ACTA ARITHMETICA
LXXX.4 (1997)

The average least witness is 2

by

Ronald Joseph Burthe Jr. (Columbia, Md.)

1. Introduction. Let n be a positive odd number greater than 1 with $n-1=2^s t$ where t is odd. For $a\in[1,n-1]$, we say that n is a *strong pseudoprime to base* a if

$$\text{(1.1)}\qquad \textit{either } a^t\equiv 1 \bmod n \textit{ or } \quad a^{2^i t}\equiv -1 \bmod n \text{ for some } i\in\{0,1,\ldots,s-1\}.$$

Now if for a given positive integer n we can find an integer $a\in[1,n-1]$ such that (1.1) does not hold for a, then we know that n is composite. Such an a is said to be a *witness* for n. Note that if $a\in[1,n-1]$ and $(a,n)>1$, then surely (1.1) fails, and such an a is a witness for n. There are many other witnesses too. From the proof in [M] and [R], if n is an odd composite greater than 9, then at least three-fourths of the $\phi(n)$ numbers in $[1,n-1]$ coprime to n are witnesses for n. Of course, all the numbers in $[1,n-1]$ that are not coprime to n are witnesses for n. If one picks t a's at random from $[1,n-1]$ and discovers that each satisfies (1.1), one cannot however conclude that n is prime. We can conclude that if n is an odd composite number, the probability that all the t randomly chosen a's satisfy (1.1) is less than 4^{-t}.

It is natural to ask what can be said about the least positive witness, denoted by $w(n)$, for an odd composite n. Erdős [E1] and Pomerance [P2] have shown that any fixed integer is a witness for most odd composite n, so in particular $w(n)$ will be 2 for most n. However, $w(n)$ can be arbitrarily large as shown by Alford, Granville and Pomerance in [AGP]. Since every composite n has a prime divisor not exceeding $\sqrt{n}$, a trivial upper bound for $w(n)$ is $\sqrt{n}$ but this upper bound is too large to give a polynomial time algorithm that could prove primality. However, the works of Ankeny, Weinberger, Oesterlé, and Bach (see [B]) show that if the Generalized Rie-

1991 *Mathematics Subject Classification*: Primary 11A51.

mann Hypothesis (GRH) holds, then $w(n) < 2\log^2 n$ for all composite n and we would thus have a polynomial time deterministic primality test. We will show that this result also implies that if the GRH is true, then the "average" of the $w(n)$ is asymptotically 2. Specifically, let $C(x)$ denote the number of odd composite integers n not exceeding x and let $\sum^*$ denote a sum over the n counted by $C(x)$. We shall show in Theorem 2.1 that if the GRH holds then

$$\frac{\sum^* w(n)}{C(x)} \sim 2 \tag{1.2}$$

as $x \to \infty$. Since $C(x) \sim x/2$, we can also write (1.2) as $\sum^* w(n) \sim x$ as $x \to \infty$. So if (1.2) holds, we can conclude that even though $w(n)$ can be arbitrarily large, there cannot be too many odd composite n that have large $w(n)$.

In this paper, we also prove (1.2) *without* assuming the GRH.

There are two key results which are instrumental in our non-GRH proof of (1.2). The first uses a theorem of Montgomery (see [Mo4]), which builds on the work of Rodosskiĭ (see [Ro]). Lagarias, Montgomery, and Odlyzko (see [LMO]) derived a more general result following Rodosskiĭ's method and the version used here is actually a specific example of this more general result. We now state Montgomery's theorem.

For a non-principal Dirichlet character χ let $B(\chi)$ denote the least positive integer a such that $\chi(a) \neq 1$ and $\chi(a) \neq 0$. For principal characters χ we set $B(\chi) = 0$. Also, for a Dirichlet character χ, and real numbers σ and t with $1/2 \le \sigma \le 1$ and $t \ge 0$, let $N(\sigma, t, \chi)$ denote the number of zeroes of the Dirichlet L-function $L(s, \chi)$ with $s = \beta + \gamma i$ and $\sigma \le \beta \le 1$ and $|\gamma| \le t$. Montgomery's theorem states that there exists an absolute positive constant c_1 such that for every Dirichlet character $\chi \bmod d$ and for $(\log d)^{-1} < \delta \le 1/2$,

$$N(1-\delta, \delta^2 \log d, \chi) = 0 \Rightarrow B(\chi) < (c_1 \delta \log d)^{1/\delta}. \tag{1.3}$$

From Proposition 2.1 in [Bur] we know that one can find a character $\chi \bmod n$ such that $B(\chi) = G(n)$ where $G(n)$ is the smallest G such that the positive integers less than or equal to G and coprime to n generate $(\mathbb{Z}/n\mathbb{Z})^*$. By Lemma 2.4 in [Bur], we also know that for odd composite n, $w(n) \le G(n)$ so if the hypothesis in (1.3) holds, we obtain an upper bound for $w(n)$ as well as $G(n)$ and this will be a major component of our main theorem.

The second key result involves the use of zero density estimates for the number of zeroes of Dirichlet L-functions in specified regions. In particular, from a result due to Gallagher (see [G]) in 1970, for $1/2 \le \sigma \le 1$ and $t \ge 1$ we have

$$\sum_{d\le t}\sum_{\substack{\chi \bmod d\\ \chi\,\mathrm{primitive}}} N(\sigma,t,\chi)\le c_2 t^{c_3(1-\sigma)} \tag{1.4}$$

for absolute constants c_2 and c_3. It should be noted that results similar to (1.4) (but with more complicated upper bounds) were previously obtained by Bombieri [Bo], Jutila [Ju1], and Montgomery [Mo1], [Mo2]. Also Selberg [Se] derived a generalization of (1.4). Motohashi in 1983 (see [Mot]) showed that c_3 can be taken to be 8 over the same range for σ and t and in 1990 Coleman [C] showed, using a result of Heath-Brown [HB], that for $1/2\le\sigma\le 1$, $t\ge 1$, c_3 can be taken as $64/9+\varepsilon$ with c_2 now being dependent upon ε. However, the best result for our purposes comes from two 1977 papers of Jutila [Ju2] and [Ju3] which give a value of $6+\varepsilon$ for c_3 if $4/5\le\sigma\le 1$ and with c_2 now being dependent upon ε. In 1979, Heath-Brown in [HB] extended this range for σ to $11/14\le\sigma\le 1$.

Using these ideas we not only prove (1.2) but also the following (see Corollary 3.3): for all $x\ge 2$,

$$\sum_{n\le x} G(n)=O(x(\log x)^{97}). \tag{1.5}$$

So (1.5) implies that the average of $G(n)$ for positive integers $n\le x$ is $O(\log^{97} x)$. It should also be noted that Bach and Huelsbergen conjecture that

$$\frac{1}{x}\sum_{n\le x} G(n)\sim \log\log x\log\log\log x \tag{1.6}$$

as $x\to\infty$. So our upper bound for the average may still be far from its true value. But by choosing $z=(\log x)^{97}$ in Theorem 3.2 we see that all "large" $G(n)$ can be ignored in trying to prove (1.6). It should also be remembered that the GRH implies that $G(n)=O(\log^2 n)$ (see [Mo3]). We were not able to prove this result without assuming the GRH, but we have proved, as mentioned above, that the *average* of $G(n)$ for positive integers $n\le x$ is bounded by a power of $\log x$.

It should also be noted that Burgess and Elliott obtained in [BE] a result similar to (1.5) for primitive roots. Namely, they showed that if $g(p)$ is the least primitive root mod p and p is an odd prime then

$$\frac{1}{\pi(x)}\sum_{p\le x} g(p)=O((\log x)^2(\log\log x)^4).$$

Since $G(p)\le g(p)$, this immediately gives us that the average of the $G(p)$, taken over the primes not exceeding x, is $O((\log x)^2(\log\log x)^4)$. Note that this is close to the upperbound for the average that one would get by assuming the GRH.

Similar results can be obtained for $w(n)$. Recalling that $\sum^*$ denotes a sum over odd composite positive n which are at most x, we will show that for all $x \ge 1$ and $z > (\log x)^8$,

$$\sum_{w(n)>z}^{*} w(n) = O\biggl(\frac{x}{z^{7/2}}(\log x)^{28}\biggr). \tag{1.7}$$

This result combined with a result from [P2] gives (1.2) as a corollary without the use of the GRH.

I would like to thank Carl Pomerance and Andrew Granville for their considerable input into this paper which was derived from my dissertation (University of Georgia, 1995).

2. $w(n)$ **on average.** In this section we will prove our main theorem that the average value of $w(n)$ is asymptotically 2. First we will show why one would suspect that this would be the case. Recall that $\sum^*$ is a sum over odd composite integers less than or equal to x and that $C(x)$ is the number of odd composites less than or equal to x.

Theorem 2.1. *If the GRH holds, then*

$$\frac{\sum^* w(n)}{C(x)} \sim 2$$

as $x \to \infty$.

Proof. Since $w(n) \ge 2$ for odd composite n,

$$\frac{\sum^* w(n)}{C(x)} \ge 2.$$

Furthermore,

$$\sum^* w(n) = \sum_{w(n)=2}^{*} 2 + \sum_{w(n)\ne 2}^{*} w(n).$$

To prove our result it will suffice to show that

$$\lim_{x\to\infty} \frac{\sum^*_{w(n)\ne 2} w(n)}{C(x)} = 0.$$

Since $C(x) \sim x/2$ (as the primes have density 0), this is equivalent to

$$\sum_{w(n)\ne 2}^{*} w(n) = o(x).$$

Noting that $w(n) \ne 2 \Rightarrow 2^{n-1} \equiv 1 \bmod n$, from [P2] we see that the number of odd composite $n \le x$ with $w(n) \ne 2$ is bounded by $xL(x)^{-1/2}$ for large x where $L(x) = \exp((\log x \log\log\log x)/\log\log x)$. From [B], we see that the

GRH implies that $w(n) < 2\log^2 n$. Thus

$$\sum_{w(n)\neq 2}^{*} w(n) < 2xL(x)^{-1/2}\log^2 x = o(x)$$

for $x \to \infty$. This completes the proof.

Recall that $B(\chi)$ denotes the least positive integer a such that $\chi(a) \neq 1$ and $\chi(a) \neq 0$.

THEOREM 2.2. *For all $x \geq 2$ and $z \geq (\log x)^8$, we have uniformly*,

$$\sum_{w(n)>z}^{*} w(n) = O\biggl(\frac{x}{z^{7/2}}(\log x)^{28}\biggr).$$

Proof. We may assume that x exceeds some arbitrarily large bound.

From Proposition 2.1 in [Bur] we can find a non-principal character χ_n mod n such that $B(\chi_n) = G(n)$. Letting ψ denote the primitive character mod d that induces χ_n, we have by Lemma 2.5 in [Bur] that $w(n) \leq B(\psi)$. By Theorem 3.6 in [Bur] for every $\varepsilon > 0$, we have $B(\psi) = O_\varepsilon(d^{1/(3\sqrt{e})+\varepsilon})$.

Since $(3\sqrt{e})^{-1} < .21$, there thus exists an absolute constant E such that $w(n) \leq Ed^{.21}$. Since $w(n) > z \geq \log^8 x$, we have $d^{.21} > E^{-1}(\log^8 x)$. So by letting x be sufficiently large, we have $d^{.01} > E$ and thus $w(n) \leq d^{.22} < d^{2/9}$.

Letting $f(\chi)$ denote the conductor of χ we see that

$$\sum_{w(n)>z}^{*} w(n) = \sum_{z^{9/2}<d\leq x} \ \sum_{\substack{w(n)>z\\ f(\chi_n)=d}}^{*} w(n).$$

For a Dirichlet character χ and for $\sigma \in \mathbb{R}$, with $1/2 \leq \sigma \leq 1$, and for $t \in \mathbb{R}$ with $t \geq 0$, recall that $N(\sigma, t, \chi)$ denotes the number of zeroes of the Dirichlet L-function $L(s, \chi)$ with $s = \beta + \gamma i$, $\sigma \leq \beta \leq 1$ and $|\gamma| \leq t$.

From Montgomery's result (1.3) there exists an absolute constant c_1 such that for non-principal Dirichlet characters χ mod d and for $1/2 \leq \sigma < 1 - (\log d)^{-1}$,

$$N(\sigma, (1-\sigma)^2\log d, \chi) = 0 \Rightarrow B(\chi) < (c_1(1-\sigma)\log d)^{1/(1-\sigma)}. \tag{2.1}$$

Now let $\sigma := 1 - (1.001\log\log x)/(\log z)$. Since $z \geq (\log x)^8$, we have $\sigma \geq .874$. Also, for $x > 4$ and $z^{9/2} < d$, we have $\sigma < 1 - (\log z^{9/2})^{-1} < 1 - (\log d)^{-1}$; so for all d with $z^{9/2} < d \leq x$, we can apply (2.1).

Let ψ be the primitive character mod d that induces χ_n. We have the identity (see page 37 of [D])

$$L(s, \chi_n) = L(s, \psi)\prod_{\substack{p\mid n\\ p\nmid d}}(1 - \psi(p)p^{-s})$$

where the product is taken over primes p. Thus we have $N(\sigma,d,\chi_n) = N(\sigma,d,\psi)$. Let $\mathcal{U}_d$ denote the set of primitive characters θ of modulus d such that $N(\sigma,d,\theta)>0$. We see from (2.1) that for $d=f(\chi_n)=f(\psi)$,

$$\begin{aligned}\psi\notin\mathcal{U}_d &\Rightarrow N(\sigma,d,\psi)=0\\ &\Rightarrow N(\sigma,d,\chi_n)=0\\ &\Rightarrow N(\sigma,(1-\sigma)^2\log d,\chi_n)=0\\ &\Rightarrow B(\chi_n)<(c_1(1-\sigma)\log d)^{1/(1-\sigma)}\\ &\Rightarrow w(n)<(c_1(1-\sigma)\log d)^{1/(1-\sigma)}.\end{aligned}\tag{2.2}$$

Note that this result uses the fact that $(1-\sigma)^2\log d<d$ and the fact that $w(n)\le B(\chi_n)$ as previously mentioned, as well as the result that $N(\sigma,d,\chi_n)=N(\sigma,d,\psi)$. Since $\sigma\ge .874$, for large x we have

$$\begin{aligned}(c_1(1-\sigma)\log d)^{\frac{1}{1-\sigma}} &\le (.126c_1\log x)^{\frac{\log z}{1.001\log\log x}}\\ &\le (\log^{1.001}x)^{\frac{\log z}{1.001\log\log x}}=z.\end{aligned}$$

So if $w(n)>z$, by (2.2) we must have $\psi\in\mathcal{U}_d$. Thus, our sum for $w(n)$ will have an upper bound of

$$\sum_{z^{9/2}<d\le x}\ \sum_{\psi\in\mathcal{U}_d}\ \sum^{*}_{\chi_n \text{ induced by } \psi} w(n).$$

Since $w(n)\le d^{2/9}$ we see that (since $d\,|\,n$ whenever $\psi\in\mathcal{U}_d$ and ψ induces χ_n)

$$\begin{aligned}\sum^{*}_{w(n)>z} w(n) &\le \sum_{z^{9/2}<d\le x}\ \sum_{\psi\in\mathcal{U}_d}\ \sum_{n\le x,d|n} d^{2/9}\\ &\le \sum_{z^{9/2}<d\le x}\ \sum_{\psi\in\mathcal{U}_d}\frac{x}{d}\cdot d^{2/9}\\ &= x\sum_{z^{9/2}<d\le x}\#\mathcal{U}_d d^{-7/9}.\end{aligned}\tag{2.3}$$

Recall that since $\sigma\ge .874$, from Jutila's result mentioned in Section 1 we have

$$\begin{aligned}\sum_{d\le t}\#\mathcal{U}_d &= \sum_{d\le t}\ \sum_{\substack{\chi \bmod d\\ \chi \text{ primitive}\\ N(\sigma,d,\chi)>0}} 1 \le \sum_{d\le t}\ \sum_{\substack{\chi \bmod d\\ \chi \text{ primitive}}} N(\sigma,d,\chi)\\ &= O_\varepsilon(t^{(6+\varepsilon)(1-\sigma)}).\end{aligned}\tag{2.4}$$

Letting $b_d := \#\mathcal{U}_d$ and choosing $\varepsilon=.01$, we thus see that there is a constant c' such that

(2.5)
$$\sum_{d\le t} b_d \le c' t^{6.01(1-\sigma)}.$$

Also from (2.3) we have

(2.6)
$$\sum_{w(n)>z}^{*} w(n) \le x \sum_{z^{9/2}<d\le x} b_d d^{-7/9}.$$

From (2.5) and (2.6), we see by partial summation and a computation that

$$\sum_{w(n)>z}^{*} w(n) = O\biggl(\frac{x}{z^{7/2}}(\log x)^{28}\biggr).$$

We have used the fact that $6.01(1-\sigma) - 7/9 < -.02051 < 0$ and that

$$(z^{9/2})^{6.01(1-\sigma)-7/9} = (\log x)^{27.072045} z^{-7/2}.$$

This concludes the proof of Theorem 2.2.

It should be noted that this upper bound can be improved somewhat by taking a sharper upper bound for $w(n)$ from [Bur] and being more careful with the other estimates. By choosing sharper estimates in this proof one can show that for all $x \ge 2$ and $z \ge (\log x)^{6(1-\frac{1}{3\sqrt{e}})^{-1}+\gamma}$ where $\gamma > 0$ we have

$$\sum_{w(n)>z}^{*} w(n) = O_\gamma(xz^{1-(\frac{1}{3\sqrt{e}}+.0014+.004\gamma)^{-1}}(\log x)^{18.03\sqrt{e}+.09\sqrt{e}\gamma}).$$

Corollary 2.3. *Let $C(x)$ denote the number of odd composite integers less than or equal to x. Then*

$$\frac{\sum^{*} w(n)}{C(x)} \sim 2$$

as $x \to \infty$.

Proof. Fix an $\varepsilon > 0$ and let z be a positive real number. We have

$$\sum\nolimits^{*} w(n) = 2C(x) + \sum_{2<w(n)\le z}^{*} (w(n)-2) + \sum_{w(n)>z}^{*} (w(n)-2).$$

Now $w(n) > 2$ implies that n is a strong pseudoprime to base 2, and from [P2] we know that the number of such odd composite integers less than or equal to x does not exceed $xL(x)^{-1/2}$ for sufficiently large x, where

$$L(x) = \exp(\log x \log\log\log x/\log\log x).$$

Thus

$$\sum_{2<w(n)\le z}^{*} (w(n)-2) \le z\cdot xL(x)^{-1/2}$$

for x sufficiently large. Letting $z = L(x)^{1/9}(\log x)^{56/9}$ in Theorem 2.2 we see that for x sufficiently large,

$$\sum\nolimits^{*} w(n) = 2C(x) + O(xL(x)^{-7/18}(\log x)^{56/9}).$$

Using the fact that $C(x) \sim x/2$ gives us our result.

We have actually shown something slightly stronger; namely, that

$$\sum\nolimits^{*} w(n) = 2C(x)\{1 + O_\varepsilon(L(x)^{-7/18+\varepsilon})\}$$

for every $\varepsilon > 0$. From the proof of Theorem 2.1, the 7/18 may be replaced with a 1/2 under assumption of the GRH.

3. Similar results for $G(n)$. We would like to establish a result similar to Theorem 2.2 for $G(n)$. However, we could not get a clear inequality comparable to $w(n) \le d^{2/9}$ and a more tedious approach was used instead. The following lemma will play a key role in proving a comparable result for $G(n)$.

Let χ_0 denote the principal character mod n.

LEMMA 3.1. *Let ψ be a primitive character mod d and let n be an integer at least* 2. *Then*

$$B(\psi\chi_0) = O(d\log^2 n).$$

Proof. Let $a = B(\psi)$ and note that $(a, d) = 1$. Let M denote the largest divisor of n which is coprime to d. If $(a, M) = 1$, then $(a, dn) = 1$ so that $a = B(\psi\chi_0) = B(\psi) < d$ so the result holds in this case.

Thus we can assume that $(a, M) > 1$. We want to find a small positive integer k such that $(a+kd, M) = 1$ since this would imply that $(a+kd, n) = 1$ and so

$$\psi\chi_0(a + kd) = \psi(a)\chi_0(a + kd) = \psi(a).$$

So since $\psi(a) \notin \{0, 1\}$, we would then have $B(\psi\chi_0) \le a + kd$.

For positive integers m, let $g(m)$ denote the Jacobsthal function which is defined as the least positive integer g such that every set of g consecutive integers contains at least one integer relatively prime to m. We will show that there is an integer k with $0 < k < g(M)$ and $(a + kd, M) = 1$ by borrowing an idea used in Theorem 1 of [P1].

Suppose that $(a+kd, M) > 1$ for $k = 0, 1, \ldots, g(M)-1$. Then for any $j \in \mathbb{Z}$ we must also have $(a + jM + kd, M) > 1$ for $k = 0, 1, \ldots, g(M) - 1$. Since $(M, d) = 1$, the congruence $Mx \equiv -a \bmod d$ has a solution $x \equiv j \bmod d$; thus, we see that there exists an integer u such that $Mj = -a + ud$. Then $a + jM + kd = ud + kd$, so that $(ud + kd, M) > 1$ for $k = 0, 1, \ldots, g(M) - 1$. Since $(d, M) = 1$, this implies that $(u + k, M) > 1$ for $k = 0, 1, \ldots, g(M) - 1$

which contradicts the definition of $g(M)$. So there must be an integer k with $0 \le k < g(M)$ such that $(a + kd, M) = 1$.

Thus $B(\psi\chi_0) \le a + (g(M) - 1)d < g(M)d$ since $a < d$. Erdős [E2] and Hooley [H] have shown that there is a constant c such that for all $m \in \mathbb{Z}^+$ we have $g(m) = O(\log^c m)$ and Iwaniec [I] has shown that we can take $c = 2$. Applying Iwaniec's result, we thus see that $B(\psi\chi_0) = O(d \log^2 n)$ and this concludes the proof of Lemma 3.1.

We shall now prove the following theorem.

THEOREM 3.2. *For $x \ge 2$ and $z \ge (\log x)^{97}$, we have uniformly*

$$\sum_{n \le x, G(n) > z} G(n) = O\bigg(\frac{x}{z^{.06}} (\log x)^{7.83}\bigg).$$

Proof. It suffices to prove the theorem for all values of x beyond some absolute bound. From Proposition 2.1 in [Bur] there is a character χ_n mod n such that $B(\chi_n) = G(n)$. Thus we see that

$$\sum_{n \le x, G(n) > z} G(n) = \sum_{n \le x, B(\chi_n) > z} B(\chi_n).$$

Let ψ denote the primitive character mod d that induces χ_n, so that $\psi\chi_0 = \chi_n$. From Lemma 3.1 we see that there exists an absolute positive constant c_4 such that for $n \le x$, we have $B(\chi_n) < c_4 d \log^2 x$. Since we are only considering the case where $G(n) = B(\chi_n) = B(\psi\chi_0) > z$ and since $z \ge (\log x)^{97}$ we see that for x sufficiently large (i.e., $\log x \ge c_4$)

$$(\log x)^{97} \le z < B(\psi\chi_0) < c_4 d \log^2 x \le d \log^3 x \le d z^{3/97}$$

and thus $d \ge z^{94/97}$. So our sum above must be bounded by

$$\sum_{z^{94/97} \le d \le x} \ \sum_{\substack{\psi \bmod d \\ \psi \text{ primitive}}} \ \sum_{\substack{n \le x, d \mid n \\ B(\psi\chi_0) > z}} B(\psi\chi_0). \tag{3.1}$$

Recall the definition of $N(\sigma, t, \chi)$ from Section 1.

We take $\delta = (1 + \alpha)(\log\log x)/\log z$ in Montgomery's result (1.3) where $\alpha = .001$. Let $\sigma = 1 - \delta$. Thus if n is such that $1/2 \le \sigma < 1 - (1/\log n)$, and χ is a Dirichlet character mod n, then

$$N(\sigma, (1 - \sigma)^2 \log n, \chi) = 0 \Rightarrow B(\chi) < (c_1(1 - \sigma)\log n)^{1/(1-\sigma)}. \tag{3.2}$$

Suppose $B(\psi\chi_0) \ge z$. Since $z \ge (\log x)^{97}$, we have $\sigma \ge 1 - (1 + \alpha)/97 \ge 4/5$. Also, for $x > e^{e^2}$ and $z^{94/97} \le d$, we see from the definition of σ that $\sigma < 1 - 2(\log z)^{-1} \le 1 - (\log d)^{-1} < 1 - (\log n)^{-1}$; so for all d with $z^{94/97} \le d \le x$, we can apply (3.2) to $\psi\chi_0$. Since $\sigma \ge 1 - (1 + \alpha)/97$ we have for x sufficiently large,

$$(c_1(1-\sigma)\log n)^{\frac{1}{1-\sigma}} \le \left(\frac{c_1(1+\alpha)}{97}\log x\right)^{\frac{\log z}{(1+\alpha)\log\log x}}$$
$$\le (\log^{1+\alpha} x)^{\frac{\log z}{(1+\alpha)\log\log x}} = z.$$

Therefore by (3.2) we see that if $B(\psi\chi_0) \ge z$, then there is a zero $s = \beta + \gamma i$ of $L(s, \psi\chi_0)$ with $\beta \ge \sigma$ and $|\gamma| \le (1-\sigma)^2 \log n$. Note too that $(1-\sigma)^2 \log n < \log n \le \log x \le z^{1/97} \le d$ so that if $B(\psi\chi_0) \ge z$, then $N(\sigma, d, \psi\chi_0) > 0$.

As was done in Theorem 2.2, we will have $N(\sigma, d, \psi) = N(\sigma, d, \psi\chi_0)$. Using this fact, the definition of $\mathcal{U}_d$ from Theorem 2.2, and the above results, we see as in (2.2) that if $n \le x$ and $d \mid n$ then

$$\psi \notin \mathcal{U}_d \Rightarrow B(\psi\chi_0) < z. \tag{3.3}$$

So if $B(\psi\chi_0) > z$, by (3.3) we must have $\psi \in \mathcal{U}_d$. Our sum in (3.1) can thus be rewritten as

$$\sum_{z^{94/97} < d \le x} \sum_{\psi \in \mathcal{U}_d} \sum_{n \le x, d \mid n} B(\psi\chi_0). \tag{3.4}$$

We will now show that if ψ is a primitive character mod d, then $B(\psi\chi_0) \le d^{1/2}$ for most positive integers $n \le x$ with $d \mid n$ (i.e. with only about $O(xd^{-17/16})$ exceptions). Then we will break (3.4) into two sums, one of which will use $d^{1/2}$ as the upper bound for $B(\psi\chi_0)$ and the other will use $O(d \log^2 x)$ from Lemma 3.1 as an upper bound.

Assume that for some positive integer $n \le x$ with $d \mid n$ we have $B(\psi\chi_0) > d^{1/2}$. So for every positive integer m with $m \le d^{1/2}$ and $(m, n) = 1$, we have $\psi(m) = \psi\chi_0(m) = 1$. Also note that if $(m, d) > 1$, then $\psi(m) = 0$. Thus

$$\sum_{\substack{m \le d^{1/2} \\ (m, n/d) = 1}} \psi(m) = \sum_{m \le d^{1/2}} \psi\chi_0(m) = \sum_{\substack{m \le d^{1/2} \\ (m,n)=1}} 1.$$

Since each prime $m \le d^{1/2}$ not dividing n contributes 1 to this last sum, we have

$$\sum_{\substack{m \le d^{1/2} \\ (m,n)=1}} 1 \ge \pi(d^{1/2}) - \nu(n) \tag{3.5}$$

where $\nu(a)$ is the number of distinct prime factors of a. It is trivial to show that $\nu(n) \le (\log n)/(\log 2)$ and thus $\nu(n) \le (\log x)/(\log 2)$. As before $d \ge z^{94/97} \ge \log^{94} x$ so $\log x < d^{1/94}$. Combining these results with (3.5) and using the prime number theorem we see for d sufficiently large that

$$\sum_{\substack{m\le d^{1/2}\\(m,n/d)=1}} \psi(m) > 1.5\frac{d^{1/2}}{\log d} - \frac{d^{1/94}}{\log 2} > \frac{d^{1/2}}{\log d}. \tag{3.6}$$

This gives us a lower bound for our sum.

To get an upper bound for this sum recall the well known identity for $L \in \mathbb{Z}^+$,

$$\sum_{g|L} \mu(g) = \begin{cases} 1, & L = 1,\\ 0, & L \neq 1,\end{cases}$$

where μ is the Möbius function. We thus have

$$\begin{aligned}\Big|\sum_{\substack{m\le d^{1/2}\\(m,n/d)=1}} \psi(m)\Big| &= \Big|\sum_{m\le d^{1/2}} \psi(m) \sum_{\substack{g|m\\ g|\frac{n}{d}}} \mu(g)\Big| = \Big|\sum_{g|\frac{n}{d}} \mu(g) \sum_{\substack{m\le d^{1/2}\\ g|m}} \psi(m)\Big|\\ &= \Big|\sum_{g|\frac{n}{d}} \mu(g) \sum_{gh\le d^{1/2}} \psi(gh)\Big| = \Big|\sum_{g|\frac{n}{d}} \mu(g)\psi(g) \sum_{h\le d^{1/2}/g} \psi(h)\Big|\\ &\le \sum_{g|\frac{n}{d}} \Big|\sum_{h\le d^{1/2}/g} \psi(h)\Big|\end{aligned}$$

with the last step coming from the triangle inequality.

From [Bu], we know that if ψ is a non-principal character mod d, $r \in \mathbb{Z}^+$, d is cubefree or $r = 2$, then for every $\varepsilon > 0$ and every $H > 0$ we have

$$\Big|\sum_{h\le H} \psi(h)\Big| = O_{\varepsilon,r}(H^{1-1/r} d^{(r+1)/(4r^2)+\varepsilon}).$$

Taking $r = 2$, we thus have

$$\Big|\sum_{h\le H} \psi(h)\Big| = O_{\varepsilon}(H^{1/2} d^{3/16+\varepsilon}).$$

Applying this result to our last inner sum we see that

$$\begin{aligned}\Big|\sum_{\substack{m\le d^{1/2}\\(m,n/d)=1}} \psi(m)\Big| &= O_{\varepsilon}\bigg(\sum_{g|\frac{n}{d}} \Big(\frac{d^{1/2}}{g}\Big)^{1/2} d^{3/16+\varepsilon}\bigg)\\ &= O_{\varepsilon}\Big(d^{7/16+\varepsilon} \sum_{g|\frac{n}{d}} g^{-1/2}\Big).\end{aligned} \tag{3.7}$$

Combining (3.6) and (3.7) and letting C_ε be the O_ε constant in (3.7), we see, for d sufficiently large, that

$$\frac{d^{1/2}}{\log d} < C_\varepsilon d^{7/16+\varepsilon} \sum_{g \mid \frac{n}{d}} g^{-1/2}.$$

Since $C_\varepsilon \log d < d^\varepsilon$ for d sufficiently large we thus get

$$d^{1/16-2\varepsilon} < \sum_{g \mid \frac{n}{d}} g^{-1/2}. \tag{3.8}$$

Now if $\sum_{g\mid(n/d)} g^{-1/2} < d^{1/16-\beta}$ where $\beta = .0001$, then by choosing d sufficiently large and ε sufficiently small we get a contradiction in (3.8). This contradiction comes from the assumption made before (3.5) that $B(\psi\chi_0) > d^{1/2}$. Thus we must have $B(\psi\chi_0) \le d^{1/2}$. To see that this is what usually occurs, consider the function $f(N) := \sum_{g\mid N} g^{-1/2}$ where $N \in \mathbb{Z}^+$. For $y \ge 1$, we have

$$\begin{aligned}\sum_{N\le y} f(N) &= \sum_{N\le y}\sum_{g\mid N} g^{-1/2} = \sum_{g\le y}\sum_{\substack{N\le y\\ g\mid N}} g^{-1/2} \le \sum_{g\le y}\frac{y}{g} g^{-1/2}\\ &= y\sum_{g\le y} g^{-3/2} \le y\Big(1+\int_1^y t^{-3/2}\,dt\Big)\\ &= y(1-2y^{-1/2}+2) \le 3y.\end{aligned}$$

Let D be the number of positive integers $N \le y$ such that $f(N) \ge d^{1/16-\beta}$. From above we see that $Dd^{1/16-\beta} \le 3y$ and thus $D \le 3yd^{-(1/16-\beta)}$. Taking $y = x/d$ we thus see that there are at most $3xd^{-(17/16-\beta)}$ integers $N \le x/d$ with $f(N) \ge d^{1/16-\beta}$. Equivalently $f(N) < d^{1/16-\beta}$ for all but at most $3xd^{-(17/16-\beta)}$ integers $N \le x/d$. So $B(\psi\chi_0) \le d^{1/2}$ for all but at most $3xd^{-(17/16-\beta)}$ integers $n \le x$ with $d \mid n$.

Our sum in (3.4) can be written as

$$\sum_{z^{94/97}\le d\le x}\ \sum_{\psi\in\mathcal{U}_d}\Big(\sum_{\substack{n\le x, d\mid n\\ B(\psi\chi_0)\le d^{1/2}}} B(\psi\chi_0) + \sum_{\substack{n\le x, d\mid n\\ B(\psi\chi_0)> d^{1/2}}} B(\psi\chi_0)\Big).$$

Using the above results and letting c_4 be the implied constant from Lemma 3.1, we see that the sum above is in fact bounded by

$$\begin{aligned}\sum_{z^{94/97}\le d\le x}\ \sum_{\psi\in\mathcal{U}_d}\Big(\frac{x}{d}d^{1/2} + 3c_4\frac{x}{d^{17/16-\beta}}d\log^2 x\Big)\\ = x\sum_{z^{94/97}\le d\le x} \#\mathcal{U}_d(d^{-1/2}+3c_4 d^{-1/16+\beta}\log^2 x).\end{aligned} \tag{3.9}$$

Since $\sigma \geq 4/5$, we can apply (2.4) and recalling that $b_d = \#\mathcal{U}_d$ we see that

$$\sum_{d\leq t} b_d = O_\varepsilon(t^{(6+\varepsilon)(1-\sigma)}). \tag{3.10}$$

Also from (3.9) we have

$$\sum_{n\leq x, G(n)>z} G(n) \leq x \sum_{z^{94/97}\leq d\leq x} b_d(d^{-1/2} + 3c_4 d^{-1/16+\beta}\log^2 x). \tag{3.11}$$

By applying (3.10) (with $\varepsilon = .01$) and (3.11), and using partial summation, a computation gives

$$\begin{aligned}\sum_{n\leq x, G(n)>z} G(n) &= O\bigg(\frac{x}{z^{\frac{94}{97}(\frac{1}{16}-\beta)}}(\log x)^{2+(6+\varepsilon)\frac{94}{97}(1+\alpha)}\bigg)\\ &= O\bigg(\frac{x}{z^{.06}}(\log x)^{7.83}\bigg).\end{aligned}$$

This concludes the proof of Theorem 3.2.

It should be noted that the exponents here are not optimal and can be improved somewhat. In particular, if $z \geq (\log x)^{96+\delta}$ for $\delta > 0$, one could show by taking α, β, and ε sufficiently small that for $x \geq 2$ we have uniformly

$$\sum_{n\leq x, G(n)>z} G(n) = O_\delta\bigg(\frac{x}{z^{\frac{47}{48\cdot 16}-\frac{\delta}{48}}}(\log x)^{7.875}\bigg).$$

This is a slightly better result than that given in Theorem 3.2.

Corollary 3.3. *For all $x \geq 2$,*

$$\sum_{n\leq x} G(n) = O(x\log^{97} x).$$

Proof. Let $z = (\log x)^{97}$. First we see that

$$\sum_{n\leq x} G(n) = \sum_{n\leq x, G(n)>z} G(n) + \sum_{n\leq x, G(n)\leq z} G(n).$$

From Theorem 3.2 we see that

$$\sum_{n\leq x, G(n)>z} G(n) = O\bigg(\frac{x}{z^{.06}}(\log x)^{7.83}\bigg) = O(x(\log x)^{97}).$$

Also we have

$$\sum_{n\leq x, G(n)\leq z} G(n) \leq xz = x(\log x)^{97}.$$

Combining these results we see that

$$\sum_{n\le x} G(n) = O(x\log^{97} x).$$

This concludes the proof of our corollary.

It should be remembered that the GRH implies that $G(n) = O(\log^2 n)$ and thus that the average $G(n)$ (taken over positive integers $n \le x$) would be $O(\log^2 x)$. Dividing our result in Corollary 3.3 by x gives us that the average $G(n)$, with $n \le x$, is $O((\log x)^{97})$ without use of the GRH.

References

[AGP] W. R. Alford, A. Granville and C. Pomerance, *On the difficulty of finding reliable witnesses*, in: L. M. Adleman and M. D. Huang (eds.), Algorithmic Number Theory, Lecture Notes in Comput. Sci. 877, Springer, Berlin, 1994, 1–16.

[B] E. Bach, *Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms*, MIT Press, Cambridge, Mass., 1985.

[Bo] E. Bombieri, *On the large sieve*, Mathematika 12 (1965), 201–225.

[Bu] D. A. Burgess, *On character sums and L-series II*, Proc. London Math. Soc. 13 (1963), 524–536.

[BE] D. A. Burgess and P. D. T. A. Elliott, *The average of the least primitive root*, Mathematika 15 (1968), 39–50.

[Bur] R. J. Burthe Jr., *Upper bounds for least witnesses and generating sets*, this volume, 311–326.

[C] M. D. Coleman, *On the equation* $b_1p - b_2P_2 = b_3$, J. Reine Angew. Math. 403 (1990), 1–66.

[D] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Springer, New York, 1980.

[E1] P. Erdős, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen 4 (1956), 201–206.

[E2] —, *On the integers relatively prime to n and on a number theoretic function considered by Jacobsthal*, Math. Scand. 10 (1962), 163–170.

[G] P. X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Invent. Math. 11 (1970), 329–339.

[HB] D. R. Heath-Brown, *The density of zeros of Dirichlet's L-functions*, Canad. J. Math. 31 (1979), 231–240.

[H] C. Hooley, *On the difference of consecutive numbers prime to n*, Acta Arith. 8 (1963), 343–347.

[I] H. Iwaniec, *On the problem of Jacobsthal*, Demonstratio Math. 11 (1978), 225–231.

[Ju1] M. Jutila, *A statistical density theorem for L-functions with applications*, Acta Arith. 16 (1969), 207–216.

[Ju2] —, *On Linnik's constant*, Math. Scand. 41 (1977), 45–62.

[Ju3] —, *Zero-density estimates for L-functions*, Acta Arith. 32 (1977), 55–62.

[LMO] J. L. Lagarias, H. L. Montgomery and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. 54 (1979), 271–296.

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

[Mo1] H. L. Montgomery, *Mean and large values of Dirichlet polynomials*, Invent. Math. 8 (1969), 334–345.

[Mo2] —, *Zeros of L-functions*, ibid., 346–354.

[Mo3] —, *Topics in Multiplicative Number Theory*, Lecture Notes in Math. 227, Springer, New York, 1971.

[Mo4] —, *Zeros of L-functions*, Chap. 9 of: *Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis*, Amer. Math. Soc., Providence, R.I., 1994, 163–178.

[Mot] Y. Motohashi, *Lectures on Sieve Methods and Prime Number Theory*, Tata Institute of Fundamental Research, Springer, Bombay, 1983.

[P1] C. Pomerance, *A note on the least prime in an arithmetic progression*, J. Number Theory 12 (1980), 218–223.

[P2] —, *On the distribution of pseudoprimes*, Math. Comp. 37 (1981), 587–593.

[R] M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory 12 (1980), 128–138.

[Ro] K. A. Rodosskiĭ, *On non-residues and zeros of L-functions*, Izv. Akad. Nauk SSSR Ser. Mat. 20 (1956), 303–306 (in Russian).

[Se] A. Selberg, *Remarks on sieves*, Proc. 1972 Number Theory Conference in Boulder, 1972, 205–216.

10344 Hickory Ridge Road Apt. 418
Columbia, Maryland 21044-4622
U.S.A.
E-mail: rjburth@orion.ncsc.mil

Received on 20.5.1996
and in revised form on 11.12.1996 (2991)