Bounding Smooth Integers (Extended Abstract)

Daniel J. Bernstein
Department of Mathematics, Statistics, and Computer Science (M/C 249)
The University of Illinois at Chicago
Chicago, IL 60607–7045
djb@pobox.com

1 Introduction

An integer is \textit{y-smooth} if it is not divisible by any primes larger than \( y \). Define \( \Psi(x, y) = \# \{ n : 1 \leq n \leq x \text{ and } n \text{ is } y\text{-smooth} \} \). This function \( \Psi \) is used to estimate the speed of various factoring methods; see, e.g., [1, section 10].

Section 4 presents a fast algorithm to compute arbitrarily tight upper and lower bounds on \( \Psi(x, y) \). For example, \( 1.16 \cdot 10^{45} < \Psi(10^{54}, 10^7) < 1.19 \cdot 10^{45} \).

The idea of the algorithm is to bound the relevant Dirichlet series between two power series. Thus bounds are obtained on \( \Psi(x, y) \) for all \( x \) at one fell swoop.

More general functions can be computed in the same way.

Previous work

The literature contains many loose bounds and asymptotic estimates for \( \Psi \); see, e.g., [2], [4], [5], and [9]. Hunter and Sorenson in [6] showed that some of those estimates can be computed quickly.

Acknowledgments

The author was supported by the National Science Foundation under grant DMS–9600083.

2 Discrete generalized power series

A series is a formal sum \( f = \sum_{r \in \mathbb{R}} f_r t^r \) such that, for any \( x \in \mathbb{R} \), there are only finitely many \( r \leq x \) with \( f_r \neq 0 \).

Let \( f = \sum_{r \in \mathbb{R}} f_r t^r \) and \( g = \sum_{r \in \mathbb{R}} g_r t^r \) be series. The sum \( f + g \) is \( \sum_{r \in \mathbb{R}} (f_r + g_r) t^r \). The product \( fg \) is \( \sum_{r \in \mathbb{R}} \sum_{s \in \mathbb{R}} f_s g_{r-s} t^r \).

I write \( f \leq g \) if \( \sum_{r \leq x} f_r \leq \sum_{r \leq x} g_r \) for all \( x \in \mathbb{R} \). If \( h = \sum_{r \in \mathbb{R}} h_r t^r \) is a series with all \( h_r \geq 0 \), then \( fh \leq gh \) whenever \( f \leq g \).
3 Logarithms

Fix a positive real number $\alpha$. This is a scaling factor that determines the speed and accuracy of my algorithm: the time is roughly proportional to $\alpha$, and the error is roughly proportional to $1/\alpha$.

For each prime $p$ select integers $L(p)$ and $U(p)$ with $L(p) \leq \alpha \log p \leq U(p)$. I use the method of [7, exercise 1.2.2-25] to approximate $\alpha \log p$.

4 Bounding smooth integers

Define $f$ as the power series $\sum_{\substack{n \leq y \text{ smooth} \\alpha \log n}} \left( t^{L(p)} + \frac{1}{2} t^{2L(p)} + \frac{1}{3} t^{3L(p)} + \cdots \right)$. Then

$$\sum_{n \leq y \text{ smooth}} t^{\alpha \log n} = \prod_{p \leq y} \frac{1}{1 - t^{\alpha \log p}} \leq \prod_{p \leq y} \frac{1}{1 - t^{L(p)}} = \exp f,$$

so $\Psi(x, y) \leq \sum_{r \leq \alpha \log x} a_r$ if $\exp f = \sum_r a_r t^r$.

Similarly, if $\sum_r b_r t^r = \exp \sum_p (t^{U(p)} + \frac{1}{2} t^{2U(p)} + \frac{1}{3} t^{3U(p)} + \cdots)$, then $\Psi(x, y) \geq \sum_{r \leq \alpha \log x} b_r$.

One can easily compute $\exp f$ in $\mathbb{Q}[t]/t^m$ as $1 + f + \frac{1}{2} f^2 + \cdots$, since $f$ is divisible by a high power of $t$; it also helps to handle small $p$ separately. An alternative is Brent’s method in [8, exercise 4.7-4].

It is not necessary to enumerate all primes $p \leq y$. There are fast methods to count (or bound) the number of primes in an interval; when $y$ is much larger than $\alpha$, many primes $p$ will have the same value $[\alpha \log p]$.

5 Results

The following table shows some bounds on $\Psi(x, y)$ for various $(x, y)$, along with $u = (\log x)/\log y$.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
<th>$\alpha$</th>
<th>lower</th>
<th>upper</th>
<th>$u$</th>
<th>$x \rho(u)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^{60}$</td>
<td>$10^2$</td>
<td>$10^4$</td>
<td>$10^{18} \cdot 5.2$</td>
<td>$10^{18} \cdot 11.6$</td>
<td>$30$</td>
<td>$10^{11} \cdot 0.327^-$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^2$</td>
<td>$10^4$</td>
<td>$10^{18} \cdot 6.73$</td>
<td>$10^{18} \cdot 7.28$</td>
<td>$30$</td>
<td>$10^{11} \cdot 0.327^-$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^3$</td>
<td>$10^4$</td>
<td>$10^{32} \cdot 1.44$</td>
<td>$10^{32} \cdot 5.07$</td>
<td>$20$</td>
<td>$10^{32} \cdot 0.246^+$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^2$</td>
<td>$10^4$</td>
<td>$10^{32} \cdot 2.5278$</td>
<td>$10^{32} \cdot 2.580$</td>
<td>$20$</td>
<td>$10^{32} \cdot 0.246^+$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^3$</td>
<td>$10^4$</td>
<td>$10^{32} \cdot 2.4044$</td>
<td>$10^{32} \cdot 2.4345$</td>
<td>$20$</td>
<td>$10^{32} \cdot 0.246^+$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^4$</td>
<td>$10^4$</td>
<td>$10^{41} \cdot 0.70$</td>
<td>$10^{41} \cdot 2.88$</td>
<td>$15$</td>
<td>$10^{41} \cdot 0.759^-$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^4$</td>
<td>$10^2$</td>
<td>$10^{41} \cdot 1.191$</td>
<td>$10^{41} \cdot 1.370$</td>
<td>$15$</td>
<td>$10^{41} \cdot 0.759^-$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^4$</td>
<td>$10^3$</td>
<td>$10^{41} \cdot 1.2649$</td>
<td>$10^{41} \cdot 1.2827$</td>
<td>$15$</td>
<td>$10^{41} \cdot 0.759^-$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^4$</td>
<td>$10^1$</td>
<td>$10^{46} \cdot 0.99$</td>
<td>$10^{46} \cdot 4.07$</td>
<td>$12$</td>
<td>$10^{46} \cdot 1.420^-$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^4$</td>
<td>$10^2$</td>
<td>$10^{46} \cdot 1.679$</td>
<td>$10^{46} \cdot 1.931$</td>
<td>$12$</td>
<td>$10^{46} \cdot 1.420^-$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^4$</td>
<td>$10^3$</td>
<td>$10^{46} \cdot 1.7817$</td>
<td>$10^{46} \cdot 1.8609$</td>
<td>$12$</td>
<td>$10^{46} \cdot 1.420^-$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^4$</td>
<td>$10^1$</td>
<td>$10^{49} \cdot 1.82$</td>
<td>$10^{49} \cdot 7.14$</td>
<td>$12$</td>
<td>$10^{49} \cdot 2.770^+$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^4$</td>
<td>$10^2$</td>
<td>$10^{49} \cdot 3.025$</td>
<td>$10^{49} \cdot 3.463$</td>
<td>$12$</td>
<td>$10^{49} \cdot 2.770^+$</td>
</tr>
<tr>
<td>$10^{60}$</td>
<td>$10^4$</td>
<td>$10^3$</td>
<td>$10^{49} \cdot 3.2017$</td>
<td>$10^{49} \cdot 3.2453$</td>
<td>$12$</td>
<td>$10^{49} \cdot 2.770^+$</td>
</tr>
</tbody>
</table>

In the final column, $\rho$ is Dickman’s rho function.
References