Journal of Number Theory 201 (2019) 108–123

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Anomalous primes and the elliptic Korselt criterion ☆

L. Babinkostova [a,*], J.C. Bahr [b], Y.H. Kim [c], E. Neyman [d], G.K. Taylor [e]

[a] *Department of Mathematics, Boise State University, Boise, ID 83725, USA*
[b] *Department of Mathematics, University of California, Los Angeles, CA 90095, USA*
[c] *Department of Mathematics, Columbia University, New York, NY 10027, USA*
[d] *Department of Mathematics, Princeton University, Princeton, NJ 08544, USA*
[e] *Department of Mathematics, Statistics, and Computer Science, University of Illinois, Chicago, IL 60607, USA*

ARTICLE INFO

Article history:
Received 21 August 2018
Received in revised form 5 February 2019
Accepted 5 February 2019
Available online 19 March 2019
Communicated by S.J. Miller

MSC:
14H52
14K22
11G07
11G20
11B99

Keywords:
Elliptic curves

ABSTRACT

We explore the relationship between elliptic Korselt numbers of Type I, a class of pseudoprimes introduced by Silverman in [10], and anomalous primes. We generalize a result in [10] that gives sufficient conditions for an elliptic Korselt number of Type I to be a product of anomalous primes. Finally, we prove that almost all elliptic Korselt numbers of Type I of the form $n = pq$ are a product of anomalous primes.

☆ Supported by National Science Foundation under the Grant number DMS-1062857.

* Corresponding author.
E-mail addresses: liljanababinkostova@boisestate.edu (L. Babinkostova), jbahr@ucla.edu (J.C. Bahr), yujin.kim@columbia.edu (Y.H. Kim), eneyman@princeton.edu (E. Neyman), gtaylo9@uic.edu (G.K. Taylor).

https://doi.org/10.1016/j.jnt.2019.02.013
0022-314X/

Anomalous primes
Elliptic Korselt numbers

1. Introduction

In 1989, Gordon [5,6] defined elliptic pseudoprimes for CM elliptic curves, the first to do so according to Silverman [10]. For a full discussion of Gordon's approach, see [10, Remark 4] and the works cited there. In this paper, we work with the definition introduced by Silverman [10] which is well-defined for arbitrary elliptic curves.

Namely, for a given elliptic curve $E/\mathbb{Q}$ and point $P \in E(\mathbb{Z}/n\mathbb{Z})$ a natural number n is an *elliptic pseudoprime with respect to* $P \in E$ if n has at least two distinct prime factors, E has good reduction at every prime p dividing n, and $(n+1-a_n)P \equiv 0 \pmod{n}$ where a_n denotes the nth coefficient of the L-series of $E/\mathbb{Q}$. When we write $E(\mathbb{Z}/n\mathbb{Z})$, we follow the convention of [10, Remark 2] by assuming that E has good reduction at all primes p dividing n. In this case, a minimal Weierstrauss equation defines a smooth group scheme $E \to \mathrm{Spec}(\mathbb{Z}/n\mathbb{Z})$ (see [9, Section IV.5] for details of the construction). Then the $\mathbb{Z}/n\mathbb{Z}$-points of this group scheme form an abelian group, which we denote by $E(\mathbb{Z}/n\mathbb{Z})$.

A composite integer n is an *elliptic Carmichael number* for a given elliptic curve $E/\mathbb{Q}$ if n is an elliptic pseudoprime for every point $P \in E(\mathbb{Z}/n\mathbb{Z})$ (note that by our convention, E must have good reduction at the primes dividing n). In analogy with classical case of the Korselt criterion for Carmichael numbers, Silverman [10] gives two Korselt-type criteria for elliptic Carmichael numbers, introducing the notion of an elliptic Korselt number of Type I and of Type II. The elliptic Korselt criterion of Type I is a practical sufficient condition for elliptic Carmichael numbers, given the prime factorization of the number.

For a given elliptic curve $E/\mathbb{Q}$, a prime p is *anomalous* if E has good reduction at p and $\#E(\mathbb{F}_p) = p$. In [10, Proposition 17], Silverman proves that if $n = pq$ is a Type I elliptic Korselt number for E and p is not too small with respect to q, then p and q are anomalous primes for E. Silverman notes that Type I elliptic Korselt numbers of the form pq are interesting since there are no classical Carmichael numbers of this form. In this paper, we further explore the connection between squarefree elliptic Korselt numbers and anomalous primes.

In Section 2, we prove a generalization of [10, Proposition 17]. We show that if $n = p_1 \cdots p_m$ is a squarefree Type I elliptic Korselt number with $p_1 < \cdots < p_m$ and $\frac{\sqrt{p_m}}{4^m} \leq p_1 \cdots p_{m-1} \leq 4^m$, then p_m is anomalous and $a_n = 1$. Hence all but an even number of the primes p_i are anomalous, and if p_i is not anomalous, then $a_{p_i} = -1$. Furthermore, we note an error in the proof of [10, Proposition 17], providing a counterexample and the corrected statement. In particular, we show that if $n = pq$ is an elliptic Korselt number of Type I with $p < q$ for $E/\mathbb{Q}$ and $13 \leq p \leq \sqrt{q}/16$, then p and q are anomalous for E.

In Section 3, we prove that for an elliptic Korselt number of Type I for $E/\mathbb{Q}$ of the form $n = pq$ where $p < q$ are prime, the probability that p and q are anomalous approaches

1 as $p, q \to \infty$. Our result relies on a result proven in the preprint [1, Section 6] which appeared as a conjecture in an early draft of this paper. Computational evidence for our original conjecture is collected in an appendix.

Finally, we combine our results with a result from [8] to show that (assuming the Hardy-Littlewood Conjecture) there are infinitely many Type I elliptic Korselt numbers for any curve $E : y^2 = x^3 + D$, where $D \in \mathbb{Z}$ is neither a square nor a cube in $\mathbb{Q}(\sqrt{-3})$ and $D \neq 80d^6$ for any $d \in \mathbb{Z}[(1+\sqrt{-3})/2]$.

2. Squarefree elliptic Korselt numbers of Type I

The classical notions of pseudoprimes and Carmichael numbers are related to the orders of numbers in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$. These concepts can be generalized to other algebraic groups, such as elliptic curves. The notions of elliptic pseudoprimes and elliptic Carmichael numbers were introduced in [6] for curves with complex multiplication.

In [10] these notions were extended to arbitrary elliptic curves $E/\mathbb{Q}$. The definition of an elliptic pseudoprime for an arbitrary elliptic curve is as follows: let n be a positive integer greater than 1, 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 $L(E/\mathbb{Q}, s) = \sum a_n/n^s$. Then n is an *elliptic pseudoprime* for (E, P) if n has at least two distinct prime factors, E has good reduction at every prime dividing n, and P is $(n+1-a_n)$-torsion in $E(\mathbb{Z}/n\mathbb{Z})$. Following the analogy with classical pseudoprimes, if $n = p$ is a prime of good reduction, the last condition holds trivially. Indeed, $E(\mathbb{Z}/p\mathbb{Z})$ is an elliptic curve over $\mathbb{F}_p$ of order $p + 1 - a_p$, so every point is $(p + 1 - a_p)$-torsion.

The definition of an elliptic Carmichael number for an arbitrary elliptic curve is as follows: let n be a positive integer greater than 1 and let $E/\mathbb{Q}$ be an elliptic curve. Then n is an *elliptic Carmichael number* for E if n is an elliptic pseudoprime for (E, P) for every point $P \in E(\mathbb{Z}/n\mathbb{Z})$. In this section, we only consider integers n that are coprime with 2 and 3. In classical number theory, Korselt's criterion—which is satisfied by a composite number n if $(p-1) \mid (n-1)$ for every prime p dividing n—can be used to test for Carmichael numbers. In [10], Silverman introduces an analogous criterion for elliptic curves.

Definition 2.1. Fix an elliptic curve $E/\mathbb{Q}$. A positive integer n is called an *elliptic Korselt number of Type I* for E if it has at least two distinct prime factors, such that for every prime p dividing n, the following hold:

(1) E has good reduction at p
(2) $p + 1 - a_p \mid n + 1 - a_n$
(3) $\operatorname{ord}_p(a_n - 1) \geq \operatorname{ord}_p(n) - \begin{cases} 1 & a_p \not\equiv 1 \pmod{p} \\ 0 & a_p \equiv 1 \pmod{p} \end{cases}$.

Here, a_p is the Frobenius trace of $E(\mathbb{F}_p)$ as usual, and a_n is the n^{th} coefficient of the L-series of $E/\mathbb{Q}$; for how to compute this coefficient, see [12]. In particular, a_n is a multiplicative function when n is square-free, in the sense that if $n = \prod_i p_i$ for distinct p_i, then $a_n = \prod_i a_{p_i}$. Finally, $\mathrm{ord}_p(n)$ denotes the highest power of p that appears in the prime factorization of n, with $\mathrm{ord}_p(0) = \infty$. In [10] it has been shown that any number satisfying this elliptic Korselt criterion is an elliptic Carmichael number, but the converse need not be true.

Proposition 2.2. *If n is an elliptic Korselt number of Type I for an elliptic curve E, then n is an elliptic Carmichael number for E.*

Proof. See [10, Proposition 11]. □

Recall that an anomalous prime for an elliptic curve $E/\mathbb{Q}$ is a prime such that E has good reduction at p and $\#E(\mathbb{F}_p) = p$ (or equivalently, $a_p = 1$).

Proposition 2.3. *Let E be an elliptic curve and let $p_1, p_2, \ldots, p_m$ be distinct anomalous primes for E. Then $n = \prod_{i=1}^{m} p_i$ is an elliptic Korselt number of Type I for E.*

Proof. The first condition of Definition 2.1 is satisfied since elliptic curves have good reduction at anomalous primes. The second condition is satisfied since $a_n = \prod_{i=1}^{m} a_{p_i} = 1$, and each p_i divides n. The third condition is satisfied because for each i, $\mathrm{ord}_{p_i}(a_n - 1) = \mathrm{ord}_{p_i}(0) = \infty$. □

The converse of Proposition 2.3 is not true: not all elliptic Korselt numbers of Type I for an elliptic curve E are products of distinct primes which are anomalous for E. However, for a product of two distinct primes $n = pq$ there are conditions on p and q under which both p and q must be anomalous. A result of this form was obtained in [10, Proposition 17]. This proposition states if $n = pq$ is Type I elliptic Korselt for E with $17 < p < \sqrt{q}$, then $a_p = a_q = 1$ i.e. p and q are anomalous for E. However, there is a mistake in the proof, resulting in incorrect bounds. A counterexample is included below.

Counterexample 2.4. *Let $E : y^2 = x^3 + 1$, $p = 53$ and $q = 2971$. We have $a_p = 0$ and $a_q = 56$, and pq an elliptic Korselt number of Type I for E. However, $17 < p < \sqrt{q}$ is satisfied.*

The remainder of this section is devoted to proving a generalization of [10, Proposition 17] to squarefree Type I elliptic Korselt numbers. In particular, we include conditions on distinct primes p, q so that if pq is Type I elliptic Korselt for a curve E, then p and q are anomalous for E.

Theorem 2.5. *Let $E/\mathbb{Q}$ be an elliptic curve and let $n = p_1 p_2 \dots p_m$ be an elliptic Korselt number of Type I for E such that $5 \leq p_1 < p_2 < \cdots < p_m$, where $m \geq 2$. Then one of the following conditions is satisfied:*

(1) $p_1 \cdot \cdots \cdot p_{m-1} \leq 4^m$
(2) $a_{p_m} = 1$, *and for* $1 \leq i \leq m-1$, $a_{p_i} = -1$ *for an even number of values of* i *and the remaining traces are equal to* 1
(3) $p_1 \cdot \cdots \cdot p_{m-1} \geq \frac{\sqrt{p_m}}{4^m}$.

Proof. Assume $p_1 \cdots p_{m-1} = \frac{n}{p_m} > 4^m$. We show that one of the two remaining conditions of the theorem are satisfied. We have

$$n + 1 - a_n = \frac{n}{p_m}(p_m + 1 - a_{p_m}) - \frac{n}{p_m} + a_{p_m}\frac{n}{p_m} + 1 - a_n. \tag{1}$$

The divisibility criterion of Type I elliptic Korselt numbers with (1) implies

$$(p_m + 1 - a_{p_m}) \mid \left(-\frac{n}{p_m} + a_{p_m}\frac{n}{p_m} + 1 - a_n\right).$$

We now consider two cases: $-\frac{n}{p_m} + a_{p_m}\frac{n}{p_m} + 1 - a_n = 0$ and $-\frac{n}{p_m} + a_{p_m}\frac{n}{p_m} + 1 - a_n \neq 0$.

Case 1 $-\frac{n}{p_m} + a_{p_m}\frac{n}{p_m} + 1 - a_n = 0$.

In this case, we have

$$\frac{n}{p_m}(a_{p_m} - 1) = a_n - 1. \tag{2}$$

Suppose for sake of contradiction that $a_{p_m} \neq 1$. We will show that this leads to $\frac{n}{p_m} \leq 4^m$. We have

$$\frac{n}{p_m} = \frac{a_n - 1}{a_{p_m} - 1} = \frac{(a_{p_1} \cdots a_{p_{m-1}})a_{p_m} - 1}{a_{p_m} - 1}.$$

For simplicity of notation, let r denote $a_{p_1} \cdots a_{p_{m-1}}$. Since $a_{p_m} \neq 1$ is an integer, the possible values of $\frac{n}{p_m}$ in terms of r are

$$\dots, \frac{2r+1}{3}, \frac{r+1}{2}, 1, 2r-1, \frac{3r-1}{2}, \frac{4r-1}{3}, \dots,$$

where $a_{p_m} \in \mathbb{Z} - \{1\}$, respectively. If $r < 0$ then the maximum of these values is 1, so the desired inequality is clear. Assume instead that r is positive. Then $\frac{n}{p_m}$ is maximized when $a_{p_m} = 2$, in which case $\frac{n}{p_m} = 2r - 1$. Now by Hasse's theorem, $r \leq 2^{m-1}\sqrt{\frac{n}{p_m}}$, and so

$$\frac{n}{p_m} \leq 2 \cdot 2^{m-1}\sqrt{\frac{n}{p_m}} - 1 < 2^m\sqrt{\frac{n}{p_m}},$$

so $\frac{n}{p_m} \leq 4^m$, as desired. However, by assumption, $\frac{n}{p_m} > 4^m$. Thus, we have a contradiction: if $a_{p_m} - p_1 \cdots p_{m-1} - a_{p_1} \cdots a_{p_m} + 1 = 0$, then a_{p_m} must be 1. We can say more: if $a_{p_m} = 1$, then by (2), $a_{p_1} \cdots a_{p_{m-1}} = 1$. Thus, an even number of traces a_{p_i} for $1 \leq i \leq m-1$ must be equal to -1, while the rest of these traces must be equal to 1.

Case 2 $-\frac{n}{p_m} + a_{p_m}\frac{n}{p_m} + 1 - a_n \neq 0$.

Since $p_m + 1 - a_{p_m} \mid -\frac{n}{p_m} + a_{p_m}\frac{n}{p_m} + 1 - a_n$, we have

$$p_m + 1 - 2\sqrt{p_m} \leq |p_m + 1 - a_{p_m}| \leq 2\frac{n}{p_m}\sqrt{p_m} + \frac{n}{p_m} + 2^m\sqrt{p_m}\sqrt{\frac{n}{p_m}} - 1. \tag{3}$$

Subtracting the left-most quantity from the right-most in (3) gives:

$$(2\sqrt{p_m} + 1)\frac{n}{p_m} + 2^m\sqrt{p_m}\sqrt{\frac{n}{p_m}} - p_m - 2 + 2\sqrt{p_m} \geq 0.$$

Solving the quadratic equation for $\sqrt{\frac{n}{p_m}}$ yields:

$$\sqrt{\frac{n}{p_m}} \geq \frac{-2^m\sqrt{p_m} + \sqrt{4^m p_m - 4(2\sqrt{p_m}+1)(-p_m - 2 + 2\sqrt{p_m})}}{2(2\sqrt{p_m}+1)}. \tag{4}$$

Using the following claim, we will show the right-hand side of (4) is at least $\frac{1}{2^m}p_m^{1/4}$.

Claim.

$$\left(8 - \frac{16}{4^m}\right)p_m^{3/2} - 8p_m^{5/4} - \left(12 + \frac{16}{4^m}\right)p_m - 4p_m^{3/4} + \left(8 - \frac{4}{4^m}\right)p_m^{1/2} + 8 \geq 0. \tag{5}$$

For $m = 2$ it can be verified with a computer algebra system (e.g. [11]) that (5) is true when $p_2 \geq 19$. By assumption, $p_1 > 16$, so this is always the case. Specifically, note that for fixed m, the left-hand side of (5) is a polynomial in $\sqrt{4}p_m$. One may find the roots numerically and determine the asymptotic behavior. For $m = 3$ it can be verified with a computer algebra system that (5) is true when $p_3 \geq 13$ (using the same process described above). Note that $p_3 > 11$ because otherwise we have $p_1 p_2 \leq 5 \cdot 7 = 35$, contradicting our assumption. Thus, the claim holds for $m = 3$.

Now, let $f(m, p_m)$ be the left-hand side of (5). Observe that if $p_m > 0$ is held constant and m is increased, then $f(m, p_m)$ increases. This is because we may write

$$f(m, p_m) = g(p_m) - \frac{16}{4^m}p_m^{3/2} - \frac{16}{4^m}p_m - \frac{4}{4^m}p_m^{1/2},$$

where

$$g(p_m) = 8p_m^{3/2} - 8p_m^{5/4} - 12p_m - 4p_m^{3/4} + 8p^{1/2} + 8,$$

and as m increases, $-\frac{16}{4^m}$ and $-\frac{4}{4^m}$ increase. Thus, since $f(3, p_m) \geq 0$ for $p_m \geq 13$, $f(m, p_m) \geq 0$ for $p_m \geq 13$ for all $m > 3$. Since 13 is the fourth prime greater than or equal to 5, $p_m \geq 13$ for all $m > 3$. This completes the proof of the claim.

Thus, we have

$$\left(8 - \frac{16}{4^m}\right) p_m^{3/2} - 8p_m^{5/4} - \left(12 + \frac{16}{4^m}\right) p_m - 4p_m^{3/4} + \left(8 - \frac{4}{4^m}\right) p_m^{1/2} + 8 \geq 0,$$

which implies

$$4^m p_m + 8p_m\sqrt{p_m} - 12p_m + 8\sqrt{p_m} + 8 \geq \left(\frac{2}{2^m}(2\sqrt{p_m} + 1)p_m^{1/4} + 2^m\sqrt{p_m}\right)^2.$$

The right-hand side above is positive and smaller than the left-hand side, so the left-hand side is also positive. Taking square roots and rearranging yields

$$\frac{-2^m\sqrt{p_m} + \sqrt{4^m p_m - 4(2\sqrt{p_m} + 1)(-p_m - 2 + 2\sqrt{p_m})}}{2(2\sqrt{p_m} + 1)} \geq \frac{1}{2^m} p_m^{1/4}.$$

Thus, $\frac{n}{p_m} = p_1 \cdots p_{m-1} \geq \frac{\sqrt{p_m}}{4^m}$, concluding the proof of Theorem 2.5. □

Note that for $m \geq 4$ the inequality $p_1 \cdots p_{m-1} \leq 4^m$, i.e. the first condition of Theorem 2.5, is never satisfied.

Remark 2.6. Theorem 2.5 can be restated as follows. Let E be an elliptic curve and let $n = p_1 p_2 \cdots p_m$ be an elliptic Korselt number of Type I for E such that $5 \leq p_1 < p_2 < \cdots < p_m$, for $m \geq 2$. If $4^m < p_1 \cdots p_{m-1} < \frac{\sqrt{p_m}}{4^m}$, then $a_{p_m} = 1$ and for $1 \leq i \leq m-1$, $a_{p_i} = -1$ for an even number of values of i and $a_{p_i} = 1$ for the remaining values.

The following corollary of Theorem 2.5 corrects the claim of Proposition 17 in [10].

Corollary 2.7. *Let E be an elliptic curve and let $n = pq$ be an elliptic Korselt number of Type I for E such that $p < q$. Then one of the following conditions holds:*

- $p \leq 13$
- *p and q are anomalous for E.*
- $p \geq \frac{\sqrt{q}}{16}$

3. Elliptic Korselt numbers of Type I of the form *pq*

In Proposition 2.3, we showed that any product of distinct anomalous primes of an elliptic curve is an elliptic Korselt number of Type I. Corollary 2.7 gives sufficient conditions for when an elliptic Korselt number of Type I of the form $n = pq$ is a product of anomalous primes. In this section, we show that the probability that an elliptic Korselt number of Type I of the form $n = pq$ is a product of anomalous primes goes to 1 as $n \to \infty$.

Part of our proof relies on the following proposition which is proven in the preprint [1, Corollary 6.18]. This particular statement appeared as a conjecture in an early draft of this paper which included numerical evidence to support the conjecture. We have relegated that numerical evidence to an appendix.

Proposition 3.1. *[1] For $N \geq 7$, let $5 \leq p, q \leq N$ be distinct primes chosen uniformly, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be an elliptic curve chosen uniformly from the set of elliptic curves defined over $\mathbb{Z}/n\mathbb{Z}$ with good reduction over $\mathbb{F}_p$ and $\mathbb{F}_q$ such that $\#E(\mathbb{F}_p)$ and $\#E(\mathbb{F}_q)$ divide $n + 1 - a_n$. Then*

$$\lim_{N\to\infty} \Pr[\#E(\mathbb{Z}/n\mathbb{Z}) = n + 1 - a_n] = 1.$$

Note that $\#E(\mathbb{Z}/n\mathbb{Z}) = (p + 1 - a_p)(q + 1 - a_q)$ and $n + 1 - a_n = pq + 1 - a_p a_q$. We have the following heuristic justification for the conjecture. Note that by Hasse's bound, $p + 1 - a_p$ and $q + 1 - a_q$ are close in value to p and q, respectively, and $pq + 1 - a_p a_q$ is close in value to pq. Thus, if $p + 1 - a_p$ and $q + 1 - a_q$ divide $n + 1 - a_n$ and their product is not equal to $n + 1 - a_n$, then $p + 1 - a_p$ and $q + 1 - a_q$ must share many factors; this should happen rarely.

From the conditions listed in Proposition 3.1, it is clear that n satisfies the first two conditions of the elliptic Korselt of Type I criterion for E. In other words, n is "nearly;; elliptic Korselt number of Type I. The lemma below states that when $p, q \geq 7$, the third elliptic Korselt condition is a redundancy given the first and second. We will need this and the following results to prove the Theorem 3.7 of this section.

Lemma 3.2. *For $N \geq 7$, let $5 \leq p, q \leq N$ be uniformly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be an elliptic curve chosen uniformly among those for which n is an elliptic Korselt number of Type I. Then*

$$\lim_{N\to\infty} \Pr[p \textit{ is anomalous for } E \textit{ and } q \textit{ is not}] = 0.$$

In this statement, we do not fix a particular curve E. Instead, for a given N, we pick random values of p and q and then pick a random E with the stated property. Lemma 3.2 states that as N approaches infinity, the probability that for these random p, q, E, p is anomalous for E and q is not approaches zero.

Proof. Let N, p, q, and E be as in the statement. Assume that $a_p = 1$ and $a_q \neq 1$. By the Korselt divisibility condition, we have that p and $q+1-a_q$ divide $pq+1-a_q$. Since $p \mid pq+1-a_q$, we have $p \mid 1-a_q$. Since $1-a_q \neq 0$,

$$p \leq |1-a_q| \leq |a_q|+1 \leq 2\sqrt{q}+1 \leq 2\sqrt{N}+1.$$

The probability that a randomly chosen prime below N is at most $2\sqrt{N}+1$ goes to zero as $N \to \infty$. Since $p \leq 2\sqrt{N}+1$ is a necessary condition for $a_p = 1$ and $a_q \neq 1$ for E, it follows that the desired probability approaches zero. □

Although the proposition below holds for any squarefree integer, we will only use the case $n = pq$.

Proposition 3.3. *If $n = p_1 \cdots p_k$ is squarefree with $p_i \geq 7$ for all i and E is an elliptic curve with good reduction over each $\mathbb{F}_{p_i}$, then n is an elliptic Korselt number of Type I for E if and only if $p_i + 1 - a_{p_i}$ divides $n+1-a_n$ for all i.*

Proof. The "only if" direction holds by definition. Suppose that E has good reduction at each p_i and that each $p_i + 1 - a_{p_i}$ divides $n+1-a_n$. Since n is squarefree, $a_{p_i} \not\equiv 1 \pmod{p_i}$ trivially implies the third condition of the elliptic Korselt criterion is satisfied for p_i.

If $a_{p_i} \equiv 1 \pmod{p_i}$ for some p_i, then $a_p = 1$ since $|a_{p_i}| \leq 2\sqrt{p_i}$ and $p_i \geq 7$. By assumption, p_i divides $n+1-a_n$, and so $p_i \mid 1-a_n$. Thus,

$$\operatorname{ord}_{p_i}(a_n - 1) \geq 1 = \operatorname{ord}_{p_i}(n),$$

so p_i satisfies the third condition of the elliptic Korselt criterion. □

Lemma 3.4. *For $N \geq 7$, let $5 \leq p, q \leq N$ be uniformly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be an elliptic curve chosen uniformly among those for which n is an elliptic Korselt number of Type I. Then*

$$\lim_{N\to\infty} \Pr[p \text{ and } q \text{ are not anomalous for } E \text{ and } (p+1-a_p)(q+1-a_q) \neq n+1-a_n] = 0.$$

Proof. Let N, p, q, and E be as in the lemma statement. By Proposition 3.3, this is equivalent to the statement that p, q and E are selected in such a way that $E(\mathbb{Z}/nZ)$ has good reduction over $\mathbb{F}_p$ and $\mathbb{F}_q$, and $\#E(\mathbb{F}_p)$ and $\#E(\mathbb{F}_q)$ divide $n+1-a_n$.[1] By Proposition 3.1, the probability that

[1] If $p = 5$ or $q = 5$, this does not follow from Proposition 3.3, but the probability of this happening approaches zero as $N \to \infty$, so we can ignore this case.

$$\#E(\mathbb{Z}/nZ) = \#E(\mathbb{F}_p)\#E(\mathbb{F}_q) = (p+1-a_p)(q+1-a_q) \neq n+1-a_n$$

approaches zero as $N \to \infty$. Thus, the probability that this condition is satisfied *and* p and q are not anomalous for E also approaches zero, as desired. □

Proposition 3.5. *Let n be a positive integer and let S be a finite multiset of factors of n. For each $d \mid n$, let $m_d(S)$ be the number of multiples of d in S. Then*

$$\sum_{k \in S} k = \sum_{d|n} m_d(S)\phi(d).$$

Proof. This is an induction on the number of elements of S. The theorem is clear for $|S| = 0$; suppose it holds for $|S| = r$. Now let S have $r+1$ elements and choose $k \in S$. Let S' be S with one fewer copy of k; the theorem holds for S'. Adding k to S' increments the left-hand sum by k and the right-hand sum by $\sum_{d|k} \phi(d)$, since $m_d(S) = m_d(S') + 1$ for $d \mid k$ and $m_d(S) = m_d(S')$ for all other d. But $\sum_{d|k} \phi(d) = k$ [7, Proposition 2.2.4], so the statement holds for S. □

Lemma 3.6. *For $N \geq 7$, let $5 \leq p, q \leq N$ be distinct primes chosen uniformly, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be an elliptic curve chosen uniformly among those for which n is an elliptic Korselt number of Type I. Then*

$$\lim_{N \to \infty} \Pr[p \text{ and } q \text{ are not anomalous for } E \text{ and } (p+1-a_p)(q+1-a_q) = n+1-a_n] = 0.$$

Proof. Let N, p, q, and E be as in the lemma statement. We impose the additional restriction that $q \geq 67$; this assumption is harmless as the probability of a randomly selected prime below N being less than 67 approaches 0 as N approaches ∞. Assume that $a_p \neq 1$, $a_q \neq 1$, and $(p+1-a_p)(q+1-a_q) = n+1-a_n$. Hence

$$a_p = \frac{p+q-(p+1)a_q}{q+1-2a_q}.$$

Thus, $q+1-2a_q$ divides $p+q-(p+1)a_q$. Subtracting $q+1-2a_q$ from the dividend, we have

$$q+1-2a_q \mid p - pa_q + a_q - 1 = (p-1)(1-a_q).$$

Letting $x = a_q - 1$, $p' = p-1$, and $q' = q-1$, we find that $q' - 2x$ divides $p'x$. It follows that

$$\frac{q'-2x}{\gcd(q'-2x, x)} = \frac{q'-2x}{\gcd(q', x)} \mid p'. \tag{6}$$

We claim that the probability for randomly chosen $5 \leq p, q \leq N$ that there exists $x \in [-2\sqrt{q}-1, 2\sqrt{q}-1]$ such that (6) holds is satisfied approaches zero as $N \to \infty$; this is sufficient to prove our lemma.

To prove this claim, fix q (and thus q') and examine how many values of $p' < N$ (and thus $p \leq N$) satisfy the condition in (6) for some x in the interval.

For a fixed x, the number of values of p' divisible by $\frac{q'-2x}{\gcd(q',x)}$ is bounded above by

$$\frac{N}{\frac{q'-2x}{\gcd(q',x)}} = \frac{N\gcd(q',x)}{q'-2x} \leq \frac{2N\gcd(q',x)}{q'}.$$

(The last step is justified by the fact that $q \geq 67$.) Thus, the total number of values of p' that are divisible by $\frac{q'-2x}{\gcd(q',x)}$ for some $x \in [-2\sqrt{q}-1, 2\sqrt{q}-1]$ is at most

$$\sum_{\substack{x \in [-2\sqrt{q}-1, 2\sqrt{q}-1] \\ x \neq 0}} \frac{2N\gcd(q',x)}{q'} \leq 2 \sum_{x=1}^{\lfloor 2\sqrt{q}+1 \rfloor} \frac{2N\gcd(q',x)}{q'} = \frac{4N}{q'} \sum_{x=1}^{\lfloor 2\sqrt{q}+1 \rfloor} \gcd(q',x). \quad (7)$$

Now, let $g(k) = \sum_{x=1}^{k} \gcd(x,k)$. We claim that

$$\sum_{x=1}^{\lfloor 2\sqrt{q}+1 \rfloor} \gcd(q',x) \leq g(q') \cdot \frac{2\sqrt{q}+1}{q'}.$$

For n implicit, define the multiset $S_{a,k} = \{\gcd(x,n) \mid x \in \{a, a+1, \ldots, a+k-1\}\}$. Observe that for all $d \mid n$, holding k constant, $m_d(S_{a,k})$ is minimal for $a = 1$. It follows from Proposition 3.5 that

$$\sum_{x=a}^{a+k-1} \gcd(x,n) \quad (8)$$

is minimized for $a = 1$. In particular, let $h(a)$ be (8) with $n = q'$ and $k = \lfloor 2\sqrt{q}+1 \rfloor$. Note that

$$h(1) + h(2) + \cdots + h(q') = g(q') \cdot \lfloor 2\sqrt{q}+1 \rfloor, \quad (9)$$

since the fact that $\gcd(q', q'+x) = \gcd(q', x)$ means that for every $x \in \{1, 2, \ldots, q'\}$, x appears $\lfloor 2\sqrt{q}+1 \rfloor$ times in (9). Since $h(1)$ is the smallest value among the q' values in (9), we obtain

$$\sum_{x=1}^{\lfloor 2\sqrt{q}+1 \rfloor} \gcd(q',x) \leq g(q') \cdot \frac{2\sqrt{q}+1}{q'}, \quad (10)$$

as desired. Combining (7) and (10), we obtain

$$\sum_{\substack{x\in[-2\sqrt{q}-1,2\sqrt{q}-1]\\ x\neq 0}} \frac{2N\gcd(q',x)}{q'} \leq \frac{4N}{q'}\sum_{x=1}^{\lfloor 2\sqrt{q}+1\rfloor}\gcd(q',x) \leq \frac{4N}{q'}g(q')\cdot\frac{2\sqrt{q}+1}{q'}.$$

Now, the number of primes $p \leq N$ is on the order of $\frac{N}{\log N}$. Thus, the probability that p is chosen so that (6) holds for some x is

$$O\left(\frac{4\log N}{q'}g(q')\cdot\frac{2\sqrt{q}+1}{q'}\right) = O\left(\log N\cdot g(q')q^{\frac{-3}{2}}\right). \tag{11}$$

It is known that $g(k) = O(k^{1+\epsilon})$ for every positive ϵ [2, Theorem 3.2]. Combining this with the bound (11), we see that the probability of (6) holding is $O\left(\log N\cdot q^{\frac{-1}{2}+\epsilon}\right)$ for every positive ϵ, as a function of q and N.

Now we express the probability that (6) holds as a function of just N, randomly choosing q to be a prime below N. The probability that $q \leq N^{\frac{1}{2}}$ is on the order of

$$\frac{N^{1/2}/\log N^{1/2}}{N/\log N} = \frac{2N^{\frac{1}{2}}}{N},$$

which is on the order of $N^{\frac{-1}{2}}$. If $q > N^{\frac{1}{2}}$, then the probability that (6) holds is $O\left(\log N\cdot N^{\frac{-1}{4}+\epsilon}\right)$ for all ϵ. Thus, the total probability is at most on the order of $N^{\frac{-1}{2}} + \log N\cdot N^{\frac{-1}{4}+\epsilon}$, which approaches zero as $N\to\infty$, and so we are done. □

Theorem 3.7. *For $N \geq 7$, let $5 \leq p, q \leq N$ be uniformly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be an elliptic curve chosen uniformly among those for which n is an elliptic Korselt number of Type I. We have*

$$\lim_{N\to\infty}\Pr[p \text{ and } q \text{ are anomalous primes for } E] = 1.$$

Proof. A result of Deuring [4] states that for all primes p, for every integer $-2\sqrt{p} \leq t \leq 2\sqrt{p}$, there is an elliptic curve over $\mathbb{F}_p$ with order $p+1-t$. In particular, for every p there is an elliptic curve that is anomalous over $\mathbb{F}_p$. Thus, for any two primes p and q, we may use the Chinese Remainder Theorem to construct a curve over $\mathbb{Q}$ that is anomalous both when reduced over $\mathbb{F}_p$ and over $\mathbb{F}_q$. It follows by Proposition 2.3 that for all (p,q) there is a curve E that makes p and q anomalous and therefore makes $n = pq$ elliptic Korselt number of Type I.

Suppose now that $n = pq$ is an elliptic Korselt number of Type I for some elliptic curve E. Then the cases in which p and q are not both anomalous primes for E are as follows:

(1) Exactly one of p and q is anomalous for E.
(2) Neither p nor q is anomalous for E, and $(p+1-a_p)(q+1-a_q) \neq n+1-a_n$.
(3) Neither p nor q is anomalous for E, and $(p+1-a_p)(q+1-a_q) = n+1-a_n$.

Lemmas 3.2, 3.4, and 3.6 show that the probability that p, q, and E satisfy cases (1), (2), (3), respectively, goes to zero as $N \to \infty$. Therefore, as $N \to \infty$, the probability that p and q are both anomalous for E approaches 1. This completes the proof. □

A natural follow-up question to ask is whether Theorem 3.7 holds not just for products of two primes, but in general. In other words, we may ask whether the following conjecture holds.

Conjecture 3.8. *Let $N \geq 35$ and let n be a random positive integer less than or equal to N with the property that n is a product of distinct primes $p_1, \ldots, p_k$ (with $k \geq 2$) that are all greater than 3. Let $E(\mathbb{Z}/n\mathbb{Z})$ be an elliptic curve chosen uniformly among those for which n is an elliptic Korselt number of Type I. Then*

$$\lim_{N\to\infty} \Pr[p_1, \ldots, p_k \text{ are anomalous primes for } E] = 1.$$

We have experimental evidence in favor of this conjecture; see the appendix for details.

4. Conclusions

Fix an elliptic curve E. Then Proposition 2.3 and Proposition 11 from [10] give the following implications.

$$\text{product of anomalous primes} \xrightarrow{\text{Prop. 2.3}} \text{elliptic Korselt Type I} \xrightarrow{\text{Prop. 11}} \text{elliptic Carmichael}$$

These implications, together with Theorem 1.2 from [8], imply the following result.

Corollary 4.1. *Assuming the Hardy-Littlewood Conjecture, there are infinitely many elliptic Korselt numbers of Type I for the curve $E : y^2 = x^3 + D$, where $D \in \mathbb{Z}$ is neither a square nor a cube in $\mathbb{Q}(\sqrt{-3})$ and $D \neq 80d^6$ for any $d \in \mathbb{Z}[(1+\sqrt{-3})/2]$.*

In section 2, we explore the strictness of the left-most inclusion in the above diagram. Theorem 2.5 establishes deterministic conditions under which an elliptic Korselt number of Type I can be a product of anomalous primes. Furthermore, for $n = pq$ a product of two distinct primes, Theorem 3.7 states that nearly all the elliptic curves that make n an elliptic Korselt number of Type I also have n a product of anomalous primes. If Conjecture 3.8 holds, then in fact anomalous primes form the building blocks of nearly all squarefree elliptic Korselt numbers of Type I — not just those that are products of two primes. Because the Lang-Trotter conjecture has been proven "on average" in [3], we can say more.

Corollary 4.2 *([3]). Let $E(a,b)$ denote the elliptic curve $y^2 = x^3+ax+b$, and let $\pi^1_{E(a,b)}(x)$ denote the number of anomalous primes of $E(a,b)$ less than or equal to x. Take $A, B > x^{2+\varepsilon}$ for some $\varepsilon > 0$ and fix $c > 0$. Then for all $d > 2c$, and for all elliptic curves $E(a,b)$*

with $|a| \leq A$ and $|b| \leq B$, there exists a constant $C > 0$ such that the following inequality holds with $\mathcal{O}\left(\frac{1}{\log^d x} AB\right)$ many exceptions:

$$\pi^1_{E(a,b)}(x) \geq C_r \pi_{1/2}(x) - C\frac{\sqrt{x}}{\log^c x}, \tag{12}$$

where we define

$$\pi_{1/2}(x) := \int_2^x \frac{dt}{2\sqrt{t}\log t} \sim \frac{\sqrt{x}}{\log x}, \text{ and}$$

$$C_1 := \frac{2}{\pi} \prod_l \frac{l(l^2-l-1)}{(l-1)(l^2-1)}.$$

Since $C_1 > 0$, the right-hand side of (12) goes to infinity as $x \to \infty$. In particular, Corollary 4.2 gives the following.

Corollary 4.3. *All but a density zero set of elliptic curves have infinitely many anomalous primes, and thus also have infinitely many elliptic Korselt numbers of Type I.*

Acknowledgments

The authors would like to thank Lawrence Washington and Steven J. Miller for many helpful discussions and suggestions. In addition, we would like to thank the referee for a careful reading and for pointing out the existing literature on the Lang-Trotter conjecture.

Appendix A. Numerical evidence for Conjecture 3.8

We wrote a program that takes as input an integer N, randomly chooses a positive integer n between N and $2N$ with the property that $n = p_1 \dots p_k$ for $k \geq 2$ distinct primes that are greater than 3. For each p_i, we select a_{p_i} from a semicircular distribution of radius $2\sqrt{p_i}$ (since this is how traces are distributed).[2] If the resulting traces describe a curve E with the property that n is an elliptic Korselt number of Type I for E, we check whether every a_{p_i} is 1. We do this until we have a sample size of 1000 (i.e. have found a thousand random values of n and curves E such that n is an elliptic Korselt number of Type I for E). Below is our experimental data for $\Pr(N)$, which is the fraction of these 1000 curves whose values of a_{p_i} were all 1 (Fig. 1).

[2] This is in effect the same as picking an elliptic curve with random coefficients, since n is square-free and by the Chinese remainder theorem picking random coefficients and reducing modulo each prime is the same as picking random coefficients modulo each prime (and so the traces of an elliptic curve modulo different primes are independent random variables).

N	$\Pr(N)$
2^6	0.194
2^7	0.280
2^8	0.317
2^9	0.300
2^{10}	0.356
2^{11}	0.404
2^{12}	0.436
2^{13}	0.455
2^{14}	0.467
2^{15}	0.547
2^{16}	0.572
2^{17}	0.586
2^{18}	0.600
2^{19}	0.670
2^{20}	0.651
2^{21}	0.684
2^{22}	0.744
2^{23}	0.746
2^{24}	0.785
2^{25}	0.788

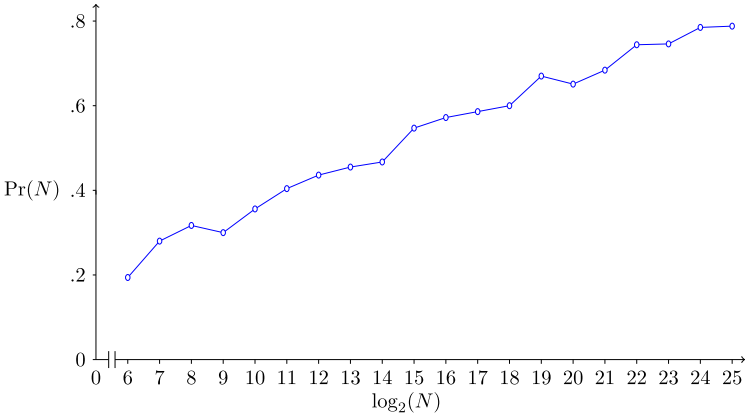

Fig. 1. $\Pr(N)$ vs. $\log_2(N)$.

References

[1] L. Babinkostova, A. Hernández-Espiet, H. Kim, On types of elliptic pseudoprimes, preprint, arXiv: 1710.05264v1.
[2] K.A. Broughan, The gcd-sum function, J. Integer Seq. 4 (2001) 01.2.2.
[3] C. David, F. Pappalardi, Average Frobenius distributions of elliptic curves, Int. Math. Res. Not. (4) (1999) 165–183.
[4] M. Deuring, Die typen der multiplikatorenringe elliptischer functiönenkorper, Abh. Math. Semin. Univ. Hambg. 14 (1941) 197–272.
[5] D.M. Gordon, On the number of elliptic pseudoprimes, Math. Comp. 52 (185) (1989) 231–245.
[6] D.M. Gordon, Pseudoprimes on elliptic curves, in: Théorie des Nombres: Proceedings of the 1987 International Number Theory Conference, De Gruyter, Berlin, 1989, pp. 290–305.
[7] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, 1998.
[8] H. Qin, Anomalous primes of the elliptic curve $E_D : y^2 = x^3 + D$, Proc. Lond. Math. Soc. 3 (112) (2016) 415–453.
[9] J.H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Math., vol. 151, 1994.

[10] J.H. Silverman, Elliptic carmichael numbers and elliptic Korselt criteria, Acta Arith. 155 (3) (2012) 233–246.
[11] Wolfram Research, Inc., Mathematica, Version 11.3, Champaign, IL, 2018.
[12] S. Zhang, Elliptic Curves, L-Functions, and CM-Points, Current Developments in Mathematics, Int. Press, Somerville, MA, 2002, pp. 179–219.