INFINITUDE OF ELLIPTIC CARMICHAEL NUMBERS

AARON EKSTROM, CARL POMERANCE AND DINESH S. THAKUR

Abstract. We prove existence of infinitely many composite numbers passing all elliptic curve primality tests (i.e., elliptic analog of Carmichael numbers), assuming a weak form of standard conjecture on the bound on the least prime in (special) arithmetic progressions. We also discuss various several related developments. The main result mentioned above is from the PhD thesis [Eks99] of the first author done under the direction of the third author and based on ideas of the joint work [AGP1] of the second author proving the infinitude of Carmichael numbers.

1. Introduction

The problem of efficiently distinguishing the prime numbers from the composites has been a fundamental problem in number theory for long, and its practical significance has increased a lot since number theory applications in cryptology became pervasive in modern technology and communications industry due to computers and internet. By Fermat's little theorem, $a^n \equiv a \bmod n$ for a prime number n. By repeated squaring and reductions the congruence can be tested fast for a given numbers a and n, and thus if it fails we know that n is not a prime. A number n is called base a probable prime, if the congruence is satisfied (Lucas's test [Wil98] around 1876). But $n = 314 = 11 * 31$ is a composite number satisfying this congruence for $a = 2$, thus it is a base 2 pseudo prime.

Unfortunately for such tests, there are [AGP1] infinitely many composite numbers such that for any 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 the order of $E(\mathbb{F}_p)$ is $p+1$ for any prime p with $\gcd\{3\Delta_E, p\} = 1$ and $(-d|p) = -1$. Let E be such an elliptic curve, and $Q \in E$ be a rational point of infinite order. If N is an odd integer with $(-d|N) = -1$ and $\gcd\{3\Delta_E, N\} = 1$, we can test N using $Q \in E$. If $[N+1] \cdot Q \not\equiv O \pmod{N}$ (where O denotes the point at infinity and calculations are done using the addition law of E) then N is a composite number. If $[N+1] \cdot Q \equiv O \pmod{N}$ 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 [Gor89] defined an

Date: March 9, 2011.

elliptic Carmichael number to be an elliptic pseudoprime for all rational points of infinite order on a given elliptic curve E. We will call such a number an "elliptic Carmichael number for E" and use the term "elliptic Carmichael number" to denote an odd composite number N which passes

$$(-d|N) = -1 \quad \text{and} \quad [N+1] \cdot Q = O \pmod{N} \tag{0.2}$$

for every rational point of infinite order on *every* CM elliptic curve $E/\mathbb{Q}$ with discriminant prime to N. The smallest elliptic Carmichael number we have found thus far is

$$907787752480943719546615545955087223 99.$$

Let $\mathcal{T}(x)$ denote the number of elliptic Carmichael numbers up to x. We modify the methods of [AGP1] to give a conditional lower bound for the number of elliptic Carmichael numbers. The major modification occurs in the group theory argument of [AGP1]. We also force an additional congruence condition. The result, under a suitable hypothesis and large enough x, is $\mathcal{T}(x) \geq x^{2/7}$. This theorem implies there are infinitely many elliptic Carmichael numbers, assuming the smallest prime congruent to -1 modulo q is at most $q \exp[(\log q)^{1-\varepsilon}]$. Note this assumption is much weaker than conjectured bounds, recalled below.

2. Preliminaries

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

Theorem 1 (Korselt's Criterion)**.** *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 up to x. In [AGP1] 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 [Sil86, Len86] 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. A triple $(x, y, z) \in R^3$ will be called *primitive* if there exists $a_1, a_2, a_3 \in R$ such that $a_1x + a_2y + a_3z = 1$. The group of units R^* acts on the set of primitive triples $(x, y, z) \in R^3$ by $u(x, y, z) = (ux, uy, uz)$. The set of orbits under this action is denoted by $\mathbb{P}^2(R)$, and called the *projective plane over* R. An orbit of (x, y, z) is denoted by $(x : y : z)$.

An elliptic curve over R is a pair of elements $A, B \in R$ for which $\Delta := -16(4A^3 + 27B^2) \in R^*$. These elements are to be thought of as the coefficients in the homogeneous Weierstrass equation

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

We denote the elliptic curve (A, B) by $E_{A,B}$ or simply by E. The j-invariant of E is $6912A^3/(4A^3 + 27B^2)$. If we multiply equation (1.1) by u^6, for some $u \in R^*$, and replace u^2x by x and u^3y by y then we obtain the equation for $E'_{A',B'} : y^2z =$

$x^3 + A'xz^2 + B'z^3$, where $A' = u^4A$ and $B' = u^6B$. Two such curves have the same j-invariant and are said to be *isomorphic over* R.

Let E be an elliptic curve over R. The *set of points* $E(R)$ of E over R is defined by

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

The point $(0 : 1 : 0) \in E(R)$ is called the *zero point* 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 zero. The set $E(R)$ forms a group with O acting as the identity element (see [Len86]).

If R is a field, then

$$E(R) = \{(x, y) \in R^2 : y^2 = x^3 + Ax + B\} \cup \{O\}.$$

We will often call the points $\{(x, y) \in R^2 : y^2 = x^3 + Ax + B\}$ the finite points, and O the point at infinity. If $R = \mathbb{Z}/N\mathbb{Z}$, then

$$\begin{aligned} E(\mathbb{Z}/N\mathbb{Z}) = \{(x, y) \in (\mathbb{Z}/N\mathbb{Z})^2 : y^2 = x^3 + Ax + B\} \cup \\ \{(x : y : z) \in \mathbb{P}^2(\mathbb{Z}/N\mathbb{Z}) : z \notin (\mathbb{Z}/N\mathbb{Z})^* \text{ and } y^2z = x^3 + Axz^2 + Bz^3\}. \end{aligned}$$

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 $3 \cdot \Delta_E$. 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 $\mathbb{F}_p$. There is a natural homomorphism $\eta_p : E(\mathbb{Q}) \to E(\mathbb{F}_p)$ given by

$$\begin{array}{rcll} \eta_p(O) & \mapsto & O & \\ \eta_p((x, y)) & \mapsto & \begin{cases} O & \text{if } p \text{ divides denominator of } x \text{ or } y, \\ (x \pmod p, y \pmod p) & \text{otherwise.} \end{cases} \end{array}$$

Proposition 2 (Group Law Algorithm)**.** *Let E be an elliptic curve given by an equation*

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

Let $P_0 = (x_0, y_0) \in E$. Then

$$-P_0 = (x_0, -y_0).$$

Now let $P_1 + P_2 = P_3$ with $P_i = (x_i, y_i) \in E$.

(a): *If $x_1 = x_2$ and $y_1 = -y_2$, then*

$$P_1 + P_2 = O.$$

(b): *Otherwise, let*

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \qquad \text{if } x_1 \neq x_2$$

$$\lambda = \frac{3x_1^2 + A}{2y_1} \quad \nu = \frac{-x_1^3 + Ax_1 + 2B}{2y_1} \qquad \text{if } x_1 = x_2$$

$P_3 = P_1 + P_2$ is given by

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda x_3 - \nu \end{aligned}$$

When adding points on $E(\mathbb{Z}/N\mathbb{Z})$ for composite N, one has to be aware the point at infinity is not the only point with $z \notin (\mathbb{Z}/N\mathbb{Z})^*$. Lenstra [Len86] gives a method that correctly adds points on $E(\mathbb{Z}/N\mathbb{Z})$.

An endomorphism of E is a rational map $\varphi : E \to E$ such that $\varphi(O) = O$. The set of endomorphisms of an elliptic curve E, denoted by $\mathrm{End}(E)$, 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*, $(m \in \mathbb{Z})$ $[m] : E \to E$.

The ring of endomorphisms of $E(\mathbb{Q})$ is either $\mathbb{Z}$ or an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ where $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. 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 showed that $\#E(\mathbb{F}_p) = p + 1 - a_p$, where $|a_p| \leq 2\sqrt{p}$. We can do even better when E has complex multiplication.

Theorem 3. *(Deuring* [Deu57]*) Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathbb{Q}(\sqrt{-d})$.*

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

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

The structure of $E(\mathbb{F}_p)$ is also well known (see [Len86]).

Proposition 4.

$$E(\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$$

where m divides $\gcd\{p-1, \#E(\mathbb{F}_p)\}$.

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 $3 \cdot \Delta_E$ and $(-d|p) = -1$, then we can predict the order of the curve reduced modulo p; Theorem 3 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 $\mathbb{Q}(\sqrt{-d})$; a point $Q \in E(\mathbb{Q})$ of infinite order. Let $N > 163$ denote the odd number prime to 3 to be tested. We Compute $\left(\frac{-d}{N}\right)$: If it is 1, we can not test, if it is 0, N is composite. If it is -1, we compute $[N+1] \cdot Q \pmod N$: If it is 0, N is Probable Prime, otherwise Composite.

A number which is declared a "probable prime" by the elliptic curve compositeness test for $Q \in E$ is called an elliptic probable prime for $Q \in E$; a composite elliptic probable prime for $Q \in E$ is an elliptic pseudoprime for $Q \in E$. Let $\mathcal{N}(x)$ denote the number of elliptic pseudoprimes up to 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

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

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

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

For some special curves, Gordon [Gor89] showed the number of elliptic pseudoprimes for $P \in E$ is at least $\sqrt{\log x}/\log\log x$.

Elliptic Carmichael Numbers. If N is an elliptic pseudoprime for each rational point of infinite order of E, then N is an *elliptic Carmichael number for* E. An *elliptic Carmichael number for* $\mathbb{Q}(\sqrt{-d})$ 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 [AGP1] use Korselt's criterion to prove there are infinitely many Carmichael numbers. We have a similar criterion for elliptic Carmichael numbers.

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-d})$, and let N be the product of an odd number of distinct primes $p_1, \ldots, p_k$. Suppose $\gcd\{N, 3\Delta_E\} = 1$ and $(-d|p_i) = -1$ for each i , $1 \leq i \leq k$. For any rational point $Q \in E$ of infinite order, $[p_i + 1] \cdot Q = O \pmod{p_i}$ for each i. If we insist that for each i, $p_i + 1|N + 1$, then we will have $[N + 1] \cdot Q = O \pmod{p_i}$ for each i, which implies $[N + 1] \cdot Q = O \pmod{N}$.

Elliptic Carmichael Criterion for $\mathbb{Q}(\sqrt{-d})$*: Suppose the composite number* $N = p_1 \cdots p_k$ *is a product of an odd number of distinct primes. If* $(-d|p_i) = -1$ *and* $(p_i + 1)|(N + 1)$ *for all* i*, then* N *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 $\alpha = 8 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 43 \cdot 67 \cdot 163$. If $N \equiv -1 \pmod \alpha$, then N satisfies the condition $(-d|N) = -1$ for all d listed above.

Elliptic Carmichael Criterion*: Let the composite number* $N = p_1 \cdots p_k$ *be a product of an odd number of distinct primes, and*

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

If $p_i \equiv -1 \pmod \alpha$ *and* $(p_i + 1)|(N + 1)$ *for all* i*, then* N *is an elliptic Carmichael number.*

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 criterion because it is the most convenient congruence class to deal with. We should note that this restriction will not have detrimental effect on our main result.

3. Infinitude of elliptic Carmichael numbers

In [AGP1], 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 [AGP2].

Recently Banks and Pomerance [BP], 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 [BP] had appeared earlier in Ekstrom [Eks99] and was rediscovered in the later paper.

In this section we modify the methods of [BP] 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. 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 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 somewhat weaker forms of Heath-Brown's conjecture. 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]. The smallest value of C for which this is known to hold is $C = 5.2$, an arxiv result of Xylouris.

Definition 7. For integers m, a, b with $m > 0$, $(m,a) = 1$, and $b = \pm 1$, let $C(x; m, a, b)$ denote the number of composite squarefree integers $n \leq x$ 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 [BP], while the case of $b = 1$, $m = \alpha$, and $a = -1$ is of interest for elliptic Carmichael numbers.

In this section we shall prove the following two theorems.

Theorem 8. *If Conjecture 5 holds with $\xi = 1/100$, then for all choices of integers m, a, b with $m > 0$, $(m,a) = 1$, and $b = \pm 1$,*

$$C(x; m, a, b) > x^{1/(30 \log\log\log x)}$$

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

In particular, if Conjecture 5 holds for the value of ξ identified in the proof of Theorem 8, then there are infinitely many integers that are elliptic Carmichael numbers for every imaginary quadratic number field of class number 1.

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 $m > 0$, $(m,a) = 1$, 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. It is likely the number "5/12" in this theorem can be slightly increased by the method of [Har].

3.1. **Some tools.** We begin with a result that shows the existence of numbers with many divisors that are shifted primes.

Proposition 10. *Let m, a, b be integers with $m > 0$, $(m,a) = 1$, and $b \ne 0$. Let B be a positive number with $B < 5/12$. There are positive number 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*

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

Proof. This result is almost identical to Proposition 1.5 in [AGP2], but we give the details for convenience. Let B' be the average of B and $5/12$. According to [AGP1], there is a set $\mathcal{S}_B(x)$ of integers all greater than $\log x$ with the cardinality of the set at most a constant S_B, depending only on B, such that if q, u are integers with $1 < q \le x^{B'}$, $(q,u) = 1$, and q not divisible by any member of $\mathcal{S}_B(x)$, then

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

We may take $x_{B,m} > e^m$, so that no member of $\mathcal{S}_B(x)$ divides m. For each member of $\mathcal{S}_B(x)$ that divides L, remove one prime factor of L so that this divisibility no longer holds. This creates a new number L' where $L' \mid L$, L/L' has at most S_B prime factors, and no member of $\mathcal{S}_B(x)$ divides L'. Since m and L are coprime, 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 $d \mid L'$, $d \le x^B$, $k \le x^{1-B}$, and $p = dk - b$ is a prime with $p \equiv a \pmod m$. Note that for $x_{B,m}$ large enough, we have $dm \le x^{B'}$. The count of d, k pairs is precisely

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

using (10.1).

We wish to show that the number of such pairs d, k where $(L, k) > 1$ 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

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

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

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

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 $l \le x^{2/7}$, getting the majorization

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

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 [AGP1, 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 [AGP1, 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.*

3.2. **Proof of Theorem 8.** Fix integers m, a, b with $m > 0$, $(m, a) = 1$, and $b = \pm 1$. Fix some real number B with $1/3 < B < 5/12$. Let y be a large real parameter and let

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

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. It follows from [Pom80, Theorem 2] that

$$\#\mathcal{L} \ge (1 - 4\log(5/4) + o(1))y^2/\log(y^2) \text{ as } y \to \infty,$$

and so we may assume that y is so large that

$$\#\mathcal{L} \ge y^2/(20\log y). \tag{12.1}$$

Further, by the prime number theorem we have

$$L \le e^{(1+o(1))y^2}, \text{ as } y \to \infty.$$

We would like to apply Proposition 10 with $x = L^{1/B}$. 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)

$$|\mathcal{P}| \ge \frac{c_B}{\varphi(m)\log x}\tau(L) = \frac{c_B 2^{|\mathcal{L}|}}{\varphi(m)\log x} \gg 2^{y^2/(20\log y)}/y^2. \tag{12.2}$$

(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 $(m, L) = 1$, 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 $\xi = 1/100$ and let p_0 be the least prime with $p_0 \equiv a' \pmod M$. Thus,

$$p_0 \ll M^{1+1/(100\log\log M)}.$$

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

$$u \le e^{(1+o(1))y^2/(200B\log y)} \text{ as } y \to \infty,$$

using that m is fixed and $kL \le L^{1/B} \le e^{(1+o(1))y^2/B}$.

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,

$$|\mathcal{P}'| \geq e^{y^2/(29\log y)}. \tag{12.3}$$

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

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

Since $l \in \mathcal{L}$ implies $P(l-1) \leq y$ and $l \leq y^2$, the prime number theorem implies that the lcm of these numbers $l-1$ is at most $e^{(2+o(1))y}$ as $y \to \infty$. Thus, with the above estimate on u and using that m is fixed, we have

$$\lambda(G) \leq e^{(1+o(1))y^2/(200B\log y)} \text{ as } y \to \infty.$$

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

$$D(G) \leq e^{(1+o(1))y^2/(200B\log y)} \text{ as } y \to \infty.$$

Suppose $\mathcal{S}$ is a nonempty subsequence of $\mathcal{P}'$ with product $n_{\mathcal{S}}$ equal to the identity in G. Then n_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 $\epsilon = 1/30$ and let y be so large that

$$D(G) \leq \overline{D}(G) := \left\lfloor e^{(1+\epsilon)y^2/(200B\log y)} \right\rfloor.$$

Let $t = 2\overline{D}(G)$ and let $X = X(y) = e^{(1+\epsilon)ty^2/B}$. We have $\log\log\log X = (2 + o(1))\log y$ as $y \to \infty$. Further, if N is the product of p_0 and at most t primes from $\mathcal{P}'$, then $N \leq x^{t+1+o(1)}$ so that for large values of y, we have $N \leq X$. (Here we have used $x \leq e^{(1/B+o(1))y^2}$.)

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

$$C(X; m, a, b) \geq \binom{|\mathcal{P}'|}{t} \Big/ \binom{|\mathcal{P}'|}{\overline{D}(G))} \geq \left(\frac{|\mathcal{P}'|}{t}\right)^t |\mathcal{P}'|^{-\overline{D}(G)} = |\mathcal{P}'|^{\overline{D}(G)} (2\overline{D}(G))^{-2\overline{D}(G)}.$$

Using our lower bound (12.3) for $|\mathcal{P}'|$, together with $B \geq 1/3$, we have

$$\begin{aligned} C(X; m, a, b) &\geq \exp\left(\overline{D}(G)\left(\frac{y^2}{29\log y} - 2(\log 2 + \log\overline{D}(G))\right)\right) \\ &\geq \exp\left((1+o(1))\overline{D}(G)\frac{y^2}{29\log y}\right) \end{aligned}$$

as $y \to \infty$. Thus, $C(X; m, a, b) \geq X^{(1+o(1))/(2(1+\epsilon)\cdot 29\log y)}$. We conclude that for sufficiently large y we have $C(X; m, a, b) \geq X^{1/(30\log\log\log X)}$. 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.

Next we will consider integers that are v-power free, divisible by α, and prime to L. In Section 3.5, we demonstrate that at least one of these integers, which we will call k, has the additional property that there are many primes of the form $lk - 1$,

where l divides L. A key concept that allows us to find such an integer k will be introduced in Section 3.4. We will set

$$\mathcal{P}' = \{lk - 1 : l \text{ divides } L, lk - 1 \text{ a prime not in } \mathcal{Q}\}.$$

Let $\wp$ denote the least prime in the arithmetic progression -1 modulo Lk and set $L_1 = nL(\gcd\{n, k\})^v$. We want $n = (\wp + 1)/(Lk)$ to be very small compared to Lk, and will use a hypothesis offered in Section 3.6.

Finally, we will find a large number of nonempty subsets $\mathcal{S} \subseteq \mathcal{P}'$ with $\#\mathcal{S}$ even and $\prod_{s\in\mathcal{S}} s \equiv 1 \pmod{L_1}$; each such subset $\mathcal{S}$ will yield an elliptic Carmichael number $N = \wp \prod_{s\in\mathcal{S}} s$. Exactly how many such subsets $\mathcal{S}$ we can find will be discussed in Section 3.3.

3.3. **Group theory lemma.** We will use the next proposition to prove the main theorem.

Proposition 13. *Let G be a finite abelian group and let $t > n = n(G)$, $r > t + n$ be integers. Any sequence of r elements of G contains at least $\binom{r-n}{t}/\binom{r-n}{n}$ distinct subsequences of even length at most $t + n$ and at least $t - n$, whose product is the identity.*

Proof. Let R denote a sequence of r elements of G. By the above proposition, there are at least $\binom{r}{t}/\binom{r}{n}$ distinct subsequences of length at most t and at least $t - n$ whose product is the identity. Suppose all these subsequences are of even length. We have $\dfrac{(r-n)!}{(r-t)!} \geq \dfrac{(r-n-n)!}{(r-t-n)!}$, hence $\binom{r}{t}/\binom{r}{n} \geq \binom{r-n}{t}/\binom{r-n}{n}$.

Now consider the case that some of the above subsequences whose product is the identity are of odd length. Let V denote the smallest such sequence of odd length. Note that the length of V is at most n; for if the length of V was more than n, we could find some proper subsequence V' of V whose product would be the identity, hence $V \backslash V'$ would also have product the identity. Either V' or $V \backslash V'$ must have an odd number of elements, contradicting the minimality of V.

Let R' denote the subsequence of R obtained by removing V from R. There are at least $r - n$ elements in this subsequence, and by the above proposition, there are at least $\binom{r-n}{t}/\binom{r-n}{n}$ subsequences of R' of length at most t and at least $t - n$ whose product is the identity. If there are any such sequences of odd length, adjust them by V to obtain a subsequence of R whose product is the identity. Thus there are at least $\binom{r-n}{t}/\binom{r-n}{n}$ subsequences of R of even length at most $t + n$ and at least $t - n$ whose product is the identity. □

3.4. **Preliminaries regarding the distribution of primes.** Define $\pi(x)$ to be the number of primes $p \leq x$, and $\pi(x, y)$ to be the number of primes $p \leq x$ for which $p - 1$ is free of prime factors exceeding y. We would like to bound $\pi(x, y)$ from below for at least some values of y. In particular, we would like to bound $\pi(x, x^{1-E})$ when $0 < E < 1$. Let $\mathcal{E} \subseteq (0, 1)$ denote the set of numbers E for which there exist numbers $x_1(E), \gamma_1(E) > 0$ such that

$$\pi(x, x^{1-E}) \geq \gamma_1(E)\pi(x) \tag{13.1}$$

for all $x \geq x_1(E)$. Erdös [Erd35] proved that $\mathcal{E}$ is nonempty and conjectured that $\mathcal{E}$ is the open interval $(0,1)$. Currently the best result known [Fri89] is that $(0, 1-(2\sqrt{e})^{-1}) \subseteq \mathcal{E}$.

Let $\pi(y;d,a)$ be the number of primes up to y that belong to the arithmetic progression a mod d. The prime number theorem for arithmetic progressions states that whenever $\gcd\{a,d\} = 1$,

$$\pi(y;d,a) \sim \pi(y)/\varphi(d) \text{ for } y \to \infty, \tag{13.2}$$

where φ is Euler's totient function. We are interested in establishing a bound of the form

$$\pi(y;d,a) \geq \frac{\pi(y)}{2\varphi(d)} \tag{13.3}$$

for d in a wide range, such as $1 \leq d \leq y/c$. The bound (13.3) will be easier to establish if we can disregard some set of 'exceptional' d in the range. For our purposes, the set of exceptional d must not depend on y. We do this by selecting the range for which (13.3) is to hold to be of the form

$$[1, \min\{x^B, y/x^{1-B}\}]$$

for some $0 < B < 1$ with the exception of some d in a set $\mathcal{D}_B(x)$. Further we need a limit on the size of $\mathcal{D}_B(x)$. In [AGP1], we see how this can be done.

Theorem 14. *Let $\mathcal{B}$ be the set of numbers $0 < B < 1$ for which there are bounds $x_2(B)$ and $D(B)$ such that: if $x \geq x_2(B)$, $\gcd\{a,d\} = 1$,*
and $1 \leq d \leq \min\{x^B, y/x^{1-B}\}$, then

$$\pi(y;d,a) \geq \frac{\pi(y)}{2\varphi(d)}$$

for all d not divisible by elements in a set $\mathcal{D}_B(x)$; the set $\mathcal{D}_B(x)$ has at most $D(B)$ elements and all the elements of $\mathcal{D}_B(x)$ exceed $\log x$. We have $(0, 5/12) \subseteq \mathcal{B}$.

3.5. **Prachar's theorem revisited.** Prachar [Pra55] showed that there are infinitely many integers m with more than $2^{c \log m/\log\log m}$ divisors of the form $p-1$, p prime. In [AGP1], the authors modify Prachar's argument. The following is a slight modification of the result in [AGP1].

Theorem 14. *Suppose that B is in the set $\mathcal{B}$ above, and α is the number defined in the criterion for elliptic Carmichael numbers. There exists a number $x_3(B)$ such that if $x \geq x_3(B)$ and L is a squarefree integer relatively prime to α, not divisible by any prime exceeding $x^{(1-B)/2}$, and for which $\sum_{\text{primes } q|L} \frac{1}{q} \leq \frac{1-B}{32}$, then there is a positive integer $k \leq \alpha x^{1-B}$, $\alpha | k$, with $\gcd\{k, L\} = 1$, such that*

$$\#\{l|L : lk - 1 \leq x, lk - 1 \text{ is prime}\} \geq \frac{2^{-D_B-2}}{\log x} \# \left\{ l|L : 1 \leq l \leq \frac{x^B}{\alpha} \right\}.$$

Proof. For each $d \in \mathcal{D}_B(x)$ which divides L, we divide some prime factor of d out from L, so as to obtain a number L' which is not divisible by any number in $\mathcal{D}_B(x)$. Thus $\omega(L') \geq \omega(L) - D_B$, where $\omega(m)$ is the number of distinct prime factors of m, and

$$\#\{l|L' : 1 \leq l \leq y\} \geq 2^{-D_B} \#\{l|L : 1 \leq l \leq y\} \tag{14.1}$$

for any $y \geq 1$. To see this, think of a divisor l' of L' as corresponding to a divisor l of L if and only if l' divides l and l/l' divides L/L'. So if $l \leq y$ then the corresponding l' is $\leq y$. Moreover, for any divisor l' of L', the number of divisors l of L which correspond to l' is at most the number of divisors of L/L', which is at most 2^{D_B}.

¿From (13.3) we see that, for each divisor l of L' with $1 \leq l \leq \frac{x^B}{\alpha}$, we have

$$\pi(\alpha l x^{1-B}; \alpha l, -1) \geq \frac{\pi(\alpha l x^{1-B})}{2\varphi(\alpha l)} \geq \frac{\alpha l x^{1-B}}{2\varphi(\alpha l)\log(\alpha l x^{1-B})} \geq \frac{\alpha l x^{1-B}}{2\varphi(\alpha l)\log x}, \tag{14.2}$$

since $\pi(y) \geq y/\log y$ for all $y \geq 17$ (see [RS62]). Furthermore, since any prime factor q of L is at most $x^{(1-B)/2}$ (by hypothesis), we can use Montgomery and Vaughan's explicit version of the Brun-Titchmarsh theorem [MV73], to get

$$\begin{aligned}\pi(\alpha l x^{1-B}; \alpha l q, -1) &\leq \frac{2\alpha l x^{1-B}}{\varphi(\alpha l q)\log(x^{1-B}/q)} \leq \frac{4}{\varphi(q)(1-B)}\frac{\alpha l x^{1-B}}{\varphi(\alpha l)\log x} \\ &\leq \frac{8}{q(1-B)}\frac{\alpha l x^{1-B}}{\varphi(\alpha l)\log x}.\end{aligned}$$

Therefore, by (14.2), the number of primes $p \leq \alpha l x^{1-B}$ with $p \equiv -1 \pmod{l}$, $\gcd\{(p+1)/l, L\} = 1$ and $\alpha | (p+1)/l$ is at least

$$\pi(\alpha l x^{1-B}; \alpha l, -1) - \sum_{\text{primes } q | L} \pi(\alpha l x^{1-B}; \alpha l q, -1) \geq$$
$$\left(\frac{1}{2} - \frac{8}{1-B}\sum_{\text{primes } q|L}\frac{1}{q}\right)\frac{\alpha l x^{1-B}}{\varphi(\alpha l)\log x} \geq \frac{x^{1-B}}{4\log x}.$$

Thus we have at least

$$\frac{x^{1-B}}{4\log x}\#\left\{l | L' : 1 \leq l \leq \frac{x^B}{\alpha}\right\}$$

pairs (p, l) where $p \leq \alpha l x^{1-B}$ is prime, $p \equiv -1 \pmod{l}$, $\gcd\{(p+1)/l, L\} = 1$, $\alpha | (p+1)/l$, $l | L'$, and $1 \leq l \leq \frac{x^B}{\alpha}$. Each such pair (p, l) corresponds to an integer $(p+1)/l \leq \alpha x^{1-B}$ that is divisible by α and coprime to L. Thus there is at least one integer $k \leq \alpha x^{1-B}$ with $\alpha | k$ and $\gcd\{k, L\} = 1$ such that k has at least

$$\frac{1}{4\log x}\#\left\{l | L' : 1 \leq l \leq \frac{x^B}{\alpha}\right\}$$

representations as $(p+1)/l$ with (p, l) as above. Thus for this integer k we have

$$\#\{l | L : lk - 1 \leq x, lk - 1 \text{ is prime}\} \geq \frac{1}{4\log x}\#\left\{l | L' : 1 \leq l \leq \frac{x^B}{\alpha}\right\}$$

and the theorem now follows from (14.1). □

Theorem 15. *Let B be in the set $\mathcal{B}$ above, E be in the set $\mathcal{E}$ above, L as in Theorem 14 above, α the number defined in the criterion for elliptic Carmichael numbers, and $\epsilon > 0$. Set $\delta = \epsilon/(4B(1-E))$, and $x = \exp(y^{1+\delta})$. For y large enough, there is a positive $y^{\delta/4}$th power free integer $k \leq \alpha x^{1-B}$, $\alpha | k$, with $(k, L) = 1$, such that*

$$\#\{l | L : lk - 1 \leq x, lk - 1 \text{ is prime}\} \geq \frac{2^{-D_B-3}}{\log x}\#\left\{l | L : 1 \leq l \leq \frac{x^B}{\alpha}\right\}.$$

Proof. Let L' be as in the proof of Theorem 14. From the proof of Theorem 14, we have at least

$$\frac{x^{1-B}}{4\log x}\#\left\{l|L' : 1 \le l \le \frac{x^B}{\alpha}\right\}$$

pairs (p,l) where $p \le \alpha l x^{1-B}$ is prime, $p \equiv -1 \pmod{l}$, $\gcd\{(p+1)/l, L\} = 1$, $\alpha|(p+1)/l$, $l|L'$, and $1 \le l \le \frac{x^B}{\alpha}$. Each such pair (p,l) corresponds to an integer $(p+1)/l \le \alpha x^{1-B}$ that is divisible by α and coprime to L.

Next we will estimate the number of multiples of α less than αx^{1-B} which are not $y^{\delta/4}$th power free. If $p^{y^{\delta/4}}$ divides $\alpha \cdot r$, then $p^{y^{\delta/4}-3}$ divides r. There are $x^{1-B}/p^{y^{\delta/4}-3}$ numbers less than x^{1-B} that are divisible by $p^{y^{\delta/4}-3}$. Thus there are at most

$$\begin{aligned}\sum_{\text{primes } p} \frac{x^{1-B}}{p^{y^{\delta/4}-3}} &\le x^{1-B}\left[\frac{1}{2^{y^{\delta/4}-3}} + \int_2^\infty \frac{1}{z^{y^{\delta/4}-3}}dz\right] \\ &\le x^{1-B}\left[\frac{1}{2^{y^{\delta/4}-3}} + \frac{1}{(y^{\delta/4}-4)(2^{y^{\delta/4}-4})}\right] \\ &\le \frac{x^{1-B}}{2^{y^{\delta/4}-4}} \le \frac{x^{1-B}}{16y^{1+\delta}} = \frac{x^{1-B}}{16\log x}\end{aligned}$$

multiples of α less than αx^{1-B} which are not $y^{\delta/4}$th power free. Each of these multiples of α corresponds to at most $\#\{l|L' : 1 \le l \le \frac{x^B}{\alpha}\}$ pairs (p,l), so there are

$$\left[\frac{x^{1-B}}{4\log x} - \frac{x^{1-B}}{16\log x}\right]\#\left\{l|L' : 1 \le l \le \frac{x^B}{\alpha}\right\}$$

pairs (p,l) such that $p \le \alpha l x^{1-B}$ is prime, $p \equiv -1 \pmod{l}$, $\gcd\{(p+1)/l, L\} = 1$, $\alpha|(p+1)/l$, $(p+1)/l$ is $y^{\delta/4}$th power free, $l|L'$, and $1 \le l \le \frac{x^B}{\alpha}$.

Thus there is at least one $y^{\delta/4}$th power free integer $k \le \alpha x^{1-B}$ with $\alpha|k$, $\gcd\{k, L\} = 1$, such that k has at least

$$\frac{1}{8\log x}\#\left\{l|L' : 1 \le l \le \frac{x^B}{\alpha}\right\}$$

representations as $(p+1)/l$ with (p,l) as above. Thus for this integer k we have

$$\#\{l|L : lk - 1 \le x, lk - 1 \text{ is prime}\} \ge \frac{1}{8\log x}\#\left\{l|L' : 1 \le l \le \frac{x^B}{\alpha}\right\}$$

and the theorem now follows from (14.1). □

3.6. **Least prime in an arithmetic progression.** For coprime integers a and q, $q > 0$, we define $p(q,a)$ to be the least prime p that is greater than q and congruent to $a \bmod q$. Let

$$p(q) = \max\{p(q,a) : \ 1 \le a \le q-1, \ \gcd\{a,q\} = 1\}.$$

Linnik [Lin44] showed that there exists an absolute constant c for which $p(q) \ll q^c$, and Heath-Brown [HB92] demonstrated that the c is at most $11/2$. Titchmarsh [Tit30] showed, under the assumption of the Extended Riemann hypothesis, that $p(q) \ll q^2(\log q)^4$. Uchiyama [Uch72] proved that if $A > 3$ is a real number and $0 < \varepsilon < A - 3$, then for almost all positive integers q

$$p(q,a) < \varphi(q)\log^A(q)$$

except for possibly $\varphi(q)\cdot(\log q)^{-\varepsilon}$ values of a with $(a,q)=1$, $1\le a<q$. Erdös [Erd49] proved that if $c_1>0$ is any constant, then there exists a constant c_2 depending on c_1 such that for $c_2\varphi(q)$ values of a

$$p(q,a)<c_1\varphi(q)\log q.$$

Granville [Gra89] showed that the density of integers $q>0$ for which $p(q,a)\le qf(q)$ is one provided $f(q)\ge q^{1-o(1)}$.

Heath-Brown [HB78] conjectured that $p(q)\ll q(\log q)^2$, and Wagstaff [Wag79] gave heuristic arguments which support this; more precisely, McCurley noted that an adaptation of his heuristic arguments in [McC86] suggests that

$$\overline{\lim_{q\to\infty}}\frac{p(q)}{\phi(q)\log^2 q}=2$$

(see also [MSC95, pages 278–280] and [BS96]).

We will use the following hypothesis, which is much weaker than the above conjecture.

Hypothesis 3.6_E. *For q large enough*

$$p(q,-1)\le q[\exp\{(\log q)^{1-E}\}],$$

where $E\in\mathcal{E}$ and $\mathcal{E}$ was defined in Section 3.4.

4. Lower Bound for Elliptic Carmichael Numbers

Let $\mathcal{T}(x)$ denote the number of elliptic Carmichael numbers up to x.

Theorem 17. *If Hypothesis 3.6_E holds, then for each $B\in\mathcal{B}$ and $\eta>0$, there is a number $x_4(E,B,\eta)$, such that whenever $x\ge x_4(E,B,\eta)$, we have $\mathcal{T}(x)\ge x^{EB-\eta}$.*

Remark. It is known that $\mathcal{E}$ contains $(0,1-(2\sqrt{e})^{-1})$. Taking E close to $1-(2\sqrt{e})^{-1}$ gives a large lower bound, $\mathcal{T}(x)\ge x^{\frac{2}{7}}$, for large enough x. However, any value of $E\in(0,1-(2\sqrt{e})^{-1})$ is enough to give infinitely many elliptic Carmichael numbers. In particular, there exist infinitely many elliptic Carmichael numbers under the condition that $p(q,-1)\le q[\exp\{(\log q)^{1-\varepsilon}\}]$.

Proof. Let $E\in\mathcal{E}$, $B\in\mathcal{B}$, $\epsilon>0$. We may assume $\epsilon<EB$. Set $\theta=(1-E)^{-1}$ and let $y>2$ be a parameter to be made sufficiently large eventually. Denote by $\mathcal{Q}$ the set of primes $q\in(y^\theta/\log y,y^\theta]$ for which $q-1$ is free of prime factors exceeding y. By (13.1) and the Prime Number Theorem,

$$\begin{aligned}|\mathcal{Q}| &\ge \gamma_1(E)\frac{y^\theta}{\log(y^\theta)}-\frac{2\frac{y^\theta}{\log y}}{\log(\frac{y^\theta}{\log y})}\\ &= \gamma_1(E)\frac{y^\theta}{\log y^\theta}-\frac{1}{2}\gamma_1(E)\frac{y^\theta}{\log y^\theta}\left(\frac{4\theta}{\gamma_1(E)(\theta\log y-\log\log y)}\right).\end{aligned}$$

Since $4\theta[\gamma_1(E)(\theta\log y-\log\log y)]^{-1}\le 1$ for large enough y, we have

$$|\mathcal{Q}|\ge\frac{1}{2}\gamma_1(E)\frac{y^\theta}{\log(y^\theta)} \tag{17.1}$$

for all sufficiently large y.

Let L be the product of the primes $q \in \mathcal{Q}$. Then

$$\sum_{\text{primes } q|L} \frac{1}{q} \;\le\; \sum_{\frac{y^\theta}{\log y}<q<y^\theta} \frac{1}{q} \;\le\; \log\log(y^\theta) - \log\log(\tfrac{y^\theta}{\log y}) + O(1/[\log(\tfrac{y^\theta}{\log y})])$$

$$\le \log\left(\frac{1}{1-\frac{\log\log y}{\theta\log y}}\right) + O(1/[\log(\tfrac{y^\theta}{\log y})]) \;\le\; 2\frac{\log\log y}{\theta\log y} \;\le\; \frac{1-B}{32} \tag{17.2}$$

for sufficiently large y.

Let $\delta = \epsilon\theta/(4B)$ and let $x = e^{y^{1+\delta}}$. By (17.2) we may apply Theorem 15 with B, E, x, L, δ. Thus for all sufficiently large values of y, there is a $y^{\delta/4}$th powerfree positive integer $k \le \alpha x^{1-B}$ coprime to L, divisible by $\alpha = 16,488,700,536 = 3\cdot 7\cdot 8\cdot 11\cdot 19\cdot 43\cdot 67\cdot 163$, for which the set $\mathcal{P}$ of primes $p \le x$ with $p = lk-1$ for some divisor l of L, satisfies

$$|\mathcal{P}| \ge \frac{2^{-D_B-3}}{\log x} \#\left\{l|L : 1 \le l \le \frac{x^B}{\alpha}\right\}. \tag{17.3}$$

Since the prime factors of L are all less than y^θ, the product of any

$$u := \left[\log_{y^\theta}\left(\frac{x^B}{\alpha}\right)\right] = \left[\frac{B\log x - \log(\alpha)}{\theta\log y}\right]$$

distinct prime factors of L, is a divisor l of L with $l \le \frac{x^B}{\alpha}$. Thus

$$\#\left\{l|L : 1 \le l \le \frac{x^B}{\alpha}\right\} \ge \binom{\omega(L)}{u} \ge \left(\frac{\omega(L)}{u}\right)^u \tag{17.4}$$

where $\omega(L)$ denotes the number of distinct prime factors of L. By (17.1) we get

$$\left(\frac{\omega(L)}{u}\right)^u \ge \left(\frac{\gamma_1(E)y^\theta}{2B\log x}\right)^u = \left(\frac{\gamma_1(E)}{2B}y^{\theta-1-\delta}\right)^u,$$

which with (17.3) and (17.4) gives

$$\begin{aligned}
|\mathcal{P}| &\ge \frac{2^{-D_B-3}}{\log x}\left(\frac{\gamma_1(E)}{2B}y^{\theta-1-\delta}\right)^{\left[\frac{B\log x-\log(\alpha)}{\theta\log y}\right]} \\
&\ge \frac{2^{-D_B-3}}{\log x}\left[\left(\left(\tfrac{\gamma_1(E)}{2B}\right)^{(\theta-1-\delta)^{-1}} y\right)^{\left[\frac{\log x-\log(\alpha^{1/B})}{\log y}\right]}\right]^{(\theta-1-\delta)[B/\theta]} \\
&\ge \frac{2^{-D_B-3}}{\log x}\left[\left(\frac{x}{\alpha^{1/B}}\right)^{1-\epsilon/27}\right]^{(\theta-1-\delta)B/\theta},
\end{aligned}$$

for large enough y. Note that $(\theta-1-\delta)B/\theta = EB - \epsilon/4$, so

$$|\mathcal{P}| \ge \frac{2^{-D_B-3}}{\log x}\left(x^{1-\epsilon/24}\right)^{EB-\epsilon/4} \ge \frac{2^{-D_B-3}}{\log x}x^{EB-7\epsilon/24} \ge x^{EB-\epsilon/3}. \tag{17.5}$$

for all sufficiently large values of y.

By Hypothesis 3.6_E, there exists $n \le \exp[(\log(kL))^{1-E}]$ such that $\wp = nLk-1$ is prime. By the Prime Number Theorem

$$\log L \le |\mathcal{Q}|\log(y^\theta) \le \pi(y^\theta)\log(y^\theta) \le 2y^\theta, \tag{17.6}$$

for all large y. Since $k \le \alpha x^{1-B}$,

$$\log k \le \log\alpha + (1-B)\log x \le \log\alpha + (1-B)y^{1+\delta} \le y^\theta.$$

Thus

$$n \le \exp[(3y^\theta)^{1-E}] \le e^{3y} \tag{17.7}$$

for large enough y. Now $\lambda(L)$ is the least common multiple of the numbers $q-1$ for those primes q that divide L. Since each such $q-1$ is free of prime factors exceeding y, we know that if the prime power p^a divides $\lambda(L)$ then $p \le y$ and $p^a \le y^\theta$ (since p^a divides one of $q-1 \le y^\theta$). Thus if we let p^{a_p} be the largest power of p with $p^{a_p} \le y^\theta$, then by the Prime Number Theorem

$$\lambda(L) \le \prod_{p \le y} p^{a_p} \le \prod_{p \le y} y^\theta \le (y^\theta)^{2\frac{y}{\log y}} \le e^{2\theta y} \tag{17.8}$$

for all large y.

Let $L_1 = nL \cdot (\gcd\{n,k\})^{y^{\delta/4}}$ and let G be the group $(\mathbb{Z}/L_1\mathbb{Z})^*$. We conclude from Theorem **??**, (17.6), (17.7), and (17.8) that

$$\begin{aligned} n(G) &< n^{y^{\delta/4}+1}\lambda(L)(1+\log\varphi(L_1)) \\ &\le e^{3y(y^{\delta/4}+1)}e^{2\theta y}(1+3y^{1+\delta/4}+3y+2y^\theta) \ \le \ e^{5y^{1+\delta/4}} \end{aligned} \tag{17.9}$$

for all large y.

Set $\mathcal{P}' = \mathcal{P}\backslash(\mathcal{Q} \cup \{\text{prime factors of } n\})$. Since $|\mathcal{Q}| < y^\theta$, and $n \le e^{3y}$ we have by (17.5) that

$$|\mathcal{P}'| \ge x^{EB-\epsilon/2} \tag{17.10}$$

for all sufficiently large values of y.

We may view $\mathcal{P}'$ as a subset of the group $G = (\mathbb{Z}/L_1\mathbb{Z})^*$ by considering the residue class of each $p \in \mathcal{P}'$ modulo L_1. If $\mathcal{S}$ is a nonempty subset of $\mathcal{P}'$, denote the product of the elements of $\mathcal{S}$ by $\Pi(\mathcal{S})$. We claim that if $\mathcal{S}$ contains an even number of elements and if $\Pi(\mathcal{S})$ is congruent to 1 modulo L_1 then $\wp\Pi(\mathcal{S})$ satisfies the elliptic Carmichael criterion, making it an elliptic Carmichael number.

Every member of $\mathcal{P}'$ is congruent to -1 modulo k, so $\Pi(S) \equiv 1 \pmod k$. The product $\Pi(\mathcal{S})$ is also congruent to 1 modulo L_1, where $L_1 = nL(\gcd\{n,k\})^{y^{\delta/4}}$. Since k is $y^{\delta/4}$th power-free, $\Pi(\mathcal{S}) \equiv 1 \pmod{nLk}$. The prime $\wp$ is equal to $nLk-1$ which implies both

$$N = \wp\Pi(\mathcal{S}) \equiv -1 \pmod{nLk}, \tag{17.11}$$

and $\wp+1|N+1$. All primes $p \in \mathcal{P}'$ have the form $p = lk-1$ for some $l|L$; therefore $p+1|kL$, and by (17.11), $p+1|N+1$. Thus $N = \wp\Pi(S)$ is a squarefree number with $p+1|N+1$ for all primes p that divide N. Since $\alpha|k$, each prime that divides N is congruent to -1 modulo α. As a result, the composite N satisfies the elliptic Carmichael criterion.

Let $t = e^{y^{1+\delta/2}}$. Then, by Proposition 13, we see that the number of distinct products $\Pi(\mathcal{S}) \equiv 1 \pmod{L_1}$, where $\mathcal{S} \subset \mathcal{P}'$ has an even number of elements, and $|\mathcal{S}| \le t + n(G)$, is at least

$$\begin{aligned} R &:= \binom{\lfloor|\mathcal{P}'|-n(G)\rfloor}{\lfloor t\rfloor} \Big/ \binom{\lfloor|\mathcal{P}'|-n(G)\rfloor}{n(G)} \ge \frac{\left(\frac{\lfloor|\mathcal{P}'|-n(G)\rfloor}{\lfloor t\rfloor}\right)^{\lfloor t\rfloor}}{[|\mathcal{P}'|-n(G)]^{n(G)}} \\ &\ge \lfloor|\mathcal{P}'|-n(G)\rfloor^{\lfloor t\rfloor-n(G)}\lfloor t\rfloor^{-\lfloor t\rfloor}. \end{aligned}$$

By (17.9) and (17.10) we get

$$R \geq (x^{EB-3\epsilon/4})^{t-n(G)} \lfloor t \rfloor^{-\lfloor t \rfloor}.$$

Note that for large enough y,

$$t = e^{y^{1+\delta/2}} \leq \left(e^{y^{1+\delta}}\right)^{(EB-3\epsilon/4)\epsilon/8} \quad \text{and} \quad n(G) \leq \left(e^{y^{1+\delta/2}}\right)\epsilon/8 = t\epsilon/8.$$

Thus

$$R \geq (x^{EB-3\epsilon/4})^{t-t\epsilon/8}(x^{EB-3\epsilon/4})^{-t\epsilon/8} \geq (x^{EB-3\epsilon/4})^{t(1-\epsilon/4)} \geq x^{t(EB-\epsilon)},$$

for all sufficiently large values of y.

We know each $p \in \mathcal{P}$ is less than or equal to x, and

$$\wp \leq nLk \leq e^{3y}e^{2y^{\theta}}\alpha x^{1-B} \leq x^{t\epsilon/2}$$

by (17.6) and (17.7). So each elliptic Carmichael number $\wp\Pi(\mathcal{S})$ so formed is such that $\wp\Pi(\mathcal{S}) \leq x^{t+n(G)+t\epsilon/2} \leq x^{t(1+\epsilon)}$. Thus for $X = x^{t(1+\epsilon)}$ we have $\mathcal{T}(X) \geq X^{\frac{EB}{1+\epsilon}-\epsilon} \geq X^{EB-\eta}$ for all sufficiently large y. But $X = \exp((1+\epsilon)y^{l+\delta}\exp(y^{l+\delta/2}))$, so that $\mathcal{T}(X) \geq X^{EB-\eta}$, for all sufficiently large values of X. Since y can be uniquely determined from X, this completes the proof. □

5. Complements

For many examples, numerical issues and tables, 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 square-free, (2) For any $\epsilon > 0$, the number of elliptic Carmichael numbers up to x which have exactly k distinct prime factors is at most $x^{(2k-1)/(2k)+\epsilon}$ for large enough x.

The Lucas-Fermat compositeness test has a strong version: If $a^{(N-1)/2^k} \equiv 1 \pmod N$, 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 $[(N+1)/2^k]Q \equiv O \pmod N$, but $[(N+1)/2^{k+1}]Q \pmod N \not\equiv$ 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.

References

[AGP1] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Annals of Mathematics*, 139(3):703–722, 1994. (document), 1, 1, 2.1, 2.3, 3, 3.1, 3.1, 3.1, 3.4, 3.5

[AGP2] 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. 3, 3.1

[AM93] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993. 1

[BS96] E. Bach and J. Shallit. *Algorithmic Number Theory*. Foundations of Computing. MIT Press, Cambridge, Mass., 1996. 3.6

[BM90] R. Balasubramanian and M. R. Murty. Elliptic pseudoprimes. II. In *Seminaire de Theorie des Nombres, Paris 1988-1989*, number 91 in Progr. Math., pages 13–25, Boston, MA, 1990. Birkhauser Boston. 2.3

[BP] W. D. Banks and C. Pomerance. On Carmichael numbers in arithmetic progressions *J. Australian Math. Soc.*, 28:313–321 ,2010. 3, 3

[Car10] R. D. Carmichael. Note on a new number theory function. *Bull. Amer. Math. Soc.*, 16:232–238, 1910. 1

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

[Che39] J. Chernick. On Fermat's simple theorem. *Bull. Amer. Math. Soc.*, 45:269–274, 1939. 5

[Deu57] M. Deuring. Die zetafunktion einer algebraischen kurve vom geschlechte eins. *Nachrichten Akad. Wiss. Gottingen*, pages 55–80, 1957. 3

[Eks99] A. Ekstrom. On the infinitude of Elliptic Carmichael Numbers. Ph. D. thesis, University of Arizona (1999). (document), 3, 5

[Erd35] P. Erdos. On the normal number of prime factors of $p-1$ and some other related problems concerning Euler's φ-function. *Quart. J. Math. (Oxford Ser.)*, 6:205–213, 1935. 3.4

[Erd49] P. Erdos. On some applications of Brun's method. *Acta Univ. Szeged. Sect. Sci. Math.*, 3:57–63, 1949. 3.6

[Fri89] J. B. Friedlander. Shifted primes without large prime factors. In R. A. Mollin, editor, *Number Theory and Applications*, pages 393–401, Kluwer, NATO ASI, 1989. 3.4

[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. 1

[Gor87] D. M. Gordon. Pseudoprimes on elliptic curves. *Proc. Internat. Number Theory Conference, Laval*, pages 291–305, 1987. 1, 2.3, 5

[Gor89] D. M. Gordon. On the number of elliptic pseudoprimes. *Mathematics of Computation*, 52(185):231–245, January 1989. 1, 2.3

[GP91] D. M. Gordon and C. Pomerance. The distribution of Lucas and elliptic pseudoprimes. *Mathematics of Computation*, 57(196):825–838, October 1991. 2.3

[Gra89] A. Granville. Least primes in arithmetic progressions. In J. M. De Koninck and C. Levesque, editors, *Theorie des nombres/Number Theory*, pages 306–321. de Gruyter, New York, 1989. 3.6

[Har] G. Harman. Watt's mean value theorem and Carmichael numbers. *Int. J. Number Theory*, 4:241–248, 2008. 3

[HB78] D. R. Heath-Brown. Almost-primes in arithmetic progressions and short intervals. *Math. Proc. Camb. Phil. Soc.*, 83:357–375, 1978. 3.6

[HB92] D. R. Heath-Brown. Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression. *Proc. Lond. Math. Soc.*, 64:265–338, 1992. 3.6

[Kor99] A. Korselt. Problèm chinois. *L'intermédiaire des Mathématiciens*, 6:142–143, 1899. 2.1

[Leh76] D. H. Lehmer. Strong Carmichael numbers. *J. Austral. Math. Soc.*, 21:508–510, 1976. 5

[Len86] H. W. Lenstra, Jr. Elliptic curves and number-theoretic algorithms. *Proceedings of the International Congress of Mathematicians, Berkeley, California, USA, 1986*, pages 99–120, 1986. 1, 2.2, 2.2, 2.2, 2.2

[Len87] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, 126(3):649–673, 1987. 1

[Lin44] U. V. Linnik. On the least prime in an arithmetic progression II. *Rec. Math. [Mat. Sb.]*, 15(57):347–368, 1944. 3, 3.6

[McC86] K. S. McCurley. The least r-free number in an arithmetic progression. *Trans. Amer. Math. Soc.*, 293:467–475, 1986. 3.6

[Mes90] R. Meshulam. An uncertainty inequality and zero subsums. *Disc. Math.*, 84:197–200, 1990.

[MM89] M. R. Murty and I. Miyamoto. Elliptic pseudoprimes. *Mathematics of Computation*, 53(187):415–430, 1989. 2.3

[MSC95] D. S. Mitrinovic, J. Sandor, and B. Crstici. *Handbook of Number Theory*. Mathematics and its Applications. Kluwer, 1995. 3.6

[MV73] H. L. Montgomery and R. C. Vaughan. The large sieve. *Mathematika*, 20(40):119–134, December 1973. 3.1, 3.5

[Pom80] C. Pomerance. Popular values of Euler's funcion. *Mathematika*, 27:84–89, 1980. 3.2

[Pom81] C. Pomerance. On the distribution of pseudoprimes. *Mathematics of Computation*, 37(156):587–593, October 1981. 2.1

[Pra55] K. Prachar. Uber die anzahl der teiler einer naturlichen zahl, welche die form $p-1$ haben. *Monatsh. Math.*, 59:91–97, 1955. 3.5

[PSW80] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr. The pseudoprimes to $25 \cdot 10^9$. *Mathematics of Computation*, 35(151):1003–1026, July 1980. 2.1

[RS62] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962. 3.5

[Sil86] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986. 2.2

[Tit30] E. C. Titchmarsh. A divisor problem. *Rend. Circ. Mat. Palerno*, 54:414–429, 1930. 3.6

[Uch72] S. Uchiyama. An application of the large sieve. *Proc. Jap. Acad.*, 48:67–69, 1972. 3.6

[vEBK69] P. van Emde Boas and D. Kruyswijk. A combinatorial problem on finite abelian groups III. In *Math. Centrum*. Amsterdam, 1969.

[Wag79] S. S. Wagstaff Jr. Greatest of the least primes in arithmetic progressions having a given modulus. *Math. Comp.*, 33:1073–1080, 1979. 3.6

[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. 1