Elliptic Pseudoprimes and Elliptic Carmichael Numbers

Joseph H. Silverman

Brown University

AMS–SIAM Session on Math. of Computation:
Algebra and Number Theory
AMS–MAA Joint Math Meeting, Boston, 2012

Friday January 6, 9:00–9:20am

Pseudoprimes and Carmichael Numbers

Let $a \geq 2$. Classically, a natural number n is a

pseudoprime to the base a

if n is composite and satisfies

$$a^{n-1} \equiv 1 \pmod{n}.$$

Then n is a **Carmichael number** if n is a pseudoprime to the base a for all $\gcd(a, n) = 1$.

The first few Carmichael numbers are

$$561,\ 1105,\ 1729,\ 2465, \ldots.$$

Theorem. (Alford, Granville, Pomerance, 1994)
There are infinitely many Carmichael numbers.

Elliptic Pseudoprimes

The reason that

$$a^{p-1} \equiv 1 \pmod{p}$$

is because the group $\mathbb{F}_p^*$ has order $p-1$.
Let $E/\mathbb{Q}$ be an elliptic curve. Then

$$E(\mathbb{F}_p) \text{ has order } p+1-a_p.$$

The a_p coefficients appear in the L-series for E,

$$L(E/\mathbb{Q}, s) = \sum \frac{a_n}{n^s}.$$

Let n have at least two distinct prime factors and satisfy $\gcd(n, \Delta_E) = 1$, and let $P \in E(\mathbb{Z}/n\mathbb{Z})$ be a point on E modulo n. We say that n is an **elliptic pseudoprime to the base P** if

$$(n+1-a_n)P \equiv 0 \pmod{n}, \quad \text{i.e., in } E(\mathbb{Z}/n\mathbb{Z}).$$

Gordon elliptic pseudoprimes

Dan Gordon (1989) was the first to define elliptic pseudoprimes for CM elliptic curves. Subsequent work on Gordon elliptic pseudoprimes was done by Balasubramanian, Cojocaru, Ekstrom, Guillaume, H. Ito, Luca, Miyamoto, Morain, Müller, M.R. Murty, Pomerance, Shparlinski, Thakur.

Let $E/\mathbb{Q}$ be an elliptic curve with CM by an order in $\mathbb{Q}(\sqrt{-D})$. A composite number n is a **Gordon elliptic pseudoprime to the base** P if

$$(-D \mid n) = -1 \qquad \text{and} \qquad (n+1)P \equiv 0 \pmod{n}.$$

It is not hard to check that for (most) n,

$$(-D \mid n) = -1 \quad \text{and} \quad n \text{ square-free} \iff a_n = 0.$$

Thus $(n+1-a_n)P = (n+1)P$, so (most) Gordon pseudoprimes are pseudoprimes in our sense.

Elliptic Carmichael Numbers

A natural number n is an

elliptic Carmichael number for E

if n is an elliptic pseudoprime to the base P for every $P \in E(\mathbb{Z}/n\mathbb{Z})$.

Example. The elliptic curve

$$E : y^2 = x^3 + x + 3$$

has elliptic Carmichael numbers

$$15,\ 77,\ 203,\ 245,\ 725,\ 875, \ldots.$$

Example. The curve

$$E : y^2 = x^3 + x + 3$$

has no elliptic Korselt–Carmichael numbers smaller than 25000. The first such number for E is 27563.

Parity of Carmichael Numbers

It is a classical fact that a Carmichael number is odd. This follows from

$$(-1)^{n-1} \equiv 1 \pmod{n},$$

which reflects the fact that $\mathbb{Q}^*$ has an element of order 2.

Here is an elliptic analogue.

Theorem. Suppose that $E(\mathbb{Q})$ has a point of exact order m. Then any Carmichael number n for E satisfies

$$n \equiv a_n - 1 \pmod{m}.$$

The proof follows from the injectivity of torsion under reduction.

Korselt's Criterion

In the classical case:

Korselt's Criterion. A composite number n is a Carmichael number if and only if

- n is odd,
- n is square-free,
- $p - 1 \mid n - 1$ for every prime $p \mid n$.

We already discussed the elliptic analogue of the parity condition on the last slide.

There are many examples showing that elliptic Carmichael numbers need not be squarefree. We formulate elliptic analogues of the second and third properties.

Elliptic Korselt Numbers

We say that n is an **elliptic Korselt number** (of **Type I**) for E if it satisfies the following conditions:

- n has at least two distinct prime factors.
- $\gcd(n, \Delta_E) = 1$.
- $p + 1 - a_p$ divides $n + 1 - a_n$ for every $p \mid n$.
- $\operatorname{ord}_p(a_n - 1) \geq \operatorname{ord}_p(n) - \begin{cases} 1 & \text{if } a_p \not\equiv 1 \pmod{p}, \\ 0 & \text{if } a_p \equiv 1 \pmod{p}. \end{cases}$

We remark that the ord_p condition is an elliptic analogue of the classical condition that n be square-free, since for supersingular primes we have $a_p = a_n = 0$, so the elliptic condition becomes $1 \geq \operatorname{ord}_p(n)$.

If $p \geq 7$, then $a_p \equiv 1 \pmod{p}$ iff $a_p = 1$. Then $\#E(\mathbb{F}_p) = p$, and p is called **anomalous**.

An Elliptic Korselt Criterion

Elliptic Korselt Criterion I. Let n be odd and suppose that n is a Type I elliptic Korselt number for E. Then n is an elliptic Carmichael number for E.

The proof is more-or-less immediate if n is square-free. Otherwise one must do a careful analysis using the formal group, which is what leads to the ord_p condition in the definition of elliptic Korselt number.

The elliptic Korselt criterion is very easy to use in practice, provided that n is small enough to factor, since then the SEA algorithm is a polynomial-time algorithm for computing a_p and a_n.

A drawback of the Type I Korselt criterion is that it only works one way.

A Two-Way Elliptic Korselt Criterion

For $n \geq 1$ and $p^e \parallel n$, let

$$\epsilon_{n,p}(E) = \text{exponent of the group } E(\mathbb{Z}/p^e\mathbb{Z}).$$

We define n to be an **elliptic Korselt number** of **Type II** for E if it satisfies the following conditions:

- n has at least two distinct prime factors.
- $\gcd(n, \Delta_E) = 1$.
- $\epsilon_{n,p}(E)$ divides $n + 1 - a_n$ for all $p \mid n$.

Elliptic Korselt Criterion II. Let n be odd. Then n is a Type II elliptic Korselt number for E if and only if n is an elliptic Carmichael number for E.

It is possible, but somewhat painful, to compute the quantities $\epsilon_{n,p}(E)$ appearing in the Type II criterion.

Korselt Numbers of the Form pq

Using the classical Korselt criterion, it is easy to prove that a classical Carmichael number has at least three distinct prime factors. This is not true in the elliptic case, but we do have the following.

Theorem. Suppose that $n = pq$ is a Type I elliptic Korselt number for E with $p < q$. Then one of the following is true:

- $p \leq 17$.
- $a_p = a_q = 1$, i.e., both p and q are anomalous.
- $p \geq \sqrt{q}$.

The proof uses the Korselt divisibility condition, some elementary algebra, and Hasse's estimate for $|a_p|$ and $|a_q|$.

Universal Elliptic Carmichael Numbers

We will say that n is a **universal elliptic Carmichael number** if it is an elliptic Carmichael number for every elliptic curve over $\mathbb{Z}/n\mathbb{Z}$.

Question. Do there exist any universal Carmichael numbers? (Guess: Probably not.)

This raises the interesting problem of estimating (from above or below)

$$\mathcal{C}(n) = \#\left\{ E \bmod n\mathbb{Z} : \begin{array}{l} n \text{ is an elliptic Carmichael} \\ \text{number for } E \end{array} \right\}$$

Rough heuristic estimates suggest, at least for $n = pq$, that $\mathcal{C}(n)$ might be bounded independent of n.

In Conclusion

Ongoing research on elliptic Carmichael numbers is currently a joint project with Chantal David.

I want to thank you for your attention and the organizers for inviting me to speak.

Elliptic Pseudoprimes and Elliptic Carmichael Numbers

Joseph H. Silverman

Brown University

AMS–SIAM Session on Math. of Computation:
Algebra and Number Theory
AMS–MAA Joint Math Meeting, Boston, 2012

Friday January 6, 9:00–9:20am