Asymptotic Semi-Smoothness Probabilities

Eric Bach
Rene Peralta

Technical Report #1115

October 1992

Asymptotic Semi-Smoothness Probabilities

Eric Bach [*] *René Peralta* [†]

20 October 1992

Abstract

We call an integer *semi-smooth* with respect to x and y if each of its prime factors is $\leq y$, and all but one are $\leq x$. Such numbers are useful in various factoring algorithms, including the quadratic sieve. Let $G(\alpha, \beta)$ be the asymptotic probability that a random integer n is semi-smooth with respect to n^α and n^β. We present numerical methods for computing G, tables of G, and estimates for the error incurred by this asymptotic approximation.

---

[*]Computer Sciences Department, University of Wisconsin–Madison, 1210 W. Dayton St., Madison, WI 53706. E-mail: bach@cs.wisc.edu. Supported in part by NSF Grants DCR-8552596 and CCR-9208639.

[†]Department of Electrical Engineering and Computer Science, University of Wisconsin–Milwaukee, P.O. Box 784, Milwaukee, WI 53201. E-mail: peralta@cs.uwm.edu. Supported in part by NSF Grant CCR-9207204.

1 Introduction

Many number-theoretic algorithms, such as the quadratic sieve factoring method [13], rely on auxiliary numbers whose prime factors lie within prescribed bounds. In practice, one often uses so-called "large prime" versions of these algorithms, in which the auxiliary numbers are composed of one moderately large prime factor, and a number of smaller ones. In analyzing these, it is useful to know the asymptotic probability that a random number has this form. In this paper, we show how to compute this probability quickly and accurately, and assess the accuracy of our asymptotic approximations.

Following Knuth and Trabb Pardo [4], we let n_i be the ith largest prime factor of an integer $n > 1$. If i is greater than the number of prime factors, we define n_i to be 1. Note that the n_i are not necessarily distinct.

We will say that n is *semi-smooth* with respect to y and z if $n_1 \leq y$ and $n_2 \leq z$. That is, all the prime factors of n are bounded by z, with the possible exception of a prime factor bounded by y. We let

$$\Psi(x, y, z) = \#\{n \leq x : n_1 \leq y, n_2 \leq z\}.$$

This generalizes de Bruijn's function [2]

$$\Psi(x, y) = \#\{n \leq x : n_1 \leq y\}.$$

We will prove that for every α, β satisfying $0 < \alpha < \beta < 1$,

$$G(\alpha, \beta) = \lim_{x \to \infty} \Psi(x, x^\beta, x^\alpha)/x \tag{1.1}$$

exists. This should be thought of as the asymptotic joint distribution of the relative lengths of n_1 and n_2. Thus, the function $\sigma(u, v) = G(1/u, 1/v)$ can be considered a two-dimensional analog of Dickman's well-known rho function.

The function G satisfies some interesting recurrence relations. In Section 3, we use these to show the limit in (1.1) exists, and to estimate the rate of convergence. In Section 4 we discuss methods for computing G numerically, and tabulate the results in Section 5. Finally, Section 6 discusses the accuracy of our asymptotic approximations.

2 Background

The *Dickman rho function* is defined for real $x \geq 0$ by the relation

$$\rho(x) = \begin{cases} 1, & \text{if } 0 \leq x \leq 1; \\ \frac{1}{x}\int_{x-1}^{x} \rho(t)dt, & \text{otherwise.} \end{cases} \tag{2.1}$$

We also let $F(\alpha) = \rho(1/\alpha)$.

Norton [11] surveys some useful properties of the rho function, which we summarize here. First, $0 < \rho(x) \leq 1$, and

$$\rho'(x) = -\rho(x-1)/x \tag{2.2}$$

when $x \geq 1$. This implies that ρ is non-increasing, and $|\rho'(x)| \leq 1$. In fact, the rho function decreases very rapidly for large x; we have $\rho(x) \leq 1/x!$.

The differential-delay equation (2.2) implies that ρ is piecewise analytic. More precisely, there is an analytic function ρ_k agreeing with $\rho(x)$ when $k-1 \leq x \leq k$, for $k = 1, 2, 3, \ldots$. We have, for example, $\rho_1 = 1$, and $\rho_2 = 1 - \log x$. It can also be shown that ρ belongs to the class C^k on the interval $[k, \infty)$.

Let $\pi(x)$ denote the number of primes $\leq x$, and let $\mathrm{li}(x) = \int_0^x dt/\log t$ (the Cauchy principal value is intended here). We will use the prime number theorem, in the form

$$\pi(x) = \mathrm{li}(x) + O(\frac{x}{\log^c x}); \tag{2.3}$$

this relation holds for any $c > 0$. We write $\epsilon(x)$ for the error term, so that $\pi(x) = \mathrm{li}(x) + \epsilon(x)$. Schoenfeld proved, assuming the Riemann hypothesis, that

$$|\epsilon(x)| < (\sqrt{x}\log x)/(8\pi) \tag{2.4}$$

provided $x \geq 2,657$. (See (6.18) of [16].)

The prime number theorem implies

$$\sum_{p<x} \frac{1}{p} = \log\log x + O(1) \tag{2.5}$$

and

$$\sum_{p<x} \frac{1}{p\log p} = O(1). \tag{2.6}$$

Let $0 < \alpha < 1$. Results of de Bruijn imply that if $0 < \alpha \leq \gamma$ and $t^\alpha \geq 2$, we have

$$\Psi(t, t^\gamma) = tF(\gamma) + O(\frac{t}{\alpha \log t}). \tag{2.7}$$

(To prove this, combine (1.4) and (5.3) of [2] with (2.3) above, taking $c = 4$.)

In results such as the above, an unadorned *"O"* symbol indicates an absolute constant.

3 Recurrence Relations for Smoothness Distributions

Many of the useful properties of asymptotic smoothness distributions can be derived from a simple heuristic model, which we call *random bisection*. The idea is that asymptotically, the relative lengths of the prime factors of a random number can be obtained by choosing a random λ uniformly from $(0, 1)$ – this gives the relative length of the first factor – and then proceeding recursively with the smaller interval $(0, 1 - \lambda)$. (This was previously applied to prime factorizations in [1].)

To illustrate, we derive a recurrence for $F(\alpha)$, the asymptotic probability that none of n's prime factors exceed n^α. This is the probability that all lengths chosen by random bisection are $\leq \alpha$; conditioning on the first length λ, we should have

$$F(\alpha) = \int_0^\alpha F(\frac{\alpha}{1-\lambda})d\lambda. \tag{3.1}$$

This is equivalent to (2.1), as the substitutions $t = (1 - \lambda)/\alpha$ and $x = 1/\alpha$ show.

Using a similar argument, one can deduce that $F_2(\alpha)$, the asymptotic probability that $n_2 \leq n^\alpha$, should satisfy

$$F_2(\alpha) = \int_0^\alpha F_2(\frac{\alpha}{1-\lambda})d\lambda + \int_\alpha^1 F(\frac{\alpha}{1-\lambda})d\lambda. \tag{3.2}$$

(Compare with (3.8) and (3.11) of [4].)

Now, we let $G(\alpha, \beta)$ denote the asymptotic probability that $n_2 \leq n^\alpha$ and $n_1 \leq n^\beta$. Again by conditioning on the first length λ, we conclude that G, if it exists, should satisfy

$$G(\alpha, \beta) = \int_0^\alpha G(\frac{\alpha}{1-\lambda}, \frac{\beta}{1-\lambda})d\lambda + \int_\alpha^\beta F(\frac{\alpha}{1-\lambda})d\lambda. \tag{3.3}$$

We will prove this rigorously below, using a different relation for G that is not as easy to motivate:

$$G(\alpha, \beta) = F(\alpha) + \int_\alpha^\beta F(\frac{\alpha}{1-\lambda})\frac{d\lambda}{\lambda}. \tag{3.4}$$

We can, however, give it a probabilistic interpretation. We condition on the *largest* length λ produced by random bisection. Either $\lambda \leq \alpha$ (which accounts for the term $F(\alpha)$), or it lies between α and β. The second event contributes a term

$$\int_\alpha^\beta \Pr[\lambda_{(2)} \leq \alpha | \lambda_{(1)} = \lambda] dF(\lambda).$$

(Here $\lambda_{(1)} > \lambda_{(2)} > \ldots$ are the lengths produced by random bisection, in sorted order.) The distribution of $\lambda_{(1)}$ is absolutely continuous; from (2.2), we get

$$dF(\lambda) = F(\frac{\lambda}{1-\lambda})\frac{d\lambda}{\lambda}.$$

Because (3.4) holds for arbitrary $\alpha \leq \beta$, a standard theorem of analysis (see [17], p. 360) implies that we can take

$$\Pr[\lambda_{(2)} \leq \alpha | \lambda_{(1)} = \lambda] = F(\frac{\alpha}{1-\lambda})/F(\frac{\lambda}{1-\lambda}). \tag{3.5}$$

So far we have relied on heuristic arguments. We now prove (3.4) and (3.3).

Theorem 3.1 *If $0 < \alpha < \beta < 1$, then*

$$\Psi(x, x^\beta, x^\alpha) = xF(\alpha) + x\int_\alpha^\beta F(\frac{\alpha}{1-\lambda})\frac{d\lambda}{\lambda} + O(\frac{\log(\alpha^{-1})}{\alpha}\frac{x}{\log x}).$$

Therefore, the limit

$$G(\alpha, \beta) = \lim_{x\to\infty} \Psi(x, x^\beta, x^\alpha)/x$$

exists, and satisfies (3.4).

Proof. The basic idea of the proof is to carefully repeat the conditioning argument for (3.4), employing a uniform estimate for the Ψ function and the prime number theorem.

We have

$$\Psi(x, x^\beta, x^\alpha) = \sum_{p \leq x^\alpha} \#\{n \leq x : n_1 = p\} + \sum_{x^\alpha < p \leq x^\beta} \#\{n \leq x : n_1 = p, n_2 \leq x^\alpha\}. \tag{3.6}$$

For the first sum, we have

$$\sum_{p \leq x^\alpha} \#\{n \leq x : n_1 = p\} = \#\{n \leq x : n_1 \leq x^\alpha\} = xF(\alpha) + O(\frac{x}{\alpha \log x}).$$

The second sum requires more work. We first observe that

$$\sum_{x^\alpha<p\le x^\beta} \#\{n\le x : n_1=p, n_2\le x^\alpha\} = \sum_{x^\alpha<p\le x^\beta} \#\{m\le x/p : m_1\le x^\alpha\}$$

$$= \sum_{x^\alpha<p\le x^\beta} \#\{m\le x/p : m_1\le (x/p)^{\frac{\alpha}{1-\log p/\log x}}\}. \tag{3.7}$$

When $x^\alpha < p \le x^\beta$,

$$0\le\alpha<\frac{\alpha}{1-\alpha}<\frac{\alpha}{1-\log p/\log x}\le\frac{\alpha}{1-\beta}.$$

The estimate (2.7) applies, so

$$\sum_{x^\alpha<p\le x^\beta} \#\{m\le x/p : m_1\le (x/p)^{\frac{\alpha}{1-\log p/\log x}}\}$$

$$= \sum_{x^\alpha<p\le x^\beta} \frac{x}{p}F(\frac{\alpha}{1-\log p/\log x}) + O(\frac{1}{\alpha}\sum_{x^\alpha<p\le x^\beta}\frac{x/p}{\log(x/p)}).$$

Applying (2.5) and (2.6), we get

$$\Psi(x,x^\beta,x^\alpha) = xF(\alpha) + \sum_{x^\alpha<p\le x^\beta}\frac{x}{p}F(\frac{\alpha}{1-\log p/\log x}) + O(\frac{\log(\alpha^{-1})}{\alpha}\frac{x}{\log x}). \tag{3.8}$$

Using Stieltjes integration, we have

$$\sum_{x^\alpha<p\le x^\beta}\frac{1}{p}F(\frac{\alpha}{1-\log p/\log x}) = \int_{x^\alpha}^{x^\beta}\rho(\frac{1-\log t/\log x}{\alpha})\frac{d\pi(t)}{t}. \tag{3.9}$$

If we integrate by parts, substitute $\pi(t)=\mathrm{li}(t)+\epsilon(t)$, and recombine the terms involving $\mathrm{li}(t)$, we obtain

$$\int_{x^\alpha}^{x^\beta}\rho(\frac{1-\log t/\log x}{\alpha})\frac{d\pi(t)}{t} = \int_{x^\alpha}^{x^\beta}\rho(\frac{1-\log t/\log x}{\alpha})\frac{dt}{t\log t}$$

$$+\Big[\rho(\frac{1-\log t/\log x}{\alpha})\frac{\epsilon(t)}{t}\Big]_{x^\alpha}^{x^\beta} - \int_{x^\alpha}^{x^\beta}\frac{d}{dt}(\frac{1}{t}\rho(\frac{1-\log t/\log x}{\alpha}))\epsilon(t)dt. \tag{3.10}$$

We now show the error terms in (3.10) are small. Using $|\rho|\le 1$ and (2.3) (with $c=1$), we obtain

$$\Big[\rho(\frac{1-\log t/\log x}{\alpha})\frac{\epsilon(t)}{t}\Big]_{x^\alpha}^{x^\beta} = O(\frac{1}{\alpha\log^2 x}).$$

After differentiating the quotient and estimating each resulting term separately, we get

$$\int_{x^\alpha}^{x^\beta}\frac{d}{dt}(\frac{1}{t}\rho(\frac{1-\log t/\log x}{\alpha}))\epsilon(t)dt = O(\int_{x^\alpha}^{x^\beta}\frac{dt}{t\log^2 t}) = O(\frac{1}{\alpha\log x}).$$

This shows that

$$\Psi(x, x^\beta, x^\alpha) = xF(\alpha) + \int_{x^\alpha}^{x^\beta} \rho(\frac{1 - \log t/\log x}{\alpha})\frac{dt}{t\log t} + O(\frac{\log(\alpha^{-1})x}{\alpha \log x}).$$

Making the substitution $\lambda = \log t/\log x$, we obtain the first statement of the theorem. The second follows from dividing by x and letting $x \to \infty$. ∎

The novelty in the above theorem is a careful estimate of the error term. Knuth and Trabb Pardo gave (3.4) for the special case $\beta = 2\alpha$. Weaker statements of Theorem 3.1 (that is, without error estimates) appear in [5] and [9]. We also remark that a more careful argument shows that the theorem holds for $\beta = 1$. We now prove (3.3), which we believe to be new.

Theorem 3.2 *We have*

$$G(\alpha, \beta) = \int_0^\alpha G(\frac{\alpha}{1-\lambda}, \frac{\beta}{1-\lambda})d\lambda + \int_\alpha^\beta F(\frac{\alpha}{1-\lambda})d\lambda.$$

Proof. If $0 < \gamma < 1$, we have

$$F(\gamma) = \int_0^\gamma F(\frac{\gamma}{1-\zeta})d\zeta.$$

Now substitute $\zeta = \lambda/(1-\nu)$ and $\gamma = \alpha/(1-\nu)$, and rearrange terms to obtain

$$F(\frac{\alpha}{1-\nu}) = \int_0^\alpha F(\frac{\alpha}{1-\nu-\lambda})d\lambda + \nu F(\frac{\alpha}{1-\nu}).$$

If we divide this by ν, integrate over $\alpha \le \nu \le \beta$, reverse the order of integration, and substitute $\nu = (1-\lambda)\mu$, we get

$$\int_\alpha^\beta F(\frac{\alpha}{1-\nu})\frac{d\nu}{\nu} = \int_0^\alpha d\lambda \int_{\frac{\alpha}{1-\lambda}}^{\frac{\beta}{1-\lambda}} F(\frac{\alpha}{(1-\lambda)(1-\mu)})\frac{d\mu}{\mu} + \int_\alpha^\beta F(\frac{\alpha}{1-\nu})d\nu.$$

If we add $F(\alpha) = \int_0^\alpha F(\alpha/(1-\lambda))d\lambda$ to both sides and apply (3.4), we get

$$G(\alpha, \beta) = F(\alpha) + \int_\alpha^\beta F(\frac{\alpha}{1-\nu})\frac{d\nu}{\nu}$$

$$= \int_0^\alpha d\lambda\Big[\int_{\frac{\alpha}{1-\lambda}}^{\frac{\beta}{1-\lambda}} F(\frac{\alpha}{(1-\lambda)(1-\mu)})\frac{d\mu}{\mu} + F(\frac{\alpha}{(1-\lambda)})\Big] + \int_\alpha^\beta F(\frac{\alpha}{1-\nu})d\nu$$

$$= \int_0^\alpha G(\frac{\alpha}{1-\lambda}, \frac{\beta}{1-\lambda})d\lambda + \int_\alpha^\beta F(\frac{\alpha}{1-\lambda})d\lambda.$$

∎

4 Numerical Methods

Several authors have discussed computing smoothness distributions such as the Dickman rho function. We briefly discuss this work, and then present our numerical methods for the semi-smoothness distribution G.

Implicit in the random bisection idea is the notion that smoothness distributions can be computed by Monte Carlo methods. This was done for the rho function by Chamayou [3], albeit with a different probabilistic model than ours. Although one could also approximate G by simulation, we have not done this because the probabilities of current interest are so small.

It is also possible to combine a recurrence relation with numerical integration. This was done by van de Lune and Wattel [8] and Knuth and Trabb Pardo [4]. For example, replacing the integral in (2.1) with an appropriate quadrature rule gives a linear equation that can be solved to obtain an approximation to $\rho(x)$. Either of the relations (3.3) and (3.4) can be used in this way to compute G. In practice, however, we were dissatisfied with the performance of the resulting methods. Use of the recurrence relation (3.3) involves computing values of G in a two-dimensional region, and interpolating the values on a line of integration. The relation (3.4) is more useful, as it only relies on values of F (i.e. ρ); however, one needs an accurate table of this function before numerical integration is feasible.

The fastest method we have so far found is based on the algorithm of Patterson and Rumsey [12] for the rho function. Since their method is apparently still unpublished, we explain it in detail.

Patterson and Rumsey's algorithm is based on the idea that the rho function is piecewise analytic. Recall that there is an analytic function $\rho_k(x)$ that agrees with $\rho(x)$, when $x \in [k-1, k]$. The algorithm precomputes the Taylor series

$$\rho(k-\xi) = \rho_k(k-\xi) = \sum_{i=0}^{\infty} c_i^{(k)} \xi^i$$

for each ρ_k around $x = k$ and stores the coefficients; to evaluate ρ it first decides which ρ_k is to be used and then evaluates the corresponding Taylor series.

The function ρ_1 is identically 1. The Taylor series for ρ_2 around $x = 2$ can be easily

computed from $\rho_2(x) = 1 - \log(x)$. We have

$$\rho(2-\xi) = 1 - \log 2 - \log(1-\xi/2) = 1 - \log 2 + \sum_{i=1}^{\infty} \frac{\xi^i}{i2^i}, \tag{4.1}$$

valid for $0 \le \xi \le 1$.

Now, suppose we know the Taylor series for ρ_{k-1}, so that

$$\rho(k-1-\xi) = \sum_{j=0}^{\infty} c_j^{(k-1)} \xi^j$$

holds when $0 \le \xi \le 1$. Using (2.2), we have

$$\begin{aligned} \rho'(k-\xi) &= -\frac{1}{k}(1-\xi/k)^{-1}\rho(k-1-\xi) \\ &= -\frac{1}{k}(\sum_{j=0}^{\infty} c_j^{(k-1)}\xi^j)(1+\sum_{\ell=1}^{\infty}(\xi/k)^\ell) \\ &= -\sum_{i=1}^{\infty} i c_i^{(k)} \xi^{i-1}, \end{aligned}$$

where the last equality is obtained by differentiating $\rho_k(x) = \sum_{i=0}^{\infty} c_i^{(k)}(k-x)^i$ and evaluating at $x = k - \xi$.

Therefore, for $i > 0$, we have

$$c_i^{(k)} = \sum_{j=0}^{i-1} \frac{c_j^{(k-1)}}{ik^{i-j}}. \tag{4.2}$$

This determines all coefficients $c_i^{(k)}$ except for the constant term $c_0^{(k)}$. Now use (2.1) and substitute $t = k - \xi$ to obtain

$$kc_0^{(k)} = k\rho(k) = \int_0^1 \rho(k-\xi)d\xi = \sum_{j=0}^{\infty} \frac{c_j^{(k)}}{j+1},$$

which implies

$$c_0^{(k)} = \frac{1}{k-1} \sum_{j=1}^{\infty} \frac{c_j^{(k)}}{j+1}. \tag{4.3}$$

The relations (4.1), (4.2), and (4.3) define the Taylor series of ρ_k for all $k \ge 2$, and in practice it suffices to use $O(m)$ terms of each series to get precision m. (This is because the radius of convergence of each Taylor series is at least 2.) This routine requires storage for the coefficients $c_i^{(k)}$, and a precomputation of $O(m^2 k)$ arithmetic operations, to evaluate $\rho(x)$ for $x \le k$ to m bits of accuracy. (Asymptotically, one could use the FFT to reduce the

precomputation to $O(mk \log m)$.) Empirically, we have found that 55 coefficients are sufficient to compute ρ to IEEE standard double precision (about 10^{-17}) in the range $0 \le x \le 20$.)

Our method for computing G uses (3.4), together with term-by-term integration of the Taylor series for pieces of the rho function. Rather than use (3.4) directly, it is more convenient to work with $\sigma(u,v) = G(1/u, 1/v)$, which satisfies

$$\sigma(u,v) = \rho(u) + \int_v^u \rho(u - u/t)\frac{dt}{t}.$$

(To prove this, make the substitutions $\alpha = 1/u$, $\beta = 1/v$, and $\lambda = 1/t$ in (3.4).) We define

$$J(u,v,w) = \int_v^u \rho(w - w/t)\frac{dt}{t},$$

so that

$$\sigma(u,v) = \rho(u) + J(u,v,u).$$

We now show how to compute $J(u,v,w)$. Let $k = \lceil w - w/u \rceil$, and define $\xi(t)$ by $w - w/t = k - \xi(t)$.

If $\xi(t) \in [0,1]$ for $v \le t \le u$, we can proceed as follows:

$$J(u,v,w) = \int_v^u \rho(k - \xi(t))\frac{dt}{t} = \sum_{i=0}^{\infty} c_i^{(k)} \int_v^u \xi(t)^i \frac{dt}{t}$$

$$= \sum_{i=0}^{\infty} c_i^{(k)} \int_{w/u}^{w/v} \frac{(\eta + k - w)^i}{\eta} d\eta.$$

(Here we have substituted $\eta = w/t$.) If $H_i(u,v,w) = \int_{w/u}^{w/v} \frac{(\eta+k-w)^i}{\eta} d\eta$, then writing $(\eta + k - w)^i/\eta$ as $(\eta + k - w)^{i-1} + (\eta + k - w)^{i-1}(k-w)/\eta$ gives

$$H_i(u,v,w) = \begin{cases} \log(u/v), & \text{if } i = 0; \\ \frac{(w/v+k-w)^i - (w/u+k-w)^i}{i} + (k-w)H_{i-1}(u,v,w), & \text{otherwise.} \end{cases} \tag{4.4}$$

Thus, in this case

$$J(u,v,w) = \sum_{i=0}^{\infty} c_i^{(k)} H_i(u,v,w) \tag{4.5}$$

where the H_i's can be computed via (4.4). If $\xi(t) \notin [0,1]$, we must split the integral. Note that when $t = w/(w-k+1)$, we have $\xi(t) = 1$, that is, $w - w/t = k - 1$. In this case, we have

$$J(u,v,w) = \int_v^{w/(w-k+1)} \rho(w - w/t)\frac{dt}{t} + \int_{w/(w-k+1)}^u \rho(w - w/t)\frac{dt}{t}.$$

The second integral can be computed via (4.5) and the first integral is computed recursively.

Note that we can decide whether the integral must be split by comparing v to $w/(w-k+1)$. The integral is split iff $v < w/(w-k+1)$. The number of times the integral must be split is no more than u/v.

5 Tables

In this section we give tables of the asymptotic semi-smoothness distribution, computed with the methods of Section 4. We used 60 terms in the expansion for $\rho(x)$ and 20 terms in the expansion given by (4.5). As a check on our computations we used an independent computation of $G(\alpha, 2\alpha)$ (using (3.2) and numerical integration), as well as Table 1 in [4]. This table includes values of $G(\alpha, \alpha) = \rho(\alpha^{-1})$, as well as values of $G(\alpha, 2\alpha)$. Our results agree with [4] to six significant figures.

Table 1 shows $\sigma(u, v) = G(\frac{1}{u}, \frac{1}{v})$ for u, v in the range $2 \le u \le 20$ and $2 \le v \le 10$.

u	v								
	2	3	4	5	6	7	8	9	10
2	3.068528e-01	—	—	—	—	—	—	—	—
3	2.246518e-01	4.860839e-02	—	—	—	—	—	—	—
4	9.639901e-02	2.465561e-02	4.910926e-03	—	—	—	—	—	—
5	3.079212e-02	6.144568e-03	1.849280e-03	3.547247e-04	—	—	—	—	—
6	8.511187e-03	1.092267e-03	3.127192e-04	1.051674e-04	1.964970e-05	—	—	—	—
7	2.184024e-03	1.596965e-04	3.754974e-05	1.317947e-05	4.778139e-06	8.745670e-07	—	—	—
8	5.297043e-04	2.058327e-05	3.662652e-06	1.179057e-06	4.696284e-07	1.796314e-07	3.232069e-08	—	—
9	1.221795e-04	2.418992e-06	3.097157e-07	8.573660e-08	3.319264e-08	1.439810e-08	5.732620e-09	1.016248e-09	—
10	2.684198e-05	2.633999e-07	2.352672e-08	5.382861e-09	1.915717e-09	8.358903e-10	3.855071e-10	1.583472e-10	2.770172e-11
11	5.627512e-06	2.679280e-08	1.637888e-09	3.019323e-10	9.556196e-11	3.985501e-11	1.890085e-11	9.128686e-12	3.844123e-12
12	1.128672e-06	2.559021e-09	1.057229e-10	1.544758e-11	4.254912e-12	1.647475e-12	7.654740e-13	3.859215e-13	1.932249e-13
13	2.170148e-07	2.304231e-10	6.373298e-12	7.303377e-13	1.725544e-13	6.086492e-14	2.698020e-14	1.355061e-14	7.158754e-15
14	4.009759e-08	1.962928e-11	3.606489e-13	3.218087e-14	6.459110e-15	2.048898e-15	8.518898e-16	4.157376e-16	2.213880e-16
15	7.134198e-09	1.587081e-12	1.923443e-14	1.329397e-15	2.252007e-16	6.367265e-17	2.454356e-17	1.145796e-17	6.005714e-18
16	1.224713e-09	1.221450e-13	9.701521e-16	5.171612e-17	7.360498e-18	1.843517e-18	6.534072e-19	2.887008e-19	1.467795e-19
17	2.032238e-10	8.971949e-15	4.641835e-17	1.901399e-18	2.266007e-19	5.005962e-20	1.621962e-20	6.731238e-21	3.286696e-21
18	3.265002e-11	6.304945e-16	2.112631e-18	6.627200e-20	6.595739e-21	1.281259e-21	3.779199e-22	1.465048e-22	6.821566e-23
19	5.086646e-12	4.248307e-17	9.169125e-20	2.195713e-21	1.820808e-22	3.103008e-23	8.307233e-24	2.996162e-24	1.323455e-24
20	7.695283e-13	2.750199e-18	3.803595e-21	6.932224e-23	4.779992e-24	7.133404e-25	1.729532e-25	5.786581e-26	2.415504e-26

Table 1: Values of $\sigma(u, v) = G(1/u, 1/v)$ for $2 \le u \le 20$; $2 \le v \le 10$.

Of particular interest nowadays are values of $G(\alpha, \beta)$ for (α, β) near $(1/12, 1/7.5)$. This is so because recent implementations of the multiple polynomial quadratic sieve are designed to factor 100-digit cryptographic integers (i.e. products of two large primes), using auxiliary 60-digit numbers which are semi-smooth with respect to bounds near 10^8 and 10^5. It is believed that these auxiliary numbers are semi-smooth with the same probability as random numbers, so that the bulk of the algorithm's work can be viewed as a search for semi-smooth numbers among what are essentially random 60-digit numbers. Thus the probability of a "hit" is given by $\Psi(10^{60}, 10^8, 10^5)$, which is approximately $G(1/12, 1/7.5)$ (for details, see [6]). Most other factoring algorithms also allow for a "large prime" variation (see [9, 10]). Semi-smoothness tables should be of aid in choosing optimal parameters for these algorithms as well.

Tables 2.a, 2.b, and 2.c give values of $G(\alpha, \beta)$ for α and β in the current range of interest for factorization algorithms.

u	v							
	6.5	6.6	6.7	6.8	6.9	7.0	7.1	7.2
10.0	1.246194e-09	1.148345e-09	1.059326e-09	9.781358e-10	9.039084e-10	8.358903e-10	7.734239e-10	7.159343e-10
10.1	9.267054e-10	8.537368e-10	7.874246e-10	7.270088e-10	6.718311e-10	6.213195e-10	5.749760e-10	5.323650e-10
10.2	6.880222e-10	6.336660e-10	5.843225e-10	5.394142e-10	4.984417e-10	4.609719e-10	4.266273e-10	3.950788e-10
10.3	5.100216e-10	4.695735e-10	4.328958e-10	3.995504e-10	3.691589e-10	3.413934e-10	3.159687e-10	2.926361e-10
10.4	3.775021e-10	3.474354e-10	3.202012e-10	2.954679e-10	2.729489e-10	2.523964e-10	2.335950e-10	2.163571e-10
10.5	2.790060e-10	2.566795e-10	2.364786e-10	2.181523e-10	2.014841e-10	1.862869e-10	1.723981e-10	1.596764e-10
10.6	2.059151e-10	1.893533e-10	1.743849e-10	1.608201e-10	1.484955e-10	1.372698e-10	1.270207e-10	1.176419e-10
10.7	1.517608e-10	1.394879e-10	1.284081e-10	1.183780e-10	1.092743e-10	1.009909e-10	9.343555e-11	8.652838e-11
10.8	1.116975e-10	1.026120e-10	9.441888e-11	8.700994e-11	8.029241e-11	7.418630e-11	6.862242e-11	6.354074e-11
10.9	8.210206e-11	7.538299e-11	6.933052e-11	6.386329e-11	5.891146e-11	5.441493e-11	5.032176e-11	4.658693e-11
11.0	6.027060e-11	5.530650e-11	5.083987e-11	4.680950e-11	4.316292e-11	3.985501e-11	3.684682e-11	3.410465e-11
11.1	4.418869e-11	4.052478e-11	3.723173e-11	3.426355e-11	3.158083e-11	2.914976e-11	2.694117e-11	2.492983e-11
11.2	3.235813e-11	2.965652e-11	2.723108e-11	2.504729e-11	2.307562e-11	2.129072e-11	1.967079e-11	1.819697e-11
11.3	2.366654e-11	2.167641e-11	1.989173e-11	1.828661e-11	1.683893e-11	1.552974e-11	1.434274e-11	1.326385e-11
11.4	1.728927e-11	1.582466e-11	1.451272e-11	1.333407e-11	1.227216e-11	1.131282e-11	1.044389e-11	9.654871e-12
11.5	1.261597e-11	1.153912e-11	1.057562e-11	9.710955e-12	8.932758e-12	8.230457e-12	7.594978e-12	7.018507e-12
11.6	9.195530e-12	8.404539e-12	7.697601e-12	7.063874e-12	6.494131e-12	5.980486e-12	5.516181e-12	5.095402e-12
11.7	6.695078e-12	6.114598e-12	5.596390e-12	5.132359e-12	4.715623e-12	4.340310e-12	4.001392e-12	3.694546e-12
11.8	4.869302e-12	4.443704e-12	4.064192e-12	3.724732e-12	3.420196e-12	3.146216e-12	2.899054e-12	2.675502e-12
11.9	3.537687e-12	3.225930e-12	2.948249e-12	2.700146e-12	2.477808e-12	2.277986e-12	2.097906e-12	1.935188e-12
12.0	2.567571e-12	2.339412e-12	2.136422e-12	1.955256e-12	1.793077e-12	1.647475e-12	1.516392e-12	1.398063e-12
12.1	1.861591e-12	1.694763e-12	1.546509e-12	1.414340e-12	1.296150e-12	1.190152e-12	1.094821e-12	1.008850e-12
12.2	1.348382e-12	1.226509e-12	1.118327e-12	1.021990e-12	9.359358e-13	8.588391e-13	7.895711e-13	7.271670e-13
12.3	9.757011e-13	8.867465e-13	8.078763e-13	7.377195e-13	6.751189e-13	6.190934e-13	5.688083e-13	5.235512e-13
12.4	7.053473e-13	6.404771e-13	5.830270e-13	5.319809e-13	4.864819e-13	4.458048e-13	4.093328e-13	3.765403e-13
12.5	5.094235e-13	4.621580e-13	4.203471e-13	3.832384e-13	3.501982e-13	3.206906e-13	2.942606e-13	2.705207e-13
12.6	3.675798e-13	3.331711e-13	3.027684e-13	2.758151e-13	2.518429e-13	2.304565e-13	2.113203e-13	1.941490e-13
12.7	2.649890e-13	2.399613e-13	2.178729e-13	1.983127e-13	1.809348e-13	1.654477e-13	1.516045e-13	1.391951e-13
12.8	1.908595e-13	1.726707e-13	1.566366e-13	1.424536e-13	1.298668e-13	1.186614e-13	1.086558e-13	9.969541e-14
12.9	1.373459e-13	1.241384e-13	1.125089e-13	1.022337e-13	9.312478e-14	8.502423e-14	7.779842e-14	7.133403e-14
13.0	9.875063e-14	8.916813e-14	8.074041e-14	7.330244e-14	6.671602e-14	6.086492e-14	5.565107e-14	5.099132e-14
13.1	7.094006e-14	6.399341e-14	5.789102e-14	5.251137e-14	4.775285e-14	4.353010e-14	3.977114e-14	3.641506e-14
13.2	5.091859e-14	4.588690e-14	4.147188e-14	3.758416e-14	3.414909e-14	3.110405e-14	2.839627e-14	2.598114e-14
13.3	3.651739e-14	3.287573e-14	2.968411e-14	2.687688e-14	2.439922e-14	2.220523e-14	2.025627e-14	1.851972e-14
13.4	2.616777e-14	2.353427e-14	2.122892e-14	1.920352e-14	1.741789e-14	1.583838e-14	1.443675e-14	1.318913e-14
13.5	1.873623e-14	1.683332e-14	1.516948e-14	1.370934e-14	1.242348e-14	1.128729e-14	1.028009e-14	9.384479e-15
13.6	1.340451e-14	1.203060e-14	1.083071e-14	9.778933e-15	8.853711e-15	8.037056e-15	7.313879e-15	6.671477e-15
13.7	9.582477e-15	8.591293e-15	7.726672e-15	6.969640e-15	6.304439e-15	5.717927e-15	5.199095e-15	4.738683e-15
13.8	6.844897e-15	6.130384e-15	5.507841e-15	4.963387e-15	4.485510e-15	4.064618e-15	3.692684e-15	3.362968e-15
13.9	4.885653e-15	4.370984e-15	3.923091e-15	3.531829e-15	3.188794e-15	2.886990e-15	2.620574e-15	2.384639e-15
14.0	3.484569e-15	3.114135e-15	2.792145e-15	2.511190e-15	2.265139e-15	2.048898e-15	1.858213e-15	1.689517e-15
14.1	2.483420e-15	2.217004e-15	1.985703e-15	1.784111e-15	1.607762e-15	1.452946e-15	1.316570e-15	1.196046e-15
14.2	1.768601e-15	1.577140e-15	1.411112e-15	1.266576e-15	1.140280e-15	1.029526e-15	9.320671e-16	8.460245e-16
14.3	1.258611e-15	1.121121e-15	1.002037e-15	8.984871e-16	8.081063e-16	7.289341e-16	6.593398e-16	5.979609e-16
14.4	8.950331e-16	7.963744e-16	7.110243e-16	6.368943e-16	5.722643e-16	5.157112e-16	4.660524e-16	4.223008e-16
14.5	6.360275e-16	5.652855e-16	5.041593e-16	4.511301e-16	4.049488e-16	3.645830e-16	3.291758e-16	2.980127e-16
14.6	4.516534e-16	4.009662e-16	3.572211e-16	3.193147e-16	2.863404e-16	2.575501e-16	2.323233e-16	2.101433e-16
14.7	3.205019e-16	2.842107e-16	2.529275e-16	2.258511e-16	2.023243e-16	1.818052e-16	1.638451e-16	1.480704e-16
14.8	2.272766e-16	2.013118e-16	1.789566e-16	1.596303e-16	1.428565e-16	1.282431e-16	1.154658e-16	1.042551e-16
14.9	1.610575e-16	1.424941e-16	1.265307e-16	1.127460e-16	1.007956e-16	9.039584e-17	8.131245e-17	7.335097e-17
15.0	1.140545e-16	1.007922e-16	8.940112e-17	7.957629e-17	7.106841e-17	6.367265e-17	5.721994e-17	5.157011e-17

Table 2.a: Values of $\sigma(u,v) = G(1/u, 1/v)$ for $10 \leq u \leq 15$; $6.5 \leq v \leq 7.2$.

u	v							
	7.3	7.4	7.5	7.6	7.7	7.8	7.9	8.0
10.0	6.629167e-10	6.139272e-10	5.685742e-10	5.265113e-10	4.874315e-10	4.510619e-10	4.171594e-10	3.855071e-10
10.1	4.931048e-10	4.568599e-10	4.233348e-10	3.922682e-10	3.634286e-10	3.366108e-10	3.116318e-10	2.883286e-10
10.2	3.660381e-10	3.392518e-10	3.144972e-10	2.915775e-10	2.703184e-10	2.505657e-10	2.321818e-10	2.150445e-10
10.3	2.711779e-10	2.514035e-10	2.331448e-10	2.162540e-10	2.006000e-10	1.860670e-10	1.725519e-10	1.599628e-10
10.4	2.005187e-10	1.859363e-10	1.724835e-10	1.600491e-10	1.485349e-10	1.378539e-10	1.279288e-10	1.186910e-10
10.5	1.479985e-10	1.372563e-10	1.273550e-10	1.182110e-10	1.097509e-10	1.019093e-10	9.462841e-11	8.785696e-11
10.6	1.090406e-10	1.011356e-10	9.385589e-11	8.713880e-11	8.092918e-11	7.517828e-11	6.984289e-11	6.488462e-11
10.7	8.019970e-11	7.438869e-11	6.904200e-11	6.411281e-11	5.955985e-11	5.534666e-11	5.144101e-11	4.781425e-11
10.8	5.888904e-11	5.462171e-11	5.069884e-11	4.708542e-11	4.375060e-11	4.066718e-11	3.781112e-11	3.516107e-11
10.9	4.317132e-11	4.004081e-11	3.716555e-11	3.451939e-11	3.207932e-11	2.982505e-11	2.773868e-11	2.580431e-11
11.0	3.159921e-11	2.930499e-11	2.719972e-11	2.526388e-11	2.348031e-11	2.183392e-11	2.031136e-11	1.890085e-11
11.1	2.309387e-11	2.141423e-11	1.987430e-11	1.845952e-11	1.715715e-11	1.595593e-11	1.484596e-11	1.381847e-11
11.2	1.685293e-11	1.562446e-11	1.449917e-11	1.346625e-11	1.251619e-11	1.164066e-11	1.083228e-11	1.008457e-11
11.3	1.228089e-11	1.138329e-11	1.056181e-11	9.808424e-12	9.116065e-12	8.478541e-12	7.890398e-12	7.346819e-12
11.4	8.936693e-12	8.281479e-12	7.682380e-12	7.133414e-12	6.629349e-12	6.165592e-12	5.738103e-12	5.343317e-12
11.5	6.494290e-12	6.016476e-12	5.579976e-12	5.180354e-12	4.813731e-12	4.476707e-12	4.166292e-12	3.879851e-12
11.6	4.713129e-12	4.365016e-12	4.047290e-12	3.756664e-12	3.490265e-12	3.245577e-12	3.020392e-12	2.812763e-12
11.7	3.416045e-12	3.162668e-12	2.931618e-12	2.720460e-12	2.527071e-12	2.349592e-12	2.186392e-12	2.036035e-12
11.8	2.472795e-12	2.288545e-12	2.120683e-12	1.967410e-12	1.827154e-12	1.698546e-12	1.580381e-12	1.471602e-12
11.9	1.787785e-12	1.653928e-12	1.532088e-12	1.420935e-12	1.319310e-12	1.226203e-12	1.140726e-12	1.062103e-12
12.0	1.290974e-12	1.193818e-12	1.105464e-12	1.024931e-12	9.513655e-13	8.840223e-13	8.222492e-13	7.654740e-13
12.1	9.311211e-13	8.606675e-13	7.966554e-13	7.383615e-13	6.851571e-13	6.364939e-13	5.918925e-13	5.509324e-13
12.2	6.707994e-13	6.197558e-13	5.734215e-13	5.312639e-13	4.928203e-13	4.576878e-13	4.255141e-13	3.959910e-13
12.3	4.827113e-13	4.457637e-13	4.122555e-13	3.817951e-13	3.540423e-13	3.287013e-13	3.055137e-13	2.842535e-13
12.4	3.469771e-13	3.202566e-13	2.960458e-13	2.740568e-13	2.540398e-13	2.357778e-13	2.190815e-13	2.037854e-13
12.5	2.491393e-13	2.298323e-13	2.123547e-13	1.964951e-13	1.820705e-13	1.689218e-13	1.569104e-13	1.459152e-13
12.6	1.786987e-13	1.647605e-13	1.521546e-13	1.407260e-13	1.303406e-13	1.208819e-13	1.122484e-13	1.043518e-13
12.7	1.280403e-13	1.179868e-13	1.089026e-13	1.006743e-13	9.320352e-14	8.640519e-14	8.020518e-14	7.453891e-14
12.8	9.164885e-14	8.440355e-14	7.786293e-14	7.194382e-14	6.657441e-14	6.169246e-14	5.724389e-14	5.318159e-14
12.9	6.553456e-14	6.031756e-14	5.561233e-14	5.135805e-14	4.750225e-14	4.399951e-14	4.081037e-14	3.790053e-14
13.0	4.681497e-14	4.306165e-14	3.967965e-14	3.662456e-14	3.385806e-14	3.134703e-14	2.906274e-14	2.698020e-14
13.1	3.341009e-14	3.071207e-14	2.828325e-14	2.609117e-14	2.410792e-14	2.230936e-14	2.067458e-14	1.918539e-14
13.2	2.382080e-14	2.188300e-14	2.014017e-14	1.856864e-14	1.714809e-14	1.586093e-14	1.469196e-14	1.362798e-14
13.3	1.696790e-14	1.557726e-14	1.432771e-14	1.320201e-14	1.218534e-14	1.126494e-14	1.042976e-14	9.670215e-15
13.4	1.207534e-14	1.107819e-14	1.018305e-14	9.377356e-15	8.650353e-15	7.992758e-15	7.396551e-15	6.854781e-15
13.5	8.585723e-15	7.871309e-15	7.230573e-15	6.654396e-15	6.134953e-15	5.665510e-15	5.240249e-15	4.854135e-15
13.6	6.099114e-15	5.587681e-15	5.129423e-15	4.717714e-15	4.346876e-15	4.012023e-15	3.708943e-15	3.433990e-15
13.7	4.328875e-15	3.963046e-15	3.635562e-15	3.341612e-15	3.077079e-15	2.838423e-15	2.622596e-15	2.426959e-15
13.8	3.069782e-15	2.808313e-15	2.574471e-15	2.364766e-15	2.176216e-15	2.006259e-15	1.852689e-15	1.713601e-15
13.9	2.175053e-15	1.988322e-15	1.821477e-15	1.671993e-15	1.537708e-15	1.416770e-15	1.307587e-15	1.208781e-15
14.0	1.539811e-15	1.406559e-15	1.287611e-15	1.181137e-15	1.085576e-15	9.995880e-16	9.220233e-16	8.518898e-16
14.1	1.089195e-15	9.941800e-16	9.094449e-16	8.336662e-16	7.657148e-16	7.046246e-16	6.495656e-16	5.998231e-16
14.2	7.698198e-16	7.021225e-16	6.418066e-16	5.879159e-16	5.396351e-16	4.962673e-16	4.572145e-16	4.219621e-16
14.3	5.436545e-16	4.954578e-16	4.525570e-16	4.142617e-16	3.799838e-16	3.492210e-16	3.215428e-16	2.965789e-16
14.4	3.836294e-16	3.493423e-16	3.188517e-16	2.916595e-16	2.673420e-16	2.455373e-16	2.259357e-16	2.082713e-16
14.5	2.704958e-16	2.461224e-16	2.244685e-16	2.051750e-16	1.879366e-16	1.724933e-16	1.586222e-16	1.461324e-16
14.6	1.905782e-16	1.732651e-16	1.578984e-16	1.442195e-16	1.320088e-16	1.210792e-16	1.112708e-16	1.024465e-16
14.7	1.341696e-16	1.218808e-16	1.109841e-16	1.012932e-16	9.265023e-17	8.492093e-17	7.799053e-17	7.176069e-17
14.8	9.438591e-17	8.566991e-17	7.794857e-17	7.108809e-17	6.497507e-17	5.951309e-17	5.461987e-17	5.022500e-17
14.9	6.634935e-17	6.017191e-17	5.470470e-17	4.985155e-17	4.553110e-17	4.167420e-17	3.822192e-17	3.512384e-17
15.0	4.660648e-17	4.223145e-17	3.836313e-17	3.493252e-17	3.188123e-17	2.915975e-17	2.672588e-17	2.454356e-17

Table 2.b: Values of $\sigma(u,v) = G(1/u, 1/v)$ for $10 \leq u \leq 15$; $7.3 \leq v \leq 8.0$.

u	v							
	8.1	**8.2**	**8.3**	**8.4**	**8.5**	**8.6**	**8.7**	**8.8**
10.0	3.559109e-10	3.281966e-10	3.022081e-10	2.778045e-10	2.548590e-10	2.332569e-10	2.128945e-10	1.936777e-10
10.1	2.665554e-10	2.461817e-10	2.270902e-10	2.091754e-10	1.923426e-10	1.765058e-10	1.615875e-10	1.475175e-10
10.2	1.990444e-10	1.840836e-10	1.700744e-10	1.569379e-10	1.446031e-10	1.330059e-10	1.220884e-10	1.117983e-10
10.3	1.482180e-10	1.372441e-10	1.269756e-10	1.173535e-10	1.083248e-10	9.984165e-11	9.186095e-11	8.434361e-11
10.4	1.100791e-10	1.020384e-10	9.452002e-11	8.747982e-11	8.087831e-11	7.467986e-11	6.885233e-11	6.336666e-11
10.5	8.154913e-11	7.566404e-11	7.016513e-11	6.501961e-11	6.019803e-11	5.567387e-11	5.142323e-11	4.742450e-11
10.6	6.026933e-11	5.596654e-11	5.194899e-11	4.819228e-11	4.467449e-11	4.137593e-11	3.827882e-11	3.536713e-11
10.7	4.444092e-11	4.129832e-11	3.836618e-11	3.562635e-11	3.306253e-11	3.066011e-11	2.840590e-11	2.628801e-11
10.8	3.269808e-11	3.040525e-11	2.826753e-11	2.627142e-11	2.440485e-11	2.265696e-11	2.101798e-11	1.947911e-11
10.9	2.400785e-11	2.233676e-11	2.077984e-11	1.932709e-11	1.796956e-11	1.669921e-11	1.550880e-11	1.439182e-11
11.0	1.759189e-11	1.637519e-11	1.524245e-11	1.418625e-11	1.319996e-11	1.227763e-11	1.141391e-11	1.060401e-11
11.1	1.286570e-11	1.198074e-11	1.115745e-11	1.039034e-11	9.674496e-12	9.005535e-12	8.379505e-12	7.792856e-12
11.2	9.391755e-12	8.748736e-12	8.150961e-12	7.594375e-12	7.075353e-12	6.590651e-12	6.137358e-12	5.712856e-12
11.3	6.843541e-12	6.376785e-12	5.943188e-12	5.539757e-12	5.163816e-12	4.812975e-12	4.485086e-12	4.178225e-12
11.4	4.978084e-12	4.639609e-12	4.325411e-12	4.033282e-12	3.761250e-12	3.507553e-12	3.270612e-12	3.049011e-12
11.5	3.615057e-12	3.369848e-12	3.142394e-12	2.931068e-12	2.734419e-12	2.551149e-12	2.380100e-12	2.220228e-12
11.6	2.620974e-12	2.443504e-12	2.279006e-12	2.126282e-12	1.984265e-12	1.852002e-12	1.728640e-12	1.613416e-12
11.7	1.897256e-12	1.768937e-12	1.650085e-12	1.539819e-12	1.437356e-12	1.341995e-12	1.253113e-12	1.170149e-12
11.8	1.371278e-12	1.278585e-12	1.192794e-12	1.113260e-12	1.039405e-12	9.707175e-13	9.067393e-13	8.470602e-13
11.9	9.896459e-13	9.227517e-13	8.608849e-13	8.035708e-13	7.503876e-13	7.009596e-13	6.549516e-13	6.120635e-13
12.0	7.131931e-13	6.649626e-13	6.203899e-13	5.791274e-13	5.408660e-13	5.053309e-13	4.722768e-13	4.414847e-13
12.1	5.132444e-13	4.785027e-13	4.464198e-13	4.167410e-13	3.892405e-13	3.637173e-13	3.399922e-13	3.179053e-13
12.2	3.688476e-13	3.438453e-13	3.207737e-13	2.994466e-13	2.796988e-13	2.613837e-13	2.443704e-13	2.285425e-13
12.3	2.647222e-13	2.467455e-13	2.301694e-13	2.148578e-13	2.006902e-13	1.875596e-13	1.753706e-13	1.640384e-13
12.4	1.897444e-13	1.768308e-13	1.649322e-13	1.539494e-13	1.437944e-13	1.343893e-13	1.256646e-13	1.175586e-13
12.5	1.358300e-13	1.265619e-13	1.180286e-13	1.101579e-13	1.028856e-13	9.615510e-14	8.991579e-14	8.412278e-14
12.6	9.711449e-14	9.046860e-14	8.435430e-14	7.871886e-14	7.351568e-14	6.870345e-14	6.424551e-14	6.010922e-14
12.7	6.934988e-14	6.458855e-14	6.021138e-14	5.617999e-14	5.246050e-14	4.902290e-14	4.584057e-14	4.288983e-14
12.8	4.946438e-14	4.605620e-14	4.292538e-14	4.004400e-14	3.738747e-14	3.493400e-14	3.266428e-14	3.056116e-14
12.9	3.523999e-14	3.280253e-14	3.056511e-14	2.850750e-14	2.661181e-14	2.486226e-14	2.324486e-14	2.174719e-14
13.0	2.507759e-14	2.333587e-14	2.173831e-14	2.027022e-14	1.891864e-14	1.767214e-14	1.652058e-14	1.545499e-14
13.1	1.782597e-14	1.658246e-14	1.544275e-14	1.439618e-14	1.343336e-14	1.254603e-14	1.172685e-14	1.096934e-14
13.2	1.265748e-14	1.177043e-14	1.095804e-14	1.021260e-14	9.527310e-15	8.896194e-15	8.313958e-15	7.775915e-15
13.3	8.977959e-15	8.345721e-15	7.767136e-15	7.236625e-15	6.749280e-15	6.300779e-15	5.887303e-15	5.505469e-15
13.4	6.361405e-15	5.911157e-15	5.499434e-15	5.122201e-15	4.775916e-15	4.457458e-15	4.164074e-15	3.893326e-15
13.5	4.502794e-15	4.182417e-15	3.889676e-15	3.621659e-15	3.375809e-15	3.149877e-15	2.941878e-15	2.750059e-15
13.6	3.184000e-15	2.956220e-15	2.748249e-15	2.557985e-15	2.383585e-15	2.223428e-15	2.076087e-15	1.940300e-15
13.7	2.249228e-15	2.087416e-15	1.939788e-15	1.804831e-15	1.681217e-15	1.567781e-15	1.463494e-15	1.367451e-15
13.8	1.587345e-15	1.472488e-15	1.367780e-15	1.272131e-15	1.184586e-15	1.104306e-15	1.030553e-15	9.626763e-16
13.9	1.119164e-15	1.037702e-15	9.634961e-16	8.957608e-16	8.338098e-16	7.770408e-16	7.249241e-16	6.769927e-16
14.0	7.883298e-16	7.305993e-16	6.780515e-16	6.301222e-16	5.863181e-16	5.462069e-16	5.094088e-16	4.755891e-16
14.1	5.547795e-16	5.138995e-16	4.767183e-16	4.428306e-16	4.118824e-16	3.835637e-16	3.576023e-16	3.337586e-16
14.2	3.900657e-16	3.611406e-16	3.348530e-16	3.109121e-16	2.890641e-16	2.690867e-16	2.507853e-16	2.339884e-16
14.3	2.740099e-16	2.535597e-16	2.349885e-16	2.180880e-16	2.026764e-16	1.885945e-16	1.757031e-16	1.638796e-16
14.4	1.923145e-16	1.778672e-16	1.647576e-16	1.528364e-16	1.419735e-16	1.320550e-16	1.229815e-16	1.146654e-16
14.5	1.348592e-16	1.246607e-16	1.154136e-16	1.070112e-16	9.936033e-17	9.237976e-17	8.599835e-17	8.015367e-17
14.6	9.448833e-17	8.729448e-17	8.077690e-17	7.485915e-17	6.947473e-17	6.456560e-17	6.008102e-17	5.597648e-17
14.7	6.614693e-17	6.107641e-17	5.648612e-17	5.232148e-17	4.853498e-17	4.508524e-17	4.193608e-17	3.905580e-17
14.8	4.626799e-17	4.269676e-17	3.946630e-17	3.653762e-17	3.387685e-17	3.145449e-17	2.924477e-17	2.722512e-17
14.9	3.233672e-17	2.982334e-17	2.755157e-17	2.549360e-17	2.362529e-17	2.192562e-17	2.037625e-17	1.896115e-17
15.0	2.258191e-17	2.081434e-17	1.921795e-17	1.777290e-17	1.646200e-17	1.527031e-17	1.418477e-17	1.319399e-17

Table 2.c: Values of $\sigma(u,v) = G(1/u, 1/v)$ for $10 \leq u \leq 15$; $8.1 \leq v \leq 8.8$.

6 Error Analysis

In this section, we consider the question of how closely asymptotic distributions such as ρ and σ approximate actual smoothness probabilities. We will show, in a certain sense, that if ρ is a good approximation to the smoothness distribution, then σ is a good approximation to the semi-smoothness distribution.

We first consider the question of whether $x\rho(u)$ is a good approximation to $\Psi(x, x^{1/u})$. This is of practical importance since asymptotic relations such as $x\rho(u) \sim \Psi(x, x^{1/u})$ do not guarantee that $\rho(u)$ is a good approximation to the probability of $1/u$-smoothness for any numbers of practical interest.

For example, from results of Ramaswami [14] (cited as equations 3.7 and 3.8 of [11]) and Knuth and Trabb Pardo [4], we know that

$$\Psi(x, x^{1/u}) = x\rho(u) + \frac{x(1-\gamma)\rho(u-1)}{\log x} + O(\frac{x}{\log^2 x}),$$

and therefore

$$\frac{\Psi(x, x^{1/u})}{x\rho(u)} = 1 + \frac{\rho(u-1)}{\rho(u)}\frac{(1-\gamma)}{\log x} + O(\frac{1}{\rho(u)\log^2 x}).$$

(Here $\gamma = 0.5772...$ is Euler's constant.) The unknown part of the relative error is

$$O(\frac{1}{\rho(u)\log^2 x}). \tag{6.1}$$

Taking the crude approximation $\rho(u) \approx u^{-u}$, we note that for (6.1) to be small, we need $\log x \gg u^{u/2}$. This is not likely to be attained in practical situations; for example, if $u = 7.5$ and $x = 10^{60}$, we have $(u^{-u}\log^2 x)^{-1} = 191.5$.

On the other hand, accurate tables of $\rho(u)$ have been available for at least two decades, going well beyond the values of u needed to evaluate current factoring methods. As far as we know, no discrepancy has been observed between values of the rho function and smoothness probabilities, in the range of interest to algorithm designers. For example, Table 3 below exhibits smooth number counts found by Odlyzko (from [15]); as soon as the predicted count of smooth numbers is moderately large, one finds reasonable agreement with the rho function. (We note that Odlyzko only counted numbers whose prime power factors are small, a definition more stringent than ours.)

k	count	$u = \frac{\log(10^{15})}{\log(2^k)}$	$10^5\rho(u)$	ratio
6	0	8.305	0.001144	0.000
7	0	7.118	0.05981	0.000
8	1	6.229	0.9810	1.019
9	6	5.537	7.727	0.777
10	27	4.983	37.18	0.726
11	110	4.530	126.6	0.869
12	326	4.152	336.0	0.970
13	691	3.833	739.3	0.935
14	1425	3.559	1416	1.006
15	2416	3.322	2425	0.996
16	3852	3.114	3816	1.009
17	5691	2.931	5616	1.013
18	7979	2.768	7823	1.020

Table 3: Counts of even 2^k-smooth numbers in $[10^{15}, 10^{15} + 2 \times 10^5]$.

Therefore we will simply take as given that ρ is a good approximation to smoothness probabilities; investigating this question further is beyond the scope of this paper. We proceed from this assumption to study the question of when $\sigma(u, v)$ is a good approximation to $\Psi(x, x^{1/u}, x^{1/v})/x$.

The following theorem states that if F is a good approximation to the smoothness distribution, then G is a good approximation to the semi-smoothness distribution. In this result, α and β satisfy $0 < \alpha < \beta < 1$, and $\rho(x)$ is extended to be 1 for negative numbers.

Theorem 6.1 *Assume the Riemann hypothesis. Choose c_1 and c_2 so that*

$$c_1 \leq \frac{\Psi(t, t^\gamma)}{tF(\gamma)} \leq c_2$$

whenever $\frac{\alpha}{1-\alpha} \leq \gamma \leq \frac{\alpha}{1-\beta}$ and $t \geq x^{1-\beta}$. Then if $x^\alpha \geq 2,657$, we have

$$c_1(1-\Delta) \leq \frac{\Psi(x, x^\beta, x^\alpha)}{xG(\alpha, \beta)} \leq c_2(1+\Delta)$$

where

$$|\Delta| \leq \frac{\beta}{4\pi G(\alpha, \beta)} \left[2\rho(\frac{1-\beta}{\alpha}) + \frac{\rho(\frac{1-\alpha-\beta}{\alpha})}{(1-\beta)\log x} \right] \frac{\log x}{x^{\alpha/2}}. \tag{6.2}$$

Proof. From (3.6) and (3.7) we obtain

$$\Psi(x, x^\beta, x^\alpha) = \Psi(x, x^\alpha) + \sum_{x^\alpha < p \le x^\beta} \Psi(x/p, (x/p)^{\frac{\alpha}{1-\log p/\log x}}). \tag{6.3}$$

From the definition of c_2, plus (3.9) and (6.3), we have

$$\begin{aligned} c_2^{-1}\Psi(x, x^\beta, x^\alpha) &\le xF(\alpha) + x \sum_{x^\alpha < p \le x^\beta} \frac{1}{p} F(\frac{\alpha}{1 - \log p/\log x}) \\ &= xF(\alpha) + x \int_{x^\alpha}^{x^\beta} \rho(\frac{1 - \log t/\log x}{\alpha}) \frac{d\pi(t)}{t}. \end{aligned}$$

Using (3.4) and (3.10), and writing $\lambda(t) = \log t/\log x$, we have

$$\begin{aligned} c_2^{-1}\Psi(x, x^\beta, x^\alpha) &\le xF(\alpha) + x \int_{x^\alpha}^{x^\beta} \rho(\frac{1-\lambda(t)}{\alpha}) \frac{dt}{t \log t} + xE_1(\alpha, \beta, x) + xE_2(\alpha, \beta, x) \\ &= xG(\alpha, \beta) + xE_1(\alpha, \beta, x) + xE_2(\alpha, \beta, x) \end{aligned} \tag{6.4}$$

where

$$E_1(\alpha, \beta, x) = \left[\rho(\frac{1-\lambda(t)}{\alpha}) \frac{\epsilon(t)}{t}\right]_{x^\alpha}^{x^\beta} = \rho(\frac{1-\beta}{\alpha}) \frac{\epsilon(x^\beta)}{x^\beta} - \rho(\frac{1-\alpha}{\alpha}) \frac{\epsilon(x^\alpha)}{x^\alpha} \tag{6.5}$$

and

$$\begin{aligned} E_2(\alpha, \beta, x) &= -\int_{x^\alpha}^{x^\beta} \frac{d}{dt}(\frac{1}{t}\rho(\frac{1-\lambda(t)}{\alpha}))\epsilon(t)dt \\ &= \int_{x^\alpha}^{x^\beta} \epsilon(t)t^{-2}[\rho(\frac{1-\lambda(t)}{\alpha}) + \rho'(\frac{1-\lambda(t)}{\alpha})/(\alpha \log x)]dt. \end{aligned} \tag{6.6}$$

Schoenfeld's bound (2.4) (which assumes the Riemann hypothesis) and (6.5) imply

$$|E_1| \le \frac{\log x}{8\pi} \left[\rho(\frac{1-\beta}{\alpha})\beta x^{-\beta/2} + \rho(\frac{1-\alpha}{\alpha})\alpha x^{-\alpha/2}\right] \le \frac{\log x}{4\pi} \left[\rho(\frac{1-\beta}{\alpha})\beta x^{-\alpha/2}\right]. \tag{6.7}$$

Similarly, but using (2.2) and (6.6), we have

$$|E_2| \le \int_{x^\alpha}^{x^\beta} \frac{\log t}{8\pi t^{3/2}} \left[\rho(\frac{1-\lambda(t)}{\alpha}) + \rho(\frac{1-\lambda(t)}{\alpha} - 1)/(\log x - \log t)\right] dt.$$

So far we have assumed that $\rho(x) = 0$ when $x < 0$. If we redefine $\rho(x)$ to be 1 when $x < 0$, the inequality above still holds, and we have made ρ monotonic. Using this new extension of ρ, we find

$$|E_2| \le \frac{A}{8\pi} \int_{x^\alpha}^{x^\beta} t^{-3/2} \log t \; dt \le \frac{A\beta \log x}{8\pi} \int_{x^\alpha}^{\infty} t^{-3/2} dt = \frac{A\beta \log x}{4\pi} x^{-\alpha/2}, \tag{6.8}$$

where A denotes the expression

$$\rho(\frac{1-\beta}{\alpha}) + \rho(\frac{1-\alpha-\beta}{\alpha})\frac{1}{(1-\beta)\log x}.$$

Letting

$$\Delta(\alpha,\beta,x) = \frac{(E_1+E_2)}{G(\alpha,\beta)},$$

(6.4), the inequalities (6.7) and (6.8), and a little algebra give the upper bound in the theorem. The lower bound is proved by an entirely analogous argument starting with the estimate $\Psi(t,t^\gamma) \geq c_1 t F(\gamma)$. ■

Using Theorem 6.1, the extra relative error incurred by using the asymptotic two-dimensional smoothness distribution can be explicitly estimated. For example, if $x \approx 10^{60}$, $\alpha = \frac{1}{12}$, and $\beta = \frac{1}{7.5}$ then (6.2) gives $|\Delta| \leq 0.062$.

We also remark that Theorem 6.1 can be improved slightly at some cost in readability. For example, the first inequalities in (6.7) and (6.8) could be used directly (note that the first integral in (6.8) can be expressed in closed form).

In a certain sense, Theorem 6.1 ascribes most of the error in the approximation

$$\Psi(x,x^\alpha,x^\beta) \approx xG(\alpha,\beta)$$

to the use of the rho function. Hildebrand [7] proved that if the Riemann hypothesis holds, then

$$\Psi(x,x^\alpha) = xF(\alpha)\left(1 + O(\frac{\log(\alpha^{-1})}{\alpha\log x})\right), \tag{6.9}$$

as $x \to \infty$. However, Theorem 6.1 and equation (3.4) imply that

$$\Delta = O(\frac{\log x}{x^{\alpha/2}}),$$

which is asymptotically much smaller than the relative error in (6.9).

References

[1] E. Bach. How to generate factored random numbers. *SIAM J. Computing*, 17:179–193, 1988.

[2] N. G. de Bruijn. On the number of positive integers $\leq x$ and free of prime factors $> y$. *Indag. Math*, 13:50–60, 1951.

[3] J.-M.-F. Chamayou. A probabilistic approach to a differential-difference equation arising in analytic number theory. *Math. Comp.*, 27:197–203, 1973.

[4] D. Knuth and L. Trabb Pardo. Analysis of a simple factorization algorithm. *Theoretical Computer Science*, 3:321–348, 1976.

[5] G. Kolesnik and E. G. Strauss. On the first occurrence of values of a character. *Transactions of the American Mathematical Society*, 246:385–394, December 1978.

[6] A.K. Lenstra and M.S. Manasse. Factoring by electronic mail. In *EUROCRYPT 89*, volume 434 of Lecture Notes in Computer Science, pages 355–371. Springer-Verlag, 1990.

[7] A. Hildebrand. Integers free of large prime factors and the Riemann hypothesis. *Mathematika*, 31:258-271, 1984.

[8] J. van de Lune and E. Wattel. On the numerical solution of a differential-difference equation arising in analytic number theory. *Math. Comp.*, 23:417–421, 1969.

[9] P. L. Montgomery. *An FFT extension of the elliptic curve method of factorization.* Ph.D. thesis, University of California - Los Angeles, 1992.

[10] P. L. Montgomery and R. D. Silverman. An FFT extension to the $p-1$ factoring algorithm. *Mathematics of Computation*, 54(190):839–854, 1990.

[11] K. K. Norton. Numbers with small prime factors, and the least k-th power non-residue. *Memoirs of the American Mathematical Society*, 106, 1971.

[12] N. Patterson. Letter to Eric Bach, November 1988.

[13] C. Pomerance. The quadratic sieve factoring algorithm. In *EUROCRYPT '84*, volume 209 of Lecture Notes in Computer Science, pages 169-182. Springer-Verlag, 1985.

[14] V. Ramaswami. The number of positive integers $< x$ and free of prime divisors $> x^c$, and a problem of S.S. Pillai. *Duke Math. Journal*, 16:99–109, 1949.

[15] C.-P. Schnorr and H. W. Lenstra, Jr. A Monte Carlo factoring algorithm with linear storage. *Mathematics of Computation*, 43:289–311, 1984.

[16] L. Schoenfeld. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II. *Mathematics of Computation*, 30:337–360, 1976.

[17] E. C. Titchmarsh, *The Theory of Functions.* Second Edition, Oxford Univ. Press, 1939.