Refereed. Pages 128–130 in *Algorithmic number theory: ANTS-III*, edited by Joe Buhler, Lecture Notes in Computer Science 1423, Springer, 1998.

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 **y-smooth** if it is not divisible by any primes larger than y. Define $\Psi(x,y) = \#\{n : 1 \le n \le x \text{ and } n \text{ is } y\text{-smooth}\}$. This function Ψ 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, $1.16 \cdot 10^{45} < \Psi(10^{54}, 10^6) < 1.19 \cdot 10^{45}$.

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 Ψ; 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 $f = \sum_{r \in \mathbf{R}} f_r t^r$ such that, for any $x \in \mathbf{R}$, there are only finitely many $r \le x$ with $f_r \ne 0$.

Let $f = \sum_r f_r t^r$ and $g = \sum_r g_r t^r$ be series. The sum $f + g$ is $\sum_r (f_r + g_r) t^r$. The product fg is $\sum_r \sum_s f_r g_s t^{r+s}$.

I write $f \le g$ if $\sum_{r \le x} f_r \le \sum_{r \le x} g_r$ for all $x \in \mathbf{R}$. If $h = \sum_r h_r t^r$ is a series with all $h_r \ge 0$, then $fh \le gh$ whenever $f \le g$.

3 Logarithms

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

For each prime p select integers $L(p)$ and $U(p)$ with $L(p) \le \alpha \log p \le U(p)$. 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 $\sum_{p \le y} \bigl(t^{L(p)} + \frac{1}{2} t^{2L(p)} + \frac{1}{3} t^{3L(p)} + \cdots\bigr)$. Then

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

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

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

One can easily compute $\exp f$ in $\mathbf{Q}[t]/t^m$ 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 $p \le y$. There are fast methods to count (or bound) the number of primes in an interval; when y is much larger than α, many primes p will have the same value $\lfloor \alpha \log p \rfloor$.

5 Results

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

x	y	α	lower	upper	u	$x\rho(u)$
10^{60}	10^2	10^1	$10^{18} \cdot 5.2$	$10^{18} \cdot 11.6$	30	$10^{11} \cdot 0.327-$
10^{60}	10^2	10^2	$10^{18} \cdot 6.73$	$10^{18} \cdot 7.28$	30	$10^{11} \cdot 0.327-$
10^{60}	10^3	10^1	$10^{32} \cdot 1.44$	$10^{32} \cdot 5.07$	20	$10^{32} \cdot 0.246+$
10^{60}	10^3	10^2	$10^{32} \cdot 2.278$	$10^{32} \cdot 2.580$	20	$10^{32} \cdot 0.246+$
10^{60}	10^3	10^3	$10^{32} \cdot 2.4044$	$10^{32} \cdot 2.4345$	20	$10^{32} \cdot 0.246+$
10^{60}	10^4	10^1	$10^{41} \cdot 0.70$	$10^{41} \cdot 2.88$	15	$10^{41} \cdot 0.759-$
10^{60}	10^4	10^2	$10^{41} \cdot 1.191$	$10^{41} \cdot 1.370$	15	$10^{41} \cdot 0.759-$
10^{60}	10^4	10^3	$10^{41} \cdot 1.2649$	$10^{41} \cdot 1.2827$	15	$10^{41} \cdot 0.759-$
10^{60}	10^5	10^1	$10^{46} \cdot 0.99$	$10^{46} \cdot 4.07$	12	$10^{46} \cdot 1.420-$
10^{60}	10^5	10^2	$10^{46} \cdot 1.679$	$10^{46} \cdot 1.931$	12	$10^{46} \cdot 1.420-$
10^{60}	10^5	10^3	$10^{46} \cdot 1.7817$	$10^{46} \cdot 1.8069$	12	$10^{46} \cdot 1.420-$
10^{60}	10^6	10^1	$10^{49} \cdot 1.82$	$10^{49} \cdot 7.14$	10	$10^{49} \cdot 2.770+$
10^{60}	10^6	10^2	$10^{49} \cdot 3.025$	$10^{49} \cdot 3.463$	10	$10^{49} \cdot 2.770+$
10^{60}	10^6	10^3	$10^{49} \cdot 3.2017$	$10^{49} \cdot 3.2453$	10	$10^{49} \cdot 2.770+$

In the final column, ρ is Dickman's rho function.

References

1. Joseph P. Buhler, Hendrik W. Lenstra, Jr., Carl Pomerance, *Factoring integers with the number field sieve*, in [10], 50–94.
2. E. Rodney Canfield, Paul Erdős, Carl Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum"*, Journal of Number Theory **17** (1983), 1–28.
3. Ronald L. Graham, Jaroslav Nešetřil, *The mathematics of Paul Erdős, volume 1*, Algorithms and Combinatorics 13, Springer-Verlag, Berlin, 1997.
4. Adolf Hildebrand, Gérald Tenenbaum, *On integers free of large prime factors*, Transactions of the AMS **296** (1986), 265–290.
5. Adolf Hildebrand, Gérald Tenenbaum, *Integers without large prime factors*, Journal de Théorie des Nombres de Bordeaux **5** (1993), 411–484.
6. Simon Hunter, Jonathan Sorenson, *Approximating the number of integers free of large prime factors*, Mathematics of Computation **66** (1997), 1729–1741.
7. Donald E. Knuth, *The art of computer programming, volume 1: fundamental algorithms*, 2nd edition, Addison-Wesley, Reading, Massachusetts, 1973.
8. Donald E. Knuth, *The art of computer programming, volume 2: seminumerical algorithms*, 2nd edition, Addison-Wesley, Reading, Massachusetts, 1981.
9. Sergei Konyagin, Carl Pomerance, *On primes recognizable in deterministic polynomial time*, in [3], 176–198.
10. Arjen K. Lenstra, Hendrik W. Lenstra, Jr. (editors), *The development of the number field sieve*, Lecture Notes in Mathematics 1554, Springer-Verlag, Berlin, 1993.