

On the difficulty of finding reliable witnesses

W. R. Alford, Andrew Granville, and Carl Pomerance

Department of Mathematics, The University of Georgia, Athens, GA 30602, USA

Abstract. For an odd composite number n , let $w(n)$ denote the least witness for n ; that is, the least positive number w for which n is not a strong pseudoprime to the base w . It is widely conjectured, but not proved, that $w(n) > 3$ for infinitely many n . We show the stronger result that $w(n) > (\log n)^{1/(3 \log \log \log n)}$ for infinitely many n . We also show that there are finite sets of odd composites which do not have a *reliable witness*, namely a common witness for all of the numbers in the set.

Introduction

Fermat's 'little' theorem asserts that

$$a^{n-1} \equiv 1 \pmod{n}, \quad (1)$$

whenever n is a prime that does not divide a . If (1) holds for a composite integer n then we call n a 'pseudoprime to base a '. If a composite number n is a pseudoprime to every base a , for which $(a, n) = 1$, then we call n a 'Carmichael number'. One can identify Carmichael numbers fairly easily by using

Korselt's criterion: A composite number n is a Carmichael number if and only if n is squarefree and $p - 1$ divides $n - 1$ for every prime p dividing n .

The smallest such number, 561 ($= 3 \times 11 \times 17$), was found by Carmichael in 1910. Recently we proved that there are infinitely many Carmichael numbers; in fact, that there are more than $x^{2/7}$ Carmichael numbers up to x , once x is sufficiently large (see [AGP]).

If n is neither prime nor a Carmichael number, then there are more than $n/2$ integers a in $[1, n - 1]$ for which the congruence (1) does not hold. Thus if we pick an integer a at random in the interval $[1, n - 1]$ then there is a better than even chance that (1) will fail and so we will have a proof that n is composite. If we repeat this 'test' say 100 times, then there is only a minuscule chance that we will fail to recognize such an integer n as composite (and, in fact, we expect to obtain such a 'witness' a in no more than two such tests). This algorithm is very efficient because one can determine powers modulo n extremely rapidly.

The only way that this test will recognize a Carmichael number n as composite is if some a is chosen in $[1, n - 1]$ with $(a, n) > 1$. In section 2 we will show that there are infinitely many Carmichael numbers with no "small" prime factors¹. So we cannot skirt this difficulty by instructing our algorithm to just

¹ specifically, we will show that for each fixed k , there are infinitely many Carmichael numbers n such that the probability that $(a, n) > 1$, for a random integer a in $[1, n - 1]$, is $< 1/\log^k n$

look out for a finite list of exceptional integers. However this difficulty can be neatly resolved by replacing the ‘Fermat test’ based on (1) by a slightly stronger test: For any given odd integer $n > 1$, let t be the largest odd factor of $n - 1$, so we can write $n - 1 = 2^u t$ for some positive integer u . If n is a prime which does not divide a , then

$$\text{Either } a^t \equiv 1 \pmod{n}, \text{ Or } a^{2^i t} \equiv -1 \pmod{n} \text{ for some } i \in \{0, 1, \dots, u - 1\}. \quad (2)$$

If this is true when n is an odd composite then we call n a ‘strong pseudoprime to base a ’. In the mid-70’s Selfridge used (2) to rapidly identify composite numbers, which works whether or not they are Carmichael numbers.

An integer a is called a ‘witness’² for n if n does not divide a and if (2) fails³. Selfridge had observed that there are always a lot of witnesses for any odd composite integer n ; more precisely, Monier [M] and Rabin [R] independently proved that at least three-quarters of the integers a in the interval $[1, n - 1]$ are witnesses for n . Imitating the procedure above, we note that now if we select an integer a at random in the interval $[1, n - 1]$ then there is a far better than even chance that it will be a witness for n ; and so we can be almost certain that we identify any composite number in just a few such tests⁴.

So maybe we can use (2) to test whether a number is prime? Indeed, Miller proved, assuming the truth of an appropriate generalization of the Riemann Hypothesis (GRH), that if n is composite then there must be some ‘small’ value of a for which (2) fails, thus giving a ‘polynomial time’ deterministic primality test. Let $w(n)$ denote the least positive witness for n . Following work of Miller, Ankeny, Weinberger, Oesterlé and Bach (see [B]), we now know that

$$\text{If the GRH is true then } w(n) < 2 \log^2 n. \quad (3)$$

We are concerned in this paper with determining how large $w(n)$ can get. It is known that 2 is a witness for most odd composite numbers (see [E] and [P]). However it is also known that there are infinitely many strong pseudoprimes base 2, so that the least witness is then at least 3. Specific examples have been found in which $w(n)$ is fairly large: For instance $w(3215031751) = 11$ ([PSW]) and $w(341550071728321) = 23$ ([J])⁵. [Ar] provides an extraordinary example of a 337-digit odd composite, whose least prime witness exceeds 200.

Prior to this paper it had not been proved that $w(n) > 3$ for infinitely many n , even though it has long been expected that $w(n)$ can get arbitrarily large. Here we prove this and more:

² to the fact that n is composite

³ that is, n is not a strong pseudoprime to base a . Perhaps bases a to which n is a strong pseudoprime should be referred to as ‘*alibis*’, though the usual terminology is ‘*liars*’.

⁴ Actually Lehmer [Leh] and Solovay and Strassen [SS] noted that one can obtain such a surefire compositeness test using a procedure intermediate in strength between (1) and (2).

⁵ These numbers are, in fact, ‘*champions*’, in that $w(n)$ is smaller for all smaller n .

Theorem 1. *There are infinitely many Carmichael numbers n with least witness larger than $(\log n)^{1/(3 \log \log \log n)}$. In fact, there are at least $x^{1/(35 \log \log \log x)}$ such n up to x , once x is sufficiently large.*

In section 3 we will argue that the maximal order of $w(n)$ is presumably $c \log n \log \log n$, for some constant $c > 0$, though there are many obstacles to turning our ‘argument’ into a proof⁶. However under the assumption of a suitable uniform version of the prime k -tuplets conjecture we are able to show that the maximal order of $w(n)$ is at least $\alpha \log n$ for some constant $\alpha > 0$. (A set of linear forms $\{a_i x + b_i, 1 \leq i \leq k\}$ is called ‘admissible’ if $1 \leq b_i < a_i$ for each i , and for every prime p , there exists an integer n_p such that p does not divide any of the $a_i n_p + b_i$. Hardy and Littlewood’s ‘prime k -tuplets conjecture’ [HL] contends that for any admissible set of linear forms, there are infinitely many integers n for which each $a_i n + b_i$ is prime.)

Uniform prime k -tuplets conjecture. *For each integer $k \geq 1$, there exist constants $A_k, \gamma_k > 0$ such that for any ‘admissible’ set of linear forms $\{a_i x + b_i, 1 \leq i \leq k\}$ there exists an integer $n \leq \gamma_k (a_1 a_2 \dots a_k)^{A_k}$ such that each $a_i n + b_i$ is prime.*

Such a result is known for $k = 1$ (Linnik’s Theorem) and even with $A_1 = 5.5$ (see [HB], and [C] for a related theorem); and it is widely believed that the above uniform version of the prime k -tuplets conjecture is true. In section 3 we prove the following result.

Theorem 2. *Suppose that the ‘Uniform prime triplets conjecture’ is true (that is for $k = 3$). There exists a constant $\alpha > 0$ such that there are infinitely many Carmichael numbers n whose least witness is larger than $\alpha \log n$. Moreover there are at least x^β such n up to x , once x is sufficiently large, for some constant $\beta > 0$.*

Lenstra [Len] asked whether, for any given finite set of odd, composite numbers, there exists an integer w , perhaps very large, which serves as a witness for every number in the set (we will call w a ‘reliable witness’). In particular, we would like to have a reliable witness for the set of odd composites up to x . Unfortunately we will prove that there cannot be a reliable witness once x is sufficiently large⁷. We shall actually prove that one needs quite a few numbers to correctly identify all of the odd, composite numbers up to x :

Theorem 3. *For all sufficiently large numbers x and for any set \mathcal{W} of at most $(\log x)^{1/(3 \log \log \log x)}$ integers, there are more than $x^{1/(35 \log \log \log x)}$ Carmichael numbers $n \leq x$ with no witness in the set \mathcal{W} .*

⁶ See also [BH].

⁷ Two interesting computational problems come to mind: to find the smallest integer x for which there is no reliable witness for all of the odd composites up to x , and to find the smallest set of odd composites without a reliable witness.

Theorem 1 is a corollary of Theorem 3. If \mathcal{W} is not so large then we can obtain larger sets of Carmichael numbers which have no witnesses in \mathcal{W} .

Theorem 4. *For any fixed δ , $0 < \delta < 1$, there exists a constant $c_\delta > 0$, such that for any set \mathcal{W} of $\leq e^{c_\delta(\log \log x)^{1-\delta}}$ integers, there are more than $x^{3\delta/25}$ Carmichael numbers $n \leq x$ with no witness in the set \mathcal{W} .*

Besides determining $w(n)$, it is also of interest to determine the size of the smallest ‘reliable set’ \mathcal{W} of witnesses; this is a set \mathcal{W} with the property that every composite integer up to x has a witness in \mathcal{W} . Theorem 3 implies that any such set contains more than $(\log x)^{1/(3 \log \log \log x)}$ numbers. We might wish to restrict the members of \mathcal{W} to themselves be $\leq x$. By (3) we know that if the GRH is true then there is such a set of size $< 2 \log^2 x$. Adleman [A] and Dixon [D; Exercise 12] have shown how to get such a set of size $O(\log x)$ unconditionally (we shall also prove this in Proposition 3.1). We will further argue, in section 3, that it seems unlikely that there is a reliable set of witnesses of size $o(\log x)$.

On the other hand we are not sure what to conjecture about the size of the smallest set of reliable witnesses for the odd composites up to x , where we make no restriction on the size of the witnesses.

Although our arguments construct Carmichael numbers as obstructions to efficient primality testing, we point out that they are well known to be very easy to factor. Indeed, if $n = 2^u t + 1$ is a Carmichael number and w is a witness for n that is coprime to n , then $w^{2^i t}$ is a non-trivial square root of 1 mod n for some i , $0 \leq i \leq u - 1$, and so $w^{2^i t} - 1$ has a non-trivial gcd with n . See [BBCGP] for more in this vein.

Style and notation: Most of the proofs given involve modifications of the proofs in [AGP]; for brevity’s sake we suppress details that remain exactly the same, referring the reader to [AGP]; though we have tried to make our explanations here as self-contained as possible. Throughout the paper there are inexplicit constants ‘ c_j ’, as well as ‘for sufficiently large’ hypotheses; these can be made explicit with considerable extra work.

1 Tools

We begin with a simple characterization of strong pseudoprimes which is stated without proof in [PSW]. For any pair of coprime integers a and n with $n > 0$, let $\ell_a(n)$ denote the order⁸ of a modulo n .

Proposition 1.1. *Let n be a positive, odd composite integer. Then n is a strong pseudoprime to base a if and only if $a^{n-1} \equiv 1 \pmod{n}$ and there exists an integer k such that, for every prime factor p of n , 2^k divides $\ell_a(p)$ but 2^{k+1} does not.*

Proof. Throughout the proof we write $n = 2^u t + 1$ where t is odd.

Suppose that n is a strong pseudoprime to base a . Either $a^t \equiv 1 \pmod{n}$, so that $a^t \equiv 1 \pmod{p}$ for each prime factor p of n , and thus each $\ell_a(p)$ is odd

⁸ that is, the order of a in the group $(\mathbb{Z}/n\mathbb{Z})^*$

(giving $k = 0$ above). Or there must exist some integer k in the range $1 \leq k \leq u$ for which $a^{2^{k-1}t} \equiv -1 \pmod n$. But then $a^{2^{k-1}t} \equiv -1 \pmod p$ for each prime p dividing n , and so 2^k is the exact power of 2 dividing each $\ell_a(p)$.

Suppose conversely that $a^{n-1} \equiv 1 \pmod n$ and that 2^k is the exact power of 2 dividing $\ell_a(p)$ for each prime factor p of n . It is well known that for any prime power p^b , the order of a modulo p^b equals some power of p times $\ell_a(p)$. Since n is odd this means that 2^k is the exact power of 2 dividing $\ell_a(p^b)$ for each prime power p^b dividing n . However, since we already know that $a^{2^{kt}} \equiv a^{n-1} \equiv 1 \pmod p^b$ we thus deduce that $a^{2^{kt}} \equiv 1 \pmod p^b$, whereas $a^{2^{k-1}t} \equiv -1 \pmod p^b$ if $k \geq 1$. By the Chinese Remainder Theorem, this implies that $a^{2^{kt}} \equiv 1 \pmod n$, whereas $a^{2^{k-1}t} \equiv -1 \pmod n$ if $k \geq 1$, and so n is a strong pseudoprime to base a .

We shall apply Proposition 1.1 to special types of Carmichael numbers in the following way.

Corollary 1.2. *Suppose that n is a Carmichael number, and that every prime factor of n is $\equiv 3 \pmod 4$. Then a is not a witness for n if and only if the quadratic residue symbol $\left(\frac{a}{p}\right)$ takes the same value for each prime divisor p of n . In particular, the least witness for n is prime.*

Proof. Note that n divides a if and only if p divides a for every prime divisor p of n (since any Carmichael number n is squarefree by Korselt's criterion); and this is true if and only if $\left(\frac{a}{p}\right) = 0$ for each prime divisor p of n .

Otherwise we may assume n does not divide a , and so a is not a witness for n if and only if n is a strong pseudoprime to base a . Let p be any prime divisor of n , which must be $\equiv 3 \pmod 4$ by hypothesis. Since $\ell_a(p)$ divides $p-1$ (which is divisible by 2 but not by 4), we see that the exact power of 2 dividing $\ell_a(p)$ can be either 2^0 or 2^1 , but no higher power. However, if 2^0 is the exact power of 2 dividing $\ell_a(p)$, then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv 1 \pmod p$ and so $\left(\frac{a}{p}\right) = 1$. Alternatively, if 2^1 is the exact power of 2 dividing $\ell_a(p)$, then $a^{(p-1)/2} \not\equiv 1 \pmod p$ and so $\left(\frac{a}{p}\right) = -1$. The result follows now directly from Proposition 1.1.

Let $\lambda(n)$ denote the largest order of any element of the group $(\mathbb{Z}/n\mathbb{Z})^*$; note that $a^{\lambda(n)} \equiv 1 \pmod n$ for any integer a which is coprime to n , and that $\lambda(n)$ is the least such integer. Thus, $\lambda(n)$ is the lcm of the numbers $\lambda(p^a)$, where p^a runs over the prime power divisors of n , and $\lambda(p^a) = p^{a-1}(p-1)$ if $p > 2$ or $p^a = 2$ or 4 , and $\lambda(2^a) = 2^{a-2}$ if $a \geq 3$. Known as Carmichael's function⁹, $\lambda(n)$ is intimately connected with Carmichael numbers: a composite number n is Carmichael if and only if $\lambda(n)$ divides $n-1$.

Proposition 1.3. *Suppose n and k are coprime integers with $n > 2$ and S is a set of primes not dividing n which are all of the form $dk+1$, where d is a divisor*

⁹ Gauss discovered Carmichael's function over a hundred years before Carmichael: see article 92 of 'Disquisitiones Arithmeticae' where Gauss discussed the function whilst classifying those moduli for which there is a primitive root.

of n . If $\#\mathcal{S} > \lambda(n) \log n$ then there is a nonempty subset of \mathcal{S} whose product is a Carmichael number.

Proof. Since n and k are coprime, $(\mathbb{Z}/n\mathbb{Z})^*$ is isomorphic to the subgroup of $(\mathbb{Z}/nk\mathbb{Z})^*$ of residues that are 1 mod k . Note that \mathcal{S} is naturally embedded in this subgroup. Since $n > 2$, we have $\lceil \lambda(n) \log n \rceil > \lceil \lambda(n)(1 + \log(\varphi(n)/\lambda(n))) \rceil$, where $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$. From a result of van Emde Boas and Kruswijk (see [AGP, Theorem 1.1]), there is a subset of $\mathcal{S} \setminus \{nk+1\}$ whose product is 1 mod nk . But then this product is a Carmichael number by Korselt's criterion.

Corollary 1.4. *Suppose n and k are coprime integers with $n > 2$ and \mathcal{S} is a set of primes not dividing n which are all 3 mod 4 and all of the form $dk+1$, where d is a divisor of n . If ℓ, t and Λ are integers for which $3^{-\ell}\#\mathcal{S} > t > \Lambda > \lambda(n) \log n$, then for any set \mathcal{W} of ℓ integers, there are at least $\binom{3^{-\ell}\#\mathcal{S}}{t} / \binom{3^{-\ell}\#\mathcal{S}}{\Lambda}$ distinct subsets of \mathcal{S} , each containing $\leq t$ elements, such that the product of the elements in each such subset is a Carmichael number with no witness in \mathcal{W} .*

Proof. Suppose that $\mathcal{W} = \{w_1, \dots, w_\ell\}$, and consider the function $\chi_{\mathcal{W}} : \mathcal{S} \rightarrow \{1, 0, -1\}^\ell$, where

$$\chi_{\mathcal{W}}(p) = \left(\left(\frac{w_1}{p} \right), \left(\frac{w_2}{p} \right), \dots, \left(\frac{w_\ell}{p} \right) \right) \quad \text{for every } p \in \mathcal{S},$$

and where $\left(\frac{w}{p} \right)$ is the Legendre symbol. Since there are only 3^ℓ possible values that $\chi_{\mathcal{W}}(p)$ can take, there must be a subset \mathcal{S}_0 of \mathcal{S} , of order $\geq 3^{-\ell}\#\mathcal{S}$, on which $\chi_{\mathcal{W}}$ remains constant. But by Corollary 1.2, any Carmichael number formed from the primes in \mathcal{S}_0 has no witness in \mathcal{W} . The assertion about the number of such Carmichael numbers with $\leq t$ prime factors follows directly from Proposition 1.3 and [AGP, Proposition 1.2].

Our principal results follow from Corollary 1.4, but to make use of it, we must show how numbers n and k may be constructed satisfying the hypotheses. The next result, which is derived from [AGP, Theorem 3.1], provides a way.

Proposition 1.5. *There exists a constant $c_0 > 0$ such that for any given arithmetic progression $l \pmod m$ with $(l, m) = 1$, if x is sufficiently large (depending on the choice of m) and if n is a squarefree integer which is coprime to m , then there exists an integer $k \leq x^{3/5}$ such that*

$$\begin{aligned} \#\{p \text{ prime} : p \leq x, p = dk + 1 \text{ for some } d|n, p \equiv l \pmod m\} \\ > \frac{c_0}{\varphi(m) \log x} \#\{d|n : d \leq x^{2/5}\}. \end{aligned}$$

Further, if n has $\leq x^{1/4}$ prime factors, and the sum of the reciprocals of the primes dividing n is $\leq 1/60$, then we may take k to be coprime to n .

Proof. We shall modify the proof of Theorem 3.1 in [AGP], taking $B = 2/5$ there¹⁰ to simplify matters. Note that by definition every element of $\mathcal{D}_B(x)$ is $> \log x$, so if we take $x \geq e^m$ then no member of the set $\mathcal{D}_B(x)$ of exceptional moduli can divide m . Analogously to the proof of Theorem 3.1 in [AGP] we begin by forming a new number n' , obtained by removing from n some prime factor of (d, n) for each $d \in \mathcal{D}_B(x)$, so that no member of $\mathcal{D}_B(x)$ divides mn' (since $(m, n) = 1$ and n is squarefree). Note that there are $\leq D_B$ prime factors of n/n' .

For every integer d coprime to m , let a_d be the congruence class mod dm which is $\equiv 1 \pmod{d}$ and $\equiv l \pmod{m}$. For $d|n'$, $d \leq x^{2/5}$, we are interested in counting the number of primes $p \leq dx^{3/5}$ with $p \equiv a_d \pmod{dm}$ and $((p-1)/d, n) = 1$. We proceed as in the proof of Theorem 3.1 in [AGP], though replacing the various estimates for the number of primes $\equiv 1 \pmod{D}$ by the analogous estimates for the number of primes $\equiv a_D \pmod{Dm}$ (here $D = d$ or dq of [AGP])¹¹. One difference is that there we assumed that n had no prime factor $q > x^{3/10}$; whereas here we shall bound the 'contribution' of all of the primes $q > x^{2/7}$ dividing n by using the trivial fact that the number of primes $\leq dx^{3/5}$ which are $\equiv a_{dq} \pmod{dqm}$, is less than the number of integers in this arithmetic progression, which is $\leq 1 + x^{3/5}/qm$. However, by (the extended) hypothesis we know that there are $\leq x^{1/4}$ such primes q , so their total contribution is $\leq x^{1/4}(1 + x^{3/5}/x^{2/7}m) \leq x^{3/5}/(9m \log x)$ if x is sufficiently large. Therefore there are at least

$$\frac{x^{3/5}}{3\varphi(m) \log x} \#\{d|n' : d \leq x^{2/5}\}$$

pairs (p, d) , where d divides n' and $d \leq x^{2/5}$, and p is a prime $\equiv a_d \pmod{dm}$ with $p \leq dx^{3/5}$ and $((p-1)/d, n) = 1$. Each such pair corresponds to an integer $k = (p-1)/d$ which is coprime to n and $\leq x^{3/5}$. Thus there is some such k which corresponds to at least $\#\{d|n' : d \leq x^{2/5}\}/(3\varphi(m) \log x)$ such pairs (p, d) . The result with k coprime to n now follows from (3.1) of [AGP], where $c_0 = 1/(3 \cdot 2^{D_B})$.

The arithmetic progressions mod dqm occurred in the proof solely to ensure that the integer k produced is coprime to n . If we remove this assertion from the theorem then it is easy to remove the restrictions placed on the number of prime factors of n , and the sum of their reciprocals, leading to our result in the case when k is not guaranteed to be coprime to n .

Let $\tau(n)$ denote the number of positive integers which divide n . Take $l = m = 1$ and $x = n^{5/2}$ in Proposition 1.5. Since $\tau(n) = \#\{d|n : d \leq n\}$ we have the following result with $c_1 = 2c_0/5$.

Corollary 1.6. *For any sufficiently large squarefree integer n , there is some positive integer $k \leq n^{3/2}$ for which*

$$\#\{d|n : p = dk + 1 \text{ is a prime}\} > \frac{c_1 \tau(n)}{\log n}.$$

¹⁰ which is in the set \mathcal{B} of [AGP] since $2/5 < 5/12$.

¹¹ and we still look at such primes $\leq dx^{3/5}$.

We make one further observation that will be implicitly used in the next section:

Lemma 1.7. *For any sufficiently large finite set of primes \mathcal{P} , if \mathcal{P}' consists of the largest $\lfloor (\#\mathcal{P})/2 \rfloor$ primes in \mathcal{P} , then the sum of the reciprocals of the primes in \mathcal{P}' is $\leq 1/60$.*

Proof. Say the least prime in \mathcal{P}' is p and say $\#\mathcal{P}' = k$. Then the sum of the reciprocals of the members of \mathcal{P}' is majorized by k/p . But there are at least k primes below p (in \mathcal{P}), so p is larger than the k -th prime. By the prime number theorem, the k -th prime is $\sim k \log k$ as $k \rightarrow \infty$, so the sum of the reciprocals of the members of \mathcal{P}' is $\leq (1 + o(1))k/k \log k = o(1)$ as $k \rightarrow \infty$, and the result follows.

2 Two constructions – three proofs

In this section we prove Theorems 1, 3 and 4. The emphasis in Theorems 1 and 3 is more on producing numbers with an extreme property and less on producing many such numbers, while the emphasis in Theorem 4 is the reverse. To accomplish these different goals we shall use two different, but related constructions.

The first construction. Let α and ε be arbitrary, but fixed numbers with $0 < 5\varepsilon < \alpha < 1$. We assume that y is sufficiently large depending on the choice of α and ε . Let N be the product of the primes up to y , and let $X = N^{5/4}$. Let $L = M = 1$, and let $K \leq X^{3/5} = N^{3/4}$ be the number produced by Proposition 1.5 (taken with capital letters N, X, L, M, K, D). We now let n be the product of the larger half of the primes of the form $DK + 1 \leq X = N^{5/4}$, for which D divides N . As usual, let $\omega(n)$ denote the number of prime factors of n , $\pi(y)$ denote the number of primes up to y and $\theta(y)$ the sum of their logarithms. We have

$$N = e^{\theta(y)}, \quad \tau(N) = 2^{\pi(y)}, \quad (1/2)\tau(N) \geq \omega(n) > (2c_0/5)2^{\pi(y)}/\theta(y),$$

$$\lambda(n) \leq KN \leq e^{(7/4)\theta(y)}, \quad \log n \leq \omega(n) \log(N^{5/4}) \leq \tau(N) \log N \leq e^{\varepsilon^2 y}.$$

Note that $\theta(y) \sim y$ as $y \rightarrow \infty$, so we may assume that $\theta(y) < 1.01y$.

Given a positive integer s , consider those divisors d of n with exactly s prime factors. The number of such divisors is $\binom{\omega(n)}{s}$, and each of these divisors is $\leq N^{(5/4)s} < e^{1.3ys}$. We shall let $s = \lceil 2^{\alpha\pi(y)} \rceil$, and we take $x = N^{(25/8)s} < e^{3.2ys}$, so that $x^{2/5}$ is larger than every divisor d of n with exactly s prime factors. By Proposition 1.5 applied to n and x there exists an integer $k \leq x^{3/5}$, coprime to n , such that the set \mathcal{S} of primes $p \leq x$ not dividing n for which $p \equiv 3 \pmod{4}$ and $p = dk + 1$ for some divisor d of n is of order

$$\begin{aligned} \#\mathcal{S} &\geq \frac{c_0}{2 \log x} \#\{d|n : d \leq x^{2/5}\} - \omega(n) \geq \frac{c_0}{2(3.2ys)} \binom{\omega(n)}{s} - \omega(n) \\ &\geq \frac{c_0}{6.4ys} \left(\frac{\omega(n)}{s} \right)^s - \omega(n) \geq 2^{(1-\alpha-\varepsilon)\pi(y)} 2^{\alpha\pi(y)}. \end{aligned}$$

We now will apply Corollary 1.4. Let $\Lambda = [e^{1.78y}]$ and $t = [e^{1.8y}]$, so that $t > \Lambda > \lambda(n) \log n$. We choose $\ell = s (= [2^{\alpha\pi(y)}])$. From the above calculation,

$$3^{-\ell} \#\mathcal{S} \geq 2^{(1-\alpha-2\varepsilon)\pi(y)} 2^{\alpha\pi(y)}.$$

Thus, from Corollary 1.4, the number of Carmichael numbers which are the product of at most t primes from \mathcal{S} and which do not have a witness in any given set \mathcal{W} of ℓ integers is at least

$$\begin{aligned} \binom{3^{-\ell} \#\mathcal{S}}{t} / \binom{3^{-\ell} \#\mathcal{S}}{\Lambda} &\geq \left(\frac{3^{-\ell} \#\mathcal{S}}{t} \right)^t (3^{-\ell} \#\mathcal{S})^{-\Lambda} = (3^{-\ell} \#\mathcal{S})^{t-\Lambda} t^{-t} \\ &> 2^{(1-\alpha-3\varepsilon)\pi(y)} 2^{\alpha\pi(y)} e^{1.8y}. \end{aligned}$$

Further, each Carmichael number produced is bounded by

$$Y := x^t < e^{3.2y\pi t} \leq e^{3.2y2^{\alpha\pi(y)} e^{1.8y}}.$$

We now rewrite ℓ and the number of Carmichael numbers produced in terms of Y . Since $\log \log \log Y \sim \log y$ as $y \rightarrow \infty$, and $\pi(y) \sim y/\log y$, the number of Carmichael numbers produced exceeds $Y^{(1-\alpha-4\varepsilon)(\log 2)/3.2 \log \log \log Y}$. And since $\log \log Y \sim 1.8y$ as $y \rightarrow \infty$, we have that $\ell > 2^{(\alpha-\varepsilon) \log \log Y / 1.8 \log \log \log Y}$. We now choose $\alpha = .866$, $\varepsilon = .0001$, so that $\ell > (\log Y)^{1/3 \log \log \log Y}$; and the number of Carmichael numbers produced below Y with no witness in any given set of ℓ integers exceeds $Y^{1/35 \log \log \log Y}$. This concludes the proofs of both Theorems 1 and 3.

Remarks. By Proposition 1.3, there is some Carmichael number ν which is the product of a subset of the t largest primes in \mathcal{S} . Then $\nu \leq Y$ and ν has no prime factor below the t -th largest member of \mathcal{S} , which is $> \#\mathcal{S}/2 > e^\varepsilon = e^\ell > \exp((\log Y)^{1/3 \log \log \log Y})$. That is, for each fixed k there are infinitely many Carmichael numbers ν with no prime factor below $\log^k \nu$. For such Carmichael numbers ν , the probability that $a^{\nu-1} \not\equiv 1 \pmod{\nu}$ for a random choice of a in $[1, \nu-1]$ is $< \log^{-k+1} \nu$. Thus, these numbers cannot be shown composite in polynomial time via the simple Fermat congruence, with either the deterministic test of choosing $a = 2, 3, \dots$, or the probabilistic test of choosing a at random. Thanks are due to Neal Koblitz for steering us to these observations.

The constant "1/3" in Theorems 1 and 3 and in the remark above is not optimal. If one is willing to replace "1/35" with a smaller positive number and one replaces "2/5" in Proposition 1.5 with a number less than and arbitrarily close to 5/12, we may improve "1/3" to any number smaller than $(10/17) \log 2 = .4077\dots > 2/5$.

The second construction is similar to the first, but with X and x chosen differently in the two applications of Proposition 1.5. We shall let $\alpha, \beta, \varepsilon$ be arbitrary, but fixed numbers with $0 < \alpha, \beta < 1$ and $0 < \varepsilon < 1/10$. We shall assume that y is sufficiently large, depending on the choice of α, β and ε . Let $u = [y^\beta / \log y]$, and, as before, let N be the product of the primes $\leq y$. The

number of divisors D of N with $\omega(D) = u$ is at least $\binom{\pi(y)}{u} \geq ye^{(1-\beta)y^\beta}$, since $\pi(y) \geq y/(\log y - 1)$. Note that each such D is $\leq y^u$. We apply Proposition 1.5 with N as above, $X = y^{(5/2)u} \leq e^{(5/2)y^\beta}$, and $L = M = 1$. Let $K \leq X^{3/5} = e^{\alpha(y)}$ be the number produced by Proposition 1.5 and let n be the product of the larger half of the primes $DK + 1 \leq e^{(5/2)y^\beta}$ for which D divides N . We have

$$\omega(n) \geq \frac{c_0}{2 \log X} \#\{D|N : \omega(D) = u\} > e^{(1-\beta)y^\beta},$$

$$\lambda(n) \leq KN \leq e^{(1+\varepsilon)y}, \quad \log n \leq \tau(N) \log(KN + 1) \leq e^\varepsilon y.$$

We now take $\ell = \lceil e^{\alpha(1-\beta)y^\beta} \rceil$ and consider divisors d of n with exactly ℓ prime factors. Each such divisor d is at most $e^{(5/2)y^\beta \ell}$. We apply Proposition 1.5 to n , with $x = e^{(25/4)y^\beta \ell}$ and $l \bmod m = 3 \bmod 4$. Let $k \leq x^{3/5}$, $(k, n) = 1$, be the number produced by Proposition 1.5 and let \mathcal{S} be the set of primes $p \leq x$ not dividing n with $p \equiv 3 \pmod{4}$ and $p = dk + 1$ for some divisor d of n . Then

$$\begin{aligned} 3^{-\ell} \#\mathcal{S} &\geq \frac{3^{-\ell} c_0}{2 \log x} \#\{d|n : d \leq x^{2/5}\} - 3^{-\ell} \omega(n) > \frac{3^{-\ell} c_0}{13 y^\beta \ell} \binom{\omega(n)}{\ell} - \omega(n) \\ &\geq \frac{c_0}{13 y^\beta \ell} \left(\frac{\omega(n)}{3\ell} \right)^\ell - \omega(n) \geq \exp \left((1-\varepsilon)(1-\alpha)(1-\beta)y^\beta e^{\alpha(1-\beta)y^\beta} \right). \end{aligned}$$

We choose $A = \lceil e^{(1+3\varepsilon)y} \rceil$ and $t = \lceil e^{(1+4\varepsilon)y} \rceil$. From Corollary 1.4, the number of Carmichael numbers which are a product of at most t primes from \mathcal{S} and which do not have a witness in any given set \mathcal{W} of ℓ integers is at least

$$(3^{-\ell} \#\mathcal{S})^{t-A} t^{-t} > \exp \left((1-2\varepsilon)(1-\alpha)(1-\beta)y^\beta e^{\alpha(1-\beta)y^\beta} e^{(1+4\varepsilon)y} \right).$$

Since each prime in \mathcal{S} is $\leq x$, these Carmichael numbers are all $\leq x^t \leq Y := \exp \left((25/4)y^\beta e^{\alpha(1-\beta)y^\beta} e^{(1+4\varepsilon)y} \right)$. In terms of the new variable Y we have $\ell > \exp \left((1-4\varepsilon)\alpha(1-\beta)(\log \log Y)^\beta \right)$; and the number of Carmichael numbers produced below Y , with no witness in any given set of ℓ integers, is at least Y^c , where $c = (4/25)(1-2\varepsilon)(1-\alpha)(1-\beta)$. Taking ε and α so that $(1-2\varepsilon)(1-\alpha) = 3/4$ and letting $\beta = 1 - \delta$ completes the proof of Theorem 4 (with $c_\delta \gg \delta$).

Remarks. By taking ε , α and β small, the above argument implies that up to Y there are at least Y^c Carmichael numbers, for any $c < 4/25$, for Y exceeding some number $Y_0(c)$. Since the number "2/5" in Proposition 1.5 may be replaced by any number smaller than 5/12, we have the above for any $c < 25/144$, which is Theorem 5 in [AGP], though with a somewhat different proof. This result is effective, in that a value for $Y_0(c)$ may be computed in principle. Using the main theorem from [F], we were able to prove in [AGP] the non-effective result that there are more than $Y^{2/7}$ Carmichael numbers up to Y , for Y sufficiently large. That construction is not particularly amenable to producing composite numbers with no witness in a large predetermined set, but does at least give that for any number ρ with $0 < \rho < 2$ and for any predetermined set of size $(\log \log Y)^{2+\rho}$, there are more than $Y^{(2-\rho)/7}$ Carmichael numbers up to Y with no witness in the set, provided Y is sufficiently large, depending on the choice of ρ .

3 Upper bounds and heuristics

Proposition 3.1. *For any integer $x \geq 1$ there is a set \mathcal{W} of at most $(6/5)\log x$ integers $\leq x$ such that every odd, composite integer $\leq x$ has a witness in \mathcal{W} .*

Proof. A slightly stronger version of the result of Monier [M] and Rabin [R] mentioned in the introduction is that if $n > 9$ is an odd composite, then at least $3/4$ of the integers in $[1, n]$ are witnesses for n . Since $a + kn$ is a witness for n whenever a is, we see that the number of witnesses up to x for any odd composite n with $9 < n \leq x$ is at least the maximum of $(3/4)n \lfloor x/n \rfloor$ and $x - (1/4)n \lfloor x/n \rfloor$. A simple calculation shows that this is at least $(3/5)x$; and that for $n = 9$ as well, there are at least $(3/5)x$ witnesses up to x .

Suppose \mathcal{S} is a set of odd composites in $[1, x]$. There are two ways to count the number of pairs w, s , where $w \leq x$, $s \in \mathcal{S}$ and w is a witness for s . The first way is to count the number of w 's for each $s \in \mathcal{S}$ and the second way is to count the number of s 's for each $w \leq x$. From the first way we learn that there are at least $(3/5)x \cdot \#\mathcal{S}$ pairs w, s . Thus from the second way of counting we learn that there is some $w \leq x$ which is a witness for at least $3/5$ of the members of \mathcal{S} .

We apply this principle iteratively starting with \mathcal{S} the set of all odd composites in $[1, x]$, to find some $w_1 \leq x$ which is a witness for at least $3/5$ of the members of \mathcal{S} , then to find some $w_2 \leq x$ which is a witness for at least $3/5$ of the remaining members of \mathcal{S} for which w_1 is not a witness, and so on. Thus if $(2/5)^k x/2 \leq 1$, there is some choice of $w_1, \dots, w_k \leq x$ such that every odd composite has a witness in $\{w_1, \dots, w_k\}$, and the Proposition follows from a simple calculation.

Remarks: The proof shows that we may replace the number $6/5$ in the Proposition with any constant c larger than $1/\log(5/2) = 1.09135\dots$, provided x is sufficiently large depending on the choice of c . An argument based on showing that the witnesses for an odd composite are roughly uniformly distributed allows one to do this for any $c > 1/\log 4 = .72134\dots$. It is likely that one could do a little better using Theorem 4 in [DLP]. We suggest below that there is a limit to these improvements and that $o(\log x)$ is not attainable in the Proposition.

Lemma 3.2. *Suppose $m \equiv 150 \pmod{180}$ and $m+1, 5m+1, 9m+1$ are all prime. Then the Carmichael number $n = (m+1)(5m+1)(9m+1)$ has no witness $\leq Q$ if and only if $\left(\frac{m+1}{q}\right) = \left(\frac{5m+1}{q}\right) = \left(\frac{9m+1}{q}\right)$ for each prime q with $7 \leq q \leq Q$.*

Proof. From the hypothesis it is easy to see that n is a Carmichael number, each of its prime factors is $3 \pmod{4}$ and its prime factors are congruent $\pmod{8}$. Thus $\left(\frac{2}{m+1}\right) = \left(\frac{2}{5m+1}\right) = \left(\frac{2}{9m+1}\right)$, so Corollary 1.2 implies 2 is not a witness for n . Suppose q is an odd prime. Since $m+1, 5m+1, 9m+1$ are all $3 \pmod{4}$, the law of quadratic reciprocity and Corollary 1.2 imply that q is not a witness for n if and only if $\left(\frac{m+1}{q}\right) = \left(\frac{5m+1}{q}\right) = \left(\frac{9m+1}{q}\right)$. It remains to note that $m+1, 5m+1, 9m+1$ are each quadratic residues \pmod{q} for $q = 3$ and 5 , since 15 divides m .

The proof of Theorem 2: We shall consider numbers $n = (m+1)(5m+1)(9m+1)$ as described in Lemma 3.2. For every prime $q \leq Q$ we will only allow $m \equiv 0 \pmod q$, so that $\left(\frac{m+1}{q}\right) = \left(\frac{5m+1}{q}\right) = \left(\frac{9m+1}{q}\right) = 1$. Therefore the least witness for n is $> Q$ by Lemma 3.2. The above congruence conditions, when combined, fix m in a congruence class mod $N = 6 \prod_{q \leq Q} q$. We thus apply the ‘Uniform prime triplets conjecture’ with $a_1 = N, a_2 = 5N, a_3 = 9N$, and deduce that there is such a prime triplet with $m \leq \gamma_3 N (45N^3)^{A_3}$. The resulting Carmichael number n is $\leq c_2 N^{9A_3+3}$, and this is $\leq x$ for $Q = \log x / (9A_3 + 4)$ by the prime number theorem.

In the above argument we could actually have chosen any $m \pmod q$, for which $\left(\frac{m+1}{q}\right) = \left(\frac{5m+1}{q}\right) = \left(\frac{9m+1}{q}\right)$, for each prime $7 \leq q \leq Q$. One can use Weil’s theorem¹² to show that this holds for $q/4 + O(\sqrt{q})$ of the congruence classes $m \pmod q$. We thus can construct $N/4^{(1+o(1))\pi(Q)}$ such prime triplets, and apply the ‘Uniform prime triplets conjecture’ to each such triplet. This gives the second part of the theorem.

One could state a plausible variant of the prime triplets conjecture with the criterion $\left(\frac{m+1}{q}\right) = \left(\frac{5m+1}{q}\right) = \left(\frac{9m+1}{q}\right)$ for each prime $7 \leq q \leq Q$, in the hypothesis. Instead we wish to be a little more general¹³: Consider all triplets of the form $m+1, 5m+1, 9m+1$ where $m \equiv 150 \pmod{180}$. As above, for each integer $w \leq x$ we have $\left(\frac{w}{m+1}\right) = \left(\frac{w}{5m+1}\right) = \left(\frac{w}{9m+1}\right)$ for roughly a quarter or more of the congruence classes mod w . Thus, for any given set \mathcal{W} of ℓ integers $\leq x$, we expect that $\left(\frac{w}{m+1}\right) = \left(\frac{w}{5m+1}\right) = \left(\frac{w}{9m+1}\right)$ for all $w \in \mathcal{W}$, for at least $c_3 x^{1/3}/4^\ell$ values of $m \leq x^{1/3}/3$. Now, the usual heuristic is that a proportion $\gg 1/(\log x)^3$ of these triples will be simultaneously prime. We thus expect that *There are at least $x^{1/5}$ Carmichael numbers up to x without a witness from any given set of $\ell = \lfloor \frac{1}{11} \log x \rfloor$ integers $\leq x$.*

Combining this with Proposition 3.1 it seems likely that

The smallest set of reliable witnesses in $[1, x]$ for the odd composites up to x has size $\sim c \log x$ for some positive constant c .

If we take our set \mathcal{W} to be the set of primes q up to $Q = \frac{1}{12} \log x \log \log x$ then, by Lemma 3.2 and arguing as above we expect that

There are at least $x^{1/5}$ Carmichael numbers $n \leq x$, each of whose least witness is $\geq \frac{1}{12} \log n \log \log n$.

On the other hand (cf. [BH]), we conjecture that

Every odd composite number n has a witness $\leq (1/\log 4 + o(1)) \log n \log \log n$.

Since the non-zero residue classes mod n which are not witnesses for n lie in a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ of index at least 4, the ‘probability’ that each of the first k primes lies in this subgroup is 4^{-k} ; so that if $k \geq (1/\log 4 + \epsilon) \log n$, then

¹² That is, the ‘Riemann Hypothesis for curves’

¹³ and hopefully still plausible

we expect there are at most finitely many such n . This heuristic implies the conjecture, though we suspect that the constant "1/log 4" is not best possible.

Carmichael numbers which are the product of three primes $\equiv 3 \pmod{4}$ are among the integers which have the fewest witnesses; which is why we used them to (heuristically) argue that there are some integers with an extraordinarily large least witness. However, in some cases it is possible to find a small witness for such numbers: for example, if the three primes are not all congruent mod 8, then 2 is a witness. Suppose now that n is a Carmichael number with exactly three prime factors. Then n is the product of a prime triplet $am + 1$, $bm + 1$, $cm + 1$, where a , b , c are pairwise coprime, and m is in that residue class mod abc such that abc divides $m(bc + ca + ab) + a + b + c$. If we also want the three primes to be $3 \pmod{4}$ and congruent mod 8, then we need to add the conditions that a , b , c are congruent mod 4 and that $m \equiv 2 \pmod{4}$. For fixed a , b , c , the prime triplets conjecture implies that there are infinitely many m in the prescribed residue class mod $4abc$ with $am + 1$, $bm + 1$, $cm + 1$ all prime. We now investigate whether some fixed number w can be a witness for every number n in this family.

Proposition 3.3. *Assume the prime triplets conjecture. Suppose that a , b and c are pairwise coprime integers which are all congruent mod 4. There is no reliable witness for all the Carmichael numbers given as the product of 3 primes $(am + 1)(bm + 1)(cm + 1)$ with $m \equiv 2 \pmod{4}$ if and only if (*) $\left(\frac{-bc}{p}\right) = 1$ for each prime p dividing a , $\left(\frac{-ca}{q}\right) = 1$ for each prime q dividing b , and $\left(\frac{-ab}{r}\right) = 1$ for each prime r dividing c .*

Proof. Suppose $\left(\frac{-bc}{p}\right) = -1$ for some prime divisor p of a . Then $\left(\frac{am+1}{p}\right) = 1$. But since $bm+1 \equiv -b/c \pmod{p}$, $\left(\frac{bm+1}{p}\right) = -1$, so by Corollary 1.2 and quadratic reciprocity, p is a witness for all such Carmichael numbers. A similar argument works for prime divisors of b and c with appropriate Legendre symbol $= -1$.

On the other hand suppose w is a reliable witness for the family, yet (*) holds. Let w_0 be the largest odd divisor of w . Thus, $\left(\frac{w}{um+1}\right) / \left(\frac{w_0}{um+1}\right)$ has the same value for $u = a, b, c$. By quadratic reciprocity, $\left(\frac{w_0}{um+1}\right) / \left(\frac{um+1}{w_0}\right)$ has the same value for $u = a, b, c$. Let w_1 be the largest divisor of w_0 coprime to abc . Then $\left(\frac{um+1}{w_0/w_1}\right) = 1$ for $u = a, b, c$, by (*). Consider those Carmichael numbers with $m \equiv 0 \pmod{w_1}$ (of which there are infinitely many by the prime triplets conjecture). We have $\left(\frac{um+1}{w_1}\right) = 1$ for $u = a, b, c$. Thus, by Corollary 1.2, w is a witness for none of these Carmichael numbers, so (*) must fail.

Remark: These criteria appear in a seemingly unrelated theorem of Legendre: Suppose that a, b and c are given pairwise coprime integers, not all having the same sign. Then there exist non-zero integer solutions x, y, z to the equation $ax^2 + by^2 + cz^2 = 0$ if and only if there is a solution to $ax^2 + by^2 + cz^2 \equiv 0 \pmod{8}$ and (*) holds for the odd prime factors of abc . Surely this is a coincidence?

4 Further remarks

Theorem 4.1. *For any fixed non-zero integer a , there exist infinitely many squarefree, composite integers n for which $p - a$ divides $n - 1$ for every prime p dividing n .*

In [AGP] we claimed we could prove this result. We provide a short argument below. Note how the condition in the theorem generalizes Korselt's criterion in a natural way. The case $a = -1$ is of particular interest in the Lucas probable prime test, and related tests.

We will need the following Lemma which is proved exactly as Theorem 3.1 in [AGP]¹⁴.

Lemma 4.2. *If x is sufficiently large and if m is any squarefree integer, coprime to a , which is not divisible by any prime bigger than $x^{3/10}$, such that the sum of the reciprocals of the primes dividing m is $\leq 1/60$, then there exists a positive integer $k \leq x^{3/5}$, coprime to m , such that*

$$\#\{d|m : dk + a \text{ is a prime} \leq x\} \geq \frac{c_0}{\log x} \#\{d|m : 1 \leq d \leq x^{2/5}\}.$$

Proof of Theorem 4.1. We again modify the proof in [AGP]. By the main theorem of [F], there are $\gg y^3/\log y$ primes q which do not divide a , in the range $y^{5/2} \leq q \leq y^3$, for which the largest prime factor of $q - 1$ is $\leq y$. Let m be the product of $[y^2/\log y]$ of these primes, so that $m < e^{3y^2}$, and $\lambda(m) \leq e^{(3+o(1))y}$.

We apply Lemma 4.2 with $x = m^{5/2}$. There exists an integer $k \leq m^{3/2}$, coprime to m , such that the number of primes of the form $dk + a$ where $d|m$ is

$$\geq 2c_0\tau(m)/5 \log m \geq 2y^{2/2 \log y} \geq \lambda(m) \log m.$$

By Theorem 1.1 of [AGP] (modified analogously to our Proposition 1.3) there is some non-trivial subset of these primes with product $n \equiv 1 \pmod{mk}$. For each prime factor p of n , we have $p - a = dk$ for some divisor d of m , so that $p - a$ divides $n - 1$.

There are two related questions that highlight the depth of our ignorance on this topic, and provide interesting problems for further research:

1. Are there infinitely many squarefree integers n for which $p^2 - 1$ divides $n - 1$ for every prime p dividing n ?

The least such number n has the prime factorization $17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331$ and was found by Richard Pinch. For this question we have no idea how to prove the necessary analogue of Proposition 1.5 (or Theorem 3.1 in [AGP]).

2. Are there infinitely many squarefree composite integers n for which $p + 1$ divides $n + 1$ for every prime p dividing n ?

¹⁴ except that now we need to use the same bounds for $\pi(dx^{3/5}, D, a)$ (with $D = d$ or dq); and we shall again pick $B = 2/5$.

The least such number n is 399. For this question we have no idea how to prove the necessary analogue of Proposition 1.3 (or Theorem 1.1 in [AGP]).

Acknowledgements: The second and third authors wish to acknowledge support from an NSF grant. The second author is an Alfred P. Sloan Research Fellow. Thanks are due to Eric Bach, Ronnie Burthe, Paul Erdős, Neal Koblitz and Sergei Konyagin for valuable comments concerning this paper.

References

- [Ad] L. M. Adleman, *Two theorems on random polynomial time*, Proc. IEEE Symp. Found. Comp. Sci., 19 (1978), 75–83.
- [AGP] W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Annals Math., to appear.
- [Ar] F. Arnault, *Rabin-Miller primality test: composite numbers which pass it*, Math. Comp., to appear.
- [B] E. Bach, *Analytic methods in the analysis and design of number-theoretic algorithms*, MIT Press, Cambridge, Mass., 1985.
- [BH] E. Bach and L. Huelsbergen, *Statistical evidence for small generating sets*, Math. Comp. 61 (1993), 69–82.
- [BBCGP] P. Beauchemin, G. Brassard, C. Crépeau, C. Goutier and C. Pomerance, *The generation of random integers that are probably prime*, J. Cryptology 1 (1988), 53–64.
- [C] M. D. Coleman, *On the equation $b_1 p - b_2 P_2 = b_3$* , J. reine angew. Math. 403 (1990), 1–66.
- [DLP] I. Dămgard, P. Landrock and C. Pomerance, *Average case error estimates for the strong probable prime test*, Math. Comp. 61 (1993), 177–194.
- [D] J. D. Dixon, *Factorization and primality tests*, Amer. Math. Monthly 91 (1984), 333–352.
- [E] P. Erdős, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen 4 (1956), 201–206.
- [F] J. B. Friedlander, *Shifted primes without large prime factors*, in *Number Theory and Applications* (ed. R. A. Mollin), (Kluwer, NATO ASI, 1989), 393–401.
- [HB] D. R. Heath-Brown, *Zero-free regions for Dirichlet L -functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) 64 (1992), 265–338.
- [HL] G. H. Hardy and J. E. Littlewood, *Some problems on partitio numerorum III. On the expression of a number as a sum of primes*, Acta Math. 44 (1923), 1–70.
- [J] G. Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp. 61 (1993), 915–926.
- [Leh] D. H. Lehmer, *Strong Carmichael numbers*, J. Austral. Math. Soc. Ser. A 21 (1976), 508–510.
- [Len] H. W. Lenstra, Jr., private communication.
- [M] L. Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoret. Comput. Sci. 12 (1980), 97–108.

- [P] C. Pomerance, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587–593.
- [PSW] C. Pomerance, J. L. Selfridge and S. S. Wagstaff, Jr., *The pseudoprimes to $25 \cdot 10^9$* , Math. Comp. **35** (1980), 1003–1026.
- [R] M. O. Rabin, *Probabilistic algorithm for primality testing*, J. Number Theory **12** (1980), 128–138.
- [SS] R. Solovay and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), 84–85; *erratum*, *ibid.* **7** (1978), 118.