ARBITRARILY TIGHT BOUNDS ON THE DISTRIBUTION OF SMOOTH INTEGERS

DANIEL J. BERNSTEIN

ABSTRACT. This paper presents lower bounds and upper bounds on the distribution of smooth integers; builds an algebraic framework for the bounds; shows how the bounds can be computed at extremely high speed using FFT-based power-series exponentiation; explains how one can choose the parameters to achieve any desired level of accuracy; and discusses several generalizations.

1. Introduction

A positive integer is **y-smooth** if it has no prime divisors larger than y. Define $\Psi(H, y)$ as the number of y-smooth integers in $[1, H]$.

This paper presents lower bounds and upper bounds on Ψ. The bounds are parametrized, and can be made arbitrarily close to Ψ, as discussed in section 4. The proofs are easy; for example, a typical lower bound is

$$\begin{aligned}\Psi(H,17) &= \#\left\{(a,b,c,d,e,f,g) : 2^a3^b5^c7^d11^e13^f17^g \le H\right\}\\ &\ge \#\left\{(a,b,c,d,e,f,g) : 2^a\overline{3}^b\overline{5}^c\overline{7}^d\overline{11}^e\overline{13}^f\overline{17}^g \le H\right\}\end{aligned}$$

where $\overline{3} = 2^{1230/776} > 3$, $\overline{5} = 2^{1802/776} > 5$, $\overline{7} = 2^{2179/776} > 7$, $\overline{11} = 2^{2685/776} > 11$, $\overline{13} = 2^{2872/776} > 13$, and $\overline{17} = 2^{3172/776} > 17$. What makes these bounds interesting is that they can be computed at extremely high speed, even when y is large. See section 3.

As far as I know, the first publication of bounds of this type was by Coppersmith in [24]. Coppersmith showed how to compute an arbitrarily tight lower bound on a variant of Ψ in a reasonable amount of time. The main improvements in this paper are the fast algorithms in section 3 and the algebraic framework in section 2.

Several generalizations are discussed in section 5. For example, one can quickly compute accurate bounds on the distribution of y-smooth ideals in each ideal class in a number field.

Date: 20010410.

1991 *Mathematics Subject Classification.* Primary 11N25; Secondary 11Y16.

The author was supported by the National Science Foundation under grants DMS–9600083 and DMS–9970409, and by the Mathematical Sciences Research Institute.

Other work. There are many limited-precision approximations to Ψ. See [82], [72], [66], and [81] for detailed surveys of the results and the underlying techniques.

Dickman in [29] observed that $\lim_{y\to\infty} \Psi(y^u, y)/y^u = \rho(u)$ for $u > 0$. Here ρ is the unique continuous function satisfying $\rho(u) = 1$ for $0 < u \le 1$ and $u\rho(u) = \int_{u-1}^{u} \rho(t)\,dt$ for $u > 1$. One can rapidly compute ρ and some useful variants of ρ to high accuracy; see [95], [20], [71, section 9], [50], [49], [77], [21, section 3], [70], and [3, section 4]. For asymptotics as $u \to \infty$ see [15], [26], [17], [64], [88], and [96]. Hildebrand in [61] showed that the error $|\Psi(H, y)/H\rho(u) - 1|$, where $H = y^u$, is at most a constant (which has not been computed) times $(\log(u + 1))/\log y$ if $u \ge 1$, $H \ge 3$, and $\log y \ge (\log\log H)^{1.667}$. For prior results see [23], [16], [84], [22], [27], [31], [32], [51], [18], [59], and [57].

De Bruijn in [25] pointed out that $H\int_0^H \rho(u - (\log t)/\log y)\,d(\lfloor t\rfloor/t)$ is a better approximation to $\Psi(H, y)$. See [87] and [66] for further information. I am not aware of any attempts to compute this approximation.

Rankin in [85] observed that $\Psi(H, y) \le H^s/\prod_{p\le y}(1-p^{-s})$ for any $s > 0$. This upper bound is minimized when s satisfies $\sum_{p\le y}(\log p)/(p^s - 1) = \log H$. Hildebrand and Tenenbaum in [65] showed that the approximation

$$\frac{1}{s}\left(2\pi\sum_{p\le y}\frac{p^s(\log p)^2}{(p^s-1)^2}\right)^{-1/2} H^s \prod_{p\le y}\frac{1}{1-p^{-s}}$$

to $\Psi(H, y)$, with the same choice of s as in Rankin's bound, has error at most a constant (again not computed) times $1/u + (\log y)/y$. Hunter and Sorenson in [67] showed that one can compute these approximations in time roughly y. Sorenson subsequently suggested replacing each $\sum_{p\le y}$ with $\sum_{p\le y^c} + \sum_{y^c<p\le y}$ for some c between 0 and 1, then approximating $\sum_{y^c<p\le y}$ by an integral; this saves time at the expense of accuracy.

See [92] and [30] for more information on $\Psi(H, y)$ when y is extremely small: in particular, on the accuracy of approximations such as $\Psi(H, 5) \approx (\log H)^3/6(\log 2)(\log 3)(\log 5)$.

Notation. lg means $\log_2$.

$[\cdots]$ means 1 if $\cdots$ is true, 0 otherwise. For example, $[r \ge 0]$ means 1 if r is nonnegative, 0 otherwise.

$r \mapsto \cdots$ means the function that maps r to $\cdots$. Here r is a dummy variable used in $\cdots$. The domain of the function is usually $\mathbf{R}$ and is always clear from context. For example, $r \mapsto r^2$ is the function $f : \mathbf{R} \to \mathbf{R}$ such that $f(r) = r^2$, and $r \mapsto [r \in \mathbf{Z}]$ is the function $g : \mathbf{R} \to \mathbf{R}$ such that $g(r) = 1$ for $r \in \mathbf{Z}$ and $g(r) = 0$ for $r \notin \mathbf{Z}$.

Acknowledgments. Thanks to Pieter Moree and an anonymous referee for their comments.

2. One-variable discrete generalized power series

A **series over Q** is a function $f : \mathbf{R} \to \mathbf{Q}$ such that $\{r \le h : f(r) \ne 0\}$ is finite for every $h \in \mathbf{R}$. A **distribution over Q** is a function $e : \mathbf{R} \to \mathbf{Q}$ such that $\{r < v : e(r) \ne 0\}$ is empty for some $v \in \mathbf{R}$. Observe that any series over $\mathbf{Q}$ is a distribution over $\mathbf{Q}$.

The reader should think of a series f as a formal sum $\sum_{r\in\mathbf{R}} f(r)x^r$. The set of series includes (formal) fractional power series such as $1 + x^{1230/776} + x^{2460/776} + \cdots$, i.e., $r \mapsto [r \ge 0][r \in (1230/776)\mathbf{Z}]$. It also includes Dirichlet series such as $\zeta = \sum_{n\ge1} x^{\lg n} = 1 + x + x^{\lg 3} + x^2 + x^{\lg 5} + \cdots$.

Theorem 2.1. *Let e be a distribution over $\mathbf{Q}$. Let f be a series over $\mathbf{Q}$. Then $\{r \in \mathbf{R} : e(r)f(t-r) \ne 0\}$ is finite for every $t \in \mathbf{R}$; the function $c = (t \mapsto \sum_{r\in\mathbf{R}} e(r)f(t-r))$ is a distribution over $\mathbf{Q}$; and if e is a series over $\mathbf{Q}$ then c is a series over $\mathbf{Q}$.*

The distribution c here is the **product of e and f**, abbreviated ef.

Proof. There is some $v \in \mathbf{R}$ such that $\{r < v : e(r) \ne 0\}$ is empty; and $\{s \le t - v : f(s) \ne 0\}$ is finite, so $\{r \ge v : f(t-r) \ne 0\}$ is finite. Thus $\{r : e(r)f(t-r) \ne 0\}$ is finite.

There is some $w \in \mathbf{R}$ such that $\{s < w : f(s) \ne 0\}$ is empty. Now $e(r)f(t-r) = 0$ for all $t < v + w$ and all $r \in \mathbf{R}$: if $r < v$ then $e(r) = 0$; if $r \ge v$ then $t - r < w$ so $f(t-r) = 0$. Hence $\sum_{r\in\mathbf{R}} e(r)f(t-r) = 0$ for all $t < v + w$. Thus c is a distribution.

Finally, fix $h \in \mathbf{R}$. If e is a series then $\{r \le h - w : e(r) \ne 0\}$ is finite, and $\{s \le h - v : f(s) \ne 0\}$ is finite, so $\{t \le h : c(t) \ne 0\}$ is finite. (If $t \le h$ and $c(t) \ne 0$ then $e(r)f(s) \ne 0$ for some r, s with $r + s = t$. Then $e(r) \ne 0$ so $r \ge v$ so $s = t - r \le h - v$; similarly $r \le h - w$.) □

Theorem 2.2. *Let e be a distribution over $\mathbf{Q}$. Let f and g be series over $\mathbf{Q}$. Then $e(fg) = (ef)g$.*

Proof. $(e(fg))(t) = \sum_s e(s) \cdot (fg)(t-s) = \sum_s \sum_r e(s)f(r)g(t-s-r) = \sum_s \sum_u e(s)f(u-s)g(t-u) = \sum_u (ef)(u) \cdot g(t-u) = ((ef)g)(t)$. □

In particular, product is associative on series. Consequently the set of series is a commutative ring under the following operations: 0 is $r \mapsto 0$; 1 is $r \mapsto [r = 0]$; $-f$ is $r \mapsto -f(r)$; $f + g$ is $r \mapsto f(r) + g(r)$; and fg is the product defined above. The set of fractional power series is a subring, as is the set of Dirichlet series.

Define distr as the distribution $r \mapsto [r \ge 0]$. The **distribution of terms of f** is the product distr f, i.e., the function $h \mapsto \sum_{s\le h} f(s)$. This is consistent with the usual notion of the (logarithmic) distribution of terms of a Dirichlet series: for example, $\operatorname{distr}\zeta$ is the function $h \mapsto \lfloor 2^h \rfloor$, which counts positive integers n with $\lg n \le h$.

Theorem 2.3. *Let e_1, e_2 be distributions over* $\mathbf{Q}$. *Let f be a series over* $\mathbf{Q}$. *If $e_1 \ge e_2$ and $f \ge 0$ then $e_1 f \ge e_2 f$.*

Here $\ge$ is pointwise comparison of functions: $f \ge 0$ means that $f(r) \ge 0$ for all r, and $e_1 \ge e_2$ means that $e_1(r) \ge e_2(r)$ for all r.

Proof. $(e_1 f)(t) = \sum_r e_1(r) \cdot f(t-r) \ge \sum_r e_2(r) \cdot f(t-r) = (e_2 f)(t)$. □

Theorem 2.4. *Let $f_1, \dots, f_n, g_1, \dots, g_n$ be series over* $\mathbf{Q}$ *with $f_i \ge 0$, $g_i \ge 0$, and $\operatorname{distr} f_i \ge \operatorname{distr} g_i$ for all i. Then $\operatorname{distr} f_1 \dots f_n \ge \operatorname{distr} g_1 \dots g_n$.*

Proof. For $n = 0$: $\operatorname{distr} 1 \ge \operatorname{distr} 1$.

For $n \ge 1$: By induction $\operatorname{distr} f_1 \dots f_{n-1} \ge \operatorname{distr} g_1 \dots g_{n-1}$. Apply Theorem 2.3 twice:

$$\begin{aligned}\operatorname{distr} f_1 \dots f_{n-1} f_n &\ge \operatorname{distr} g_1 \dots g_{n-1} f_n = \operatorname{distr} f_n g_1 \dots g_{n-1} \\ &\ge \operatorname{distr} g_n g_1 \dots g_{n-1} = \operatorname{distr} g_1 \dots g_{n-1} g_n\end{aligned}$$

since $f_n \ge 0$ and $g_1 \dots g_{n-1} \ge 0$. □

Notes. The proofs here are standard, but I do not know a reference for the results. The larger ring of "one-variable generalized power series over $\mathbf{Q}$"—functions $f : \mathbf{R} \to \mathbf{Q}$ such that every nonempty subset of $\{r \in \mathbf{R} : f_r \ne 0\}$ has a least element—is widely known but is not equipped with a useful notion of distribution. This larger ring was introduced by Malcev; see [86] for more information.

3. Bounds on the distribution of smooth integers

Fix positive integers y and α. For each prime $p \le y$ select a real number $\overline{p} \ge p$, preferably as small as possible, with $\alpha \lg \overline{p} \in \mathbf{Z}$. Define f as the series $\sum_n [n \text{ is } y\text{-smooth}]\, x^{\lg n} = \prod_{p \le y} (1 + x^{\lg p} + x^{2 \lg p} + \cdots)$, and define g as the series $\prod_{p \le y} (1 + x^{\lg \overline{p}} + x^{2 \lg \overline{p}} + \cdots)$.

Observe that g is a fractional power series with far fewer terms than f. For example, if $y = 10^6$, $\alpha = 776$, and $\overline{p}$ is chosen reasonably, then g is the series

$$\begin{aligned}&x^{0/776} + x^{776/776} + x^{1230/776} + x^{1552/776} + x^{1802/776} + x^{2006/776} \\ &\quad + \cdots + 2286594704425498206172550218939 x^{100000/776} + \cdots,\end{aligned}$$

with fewer than 100000 terms having exponents below 100000/776, while f has more than 10^{33} terms in the same exponent range.

Now $\operatorname{distr}(1 + x^{\lg p} + x^{2\lg p} + \cdots) \ge \operatorname{distr}(1 + x^{\lg \overline{p}} + x^{2\lg \overline{p}} + \cdots)$, so $\operatorname{distr} f \ge \operatorname{distr} g$ by Theorem 2.4. In other words,

$$(h \mapsto \Psi(2^h, y)) \ge \operatorname{distr} \exp \sum_{p \le y} \left(x^{\lg \overline{p}} + \frac{1}{2} x^{2\lg \overline{p}} + \frac{1}{3} x^{3\lg \overline{p}} + \cdots \right)$$

where exp is the usual exponential function on fractional power series. This is my lower bound on Ψ. The analogous upper bound is

$$(h \mapsto \Psi(2^h, y)) \le \operatorname{distr} \exp \sum_{p \le y} \left(x^{\lg \underline{p}} + \frac{1}{2} x^{2\lg \underline{p}} + \frac{1}{3} x^{3\lg \underline{p}} + \cdots \right)$$

with $\underline{p} \le p$. See Figure 1 for an example of the lower bound.

If $g = \sum_{n \ge 0} g_n x^{n/\alpha}$ then $\Psi(2^{n/\alpha}, y) \ge (\operatorname{distr} g)(n/\alpha) = g_0 + \cdots + g_n$. By computing $g \bmod x^h$, i.e., computing the integers $g_0, g_1, \ldots, g_{h\alpha - 1}$, one obtains lower bounds on $\Psi(H, y)$ for every H in the geometric progression $2^0, 2^{1/\alpha}, \ldots, 2^{h-2/\alpha}, 2^{h-1/\alpha}$. See Figure 2.

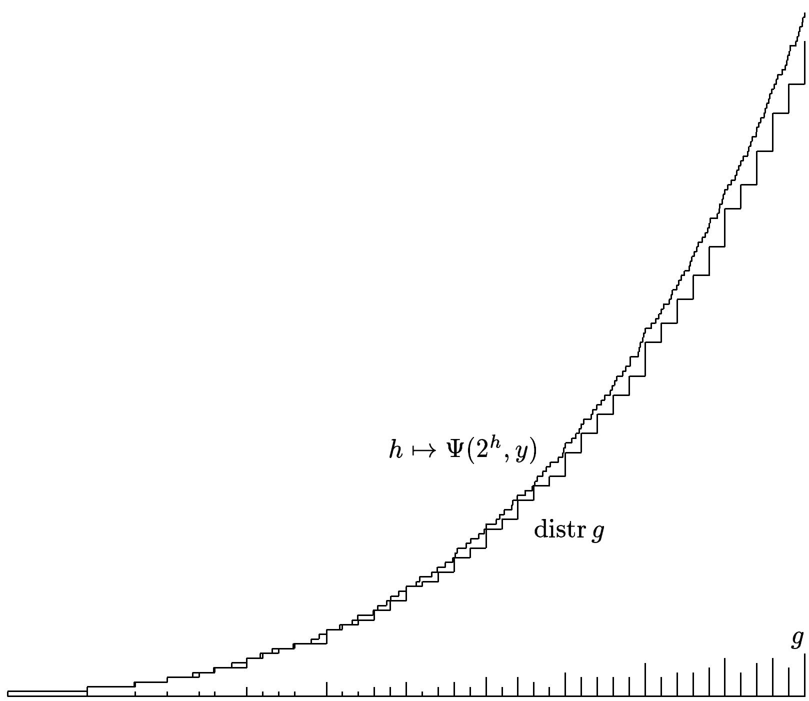

FIGURE 1. For $y = 7$ and $\alpha = 5$: Graphs of g, $\operatorname{distr} g$, and $h \mapsto \Psi(2^h, y)$, restricted to $[0, 10]$. Vertical range $[0, 143]$.

Enumerate primes $p \le y$

$$\Big\downarrow\, 2, 3, 5, \ldots$$

For each p, find multiple of $1/\alpha$ no smaller than $\lg p$

$$\Big\downarrow\, \lg \overline{2}, \lg \overline{3}, \lg \overline{5}, \ldots$$

Compute $\sum_{p \le y} \left(x^{\lg \overline{p}} + \frac{1}{2} x^{2 \lg \overline{p}} + \cdots\right) \bmod x^h$

$$\Big\downarrow\, \log g \bmod x^h$$

Exponentiate

$$\Big\downarrow\, g \bmod x^h = g_0 + g_1 x^{1/\alpha} + \cdots$$

Compute partial sums $g_0, g_0 + g_1, \ldots, g_0 + g_1 + \cdots + g_{h\alpha - 1}$

FIGURE 2. How to compute lower bounds on $\Psi(2^0, y)$, $\Psi(2^{1/\alpha}, y)$, …, $\Psi(2^{h-1/\alpha}, y)$.

A split-radix FFT uses $(12 + o(1))h\alpha \lg h\alpha$ additions and multiplications in $\mathbf{R}$ to multiply in $\mathbf{R}[x^{1/\alpha}]/x^h$; see [9]. Brent's exponentiation algorithm in [11] then uses $(88 + o(1))h\alpha \lg h\alpha$ additions and multiplications in $\mathbf{R}$ to compute $g \bmod x^h$ given $\log g \bmod x^h$. The constant 88 can be improved to 34; see [10]. One can enumerate primes $p \le y$ as described in [2]; the computation of $\log g \bmod x^h$ involves a few additions for each p.

It should be possible to carry out the operations in $\mathbf{R}$ in rather low precision if all the coefficients are scaled properly. However, I have not yet analyzed the roundoff error here. I instead compute $g \bmod (x^h, q)$ for several primes q by exponentiating $\log g \bmod (x^h, q)$. Logarithms do not make sense in $(\mathbf{Z}/q)[x^{1/\alpha}]$, but they do make sense in $(\mathbf{Z}/q)[x^{1/\alpha}]/x^h$ when q exceeds $h\alpha$.

Software that performs these computations for any $y \le 2^{30}$, with $h\alpha = 262144$ and $\alpha = 776$, is available from `http://cr.yp.to/psibound.html`. The software uses $4.5 \cdot 10^{10}$ Pentium-III cycles for $y = 10^8$ or $9.3 \cdot 10^{10}$ cycles for $y = 10^9$. It prints a sequence of lower bounds on $\Psi(H, y)$ for 262144 values of H up to $2^{262144/776}$. The choice of α is explained in the next section; the analogous upper-bound computation uses $\alpha = 771$.

The computation of $\log g$ can be improved. If y is large then there are many primes p for each value of $\lg \overline{p}$, and there are faster ways to count them than to enumerate them. Sorenson points out that the counts can be saved if one wants to handle several values of y.

4. Accuracy

Write $g = \prod_{p \le y}(1 + x^{\lg \overline{p}} + x^{2 \lg \overline{p}} + \cdots)$ as in the previous section, so that $\Psi(H, y) \ge (\operatorname{distr} g)(\lg H)$. How close is $\Psi(H, y)$ to $(\operatorname{distr} g)(\lg H)$? How close is it to the analogous upper bound?

One can answer this question by computing and comparing the bounds. The software described above finds that $\Psi(2^{300}, 2^{30})/2^{300} > 3.012 \cdot 10^{-11}$, for example, and $\Psi(2^{300}, 2^{30})/2^{300} < 3.047 \cdot 10^{-11}$; evidently both bounds are quite close. (In contrast, $\rho(10) \approx 2.770 \cdot 10^{-11}$.)

But this answer does not provide any guidance in choosing α before the computation is done. How can we select α to achieve a particular level of accuracy? Are some choices of α better than others?

This section considers another answer: if ϵ is chosen properly then $1 \le \Psi(H, y)/(\operatorname{distr} g)(\lg H) \le \Psi(H, y)/\Psi(H^{1/(1+\epsilon)}, y)$. The point is that one already has a good estimate for the ratio $\Psi(H, y)/\Psi(H^{1/(1+\epsilon)}, y)$, namely $1 + \epsilon \log H$. Here is a brief summary of the literature:

- Hildebrand in [60] proved that, for an extremely broad range of H and y, the ratio is at most about $1 + \epsilon(H/\Psi(H^{1/(1+\epsilon)}, y)) \log y$.
- Hildebrand in [62] proved that, when ϵ is not very small, the ratio is at most $H^{\epsilon/(1+\epsilon)}$, which is approximately $1 + \epsilon \log H$.
- Hensley in [58] proved that $\Psi(H, y)/\Psi(H/c, y)$ is around c for typical values of H and y if c is close to 2. Consequently the product of many ratios of the form $\Psi(H, y)/\Psi(H^{1/(1+\epsilon)}, y)$, for varying H, must be large. Quite a few of the ratios have to be at least about $H^{\epsilon/(1+\epsilon)}$.

For uniform lower bounds see [41], [4], [52], [75], [69], and [98]. See [66] and [40] for precise asymptotics when ϵ is not very small and $\log y$ is noticeably bigger than $(\log H)^{5/6}$.

How ϵ depends on α. Define ϵ as the maximum of $(\lg \overline{p})/\lg p - 1$ for primes $p \le y$. Then

$$\operatorname{distr}(1 + x^{(1+\epsilon)\lg p} + x^{2(1+\epsilon)\lg p} + \cdots) \le \operatorname{distr}(1 + x^{\lg \overline{p}} + x^{2 \lg \overline{p}} + \cdots)$$

so $\Psi(H^{1/(1+\epsilon)}, y) \le (\operatorname{distr} g)(\lg H)$. (Zagier comments that this inequality also allows g to serve as an upper bound on Ψ.)

Assume for simplicity that $\overline{p}$ is chosen as small as possible, so that $\alpha \lg \overline{p} = \lceil \alpha \lg p \rceil$. Note that $\overline{2} = 2$; this is the point of the requirement that α be an integer. Then $\epsilon \le 1/(\alpha \lg 3)$.

When α increases by a factor of 10, this upper bound on ϵ decreases by a factor of 10. The computation described in the previous section takes about 10 times as long and produces bounds for 10 times as many values of H.

Some values of α are particularly good. If $\alpha \lg 3$ is within $(\lg 3)/\lg 7$ of the next integer, and $\alpha \lg 5$ is within $(\lg 5)/\lg 7$ of the next integer, then $\epsilon \le 1/(\alpha \lg 7)$. If $\alpha = 776$ then $1/(\alpha \lg 3) \approx 0.000813$, while $\epsilon \approx 0.000226$. It is easy to see that $\epsilon\alpha \to 0$ for selected $\alpha \to \infty$.

Experiments show that $(\operatorname{distr} g)(\lg H)$ is usually closer to $\Psi(H, y)$ than to $\Psi(H^{1/(1+\epsilon)}, y)$. A more precise analysis would be interesting.

Exact computation of Ψ. If H is slightly below an integer, and ϵ is slightly below $1/H \log H$, then $\lfloor H^{1/(1+\epsilon)} \rfloor = \lfloor H \rfloor$, so $\Psi(H, y)$ is exactly $(\operatorname{distr} g)(\lg H)$.

Fast power-series exponentiation is not useful in this extreme case. Series such as g should be represented in sparse form: a multiset S of integers represents the series $\sum_{n \in S} x^{n/\alpha}$. Straightforward series multiplication then takes at most $2\Psi(H, y)$ additions of integers, each integer having about $\lg H$ bits, to produce the portion of g relevant to $\Psi(H, y)$. The result reveals the approximate logarithm of every smooth number $n \le H$ with enough accuracy to recover n or $n - 1$.

Occasionally one wants to know $\Psi(H, y)$ for only one H. Partition $\{p \le y\}$ into two sets P_1 and P_2; factor g as $g_1 g_2$ accordingly; compute g_1 and g_2; finally compute $(\operatorname{distr} g)(\lg H)$ as $\sum_r (\operatorname{distr} g_1)(r) \cdot g_2(\lg H - r)$. The total number of relevant terms of g_1 and g_2, hence the total time needed, can be quite a bit smaller than $\Psi(H, y)$.

Notes. The ideas in this paper evolved as follows.

I presented the exact Ψ algorithms in [7]. That paper was not phrased in the language of series; I used logarithms and α merely because additions are faster than multiplications.

I subsequently noticed that reducing α would produce bounds on Ψ at high speed. In 1997, I rephrased the algorithms in the language of series, and realized the relevance of fast power-series exponentiation. An extended abstract of this paper appeared in [8]. I found Coppersmith's article [24] in 2000 as I was preparing the bibliography for this paper.

5. Generalizations and variants

Omitting tiny primes. One can replace $\{p \le y\}$ by a subset, such as $\{p : z < p \le y\}$. For previous work see [37], [89], and [90].

Squarefree integers. One can restrict the powers of p that are allowed to appear: for example, one can replace $1 + x^{\lg p} + x^{2 \lg p} + \cdots$ by $1 + x^{\lg p}$ to bound the distribution of smooth squarefree integers. For previous work see [44] and [80].

Arithmetic progressions. Fix a positive integer m. Define $\Psi(H, y, i)$ as the number of y-smooth integers $n \in [1, H]$ with $n \equiv i \pmod{m}$.

Let S be the finite monoid $\mathbf{Z}/m$ under multiplication. The ring $\mathbf{Q}[S]$ is the set of functions $a : S \to \mathbf{Q}$ with the following operations: 0 is $s \mapsto 0$; 1 is $s \mapsto [s = 1]$; $-a$ is $s \mapsto -a(s)$; $a + b$ is $s \mapsto a(s) + b(s)$; and ab is $s \mapsto \sum_{t,u:tu=s} a(t)b(u)$. Define a partial order $a \geq b$ meaning that $a(s) \geq b(s)$ for all s. Everything in section 2 generalizes immediately to series over $\mathbf{Q}[S]$.

Define $\pi : \mathbf{Z} \to \mathbf{Q}[S]$ as $n \mapsto (s \mapsto [s = n \bmod m])$. Then π is a monoid morphism: $\pi(1) = 1$ and $\pi(nn') = \pi(n)\pi(n')$. The images $\pi(0), \pi(1), \ldots, \pi(m-1)$ are linearly independent over $\mathbf{Q}$.

Define f as the series $\sum_n [n \text{ is } y\text{-smooth}]\, \pi(n) x^{\lg n}$ over $\mathbf{Q}[S]$. Then $(\operatorname{distr} f)(\lg H) = \sum_{0 \leq i < m} \pi(i)\Psi(H, y, i)$. For example, if $m = 3$ and $y = 5$, then f is the series

$$\begin{aligned} &\pi(0)(x^{\lg 3} + x^{\lg 6} + x^{\lg 9} + x^{\lg 12} + x^{\lg 15} + x^{\lg 18} + \cdots) \\ &+ \pi(1)(x^{\lg 1} + x^{\lg 4} + x^{\lg 10} + x^{\lg 16} + x^{\lg 25} + x^{\lg 40} + \cdots) \\ &+ \pi(2)(x^{\lg 2} + x^{\lg 5} + x^{\lg 8} + x^{\lg 20} + x^{\lg 32} + x^{\lg 50} + \cdots), \end{aligned}$$

and $(\operatorname{distr} f)(\lg 12) = 4\pi(0) + 3\pi(1) + 3\pi(2)$.

Now f is the product over p of $1 + \pi(p)x^{\lg p} + \pi(p)^2 x^{2\lg p} + \cdots$, and $\operatorname{distr}(1 + \pi(p)x^{\lg p} + \pi(p)^2 x^{2\lg p} + \cdots) \geq \operatorname{distr}(1 + \pi(p)x^{\lg \overline{p}} + \pi(p)^2 x^{2\lg \overline{p}} + \cdots)$, so $\operatorname{distr} f \geq \operatorname{distr} \exp \sum_{p \leq y} (\pi(p)x^{\lg \overline{p}} + \frac{1}{2}\pi(p)^2 x^{2\lg \overline{p}} + \cdots)$. A fractional-power-series exponentiation over $\mathbf{Q}[S]$ thus produces a lower bound on $\operatorname{distr} f$, i.e., a lower bound on $\Psi(H, y, i)$ for each i and various H. One can save time by working in the smaller ring $\mathbf{Q}[(\mathbf{Z}/m)^*]$ and ignoring primes that divide m.

For previous work see [16], [36], [53], [54], [38], [39], [33], [5], [47], [48], [93], [97], and [34]. See [43] for more information on monoid rings and group rings.

Number fields. Let K be a number field, R its ring of integers. A nonzero ideal n of R is **y-smooth** if it has no prime divisors of norm larger than y. Define f as the series $\sum_n [n \text{ is } y\text{-smooth}]\, x^{\lg \operatorname{norm} n}$. Then f is the product of $1 + x^{\lg \operatorname{norm} p} + x^{2\lg \operatorname{norm} p} + \cdots$ over smooth prime ideals p. One obtains a lower bound on $\operatorname{distr} f$ by increasing each $\lg \operatorname{norm} p$ to a nearby multiple of $1/\alpha$. For previous work see [68] (in the case $K = \mathbf{Q}[\sqrt{-1}]$), [42], [35], [55], [72], [73], [79], and [12].

In some applications—notably integer factorization with the number field sieve, as described in [74]—one wants to know the distribution of smooth *elements* of R. A fractional-power-series exponentiation over $\mathbf{Q}[G]$, where G is the ideal class group of R, produces bounds on the distribution of smooth ideals in each ideal class; in particular, the distribution of smooth principal ideals. One can replace G by a ray class group or a ray class monoid to bound smoothness in arithmetic progressions. The use of these techniques to estimate the speed of the number field sieve will be discussed in a subsequent paper.

Function fields. Dirichlet series for function fields over $\mathbf{F}_q$ are already power series: $\lg \operatorname{norm} n \in (\lg q)\mathbf{Z}$ for every nonzero ideal n. For example, the sum of $[n \text{ is } 2^{20}\text{-smooth}]\, x^{\lg \operatorname{norm} n}$ for nonzero polynomials n over $\mathbf{F}_2$ is $1+2x+4x^2+\cdots+335653893002534131235548574x^{99}+\cdots$. The bounds in this paper boil down to a known algorithm to compute the exact coefficients of this series. For asymptotic estimates see [19], [76], [6], and [83].

Coprime pairs. Consider the series

$$\sum_{n_1,n_2} [n_1 \text{ is } y\text{-smooth}][n_2 \text{ is } y\text{-smooth}][\gcd\{n_1,n_2\}=1]\, x_1^{\lg n_1} x_2^{\lg n_2}$$

in two variables x_1, x_2. This series is the product over smooth primes p of $1+x_1^{\lg p}+x_1^{2\lg p}+\cdots+x_2^{\lg p}+x_2^{2\lg p}+\cdots$. With a two-variable power-series exponentiation one can bound the distribution of smooth coprime pairs (n_1, n_2).

This is, for $y = 89$, the problem considered by Coppersmith in [24]. Coppersmith replaced exponents $k \lg p$ by $\lceil \alpha k \lg p \rceil/\alpha$, and multiplied the resulting series; I replace $k \lg p$ by $k\lceil \alpha \lg p\rceil/\alpha$, which is not quite as small but is better suited for exponentiation.

For limited-precision estimates see [44], [45], and [46].

Number of prime factors. The series $\sum_n [n \text{ is } y\text{-smooth}]\, x^{\lg n} w^{\Omega(n)}$ in two variables x, w, where $\Omega(n) = \sum_p \operatorname{ord}_p n$, is the product over smooth primes p of $1 + x^{\lg p} w + x^{2\lg p} w^2 + \cdots$. The exponentiation here is faster than in the case of coprime pairs, because the exponents of w are very small. For previous work see [28], [56], and [63].

Semismoothness. The analysis and optimization of factoring algorithms often relies on the distribution of positive integers n that have no prime divisors larger than z and at most one prime divisor larger than y. This is not a local condition, but the sum of $x^{\lg n}$ is nevertheless a product

$$\left(1 + \sum_{y<p\le z} x^{\lg p}\right) \prod_{p \le y} (1 + x^{\lg p} + x^{2\lg p} + \cdots)$$

of sparse series with nonnegative coefficients, so one can efficiently bound the distribution of these n's. For previous work see [71] and [3].

References

[1] —, *Journées arithmétiques de Besançon*, Astérisque 147–148, Société Mathématique de France, Paris, 1987. MR 87m:11003.

[2] A. O. L. Atkin, Daniel J. Bernstein, *Prime sieves using binary quadratic forms*, submitted for publication; available from `http://cr.yp.to/papers/primesieves.dvi`.

[3] Eric Bach, René Peralta, *Asymptotic semismoothness probabilities*, Mathematics of Computation **65** (1996), 1701–1715. MR 98a:11123.

[4] Antal Balog, *On the distribution of integers having no large prime factor*, in [1] (1987), 27–31. MR 88g:11061.

[5] Antal Balog, Carl Pomerance, *The distribution of smooth numbers in arithmetic progressions*, Proceedings of the American Mathematical Society **115** (1992), 33–43. MR 92h:11075.

[6] Renet Lovorn Bender, Carl Pomerance, *Rigorous discrete logarithm computations in finite fields via smooth polynomials*, in [13] (1998), 221–232. MR 99c:11156.

[7] Daniel J. Bernstein, *Enumerating and counting smooth integers*, chapter 2, Ph.D. thesis (1995), University of California at Berkeley; available from `http://cr.yp.to/papers/epsi.dvi`.

[8] Daniel J. Bernstein, *Bounding smooth integers (extended abstract)*, in [14] (1998), 128–130; available from `http://cr.yp.to/papers/psi-abs.dvi`.

[9] Daniel J. Bernstein, *Multidigit multiplication for mathematicians*, to appear, Advances in Applied Mathematics; available from `http://cr.yp.to/papers/m3.dvi`.

[10] Daniel J. Bernstein, *Removing redundancy in high-precision Newton iteration*, draft.

[11] Richard P. Brent, *Multiple-precision zero-finding methods and the complexity of elementary function evaluation*, in [94], 151–176; available from `http://web.comlab.ox.ac.uk/oucl/work/richard.brent/pub/pub028.html`. MR 54 #11843.

[12] Johannes A. Buchmann, Christine S. Hollinger, *On smooth ideals in number fields*, Journal of Number Theory **59** (1996), 82–87. MR 97h:11140.

[13] Duncan A. Buell, Jeremy T. Teitelbaum, *Computational perspectives on number theory*, American Mathematical Society, Providence, Rhode Island, 1998. ISBN 0–8218–0880–X. MR 98g:11001.

[14] Joe P. Buhler (editor), *Algorithmic number theory: ANTS-III*, Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998. ISBN 3–540–64657–4. MR 2000g:11002.

[15] Aleksandr A. Buchstab, *Asymptotic estimates of a general number theoretic function*, Matematicheskiĭ Sbornik **44** (1937), 1239–1246.

[16] Aleksandr A. Buchstab, *On those numbers in an arithmetic progression all prime factors of which are small in order of magnitude*, Doklady Akademii Nauk SSSR **67** (1949), 5–8. MR 11,84b.

[17] E. Rodney Canfield, *The asymptotic behavior of the Dickman-de Bruijn function*, Congressus Numerantium **35** (1982), 139–148. MR 85g:11082.

[18] E. Rodney Canfield, Paul Erdős, Carl Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum"*, Journal of Number Theory **17** (1983), 1–28. MR 85j:11012.

[19] Mireille Car, *Théorèmes de densité dans* $\mathbf{F}_q[x]$, Acta Arithmetica **48** (1987), 145–165. MR 88g:11090.

[20] Jean-Marie-François Chamayou, *A probabilistic approach to a differential-difference equation arising in analytic number theory*, Mathematics of Computation **27** (1973), 197–203. MR 49 #1725.

[21] Angela Y. Cheer, Daniel A. Goldston, *A differential delay equation arising from the sieve of Eratosthenes*, Mathematics of Computation **55** (1990), 129–141. MR 90j:11091.

[22] Sarvadaman D. Chowla, William E. Briggs, *On the number of positive integers $\le x$ all of whose prime factors are $\le y$*, Proceedings of the American Mathematical Society **6** (1955), 558–562. MR 17,127l.

[23] Sarvadaman D. Chowla, T. Vijayaraghavan, *On the largest prime divisors of numbers*, Journal of the Indian Mathematical Society **11** (1947), 31–37. MR 9,332d.

[24] Don Coppersmith, *Fermat's last theorem (case 1) and the Wieferich criterion*, Mathematics of Computation **54** (1990), 895–902. MR 90h:11024.

[25] Nicolaas G. de Bruijn, *On the number of positive integers $\le x$ and free of prime factors $> y$*, Indagationes Mathematicae **13** (1951), 50–60. MR 13,724e.

[26] Nicolaas G. de Bruijn, *The asymptotic behaviour of a function occurring in the theory of primes*, Journal of the Indian Mathematical Society **15** (1951), 25–32. MR 13,326f.

[27] Nicolaas G. de Bruijn, *On the number of positive integers $\le x$ and free of prime factors $> y$. II*, Indagationes Mathematicae **28** (1966), 239–247. MR 34 #5770.

[28] Jean-Marie De Koninck, Douglas Hensley, *Sums taken over $n \le x$ with prime factors $\le y$ of $z^{\Omega(n)}$, and their derivatives with respect to z*, Journal of the Indian Mathematical Society **42** (1979), 353–365. MR 81k:10065.

[29] K. Dickman, *On the frequency of numbers containing primes of a certain relative magnitude*, Ark. Mat. Astr. Fys. **22** (1930), 1–14.

[30] Veikko Ennola, *On numbers with small prime divisors*, Annales Academiae Scientiarum Fennicae Series A I **440** (1969). MR 39 #5492.

[31] Paul Erdős, Jack H. van Lint, *On the number of positive integers $\le x$ and free of prime factors $> y$*, Simon Stevin **40** (1966/1967), 73–76. MR 35 #2836.

[32] A. S. Faĭnleĭb, *The estimate from below of the quantity of numbers with small prime divisors*, Doklady Akademii Nauk UzSSR (1967), 3–5. MR 46 #5265.

[33] Étienne Fouvry, Gérald Tenenbaum, *Entiers sans grand facteur premier en progressions arithmetiques*, Proceedings of the London Mathematical Society **63** (1991), 449–494. MR 93c:11074.

[34] Étienne Fouvry, Gérald Tenenbaum, *Répartition statistique des entiers sans grand facteur premier dans les progressions arithmétiques*, Proceedings of the London Mathematical Society **72** (1996), 481–514. MR 97h:11098.

[35] John B. Friedlander, *On the number of ideals free from large prime divisors*, Journal für die Reine und Angewandte Mathematik **255** (1972), 1–7. MR 45 #8627.

[36] John B. Friedlander, *Integers without large prime factors*, Indagationes Mathematicae **35** (1973), 443–451. MR 49 #4957.

[37] John B. Friedlander, *Integers free from large and small primes*, Proceedings of the London Mathematical Society **33** (1976), 565–576. MR 54 #5139.

[38] John B. Friedlander, *Integers without large prime factors. II*, Acta Arithmetica **39** (1981), 53–57. MR 83b:10052.

[39] John B. Friedlander, *Integers without large prime factors. III*, Archiv der Mathematik **43** (1984), 32–36. MR 86d:11072.

[40] John B. Friedlander, Andrew Granville, *Smoothing "smooth" numbers*, Philosophical Transactions of the Royal Society of London Series A **345** (1993), 339–347; available from `http://www.math.uga.edu/~andrew/agpapers.html`. MR 95b:11086.

[41] John B. Friedlander, Jeffrey C. Lagarias, *On the distribution in short intervals of integers having no large prime factor*, Journal of Number Theory **25** (1987), 249–273. MR 88d:11084.

[42] John R. Gillett, *On the largest prime divisors of ideals in fields of degree n*, Duke Mathematical Journal **37** (1970), 589–600. MR 42 #3052.

[43] Robert Gilmer, *Commutative semigroup rings*, University of Chicago, Chicago, Illinois, 1984. ISBN 0–226–29391–2. MR 85e:20058.

[44] Andrew Granville, *On positive integers $\leq x$ with prime factors $\leq t \log x$*, in [78] (1989), 403–422; available from `http://www.math.uga.edu/~andrew/agpapers.html`. MR 92h:11076.

[45] Andrew Granville, *The lattice points of an n-dimensional tetrahedron*, Aequationes Mathematicae **41** (1991), 234–241; available from `http://www.math.uga.edu/~andrew/agpapers.html`. MR 92b:11070.

[46] Andrew Granville, *On pairs of coprime integers with no large prime factors*, Expositiones Mathematicae **9** (1991), 335–350. MR 92m:11095.

[47] Andrew Granville, *Integers, without large prime factors, in arithmetic progressions. I*, Acta Mathematica **170** (1993), 255–273; available from `http://www.math.uga.edu/~andrew/agpapers.html`. MR 94f:11091.

[48] Andrew Granville, *Integers, without large prime factors, in arithmetic progressions. II*, Philosophical Transactions of the Royal Society of London Series A **345** (1993), 349–362; available from `http://www.math.uga.edu/~andrew/agpapers.html`. MR 94k:11104.

[49] Frieder Grupp, *On difference-differential equations in the theory of sieves*, Journal of Number Theory **24** (1986), 154–173. MR 87k:11101.

[50] Frieder Grupp, Hans-Egon Richert, *The functions of the linear sieve*, Journal of Number Theory **22** (1986), 208–239. MR 87f:11071.

[51] Heini Halberstam, *On integers all of whose prime factors are small*, Proceedings of the London Mathematical Society **21** (1970), 102–107. MR 42 #4509.

[52] Glyn Harman, *Short intervals containing numbers without large prime factors*, Mathematical Proceedings of the Cambridge Philosophical Society **109** (1991), 1–5. MR 91h:11093.

[53] D. G. Hazlewood, *On integers all of whose prime factors are small*, Bulletin of the London Mathematical Society **5** (1973), 159–163. MR 49 #2615.

[54] D. G. Hazlewood, *On k-free integers with small prime factors*, Proceedings of the American Mathematical Society **52** (1975), 40–44. MR 51 #10256.

[55] D. G. Hazlewood, *On ideals having only small prime factors*, Rocky Mountain Journal of Mathematics **7** (1977), 753–768. MR 56 #2941.

[56] Douglas Hensley, *The sum of $\alpha^{\Omega(n)}$ over integers $n \leq x$ with all prime factors between α and y*, Journal of Number Theory **18** (1984), 206–212. MR 85i:11071.

[57] Douglas Hensley, *The number of positive integers $\leq x$ and free of prime factors $> y$*, Journal of Number Theory **21** (1985), 286–298. MR 87e:11110.

[58] Douglas Hensley, *A property of the counting function of integers with no large prime factors*, Journal of Number Theory **22** (1986), 46–74. MR 87f:11065.

[59] Adolf Hildebrand, *Integers free of large prime factors and the Riemann hypothesis*, Mathematika **31** (1984), 258–271. MR 87a:11086.

[60] Adolf Hildebrand, *Integers free of large prime divisors in short intervals*, Quarterly Journal of Mathematics **36** (1985), 57–69. MR 86f:11066.

[61] Adolf Hildebrand, *On the number of positive integers $\leq x$ and free of prime factors $> y$*, Journal of Number Theory **22** (1986), 289–307. MR 87d:11066.

[62] Adolf Hildebrand, *On the local behavior of $\Psi(x, y)$*, Transactions of the American Mathematical Society **297** (1986), 729–751. MR 87k:11099.

[63] Adolf Hildebrand, *On the number of prime factors of integers without large prime divisors*, Journal of Number Theory **25** (1987), 81–106. MR 88d:11085.

[64] Adolf Hildebrand, *The asymptotic behavior of the solutions of a class of differential-difference equations*, Journal of the London Mathematical Society **42** (1990), 11–31. MR 92f:11123.

[65] Adolf Hildebrand, Gérald Tenenbaum, *On integers free of large prime factors*, Transactions of the American Mathematical Society **296** (1986), 265–290. MR 87f:11066.

[66] Adolf Hildebrand, Gérald Tenenbaum, *Integers without large prime factors*, Journal de Théorie des Nombres de Bordeaux **5** (1993), 411–484. MR 95d:11116.

[67] Simon Hunter, Jonathan Sorenson, *Approximating the number of integers free of large prime factors*, Mathematics of Computation **66** (1997), 1729–1741. MR 98c:11093.

[68] James H. Jordan, *The divisibility of Gaussian integers by large Gaussian primes*, Duke Mathematical Journal **32** (1965), 503–509. MR 32 #2392.

[69] Jerzy Kaczorowski, Alberto Perelli, *On the distribution in short intervals of products of a prime and integers from a given set*, Mathematical Proceedings of the Cambridge Philosophical Society **124** (1998), 1–14. MR 99g:11111.

[70] H. G. Khajah, Eduardo L. Ortiz, *On a differential-delay equation arising in number theory*, Applied Numerical Mathematics **21** (1996), 431–437. MR 98d:11160.

[71] Donald E. Knuth, Luis Trabb Pardo, *Analysis of a simple factorization algorithm*, Theoretical Computer Science **3** (1976), 321–348. MR 58 #16485.

[72] Uwe Krause, *Anzahl der Ideale a mit $Na \le x$ und Primteilern p mit $Np \le y$*, Diplomarbeit, Philipps-Universität Marburg, 1989.

[73] Uwe Krause, *Abschätzungen für die Funktion $\Psi_K(x, y)$ in algebraischen Zahlkörpern*, Manuscripta Mathematica **69** (1990), 319–331. MR 91i:11165.

[74] Arjen K. Lenstra, Hendrik W. Lenstra, Jr. (editors), *The development of the number field sieve*, Lecture Notes in Mathematics 1554, Springer-Verlag, Berlin, 1993. ISBN 3–540–57013–6. MR 96m:11116.

[75] Hendrik W. Lenstra, Jr., Jonathan Pila, Carl Pomerance, *A hyperelliptic smoothness test. I*, Philosophical Transactions of the Royal Society of London Series A **345** (1993), 397–408. MR 94m:11107.

[76] Eugenijus Manstavičius, *Semigroup elements free of large prime factors*, in [91] (1992), 135–153. MR 93m:11091.

[77] George Marsaglia, Arif Zaman, John C. W. Marsaglia, *Numerical solution of some classical differential-difference equations*, Mathematics of Computation **53** (1989), 191–201. MR 90h:65124.

[78] Richard A. Mollin (editor), *Number theory and applications*, Kluwer, Dordrecht, 1989. ISBN 0–7923–0149–8. MR 92c:11002.

[79] Pieter Moree, *An interval result for the number field $\psi(x, y)$ function*, Manuscripta Mathematica **76** (1992), 437–450. MR 93h:11127.

[80] Pieter Moree, *On the number of y-smooth natural numbers $\le x$ representable as a sum of two integer squares*, Manuscripta Mathematica **80** (1993), 199–211. MR 94g:11069.

[81] Pieter Moree, *Psixyology and Diophantine equations*, Dissertation, Rijksuniversiteit te Leiden, Leiden, 1993; available from `http://web.inter.nl.net/hcc/J.Moree/linkind2.htm`. MR 96e:11114.

[82] Karl K. Norton, *Numbers with small prime factors, and the least kth power non-residue*, American Mathematical Society, Providence, Rhode Island, 1971. MR 44 #3948.

[83] Daniel Panario, Xavier Gourdon, Philippe Flajolet, *An analytic approach to smooth polynomials over finite fields*, in [14] (1998), 226–236. MR 1 726 074.

[84] V. Ramaswami, *The number of positive integers $\leq x$ and free of prime divisors $> x^c$, and a problem of S. S. Pillai*, Duke Mathematical Journal **16** (1949), 99–109. MR 10,597b.

[85] Robert A. Rankin, *The difference between consecutive prime numbers*, Journal of the London Mathematical Society **13** (1938), 242–247.

[86] Paulo Ribenboim, *Fields: algebraically closed and others*, Manuscripta Mathematica **75** (1992), 115–150. MR 93f:13014.

[87] Éric Saias, *Sur le nombre des entiers sans grand facteur premier*, Journal of Number Theory **32** (1989), 78–99. MR 90f:11080.

[88] Éric Saias, *Entiers sans grand ni petit facteur premier. I*, Acta Arithmetica **61** (1992), 347–374. MR 93d:11096.

[89] Éric Saias, *Entiers sans grand ni petit facteur premier. II*, Acta Arithmetica **63** (1993), 287–312. MR 94c:11089.

[90] Éric Saias, *Entiers sans grand ni petit facteur premier. III*, Acta Arithmetica **71** (1995), 351–379. MR 96g:11113.

[91] Fritz Schweiger, Eugenijus Manstavičius (editors), *New trends in probability and statistics, volume 2*, VSP, Utrecht, 1992. ISBN 90–6764–094–8. MR 93g:11005.

[92] Wilhelm Specht, *Zahlenfolgen mit endlich vielen Primteilern*, Bayerische Akademie der Wissenschaften, Mathematisch-naturwissenschaftliche Klasse, Sitzungsberichte (1949), 149–169. MR 11,500f.

[93] Gérald Tenenbaum, *Cribler les entiers sans grand facteur premier*, Philosophical Transactions of the Royal Society of London Series A **345** (1993), 377–384. MR 95d:11119.

[94] Joseph F. Traub, *Analytic computational complexity*, Academic Press, New York, 1976. MR 52 #15938.

[95] Jan van de Lune, Evert Wattel, *On the numerical solution of a differential-difference equation arising in analytic number theory*, Mathematics of Computation **32** (1969), 417–421. MR 40:1050.

[96] Ti Zuo Xuan, *On the asymptotic behavior of the Dickman-de Bruijn function*, Mathematische Annalen **297** (1993), 519–533. MR 94j:11095.

[97] Ti Zuo Xuan, *Integers with no large prime factors*, Acta Arithmetica **69** (1995), 303–327. MR 96c:11106.

[98] Ti Zuo Xuan, *On smooth integers in short intervals under the Riemann hypothesis*, Acta Arithmetica **88** (1999), 327–332. MR 2000d:11110.

Department of Mathematics, Statistics, and Computer Science (M/C 249), The University of Illinois at Chicago, 851 South Morgan Street, Chicago, IL 60607–7045

E-mail address: `djb@cr.yp.to`