Crytossystems 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 \( E/Q : y^2 = x^3 + Ax + B \) over \( Q \) is defined as the set \( E(Q) = \{(x, y) \in Q^2 : y^2 = x^3 + Ax + B\} \cup \{O\} \) where \( \Delta = 4A^3 + 27B^2 \neq 0 \).

The \( L \)-function of an elliptic curve \( E/Q \) is

\[
L(E, s) = \prod_{P} \left(1 - \frac{a_P}{p^s} + \frac{1}{p^{2s}}\right)^{-1} = \sum_{n=0}^{\infty} a_n \frac{1}{n^s}.
\]

#### Elliptic Pseudoprimes

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

Moreover, \( N \) is an Euler elliptic pseudoprime for \( (E, P) \) if \( \left(\frac{N+1-a_N}{2}\right)p \equiv O \pmod{N} \) for \( P = 2Q \) for some \( Q \in E(Z/NZ) \).

Writing \( N+1-a_N = 2t \) where \( t \) is odd, \( N \) is a strong elliptic pseudoprime for \( (E, P) \) if

\[
\begin{align*}
&\text{if } (P \equiv O \pmod{N}), \text{ or } \\
&\text{if } (2t^2P \equiv (x, 0) \pmod{N}) \text{ for some } x \in Z/NZ \text{ and integer } 0 < t < \alpha.
\end{align*}
\]

### Strong to Elliptic Carmichael Numbers

#### Elliptic Korselt Criteria

Korselt Number of Type I

\[
\begin{align*}
\text{Elliptic Korselt Number of Type I} &\mid N+1-a_N \quad \text{if } N+1-a_N \text{ is even} \\
&\text{Elliptic Korselt Number of Type I} &\mid N+1-a_N \quad \text{if } N+1-a_N \text{ is odd}
\end{align*}
\]

Product of Strong Elliptic Carmichael Numbers

\[
\begin{align*}
\text{Product of Strong Elliptic Carmichael Numbers} &\mid N+1-a_N \\
&\text{Product of Strong Elliptic Carmichael Numbers} &\mid N+1-a_N
\end{align*}
\]

#### Anomalous Prime Factors vs. Elliptic Korselt Type of Number I

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

\[
\begin{align*}
Pr(a_p = a_q = 1) &\equiv \Omega(1/M^{r\epsilon}) \quad \text{and} \\
Pr(p+1-a_p, q+1-a_q \mid (N+1-a_N)) &\equiv \Omega(1/M^{r(\epsilon-\epsilon^*)}).
\end{align*}
\]

Density of \( E \) with \( \#E(Z/NZ) = N+1-a_N \) Given a Condition

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

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

### Lucas Pseudoprimes

#### Lucas Groups

Let \( D, N \) be coprime integers. The Lucas group \( L_{2NZ} \) is defined on \( L_{2NZ} = \{(x, y) \in (Z/2ZW)^2 \mid x^2 - dy^2 \equiv 1 \pmod{N}\} \).

#### Algebraic Structure of Lucas Groups

If \( p \) is a prime and \( D \) is an integer coprime to \( p \), then \( L_{2pZ} \) is a cyclic group of order \( p^{r-1}(p-D/p) \).

Moreover, \( N \) is an Euler Lucas pseudoprime for \( (D, P) \) if

\[
\left(\frac{N-D/N}{2}\right)P \equiv O \quad \text{if } P = 2Q \quad \text{for some } Q \in L_{2NZ}.
\]

Writing \( N-D/N = 2t \) where \( t \) is odd, \( N \) is a strong Lucas pseudoprime for \( (D, P) \) if

\[
\begin{align*}
&\text{if } (P \equiv O), \text{ or } \\
&\text{if } (2t^2P \equiv (x, 0)) \text{ for some integer } 0 \leq t < s.
\end{align*}
\]

#### The Nonexistence of Certain Pseudoprimes

Let \( L_{2NZ} \) be a Lucas group. Then there are no numbers that are Euler Lucas or strong Lucas numbers for every \( P \in L_{2NZ} \).

### 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.