SOME THOUGHTS ON PSEUDOPRIMES

CARL POMERANCE AND SAMUEL S. WAGSTAFF, JR.

Abstract. We consider several problems about pseudoprimes. First, we look at the issue of their distribution in residue classes. There is a literature on this topic in the case that the residue class is coprime to the modulus. Here we provide some robust statistics in both these cases and the general case. In particular we tabulate all even pseudoprimes to 10^{16}. Second, we prove a recent conjecture of Ordowski: the set of integers n which are a pseudoprime to some base which is a proper divisor of n has an asymptotic density.

In memory of Aleksandar Ivić (1949–2020)

1. Introduction

Fermat's "little" theorem is part of the basic landscape in elementary number theory. It asserts that if p is a prime, then $a^p \equiv a \pmod{p}$ for every prime p. One interest in this result is that for a given pair a, p, it is not hard computationally to check if the congruence holds. So, if the congruence fails, we have proved that the modulus p is not prime.

A pseudoprime is a composite number n with $2^n \equiv 2 \pmod{n}$, and more generally, a pseudoprime base a is a composite number n with $a^n \equiv a \pmod{n}$. Pseudoprimes exist, in fact, there are composite numbers n which are pseudoprimes to every base a, the first 3 examples being 561, 1105, and 1729. These are the Carmichael numbers. Named after Carmichael [7] who published the first few examples in 1910, they were actually anticipated by quite a few years by Šimerka [22].

We now know that there are infinitely many Carmichael numbers (see [1]), the number of them up to x exceeding $x^{0.33}$ for all sufficiently large x (see [12]). This count holds *a fortiori* for pseudoprimes to any fixed base a since the Carmichael numbers comprise a subset of the base-a pseudoprimes.

Date: November 7, 2023.

2000 *Mathematics Subject Classification.* 11N25 (11N37).

Key words and phrases. pseudoprime, Carmichael number.

S.S.W.'s work was supported by the CERIAS Center at Purdue University.

One can also ask for upper bounds on the distribution of pseudoprimes and Carmichael numbers. Let

$$L(x) = \exp(\log x \log\log\log x/\log\log x) = x^{\frac{\log\log\log x}{\log\log x}}.$$

We know (see [19]) that the number of Carmichael numbers up to x is at most $x/L(x)$ for all sufficiently large x, and it is conjectured that this is almost best possible in that the count is of the form $x/L(x)^{1+o(1)}$ as $x \to \infty$. The heuristic for this assertion is largely based on thoughts of Erdős [10].

It is conjectured that the same is true for pseudoprimes to any fixed base a, however the upper bound is not as tight. We know (see [19]) that for all large x, the number of *odd* pseudoprimes up to x is $\le x/L(x)^{1/2}$ and it seems likely that the argument goes through for those base-a pseudoprimes coprime to a, for any $a > 1$. An unpublished paper of Li [15] does achieve the same upper bound for even pseudoprimes as we have for odd ones, and it is likely here as well, that the result generalizes to an arbitrary base $a > 1$.

For positive coprime integers a, n let $l_a(n)$ denote the order of $a \pmod n$ in $(\mathbb{Z}/n\mathbb{Z})^*$. Further, let $\lambda(n)$ denote the maximal value of $l_a(n)$ over all $a \pmod n$; it is the universal exponent for the group $(\mathbb{Z}/n\mathbb{Z})^*$. If a, n are positive integers, not necessarily coprime, let n_a denote the largest divisor of n coprime to a. Note that n is a base-a pseudoprime if and only if $l_a(n_a) \mid n-1$ and $n/n_a \mid a$, as is easily verified.

It is natural to consider the distribution of pseudoprimes in residue classes. Consider the integers $n \equiv r \pmod m$, and suppose that n is a base-a pseudoprime. Let us write down some necessary conditions for n to exist. Let

$$g = \gcd(r, m), \quad h = \gcd(l_a(g_a), m).$$

Then if n is a base-a pseudoprime in the residue class $r \pmod m$, we must have

$$h \mid r-1 \ \text{ and } \ g/g_a \mid a. \tag{1}$$

We conjecture that (1) is sufficient for there to be infinitely many base-a pseudoprimes $n \equiv r \pmod m$. In fact, a heuristic argument based on that of Erdős [10] suggests that if these conditions hold for a, r, m, then the number $P_{a,r,m}(x)$ of base-a pseudoprimes $n \equiv r \pmod m$ with $n \le x$ is $x^{1-o(1)}$ as $x \to \infty$.

Let $C_{r,m}(x)$ denote the number of Carmichael numbers $n \le x$ with $n \equiv r \pmod m$. Clearly for any a, r, m we have $C_{r,m}(x) \le P_{a,r,m}(x)$.

Here are some things we know towards the conjecture.

- For all large x we have $C_{0,1}(x) > x^{.33}$. This is the main result of Harman [12], improving the earlier result with exponent $2/7$ in [1].
- If $\gcd(r, m) = 1$ and r is a square mod m, then for x sufficiently large, $C_{r,m}(x) > x^{1/5}$. This result is due to Matomäki [16].
- If $\gcd(r, m) = 1$, then $C_{r,m}(x) > x^{1/(6 \log\log\log x)}$ for x sufficiently large. This recent result of the first-named author [20] is based on the argument for a somewhat weaker bound due to Wright [24].
- If $\gcd(r, m) = 1$, then $P_{2,r,m}(x)$ is unbounded. This result of Rotkiewicz [21] is, of course, weaker than the previous item, but it preceded it by over half a century and is much simpler.

There are elementary ideas for showing $P_{2,r,m}(x)$ is unbounded even when $\gcd(r, m) > 1$. For example, there are infinitely many even pseudoprimes, the case $r = 0, m = 2$. Here's a proof. Suppose n is an even pseudoprime and let p be a prime with $l_2(p) = n$. From Bang [3] such a prime p exists. Then pn is another even pseudoprime. It remains to note that $n = 161{,}038$ is an even pseudoprime. This proof is essentially due to Beeger [6]. The example 161,038 was found by Lehmer in 1950.

A similar argument can be found for other choices of r, m, but we know no general proof that $P_{a,r,m}(x)$ is unbounded when (1) holds.

At the end of this paper we present substantial counts of pseudoprimes in residue classes.

The usual thought with pseudoprimes is to fix the base a and look at pseudoprimes n to the base a. Instead, one can take the opposite perspective and fix n, looking then at the bases a for which n is a pseudoprime. Let

$$F(n) = \#\{a \pmod n : a^{n-1} \equiv 1 \pmod n\}.$$

From Baillie–Wagstaff [2] and Monier [17], we have

$$F(n) = \prod_{p|n} \gcd(p-1, n-1),$$

where p runs over primes. Now let

$$F^*(n) = \#\{a \pmod n : a^n \equiv a \pmod n\}.$$

Note that $F^*(n) = n$ if and only if $n = 1$, n is a prime, or n is a Carmichael number. The Baillie–Wagstaff formula can be enhanced as follows:

$$F^*(n) = \prod_{p|n} (1 + \gcd(p-1, n-1)).$$

Thus, $F^*(n) - F(n)$ is the number of residues $a \pmod n$ with $a^n \equiv a \pmod n$ and $\gcd(a,n) > 1$. Among these it is interesting to consider those a that divide n. Let

$$D(n) = \#\{a \mid n : 1 < a < n,\ a^n \equiv a \pmod n\}$$

and let

$$\mathcal{S} = \{n \in \mathbb{N} : \#D(n) > 0\}.$$

T. Ordowski [18] has conjectured that $\mathcal{S}$ has an asymptotic density; counts up to 10^8 by A. Eldar suggest that this density may be about $\frac{5}{8}$. In the next section we present a proof that the density of $\mathcal{S}$ exists.

2. Proof of Ordowski's conjecture

For each integer $b \ge 2$ let

$$\mathcal{S}_b = \{n > b : n \equiv 0 \pmod b,\ (n/b)^n \equiv n/b \pmod n\},$$

Then

$$\mathcal{S} = \bigcup_{b \ge 2} \mathcal{S}_b.$$

Indeed, if $b \ge 2$ and $n \in \mathcal{S}_b$, let $a = n/b$. Then $a \in D(n)$, so $n \in \mathcal{S}$. Conversely, if $n \in \mathcal{S}$ and $a \mid n$ with $1 < a < n$ and $a^n \equiv a \pmod n$, then $n \in \mathcal{S}_{n/a}$.

We also remark that if $n \in \mathcal{S}_b$, then $\gcd(b, n/b) = 1$. Indeed, if p is a common prime factor with $p^\alpha \parallel n/b$, then we have $p^{\alpha+1} \mid n$ and $p^{\alpha+1} \mid (n/b)^n$, contradicting $(n/b)^n \equiv n/b \pmod n$.

For a set $\mathcal{S}$ of positive integers, let $\delta(\mathcal{S})$ be the asymptotic density of $\mathcal{S}$ should it exist.

Proposition 1. *For each $b \ge 2$, $\delta(\mathcal{S}_b)$ exists and*

$$c_1 := \sum_{b \ge 2} \delta(\mathcal{S}_b) < \infty. \tag{2}$$

Proof. To see that $\delta(\mathcal{S}_b)$ exists we will show that $\mathcal{S}_b \cup \{b\}$ is a finite union of residue classes.

To get a feel for things, we work out the first few b's. The case $b = 2$ is particularly simple. For n to be in $\mathcal{S}_2$ it is necessary that $n/2$ be odd, since we need $\gcd(b, n/b) = 1$. And this condition is sufficient when $n > 2$: it is easy to check that $(n/2)^n \equiv n/2 \pmod n$. Indeed the congruence is trivial modulo $n/2$ and it is trivial modulo 2. Thus $\mathcal{S}_2$ is the set of numbers that are 2 (mod 4) (other than 2), with density $\frac{1}{4}$.

Now take $b = 3$. For $ab \in \mathcal{S}_3$ we consider the two cases $a \equiv 1 \pmod 3$, $a \equiv 2 \pmod 3$. Every number of the form $3a$ with $a \equiv 1 \pmod 3$ and $a > 1$ is in $\mathcal{S}_3$, which gives density $\frac{1}{9}$. For $a \equiv 2 \pmod 3$

we need $2^{3a} \equiv 2 \pmod 3$ and this holds if and only if a is odd. That is, $a \equiv 5 \pmod 6$, and this condition is sufficient. This part of $\mathcal{S}_3$ has density $\frac{1}{18}$, so $\delta(\mathcal{S}_3) = \frac{1}{6}$.

We now work out the general structure of $\mathcal{S}_b$. We have a number ab, where $\gcd(a,b) = 1$ and $a > 1$. We trivially have $a^{ab} \equiv a \pmod a$, so the important condition is $a^{ab} \equiv a \pmod b$. Since $\gcd(a,b) = 1$, this is equivalent to $a^{ab-1} \equiv 1 \pmod b$, which holds if and only if $d \mid ab-1$, where d is the multiplicative order of $a \pmod b$. This cannot hold unless $\gcd(d,b) = 1$, and in this case, a is in a residue class $\pmod d$. So, if $a \equiv a_0 \pmod b$ and $a_0 \pmod b$ has multiplicative order d with $\gcd(d,b) = 1$, then such a's lie in a residue class of modulus bd. Thus, for each residue in $a_0 \in (\mathbb{Z}/b\mathbb{Z})^*$ with multiplicative order d coprime to b we have a residue class of modulus b^2d that consisting of all $ab \in \mathcal{S}_b$ with $a \equiv a_0 \pmod b$ and $a \equiv b^{-1} \pmod d$.

Let $\lambda(b)$ denote the universal exponent for the group $(\mathbb{Z}/b\mathbb{Z})^*$. Thus, the divisors of $\lambda(b)$ run over all of the possible multiplicative orders for elements in the group. For $d \mid \lambda(b)$, let $N(d,b)$ denote the set of elements $a_0 \pmod b$ with multiplicative order d. Thus,

$$\delta(\mathcal{S}_b) = \sum_{\substack{d|\lambda(b) \\ \gcd(d,b)=1}} \frac{N(d,b)}{b^2 d}. \tag{3}$$

It seems difficult to work out a formula for $N(d,b)$ but we do have the relation

$$\sum_{d|\lambda(b)} N(d,b) = \varphi(b), \tag{4}$$

which just reflects the partitioning of $(\mathbb{Z}/b\mathbb{Z})^*$ by the orders of its elements. We consider various cases. First suppose that $\lambda(b)$ is smooth, more specifically, assume that $P(\lambda(b)) < B(b) := \exp((\log b)^{1/2})$, where $P(n)$ denotes the largest prime factor of n. Note that the primes dividing $\lambda(b)$ are the same primes that divide $\varphi(b)$, so that $P(\varphi(b)) < B(b)$. Using the main result from [4], the number of such integers $b \le x$ is $\le x/B(x)$ for all sufficiently large x. Since (4) implies that the sum of $N(d,b)/d$ for $d \mid \lambda(b)$ is $\le \varphi(b) < b$, (3) implies that $\delta(\mathcal{S}_b) < 1/b$. But the sum of $1/b$ over such a sparse set of b's is easily seen to converge via a partial summation argument.

So, we may assume that $p_b := P(\lambda(b)) \ge B(b)$. There are two types of numbers $d \mid \lambda(b)$ to consider: $p_b \mid d$ and $p_b \nmid d$. In the first case (4)

implies that

$$\sum_{\substack{d|\lambda(b)\\ p_b|d}} \frac{N(d,b)}{d} \le \frac{1}{p_b} \sum_{d|\lambda(b)} N(d,b) \le \frac{b}{B(b)}.$$

Suppose now $p_b \nmid d$. Since $p_b \mid \lambda(b) \mid \varphi(b)$, we have either $p_b^2 \mid b$ or one or more primes $q \equiv 1 \pmod{p_b}$ divide b. In either case the number of residues mod b with order not divisible by p_b is at most $\varphi(b)/p_b$. (Actually, since $\gcd(d,b) = 1$, the case $p_b^2 \mid b$ does not occur.) Thus,

$$\sum_{\substack{d|\lambda(d)\\ p_b\nmid d}} N(d,b) \le \frac{\varphi(b)}{p_b} \le \frac{b}{B(b)}.$$

With the above display and (3), $\delta(\mathcal{S}_b) \le 2/(bB(b))$. Since the sum of $2/(bB(b))$ converges, the proof is complete. □

Theorem 1. *Let*

$$c_0 = \lim_{k\to\infty} \delta\Big(\bigcup_{2\le b\le k} \mathcal{S}_b \Big).$$

We have $\delta(\mathcal{S}) = c_0$.

Proof. First note that Proposition 1 implies that $\bigcup_{2\le b\le k} \mathcal{S}_b$ has an asymptotic density, so that c_0 exists and $c_0 \le 1$. For a given integer $b \ge 2$, we have seen in the proof of Proposition 1 that $\mathcal{S}_b$ is the union of $N(d,b)$ residue classes mod $b^2 d$, where d runs over the divisors of $\lambda(b)$ that are coprime to b and $N(d,b)$ is the number of residues mod b of multiplicative order d. Note that $b^2 d < b^3$. It follows from a complete inclusion-exclusion argument that the number of $n \le x$ in $\bigcup_{2\le b\le (\log x)^{1/3}} \mathcal{S}_b$ is $(c_0 + o(1))x$ as $x \to \infty$. It thus suffices to prove that the number of $n \le x$ with $n \in \mathcal{S}_b$ for some $b > (\log x)^{1/3}$ is $o(x)$ as $x \to \infty$.

Let $\epsilon(x) \downarrow 0$ arbitrarily slowly. It follows from Erdős [9] that but for $o(x)$ integers $n \le x$, n has no divisors in the interval $(x^{1/2-\epsilon(x)}, x^{1/2+\epsilon(x)})$. In particular, but for $o(x)$ integers $n \le x$, if $n = ab$ we may assume that either $a \le x^{1/2}/B(x)$ or $b \le x^{1/2}/B(x)$, where as before, $B(x) = \exp(\sqrt{\log x})$.

We first consider numbers $n \le x$ with $n \in \mathcal{S}_b$ and $(\log x)^{1/3} < b \le x^{1/2}/B(x)$; the argument here is mostly in parallel with the proof of Proposition 1.

Using [4], the number of integers $b \in (e^j, e^{j+1}]$ with $P(\lambda(b)) \le e^{\sqrt{j+1}}$ is $\ll e^{j-\sqrt{j}}$, so the number of integers $n \le x$ divisible by one of these b's is $\ll x/e^{\sqrt{j}}$. Since the sum of $1/e^{\sqrt{j}}$ for $e^{j+1} > (\log x)^{1/3}$ is $o(1)$

as $x \to \infty$, there are at most $o(x)$ integers $n \le x$ divisible by some $b \in ((\log x)^{1/3}, x^{1/2}/B(x)]$ with $P(\lambda(b)) \le B(b)$.

Let $p_b = P(\lambda(b))$ and assume that $p_b > B(b)$. Let $d \mid \lambda(b)$ with $\gcd(d,b) = 1$ and let r be one of the $N(d,b)$ residue classes mod bd where $l_b(r) = d$ and $br \equiv 1 \pmod d$. The number of integers $n = ab \le x$ where $a \equiv r \pmod{bd}$ is at most $1 + x/(b^2 d)$, so the number of integers $n = ab \le x$ with $l_b(a) = d$ and $n \in \mathcal{S}_b$ is at most $N(d,b) + xN(d,b)/(b^2 d)$. Using (4), we have

$$\sum_{\substack{n \le x \\ n \in \mathcal{S}_b}} 1 \le b + x \sum_{d \mid \lambda(b)} \frac{N(d,b)}{b^2 d}. \tag{5}$$

Since the sum of b for $b \le x^{1/2}/B(x) = o(x)$, we wish to show that

$$\sum_{(\log x)^{1/3} < b \le x^{1/2}/B(x)} \sum_{d \mid \lambda(b)} \frac{N(d,b)}{b^2 d} = o(1), \quad x \to \infty. \tag{6}$$

By (4) the contribution to the sum in (6) when $p_b \mid d$ is $\le 1/(bp_b) \le 1/(bB(b))$. Summing this for $b > (\log x)^{1/3}$ is $o(1)$ as $x \to \infty$.

Now consider the case $p_b \nmid d$. As we have seen in the proof of Proposition 1, we have

$$\sum_{\substack{d \mid \lambda(b) \\ p_b \nmid d}} N(d,b) \le \frac{\varphi(b)}{p_b}.$$

Thus, the inner sum in (6) is $\le 1/(bp_b) \le 1/(bB(p))$. Summing on $b > (\log x)^{1/3}$ this is $o(1)$ as $x \to \infty$.

We have just shown that the number of integers $n \le x$ of the form ab where $n \in \mathcal{S}_b$ and $(\log x)^{1/3} < b \le x^{1/2}/B(x)$ is $o(x)$ as $x \to \infty$. It remains to consider the case $a \le x^{1/2}/B(x)$.

The number of integers $n \le x$ of the form ab with $a \le x^{1/2}/B(x)$ and $P(b) \le B(x)$ is

$$\ll \sum_{a \le x^{1/2}/B(x)} \frac{x}{aB(x)} = o(x), \quad x \to \infty,$$

using standard estimates on the distribution of smooth numbers (or even using [4]). Now say $n \le x$ is of the form ab with $1 < a \le x^{1/2}/B(x)$ and $n \in \mathcal{S}_b$. This implies that $a^{ab-1} \equiv 1 \pmod b$. Let $q = P(b)$, which we may assume is $> B(x)$ and note that $l_a(q) \mid ab - 1$. Write $b = qm$ and since $b \equiv m \pmod{q-1}$, we have $l_a(q) \mid am - 1$. We distinguish two cases: $m \le B(x)^{1/2}$, $m > B(x)^{1/2}$.

Suppose that $m \le B(x)^{1/2}$. Since $l_a(q) \mid am - 1$, we have $q \mid a^{am-1} - 1$. For a given choice of a, m, the number of primes q with

this property is $\ll am \log a$. Summing this expression over a, m we get $\ll (x \log x)/B(x)$, and so the number of integers ab is $o(x)$.

Next suppose that $m > B(x)^{1/2}$, so that $q < x/(aB(x)^{1/2})$. For a, q given, the number of m is at most $1 + x/(aql_a(q))$. The sum of "1" over q is no problem, it is at most $\pi(x/(aB(x)^{1/2})$, and so summing on a, we get $\ll x/B(x)^{1/2} = o(x)$. If $l_a(q) > B(x)^{1/3}$, then summing $x/(aql_a(q)) < x/(aqB(x)^{1/3})$ is also no problem. So, suppose that $l_a(q) \le B(x)^{1/3}$. Since there are at most $k \log a$ primes dividing $a^k - 1$, by summing on $k \le B(x)^{1/3}$ we see that the number of choices for q is at most $B(x)^{2/3} \log x$. Since $q > B(x)$, we have the sum of $x/(aq)$ over these q's at most $(x \log x)/(aB(x)^{1/3})$, which is negligible when summed over a. □

An issue remains: Show that $c_0 < 1$. This could be done say by taking the sets $\mathcal{S}_b$ up to some moderate point, maybe 100, and find a good upper bound for the density of the tail for $b > 100$. We have the exact formula for $\delta(\mathcal{S}_b)$ in (3) and perhaps we can work with that to show the sum of the densities for large b is small. Some helpful thoughts on this: If $b > 2$ and $b \equiv 2 \pmod 4$, then $\mathcal{S}_b \subset \mathcal{S}_2$, so it need not be looked at again. Also see below about $\mathcal{T}_b$. Another possibly helpful thought: For $b = p$ prime,

$$\sum_{d|\lambda(p)} \frac{N(d,p)}{d} = \sum_{d|\lambda(p)} \frac{\varphi(d)}{d} \le \tau(p-1),$$

where $\tau(n)$ is the number of divisors of n.

It seems interesting in this context to consider the function $N(G)$ for a finite abelian group G defined as follows:

$$N(G) = \sum_{d|\#G} \frac{N(d,G)}{d}, \quad \text{where } N(d,G) = \#\{g \in G : g \text{ has order } d\}.$$

Writing $G = G_{p_1} \times \cdots \times G_{p_k}$, where G_p is a p-group and $p_1, \dots, p_k$ are the distinct primes dividing $\#G$, we have

$$N(G) = \prod_{p|\#G} N(G_p).$$

So to get a formula or inequality for $N(G)$ it suffices to do so in the special case of a finite abelian p-group. The literature has papers on counting cyclic subgroups, which is essentially the same problem. For example, see Tóth [23]. Using this, perhaps we have

$$N(G) \le \frac{\tau(\lambda(G))\#G}{\lambda(G)},$$

where $\lambda(G)$ is the universal exponent for G. In the case of interest for Ordowski's conjecture, this assertion is

$$\sum_{d|\lambda(b)} \frac{N(d,b)}{d} \le \frac{\tau(\lambda(b))\varphi(b)}{\lambda(b)}.$$

This would supply an alternate approach to proving our theorem that might lend itself more readily to showing that $c_0 < 1$.

These thoughts ignore the condition that $\gcd(d,b) = 1$, but especially numerically it would not be hard to remove the local factors corresponding to primes dividing $\gcd(\lambda(b), b)$.

With c_1 as in (2), I believe we have

$$\sum_{n\le x} D(n) \sim c_1 x, \quad x \to \infty.$$

Let $\mathcal{T}_b = \mathcal{S}_b \setminus \bigcup_{2\le j<b} \mathcal{S}_j$. Then $\mathcal{T}_b$ is a finite union of residue classes, $\mathcal{S}$ is the disjoint union of the $\mathcal{T}_b$'s, and

$$\delta(\mathcal{S}) = \sum_{b\ge 2} \delta(\mathcal{T}_b). \tag{7}$$

We illustrate for $b = 3$. For $\mathcal{T}_3$, note that when $a \equiv 1 \pmod 3$, we have $3a \equiv 2 \pmod 4$ with the same frequency as all numbers, so this part of $\mathcal{S}_3$ contributes a density of $\frac{3}{4} \times \frac{1}{9} = \frac{1}{12}$ to $\mathcal{T}_3$. In the other part of $\mathcal{S}_3$ when $a \equiv 5 \pmod 6$, we have $3a$ odd, so we can put all of it in $\mathcal{T}_3$. Thus, $\delta(\mathcal{T}_3) = \frac{1}{12} + \frac{1}{18} = \frac{5}{36}$.

3. Pseudoprimes in residue classes

Lots of tables and numbers go here with some words on how they were found.

Dedication Our proof of Ordowski's conjecture bears some resemblance to a series of papers of Aleksandar Ivić [8, 13, 14] dealing with tight estimates for the reciprocal sum of the largest prime factor of an integer. We trust he would have enjoyed the connection, and we dedicate this paper to his memory.

References

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

[2] R. J. Baillie and S. S.Wagstaff, Jr., Lucas pseudoprimes, *Math. Comp.* **35** (1980), 1391–1417.

[3] A. S. Bang, Taltheoretiske Undersøgelser. *Tidsskrift for Mathematik. 5. Mathematica Scandinavica. 4* **4** (1886), 70–80.

[4] W. D. Banks, J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, Counting integers with a smooth totient, *Quarterly J. Math.* **70** (2019), 1371–1386.
[5] W. D. Banks and C. Pomerance, On Carmichael numbers in arithmetic progressions, *J. Australian Math. Soc.* **28** (2010), 313–321.
[6] N. G. W. H. Beeger, On even numbers m dividing 2^m-2, *Amer. Math. Monthly* **58** (1951), 553–555.
[7] R. D. Carmichael, A new number-theoretic function, *Bull. Amer. Math. Soc.* **16** (1910), 232–238.
[8] J.-M. De Koninck and A. Ivić, Topics in arithmetical functions, Asymptotic formulae for sums of reciprocals of arithmetical functions and related results. Notas de Matemática [Mathematical Notes], 72. North-Holland Publishing Co., Amsterdam-New York, 1980.
[9] P. Erdős, A generalization of a theorem of Besicovitch, *J. London Math. Soc.* **11** (1936), 92–98.
[10] P. Erdős, On pseudoprimes and Carmichael numbers, *Publ. Math. Debrecen* **4** (1956), 201–206.
[11] H. Halberstam and H.-E. Richert, Sieve Methods, London Mathematical Society Monographs, No. 4. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London – New York, 1974.
[12] G. Harman, On the number of Carmichael numbers up to x, *Bull. London Math. Soc.* **37** (2005), 641–650.
[13] A. Ivić, Sum of reciprocals of the largest prime factor of an integer, *Arch. Math.* **36** (1981), 57–61.
[14] A. Ivić and C. Pomerance, Estimates for certain sums involving the largest prime factor of an integer, *Proc. Colloquium on Number Theory* **34** (1981), Topics in Classical Number Theory, North-Holland, 1984, 769–789.
[15] S. Li, On the distribution of even pseudoprimes, unpublished, 1996.
[16] K. Matomäki, Carmichael numbers in arithmetic progressions, *J. Australian Math. Soc.* **94** (2013), 268–275.
[17] L. Monier, Evaluation and comparison of two efficient probabilistic primality testing algorithms, *Theoret. Comput. Sci.* **12** (1980), 97–108.
[18] T. Ordowski, Density of Fermat weak pseudoprimes k to a base d, where $d \mid k$ and $1 < d < k$, http://list.seqfan.eu/pipermail/seqfan/2021-January/021256.html .
[19] C. Pomerance, On the distribution of pseudoprimes, *Math. Comp.* **37** (1981), 587–593.
[20] C. Pomerance, A note on Carmichael numbers in residue classes, preprint, 2021, arXiv:2101.09906 [math.NT].
[21] A. Rotkiewicz, On the pseudoprimes of the form $ax + b$, *Proc. Camb. Phil. Soc.* **63** (1967), 389–391.
[22] V. Šimerka, Zbytky z arithmetické posloupnosti. (Czech) [On the remainders of an arithmetic progression]. Časopis pro pěstování mathematiky a fysiky, **14** (1885), 221–225.
[23] L. Tóth, On the number of cyclic subgroups of a finite abelian group, *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)* **55(103)** (2012), 423–428.
[24] T. Wright, Infinitely many Carmichael numbers in arithmetic progressions, *Bull. London Math. Soc.* **45** (2013), 943–952.

Mathematics Department, Dartmouth College, Hanover, NH 03784
Email address: carl.pomerance@dartmouth.edu

Center for Education and Research in Information Assurance and Security and Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-1398 USA
Email address: ssw@cerias.purdue.edu