On Carmichael numbers in arithmetic progressions

William D. Banks
Department of Mathematics
University of Missouri
Columbia, MO 65211 USA
bbanks@math.missouri.edu

Carl Pomerance
Department of Mathematics
Dartmouth College
Hanover, NH 03755-3551 USA
carl.pomerance@dartmouth.edu

January 19, 2010

We dedicate this paper to our friend Alf van der Poorten

Abstract

Assuming a conjecture intermediate in strength between one of Chowla and one of Heath-Brown on the least prime in a residue class, we show that for any coprime integers a and $m \geqslant 1$, there are infinitely many Carmichael numbers in the arithmetic progression $a \bmod m$.

1 Introduction

For every prime number n, *Fermat's little theorem* states that

$$b^n \equiv b \bmod n \qquad \text{for all } b \in \mathbb{Z}. \tag{1}$$

Around 1910, Carmichael began an in-depth study of *composite* numbers n with this property, which are now known as *Carmichael numbers*. In 1994 the existence of infinitely many Carmichael numbers was established by Alford, Granville and Pomerance [1].

Since prime numbers and Carmichael numbers are linked by the common property (1), it is natural to ask whether certain known results about primes can also be established for Carmichael numbers. In the present note, we focus on the question of whether an analogue of *Dirichlet's theorem* on primes in an arithmetic progression holds for the set of Carmichael numbers. Below, we give a conditional proof in support of the following:

Conjecture. *There are infinitely many Carmichael numbers in any arithmetic progression* $a \bmod m$ *with* $\gcd(a, m) = 1$.

In fact, we believe a stronger assertion holds. A necessary condition that there is at least one Carmichael number in the residue class $a \bmod m$ is that $\gcd(g, 2\,\varphi(g)) = 1$, where $g = \gcd(a, m)$ and φ is Euler's function. It is reasonable to conjecture that this condition is also sufficient for the existence of infinitely many Carmichael numbers in the residue class $a \bmod m$. However, our conditional argument does not appear to extend to this more general case.

The idea behind our argument is to construct Carmichael numbers with the special form $n \cdot p$, where n is a Carmichael number congruent to 1 mod m, and p is a prime congruent to a mod m. To produce Carmichael numbers in the arithmetic progression 1 mod m, we use a straightforward variant of the Alford–Granville–Pomerance construction. The real difficulty in our approach lies in finding primes $p \equiv a \bmod m$ such that n and np are both Carmichael numbers. To do this, we must assume (a weak version of) a conjecture of Heath-Brown on the smallest prime in an arithmetic progression, hence our principal result is conditional.

More precisely, for any integers a, d with $1 \leqslant a \leqslant d-1$ and $\gcd(a, d) = 1$, let $\varrho(d, a)$ be the least prime p in the arithmetic progression $a \bmod d$, and put

$$\varrho(d) = \max\{\varrho(d, a) \ : \ 1 \leqslant a \leqslant d - 1, \ \gcd(a, d) = 1\}.$$

In 1934, Chowla [3] showed that the bound $\varrho(d) \ll_\varepsilon d^{2+\varepsilon}$ with any $\varepsilon > 0$ follows from the generalized Riemann hypothesis, and he conjectured that the stronger bound $\varrho(d) \ll_\varepsilon d^{1+\varepsilon}$ holds. In 1978, Heath-Brown [6], following thoughts of Cramér on gaps between consecutive primes, conjectured that the bound $\varrho(d) \ll d(\log d)^2$ holds uniformly for all $d \geqslant 2$. In the present note we shall assume that the bound

$$\varrho(d) \ll d^{1+\xi/\log\log d} \qquad (d \geqslant 2) \tag{2}$$

holds with a specific real number $\xi > 0$ identified in the proof of our principal result. Note that this hypothesis is stronger than the conjecture of Chowla but weaker than that of Heath-Brown.

Theorem 1. *There is a value of $\xi > 0$ such that if (2) holds for ξ, then there are infinitely many Carmichael numbers in any arithmetic progression $a \bmod m$ with $\gcd(a, m) = 1$.*

We remark that Rotkiewicz [10, 11] proved this result unconditionally for *pseudoprimes* (that is, composite integers n such that $2^n \equiv 2 \bmod n$), and later, van der Poorten and Rotkiewicz [9] established the same result for *strong pseudoprimes* relative to an arbitrary (fixed) base $b \geqslant 2$.

In Section 3, we give a quantitative version of Theorem 1 under the same hypothesis (2); see Theorem 2. We also give a quantitative version of Theorem 1 under the slightly stronger hypothesis that the bound

$$\varrho(d) \ll d \exp((\log d)^\kappa) \qquad (d \geqslant 2) \tag{3}$$

holds with some fixed real number $\kappa < 1$; see Theorem 3.

In Section 4 we conclude with a few additional remarks.

Acknowledgements. The authors would like to thank Igor Shparlinski for numerous helpful conversations. The work on this paper began during a visit by the first author to Macquarie University; the hospitality and support of this institution are gratefully acknowledged. The second author was supported in part by NSF grant DMS-0703850.

2 Preliminaries

In what follows, the letters p and q always denote prime numbers. We denote by $\pi(x)$ the prime counting function, and by $\lambda(n)$ the *Carmichael function*,

i.e., the order of the largest cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. For an integer $n > 1$, we denote by $P(n)$ the largest prime that divides n.

The following result, which is [2, Proposition 1.5], is crucial for our construction of Carmichael numbers in the next section.

Lemma 1. *There exists a constant $c_0 > 0$ such that for any fixed coprime integers a and $m \geqslant 1$, if x is sufficiently large (depending on m) and if L is a squarefree integer that is coprime to m, then there is an integer $k \leqslant x^{3/5}$ such that*

$$\big|\{d \mid L \ : \ p = dk + 1 \text{ is prime}, p \leqslant x, \text{and } p \equiv a \bmod m\}\big| > \frac{c_0}{\varphi(m)\log x}\big|\{d \mid L \ : \ d \leqslant x^{2/5}\}\big|.$$

For a finite abelian group $\mathcal{G}$, the *Davenport constant* $D(\mathcal{G})$ is the least positive integer D with the property that for any sequence of D elements from $\mathcal{G}$, there is a nonempty subsequence whose product is the identity. Clearly $D(\mathcal{G}) \geqslant \lambda(\mathcal{G})$, where $\lambda(\mathcal{G})$ denotes the maximal order of an element in $\mathcal{G}$. We shall use the following result, which is a weakened form of [1, Theorem 1.1].

Lemma 2. *If $\mathcal{G}$ is a finite abelian group, then $D(\mathcal{G}) < \lambda(\mathcal{G})(1 + \log|\mathcal{G}|)$.*

Finally, we need the following lemma, which is [1, Proposition 1.2].

Lemma 3. *Let $\mathcal{G}$ be a finite abelian group and let $r > t > n = D(\mathcal{G})$ be integers. Then any sequence of r elements of $\mathcal{G}$ contains at least $\binom{r}{t}/\binom{r}{n}$ distinct subsequences of length at most t and at least $t - n$, whose product is the identity.*

3 Quantitative results

Theorem 2. *There is a value of $\xi > 0$ such that if (2) holds for ξ, then there is a constant $c > 0$ such that for any fixed coprime integers a and $m \geqslant 1$, one has*

$$\big|\{n \leqslant X \ : \ n \text{ is Carmichael and } n \equiv a \bmod m\}\big| \geqslant X^{c/\log\log\log X}$$

for all sufficiently large X (depending on the choice of m).

Proof. Let the coprime integers a and $m \geqslant 1$ be fixed. Let y be a real parameter which we shall choose to be large and put

$$\mathcal{Q} = \{q \text{ prime } : \ y^3/\log y < q \leqslant y^3, \ P(q-1) \leqslant y\}.$$

Note that if y is large enough, then no prime factor of m lies in $\mathcal{Q}$. Let L denote the product of the primes in $\mathcal{Q}$. We know from Friedlander [4] that $|\mathcal{Q}| \geqslant c_1\pi(y^3)$ for some absolute constant $c_1 > 0$; therefore,

$$L \geqslant \exp((c_1 + o(1))y^3) \qquad (y \to \infty).$$

On the other hand, since L divides (hence does not exceed) the product of all primes up to y^3, we have

$$L \leqslant \exp((1 + o(1))y^3) \qquad (y \to \infty). \tag{4}$$

We apply Lemma 1 with $x = L^{5/2}$. Since all of the $2^{|\mathcal{Q}|}$ divisors d of L satisfy $d \leqslant x^{2/5}$, we see that there is an integer $k \leqslant x^{3/5}$ for which the set

$$\mathcal{P} = \{p \text{ prime } : \ p \leqslant x, \ p = dk + 1 \text{ for some } d \mid L, \text{ and } p \equiv a \bmod m\}$$

has cardinality

$$|\mathcal{P}| \geqslant \frac{c_0}{\varphi(m)\log x}\, 2^{|\mathcal{Q}|} \geqslant \exp\left(\tfrac{1}{5}c_1 y^3/\log y\right) \tag{5}$$

for all large y, since $1/5 < (\log 2)/3$.

It is not so important that members of $\mathcal{P}$ are congruent to a mod m; what *is* important is that the progressions 1 mod kL and a mod m are compatible (since $\mathcal{P}$ is nonempty and $\gcd(L, m) = 1$) and thus may be glued to a single progression a' mod $\operatorname{lcm}[kL, m]$, where $\gcd(a', \operatorname{lcm}[kL, m]) = 1$. Let p_0 be the least prime in this progression, so that assuming (2) with $\xi = \frac{1}{10}c_1$ we have

$$p_0 \ll kLm \exp\left(\tfrac{1}{10}c_1 \log(kLm)/\log\log(kLm)\right).$$

Since m is fixed and $k \leqslant x^{3/5} = L^{3/2}$, using (4) we derive the bound

$$p_0 \leqslant kL \exp\left((\tfrac{1}{12}c_1 + o(1))y^3/\log y\right) \qquad (y \to \infty). \tag{6}$$

Write $p_0 = 1 + ukL$, so that

$$u \leqslant \exp\left(\tfrac{1}{11}c_1 y^3/\log y\right) \tag{7}$$

for large y.

We now remove from $\mathcal{P}$ any prime which happens to divide uLp_0, denoting the remaining set by $\mathcal{P}'$. It is easy to see that there are $\ll y^3/\log y$ distinct primes dividing uLp_0, hence from (5) it follows that

$$|\mathcal{P}'| \geqslant \exp\left((\tfrac{1}{5}c_1 + o(1))y^3/\log y\right) \qquad (y \to \infty). \tag{8}$$

Let $\mathcal{N}$ be the set of integers n such that $\gcd(n, uLm) = 1$ and $n \equiv 1 \bmod k$; note that $\mathcal{P}' \subset \mathcal{N}$. Let $\mathcal{G}$ be the subgroup of $(\mathbb{Z}/ukL\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ consisting of pairs (α, β) with $\alpha \equiv 1 \bmod k$, and let $\Psi : \mathcal{N} \to \mathcal{G}$ be the natural map that takes each integer $n \in \mathcal{N}$ to the pair

$$\Psi(n) = (n \bmod ukL,\, n \bmod m).$$

We claim that if $\mathcal{S}$ is any subset of $\mathcal{P}'$ with more than one element, $n_{\mathcal{S}}$ is the element of $\mathcal{N}$ given by $n_{\mathcal{S}} = \prod_{p\in\mathcal{S}} p$, and $\Psi(n_{\mathcal{S}})$ is the identity in $\mathcal{G}$, then $N_{\mathcal{S}} = n_{\mathcal{S}}p_0$ is a Carmichael number in the arithmetic progression $a \bmod m$. To show this, we shall apply

Korselt's criterion. *We have $b^n \equiv b \bmod n$ for all integers b if and only if n is squarefree and $p-1$ divides $n-1$ for every prime p dividing n.*

The proof is elementary and in fact was found by Korselt before he knew of the existence of any composite examples. Now consider $N_{\mathcal{S}} = n_{\mathcal{S}}p_0$. Since $p_0 \notin \mathcal{P}'$, $N_{\mathcal{S}}$ is squarefree. Since $\Psi(n_{\mathcal{S}})$ is the identity element in $\mathcal{G}$, we have $n_{\mathcal{S}} \equiv 1 \bmod m$, hence $N_{\mathcal{S}} \equiv p_0 \equiv a \bmod m$. Further, $p_0 - 1 = ukL \mid n_{\mathcal{S}} - 1$, and it follows that $p_0 - 1 \mid N_{\mathcal{S}} - 1$. Similarly, for each prime $p \in \mathcal{S}$, we have $p - 1 \mid kL \mid n_{\mathcal{S}} - 1$, which implies $p - 1 \mid N_{\mathcal{S}} - 1$ since $p_0 \equiv 1 \bmod kL$. Thus, $N_{\mathcal{S}}$ is a Carmichael number by Korselt's criterion, and the claim is established.

To estimate the number of Carmichael numbers produced in this manner, we first need to bound the Davenport constant for the group $\mathcal{G}$. From the definition of $\mathcal{G}$ and using [1, Equation (4.3)], we see that for large y,

$$\lambda(\mathcal{G}) \leqslant um\,\lambda(L) \leqslant um\,e^{6y}.$$

In view of (7) and the fact that m is fixed, it follows that

$$\lambda(\mathcal{G}) \leqslant \exp\left((\tfrac{1}{11}c_1 + o(1))y^3/\log y\right) \qquad (y \to \infty).$$

Further, using (4), (7), and the fact that m is fixed, we have

$$|\mathcal{G}| = \frac{\varphi(ukL)\varphi(m)}{\varphi(k)} \leqslant uLm \leqslant \exp((1 + o(1))y^3) \qquad (y \to \infty).$$

Hence, applying Lemma 2 we derive that

$$D(\mathcal{G}) \leqslant \exp\left(\left(\tfrac{1}{11}c_1 + o(1)\right)y^3/\log y\right) \qquad (y \to \infty). \tag{9}$$

Put

$$t = \exp\left(\tfrac{1}{10}c_1 y^3/\log y\right) \qquad \text{and} \qquad X = \exp(3ty^3).$$

Note that

$$\log\log\log X = (3 + o(1))\log y \qquad (y \to \infty). \tag{10}$$

If $N_{\mathcal{S}}$ is a Carmichael number of the type constructed above, and $|\mathcal{S}| \leqslant t$, then by (6) we have, as $y \to \infty$,

$$N_{\mathcal{S}} = p_0 \prod_{p \in \mathcal{S}} p \leqslant x^t \left(1 + kL \exp\left(\tfrac{1}{11}c_1 y^3/\log y\right)\right) = x^{(1+o(1))t},$$

where we have used the inequality $kL \leqslant x$ in the last step. Taking into account (4) we have $\log x = \frac{5}{2}\log L \leqslant (\frac{5}{2} + o(1))y^3$, hence

$$N_{\mathcal{S}} \leqslant \exp(3ty^3) = X$$

if y is sufficiently large.

Finally, one sees that the number T of Carmichael numbers $N_{\mathcal{S}}$ produced in this manner is equal to the number of distinct nonempty subsets $\mathcal{S} \subset \mathcal{P}'$ such that $\Psi(n_{\mathcal{S}})$ is the identity in $\mathcal{G}$, and $|\mathcal{S}| \leqslant t$. Applying Lemma 3 with $r = |\mathcal{P}'|$ and $n = D(\mathcal{G})$, we obtain the lower bound

$$T \geqslant \binom{|\mathcal{P}'|}{\lfloor t \rfloor} \Big/ \binom{|\mathcal{P}'|}{D(\mathcal{G})} \geqslant \left(\frac{|\mathcal{P}'|}{\lfloor t \rfloor}\right)^{\lfloor t \rfloor} |\mathcal{P}'|^{-D(\mathcal{G})} = |\mathcal{P}'|^{\lfloor t \rfloor - D(\mathcal{G})} \lfloor t \rfloor^{-\lfloor t \rfloor}. \tag{11}$$

By (8), (9), and our definition of t, it follows that

$$T \geqslant \exp\left(\left(\tfrac{1}{5}c_1 - \tfrac{1}{10}c_1 + o(1)\right)ty^3/\log y\right) \qquad (y \to \infty).$$

From (10) it follows that $ty^3/\log y \sim \log X/\log\log\log X$ as $y \to \infty$, so it follows that with $c = \frac{1}{11}c_1$

$$\log T \geqslant \frac{c\log X}{\log\log\log X}$$

for all sufficiently large y. Since the value of y can be uniquely determined from X, the result follows. □

Theorem 3. *Suppose that* (3) *holds with some real number* $\kappa < 1$. *Then there is a constant* $c > 0$, *depending only on* κ, *such that for any coprime integers* a *and* $m \geqslant 1$, *one has*

$$\big|\{n \leqslant X \ : \ n \text{ is Carmichael and } n \equiv a \bmod m\}\big| \geqslant X^c$$

for all sufficiently large X (*depending on the choice of* m).

Proof. Our proof follows closely that of Theorem 2, so we focus mainly on the modifications that are needed.

Let $0 < \kappa < 1$ be arbitrary and suppose that (3) holds with κ. Let $\mathcal{Q}$ and L be defined as before. Let c_2 be a fixed real number larger than $5/(2-2\kappa)$. Let y be a real parameter which is assumed large. Applying Lemma 1 with $x = \exp(c_2 y^{3\kappa})$, we see that there is an integer $k \leqslant x^{3/5}$ for which

$$|\mathcal{P}| \geqslant \frac{c_0}{\varphi(m)\log x}\big|\{d \mid L \ : \ d \leqslant x^{2/5}\}\big|,$$

where $\mathcal{P}$ is defined as before. The product of any

$$s = \left\lfloor \frac{\log(x^{2/5})}{\log(y^3)} \right\rfloor = \left\lfloor \frac{2c_2 y^{3\kappa}}{15 \log y} \right\rfloor$$

distinct primes in $\mathcal{Q}$ is a divisor d of L with $d \leqslant x^{2/5}$. Since $|\mathcal{Q}| \gg \pi(y^3)$, it follows that as $y \to \infty$,

$$\big|\{d \mid L \ : \ d \leqslant x^{2/5}\}\big| \geqslant \binom{|\mathcal{Q}|}{s} \geqslant \left(\frac{|\mathcal{Q}|}{s}\right)^s \geqslant \exp((\tfrac{2-2\kappa}{5}c_2 + o(1))y^{3\kappa}).$$

Consequently, $|\mathcal{P}| \geqslant \exp(c_3 y^{3\kappa})$ for all large y, where c_3 is any fixed number such that $1 < c_3 < \frac{2-2\kappa}{5}c_2$.

As before, we glue the progressions $1 \bmod kL$ and $a \bmod m$ to a single progression $a' \bmod \operatorname{lcm}[kL, m]$, where $\gcd(a', \operatorname{lcm}[kL, m]) = 1$. By (3) the least prime p_0 in this progression satisfies the bound

$$p_0 \ll kLm \exp((\log(kLm))^\kappa).$$

Since m is fixed and $k \leqslant x^{3/5} = L^{o(1)}$, using (4) we derive the bound

$$p_0 \leqslant kL \exp(c_4 y^{3\kappa}) \tag{12}$$

for all large y, where c_4 is any fixed number such that $1 < c_4 < c_3$. Write $p_0 = 1 + ukL$, so that $u \leqslant \exp(c_4 y^{3\kappa})$.

We now proceed as in the proof of Theorem 2 to form the sets $\mathcal{P}'$ and $\mathcal{N}$, the group $\mathcal{G}$, and the map $\Psi : \mathcal{N} \to \mathcal{G}$. Arguing as before, we derive the bounds

$$|\mathcal{P}'| \geqslant \exp((c_3 + o(1))y^{3\kappa}) \qquad (y \to \infty) \tag{13}$$

and

$$D(\mathcal{G}) \leqslant \exp((c_4 + o(1))y^{3\kappa}) \qquad (y \to \infty). \tag{14}$$

Let c_5, c_6 be fixed real numbers such that $c_4 < c_5 < c_3$ and $c_6 > c_2$, and put

$$t = \exp(c_5 y^{3\kappa}) \qquad \text{and} \qquad X = \exp(c_6 t y^{3\kappa}).$$

If $N_{\mathcal{S}} = n_{\mathcal{S}} p_0$ is a Carmichael number of the type constructed in Theorem 2, with $|\mathcal{S}| \leqslant t$, then by (12) and the fact that $\log x = c_2 y^{3\kappa}$, we have

$$N_{\mathcal{S}} = p_0 \prod_{p \in \mathcal{S}} p \leqslant x^t \left(1 + kL \exp(c_4 y^{3\kappa})\right) = x^{(1+o(1))t} = \exp((c_2 + o(1))t y^{3\kappa})$$

as $y \to \infty$. Hence, $N_{\mathcal{S}} \leqslant X$ for large y. Using the lower bound (11) together with (13), (14), and our definition of t, we see the number T of Carmichael numbers $N_{\mathcal{S}}$ produced in this manner satisfies

$$T \geqslant \exp((c_3 - c_5 + o(1))t y^{3\kappa}) = X^{(c_3 - c_5)/c_6 + o(1)} \qquad (y \to \infty).$$

Thus, if $0 < c < (c_3 - c_5)/c_6$ is fixed, then $T \geqslant X^c$ for all sufficiently large y. Since the value of y can be uniquely determined from X, the result follows. □

4 Remarks

We first remark that for the residue class 1 mod m we do not need the prime p_0 as in the previous section, and without a need for bounding p_0, the rest of the proof is completely rigorous. In fact, one can easily amend the existing proofs of the infinitude of Carmichael numbers in [1] or [5] to prove the following result, where the exponent 1/3 is from [5].

Theorem 4. *Let m be an arbitrary fixed positive integer. The number of Carmichael numbers $n \leqslant X$ with $n \equiv 1 \bmod m$ exceeds $X^{1/3}$ once X is sufficiently large (depending on the choice of m).*

In this result it would be interesting to let the modulus m vary more dynamically with X; we leave this as a project for the interested reader.

Could it be that for each m, all but finitely many Carmichael numbers are congruent to 1 mod m? Certainly not if our Conjecture holds, and so certainly not if the weaker form of Heath-Brown's conjecture described above holds. Of course, there may be a cheaper way of disproving such a possibility. We have not found such a path, but we remark that it is easy to see the following: *For each number B there is some pair a, m with $a \not\equiv 1 \bmod m$ such that there are at least B Carmichael numbers $n \equiv a \bmod m$.*

Indeed, let $C(x)$ denote the number of Carmichael numbers in $[1, x]$, and let x be large. Since no positive integer $n \leqslant x$ is congruent to 1 mod m for every modulus $m \leqslant 2\log x$, there is a pair a, m with $a \not\equiv 1 \bmod m$ and $m \leqslant 2\log x$ such that at least $C(x)/(2\log^2 x)$ Carmichael numbers lie in the residue class a mod m. From [5] it follows that for all large x, $C(x)/(2\log^2 x) > x^{1/3}$, which thus proves the assertion in a stronger form.

Finally, let $C_{a,m}(x)$ denote the number of Carmichael numbers $n \leqslant x$ with $n \equiv a \bmod m$. It may be that $C_{1,m}(x) \sim C(x)$ as $x \to \infty$ for each fixed m. For example, using computations from [8] at $x = 2.5 \times 10^{10}$, we have $C_{a,3}(x)/C(x) \approx 0.0116,\ 0.9792,\ 0.0092$ for $a = 0, 1, 2$, respectively. Also, $C_{a,4}(x)/C(x) \approx 0.9783,\ 0.0217$ for $a = 1, 3$, respectively. From statistics in [7] at $x = 10^{15}$, we have $C_{a,5}(x)/C(x) \approx 0.0553,\ 0.8570,\ 0.0290,\ 0.0291,\ 0.0297$ for $a = 0, 1, 2, 3, 4$, respectively.

References

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

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

[3] S. Chowla, 'On the least prime in an arithmetical progression', *J. Indian Math. Soc. (N.S.)* **1** (1934), 1-3.

[4] J. B. Friedlander, 'Shifted primes without large prime factors', in *Number theory and applications* (ed. R. A. Mollin), (Kluwer, NATO ASI, 1989), 393–401.

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

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

[7] R. G. E. Pinch, 'The Carmichael numbers up to 10^{15}', *Math. Comp.* **61** (1993), 381–391.

[8] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., 'The pseudoprimes to 25×10^9', *Math. Comp.* **35** (1980), 1003–1026.

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

[10] A. Rotkiewicz, 'Sur les nombres pseudopremiers de la forme $ax + b$', *C. R. Acad. Sci. Paris* **257** (1963), 2601–2604.

[11] A. Rotkiewicz, 'On the pseudoprimes of the form $ax + b$', *Proc. Cambridge Philos. Soc.* **63** (1967), 389–392.