On the difficulty of finding reliable witnesses

by

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

Introduction

Fermat's 'little' theorem asserts that

$$a^{n-1} \equiv 1 \bmod n, \tag{1}$$

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 Carmichael 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 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.

Unfortunately the test just described rarely recognizes Carmichael numbers as being composite[1]. Since there are infinitely many Carmichael numbers, we cannot skirt this difficulty by instructing our algorithm to just 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

$$\textbf{Either } a^t \equiv 1 \bmod n, \textbf{ Or } a^{2^i t} \equiv -1 \bmod n \text{ for some } i \in \{0, 1, \ldots, u-1\}. \tag{2}$$

If this is true when n is a composite number then we call n a '*strong pseudoprime to base a*'. In the mid-70's Selfridge used a test based on (2) to rapidly identify composite numbers, which works whether or not they are Carmichael numbers.

*supported in part by an NSF grant.

†An Alfred P. Sloan Research Fellow.

[1]As (1) will fail only for those $a \in [1, n-1]$ which have a common factor with n.

An integer a is called a '*witness*'[2] for n if n does not divide a and if (2) fails[3]. Selfridge had observed that there are always a lot of witnesses for *any* 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 tests[4].

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, Oesterlé and Bach (see [B]), we now know that

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

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:

Theorem 1. *There are infinitely many Carmichael numbers n whose least witness is larger than $(\log n)^{1/(4\log\log\log n)}$. In fact, there are $\geq X^{1/(1000\log\log\log X)}$ such $n \leq X$, for sufficiently large X.*

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 proof[6]. 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 $c\log n$ for some constant $c > 0$. (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.)

[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*'.

[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.

[6] See also [BH].

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 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 every odd composite number up to x. Unfortunately we will prove that there cannot be a reliable witness once x is sufficiently large[7]. We shall actually prove that one needs quite a few witnesses to correctly identify all of the odd, composite numbers up to x:

Theorem 3. *If X is sufficiently large then for any set $\mathcal{W}$ of $\leq (\log X)^{1/(4 \log\log\log X)}$ integers, there are more than $X^{1/(1000 \log\log\log X)}$ Carmichael numbers $n \leq X$ which have no witnesses in the set $\mathcal{W}$.*

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 $n \leq X$ which have no witnesses 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 $(\log X)^{1/(4 \log\log\log X)}$ witnesses. 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 give their argument in Proposition 3.1). We will also argue in section 3 that it seems unlikely that there is a reliable set of witnesses of size $o(\log x)$.

Style and notation: The precise constants in our theorems are open to a little improvement: we have chosen to use 'clean' constants. 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.

[7] It is an interesting open computational problem to find the smallest integer x for which there is no reliable witness for all of the odd, composite numbers up to x.

Acknowledgements: Thanks are due to Eric Bach, Paul Erdős and Sergei Konyagin for valuable comments concerning the contents of this paper.

§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 order[8] 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 $a^{n-1} \equiv 1 \bmod n$ 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 $a^t \equiv 1 \bmod n$, so that $a^t \equiv 1 \bmod p$ for each prime factor p of n, and thus each $\ell_a(p)$ is odd (giving $k = 0$ above). Or there must exist some integer k in the range $1 \le k \le u$ for which $a^{2^{k-1}t} \equiv -1 \bmod n$. But then $a^{2^{k-1}t} \equiv -1 \bmod p$ for each prime p dividing n, and so 2^k is the exact power of 2 dividing each $\ell_a(p)$.

Suppose conversely that $a^{n-1} \equiv 1 \bmod n$ 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 $a^{2^u t} \equiv a^{n-1} \equiv 1 \bmod p^b$ we thus deduce that $a^{2^k t} \equiv 1 \bmod p^b$, whereas $a^{2^{k-1}t} \equiv -1 \bmod p^b$ if $k \ge 1$. By the Chinese Remainder Theorem, this implies that $a^{2^k t} \equiv 1 \bmod n$, whereas $a^{2^{k-1}t} \equiv -1 \bmod n$ if $k \ge 1$, 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 $\equiv 3 \bmod 4$. 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.*

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 $\equiv 3 \bmod 4$ 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 $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv 1 \bmod p$ and so $\left(\frac{a}{p}\right) = 1$. Alternatively, if 2^1 is the exact power of 2 dividing $\ell_a(p)$, then $a^{(p-1)/2} \not\equiv 1 \bmod p$ and so $\left(\frac{a}{p}\right) = -1$. The result follows now directly from Proposition 1.1.

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

Let $\lambda(n)$ denote the largest order of any element of the group $(\mathbb{Z}/n\mathbb{Z})^*$; note that $a^{\lambda(n)} \equiv 1 \bmod n$ for any integer a which is coprime to n, and that $\lambda(n)$ is the least such integer. As noted by Gauss[9], $\lambda(n)$ is the least common multiple 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 $a \geq 3$. Also called Carmichael's function, $\lambda(n)$ 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 $\mathcal{S}$ is a set of primes which are all of the form $dk+1$, where d is a divisor 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 $1 \bmod k$. 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 Kruyswijk (see [AGP, Theorem 1.1]), there is a subset of $\mathcal{S}\backslash\{nk+1\}$ whose product is $1 \bmod nk$. But then this product is a Carmichael number by Korselt's criterion.

To find *many* such Carmichael numbers we can use [AGP, Proposition 1.2], which is an elementary combinatorial result. Combining it with Proposition 1.3 above immediately gives

Corollary 1.4. *Suppose n and k are coprime integers with $n > 2$ and $\mathcal{S}$ is a set of primes which are all of the form $dk+1$, where d is a divisor of n. If t and Λ are integers for which $\#\mathcal{S} > t > \Lambda \geq [\lambda(n)\log n]$, then there are at least $\binom{\#\mathcal{S}}{t}/\binom{\#\mathcal{S}}{\Lambda}$ 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.*

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

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

If we further assume that n has $\leq x^{1/4}$ prime factors, and that 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 $B = 2/5$ there[10] to simplify matters. Note that by definition every element of $\mathcal{D}_B(x)$ is $> \log x$, so if we take $x \geq \mathrm{e}^m$ 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

[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.

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

$d \in \mathcal{D}_B(x)$, so that no member of $\mathcal{D}_B(x)$ divides mn'. Note that there are $\le D_B$ prime factors of n/n'.

For every integer d coprime to m with $d \le x^{2/5}$, let a_d be the congruence class moddm which is $\equiv 1 \bmod d$ and $\equiv \ell \bmod m$. We proceed as in the proof of Theorem 3.1 in [AGP], though replacing the various estimates for the number of primes $\equiv 1 \bmod D$ by the analogous estimates for the number of primes $\equiv a_D \bmod Dm$ (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 $\le dx^{3/5}$ which are $\equiv a_{dq} \bmod dqm$, is less than the number of integers in this arithmetic progression, which is $\le 1 + x^{3/5}/qm$. However, by (the extended) hypothesis we know that there are $\le x^{1/4}$ such primes q, so their total contribution is $\le x^{1/4}(1 + x^{3/5}/x^{2/7}m) \le x^{3/5}/9m \log x$ if x is sufficiently large. Therefore there are at least

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

pairs (p, d), where d divides n' and $d \le x^{2/5}$, and p is a prime $\equiv a_d \bmod dm$ with $p \le dx^{3/5}$ and $((p-1)/d, n) = 1$. Each such pair corresponds to an integer $k = (p-1)/d$ which is coprime to n and $\le x^{3/5}$. Thus there is some such k which corresponds to at least $\#\{d|n' : \ d \le x^{2/5}\}/(3\varphi(m)\log x)$ 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 some of the restrictions placed on the prime factors of n, leading to our result above when k is not guaranteed to be coprime to n.

Let $\tau(n)$ denote the number of positive integers which divide n. Take $\ell = m = 1$ and $x = n^{5/2}$ in Proposition 1.5. Since $\tau(n) = \#\{d|n : \ d \le n\}$ 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 $k \le n^{3/2}$ for which*

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

A *y-smooth integer* is one whose prime factors are all $\le y$. We define $\psi(x, y)$ to be the number of y-smooth integers up to x; and $\psi_2(x, y)$ to be the number of those that are squarefree. By taking $\ell = m = 1$ and n to be the product of all primes $\le y$, we deduce the following result from Proposition 1.5.

Corollary 1.7. *If $x \ge y$ are sufficiently large then there exists some positive integer $k \le x^{3/5}$ for which*

$$\#\{d| \prod_{p \le y} p : \ q = dk + 1 \text{ is a prime } \le x\} > \frac{c_0}{\log x}\psi_2(x^{2/5}, y).$$

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

We note that for any integers a, b, c, for which $0 \le c < b \le a/2$, we have

$$(4) \quad \binom{a}{b} \Big/ \binom{a}{c} = \frac{(a-c)(a-c-1)\dots(a-b-1)}{b(b-1)\dots(c+1)} \ge \left(\frac{a-c}{b}\right)^{b-c} \ge \left(\frac{a}{2b}\right)^{b-c},$$

since $(a-c-i)/(b-i) \ge (a-c)/b$ whenever $0 \le i < b$.

Estimates for $\psi_2(x,y)$ have been carefully studied in many places (see for instance [IT]). However we shall only need the lower bounds given by considering all possible products of u of the $\pi(y)$ distinct primes $\le y$. For $x \ge \mathrm{e}^{(1/2+\varepsilon)y} \ge y^{\pi(y)/2}$ we can take any $u \le \pi(y)/2$ giving at least half of all the possible products[12], and so $\psi_2(x,y) \ge 2^{\pi(y)-1}$. If $x < \mathrm{e}^{(1/2+\varepsilon)y}$ then choose $u = [\log x/\log y]$ so that, using (4) with $c = 0$,

$$(5) \qquad \psi_2(x,y) \ge \binom{\pi(y)}{u} \ge \left(\frac{\pi(y)}{u}\right)^u \ge \left(\frac{y}{\log x}\right)^u \ge \frac{x}{y(\log x)^u}.$$

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

Lemma 1.8. *For any sufficiently large finite set of primes $\mathcal{P}$, if $\mathcal{P}'$ is the larger half of the primes in $\mathcal{P}$ then the sum of the reciprocals of the primes in $\mathcal{P}'$ is $\le 1/60$.*

Proof. Suppose that $\mathcal{P} = \{p_1 < p_2 < \dots < p_n\}$, and $\mathcal{P}' = \{p_{k+1} < p_{k+2} < \dots < p_n\}$. Choose y and z so that $\pi(y) = k$ and $\pi(z) = n$; since $n \le 2k$ we see that $z \le 3y$. Evidently p_{k+j} must be at least as large as the jth prime larger than y, and so the sum of the reciprocals of the primes in $\mathcal{P}'$ is at most

$$\sum_{y<p\le z} \frac{1}{p} \le \frac{1}{y}\frac{2z}{\log z} \le \frac{6}{\log z} \le \frac{1}{60},$$

if z, and thus n, is sufficiently large.

§2. **Proofs**

We shall start by proving a rather general result which will lead to the proofs of all of our main results. To do so we will choose the parameters so that the various hypotheses are satisfied.

Proposition 2.1. *Let x be some positive integer, and for a given positive integer N, let L be a product of primes q for which $q-1$ divides N. Let K be a positive integer coprime to L, and let $\mathcal{P}$ be a set of primes $p \equiv 3 \bmod 4$, each $p \le x$, for which K divides $p-1$, and $p-1$ divides KL. Let ℓ be a positive integer $< \log(\#\mathcal{P})/\log 3$, and suppose that t is an integer for which $N \log L < t < \#\mathcal{P}/(2\cdot 3^\ell)$. Then, for any set $\mathcal{W}$ of ℓ integers, there exist at least $(\#\mathcal{P}/(2t\cdot 3^\ell))^{(t-N\log L)}$ Carmichael numbers $\le x^t$, which have no witness in the set $\mathcal{W}$.*

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

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

[12] Since the prime number theorem gives $1 < \pi(y)/(y/\log y) < 1+\varepsilon$ once y is sufficiently large

and where $\left(\frac{w}{p}\right)$ is the Legendre sybmbol. Since there are only 3^ℓ possible values that $\chi_{\mathcal{W}}(p)$ can take, there must be a subset $\mathcal{P}_0$ of $\mathcal{P}$, of order $\geq 3^{-\ell}\#\mathcal{P}$, on which $\chi_{\mathcal{W}}$ remains constant.

Since $\lambda(L)$ divides N (by definition), $\lambda(L)\log L \leq N\log L < t < \#\mathcal{P}_0/2$ by hypothesis. Thus, by Corollary 1.4 and (4), there are $\geq \binom{\#\mathcal{P}_0}{t}/\binom{\#\mathcal{P}_0}{[N\log L]} \geq (\#\mathcal{P}/(2t\cdot 3^\ell))^{(t-N\log L)}$ distinct nonempty subsets of $\mathcal{P}_0$, each containing $\leq t$ elements, whose product is a Carmichael number. Moreover, each such product is evidently $\leq x^t$ and, by Corollary 1.2, has no witness in the set $\mathcal{W}$.

Corollary 2.2. *Let x be a sufficiently large positive integer, and for given positive integer N, let L be a product of primes q for which $q-1$ divides N, such that L has $\leq x^{1/4}$ prime factors, and such that the sum of the reciprocals of the primes dividing L is $\leq 1/60$. Let $R = (c_0/2)\#\{d|L:\ d\leq x^{2/5}\}/\log x$, let ℓ be any positive integer $< \log R/\log 3$, and suppose that t is an integer for which $N\log L < t < R/(2\cdot 3^\ell)$. Then, for any set $\mathcal{W}$ of ℓ integers, there exist at least $(R/(2t\cdot 3^\ell))^{(t-N\log L)}$ Carmichael numbers $\leq x^t$, which have no witness in the set $\mathcal{W}$.*

Proof. We construct the set of primes $\mathcal{P}$ in Proposition 2.1 by using Proposition 1.5 with $\ell \bmod m = 3 \bmod 4$. Then k and n in Proposition 1.5 equal K and L in Proposition 2.1, respectively. We let R be the lower bound for $\#\mathcal{P}$ given by Proposition 1.5, where $\mathcal{P}$ is the set of primes in Proposition 2.1. The 'sufficiently large' here depends on the 'sufficiently large' in Propositions 1.5 and 2.1.

Remark: Our primary objective is to maximize ℓ as a function of $X = x^t$. However, one cannot deduce from the hypothesis of Corollary 2.2 a significantly bigger function for ℓ than is obtained in Theorem 1: As $R < \tau(L)$ and L is squarefree, and as $\tau(N) < N^{c/\log\log N}$ for some constant $c > 0$ for all integers N (see [W]), thus

$$\ell < \log R < \log\tau(L) < \omega(L) \leq \tau(N) < (\log X)^{c/\log\log\log X},$$

since $N < t < \log X$, where $\omega(L)$ denotes the number of prime factors of L.

We begin by applying Corollary 2.2 to essentially the construction of [AGP]. Thus turns out to be straightforward; however, we can get better results with a slight variant. The main difference is that in our first construction we take N to be the product of powers of the primes $\leq y$, and the primes q dividing L are no larger than a fixed power of y; whereas in our second construction we take N to be some integer k times the product of the primes $\leq y$ (as obtained by Corollary 1.7), and then the primes q dividing L get to be much larger than any fixed power of y.

Applying the construction from [AGP]: A theorem of Friedlander (see [F]) implies that there exists a constant $c_2 > 0$ such that there are at least $c_2 y^3/\log y$ primes $q \leq y^3$ for which the largest prime factor of $q-1$ is $\leq y$, once y is sufficiently large. Let L be the product of the larger half of these primes, and take $N = \prod_{p\leq y} p^{a_p}$ where p^{a_p} is the largest power of p that is $\leq y^3$. Note that $N = \mathrm{e}^{(3+o(1))y}$ by the prime number theorem, and $\log L = O(y^3)$. We let $t = \mathrm{e}^{(3+\varepsilon+o(1))y}$ in Corollary 2.2.

To satisfy the hypothesis of Corollary 2.2 we need that $x \geq R \geq N \geq \mathrm{e}^{(3+o(1))y}$. Since the largest divisor of L can be no bigger than $L = \mathrm{e}^{O(y^3)}$, we may assume x is

no bigger than this. Therefore we write $x = \mathrm{e}^{cy^{1+\rho}}$ for some $0 < \rho \le 2$. Evidently the product of any $\ell = [2cy^{1+\rho}/15\log y]$ primes dividing L is $\le x^{2/5}$, and so

$$\frac{R}{2\cdot 3^\ell} \ge \frac{c_0}{4\log x} 3^{-\ell}\binom{c_2 y^3/2\log y}{\ell} \ge \frac{c_0}{2\log x}\left(c_3 y^{2-\rho}\right)^\ell \ge \mathrm{e}^{(4-2\rho-\varepsilon)cy^{1+\rho}/15} = x^{(4-2\rho-\varepsilon)/15}.$$

Let $X = x^t$. In Corollary 2.2 we produce $\ge X^{2(2-\rho-\varepsilon)/15}$ such Carmichael numbers. Moreover, since $\log x = O(y^3)$ evidently $\log\log X \sim \log t \sim (3+\varepsilon)y$; and therefore $\ell \ge (\log\log x)^{1+\rho+o(1)}$. Selecting $\varepsilon = (2-\rho)/16$ we have now proved the following result which may be compared to Theorem 4.

Theorem 2.3. *For any fixed ρ, $0 < \rho < 2$, there exists a constant $c_\rho > 0$, such that for any set $\mathcal{W}$ of $\le (\log\log x)^{1+\rho+o(1)}$ integers, there are more than $X^{(2-\rho)/8}$ Carmichael numbers $n \le X$ which have no witnesses in the set $\mathcal{W}$.*

Remark: We can replace 3 by any $B < 2\sqrt{\mathrm{e}}$ in Friedlander's result above, and then get a corresponding improvement in Theorem 2.3.

A new construction, using Corollary 1.7 in Corollary 2.2: Let $\varepsilon > 0$ and $0 \le \eta \le 1 - 4\varepsilon$ be small, fixed constants that we will determine later. Select $Q \ge y$ sufficiently large so that we can apply Corollary 1.7 (with $x = Q$). We will insist that $Q > y^{10/\varepsilon}$, and restrict $Q \le \left(\prod_{p\le y} p\right)^{5/2} < \mathrm{e}^{3y}$ (since we will not obtain any further primes q from Corollary 1.7 for larger Q). For $\rho > 0$, let $\ell = [Q^{(1-\eta-3\varepsilon)\rho}]$ and $x = Q^{5\ell/2}$.

Let L be the product of the larger half of the primes obtained in Corollary 1.7 (taking x there to be equal to Q here). One may check that the hypotheses for L in Corollary 2.2 are satisfied (using Lemma 1.8). Let $N = k\prod_{p\le y} p$ (with k as in Corollary 1.7), and let $t = \mathrm{e}^{\varepsilon y} N\log L$.

Now, since L is the product of $\le \tau(N/k)$ primes each $\le Q$, thus $\log L \le \tau(N/k)\log Q \le 2^{\pi(y)}\log(3y) = \mathrm{e}^{o(y)}$. Moreover $1 \le k \le Q^{3/5} \le \mathrm{e}^{(3/2+o(1))y}$, by the prime number theorem. Therefore $\mathrm{e}^{(1+\varepsilon+o(1))y} \le t < Q^{3/5}\mathrm{e}^{(1+\varepsilon+o(1))y} \le \mathrm{e}^{(5/2+\varepsilon+o(1))y}$.

By Corollary 1.7 we know that L is the product of $\ge (c_0/2)\psi_2(Q^{2/5}, y)/\log Q$ primes $q \le Q$. Since $\mathrm{e}^{3y} > Q > y^{10/\varepsilon}$, we can use (5) to note that

$$\frac{c_0}{2\log Q}\psi_2(Q^{2/5}, y) \ge \frac{c_0}{6y}\psi_2(y^{4/\varepsilon}, y) \ge \frac{c_0}{6y}\cdot\frac{y^{4/\varepsilon}}{y((4/\varepsilon)\log y)^{4/\varepsilon}} \ge y^{3/\varepsilon},$$

for sufficiently large y, since $\varepsilon < 1/3$. In each case below we will choose ρ so that L has $\ge Q^\rho$ prime divisors, and we see in the display immediately above that it will be possible to select ρ so that $Q^\rho > y^{3/\varepsilon}$. Note that $\log x = O(\ell\log Q) = O(Q^\rho) = O(2^{\pi(y)}) = \mathrm{e}^{o(y)}$. Thus if $X = x^t$ then $\log t \sim \log\log X$.

Since the product of any ℓ primes dividing L is $\le x^{2/5}$, we use (4) with $c = 0$ to obtain

$$\frac{R}{2\cdot 3^\ell} \ge \frac{c_0}{4\log x} 3^{-\ell}\binom{Q^\rho}{\ell} \ge \frac{c_3}{\ell\log Q}\left(\frac{Q^\rho}{3\ell}\right)^\ell \ge Q^{(\eta+2\varepsilon)\rho\ell} = x^{(\eta+2\varepsilon)(2\rho/5)}.$$

Since $Q^\rho > y^{3/\varepsilon}$ we have $\ell \ge Q^{\varepsilon\rho} \ge y^3$ and $Q^{(\eta+2\varepsilon)\rho} \ge y^{(3/\varepsilon)2\varepsilon} = y^6$, and so $R/(2\cdot 3^\ell) \ge Q^{(\eta+2\varepsilon)\rho\ell} \ge y^{6y^3} > t^{1/\varepsilon} > t$. Thus $R/(2t\cdot 3^\ell) \ge (R/(2\cdot 3^\ell))^{1-\varepsilon} > x^{(\eta+2\varepsilon)(2\rho/5)(1-\varepsilon)} > x^{(\eta+\varepsilon)(2\rho/5)}$. Therefore the number of Carmichael numbers produced in Corollary 2.2 is $\ge (x^{(\eta+\varepsilon)(2\rho/5)}/t)^t \ge x^{2t\eta\rho/5} = X^{2\eta\rho/5}$.

Completion of the proof of Theorem 4: For any fixed $0<\delta<1$, we can take $\rho = (2/5)(\delta-\varepsilon)$ for $\log Q = y^{1-\delta}$, by (5). Let $\eta = 1-4\varepsilon$ with $\varepsilon = \delta/20$ above. Therefore we have $\ge X^{3\delta/25}$ such Carmichael numbers up to X. Moreover $y \sim \log\log X$ for such Q, so that $\ell = \mathrm{e}^{c_\delta(\log\log X)^{(1-\delta)}}$ for some constant $c_\delta > 0$.

Completion of the proof of Theorems 3 and 1: If we take $Q = \left(\prod_{p\le y} p\right)^{5/2}$ above, then $\psi_2(Q^{2/5}, y) = 2^{\pi(y)}$ and we can take $\rho = 2\log 2/5\log y$. Let $\eta = \varepsilon = 1/100$ so that $\ell > 2^{.95\pi(y)} \ge (\log X)^{1/4\log\log\log X}$, since $1.01 + o(1) \le (\log\log X)/y \le 2.51 + o(1)$. By the above we have $\ge X^{4\log 2/2500\log\log\log X}$ such Carmichael numbers up to X.

§3. **Upper bounds and heuristics**

We shall prove

Proposition 3.1. *For any $x \ge 1$ there is a set $\mathcal{W}$ of at most $3\log x$ integers $\le x$ such that there is a witness in $\mathcal{W}$ for every odd, composite integer $n \le x$.*

Proof. As mentioned in the introduction, Monier [M] and Rabin [R] proved that at least three-quarters of the integers a in the interval $[1, n-1]$ are witnesses for any composite n. Since $a+kn$ is a witness for n whenever a is, we see that the number of witnesses up to x for $n \le x$ is $\ge x - (n/4)([x/n]+1) \ge x/2$.

We will select the elements of $\mathcal{W}$ in as 'greedy' a way as possible: First select w_1 to be that integer up to x which is most often a witness for composite $n \le x$, and discard those values of n. Next select w_2 to be that integer up to x which is most often a witness for the remaining values of n, and then discard those values of n. Then pick, in analogous way $w_3, w_4, \dots$ etc. until we have a witness for every composite $n \le x$. Note that after $w_1, \dots, w_k$ have been selected, each remaining n has at least $x/2 - k$ witnesses up to x; and so there must be some w which is a witness to a proportion of at least $(x/2-k)/(x-k)$ of the remaining values of n. We will see that $k \le x/4$ so that this proportion is $> 1/3$. Indeed we can select our w_n with $n \le \log x/\log(3/2) < 3\log x$.

Remark: The constant 3 can evidently be improved.

As a consequence of Corollary 1.2 we have

Corollary 3.2. *Suppose that n is a Carmichael number, for which every prime factor of n is congruent* mod 8*, and which are each $\equiv 3 \bmod 4$. Then there is no witness $\le Q$ for n if and only if for each odd prime $q \le Q$, the quadratic residue symbol $\left(\frac{p}{q}\right)$ takes the same value for each prime divisor p of n.*

Proof. By Corollary 1.2, if a and b are not witnesses for n then $\left(\frac{a}{p}\right)$ takes the same value for each prime divisor p of n, as does $\left(\frac{b}{p}\right)$, and so $\left(\frac{ab}{p}\right)$ does also; thus ab

is not a witness for n. Therefore the least witness for n must be a prime; and so there is a witness $\le Q$ for n if and only if there is a prime witness $q \le Q$ for n.

Now, by hypothesis $\left(\frac{2}{p}\right)$ takes the same value for each prime divisor p of n, so 2 is not a witness for n. Moreover, since each $p \equiv 3 \bmod 4$, thus $\left(\frac{q}{p}\right)$ takes the same value for each prime divisor p of n if and only if $\left(\frac{p}{q}\right)$ does, by the law of quadratic reciprocity. The result then follows form Corollary 1.2.

Carmichael numbers which have exactly three prime factors are the product of a prime triplet of the form $ag+1,\ bg+1,\ cg+1$ where a, b, c are pairwise coprime, and g is selected mod abc so that abc divides $g(bc+ca+ab)+a+b+c$. To guarantee that each of these primes is $\equiv 3 \bmod 4$ we take $g \equiv 2 \bmod 4$ and a, b, c all odd. To guarantee that the prime factors are all congruent mod8 we take $a \equiv b \equiv c \bmod 4$.

Now let's determine whether or not a prime q which divides abc can be a witness for such a Carmichael number. Let's assume that q divides c so that $\left(\frac{cg+1}{q}\right) = 1$. Thus q must divide $gab+a+b$, so that $ga+1 \equiv -a/b \bmod q$ and $gb+1 \equiv -b/a \bmod q$. Therefore $\left(\frac{ag+1}{q}\right) = \left(\frac{bg+1}{q}\right) = 1$ if and only if $\left(\frac{-ab}{q}\right) = 1$. Thus we have proved

Lemma 3.3. *Suppose that a, b and c are given odd, pairwise coprime integers which are all congruent* mod 4. *Suppose that Carmichael number n is the product of three primes $ag+1,\ bg+1,\ cg+1$ where $g \equiv 2 \bmod 4$. Then none of the prime factors q of abc are witnesses for n 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.*

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 $ax^2+by^2+cz^2 \equiv 0 \bmod 8$ and $\left(\frac{-bc}{p}\right) = 1$ 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. Surely this is a co-incidence?

The proof of Theorem 2: We shall consider prime triplets of the form $g+1, 5g+1, 9g+1$. We only allow $g \equiv 2 \bmod 4$ and $g \equiv 15 \bmod 45$, so that if all three of these numbers are prime then their product n is indeed a Carmichael number. For every prime $q \le Q$ we will only allow $g \equiv 0 \bmod q$, so that $\left(\frac{g+1}{q}\right) = \left(\frac{5g+1}{q}\right) = \left(\frac{9g+1}{q}\right) = 1$. Therefore the least witness for n is $> Q$ by Corollary 3.2. The above congruence conditions, when combined, fix g in a congruence class mod$N = 6\prod_{q \le Q} q$. 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 $g \le \gamma_3 N(45N^3)^{A_3}$. The resulting Carmichael number n is $\le c_4 N^{9A_3+3}$, and this is $\le x$ for $Q = \log x/(9A_3+4)$ by the prime number theorem.

In the above argument we could actually have chosen any $g \bmod q$, for which $\left(\frac{g+1}{q}\right) = \left(\frac{5g+1}{q}\right) = \left(\frac{9g+1}{q}\right)$, for each prime $7 \le q \le Q$. One can use Weil's

theorem[13] to show that this holds for $q/4+O(\sqrt{q})$ of the congruence classes g mod 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 $\left(\frac{g+1}{q}\right) = \left(\frac{5g+1}{q}\right) = \left(\frac{9g+1}{q}\right)$ for each prime $7 \le q \le Q$, in the hypothesis. Instead we wish to be a little more general[14]: Consider all triplets of the form $g+1, 5g+1, 9g+1$ where $g \equiv 150 \bmod 180$. For any non-square integer $q \le x$, we can prove that $\left(\frac{g+1}{q}\right) = \left(\frac{5g+1}{q}\right) = \left(\frac{9g+1}{q}\right)$ for at least a quarter of the congruence classes mod$q$. Thus for a set of ℓ such integers q we expect these identities with the Jacobi symbols to hold for all q simultaneously, for at least $c_5 x^{1/3}/4^{\ell}$ values of $g \le x^{1/3}/3$. Now, the usual heuristic is that a proportion $\gg 1/(\log x)^3$ of these triples will be simultaneously prime. Therefore we expect that

There are at least $x^{1/5}$ Carmichael numbers up to x without a witness from any given set of $\ell = \frac{1}{11}\log x$ distinct integers $\le x$.

Combining this with Proposition 3.1 it seems that we really do know the size of the optimal set of reliable witnesses $\le x$, up to the constant.

If we take our set of integers here to be the set of primes q up to $Q = \frac{1}{12}\log x \log\log x$ then, by Corollary 3.2 we expect that

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

On the other hand, we do not expect there to be *any* values of $g \le x^{1/3}$ such that $\left(\frac{g+1}{q}\right) = \left(\frac{5g+1}{q}\right) = \left(\frac{9g+1}{q}\right)$ for each of the smallest $\log x$ primes q (since the 'expected' number of such g would be $\approx x^{1/3}/4^{\log x} < 1/x$). Thus we would expect that

Every composite number n has a witness $\le \{1+o(1)\}\log n \log\log n$.

§4. **Further remarks**

In [AGP] we claimed that we could prove the following result, which we now prove here.

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

Note how this generalizes Korselt's criterion in a natural way. This result provides 'pseudoprimes' to all bases for various compositeness tests.

We will need the following Lemma which is proved exactly as Theorem 3.1 in [AGP][15]

[13] That is, the 'Riemann Hypothesis for curves'

[14] and hopefully still plausible

[15] 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 $B = 2/5$.

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 $\le 1/60$, then there exists a positive integer $k \le x^{3/5}$, coprime to am, such that*

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

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

We apply Lemma 4.2 with $x = m^{5/2}$. Therefore there exists an integer $k \le m^{3/2}$ such that the number of primes of the form $dk + a$ where d divides m is

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

By Theorem 1.1 (modified analogously to our Proposition 1.3) there is some non-trivial subset of these primes whose product $n \equiv 1 \bmod mk$. Therefore $p-a$ divides dk, which divides mk, which divides $n-1$, for each prime p dividing n.

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 composite integers n for which p^2-1 divides $n-1$ for every prime p dividing n ?*

In 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 composite integers n for which $p+1$ divides $n+1$ for every prime p dividing n ?*

In this question we have no idea how to prove the necessary analogue of Proposition 1.3 (or Theorem 1.1 in [AGP]).

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.

[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.

[IT] A. Ivić and G. Tenenbaum, *Local densities over integers free of large prime factors*, Quart. J. Math. Oxford (2) **37** (1986), 401–417.

[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.

[W] S. Wigert, *Sur l'ordre de grandeur du nombre des diviseurs d'un entier*, Arkiv. für mat. **3** (1907), 1–9.

Department of Mathematics, University of Georgia, Athens, Georgia 30602.

E-mail addresses of the authors:
Alford: red@math.uga.edu
Granville: andrew@math.uga.edu
Pomerance: carl@math.uga.edu