# ON THE DISTRIBUTION IN SHORT INTERVALS OF INTEGERS HAVING NO LARGE PRIME FACTOR

*J. B. Friedlander**

Bell Laboratories
Murray Hill, NJ 07974

*J. C. Lagarias*

Bell Laboratories
Murray Hill, NJ 07974

## 1. Introduction

Our motivation for the study of integers having no large prime factor arises from the factoring problem. The computational complexity of the problem of factoring a general integer $N$ has received a great deal of attention recently due to its relation to the security of certain public key cryptosystems [13]. All of the fastest known factoring algorithms share two common features: first, they rely on producing numbers $k$ all of whose prime factors are small which have certain special properties, and second, their asymptotic computational complexity has either only been analyzed probabilistically (Dixon [2]), or else under unproved but plausible assumptions, which it seems hopeless to prove at present, cf. Pomerance [12], Schnorr [14] and Schnorr and Lenstra [15]. The continued fraction method [9], Dixon's algorithm [2] and Pomerance's quadratic sieve algorithm [12] are based on finding solutions $x$ to congruences $x^2 \equiv k \pmod{N}$ where $k$ ranges over a large multiplicatively independent set of numbers all of whose prime factors are smaller than a bound $L^c$ where $L = \exp(\sqrt{\log N \log \log N})$, for various constants $c \geq 1$. The Schnorr-Lenstra algorithm [15] depends on finding a small integer $x$ for which the class number $k(Q(\sqrt{-Nx})) = k$ has all its prime factors smaller than $L^{3/2}$. Finally, an approach to a factoring algorithm sketched but not described in complete detail by J. C. P. Miller [8] is based on finding many multiplicatively independent solutions to congruences $k_1 \equiv k_2 \pmod{N}$, where $k_1$ and $k_2$ are distinct numbers all of whose prime factors are smaller than $L^{c_0}$ for a constant $c_0$. The worst-case asymptotic computational complexity of several of these algorithms is believed to be $O(L^c)$ for various small values of $c$ (see [12]) but no such result has been rigorously proved. (Dixon [2] has however, proved a weaker *probabilistic* complexity bound of this order of magnitude.) In fact the best unconditional worst-case complexity bound proved for factoring integers is an $O(N^{1/4 + \varepsilon})$ bound due to J. Pollard [11]. In all these algorithms the obstacle to further analysis is our lack of knowledge of ways to find numbers all of whose prime factors are small with the desired special properties. Of the methods mentioned above, the approach of J. C. P. Miller seems to us to offer the most hope for possible rigorous analysis because one can try to find many pairs $(k, k+N)$ in which both $k$ and $k+N$ have only small prime factors by searching all numbers $k$ in a short interval. This leads us to consider the *simpler* problem studied in this paper, the distribution in short intervals of numbers having no large prime factors, and in particular the problem of bounding the gaps between successive integers having no large prime factor.

We now establish definitions and notation. Let $P_1(m)$ denote the largest prime factor of the positive integer $m$. Let $\psi(x,y,z)$ be the number of integers $m$ in the interval $(x-z, x]$ whose largest prime factor satisfies $P_1(m) \le y$. We study the situation where

---

* Partially supported by NSERC grant A5123.

$y = x^\alpha$ for a constant $0 < \alpha < 1$. We are interested in the questions of when there is at least one such number in a short interval and when there are a positive proportion of them. With this in mind we define:

$f(\alpha) = inf\{\beta$: For each $\alpha_1 > \alpha$, $\psi(x, x^{\alpha_1}, x^\beta) > 0$ for all sufficiently large $x \geq x_0(\alpha_1, \beta)\}$.

$f^*(\alpha) = inf\{\beta$: For each $\alpha_1 > \alpha$ there is a constant $c(\alpha_1, \beta) > 0$ such that $\psi(x, x^{\alpha_1}, x^\beta) > c(\alpha_1, \beta) x^\beta$ for all sufficiently large $x \geq x_0(\alpha_1, \beta)\}$.

It is immediate that these functions have the following properties.

(I) $0 \leq f(\alpha) \leq f^*(\alpha) \leq 1$.

(II) The functions $f, f^*$ are non-increasing.

(III) $f(\alpha)$ and $f^*(\alpha)$ are continuous on the right, i.e. $f(\alpha) = \lim_{\alpha_1 \downarrow \alpha} f(\alpha_1)$.

The rather cumbersome definitions of $f(\alpha)$ and $f^*(\alpha)$ were chosen to ensure the right-continuity property (III).

In the case $z = x$, $\psi$ becomes the much-studied function $\psi(x, y)$. The asymptotic behavior of $\psi(x, x^\alpha)$ is described by the following well-known result.

*Theorem 0. For fixed* $\alpha$ *we have*

$$\psi(x, x^\alpha) = x\rho(1/\alpha)\{1 + O(1/\log x)\},$$

*where* $\rho$ *is the Dickman function, defined by the differential-difference equation*

$$\begin{cases} \rho(\mu) = 1 \text{ for } 0 < \mu \le 1, \\ \mu\rho'(\mu) = -\rho(\mu-1) \text{ for } \mu > 1, \\ \rho \text{ \textit{continuous on}} (0,\infty). \end{cases}$$

For a proof of Theorem 0 and properties of $\rho(\mu)$ see for example [1]. In view of Theorem 0 it is natural to expect:

*Conjecture 1. For any fixed positive* $\alpha, \beta$

$$\psi(x, x^{\alpha}, x^{\beta}) \sim \rho(1/\alpha) x^{\beta} .$$

*as* $x \to \infty$.

From Conjecture 1 immediately follows:

*Conjecture 2.* $f(\alpha)$ *and* $f^{*}(\alpha)$ *are identically zero.*

A. Hildebrand [6] has proved that the asymptotic formula

$$\psi(x, x^{\alpha}, x^{\beta}) \sim \rho(1/\alpha) x^{\beta}$$

is valid when $\beta > 1 - \frac{5}{12}\alpha$. In this paper we will be concerned with smaller values of $\beta$ where the asymptotic formula is not known to hold.

In §2 we study the function $f^{*}(\alpha)$. For large values of $\alpha$ we prove the following result.

*Theorem 1. There exists a positive constant* $c_0^*$ *such that for* $3/4 \le \alpha < 1$ *we have*

$$f^*(\alpha) \le 1 - \alpha - c_0^*(1-\alpha)^3 .$$

We then prove the following result valid for small values of $\alpha$.

*Theorem 2. There exists a positive constant* $c_1^*$ *such that for* $0 < \alpha \le 3/4$ *we have*

$$f^*(\alpha) \le 1 - (1+c_1^*)\alpha$$

Both of these results are proved starting from a familiar idea of Chebyshev. The first theorem uses a result of Jutila [7] which in turn requires Vinogradov and van der Corput estimates for exponential sums and ideas of Ramachandra. A result based along similar lines is due to Erdös and Turk [17, p. 7]. The second theorem is derived from the first using iteration and a Buchstab identity. Combining Theorems 1 and 2 gives

$$f^*(\alpha) \le 1-\alpha-c_2^*\alpha(1-\alpha)^3$$

for $0 \le \alpha \le 1$ where $c_2^* = \min(c_0^*, c_1^*)$.

Now we turn to bounds for $f(\alpha)$. We first note that upper bounds for $f(\alpha)$ give upper bounds for $f(\alpha_1)$ for all $\alpha_1 \le \alpha$, by an easy argument due to Balog and Sárközy.

*Theorem 3. For* $0 < \lambda < 1$ *we have*

$$f(\lambda\alpha) \le \lambda f(\alpha) + 1 - \lambda.$$

We obtain an explicit bound for $f(\alpha)$ for small $\alpha$ by a construction.

*Theorem 4. Let* $r \ge 2$ *be an integer. There exist positive constants* $c_1, c_2, \ldots, c_{r-1}$ *and d, depending only on r, such that if* $S_r$ *is the set of those integers of the form*

$$s = (x - a_1)(x - a_2) \cdots (x - a_{r-1})(x + \sum_{j=1}^{r-1} a_j) \tag{1.1}$$

*where* $x, a_1, \ldots, a_{r-1}$ *are integers subject to*

$$|a_j| \le c_j x^{\frac{1}{2^j}}, \quad j = 1, \ldots, r-1,$$

*then* $S_r$ *has the property that for any N there exists an s in* $S_r$ *with*

$$0 \le s - N \le d x^{r-2+\frac{1}{2^{r-1}}}. \tag{1.2}$$

*Consequently, for* $r = 2, 3, \ldots$

$$f\left(\frac{1}{r}\right) \le 1 - \frac{2}{r} + \frac{1}{r 2^{r-1}}.$$

The case $r = 2$ of this result has been discovered independently by Balog and Sarkozy. Note that the set $S_r$ has $O_r\left[N^{\frac{2}{r} - \frac{1}{r2^{r-1}}}\right]$ elements in the interval [1,N] so that (1.2) implies the elements in $S_r$ are well-spaced. An examination of the proof shows that for large *N*, one may take $c_j = r^{\frac{1}{2}}$, $1 \le j \le r-1$, and $d = 2r$; actually one may do somewhat better. The result of Theorem 4 when combined with Theorem 3 gives, for all $\alpha \le \frac{1}{2}$,

$$f(\alpha) \le 1 - 2\alpha(1 - 2^{-[\alpha^{-1}]}). \tag{1.3}$$

It is worth noting that for $\frac{1}{2} < \alpha < 1$ we do not obtain any better bound for $f(\alpha)$ than the bound for $f^*(\alpha)$ given in Theorems 1 and 2.

Now we consider upper bounds for the function $\psi(x, x^{\alpha}, x^{\beta})$. The argument in Friedlander [4] can easily be modified to obtain the following result, which may be compared to Conjecture 1. (We omit the proof.)

*Theorem 5. There exists* $c(\alpha) > 0$ *such that*

$$\psi(x, x^{\alpha}, x^{\beta}) \ll \rho(\beta\alpha^{-1} - 1) x^{\beta} , \tag{1.4}$$

*holds for all* $x > c(\alpha)$ *where the implied constant is absolute.*

Theorem 5 is non-trivial only when $\alpha$ is small compared to $\beta$. A simple argument of Erdös and Turk [17, p. 5] implies the bound

$$\psi(x, x^{\alpha}, x^{\beta}) \ll \pi(x^{\alpha}) + \alpha^{-1} x^{\beta} , \tag{1.5}$$

which is non-trivial when $\alpha \le \beta$ but not so strong as (1.4) for small $\alpha$. Recently, upper bounds have also been obtained by Hĭldebrand and Tenenbaum [16].

The question of when $\psi(x, x^{\alpha}, x^{\beta}) > 0$ receives a rather satisfactory answer if we are allowed to exclude an exceptional set of ‘‘bad’’ $x$. By a simple modification of an argument of Motohashi [10] we obtain the following result.

*Theorem 6. For any fixed* $\alpha, \beta > 0$ *the exceptional set* $E(x) = \{y : y \le x$ *and* $\psi(y, y^{\alpha}, y^{\beta}) = 0\}$ *has measure* $o(x)$ *as* $x \to \infty$.

Theorem 6 is proved by following the argument of Motohashi [10], making the choice

$$P(s) = \sum{}' \, m^{-s}$$

where the summation is over all $m$ with $x^{1-\alpha} \le m < 2x^{1-\alpha}$ for which $P_1(m) \le x^{\alpha}$, and then using Theorem 0 to estimate $P(s)$. We omit further details.

Some of our arguments can be carried over to the analogous problem where "short interval" is replaced by "short arithmetic progression."

We remark that the proofs of the bounds for $f(\alpha)$ given in section 3 can be read independently of the proofs of the bounds for $f^*(\alpha)$ proved in section 2.

## 2. Positive Proportion of Integers with No Large Prime Factor

We shall derive Theorem 1 as a consequence of the following stronger result.

*Theorem 2.1 Let* $\varepsilon > 0$ *be given. Then there exist absolute positive constants* $c_0, c_1$ *such that for any* $\varepsilon_1$ *with* $0 < \varepsilon_1 \le \frac{1}{3}\varepsilon$ *the bound*

$$\psi(x,y,z) > \varepsilon_1 z$$

*holds uniformly for all y and z such that*

(1) $\quad y = x^{\alpha}$ *with* $\frac{1}{2} + \varepsilon \le \alpha \le 1$

(2) $\quad yz \ge x^{1 - c_0 (1 - \frac{\log y}{\log x})^3 + 2\varepsilon_1} \exp(c_1 (\log\log x)^2)$

*provided* $x > x_0(\varepsilon_1)$ *is sufficiently large.*

Theorem 1 follows immediately from Theorem 2.1 by choosing $\varepsilon = 1/4$ and letting $\varepsilon_1 \to 0$.

*Proof of Theorem 2.1.* Define $\alpha = \frac{\log y}{\log x}$, so that $y = x^{\alpha}$. We suppose throughout the proof that $\alpha \ge \frac{1}{2} + \varepsilon$. We start from Chebyshev's identity

$$\sum_{x-z\,<\,n\leq x} \log\, n \;=\; \sum_{d\leq x} \Lambda(d) \sum_{\substack{x-z<n\leq x \\ n\equiv 0(mod\ d)}} 1\ , \tag{2.1}$$

which implies that

$$(z+1)\log x \;\geq\; \sum_{p\leq x} \log p \;\left[ \left[ \frac{x}{p} \right] \;-\; \left[ \frac{x-z}{p} \right] \right] . \tag{2.2}$$

Now for $w \leq y \leq x$ we have

$$(z+1)\log x \;\geq\; \left[ \sum_{p\leq w} \;+\; \sum_{p>y} \right] \log p \;\left[ \left[ \frac{x}{p} \right] \;-\; \left[ \frac{x-z}{p} \right] \right] \tag{2.3}$$

so that

$$(z+1)\log x \;\geq\; \left[ z(\log w + O(1)) \;-\; \sum_{p\leq w} \log p \;\left[ \left\{ \frac{x}{p} \right\} \;-\; \left\{ \frac{x-z}{p} \right\} \right] \right] \tag{2.4}$$

$$+\; \sum_{p>y} \log p \;\left[ \left[ \frac{x}{p} \right] \;-\; \left[ \frac{x-z}{p} \right] \right] .$$

Now if we suppose

$$\psi(x,y,z) \;\leq\; \varepsilon_1 z \tag{2.5}$$

the right side of (2.4) becomes large. For since more than $(1-\varepsilon_1)z$ integers in $(x-z,x]$ are divisible by some $p>y$, we have

$$\sum_{p>y} \log p \;\left[ \left[ \frac{x}{p} \right] \;-\; \left[ \frac{x-z}{p} \right] \right] \;\geq\; (1-\varepsilon_1)z\ \log y\ . \tag{2.6}$$

We will show this contradicts (2.4) when we choose $w = x^{1-\alpha+2\varepsilon_1\alpha}$ and $z$ is large enough. (The condition $0 < \varepsilon_1 < \frac{1}{3}\varepsilon$ and $\alpha \geq \frac{1}{2} + \varepsilon$ implies that this choice of $w$ has $w \leq y$, so that (2.4) is valid.) Substituting $y = x^{\alpha}$, $w = x^{1-\alpha+2\varepsilon_1\alpha}$ and (2.6) into (2.4) we obtain

$$-\varepsilon_1 \alpha \; z \log x \geq O(z) - \sum_{p \leq x^{1-\alpha+2\varepsilon_1\alpha}} \log p \left[ \left\{ \frac{x}{p} \right\} - \left\{ \frac{x-z}{p} \right\} \right] . \tag{2.7}$$

This inequality cannot hold provided $z$ is chosen large enough that

$$\sum_{p \leq x^{1-\alpha+2\varepsilon_1\alpha}} \log p \left[ \left\{ \frac{x}{p} \right\} - \left\{ \frac{x-z}{p} \right\} \right] = O(z) . \tag{2.8}$$

We estimate the sum on the left side of (2.8) using the following result, which is essentially a consequence of a result of Jutila [7].

*Lemma 2.2. There are positive absolute constants $c_2, c_3$ such that for all $x$ and all $w$ with $1 \leq w \leq x$ the sum*

$$S(x,w) = \sum_{p \leq w} \left[ \left\{ \frac{x}{p} \right\} - \frac{1}{2} \right] \log p$$

*satisfies*

$$|S(x,w)| \leq c_3 \left[ w^{1-c_2 (\frac{\log w}{\log x})^2} + w^{\frac{3}{2}} x^{-\frac{1}{2}} \right] \exp(c_3 (\log\log w)^2) \; (\log x)^2 . \tag{2.9}$$

We defer the proof of this lemma.

To apply Lemma 2.2, we observe that the conditions $\alpha > \frac{1}{2} + \varepsilon$ and $0 < \varepsilon_1 < \frac{1}{3}\varepsilon$ imply that $w = x^{\beta}$ with $\beta = 1 - \alpha + 2\varepsilon_1 \alpha \le \frac{1}{2}$. In the range $1 \le w \le x^{\frac{1}{2}}$ the inequality (2.9) simplifies since

$$w^{\frac{3}{2}} x^{-\frac{1}{2}} \le w^{1 - (\frac{\log w}{\log x})^2} .$$

Now

$$\sum_{p \le w} \log p \left[ \left\{ \frac{x}{p} \right\} - \left\{ \frac{x-z}{p} \right\} \right] = S(x,w) - S(x-z,w)$$

so using Lemma 2.2 with $w = x^{\beta}$ implies

$$\left| \sum_{p \le x^{1-\alpha+2\varepsilon_1\alpha}} \log p \left[ \left\{ \frac{x}{p} \right\} - \left\{ \frac{x-z}{p} \right\} \right] \right| \le c_1 x^{\beta(1-c_0\beta^2)} \exp(c_1 (\log\log x)^2) \quad (2.10)$$

where $c_0 = \min(c_2, 1)$ and $c_1 = 2c_3$. Thus if we choose

$$z \ge x^{\beta(1-c_0\beta^2)} \exp(c_1 (\log\log x)^2) \quad (2.11)$$

then (2.10) implies (2.8) holds and so (2.7) is false for sufficiently large $x > x_0(\varepsilon_1)$. This contradiction shows that

$$\psi(x,y,z) > \varepsilon_1 z$$

must then hold.

To finish the proof, we show that

$$yz \ge x^{1 - c_0 (1 - \frac{\log y}{\log x})^3 + 2\varepsilon_1} \exp(c_1 (\log\log x)^2) \quad (2.12)$$

implies that (2.11) holds. Indeed (2.12) is equivalent to

$$z \geq x^{1-\alpha-c_0(1-\alpha)^3+2\varepsilon_1} \exp(c_1(\log\log x)^2) \tag{2.13}$$

and this implies that (2.11) follows from

$$\begin{aligned}\beta(1-c_0\beta^2) &= 1-\alpha+2\varepsilon_1\alpha - c_0(1-\alpha+2\varepsilon_1\alpha)^3 \\ &\leq 1-\alpha-c_0(1-\alpha)^3 + 2\varepsilon_1 .\end{aligned}$$

This proves Theorem 2.1, modulo proving Lemma 2.2. ■

*Proof of Lemma 2.2.*

The main step in this proof is supplied by a result of Jutila ([7], Theorem 2) which asserts that there are absolute constants $c_4, c_5 > 0$ such that for $2 \leq w \leq x$,

$$\left|\sum_{p\leq w} e\left[\frac{x}{p}\right]\right| \leq \left[w^{1-c_4(\frac{\log w}{\log x})^2} + w^{\frac{3}{2}} x^{-\frac{1}{2}}\right] \exp(c_5(\log\log w)^2) . \tag{2.14}$$

Now we earlier defined

$$S(x,w) = \sum_{p\leq w} e\left[\frac{x}{p}\right] \log p . \tag{2.15}$$

By partial summation we obtain from (2.14) that

$$|S(x,w)| \leq 2\left[w^{1-c_4(\frac{\log w}{\log x})^2} + w^{\frac{3}{2}} x^{-\frac{1}{2}}\right] \exp(c_5(\log\log w)^2)\ (\log x) . \tag{2.16}$$

We also have the trivial estimate

$$|S(x,w)| \leq \sum_{p\leq w} \log p \leq 2w , \tag{2.17}$$

the last inequality following from

$$\sum_{\frac{1}{2}w < p \le w} \log p \le \log \binom{w}{\frac{1}{2}w} \le w \ .$$

Now we combine sums of the form (2.15) into Fourier series approximating the function $\left\{\frac{x}{p}\right\} - \frac{1}{2}$. We use the following result ([5], Lemma 2), which embodies an idea of Vinogradov.

*Proposition 2.3. For any $\Delta$ with $0 < \Delta < \frac{1}{2}$ there exist complex Fourier coefficients $\{\alpha_m(\Delta) : -\infty < m < \infty,\ m \ne 0\}$ and $\{\beta_m(\Delta) : -\infty < m < \infty,\ m \ne 0\}$ depending on $\Delta$ such that*

$$-\Delta + \sum_{m \ne 0} \alpha_m(\Delta) e(mt) \le t - [t] - \frac{1}{2} \le \Delta + \sum_{m \ne 0} \beta_m(\Delta) e(mt) \qquad (2.18)$$

*for $-\infty < t < \infty$ with $t$ not an integer, and these coefficients satisfy the bounds*

$$|\alpha_m(\Delta)|,\ |\beta_m(\Delta)| \le \min\left\{\frac{2}{m}\ ,\ \frac{2}{\Delta m^2}\right\} . \qquad (2.19)$$

Applying Proposition 2.3, and (2.16), we obtain

$$\sum_{p \le w} \left[\left\{\frac{x}{p}\right\} - \frac{1}{2}\right] \log p \le \sum_{p \le w} \Delta \log p + \sum_{m \ne 0} \beta_m(\Delta) \sum_{p \le w} e\left[\frac{xm}{p}\right] \log p + (\log x)^2$$
$$\le 2\Delta w + \sum_{m \ne 0} \beta_m(\Delta)\ S(xm, w) + (\log x)^2 \ , \qquad (2.20)$$

where the $(\log x)^2$ term arises from the at most $\log x$ terms $p$ having $p | x$, where $\frac{x}{p} \in Z$.

Now we choose $\Delta = x^{-1/2}$ and obtain using (2.16) and (2.19) that

$$\Big| \sum_{\substack{m \neq 0 \\ |m| \leq x}} \beta_m(\Delta) S(xm,w) \Big| \leq c_6 \left( w^{1 - \frac{1}{4} c_4 \left(\frac{\log w}{\log x}\right)^2} + w^{\frac{3}{2}} x^{-\frac{1}{2}} \right) \exp(c_5 (\log\log w)^2)\ (\log x)^2 , \tag{2.21}$$

using

$$\sum_{|m| \leq x^{1/2}} \frac{1}{m} + \sum_{x^{1/2} < m \leq x} \frac{x^{1/2}}{m^2} \leq 2 \log x + O(1) .$$

We also have the estimate

$$\Big| \sum_{|m| > x} \beta_m(\Delta) S(xm,w) \Big| \leq 2 \left[ \sum_{m > x} \frac{x^{\frac{1}{2}}}{m^2} \right] 2w \leq 4 w x^{-1/2} , \tag{2.22}$$

obtained using (2.17), and (2.19). Combining (2.21) and (2.22) with (2.20) gives

$$\sum_{p \leq w} \left[ \left\{ \frac{x}{p} \right\} - \frac{1}{2} \right] \log p \leq 2 c_7 \left[ w^{1 - \frac{1}{4} c_4 \left(\frac{\log w}{\log x}\right)^2} + w^{\frac{3}{2}} x^{-\frac{1}{2}} \right] \exp(c_5 (\log\log w)^2)\ (\log x)^2 .$$

Starting from the other inequality in (2.18) leads similarly to

$$\sum_{p \leq w} \left[ \left\{ \frac{x}{p} \right\} - \frac{1}{2} \right] \log p \geq -2 c_7 \left[ w^{1 - \frac{1}{4} c_4 \left(\frac{\log w}{\log x}\right)^2} + w^{\frac{3}{2}} x^{-\frac{1}{2}} \right] \exp(c_5 (\log\log w)^2)\ (\log x)^2$$

which proves the lemma with $c_2 = \frac{1}{4} c_4$, $c_3 = \max(c_5, 2c_7)$. ■

We shall derive Theorem 2 from two other stronger results. First, we directly extend Theorem 2.1 to a larger range of $y$.

*Theorem 2.4. There exist positive absolute constants* $\eta$ *and* $c_3^*$ *with* $\eta < \frac{1}{4}$ *such that*

$$\psi(x,y,z) > c_3^* z$$

*holds uniformly for all y and z such that*

(1) $y = x^{\alpha}$ with $\frac{1}{2} - \eta \le \alpha \le 1-\eta$

(2) $yz \ge x^{1-\eta}$.

*for all sufficiently large x.*

*Proof of Theorem 2.4.*

It suffices to prove the result in the restricted range $y = x^{\alpha}$ with $\frac{1}{2} - \eta \le \alpha \le \frac{1}{2} + \eta$ since the result then follows for the larger range using Theorem 2.1 with $\varepsilon = \eta$, after possibly decreasing the constant $c_3^*$.

We start from the Chebyshev inequality (2.2), written as

$$z \log x \ge \left[ \sum_{p \le w} + \sum_{p > w} \right] \left[ \left[ \frac{x}{p} \right] - \left[ \frac{x-z}{p} \right] \right] \log p \tag{2.23}$$

We choose $w = x^{½ + \eta_0}$ for a small constant $\eta_0$ to be determined. Then using Lemma 2.2 we obtain for all $v \le x^{\frac{1}{2} + \eta_0}$ that

$$\sum_{p \le v} \left[ \left[ \frac{x}{p} \right] - \left[ \frac{x-z}{p} \right] \right] \log p = z \left[ \log v + c_8 + o(1) \right] \tag{2.24}$$

$$+ O\left[ x^{\gamma} \exp(c_4 (\log\log x)^2) \right]$$

where $\gamma = (\frac{1}{2}+\eta_0)\ (1-c_0(\frac{1}{2}+\eta_0)^2 + 2\varepsilon_1)$. We now choose $\eta_0 \le 1$ and $\varepsilon_1$ sufficiently small that $\gamma < \frac{1}{2} - \eta_0$, e.g. take $\eta_0 \le \frac{1}{20}c_0$ and $\varepsilon_1 \le \frac{1}{2}\eta_0$. Then (2.24) implies

$$\sum_{v_1 \le p \le v_2} \left[ \left[\frac{x}{p}\right] - \left[\frac{x-z}{p}\right] \right] \log p = z \left[ \log \frac{v_2}{v_1} + o(1) \right] + O(x^{\frac{1}{2}-\eta_o}) . \quad (2.25)$$

We will need the:

*FACT. For* $\frac{1}{2}-\eta_0 < \alpha \le \beta < \frac{1}{2}+\eta_0$ *and* $z > x^{\frac{1}{2}-\eta_0}$ *the number of integers in* $[x-z, x]$ *having a prime factor p with* $x^\alpha < p < x^\beta$ *is at most*

$$(1+\varepsilon)\ \log \left[\frac{\beta}{\alpha}\right] z .$$

*for* $x \ge x_0(\varepsilon)$.

To prove the fact, observe that this number is

$$N = \sum_{x^\alpha < p < x^\beta} \left[ \left[\frac{x}{p}\right] - \left[\frac{x-z}{p}\right] \right] \le \sum_{j=0}^{(\beta-\alpha)\log x} \frac{1}{\alpha \log x + j} \left[ \sum_{e^j x^\alpha < p \le e^{j+1} x^\alpha} \left[ \left[\frac{x}{p}\right] - \left[\frac{x-z}{p}\right] \right] \log p \right]$$

and using (2.25) we obtain

$$N \le \sum_{j=0}^{(\beta-\alpha)\log x} \left[\frac{1}{\alpha\log x + j}\right] \left[1 + o(1)\right]$$

$$\le (1 + o(1)) \log \left[\frac{\beta}{\alpha}\right]$$

as $x \to \infty$. This proves the fact.

Now choose $\eta = \frac{1}{4}\eta_0$ and suppose that

$$\psi(x,y,z) < \varepsilon_1 z$$

for some $y \ge x^{½-\eta}$. Then at least $(1-\varepsilon_1)z$ of the integers in $(x-z,x]$ have a prime factor $\ge y$, and using the Fact we conclude that at least $(1-2\varepsilon_1 - \log\left[\frac{\frac{1}{2}+\eta_0}{\frac{1}{2}-\eta}\right])z$ integers in $(x-z,x]$ have a prime factor $\ge w = x^{½+\eta_0}$. This implies that

$$\sum_{p \ge w} \left[\left[\frac{x}{p}\right] - \left[\frac{x-z}{p}\right]\right] \log p \ge \left[1 - 2\varepsilon_1 - \log\left[\frac{\frac{1}{2}+\eta_0}{\frac{1}{2}-\eta}\right]\right] (\frac{1}{2}+\eta_0) z \log x \quad (2.26)$$

Substituting (2.26) and (2.24) with $v = w = x^{\frac{1}{2}+\eta_0}$ into (2.23), we obtain

$$\Delta z \log x \ge c_9 (z + x^{\frac{1}{2}-\eta_0}) \ .$$

for some positive constant $c_9$, where

$$\Delta = -2\eta_0 + (\frac{1}{2}+\eta_0)\ (2\varepsilon_1 + \log\frac{\frac{1}{2}+\eta_0}{\frac{1}{2}-\eta})\ . \tag{2.27}$$

We obtain a contradiction if $\Delta < 0$ and $z \geq x^{\frac{1}{2}-\eta_0}$. Now since $\eta = 1/4\eta_0$ we have

$$(\frac{1}{2}+\eta_0)\log\left[\frac{\frac{1}{2}+\eta_0}{\frac{1}{2}-\frac{1}{4}\eta_0}\right] = (\frac{1}{2}+\eta_0)\log\left[1 + \frac{5/4\eta_0}{\frac{1}{2}-\frac{1}{4}\eta_0}\right] \leq \frac{5}{4}\eta_0 + O(\eta_0^2)\ .$$

which with (2.27) and $\varepsilon_1 = \frac{1}{4}\eta_0$ yields

$$\Delta \leq -\frac{1}{2}\eta_0 + O(\eta_0^2)\ .$$

Hence choosing $\eta_0$ sufficiently small, once and for all, we have $\Delta < 0$. We conclude that

$$z \geq x^{½-\eta_0} \tag{2.27}$$

implies that

$$\psi(x,y,z) > \eta\, z$$

whenever

$$x^{½-\eta} \leq y \leq x^{½+\eta}\ . \tag{2.28}$$

Finally the condition

$$yz > x^{1-2\eta}$$

together with (2.28) implies that (2.27) holds, since $\eta = \frac{1}{4}\eta_0$. Note $\eta = \frac{1}{4}\eta_0 \leq \frac{1}{4}$.

■

Second, using a Buchstab identity we extend Theorem 2.1 to cover $y = x^{\alpha}$ for all $\alpha > 0$. The basic iteration step is given by the following result.

*Theorem 2.5. Suppose that there are positive constants* $\alpha_0$, $\varepsilon_0$, $c_0$, $\delta$, *and* $x_0$ *such that* $\varepsilon_0 < \frac{1}{2}$ *and*

$$\psi(x,y,z) > c_0 z$$

*whenever*

(i) $y = x^{\beta}$ *with* $\beta \in [\alpha_0(1-\varepsilon_0), \alpha_0]$,

(ii) $yz \geq x^{1-\delta\alpha_0}$

*and* $x \geq x_0$ *is sufficiently large. Then for* $\alpha_1 = \frac{\alpha_0}{1+\alpha_0}$, $\varepsilon_1 = \frac{1}{20}\varepsilon_0$, $c_1 = \frac{1}{20}\varepsilon_0 c_0$ *there exists a bound* $x_1$ *depending on* $x_0$ *and* $\varepsilon_0$ *such that*

$$\psi(x,y,z) > c_1 z$$

*whenever*

(i$^*$) $y = x^{\beta}$ *with* $\beta \in [\alpha_1(1-\varepsilon_1), \alpha_1]$,

(ii$^{**}$) $yz \geq x^{1-\delta\alpha_1+\varepsilon_1}$

*and* $x \geq x_1$ *is sufficiently large.*

*Proof.* We use the Buchstab identity

$$\psi(x,y,z) = \sum_{p \leq y} \psi\left(\frac{x}{p}, p, \frac{z}{p}\right) \tag{2.29}$$

to infer that

$$\psi(x,y,z) \ge \sum_{y_1 \le p \le y} \psi\left(\frac{x}{p},\ p, \frac{z}{p}\right)\ . \tag{2.30}$$

We will apply this inequality with $y_1 = y^{1-\varepsilon_2}$, where $\varepsilon_2$ will be chosen suitably later. We suppose that (i$^*$), (ii$^{**}$) hold for the triple $(x,y,z)$. We claim that for $\varepsilon_2 = \frac{1}{20}\varepsilon_0$ that (i), (ii) hold for all triples $\left(\frac{x}{p},\ p, \frac{z}{p}\right)$ with $y^{1-\varepsilon_2} < p < y$.

Supposing this claim to be true, (2.29) gives for $x \ge x_0$ that

$$\psi(x,y,z) \ge \sum_{y^{1-\varepsilon_2} < p < y} c_0 \frac{z}{p} \tag{2.31}$$

Then using

$$\sum_{p \le y} \frac{1}{p} = \log\log y + \gamma_0 + o(1)$$

where $\gamma_0$ is Euler's constant, we obtain from (2.31) that

$$\psi(x,y,z) \ge c_0 \left[\log \frac{1}{1-\varepsilon_2} + o(1)\right] z \tag{2.32}$$

Since $\log \frac{1}{1-\varepsilon_2} > \varepsilon_2$ this implies that for sufficiently large $x \ge x_1(\varepsilon_0, x_0)$

$$\psi(x,y,z) > \varepsilon_2 c_0 z = c_1 z\ ,$$

the desired conclusion.

It remains to prove the claim. Set $y = x^\beta$, $p = x^\gamma$, and observe since $y^{1-\varepsilon_2} \le p \le y$ that

$$\beta(1-\varepsilon_2) \leq \gamma \leq \beta \tag{2.33}$$

and (i$^*$) gives

$$\alpha_1(1-\varepsilon_1)\,(1-\varepsilon_2) \leq \gamma \leq \alpha_1$$

Now define $(\tilde{x},\tilde{y},\tilde{z}) \equiv (\frac{x}{p},\, p, \frac{z}{p})$ and observe $\tilde{x} = x^{1-\gamma}$, $\tilde{y} = x^{\gamma} = \tilde{x}^{\frac{\gamma}{1-\gamma}}$, and (2.33) implies that

$$\frac{\alpha_1(1-\varepsilon_1)(1-\varepsilon_2)}{1-\alpha_1(1-\varepsilon_1)(1-\varepsilon_2)} \leq \frac{\gamma}{1-\gamma} \leq \frac{\alpha_1}{1-\alpha_1} = \alpha_0 \ . \tag{2.34}$$

We simplify this by observing that

$$\frac{1}{1-\alpha w} \geq \frac{w}{1-\alpha} \quad \text{when} \quad 0<\alpha\leq\frac{1}{2}\ ,\ 0\leq w\leq 1 \ . \tag{2.35}$$

(Check that $\frac{d}{dw}(\frac{1}{1-\alpha w} - \frac{w}{1-\alpha}) = \frac{\alpha}{(1-\alpha w)^2} - \frac{1}{1-\alpha} \leq \frac{1}{1-\alpha}(\frac{\alpha}{1-\alpha} - 1) \leq 0$ for $0\leq w\leq 1$ and that equality holds for $w=1$.) Then (2.34) and (2.35) together imply that

$$\frac{\gamma}{1-\gamma} \geq (1-\varepsilon_1)^2(1-\varepsilon_2)^2 \frac{\alpha_1}{1-\alpha_1} = (1-\varepsilon_1)^2(1-\varepsilon_2)^2\alpha_0 \ . \tag{2.36}$$

Hence (i) will hold for $(\tilde{x},\tilde{y},\tilde{z})$ provided that

$$(1-\varepsilon_1)^2(1-\varepsilon_2)^2 \geq 1-\varepsilon_0 \ . \tag{2.37}$$

Our choice of $\varepsilon_1 \leq \frac{1}{20}\varepsilon_0$, $\varepsilon_2 \leq \frac{1}{20}\varepsilon_0$ guarantees (2.37) is valid for $0\leq\varepsilon_0\leq\frac{1}{2}$, hence (i) holds. To verify (ii) holds, we calculate using (ii$^*$) that

$$\tilde{y}\tilde{z} = z \geq \frac{x^{1-\delta\alpha_1+\varepsilon_1}}{y}$$
$$= x^{1-\beta-\delta\alpha_1+\varepsilon_1}$$
$$= \tilde{x}^{\frac{1-\beta-\delta\alpha_1+\varepsilon_1}{1-\gamma}}$$
$$\geq \tilde{x}^{1-\delta\alpha_0 + \frac{\gamma-\beta+\varepsilon_1}{1-\gamma}}$$
$$\geq \tilde{x}^{1-\delta\alpha_0}$$

using the facts that

$$\frac{\alpha_1}{1-\gamma} \leq \frac{\alpha_1}{1-\alpha_1} = \alpha_0 ,$$

and that $\beta-\gamma \leq \varepsilon_2\beta \leq \varepsilon_2$. This shows (ii) holds for $(\tilde{x},\tilde{y},\tilde{z})$ and the claim is proved. ■

Now we combine the last two theorems to prove Theorem 2.

*Proof of Theorem 2*. Theorem 2.4 implies that if $c_1^* = \frac{\eta}{1-\eta} > 0$ then

$$f(\alpha) \leq 1 - (1+c_1^*)\alpha ; \qquad \frac{1}{2}-\eta \leq \alpha \leq 1-\eta .$$

Since $\eta < \frac{1}{4}$ this includes the region $\alpha \in [\frac{1}{2}, \frac{3}{4}]$. Now suppose we are given $\alpha$ and that $\frac{1}{k+1} \leq \alpha < \frac{1}{k}$ for some $k \geq 2$. The map $T(x) = \frac{x}{1-x}$ has the property that it maps $[\frac{1}{j+1}, \frac{1}{j})$ onto $[\frac{1}{j}, \frac{1}{j-1})$. Hence $T^{(k-2)}(\alpha) \in [\frac{1}{3}, \frac{1}{2})$ and $T^{(k-1)}(\alpha) \in [\frac{1}{2}, 1)$ and at least one of these iterates falls in the open interval $(\frac{1}{2}-\eta, 1-\eta)$. Suppose it is $\alpha_0 = T^{(k-2)}(\alpha)$. Now $U(x) = \frac{x}{1+x}$ has $U^{-1} = T$ so that $U^{(k-2)}(\alpha_0) = \alpha$. Now by Theorem 2.4 the hypothesis of Theorem 2.5 holds starting with the interval $[\alpha_0(1-\varepsilon_0), \alpha_0]$, $c_0 = c_3^*$, $\delta = c_1^*$, and some $x_0$. Apply Theorem 2.5 recursively $k-2$ times to conclude that

$$\psi(x,y,z) > c_1(\varepsilon_0) z$$

holds whenever

(i$^*$) $\quad y = x^\beta$ with $\beta \in [\alpha(1-\varepsilon^*), \alpha]$

(ii$^{**}$) $\quad yz \ge x^{1-c_1^*\alpha+\varepsilon^{**}}$

for sufficiently large $x$, where $\varepsilon^* = \left[\frac{1}{20}\right]^{k-2} \varepsilon_0$ and $\varepsilon^{**} = \frac{1}{19}\left[1-(\frac{1}{20})^{k-2}\right]\varepsilon_0$. A similar argument applies when $\alpha_0 = T^{(k-1)}(\alpha)$ lies in $(\frac{1}{2}-\eta,\ 1-\eta)$ and implies the same result. Taking $y = x^\alpha$, $z = x^{1-(1+c_1^*)\alpha+\varepsilon^{**}}$ we conclude $f^*(\alpha) \le 1-(1+c_1^*)\alpha+\varepsilon^{**}$. Letting $\varepsilon_0 \to 0$ implies that $f^*(\alpha) \le 1 - (1+c_1^*)\alpha$. ■

## 3. Existence of Integers with No Large Prime Factor

Theorems 1 and 2 imply that $f(\alpha) \le 1-\alpha$. This can be proved directly by noting that by Theorem 0 there is, for large $x$, an integer $m$ in the interval $(\frac{1}{2}x^{1-\alpha},\ x^{1-\alpha}]$ with $P_1(m) < x^\alpha$. The integer $n = m[\frac{x}{m}]$ is in the interval $(x-x^{1-\alpha}, x]$ and has $P_1(n) < 2x^\alpha$.

*Proof of Theorem 3.* Let $\varepsilon > 0$ be given. Pick an integer $n$ with $x^{1-\lambda} < n < 2x^{1-\lambda}$ with $P_1(n) \le x^\varepsilon$, which is possible by Theorem 0. Now $\frac{1}{2}x^\lambda \le \frac{x}{n} \le x^\lambda$ so one can find $y$ with $P_1(y) < (\frac{x}{n})^\alpha \le x^{\lambda\alpha}$ such that

$$|y - \frac{x}{n}| \le (\frac{x}{n})^{f(\alpha) + \varepsilon} \le x^{\lambda f(\alpha) + \lambda\varepsilon} .$$

Hence

$$|ny - x| \le nx^{\lambda f(\alpha) + \lambda\varepsilon} \le 2x^{\lambda f(\alpha) + 1 - \lambda + \lambda\varepsilon} ,$$

while $P_1(ny) \le MAX(x^{\varepsilon}, x^{\lambda\alpha}) \le x^{\lambda\alpha}$ if $\varepsilon \le \lambda\alpha$. So $f(\lambda\alpha) \le \lambda f(\alpha) + 1 - \lambda + \lambda\varepsilon$. Letting $\varepsilon \to 0$ gives the result. ■

*Proof of Theorem 4.* Let $x^r$ be the smallest r-th power which is ≥ $N$ and consider

$$s(\mathbf{a}) = (x - a_1)(x - a_2) \cdots (x - a_{r-1})(x + \sum_{j=1}^{r-1} a_j)$$

where $\mathbf{a} = (a_1, \ldots, a_{n-1})$ and for each $j$, we allow $a_j$ to run through the values $|a_j| \le A_j(x)$ with $A_j(x) = c_j x^{\frac{1}{2^j}}$ for suitable positive $c_j$ which will be chosen to depend only on $r$. Throughout this proof all implied constants are permitted to depend on $r$ and $N$ is required to satisfy a finite number of constraints of the form $N > N_j(r)$.

The proof is based on the easily verified fact that if for some $j$, $a_j$ is replaced by $1 + a_j$ while all other $a_k$ are kept fixed then the value of $s(\mathbf{a})$ is replaced by

$$s(\mathbf{a}) - \prod_{k \ne j} (x - a_k) \left\{ 2a_j + \sum_{k \ne j} a_k + 1 \right\} . \tag{3.1}$$

We begin with the zero vector $\mathbf{a} = (a_1, \ldots, a_{r-1}) = \mathbf{0}$, keeping $a_2 = a_3 = \ldots = a_{r-1} = 0$, and increasing $a_1$. By (3.1), as $a_1 \to a_1 + 1$ , $s(\mathbf{a})$ is decreased by the amount

$$2a_1 x^{r-2} + O(x^{r-2}) .$$

Hence for $\mathbf{a}^{(1)} = (a_{11}, 0, \ldots, 0)$ we have

$$S(\mathbf{0}) - S(\mathbf{a}_1) = 2\begin{bmatrix} a_{11} \\ 2 \end{bmatrix} x^{r-2} + O\left[a_{11}x^{r-2}\right] .$$

Since

$$S(\mathbf{0}) = x^r \geq N > (x-1)^r = x^r - rx^{r-1} + O(x^{r-2})$$

it follows that we can find $\mathbf{a}^{(1)} = (a_{11}, 0, \ldots, 0)$ with $0 \leq a_{11} < A_1(x)$ with

$$0 \leq s(\mathbf{a}^{(1)}) - N \leq 2A_1 x^{r-2} + O(x^{r-2}) .$$

provided that $c_1 > 2r^{\frac{1}{2}}$ and $N > N_1(r)$.

We now find a vector of the form

$$\mathbf{a}^{(2)} = (a_{21}, a_{22}, 0, \ldots, 0)$$

where $a_{21} = a_{11} - m$ , $a_{22} = 2m$, for some integer $m$ with $0 \leq m \leq \frac{1}{2}A_2(x)$. By the choice of $A_1(x), A_2(x)$ we have $|a_{21}| \leq A_1(x)$ (if $N$ is large). If we replace $m$ by $m+1$ we have $(a_1, a_2) \to (a_1 - 1, a_2 + 2)$ and from (3.1) a calculation shows the corresponding value of $s(\mathbf{a})$ decreases by an amount equal to

$$3a_2 x^{r-2} + O(x^{r-2}) .$$

provided $a_3 = a_4 = \ldots = a_{r-1} = 0$. If we assume that $c_2^2 > \frac{4}{3}c_1$ (and that $N$ is sufficiently large) steps of this size will eventually carry $s(\mathbf{a})$ below $N$ for some $m$ in the range $0 \leq m \leq \frac{1}{2}A_2(x)$ and so we can choose $\mathbf{a}^{(2)}$ as above with

$$0 \le s(\mathbf{a}^{(2)}) - N \le 3A_2(x)^{r-2} + O(x^{r-2}) \ .$$

To proceed to the general case we now assume that $j < r$ and that we have chosen $\mathbf{a}^{(j-1)}$ with $a_{j-1,k} = 0$ for $j \le k \le r-1$, and such that

$$0 \le s(\mathbf{a}^{(j-1)}) - N \le jA_{j-1}(x)x^{r-2} + O(x^{r-2}) \ .$$

We now choose $\mathbf{a}^{(j)}$ with $a_{jk} = 0$ for $j+1 \le k \le r-1$, with $a_{jk} = a_{j-1,k} - m$, for $1 \le k \le j-1$, and with $a_{jj} = jm$, for some integer $m$ with $0 \le m \le \frac{1}{j}A_j(x)$. We have, for sufficiently large $N$,

$$|a_{jk}| \le A_k(x) \quad \text{for } 1 \le k \le j-1 \ .$$

It follows from (3.1) that as we replace $m$ by $m+1$, that is, as $(a_1, \ldots, a_j) \to (a_1 - 1, \ldots, a_{j-1} - 1, a_j + j)$, the corresponding decrease in $s(\mathbf{a})$ is

$$(j+1)a_j x^{r-2} + O(x^{r-2}) \ .$$

Provided that we assume that $N$ is sufficiently large and that

$$c_j^2 > \frac{2j}{j+1} c_{j-1} \ ,$$

then steps of this size will carry $s(\mathbf{a})$ below $N$ and so we can choose $\mathbf{a}^{(j)}$ as above with

$$0 \le s(\mathbf{a}^{(j)}) - N \le (j+1) A_j(x)x^{r-2} + O(x^{r-2}) \ .$$

Continuing until the end of the case $j = r-1$, we complete the proof of Theorem 4. ■

*Remark.* Note that by constrast to the set $S_2$ of Theorem 4 the set

$$S_2^* = \{k_1 k_2 : |k_2 - k_1| \le \frac{1}{2} k_1^{1/2} \}$$

has the property that there exist infinitely many integers $x$ for which

$$|x-k| \geq \frac{1}{2} x^{1/2} \tag{3.2}$$

for all $k \in S_2^*$. Indeed the elements of $S_2^*$ cluster near squares of half-integers. Using the identity

$$k_1 k_2 = \left(\frac{k_1+k_2}{2}\right)^2 - \left(\frac{k_1-k_2}{2}\right)^2$$

with $m = k_1 + k_2$ we have

$$\left|k_1 k_2 - \frac{m^2}{4}\right| \leq \frac{1}{16} k_1 \leq \frac{1}{16} m .$$

Since the jump between $\left(\frac{m}{2}\right)^2$ and $\left(\frac{m+1}{2}\right)^2$ is $\geq m$, (3.2) follows.

**References**


[1] N. G. de Bruijn, On the number of positive integers $\leq x$ and free of prime factors $> y$, Proc. Ned. Akad. van Wetens. A, 54 (1951) 50-60.

[2] J. D. Dixon, Asymptotically Fast Factorization of Integers, Math. Comp. *36* (1981), 255-260.

[3] P. Erdös and J. Selfridge, Some problems on the prime factors of consecutive integers II, Proc. Washington State University Conference on Number Theory (1971), 13-21.

[4] J. B. Friedlander, Integers without large prime factors II, Acta Arith. 39 (1981) 53-57.

[5] J. Friedlander and H. Iwaniec, Quadratic Polynomials and Quadratic Forms, Acta Mathematica *141*, (1978), 1-15.

[6] A. Hildebrand, On the number of positive integers $\leq x$ and free of prime factors $> y$, preprint.

[7] M. Jutila, On numbers with a large prime factor II, J. Indian Math. Soc. 38 (1974), 125-130.

[8] J. C. P. Miller, On Factorization, with a Suggested New Approach, Math. Comp. *29* (1975), 155-172.

[9] M. A. Morrison and J. Brillhart, A method of factoring and the factorization of $F_7$, Math. Comp. *29* (1975), 183-205.

[10] Y. Motohashi, A note on almost primes in short intervals, Proc. Japan Acad., Ser. A, 55 (1979) 225-226.

[11] J. M. Pollard, Theorems on Factorization and Primality Testing, Proc. Camb. Phil. Soc. 76 (1974), 526-528.

[12] C. Pomerance, Analysis and Comparison of some Integer Factoring Algorithms, in: *Computational Number Theory Part 1* (H. W. Lenstra, Jr. and R. Tijdeman Eds.), Math. Centre Tract No. 154, Math. Centrum, Amsterdam 1982, 89-140.

[13] R. Rivest, A. Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Commun. A.C.M. 21 (1978), 120-128.

[14] C. P. Schnorr, Refined analysis and improvements on some factoring algorithms, J. Algorithms *3* (1982) 101-127.

[15] C. P. Schnorr and H. W. Lenstra, Jr., A Monte Carlo factoring algorithm with linear storage, Math. Comp., *43* (1984) 289-311.

[16] G. Tenenbaum, Sur le comportement local de la fonction de Dickman-de Bruijn, preprint.

[17] J. W. M. Turk, Products of integers in short intervals, Report 8228/M, Erasmus University 1982, Rotterdam.

# ON THE DISTRIBUTION IN SHORT INTERVALS OF INTEGERS HAVING NO LARGE PRIME FACTOR

*J. B. Friedlander**

Bell Laboratories
Murray Hill, NJ 07974

*J. C. Lagarias*

Bell Laboratories
Murray Hill, NJ 07974

*ABSTRACT*

We consider the problem of estimating the number $\psi(x, x^{\alpha}, x^{\beta})$ of integers in the interval $(x - x^{\beta}, x]$ having no prime factor greater than $x^{\alpha}$. We study when one can guarantee $\psi(x, x^{\alpha}, x^{\beta}) > 0$ for large $x$ and when one can guarantee $\psi(x, x^{\alpha}, x^{\beta}) \geq c(\alpha, \beta)\ x^{\beta}$ for large $x$, for some positive constant $c(\alpha, \beta)$. In particular let $f(\alpha)$ be the infimum of the values of $\beta$ for which for all $\alpha_1 > \alpha$ we have $\psi(x, x^{\alpha_1}, x^{\beta}) > 0$ for sufficiently large $x$, and let $f^*(\alpha)$ be the infimum of values of $\beta$ for which for all $\alpha_1 > \alpha$ we have $\psi(x, x^{\alpha_1}, x^{\beta}) \geq c(\alpha_1, \beta)\ x^{\beta}$ for some $c(\alpha_1, \beta) > 0$ for sufficiently large $x$. We prove using an idea of Chebyshev that there exists a positive constant $c$ such that, for $0 \leq \alpha \leq 1$,

$$f^*(\alpha) \leq 1 - \alpha - c\alpha(1-\alpha)^3.$$

By combining an elementary extrapolation technique with an explicit construction valid for $\alpha^{-1} = 2, 3, 4$ .., we show that for $0 < \alpha \leq \frac{1}{2}$,

$$f(\alpha) \leq 1 - 2\alpha(1 - 2^{-[\alpha^{-1}]}).$$

---

* Institute for Advanced Study, Princeton, New Jersey Scarborough College, University of Toronto.