ON ELLIPTIC CARMICHAEL NUMBERS IN ARITHMETIC PROGRESSIONS

Nick Egbert[1]
Department of Mathematics, Purdue University, West Lafayette, Indiana
egbertn@purdue.edu

Received: 3/2/21, Accepted: 12/21/21, Published: 1/7/22

Abstract

In 1987, Dan Gordon defined the notion of an elliptic Carmichael number as a composite integer n which satisfies a Fermat-like criterion on elliptic curves with complex multiplication. More recently, in 2018, Thomas Wright showed that there are infinitely such numbers. We build off the work of Wright to prove that there are infinitely many elliptic Carmichael numbers of the form $a \pmod M$ for a certain M, using an improved lower bound due to Carl Pomerance. We then apply this result to comment on the infinitude of strong pseudoprimes and strong Lucas pseudoprimes.

1. Introduction

1.1. Carmichael Numbers

The Fermat primality test is one of the simplest primality tests. It is derived from Fermat's little theorem, which states that for a prime p and an integer a with $\gcd(a, p) = 1$, one has $a^{p-1} \equiv 1 \pmod p$. It is well-known that the converse of Fermat's little theorem is false. A composite number n satisfying $a^{n-1} \equiv 1 \pmod n$ is called a *pseudoprime to base* a, or $\mathrm{psp}(a)$.

Suppose $n > 2$ is an odd integer, and write $n - 1 = 2^f d$, where f, d are positive integers and $2 \nmid d$. If either $a^d \equiv 1 \pmod n$ or $a^{d \cdot 2^e} \equiv -1 \pmod n$ for some e with $0 \leq e < f$, then we call n a *strong probable prime to base* a. If n is composite, then we call n a *strong pseudoprime to base* a.

More generally, a *Carmichael number* is a composite number n which satisfies the conclusion to Fermat's little theorem for every integer a coprime to n. That is,

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

for all a with $\gcd(a, n) = 1$. There is no analogue of Carmichael numbers for strong

[1]This work is based on part of a PhD thesis at Purdue University under the supervision of Samuel Wagstaff.

pseudoprimes. In 1899 Korselt gave an equivalent characterization of Carmichael numbers that can be more easily tested.

Theorem 1 (Korselt's criterion)**.** *A composite number n is a Carmichael number if and only if n is squarefree and for each prime divisor p of n one has $p-1 \mid n-1$.*

In their famous 1994 paper, Alford, Granville and Pomerance [2] used this characterization to show that there are infinitely many Carmichael numbers. A natural next question is to ask whether there are infinitely many Carmichael numbers in various arithmetic progressions. Wright [18] proved this to be the case in 2013 after progress had been made on this problem by Banks and Pomerance [6] and Matomäki [12].

An analogous story can be told in the case of so-called *elliptic Carmichael numbers*. Dan Gordon [10] defined the notion of an elliptic Carmichael number in 1987 when he devised a primality test in the spirit of the Fermat test using the arithmetic of elliptic curves with complex multiplication. Following his earlier paper, Wright [19] proved in 2018 that there are infinitely many elliptic Carmichael numbers. We finish the story in proving the following theorem.

Theorem 2. *Let $\mathcal{N}_{M,a}(X)$ be the number of elliptic Carmichael numbers up to X congruent to a modulo M. Then $\mathcal{N}_{M,a}(X) \geq X^{1/(6\log\log\log X)}$ for all sufficiently large X depending on the choice of M.*

1.2. Organization of this Chapter

In Section 2, we give the basic background material on elliptic curves with complex multiplication and elliptic Carmichael numbers. We then recall the definitions of pseudoprimes related to Lucas sequences first given in Baillie-Wagstaff [4] and Baillie-Fiori-Wagstaff [3]. In Section 3, we modify the arguments of Wright [18, 19] and Pomerance [15], and then apply them to show that there are infinitely many elliptic Carmichael numbers in some arithmetic progressions. Finally, in Section 4, we show that there are infinitely many elliptic Carmichael numbers which are also (strong) Lucas pseudoprimes.

2. Preliminaries

2.1. Elliptic Curves

We recall some basic theory of elliptic curves needed for this discussion. The standard reference here is Silverman [17]. For our purposes, an elliptic curve E over $\mathbb{Q}$ is a smooth projective curve that satisfies the short Weierstrass equation

$$E : Y^2 = X^3 + aX + b,$$

with $a, b \in \mathbb{Q}$ and nonzero discriminant $\Delta = 4a^3 + 27b^2$. The set of rational points of E plus the point at infinity $\mathcal{O}$ form an additive group $E(\mathbb{Q})$.

We may then consider the endomorphism ring of $E(\mathbb{Q})$. Using the group law, for an integer n and a point $P \in E$, one clearly has $nP \in E$, so that $\mathbb{Z} \subset \operatorname{End} E$. If $\operatorname{End} E$ is strictly larger than $\mathbb{Z}$, then we say that E has complex multiplication (CM), or that E is a CM-elliptic curve. In this case, $\operatorname{End} E$ is isomorphic to an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ with class number 1, and we say that E has complex multiplication by $\mathbb{Q}(\sqrt{-d})$. By the Stark-Heegner theorem, the values of d for which $\mathbb{Q}(\sqrt{-d})$ has class number 1 are precisely $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

2.2. Elliptic Carmichael Numbers

With this, we can consider the following primality test due to Dan Gordon [10]. For an elliptic curve E with complex multiplication by $\mathbb{Q}(\sqrt{-d})$, let $P \in E(\mathbb{Q})$ be a rational point of infinite order on E. Moreover, let n be a natural number such that $\gcd(n, 6\Delta) = 1$ and $(-d \,|\, n) = -1$, where $(-d \,|\, n)$ denotes the Jacobi symbol. If n is prime, then

$$[n+1]P \equiv \mathcal{O} \pmod{n}.$$

If the primality of n is not known, and n satisfies the above congruence, then n is a probable prime by Gordon's primality test. The setup here is analogous to that of Carmichael numbers. In this way, we can define elliptic Carmichael numbers.

Definition 1. Let n be a composite natural number. Given a CM-elliptic curve E, if n satisfies the Gordon primality test then n is called an *elliptic Carmichael number for* E. If n is an E-elliptic Carmichael number for every CM-elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-d})$ where $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$, then n is an *elliptic Carmichael number*.

Note that such numbers exist, although they are relatively rare. Ekstrom et al. [8] give the smallest known example of an elliptic Carmichael number:

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

where $p = 468\,686\,771\,783$.

We wish to use a Korselt-like criterion for elliptic Carmichael numbers first proved in Ekstrom et al. [8]. Consider the condition $(-d \,|\, n) = -1$ in Gordon's primality test. In the case $d \in \{1, 2\}$, then $n \equiv -1 \pmod 8$ satisfies this condition. For the other values of d listed in Definition 1, note that each of these d's is congruent to $-1 \pmod 4$. Thus one has $(-d \,|\, n) = (n \,|\, d)$ and $(n \,|\, d) = -1$ whenever $n \equiv -1 \pmod d$. So put

$$\rho = 8 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 43 \cdot 67 \cdot 163, \tag{1}$$

and note that $n \equiv -1 \pmod \rho$ satisfies the condition $(-d \,|\, n) = -1$ for all d listed in Definition 1. Now we have the following elliptic Carmichael condition due to Ekstrom et al. [8].

Theorem 3 (Elliptic Carmichael condition)**.** *Let n be a squarefree, composite positive integer with an odd number of prime factors. Then n is an elliptic Carmichael number if for each prime p dividing n, one has $\rho \mid p+1$ and $p+1 \mid n+1$.*

2.3. Lucas Sequences and Pseudoprimes

We will later show that there are infinitely many elliptic Carmichael numbers that are also (strong) Lucas pseudoprimes. To this end, we summarize some basic definitions. For integers D, P, Q with $P > 0$ and $D = P^2 - 4Q \neq 0$, define $U_0 = 0, U_1 = 1, V_0 = 2$ and $V_1 = P$. Then the Lucas sequences U_k, V_k with parameters P, Q are defined for $k \geq 2$ by the recursive equations

$$U_k = PU_{k-1} - QU_{k-2} \quad \text{and} \quad V_k = PV_{k-1} - QV_{k-2}.$$

Let α and β be the distinct roots of the polynomial $f(x) = x^2 - Px + Q$. Then $\alpha\beta = Q$, $\alpha + \beta = P$, and for $k \geq 0$, we have

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} \quad \text{and} \quad V_k = \alpha^k + \beta^k.$$

If $n > 1$ is an odd integer and D, P, Q are chosen so that $(D \mid n) = -1$, and if n is prime and $\gcd(n, Q) = 1$, then by Theorem 8 of [7]

$$U_{n+1} \equiv 0 \pmod{n}, \tag{2}$$

$$V_{n+1} \equiv 2Q \pmod{n}. \tag{3}$$

In [4], they first defined a *Lucas pseudoprime* with parameters P and Q, denoted $\text{lpsp}(P, Q)$, to be a composite integer n satisfying Congruence (2). If n satisfies Congruence (2), but it is not known whether n is prime or composite, then n is said to be a *probable* Lucas pseudoprime with parameters P and Q, or $\text{lprp}(P, Q)$. Then in [3], they give the following definition.

Definition 2. If n satisfies Congruence (3), we call n a *Lucas-V probable prime* with parameters P and Q, or $\text{vprp}(P, Q)$. If n is composite and satisfies Congruence (3) with parameters P and Q, we call n a *Lucas-V pseudoprime*, or $\text{vpsp}(P, Q)$.

We further have the notion of *strong* Lucas pseudoprimes as defined in [7]. For n odd, we can write $n + 1 = d \cdot 2^s$ with d odd for some $s > 0$. If n is prime and $(D \mid n) = -1$, then either

$$U_d \equiv 0 \pmod{n}, \quad \text{or} \tag{4}$$

$$V_{d \cdot 2^r} \equiv 0 \pmod{n}, \quad \text{for some } r \text{ with } 0 \leq r < s. \tag{5}$$

Definition 3. If $(D \mid n) = -1$ and n satisfies Congruence (4) or (5), then n is called a *strong Lucas probable prime* with parameters P and Q, or $\text{slprp}(P, Q)$. If n is also composite, then n is called a *strong Lucas pseudoprime*, or $\text{slpsp}(P, Q)$.

3. Elliptic Carmichael Numbers in Arithmetic Progressions

In proving Theorem 2, the main idea is to construct a number L which has many factors d yielding many primes of the form $dk-1$ for some k relatively prime to L. We find a particular k that gives sufficiently many primes of this form and combine subsets of these primes to form elliptic Carmichael numbers. As in [19], we will additionally require that these primes be quadratic nonresidues modulo L. Unlike Wright, though, we will require that L has an even number of prime factors. We supplement the ideas of Wright [18, 19] with those of Pomerance [15] in order to utilize the better lower bound obtained in Pomerance [15].

Throughout the rest of this discussion, we assume $M \geq 2$ and let $\mu = 4\phi(M)$ so that $4 \,|\, \mu$. Let $P(q-1)$ denote the largest prime divisor of $q-1$. We define the following set:

$$\mathcal{Q}_0 := \mathcal{Q}_0(y) = \{q \text{ prime} : y < q \leq y\log^2 y,\ q \equiv -1 \pmod{\mu},\ P(q-1) \leq y\}.$$

Note that this deviates from the set $\mathcal{Q}$ that Wright defines, where he considers the primes q not dividing M on the interval $[\frac{y^\theta}{\log y}, y^\theta]$ with $q \equiv -1 \pmod{\mu}$ and $P(q-1) \leq y$ for θ fixed between 1 and 2.

As noted in [15], if $q \leq y\log^2 y$ and $P(q-1) > y$, then $q = mr+1$, where $m < \log^2 y$ and r is prime. Then by Brun's sieve, the number of such primes q is at most

$$\sum_{m<\log^2 y} \sum_{\substack{r \text{ prime} \\ mr \leq y\log^2 y \\ rm+1 \text{ prime}}} 1 \ll \sum_{m<\log^2 y} \frac{y\log^2 y}{\phi(m)\log^2 y} \ll y\log\log y. \tag{6}$$

And by the prime number theorem for arithmetic progressions, the number of primes $q \leq y\log^2 y$ with $q \equiv -1 \pmod{\mu}$ is asymptotic to $\frac{1}{\phi(\mu)} y\log y$. This, together with (6), gives

$$\#\mathcal{Q}_0 \sim \frac{1}{\phi(\mu)} y\log y \quad \text{and} \quad \prod_{q\in\mathcal{Q}_0} q = \exp\left(\frac{1+o(1)}{\phi(\mu)} y\log^2 y\right),\ y \to \infty. \tag{7}$$

We will also make use of the following fact:

$$\sum_{q\in\mathcal{Q}_0} \frac{1}{q} < \sum_{\substack{y<q\leq y\log^2 y \\ q \text{ prime}}} \frac{1}{q} = o(1), \quad y \to \infty. \tag{8}$$

We fix B such that $0 < B < \frac{5}{12}$; later, we will choose B to be near $\frac{5}{12}$. Let $\pi(z; d, a)$ denote the number of primes up to z which are congruent to a modulo d. Then we have the following theorem due to Alford et al. [2].

Theorem 4. *For any x, there exists a set $\mathcal{D}_B(x)$ of at most D_B integers, all of which exceed $\log x$, such that if d is not divisible by an element in $\mathcal{D}_B(x)$ and $d \le \min\left\{x^B, z/x^{1-B}\right\}$ then*

$$\pi(z;d,a) \ge \frac{\pi(z)}{2\phi(d)}$$

for any a with $\gcd(a,d)=1$.

With $\mathcal{Q}_0$ as defined above, let $L' = \prod_{q\in\mathcal{Q}_0} q$, and let

$$x = (M\rho L')^{1/B}.$$

Then by Theorem 4 if $n \le x^B$, n is not divisible by any element of $\mathcal{D}(x)$, $\gcd(b,n) = 1$, and $z \ge nx^{1-B}$, then

$$\pi(z;n,b) \ge \frac{\pi(z)}{2\phi(n)}.$$

We can construct a set of primes $P_B(x)$ with $\#P_B(x) \le D_B$ in the following way: for each number d in $\mathcal{D}_B(x)$, choose a prime factor of d and add it to $P_B(x)$ if it is not already in there. Thus any element of $\mathcal{D}_B(x)$ is divisible by at least one of the primes in $P_B(x)$. With this, we define $\mathcal{Q} = \mathcal{Q}_0 \setminus P_B(x)$. We will assume that $\#\mathcal{Q}$ is even. Then put

$$L = \prod_{q\in\mathcal{Q}} q \tag{9}$$

so that no factor of L is divisible by any element in $\mathcal{D}_B(x)$. One also has that $\gcd(q,M) = 1$ for all $q \in \mathcal{Q}$, and hence $\gcd(M,L) = 1$. Notice that we still have that $\mathcal{Q}$ satisfies (7) and (8). In terms of L, this means

$$L = \exp\left(\frac{1+o(1)}{\phi(\mu)} y\log^2 y\right), \tag{10}$$

$$\omega(L) \sim \frac{1}{\phi(\mu)} y\log y, \quad \text{and} \quad \sum_{q\,|\,L}\frac{1}{q} = o(1) \quad \text{as} \quad y\to\infty, \tag{11}$$

where $\omega(L)$ is the number of distinct prime divisors of L.

Analogous to [15], for each $d\,|\,L$ and each quadratic nonresidue $b \pmod{L/d}$ we consider the primes p such that

- $p \le dx^{1-B}$
- $p \equiv -1 \pmod{d}$,
- $p \equiv a \pmod{M}$ and
- $p \equiv b \pmod{L/d}$.

Note that for y sufficiently large relative to M, $\mathcal{D}_B(x)$ contains no factors of M, and by construction L has no factors in $\mathcal{D}_B(x)$, hence ML has no factors in $\mathcal{D}_B(x)$.

Moreover, since $\gcd(M, L) = 1$, we can combine the above congruences to obtain a single congruence modulo ML and apply Theorem 4 to reduced residue classes modulo ML. Consequently, we have the following analogue of Lemma 2.2 of [18].

Lemma 1. *Let L be as in Equation (9), and let $\gcd(a, M) = 1$. Then for each $d \mid L$ and each quadratic nonresidue $b \pmod{L/d}$, the number of primes p satisfying $p \le dx^{1-B}$, $p \equiv -1 \pmod{d}$, $p \equiv a \pmod{M}$ and $p \equiv b \pmod{L/d}$ is greater than*

$$\frac{dx^{1-B}2^{\omega(d)}}{3 \cdot 2^{\omega(L)}\phi(Md)\log x}.$$

Proof. The absolute number of congruence classes that are quadratic nonresidues modulo each $q \mid L$ is $\frac{q-1}{2}$ of the $q-1$ classes which can contain more than one prime number. By the Chinese Remainder Theorem, we get that for a given divisor d, the number of congruence classes modulo L/d which are quadratic nonresidues for every q is

$$\prod_{q \mid L/d} \frac{q-1}{2} = \frac{\phi(L/d)}{2^{\omega(L/d)}} \quad \text{of the} \quad \prod_{q \mid L/d} (q-1) = \phi(L/d)$$

congruence classes which contain more than one prime. Now, there are $\phi(ML)$ congruence classes modulo ML which can contain more than one prime, and by Theorem 4, the number of primes in such a class is at least

$$\frac{\pi(dx^{1-B})}{2\phi(ML)} > \frac{dx^{1-B}}{3\phi(ML)\log x},$$

and thus the number of classes which are quadratic nonresidues modulo L/d and congruent to $a \pmod{M}$ is at least

$$\frac{\pi(dx^{1-B})2^{\omega(d)}}{3 \cdot 2^{\omega(L)}\phi(Md)} > \frac{dx^{1-B}2^{\omega(d)}}{3 \cdot 2^{\omega(L)}\phi(Md)\log x}. \qquad \square$$

For a given divisor d of L and our fixed B, we want to count the number of primes $p \equiv -1 \pmod{d}$ that also satisfy $\gcd((p+1)/d, L) = 1$. Analogous to [2], note that for our chosen x, we have $1 \le d \le x^B$ for any $d \mid L$. We find the following lower bound on primes satisfying the above conditions. Here, and throughout the rest of this section, ρ is as defined in Equation (1). We will also abbreviate quadratic nonresidue as QNR.

Lemma 2. *Let $B < 5/12$, L as above. Let $M > 2$ be such that $\gcd(M, \rho) = 1$ or $\gamma := \gcd(M, \rho) > 1$ with $a \equiv -1 \pmod{\gamma}$. Then there exists an integer $k \le x^{1-B}$ with $\gcd(k, L) = 1$ such that*

$$\begin{aligned}&\#\{d \mid L : p = dk - 1 \text{ is prime, } p \text{ a QNR mod } q \text{ for every } q \mid L,\\ &\qquad\qquad \rho \mid p+1,\ p \equiv a \bmod M,\ p \le dx^{1-B}\}\\ &> \frac{(3/2)^{\omega(L)}}{4\phi(M)\phi(\rho)\log x}.\end{aligned}$$

Proof. In Lemma 1 we showed that for a given divisor d of L, the number of primes $p \leq dx^{1-B}$ that are both quadratic nonresidues modulo L/d and congruent to $a \pmod M$ is greater than

$$\frac{dx^{1-B}2^{\omega(d)}}{3 \cdot 2^{\omega(L)}\phi(M)\log x}.$$

We want to add the additional requirement that the primes p be congruent to $-1 \pmod \rho$. That is, we are looking to satisfy

$$\begin{aligned} p &\equiv \quad a \pmod M \\ p &\equiv -1 \pmod \rho. \end{aligned} \tag{12}$$

We claim that the number of such primes is greater than

$$\frac{dx^{1-B}2^{\omega(d)}}{3 \cdot 2^{\omega(L)}\phi(Md)\phi(\rho)\log x}. \tag{13}$$

To see this, first consider the case $\gcd(\rho, M) = 1$. Then $t\rho + sM = 1$ for some integers t, s. Then a solution to (12) is given by $p = at\rho - sM$, so

$$p \equiv at\rho - sM \pmod{M\rho}. \tag{14}$$

Then we can replace a by $at\rho - sM$ and M by $M\rho$ in Lemma 1 to obtain the bound in (13).

Next consider the case when $\gcd(\rho, M) > 1$. Let $\gamma = \gcd(\rho, M)$, and write $\gamma = t\rho + sM$. If $a \equiv -1 \pmod \gamma$, then (12) has a unique solution modulo $[\rho, M] = \rho M/\gamma$ given by

$$p = \frac{at\rho - sM}{\gamma}.$$

Otherwise, no solution exists. So in the case $a \equiv -1 \pmod \gamma$, we can replace a by $(at\rho - sM)/\gamma$ and M by $\rho M/\gamma$ in Lemma 1 to obtain the bound in (13).

We further want to constrain to have $p \equiv -1 \pmod d$ for a given divisor d of L. We claim that there are more than

$$\frac{dx^{1-B}2^{\omega(d)}}{2^{\omega(L)+2}\phi(M)\phi(\rho)\log x}. \tag{15}$$

such primes. In counting the number of primes in various residue classes, allow us to abuse intersection notation, and let $\pi(d, q, a) \cap \pi(d, r, b)$ denote the number of primes up to d that are both congruent to a modulo q and congruent to b modulo r. Then in the case that $\gcd(M, \rho) = 1$, we have

$$\pi(dx^{1-B}, M, a) \cap \pi(dx^{1-B}, \rho, -1) = \pi(dx^{1-B}, M\rho, at\rho - sM),$$

where t, s are as in Congruence (14). The claim then follows immediately from proof of Lemma 6.2 of [19]. Next, in the case that $\gcd(\rho, M) > 1$ with $a \equiv -1 \pmod{M\rho}$, we have

$$\pi(dx^{1-B}, M, a) \cap \pi(dx^{1-B}, \rho, -1) = \pi\left(dx^{1-B}, \frac{M}{\gamma}\rho, \frac{at\rho - sM}{\gamma}\right),$$

and then (15) follows in the same way as in the first case.

We wish to determine how many of these primes satisfy $\gcd\left(\frac{p+1}{d}, L\right) = 1$. Using the notation of [19], let $\pi(x, L, \text{QNR})$ denote the number of primes up to x which are quadratic nonresidues modulo every divisor of L. Now, for any prime $q \mid L$, we have by the Brun-Titchmarsh inequality (see [14]) that

$$\begin{aligned}\pi(dx^{1-B}, dq, -1) \cap \pi(dx^{1-B}, L, \text{QNR}) \cap \pi(dx^{1-B}, M, a) \cap \pi(dx^{1-B}, \rho, -1) \\ \ll \frac{dx^{1-B}2^{\omega(d)}}{2^{\omega(L)}q\phi(Md)\phi(\rho)\log(x/(qML))} \\ \ll \frac{dx^{1-B}2^{\omega(d)}}{2^{\omega(L)}q\phi(Md)\phi(\rho)\log x}. \end{aligned} \tag{16}$$

Now combining (13) and (16), one has

$$\begin{aligned}&\pi(dx^{1-B}, d, -1) \cap \pi(dx^{1-B}, L, \text{QNR}) \cap \pi(dx^{1-B}, M, a) \cap \pi(dx^{1-B}, \rho, -1) \\ &- \sum_{\substack{q \mid L \\ q \text{ prime}}} \pi(dx^{1-B}, dq, -1) \cap \pi(dx^{1-B}, L/d, \text{QNR}) \cap \pi(dx^{1-B}, M, a) \cap \pi(dx^{1-B}, \rho, -1) \\ &> \frac{dx^{1-B}2^{\omega(d)}}{3 \cdot 2^{\omega(L)}\phi(Md)\phi(\rho)\log x} - \sum_{\substack{q \mid L \\ q \text{ prime}}} \frac{dx^{1-B}2^{\omega(d)}}{2^{\omega(L)}q\phi(Md)\phi(\rho)\log x} \\ &> \frac{x^{1-B}2^{\omega(d)}}{4 \cdot 2^{\omega(L)}\phi(M)\phi(\rho)\log x}, \end{aligned} \tag{17}$$

where the last inequality uses the fact that $\sum_{q \mid L} \frac{1}{q} = o(1)$ and that $d > \phi(d)$.

Summing over all divisors d of L, the inequality in (17) implies that we have at least

$$\sum_{d \mid L} \frac{x^{1-B}2^{\omega(d)}}{4 \cdot 2^{\omega(L)}\phi(M)\phi(\rho)\log x}$$

pairs (p, d) such that all of the following requirements hold: $p \leq dx^{1-B}$ is prime, d divides L, $\frac{p+1}{d}$ is coprime to L, $p \equiv -1 \pmod{\rho}$, $p \equiv a \pmod{M}$, p is a quadratic nonresidue modulo L, and $d \leq x^B$. Now since the number of distinct values of $\frac{p+1}{d}$ is bounded by x^{1-B}, there must be some k coprime to L having at least

$$\sum_{d \mid L} \frac{2^{\omega(d)}}{4 \cdot 2^{\omega(L)}\phi(M)\phi(\rho)\log x} \tag{18}$$

representations as $\frac{p+1}{d}$ for p, d as above. For the numerator in (18), one has

$$\sum_{d \mid L} 2^{\omega(d)} = \sum_{i=0}^{\omega(L)} \binom{\omega(L)}{i} 2^{\omega(L)-i} = (2+1)^{\omega(L)} = 3^{\omega(L)},$$

which gives

$$\sum_{d \mid L} \frac{2^{\omega(L)}}{4 \cdot 2^{\omega(L)} \phi(M)\phi(\rho) \log x} = \frac{\left(\frac{3}{2}\right)^{\omega(L)}}{4 \cdot \phi(M)\phi(\rho) \log x},$$

and this completes the proof. □

Let k_0 be the k found by the above lemma and define

$$\mathcal{P} = \big\{p \text{ prime}\colon p = dk_0 - 1 \text{ for some } d \mid L, p \text{ is a QNR mod } q \text{ for every } q \mid L, \\ p \equiv a \bmod M, \rho \mid p+1, p \le x\big\}. \tag{19}$$

We will generate pseudoprimes by taking products of elements of $\mathcal{P}$. Note that Lemma 2 gives a lower bound on the size of $\mathcal{P}$. We will make use of this in the proof of Theorem 5.

We require the use of Lemma 6 of [12]. Here, $\Omega(n)$ denotes the number of prime factors of n, counted with multiplicity. For a multiplicative abelian group G, $\lambda(G)$ denotes the largest order of an element in G, and $n(G)$ is Davenport's constant—the smallest number such that a collection of at least $n(G)$ elements must contain some subset whose product is the identity. Then we have

$$\lambda(G) \le n(G) \le \lambda(G)\left(1 + \frac{\log(\#G)}{\lambda(G)}\right).$$

The first inequality is clear, and the second is due to van Emde Boas–Kruyswijk [9] and Meshulam [13]. For a simplified proof of this result, see Theorem 1.1 of [2].

As noted in [12], the following lemma is a consequence of Proposition 1.2 of [2] and Proposition 1 of [5].

Lemma 3 ([12])**.** *For any multiplicative abelian group G, write*

$$s(G) = \lceil 5\lambda(G)^2 \Omega(\lambda(G)) \log(3\lambda(G)\Omega(\#G)) \rceil.$$

Let A be a sequence of length n consisting of non-identity elements of G. Then there exists a nontrivial subgroup $H \subset G$ such that the following conditions are satisfied.

i. If $n \ge s(G)$, then for every $h \in H$, $A \cap H$ has a subsequence whose product is h.

ii. If t is an integer such that $s(G) < t < n - n(G)$, then for every $h \in H$, A has at least $\binom{n-n(G)}{t-n(G)}/\binom{n}{n(G)}$ distinct subsequences of length at most t and at least $t - n(G)$ whose product is h.

Lemma 4. *Let H be the subgroup of $(\mathbb{Z}/kML\mathbb{Z})^*$ of residues congruent to $-1 \pmod k$. Let $G = H \times \{-1, 1\}$. For $n(G)$ and $s(G)$ as above, we have $n(G) \le e^{2y}$ and $s(G) \le e^{3y}$.*

Proof. First note that $\#G \le 2ML$. Denoting $\lambda((\mathbb{Z}/L\mathbb{Z})^*)$ by $\lambda(L)$, this is the lcm of $q-1$ for the primes $q \mid L$. By assumption the largest prime dividing $q-1$ is less than or equal to y. Thus if q^e is the largest prime power dividing $\lambda(L)$, then $q^e \le y \log^2 y$; hence

$$\lambda(L) \le (y \log^2 y)^{\pi(y)}.$$

On noting that $\lambda(G) \le 2M\lambda(L)$ and using (10), we obtain

$$n(G) \le 2M(y \log^2 y)^{\pi(y)} \log(ML) \le e^{2y}.$$

Finally, the estimate on $s(G)$ follows from Lemma 3 and our estimate on $\lambda(G)$. □

With this, we can state the key theorem which combines the ideas of [18, Theorem 5.1] and [19, Theorem 8.1].

Theorem 5. *Let $\mathcal{P}$ be the set of primes defined in (19). Let G be the group defined in Lemma 4 and let $s(G)$ be as in Lemma 3. Then $\#\mathcal{P} > s(G)$. If H is the subgroup of G guaranteed by Lemma 3, then there exists an element $h \in H$ such that*

$$h = (\zeta, -1),$$

with

$$\begin{aligned} \zeta &\equiv -1 \pmod L \\ \zeta &\equiv \ \ a \pmod M. \end{aligned} \tag{20}$$

Equivalently, there exists a subset of $\mathcal{P}$ whose product multiplies to a number m for which $m \equiv a \pmod M$ and $p \mid m$ implies $p + 1 \mid m + 1$.

Proof. First note that we have $s(G) < \#\mathcal{P}$. Let $A = \{(p, -1) : p \in \mathcal{P}\}$ be the sequence referenced in Lemma 3. Then clearly $\#A = \#\mathcal{P} > s(G)$. Then in particular, it follows from part (i) of Lemma 3 that $A \cap H \ne \varnothing$. So let $\hat{p}$ be a prime such that $(\hat{p}, -1) \in A \cap H$.

Since $\hat{p} \in \mathcal{P}$, $\hat{p}$ is a quadratic nonresidue modulo each q dividing L. Put

$$j = \prod_{q \mid L} \frac{q-1}{2},$$

and note that j is necessarily odd since each $q \equiv 3 \pmod 4$. Consequently, we have

$$\hat{p}^j \equiv \left(\hat{p}^{\frac{q-1}{2}}\right)^{j/\left(\frac{q-1}{2}\right)} \equiv (-1)^{j/\left(\frac{q-1}{2}\right)} \equiv -1 \pmod q$$

for each $q \,|\, L$, and $(-1)^j \equiv -1 \pmod q$. Also note that by assumption we have $q \equiv -1 \pmod{4\phi(M)}$. But this gives

$$\frac{q-1}{2} \equiv -1 \pmod{2\phi(M)}$$

so that $\frac{q-1}{2} \equiv -1 \mod \phi(M)$. Then since by assumption L has an even number of factors, we obtain

$$j \equiv 1 \pmod{\phi(M)},$$

giving

$$\hat{p}^j \equiv a \pmod M.$$

So putting $h = (\hat{p}, -1)^j = (\hat{p}^j, (-1)^j)$ gives the desired congruences in (20), proving the first half of the theorem.

For the second half, by Lemma 3, there exists a sequence $\{p_1, \ldots, p_s\} \subset \mathcal{P}$ such that

$$(p_1, -1) \cdots (p_s, -1) = h.$$

Put $m = p_1 \cdots p_s$. Since each $p_i \in \mathcal{P}$ is $-1 \bmod k_0$ and s is odd (being that $(-1)^s = -1$), it must be that $m \equiv -1 \pmod{k_0}$. Hence modulo L, one has

$$m \equiv p_1 \cdots p_s \equiv -1 \pmod L.$$

Note also that we still have $m \equiv a \pmod M$, so m satisfies (20). Putting this all together, for any prime p_i dividing m, one has $\rho \,|\, p_i + 1$ and

$$p_i + 1 \,|\, dk \,|\, Lk \,|\, m + 1. \qquad \square$$

We are now ready to prove Theorem 2, where we give an explicit lower bound on the number of elliptic Carmichael numbers up to X. The proof appears in [15] for the case of Carmichael numbers. It still applies to the present case, so we include it here.

Proof of Theorem 2. We define $t = \lceil e^{3y} \rceil$ so that $t \geq s(G)$. Then, by Lemma 3, $\mathcal{P}$ has at least

$$N := \binom{\#\mathcal{P} - n(G)}{t - n(G)} \Big/ \binom{\#\mathcal{P}}{n(G)}$$

distinct products of at most t primes which are congruent to $-1 \bmod L$. Moreover, it follows from Lemma 4 that for y large enough, one has $n(G) > (\#P)^2 e$. This, combined with the standard bounds

$$\left(\frac{\alpha}{\beta}\right)^\beta \leq \binom{\alpha}{\beta} \leq \left(\frac{\alpha e}{\beta}\right)^\beta,$$

gives the following string of inequalities:

$$\begin{aligned} N &> \left(\frac{\#\mathcal{P}-n(G)}{t-n(G)}\right)^{t-n(G)}(\#\mathcal{P})^{-n(G)} \\ &> \left(\frac{\#\mathcal{P}}{t}\right)^{t-n(G)}(\#\mathcal{P})^{-n(G)} > (\#\mathcal{P})^{t-2n(G)}t^{-t}. \end{aligned}$$

Now, define $X := x^t$. Note that each $p \in \mathcal{P}$ satisfies $p \le x$. Hence, all of the elliptic Carmichael numbers constructed in Theorem 5 are at most X. Then using (7), Lemma 4 and the definition of x, we obtain

$$X = \exp\left(\frac{1/B + o(1)}{\phi(\mu)} ty \log^2 y\right).$$

Moreover, using (10) and the lower bound on $\#\mathcal{P}$ obtained in Lemma 2, we have

$$\begin{aligned} N &\ge \exp\left(\frac{\log(3/2)+o(1)}{\phi(\mu)} ty\log y - t\log t\right) \\ &= \exp\left(\frac{\log(3/2)+o(1)}{\phi(\mu)} ty\log y\right), \end{aligned}$$

giving $N \ge X^{(B\log(3/2)+o(1))/\log y}$. Now, $\log X$ is asymptotic to

$$\frac{1}{B\phi(\mu)} ty\log^2 y,$$

and using the definition of t, we see

$$\log\log X = 3y + O(\log y), \quad \log\log\log X = \log y + O(1).$$

Hence $N \ge X^{(B\log(3/2)+o(1))/\log\log\log X}$. Because $B < 5/12$ can be chosen to be arbitrarily close to $5/12$ and $(5/12)\log(3/2) > 1/6$, this completes the proof. □

4. Elliptic Carmichael Numbers and (Strong) Lucas Pseudoprimes

We prove an analogue of Theorem 2 of [3]. This requires the following lemma from the same paper. The number a constructed in the proof is used in Theorem 6; consequently, we must modify the proof given in [3] to be able to use it.

Lemma 5. *For every positive integer r, there exists an integer $a \equiv 3 \pmod 4$ such that for every odd prime p, if $p \equiv a \pmod{4r}$, then r is a quadratic residue modulo p, i.e., $(r \mid p) = +1$.*

Proof. Write $r = 2^s t$ with t odd. If s is even, let $a = 4t - 1$, and if s is odd, let $a = 8t - 1$. Then clearly $a \equiv 3 \pmod 4$. Suppose p is an odd prime with $p \equiv a \pmod{4r}$. In particular, we have $p \equiv 3 \pmod 4$.

If $t = 1$, we have two possibilities: r is a power of 4, or r is twice a power of 4. In the first case, s is even, $a = 3$ and $(r \,|\, p) = (1 \,|\, p) = +1$. In the second case, s is odd, so $(r \,|\, p) = (2 \,|\, p) = +1$ by the supplement to the law of quadratic reciprocity since $p \equiv 7 \pmod 8$.

Now suppose $t > 1$ and s is even; then $a = 4t - 1$. If $t \equiv 1 \pmod 4$, then

$$\left(\frac{r}{p}\right) = \left(\frac{2^s t}{p}\right) = \left(\frac{t}{p}\right) = \left(\frac{p}{t}\right) = \left(\frac{4t-1}{t}\right) = \left(\frac{-1}{t}\right) = +1.$$

And if $t \equiv 3 \pmod 4$, then

$$\left(\frac{r}{p}\right) = \left(\frac{2^s t}{p}\right) = \left(\frac{t}{p}\right) = -\left(\frac{p}{t}\right) = -\left(\frac{4t-1}{t}\right) = -\left(\frac{-1}{t}\right) = +1.$$

Finally suppose $t > 1$ and s is odd. Then $a = 8t - 1$. If $t \equiv 1 \pmod 4$, then

$$\left(\frac{r}{p}\right) = \left(\frac{2t}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{t}{p}\right) = \left(\frac{p}{t}\right) = \left(\frac{8t-1}{t}\right) = \left(\frac{-1}{t}\right) = +1.$$

And if $t \equiv 3 \pmod 4$, then

$$\left(\frac{r}{p}\right) = \left(\frac{2t}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{t}{p}\right) = -\left(\frac{p}{t}\right) = -\left(\frac{8t-1}{t}\right) = -\left(\frac{-1}{t}\right) = +1. \qquad \square$$

We can now prove the following theorem. Unlike the analogous theorem in [3], we must take special care in the case that $\gcd(r, \rho) > 1$.

Theorem 6. *If $r > 1$ is an integer, there are infinitely many elliptic Carmichael numbers $m \equiv 3 \pmod 4$ that are also strong pseudoprimes to base r. Moreover, the number of such $m < X$ is at least $X^{1/(6 \log\log\log X)}$ for all sufficiently large X.*

Proof. Write $r = 2^s t$, with t odd. If $s = 0$, let $M = 4r$; if $s = 1$, take $M = 2r$; if $s \geq 2$, let $M = r$, and choose a according to Lemma 5. Then in any case, $a \equiv -1 \pmod M$, which implies that $a \equiv -1 \pmod{\gcd(M, \rho)}$. Thus by Theorem 2, we have $\mathcal{N}_{M,a}(X) \gg X^{1/(6 \log\log\log X)}$. Note also that since $a \equiv 3 \pmod 4$ and $4 \,|\, M$, one has $m \equiv 3 \pmod 4$. By construction each p dividing m is odd and congruent to a modulo M, and congruent to 3 modulo 4. Hence by Lemma 5 for each $p \,|\, M$ we have $(r \,|\, p) = +1$. By Corollary 1.2 of [1], since for each p dividing M, $(r \,|\, p)$ takes the same value, m is a strong pseudoprime to base r. $\square$

In light of Theorem 6, we can actually say that there are infinitely many elliptic Carmichael numbers that are also strong lpsp's and vpsp's for certain parameters P and Q.

Corollary 1. *Let k be a positive integer. Let $P = 2^k$ and $Q = 2^{2k-1}$. Then there exist infinitely many elliptic Carmichael numbers $m \equiv 3 \pmod 4$ that are strong pseudoprimes to base 2, strong* $\mathrm{lpsp}(P, Q)$ *and* $\mathrm{vpsp}(P, Q)$*. Moreover, the number of such $m < X$ is at least $X^{1/(6 \log\log\log X)}$ for all sufficiently large X.*

Corollary 2. *Let k be a positive integer. Let $P = 4 \cdot r^k$ and $Q = 8 \cdot r^{2k}$. Then there exist infinitely many elliptic Carmichael numbers $m \equiv 3 \pmod 4$ that are strong pseudoprimes to base r and strong* $\mathrm{lpsp}(P, Q)$*. Moreover, the number of such $m < X$ is at least $X^{1/(6 \log\log\log X)}$ for all sufficiently large X.*

These corollaries immediately follow from Theorem 6 and the following two theorems. The first is due to Baillie-Fiori-Wagstaff [3], and the second is analogous, which we prove.

Theorem 7. [3, Theorem 1] *Let $n \equiv 3 \pmod 4$ be a strong pseudoprime base 2. Let $k \geq 0$ be an integer. Set $P = 2^k$ and $Q = 2^{2k-1}$. Then n is also a strong* $\mathrm{lpsp}(P, Q)$ *and a* $\mathrm{vpsp}(P, Q)$*.*

Theorem 8. *Let $n \equiv 3 \pmod 4$ be a strong pseudoprime base r. Let $k \geq 0$ be an integer. Set $P = 4 \cdot r^k$ and $Q = 8 \cdot r^{2k}$. Then n is also a strong* $\mathrm{lpsp}(P, Q)$*.*

Proof. Note that $D = P^2 - 4Q = 16 \cdot r^{2k} - 4 \cdot 8 \cdot r^{2k} = -16(r^k)^2$. Then since $n \equiv 3 \pmod 4$, one has

$$\left(\frac{D}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{4^2}{n}\right)\left(\frac{(r^k)^2}{n}\right) = -1.$$

Now write $n + 1 = d \cdot 2^s$ where $2 \nmid d$. Then $s > 1$ and $\frac{n+1}{2}$. We want to prove that $V_{2d} \equiv 0 \pmod n$ since then the congruence in (5) will imply that n is a $\mathrm{slpsp}(P, Q)$.

Let α, β be the roots of the equation $x^2 - Px + Q = 0$. Then we have

$$\alpha = \frac{P + \sqrt{D}}{2} = \frac{4 \cdot r^k + \sqrt{-16 \cdot r^{2k}}}{2} = 2 \cdot r^k(1 + i)$$
$$\beta = \frac{P - \sqrt{D}}{2} = \frac{4 \cdot r^k - 2\sqrt{-16 \cdot r^{2k}}}{2} = 2 \cdot r^k(1 - i),$$

and after observing that $(1 + i)^2 = 2i$ and $(1 - i)^2 = -2i$, we see that

$$\alpha^{2d} = (2 \cdot r^k)^{2d}(1 + i)^{2d} = 2^{3d} \cdot r^{2kd} \cdot i^d$$
$$\beta^{2d} = (2 \cdot r^k)^{2d}(1 - i)^{2d} = 2^{3d} \cdot r^{2kd} \cdot (-i)^d.$$

Whence,

$$V_{2d} = \alpha^{2d} + \beta^{2d} = 2^{3d} \cdot r^{2kd}\big(i^d + (-i)^d\big) = 0.$$

Thus, by (5) n is a $\mathrm{slpsp}(P, Q)$. □

Note that the key in the proof of Theorem 8 is that $4^2 = 2 \cdot 8$ when obtaining the values for α and β. Therefore the proof works exactly the same for any even integer A where $P = A \cdot r^k$ and $Q = \frac{A^2}{2} \cdot r^{2k}$.

We also have an analogue to the second part of Theorem 7. However, we need to further assume that the number $n \equiv 3 \pmod 4$ is an Euler pseudoprime to base 2 in addition to being a strong pseudoprime to base r. By an Euler pseudoprime we mean an odd composite integer n that satisfies Euler's criterion:

$$2^{(n-1)/2} \equiv \left(\frac{2}{n}\right) \pmod n.$$

Theorem 9. *Let $n \equiv 3 \pmod 4$ be a strong pseudoprime base r that is also an Euler pseudoprime base 2. Let $k \geq 0$ be an integer. Set $P = r^k$ and $Q = 2r^{2k}$. Then n is also a* $\mathrm{vpsp}(P, Q)$.

Proof. We will prove that $V_{n+1} \equiv 2Q \pmod n$ as this will show that n is a $\mathrm{vpsp}(P, Q)$ by (3). As in the proof of Theorem 8, let α, β be the roots of the equation $x^2 - Px + Q = 0$. In this case we have

$$\alpha = r^k(1 + i) \quad \text{and} \quad \beta = r^k(1 - i).$$

Write $n + 1 = 4M$, and note that $(1 + i)^4 = (1 - i)^4 = -4$, hence

$$\alpha^{n+1} = \beta^{n+1} = \left(r^k\right)^{n+1}(-1)^M \cdot 4^M,$$

and so

$$\begin{aligned} V_{n+1} = \alpha^{n+1} + \beta^{n+1} &= 2 \cdot \left(r^k\right)^{n+1}(-1)^M \cdot 4^M \\ &= 2 \cdot \left(r^2 r^{n-1}\right)^k (-1)^M \cdot 4^M \\ &= 2 \cdot r^{2k}\left(r^k\right)^{n-1}(-1)^M \cdot 2^{2M} \\ &= 2Q\left(r^k\right)^{n-1}(-1)^M \cdot 2^{2M-1} \\ &= 2Q\left(r^k\right)^{n-1}(-1)^M \cdot 2^{(n-1)/2}. \end{aligned} \tag{21}$$

Now since n is $\mathrm{spsp}(r)$, one has $2^{n-1} \equiv 1 \pmod n$. Moreover, by assumption n is also an Euler pseudoprime base 2, which gives that $2^{(n-1)/2} \equiv (2 \,|\, n) \pmod n$. This gives rise to two possible cases for (21). Suppose $n \equiv 3 \pmod 8$. Then M is odd, which forces $(-1)^M = -1$ and $(2 \,|\, n) = -1$. On the other hand suppose $n \equiv 7 \pmod 8$. Then M is even, and in this case $(-1)^M = 1$ and $(2 \,|\, n) = 1$. In either case, this simplifies (21) to

$$V_{n+1} = 2Q(r^k)^{n-1}(-1)^M \cdot 2^{(n-1)/2} \equiv 2 \cdot 1 \cdot (-1)^M \cdot (2 \,|\, n) \equiv 2Q \pmod n. \quad \square$$

5. Conclusion and Future Work

Knowledge of the existence of Carmichael numbers dates back to the early 1900s. Alford et al. [2] proved in 1994 that there are infinitely many Carmichael numbers. In 2013, Wright [18] gave the first unconditional proof that there are infinitely many Carmichael numbers in every possible arithmetic progression. Using his methods, along with recent results from Pomerance [15], we were able to give an explicit lower bound on the number of elliptic Carmichael numbers up to X that are congruent to a modulo M for particular M in our Theorem 2.

We recently noticed a paper by Kellner and Sondow [11] that gives a new characterization of Carmichael numbers. By specializing one parameter in the new characterization, they define a proper subset of Carmichael numbers they call primary Carmichael numbers. Numerical experiments suggest that a sizable proportion of all Carmichael numbers are primary, but it is not even known whether there are infinitely many of them. It may be possible to prove a characterization of primary Carmichael numbers similar to Korselt's criterion. If this is done, one should be able to modify the results of Section 3 to show there are infinitely many primary Carmichael numbers in many arithmetic progressions. Perhaps one can define primary elliptic Carmichael numbers and prove similar results.

In Section 4, we gave several results on strong Lucas pseudoprimes and Lucas V-pseudoprimes. As noted in [3], there are many related open questions. It would be nice to have a formula that bounds the number of D or the number of pairs (P, Q) for which n is a vpsp. Another open question is the asymptotic growth rate for the number of vpsp's up to x. This growth rate probably depends on the algorithm for choosing the parameters P and Q as described in [3].

Let r be an integer > 1. Then Corollary 2 of Theorem 6 shows that there are infinitely elliptic Carmichael numbers $m \equiv 3 \pmod 4$ that are also strong pseudoprimes to base r and strong lpsp(P, Q) and vpsp(P, Q) for $P = 4 \cdot r^k$ and $Q = 8 \cdot r^{2k}$. Perhaps one could prove an analogous corollary with a different (P, Q) pair such that (P, Q) would be chosen by the algorithm described in Baillie et al. [3]. Such a result would prove that there are infinitely many counterexamples to the Baillie-PSW primality test.

Acknowledgements. The author would like to thank Carl Pomerance for an advance copy of [15]. The author would also like to thank Samuel Wagstaff for an advance copy of [3] as well as his many suggestions throughout writing this paper.

References

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

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

[3] R. Baillie, A. Fiori, and S. S. Wagstaff, Jr., Strengthening the Baillie-PSW primality test, *Math. Comp.* **90** (2021), 1931–1955.

[4] R. Baillie and S. S. Wagstaff, Jr., Lucas pseudoprimes, *Math. Comp.* **152** (1980), 1391–1417.

[5] R. C. Baker and W. M. Schmidt, Diophantine problems in variables restricted to the values 0 and 1, *J. Number Theory* **12** (1980), 460–486.

[6] W. D. Banks and C. Pomerance, On Carmichael numbers in arithmetic progressions, *J. Aust. Math. Soc.* **88** (2010), 313–321.

[7] J. Brillhart, D. H. Lehmer, and J. L. Selfridge, New primality criteria and factorizations of $2^m \pm 1$ *Math. Comp.* **29** (1975), 620–647.

[8] A. Ekstrom, C. Pomerance, and D. S. Thakur, Infinitude of elliptic Carmichael numbers, *J. Aust. Math. Soc.* **92** (2012), 45–60.

[9] P. van Emde Boas and D. Kruyswijk, A combinatorial problem on finite Abelian groups, *Math. Centrum Amsterdam Afd. Zuivere Wisk.* 1967 (1967), ZW-009, 27 pp.

[10] D. M. Gordon, Pseudoprimes on elliptic curves, *Théorie des nombres (Quebec, PQ, 1987)*, (1989), 290–305.

[11] B. C. Kellner and J. Sondow, On Carmichael and polygonal numbers, Bernoulli polynomials, and sums of base-P digits, *Integers* **21** (2021), #A52.

[12] K. Matomäki, Carmichael numbers in arithmetic progressions, *J. Aust. Math. Soc.*, **94** (2013), 268–275.

[13] R. Meshulam, An uncertainty inequality and zero subsums, *Discrete Math.*, **2** (1990), 197–200.

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

[15] C. Pomerance, A note on Carmichael numbers in residue classes, *Integers*, **21A** (2021), #A19.

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

[17] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[18] T. Wright, Infinitely many Carmichael numbers in arithmetic progressions, *Bull. Lond. Math. Soc.*, **5** (2013), 943–952.

[19] T. Wright, There are infinitely many elliptic Carmichael numbers, *Bull. Lond. Math. Soc.*, **50** (2018), 791–800.