Bulletin T. CLIV de l'Académie serbe des sciences et des arts − 2021
Classe des Sciences mathématiques et naturelles
Sciences mathématiques, № 46

SOME THOUGHTS ON PSEUDOPRIMES

CARL POMERANCE, SAMUEL S. WAGSTAFF, JR.

In memory of Aleksandar Ivić (1949–2020)

(Presented at the 2nd Meeting, held on March 26, 2021)

A b s t r a c t. *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.*

AMS Mathematics Subject Classification (2020): 11N25, 11N37.
Key Words: pseudoprime, Carmichael number.

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 [26].

We now know that there are infinitely many Carmichael numbers (see [1]), the number of them up to x exceeding x^c for a constant $c > 1/3$ and for all sufficiently large x (see [16]). This count holds *a fortiori* for pseudoprimes to any fixed base a since the Carmichael numbers comprise a subset of the base-a pseudoprimes.

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 [22]) 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 [11].

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 [22]) that for all large x, the number of *odd* pseudoprimes up to x is $\le x/L(x)^{1/2}$ and an analogous result holds for base-a pseudoprimes coprime to a, for any fixed $a > 1$. Some years ago, Shuguang Li and the first author worked out a similar bound where the coprime condition is relaxed.

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 n is composite, $l_a(n_a) \mid n-1$, 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 with $n \equiv r \pmod m$, and suppose that n is a base-a pseudoprime. Let us write down some necessary conditions for this to occur. 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

$$h \mid r - 1 \quad \text{and} \quad g/g_a \mid a. \tag{1.1}$$

Further, if g is even, the residue class $r \pmod{m}$ must contain some integer k with the Jacobi symbol $(a/k_{2a}) = 1$. These facts are proved in Lemma 4.1. We conjecture that these conditions are 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 [11] 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 $x \to \infty$. We discuss this further in Section 4.

Here are a few examples. If $\gcd(r, m) = 1$ then the conditions hold for any a, and the conjecture asserts that there are infinitely many base-a pseudoprimes that are $\equiv r \pmod{m}$. In fact, this is known, see below. If $a = 2$, $r = 0$, $m = 2$, the conditions hold and we are looking at even (base-2) pseudoprimes. The first example was found by Lehmer, and their infinitude was proved by Beeger, see below. The criteria instantly tell us there are no (base-2) pseudoprimes divisible by 4, since if $a = 2$, $r = 0$, $m = 4$ we have $g = g/g_a = 4$ and $4 \nmid 2$. An interesting case is $a = 2$, $r = 15$, $m = 20$. Then $g = 5$ and $h = 4$. Since $4 \nmid 15 - 1$, the condition (1.1) fails, and indeed there are no pseudoprimes in the class 15 (mod 20). Another interesting case is $a = 2$, $r = 6$, $m = 16$. We have $g = 2$, $g_a = 1$, $h = 1$, so that (1.1) holds. But any integer $k \equiv 6 \pmod{16}$ has $k_{2a} \equiv 3 \pmod{8}$, and $(2/k_{2a}) = -1$. So, the final condition fails, and indeed there are no base-2 pseudoprimes in the class $6 \pmod{16}$.

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.

- For all large x we have $C_{0,1}(x) > x^c$, where $c > 1/3$. This is the main result of Harman [16], 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 [19].
- 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 [23] is based on the argument for a somewhat weaker bound due to Wright [28].
- If $\gcd(r, m) = 1$, then $P_{2,r,m}(x)$ is unbounded. This result of Rotkiewicz [25] 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.

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

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

From Baillie–Wagstaff [2] and Monier [20], we have

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

where p runs over primes. Now let

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

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

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

Note that $F^*(n) - F(n)$ 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

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

and let

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

T. Ordowski [21] has conjectured that $\mathcal{S}$ has an asymptotic density; counts up to 10^8 by A. Eldar suggest that this density may be about $5/8$. In Section 2 we present a proof that the density of $\mathcal{S}$ exists and in Section 3 we discuss the computation of the density.

2. *Proof of Ordowski's conjecture*

For each integer $b \geq 2$ let

$$\mathcal{S}_b = \{ab : a \geq 2,\ a^{ab} \equiv a \pmod{ab}\},$$

Then

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

Indeed, if $b \geq 2$ and $n = ab \in \mathcal{S}_b$, then $a \in \mathcal{D}(n)$, 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 $n = ab \in \mathcal{S}_b$, then $\gcd(b, a) = 1$. Indeed, if p is a common prime factor with $p^\alpha \parallel a$, then we have $p^{\alpha+1} \mid n$ and $p^{\alpha+1} \mid a^n$, contradicting $a^n \equiv a \pmod{n}$.

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

Proposition 2.1. *For each integer $b \geq 2$, $\delta(\mathcal{S}_b)$ exists and*

$$c_1 := \sum_{b \geq 2} \delta(\mathcal{S}_b) < \infty. \tag{2.1}$$

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 $2 \pmod 4$ (other than 2), with density $1/4$.

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 $1/9$. 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 $1/18$, so $\delta(\mathcal{S}_3) = 1/6$.

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 (mod 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 $b^2 d$ 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 number of elements $a_0 \pmod{b}$ with multiplicative order d. Thus,

$$\delta(\mathcal{S}_b) = \sum_{\substack{d \mid \lambda(b) \\ \gcd(d,b)=1}} \frac{N(d,b)}{b^2 d}. \tag{2.2}$$

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

$$\sum_{d \mid \lambda(b)} N(d,b) = \varphi(b), \tag{2.3}$$

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 (2.3) implies that the sum of $N(d,b)/d$ for $d \mid \lambda(b)$ is $\le \varphi(b) < b$, (2.2) 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 (2.3) implies that

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

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,

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

With the above two displays and (2.2), $\delta(\mathcal{S}_b) \le 2/(bB(b))$. Since the sum of $2/(bB(b))$ converges, the proof is complete.

Remark 2.1. An immediate corollary of Proposition 2.1 is that

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

Theorem 2.1. *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 2.1 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 2.1 that $\mathcal{S}_b$ is the union of $N(d,b)$ residue classes mod b^2d, 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 $b^2d < b^3$. 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 [10] 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 2.1.

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 $1 + x/(b^2d)$, so the number of integers $n = ab \le x$ with $l_b(a) = d$ and $n \in \mathcal{S}_b$ is at most $N(d,b) + xN(d,b)/(b^2d)$. Using (2.3), we have

$$\sum_{\substack{n\le x\\ n\in\mathcal{S}_b}} 1 \le b + x \sum_{d\,|\,\lambda(b)} \frac{N(d,b)}{b^2d}. \tag{2.4}$$

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

$$\sum_{(\log x)^{1/3} < b \le x^{1/2}/B(x)} \ \sum_{d \,|\, \lambda(b)} \frac{N(d,b)}{b^2 d} = o(1), \quad x \to \infty. \tag{2.5}$$

By (2.3) the inner sum in (2.5) 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 2.1, we have

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

Thus, the inner sum in (2.5) 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. $\square$

3. *Computation of* c_0 *and* c_1

We immediately have $0 < c_0 \le c_1$. Indeed, the second inequality is obvious from the definitions, and the first inequality follows since $\mathcal{S}$ contains all numbers $n > 2$ with $n \equiv 2 \pmod 4$. Further, it is not hard to get larger lower bounds for c_0 via an inclusion-exclusion to find the density of $\bigcup_{2\le b\le k} \mathcal{S}_b$ for small values of k. Doing this with $k = 10$ gives $880651/1260^2 \approx 0.554706$.

It is somewhat easier to get lower bounds for c_1. We have computed the sum of $\delta(\mathcal{S}_b)$ for $2 \le b \le 10^4$, getting ≈ 0.934328.

However, getting numerical upper bounds for c_0, c_1 is a challenge. Below is a table of counts of $\mathcal{S}$ up to various powers of 10, the counts to 10^8 confirm those of Eldar. In addition, we report on the sum of $D(n)$ to various powers of 10.

Table 1: Count of members of $\mathcal{S}$ below various bounds and partial sums of $D(n)$.

Bound	Count	Sum
10	2	2
10^2	52	61
10^3	591	822
10^4	6169	8962
10^5	62389	92383
10^6	625941	932490
10^7	6265910	9352861
10^8	62677099	93613688
10^9	626836390	936403866
10^{10}	6268593131	

Thus, it may be that $c_0 < 0.627$ and $c_1 < 0.937$. We can at least rigorously prove that $c_0 < 1$. Further numerical evidence is given at the end of this section.

For a finite abelian group G consider the function $N(G)$ defined as follows:

$$N(G) = \sum_{d \mid \#G} \frac{N(d, G)}{d},$$

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 $p_1, \ldots, p_k$ are the distinct primes dividing $\#G$, we have

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

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 [27]. However, it is not hard to directly prove (see below) the inequality

$$N(G) \le \frac{\tau(\lambda(G))\#G}{\lambda(G)}, \tag{3.1}$$

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

$$\sum_{d\,|\lambda(b)} \frac{N(d,b)}{d} \le \frac{\tau(\lambda(b))\varphi(b)}{\lambda(b)}. \tag{3.2}$$

This supplies an alternate approach to proving Proposition 2.1.

Indeed, we know from [12] that there is a positive constant c such that for all large n, $\lambda(n) > (\log n)^{c \log\log\log n}$. Since $\tau(k) < k^{1/2}$ for all large k, (3.2) implies that

$$\sum_{b\ge b_0} \sum_{d\,|\lambda(b)} \frac{N(d,b)}{b^2 d} \le \sum_{b\ge b_0} \frac{\tau(\lambda(b))\varphi(b)}{b^2\lambda(b)} \le \sum_{b\ge b_0} \frac{1}{b(\log b)^{\frac{c}{2}\log\log\log b}}$$

for b_0 sufficiently large. This implies the sum in Proposition 2.1 converges.

Now we show that $c_0 < 1$. Indeed, it follows from the above paragraph that for b sufficiently large, we have

$$\frac{\tau(\lambda(b))}{\lambda(b)} < \frac{1}{(\log b)^3}. \tag{3.3}$$

Note that for any k,

$$\mathcal{A}_k := \mathbb{N} \setminus \Bigg(\bigcup_{2\le b\le k} \mathcal{S}_b \Bigg)$$

contains all n with least prime factor exceeding k, so that $\delta(\mathcal{A}_k) > 1/(2\log k)$ for k sufficiently large. Thus, for k sufficiently large,

$$\begin{aligned} \delta(\mathbb{N}\setminus\mathcal{S}) &\ge \delta(\mathcal{A}_k) - \delta\Bigg(\bigcup_{b>k}\mathcal{S}_b\Bigg) \\ &> \frac{1}{2\log k} - \sum_{b>k}\delta(\mathcal{S}_b) > \frac{1}{2\log k} - \sum_{b>k}\frac{1}{b(\log b)^3}, \end{aligned}$$

using (3.2) and (3.3). Now

$$\sum_{b>k}\frac{1}{b(\log b)^3} < \int_k^\infty \frac{1}{t(\log t)^3}\,\mathrm{d}t = \frac{1}{2(\log k)^2},$$

so that for n large, $\delta(\mathbb{N} \setminus \mathcal{S}) > 1/(3 \log k) > 0$. This shows that $c_0 < 1$ as claimed.

This argument could be used in principle to get a numerical upper bound for c_0 that is < 1, but it likely would not be a very good bound.

Here is a proof of (3.1).

Lemma 3.1. *Let G be a finite abelian p group of order p^n and with exponent p^λ. Then for $0 \le j \le \lambda$, $N(p^j, G)/p^j \le p^{n-\lambda}$, and $N(G) \le \tau(p^\lambda)p^{n-\lambda}$.*

PROOF. The second assertion clearly follows from the first one, since $\tau(p^\lambda) = \lambda + 1$. So, we concentrate on the first assertion, which we prove by induction. Write G as $C_{p^{\lambda_1}} \times \cdots \times C_{p^{\lambda_k}}$, where $1 \le \lambda_1 \le \cdots \le \lambda_k$, $n = \lambda_1 + \cdots + \lambda_k$, and $\lambda = \lambda_k$. For our base cases we have $j = 0$ or $k = 1$, the lemma being clear in either case. Now assume that $j \le \lambda_1$. Then $N(p^j, G) = p^{jk} - p^{(j-1)k} < p^{jk}$, so that $N(p^j, G)/p^j < p^{j(k-1)}$. Now

$$j(k-1) \le \lambda_1(k-1) \le \lambda_1 + \cdots + \lambda_{k-1} = n - \lambda_k,$$

so the lemma holds in this case.

We assume the lemma holds for p-groups of order smaller than p^n. Suppose G has order p^n, exponent p^λ, rank $k \ge 2$, and assume that $\lambda \ge j > \lambda_1$. Let G' be the same as G except that $C_{p^{\lambda_1}}$ is replaced with $C_{p^{\lambda_1 - 1}}$ and let $G'' = C_{p^{\lambda_2}} \times \cdots \times C_{p^{\lambda_k}}$. An element of order p^j in G is uniquely expressible as (u, v) where u is an arbitrary element of $C_{p^{\lambda_1}}$ and v is an element in G'' of order p^j. The same goes for G', except u is only roaming over $C_{p^{\lambda_1 - 1}}$ instead of $C_{p^{\lambda_1}}$. Thus, we have $N(p^j, G) = pN(p^j, G')$. By the induction hypothesis, we have $N(p^j, G')/p^j \le p^{n-1-\lambda}$. Multiplying both sides by p, we have $N(p^j, G)/p^j \le p^{n-\lambda}$, which completes the proof. □

These thoughts ignore the condition that $\gcd(d, b) = 1$, but it is not hard to remove the local factors corresponding to primes dividing $\gcd(\lambda(b), b)$. In particular if $\varphi_0(b)$ is the largest divisor of $\varphi(b)$ that is coprime to b and $\lambda_0(b)$ is the largest divisor of $\lambda(b)$ coprime to b, then (3.2) can be improved to

$$\delta(\mathcal{S}_b) \le \frac{\tau(\lambda_0(b))\varphi_0(b)}{\lambda_0(b) b^2}. \tag{3.4}$$

We have summed this bound for all b with $10^4 < b \le 10^6$, getting ≈ 0.00638378, with $10^4 < b \le 10^7$, getting ≈ 0.00673006, and with $10^4 < b \le 2 \cdot 10^7$, getting ≈ 0.00677103. It seems reasonable to assume that the infinite sum of this bound for all $b > 10^4$ is < 0.007. Assuming this is so, our rigorous lower estimate of 0.934328 for c_1 should be within 0.007 of the true value, which is indeed consistent with the evidence afforded by our partial sums of $D(n)$ in Table 1.

One can also try to use these methods to get a numerical estimation for c_0, however, the rigorous estimation from below is difficult. As mentioned above, the density of $\bigcup_{2\le b\le 10}\mathcal{S}_b$ is about 0.554706. To get a reasonable bound one would want to at least replace "10" with "100" here. In estimating the tail one can ignore *imprimitive* values of b, namely a value of b with $\mathcal{S}_b\subset\mathcal{S}_{b_0}$ for some $2\le b_0<b$. For example, if $b=a_0b_0$ where $a_0,b_0\ge 2$ and $a_0\equiv 1\pmod{b_0}$, then $\mathcal{S}_b\subset\mathcal{S}_{b_0}$. In particular, this holds whenever $b\equiv 2\pmod 4$ with $b>2$, or when $b=3m$ with $m>1$ and $m\equiv 1\pmod 3$.

We have shown that the density of the set $\mathcal{S}$ of n with $D(n)\ge 1$ exists. We mention that our results show that the set of numbers n with $D(n)\ge k$, for any fixed k, has a positive asymptotic density. To see this, note that if $n\equiv p\pmod{p^2}$ for each of the first k primes (or any set of k primes), then $D(n)\ge k$. A complicated inclusion-exclusion shows that the density exists.

4. *Pseudoprimes in residue classes*

We begin with a proof of necessity of the conditions from the Introduction for a residue class to contain a base-a pseudoprime. Recall the notation n_a as the largest divisor of n that is coprime to a.

Lemma 4.1. *Suppose a,r,m are integers with $a\ge 2$ and $m>0$. Let $g=\gcd(r,m)$ and $h=\gcd(l_a(g_a),m)$. If there is an integer $n\equiv r\pmod m$ with n a base-a pseudoprime, then $h\mid r-1$, $g/g_a\mid a$, and in the case that g is even, there is an integer $k\equiv r\pmod m$ with the Jacobi symbol $(a/k_{2a})=1$.*

PROOF. Suppose $n\equiv r\pmod m$ is a base-a pseudoprime. Then $a^n\equiv a\pmod n$ and this implies that $a^n\equiv a\pmod{g_a}$. Since $\gcd(a,g_a)$ is 1, we thus have $a^{n-1}\equiv 1\pmod{g_a}$. Thus, $l_a(g_a)\mid n-1$, so that $h\mid n-1$. We have $n-1\equiv r-1\pmod m$, so that $n-1\equiv r-1\pmod h$, which implies $r-1\equiv 0\pmod h$. Also, write g as ug_a, so that $u=g/g_a$ is the largest divisor of a all of whose prime factors also divide a. Since $u\mid n$, the congruence $a^n\equiv a\pmod n$ implies that $u\mid a$ (if some prime divides u to a higher exponent than it divides a, then a^n and n both have more factors of this prime than does a, a contradiction). This proves the first part of the condition. Now suppose that g is even. Then n is even, so that a^n is a square mod n. Since $a^n\equiv a\pmod n$, we have that a too is a square mod n. In particular a is a square modulo the largest odd divisor of n coprime to a, namely n_{2a}. Thus, $(a/n_{2a})=1$. This completes the proof. □

As mentioned in the Introduction, we conjecture that the conditions of Lemma 4.1 are not only sufficient for there to be a pseudoprime base a in the residue class $r\pmod m$, but sufficient for there to be infinitely many. We conjecture this based not only on the fact that it has been proved in many cases, but on the Erdős heuristic in [11].

Let us illustrate this heuristic in the case of (base-2) pseudoprimes $n \equiv 0 \pmod 2$. We already know that there are infinitely many, but the Erdős heuristic implies the number of them up to x is $> x^{1-\epsilon}$ for any fixed $\epsilon > 0$ and x sufficiently large depending on ϵ. Consider primes $p \le y$ with $P(p-1) < y^\epsilon$ and $p \equiv 7 \pmod 8$. Without the congruence condition it is already conjectured that this entails a positive proportion of the primes to y, just as we know unconditionally that there is a positive proportion of integers $n \le y$ with $P(n) < y^\epsilon$. Adding in the congruence condition mod 8 for primes should not matter, and it provably doesn't matter when counting integers. So, assume there are at least $c_\epsilon \pi(y)$ primes $p \le y$ with $P(p-1) < y^\epsilon$ and $p \equiv 7 \pmod 8$, where $c_\epsilon > 0$ and y is sufficiently large depending on the choice of ϵ. Say the set of primes is $\mathcal{P}_\epsilon(y)$.

Let $x = y^y$ and take subsets of $\mathcal{P}_\epsilon(y^{1/\epsilon})$ of size $\lfloor \epsilon \log(x/2)/\log y \rfloor$. Multiply the primes in each subset, so in this way, each such subset corresponds to an integer $n \le x/2$. Since we are assuming that $\#\mathcal{P}_\epsilon(y^{1/\epsilon}) \ge c_\epsilon \pi(y^{1/\epsilon})$, the number of subsets formed in this way is $x^{1-\epsilon+o(1)}$. Is $2n$ a pseudoprime? For this to be so we would need $l(n) \mid 2n-1$, that is, $2n \equiv 1 \pmod{l(n)}$. This condition forces $l(n)$ to be odd, but at least we already know this since the primes dividing n are all $\equiv 7 \pmod 8$, which implies that $l(n) \mid \lambda(n)/2$ and that $\lambda(n) \equiv 2 \pmod 4$. Let L be the lcm of all prime powers $p^a \le y^{1/\epsilon}$ with $2 < p < y$. Then $L < (y^{1/\epsilon})^{\pi(y)} = x^{o(1)}$. The "probability" that $2n \equiv 1 \pmod L$ should be about $1/L$. Assuming this, the "expected" number of pseudoprimes constructed this way is at least $x^{1-\epsilon+o(1)}$.

Tables 2 to 5 show the counts of pseudoprimes to base 2 for even moduli up to 20. Compare with the first columns of Table 4 in [24]. The "Fraction" column gives the fraction of pseudoprimes in that class below 10^{16}. The symbol "–" means that there are no pseudoprimes in that class due to the conditions in Lemma 4.1. The symbol "na" in the last column means that that count is not available.

Observe that the odd pseudoprimes far outnumber the even ones for numbers of the sizes we can compute. It would be nice to prove that this continues to hold as one counts to higher levels.

As we mentioned in [24], for most moduli m, the residue class $1 \pmod m$ is most popular. In that work, which gave the counts up to $25 \cdot 10^9$, we said that the first exception was $m = 37$, which had more pseudoprimes in class 0 than in class $1 \pmod{37}$. Additional computing reported here finds that $1 \pmod{37}$ had more pseudoprimes than $0 \pmod{37}$ already at 10^{14}.

Important table entries for judging the conditions in Lemma 4.1 are the zero counts. We list the first few classes with no pseudoprimes up to 10^{16} in Table 6.

The reader can check using Lemma 4.1 that the residue classes in Table 6 contain no pseudoprime to base 2. We searched all moduli $m \leq 300$ for empty residue classes up to 10^{16} and found only those predicted by Lemma 4.1.

Feitsma has computed all odd pseudoprimes to base 2 below 2^{64}. They are available at the url [13]. We computed the even pseudoprimes to base 2 below 10^{16} on two compute clusters at Purdue University. The algorithm tested the congruence $2^n \equiv 2 \pmod{n}$ for every $n \equiv 2$ or $14 \pmod{16}$, except for multiples of 9. It would have run in about half of the time if we had replaced the condition on multiples of 9 with the condition that $\gcd(n, 2145) = 1$. Also, the methods of Feitsma (based on earlier work of Galway) could be applied to the even pseudoprime count, giving further speed-ups.

Table 2: Number of pseudoprimes to base 2 below various limits in residue classes mod 2, 4, 6, and 8

Mod	Class	$\leq 10^8$	$\leq 10^{12}$	$\leq 10^{16}$	Fraction	odd $\leq 2^{64}$
2	0	7	155	2045	0.000431	na
	1	2057	101629	4744920	0.999569	118968378
4	0	–	–	–	–	–
	1	1781	90317	4215953	0.888137	104532818
	2	7	155	2045	0.000431	na
	3	276	11312	528967	0.111433	14435560
6	0	–	–	–	–	–
	1	1667	86672	4074420	0.858321	101153215
	2	0	12	72	0.000015	na
	3	117	2251	44084	0.009287	532193
	4	7	143	1973	0.000416	na
	5	273	12706	626416	0.131961	17282970
8	0	–	–	–	–	–
	1	1144	60415	2869324	0.604454	70734813
	2	4	84	1030	0.000217	na
	3	131	5646	264955	0.055816	7220309
	4	–	–	–	–	–
	5	637	29902	1346629	0.283682	33798005
	6	3	71	1015	0.000214	na
	7	145	5666	264012	0.055617	7215251

Table 3: Number of pseudoprimes to base 2 below various limits in residue classes mod 10, 12, and 14

Mod	Class	$\leq 10^8$	$\leq 10^{12}$	$\leq 10^{16}$	Fraction	odd $\leq 2^{64}$
10	0	–	–	–	–	–
	1	1082	61119	2969756	0.625612	73942273
	2	0	14	100	0.000021	na
	3	255	12198	565493	0.119127	14942850
	4	0	14	112	0.000024	na
	5	203	5695	160728	0.033859	2517967
	6	6	116	1735	0.000365	na
	7	286	12643	597165	0.125799	15879976
	8	1	11	98	0.000021	na
	9	231	9974	451778	0.095172	11685312
12	0	–	–	–	–	–
	1	1436	77269	3641316	0.767083	89412801
	2	0	12	72	0.000015	na
	3	6	90	1048	0.000221	7743
	4	–	–	–	–	–
	5	234	10887	531601	0.111988	14595567
	6	–	–	–	–	–
	7	231	9403	433104	0.091238	11740414
	8	–	–	–	–	–
	9	111	2161	43036	0.009066	524450
	10	7	143	1973	0.000416	na
	11	39	1819	94815	0.019974	2687403
14	0	1	28	363	0.000076	na
	1	757	42605	2155951	0.454175	54972365
	2	1	8	119	0.000025	na
	3	230	11111	510841	0.107614	13250508
	4	0	12	120	0.000025	na
	5	212	10315	476087	0.100293	12230634
	6	2	12	117	0.000025	na
	7	228	8546	288424	0.060760	5156009
	8	0	65	1073	0.000226	na
	9	218	9407	420766	0.088639	10637121
	10	2	14	124	0.000026	na
	11	184	9178	409825	0.086334	10310802
	12	1	16	129	0.000027	na
	13	228	10467	483026	0.101755	12410939

Table 4: Number of pseudoprimes to base 2 below various limits in residue classes mod 16 and 18

Mod	Class	$\leq 10^8$	$\leq 10^{12}$	$\leq 10^{16}$	Fraction	odd $\leq 2^{64}$
16	0	–	–	–	–	–
	1	716	39177	1896100	0.399434	47068200
	2	4	84	1030	0.000217	na
	3	65	2795	132181	0.027845	3609796
	4	–	–	–	–	–
	5	320	15334	696877	0.146805	17571790
	6	–	–	–	–	–
	7	76	2901	132347	0.027880	3609439
	8	–	–	–	–	–
	9	428	21238	973224	0.205020	23666613
	10	–	–	–	–	–
	11	66	2851	132774	0.027970	3610513
	12	–	–	–	–	–
	13	317	14568	649752	0.136877	16226215
	14	3	71	1015	0.000214	na
	15	69	2765	131665	0.027737	3605812
18	0	–	–	–	–	–
	1	990	54852	2654508	0.559201	65743806
	2	0	5	24	0.000005	na
	3	54	1117	21926	0.004619	266159
	4	1	20	247	0.000052	na
	5	101	4197	208745	0.043974	5762593
	6	–	–	–	–	–
	7	341	15987	709937	0.149556	17704708
	8	0	6	27	0.000006	na
	9	–	–	–	–	–
	10	6	98	1488	0.000313	na
	11	90	4287	208982	0.044024	5760564
	12	–	–	–	–	–
	13	336	15833	709975	0.149564	17704701
	14	0	1	21	0.000004	na
	15	63	1134	22158	0.004668	266034
	16	0	25	238	0.000050	na
	17	82	4222	208689	0.043963	5759813

Table 5: Number of pseudoprimes to base 2 below various limits in residue classes mod 20

Mod	Class	$\leq 10^8$	$\leq 10^{12}$	$\leq 10^{16}$	Fraction	odd $\leq 2^{64}$
20	0	–	–	–	–	–
	1	943	55255	2711430	0.571192	67162651
	2	0	14	100	0.000021	na
	3	33	1558	76876	0.016195	2162054
	4	–	–	–	–	–
	5	203	5695	160728	0.033859	2517967
	6	6	116	1735	0.000365	na
	7	69	2505	127520	0.026863	3630971
	8	–	–	–	–	–
	9	196	8589	385533	0.081217	9822399
	10	–	–	–	–	–
	11	139	5864	258326	0.054419	6779622
	12	–	–	–	–	–
	13	222	10640	488617	0.102933	12780796
	14	0	14	112	0.000024	na
	15	–	–	–	–	–
	16	–	–	–	–	–
	17	217	10138	469645	0.098936	12249005
	18	1	11	98	0.000021	na
	19	35	1385	66245	0.013955	1862913

Table 6: List of residue classes for even moduli up to 26 with no pseudoprimes to base 2 up to 10^{16}

Modulus	Empty classes
4	0
6	0
8	0 4
9	0
10	0
12	0 4 6 8
16	0 4 6 8 10 12
18	0 6 9 12
20	0 4 8 10 12 15 16
21	0 14
22	0
24	0 4 6 8 12 16 18 20
25	0
26	0

Dedication. Our proof of Ordowski's conjecture bears some resemblance to a series of papers of Aleksandar Ivić [9, Ch. 6], [17], [18] 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.

In addition to Professor Ivić, the year 2020 saw the passing of too many people. Among these were John Conway and Richard Guy. They had a deep interest in pseudoprimes, for example, Section A12 of [14] is devoted entirely to this subject. With Schneeberger and Sloane, they had a quite remarkable paper [8] on pseudoprimes. For each integer $a \geq 0$, let n_a be the least composite number with $a^{n_a} \equiv a \pmod{n_a}$. Then of course $n_a \leq 561$, the first Carmichael number. What they showed is the remarkable fact that the sequence $n_0, n_1, \ldots$ is periodic with period $23\#277\#$, where $p\#$ is the product of the primes up to p. Who knew?

Acknowledgement. The research of the second author was supported by the CERIAS Center at Purdue University.

REFERENCES

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

[2] R. J. Baillie, 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** (1886), 70–80.

[4] W. D. Banks, J. B. Friedlander, C. Pomerance, I. E. Shparlinski, *Counting integers with a smooth totient*, Quarterly J. Math. **70** (2019), 1371–1386.

[5] W. D. Banks, 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. H. Conway, R. K. Guy, W. A. Schneeberger, N. J. A. Sloane, *The primary pretenders*, Acta Arith. **78** (1997), 307–313.

[9] J.-M. De Koninck, 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.

[10] P. Erdős, *A generalization of a theorem of Besicovitch*, J. London Math. Soc. **11** (1936), 92–98.

[11] P. Erdős, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen **4** (1956), 201–206.

[12] P. Erdős, C. Pomerance, E. Schmutz, *Carmichael's λ function*, Acta Arith. **58** (1991), 363–385.

[13] Jan Feitsma, *The database of odd pseusdoprimes to base 2 <* 2^{64} *is at* http://www.cecm.sfu.ca/Pseudoprimes/index-2-to-64.html.

[14] R. K. Guy, *Unsolved Problems in Number Theory,* 3rd ed., Springer–Verlag, New York, 2004.

[15] H. Halberstam, H.-E. Richert, *Sieve Methods*, London Mathematical Society Monographs, No. 4. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London – New York, 1974.

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

[17] A. Ivić, *Sum of reciprocals of the largest prime factor of an integer*, Arch. Math. **36** (1981), 57–61.

[18] A. Ivić, 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.

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

[20] L. Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoret. Comput. Sci. **12** (1980), 97–108.

[21] 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 . Also see A340749 in the Online Encyclopedia of Integer Sequences.

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

[23] C. Pomerance, *A note on Carmichael numbers in residue classes*, preprint, 2021, arXiv:2101.09906 [math.NT].

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

[25] A. Rotkiewicz, *On the pseudoprimes of the form* $ax + b$, Proc. Camb. Phil. Soc. **63** (1967), 389–391.

[26] V. Šimerka, *Zbytky z arithmetické posloupnosti* (Czech) [*On the remainders of an arithmetic progression*]. Časopis pro pěstování mathematiky a fysiky, **14** (1885), 221–225.

[27] 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.

[28] T. Wright, *Infinitely many Carmichael numbers in arithmetic progressions*, Bull. London Math. Soc. **45** (2013), 943–952.

Mathematics Department, Dartmouth College, Hanover, NH 03784
e-mail: 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
e-mail: ssw@cerias.purdue.edu