# INTEGERS WITH A LARGE SMOOTH DIVISOR

**William D. Banks**
*Department of Mathematics, University of Missouri, Columbia, MO 65211, USA*
bbanks@math.missouri.edu

**Igor E. Shparlinski**
*Department of Computing, Macquarie University, Sydney, NSW 2109, Australia*
igor@ics.mq.edu.au

*Received: 7/19/06, Revised: 1/31/07, Accepted: 2/2/07, Published: 4/3/07*

## Abstract

We study the function $\Theta(x, y, z)$ that counts the number of positive integers $n \le x$ which have a divisor $d > z$ with the property that $p \le y$ for every prime $p$ dividing $d$. We also indicate some cryptographic applications of our results.

## 1. Introduction

For every integer $n \ge 2$, let $P^+(n)$ and $P^-(n)$ denote the largest and the smallest prime factor of $n$, respectively, and put $P^+(1) = 1$, $P^-(1) = \infty$. For real numbers $x, y \ge 1$, let $\Psi(x, y)$ and $\Phi(x, y)$ denote the counting functions of the sets of *$y$-smooth numbers* and *$y$-rough numbers*, respectively; that is,

$$\Psi(x, y) = \#\{n \le x \ : \ P^+(n) \le y\} \qquad \text{and} \qquad \Phi(x, y) = \#\{n \le x \ : \ P^-(n) > y\}.$$

For a very wide range in the $xy$-plane, it is known that

$$\Psi(x, y) \sim \varrho(u)\, x \qquad \text{and} \qquad \Phi(x, y) \sim \omega(u)\, \frac{x}{\log y},$$

where $u$ denotes the ratio $(\log x)/\log y$, $\varrho(u)$ is the *Dickman function*, and $\omega(u)$ is the *Buchstab function*; the definitions and certain analytic properties of $\varrho(u)$ and $\omega(u)$ are reviewed in Sections 2 and 3 below.

In this paper, our principal object of study is the function $\Theta(x, y, z)$ that counts positive integers $n \le x$ for which there exists a divisor $d \mid n$ with $d > z$ and $P^+(d) \le y$; in other words,

$$\Theta(x, y, z) = \#\{n \le x \ : \ n_y > z\},$$

where $n_y$ denotes the largest $y$-smooth divisor of $n$. The function $\Theta(x, y, z)$ has been previously studied in the literature; see [1, 6, 7, 8].

For $x, y, z$ varying over a wide domain, we derive the first two terms of the asymptotic expansion of $\Theta(x, y, z)$. We show that the main term can be naturally defined in terms of the *partial convolution* $\mathcal{C}_{\omega,\varrho}(u, v)$ of $\varrho$ with $\omega$, which is defined by

$$\mathcal{C}_{\omega,\varrho}(u, v) = \int_v^\infty \omega(u - s)\varrho(s)\, ds.$$

Using precise estimates for $\Psi(x, y)$ and $\Phi(x, y)$, we also identify the second term of the asymptotic expansion of $\Theta(x, y, z)$, which is naturally expressed in terms of the partial convolution $\mathcal{C}_{\omega,\varrho'}(u, v)$ of $\varrho'$ with $\omega$:

$$\mathcal{C}_{\omega,\varrho'}(u, v) = \int_v^\infty \omega(u - s)\varrho'(s)\, ds.$$

**Theorem 1.** *For fixed $\varepsilon > 0$ and uniformly in the domain*

$$x \geq 3, \qquad y \geq \exp\{(\log\log x)^{5/3+\varepsilon}\}, \qquad y \log y \leq z \leq x/y,$$

*we have*

$$\Theta(x, y, z) = \big(\varrho(u) + \mathcal{C}_{\omega,\varrho}(u, v)\big)x - \gamma\, \mathcal{C}_{\omega,\varrho'}(u, v)\, \frac{x}{\log y} + O\big(\mathcal{E}(x, y, z)\big),$$

*where $u = (\log x)/\log y$, $v = (\log z)/\log y$, $\gamma$ is the Euler-Mascheroni constant, and*

$$\mathcal{E}(x, y, z) = \frac{x}{\log y}\left\{\varrho(u - 1) + \frac{\varrho(v)\log(v + 1)}{\log y} + \frac{\varrho(v)}{\log(v + 1)}\right\}.$$

Similar results have been obtained concomitantly, using a more elaborate approach, by Tenenbaum [8].

The proof of Theorem 1 is given below in Section 4; our principal tools are the estimates of Lemma 4 (Section 2) and Lemma 6 (Section 3). In Section 5, we use the formula of Theorem 1 to give a heuristic prediction for the density of certain integers of cryptographic interest which appear in a work by Menezes [3].

## 2. Integers Free of Large Prime Factors

In this section, we collect various estimates for the counting function $\Psi(x, y)$ of *$y$-smooth numbers*:

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

As usual, we denote by $\varrho(u)$ the *Dickman function*; it is continuous at $u = 1$, differentiable for $u > 1$, and it satisfies the differential-difference equation

$$u\varrho'(u) + \varrho(u-1) = 0 \qquad (u > 1), \tag{1}$$

along with the initial condition $\varrho(u) = 1$ $(0 \le u \le 1)$. It is convenient to define $\varrho(u) = 0$ for all $u < 0$ so that (1) is satisfied for $u \in \mathbb{R} \setminus \{0, 1\}$, and we also define $\varrho'(u)$ by right-continuity at $u = 0$ and $u = 1$. For a discussion of the analytic properties of $\varrho(u)$, we refer the reader to [6, Chapter III.5].

We need the following well known estimate for $\Psi(x, y)$, which is due to Hildebrand [2] (see also [6, Corollary 9.3, Chapter III.5]):

**Lemma 1.** *For fixed $\varepsilon > 0$ and uniformly in the domain*

$$x \ge 3, \qquad x \ge y \ge \exp\{(\log\log x)^{5/3+\varepsilon}\},$$

*we have*

$$\Psi(x, y) = \varrho(u)\, x \left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\},$$

*where $u = (\log x)/\log y$.*

We also need the following extension of Lemma 1, which is a special case of the results of Saias [5]:

**Lemma 2.** *For fixed $\varepsilon > 0$ and uniformly in the domain*

$$x \ge 3, \qquad y \ge \exp\{(\log\log x)^{5/3+\varepsilon}\}, \qquad x \ge y \log y,$$

*the following estimate holds:*

$$\Psi(x, y) = \varrho(u)\, x + (\gamma - 1)\varrho'(u)\,\frac{x}{\log y} + O\left(\varrho''(u)\frac{x}{\log^2 y}\right),$$

*where $u = (\log x)/\log y$.*

The following lemma provides a precise estimate for the sum

$$S(y, z) = \sum_{\substack{d > z \\ P^+(d) \le y}} \frac{1}{d}$$

over a wide range, which is used in the proofs of Lemmas 4 and 6 below. The sum $S(y, z)$ has been previously studied; see, for example, [7].

**Lemma 3.** *For fixed* $\varepsilon > 0$ *and uniformly in the domain*

$$y \geq 3, \qquad 1 \leq z \leq \exp\exp\{(\log y)^{3/5-\varepsilon}\},$$

*we have*

$$S(y,z) = \tau(v)\log y - \gamma\varrho(v) + O\big(E(y,z)\big),$$

*where* $v = (\log z)/\log y$,

$$\tau(v) = \int_v^\infty \varrho(s)\,ds,$$

*and*

$$E(y,z) = \begin{cases} \dfrac{\varrho(v)\log(v+1)}{\log y} & \text{if } z \geq y\log y; \\[2ex] \dfrac{1}{z} + \dfrac{\log\log y}{\log y} & \text{if } z < y\log y. \end{cases}$$

*Proof.* Let $Y = y\log y$. First, suppose that $z > Y$, and put $T = \dfrac{\exp\{(\log y)^{3/5-\varepsilon/2}\}}{\log y}$. By partial summation, it follows that

$$\begin{aligned} S(y,z) &= \sum_{\substack{z<d\leq y^T \\ P^+(d)\leq y}} \frac{1}{d} + S(y,y^T) \\ &= \frac{\Psi(y^T,y)}{y^T} - \frac{\Psi(z,y)}{z} + \log y \int_v^T \frac{\Psi(y^s,y)}{y^s}\,ds + S(y,y^T). \end{aligned} \tag{2}$$

By Lemma 1, we have the estimate $\dfrac{\Psi(z,y)}{z} = \varrho(v) + O\left(\dfrac{\varrho(v)\log(v+1)}{\log y}\right)$.

We now recall that

$$\varrho(w) = \exp\left(-w\log w + O(w\log\log w)\right); \tag{3}$$

see [5, Lemma 3(iv)]. Thus, by our choice of $T$ we have

$$\varrho(T) = \exp\left\{-(1+o(1))\frac{\exp\{(\log y)^{3/5-\varepsilon/2}\}}{(\log y)^{2/5+\varepsilon/2}}\right\}.$$

On the other hand, since $v \leq \log z \leq \exp\{(\log y)^{3/5-\varepsilon}\}$, it follows that

$$\begin{aligned} \frac{\varrho(v)\log(v+1)}{\log y} &= \frac{\exp\left(-v\log v + O(v\log\log v)\right)}{\log y} \\ &\geq \exp\left\{-(1+o(1))\exp\{(\log y)^{3/5-\varepsilon}\}(\log y)^{3/5-\varepsilon}\right\}. \end{aligned}$$

Therefore,

$$\frac{\Psi(y^T,y)}{y^T} \ll \varrho(T) \ll \frac{\varrho(v)\log(v+1)}{\log y}. \tag{4}$$

The following bound is given in the proof of [7, Corollary 2]:

$$S(y, y^T) = \sum_{\substack{d>y^T \\ P^+(d)\le y}} \frac{1}{d} \ll \varrho(T)e^{\varepsilon T} + y^{-(1-\varepsilon)T},$$

from which we deduce that

$$S(y, y^T) \ll \frac{\varrho(v)\log(v+1)}{\log y}. \tag{5}$$

To estimate the integral in (2), we apply Lemma 2 and write

$$\int_v^T \frac{\Psi(y^s, y)}{y^s}\, ds = I_1 + I_2 + O(I_3),$$

where

$$\begin{aligned} I_1 &= \int_v^T \varrho(s)\, ds = \tau(v) - \tau(T), \\ I_2 &= \frac{(\gamma-1)}{\log y}\int_v^T \varrho'(s)\, ds = \frac{(\gamma-1)(\varrho(T)-\varrho(v))}{\log y}, \\ I_3 &= \frac{1}{\log^2 y}\int_v^T \varrho''(s)\, ds = \frac{\varrho'(T)-\varrho'(v)}{\log^2 y}. \end{aligned}$$

Using (1) together with [6, Lemma 8.1 and bound (61), Chapter III.5] we see that $|\varrho'(v)| \asymp \varrho(v)\log(v+1)$. Furthermore, as in our derivation of (4), we see that (3) yields

$$\tau(T) \ll \varrho(T) \ll \frac{\varrho(v)\log(v+1)}{\log^2 y}.$$

Therefore,

$$\int_v^T \frac{\Psi(y^s, y)}{y^s}\, ds = \tau(v) - \frac{(\gamma-1)\varrho(v)}{\log y} + O\left(\frac{\varrho(v)\log(v+1)}{\log^2 y}\right). \tag{6}$$

Inserting the estimates (4), (5), and (6) into (2), we obtain the desired estimate when $z > Y$.

Next, suppose that $y \le z \le Y$, and put $V = \frac{\log Y}{\log y} = 1 + \frac{\log\log y}{\log y}$. Since $\varrho(s) = 1 - \log s$ for $1 \le s \le 2$, we have $1 \ge \varrho(v) \ge \varrho(V) = 1 + O\left(\frac{\log\log y}{\log y}\right)$; therefore,

$$\varrho(v) - \varrho(V) \ll \frac{\log\log y}{\log y}. \tag{7}$$

By partial summation, it follows that

$$\begin{aligned} S(y, z) &= \sum_{\substack{z<d\le Y \\ P^+(d)\le y}} \frac{1}{d} + S(y, Y) \\ &= \frac{\Psi(Y, y)}{Y} - \frac{\Psi(z, y)}{z} + \log y \int_v^V \frac{\Psi(y^s, y)}{y^s}\, ds + S(y, Y). \end{aligned} \tag{8}$$

Using Lemma 1 together with (7), it follows that

$$\frac{\Psi(Y,y)}{Y} - \frac{\Psi(z,y)}{z} = \varrho(V) - \varrho(v) + O\left(\frac{1}{\log y}\right) \ll \frac{\log\log y}{\log y}. \tag{9}$$

Applying the estimate from the previous case, we also have

$$S(y,Y) = \tau(V)\log Y - \gamma\varrho(V) + O\left(\frac{1}{\log y}\right). \tag{10}$$

To estimate the integral in (8), we use Lemma 1 again and write

$$\int_v^V \frac{\Psi(y^s,y)}{y^s}\,ds = I_4 + O(I_5),$$

where

$$\begin{aligned} I_4 &= \int_v^V \varrho(s)\,ds = \tau(v) - \tau(V), \\ I_5 &= \frac{1}{\log y}\int_v^V ds = \frac{\log(Y/z)}{\log^2 y} \ll \frac{\log\log y}{\log^2 y}. \end{aligned}$$

Therefore,

$$\int_v^V \frac{\Psi(y^s,y)}{y^s}\,ds = \tau(v) - \tau(V) + O\left(\frac{\log\log y}{\log^2 y}\right). \tag{11}$$

Inserting the estimates (9), (10) and (11) into (8), and taking into account (7), we obtain the stated estimate for $y \le z \le Y$.

Finally, suppose that $1 \le z < y$. In this case,

$$S(y,z) = \sum_{z<d\le y}\frac{1}{d} + S(y,y). \tag{12}$$

By partial summation, we have

$$\begin{aligned} \sum_{z<d\le y}\frac{1}{d} &= \log y - \log z + O(z^{-1}) = (1-v)\log y + O(z^{-1}) \\ &= \log y\int_v^1 \varrho(s)\,ds + O(z^{-1}) = (\tau(v)-\tau(1))\log y + O(z^{-1}). \end{aligned}$$

Applying the estimate from the previous case, we also have

$$S(y,y) = \tau(1)\log y - \gamma\varrho(1) + O\left(\frac{\log\log y}{\log y}\right).$$

Inserting these estimates into (12), and using the fact that $\varrho(v) = \varrho(1) = 1$, we obtain the desired result. □

**Lemma 4.** *For fixed* $\varepsilon > 0$ *and uniformly in the domain*

$$x \geq 3, \qquad y \geq \exp\{(\log\log x)^{5/3+\varepsilon}\}, \qquad 1 \leq z \leq x/y,$$

*we have*

$$\sum_{\substack{z<d\leq x/y \\ P^+(d)\leq y}} \frac{\varrho(u-u_d)}{d} \ll \mathcal{C}_{\varrho,\varrho}(u,v)\log(u+1) + \varrho(u-v)\varrho(v) + \varrho(u-1),$$

*where* $u = (\log x)/\log y$, $v = (\log z)/\log y$, $u_d = (\log d)/\log y$ *for every integer* $d$ *in the sum, and*

$$\mathcal{C}_{\varrho,\varrho}(u,v) = \int_v^\infty \varrho(u-s)\varrho(s)\,ds.$$

*Proof.* By partial summation, we have

$$\sum_{\substack{z<d\leq x/y \\ P^+(d)\leq y}} \frac{\varrho(u-u_d)}{d} = S(y,x/y) - \varrho(u-v)S(y,z) + \int_v^{u-1} \varrho'(u-s)S(y,y^s)\,ds.$$

Lemma 3 implies that

$$S(y,x/y) = \tau(u-1)\log y + O\big(\varrho(u-1)\big),$$
$$S(y,z) = \tau(v)\log y + O\big(\varrho(v)\big),$$

and

$$\int_v^{u-1} \varrho'(u-s)S(y,y^s)\,ds = I_1 \log y + O(I_2),$$

where

$$I_1 = \int_v^{u-1} \varrho'(u-s)\tau(s)\,ds = \varrho(u-v)\tau(v) - \tau(u-1) + \mathcal{C}_{\varrho,\varrho}(u,v),$$
$$I_2 = \int_v^{u-1} \big|\varrho'(u-s)\big|\varrho(s)\,ds.$$

Finally, using the bound $\big|\varrho'(t)\big| \ll \varrho(t)\log(t+1)$ (for $t > 1$), we see that

$$I_2 \ll \log(u+1)\int_v^{u-1} \varrho(u-s)\varrho(s)\,ds \leq \mathcal{C}_{\varrho,\varrho}(u,v)\log(u+1).$$

Putting everything together, the result follows. □

## 3. Integers Free of Small Prime Factors

In this section, we collect various estimates for the counting function $\Phi(x,y)$ of *y-rough numbers*:

$$\Phi(x,y) = \#\{n \le x \ : \ P^-(n) > y\}.$$

As usual, we denote by $\omega(u)$ the *Buchstab function*; for $u > 1$, it is the unique continuous solution to the differential-difference equation

$$\big(u\omega(u)\big)' = \omega(u-1) \qquad (u > 2) \tag{13}$$

with initial condition $u\omega(u) = 1$ $(1 \le u \le 2)$. It is convenient to define $\omega(u) = 0$ for all $u < 1$ so that (13) is satisfied for $u \in \mathbb{R} \setminus \{1, 2\}$, and we also define $\omega'(u)$ by right-continuity at $u = 1$ and $u = 2$. For a discussion of the analytic properties of $\omega(u)$, we refer the reader to [6, Chapter III.6]

The next result follows from [6, Corollary 7.5, Chapter III.6]:

**Lemma 5.** *For fixed* $\varepsilon > 0$ *and uniformly in the domain*

$$x \ge 3, \qquad x \ge y \ge \exp\{(\log\log x)^{5/3+\varepsilon}\},$$

*the following estimate holds:*

$$\Phi(x,y) = \big(x\omega(u) - y\big)\frac{e^\gamma}{\zeta(1,y)} + O\left(\frac{x\varrho(u)}{\log^2 y}\right),$$

*where* $u = (\log x)/\log y$, *and* $\zeta(1,y) = \prod_{p\le y}\left(1-p^{-1}\right)^{-1}$.

**Lemma 6.** *For fixed* $\varepsilon > 0$ *and uniformly in the domain*

$$x \ge 3, \qquad y \ge \exp\{(\log\log x)^{5/3+\varepsilon}\}, \qquad 1 \le z \le x/y,$$

*we have*

$$\sum_{\substack{z<d\le x/y\\ P^+(d)\le y}} \frac{\omega(u-u_d)}{d} = \mathcal{C}_{\omega,\varrho}(u,v)\log y - \gamma\,\mathcal{C}_{\omega,\varrho'}(u,v) + O\big(E(y,z)\big),$$

*where* $u = (\log x)/\log y$, $v = (\log z)/\log y$, $u_d = (\log d)/\log y$ *for every integer* $d$ *in the sum, and* $E(y,z)$ *is the error term of Lemma 3.*

*Proof.* By partial summation, it follows that

$$\sum_{\substack{z<d\le x/y\\ P^+(d)\le y}} \frac{\omega(u-u_d)}{d} = S(y,x/y) - \omega(u-v)S(y,z) + \int_v^{u-1} \omega'(u-s)S(y,y^s)\,ds.$$

By Lemma 3 we have the estimates $S(y, x/y) = \tau(u-1)\log y - \gamma\varrho(u-1) + O\big(E(y, x/y)\big)$ and $S(y, z) = \tau(v)\log y - \gamma\varrho(v) + O\big(E(y, z)\big)$. Also,

$$\int_v^{u-1} \omega'(u-s)S(y, y^s)\,ds = I_1 \log y - \gamma I_2 + O(I_3),$$

where

$$\begin{aligned} I_1 &= \int_v^{u-1} \omega'(u-s)\tau(s)\,ds = \omega(u-v)\tau(v) - \tau(u-1) + \mathcal{C}_{\omega,\varrho}(u, v), \\ I_2 &= \int_v^{u-1} \omega'(u-s)\varrho(s)\,ds = \omega(u-v)\varrho(v) - \varrho(u-1) + \mathcal{C}_{\omega,\varrho'}(u, v), \\ I_3 &= \frac{1}{\log y}\int_v^{u-1} \big|\omega'(u-s)\big| E(y, y^s)\,ds. \end{aligned}$$

Putting everything together, we see that the stated estimate follows from the bound

$$E(y, x/y) + \omega(u-v)E(y, z) + I_3 \ll E(y, z). \tag{14}$$

To prove this, observe that $E(y, z_1) \ll E(y, z_2)$ holds for all $z_1 \geq z_2 \geq 1$. Therefore, $E(y, x/y) \ll E(y, z)$, and

$$I_3 \ll \frac{E(y, z)}{\log y}\int_v^{u-1} \big|\omega'(u-s)\big|\,ds \ll \frac{E(y, z)}{\log y}.$$

Taking into account the fact that $\omega(u-v) \asymp 1$, we derive (14), completing the proof. □

## 4. Proof of Theorem 1

For fixed $y$, every positive integer $n$ can be uniquely decomposed as a product $n = de$, where $P^+(d) \leq y$ and $P^-(e) > y$. Therefore,

$$\begin{aligned} \Theta(x, y, z) &= \sum_{\substack{z<d\leq x \\ P^+(d)\leq y}} \sum_{\substack{e\leq x/d \\ P^-(e)>y}} 1 = \sum_{\substack{z<d\leq x \\ P^+(d)\leq y}} \Phi(x/d, y) \\ &= \Psi(x, y) - \Psi(x/y, y) + \sum_{\substack{z<d\leq x/y \\ P^+(d)\leq y}} \Phi(x/d, y). \end{aligned}$$

Using Lemma 1, it follows that $\Psi(x,y)-\Psi(x/y,y) = \varrho(u)\,x + O\left(\frac{\varrho(u-1)\,x}{\log y}\right)$. By Lemma 5, we also have

$$\begin{aligned}\sum_{\substack{z<d\le x/y\\ P^+(d)\le y}} \Phi(x/d,y) &= \sum_{\substack{z<d\le x/y\\ P^+(d)\le y}} \left\{\left(\frac{x\,\omega(u-u_d)}{d} - y\right)\frac{e^\gamma}{\zeta(1,y)} + O\left(\frac{x\varrho(u-u_d)}{d\log^2 y}\right)\right\}\\ &= \frac{e^\gamma x}{\zeta(1,y)} \sum_{\substack{z<d\le x/y\\ P^+(d)\le y}} \frac{\omega(u-u_d)}{d} - \frac{e^\gamma y}{\zeta(1,y)}\big\{\Psi(x/y,y)-\Psi(z,y)\big\} \\ &\quad + \quad O\left(\frac{x}{\log^2 y}\sum_{\substack{z<d\le x/y\\ P^+(d)\le y}} \frac{\varrho(u-u_d)}{d}\right).\end{aligned} \tag{15}$$

Applying Lemma 1 again, we have $-\frac{e^\gamma y}{\zeta(1,y)}\big\{\Psi(x/y,y)-\Psi(z,y)\big\} \ll \frac{\varrho(u-1)\,x}{\log y}$. Inserting the estimates of Lemmas 4 and 6 into (15), and making use of the trivial estimate

$$\mathcal{C}_{\varrho,\varrho}(u,v)\log(u+1) \ll \log y \int_v^\infty \varrho(s)\,ds \ll \frac{\varrho(v)\log y}{\log(v+1)}.$$

it is easy to see that

$$\Theta(x,y,z) = \left(\varrho(u) + \mathcal{C}_{\omega,\varrho}(u,v)\frac{e^\gamma \log y}{\zeta(1,y)}\right)x - \gamma\,\mathcal{C}_{\omega,\varrho'}(u,v)\frac{e^\gamma x}{\zeta(1,y)} + O\big(\mathcal{E}(x,y,z)\big).$$

To complete to proof, we use the estimate (see Vinogradov [9]):

$$\zeta(1,y) = e^\gamma \log y\big(1+\exp\{-c(\log y)^{3/5}\}\big),$$

which holds for some absolute constant $c>0$, together with the trivial estimate

$$\max\big\{\mathcal{C}_{\omega,\varrho}(u,v),\mathcal{C}_{\omega,\varrho'}(u,v)\big\} \ll \int_v^\infty \varrho(s)\,ds \ll \frac{\varrho(v)}{\log(v+1)}.$$

## 5. Cryptographic Applications

Suppose that two primes $p$ and $q$ are selected for use in the *Digital Signature Algorithm* (see, for example, [4]) using the following standard method:

- Select a random $m$-bit prime $q$;
- Randomly generate $k$-bit integers $n$ until a prime $p = 2nq+1$ is reached.

The *large subgroup attack* described in [3, Section 3.2.3] leads one naturally to consider the following question: What is the probability $\eta(k,\ell,m)$ that $n$ has a divisor $s > q$ which is $2^\ell$-smooth?

It is natural to expect that the proportion of those integers in the set $\{2^{k-1} \le n < 2^k\}$ having a large smooth divisor should be roughly the same as the proportion of integers in

$$\left\{2^{k-1} \le n < 2^k \ : \ n = (p-1)/(2q) \text{ for some prime } p \equiv 1 \pmod{2q}\right\}$$

having a large smooth divisor. Accordingly, we expect that the probability $\eta(k,\ell,m)$ is reasonably close to

$$\frac{\Theta(2^k, 2^\ell, 2^m) - \Theta(2^{k-1}, 2^\ell, 2^m)}{2^{k-1}}.$$

Theorem 1 then suggests that $\eta(k,\ell,m) \approx 2\,\wp(k,\ell,m) - \wp(k-1,\ell,m)$, where

$$\wp(k,\ell,m) = \varrho(k/\ell) + \mathcal{C}_{\omega,\varrho}(k/\ell, m/\ell) - \frac{\gamma\,\mathcal{C}_{\omega,\varrho'}(k/\ell, m/\ell)}{\ell \log 2}.$$

In particular, the most interesting choice of parameters at the present time is $k = 863$, $\ell = 80$, and $m = 160$ (which produce a 1024-bit prime $p$); we expect $\eta(863, 80, 160) \approx 0.09576$.

**Acknowledgements.** The authors would like to thank Alfred Menezes for bringing to our attention the cryptographic applications which initially motivated our work. We also thank Gérald Tenenbaum for pointing out a mistake in the original manuscript, and for many subsequent discussions. This work was started during a visit by W. B. to Macquarie University; the support and hospitality of this institution are gratefully acknowledged. During the preparation of this paper, I. S. was supported in part by ARC grant DP0556431.

## References

[1] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge University Press, Cambridge, UK, 1988.

[2] A. Hildebrand, 'On the number of positive integers $\le x$ and free of prime factors $> y$,' *J. Number Theory* **22**, (1986), no. 3, 289–307.

[3] A. J. Menezes, 'Another look at HMQV', *Cryptology ePrint Archive, Report 2005/205*, 2005, 1–15.

[4] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1996.

[5] É. Saias, 'Sur le nombre des entiers sans grand facteur premier,' (French) *J. Number Theory* **32** (1989), no. 1, 78–99.

[6] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, Cambridge, UK, 1995.

[7] G. Tenenbaum, *Crible d'Ératosthéne et modéle de Kubilius*, Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, 1099–1129.

[8] G. Tenenbaum, *Integers with a large friable component*, Preprint, 2006.

[9] A. I. Vinogradov, 'On the remainder in Merten's formula,' (Russian) *Dokl. Akad. Nauk SSSR* **148** (1963), 262–263.