# TWO METHODS IN ELEMENTARY ANALYTIC NUMBER THEORY

CARL POMERANCE*
Department of Mathematics
University of Georgia
Athens, Georgia 30602
USA

**ABSTRACT.** This survey paper discusses the role of two elementary methods in getting good upper and lower bound estimates for a variety of counting functions and for computing maximal orders of certain arithmetic functions. The upper bound method involves introducing a new parameter, replacing a finite sum with an infinite sum which may be rewritten as a product, and then specifying an optimal choice for the new parameter. The lower bound method involves using combinatorial counting arguments to show that there are many numbers which can be built up with small primes or, with an extra step, showing there are many numbers built up with primes $p$ such that all the primes in $p-1$ are small. These methods will be illustrated in the context of several attractive problems: the distribution of numbers which have only small prime factors, the maximal order for the "number of factorizations" function, the maximal order for the number of solutions $m$ of $\varphi(m) = n$ where $\varphi$ is Euler's function, and the distribution of pseudoprimes. The last problem has practical applications for finding large random primes.

*Supported in part by an NSF grant.



*R. A. Mollin (ed.), Number Theory and Applications, 135–161.*

## §1. INTRODUCTION.

The usual definition of elementary number theory is one of exclusion. It does not use complex analysis, it does not deal with algebraic number fields, it is not probabilistic number theory, etc. Thus the title of this paper seems to be a contradiction in terms. What I mean by "elementary analytic number theory" is the use of elementary techniques in areas whose greatest successes are dominated by analytic methods. For example, the estimation of counting functions is such an area. Its central result, the prime number theorem, is proved in its sharpest form with analytic methods. I would consider the various elementary proofs of the prime number theorem as crowning achievements of elementary analytic number theory. Another achievement can be found in Brun's sieve and, in general, combinatorial sieve methods.

This paper will discuss, in the context of a few specific problems, variations on two elementary themes. One of these themes, sometimes referred to as "Rankin's method," can be used to obtain upper bounds, sometimes quite sharp ones, for certain counting functions. The other theme is concerned with lower bounds and has a distinctly combinatorial flavor.

The following problems will be discussed:

1. The distribution of smooth numbers, that is, numbers which have only small prime factors.
2. The maximal order of the function $f(n)$ which counts the number of unordered factorizations of $n$.
3. The maximal order of the function $N(n)$ which counts the number of solutions $m$ of $\varphi(m) = n$, where $\varphi$ is Euler's function.
4. The distribution of pseudoprimes.

Although this is primarily a survey paper, fairly complete proofs will be given. It is possible that some



of the material presented here would be of use in a graduate number theory course. In my opinion, to see the power and breadth of elementary methods better defines the role of analytic methods in number theory.

For balance, the reader might also consult Tenenbaum [26], a survey paper showing the role of analytic methods with some of these problems.

## §2. THE DISTRIBUTION OF SMOOTH NUMBERS.

Let $\psi(x,y)$ denote the number of natural numbers $n \le x$, whose largest prime factor, $P(n)$, satisfies $P(n) \le y$. By convention, we let $P(1) = 1$, so that if $x,y \ge 1$, we have $\psi(x,y) \ge 1$. The problem is to get good estimates for $\psi(x,y)$ for various ranges of $x,y$. If $y$ is fixed or tends to infinity very slowly in comparison to $x$, then $\psi(x,y)$ can be quite well approximated by counting lattice points in the simplex

$$\{(a_1,\dots,a_k): a_i \ge 0, \sum_{i=1}^{k} a_i \log p_i \le \log x\}$$

where $p_1,\dots,p_k$ are the primes up to $y$. The best results in this range are due to Ennola [6] and Specht [25].

If we let

$$u = (\log x)/\log y ,$$

so that $y = x^{1/u}$, then for fixed $u$, we have

$$\psi(x,y) \sim \rho(u)x , \tag{2.1}$$

where $\rho(u)$, the Dickman-deBruijn function, is the continuous solution of a certain differential-delay

equation. In fact, it is now known from work of Hildebrand, Maier, and Tenenbaum (see [15], [16], [18]), that (2.1) holds even for $y$ as small as $\exp((\log\log x)^c)$ , $c > 5/3$ .

The function $\rho(u)$ decays to 0 quite rapidly as $u \to \infty$ . It is known (deBruijn [3]) that

$$\rho(u) = \exp(-(1 + o(1))u \log u) \quad \text{as} \quad u \to \infty .$$

Thus from the work of Hildebrand, Maier, and Tenenbaum, we have the following weaker result.

**Theorem 2.1.** Suppose $\epsilon > 0$ is arbitrarily small, but fixed. If $y$ satisfies $\exp((\log x)^{\epsilon}) < y < \exp((\log x)^{1-\epsilon})$ , then

$$\psi(x,y) = x \cdot \exp(-(1 + o(1))u \log u)$$

uniformly as $x \to \infty$ , where $u = (\log x)/\log y$ .

This section will be devoted to an elementary proof of Theorem 2.1. The argument presented pre-dates the finer results of [15], [16], [18].

We begin with an upper bound argument. The idea was used in 1938 by Rankin [24] and was developed more fully in deBruijn [4]. The upper bound implicit in Theorem 2.1 is actually proved for a wider range of $y$ than is indicated in the statement.

The key idea occurs in the very first step. If $c > 0$, then

$$\text{(2.2)} \qquad \psi(x,y) = \sum_{\substack{n \le x \\ P(n) \le y}} 1 \le x^c \sum_{P(n) \le y} n^{-c} = x^c \prod_{p \le y} (1-p^{-c})^{-1} ,$$

where $p$ denotes a prime. We thus replace a finite sum with an infinite sum which has an Euler product. Our goal



is to estimate this product using prime number theory and then choose $c$ optimally in (2.2).

Note that if $c \ge 1/2 + \epsilon$ , then

$$\text{(2.3)} \qquad \prod_{p \le y} (1-p^{-c})^{-1} = \exp\left( - \sum_{p \le y} \log (1-p^{-c}) \right)$$

$$= \exp\left( \sum_{p \le y} p^{-c} + O_{\epsilon}(1) \right).$$

The final sum in (2.3) is easily estimated with the prime number theorem: if $0 < c < 1$ and $y^{1-c} \ge 2$ , then

$$\text{(2.4)} \qquad \sum_{p \le y} p^{-c} = \mathrm{li}(y^{1-c})\left(1 + O\left(\frac{1}{\log y}\right)\right) + O(|\log(1-c)|).$$

Assembling (2.2)-(2.4) and taking the logarithm suggests we look at the function

$$h(c) = c \log x + \mathrm{li}(y^{1-c}) ,$$

where $c$ satisfies $1/2 + \epsilon \le c < 1$ , $y^{1-c} \ge 2$ . Taking the derivative of $h(c)$ and setting it equal to 0 implies that our optimal value of $c$ should satisfy $y^{1-c} = (1-c)\log x$ . We shall choose a nearby value, namely

$$c = 1 - (\log u)/\log y .$$

Thus $x^c = u^{u}x$ , $\mathrm{li}(y^{1-c}) = o(u)$ , so that the assembly of (2.2)-(2.4) gives

$$\psi(x,y) \le x \cdot \exp(-u \log u + o(u))$$

for $(\log x)^{2+\epsilon} \le y \le x^{1/(\log\log x)^{1+\epsilon}}$

For the lower bound argument, we shall assume that $y$ is in the range stated by the theorem. We first consider the set $\mathcal{M}$ of integers $m$ composed of $[u]$ not necessarily distinct primes from the interval

$$(y^{1-1/\log u},\ y] .$$

Then every member $m$ of $\mathcal{M}$ satisfies $m \le y^{[u]} \le x$. Moreover,

$$\psi(x,y) \ge \sum_{m\in\mathcal{M}} \psi(\frac{x}{m},\ y^{1-1/\log u}) . \tag{2.5}$$

Indeed, every number of the form $mj \le x$ where $m \in \mathcal{M}$ and $P(j) \le y^{1-1/\log u}$ satisfies $P(mj) \le y$ and various pairs $m,j$ account for distinct products $mj$.

Let $z = y^{1-1/\log u}$, $w = y^{1-2/\log u}$, $u_0(m) = (\log(x/m))/\log z$. In the same way as we proved (2.5), we have

$$\psi(\frac{x}{m},z) \ge \sum_{j\in\mathcal{J}(m)} \psi(\frac{x}{mj},w) \tag{2.6}$$

where $\mathcal{J}(m)$ is the set of products of $[u_0(m)]$ not necessarily distinct primes from $(w,z]$. Now for any $m \in \mathcal{M}$, $j \in \mathcal{J}(m)$, we have

$$\frac{x}{mj} \ge \frac{x/m}{z^{[u_0(m)]}} = z^{\{u_0(m)\}} ,$$

where $\{\ \}$ denotes the fractional part. Thus, since $\sum_{w<p<z} 1/p = o(1)$, we have



$$\begin{aligned}\psi(\frac{x}{mj},w) &\ge \psi(z^{\{u_0(m)\}},w)\\ &\ge [z^{\{u_0(m)\}}] - \sum_{w<p<z} [z^{\{u_0(m)\}}/p]\\ &>> z^{\{u_0(m)\}}\end{aligned}$$

uniformly for $m \in \mathcal{M}$, $j \in \mathcal{J}(m)$.

Putting this estimate in (2.6), we have

$$\begin{aligned}\psi(\frac{x}{m},z) &>> \sum_{j\in\mathcal{J}(m)} z^{\{u_0(m)\}} = z^{\{u_0(m)\}}|\mathcal{J}(m)|\\ &\ge z^{\{u_0(m)\}} \frac{1}{[u_0(m)]!} (\pi(z)-\pi(w))^{[u_0(m)]}\\ &\ge z^{\{u_0(m)\}} z^{[u_0(m)]}/((u_0(m)+1)2\log z)^{u_0(m)}\\ &= (x/m)/((u_0(m)+1)2\log z)^{u_0(m)} ,\end{aligned} \tag{2.7}$$

where, for the last inequality, we used $\pi(z) - \pi(w) \ge z/(2\log z)$, which is valid for $x$ (and hence $z$) sufficiently large. The lower bound for $|\mathcal{J}(m)|$ used in (2.7) comes from the combinatorial counting principal for the number of ways of choosing $k$ not necessarily distinct things from a t-element set: it is at least $t^k/k!$.

We have $m \ge z^{[u]}$, so that

$$\begin{aligned}0 \le u_0(m) &\le \frac{\log(x/z^{[u]})}{\log z} = \frac{\log x}{\log z} - [u]\\ &= \frac{u \log u}{\log u - 1} - [u] \le \frac{u}{\log u - 1} + 1 .\end{aligned} \tag{2.8}$$

Since

$$\text{loglog } z \le \text{loglog } y = \mathcal{O}_\epsilon(\log u) ,$$

(2.8) implies there is some constant $K_\epsilon$ depending only on the choice of $\epsilon$ with

$$1 \le ((u_0(m) + 1)2\log z)^{u_0(m)} \le \exp(K_\epsilon u) ,$$

for all $m \in \mathcal{M}$. Thus from (2.7) we have

$$\psi(\frac{x}{m}, z) >> \frac{x}{m} \exp(-K_\epsilon u) \tag{2.9}$$

uniformly for all $m \in \mathcal{M}$.

Putting (2.9) in (2.5) we have

$$\psi(x,y) >> x \cdot \exp(-K_\epsilon u) \sum_{m\in\mathcal{M}} \frac{1}{m}$$

$$\ge x \cdot \exp(-K_\epsilon u) \cdot \frac{1}{[u]!} \Big(\sum_{z<p\le y} \frac{1}{p}\Big)^{[u]}$$

$$\ge x \cdot \exp(-u(\log u + \text{loglog } u + \mathcal{O}_\epsilon(1))) , \tag{2.10}$$

since $\sum_{z<p\le y} 1/p \sim 1/\log u$. The lower bound for $\sum_{m\in\mathcal{M}} 1/m$ used in (2.10) comes from the multinomial theorem. Note that (2.10) completes the proof of the theorem.

The combinatorial arguments used for the lower bound for $\psi(x,y)$ will be echoed in the following sections in various ways. The argument just presented is a condensed version of the proof in [5].



## §3. HIGHLY FACTORABLE NUMBERS.

Let $f(n)$ denote the number of unordered factorizations of $n$ into factors exceeding 1. By convention, we let $f(1) = 1$. Then, for example, $f(12) = 4$, since 12 has the factorizations $12$, $2\cdot 6$, $3\cdot 4$, $2\cdot 2\cdot 3$. We say a natural number $n$ is <u>highly factorable</u> if $f(n) > f(m)$ for all $m < n$. Thus highly factorable numbers are champion numbers for the function $f(n)$ just as Ramanujan's highly composite numbers are champion numbers for the divisor function.

Let

$$F^*(x) = \max\{f(n): n \le x\}$$

and let

$$L(x) = \exp(\log x \, \text{logloglog } x/\text{loglog } x) .$$

In this section we shall prove the following result.

**Theorem 3.1.** As $x \to \infty$, $F^*(x) = x/L(x)^{1+o(1)}$.

As a consequence, we have that if $n$ is highly factorable, then $f(n) = n/L(n)^{1+o(1)}$. Theorem 3.1 is the principal result of [5], which corrects a paper of Oppenheim [19] where it is claimed that $F^*(x) = x/L(x)^{2+o(1)}$.

Let $p_i$ denote the i-th prime. It is clear that if $n$ is any natural number, then there is a number $m \le n$ such that the prime factorization of $m$ is $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ for some $k$, $a_1 \ge a_2 \ge \dots \ge a_k$, and $f(m) \ge f(n)$. Further, if $n$ is sufficiently large, then the prime

number theorem implies $p_k \le 2\log n$. Thus $F^*(x) = f(m)$ for some $m \le x$ with $P(m) \le 2\log x$, for $x$ sufficiently large. In particular, for all large $x$ and any $c > 0$,

$$(3.1) \qquad F^*(x) \le \sum_{\substack{n\le x \\ P(n)\le 2\log x}} f(n) \le x^c \sum_{P(n)\le 2\log x} f(n)/n^c .$$

This inequality is similar to (2.2), except that we cannot now replace the last sum with an Euler product since the function $f(n)$ is not multiplicative. However, a generalization of a formula of MacMahon [17] gives us something very similar:

$$(3.2) \qquad \sum_{P(n)\le 2\log x} f(n)/n^{-c} = \prod_{\substack{P(m)\le 2\log x \\ m>1}} (1-m^{-c})^{-1}$$

which can be easily seen by replacing $(1-m^{-c})^{-1}$ with $1 + m^{-c} + m^{-2c} + \dots$ and multiplying out the product. It is easy to show that the right side of (3.2) is convergent for $c > 0$ and so the left side is as well.

Assuming $c \ge 1/2 + \epsilon$, we have from (3.1) and (3.2) that

$$F^*(x) \le x^c \prod_{\substack{P(m)\le 2\log x \\ m>1}} (1-m^{-c})^{-1}$$

$$\ll_\epsilon x^c \exp\left[\sum_{P(m)\le 2\log x} m^{-c}\right]$$

$$= x^c \exp\left[\prod_{p\le 2\log x} (1-p^{-c})^{-1}\right]$$



$$(3.3) \qquad = x^c \exp \exp\left[\sum_{p\le 2\log x} p^{-c} + O_\epsilon(1)\right] .$$

Using (2.4) for $\sum_{p\le 2\log x} p^{-c}$ and choosing $c = 1 - (\log\log\log x)/\log\log x$, we have $x^c = x/L(x)$ and $\sum_{p\le 2\log x} p^{-c} = O((\log\log x)/\log\log\log x)$, so that (3.3) implies $F^*(x) \le x/L(x)^{1+o(1)}$.

The proof of the lower bound is not only similar to the proof of the lower bound in Theorem 2.1, but it actually uses this theorem as well. Let $\ell = \log\log x$ and let

$$\mathcal{F} = \{f: 1 < f \le e^{\ell^2}, P(f) \le \log x\} .$$

From Theorem 2.1 it follows that

$$|\mathcal{F}| = e^{\ell^2 - (1+o(1))\ell \log \ell} .$$

Let $k = [(\log x)/(\log\log x)^2]$. Note that if $f_1, f_2, \dots, f_k \in \mathcal{F}$, then $n = f_1 f_2 \dots f_k \le e^{k\ell^2} \le x$. Not only is this integer $n \le x$, but $n$ has been endowed with the factorization $f_1 f_2 \dots f_k$ and $P(n) \le \log x$. We thus have

$$(3.4) \qquad \sum_{\substack{n\le x \\ P(n)\le \log x}} f(n) \ge \frac{1}{k!} |\mathcal{F}|^k = \frac{1}{k!} e^{k(\ell^2 - (1+o(1))\ell \log \ell)} = x/L(x)^{1+o(1)} ,$$

since there are at least $\frac{1}{k!}|\mathcal{F}|^k$ choices of unordered $k$-tuples drawn from $\mathcal{F}$.

From (3.4) we derive

$$F^*(x) \geq \max\{f(n): n \leq x,\ P(n) \leq \log x\}$$

$$(3.5) \qquad \geq \psi(x,\log x)^{-1} \sum_{\substack{n\leq x \\ P(n)\leq \log x}} f(n)$$

$$\geq x\, L(x)^{-1+o(1)}\ \psi(x,\log x)^{-1} .$$

Thus to finish the proof of Theorem 3.1, we have only to note that

$$(3.6) \qquad \psi(x,\log x) = L(x)^{o(1)} ,$$

since putting (3.6) into (3.5) gives $F^*(x) \geq x/L(x)^{1+o(1)}$. In fact the lattice point argument mentioned in the first paragraph of section 2 can be used to show $\psi(x,\log x) = \exp(0(\log x/\log\log x))$ which implies (3.6). The same estimate can be seen from (2.2) by choosing $c = 1/\log\log x$ and estimating the product on the right of (2.2) carefully. From a result of Erdös [10], we have the finer estimate

$$\psi(x,\log x) = 4^{(1+o(1))(\log x)/\log\log x} ,$$

which also can be established by elementary methods.

## §4. POPULAR VALUES OF EULER'S FUNCTION.

Some numbers $n$ occur many times as a value of Euler's function $\varphi$. For example 24 has 10 pre-images under $\varphi$, namely 35, 39, 45, 52, 56, 70, 72, 78, 84, 90. In a remarkable paper from 1935, Erdös [7] showed among other results, that there is a constant $c > 0$ such that



$N(n) \geq n^c$ for infinitely many $n$, where $N(n)$ is the number of $m$ with $\varphi(m) = n$. Moreover, Erdös conjectured that $c$ can be taken arbitrarily close to 1. In this section we shall discuss this problem.

Let

$$N^*(x) = \max\{N(n): n \leq x\} .$$

By an argument very similar to the upper bound in Theorem 3.1, we have the following result which first appeared in [20].

**Theorem 4.1.** As $x \to \infty$, $N^*(x) \leq x/L(x)^{1+o(1)}$.

Proof. Let $n \leq x$ be such that $N(n) = N^*(x)$. If $x$ is sufficiently large and if $\varphi(m) = n$, then $m \leq z := 2x \log\log x$. This follows from the prime number theorem - see Hardy and Wright [14], Theorem 328. Thus for any $c > 0$,

$$N(n) = \sum_{\substack{m\leq z \\ \varphi(m)=n}} 1 \leq z^c \sum_{\varphi(m)=n} m^{-c} \leq z^c \sum_{p|m\Rightarrow p-1|n} m^{-c}$$

$$(4.1) \qquad = z^c \prod_{p-1|n} (1-p^{-c})^{-1} .$$

We now assume that $c \geq 1/2 + \epsilon$, so that (4.1) implies

$$N(n) <<_\epsilon z^c \exp\left(\sum_{p-1|n} p^{-c}\right) < z^c \exp\left(\sum_{d|n} d^{-c}\right)$$

$$(4.2) \qquad < z^c \exp\left(\prod_{p|n} (1-p^{-c})^{-1}\right)$$

$$= z^c \operatorname{expexp}\left[\sum_{p|n} p^{-c} + \theta_\epsilon(1)\right] .$$

As in the argument prior to (3.1), we have

$$\sum_{p|n} p^{-c} \le \sum_{p \le 2\log x} p^{-c}$$

for $x$ sufficiently large. Putting this estimate into (4.2) we get almost exactly (3.3). Choosing the same value of $c$ as in section 3, namely $c = 1 - (\log\log\log x)/\log\log x$, thus gives $N^*(x) \le x/L(x)^{1+o(1)}$, which proves the theorem.

The same themes as in the preceding sections appear to be working very well for $N^*(x)$. However attempting to prove a lower bound, we run into a large hurdle. To prove there is some $n$ with $N(n)$ very large we should like to show there are many $m$ with $P(\varphi(m))$ small, so that $\varphi$ maps a large set to a small set. But for $P(\varphi(m))$ to be small, we shall need $P(p-1)$ small for each prime factor $p$ of $m$. Suppose we knew the following:

**Hypothesis 4.2.** The number $M(x)$ of primes $p \le x$ with $P(p-1) \le e^{(\log x)^{1/2}}$ satisfies $M(x) >> \psi(x, e^{(\log x)^{1/2}})/\log x$.

Then we could prove $N^*(x) = x/L(x)^{1+o(1)}$. In fact this follows from a weaker hypothesis as we shall now see. Note that Theorem 2.1 implies



$$\psi(x, e^{(\log x)^{1/2}}) = x/\exp((\tfrac{1}{2} + o(1))(\log x)^{1/2} \log\log x) .$$

**Hypothesis 4.3.** With $M(x)$ defined as in Hypothesis 4.2, we have

$$M(x) = x/\exp((\tfrac{1}{2} + o(1))(\log x)^{1/2} \log\log x) .$$

**Theorem 4.4.** Assuming Hypothesis 4.3, we have $N^*(x) = x/L(x)^{1+o(1)}$.

Proof. We have already seen in Theorem 4.1 that we have $N^*(x) \le x/L(x)^{1+o(1)}$ unconditionally. We now show the reverse inequality. Let $\ell = \log\log x$ as in the proof of Theorem 3.1, and let

$$\mathcal{P} = \{p \text{ prime}: \ p \le e^{\ell^2}, \ P(p-1) \le \log x\} .$$

Then from Hypothesis 4.3, we have

$$|\mathcal{P}| = e^{\ell^2 - (1+o(1))\ell \log \ell} .$$

Thus $\mathcal{P}$ is entirely analogous to the set $\mathcal{I}$ constructed in the proof of Theorem 3.1. Let $k = [(\log x)/(\log\log x)^2]$. Instead of choosing unordered k-tuples from $\mathcal{P}$, we choose k-element subsets. The number of these subsets is

$$\binom{|\mathcal{P}|}{k} \ge \left[\frac{|\mathcal{P}|}{k}\right]^k = k^{-k} \, e^{k(\ell^2 - (1+o(1))\ell \log \ell)}$$

(4.3) $\qquad = x/L(x)^{1+o(1)}$ .

For each k-element subset, we multiply these primes together forming an integer $m \le x$ with the property that $P(\varphi(m)) \le \log x$ . Thus $\varphi$ maps a set of size $\binom{|\mathcal{P}|}{k}$ to a set of size $\psi(x,\log x)$ . From (4.3) and (3.6), we have that some $n$ counted by $\psi(x,\log x)$ has at least $x/L(x)^{1+o(1)}$ pre-images under $\varphi$ , that is, $N^*(x) \ge x/L(x)^{1+o(1)}$ .

Although Hypotheses 4.2 and 4.3 appear hopeless to prove at this time, we can salvage something.

**Definition 4.5.** Let $E$ denote the supremum of the set of $\alpha \in [0,1)$ for which there is some $c_\alpha > 0$ with the property that the number of primes $p \le x$ with $P(p-1) \le x^{1-\alpha}$ exceeds $c_\alpha x/\log x$ for all $x \ge 2$ .

In [7], Erdös used Brun's method to show that $E > 0$ and conjectured that $E = 1$ . Wooldridge [27] used Selberg's sieve to show $E \ge 3-2\sqrt{2} = .17157...$ . In [20], Bombieri's theorem and some results of Hooley and Iwaniec concerning the Brun-Titchmarsh theorem on average are used to show that $E > 5/9$ . Just this year, Friedlander [13] used his extension of Bombieri's theorem with Bombieri and Iwaniec to show $E \ge 1 - (2\sqrt{e})^{-1} = .69673...$ . Other relevant papers on the subject are Balog [1] and Fouvry and Grupp [12].

**Theorem 4.6.** As $x \to \infty$ we have $N^*(x) \ge x^{E+o(1)}$ .

Proof. Fix an arbitrary $\epsilon$ with $0 < \epsilon < E$ and let $\beta = (1 - E + \epsilon)^{-1}$ . Let $\mathcal{P}$ be the set of primes $p \le (\log x)^\beta$ with $P(p-1) \le \log x$ . From the definition



of $E$ , we have

(4.4) $\qquad |\mathcal{P}| \gg (\log x)^\beta/\log\log x$ .

Let $u = [(\log x)/(\beta \log\log x)]$ and let $\mathcal{M}$ be the set of integers composed of $u$ distinct primes from $\mathcal{P}$ . Then each $m \in \mathcal{M}$ satisfies $m \le x$ and $P(\varphi(m)) \le \log x$ . Moreover, from (4.4),

$$|\mathcal{M}| = \binom{|\mathcal{P}|}{u} \ge \left(\frac{|\mathcal{P}|}{u}\right)^u = x^{(\beta-1)/\beta+o(1)} .$$

Since $\varphi$ maps $\mathcal{M}$ to a set of size $\psi(x,\log x) = x^{o(1)}$ (see (3.6)), there is some $n$ counted by $\psi(x,\log x)$ with $x^{(\beta-1)/\beta+o(1)}$ pre-images under $\varphi$ . But

$$(\beta - 1)/\beta = E - \epsilon ,$$

so that $N^*(x) \ge x^{E-\epsilon+o(1)}$ . Since $\epsilon$ can be arbitrarily small we have our theorem.

Theorem 4.6 was first proved by Erdös in [7].

## § 5. THE DISTRIBUTION OF PSEUDOPRIMES.

Since Fermat we have known that if $n$ is prime and $n \nmid a$, then $a^{n-1} \equiv 1 \pmod n$. This congruence can sometimes hold when $n$ is composite. For example, it holds for all $n$ when $a = 1$ , it holds for $n = 341 = 11 \cdot 31$ when $a = 2$, and it holds for $n = 91$ when $a = 3$ . If $n$ is a composite natural number and $a^{n-1} \equiv 1 \pmod n$, then $n$ is said to be a pseudoprime to the base $a$ . Let $P_a(x)$ denote the number of base $a$ pseudoprimes $n \le x$ .

One might conjecture that for a fixed $a \ne \pm 1$ , the base $a$ pseudoprimes are rare compared with primes, that is,

that $P_a(x) = o(\pi(x))$. This result was first proved by Erdös in [8]. The strongest result of this type is found in [21] : if $a \neq \pm 1$ , there is an $x_0(a)$ such that

$$(5.1) \qquad P_a(x) \leq x/L(x)^{1/2} \quad \text{for all } x \geq x_0(a) ,$$

with $L(x)$ the same as in sections 3 and 4. This proof is a bit technical and the theorem is probably not best possible. I conjecture that for every $a$ with $|a| > 1$ we have $P_a(x) = x/L(x)^{1+o(1)}$ .

It will probably be more illuminating to work through the proof of a similar theorem that gives a stronger result for a more restrictive set of numbers. Some composite numbers $n$ , such as 561, 1105, and 1729, have the property that they are "absolute pseudoprimes," that is, they are pseudoprimes to every base to which they are coprime. These numbers are also called Carmichael numbers.

Let $\lambda(n)$ denote the maximal order for an element in the multiplicative group $(\mathbb{Z}/n)^*$ . By the theorem on the primitive root, $\lambda(p^a) = p^{a-1}(p - 1)$ for an odd prime $p$ or for $p^a = 2$ or $4$ . Also $\lambda(2^a) = 2^{a-2}$ for $a \geq 3$ . Further, from the Chinese remainder theorem, it is easy to see that $\lambda(n) = \text{lcm}\,\{\lambda(p^a): p^a \| n\}$ . It is also easy to see that $a^{\lambda(n)} \equiv 1 \pmod n$ for all $a \in (\mathbb{Z}/n)^*$ . Thus we have the following simple criterion: the composite integer $n$ is a Carmichael number if and only if $\lambda(n) | n - 1$ .

In 1956, Erdös [9] proved that $C(x)$ , the number of Carmichael numbers up to $x$ , satisfies $C(x) \leq x/L(x)^c$ for some $c > 0$ and $x$ large. This was improved to $c = 1 + o(1)$ in [23]. We now give a simplified proof.

**Theorem 5.1.** As $x \to \infty$ , $C(x) \leq x/L(x)^{1+o(1)}$ .

Proof. If $d$ is a natural number, we ask how many Carmichael numbers $n \leq x$ are multiples of $d$ . If $d|n$, then $\lambda(d)|\lambda(n)$ , so that the condition $\lambda(n)|n - 1$ implies $\lambda(d)|n - 1$ . Thus the number $C_{(d)}(x)$ of Carmichael numbers $n \leq x$ with $d|n$ is at most the number of composite numbers $n \leq x$ with

$$(5.2) \qquad n \equiv 0 \pmod d, \quad n \equiv 1 \pmod{\lambda(d)} .$$

Thus for $C_{(d)}(x)$ to be positive, it is necessary that $(d,\lambda(d)) = 1$ . We thus have by the Chinese remainder theorem:

$$(5.3) \qquad C_{(d)}(x) \leq 1 + \left[\frac{x}{d\lambda(d)}\right] .$$

Further, if $d = p$ is prime, then the solution $n = p$ of (5.2) should not be counted since it is not composite. Thus for $p$ prime, we have

$$(5.4) \qquad C_{(p)}(x) \leq \left[\frac{x}{p(p - 1)}\right] .$$

From (5.4) we quickly see that we can restrict our attention to Carmichael numbers $n \leq x$ satisfying $P(n) \leq L(x)$ , for the number of other Carmichael numbers up to $x$ is at most

$$\sum_{p>L(x)} C_{(p)}(x) \leq x \sum_{p>L(x)} \frac{1}{p(p - 1)} = o(x/L(x)).$$

Thus it will be sufficient to show that $C'(x) \leq x/L(x)^{1+o(x)}$ where $C'(x)$ is the number of Carmichael numbers $n$ with $x/L(x) < n \leq x$ and $P(n) \leq L(x)$ . If $n$ is counted by $C'(x)$ , then $n$ has a divisor $d$ satisfying

(5.5) $\quad x/L(x)^2 < d \le x/L(x)$ .

Indeed, $n$ has a divisor $d$ satisfying $d > x/L(x)^2$, namely $n$ itself. But since $n > x/L(x)$ and $P(n) \le L(x)$, the least such divisor $d$ must also satisfy $d \le x/L(x)$.

Thus by (5.3),

$$C'(x) \le \sum_d{}'\left(1 + \left[\frac{x}{d\lambda(d)}\right]\right),$$

where $\sum'$ denotes a sum over $d$ satisfying (5.5). We thus have

$$C'(x) \le \frac{x}{L(x)} + x \sum_{d\lambda(d)\le x}{}' \frac{1}{d\lambda(d)}$$

(5.6) $$= \frac{x}{L(x)} + x \sum_{m<L(x)^2} \frac{1}{m} \sum_{\lambda(d)=m}{}' \frac{1}{d} .$$

We now treat the inner sum in (5.6) by partial summation:

(5.7) $$\sum_{\lambda(d)=m}{}' \frac{1}{d} = \frac{L(x)}{x} \sum_{\lambda(d)=m}{}' 1 + \int_{x/L(x)^2}^{x/L(x)} \frac{1}{t^2} \sum_{\substack{\lambda(d)=m \\ d\le t}}{}' 1 \, dt .$$

We thus shall be interested in obtaining an upper bound for $\Lambda(t,m)$, the number of $d \le t$ with $\lambda(d) = m$.

**Lemma 5.2.** As $t \to \infty$, $\Lambda(t,m) \le t/L(t)^{1+o(1)}$ uniformly for all $m$.



Before we prove the lemma, we show how the theorem follows from it. From (5.7) and the lemma,

$$\sum_{\lambda(d)=m}{}' \frac{1}{d} \le \frac{L(x)}{x} \Lambda\left(\frac{x}{L(x)}, m\right) + \int_{x/L(x)^2}^{x/L(x)} \frac{1}{t^2} \Lambda(t,m)\,dt$$

$$\le L(x)^{-1+o(1)}$$

uniformly for all $m$. Putting this in (5.6) immediately gives $C'(x) \le x/L(x)^{1+o(1)}$, which as we have noted, is sufficient for the theorem.

To prove the lemma we resort to the trick used in the previous sections. Note that we may assume $m \le t$, for otherwise $\Lambda(t,m) = 0$. We have for any $c > 0$,

$$\Lambda(t,m) \le t^c \sum_{\lambda(d)=m} d^{-c} \le t^c \sum_{p|d \Rightarrow p-1|m} d^{-c}$$

$$= t^c \prod_{p-1|m} (1 - p^{-c})^{-1} .$$

We now have an expression that is essentially the same as the right side of (4.1), so that the lemma follows from the rest of the proof of Theorem 4.1.

Although we still do not know if there are infinitely many Carmichael numbers, probably Theorem 5.1 is close to best possible. An elaboration of a heuristic argument given by Erdös in [9], suggests that $C(x) \ge x/L(x)^{1+o(1)}$. This argument is very similar to the proof of Theorem 4.4; we now sketch it.

Let $P'(n)$ denote the largest prime power factor of $n$. If $M'(x)$ is the number of primes $p \le x$ with $P'(p-1) \le e^{(\log x)^{1/2}}/(\log x)^{1/2}$, we conjecture, analogously to

Hypothesis 4.3, that

$$M'(x) = x/\exp((\tfrac{1}{2} + o(1))(\log x)^{1/2}\operatorname{loglog} x) \quad (5.8)$$

It is not hard to show from Theorem 2.1 that the number of $n \le x$ with $P'(n) \le e^{(\log x)^{1/2}}/(\log x)^{1/2}$ satisfies the same estimate, so that (5.8) is perhaps a reasonable conjecture.

As in the two previous sections, let $\ell = \operatorname{loglog} x$. Let $A = A(x)$ denote the least common multiple of the integers up to $(\log x)/\operatorname{loglog} x$ $(=e^{\ell}/\ell)$. If $\mathcal{M}$ is the set of products of $[(\log x)/(\operatorname{loglog} x)^2]$ distinct primes $p$ with $\log x \le p \le e^{\ell^2}$ and $p - 1 | A$, then from (5.8) and the argument in section 4 (see (4.3)) we have

$$|\mathcal{M}| \ge x/L(x)^{1+o(1)} .$$

Note that every member $m$ of $\mathcal{M}$ is composite, $m \le x$, $(m,A) = 1$, and $\lambda(m) | A$.

We now make a second heuristic assumption. We conjecture that the members of $\mathcal{M}$ are approximately uniformly distributed among the residue classes mod $A$ that are coprime to $A$. If so, we would expect about $|\mathcal{M}|/A$ members $m$ of $\mathcal{M}$ to satisfy $m \equiv 1 \pmod A$. But

$$A \le \exp(O(\log x/\operatorname{loglog} x)) = L(x)^{o(1)} ,$$

so we are conjecturing there are at least $x/L(x)^{1+o(1)}$ members $m$ of $\mathcal{M}$ with $m \equiv 1 \pmod A$. But since $m \in \mathcal{M}$ implies $\lambda(m) | A$, each such $m$ is a Carmichael number.

It is possible to show there are infinitely many pseudoprimes to the base $a$ for any fixed $a$. The best result of this sort is in [22]: for any fixed $a \ne 0$, $P_a(x) \ge \exp((\log x)^{E/(E+1)+o_a(1)})$, where $E$ is given in



Definition 4.5. Thus, for example, using Friedlander's result that $E \ge 1 - (2\sqrt{e})^{-1}$, we have

$$P_2(x) \ge \exp((\log x)^{85/207}) \quad \text{for} \quad x \ge x_0 .$$

Again, the conjecture is that for each $a \ne 0, \pm 1$ we have $P_a(x) = x/L(x)^{1+o(1)}$.

Better results can be proved if we average over $a$. In [11], it is shown that

$$x^{E+o(1)} \le \frac{1}{x} \sum_{1<a\le x} P_a(x) \le x/L(x)^{1+o(1)} . \quad (5.9)$$

The upper bound proof is similar to the proof of Theorem 5.1 and the lower bound proof is similar to the proof of Theorem 4.6. Assuming Hypothesis 4.3 it is possible to show that the upper bound is sharp.

Finally we note that the upper bound in (5.9) actually has a "real world" application, as noted in [2]. Namely, if you would like to quickly find a random prime number $p \le x$, you might try the following random algorithm. Choose a random number $n \le x$ and a random integer $a$ with $1 < a < n$. Keep choosing such random pairs until one is found that satisfies $a^{n-1} \equiv 1 \pmod n$. The expected number of choices before a good pair is found is $\log x$, by the prime number theorem and (5.9). The probability that the number $n$ found in this fashion is composite is at most $L(x)^{-1+o(1)}$, by (5.9). Although not proved prime, the number $n$ probably is prime, and might be used as such in a practical application. (If one wants a procedure which has a higher probability that the output $n$ is prime, one can further subject $n$ to a series of "strong" pseudoprime tests - see [2].)

The expression "$o(1)$" that appears in the upper bound in (5.9) detracts from (5.9) as a practical theorem. However the methods used to prove the upper bound in (5.9) can be

made effective and would be an interesting subject for further research. Some preliminary results in this direction have been found by Kim Su Hee in her upcoming master's thesis at the University of Georgia.



## References


1. A. Balog, 'p+a without large prime factors', Séminaire de Théorie des Nombres, Bordeaux (1983-84), no. 31, 5 pp.

2. P. Beauchemin, G. Brassard, C. Crépeau, C. Goutier, and C. Pomerance, 'The generation of random numbers that are probably prime', J. Cryptology **1**(1988), 53-64.

3. N.G. deBruijn, 'The asymptotic behavior of a function occurring in the theory of primes', J. Indian Math. Soc. (N.S.) **15**(1951), 25-32.

4. N.G. deBruijn, 'On the number of number of positive integers $\leq x$ and free of prime factors $> y$ ', Nederl. Akad. Wetensch. Proc. Ser. A **54**(1951), 50-60; II, **69**(1966), 239-247.

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

6. V. Ennola, 'On numbers with small prime divisors', Ann. Acad. Sci. Fenn. Ser. A I (1969) No. 440, 16 pp.

7. P. Erdös, 'On the normal number of prime factors of $p - 1$ and some other related problems concerning Euler's $\varphi$-function', Quant. J. Math.(Oxford Ser.) **6**(1935), 205-213.

8. P. Erdös, 'On almost primes', American Math. Monthly **57**(1950), 404-407.

9. P. Erdös, 'On pseudoprimes and Carmichael numbers', Publ. Math. Debrecen **4**(1956), 201-206.

10. P. Erdös, 'Problem and solution Number 136', Wisk. Opgaven **21**(1963), 133-135.

11. P. Erdös and C. Pomerance, 'On the number of false witnesses for a composite number', Math. Comp. **46**(1986), 259-279.

12. E. Fouvry and F. Grupp, 'On the switching principle in sieve theory', J. Reine Angew. Math. **370**(1986), 101-126.

13. J.B. Friedlander, 'Shifted primes without large prime facotrs', these proceedings.

14. G.H. Hardy and E.M. Wright, Introduction to the Theory of Numbers, 4th ed., Oxford Univ. Press, London, 1965.

15. A. Hildebrand, 'On the number of positive integers $\leq x$ and free of prime factors $> y$', J. Number Theory **22**(1986), 289-307.

16. A Hildebrand and G. Tenenbaum, 'On integers free of large prime factors', Trans. Amer. Math. Soc. **296**(1986), 265-290.

17. P.A. MacMahon, 'The enumeration of the partitions of multipartite numbers', Proc. Cambridge Philos. Soc. **22**(1925), 951-963.

18. H. Maier, 'On integers free of large prime factors', unpublished manuscript.

19. A. Oppenheim, 'On an arithmetic function', J. London Math. Soc. **1**(1926), 205-211; II **2**(1927), 123-130.



20. C. Pomerance, 'Popular values of Euler's function', Mathematika **27**(1980), 84-89.

21. C. Pomerance, 'On the distribution of pseudoprimes', Math. Comp. **37**(1981), 587-593.

22. C. Pomerance, 'A new lower bound for the pseudoprime counting function', Illinois J. Math. **26**(1982), 4-9.

23. C. Pomerance, J.L. Selfridge, and S.S. Wagstaff, Jr., 'The pseudoprimes to $25 \cdot 10^9$', Math. Comp. **35**(1980), 1003-1026.

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

25. W. Specht, 'Zahlenfolgen mit endlich vielen Primteilern', Bayer. Akad. Wiss. Math. - Natur. Abt. S.-B. **1948**(1949), 149-169.

26. G. Tenenbaum, 'La méthode du col en théorie analytique des nombres', Séminaire de Théorie des Nombres de Paris 1986-87 (Birkhäuser), 411-441.

27. K.R. Woolridge, 'Values taken many times by Euler's phi-function', Proc. Amer. Math. Soc. **76**(1979), 229-234.