SMOOTH NUMBERS: COMPUTATIONAL NUMBER THEORY AND BEYOND

Andrew Granville

Abstract. The analysis of many number theoretic algorithms turns on the role played by integers which have only small prime factors; such integers are known as "smooth numbers." To be able to determine which algorithm is faster than which, it has turned out to be important to have accurate estimates for the number of smooth numbers in various sequences. In this chapter, we will first survey the important estimates for application to computational number theory questions, results as well as conjectures, before moving on to give sketches of the proofs of many of the most important results. After this, we will describe applications of smooth numbers to various problems in different areas of number theory. More complete surveys, with many more references, though with a different focus, were given by Norton (1971) and Hildebrand and Tenenbaum (1993).

Contents

Notation and references

This article has two target audiences. For those primarily interested in computational number theory, I have tried to write this paper in a way that they can better understand the main tools used in analyzing algorithms. For those primarily interested in analytic problems, I have tried to give concise introductions to simplified versions of various key computational number theory algorithms, and to highlight applications and open counting questions. Besides the danger of never quite getting it right for either reader, I have had to confront the difficulty of the differences in notation between the two areas, and to work with some standard concepts in one area that might be puzzling to people in the other. Please consult the appendix for notation that is non-standard for one of the two fields.

L'auteur est partiellement soutenu par une bourse de la Conseil de recherches en sciences naturelles et engénie du Canada.

This article is not meant to be a complete survey of all progress in this very active field. Thus I have not referred to many excellent works that are not entirely pertinent to my view of the subject, nor to several impressive works that have been superseded in the aspects in which I am interested.

1. The basic estimates for practical applications

Let $S(x,y)$ be the set of integers up to x, all of whose prime factors are $\le y$ (such integers are called "y-smooth"), and let $\Psi(x,y)$ be the number of such integers. Throughout we will let $p_1 = 2 < p_2 = 3 < p_3 < \dots$ be the sequence of primes, and select k so that p_k is the largest prime $\le y$ (and thus $k = \pi(y)$, the number of primes $\le y$).

In 1930, Dickman showed the remarkable result that for any fixed $u \ge 1$, the proportion of the integers up to x, which only have prime factors $\le x^{1/u}$, tends to a non-zero limit, as $x \to \infty$. This limit, denoted by $\rho(u)$, is known as the Dickman-de Bruijn ρ-function, and we shall describe it more fully below. Dickman's result may be stated more precisely as:

$$\Psi(x,y) \sim x\rho(u) \quad \text{as} \quad x \to \infty \quad \text{where} \quad x = y^u. \tag{1.1}$$

It is obvious that

$$\rho(u) = 1 \quad \text{for} \quad 0 \le u \le 1, \tag{1.2}$$

and we shall prove below that

$$\rho(u) = 1 - \log u \quad \text{for} \quad 1 \le u \le 2. \tag{1.3}$$

One cannot write down a useful, simple function that gives the value of $\rho(u)$ for all u. The neatest way to define $\rho(u)$ in general is via the *integral delay equation*

$$\rho(u) = \frac{1}{u}\int_{u-1}^{u} \rho(t)\,dt \quad \text{for all } u > 1. \tag{1.4}$$

Note that, by differentiating this expression we obtain

$$\rho'(u) = -\frac{\rho(u-1)}{u}. \tag{1.5}$$

As we shall see later, $\rho(u)$ decays to 0 extremely rapidly as a function of u. A crude but very useful estimate is

$$\rho(u) = 1/u^{u+o(u)} \quad \text{as } u \to \infty, \tag{1.6}$$

and even a little more precisely

$$\rho(u) = \Big(\frac{e+o(1)}{u\log u}\Big)^u \quad \text{as} \quad u \to \infty. \tag{1.7}$$

In many applications we need to take y to be smaller than a given, fixed positive power of x, and so we might ask in what range the asymptotic formula $\Psi(x,y) \sim x\rho(u)$ actually holds? In 1951 de Bruijn showed that

$$\Psi(x,y) = x\rho(u)\Big\{1 + O\Big(\frac{\log(u+1)}{\log y}\Big)\Big\} \quad \text{where} \quad x = y^u \tag{1.8}$$

holds for

$$1 \le u \le (\log y)^{3/5-\varepsilon};\ \text{that is, } y > \exp\big((\log x)^{5/8+\varepsilon}\big). \tag{1.9}$$

Hildebrand (1986) improved this substantially to the range

$$1 \le u \le \exp\big((\log y)^{3/5-\varepsilon}\big);\ \text{that is, } y > \exp\big((\log\log x)^{5/3+\varepsilon}\big), \tag{1.10}$$

How much further is possible? Hildebrand (1984a) showed that such an estimate holds uniformly for

$$1 \le u \le y^{1/2-\varepsilon};\ \text{that is, } y \ge (\log x)^{2+\varepsilon}, \tag{1.11}$$

if and only if the Riemann Hypothesis is true. We shall sketch the ideas of these proofs later.

Some authors work (e.g Tenenbaum (1990)) with the more accurate though (what I find to be) more unwieldy approximation

$$\Psi(x,y) \approx x\int_0^x \rho\left(u - \frac{\log t}{\log y}\right)\ d\Big(\frac{[t]}{t}\Big)$$

(due to de Bruijn). We shall not pursue this here.

Canfield, Erdős, and Pomerance (1983) proved a weaker result than (1.8) but which is applicable in a much wider range and so is very important for computational number theorists: We have

$$\Psi(x,y) = \frac{x}{u^{u+o(u)}}, \tag{1.12}$$

for

$$u \le y^{1-\varepsilon} \text{ with } u \to \infty;\ \text{that is, } y \ge (\log x)^{1+\varepsilon}.$$

There seems to be no hope of proving $\Psi(x,y) \sim x\rho(u)$ in such a wide range (since this would imply the Riemann Hypothesis, as we saw above!), although Hildebrand (1986) did improve (1.12) to

$$\Psi(x,y) = x\rho(u)\exp\Big(O\Big(u\exp(-(\log u)^{3/5-o(1)})\Big)\Big) \tag{1.13}$$

in the same range. Note that $x\rho(u) < 1$ if $y < \{e - o(1)\}\log x$ by (1.7), so $\Psi(x,y) \sim x\rho(u)$ certainly cannot hold in this range.

Results discussed below do tell us, for instance, that

$$\Psi(x, \log^A x) = x^{1-1/A+o(1)}, \quad \text{for any} \quad A > 1. \tag{1.14}$$

Moreover if $0 < \alpha < 1$ then

$$\Psi(x, e^{c(\log x)^\alpha (\log\log x)^\beta}) = xe^{-\{(1-\alpha)/c+o(1)\}(\log x)^{1-\alpha}(\log\log x)^{1-\beta}}, \tag{1.15}$$

the most important special case being

$$\Psi(x, L(x)^c) = x/L(x)^{1/2c+o(1)} \tag{1.16}$$

where, here and henceforth, we adopt the commonly used notation

$$L(x) := \exp(\sqrt{\log x \log\log x}).$$

What about for smaller y? In the next section we shall see that if y is very small compared to x then one can obtain an asymptotic formula for $\Psi(x,y)$ which looks quite different from the formulae above, since it now depends very much on the primes $\le y$: For $y \le \sqrt{\log x \log\log x}$ we have

$$\Psi(x,y) = \frac{1}{\pi(y)!}\prod_{p\le y}\Big(\frac{\log x}{\log p}\Big)\left\{1 + O\left(\frac{y^2}{\log x \log y}\right)\right\}. \tag{1.17}$$

For $y = o(\log x)$ with $y \to \infty$ we have

$$\Psi(x,y) = \Big(\frac{\log x}{y}\Big)^{(1+o(1))\pi(y)}. \tag{1.18}$$

In fact for any $x \ge y \ge 2$ we have

$$\log\Psi(x,y) = ug\Big(\frac{y}{\log x}\Big)\Big\{1 + O\Big(\frac{1}{\log y} + \frac{1}{\log\log x}\Big)\Big\}, \tag{1.19}$$

where

$$g(\kappa) = \log(1+\kappa) + \kappa\log(1+1/\kappa).$$

Notice that the estimates (1.14) as $\alpha \to 1$, and (1.18) as $y \to \log x$, take a rather different shape. For the rather delicate region in-between, where y is a constant multiple of $\log x$, say $y = \kappa\log x$, we get from (1.19) that

$$\Psi(x, \kappa\log x) = \exp\Big\{g(\kappa)\frac{\log x}{\log\log x}\Big\{1 + O\Big(\frac{1}{\log\log x}\Big)\Big\}\Big\}.$$

This is a typical "phase transition" type function. The reasons for such a change in behavior are explored in detail in Granville (1989).

1b. The supposed universality of Dickman's density function.

Computational number theory abounds with examples of sequences $\mathcal{N}$ of integers from which we need to extract y-smooth numbers. As we saw in the previous section, if $y = x^{1/u}$ then the proportion of y-smooth integers up to x is $\rho(u)$, in the surprisingly wide range (1.10) for y. However, in most examples that arise, the sequence $\mathcal{N}$ is rarely so simple as a random sample of integers up to x. Nonetheless, we typically assume for the sequences $\mathcal{N}$ which arise, that more-or-less the same proportion of them are y-smooth as for randomly chosen numbers of roughly the same size. In section 1f, we will attempt to formulate appropriate hypotheses to precisely understand what we are assuming in the most important algorithms. These hypotheses appear to be fairly ad hoc, tied in to the algorithms, but as an analytic number theorist, I prefer to formulate more natural conjectures from which our hypotheses may follow: Greg Martin (2001) made an in-depth study of smooth values of polynomials and made a remarkable universal prediction:

Conjecture. *Suppose that $f(x) \in \mathbb{Z}[x]$ has distinct irreducible factors, over $\mathbb{Z}[x]$, of degrees $d_1, d_2, \dots, d_k \geq 1$, respectively, and fix $u > 0$. There are*

$$\sim \rho(d_1u)\rho(d_2u)\dots\rho(d_ku)x \tag{1.20}$$

integers $n \leq x$ for which $|f(n)|$ is y-smooth, where $x = y^u$, as $x \to \infty$.

The case $k = 1$ implies that for irreducible polynomials, $f(n)$ is as likely to be y-smooth as random integers of the same size. The general conjecture implies that the property of being y-smooth for the various irreducible factors of f is statistically independent. The jury is out on this as a conjecture: Under rather strong assumptions about prime values of polynomials, Martin proves this in a very limited range ($y > x^{d-1/k+\varepsilon}$), but it is plausible that rather different behavior emerges for $y = \sqrt{x}$ say. The conjecture is true for $k = 1$ with f of degree 1, but that is the only case we know for sure. See section 4c for more on what is known.

It is also true that what we have conjectured here is not really what is needed for applications to algorithmic number theory issues. What we really need to understand is far more difficult: In what range of values for x and y does (1.20) hold? Such a range is certainly dependent on the coefficients of f, but we need results in which this dependence is simply stated and easily applicable. As far as I know, no-one has thought through appropriate general conjectures of this nature, though I hope some reader will accept this as a challenge. In section 4c we state what current results imply about such ranges in the degree one case.

One should not be seduced into thinking that these proportions (as in (1.20)) hold up for all naturally defined sequences. Although it is true that the proportion of y-smooth values of $\{a^2 + b^2 \leq x : a, b \geq 1\}$ is $\rho(u)$, note that we are counting here our numbers with multiplicity (that is, how often each n is represented as a sum of two squares). However, if we don't count with multiplicities, that is we look at the proportion of y-smooth values of $\{n \leq x : n = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\}$, then the proportion changes to $\sigma(u)$ where $\sigma(u) = 1$ for $0 \leq u \leq 1$ and $\sigma'(u) = -\sigma(u-1)/2\sqrt{u^2-u}$ for $u > 1$ (see Moree (1993)). In fact, $\sigma(u) = \rho(u)/\{2 + o(1)\}^u$ is quite a bit smaller than $\rho(u)$.

1c. Beliefs, in cryptography and in estimates.

There are many cryptographic schemes around, mostly based on ideas in number theory and combinatorics. For public key cryptography, the goal is to produce a truly "one-way" function in which a practical decryption method cannot be deduced from the (publicly available) encryption method. Most such schemes rely on the difficulty of solving a particular mathematics problem, be it factoring, discrete logs on some group, or an atrociously convoluted linear algebra problem. None of these are provably difficult to solve but, correctly formulated, they certainly seem difficult (indeed we know of no sensible mathematics problem at all that is provably difficult to solve; finding one is an outstanding question in theoretical computer science). Some of the mathematical problems used are ancient chestnuts, like factoring (see sections 2c,d,e,f below), and it perhaps gives one some faith when a cryptoscheme is based on a problem that has remained unscathed through two centuries of attacks by the finest minds from Gauss onwards. By the same token I have less faith in cryptoschemes that rely on convoluted problems a few years old, that are too ugly to attract the finest minds. For some applications one must trade such a feeling of security for speed, so I would advise the reader to remain wary of what they say into their cellphone!

There is now an extensive literature on counting smooth numbers (much of which we are reviewing in this chapter) and in some situations there are sharp estimates in wide ranges, and yet in other seemingly tractable situations, there does seem to be serious difficulty in extending the range of what is known. In particular it is intriguingly difficulty to prove that there are smooth numbers in all intervals of length $\sqrt{x}$, close to x. It is unclear whether our inability to prove strong results in this problem is due to some intrinsic difficulty in the problem, or to our own incompetence. I write this because most work on smooth numbers uses tools that were designed for other questions and modified to fit here, in particular tools used in understanding the distribution of primes where there are certain natural barriers (like proving that there are primes in every interval of length $\sqrt{x}$ close to x). In the case of smooths in arithmetic progressions I overcame such barriers that restrict the range in which one can estimate primes in arithmetic progressions (see section 4b for the range (4.6)), by applying an elementary idea of Hildebrand (although even this has its roots in Selberg's elementary proof of the prime number theorem); this success with "smooths in arithmetic progressions" had long made me suspect that these "smooths in short intervals" problems might succumb to a clever combinatorial argument, rather than sophisticated technique.

However, I am now pessimistic about solving the main "smooths in short intervals" problem (that every interval of length x^ε close to sufficiently large x, contains an x^ε-smooth integer). The reason for my pessimism is, as we shall see in section 4d, that solving this problem will allow us to solve an old well-tested chestnut of analytic number theory, which one feels certain lies deep. Let me explain. Obviously if an estimate implies some version of the Riemann Hypothesis, like (1.8) in the range $y > (\log x)^{2+\varepsilon}$, then we expect that it will be hard to prove! There are many other problems in analytic number theory which have been intensively studied for a long time with little success, and the one we need is one of my favorites:

Vinogradov's conjecture. *Fix $\varepsilon > 0$. If p is a sufficiently large prime then the least quadratic non-residue* $\pmod p$ *is $< p^{\varepsilon}$.*

As we will discuss in section 6d, Burgess (1962) proved this for any $\epsilon > 1/(4\sqrt{e})$. There have been no improvement in forty years, though we do now understand how improvements are intimately tied in to deep questions on the zeros of L-functions. In section 4d we prove that Vinogradov's conjecture for ϵ for primes $p \equiv 3 \pmod 4$ does follow if every interval of length x^{ε} close to sufficiently large x, contains an x^{ε}-smooth integer. Given my belief that Vinogradov's conjecture is an intrinsically difficult problem, I am pessimistic that researchers will prove such a "smooths in short intervals" result for some $\epsilon < 1/(4\sqrt{e})$ in the near future, though I would be delighted to be wrong!

1d. Smooths in number fields.

For a given number field K define $\Psi_K(x, y)$ to be the number of ideals in the ring of integers of K which have norm $\le x$, and all of whose prime ideal factors have norm $\le y$. It is easy to imitate methods from $K = \mathbb{Q}$ to prove that

$$\Psi_K(x, y) = \Psi_K(x, x)\rho(u)\Big\{1 + O_K\Big(\frac{\log(u+1)}{\log y}\Big)\Big\} \tag{1.21}$$

in the range (1.10); and results analogous to (1.12) and (1.13).

There is a much harder and more mysterious problem: When K has units of infinite order, to give an asymptotic estimate for the number of algebraic integers in K of height $\le x$, all of whose prime ideal factors have norm $\le y$. There are several substantial technical problems in solving this, particularly because of the involvement of the class and unit groups in such estimates. This question is pertinent to better analyzing the number field sieve, as well as discrete logarithms in finite fields when the field is presented as a ring of integers modulo a prime ideal.

1e. Entirely explicit results.

There are very few results in the literature with precise inequalities where every constant is explicit. However, these can be very useful. I will list a few here: Konyagin and Pomerance (1997) showed that if $x \ge y \ge 2$ and $x \ge 4$ then

$$\Psi(x, y) \ge x/(\log x)^u \tag{1.22}$$

which implies Lenstra's result that $\Psi(x, \log^2 x) \ge \sqrt{x}$. In section 3a, we will see that

$$\Big(\begin{matrix}\Big[\frac{\log x}{\log 2}\Big] + \pi(y) \\ \pi(y)\end{matrix}\Big) \ge \Psi(x, y) \ge \Big(\begin{matrix}[u] + \pi(y) \\ \pi(y)\end{matrix}\Big) \ge \Big(\frac{\pi(y)}{[u]}\Big)^{[u]}; \tag{1.23}$$

and in section 3b that

$$\frac{1}{k!}\prod_{p \le y}\frac{\log x}{\log p} \le \Psi(x, y) \le \frac{1}{k!}\prod_{p \le y}\frac{\log X}{\log p} \tag{1.24}$$

where $X = x\prod_{p\le y} p$.

One can show (using (3.18)) that the lower bound in (1.23) is $> 2x\rho(u)$ for $y \ll (\log x \log\log x)/(\log\log\log x)$, so that the asymptotic formula $\Psi(x,y) \sim x\rho(u)$ evidently cannot hold in this range.

Pomerance notes that the asymptotic expansion for $\Psi(x,y)$ is

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

where γ is Euler's constant, so that

$$\Psi(x,y) \ge x\rho(u) \tag{1.25}$$

if u or y is sufficiently large. He asks whether this is true for all $x \ge 2y \ge 2$?

Hildebrand (1985a) gave a gorgeous upper bound for smooths in short intervals:

$$\Psi(x+z,y) \le \Psi(x,y) + \Psi(z,y) \tag{1.26}$$

for all $x, z > y$ if y is sufficiently large. Does this hold for all $x, z > y \ge 2$?

1f. Useful conjectures.

We conjecture that for some fixed $c, 0 < c < 4$, and sufficiently small $c' > 0$, we have

$$\Psi(x+c\sqrt{x},y) - \Psi(x,y) \gg \sqrt{x}/u^{u+o(u)} \text{ where } y = x^{1/u} \tag{1.27}$$

for $y > L(x)^{c'}$. Several known methods might allow us, if pushed to their extreme, to prove such an estimate if $c \to \infty$ slowly, perhaps like a power of $\log x$. Unfortunately, in the essential application to the elliptic curve factoring method (section 2f), we must have $c < 4$; results for larger c have no such consequences!

The elliptic curve primality test (section 2h) can be proved to always run in random polynomial time provided

$$\sum_{n\in S(x,y)} \left\{\pi\left(\frac{x+4\sqrt{x}}{n}\right) - \pi\left(\frac{x}{n}\right)\right\} \gg \frac{\sqrt{x}}{\log^A x} \tag{1.28}$$

for $y = \exp(O((\log\log x)^2/\log\log\log x))$. Unfortunately we can only prove this estimate for considerably larger y.

To unconditionally prove that the basic quadratic sieve algorithm (section 2d) factors n in the time claimed we need to show that for a given quadratic polynomial $f(t) = t^2+2bt-c$ with $1 \le c < 2b$ and $y = L(b)^{1/\sqrt{2}}$, there are $\gg y^{1+o(1)}$ values of $m \le y^2$ for which $f(m)$ is y-smooth. (Note that f has discriminant $4n$).

1g. The dual problem.

Define $\Phi(x,y)$ to be the number of integers up to x, all of whose prime factors are $> y$. Buchstab (1949) showed that

$$\Phi(x,y) \sim \omega(u)\frac{x}{\log y}, \tag{1.29}$$

where $\omega(u) = 1/u$ for $1 \le u \le 2$ and

$$u\omega(u) = 1 + \int_1^{u-1} \omega(t)dt \quad \text{for all} \quad u \ge 2. \tag{1.30}$$

Note that $(u\omega(u))' = \omega(u-1)$. In fact $\lim_{u\to\infty} \omega(u) = e^{-\gamma}$ and

$$\max_{u+2\ge v\ge u} |\omega(u) - e^{-\gamma}| = \rho(u)e^{O(u)}. \tag{1.31}$$

2. Applications to computational number theory

In this section we shall survey the use of smooth numbers in computational number theory, without too detailed descriptions of the algorithms (which may be found elsewhere in this volume). Further considerations of the rôle played by smooth numbers in computational number theory can be found in Pomerance's beautiful article (1995).

2a. Why are smooth numbers so often involved?.

As we shall see, a significant step in many algorithms that we encounter is to quickly determine a non-empty subset of a sequence $m_1, m_2, \dots$ of integers whose product is a square. Often elements of the sequence, although explicitly determined, seem like they probably have more-or-less the same multiplicative properties as randomly chosen integers in $[1,x]$. Pomerance (1996a) showed that if $m_1, \dots, m_N, \dots$ are indeed selected randomly and independently from $[1,x]$ then with probability 1, the smallest N for which there is such a non-empty subset of $m_1, \dots, m_N$ whose product is a square, satisfies $N = L(x)^{\sqrt{2}+o(1)}$. Moreover if $N = L(x)^{\sqrt{2}+o(1)}$ then with probability 1 there is a non-empty subset of $m_1, \dots, m_N$ consisting only of $L(x)^{1/\sqrt{2}}$–smooth integers whose product is a square; and these lead us to a very simple linear algebra algorithm to determine such subsets (see section 2b). Similar remarks may also be made when looking for a multiplicatively dependent finite subsequence of the m_i's.

Smooths also appear in other contexts: for example, integers that we know we can factor in polynomial time are typically smooth, or a smooth times a prime (see section 2i).

2b. Products that are a square.

If $u_1, u_2, \dots$ are y-smooth integers factor each u_j as

$$u_j = 2^{a_{j,1}}3^{a_{j,2}}\dots p_k^{a_{j,k}}.$$

Then $\prod_{j\in J} u_j$ is a square if and only if

$$\sum_{j\in J}(a_{j,1}, a_{j,2}, \dots, a_{j,k}) = 0 \text{ as a vector in } (\mathbb{Z}/2\mathbb{Z})^k.$$

Thus such a non-trivial subset is guaranteed amongst $u_1, u_2, \dots, u_{k+1}$. To determine the appropriate subset one can use Gaussian elimination or other algorithms.

Using this we can justify at least part of Pomerance's result (with an argument due, earlier, to Schroeppel): If we randomly choose N integers from $[1, x]$ we expect $\approx N\Psi(x, y)/x$ to be y-smooth. Once this is $> \pi(y)$ then we are guaranteed a subset whose product is a square. Thus we pick y so as to minimize $N_x := x\pi(y)/\Psi(x, y)$. By (1.16) this occurs when $u = \{\sqrt{2}+o(1)\}\sqrt{\log x/\log\log x}$ and $y = L(x)^{1/\sqrt{2}+o(1)}$, so that $N_x = L(x)^{\sqrt{2}+o(1)}$ as claimed in section 2a. Recently Croot, Granville and Tetali (2006) improved Pomerance's result showing that the smallest N for which there is a non-empty subset of $m_1, \dots, m_N$ whose product is a square, satisfies $\frac{1}{4}N_x \le N \le \frac{3}{4}N_x$ with probability $1+o(1)$. Pomerance conjectures that this transition is much sharper than what has been proved.

2c. Dixon's random squares factoring method.

Our goal is to determine "random" integers a and b such that

$$a^2 \equiv b^2 \pmod{n} \tag{2.1}$$

and then, with a little luck, $(a \pm b, n)$ is a non-trivial factor of n.

In Dixon's method one randomly selects $r_1, r_2, \dots$ and determines $m_j \equiv r_j^2 \pmod{n}$ with $|m_j| \le n$. By Pomerance's result in section 2a we expect that there is a subset J of $\{1, \dots, N\}$ once $N = L(n)^{\sqrt{2}+o(1)}$ such that $a^2 = \prod_{j\in J} m_j$ for some integer a. Taking $b = \prod_{j\in J} r_j$ we have candidates for (2.1). This argument can be modified to rigorously prove an expected running time of $L(n)^{\sqrt{2}+o(1)}$ (see the remarks at the end of section 2f).

2d. Smaller squares.

In 1640 Fermat suggested to Frenicle a method of factoring n : Take $r_j = [\sqrt{n}] + j$ for $j = 1, 2, \dots$ so that $m_j = r_j^2 - n$. If any m_j is a square then $n = (r_j - \sqrt{m_j})(r_j + \sqrt{m_j})$. Calculation of consecutive m_j's is easy since $m_{j+1} = m_j + 2[\sqrt{n}] + 2j + 1$; determining whether m_j is not a square is easy by successively testing whether it is a quadratic residue mod $8, 3, 5, 7, \dots$. In this way Fermat factored some impressively large numbers.

In the most primitive version of the quadratic sieve one uses the same values of m_j with $j < n^{o(1)}$, so that each $m_j < n^{1/2+o(1)}$. Then the result of section 2a indicates that the running time is $L(n^{1/2+o(1)})^{\sqrt{2}} = L(n)^{1+o(1)}$, faster than the random squares method. In fact Brillhart and Morrison's "continued fractions method" and Lenstra and Pomerance's "class group method" both attain the same speed up for the same reason, but the first has the advantage of being very practical, the second of being rigorously analyzable. However the flexibility of the quadratic sieve allows various, very effective, speed up strategies.

2e. Spectacular savings with smaller squares: The number field sieve.

Let d be a large integer, define $m = [n^{1/d}]$ and write n in base m as $n = m^d + a_1 m^{d-1} + a_2 m^{d-2} + \cdots + a_d$ where each a_i is an integer, $0 \le a_i \le m - 1$; and define $f(T) = T^d + a_1 T^{d-1} + \cdots + a_d$.

If f factors as $g(T)h(T)$ then $n = f(m) = g(m)h(m)$ provides a non-trivial factorization of n, as follows from a clever 1981 theorem of Brillhart, Filaseta and Odlyzko. Thus we

can assume f is irreducible and let α be a root of f. Let I be the ideal $(\alpha - m, n)$ so that $\text{Norm}(I) = n$. The idea is to find $u, v \in \mathbb{Q}(\alpha)$ so that $u^2 \equiv v^2 \pmod I$ and hopefully $\text{Norm}(u \pm v, \alpha - m, n)$ will provide non-trivial factors of n.

Now for any integers a and b, we have

$$a + b\alpha \equiv a + bm \pmod I;$$

and we proceed, as in the quadratic sieve, keeping only pairs a, b where $a + bm$ is y-smooth and $a + b\alpha$ is y-smooth in $\mathbb{Q}(\alpha)$.

We need a product of terms $(a + b\alpha)(a + bm)$ to be a square: To use Pomerance's estimate we consider trying to make a product of terms $(a + bm)\text{Norm}(a + b\alpha)$ a square. Note though that even if this is a square this calculation is insufficient to guarantee things work, for several reasons: Most important is that different primes of our field can have the same norm — however each unramified prime ideal that arises is of the form $(p, \alpha - w)$ and this divides $\text{Norm}(a + b\alpha)$ if and only if $a + bw \equiv 0 \pmod p$ so we can easily distinguish, in our calculation, between unramified prime ideals of the same norm. There are several other obstructions: ramified primes of the same norm, the difference between $\mathbb{Z}[\alpha]$ and the ring of integers of $\mathbb{Q}(\alpha)$, and various considerations of the 2-parts of the unit and class groups of $\mathbb{Q}(\alpha)$, but all of these difficulties can be handled (see Stevenhagen's article in this volume, or chapter 6.2 in the new book of Crandall and Pomerance, 2001). If we take all $0 < a, b \le y$ then

$$|(a + bm)\text{Norm}(a + b\alpha)| = |(a + bm)b^d f(-a/b)| \le 2(d + 1)m^2 y^{d+1}.$$

By Pomerance's result we thus want $y^2 = L(dm^2 y^{d+1})^{\sqrt{2}+o(1)}$ which implies that $(\log^2 y)/(\log\log y) \sim (2\log n)/d + d\log y$ assuming $d \to \infty$. To minimize the left side we take $d = \sqrt{(2\log n)/(\log y)}$ leading to the choices $\log y \approx \left((8/9)\log n(\log\log n)^2\right)^{1/3}$ and $d = ((3\log n)/(\log\log n))^{1/3} + O(1)$. This gives a running time of

$$\exp\left(\{1 + o(1)\}\left(\frac{64}{9}\log n(\log\log n)^2\right)^{1/3}\right), \tag{2.2}$$

an amazing speed up over $L(n)^{1+o(1)}$ from the previous section.

The constant $(64/9)^{1/3}$ can be slightly improved, though at the price of complicating the algorithm.

2f. Factoring using smooth group orders.

Pollard's $p - 1$ method: If p is a prime factor of n and the order of $2 \pmod p$ is y-smooth, whereas this is not so for all other prime factors of n, then $\gcd(2^\ell - 1, n) = p$ where ℓ is any multiple of the order of $2 \pmod p$, yet still a y-smooth integer. In practice one takes $\ell = \text{lcm}[1, 2, \dots, y]$ for each successive integer y, and computes $2^\ell \pmod n$. This is an efficient algorithm if the structure of the factorization of n is just right; though this will not be so for many integers n.

Lenstra suggested replacing the group $(\mathbb{Z}/p\mathbb{Z})^*$ in this calculation by the group of $\mathbb{F}_p$-points on an elliptic curve. The advantage is that these groups have orders between $p-2\sqrt{p}+1$ and $p+2\sqrt{p}+1$, and in fact for any integer in-between there is an elliptic curve group of that order. It seems far more likely that some, even many, of these numbers are smooth, and so with an algorithm analogous to Pollard's $p-1$ method, Lenstra provided an efficient general purpose factoring method.

Lenstra's "elliptic curve factoring method" proceeds by first randomly choosing elliptic curves $\pmod n$ together with a point R (first select $R=(x_0,y_0)$ and a and then pick b so that $y_0^2\equiv x_0^3+ax_0+b \pmod n$), and then compute ℓR on $E: y^2=x^3+ax+b$ over $\mathbb{Z}/n\mathbb{Z}$. If p is a prime factor of n such that $\#E(\mathbb{F}_p)$ divides ℓ, then this procedure is likely to factor n. The algorithm takes expected time $L(p)^{\sqrt{2}+o(1)}$ to find p provided it is true that there are roughly the number of y-smooths in $(p-\sqrt{p},p+\sqrt{p})$ as we might guess (see section 1f). The proof uses Deuring's theory of CM-elliptic curves which implies that there are $H(t^2-4p)$ elliptic curves $\pmod p$ with $p+1-t$ points, where $H(*)$ is the Kronecker class number; and also Siegel's work in analytic number theory which shows that $H(d)=\sqrt{d}(\log d)^{O(1)}$ with very few exceptions. The great advantage of Lenstra's idea (over Pollard's $p-1$ method, and variants like the $p+1$ method) is that it should always work and its success does not depend on properties of the factorization of n.

Analysis of the elliptic curve factoring method hinges on an unproved assumption, that there are roughly the number of y-smooths in $(p-\sqrt{p},p+\sqrt{p})$ as we might guess; thus for any particular n we cannot rigorously prove that the algorithm has the claimed expected running time. However we can prove that the algorithm does have the claimed expected running time for all but a small set of exceptional n: In certain circumstances this is very useful for we may have an algorithm that applies the method to any of a large set of n, chosen at random, and so that the overall running time can be proved rigorously; for examples, Dixon's algorithm described in barest outline in section 2c was made rigorous in this way by Pomerance (1986), the hyperelliptic smoothness test as proposed by Lenstra, Pila and Pomerance (1993), as well as Lenstra and Pomerance's rigorous time bound for factoring (1992).

2g. Smooths solving the discrete log **problem.**

One wishes to find, for given elements g and b of a group G, an integer m for which $g^m=b$ in G. Typically one takes $G=(\mathbb{Z}/p\mathbb{Z})^*$. This can be solved in (provable) expected running time $L(p)^{\sqrt{2}+o(1)}$ using smooth numbers. The idea is to start by computing $u_j\equiv g^{m_j} \pmod p$ for random integers m_j with $|u_j|<p$, and keeping u_j if it is y-smooth. Once we find enough such u_j we should be able to solve for each prime $q\le y$, writing $q=g^{\nu_q} \pmod p$. Once this is done, we compute $u\equiv bg^{-k} \pmod p$ for random k. If u is ever y-smooth then we know how to write it as a power of g, and therefore also bg^{-k}, and thus we determine m.

This can be generalized to finite fields $\mathbb{F}_{p^d}$: One way is by representing the field as $\mathbb{F}_p[x]/(f(x))$ where f is irreducible over $\mathbb{F}_p[x]$ of degree d, and then developing a theory of smooth $\mathbb{F}_p[x]$–polynomials (see section 5b).

A similar strategy can be used to efficiently determine the structure of the class group of an imaginary quadratic field.

There is no obvious analogy of this solution in the discrete logarithm problem for elliptic curves over finite fields, which makes these groups tempting to use for cryptographic protocols. It seems to me, however, foolish to view this as the basis for a belief that such protocols are more secure!

2h. Goldwasser and Kilian's elliptic curve primality test.

This generalizes Pocklington's test, and almost certainly works in random polynomial time even providing a certificate of primality for p. To prove the primality of p we find an elliptic curve E defined over $\mathbb{F}_p$ such that a completely factored integer $m > (p^{1/4}+1)^2$ divides the order of a point on $E(\mathbb{F}_p)$. (See Schoof's article in the volume for details on how to do this in practice.) For simplicity authors often restrict $\#E(\mathbb{F}_p)$ to be a prime or twice a prime, and so a probabilistic primality test follows provided, for $x = (\sqrt{p}-1)^2$,

$$\pi(x+4\sqrt{x}) - \pi(x) \gg \sqrt{x}/\log^A x \tag{2.3}$$

for some fixed $A(>1)$. Although this holds for "almost all x", we cannot prove it for all x even assuming the Riemann Hypothesis. However one does get a random polynomial time algorithm provided (1.28) holds, since then $\#E(\mathbb{F}_p)$ is an easily factorable number (see the next section).

Adleman and Huang's (1987) hyperelliptic curve primality test does provably work in random polynomial time. The idea is that since such a curve has between $p^2 - cp^{3/2}$ and $p^2 + cp^{3/2}$ points, we can find a curve with a prime q number of points in this interval. Then with probability 1, we can prove q prime by the elliptic curve test.

In light of the recent deterministic polynomial time primality testing algorithm of Agrawal, Kayal and Saxena (2004) (see also Granville (2005)), the test of Adleman and Huang is now of mostly historical interest.

2i. Easily factorable numbers.

What numbers can be factored in polynomial time, in practice? Certainly almost all primes can be identified as primes in probabilistic polynomial time, for example by the Goldwasser-Kilian test; and $\log^C x$ - smooth numbers by trial division. Lenstra's "elliptic curve factoring method" completely factors x in expected running time $(L(y)\log x)^{O(1)}$ where y is the second largest prime factor of x. Thus an integer that is a prime times a y-smooth, with $y = \exp(O((\log\log x)^2/\log\log\log x))$, can be factored in practice in polynomial time. There are

$$\sim e^\gamma x/u \asymp x(\log\log x)^2/(\log x \log\log\log x)$$

such integers $\le x$. In fact one can rigorously prove that this number of integers can be factored in expected polynomial time by this method, despite the fact that Lenstra's elliptic curve factoring method is only guaranteed to work for some, not all, n, since in this calculation we are averaging over many possibilities.

2j. Lenstra's polynomial time test as to whether an integer that is conjecturally prime, is rigorously squarefree.

If $n > 32$ and $a^{n-1} \equiv 1 \pmod n$ for all $a < \log^2 n$ then n is squarefree: This algorithm is only of interest if we already suspect that n is prime, else it is extremely unlikely that the hypothesis will be satisfied (note that if the Generalized Riemann Hypothesis holds and $a^{n-1} \equiv 1 \pmod n$ for all $a < 2\log^2 n$ then n is indeed prime). To see that Lenstra's algorithm works, note that if p^2 divides n then for any $a < 4\log^2 p$ $(< \log^2 n)$ we have $a^{n-1} \equiv 1 \equiv a^{p(p-1)} \pmod{p^2}$ and since $(p, n-1) = 1$ thus $a^{p-1} \equiv 1 \pmod{p^2}$. Therefore every $(4\log^2 p)$–smooth integer n satisfies $n^{p-1} \equiv 1 \pmod{p^2}$, and there are just $p-1$ of these $\le p^2$, so that

$$p - 1 \ge \Psi(p^2, 4\log^2 p) \ge p$$

by (1.22), giving a contradiction.

3. Estimates: More details

In this section we introduce many of the important techniques used in estimating $\Psi(x, y)$. These ideas were introduced by various authors, though de Bruijn and later, Hildebrand, certainly deserve the lion's share of the credit.

3a. Upper and Lower Bounds: Elementary combinatorics.

Evidently $n \in S(x, y)$ if and only if we can write n in the form $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ where the a_k are non-negative integers with $n \le x$, that is

$$a_1 \log p_1 + a_2 \log p_2 + \cdots + a_k \log p_k \le \log x. \tag{3.1}$$

Since each $\log p_i \ge \log 2$ this implies that

$$a_1 + a_2 + \cdots + a_k \le \left[\frac{\log x}{\log 2}\right] = A,$$

say, so that

$$\Psi(x, y) \le \binom{A+k}{k},$$

the upper bound in (1.23). Similarly, as each $\log p_i \le \log y$ so any solution to

$$a_1 + a_2 + \cdots + a_k \le \left[\frac{\log x}{\log y}\right] = [u]$$

gives a solution to (3.1), where $x = y^u$, which implies

$$\Psi(x, y) \ge \binom{[u]+k}{k},$$

the lower bound in (1.23). We can use these bounds, in practice, since

$$k = \pi(y) \sim \frac{y}{\log y}, \quad u = \frac{\log x}{\log y} \text{ and } A = \frac{\log x}{\log 2} + O(1),$$

by the prime number theorem:
If $k > c\log x$ then $\binom{A+k}{k} > x$ so the upper bound is useless! But

$$\Psi(x,y) \ge \frac{k^{[u]}}{[u]!} \approx \Big(\frac{ey}{\log x}\Big)^u = \frac{x}{(\frac{1}{e}\log x)^u} \tag{3.2}$$

(which should be compared to (1.22)). If $k < \varepsilon \log x/(\log\log x)$ then

$$\frac{A^k}{k!} \gtrapprox \Psi(x,y) \gtrapprox \frac{[u]^k}{k!} \approx \frac{u^k}{k!}. \tag{3.3}$$

3b. Upper and lower bounds: Lattices.

In general, if we wish to determine the number of lattice points inside an n-dimensional tetrahedron then we can get good estimates using a little geometry. For if we represent the number of lattice points inside the triangle $\{x_1, x_2 \ge 0,\ w_1x_1 + w_2x_2 \le \tau\}$ by shading in the unit square to the right and above each lattice point, we get a shaded region whose area equals the number of such lattice points. However the original triangle is entirely in the shade, and so has area less than or equal to the number of lattice points, so that there are $\ge \tau^2/(2!w_1w_2)$ lattice points. On the other hand the shaded region is contained inside the triangle $\{x_1, x_2 \ge 0,\ w_1(x_1-1) + w_2(x_2-1) \le \tau\}$ and so the number of lattice points is no more than this triangle's area, which is $(\tau + w_1 + w_2)^2/(2!w_1w_2)$. More generally the boxes "to the right and above" each lattice point in

$$\{x_1, \dots, x_k \ge 0 : x_1w_1 + x_2w_2 + \cdots + x_kw_k \le \tau\},$$

contain this k-dimensional tetrahedron and are contained inside the tetrahedron

$$\{x_1, \dots, x_k \ge 0 : (x_1-1)w_1 + (x_2-1)w_2 + \cdots + (x_k-1)w_k \le \tau\}.$$

Now, $\Psi(x,y)$ equals the number of solutions to (3.1), and so

$$\frac{1}{k!}\prod_{p\le y}\frac{\log x}{\log p} \le \Psi(x,y) \le \frac{1}{k!}\prod_{p\le y}\frac{\log X}{\log p} \tag{1.24}$$

where $\log X = \log x + \sum_{p\le y}\log p$. The ratio of the upper bound to the lower bound is $((\log X)/(\log x))^k$, and since $\sum_{p\le y}\log p \sim y$ by the prime number theorem , we get

$$\Big(\frac{\log X}{\log x}\Big)^k \approx \Big(\frac{\log x + y}{\log x}\Big)^{y/\log y} \approx e^{y^2/(\log x \log y)}$$

which implies (1.17) and (1.18); and if $y \le \log x$ then we get

$$\Psi(x,y) = \frac{1}{\pi(y)!}\prod_{p\le y}\Big(\frac{\log x}{\log p}\Big)e^{O(y^2/(\log x\log y))}. \tag{3.4}$$

3c. Sieving.

Begin with the numbers $1, 2, \dots, [x]$. If we remove those integers divisible by 2 or 3 then the number of integers left is

$$x\Big(1-\frac{1}{2}\Big)\Big(1-\frac{1}{3}\Big)$$

plus or minus 2, since each prime p "removes" about $1/p$ of the remaining integers, leaving a proportion of about $1-1/p$ of them. Therefore after sieving with primes from a finite set P we expect to have approximately

$$x\prod_{p\in P}\Big(1-\frac{1}{p}\Big) \tag{3.5}$$

integers left. Sieve theory tells us that this is a good guess if $p < x^{1/4}$ for all $p \in P$. If P is the set of primes between y and x where $x = y^u$ then, by the above heuristic, we might expect

$$\Psi(x,y) \approx x\prod_{y<p\le x}\Big(1-\frac{1}{p}\Big) \sim \frac{x}{u},$$

integers left but this is very wrong. We will now see this by determining $\Psi(x, x^{1/u})$ for $1 \le u \le 2$. Suppose that n is a positive integer $\le x$ that does not belong to $S(x, x^{1/u})$. Then n must have a prime factor $p > x^{1/u}$. Evidently, n cannot have two such prime factors else $x \ge n \ge pq > x^{2/u} \ge x$. Therefore, any such n can be written as $n = pm$ where p is a prime in $[x^{1/u}, x]$ and $m \le x/p$. Moreover any n that can be written in this form is $\le x$ and $\notin S(x, x^{1/u})$. Therefore

$$\begin{aligned}\Psi(x,x^{1/u}) &= [x] - \sum_{x^{1/u}<p\le x} \#\Big\{m \le \frac{x}{p}\Big\} = x - \sum_{x^{1/u}<p\le x}\Big\{\frac{x}{p}+O(1)\Big\}\\ &= x\Big(1-\Big(\log\log x - \log\log(x^{1/u})+o(1)\Big)\Big)+O(x/\log x)\\ &= x\Big(1-\log\Big(\frac{\log x}{(1/u)\log x}\Big)+o(1)\Big) = x(1-\log u+o(1)).\end{aligned}$$

(Here we use that $\sum_{p\le x} 1/p = \log\log x + C + o(1)$ for some constant C, as well as that there are $\ll x/\log x$ primes $\le x$). We thus see that for $1 \le u \le 2$ we actually get the proportion $1-\log u$ of the integers left, rather than the proportion $1/u$ as had been expected. More generally (1.6) states that the proportion left is $\rho(u) = 1/u^{u+o(u)}$, a far cry from $1/u$. This big difference can be explained by the proof above: (3.5) is valid as long as divisibility for two different primes $p, q \in P$ is essentially independent. However, we saw in our proof that no $n \le x$ can ever be divisible by two such primes p, so such divisibility is certainly not statistically independent.

3d. Estimates for larger u.

The inclusion-exclusion principle gives:

$$\Psi(x,y) = [x] - \sum_{y<p\le x}\Big[\frac{x}{p}\Big] + \sum_{y<p<q\le x}\Big[\frac{x}{pq}\Big] - \sum_{y<p<q<r\le x}\Big[\frac{x}{pqr}\Big] + \dots$$
$$\approx x\Big(1 - \sum_{y<p\le x}\frac{1}{p} + \sum_{y<p<q\le x}\frac{1}{pq} - \sum_{y<p<q<r\le x}\frac{1}{pqr} + \dots\Big) = x\prod_{y<p\le x}\Big(1-\frac{1}{p}\Big)\ ?$$

This looks unlikely to provide a good approximation since there are $\pi(x)-\pi(y)$ terms here to worry about for the first term, and far more for the second, usually more than x. However, if $p_1\dots p_k > x$ then $[x/(p_1\dots p_k)] = 0$ so we may ignore this term; in particular, any term with at least u prime divisors is $> y^u = x$ so that $\Big[\frac{x}{p_1p_2\dots p_k}\Big] = 0$. Thus we may refine the above formula to

$$\Psi(x,x^{1/u}) = [x] - \sum_{y<p\le x}\Big[\frac{x}{p}\Big] + \sum_{\substack{y<p<q\le x\\ pq\le x}}\Big[\frac{x}{pq}\Big] - \sum_{\substack{y<p<q<r\le x\\ pqr\le x}}\Big[\frac{x}{pqr}\Big] + \dots$$

$$\approx x\Big(1 - \sum_{y<p\le x}\frac{1}{p} + \sum_{\substack{y<p<q\le x\\ pq\le x}}\frac{1}{pq} - \sum_{\substack{y<p<q<r\le x\\ pqr\le x}}\frac{1}{pqr} + \dots\Big) \tag{3.6}$$

$$= x\sum_{\substack{d\le x\\ p\mid d\Rightarrow y<p\le x}}\frac{\mu(d)}{d}. \tag{3.7}$$

Notice that the error term here is

$$\le \sum_{\substack{n\le x\\ p\mid n\Rightarrow p>y}} 1 \ll \frac{x}{\log y} = u\frac{x}{\log x}$$

where the second inequality follows from the "fundamental lemma of the sieve" (which implies that if m is an x-smooth integer then there are $\ll \varphi(m)x/m$ integers up to x which are coprime to m). However, it is complicated to evaluate (3.7). We note though that combining the above estimates with (1.1) in the range (1.9) implies

$$\sum_{\substack{d\le x\\ p\mid d\Rightarrow y<p\le x}}\frac{\mu(d)}{d} = \rho(u) + O\Big(\frac{1}{\log y}\Big) \tag{3.8}$$

in that range.

3e. How about for larger u? (II).

We now proceed by induction: We shall "prove" that there exists a constant $\rho(u)$ for each $u>0$, such that

$$\Psi(x,x^{1/u}) \sim x\rho(u). \tag{3.9}$$

As we saw above, this is true for $0 \le u \le 2$, with:

$$\rho(u) = \begin{cases} 1 & \text{for } 0 < u \le 1; \\ 1 - \log u & \text{for } 1 \le u \le 2. \end{cases}$$

We will use the Buchstab-de Bruijn identity

$$\Psi(x,y) = 1 + \sum_{p \le y} \Psi\Big(\frac{x}{p}, p\Big), \tag{3.10}$$

which may be proved by writing each $n \in S(x,y)$ with $n > 1$, as $n = pm$ where p is the largest prime factor of n.

Suppose (3.9) is true for $0 \le u \le N$ and now consider values of $u \in (N, N+1]$: Subtracting (3.10) with $y = x^{1/N}$, from the same equation with $y = x^{1/u}$, we obtain

$$\begin{aligned} \Psi(x, x^{1/u}) &= \Psi(x, x^{1/N}) - \sum_{x^{1/u} < q \le x^{1/N}} \Psi\Big(\frac{x}{q}, q\Big) \\ &\approx x\Big(\rho(N) - \sum_{x^{1/u} < q \le x^{1/N}} \frac{1}{q} \rho\Big(\frac{\log(x/q)}{\log q}\Big)\Big). \end{aligned}$$

Note that

$$\frac{\log(x/q)}{\log q} = \frac{\log x}{\log q} - 1 < \frac{\log x}{\log(x^{1/u})} - 1 = u - 1 \le N,$$

so we can apply the induction hypothesis. The prime number theorem states, in one form, that $\theta(T) := \sum_{p \text{ prime},\ p \le T} \log p = T + O(T/\log^A T)$ for any fixed $A > 0$. Taking now $T = x^{1/t}$ we obtain

$$\begin{aligned} \sum_{x^{1/u} < q < x^{1/N}} \frac{1}{q} \rho\Big(\frac{\log(x/q)}{\log q}\Big) &= \int_{x^{1/u}}^{x^{1/N}} \rho\Big(\frac{\log x}{\log T} - 1\Big) \frac{d\theta(T)}{T \log T} \\ &\approx \int_{x^{1/u}}^{x^{1/N}} \rho\Big(\frac{\log x}{\log T} - 1\Big) \frac{dT}{T \log T} = \int_N^u \rho(t-1) \frac{dt}{t}, \end{aligned}$$

so we deduce that

$$\rho(u) = \rho(N) - \int_N^u \rho(t-1) \frac{dt}{t}. \tag{3.11}$$

This implies (1.5), and so (1.4). Such an approach to (1.1) involves a double induction and has led to the proof of (1.1) in the range (1.9) in the skillful hands of de Bruijn. We shall now see how a different identity, based on ideas of Chebyshev, allowed Hildebrand to prove (1.1) in the far wider range (1.10).

3f. Hildebrand's identity (1984a).

An easier approach is to use the (Chebyshev)-Hildebrand identity

$$\Psi(x,y)\log x = \int_1^x \Psi(t,y)\,\frac{dt}{t} + \sum_{\substack{p^m\le x\\ p\le y}} \Psi\Big(\frac{x}{p^m},y\Big)\log p. \tag{3.12}$$

As we shall see, the (Chebyshev)-Hildebrand identity has an advantage over the Buchstab-de Bruijn identity in that one of the parameters is held fixed; this perhaps explains the exponential difference in the ranges (1.9) and (1.10).

The (Chebyshev)-Hildebrand identity is proved in two steps: First write

$$\begin{aligned}\sum_{n\in S(x,y)}\log n &= \int_1^x \log t\, d\Psi(t,y) = [\Psi(t,y)\log t]_1^x - \int_1^x \frac{\Psi(t,y)}{t}\,dt\\ &= \Psi(x,y)\log x - \int_1^x \frac{\Psi(t,y)}{t}\,dt;\end{aligned}$$

then write

$$\sum_{n\in S(x,y)}\log n = \sum_{n\in S(x,y)}\sum_{p^a\mid n}\log p = \sum_{\substack{p^a\le x\\ p\le y}}\log p \sum_{\substack{n\in S(x,y)\\ p^a\mid n}} 1 = \sum_{\substack{p^a\le x\\ p\le y}}\log p\,\Psi\Big(\frac{x}{p^a},y\Big)$$

and compare. Note that $\Psi(x,y)\log x \approx x\rho(u)\log x$. So,

$$\int_1^x \frac{\Psi(t,y)}{t}\,dt \le x \quad\text{and}\quad \sum_{\substack{p\le y\\ a\ge 2}}\log p\,\Psi\Big(\frac{x}{p^a},y\Big) \le \sum_{p\le y}\frac{x\log p}{p(p-1)} \le cx$$

can be safely ignored in a (narrow) range for u (though see (3.20) below for a more careful estimate), leading to

$$\Psi(x,y)\log x = \sum_{p\le y}\log p\,\Psi\Big(\frac{x}{p},y\Big) + O(x). \tag{3.13}$$

Therefore, using the prime number theorem again, taking $t = y^v$,

$$\begin{aligned}x\log y\cdot u\rho(u) &\approx \int_1^y \Psi\Big(\frac{x}{t},y\Big)\,d\theta(t) \approx \int_1^y \frac{x}{t}\rho\Big(u-\frac{\log t}{\log y}\Big)\,dt\\ &= x\int_0^1 \rho(u-v)\,dv\log y = x\log y\int_{u-1}^u \rho(w)\,dw\end{aligned}$$

which gives (1.4).

3g. The value of ρ.

From (1.4) one can compute values of the function ρ but it is appealing to find a non-self-referential expression to describe ρ, perhaps in terms of "simple" functions. By iterating (1.4) one determines the values

$$\rho(u) = \begin{cases} 1 & \text{for } 0 < u \le 1; \\ 1 - \log u & \text{for } 1 \le u \le 2; \\ 1 - \log u + \int_2^u \log(v-1)\,\frac{dv}{v} & \text{for } 2 \le u \le 3. \end{cases} \tag{3.14}$$

One can continue in this way, or one can refer back to our inclusion-exclusion argument (3.6), to deduce

$$\begin{aligned} \rho(u) = 1 - \int_{t_1=1}^{u} \frac{dt_1}{t_1} + \frac{1}{2!} \int_{\substack{t_1=1 \\ t_1+t_2\le u}}^{u} \int_{t_2=1}^{u} \frac{dt_1\,dt_2}{t_1 t_2} - \cdots\cdots \\ + \frac{(-1)^k}{k!} \int_{\substack{t_1=1 \\ t_1+t_2+\cdots+t_k\le u}}^{u} \int_{t_2=1}^{u} \cdots \int_{t_k=1}^{u} \frac{dt_1\,dt_2 \ldots dt_k}{t_1 t_2 \ldots t_k} + \ldots \end{aligned} \tag{3.15}$$

One can use these formulae to approximate $\rho(u)$, as we do in the table in Appendix B.

3h. The Laplace transform.

A more sophisticated way to evaluate $\rho(u)$ is to take the integral equation just derived, multiply by e^{-su}, and integrate over u:

$$\int_{u\ge 0} u\rho(u) e^{-su} = \int_{u\ge 0} \int_{t=u-1}^{u} \rho(t) e^{-st} \cdot e^{-s(u-t)}\,dt.$$

If $\mathcal{L}(\sigma, s) = \int_0^\infty \sigma(t) e^{-st}\,dt$ then

$$-\mathcal{L}'(\rho, s) = \mathcal{L}(\rho, s) \int_0^1 e^{-sv}\,dv = \mathcal{L}(\rho, s)\Big(\frac{1-e^{-s}}{s}\Big),$$

so that

$$\mathcal{L}(\rho, s) = \mathcal{L}(\rho, 0) \exp\Big(-\int_0^s \frac{1-e^{-t}}{t}\,dt\Big). \tag{3.16}$$

Using the formula for the inverse Laplace transform gives

$$\begin{aligned} \rho(u) &= \frac{1}{2i\pi} \int_{\mathrm{Re}(s)=\alpha} \mathcal{L}(\rho, s) e^{us}\,ds \\ &= c \int_{\mathrm{Re}(s)=\alpha} \exp\Big(us - \int_0^s \frac{1-e^{-t}}{t}\,dt\Big)\,ds, \end{aligned} \tag{3.17}$$

where $c = \mathcal{L}(\rho, 0)/(2i\pi)$ $(= e^\gamma/(2i\pi))$. This formula is not easy to work with, though one can deduce that

$$\rho(u) = \Big\{1 + O\Big(\frac{1}{u}\Big)\Big\} \sqrt{\frac{\xi'(u)}{2\pi}} \exp\left\{\gamma - u\xi + \int_0^\xi \frac{e^t - 1}{t} dt\right\} \tag{3.18}$$

where $\xi = \xi(u)$ is the unique positive solution to the equation $e^\xi = 1 + \xi u$.

3i. More about ρ.

One can deduce

$$\rho(u) = \left(\frac{e+o(1)}{u\log u}\right)^u \tag{1.7}$$

from (3.18) though this can be derived more simply as follows: A simple calculation gives

$$\int_{u-1}^{u} \Big(\frac{k}{t\log t}\Big)^t\,dt \sim \frac{eu}{k}\Big(\frac{k}{u\log u}\Big)^u.$$

Fix $k<e$ and select u_0 sufficiently large. Pick $c>0$ so that $\rho(t) > c\big(\frac{k}{t\log t}\big)^t$ for all $t\le u_0$. We claim that this inequality holds for all t. If not, select the smallest u for which it fails so that, since ρ is continuous,

$$c\Big(\frac{k}{u\log u}\Big)^u = \rho(u) = \frac{1}{u}\int_{u-1}^{u}\rho(t)\,dt > \frac{c}{u}\int_{u-1}^{u}\Big(\frac{k}{t\log t}\Big)^t\,dt \sim \frac{ce}{k}\Big(\frac{k}{u\log u}\Big)^u$$

which gives a contradiction since $k<e$. The upper bound can be proved analogously.

A more elegant upper bound can be derived as follows: Since $\rho(u)>0$ for all u by (1.2) and (1.4), but is non-increasing by (1.5), we see that $\rho(t)\le\rho(u-1)$ for all $t, u-1\le t\le u$, and so $\rho(u)\le\rho(u-1)/u$ by (1.4). Therefore, if m is that integer for which $m+1\ge u>m$ then, by induction,

$$\rho(u) \le \frac{\rho(u-m)}{u(u-1)\dots(u-m+1)} = \frac{\rho(u-m)\Gamma(u-m+1)}{\Gamma(u+1)} \le \frac{1}{\Gamma(u+1)},$$

since $\rho(t)\le 1$ for all t, and $\Gamma(t)\le 1$ for $t\in[1,2]$.

Amusing identities involving the ρ function include

$$e^\gamma = \int_0^\infty \rho(t)dt = \delta + \sum_{n\ge1}(n+\delta)\rho(n+\delta) \quad \text{for any } 0\le\delta\le 1.$$

3j. Rankin's (clever) upper bound method (1938).

Fix any $\sigma>0$. Then, since $(x/n)^\sigma\ge 1$ if $n\le x$, and >0 if $n>x$,

$$\Psi(x,y) \le \sum_{\substack{n\le x\\ p\mid n\Rightarrow p\le y}} \Big(\frac{x}{n}\Big)^\sigma = x^\sigma \prod_{p\le y}\Big(1-\frac{1}{p^\sigma}\Big)^{-1}.$$

To minimize the right hand side (RHS) we can use calculus:

$$\log(\text{RHS}) = \sigma\log x - \sum_{p\le y}\log(1-p^{-\sigma}).$$

Differentiating gives

$$\log x = \sum_{p\le y} \frac{\log p}{p^\sigma - 1}. \tag{3.19}$$

Not easy to explicitly solve! Since the right side is monotone decreasing and continuous as a function of σ, decreasing from ∞ to 0, there is a unique solution $\sigma = \alpha(x,y)$. In fact,

$$\alpha(x,y) = \frac{\log(1+y/\log x)}{\log y}\Big\{1 + O\Big(\frac{\log\log(1+y)}{\log y}\Big)\Big\} \approx 1 - \frac{u\log u}{\log y},$$

where the last approximation is valid if it is $> 1/2$. This formula for α is tricky and technical to substitute in, and comes out bigger than the correct answer by a small factor (see below (3.23)). However it has the great advantage of being a relatively simple method to obtain a good upper bound in all ranges for x and y, and so has been very useful for applications. In fact this method has featured in many of Erdős and Pomerance's works on counting numbers of interest in computational number theory (see Pomerance's 1989 survey, for example).

Special Case: $y = (\log x)^A$ for $A > 1$. Let $\sigma = 1 - 1/A$ to get

$$\log \prod_{p\le y}\Big(1 - \frac{1}{p^\sigma}\Big)^{-1} \ll \sum_{p\le y}\frac{1}{p^\sigma} = \sum_{p\le y}\frac{p^{1/A}}{p} \ll \frac{y^{1/A}}{\log y} \ll \frac{\log x}{\log\log x}.$$

Therefore

$$\Psi\Big(x, (\log x)^A\Big) \le x^{1-1/A+O(1/\log\log x)}.$$

Combining this with (3.3), we obtain

$$\Psi\big(x, (\log x)^A\big) = x^{1-1/A+O(1/\log\log x)}.$$

3k. Iterating the identities more carefully.

With more care the error term in (3.13) can be improved to, for all $y \ge \log^{2+\varepsilon} x$,

$$\Psi(x,y)\log x = \sum_{p\le y}\Psi\Big(\frac{x}{p}, y\Big)\log p + O(\Psi(x,y)). \tag{3.20}$$

From this we can deduce the following result (much as in the proof of Proposition 1 in Granville (1993a)), which explains Hildebrand's result (1.10) (and after):

Theorem. *Define $\rho_y(u)$ as follows:*

$$\rho_y(u) = 1 \qquad \text{for } \ 0 \le u \le 1$$

and

$$\rho_y(u) = \frac{1}{u\log y} \quad \sum_{p\le y}\rho_y\Big(u - \frac{\log p}{\log y}\Big)\frac{\log p}{p}$$

for $u > 1$. Then

$$\Psi(x,y) = x\rho_y(u)\left\{1 + O_\varepsilon\left(\frac{\log(u+1)}{\log y}\right)\right\}$$

for all $x \ge y \ge (\log x)^{2+\varepsilon}$, where $x = y^u$.

Moreover

$$\rho_y(u) = \rho(u)\left\{1 + O_\varepsilon\left(\frac{\log(u+1)}{\log y}\right)\right\}$$

uniformly in a range for u and y, if and only if

$$|\theta(y) - y| \ll \frac{y}{u^{1+o(1)}} \tag{3.21}$$

uniformly in the same range for u and y, where $\theta(y) := \sum_{p\le y} \log p$. The strongest form of the prime number theorem known gives the range (1.10). The Riemann Hypothesis is equivalent to: One can take $u = y^{1/2-\varepsilon}$ for all $\varepsilon > 0$ in (3.21), which gives us (1.11).

3l. The saddle point method.

In 1986 Hildebrand and Tenenbaum, developing an old approach of de Bruijn, used the saddle point method to get an asymptotic for $\Psi(x,y)$ in all ranges that are not easily handled by other methods. They started with Perron's formula: Fix $\alpha > 0$ real. Then

$$\int_{\mathrm{Re}(s)=\alpha} \frac{y^s}{s}\,ds = \begin{cases} 1 & \text{if } y > 1; \\ 1/2 & \text{if } y = 1; \\ 0 & \text{if } 0 < y < 1. \end{cases}$$

If we want those $n \ge 1$ for which $n < x$, we can recognize them as those with $x/n > 1$. Therefore

$$\begin{aligned} \Psi(x,y) &= \sum_{\substack{n\le x\\ p|n\Rightarrow p\le y}} 1 = \sum_{\substack{n\ge 1\\ p|n\Rightarrow p\le y}} \int_{\mathrm{Re}(s)=\alpha} \frac{(x/n)^s}{s}\,ds + O(1) \\ &= \int_{\mathrm{Re}(s)=\alpha} \Bigg(\sum_{\substack{n\ge 1\\ p|n\Rightarrow p\le y}} \frac{1}{n^s}\Bigg)\frac{x^s}{s}\,ds + O(1) = \int_{\mathrm{Re}(s)=\alpha} \xi(s,y)\frac{x^s}{s}\,ds + O(1), \end{aligned} \tag{3.22}$$

where $\xi(s,y) := \prod_{p\le y}\left(1 - \frac{1}{p^s}\right)^{-1}$.

Select $\alpha = \alpha(x,y)$ (the optimization point in Rankin's upper bound). Define $\varphi_k = \varphi_k(s,y) = \left(\frac{d}{ds}\right)^k \log\xi(s,y)$ with $\varphi = \varphi_0$; so that $\log x + \varphi_1(\alpha,y) = 0$ by (3.19). One shows that the main contribution to this integral comes from a very short segment close to $\alpha(x,y)$, the "saddle point", so that

$$\Psi(x,y) = \frac{1}{2i\pi}\int_{\alpha(x,y)-i/\log y}^{\alpha(x,y)+i/\log y} \xi(s,y)x^s\,\frac{ds}{s} + \text{small error.}$$

Now if $s = \alpha + it$ then

$$\frac{x^s}{s} = \frac{x^\alpha}{\alpha} \cdot \frac{x^{it}}{1+it/\alpha} = \frac{x^\alpha}{\alpha} e^{it\log x}\Big(1 - \frac{it}{\alpha} + \text{error}\Big);$$

and, developing the Taylor series,

$$\log\left(\frac{\xi(s,y)}{\xi(\alpha,y)}\right) = \varphi(\alpha+it,y) - \varphi(\alpha,y) = it\varphi_1 - \frac{t^2}{2}\varphi_2 - \frac{it^3}{6}\varphi_3 + O(t^4\varphi_4),$$

so that

$$\frac{x^s}{s}\xi(s,y) = \frac{x^\alpha}{\alpha}\xi(\alpha,y)e^{it(\log x+\varphi_1(\alpha,y))} * e^{-t^2\varphi_2/2}\Big\{1 - \frac{it}{\alpha} - \frac{it^3}{6}\varphi_3 + \text{error}\Big\}.$$

Therefore, since $\log x + \varphi_1(\alpha,y) = 0$,

$$\begin{aligned}\frac{1}{2i\pi}\int_{\alpha-i/\log y}^{\alpha+i/\log y} \xi(s,y)\frac{x^s}{s}\,ds &= \frac{x^\alpha}{\alpha}\xi(\alpha,y)\frac{1}{2\pi}\int_{-1/\log y}^{1/\log y} e^{-t^2\varphi_2/2}\Big(1 - \frac{it}{\alpha} - \frac{it^3}{6}\varphi_3 + \text{error}\Big)\,dt\\ &= \frac{x^\alpha}{\alpha}\xi(\alpha,y)\frac{1}{\sqrt{2\pi\varphi_2}}\{1+\text{error}\}\end{aligned}$$

$\Big(\text{since } \int_{-\infty}^{\infty} e^{-at^2}\,dt = \sqrt{\frac{\pi}{a}}\Big)$. Therefore, for all $x \ge y \ge 2$,

$$\Psi(x,y) = \frac{x^\alpha\xi(\alpha,y)}{\alpha\sqrt{2\pi\varphi_2(\alpha,y)}}\Big\{1 + O\Big(\frac{1}{u} + \frac{\log y}{y}\Big)\Big\}. \tag{3.23}$$

Note that this is smaller than the upper bound $\Psi(x,y) \le x^\alpha\xi(\alpha,y)$, given by Rankin's method, by a factor $\asymp \alpha\sqrt{\varphi_2(\alpha,y)} \ll \log x$. Evaluating the esoteric expression on the right side of (3.23) is in general a difficult problem (indeed it may be argued that we have traded in one intractable problem for another!). However one can make some interesting deductions; for example one can deduce that if $1 \le c \le y$ then

$$\Psi(cx,y) = \Psi(x,y)c^{\alpha(x,y)}\Big\{1 + O\Big(\frac{1}{u} + \frac{\log y}{y}\Big)\Big\}, \tag{3.24}$$

so that one can solve an old conjecture of Erdős:

$$\Psi(2x,y)/\Psi(x,y) \sim \Big(1 + \frac{y}{\log x}\Big)^{(\log 2)/(\log y)} \sim \begin{cases} 1 & \text{if and only if } y \le (\log x)^{1+o(1)};\\ 2 & \text{if and only if } y > (\log x)^\infty.\end{cases}$$

In between is a transition:

$$\Psi(2x,y) \sim 2^{1-1/\alpha}\Psi(x,y) \quad \text{when} \quad y = (\log x)^{\alpha+o(1)} \quad \text{with} \quad \alpha > 1.$$

This, and a function field analogue, inspired Soundararajan to find an easy deduction of (1.8) in the range (1.10) from (3.23), based on the idea that, in a wide range,

$$\frac{\Psi(x^2,y^2)}{x^2} \sim \frac{\Psi(x,y)}{x}.$$

4. Smooths in short intervals, in arithmetic progressions, and as values of polynomials

4a. Smooths in short intervals.

One might guess that smooth numbers are "well-distributed" in short intervals; that is that roughly the same proportion of integers in a short interval near x are smooth, as amongst all of the integers up to x. More precisely we expect that, usually, we have

$$\Psi(x+z,y)-\Psi(x,y)\sim \frac{z}{x}\Psi(x,y)\sim z\rho(u). \tag{4.1}$$

In 1986 Hildebrand showed this for $x\ge z\ge x/y^{5/12}$ in the range (1.10); this can be improved to the range $x\ge z\ge x/y^{1-o(1)}$ (using identities involving integers with exactly two prime factors, in short intervals, as at the end of section 4b). In 1993 Friedlander and I proved (4.1) in the range

$$\exp\big((\log x)^{5/6+o(1)}\big)\le y\le x \quad\text{and}\quad \sqrt{x}y^2\exp\big((\log x)^{1/6}\big)\le z\le x.$$

The most elusive goal in the subject is to show that (4.1) holds when y and z are arbitrary powers of x. Specifically if $1>\beta,\alpha>0$ then one wants to show that

$$\Psi(x+x^\beta,x^\alpha)-\Psi(x,x^\alpha)\sim x^\beta\rho(1/\alpha); \tag{4.2}$$

our result implies this for $\beta>1/2+2\alpha$. Remarks in section 4d suggest that (4.2) is inaccessible if $\alpha<1/(4\sqrt{e})=.15163\dots$ and $\beta<\alpha e^{\rho(1/\alpha)}$ (for if we can prove this then we can improve what is known on Vinogradov's conjecture; see section 1c). Note that for α in this range, $1<e^{\rho(1/\alpha)}<1+3/10^5$, so the most accessible inaccessible cases have $\alpha,\beta\approx 5/33$.

A slight improvement of Balog (1987) gives that

$$\Psi(x+x^\beta,x^\alpha)-\Psi(x,x^\alpha)\gg_{\alpha,\beta} x^\beta \tag{4.3}$$

for all $\beta>1/2$ and $\alpha>0$. Harman (1991) extended Balog's result by showing that

$$\Psi(x+x^\beta,y)-\Psi(x,y)>0$$

for any fixed $\beta>1/2$ and $x\ge y\ge\exp((\log x)^{2/3+o(1)})$. Lenstra, Pila and Pomerance (1993) slightly strengthened this result and gave an explicit lower bound of the correct order of magnitude. Xuan (1999) showed, assuming the Riemann Hypothesis, that there is an x^ϵ–smooth integer in any interval $[x,x+\sqrt{x}(\log x)^{1+o(1)}]$.

Obtaining results like (4.2) and (4.3) with $\beta=1/2$ and $\alpha>0$ fixed but small seems to be rather difficult, and there are few results. I believe that this is the outstanding problem in the whole area of the distribution of smooth numbers:

Challenge Problem 2000. *Prove that, for all $\alpha > 0$, if x is sufficiently large then*

$$\Psi(x+\sqrt{x}, x^\alpha) - \Psi(x, x^\alpha) > 0. \tag{4.4}$$

The "$\sqrt{x}$" barrier for the length of the interval has only been broken in certain special circumstances: In 1987, Friedlander and Lagarias showed, by ingeniously constructing such an integer, that there is always an $x^{1/2}$-smooth integer in any interval of length $x^{1/4+\varepsilon}$ near to x, and also an $x^{1/3}$-smooth integer in any interval of length $x^{5/12+\varepsilon}$ near to x. Harman (2001) proved (4.3) for $1/2 \ge \beta \ge 3/7$ with $\alpha > (3-5\beta)/(2\sqrt{e})$. In particular this shows one can take any $\alpha > 1/(4\sqrt{e})$ for $\beta = 1/2$ in (4.3). This was recently improved by Croot (2001), who showed that for any fixed $\varepsilon > 0$,

$$\Psi(x+c\sqrt{x}, x^{3/(14\sqrt{e})+\varepsilon}) - \Psi(x, x^{3/(14\sqrt{e})+\varepsilon}) \gg_\varepsilon \sqrt{x}/(\log x)^{\log 4+o(1)}$$

for some constant $c = c(\varepsilon) > 0$. This is far from what we need for applications: In section 1f, we saw that we would like to prove a rather better lower bound than that given in (4.4), with "x^α" replaced by "$L(x)^c$".

Following conjecture 4d2 we will justify our belief that an estimate like $\Psi(x+x^\beta, x^\alpha) - \Psi(x, x^\alpha) > 0$ is inaccessible whenever $\alpha, \beta < 1/(4\sqrt{e})$; in this context the results of Harman and Croot seem all the more remarkable for having been obtained with such small α.

Friedlander and Lagarias (1987) also proved that one can "break the $\sqrt{x}$ barrier" most of the time. The best result to date of this type, due to Hildebrand and Tenenbaum (1993), states that for any fixed $\varepsilon > 0$, (4.1) holds when

$$\exp\big((\log X)^{5/6+\varepsilon}\big) \le y \le X \quad \text{and} \quad y\exp\big((\log X)^{1/6}\big) \le z \le X,$$

for all, but at most $X/\exp\big((\log X)^{1/6-\varepsilon}\big)$, integers $x \le X$. Assuming the Riemann Hypothesis, Hafner showed such a result for $L(X) \le y \le X$ with $\sqrt{L(X)} \le z \le X$.

4b. Smooths in arithmetic progressions.

Let $\Psi_q(x,y)$ be the number of integers in $S(x,y)$ which are coprime to q. As one might guess,

$$\Psi_q(x,y) \sim \frac{\varphi(q)}{q}\Psi(x,y)$$

in a very wide range: Tenenbaum (1993) showed this provided there are at most $y^{o(1/\log u)}$ prime factors of q that are $\le y$. In fact Xuan (1995) showed that if q has no more than $y^{1/2}$ prime factors $\le y$ then

$$\Psi_q(x,y) \sim \prod_{p|q,\ p\le y}\left(1-\frac{1}{p^{\alpha(x,y)}}\right)\Psi(x,y)$$

for $(\log x)^{1+o(1)} < y < x^{o(1)}$.

Let $\Psi(x,y;a,q)$ be the number of integers in $S(x,y)$ which are $\equiv a \pmod q$. We would expect

$$\Psi(x,y;a,q) \sim \frac{1}{\varphi(q)}\Psi_q(x,y) \text{ whenever } (a,q)=1. \tag{4.5}$$

I showed that this is true for

$$x \ge y \ge q^{1+\varepsilon} \text{ as } (\log x)/(\log q) \to \infty. \tag{4.6}$$

For $y \ge q^{3/4+\varepsilon}$ and $x \ge y^2$ we get (using results of Balog and Pomerance (1992))

$$\Psi(x,y;a,q) \asymp \frac{1}{\varphi(q)}\Psi_q(x,y) \text{ whenever } (a,q)=1. \tag{4.7}$$

Harman (1999) remarkably proves that if q is cube free then

$$\Psi(x,y;a,q) \gg \frac{1}{\varphi(q)}\Psi_q(x,y) \text{ whenever } (a,q)=1$$

for $y > q^{1/(4\sqrt{e})+\varepsilon}$ and $x > q^{9/4+\varepsilon}$. No wider range for y is feasible with the current state of knowledge (see section 4d). Recently Soundararajan (2006) has developed a new analytic method which is likely to give asymptotics like (4.5) in a range like $y > q^{1/(4\sqrt{e})+\varepsilon}$, for a wide range of values of x. Moreover the method is liable to prove that the smooth numbers are equidistributed in the subgroup of $(\mathbb{Z}/q\mathbb{Z})^*$ generated by the primes $\le y$ in an even wider range for y.

Fouvry and Tenenbaum (1996) showed that (4.5) holds for almost all $x \le X$ and for almost all $q \le \min\{x^{3/5-o(1)},\ \exp(c(\log y \log\log y)/(\log\log\log y))\}$; and for almost all $q \le \sqrt{x}/\exp((\log x)^{1/3})$ provided $y > \exp((\log x)^{2/3+o(1)})$.

For a given sequence $\mathcal{N} = n_1 < n_2 < \dots$ of integers it is often relatively easy to give an asymptotic estimate for

$$\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|\sum_{\substack{n\in\mathcal{N},n\le x\\ n\equiv a \pmod q}} 1 - \frac{1}{\varphi(q)}\sum_{\substack{n\in\mathcal{N},n\le x\\(n,q)=1}} 1\right|^2 \tag{4.8}$$

when $Q = x/\log^A x$: For example, when $\mathcal{N}$ is the sequence of primes, this is $\sim Qx\log x$. Bob Vaughan and I have noted that we can get a non-trivial upper bound, but have had difficulties obtaining an asymptotic, when $\mathcal{N}$ is the sequence of y-smooth numbers, for various ranges of values of y.

One proves results like (4.5) and (4.7) in a similar way to Hildebrand's method in section 3f. By summing

$$\sum_{\substack{n\le x, p|n\Rightarrow p\le y\\ n\equiv a \pmod q}} \log n$$

in two ways, we get the analogy of the Chebyshev-Hildebrand identity (3.12), namely

$$\Psi(x,y;q,a)\log x = \int_1^x \Psi(t,y;q,a)\,\frac{dt}{t} + \sum_{\substack{p^m\le x\\ p\le y, p\nmid q}} \Psi\Big(\frac{x}{p^m},y;q,\frac{a}{p^m}\Big)\log p. \tag{4.9}$$

Now sum this over all a with $1\le a\le q$ and $(a,q)=1$, and divide by $\varphi(q)$, to get

$$\frac{\Psi_q(x,y)}{\varphi(q)}\log x = \int_1^x \frac{\Psi_q(t,y)}{\varphi(q)}\,\frac{dt}{t} + \sum_{\substack{p^m\le x\\ p\le y, p\nmid q}} \frac{\Psi_q(x/p^m,y)}{\varphi(q)}\log p, \tag{4.10}$$

and we have functional equations for $\Psi(x,y;q,a)$ and $\Psi_q(x,y)/\varphi(q)$ that are the same. We can use this to show that (4.5) holds for all $x\ge y$ provided it holds for all x in the range $y^{2+\delta}/q > x \ge y$.

To get a very sharp range like (4.6) we first write our functional equation as

$$\Psi(x,y;q,a)\log x = \sum_{p\le y, p\nmid q} \Psi\Big(\frac{x}{p},y;q,\frac{a}{p}\Big)\log p + O\Big(\frac{\Psi_q(x,y)}{\varphi(q)}\Big). \tag{4.11}$$

"Iterate this", that is, substitute in

$$\Psi\Big(\frac{x}{p},y;q,\frac{a}{p}\Big)\log\Big(\frac{x}{p}\Big) = \dots$$

as determined by (4.11), to get

$$\Psi(x,y;q,a)\log x = \sum_{\substack{p_1,p_2\le y\\ p_1,p_2\nmid q}} \frac{\log p_1\log p_2}{\log(x/p_1)}\Psi\Big(\frac{x}{p_1p_2},y;q,\frac{a}{p_1p_2}\Big) + O\Big(\frac{\Psi_q(x,y)}{\varphi(q)}\Big).$$

To use this functional equation we need to know that integers with exactly two prime factors are well distributed in arithmetic progressions, rather than primes. Such a result is provided by a paper of Mikawa (1989): If $x\ge y\ge x^{1-\varepsilon}$ and $q=o(y/\log^5 x)$ then

$$\sum_{\substack{x-y\le n<x\\ n\equiv a \pmod q\\ n=p_1p_2}} \log p_1\log p_2 \gg \frac{y\log x}{\varphi(q)}$$

for almost all $(a,q)=1$. Therefore (4.5) holds in the range (4.6).

4c. Polynomial values.

For a given polynomial $f(x)\in\mathbb{Z}[x]$, define

$$\Psi_f(x,y) = \#\{n\le x : p|f(n)\Rightarrow p\le y\}.$$

For f of degree one, the results above imply $\Psi_f(x, x^{1/u}) \sim x\rho(u)$ for fixed u, as $x \to \infty$. Actually they even imply that $\Psi_f(x, y) \sim x\rho(u)$ uniformly for such f, when $u \to \infty$ and $v/\log u \to \infty$ where $x = y^u$ and $y = H(f)^v$, and $H(f)$, the height of f, equals the maximum of the absolute values of the coefficients of f.

For irreducible f of degree d we expect

$$\Psi_f(x, x^{1/u}) \sim \rho(du)x \quad \text{as} \quad x \to \infty, \tag{4.12}$$

for fixed $u > 0$, as we discussed in section 1b. Hmyrova (1966) gave an upper bound of similar order of magnitude[1] for irreducible polynomials: $\Psi_f(x, x^{1/u}) \ll_f x(e/u)^u$ if $y = x^{1/u} \geq \log x$.

Balog and Ruzsa (1997) showed that

$$\Psi_f(x, x^{1/u}) \asymp_{f,u} x \tag{4.13}$$

when f is the product of two linear polynomials in $\mathbb{Z}[x]$. Hildebrand (1989) proved (4.13) for $k/u > e^{-1/(k-1)}$ when f splits completely into k distinct linear factors over $\mathbb{Z}[x]$. Dartyge (1996) proved (4.13) for $f(t) = t^2 + 1$ when $u < 179/149$.

For general f of higher degree, let $d_1, d_2, \ldots, d_k$ be the degrees of the distinct irreducible factors of f, with d the maximum of the d_j, and ℓ the number of j for which $d_j = d$. Very recently Dartyge, Martin and Tenenbaum (2001) proved (4.12) for fixed $1/u > d - 1/\ell$; and Martin (2001) proved

$$\Psi_f(x, x^{1/u}) \sim \rho(d_1u)\rho(d_2u)\ldots\rho(d_ku)x \tag{1.20}$$

in the same range, assuming a suitable and plausible uniform version of hypothesis H. (Hypothesis H is a grand generalization of the prime twins conjecture which, in its simplest form, states that if $f_1(t), \cdots, f_k(t) \in \mathbb{Z}[t]$ are irreducible polynomials, which have the property that for every prime p there exists an integer a_p such that p does not divide $f_1(a_p)f_2(a_p)\cdots f_k(a_p)$, then there are infinitely many distinct integers n for which $|f_1(n)|, |f_2(n)|, \cdots, |f_k(n)|$ are all prime.)

Dartyge, Martin and Tenenbaum (2001) also showed that

$$\pi_f(x, x^{1/u}) \gg \pi(x)$$

where $\pi_f(x, y) = \#\{q \leq x : q \text{ prime and } p|f(q) \Rightarrow p \leq y\}$ for $1/u > d - 1/(2\ell)$. Hmyrova (1966) gave the general upper bound[1]: $\pi_f(x, x^{1/u}) \ll_f \pi(x)/u^{\{1+o(1)\}u}$ for $y = x^{1/u} > \log x$.

4d. Limitations on what we might prove.

In our current state of knowledge it seems inaccessible to improve upon what is known about Vinogradov's conjecture, or the following generalization:

[1]Wolke (1971) claimed to have given an upper bound with a factor $1/u^{du}$ in both these problems but Friedlander points out that the deduction of (24) there, and thus the whole proof, seems flawed.

Vinogradov's Conjecture ($+\epsilon$). *Fix integer $k \geq 2$. For each prime p, the least kth power non-residue* $\pmod p$ *is* $\ll_{\varepsilon,k} p^{\varepsilon}$.

In section 6d we give the proof that this holds for any $\varepsilon > 1/(4u_k)$ where u_k is defined so that $\rho(u_k) = 1/k$ (and thus $u_k \sim (\log k)/(\log\log k)$). Given how long this result has remained unimproved, one must surely regard any estimate on smooth numbers which implies an improvement to be "inaccessible" for now, since it would have wide ramifications, not only affecting problems in computational number theory but also such an old chestnut of analytic number theory (see section 1c for further discussion).

If $\Psi(x, y; a, q) > 0$ for sufficiently large x then every residue class $\pmod q$ is generated by the primes $\leq y$ implying Vinogradov's Conjecture ($+\epsilon$) if we can take y to be an arbitrarily small power of x. Thus we assume that such a result is inaccessible. This is why Harman's result, mentioned in section 4b, seems so remarkable in the context of the $k = 2$ case of Vinogradov's conjecture (see section 6d).

In fact if $\Psi(x, y; a, p) > 0$ for sufficiently large x for more than $(p-1)/k$ residue classes $a \pmod p$ with $(a, p) = 1$ then the primes $\leq y$ generate more than just the kth power residues $\pmod p$. Such a result would be implied if $\Psi(x, y; a, p) < k\Psi_p(x, y)/(p-1)$. Thus we believe that the following conjecture is inaccessible for any $\epsilon < 1/(4\sqrt{e})$:

Conjecture 4d1. *Fix $\varepsilon > 0$ sufficiently small. If $y = q^{\varepsilon}$ then for sufficiently large x we have*

$$\Psi(x, y; a, q) < \frac{2\Psi_q(x, y)}{\varphi(q)}. \tag{4.14}$$

These observations are all due to Friedlander who was motivated by them to give the first bounds of type (4.7).

The following conjecture is certainly a goal of researchers into smooths in short intervals (see section 4a):

Conjecture 4d2. *Fix $\varepsilon > 0$. If x is sufficiently large then*

$$\Psi(x, x^{\varepsilon}) - \Psi(x - x^{\varepsilon}, x^{\varepsilon}) > 0. \tag{4.15}$$

If this conjecture is true then Vinogradov's Conjecture ($+\epsilon$) holds whenever -1 is not a kth power residue $\pmod p$: Let q be the least positive kth power non-residue $\pmod p$ which we can assume is $> p^{\varepsilon}$. By the above conjecture, there exists a y-smooth integer $p - m$ in $(p - q, p - 1)$ where $y = q - 1$, which is thus a kth power residue $\pmod p$; but then so is $-1 \equiv (p-m)/m \pmod p$ which gives a contradiction.

Thus Conjecture 4d2 seems inaccessible even for $\varepsilon < 1/(4\sqrt{e})$ since this would imply an improvement on what is known about Vinogradov's conjecture for primes $p \equiv 3 \pmod 4$ (though Croot and Harman have recently given results that approach this boundary, as reported in section 4a).

This argument still works if $\Psi(x^{\beta}, x^{\alpha}) + \{\Psi(x, x^{\alpha}) - \Psi(x - x^{\beta}, x^{\alpha})\} > x^{\beta}$ for sufficiently large x. Such an estimate would be guaranteed if (4.2) holds, for $\beta < \alpha e^{\rho(1/\alpha)}$.

Even a rather weaker conjecture of the form (4.3) seems inaccessible for similar reasons:

Conjecture 4d3. *Fix $\varepsilon > 0$. For $\delta > 0$ sufficiently small we have*

$$\Psi(x+z,y) - \Psi(x,y) \gtrsim \frac{\delta}{\varepsilon} z \quad \text{for} \quad x \ge z \ge x^{\delta} \quad \text{and} \quad x \ge y \ge x^{\varepsilon}, \tag{4.16}$$

whenever x is sufficiently large.

Note that this follows from (4.2) for any fixed $0 < \delta < \frac{1}{2}\varepsilon\rho(1/\varepsilon)$.

Vinogradov's Conjecture $(+\epsilon)$ does follow, in general, from this conjecture: Let q be the least positive kth power non-residue $\pmod p$, which we can assume is $> p^{\varepsilon}$. We may also assume that $\epsilon < 1/\sqrt{e}$ (since Vinogradov's conjecture is known to be true for larger α).

Let $y = q-1$. Define $t_j = [jp/q]$. Note that at most one of $t_j + i$ and $q(t_j+i) - jp$ is a kth power residue $\pmod p$ since their ratio is $q \pmod p$. Thus, taking $0 \le j \le q-1$ and $1 \le i \le I = [p^{\delta}]$ we deduce that there are at most $(q-1)I$ k-th power residues $\pmod p$ amongst the union of

$$\bigcup_{j=0}^{q-1} (t_j, t_j + I]$$

and

$$\bigcup_{j=0}^{q-1} \bigcup_{i=1}^{I} \{q(t_j+i) - jp\} = (0, qI].$$

Since every y-smooth integer amongst these is a k-th power residue, we deduce that

$$qI > \Psi(qI, y) + \sum_{j=0}^{q-1} \{\Psi(t_j + I, y) - \Psi(t_j, y)\}. \tag{4.17}$$

By (4.2) we expect the above to be $\sim qI(\rho(1+\delta/\varepsilon) + \rho(1/\varepsilon))$. Now $1/\varepsilon > \sqrt{e}$ so that $\rho(1/\varepsilon) < 1/2$, and thus to get a contradiction we certainly need $\rho\Big(1+\delta/\varepsilon) > 1/2$, so that $\delta/\varepsilon < 1$ and therefore $\rho(1+\delta/\varepsilon) = 1 - \log(1+\delta/\varepsilon)$ by (1.3). This implies we get a contradiction (so that Vinogradov's Conjecture $(+\epsilon)$ holds) provided (4.2) holds uniformly for $\delta < \varepsilon(e^{\rho(1/\varepsilon)} - 1)$.

In the hypothesis of Conjecture 4d3 we allow "$\delta > 0$ sufficiently small"; in particular, assume $\delta < \epsilon$. Then the right side of (4.17) is

$$\gtrsim qI\left(\rho\Big(1+\frac{\delta}{\varepsilon}\Big) + \frac{\delta}{\varepsilon}\right) = qI\left(1 + \left(\frac{\delta}{\varepsilon} - \log\Big(1+\frac{\delta}{\varepsilon}\Big)\right)\right)$$

by Conjecture 4d3, giving a contradiction. Thus Vinogradov's Conjecture $(+\epsilon)$ also follows from Conjecture 4d3.

4e. The distribution of y-smooth integers and their prime divisors.

It is evident that if y is sufficiently small then most y-smooth integers up to x will be divisible by high powers of primes, whereas if y is large (say $y = x$) then few y-smooth

integers are divisible by high powers. To understand the change in nature of $\Psi(x,y)$ at y near $\log x$, from (1.14) if $y > (\log x)^{1+\varepsilon}$ to (1.18) if $y = o(\log x)$, we need to better understand what the elements of $S(x,y)$ look like.

A proportion $6/\pi^2$ of the y-smooth integers up to x are square free, whenever y is larger than any fixed power of $\log x$ (that is, $(\log y)/(\log\log x) \to \infty$). That proportion drops to 0 once $y < (\log x)^{2+o(1)}$; and, since there are only $2^{\pi(y)}$ y-smooth, square free integers, this is $\Psi(x,y)^{o(1)}$ for $y = o(\log x)$, by (1.18).

Alladi (1982) noted that for $u > 2$ but fixed one has

$$\sum_{n\in S(x,y)} \mu(n) \sim \omega'(u)\frac{x}{\log^2 y}$$

where ω is as in section 1f.

In 1940 Erdős and Kac showed that the values of $\Omega(n)$, the total number of prime factors of n, for n up to x, satisfy the normal distribution with mean and variance $\sim \log\log x$. Alladi, Hensley and Hildebrand (all 1987) showed for $n \in S(x,y)$, the values of $\Omega(n)$ also satisfy the normal distribution whenever $y \gg \log x$: The mean and variance are $\sim \log\log x$ when $u = o(\log\log x)$; and the mean is $\approx u$ and the variance is $\approx u/\log^2 u$ for

$$\log x \ll y \ll \exp((\log x)^{1/21}).$$

Fouvry and Tenenbaum (1991) considered exponential sums over smooth numbers, getting the upper bound

$$\sum_{n\in S(x,y)} e^{2i\pi an/q} \ll x(\log qx)^3\Big\{\frac{\sqrt{y}}{x^{1/4}} + \frac{1}{\sqrt{q}} + \sqrt{\frac{qy}{x}}\Big\}. \tag{4.18}$$

I particularly like their result on Riemann's summation theorem: Of course if $\theta \in (0, 2\pi)$ then

$$\sum_{n\ge 1} e^{i\theta n}/n = -\log(1-e^{i\theta}).$$

However, ordering n in the sum by their largest prime factor, we get

$$\lim_{y\to\infty} \sum_{n\in S(x,y)} \frac{e^{i\theta n}}{n} = -\log(1-e^{i\theta}) + \begin{cases} \log p/\varphi(p^k) & \text{if } \theta = a/p^k,\ p \text{ prime;} \\ 0 & \text{otherwise.} \end{cases} \tag{4.19}$$

The types of results discussed in this subsection are beautifully developed by de la Bretéche and Tenenbaum (2005b)

5. Understanding, computing and playing with smooth numbers

5a. Gaps in the sequence of smooth numbers.

Let $S(x,y) = \{1 = n_1 < n_2 < \dots\}$. What can we say about gaps in this sequence? In 1973/74, Tijdeman showed there exist constants $c_1(y), c_2(y) > 0$ such that

$$\frac{n_i}{(\log n_i)^{c_1(y)}} \ll_y n_{i+1} - n_i \ll_y \frac{n_i}{(\log n_i)^{c_2(y)}}.$$

By (1.17) the average gap is $\asymp_y n_i/(\log n_i)^{\pi(y)}$, so that $c_2(y) \le \pi(y) \le c_1(y)$.

In 1955, Erdős showed there are no more than $cy/\log y$ consecutive integers n_i with each $n_i \gg y$; this was subsequently improved to $c(y \log\log\log y)/(\log y \log\log y)$ by Shorey (1973).

5b. Smooth polynomials in finite fields (related to discrete log problem).

We define $N_q(n,m)$ to be the number of polynomials $f \in \mathbb{F}_q[t]$ of degree n, all of whose irreducible polynomial factors in $\mathbb{F}_q[t]$ have degree $\le m$.

In 1993, Manstavičius gave an asymptotic formula for $n \ge m$ with $m/\sqrt{n\log n} \to \infty$, namely that

$$N_q(n,m) \sim \rho(n/m) q^n,$$

which is not hard to prove using the Buchstab-de Bruijn identity

$$N_q(n,m) - N_q(n,m-1) = I_q(m) N_q(n-m,m)$$

where $I_q(m) = \frac{1}{m}\sum_{d|m} \mu(d) q^{m/d}$, the number of irreducible polynomials in $\mathbb{F}_q[t]$ of degree m. He also showed that for $\sqrt{n\log n} \ge m \ge \{1+o(1)\}(\log n)/(\log q)$ one can prove an asymptotic formula for $N_q(n,m)$ analogous to Hildebrand and Tenenbaum's (3.23): note that since $f_m(z) = \Pi_{k\le m}(1-z^k)^{-I_q(k)} = \sum_{n\ge 1} N_q(n,m) z^n$, we have, for any $0 < r < 1$, the Rankin type upper bound

$$N_q(n,m) = \frac{1}{2i\pi}\int_{|z|=r} \frac{f_m(z)}{z^{n+1}} dz \le \frac{f_m(r)}{r^n};$$

which when optimized at the saddle point $r(n,m)$ is too large by only a small factor. Manstavičius's estimate is difficult to work with, but by comparing $r(n,m)$ with $r(2n,2m)$, Soundararajan (2002) deduces that

$$N_q(n,m) = \rho(n/m) q^n \exp\Big(O\Big(\frac{n\log n}{m^2}\Big)\Big)$$

for $n \ge m \ge \log(n\log^2 n)/(\log q)$ (and a similar method works for $\Psi(x,y)$). As another consequence, Soundararajan shows that if $n^{2/3} \ge m \ge 1$, then

$$\frac{N_q(n+1,m)}{N_q(n,m)} \sim \max(1, qn^{-1/m}).$$

A consequence of this is that $N_q(n,m) = q^n/u^{u+o(u)}$ where $u = n/m$, provided $q \ge (n\log^2 n)^{1/m}$. Bender and Pomerance (1998) showed that $N_q(n,m) \ge q^n/n^u$ whenever $m \le \sqrt{n}$.

Soundararajan also noted that for $m \le (\log n)/(2\log q)$ one has the analogy to (1.17) and for $m \le (\log n)/(\log q)$ the analogy to (1.18), so that in this range $N_q(n,m)$ is "polynomial in n" whereas for $m \gtrsim (\log n)/(\log q)$ it is "exponential in n". The transition is analogous to (1.19): For all $n \ge m \ge 1$ we have

$$\log N_q(n,m) = \frac{n}{m} g\Big(\frac{1}{n}\sum_{k\le m} kI_q(k)\Big)\Big\{1 + O\Big(\frac{1}{m} + \frac{1}{\log n}\Big)\Big\}.$$

Soundararajan's title "Smooth polynomials: Analogies and Asymptotics" is thus very fitting.

The referee has justifiably complained that I have not adequately discussed the contributions of Adleman, Bender, ElGamal, Odlyzko, Pomerance and Schirokauer in giving subexponential bounds for the discrete logarithm problem over finite fields, using various clever and difficult techniques. However this is one subject I will leave the interested reader to check up on independently!

5c. Primes p where $p-1$ is smooth.

Define

$$\pi(x,y) = \#\{p \le x : p-1 \in S(x,y)\}.$$

One would guess that

$$\pi(x,y) \sim \pi(x)\rho(u) \text{ when } y = x^{1/u}; \tag{5.1}$$

and, indeed, this follows for all $u \ge 1$ from a weak form of the Elliott-Halberstam conjecture, a well-believed conjecture in analytic number theory. For some applications $\pi(x,y) \gg_u \pi(x)$ is enough, which is known to hold for $u \le 2\sqrt{e} = 3.297442542\ldots$ (Friedlander, 1989), and for other applications even $\pi(x,y) \gg_u x/\log^A x$, which is known for $u \le 3.3772\ldots$ (Baker and Harman, 1998) and some value of A. One quite surprising application is due to Erdős (1935):

If (5.1) holds uniformly for given u then there exist arbitrarily large integers n, for which there are more than $n^{1-1/u-\varepsilon}$ solutions m to $\varphi(m) = n$.

Proof. Let P be the set of primes $p \le (\log N)^u$, such that all prime factors of $p-1$ are $\le y := \log N$. Consider the set A of integers m which are the product of $k = [(\log N)/(u\log\log N)]$ distinct primes in P: There are

$$\begin{aligned}\binom{\pi((\log N)^u, \log N)}{k} &\ge \Big(\frac{\pi((\log N)^u, \log N)}{k}\Big)^k \\ &\ge \Big(\frac{\{1+o(1)\}\rho(u)\pi((\log N)^u)}{k}\Big)^k = N^{1-1/u+o(1)}\end{aligned}$$

such integers. However, if $m \in A$ then $\varphi(m) < m \le N$, and $q|\varphi(m) \Rightarrow q|p-1$ for some $p \in P \Rightarrow q \le y$, so that there are $\le \Psi(N,y) = N^{o(1)}$ such values. Therefore some such value of $\varphi(m)$ is taken by $\ge N^{1-1/u-o(1)}$ different $m \in A$.

Assuming (5.1) holds uniformly with $y = e^{\sqrt{\log x}}$, Pomerance (1980) showed

$$\max_{n\le x} \#\{m : \varphi(m) = n\} = x/\exp\left(\{1+o(1)\}(\log x \log\log\log x)/(\log\log x)\right).$$

Using the ideas of the proof of Theorem 4 and of the second part of Corollary 3 of Fouvry and Tenenbaum (1996) one can show that

$$\pi(x,y) \ll \pi(x)\rho(u)$$

for $x \ge y \ge \exp((\log x)^{2/3+o(1)})$. The slightly weaker upper bound $\pi(x,y) \ll \pi(x)u\rho(u)$ is given in the extended range $x \ge y \ge \exp(\sqrt{\log x \log\log x})$ by Pomerance and Shparlinski (2005).

In 1983, Adleman, Pomerance and Rumely developed the fastest known deterministic primality test using primes p where $p-1$ is y-smooth; a test made practical by Cohen and Lenstra.

Alford, Pomerance and I gave another application in 1994 showing that there are more than $x^{c(1-1/u)-\varepsilon}$ Carmichael numbers $\le x$. We believe one can take u arbitrarily large in (5.1), and c arbitrarily close to 1 (which also follows from a weak form of the Elliott-Halberstam conjecture), so that there are $\gg x^{1-\varepsilon}$ Carmichael numbers $\le x$. From the current state of these analytic quantities one can then deduce that there are $\gg x^{2/7}$ Carmichael numbers $\le x$; recently Harman (2005 and subsequently) improved the method to obtain $\gg x^{1/3}$ Carmichael numbers $\le x$.

5d. As a sieve, again.

Again consider sieving $[1,x]$ with a set of primes P such that $\prod_{p\in P}(1-\frac{1}{p}) \sim \frac{1}{u}$. We wish to determine the (best possible) upper and lower bounds for the number of integers left unsieved. In section 3c we saw that the expected number is $\sim x/u$. Hildebrand (1984b/1987b) showed:

$$\rho(u)x \lesssim \quad \text{the number of integers left unsieved} \quad \le \Big(e^\gamma - \frac{c}{u^u}\Big)\frac{x}{u},$$

for some constant $c > 0$. Soundararajan and I (2002) recently improved this upper bound to

$$\le \Big(e^\gamma - \frac{1}{u^{1+o(1)}}\Big)\frac{x}{u}$$

which is "best possible". Note that the bound $\rho(u)x$ cannot be reduced since smooth numbers give such an example. From this perspective, one sees that there are remarkably few smooth numbers compared to what one might expect from the sieve; on the other hand, Pomerance (1995, 2001) again and again makes the opposite assertion, that smooths are "fairly numerous", at least in the contexts that arise in computational number theory. The point is that in sieve theory one is interested in the number of integers composed of primes from the given set using the Euler product as the measure of the size of the set, whereas in computational number theory the correct measure is simply the number of elements of the set, and thus one reaches such different conclusions.

5e. Smooth twins and the smooth Goldbach problem.

Hildebrand (1985b) showed that there are infinitely many pairs of consecutive n^ε-smooth integers $n, n+1$. This has been improved to $n^{c(\log\log\log n)/(\log\log n)}$-smooth. Konyagin (unpublished), and Balog and Wooley (2000) showed for any fixed $\varepsilon > 0$ and integer k, there are infinitely many k-tuples of consecutive n^ε-smooth integers. Note that the conjecture in section 1b implies that there are $\sim \rho(1/\varepsilon)^k x$ such k-tuples up to x. The construction of Konyagin, and of Balog and Wooley is remarkably clever yet simple:

Find coprime integers $m_1, m_2, \dots, m_k$ with each $\varphi(m_i)/m_i \le \epsilon/2$, and denote $M = m_1 m_2 \dots m_k$. For each prime $p \le k$ determine integer a_p with $a_p \equiv v_p(j) \pmod{m_j}$ for each $1 \le j \le k$ and $0 \le a_p \le M-1$ (here $v_p(j)$ is the exact power of p dividing j). Let $b = \prod_{p\le k} p^{a_p}$ and then $N = bn^M$ for any large integer n. We claim $N-1, ..., N-k$ are all N^ϵ-smooth for

$$N - j = j(N/j - 1) = j(n_j^{m_j} - 1) = j \prod_{d \mid m_j} \varphi_d(n_j)$$

where $n_j = n^{M/m_j} \prod_{p\le k} p^{(a_p - v_p(j))/m}$; and each $\varphi_d(n_j) \ll n_j^{\varphi(d)} \le n_j^{\varphi(m_j)} \le n_j^{\epsilon m_j/2} = (N/j)^{\epsilon/2} \le N^{\epsilon/2}$.

Balog (1989) showed that every integer N can be written as the sum of two $N^{.2695}$-smooths. Balog and Sarközy (1984a) showed that every integer N can be written as the sum of three $L(N)^{3+o(1)}$-smooths.

5f. Average sizes of factors.

Dickman's original motivation for studying smooth numbers was to gain a better understanding of the distribution of the largest prime factor $p(n)$ of integers n. One can easily deduce from his result that the average size of $(\log p(n))/(\log n)$ is

$$\sim \int_0^\infty \frac{\rho(t)}{(1+t)^2} dt = 0.624\dots$$

which is called Golomb's constant.

Knuth and Trabb Prado (1976) studied the distribution of the kth largest prime factor of an integer proving that there are $\sim \rho_k(u)x$ integers[2] $\le x$ with kth largest prime factor $\le x^{1/u}$, where $\rho_k(u) = 1$ for $u \le 1$, and

$$\rho_k(u) = 1 - \int_1^u (\rho_k(t-1) - \rho_{k-1}(t-1)) \frac{dt}{t}$$

for $u > 1$. They gave the lovely inclusion-exclusion formula (analogous to (3.15) above),

$$\rho_k(u) = 1 - \sum_{n\ge 0} \binom{n+k-1}{k-1} (-1)^n \log_{n+k}(u)$$

[2]note that this function ρ_k is not related to ρ_y of section 3k.

where $\log_1(u) = \log(u)$, and $\log_m(u) = \int_1^u (\log_{m-1}(t-1)/t)dt$. It turns out $\rho_k(u) \sim e^\gamma (\log u)^{k-2}/((k-2)!u)$ for all $k \geq 2$, a very different behaviour from the $k = 1$ case.

Using the above, they show that the average order of the logarithm of the second largest prime factor is $\sim .20958 \ldots \log n$, and of the third largest is $\sim .08831 \ldots \log n$.

Suggestively, they show that $\rho_k(u)$ is also the probability that the kth longest cycle in a random permutation of N letters has length $\leq N/u$.

Billingsley (1972) generalized Dickman's result to the following: For any $1 \geq \alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k > 0$ there are $\sim \rho(\alpha_1, \alpha_2, \ldots, \alpha_k)x$ integers n up to x such the jth largest prime factor of n is $\leq x^{\alpha_j}$ for $j = 1, 2, \ldots, k$ where

$$\rho(\alpha_1, \cdots, \alpha_k) = \int \cdots \int_{\substack{v_1 \geq v_2 \geq \cdots \geq v_k \geq 0 \\ v_1 + v_2 + \cdots + v_k \leq 1 \\ \text{each } v_j \leq \alpha_j}} \rho\Big(\frac{1 - v_1 - v_2 - \cdots - v_k}{v_k}\Big) \frac{dv_1 \cdots dv_k}{v_1 \cdots v_k}.$$

As discussed in Arratia, Barbour and Tararé (1997) this is also the probability that the jth longest cycle in a random permutation of N letters has length $\leq \alpha_j N$ for $j = 1, 2, \cdots, k$. In fact, they show that $\rho(\alpha_1, \cdots, \alpha_k)$ is the distribution function for several interesting combinatorial problems.

De Koninck (1994) showed that the prime p for which there are the most integers n up to x for which p is the largest prime factor of n, satisfies $p = L(x)^{1/\sqrt{2}+o(1)}$. He went on to make the delightful observation that, for any $k \geq 2$, the prime which is most often the kth largest prime factor of n is $p = 3$ (where we range over integers n up to sufficiently large x).

Another related combinatorial problem was found by Chamayou (1973): If $X_1, X_2, \cdots$ are independent random variables each uniformly distributed on $(0, 1)$ then the probability that

$$X_1 + X_1X_2 + X_1X_2X_3 + X_1X_2X_3X_4 + \cdots \leq u$$

is $e^{-\gamma} \int_0^u \rho(t)dt$.

5g. Finding smooth numbers computationally.

The obvious way to find y-smooth numbers in $(x, x + z)$ with $z \leq x$ is to initialize an array $a[i] := 0$ for $1 \leq i \leq z$ (where $a[i]$ corresponds to $x + i$). For each successively larger prime power $p^j \leq x + z$ with $p \leq y$, determine the smallest i such that p^j divides $x + i$ and then add $\log p$ to $a[i], a[i + p^j], a[i + 2p^j], \cdots$ etc., up until the end of the array. When we've finished, if any $a[i] \geq \log x$ then $x + i$ is y-smooth. This algorithm has running time $\ll z \log\log y + uy$.

A very similar idea can be used when we wish to find smooth values of polynomials since then $p|f(n)$ if and only if $p|f(n + p)$.

It seems likely that any such algorithm must have a running time $\geq \pi(y)$, since the primes up to y are part of the input in the problem. However, one might guess that it is not necessary to have z in the running time (if z is part of the running time, it suggests that the algorithm examines most integers in the interval) since one might be able to find smooths by a more constructive approach. Boneh (2001) did this in an ingenious way, obtaining an algorithm with running time $(y \log x)^{O(1)}$:

The goal in Boneh's method is to determine a polynomial $f(t) \in \mathbb{Z}[t]$ for which every integer $m \le z$, with $(x+m, L) \ge x$, is a root, where $L = \prod_{p \le y} p$. Now, if $g = (x+m, L)$ then g^k divides $L^j(x+m)^{k-j}$ and $(x+m)^k x^j$ for $j = 0, 1, 2, \cdots, k-1$, and so g^k also divides any linear combination of these polynomials. By the LLL-algorithm, one can rapidly find a polynomial $f(t)$ with small coefficients which is a linear combination of these polynomials, so that $f(m) \equiv 0 \mod g^k$. Now, since f has small coefficients we deduce that $|f(m)| < x^k \le g^k$, which implies that $f(m) = 0$ since $f(m) \equiv 0 \mod g^k$.

As a consequence, Boneh deduces that if $\frac{1}{5}\log^2 x > y > \log x$ then there are $\ll y/\log x$ integers in $[x, x + x^{(\log x)/(4y)}]$ which divide LCM$[1, \cdots, y]$.

5h. Computational upper and lower bounds on $\Psi(x,y)$.

Computing the precise value of $\Psi(x,y)$ is likely to be impractical once x and y are large, since it seems likely that one would have to do at least $\Psi(x,y)$ bit operations. Perhaps I am too pessimistic.

However, good approximations for $\Psi(x,y)$ may be all that are needed in certain applications: Hunter and Sorenson (1997) noted that one could estimate α and then use (3.23) to approximate $\Psi(x,y)$ up to a factor $1+O(1/u+(\log y)/y)$ in time $\ll (y \log\log x)/\log y + y/\log\log y$.

Bernstein (2001) has indicated how lattice point arguments allow one to quickly obtain good upper and lower bounds: For a large integer N select m_j to be the smallest integer with $m_j \ge N \log p_j$, so that any solution to

$$a_1 m_1 + \cdots + a_k m_k \le d \tag{5.2}$$

where $d = [N \log x]$, gives rise to a solution of (3.1), and thus a y-smooth number $\prod_{j=1}^k p_j^{a_j} \le x$. Therefore, the number of solutions to (5.2) with $d = [N \log x]$ provides a lower bound for $\Psi(x,y)$. To obtain an upper bound by similar methods note that if (3.1) holds then

$$\sum_{i=1}^k a_i m_i < \sum_{i=1}^k a_i(1 + N \log p_i) \le \Big(N + \frac{1}{\log 2}\Big) \log x = N \log X$$

for $X = x^{1+1/(N \log 2)}$; and thus the number of solutions to (5.2) with $d = [N \log X]$ provides the desired upper bound.

Now, the number of solutions to (5.2) equals the coefficient of T^d in

$$\prod_{i=0}^k (1 + T^{m_i} + T^{2m_i} + T^{3m_i} + \cdots) \mod T^{d+1}.$$

where $m_0 = 1$. The obvious algorithm for doing these multiplications takes time $\ll kd^2 \log^2 x$, and this can be speeded up in several ways (see Bernstein (2001)).

Note these bounds will get more accurate the larger N is; for example, by combining both arguments we see that the upper bound given here is $\le \Psi(x^{1+1/(N \log 2)}, y)$.

5i. Determining the smooth part of each integer in a large set.

In several algorithms we wish to rapidly determine the y-smooth parts of many integers. One can use trial division if that is not significant in the running time of the algorithm, or Lenstra's elliptic curve factoring algorithm, or even some sort of sieving technique if for instance the integers are the consecutive values of a polynomial. Recently Bernstein (2000) has come up with a remarkably clever procedure that allows one to find all the small prime factors of $\gg y$ integers, each with $(\log y)^{O(1)}$ bits, in $(\log y)^{O(1)}$ bit operations per integer on average. The central idea is to multiply many of these integers together, determine the y-smooth part of that product, and then gradually dismantle this into smaller and smaller subproducts.

6. Applications to other areas of number theory and beyond

6a. Smooth numbers and character sums.

A central problem in analytic number theory is to determine when

$$\left|\sum_{n\le x}\chi(n)\right| = o(x) \tag{6.1}$$

for a primitive character $\chi \pmod q$. Burgess (1957) used ingenious combinatorial methods together with the "Riemann Hypothesis for hyperelliptic curves" to establish (6.1) whenever $x > q^{\frac14+o(1)}$, when q is cubefree. Soundararajan and I (2001a) investigated the idea that $\sum_{n\le x}\chi(n)$ is well approximated by

$$\Psi(x,y;\chi) := \sum_{n\in S(x,y)}\chi(n),$$

for y "small". We conjecture that there exists $A>0$ for which

$$\sum_{n\le x}\chi(n) = \Psi(x,y;\chi) + o(\Psi(x,y;\chi_0)) \tag{6.2}$$

holds uniformly for $y = (\log q + \log^2 x)(\log\log q)^A$. Here χ_0 is the principal character $\pmod q$; that is $\chi_0(n)=1$ if $(n,q)=1$, and $\chi_0(n)=0$ otherwise. This implies that

$$\max_{\chi\ne\chi_0}\left|\sum_{n\le x}\chi(n)\right| \sim \Psi(x,\log q) \tag{6.3}$$

whenever $\log x = o(((\log\log q)/(\log\log\log q))^2)$, for any prime q. Thus smooth numbers appear naturally in a central question in analytic number theory. Assuming the Generalized Riemann Hypothesis, we showed that (6.2) holds with $y = \log^2 q \log^2 x (\log\log q)^{O(1)}$, which implies that $|\sum_{n\le \log^u q}\chi(n)| \le \{1+o(1)\}\rho(u/2)\log^u q$. If we assume, as is now widely believed, that the imaginary part of the zeros of zeta functions follow the same distributions as the eigenvalues of (the classical) groups of random matrices (see Katz and Sarnak (1999))

then we can improve this to the upper bound implicit in (6.3). Unconditionally we showed that (6.2) holds for "almost all" characters $\chi \pmod q$ with $y = \log q \log x (\log\log q)^{O(1)}$.

We also derived lower bounds for character sums, unconditionally. For example, we proved the lower bound implicit in (6.3): that is that for any fixed $A > 0$, for any given angle θ, there are many χ modulo prime q for which $\sum_{n\le \log^u q} \chi(n) = \{e^{i\theta} + o(1)\}\rho(u)\log^u q$.

In the more useful case of real characters, we showed that there are infinitely many fundamental discriminants $-D < 0$ for which $\sum_{n\le \log^u D}(-D/n) \ge (\rho(u) + o(1))x$. Montgomery and Vaughan (1977) showed that character sums are always $\ll \sqrt{q}\log\log q$ assuming the Generalized Riemann Hypothesis; Paley (1932) had shown that this is best possible other than the constant. Smooth numbers have something to say about this problem: There are infinitely many fundamental discriminants $-D < 0$ for which $\sum_{n\le D/\log^u D}(-D/n) \gg (\rho(u)/\log(u+2))\sqrt{D}\log\log D$.

Recently Soundararajan and I (2006) further developed the idea of (6.2) showing, under the Generalized Riemann Hypothesis: If $\chi \pmod q$ is a primitive character and $x < q^{3/2}$ then

$$\sum_{n\le x} \chi(n)e^{2i\pi n\alpha} = \sum_{\substack{n\le x\\ n\in\mathcal{S}(y)}} \chi(n)e^{2i\pi n\alpha} + O(xy^{-1/6}\log q),$$

for any $\alpha \in [0,1)$; a result which we apply to give new upper bounds on character sums.

6b. The proportion of integers that are quadratic residues, and a generalization.

We can describe $\Psi(x,y)/x$ as a "mean value" of a multiplicative function, it being the $\alpha = 1$ case of

$$F_\alpha(x) = \sum_{n\le x} f_\alpha(n) \quad \text{where} \quad f_\alpha(p) = \begin{cases} 1 & \text{for } p \le y;\\ 1-\alpha & \text{for } p > y.\end{cases}$$

One can show that

$$F_\alpha(x) \sim x\rho_\alpha(u)$$

where

$$\rho_\alpha(u) = 1 \quad \text{for } 0 \le u \le 1,$$

and

$$u\rho_\alpha(u) = \int_{u-1}^{u} \rho_\alpha(t)dt + (1-\alpha)\int_0^{u-1} \rho_\alpha(t)dt,$$

for each $u > 1$, which implies that $\rho'_\alpha(u) = -\alpha\rho_\alpha(u-1)/u$.

Goldston and McCurley (1988) showed that there are $x\rho_\alpha(u)\{1 + O(1/\log y)\}$ integers all of whose prime factors are either $\le y$ or from a set of primes that has density $1-\alpha$. The asymptotic behavior of ρ_α is surprising: For $\mathrm{Re}(\alpha) > 0$ we have

$$\rho_\alpha(u) \sim \frac{e^{\gamma\alpha}}{\Gamma(1-\alpha)}u^{-\alpha}$$

if α is not a positive integer. However, if α is a positive integer then the behaviour of ρ_α is quite different: For large u,

$$\rho_\alpha(u) = (-1)^{1-\alpha}\Big(\frac{e\alpha + o(1)}{u\log u}\Big)^u;$$

and, for small u, the function $\rho_\alpha(u)$ oscillates about the real axis if $\alpha \ge 2$.

Now $\rho_2(u)$ can get negative and the minimum of $\rho_2(u)$ occurs at $u = 1+\sqrt{e}$ where

$$\rho_2(1+\sqrt{e}) = 1 - \frac{\pi^2}{3} - 2\log(1+\sqrt{e})\log\Big(\frac{e}{1+\sqrt{e}}\Big) + 4\sum_{n=1}^{\infty}\frac{1}{n^2}\frac{1}{(1+\sqrt{e})^n}.$$

Soundararajan and I (2001b) deduced that for every sufficiently large integer N and every prime p, more than 17.15% of the integers $\le N$ are quadratic residues $\pmod p$. (Note $(1+\rho_2(1+\sqrt{e}))/2 \approx .1715$.)

In a further generalization, suppose that $f(p) = 1$ for all $p \le y$, and $f(p)$ lies inside or on the unit circle for $p > y$. Define $\chi(t) = 1$ for $0 \le t \le 1$, and $\chi(t) := y^{-t}\sum_{p\le y^t}\log p$ for $1 < t \le u$. Then define $\sigma(t) = 1$ for $0 \le t \le 1$, and

$$u\sigma(u) = \int_0^u \chi(t)\sigma(u-t)dt$$

for all $u > 1$. Soundararajan and I showed that $\sum_{n\le x} f(n) = \{\sigma(u) + o(1)\}x$ for $x = y^u$.

6c. Large gaps between primes.

In 1938, Rankin and Erdős showed how to construct large gaps between consecutive primes by finding long sequences of consecutive integers which each have a small prime factor, say $\le x$. Suppose $[r+1, r+V]$ is such an interval. For each prime $p \le x$ let $a_p \equiv -r \pmod p$. Then $p|r+n$ if and only if $p|n-a_p$, that is $n \equiv a_p \pmod p$. On the other hand, if every $n \in [1,V]$ belongs to some arithmetic progression $a_p \pmod p$, then select $r \equiv -a_p \pmod p$ for every prime $p \le x$, and so every number in $[r+1, r+V]$ is composite. Therefore finding such an interval is equivalent to selecting arithmetic progressions $a_p \pmod p$ to sieve out the integers in $[1,V]$. Now, in section 5d, we saw that very efficient sieving is given by using smooth numbers appropriately. That is how everyone proceeded ... In fact, using the primes up to x we know how to sieve out an interval of length $(2e^\gamma + o(1))x\log x(\log\log\log x)/(\log\log x)^2$. Iwaniec (1978) showed that we cannot sieve out an interval of length $\gg x^2$.

6d. Least quadratic non-residue $\pmod p$.

From the work of Littlewood, Ankeny, Montgomery, and then Bach, we have the following: Assuming the Riemann Hypothesis for $L\big(s, (\frac{\cdot}{q})\big)$, there is an integer $n \le 2\log^2 q$ such that $\big(\frac{n}{q}\big) = 0$ or -1. (Here q may be composite.)

In 1957, Burgess showed unconditionally, via an argument of Vinogradov, that there is a value of $n \le p^{1/(4\sqrt{e})+\varepsilon}$ such that $\left(\frac{n}{p}\right) = -1$, if p is a sufficiently large prime.

Proof. Burgess had already proved (6.1) for $x > q^{1/4+o(1)}$. Taking $\chi = (./p)$ with $q = p$ in (6.1), this implies that if $N > p^{1/4+\varepsilon}$ then there are $\sim N/2$ integers $n \le N$ for which $\left(\frac{n}{p}\right) = 1$. He then applied an old argument of Vinogradov as follows: If $\left(\frac{q}{p}\right) = 1$ for all primes $q \le y$ then $\left(\frac{n}{p}\right) = 1$ for all $n \in S(N, y)$. Therefore $N\rho(u) \sim \Psi(N, y) \lesssim N/2$ where $N = y^u$ so that $\rho(u) \le 1/2$ which holds if and only if $u \ge 1/\sqrt{e}$.

Remark: Vinogradov observed that one can proceed analogously for kth power residues, for any integer $k \ge 2$: Define u_k so that $\rho(u_k) = 1/k$ and $u_k \sim (\log k)/(\log\log k)$ by (1.6). By an analogous proof, for every sufficiently large prime $p \equiv 1 \pmod k$, there is an integer $n \le p^{1/(4u_k)+\varepsilon}$ which is not a kth power $\pmod p$.

The large sieve inequality: Let $\mathcal{N}$ be a sequence of positive integers with

$$N(x) := \sum_{\substack{n\in\mathcal{N}\\ n\le x}} 1 \quad \text{and} \quad N(x;p,a) := \sum_{\substack{n\in\mathcal{N},\, n\le x\\ n\equiv a \pmod p}} 1.$$

Then

$$\sum_{p\le\sqrt{x}} p \sum_{a=1}^{p} \Big(N(x;p,a) - \frac{N(x)}{p}\Big)^2 \le 2xN(x).$$

In 1941, Linnik showed there are no more than $4/\rho(2u)$ primes $\le z$ for which the least quadratic non-residue is $> y$ where $z = y^u$.

Proof. Let $\mathcal{N}$ be the sequence of integers whose prime factors are all $\le y$. Let $x = z^2$. If $p \le z\,(= \sqrt{x})$ is a prime for which the least quadratic non-residue q_p is $> y$ then $(n/p) = 1$ for all $n \in \mathcal{N}$: In particular $N(x;p,a) = 0$ if $(a/p) = -1$ or 0. Therefore,by the large sieve inequality above,

$$\sum_{\substack{p\le z\\ q_p>y}} p \cdot \frac{(p+1)}{2}\left(\frac{N(x)}{p}\right)^2 \le 2xN(x)$$

so that the number of such primes is $\le 4x/N(x)$. Note that $N(x) = \Psi(x, y) = \Psi(z^2, y) \sim x\rho(2u)$.

Linnik's result implies that there are $\ll_\varepsilon \log\log x$ counterexamples to Vinogradov's conjecture up to x.

6e. Fermat's last theorem (first case).

Long before the famous work of Andrew Wiles, there were other, simpler approaches! The first case of Fermat's last Theorem (FLT I) states that there are no solutions to

$$x^p + y^p = z^p,\ x, y, z > 0,\ p \nmid xyz.$$

In 1910, Wieferich showed that a solution implies $2^{p-1} \equiv 1 \pmod{p^2}$. Others then proved a solution implies $3^{p-1} \equiv 1 \pmod{p^2}$—it's unlikely that these two congruences ever happen simultaneously—then $5^{p-1}, 7^{p-1}, \ldots \equiv 1 \pmod{p^2}$. Hendrik Lenstra proved

$\Psi(x,(\log x)^2) > \sqrt{x}$ (which also follows from (1.22)) which implies that there is a $q < 4\log^2 p$ for which $q^{p-1} \not\equiv 1 \pmod{p^2}$.

Proof. Otherwise take $x = p^2$ above to get $\Psi(p^2, 4\log^2 p) > p$. Now if $n \in S(p^2, 4\log^2 p)$ then $q^{p-1} \equiv 1 \pmod{p^2}$ for every prime q dividing n so that $n^{p-1} \equiv 1 \pmod{p^2}$. But there are only $p-1$ such values of $n < p^2$.

In my Ph.D thesis, I showed how to deduce $q^{p-1} \equiv 1 \pmod{p^2}$ for each successive prime q systematically from a supposed solution to FLTI, developing an approach of Frobenius. Maple implementation gave each $q \le 89$. If my algorithm never degenerated one would deduce that $q^{p-1} \equiv 1 \pmod{p^2}$ for every prime $q \le (\log p)^{1/4}$, which is unfortunately not quite enough to deduce FLT I!

6f. Important applications to Waring's problem, and beyond.

In 1941 Vinogradov used the circle method to prove that every sufficiently large integer is the sum of $\le (2+\varepsilon)k\log k$, kth powers of integers. Vaughan's work (1989) suggested that one might do better by working with kth powers of smooth numbers. Wooley (1992) did this in improving Vinogradov's result to $\le k\log k + k\log\log k + Ck$, kth powers of integers, the biggest breakthrough in this well-explored problem in fifty years! Moreover, Vaughan and Wooley have developed this into a powerful tool, not only for Waring's problem, but for various other questions: For instance, Harman (1993) uses an exponential sum estimate in the circle method, involving only smooth numbers in the exponents, to study when there are solutions to $||a_1 n_1^k + \cdots + a_r n_r^k|| \ll 1/N^k$ where $1 \le n_i \le N$, the a_i's are given real algebraic numbers, and $||t||$ is the distance from the nearest integer to t. See Vaughan's survey (1993) and Vaughan and Wooley (2002) for a thorough discussion of related questions.

6g. Egyptian fractions.

In his PhD thesis, Croot solved an old ($500) problem of Erdős and Graham. For any r-coloring of the integers in $[2, e^{167000r}]$, there is a monochromatic subset S for which

$$\sum_{n\in S} \frac{1}{n} = 1.$$

The proof reduces the problem to looking over smooth subsets of the integers. The "167000" comes from an estimate involving $\rho(u)$. Clearly, one needs an interval longer than $[2, e^{(1-\varepsilon)r}]$. What is the correct upper limit for the interval?

6h. The abc-conjecture.

Suppose $c > a > 0$ are both y-smooth. The "abc-conjecture" (see Granville-Tucker (2002)) tells us that

$$c^{1-\varepsilon} \ll_\varepsilon \prod_{p \mid ac(c-a)} p \le (c-a) \prod_{p\le y} p.$$

Thus if $a < c$ are the first two y-smooth integers $\ge x$, then

$$c - a \gg_\varepsilon x^{1-\varepsilon}/e^{\{1+o(1)\}y}.$$

So for $y = o(\log x)$ we see that $\Psi(x + x^{1-o(1)}, y) - \Psi(x,y) = 0$ or 1.

6i. S-unit equations with lots of solutions.

Let S be a set of s primes. Evertse (1984) showed that there are $\le 3\cdot 7^{2s+3}$ solutions to $a+b=c$ in coprime integers a,b,c whose prime divisors all come from the set S (that is, a,b,c are "S-units"). Erdős, Stewart and Tijdeman (1988) showed that there exist sets S with at least $\exp(\{4+o(1)\}(s/\log s)^{1/2})$ solutions. Recently Konyagin and Soundararajan (2006) improved this to at least $\exp(s^{2-\sqrt{2}-o(1)})$ solutions. They also prove that there exist sets S with at least $\exp(s^{\frac{1}{16}})$ solutions to $a+1=c$ in S-units, and as a consequence that there exist integers N with more than $\exp((\log N)^{\frac{1}{16}})$ consecutive divisors.

More generally, it is known that there are only finitely many solutions to

$$a_1+a_2+\cdots+a_n=b \tag{6.4}$$

in positive integers $a_1,\dots,a_n,b$ with $\gcd(a_1,\dots,a_n,b)=1$, where all prime factors of $a_1\dots a_nb$ come from S. One can easily show that there are sets with at least

$$\exp(\{n^2/(n-1)+o(1)\}s/(s\log s)^{1/n}) \tag{6.5}$$

solutions: Let y be large and let $u=y^{1-1/n}/((1-1/n)\log y)$. If $a_1,\dots,a_n\in S(y^u,y)$ then $1\le b\le ny^u$. Thus some value of b is taken in (6.4) at least $\Psi(y^u,y)^n/(ny^u)$ times, which is (6.5) by (1.13) and (1.7). To assume coprimeness divide each solution through by $\gcd(a_1,\dots,a_n,b)$. (Here $S=\{p:p|b\}\cup\{p\le y\}$.)

One might guess that each such value of b is taken roughly equally often, in which case the number of solutions is at least (6.5) replacing n by $n+1$.

6j. Ramanujan-Nagell equations with lots of solutions.

Evertse (1984) showed that if $F(x,y)\in\mathbb{Z}[x,y]$ is homogenous of degree d, with at least three distinct linear factors then $F(m,n)$ is an S-unit for at most $2\cdot 7^{(2s+3)d^3}$ pairs of coprime integers m,n, which Bombieri (1987) improved to $(12(d+5))^{12(s+1)}$. On the other hand, Erdős, Stewart and Tijdeman (1988) showed there exist such F with at least

$$\exp\{(d^2+o(1))(s\log s)^{1/d}/\log s\}. \tag{6.6}$$

solutions. The proof is similar to that in the previous section. Fix large y and let $u=dy^{1/d}/\log y$. Consider all vectors of the form

$$(n-a_1,n-a_2,\dots,n-a_d)\ \text{ with } n\le x \text{ and each } a_i\in S(x,y). \tag{6.7}$$

Each entry of each vector is in $(-x,x)$ and there are $x\Psi(x,y)^d$ vectors, so some vector, say $(r_1,\dots,r_d)$ is attained $\ge x\Psi(x,y)^d/(2x)^d$ times, which equals (6.6) with $s=\pi(y)$. Thus if $F(x,y)=\prod_{i=1}^d(x-r_iy)$ then for each such vector in (6.7) we get $F(n,1)=a_1\dots a_d\in S(x,y)$.

Acknowledgements. I would like to thank Dan Bernstein, John Friedlander, Adolf Hildebrand, the referee, Carl Pomerance, K. Soundararajan and Gerald Tenenbaum for their help in preparing this article.

References

L.M. Adleman and M.-D. A. Huang,
(1992) Primality testing and abelian varieties over finite fields, *Lecture Notes in Mathematics,***1512**. Springer-Verlag, Berlin.

L.M. Adleman, C. Pomerance and R.S. Rumely,
(1983) On distinguishing prime numbers from composite numbers, *Ann. of Math.* (2) **117**, 173–206.

M. Agrawal, N. Kayal, N. Saxena,
(2004) PRIMES is in P. *Ann. of Math.*(2) **160**,*no* 2, 781–793.

W. R. Alford, A. Granville, and C. Pomerance,
(1994) There are infinitely many Carmichael numbers *Ann. of Math.*(2) **139**,*no* 3, 703–722.

K. Alladi,
(1982) Asymptotic estimates of sums involving the Moebius function. II, *Trans. Amer. Math. Soc.* **272**, 87–105.
(1987) An Erdős-Kac theorem for integers without large prime factors, *Acta Arith.* **49**, 81–105.

R. Arratia, A.D. Barbour and S. Tavaré,
(1997) Random combinatorial structures and prime factorizations, *Notices Amer. Math. Soc.***44**, 903–910.

E. Bach,
(1985) Analytic methods in the analysis and design of number-theoretic algorithms, *ACM Distinguished Dissertations*. MIT Press, Cambridge, MA, 48 pp.

R. C. Baker and G. Harman,
(1998) Shifted primes without large prime factors, *Acta Arith.* **83**, 331–361.

A. Balog,
(1984) $p + a$ without large prime factors, in: *Séminaire de Théorie des Nombres*, Bordeaux 1983-84, Univ. Bordeaux, Talence, Exp. No. 31, 5 pp.
(1987) On the distribution of integers having no large prime factor, in: *Journées Arithmétiques*, Besançon 1985, *Astérisque* **147/148**, pp. 27–31.
(1989) On additive representations of integers, *Acta Math. Hungar.* **54**, 297–301.

A. Balog and C. Pomerance,
(1992) The distribution of smooth numbers in arithmetic progressions, *Proc. Amer. Math. Soc.* **115**, 33–43.

A. Balog and I.Z. Ruzsa,
(1995) On an additive property of stable sets. Sieve methods, exponential sums, and their applications in number theory *London Math. Soc. Lecture Note Series* **237**, 55–63.

A. Balog and A. Sárkőzy,
(1984a) On sums of integers having small prime factors. I, *Stud. Sci. Math. Hungar.* **19**, 35–47.
(1984b) On sums of integers having small prime factors. II, *Stud. Sci. Math. Hungar.* **19**, 81–88.

A. Balog and T.D. Wooley,

(1998) On strings of consecutive integers with no large prime factors, *J. Austral. Math. Soc. Ser. A* **64**, 266–276.

R.L. Bender and C. Pomerance,
(1995) Rigorous discrete logarithm computations in finite fields via smooth polynomials, *Computational perspectives on number theory (Chicago, IL, 1995)*, 221-232.

D.J. Bernstein,
(2000) How to find small factors of integers, preprint.
(2002) Arbitrarily tight bounds on the distribution of smooth numbers, *Number theory for the millennium,* I (Urbana, IL, 2000), 49–66, A K Peters, Natick, MA

P. Billingsley,
(1972) On the distribution of large prime divisors, *Period. Math. Hungar.* **2**, 283–289.

D. Boneh,
(2002) Finding smooth integers in short intervals using CRT decoding, *J. Comput. System Sci.* **64**, 768–784

R. de la Bretéche and G. Tenenbaum,
(2005a) Propriétés statistiques des entiers friables, *Ramanujan J.* **9**, 139–202
(2005b) Entiers friables: inégalité de Turán-Kubilius et applications, *Invent. Math.* **159**, 531–588.

J. Brillhart, M. Filaseta and A. Odlyzko,
(1981) On an irreducibility theorem of A. Cohn, *Canad. J. Math.* **33**, 1055–1059.

N. G. de Bruijn,
(1951a) The asymptotic behaviour of a function occurring in the theory of primes, *J. Indian Math. Soc.(N.S.)* **15**, 25–32.
(1951b) On the number of positive integers $\leq x$ and free of prime factors $> y$, *Nederl. Akad. Wetensch. Proc. Ser. A* **54**, 50–60.
(1966) On the number of positive integers $\leq x$ and free of prime factors $>y$, II, *Nederl. Akad. Wetensch. Proc. Ser. A* **69**, 239–247.

A. A. Buchstab,
(1949) On those numbers in an arithmetic progression all prime factors of which are small in magnitude (Russian), *Dokl. Akad. Nauk SSSR* **67**, 5–8.

D.A. Burgess,
(1957) The distribution of quadratic residues and non-residues, *Mathematika* **4**, 106-112

E. R. Canfield, P. Erdős and C. Pomerance,
(1983) On a problem of Oppenheim concerning "Factorisatio Numerorum", *J. Number Theory* **17**, 1–28.

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

R. Crandall and C. Pomerance,
(2001) Prime numbers. A computational perspective, *Springer-Verlag, New York*

E.S. Croot,
(2001) Smooth Numbers in Short Intervals, preprint

E.S. Croot, A. Granville and P. Tetali

(2006) Sharp Transitions in making squares, preprint

C. Dartyge,
(1996) Entiers de la forme n^2+1 sans grand facteur premier, *Acta Math. Hungar.* **72**, 1–34.

C. Dartyge, G. Martin and G. Tenenbaum,
(2001) Polynomial values free of large prime factors, *Periodica Math. Hungar.* **43**, 111–119.

J.-M. De Koninck,
(1994) On the largest prime divisors of an integer, in: *Extreme Value Theory and its applications*, (J. Galambos et. al., eds.), Kluwer, pp. 447-462

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

P. Erdős,
(1935) On the normal number of prime factors of $p-1$ and some other related problems concerning Euler's Φ-function, *Quart. J. Math. (Oxford)* **6**, 205–213.
(1955) On consecutive integers, *Nieuw Arch. Wisk.* (3) **3**, 124–128.

P. Erdős, C. L. Stewart and R. Tijdeman,
(1988) Some diophantine equations with many solutions, *Compos. Math.* **66**, 37-56.

J.-H. Evertse
(1984) On equations in S-units and the Thue-Mahler equation, *Invent. Math.* **75**, 561-584.

E. Fouvry and G. Tenenbaum,
(1991) Entiers sans grand facteur premier en progressions arithmétiques, *London Math. Soc.* (3) **63**, 449–494.
(1996) Répartition statistique des entiers sans grand facteur premier dans les progressions arithmtiques. (French) [Statistical distribution of integers without large prime factors in arithmetic progressions] *Proc. London Math. Soc.* (3) **72**, *no* 3, 481–514.

J. B. Friedlander
(1973) Integers without large prime factors, *Indag. Math.* **35**, 443–451.
(1989) Shifted primes without large prime factors, in: *Number Theory and Applications* (R. A. Mollin, ed.), Kluwer, pp. 393–401.

J. B. Friedlander and A. Granville,
(1993) Smoothing "smooth" numbers, *Philos. Trans. Roy. Soc. London Ser. A* **345**, 339–347.

J. B. Friedlander and J. C. Lagarias,
(1987) On the distribution in short intervals of integers having no large prime factor, *J. Number Theory* **25**, 249–273.

D. A. Goldston and K. S. McCurley,
(1988) Sieving the positive integers by large primes, *J. Number Theory* **28**, 94–115.

A. Granville,

(1989) On positive integers $\le x$ with prime factors $\le t\log x$, in: *Number Theory and Applications* (R. A. Mollin, ed.), Kluwer, pp. 403–422.
(1993a) Integers, without large prime factors, in arithmetic progressions. I, *Acta Math.* **170**, 255-273.
(1993b) Integers, without large prime factors, in arithmetic progressions. II, *Philos. Trans. Roy. Soc. London Ser.* A **345**, 349–362.
(2005) It is easy to determine whether a given integer is prime, *Bull. Amer. Math. Soc. (N.S.)* **42**, 3–38

A. Granville and K. Soundararajan
(2001a) Large character sums. *J. Amer. Math. Soc.* **14**(2), 365–397
(2001b) The spectrum of multiplicative functions. *Annals of Math.* **153**, 407–470
(2004) An upper bound for the unsieved integers up to x. *Acta Arith.* **115**, 305–328
(2006) Pretentious characters and the Polya-Vinogradov theorem, *J. Amer. Math. Soc*, to appear

A. Granville and T. Tucker,
(2002) It's as easy as *abc*. *Notices Amer. Math. Soc.* **49**(10), 1224–1231

J. L. Hafner,
(1993) On smooth numbers in short intervals under the Riemann Hypothesis, preprint.

H. Halberstam and H.-E. Richert,
(1974) *Sieve Methods,* Academic Press, London, New York, San Francisco.

G. Harman,
(1991) Short intervals containing numbers without large prime factors, *Math. Proc. Cambridge Philos. Soc.* **109**, 1–5.
(1993) Small fractional parts of additive forms, *Philos. Trans. Roy. Soc. London Ser. A* **345**, 327–338.
(1999) Integers without large prime factors in short intervals and arithmetic progressions, *Acta Arith.***91**, 279–289.
(2005) On the number of Carmichael numbers up to x, *Bull. London Math. Soc.*,**37**, 641–650.

D. Hensley,
(1987) The distribution of $\Omega(n)$ among numbers with no large prime factors, in: *Analytic Number Theory and Diophantine Problems* (A. Adolphson et al., eds.), Proc. of a Conf. at Oklahoma State University 1984, Birkhäuser, *Progress in Math.* **70**, 247–281.

A. Hildebrand,
(1984a) Integers free of large prime factors and the Riemann Hypothesis, *Mathematika* **31**, 258–271.
(1984b) Quantitative mean value theorems for nonnegative multiplicative functions. I. *J. London Math. Soc. (2)* **30**, 394–406.
(1985a) Integers free of large prime factors in short intervals, *Quart. J. Math. (Oxford) (2)* **36**, 57–69.
(1985b) On a conjecture of A. Balog, *Proc. Amer. Math. Soc.* **95**, 517–523.
(1986) On the number of positive integers $\le x$ and free of prime factors $> y$, *J. Number Theory* **22**, 289–307.
(1987a) On the number of prime factors of integers without large prime divisors, *J. Number Theory* **25**, 81–106.

(1987b) Quantitative mean value theorems for nonnegative multiplicative functions. II. *Acta Arith.* **48**, 209–260
(1989) Integer sets containing strings of consecutive integers, *Mathematika* **36**, 60–70.

A. Hildebrand and G. Tenenbaum,
(1986) On integers free of large prime factors, *Trans. Amer. Math. Soc.* **296**, 265–290.
(1993) On a class of difference differential equations arising in number theory, *J. d'Analyse Math.* **61**, 145–179.
(1993) Integers without large prime factors, *J. Théorie des Nombres.* **5**.

N. A. Hmyrova,
(1966) On polynomials with small prime divisors. II (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **30**, 1367–1372.

S. Hunter and J. Sorenson,
(1997) Approximating the number of integers free of large prime factors, *Math. Comp.* **66**, 1729–1741.

H. Iwaniec
(1978) On the problem of Jacobsthal, *Demonstratio Math.* **11**, 225–231.

N. M. Katz and P. Sarnak,
(1999) Zeroes of zeta functions and symmetry, *Bull. Amer. Math. Soc. (N.S.)* **36**, 1–26.

D. E. Knuth and L. Trabb Pardo,
(1976) Analysis of a simple factorization algorithm, *Theoret. Comput. Sci.* **3**, 321–348.

S. Konyagin and C. Pomerance,
(1997) On primes recognizable in deterministic polynomial time. *The mathematics of Paul Erds, I, Algorithms Combin.,* **13**, 176–198.

S. Konyagin and K. Soundararajan,
(1997) Two S-unit equations with many solutions, preprint

H. W. Lenstra
(1979) Miller's primality test, *Inform. Process. Lett.* **8**, 86–88.
(1987) Factoring integers with elliptic curves, *Ann. Math.* **126**, 649–673.

H. W. Lenstra, Jr., J. Pila and C. Pomerance
(1993) A hyperelliptic smoothness test, I, *Philos. Trans. Roy. Soc. London Ser. A* **345**, 397–408.

H. W. Lenstra, Jr. and C. Pomerance
(1992) A rigorous time bound for factoring integers, *J. Amer. Math. Soc.* **5**, 483–516.

U. V. Linnik
(1941) The large sieve. *C. R. (Doklady) Acad. Sci. URSS (N.S.)* **30**, 292–294.

E. Manstavičius
(1993) Remarks on elements of semigroups that are free of large prime factors, *Lithuanian Math. J.* **32**, 400–409.

G. Martin,
(2002) An asymptotic formula for the number of smooth values of a polynomial, *J. Number Theory* **93**, 108–182

H. Mikawa

(1989) Almost-primes in arithmetic progressions and short intervals. *Tsukuba J. Math.* **13** *no* 2, 387–401.

H.L. Montgomery and R.C. Vaughan,
(1977) Exponential sums with multiplicative coefficients, *Invent. Math* **43**, 69-82.

P. Moree,
(1993) *Psixyology and Diophantine equations*, Thesis, Leiden University.

P. Moree and C. L. Stewart,
(1990) Some Ramanujan–Nagell equations with many solutions, *Indag. Math. (N. S.)* **1**, 465-472.

K. K. Norton,
(1971) Numbers with small prime factors and the least kth power non residue, *Memoirs of the Amer. Math. Soc.* **106.**

R.E.A.C. Paley,
(1932) A theorem on characters, *J. London Math. Soc* **7**, 28-32.

C. Pomerance,
(1980) Popular values of Euler's function, *Mathematika* **27**, 84–89.
(1986) Fast, rigorous factorization and discrete logarithm algorithms, in: *Discrete Algorithms and Complexity (Kyoto, 1986)*, Academic Press, Boston.
(1989) Two methods in elementary analytic number theory, in: *Number Theory and Applications* (R. A. Mollin, ed.), Kluwer, pp. 135–161.
(1995) The role of smooth numbers in number-theoretic algorithms, *Pro. 1994 Int. Cong. Math.*, 411–422.
(1996) Multiplicative independence for random integers, *Analytic number theory, Vol. 2 (Allerton Park, IL, 1995), Progr. Math.,* **139** Birkhuser Boston, Boston, 703–711.
(1996) A tale of two sieves. *Notices Amer. Math. Soc.* **43**, *no* 3, 1473–1485.
(2001) Smooth numbers and the quadratic sieve, preprint.

C. Pomerance and I. Shparlinski,
(2005) Smooth orders and cryptographic applications,. *Lecture Notes in Comput. Sci.*, **2369**, 338–348.

R. A. Rankin,
(1938) The difference between consecutive prime numbers, *J. London Math. Soc.* **13**, 242–247.

T.N. Shorey
(1973/74) On gaps between numbers with a large prime factor. *II. Acta Arith.* **25**, 365–373.

K. Soundararajan,
(2001) Smooth polynomials: Analogies and asymptotics, preprint.
(2006) Smooth numbers in arithmetic progressions, personal communication.

P. Stevenhagen,
(2001) The number field sieve, preprint.

G. Tenenbaum,
(1990) *Introduction à la théorie analytique et probabiliste des nombres,* Publ. Inst. Elie Cartan, Vol. 13, Univ. Nancy 1.

(1993) Cribler les entiers sans grand facteur premier, in: R.C.Vaughan (ed.) Theory and applications of numbers without large prime factors, *Phil. Trans. Royal Soc. London, series A*, to appear.

R. Tijdeman,
(1973) On integers with many small prime factors, *Compositio Math.* **26**, 319–330.
(1974) On the maximal distance between integers composed of small primes, *Compositio Math.* **28**, 159–162.

R. C. Vaughan,
(1989) A new iterative method in Waring's problem, *Acta Math.* **162**, 1–71.
(1993) The use in additive number theory of numbers without large prime factors. *Philos. Trans. Roy. Soc. London Ser. A* **345**, *no* 1676, 363–376.

R. C. Vaughan and T.D. Wooley,
(2002) Waring's problem: a survey, in *Number theory for the millennium,* III (Urbana, IL, 2000), A K Peters, Natick, MA, 301–340.

D. Wolke,
(1971) Polynomial values with small prime divisors, *Acta Arith.* **19**, 327–333.

T.D. Wooley,
(1992) Large improvements in Waring's problem, *Annals Math.*(2) **135**, *no* 1, 135–164.

T.Z. Xuan,
(1995) Integers with no large prime factors, *Acta Arith.***69**, 303–327.
(1999) On smooth integers in short intervals under the Riemann hypothesis, *Acta Arith.***88**, 327–332.

Appendix A. Notation

Whenever ε is used in the text it means some arbitrarily small positive constant; whenever c or C is used it means some fixed, usually positive, constant, that we have not determined. When we write $f(x) := \dots$ this means that $f(x)$ is defined by the quantity on the right hand side of the equation.

As in analytic number theory:
$f(x) \ll g(x)$ and $f(x) = O(g(x))$ both mean that there exists a constant $c > 0$ such that $|f(x)| \le cg(x)$ for all x in the domain. If the domain is not specified then we usually mean for all sufficiently large x.
$f(x) \ll_{\varepsilon,k} g(x)$ means that the constant c above depends on the values of ε and k, but nothing else.
$f(x) \gg g(x)$ means that there exists a constant $c > 0$ such that $f(x) \ge c|g(x)|$ for all x in the domain.
$f(x) \asymp g(x)$ means that $f(x) \ll g(x)$ and $f(x) \gg g(x)$; in other words, there exists constants $C > c > 0$ such that $Cg(x) > f(x) > cg(x) > 0$ for all x in the domain.
$f(x) = o(g(x))$ means that $f(x)/g(x) \to 0$ as $x \to \infty$.
$f(x) \sim g(x)$ means that $f(x)/g(x) \to 1$ as $x \to \infty$.
$f(x) \lesssim g(x)$ means that $\limsup_{x\to\infty} f(x)/g(x) \le 1$. We analogously define $f(x) \gtrsim g(x)$
Finally, I have abused the notation $f(x) \approx g(x)$ to mean "it is true that f is more-or-less equal to g other than a small error for most values of x, but one needs to take care for extreme values of x as this equality might then be false. Similarly $f(x) \gtrapprox g(x)$ means "it is more-or-less true that $f(x) \ge g(x)$", and we give an analogous definition to $f(x) \lessapprox g(x)$. My reason for doing this is that in some of the more difficult analytic arguments I have

chosen to emphasize the main ideas, thereby neglecting what are sometimes very difficult error terms.

Appendix B. Values of the ρ-function

This table of values was kindly supplied by Dan Bernstein.

u	$\rho(u)$
1.0	1
1.1	$9.0468982020 \times 10^{-1}$
1.2	$8.1767844321 \times 10^{-1}$
1.3	$7.3763573553 \times 10^{-1}$
1.4	$6.6352776338 \times 10^{-1}$
1.5	$5.9453489190 \times 10^{-1}$
1.6	$5.2999637076 \times 10^{-1}$
1.7	$4.6937174895 \times 10^{-1}$
1.8	$4.1221333511 \times 10^{-1}$
1.9	$3.5814611384 \times 10^{-1}$
2.0	$3.0685281945 \times 10^{-1}$
2.1	$2.6040578017 \times 10^{-1}$
2.2	$2.2035713792 \times 10^{-1}$
2.3	$1.8579946160 \times 10^{-1}$
2.4	$1.5599126388 \times 10^{-1}$
2.5	$1.3031956184 \times 10^{-1}$
2.6	$1.0827244298 \times 10^{-1}$
2.7	$8.9418565728 \times 10^{-2}$
2.8	$7.3391580766 \times 10^{-2}$
2.9	$5.9878115989 \times 10^{-2}$
3.0	$4.8608388294 \times 10^{-2}$
3.1	$3.9322969543 \times 10^{-2}$
3.2	$3.1703444514 \times 10^{-2}$
3.3	$2.5464723875 \times 10^{-2}$
3.4	$2.0371779062 \times 10^{-2}$
3.5	$1.6229593244 \times 10^{-2}$
3.6	$1.2875434187 \times 10^{-2}$
3.7	$1.0172837816 \times 10^{-2}$
3.8	$8.0068721888 \times 10^{-3}$
3.9	$6.2803730622 \times 10^{-3}$
4.0	$4.9109256480 \times 10^{-3}$
4.1	$3.8285861740 \times 10^{-3}$
4.2	$2.9754747898 \times 10^{-3}$
4.3	$2.3050505145 \times 10^{-3}$
4.4	$1.7799424649 \times 10^{-3}$
4.5	$1.3701177412 \times 10^{-3}$
4.6	$1.0514448555 \times 10^{-3}$
4.7	$8.0455864484 \times 10^{-4}$
4.8	$6.1395732200 \times 10^{-4}$
4.9	$4.6727987480 \times 10^{-4}$

u	$\rho(u)$
5.00	$3.5472470048 \times 10^{-4}$
5.25	$1.7608050363 \times 10^{-4}$
5.50	$8.6018611125 \times 10^{-5}$
5.75	$4.1401923703 \times 10^{-5}$
6.00	$1.9649696355 \times 10^{-5}$
6.25	$9.1989056666 \times 10^{-6}$
6.50	$4.2503555174 \times 10^{-6}$
6.75	$1.9396328773 \times 10^{-6}$
7.00	$8.7456699538 \times 10^{-7}$
7.25	$3.8977236841 \times 10^{-7}$
7.50	$1.7178674921 \times 10^{-7}$
7.75	$7.4903397724 \times 10^{-8}$
8.00	$3.2320693044 \times 10^{-8}$
8.25	$1.3806442282 \times 10^{-8}$
8.50	$5.8405695633 \times 10^{-9}$
8.75	$2.4474945382 \times 10^{-9}$
9.00	$1.0162482828 \times 10^{-9}$
9.25	$4.1822758017 \times 10^{-10}$
9.50	$1.7063527387 \times 10^{-10}$
9.75	$6.9034598009 \times 10^{-11}$
10.00	$2.7701718379 \times 10^{-11}$
10.50	$4.3559526093 \times 10^{-12}$
11.00	$6.6448090707 \times 10^{-13}$
11.50	$9.8476421050 \times 10^{-14}$
12.00	$1.4197131651 \times 10^{-14}$
12.50	$1.9934633331 \times 10^{-15}$
13.00	$2.7291890306 \times 10^{-16}$
13.50	$3.6468386519 \times 10^{-17}$
14.00	$4.7606300143 \times 10^{-18}$
14.50	$6.0765096099 \times 10^{-19}$
15.00	$7.5899080047 \times 10^{-20}$
15.50	$9.2840614064 \times 10^{-21}$
16.00	$1.1129193527 \times 10^{-21}$
16.50	$1.3082753696 \times 10^{-22}$
17.00	$1.5090797501 \times 10^{-23}$
17.50	$1.7090489298 \times 10^{-24}$
18.00	$1.9013542117 \times 10^{-25}$
18.50	$2.0790325732 \times 10^{-26}$
19.00	$2.2354265872 \times 10^{-27}$
19.50	$2.3646133399 \times 10^{-28}$

u	$\rho(u)$
20	$2.4617828289 \times 10^{-29}$
21	$2.5480499999 \times 10^{-31}$
22	$2.4863827200 \times 10^{-33}$
23	$2.2937113098 \times 10^{-35}$
24	$2.0054951700 \times 10^{-37}$
25	$1.6658044238 \times 10^{-39}$
26	$1.3172582250 \times 10^{-41}$
27	$9.9360680532 \times 10^{-44}$
28	$7.1621362879 \times 10^{-46}$
29	$4.9417994435 \times 10^{-48}$
30	$3.2690443253 \times 10^{-50}$
31	$2.0762615316 \times 10^{-52}$
32	$1.2678257178 \times 10^{-54}$
33	$7.4525736262 \times 10^{-57}$
34	$4.2222207383 \times 10^{-59}$
35	$2.3080811963 \times 10^{-61}$
36	$1.2186971835 \times 10^{-63}$
37	$6.2216867863 \times 10^{-66}$
38	$3.0739529917 \times 10^{-68}$
39	$1.4711270490 \times 10^{-70}$
40	$6.8254908515 \times 10^{-73}$
41	$3.0725325059 \times 10^{-75}$
42	$1.3429776221 \times 10^{-77}$
43	$5.7038156797 \times 10^{-80}$
44	$2.3555177956 \times 10^{-82}$
45	$9.4649292957 \times 10^{-85}$
46	$3.7028093193 \times 10^{-87}$
47	$1.4112017836 \times 10^{-89}$
48	$5.2425207999 \times 10^{-92}$
49	$1.8994303041 \times 10^{-94}$
50	$6.7153344971 \times 10^{-97}$
55	$2.6127284053 \times 10^{-109}$
60	$5.8980293741 \times 10^{-122}$
65	$8.0954516406 \times 10^{-135}$
70	$7.0280992226 \times 10^{-148}$
75	$3.9915358890 \times 10^{-161}$
80	$1.5268607441 \times 10^{-174}$
85	$4.0351170225 \times 10^{-188}$
90	$7.5340256724 \times 10^{-202}$
95	$1.0137476011 \times 10^{-215}$

succ Centre-Ville, Montréal, QC H3C 3J7, Canada
E-mail address: andrew@dms.umontreal.ca