong $G$-pseudoprime for $(E, P)$ if $(\frac{-d}{N}) = -1$, $\gcd(N, 6\Delta) = 1$ and either:

- $tP \equiv (0 : 1 : 0) \mod N$ or
- $2^r tP \equiv (x : 0 : 1) \mod N$ for some $x$ and some $0 \leq r < s$.

Note that these properties are always true when $N$ is a prime number.
Definition (Gordon, 1989)

Let $N \in \mathbb{Z}$, and let $E/\mathbb{Q}$ be an elliptic curve. Then $N$ is an (strong) $G$-Carmichael number for $E$ if $N$ is a (strong) $G$ pseudoprime for $(E, P)$ for every point $P \in E(\mathbb{Z}/N\mathbb{Z})$. 
L-Series of an Elliptic Curve

**Definition**

We associate with an elliptic curve $E/\mathbb{Q}$ an $L$-series $\sum_{n \geq 1} a_n/n^s$, where $a_n$ is a multiplicative function given by

$$a_p = p + 1 - \#E(\mathbb{Z}/p\mathbb{Z})$$

and

$$a_p^k = a_p a_p^{k-1} - 1_E(p) p a_p^{k-2},$$

where $1_E(p) = 1$ if $E$ has good reduction at $p$, and 0 otherwise.

**Theorem**

Let $d(n)$ denote the number of divisors of $n$. Then for all $n$, we have that

$$|a_n| \leq d(n) \sqrt{n}$$
**Definition (Silverman, 2012)**

Let $N \in \mathbb{Z}$, and let $E/\mathbb{Q}$ be an elliptic curve of the form $y^2 = x^3 + Ax + B$, and let $P$ be a point in $E(\mathbb{Z}/N\mathbb{Z})$. Then $N$ is an $S$-pseudoprime for $(E, P)$ if it has at least two distinct prime factors and the following hold:

- $E$ has good reduction at every prime $p \mid N$
- $(N + 1 - a_N)P \equiv (0 : 1 : 0) \mod N$. 

---

**Extension of Elliptic Pseudoprimes**
Extension of Elliptic Pseudoprimes

Definition (Silverman, 2012)

Let $N \in \mathbb{Z}$, and let $E/\mathbb{Q}$ be an elliptic curve of the form $y^2 = x^3 + Ax + B$, and let $P$ be a point in $E(\mathbb{Z}/N\mathbb{Z})$. Then $N$ is an S-pseudoprime for $(E, P)$ if it has at least two distinct prime factors and the following hold:

- $E$ has good reduction at every prime $p \mid N$
- $(N + 1 - a_N)P \equiv (0 : 1 : 0) \mod N$.

Definition (Babinkostova et al., 2017)

Let $N, E, P$ be as defined above. Let $N + 1 - a_N = 2^s t$ where $t$ is odd. Then $N$ is an strong S-pseudoprime for $(E, P)$ if it has at least two distinct prime factors and the following hold:

- $E$ has good reduction at every prime $p \mid N$ and
- $tP \equiv (0 : 1 : 0) \mod N$ or
- $2^r tP = (x : 0 : 1) \mod N$ for some $x$ and some $0 \leq r < s$. 
Elliptic Carmichael Numbers

Definition (Silverman, 2012, REU 2017)

Let \( N \in \mathbb{Z} \), and let \( E/\mathbb{Q} \) be an elliptic curve. Then \( N \) is an (strong) \( S \)-Carmichael number for \( E \) if \( N \) is a (strong) \( S \)-pseudoprime for \((E, P)\) for every point \( P \in E(\mathbb{Z}/N\mathbb{Z}) \).
Lemma

Let $N$ be a composite number. If $N$ is an S-Carmichael number for an elliptic curve $E$, then

$$p + 1 - a_p \mid (p - 1)(N + 1 - a_N)$$

for all $p \mid N$. 

Carmichael Condition
Planar Points

Definition (Planar)

Let \( E(\mathbb{Z}/N\mathbb{Z}) \) be an elliptic curve, and \((x : y : z)\) a point on \( E \). We say \((x : y : z)\) is \textit{planar} if \(\gcd(z, N) = 1\). Otherwise we say \((x : y : z)\) is \textit{nonplanar}.
Planar Points

**Definition (Planar)**

Let $E(\mathbb{Z}/N\mathbb{Z})$ be an elliptic curve, and $(x : y : z)$ a point on $E$. We say $(x : y : z)$ is *planar* if $\gcd(z, N) = 1$. Otherwise we say $(x : y : z)$ is *nonplanar*.

**Definition**

Let $N \in \mathbb{Z}$, and let $E/\mathbb{Q}$ be an elliptic curve. Then $N$ is an *(strong) $(S$ or $G)$-Carmichael number for $E$* if $N$ is a *(strong) $(S$ or $G)$-pseudoprime* for $(E, P)$ for every planar point $P \in E(\mathbb{Z}/N\mathbb{Z})$. 
Planar Points

Where dashed lines hold if $a_p$ is odd for all $p | N$, and dotted lines hold if $\exp(E(\mathbb{Z}/p\mathbb{Z})) = 2$ for all $p | N$. 
Theorem

A composite integer $N$ is a strong $G$-pseudoprime for at most $5/8$ of the points in $E(\mathbb{Z}/N\mathbb{Z})$. 
Structure of $E(\mathbb{Z}/p\mathbb{Z})$

Theorem

Let $E/\mathbb{Q}$ be given by $y^2 = x^3 + Ax + B$. For a prime $p$, write $E(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/L\mathbb{Z} \oplus \mathbb{Z}/M\mathbb{Z}$ with $L \mid M$ and $p$ prime.
Structure of $E(\mathbb{Z}/p\mathbb{Z})$

**Theorem**

Let $E/\mathbb{Q}$ be given by $y^2 = x^3 + Ax + B$. For a prime $p$, write $E(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/L\mathbb{Z} \oplus \mathbb{Z}/M\mathbb{Z}$ with $L | M$ and $p$ prime. Then

- If $x^3 + Ax + B$ is irreducible in $\mathbb{Z}/p\mathbb{Z}$, then $L$ is odd and $M$ is odd.
**Theorem**

Let $E/\mathbb{Q}$ be given by $y^2 = x^3 + Ax + B$. For a prime $p$, write $E(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/L\mathbb{Z} \oplus \mathbb{Z}/M\mathbb{Z}$ with $L \mid M$ and $p$ prime. Then

- If $x^3 + Ax + B$ is irreducible in $\mathbb{Z}/p\mathbb{Z}$, then $L$ is odd and $M$ is odd.
- If $x^3 + Ax + B$ has 1 root in $\mathbb{Z}/p\mathbb{Z}$, then $L$ is odd and $M$ is even.
Structure of $E(\mathbb{Z}/p\mathbb{Z})$

**Theorem**

Let $E/\mathbb{Q}$ be given by $y^2 = x^3 + Ax + B$. For a prime $p$, write $E(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/L\mathbb{Z} \oplus \mathbb{Z}/M\mathbb{Z}$ with $L \mid M$ and $p$ prime. Then

- If $x^3 + Ax + B$ is irreducible in $\mathbb{Z}/p\mathbb{Z}$, then $L$ is odd and $M$ is odd.
- If $x^3 + Ax + B$ has 1 root in $\mathbb{Z}/p\mathbb{Z}$, then $L$ is odd and $M$ is even.
- If $x^3 + Ax + B$ has 3 roots in $\mathbb{Z}/p\mathbb{Z}$, then $L$ and $M$ are even.
Frequency of Strong S-Pseudoprime Points

**Theorem**

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

$$\frac{17q_1q_2 + 2q_1 + 2q_2 + 4}{32q_1q_2}.$$
**Lemma (Nicolas, 1987)**

*For an integer $A \geq 3$, let $d(A)$ denote the number of divisors of $A$. Then*

\[
\frac{\log d(A)}{\log 2} \leq 1.538 \frac{\log A}{\log_2 A}.
\]
Preliminary Bounds

Lemma (Nicolas, 1987)

For an integer $A \geq 3$, let $d(A)$ denote the number of divisors of $A$. Then

$$\frac{\log d(A)}{\log 2} \leq 1.538 \frac{\log A}{\log_2 A}.$$

Lemma (Lenstra, 1987)

Consider a set of integers $S \subseteq [p + 1 − 2\sqrt{p}, p + 1 + 2\sqrt{p}]$, where $p$ is prime. The probability that a random elliptic curve $E(\mathbb{Z}/p\mathbb{Z})$ has order $\#(E(\mathbb{Z}/p\mathbb{Z})) \in S$ is

$$O \left( \frac{|S|}{\sqrt{p}} \log p \log_2^2 p \right).$$
Theorem

Let $N$ be a composite number. Let $p$ be a prime factor of $N$ with $p > N^{c \log 2 / \log 2 N}$, $p^2 
mid N$. Then for a randomly chosen elliptic curve $E$ with good reduction at all primes $p \mid N$,

$$
\Pr[N \text{ is S-Carmichael for } E] = O \left( p^{-1/2 + 1.538/c + \epsilon} \right).
$$
Corollary

If $N$ is squarefree with at most $k$ prime factors, then for a randomly chosen elliptic curve $E$ with good reduction at all primes $p | N$

$$\Pr[N \text{ is S-Carmichael for } E] = O \left( N^{-\frac{1}{2k} + \epsilon} \right).$$
Probability Bounds for Fixed $N$ with Large Prime Factor

**Theorem**

Let $N$ be a composite number. Let $p$ be a prime factor of $N$ such that $p \mid N$, $p^2 \nmid N$. Then

$$\Pr[N \text{ is S-Carmichael at } E] = O \left( \frac{\log_2 N \log^3 p}{\log p} \right).$$
Probability Bounds for Large $\omega(N)$

Lemma

For a squarefree integer $N$, given $\omega(N) = r \cdot \frac{\log N}{\log \log N}$ for some $r > 1/2$. Then for a random curve $E$

$$\Pr[N \text{ is S-Carmichael at } E] = O \left( \exp \left( \frac{-cr(\log N)^{1-\frac{1}{2r}}}{\log_2 N} \right) \right).$$

Here $\exp(y) = x$ implies $e^y = x$. 

Motivation
Elliptic Pseudoprimes
Planar Points
Pointwise Bounds
Bounds for S-Carmichael
Bounds for Strong S-Carmichael
Conclusion
Theorem

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 $p | N$ is

$$O \left( \left( \log x \right)^{-o(\log_3 x)} \right).$$
Theorem (Characterization of Strong S-Carmichael Numbers)

Let $N$ be an odd composite integer. Then $N$ is a 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 $p | N$. 
Probability Bounds Based on the Parity of $a_p$

**Theorem**

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 $p | N$ is

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

where $\omega(N)$ denotes the number of distinct prime divisors of $N$. 
Probability Bounds for Strong S-Carmichael Numbers

**Theorem**

Let $N$ be an odd composite squarefree integer with $\omega(N) \leq \frac{\log(N)}{\log_2 N}$. 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

$$O \left( \frac{\log \omega(N) \log_3^3 N}{3^\omega(N) \log_2 N} \right).$$
Theorem

Let $N$ be an odd composite squarefree integer with $\omega(N) \leq \frac{\log(N)}{\log^2 N}$. 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

$$O\left(\frac{\log \omega(N) \log^3 N}{3\omega(N) \log_2 N}\right).$$

**NOTE:** The condition on $\omega(n)$ happens asymptotically with probability 1 since $\omega(n)$ for $n \leq x$ is normally distributed with mean $\log_2(x)$ and standard deviation $\sqrt{\log_2(x)}$. 
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.
References

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

H. W. Lenstra,
Factoring Integers with Elliptic Curves,

J.L. Nicolas,
On Highly Composite Numbers,

J.H. Silverman,
Elliptic Carmichael Numbers and Elliptic Korselt Criteria,
Acknowledgements

This research is sponsored by NSF grant DMS-1659872 and Boise State University.
We would especially like to thank our wonderful mentor Professor Liljana Babinkostova for all her hard work on our research, and for organizing this REU.
THANKS!