INFINITUDE OF ELLIPTIC CARMICHAEL NUMBERS

AARON EKSTROM, CARL POMERANCE, AND DINESH S. THAKUR

In memory of Alf van der Poorten

ABSTRACT. In 1987, Gordon gave an integer primality condition similar to the familiar test based on Fermat's little theorem, but based instead on the arithmetic of elliptic curves with complex multiplication. We prove the existence of infinitely many composite numbers simultaneously passing all elliptic curve primality tests assuming a weak form of a standard conjecture on the bound on the least prime in (special) arithmetic progressions. Our results are somewhat more general than both the 1999 dissertation of the first author (written under the direction of the third author) and a 2010 paper on Carmichael numbers in a residue class written by Banks and the second author.

1. INTRODUCTION

The problem of efficiently distinguishing the prime numbers from the composite numbers has been a fundamental problem for a long time. By Fermat's little theorem, $a^n \equiv a \bmod n$ for a prime number n and all integers a. By repeated squaring and reductions the congruence can be quickly tested for given numbers a and n, and thus if it fails we know that n is not a prime. A number n is called a *base a probable prime*, if the congruence is satisfied (Lucas's test [Wil98] around 1876). Note that $n = 341 = 11 \cdot 31$ is a composite number satisfying this congruence for $a = 2$; it is called a *base 2 pseudoprime*. We refer to such a procedure as a *compositeness test*, since it can definitely establish that a number is composite, but only give evidence towards a conjecture that a number is prime.

Unfortunately for the Lucas–Fermat tests, there are [AGP94.1] infinitely many composite numbers N such that for *every* integer a,

$$a^N \equiv a \pmod{N}. \tag{0.1}$$

These are called Carmichael ([Car10], [Car12]) numbers. The smallest is 561.

Elliptic curves have been used to factor numbers (see [Len86] and [Len87]) and prove the primality of numbers (see [GK86] and [AM93]). In [Gor87], Daniel Gordon developed compositeness tests using elliptic curves. Some elliptic curves possess a property which allows for a practical compositeness test that is very similar to, and just a constant factor slower than, the Lucas–Fermat test described above. If an elliptic curve E defined over $\mathbb{Q}$ has complex multiplication by an order in $\mathbb{Q}(\sqrt{-d})$ then $\#E(\mathbb{F}_p) = p + 1$ for any prime p with $\gcd(6\Delta_E, p) = 1$ and $(-d|p) = -1$. Let E be such an elliptic curve, and suppose $Q \in E$ is a rational point of infinite order. If N is an integer with $(-d|N) = -1$ and $\gcd(6\Delta_E, N) = 1$, we can test N. If $[N + 1]Q \not\equiv O \pmod{N}$, where O denotes the point at infinity and calculations are done using the addition law of E, then

Date: September 23, 2011.

The second author was supported in part by the NSF grant DMS-1001180. The third author was supported in part by NSA grant H98230-10-1-0200.

N is a composite number. If $[N+1]Q \equiv O \pmod{N}$ then N is an *elliptic probable prime for* $Q \in E$. Any composite number which is an elliptic probable prime for $Q \in E$ is called an *elliptic pseudoprime for* $Q \in E$. Gordon [Gor87, Gor89] defined an elliptic Carmichael number for E to be an elliptic pseudoprime for all rational points of infinite order on a given CM elliptic curve E. We will use the phrase *elliptic Carmichael number* to connote a composite number N coprime to 6 which is an elliptic Carmichael number for *every* CM elliptic curve $E/\mathbb{Q}$ with discriminant prime to N. (This concept is made more precise below.) An example of an elliptic Carmichael number is

$$617{,}730{,}918{,}224{,}831{,}720{,}922{,}772{,}642{,}603{,}971{,}311 = p(2p+1)(3p+2),$$

where $p = 468{,}686{,}771{,}783$.

We modify the methods of [AGP94.1, Eks99, BP10] to give a conditional lower bound for the number of elliptic Carmichael numbers in $[1,x]$. The results say that, under a suitable hypothesis and large enough x, the count exceeds $x^{2/7}$, and under a weaker hypothesis there are infinitely many elliptic Carmichael numbers. Both of these hypotheses are bounds on the least prime in arithmetic progressions and are weaker than the conjectured bound, recalled below. In addition, under the same hypotheses, we show more generally that any given coprime residue class (compatible with a technical condition stated below) contains infinitely many elliptic Carmichael numbers. We also show a similar result for ordinary Carmichael numbers, slightly strengthening the results of [BP10].

We mention that there have been some other notions of elliptic pseudoprimes in the literature, see [I94, CLS09, DW11] .

2. Preliminaries

2.1. **Carmichael numbers.** In 1899, Korselt [Kor99] noted the following property.

Theorem 1 (Korselt's criterion)**.** *A positive integer N divides $a^N - a$ for all integers a if and only if N is squarefree and $p-1$ divides $N-1$ for all primes p dividing N.*

Let $\mathcal{C}(x)$ denote the number of Carmichael numbers in $[1,x]$. In [AGP94.1] the authors use Korselt's criterion to prove $\mathcal{C}(x) \geq x^{2/7}$ for x large enough. In[PSW80], the authors show that

$$\mathcal{C}(x) \leq x^{1-\{1+o(1)\}\log\log\log x/\log\log x} \text{ for } x \to \infty.$$

It is conjectured that this upper bound gives the true size of $\mathcal{C}(x)$ (see [Pom81] and [PSW80]).

2.2. **Elliptic curves.** See [Len86, Sil86] for more details. For this section, R will either be a field with $char(R) \neq 2, 3$, or the ring $\mathbb{Z}/N\mathbb{Z}$ where N is coprime to 6. We use projective coordinates $(x:y:z)$ for points in the projective plane $\mathbb{P}^2(R)$. In the case that $R = \mathbb{Q}$, we assume as we may that $x, y, z \in \mathbb{Z}$ are coprime as a triple.

An elliptic curve over R given by the Weierstrass equation

$$y^2 z = x^3 + Axz^2 + Bz^3, \tag{1.1}$$

where $A, B \in R$ for which $\Delta := -16(4A^3 + 27B^2) \in R^*$ is denoted by $E_{A,B}$ or simply by E. The *set of points* $E(R)$ of E over R is

$$E(R) = \{(x:y:z) \in \mathbb{P}^2(R) : y^2 z = x^3 + Axz^2 + Bz^3\}.$$

The point $(0:1:0) \in E(R)$ is called the *zero point* or *point at infinity* of the curve, and denoted by O. Notice that if R is a field then this is the only element of $E(R)$ whose z-coordinate is noninvertible. Using the familiar tangent/chord construction, the set $E(R)$ forms an abelian group with O acting as the identity element. We refer to [Len86, Sil86] for explicit description of rational operations giving the group law in terms of the coordinates.

Let $E_{A,B}$ be an elliptic curve defined over $\mathbb{Q}$. We wish to consider the reduction of $E_{A,B}$ modulo a prime number. The elliptic curve $E_{A,B}$ is represented in such a way that the set of points of $E_{A,B}$ reduced modulo 2 or 3 does not have the structure we would like. However, our ultimate goal is a compositeness test, so in practice it will not be necessary to reduce by 2 or 3. Let p be a prime that does not divide $6\Delta_E$. (Since Δ_E is divisible by 16, we might have written $3\Delta_E$ here.) By abuse of notation, we will let $E(\mathbb{F}_p)$ be the set of points of the elliptic curve $E_{A \pmod p), B \pmod p)}$ defined over $\mathbb{F}_p$. For any point $(x : y : z) \in E(\mathbb{Q})$, as mentioned, we may assume that x, y, z are integers that are coprime as a triple. There is a natural homomorphism $\eta_p : E(\mathbb{Q}) \to E(\mathbb{F}_p)$ given by

$$\eta_p((x : y : z)) \mapsto (x \pmod p) : y \pmod p) : z \pmod p)).$$

This definition makes perfect sense if p is replaced with any positive integer N coprime to $6\Delta_E$, and so we have a homomorphism $\eta_N : E(\mathbb{Q}) \to E(\mathbb{Z}/N\mathbb{Z})$ given by reduction modulo N.

An endomorphism of E is a rational map $\varphi : E \to E$ that is a group homomorphism. The set of endomorphisms of an elliptic curve E, denoted by End(E), forms a ring with the group law of E as addition and the composition of maps as multiplication.

An important example of an endomorphism of E is the *multiplication by m map*, $[m] : E \to E$, where $m \in \mathbb{Z}$. (For $m > 0$, $[m]P$ is P added to itself m times and $[-m]P = -[m]P$. Further $[0]P = O$.)

For E over $\mathbb{Q}$, the ring of endomorphisms of E is either $\mathbb{Z}$ or an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ of class number 1, so that $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. In the latter case, E is said to have complex multiplication by $\mathbb{Q}(\sqrt{-d})$, or that E is a CM curve.

For the compositeness test we are going to discuss, it will be important to know how many points there are in $E(\mathbb{F}_p)$. A celebrated theorem of Hasse gives that $\#E(\mathbb{F}_p) = p + 1 - a_p$, where $|a_p| \leq 2\sqrt{p}$. We can say more when E has complex multiplication.

Theorem 2 (Deuring [Deu57]). *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathbb{Q}(\sqrt{-d})$. If p is a prime not dividing $6\Delta_E$, then*

$$\#E(\mathbb{F}_p) = \begin{cases} p + 1, & p \textit{ is inert in } \mathbb{Q}(\sqrt{-d}) \\ p + 1 - \operatorname{tr}(u\pi), & p = \pi\overline{\pi} \textit{ splits in } \mathbb{Q}(\sqrt{-d}) \end{cases}$$

where u is some unit in $\mathbb{Q}(\sqrt{-d})$ and tr *denotes the trace.*

2.3. **Elliptic curve compositeness test.** Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathbb{Q}(\sqrt{-d})$. If p is a prime that does not divide $6\Delta_E$ and $(-d|p) = -1$, then we can predict the order of the curve reduced modulo p; Theorem 2 states that $\#E(\mathbb{F}_p) = p + 1$. Gordon [Gor87] used this property to define a compositeness test: Start with E an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-d})$ and a point $Q \in E(\mathbb{Q})$ of infinite order. Let $N > 163$ denote a number coprime to 6 to be tested. We compute $(-d|N)$. If it is 1, we do not test and if it is 0, N is composite. If it is -1, we compute $[N + 1]Q \pmod N$. If it is O, N is declared a probable prime for $Q \in E$ and if it is not O, N is composite.

A composite number which is declared a probable prime for $Q \in E$ is called an *elliptic pseudoprime for* $Q \in E$. Let $\mathcal{N}(x) = \mathcal{N}_{E,Q}(x)$ denote the number of such elliptic pseudoprimes in $[1, x]$.

Gordon [Gor89] showed $\mathcal{N}(x)$ is $O(x \log\log x/\log^2 x)$ assuming the Generalized Riemann Hypothesis. In [MM89], I. Miyamoto and Ram Murty proved unconditionally that

$$\mathcal{N}(x) \ll x(\log\log x)^{7/2}/(\log x)^{3/2}.$$

(Note that the notation $A \ll B$ is synonymous with $A = O(B)$.) This was improved to

$$\mathcal{N}(x) \ll x \exp\{-c\sqrt{\log x \log\log x}\}$$

for some constant $c > 0$, by R. Balasubramanian and Ram Murty [BM90]. Gordon and Pomerance [GP91] showed

$$\mathcal{N}(x) \leq x^{1-\log\log\log x/(3\log\log x)}$$

for all sufficiently large numbers x, depending on E and Q. For some special curves, Gordon [Gor89] showed the number of elliptic pseudoprimes for $Q \in E$ is at least $\sqrt{\log x}/\log\log x$.

2.4. **Elliptic Carmichael numbers.** If N is an elliptic pseudoprime for each rational point of infinite order of a CM curve E, then N is an *elliptic Carmichael number for* E. We say N is an *elliptic Carmichael number for* $\mathbb{Q}(\sqrt{-d})$ if it is an elliptic Carmichael number for all elliptic curves $E/\mathbb{Q}$ with complex multiplication by $\mathbb{Q}(\sqrt{-d})$ whose discriminant is prime to N. If N is an elliptic Carmichael number for each $\mathbb{Q}(\sqrt{-d})$, $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ then we call N an *elliptic Carmichael number*.

The authors of [AGP94.1] use Korselt's criterion to prove there are infinitely many Carmichael numbers. We have a similar condition for elliptic Carmichael numbers.

In the following, we suppose that $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

Theorem 3 (Elliptic Carmichael condition for $\mathbb{Q}(\sqrt{-d})$)**.** *A squarefree composite number N coprime to* 6 *with an odd number of prime factors is an elliptic Carmichael number for* $\mathbb{Q}(\sqrt{-d})$ *if for each prime $p \mid N$ we have $(-d|p) = -1$ and $p + 1 \mid N + 1$.*

Proof. Since $(-d|N)$ is the product of $(-d|p)$ for primes $p \mid N$ and N has an odd number of prime factors, we have $(-d|N) = -1$. Suppose E is an elliptic curve over $\mathbb{Q}$ with CM by $\mathbb{Q}(\sqrt{-d})$ such that the discriminant of E is prime to N and Q is a point of infinite order on E. The conditions that $(-d|p) = -1$ for each prime $p \mid N$ implies via Theorem 2 that in each $E(\mathbb{F}_p)$ we have $[p + 1]\eta_p(Q) = O$. Since $p + 1 \mid N + 1$, we have each $[N + 1]\eta_p(Q) = O$. And since N is squarefree, the Chinese remainder theorem then implies that $[N + 1]\eta_N(Q) = O$ in $E(\mathbb{Z}/N\mathbb{Z})$. Thus, since N is composite, it is an elliptic Carmichael number for $\mathbb{Q}(\sqrt{-d})$. □

Consider the condition $(-d|N) = -1$. If $d = 1$ or 2 then $N \equiv -1 \pmod 8$ satisfies this condition. For $d = 3, 7, 11, 19, 43, 67, 163$, we have $(-d|N) = (N|d)$ and since these d's are all 3 modulo 4, $(N|d) = -1$ when $N \equiv -1 \pmod d$. Let

$$\alpha = 8 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 43 \cdot 67 \cdot 163 = 16{,}488{,}700{,}536.$$

Note that if $N \equiv -1 \pmod \alpha$, then N satisfies the condition $(-d|N) = -1$ for all d listed above.

Theorem 4. *[Elliptic Carmichael condition] If N is squarefree, composite, and with an odd number of prime factors, then N is an elliptic Carmichael number if for each prime $p \mid N$ we have $\alpha \mid p+1$ and $p+1 \mid N+1$.*

Remark. To ensure $(-d|p) = -1$ for all $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$, we require $p \equiv -1 \pmod{\alpha}$. The class $-1 \pmod{\alpha}$ is not the only congruence class with this property; p could be congruent to any one of $3 \cdot 5 \cdot 9 \cdot 21 \cdot 33 \cdot 81 = 7{,}577{,}955$ classes modulo α and have $(-d|p) = -1$ for all $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. We restrict the primes to the class $-1 \pmod{\alpha}$ in the above condition because it is convenient. We should note that this restriction will not have a detrimental effect on our main result.

3. Statement of hypotheses and results

In [AGP94.1], the authors prove there are infinitely many Carmichael numbers by constructing infinitely many squarefree composite numbers N such that $p-1|N-1$ for all primes p dividing N. They also mention that being able to construct infinitely many squarefree composite numbers N such that $p+1|N+1$ for all primes p dividing N would have significance for the elliptic curve compositeness test. This problem is mentioned again in [AGP94.2].

Recently Banks and Pomerance [BP10], under an unproved hypothesis concerning the size of the least prime in a coprime residue class, showed that for any positive integer m and any integer a coprime to m, there are infinitely many Carmichael numbers $N \equiv a \pmod{m}$. Actually the main idea in [BP10] had appeared earlier in Ekstrom [Eks99] and was rediscovered in the later paper.

In this section we modify the methods of [BP10] and of [Eks99] to prove somewhat more general results. Our theorems are conditional, with a weaker version requiring a weaker unproved hypothesis, and a stronger version requiring a stronger one. The weaker hypothesis is qualitatively the weakest we know that can prove an infinitude of elliptic Carmichael numbers. For a positive integer m and an integer a coprime to m, let $p(m, a)$ denote the least prime $p \equiv a \pmod{m}$, and let $p(m)$ denote the maximum of $p(m, a)$ over all choices of a.

Conjecture 5. *There is a positive number ξ such that*

$$p(m) \ll m^{1+\xi/\log\log m}$$

for all integers $m \geq 3$.

Conjecture 6. *There is a positive number $\kappa < 1$ such that*

$$p(m) \ll m^{1+(\log m)^{\kappa-1}}$$

for all integers $m \geq 3$.

We note that if Conjecture 6 holds for some value of $\kappa < 1$, then Conjecture 5 holds for each value of $\xi > 0$. A conjecture of Heath-Brown [HB78] that $p(m) \ll m(\log m)^2$ implies Conjecture 6 for each value of $\kappa > 0$, so both Conjectures 5 and 6 may be viewed as weaker forms of Heath-Brown's conjecture. For heuristic arguments supporting the Heath-Brown conjecture and results on the question, see [BS96, Erd49, Gra89, McC86, Pom80, Uch72, Wag79].

The best that is known unconditionally is that there is a constant C such that $p(m) \ll m^C$, a result of Linnik [Lin44]. Heath-Brown [HB92] showed that $C = 5.5$ works and the smallest value of C for which this is known to hold is $C = 5.2$, see [X09].

Definition 7. For integers m, a, b with $m > 0$, $\gcd(m, a) = 1$, and $b = \pm 1$, let $C(x; m, a, b)$ denote the number of composite squarefree integers $N \le x$ such that $N \equiv a \pmod{m}$ and for each prime factor p of N we have $p \equiv a \pmod{m}$ and $p + b \mid N + b$.

The case of $b = -1$ in Definition 7, namely the case when the numbers N that are counted are Carmichael numbers, was dealt with in [BP10]. The case of $b = 1$, $m = \alpha$, and $a = -1$ is of interest for elliptic Carmichael numbers (or more generally any coprime choice for m, a such that $\alpha \mid m$ and $a \equiv -1 \pmod{\alpha}$), by Theorem 4. Note that the requirement that there are an odd number of prime factors is now automatically satisfied.

We shall prove the following two theorems.

Theorem 8. *If Conjecture 5 holds with $\xi = 1/7$, then for all choices of integers m, a, b with $m > 0$, $\gcd(m, a) = 1$, and $b = \pm 1$,*

$$C(x; m, a, b) > x^{1/(7 \log\log\log x)}$$

for all sufficiently large numbers x depending on the choice of m and a.

In particular, if Conjecture 5 holds for $\xi = 1/7$, then there are infinitely many integers that are elliptic Carmichael numbers for every imaginary quadratic number field of class number 1.

We will use the notation $P(k)$ to denote the largest prime dividing an integer $k > 1$ and $\pi(x; a, b)$ to denote the number of primes in $[1, x]$ of the form $an + b$.

Theorem 9. *Suppose that the real number E in $(0, 1)$ has the property that the number of primes $l \le x$ with $P(l-1) \le x^{1-E}$ is $x^{1-o(1)}$ as $x \to \infty$. If Conjecture 6 holds with $\kappa = 1 - E$, then for each fixed choice of integers m, a, b with $m > 0$, $\gcd(m, a) = 1$, and $b = \pm 1$,*

$$C(x; m, a, b) \ge x^{\frac{5}{12}E - o(1)}, \ x \to \infty.$$

Note that the expression $o(1)$ in Theorem 9 may depend on the choices of m and a. We remark that the largest real number E known to have the property in the theorem is 0.7039, a result of Baker and Harman [BH98]. This justifies the $x^{2/7}$ lower bound mentioned for the number of elliptic Carmichael numbers in $[1, x]$. It is likely the number "5/12" in this theorem can be slightly increased by the method of [Har08].

4. Proofs of the principal results

4.1. **Some tools.** We begin with some tools, in particular a result that shows the existence of numbers with many divisors that are shifted primes.

Proposition 10. *Let m, a, b be integers with $m > 0$, $\gcd(m, a) = 1$, and $b \ne 0$. Let B be a positive number with $B < 5/12$. There are positive numbers c_B, $x_{B,m}$ with the following property. If $x \ge x_{B,m}$ and if L is a squarefree integer coprime to mb with at most $x^{1/4}$ prime factors whose reciprocal sum is at most $1/60$, then there is a positive integer $k \le x^{1-B}$ that is coprime to L such that*

$$\#\{p \text{ prime} : p = dk + b \text{ for some } d \mid L \text{ with } d \le x^B,\ p \equiv a \pmod{m}\}$$
$$\ge \frac{c_B}{\varphi(m) \log x} \#\{d \mid L : d \le x^B\}.$$

Proof. This result is almost identical to Proposition 1.5 in [AGP94.2], but we give the details for convenience. (We remark that the analogous result in [BP10], namely Lemma 2, was incorrectly stated; it left out the important conclusion that k is coprime to L.) Let B' be the average of B and $5/12$. According to [AGP94.1], there is a set $\mathcal{S}_B(x)$ of integers all greater than $\log x$ with $\#\mathcal{S}_B(x) \leq S_B$, where S_B is a constant depending only on B, such that if q, u are integers with $1 < q \leq x^{B'}$, $\gcd(q, u) = 1$, and q not divisible by any member of $\mathcal{S}_B(x)$, then

$$\pi(y; q, u) \geq \frac{y}{2\varphi(q)\log y} \text{ for all } y \geq qx^{1-B'}. \tag{10.1}$$

We may take $x_{B,m} > e^m$, so that no member of $\mathcal{S}_B(x)$ divides m. For each member s of $\mathcal{S}_B(x)$ for which $\gcd(s, L) > 1$, remove one prime factor of $\gcd(s, L)$ from L. This creates a new number L' where $L' \mid L$ and L/L' has at most S_B prime factors. Since m and L are coprime and L is squarefree, we thus have that no member of $\mathcal{S}_B(x)$ divides mL'.

For a number d coprime to m, let C_d be the solution to the Chinese remainder problem

$$C_d \equiv a \pmod{m},\ C_d \equiv -b \pmod{d}.$$

We now count positive-integer pairs d, k where $d \mid L'$, $d \leq x^B$, $k \leq x^{1-B}$, and $p = dk - b$ is a prime with $p \equiv a \pmod{m}$. Note that for $x_{B,m}$ large enough, we have $dm \leq x^{B'}$. The count of d, k pairs is precisely

$$\sum_{\substack{d \mid L' \\ d \leq x^B}} \pi(dx^{1-B}; dm, C_d) \geq \sum_{\substack{d \mid L' \\ d \leq x^B}} \frac{dx^{1-B}}{2\varphi(dm)\log(dx^{1-B})} \geq \sum_{\substack{d \mid L' \\ d \leq x^B}} \frac{dx^{1-B}}{2\varphi(dm)\log x}$$

using (10.1).

We wish to show that the number of such pairs d, k where $\gcd(L, k) > 1$ is small. For each prime $l \mid L$ consider pairs d, k as above where $l \mid k$. The number of these pairs is given by

$$\sum_{\substack{l \text{ prime} \\ l \mid L'}} \sum_{\substack{d \mid L' \\ d \leq x^B}} \pi(dx^{1-B}; dml, C_{dl}).$$

For those values of $l > x^{2/7}$, we upper-bound the summand by

$$1 + \frac{dx^{1-B}}{dml} \leq \frac{2x^{5/7-B}}{m}.$$

Multiplying by the number of primes $l \mid L$, which is assumed to be at most $x^{1/4}$, our bound in this case is at most $2x^{27/28-B}/m$. We use the Brun–Titchmarsh inequality (see [MV73]) when $l \leq x^{2/7}$, getting the majorization

$$\sum_{\substack{l \text{ prime} \\ l \mid L' \\ l \leq x^{2/7}}} \sum_{\substack{d \mid L' \\ d \leq x^B}} \frac{2dx^{1-B}}{(l-1)\phi(dm)\log(x^{1-B}/(ml))} < \sum_{\substack{d \mid L' \\ d \leq x^B}} \frac{dx^{1-B}}{5\varphi(dm)\log x},$$

using for the last estimate the assumption about the reciprocal sum of the primes $l \mid L$, that $m < \log x$, and that $B < 5/12$.

Putting these estimates together, we have that the number of pairs d, k with $d \mid L$, $d \le x^B$, $k \le x^{1-B}$, k coprime to L, and $p = dk + b$ prime with $p \equiv a \pmod{m}$ is at least

$$\sum_{\substack{d \le x^B \\ d \mid L'}} \left(\frac{dx^{1-B}}{2\varphi(dm)\log x} - \frac{2x^{27/28-B}}{m} - \frac{dx^{1-B}}{5\varphi(dm)\log x} \right) \ge \sum_{\substack{d \le x^B \\ d \mid L'}} \frac{x^{1-B}}{4\varphi(m)\log x}$$

for large x. There is thus at least one value of $k \le x^{1-B}$ coprime to L with at least

$$\sum_{\substack{d \le x^B \\ d \mid L'}} \frac{1}{4\varphi(m)\log x}$$

appearances in pairs d, k. Since the mapping that sends $d \mid L$ to the divisor $d/(d, L/L')$ of L' is at most $2^{S_B} : 1$, we have

$$\#\{d \le x^B : d \mid L'\} \ge \frac{1}{2^{S_B}} \#\{d \le x^B : d \mid L\}.$$

Our result now follows with $c_B = 1/2^{S_B+2}$. □

For a finite abelian group G, let $D(G)$ denote the Davenport constant for G defined as the least positive integer D such that for any length-D sequence of group elements, there is a non-null subsequence with product the identity (we assume G has "product" as the group operation). Let $\lambda(G)$ denote the universal exponent for G, equivalently, the order of the largest cyclic subgroup. The following result is a slightly weakened form of [AGP94.1, Theorem 2].

Proposition 11. *For any finite abelian group G,*

$$D(G) \le \lambda(G)(1 + \log(\#G)).$$

Let R denote a sequence of length r consisting of elements of G, where r is significantly larger than $D(G)$. By the definition of $D(G)$, we know there exists at least one non-null subsequence of R that has product the identity. In fact there are many such subsequences. We will use the following result which is [AGP94.1, Proposition 1.2].

Proposition 12. *Let G be a finite abelian group and let $r > t > D = D(G)$ be integers. Any length-r sequence of elements of G contains at least $\binom{r}{t}/\binom{r}{D}$ distinct subsequences of length at most t and at least $t - D$, whose product is the identity.*

4.2. **Proof of Theorem 8.** Fix integers m, a, b with $m > 0$, $\gcd(m, a) = 1$, and $b = \pm 1$. Fix some real number B with $0 < B < 5/12$. Let y be a large real parameter and let

$$\mathcal{L} = \mathcal{L}(y) = \{l \text{ prime} : y/\log y < l \le y,\ P(l-1) \le y/(\log y)^2\}.$$

We have

$$\#\mathcal{L} = (1 + o(1))y/\log y \ \text{ as } y \to \infty. \tag{12.1}$$

To see this, note that the primes in $(y/\log y, y]$ that are not in $\mathcal{L}$ are of the form $kq + 1$ with q prime and $q > y/(\log y)^2$. We conclude that $k < (\log y)^2$. Sieve methods (see [MV07]) give that uniformly for $k < (\log y)^2$, the number of primes $q \le y/k$ with $kq+1$ prime is $O(y/(\varphi(k)\log^2 y))$. Summing on k gives a total of $O(y \log\log y/\log^2 y)$ primes in $(y/\log y, y]$ that are not in $\mathcal{L}$. Thus, the prime number theorem implies that there are $(1+o(1))\pi(y) = (1+o(1))y/\log y$ primes in $\mathcal{L}$, as $y \to \infty$. This proves (12.1).

Let $L = L(y)$ denote the product of the primes in $\mathcal{L}$. We assume that y is so large that L is coprime to m. Further, by (12.1) we have

$$L = e^{(1+o(1))y} \text{ as } y \to \infty.$$

We would like to apply Proposition 10 with $x = L^{1/B}$, but we must check that the hypotheses hold. Since L has fewer than $\log L \ll \log x$ prime factors, we may assume that y is so large that L has fewer than $x^{1/4}$ prime factors. Further, the reciprocal sum of these primes is $\ll \log\log y/\log y$, so we may assume y is so large that this reciprocal sum is smaller than $1/60$. Thus, by Proposition 10, there is an integer $k \le x^{1-B}$ coprime to L such that with

$$\mathcal{P} = \mathcal{P}(y,k) = \{p \text{ prime} : p = dk - b \text{ for some } d \mid L,\ p \equiv a \pmod{m}\},$$

we have (by (12.1) and using that m is fixed)

$$\#\mathcal{P} \ge \frac{c_B}{\varphi(m)\log x}\tau(L) = \frac{c_B 2^{\#\mathcal{L}}}{\varphi(m)\log x} = 2^{(1+o(1))y/\log y} \text{ as } y \to \infty. \tag{12.2}$$

(Note that Propsition 10 requires $d \le x^B$, but $x^B = L$, so there is no extra condition on d other than $d \mid L$.) The expression $\tau(L)$ denotes the number of positive divisors of L, which in this case is $2^{\#\mathcal{L}}$.

Since $\mathcal{P}$ is nonempty and $\gcd(m, L) = 1$, it follows that there is an integer a' coprime to $M := \operatorname{lcm}[kL, m]$ with $a' \equiv -b \pmod{kL}$ and $a' \equiv a \pmod{m}$. Assume now that Conjecture 5 holds with $\xi = 1/7$ and let p_0 be the least prime with $p_0 \equiv a' \pmod{M}$. Thus,

$$p_0 \ll M^{1+1/(7\log\log M)}.$$

Write $p_0 = -b + ukL$, so that

$$u \le e^{(1+o(1))y/(7B\log y)} \text{ as } y \to \infty,$$

using that m is fixed and $kL \le L^{1/B} = e^{(1+o(1))y/B}$.

Remove from $\mathcal{P}$ any member which divides uLp_0, denoting the resulting set $\mathcal{P}'$. Since uLp_0 has $O(y^2)$ prime factors, estimate (12.2) implies that for all large y,

$$\#\mathcal{P}' \ge e^{(\log 2+o(1))y/\log y} \text{ as } y \to \infty. \tag{12.3}$$

We view the set $\mathcal{P}'$ in its natural order as a sequence in the subgroup G of $(\mathbb{Z}/ukLm\mathbb{Z})^*$ consisting of residues $g \equiv \pm 1 \pmod{k}$. Since $(k, L) = 1$, we have

$$\lambda(G) \le 2um\lambda\left((\mathbb{Z}/L\mathbb{Z})^*\right) = 2um \cdot \operatorname{lcm}\{l - 1 : l \in \mathcal{L}\}.$$

If $1 < p^{n_p}$ divides the lcm, then it divides some $l-1$ and is thus less than y, and also $p \le y/(\log y)^2$, so

$$\operatorname{lcm}\{l - 1 : l \in \mathcal{L}\} \le \prod_{p \le y/(\log y)^2} p^{n_p} \le \prod_{p \le y/(\log y)^2} y \le y^{Ay/(\log y)^3} = e^{Ay/(\log y)^2},$$

for y sufficiently large and some fixed $A > 0$, by Chebyshev's theorem on the distribution of primes. Thus, with the above estimate on u and using that m is fixed, we have

$$\lambda(G) \le e^{(1+o(1))y/(7B\log y)} \text{ as } y \to \infty.$$

Since $\#G \le 2uLm \le e^{(1+o(1))y}$, it follows from Proposition 11 that

$$D(G) \le e^{(1+o(1))y/(7B\log y)} \text{ as } y \to \infty.$$

Suppose $\mathcal{S}$ is a nonempty subsequence of $\mathcal{P}'$ with product $n_{\mathcal{S}}$ equal to the identity in G. Then $n_{\mathcal{S}}$ is squarefree, $n_{\mathcal{S}} \equiv 1 \pmod{ukLm}$, and for each prime $p \mid n_{\mathcal{S}}$ we have $p \equiv a \pmod{m}$. Now let $N_{\mathcal{S}} = p_0 n_{\mathcal{S}}$. Then $N_{\mathcal{S}}$ is squarefree and composite, $N_{\mathcal{S}} \equiv -b \pmod{ukL}$, $N_{\mathcal{S}} \equiv a \pmod{m}$, for each prime $p \mid N_{\mathcal{S}}/p_0$ we have $p + b \mid kL \mid N_{\mathcal{S}} + b$, and also $p_0 + b = ukL \mid N_{\mathcal{S}} + b$.

Let $\epsilon > 0$ be arbitrarily small but fixed, and let y be so large that

$$D(G) \le \overline{D} := \left\lceil e^{(1+\epsilon)y/(7B\log y)} \right\rceil.$$

Let $t = 100\overline{D}$ and let

$$X = X(y) = \exp\left((1+\epsilon)(y/B)100e^{(1+\epsilon)y/(7B\log y)}\right).$$

Thus, $X \ge x^{(1+\epsilon/2)t} \ge x^{t+2}$ for large y. We have

$$\log\log\log X = (1+o(1))\log y \text{ as } y \to \infty. \tag{12.4}$$

Further, if N is the product of p_0 and at most t primes from $\mathcal{P}'$, then $N \le x^{t+1+o(1)}$ so that for large values of y, we have $N \le X$.

We now produce a lower bound for $C(X; m, a, b)$. Using the above construction of numbers $N_{\mathcal{S}}$ and Proposition 12, we have

$$\begin{aligned} C(X; m, a, b) &\ge \binom{\#\mathcal{P}'}{t} \Big/ \binom{\#\mathcal{P}'}{\overline{D}} \ge \left(\frac{\#\mathcal{P}'}{t}\right)^t \#\mathcal{P}'^{-\overline{D}} \\ &= \#\mathcal{P}'^{99\overline{D}}(100\overline{D})^{-100\overline{D}}. \end{aligned}$$

Using our estimate (12.3) for $\#\mathcal{P}'$, we have

$$\begin{aligned} C(X; m, a, b) &\ge \exp\left(\overline{D}\left((99\log 2 - \epsilon)\frac{y}{\log y} - 100(\log 100 + \log\overline{D})\right)\right) \\ &\ge \exp\left(\overline{D}\frac{y}{\log y}\left((99\log 2 - \epsilon) - (1+\epsilon)^2\frac{100}{7B}\right)\right) \\ &= X^{[99\log 2 - \epsilon - (1+\epsilon)^2 100/(7B)]/[100(1+\epsilon)(\log y)/B]} \end{aligned}$$

for y large. Since $(99\log 2 - 100/(7B))/(100/B) > 1/7$ if B is sufficiently close to $5/12$, we may choose B and ϵ and use (12.4) to conclude that $C(X; m, a, b) \ge X^{1/(7\log\log\log X)}$ for all large y. Since $X = X(y)$ is a continuous increasing function, we may choose X first and then determine the value of y which allows the argument to work. This completes the proof.

4.3. **Proof of Theorem 9.** The proof follows the same general pattern as the proof of Theorem 8 that was just completed. We assume E is as given in the hypothesis, and we let $\epsilon > 0$ be arbitrarily small, but fixed. Let y be a large real parameter and let

$$\mathcal{L} = \{l \text{ prime} : y^{1/(1-E)-\epsilon} < l \le y^{1/(1-E)},\ P(l-1) \le y\}.$$

By our hypothesis, we have

$$\#\mathcal{L} = y^{1/(1-E)+o(1)} \text{ as } y \to \infty.$$

Let L denote the product of the members of $\mathcal{L}$ so that $L = \exp(y^{1/(1-E)+o(1)})$ as $y \to \infty$.

Let $x = \exp(y^{1+\epsilon})$ and apply Proposition 10 to L with parameters m, a, b. We deduce that there is an integer $k \leq x^{1-B}$ coprime to L such that if $\mathcal{P}$ is the set of primes produced in Proposition 10, we have

$$\#\mathcal{P} \gg \frac{1}{\log x} \#\{d \mid L : d \leq x^B\},$$

using that m is fixed. Let

$$s = \left\lfloor \frac{\log(x^B)}{\log(y^{1/(1-E)})} \right\rfloor = (1 + o(1))B(1-E)\frac{y^{1+\epsilon}}{\log y} \ \text{ as } y \to \infty,$$

and note that the product of any s primes from $\mathcal{L}$ is at most x^B. Thus

$$\#\{d \mid L : x \leq x^B\} \geq \binom{\#\mathcal{L}}{s} \geq \left(\frac{\#\mathcal{L}}{s}\right)^s = \exp(s(\log \#\mathcal{L} - \log s)).$$

Since $\log \#\mathcal{L} = (1/(1-E) + o(1)) \log y$ and $\log s = (1 + \epsilon + o(1)) \log y$, we have

$$\begin{aligned}\#\{d \mid L : d \leq x^B\} &\geq \exp\left((1 + o(1))B(1-E)(1/(1-E) - 1 - \epsilon)y^{1+\epsilon}\right)\\ &= \exp\left((EB - \epsilon B(1-E) + o(1))y^{1+\epsilon}\right) \ \text{ as } y \to \infty.\end{aligned}$$

We conclude that $\#\mathcal{P} \geq \exp\left((EB - \epsilon B(1-E) + o(1))y^{1+\epsilon}\right)$ as $y \to \infty$.

Define M, p_0, u as in the proof of Theorem 8. By hypothesis, we have Conjecture 6 with $\kappa = 1 - E$, so we have

$$u \leq \exp(y^{1+o(1)}) \ \text{ as } y \to \infty.$$

We define the group G as in the proof of Theorem 8. Using that $\lambda((\mathbb{Z}/L\mathbb{Z})^*) = e^{O(y)}$, we deduce as before, that

$$D(G) \leq \exp(y^{1+o(1)}) \ \text{ as } y \to \infty.$$

Let

$$\overline{D} = \left\lceil \exp\left(y^{1+\epsilon/3}\right) \right\rceil$$

so that $D(G) \leq \overline{D}$ for y large. Let

$$t = \left\lfloor \exp\left(y^{1+2\epsilon/3}\right) \right\rfloor, \ X = x^{3+\exp(y^{1+2\epsilon/3})},$$

so that $x^{t+2} \leq X$. Hence the product of any t primes from $\mathcal{P}$, multiplied by p_0, is at most X when y is large.

Removing those few primes from $\mathcal{P}$ which divide uLp_0 to form $\mathcal{P}'$, as in the proof of Theorem 8, we have

$$\#\mathcal{P}' \geq \exp\left((EB - \epsilon B(1-E) + o(1))y^{1+\epsilon}\right) \ \text{ as } y \to \infty.$$

We now apply Proposition 12 to get a lower bound for $C(X; m, a, b)$ as in the proof of Theorem 8:

$$\begin{aligned}C(X; m, a, b) &\geq \#\mathcal{P}'^{t-\overline{D}} t^{-t} \geq \exp\left((EB - \epsilon B(1-E) + o(1))y^{1+\epsilon} t\right)\\ &= X^{EB - \epsilon B(1-E) + o(1)} \ \text{ as } y \to \infty.\end{aligned}$$

Since $\epsilon > 0$ is arbitrary and B is arbitrarily close to $5/12$, we have Theorem 9.

5. Complements

For examples, numerical issues, tables and constructions of elliptic Carmichael numbers based on [Che39] in the case of Carmichael numbers, we refer to [Eks99]. Some other results proved there are (1) The elliptic Carmichael numbers are squarefree, (2) For any $\epsilon > 0$, the number of elliptic Carmichael numbers in $[1, x]$ which have exactly k distinct prime factors is at most $x^{(2k-1)/(2k)+\epsilon}$ for large enough x, depending on k and ϵ.

The Lucas–Fermat compositeness test has a strong version: If $2^{k+1} \mid N - 1$ and $a^{(N-1)/2^k} \equiv 1 \pmod N$, but $a^{(N-1)/2^{k+1}} \not\equiv \pm 1 \pmod N$, then N cannot be prime. D. H. Lehmer [Leh76] showed that every composite number is declared composite by at least one strong Lucas–Fermat test. In other words, Lehmer showed that there are no strong Carmichael numbers. Analogously, Gordon [Gor87] defined a strong version of the elliptic curve compositeness test: If $2^{k+1} \mid N + 1$ and $[(N + 1)/2^k]\eta_N(Q) = O$, but $[(N + 1)/2^{k+1}]\eta_N(Q)$ is not a 2-division point or O, then N cannot be prime. In [Eks99], it is also proved that there are no strong elliptic Carmichael numbers in this sense. On this general subject, also see the new paper [M10] of Müller. Finally we remark that it has been unconditionally shown [PR80] that any given given coprime arithmetic progression contains infinitely many (ordinary) strong pseudoprimes to any fixed base.

References

[AGP94.1] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Ann. of Math.*, 139(3):703–722, 1994.

[AGP94.2] W. R. Alford, A. Granville, and C. Pomerance. On the difficulty of finding reliable witnesses. Algorithmic Number Theory (Ithaca, NY, 1994), 1–16. *Lecture Notes in Comput. Sci.* **877**, Springer, Berlin, 1994.

[AM93] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993.

[BS96] E. Bach and J. Shallit. *Algorithmic number theory*. Foundations of Computing. MIT Press, Cambridge, MA, 1996.

[BM90] R. Balasubramanian and M. R. Murty. Elliptic pseudoprimes. II. In *Séminaire de théorie des nombres, Paris 1988-1989*, number 91 in Progr. Math., pages 13–25, Birkhäuser, Boston, 1990.

[BH98] R. C. Baker and G. Harman. Shifted primes without large prime factors. *Acta Arith.* 83:331–361, 1998.

[BP10] W. D. Banks and C. Pomerance. On Carmichael numbers in arithmetic progressions *J. Austral. Math. Soc.*, 28:313–321 ,2010.

[Car10] R. D. Carmichael. Note on a new number theory function. *Bull. Amer. Math. Soc.*, 16:232–238, 1910.

[Car12] R. D. Carmichael. On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \bmod P$. *Amer. Math. Monthly*, 19(156):22–27, 1912.

[Che39] J. Chernick. On Fermat's simple theorem. *Bull. Amer. Math. Soc.*, 45:269–274, 1939.

[CLS09] A. Cojocaru, F. Luca, and I. E. Shparlinski. Pseudoprime reductions of elliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 146(3):513–522, (2009).

[DW11] C. David and J. Wu. Pseudoprime reductions of elliptic curves. Preprint, 2011.

[Deu57] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. IV. *Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. IIa*, 1957:55–80, 1957.

[Eks99] A. Ekstrom. On the infinitude of elliptic Carmichael numbers. Ph. D. thesis, University of Arizona (1999).

[Erd49] P. Erdős. On some applications of Brun's method. *Acta Univ. Szeged. Sect. Sci. Math.*, 3:57–63, 1949.

[GK86] S. Goldwasser and J. Kilian. Almost all primes can be quickly certified. In *Proc. 18th Annual ACM Sympos. on Theory of Computing (STOC, Berkeley 1986)*, pages 316–329, New York, 1986. The Association for Computing Machinery.

[Gor87] D. M. Gordon. Pseudoprimes on elliptic curves. In J. M. De Koninck and C. Levesque, eds., *Number Theory, Proc. Internat. Number Theory Conf., Laval 1987*, pages 291–305, de Gruyter, New York, 1989.

[Gor89] D. M. Gordon. On the number of elliptic pseudoprimes. *Math. Comp.*, 52(185):231–245, 1989.

[GP91] D. M. Gordon and C. Pomerance. The distribution of Lucas and elliptic pseudoprimes. *Math. Comp.*, 57(196):825–838, 1991.

[Gra89] A. Granville. Least primes in arithmetic progressions. In J. M. De Koninck and C. Levesque, eds., *Number Theory, Proc. Internat. Number Theory Conf., Laval 1987*, pages 306–321. de Gruyter, New York, 1989.

[Har08] G. Harman. Watt's mean value theorem and Carmichael numbers. *Int. J. Number Theory*, 4:241–248, 2008.

[HB78] D. R. Heath-Brown. Almost-primes in arithmetic progressions and short intervals. *Math. Proc. Cambridge Philos. Soc.*, 83:357–375, 1978.

[HB92] D. R. Heath-Brown. Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression. *Proc. London Math. Soc.*, 64:265–338, 1992.

[I94] H. Ito. On elliptic pseudoprimes. *Mem. College Ed. Akita Univ. Natur. Sci.*, 46:1–7, 1994.

[Kor99] A. Korselt. Problème chinois. *L'intermédiaire des Mathématiciens*, 6:142–143, 1899.

[Leh76] D. H. Lehmer. Strong Carmichael numbers. *J. Austral. Math. Soc. Ser. A*, 21:508–510, 1976.

[Len86] H. W. Lenstra, Jr. Elliptic curves and number-theoretic algorithms. *Proc. ICM, Berkeley, California, USA, 1986*, pages 99–120, 1986.

[Len87] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math.*, 126(3):649–673, 1987.

[Lin44] U. V. Linnik. On the least prime in an arithmetic progression II. *Rec. Math. [Mat. Sb.]*, 15(57):347–368, 1944.

[McC86] K. S. McCurley. The least r-free number in an arithmetic progression. *Trans. Amer. Math. Soc.*, 293:467–475, 1986.

[MM89] I. Miyamoto and M. R. Murty. Elliptic pseudoprimes. *Math. Comp.*, 53(187):415–430, 1989.

[MV73] H. L. Montgomery and R. C. Vaughan. The large sieve. *Mathematika*, 20(40):119–134, 1973.

[MV07] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory I. Classical theory*. Cambridge University Press, Cambridge, 2007.

[M10] S. Müller. On the existence and non-existence of elliptic pseudoprimes. *Math. Comp.* 79(270):1171-1190, 2010.

[Pom80] C. Pomerance. A note on the least prime in an arithmetic progression. *J. Number Theory*, 12:218–223, 1980.

[Pom81] C. Pomerance. On the distribution of pseudoprimes. *Math. Comp.*, 37(156):587–593, October 1981.

[PSW80] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr. The pseudoprimes to $25 \cdot 10^9$. *Math. Comp.*, 35(151):1003–1026, July 1980.

[PR80] A. J. van der Poorten and A. Rotkiewicz. On strong pseudoprimes in arithmetic progressions. *J. Austral. Math. Soc. Ser. A* 29(3):316–321, 1980.

[Sil86] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate texts in mathematics*. Springer-Verlag, New York, 1986.

[Uch72] S. Uchiyama. An application of the large sieve. *Proc. Japan Acad.*, 48:67–69, 1972.

[Wag79] S. S. Wagstaff Jr. Greatest of the least primes in arithmetic progressions having a given modulus. *Math. Comp.*, 33:1073–1080, 1979.

[Wil98] H. C. Williams. *Edouard Lucas and primality testing*, volume 22 of *Canadian Mathematical Society series of monographs and advanced texts*. Wiley-Interscience, New York, 1998.

[X09] T. Xylouris. Über die Linniksche Konstante. arXiv:0906.2749.

Aaron Ekstrom
8505 E. Ocotillo Dr.
Tucson AZ 85750, USA
DoctorX198@gmail.com

Carl Pomerance
Mathematics Department
Dartmouth College
Hanover, NH 03755, USA
pomerance@dartmouth.edu

Dinesh S. Thakur
Mathematics Department
University of Arizona
Tucson, AZ 85721, USA
thakur@math.arizona.edu