ACTA ARITHMETICA
155.3 (2012)

Elliptic Carmichael numbers and elliptic Korselt criteria

by

JOSEPH H. SILVERMAN (Providence, RI)

This article is dedicated to Andrzej Schinzel on the occasion of his 75th birthday

1. Introduction. Classically, a composite integer $n > 2$ is called a *pseudoprime to the base* b if

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

A *Carmichael number* is an integer n that is a pseudoprime to all bases that are relatively prime to n. Explicit examples of Carmichael numbers were given by Carmichael [3] in 1912, although the concept had been studied earlier by Korselt [16] in 1899. In particular, Korselt gave the following elementary criterion for Carmichael numbers, which was rediscovered by Carmichael.

PROPOSITION 1 (Korselt's criterion). *A positive composite number n is a Carmichael number if and only if n is odd, square-free, and every prime p dividing n has the property that $p - 1$ divides $n - 1$.*

In 1994, Alford, Granville, and Pomerance [1] proved the long-standing conjecture that there are infinitely many Carmichael numbers.

The definitions of pseudoprimes and Carmichael numbers are related to the orders of numbers in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$. It is thus natural to extend these constructions to the setting of other algebraic groups, for example to elliptic curves. Gordon [9] appears to have been the first to define elliptic pseudoprimes, at least in the setting of elliptic curves having complex multiplication. See Remark 4 for a description of Gordon's definition, which includes a supersingularity condition, and for additional references.

In this note we define elliptic pseudoprimes (Section 2) and elliptic Carmichael numbers (Section 3) for arbitrary elliptic curves $E/\mathbb{Q}$. Our definition more-or-less reduces to Gordon's definition in the CM setting. We

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 11Y11.
Key words and phrases: Carmichael number, pseudoprime, elliptic curve.

DOI: 10.4064/aa155-3-1

give two Korselt-type criteria for elliptic Carmichael numbers. The first, in Section 4, only goes in one direction (Korselt implies Carmichael) and is relatively easy to check in practice if one knows how to factor n. The second version, described in Section 5, is bi-directional, but less practical. In Section 6 we discuss elliptic Carmichael numbers pq that are the product of exactly two primes. (It is an easy exercise to show that there are no classical Carmichael numbers of the form pq.) Finally, we give some numerical examples of elliptic Carmichael numbers in Section 7.

Without going into details (which are given later), we note that our construction replaces the quantity $n-1$ in the classical pseudoprime definition $b^{n-1} \equiv 1 \pmod{n}$ with the quantity $n+1-a_n$ in the case of elliptic curves, where a_n is the usual coefficient of the L-series of $E/\mathbb{Q}$. We then say that an integer n is an elliptic pseudoprime for the curve E and point $P \in E(\mathbb{Z}/n\mathbb{Z})$ if n has at least two distinct prime factors, if E has good reduction at all primes dividing n, and if

$$(n+1-a_n)P \equiv 0 \pmod{n}, \tag{1.1}$$

where the congruence (1.1) takes place in $E(\mathbb{Z}/n\mathbb{Z})$. Notice that if we take n to be a prime p, then (1.1) is automatically true, because $\#E(\mathbb{Z}/p\mathbb{Z}) = p+1-a_p$. Thus the analogy between the multiplicative group and elliptic curves that we are using may be summarized by noting that

$$\#\mathbb{G}_{\mathrm{m}}(\mathbb{Z}/p\mathbb{Z}) = p-1 \quad \text{and} \quad \#E(\mathbb{Z}/p\mathbb{Z}) = p+1-a_p, \tag{1.2}$$

replacing p by n (and removing the equality signs), and asking if the resulting quantity $n-1$, respectively $n+1-a_n$, is still an annihilator of $\mathbb{G}_{\mathrm{m}}(\mathbb{Z}/n\mathbb{Z})$, respectively $E(\mathbb{Z}/n\mathbb{Z})$.

Remark 2. In this paper, when we write $E(\mathbb{Z}/n\mathbb{Z})$, we will always assume that E has good reduction at all primes dividing n. It follows that a minimal Weierstrass equation for $E/\mathbb{Q}$ defines a group scheme

$$E \to \operatorname{Spec}(\mathbb{Z}/n\mathbb{Z}),$$

so it makes sense to talk about the group of sections, which is what we mean by the notation $E(\mathbb{Z}/n\mathbb{Z})$. Further, if n factors as $n = p_1^{e_1} \cdots p_t^{e_t}$ with $p_1, \ldots, p_t$ distinct primes, then there is a natural isomorphism (essentially by the Chinese remainder theorem)

$$E(\mathbb{Z}/n\mathbb{Z}) \cong E(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times E(\mathbb{Z}/p_t^{e_t}\mathbb{Z}).$$

2. Elliptic pseudoprimes. In this section we define elliptic pseudoprimes in general and relate our definition to Gordon's definition of elliptic pseudoprimes on CM elliptic curves.

Definition. Let $n \in \mathbb{Z}$, let $E/\mathbb{Q}$ be an elliptic curve given by a minimal Weierstrass equation, and let $P \in E(\mathbb{Z}/n\mathbb{Z})$. Write the L-series of $E/\mathbb{Q}$ as

$L(E/\mathbb{Q}, s) = \sum a_n/n^s$. We say that n is an *elliptic pseudoprime* for (E, P) if n has at least two distinct prime factors and the following two conditions hold:

- E has good reduction at every prime p dividing n;

(2.1)
- $(n + 1 - a_n)P \equiv 0 \pmod{n}$.

REMARK 3. We note that if E has good reduction at p, then every point in $E(\mathbb{Z}/p\mathbb{Z})$ is killed by $p + 1 - a_p$, since $p + 1 - a_p = \#E(\mathbb{Z}/p\mathbb{Z})$.

REMARK 4. The first definition of elliptic pseudoprimes appears to be due to Gordon [9]. Gordon's definition, which only applies to elliptic curves with complex multiplication, is as follows. Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by an order in $\mathbb{Q}(\sqrt{-D}\,)$, and let $P \in E(\mathbb{Q})$ be a non-torsion point. Then a composite number n is a *Gordon elliptic pseudoprime* for the pair (E, P) if

$$\left(\frac{-D}{n}\right) = -1 \quad \text{and} \quad (n + 1)P \equiv 0 \pmod{n}.$$

Gordon's motivation for this definition was to study elliptic pseudoprimes as tools for primality and factorization algorithms. Under GRH, he proves that the set of elliptic pseudoprimes has density 0, and gives an example of a pair (E, P) having infinitely many elliptic pseudoprimes.

For simplicity, we consider Gordon's definition for a curve E that has CM by the full ring of integers of $\mathbb{Q}(\sqrt{-D}\,)$. Then for primes $p \ge 5$ of good reduction, we have $a_p = 0$ if and only if p is inert in $\mathbb{Q}(\sqrt{-D})$, which is equivalent to $(-D \,|\, p) = -1$. Thus the condition $(-D \,|\, n) = -1$ implies that at least one prime p dividing n satisfies $a_p = 0$. If we also assume that $p^2 \nmid n$, then $a_n = 0$, since a_n is a multiplicative function. (More generally, if $a_p = 0$, then $a_{p^{2k+1}} = 0$ and $a_{p^{2k}} = (-p)^k$ for all $k \ge 0$.)

To recapitulate, we have

$$\left(\frac{-D}{n}\right) = -1 \text{ and } n \text{ square-free } \Rightarrow \ a_n = 0.$$

Thus for (most) square-free values of n, Gordon's condition $(n + 1)P \equiv 0 \pmod{n}$ is the same as our condition $(n + 1 - a_n)P \equiv 0 \pmod{n}$, because his Jacobi symbol condition $(-D \,|\, n) = -1$ forces $a_n = 0$.

For other articles that study Gordon elliptic pseudoprimes and related quantities, see [2, 4, 6, 7, 8, 10, 11, 13, 14, 15, 18, 19].

3. Elliptic Carmichael numbers

DEFINITION. Let $n \in \mathbb{Z}$ and let $E/\mathbb{Q}$ be an elliptic curve. We say that n is an *elliptic Carmichael number for E* if n is an elliptic pseudoprime for (E, P) for every point $P \in E(\mathbb{Z}/n\mathbb{Z})$.

Classically, a Carmichael number n is necessarily odd, since it satisfies $(-1)^{n-1} \equiv 1 \pmod{n}$. More intrinsically, this is true because the multiplicative group $\mathbb{G}_\mathrm{m}(\mathbb{Q})$ has an element of order 2. The elliptic analog of this fact is the following elementary proposition.

Proposition 5. *Let $E/\mathbb{Q}$ be an elliptic curve, and let $T \in E(\mathbb{Q})$ be a torsion point of exact order m. If n is a Carmichael number for E, then*

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

Proof. Suppose that n is a Carmichael number for E. To ease notation, let $N = n + 1 - a_n$. By definition, n has at least two distinct prime factors, say p and q. Further, we know that $NT \equiv 0 \pmod{n}$, and hence

$$NT \equiv 0 \pmod{p} \quad \text{and} \quad NT \equiv 0 \pmod{q}.$$

Write $m = p^i m'$ with $p \nmid m'$. Then $p^i NT \equiv 0 \pmod{p}$, and also $p^i NT$ is killed by m'. The injectivity of prime-to-p torsion under reduction modulo p [21, VII.3.1] allows us to conclude that $p^i NT = 0$.

Similarly, writing $m = q^j m''$ with $q \nmid m''$, we find that $q^j NT = 0$. Since p and q are distinct, it follows that $NT = 0$. But by assumption, T has exact order m, hence $m \mid N$. ∎

Remark 6. An appropriate formulation of Proposition 5 is true more generally for abelian varieties. Thus let $A/\mathbb{Q}$ be an abelian variety, let n be an integer with at least two distinct prime factors p and q such that A has good reduction at p and q, and let N be an integer that annihilates $A(\mathbb{Z}/n\mathbb{Z})$. (Here we can take A to be the Néron model over $\mathbb{Z}$, so A is a group scheme over $\operatorname{Spec}\mathbb{Z}$ and it makes sense to talk about the group of sections $A(\mathbb{Z}/n\mathbb{Z})$.) Suppose further that $A(\mathbb{Q})$ has a point of exact order m. Then $m \mid N$.

Definition. Let $n \in \mathbb{Z}$. We will say that n is a *universal elliptic Carmichael number* if n is an elliptic Carmichael number for every elliptic curve (elliptic scheme) over $\mathbb{Z}/n\mathbb{Z}$.

Remark 7. It is natural to ask whether there are *any* universal elliptic Carmichael numbers. Our guess is that probably none exist, or in any case, that there are at most finitely many. This raises the interesting question of finding nontrivial upper and lower bounds, in terms of n, for the size of the set

$$\mathcal{C}(n) = \{E \bmod n : n \text{ is a Carmichael number for } E\}.$$

For example, suppose that $n = pq$ is a product of distinct primes. A very rough heuristic estimate suggests that the probability that a given $E \bmod pq$ has pq as a Carmichael number is $O((pq)^{-1})$, so at least for such n one might conjecture that $\#\mathcal{C}(pq)$ is bounded independently of pq.

4. Elliptic Korselt numbers of type I. The classical Korselt criterion (Proposition 1) gives an efficient method for determining if a given integer n is a Carmichael number, assuming of course that one is able to factor n into a product of primes. In this section we give a practical one-way Korselt criterion for elliptic Carmichael numbers. Any number satisfying this elliptic Korselt criterion is an elliptic Carmichael number, but the converse need not be true.

DEFINITION. Let $n \in \mathbb{Z}$, and let $E/\mathbb{Q}$ be an elliptic curve. We say that n is an *elliptic Korselt number for E of type I* if n has at least two distinct prime factors, and if for every prime p dividing n the following conditions hold:

- E has good reduction at p;

(4.1) • $p + 1 - a_p$ divides $n + 1 - a_n$;

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

REMARK 8. If n is square-free and $a_p \not\equiv 1 \pmod{p}$ for all $p \mid n$, then condition (4.2) is vacuous, since it reduces to the statement that $\operatorname{ord}_p(a_n - 1) \geq 0$.

REMARK 9. Classical Carmichael numbers are automatically square-free. The elliptic analog of this fact is our Korselt condition (4.2). To see the relationship, we extend the analogy used by Gordon to consider values of n such that E is supersingular at all primes $p \mid n$. For ease of exposition, we will make the slightly stronger assumption that $a_p = 0$ for all $p \mid n$. (This is only stronger for $p = 2$ and $p = 3$.) Then $p \mid a_n$, since as noted earlier, a_n is a multiplicative function, and $a_p = 0$ implies that $a_{p^{2k+1}} = 0$ and $a_{p^{2k}} = (-p)^k$. Hence in this situation we have

$$\operatorname{ord}_p(a_n - 1) = 0 \quad \text{and} \quad a_p = 0 \not\equiv 1 \pmod{p},$$

so (4.2) reduces to the statement that $\operatorname{ord}_p(n) \leq 1$. This is true for all $p \mid n$, so n is square-free. Of course, this is under the assumption that $a_p = 0$ for all $p \mid n$. As we will see later in Example 18, elliptic Carmichael numbers need not in general be square-free.

REMARK 10. If $p \geq 7$, then

$$a_p \equiv 1 \pmod{p} \iff E \text{ is anomalous at } p,$$

where we recall that E is *anomalous* if $a_p = 1$, or equivalently, if we have $\#E(\mathbb{Z}/p\mathbb{Z}) = p$. In particular, condition (4.2) in the definition of type I Korselt numbers is vacuous if the following three conditions are true for all prime divisors p of n:

$$(1)\ p \geq 7; \qquad (2)\ E \text{ is not anomalous at } p; \qquad (3)\ p^2 \nmid n.$$

We also observe that the Hasse–Weil estimate $|a_p| \le 2\sqrt{p}$ implies

$$\operatorname{ord}_p(p+1-a_p) \le 1 \quad \text{unless } p=2 \text{ and } a_p=-1.$$

The exceptional case, namely $\operatorname{ord}_2(3-a_2)=2$ when $a_2=-1$, is the reason that the next proposition deals only with odd values of n.

PROPOSITION 11 (Elliptic Korselt criterion I). *Let $n \in \mathbb{Z}$ be an odd integer, and let $E/\mathbb{Q}$ be an elliptic curve. If n is an elliptic Korselt number for E of type I, then n is an elliptic Carmichael number for E.*

Proof. Let p be a prime of good reduction for E. Then the group $E(\mathbb{Z}/p\mathbb{Z})$ has order $p+1-a_p$, so the standard filtration on the formal group of $E(\mathbb{Q}_p)$ (see [21]) implies that

$$(4.3)\qquad p^{i-1}(p+1-a_p)P \equiv 0 \pmod{p^i} \quad \text{for all } i \ge 1 \text{ and all } P \in E(\mathbb{Q}_p).$$

Now let $P \in E(\mathbb{Z}/n\mathbb{Z})$, and write $n = p^i n'$ with $i \ge 1$ and $p \nmid n'$. Suppose first that $a_p \not\equiv 1 \pmod{p}$. Then $p+1-a_p$ is relatively prime to p, so (4.1) and (4.2) together imply that

$$(4.4)\qquad p^{i-1}(p+1-a_p) \text{ divides } n+1-a_n.$$

Next suppose that $a_p \equiv 1 \pmod{p}$. As noted earlier, the Hasse–Weil estimate $|a_p| \le 2\sqrt{p}$ then implies that

$$(4.5)\qquad \operatorname{ord}_p(p+1-a_p) = 1.$$

(This is where we use the assumption that n is odd, so $p \ne 2$.) We compute

$$
\begin{aligned}
(4.6)\qquad & \operatorname{ord}_p(n+1-a_n) && \\
&= \operatorname{ord}_p(p^i n' + 1 - a_n) && \text{since } n = p^i n' \\
&\ge \min\{i, \operatorname{ord}_p(a_n-1)\} && \text{by the triangle inequality} \\
&\ge \min\{i, \operatorname{ord}_p(n)\} && \text{from the Korselt condition (4.2)} \\
&= i && \text{since } n = p^i n' \\
&= \operatorname{ord}_p(p^{i-1}(p+1-a_p)) && \text{from (4.5).}
\end{aligned}
$$

Combining (4.4) and (4.6), we have proven that

$$p^{i-1}(p+1-a_p) \mid n+1-a_n \quad \text{for all primes } p \mid n.$$

It follows from (4.3) that

$$(n+1-a_n)P \equiv 0 \pmod{p^{\operatorname{ord}_p(n)}} \quad \text{for all primes } p \mid n.$$

Using the Chinese remainder theorem, we conclude that

$$(n+1-a_n)P \equiv 0 \pmod{n}.$$

Finally, since $P \in E(\mathbb{Z}/n\mathbb{Z})$ was arbitrary, this completes the proof that n is an elliptic Carmichael number for E. ∎

5. Elliptic Korselt numbers of type II. The classical Korselt criterion gives both a necessary and sufficient condition for a number n to be a Carmichael number. Our Proposition 11 gives one implication, namely type I Korselt implies Carmichael. The reason we do not get the converse implication is that condition (4.1) in the definition of type I Korselt numbers is not, in fact, the exact analog of the classical condition. Condition (4.1) comes from the analogy, already noted in (1.2) of the introduction, that

$$\#\mathbb{G}_{\mathrm{m}}(\mathbb{Z}/p\mathbb{Z}) = p-1 \quad \text{and} \quad \#E(\mathbb{Z}/p\mathbb{Z}) = p+1-a_p.$$

However, the real reason that $p-1$ appears in the classical Korselt criterion is that $p-1$ is the exponent of the group $(\mathbb{Z}/p\mathbb{Z})^*$, i.e., $p-1$ is the smallest positive integer that annihilates every element of $(\mathbb{Z}/p\mathbb{Z})^*$. This follows, of course, from the fact that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

Elliptic curve groups $E(\mathbb{Z}/p\mathbb{Z})$, by way of contrast, need not be cyclic, although it is true that they are always a product of at most two cyclic groups. So a more precise elliptic analog of the classical Korselt criterion is obtained by using the exponent of the group $E(\mathbb{Z}/p\mathbb{Z})$, rather than its order. This leads to the following definition and criterion, which while more satisfactory in that it is both necessary and sufficient, is much less practical than Proposition 11.

Definition. For a group G, we write $\epsilon(G)$ for the *exponent of* G, i.e., the least common multiple of the orders of the elements of G. Equivalently, $\epsilon(G)$ is the smallest postive integer such that $g^{\epsilon(G)} = 1$ for all $g \in G$. For an elliptic curve $E/\mathbb{Q}$, integer n, and prime p at which E has good reduction, to ease notation we will write

$$\epsilon_{n,p}(E) = \epsilon\left(E\left(\frac{\mathbb{Z}}{p^{\mathrm{ord}_p(n)}\mathbb{Z}}\right)\right).$$

Definition. Let $n \in \mathbb{Z}$, and let $E/\mathbb{Q}$ be an elliptic curve. We say that n is an *elliptic Korselt number for E of type II* if n has at least two distinct prime factors, and if for every prime p dividing n the following conditions hold:

- E has good reduction at p;
- (5.1) $\epsilon_{n,p}(E)$ divides $n+1-a_n$.

Proposition 12 (Elliptic Korselt criterion II). *Let $n > 2$ be an odd integer, and let $E/\mathbb{Q}$ be an elliptic curve. Then n is an elliptic Carmichael number for E if and only if n is an elliptic Korselt number for E of type II.*

Proof. The definitions of both elliptic Carmichael and elliptic Korselt numbers include the requirement that E have good reduction at every prime dividing n, so we assume that this is true without further comment.

Suppose first that n is an elliptic Carmichael number. By definition, this means that

$$(5.2) \qquad (n+1-a_n)P \equiv 0 \pmod{n} \quad \text{for all } P \in E(\mathbb{Z}/n\mathbb{Z}).$$

In other words, the quantity $n+1-a_n$ annihilates the group $E(\mathbb{Z}/n\mathbb{Z})$. Hence for any prime power p^i dividing n, the quantity $n+1-a_n$ will also annihilate the group $E(\mathbb{Z}/p^i\mathbb{Z})$. It follows that $n+1-a_n$ is divisible by $\epsilon_{p,n}(E)$, which is the exponent of the group $E(\mathbb{Z}/p^i\mathbb{Z})$ with $i = \operatorname{ord}_p(n)$. This is true for every prime dividing n, and hence n is a type II Korselt number for E.

Conversely, suppose that n is type II Korselt. Factoring n as $n = p_1^{e_1} \cdots p_t^{e_t}$, we have by the Chinese remainder theorem

$$E(\mathbb{Z}/n\mathbb{Z}) = E(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times E(\mathbb{Z}/p_t^{e_t}\mathbb{Z}),$$

from which we see that

$$(5.3) \qquad \epsilon(E(\mathbb{Z}/n\mathbb{Z})) = \operatorname{LCM}[\epsilon_{n,p_1}(E), \ldots, \epsilon_{n,p_t}(E)].$$

Property (5.1) of type II Korselt numbers says that

$$(5.4) \qquad \epsilon_{n,p}(E) \mid n+1-a_n \quad \text{for all } p \mid n,$$

and combining (5.3) and (5.4) yields

$$\epsilon(E(\mathbb{Z}/n\mathbb{Z})) \mid n+1-a_n.$$

It follows that $n+1-a_n$ annihilates $E(\mathbb{Z}/n\mathbb{Z})$, which means that n is an elliptic Carmichael number. ∎

COROLLARY 13. *If n is an odd elliptic Korselt number for $E/\mathbb{Q}$ of type I, then it is also an elliptic Korselt number for $E/\mathbb{Q}$ of type II.*

Proof. Propositions 11 and 12 give the implications

$$\text{Korselt type I} \xrightarrow{\text{Prop. 11}} \text{Carmichael} \xrightarrow{\text{Prop. 12}} \text{Korselt type II.} \ ∎$$

In order to elucidate the definition of elliptic Korselt numbers of type II, we gather some information about the exponents $\epsilon_{n,p}(E)$. We begin with a slightly technical definition.

DEFINITION. Let $p \geq 3$ be a prime, and let $E/\mathbb{Q}$ be an elliptic curve with good reduction at p such that

$$a_p \equiv 1 \pmod{p}.$$

(If $p \geq 7$, this is equivalent to $a_p = 1$, i.e., to p being an anomalous prime for E.) For each power p^i with $i \geq 2$, we say that E is p^i-*canonical* if

$$E(\mathbb{Z}/p^i\mathbb{Z})[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z},$$

and E is p^i-*noncanonical* if

$$E(\mathbb{Z}/p^i\mathbb{Z})[p] \cong \mathbb{Z}/p\mathbb{Z}.$$

REMARK 14. For primes $p \geq 3$, the formal group of $E/\mathbb{Q}_p$ satisfies $\hat{E}(p\mathbb{Z}_p) \cong p\mathbb{Z}_p^+$ (see [21, Theorem IV.6.4]), so there is an exact sequence

$$0 \to p\mathbb{Z}_p^+ \to E(\mathbb{Z}_p) \to E(\mathbb{Z}/p\mathbb{Z}) \to 0.$$

Reducing modulo p^i gives

$$0 \to p\mathbb{Z}/p^i\mathbb{Z} \to E(\mathbb{Z}/p^i\mathbb{Z}) \to E(\mathbb{Z}/p\mathbb{Z}) \to 0. \tag{5.5}$$

Assume now that $i \geq 2$ and $a_p \equiv 1 \pmod{p}$, so in particular

$$\#E(\mathbb{Z}/p\mathbb{Z}) = p + 1 - a_p \equiv 0 \pmod{p}.$$

The Hasse–Weil estimate $|a_p| \leq 2\sqrt{p}$ implies that $p^2 \nmid \#E(\mathbb{Z}/p\mathbb{Z})$, so taking the p-torsion of (5.5) gives

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E(\mathbb{Z}/p^i\mathbb{Z})[p] \to \mathbb{Z}/p\mathbb{Z} \to 0. \tag{5.6}$$

This shows that $E(\mathbb{Z}/p^i\mathbb{Z})[p] \cong (\mathbb{Z}/p\mathbb{Z})^k$ with $k = 1$ or 2, and hence that E is either p^i-canonical or p^i-noncanonical, i.e., there is no third option.

REMARK 15. For an ordinary elliptic curve $\tilde{C}/\mathbb{F}_p$, the *canonical lift*, also sometimes called the *Deuring lift*, is an elliptic curve $C/\mathbb{Q}_p$ whose reduction is $\tilde{C}$ and having the property that $\mathrm{End}(C) \cong \mathrm{End}(\tilde{C})$. Equivalently, the Frobenius map on $\tilde{C}$ lifts to an endomorphism of C. Necessarily, the curve C has CM. We denote the canonical lift by $\mathrm{Lift}(\tilde{C}/\mathbb{F}_p)$. Now let $E/\mathbb{Q}$ be an elliptic curve. A result of Gross [12, p. 514] implies that the sequence (5.6) splits if and only if

$$j(E) \equiv j(\mathrm{Lift}(\tilde{E}/\mathbb{F}_p)) \pmod{p^2},$$

i.e., if and only if $E \bmod p^2$ is isomorphic, modulo p^2, to the canonical lift of $E \bmod p$. Thus, at least for $i = 2$, the curve E is p^2-canonical according to our definition if $E \bmod p^2$ is a canonical lift in the usual sense. For further information about canonical lifts, see for example [12, 20].

The following proposition shows why anomalous primes lead to complications in the analysis of elliptic Carmichael numbers.

PROPOSITION 16. *Let $p \geq 3$ be a prime, and factor*

$$\epsilon_{n,p}(E) = p^f A \quad \textit{with } \gcd(A, p) = 1.$$

(a) *If $a_p \not\equiv 1 \pmod{p}$, then*

$$A \mid p + 1 - a_p \quad \textit{and} \quad f = \mathrm{ord}_p(n) - 1.$$

(b) *If $a_p \equiv 1 \pmod{p}$, then $A = 1$ (or possibly $A = 2$ if $p \leq 5$), and*

$$f = \begin{cases} \mathrm{ord}_p(n) - 1 & \textit{if } E \textit{ is } p^{\mathrm{ord}_p(n)}\textit{-canonical,} \\ \mathrm{ord}_p(n) & \textit{if } E \textit{ is } p^{\mathrm{ord}_p(n)}\textit{-noncanonical.} \end{cases}$$

Proof. To ease notation, let $i = \mathrm{ord}_p(n)$. We use the exact sequence

$$0 \to p\mathbb{Z}/p^i\mathbb{Z} \to E(\mathbb{Z}/p^i\mathbb{Z}) \to E(\mathbb{Z}/p\mathbb{Z}) \to 0 \tag{5.7}$$

as described in Remark 14.

Suppose first that $a_p \not\equiv 1 \pmod{p}$. It follows that

$$\#E(\mathbb{Z}/p\mathbb{Z}) = p + 1 - a_p \not\equiv 0 \pmod{p},$$

so the exponent of $E(\mathbb{Z}/p^i\mathbb{Z})$ has the form $p^{i-1}A$ for some A dividing $p + 1 - a_p$. This completes the proof of (a).

We now suppose that $a_p \equiv 1 \pmod{p}$, so $\#E(\mathbb{Z}/p\mathbb{Z}) = Ap$. The Hasse–Weil estimate gives

$$A = \frac{p + 1 - a_p}{p} \le \frac{p + 1 + 2\sqrt{p}}{p} = \left(1 + \frac{1}{\sqrt{p}}\right)^2.$$

Since $p \ge 3$, we see that $A \le 2$, so $p \nmid A$; and if $p \ge 7$, then A must equal 1. In any case, we have $A \mid p + 1 - a_p$.

Our assumptions imply that $E(\mathbb{Z}/p\mathbb{Z})[p] = \mathbb{Z}/p\mathbb{Z}$, so it follows from the exact sequence (5.7) that the exponent of $E(\mathbb{Z}/p^i\mathbb{Z})$ is given by

$$\epsilon(E(\mathbb{Z}/p^i\mathbb{Z})) = \begin{cases} Ap^i & \text{if the sequence (5.7) does not split,} \\ Ap^{i-1} & \text{if the sequence (5.7) does split.} \end{cases}$$

Further, since (5.7) is (essentially) the extension of a cyclic group of order p^{i-1} by a cyclic group of order p, we see that it splits if and only if $E(\mathbb{Z}/p^i\mathbb{Z})$ has a p-torsion point that does not map to 0 in $E(\mathbb{Z}/p\mathbb{Z})$. In other words,

$$\begin{aligned} \text{the sequence (5.7) splits} \;&\Leftrightarrow\; E(\mathbb{Z}/p^i\mathbb{Z})[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \\ &\Leftrightarrow\; E \text{ is } p^i\text{-canonical.} \end{aligned}$$

This chain of equivalences completes the proof of (b). ∎

6. Elliptic Korselt numbers of the form pq**.** It is an easy consequence of the classical Korselt criterion that a classical Carmichael number must be a product of at least three (distinct odd) primes. This is not true for elliptic Korselt numbers, as seen in the examples in Section 7. However, elliptic Korselt numbers of the form $n = pq$ do satisfy some restrictions, as in the following result.

PROPOSITION 17. *Let $E/\mathbb{Q}$ be an elliptic curve, and let $n = pq$ be a type I elliptic Korselt number for E that is a product of two distinct primes, say with $p < q$. Then one of the following is true:*

(i) $p \le 17$;
(ii) $a_p = a_q = 1$, *i.e., both p and q are anomalous primes for E;*
(iii) $p \ge \sqrt{q}$.

Proof. We assume that $p > 17$ and that at least one of a_p and a_q is not equal to 1, and we will prove that p satisfies the estimate in (iii). We have

$$n + 1 - a_n = pq + 1 - a_p a_q = p(q + 1 - a_q) + pa_q - p - a_p a_q + 1.$$

The Korselt condition $q + 1 - a_q \mid n + 1 - a_n$ then implies that

$$q + 1 - a_q \mid pa_q - p - a_p a_q + 1. \tag{6.1}$$

We consider two cases.

First, suppose that $pa_q - p - a_p a_q + 1 = 0$. A little bit of algebra yields

$$(p - a_p)(a_q - 1) = a_p - 1. \tag{6.2}$$

We have $p \neq a_p$, since $p \geq 5$ by assumption, so (6.2) tells us that $a_p = 1$ if and only if $a_q = 1$. We are also assuming that a_p and a_q are not both equal to 1, so (6.2) tells us that neither is equal to 1. This allows us to solve (6.2) for p,

$$p = a_p + \frac{a_p - 1}{a_q - 1}.$$

But then

$$p \leq |a_p| + \left| \frac{a_p - 1}{a_q - 1} \right| \leq |a_p| + |a_p - 1| \leq 2|a_p| + 1 \leq 4\sqrt{p} + 1.$$

This contradicts $p > 17$, so we conclude that $pa_q - p - a_p a_q + 1 \neq 0$.

It then follows from the Korselt divisibility condition (6.1) that

$$|q + 1 - a_q| \leq |pa_q - p - a_p a_q + 1|.$$

Using the Hasse–Weil estimate for a_p and a_q now gives

$$q + 1 - 2\sqrt{q} \leq p\sqrt{q} + \sqrt{pq} + (p - 1).$$

Treating this as a quadratic inequality for $\sqrt{p}$, we find that

$$\sqrt{p} \geq \frac{\sqrt{4q^{3/2} - 3q + 8} - \sqrt{q}}{\sqrt{q} + 1}. \tag{6.3}$$

Asymptotically this gives $\sqrt{p} \geq 2\sqrt[4]{q}$, and a little bit of calculus shows that the right-hand side of (6.3) is larger than $\sqrt[4]{q}$ for all $q \geq 13$. Squaring, we find that

$$p \geq \sqrt{q} \quad \text{for all } q \geq 13.$$

Since we are assuming that $q > p > 17$, this proves property (iii), which completes the proof of Proposition 17. ∎

7. Numerical examples. In this section we present several numerical examples of elliptic Carmichael and elliptic Korselt numbers. These examples were computed using PARI/GP [22].

EXAMPLE 18. Let E be the elliptic curve

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

It has discriminant $\Delta_E = -3952 = -2^4 \cdot 13 \cdot 19$ and conductor $N = 1976$, and is curve 1976a in Cremona's tables [5], which also tell us that $E(\mathbb{Q})$ has rank 1 and $E(\mathbb{Q})_{\mathrm{tors}} = 0$. The curve E has six type I Korselt (and hence Carmichael) numbers smaller than 1000. They are described in Table 1. In particular, note that the table contains the elliptic Carmichael numbers $245 = 5 \cdot 7^2$ and $875 = 5^3 \cdot 7$ that are not square-free; cf. Remark 9.

Table 1. Type I elliptic Korselt numbers for $E : y^2 = x^3 + x + 3$

n	$n+1-a_n$	p	$p+1-a_p$
$15 = 3 \cdot 5$	$16 = 2^4$	3	$4 = 2^2$
		5	$4 = 2^2$
$77 = 7 \cdot 11$	$90 = 2 \cdot 3^2 \cdot 5$	7	$6 = 2 \cdot 3$
		11	$18 = 2 \cdot 3^2$
$203 = 7 \cdot 29$	$216 = 2^3 \cdot 3^3$	7	$6 = 2 \cdot 3$
		29	$36 = 2^2 \cdot 3^2$
$245 = 5 \cdot 7^2$	$252 = 2^2 \cdot 3^2 \cdot 7$	5	$4 = 2^2$
		7	$6 = 2 \cdot 3$
$725 = 5^2 \cdot 29$	$720 = 2^4 \cdot 3^2 \cdot 5$	5	$4 = 2^2$
		29	$36 = 2^2 \cdot 3^2$
$875 = 5^3 \cdot 7$	$900 = 2^2 \cdot 3^2 \cdot 5^2$	5	$4 = 2^2$
		7	$6 = 2 \cdot 3$

EXAMPLE 19. Let E be the elliptic curve

$$E : y^2 = x^3 + 7x + 3. \tag{7.1}$$

It has discriminant $\Delta_E = -25840 = -2^4 \cdot 5 \cdot 17 \cdot 19$ and conductor $N = 25840$, and is curve 25840w in Cremona's tables [5], which also tell us that $E(\mathbb{Q})$ has rank 1 and $E(\mathbb{Q})_{\mathrm{tors}} = 0$. This curve E has no type I Korselt numbers smaller than 25000. We do not know why this is true, since the curves $y^2 = x^3 + ax + b$ with $(a, b) \in \{(6, 3), (8, 3), (7, 2), (7, 4)\}$ have lots of type I Korselt numbers smaller than 10000. The first few type I Korselt numbers for the curve (7.1) are

$$27563,\ 29711,\ 30233,\ 41683,\ 43511,\ 62413,\ 68783,\ 80519,\ 95207.$$

EXAMPLE 20. Let E be the elliptic curve

$$E : y^2 + xy + 3y = x^3 + 2x^2 + 4x.$$

It has discriminant $\Delta_E = -4006 = -2 \cdot 2003$ and conductor $N = 4006$, and is curve 4006a in Cremona's tables [5], which also tell us that $E(\mathbb{Q})$ has rank 1 and $E(\mathbb{Q})_{\mathrm{tors}} = 0$. There are exactly six numbers $n \le 5000$ that are type I elliptic Korselt numbers for E, as described in Table 2. Extending the search, there are 20 type I elliptic Korselt numbers for E that are smaller than 100000,

$$65, 143, 533, 1991, 4179, 4921, 5251, 5611, 7429, 15839, 22939, 32339, 35165, 35303, 41495, 48719, 56959, 69475, 83839, 98879.$$

Extending the search up to 200000 yields three more examples,

$$105083, 161551, 166493.$$

The non-square-free numbers in this list are

$$69475 = 5^2 \cdot 7 \cdot 397, \quad 83839 = 7^2 \cdot 29 \cdot 59, \quad 161551 = 13 \cdot 17^2 \cdot 43.$$

Table 2. Type I elliptic Korselt numbers for $E : y^2 + xy + 3y = x^3 + 2x^2 + 4x$

n	$n+1-a_n$	p	$p+1-a_p$
$65 = 5 \cdot 13$	$54 = 2 \cdot 3^3$	5	$9 = 3^2$
		13	$18 = 2 \cdot 3^2$
$143 = 11 \cdot 13$	$144 = 2^4 \cdot 3^2$	11	$12 = 2^2 \cdot 3$
		13	$18 = 2 \cdot 3^2$
$533 = 13 \cdot 41$	$486 = 2 \cdot 3^5$	13	$18 = 2 \cdot 3^2$
		41	$54 = 2 \cdot 3^3$
$1991 = 11 \cdot 181$	$1992 = 2^3 \cdot 3 \cdot 83$	11	$12 = 2^2 \cdot 3$
		181	$166 = 2 \cdot 83$
$4179 = 3 \cdot 7 \cdot 199$	$4180 = 2^2 \cdot 5 \cdot 11 \cdot 19$	3	$4 = 2^2$
		7	$10 = 2 \cdot 5$
		199	$190 = 2 \cdot 5 \cdot 19$
$4921 = 7 \cdot 19 \cdot 37$	$4950 = 2 \cdot 3^2 \cdot 5^2 \cdot 11$	7	$10 = 2 \cdot 5$
		19	$22 = 2 \cdot 11$
		37	$45 = 3^2 \cdot 5$

Acknowledgments. I would like to thank Álvaro Lozano-Robledo and Felipe Voloch [17] for the observation in Remark 15. I would also like to thank Dan Gordon, Carl Pomerance, Dinesh Thakur, and the referee for their helpful suggestions. The research described in this note was partly supported by the NSF (grant no. DMS-0854755).

References

[1] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) 139 (1994), 703–722.

[2] R. Balasubramanian and M. R. Murty, *Elliptic pseudoprimes. II*, in: Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math. 91, Birkhäuser Boston, Boston, MA, 1990, 13–25.

[3] R. D. Carmichael, *On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \bmod P$*, Amer. Math. Monthly 19 (1912), no. 2, 22–27.
[4] A. C. Cojocaru, F. Luca, and I. E. Shparlinski, *Pseudoprime reductions of elliptic curves*, Math. Proc. Cambridge Philos. Soc. 146 (2009), 513–522.
[5] J. E. Cremona, *Elliptic curve data*, http://sage.math.washington.edu/cremona.
[6] C. David and J. Wu, *Pseudoprime reductions of elliptic curves*, Canad. J. Math. 64 (2012), 81–101.
[7] A. Ekstrom, *On the infinitude of elliptic Carmichael numbers*, PhD thesis, Univ. of Arizona, 1999; available at the ProQuest LLC website.
[8] A. Ekstrom, C. Pomerance, and D. Thakur, *Infinitude of elliptic Carmichael numbers*, J. Austral. Math. Soc., to appear.
[9] D. M. Gordon, *On the number of elliptic pseudoprimes*, Math. Comp. 52 (1989), 231–245.
[10] D. M. Gordon and C. Pomerance, *The distribution of Lucas and elliptic pseudoprimes*, Math. Comp. 57 (1991), 825–838.
[11] D. M. Gordon and C. Pomerance, Corrigendum to [10], ibid. 60 (1993), 877.
[12] B. H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J. 61 (1990), 445–517.
[13] D. Guillaume and F. Morain, *Building pseudoprimes with a large number of prime factors*, Appl. Algebra Engrg. Comm. Comput. 7 (1996), 263–277.
[14] H. Ito, *An elliptic Fermat test*, Mem. College Ed. Akita Univ. Natur. Sci. 40 (1989), 5–8.
[15] H. Ito, *On elliptic pseudoprimes*, Mem. College Ed. Akita Univ. Natur. Sci. 46 (1994), 1–7.
[16] A. Korselt, *Problème chinois*, L'intermédiare des Mathématiciens 6 (1899), 142–143.
[17] Á. Lozano-Robledo and F. Voloch, Answers to *Structure of $E(\mathbb{Q}_p)$ for elliptic curves with anomalous reduction modulo p*, MathOverflow, 2011, http://mathoverflow.net/questions/70756.
[18] I. Miyamoto and M. R. Murty, *Elliptic pseudoprimes*, Math. Comp. 53 (1989), 415–430.
[19] S. Müller, *On the existence and non-existence of elliptic pseudoprimes*, Math. Comp. 79 (2010), 1171–1190.
[20] T. Satoh, *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, J. Ramanujan Math. Soc. 15 (2000), 247–270.
[21] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, Dordrecht, 2009.
[22] The PARI Group, Bordeaux, PARI/GP, version 2.3.4, 2011; http://pari.math.u-bordeaux.fr/.

Joseph H. Silverman
Mathematics Department
Box 1917
Brown University
Providence, RI 02912, U.S.A.
E-mail: jhs@math.brown.edu

Received on 23.8.2011
and in revised form on 12.9.2011 (6798)