(12)

(6)

Analysis of a Simple Factorization Algorithm

by Donald E. Knuth [redacted] Luis Trabb Pardo

(10) (11) JAN 76 (12) 51p.

Abstract

The probability that the k-th largest prime factor of a number n is at most n^x is shown to approach a limit $F_k(x)$ as $n \to \infty$. Several interesting properties of $F_k(x)$ are explored, and numerical tables are given. These results are applied to the analysis of an algorithm commonly used to find all prime factors of a given number. The average number of digits in the k-th largest prime factor of a random m-digit number is shown to be asymptotically equivalent to the average length of the k-th longest cycle in a permutation on m objects.

n to the x power

infinity

F sub K (x)

(15) N00014-70-A-0362-0001, NSF-DCR-72-03752

Keywords and phrases: asymptotic methods, cycle lengths in random permutation, Dickman's function, prime factors, probability distributions in number theory.

This research was supported in part by National Science Foundation grant DCR72-03752 A02, by the Office of Naval Research contract NR-044-402, and by IBM Corporation. Some of the computations and formula manipulation were done with the MACSYMA system supported by the Advanced Research Projects Agency (ARPA), under Office of Naval Research contract N00014-70-A-0362-0001. Reproduction in whole or in part is permitted for any purpose of the United States Government.

(16)

Perhaps the simplest way to discover the prime factorization of an integer n is to try dividing it by $2, 3, 4, 5, \ldots$ and to "cast out" each factor that is discovered; we stop when the trial divisor exceeds the square root of the remaining unfactored part.

The speed of this method obviously depends on the size of the prime factors of n. For example, if n is prime, the number of trial divisions is approximately $n^{1/2}$; but if n is a power of 2, the number is only about $\log n$. In this paper we shall analyze the algorithm when n is a "random" integer, determining the approximate probability that the number of trial divisions is $\leq n^x$ when x is a given number between 0 and $1/2$. One of the results we shall prove is that the number of trial divisions will be $\leq n^{.35}$, about half of the time.

In order to carry out the analysis, we shall study the distribution of the k-th largest prime factor of a random integer. This problem is of independent interest in number theory, and for $k > 1$ it does not appear to have been studied before. (Wunderlich and Selfridge [14] gave a heuristic argument that the second-largest prime factor will tend to be roughly $(n^{1-.61})^{.61} \approx n^{.24}$ because the median value of the largest prime factor is $\approx n^{.61}$; besides their remark, which stimulated the present investigation, the authors are not aware of any published study of the second-largest prime factor. John M. Pollard [private communication] has independently investigated the distribution of second-largest prime factors, and his computed values agree with those presented below.)

Section 1 of this paper presents the factorization algorithm in detail and proves its correctness. Quantitative analysis begins in Section 2, where the two frequency counts involved in the running time are interpreted in terms of the size of the largest two prime factors.

The distribution of k-th largest prime factors is investigated heuristically in Section 3, somewhat as a physicist might do the analysis. A rigorous derivation of this distribution, somewhat as a mathematician might do the analysis, is presented in Section 4. Sections 5 and 6 continue the mathematical play by deriving interesting identities and asymptotic formulas satisfied by these distributions. Section 7 comes back to the factorization procedure and applies the ideas to the results of Sections 1 and 2, somewhat as a computer scientist might do the analysis.

Section 8 discusses the particular theoretical model used in these analyses, and explains why the traditional "mean and variance" approach is inappropriate for algorithms such as this. Numerical tables and empirical confirmation of the theory appear in Section 9. Finally, Section 10 discusses a rather surprising connection between prime factors of random m-digit integers and the cycle lengths of random permutations on m objects.

Although we shall deal with a very simple approach to factoring, the results and methods of this paper apply to many other algorithms as well. The paper is self-contained, and includes several examples suitable for classroom exposition of asymptotic methods.

1. The Algorithm.

Here is the standard "divide and factor" algorithm which we shall analyze in detail. A proof of its validity follows immediately from the following invariant assertions governing the variables used:

$$n \geq 2 \quad ; \tag{1.1}$$

$$n = p_1 \cdots p_t m \quad ; \tag{1.2}$$

$p_1, \ldots, p_t$ are prime numbers; (1.3)

$$m \geq d \quad ; \tag{1.4}$$

all prime factors of m are $\geq d$. (1.5)

Since our goal is to analyze a simple algorithm rather than to present it in optimized form ready for extensive use, we shall simply consider the following informal Algol-like description:

```
t := 0; m := n; d := 2;                                  1
while $d^2 \leq m$ do                                    D+1
begin increase d or decrease m:
   if d divides m then                                   D
      begin
         t := t+1; $p_t$ := d; m := m/d                  T-1
      end
      else d := d+1                                      D-T+1
end;
t := t+1; $p_t$ := m; m := 1; d := 1;                    1
```

The invariant assertions hold after each line of this program. The expressions in the right-hand column specify the number of times the operations in a particular line will be performed, where

D is the number of trial divisions performed, (1.6)

T is the number of prime factors of n (counting multiplicity). (1.7)

The usual refinements of this algorithm, which avoid a lot of nonprime trial divisors by making d run through only values of the form $6k \pm 1$, say, when $d > 3$, have the effect of dividing D by a constant; so our analysis of this simple case will apply also with minor variations to the more complicated cases.

2. Preliminary Analysis.

Let n_k be the k-th largest prime factor of n ; thus $n_k = p_{T+1-k}$ after the above algorithm terminates, for $1 \le k \le T$. If n has less than k prime factors (counting multiplicities), let $n_k = 1$. We also let $n_0 = \infty$ for convenience in what follows.

The while loop in the algorithm can terminate in three different ways, depending on how we last encounter it:

Case 1, $n < 4$. Then $D = 0$.

Case 2, $n \ge 4$ and the D-th trial division succeeds. Then the final trial division was by $d = n_2$, where $d^2 > n_1$. Since d is initially 2 and the statement $d := d+1$ is performed $D-T+1$ times, we have

$$D = n_2 + T - 3 \quad , \quad n_2^2 > n_1 \quad . \tag{2.1}$$

Case 3, $n \ge 4$ and the D-th trial division fails. Then the final trial division was by d , where $n_2 \le d$ and $d^2 < n_1$ and $(d+1)^2 > n_1$. (Note that if we set $p_0 := 1$ we have $d \ge p_{t-1}$ throughout the while loop.) Thus we have

$$D = \lceil\sqrt{n_1}\rceil + T - 3 \quad , \quad n_2^2 < n_1 \quad . \tag{2.2}$$

In all three cases we have the formula

$$D = \max(n_2 , \lceil\sqrt{n_1}\rceil) + T - 3 \quad . \tag{2.3}$$

Clearly D is the dominant factor in the running time, so most of our analysis will be devoted to it. However, it turns out that the analysis of T is also very interesting; for large random n , the number T of prime factors can be regarded as a normally-distributed random variable with mean $\ln \ln n + 1.03$ and standard deviation $\sqrt{\ln \ln n}$ (see Appendix A).

3. The k-th largest prime factor.

In order to analyze D, we shall first analyze the distributions of n_1 and n_2 (and n_k in general). Let $P_k(x,N)$ be the number of integers n in the range $1 \leq n \leq N$ such that

$$n_k \leq N^x \quad , \tag{3.1}$$

where x is any number ≥ 0. Thus $P_k(x,N)/N$ is the probability that a random integer between 1 and N will have k-th largest prime factor $\leq N^x$. We will prove that this probability tends to a limiting distribution

$$\lim_{N \to \infty} \frac{P_k(x,N)}{N} = F_k(x) \quad , \tag{3.2}$$

where $F_k(x)$ has interesting properties discussed below.

Before we establish (3.2) rigorously, it will be helpful to give a heuristic derivation analogous to that given by Karl Dickman [3], who was the first to study this question in the case $k = 1$. Let us consider $P_k(t+dt, N) - P_k(t,N)$, the number of $n \leq N$ such that n_k lies between N^t and N^{t+dt}, when dt is very small. To count the number of such n, we take all primes p lying between N^t and N^{t+dt}, and multiply by all numbers $m \leq N^{1-t}$ such that $m_k \leq p$ and $m_{k-1} \geq p$. Now if $n = mp$ we have $n \leq N^{1+dt}$ and $n_k = p$; conversely every $n \leq N$ with n_k between N^t and N^{t+dt} will have the form $n = mp$ where p and m have the stated form. Note that the number of $m \leq N^{1-t}$ such that $m_k \leq p$ is approximately $P_k(t/(1-t), N^{1-t})$, and the unwanted subset consisting of those m with $m_{k-1} < p$ has approximately $P_{k-1}(t/(1-t), N^{1-t})$ members. Hence the number of m with $mp \leq N$ and $m_k \leq p$ and $m_{k-1} \geq p$ is

$P_k(t/(1-t)\,,N^{1-t}) - P_{k-1}(t/(1-t)\,,N^{1-t})$, ignoring second-order terms, and we have

$$P_k(t+dt\,,N) - P_k(t,N) \approx (\pi(N^{t+dt}) - \pi(N^t))(P_k(t/(1-t)\,,N^{1-t}) - P_{k-1}(t/(1-t)\,,N^{1-t}). \tag{3.3}$$

Here the π function is defined as usual,

$$\pi(x) = \text{the number of primes not exceeding } x\ . \tag{3.4}$$

According to the prime number theorem we have $\pi(x) \approx x/\ln x$, hence

$$\pi(N^{t+dt}) - \pi(N^t) \approx N^t dt/t\ . \tag{3.5}$$

Plugging this into the above formula and dividing by N yields

$$\frac{P_k(t+dt,N) - P_k(t,N)}{N} \approx \frac{dt}{t}\left(\frac{P_k(t/(1-t),N^{1-t})}{N^{1-t}} - \frac{P_{k-1}(t/(1-t),N^{1-t})}{N^{1-t}}\right)\ ; \tag{3.6}$$

when $N \to \infty$ we have the differential equation

$$F_k'(t)dt = \frac{dt}{t}\left(F_k\left(\frac{t}{1-t}\right) - F_{k-1}\left(\frac{t}{1-t}\right)\right)\ . \tag{3.7}$$

Since $F_k(0) = 0$, we may integrate (3.7) to deduce the formula

$$F_k(x) = \int_0^x \left(F_k\left(\frac{t}{1-t}\right) - F_{k-1}\left(\frac{t}{1-t}\right)\right)\frac{dt}{t}\ . \tag{3.8}$$

According to our convention $n_0 = \infty$, we define

$$F_0(x) = 0 \quad \text{for all } x\ . \tag{3.9}$$

We also must have

$$F_k(x) = 1 \quad \text{for } x \geq 1\ ,\ k \geq 1\ . \tag{3.10}$$

Now it is easy to see that (3.8), (3.9), (3.10) define $F_k(x)$ uniquely for $0 \le x \le 1$, since we have

$$F_k(x) = 1 - \int_x^1 \frac{dt}{t}\left(F_k\left(\frac{t}{1-t}\right) - F_{k-1}\left(\frac{t}{1-t}\right)\right) , \quad 0 \le x \le 1 \qquad (3.11)$$

and this relation defines $F_k(x)$ in terms of its values at points $> x$.

4. Proof without handwaving.

Our discussion in the previous section has been only quasi-rigorous, but it shows that *if* the limiting relationship (3.2) holds then $F_k(x)$ had better be the function defined by (3.8), (3.9), and (3.10). Now that we have a formula for F_k, let us try to prove the limiting formula (3.2).

It is more convenient to work with the functions ρ_k defined by

$$\rho_k(\alpha) = F_k(1/\alpha) \quad ; \tag{4.1}$$

the above equations transform into the somewhat simpler recurrence formulas

$$\rho_k(\alpha) = 1 - \int_1^\alpha (\rho_k(t-1) - \rho_{k-1}(t-1)) \frac{dt}{t} \quad , \quad \text{for } \alpha > 1 \; , \; k \geq 1 \; ; \tag{4.2}$$

$$\rho_k(\alpha) = 1 \quad \text{for } 0 < \alpha \leq 1 \; , \; k \geq 1 \quad ; \tag{4.3}$$

$$\rho_k(\alpha) = 0 \quad \text{for } \alpha \leq 0 \text{ or } k = 0 \quad . \tag{4.4}$$

Furthermore we let $S_k(x,y)$ be the set of positive integers $n \leq x$ such that $n_k \leq y$, and let $\Psi_k(x,y) = \|S_k(x,y)\|$ be its cardinality, so that

$$P_k(x,N) = \Psi_k(N,N^x) \quad . \tag{4.5}$$

We will show that

$$\Psi_k(N^\alpha,N) = \rho_k(\alpha)N^\alpha + O(N^\alpha / \log N^\alpha) \quad , \tag{4.6}$$

and it follows that a stronger form of (3.2) is true:

$$\frac{P_k(x,N)}{N} = F_k(x) + O\left(\frac{1}{\log N}\right) \quad . \tag{4.7}$$

Indeed, we will prove a result even stronger than (4.6), namely

$$\Psi_k(x^\alpha,x) = \rho_k(\alpha)x^\alpha + \sigma_k(\alpha)x^\alpha / \ln x^\alpha + O(x^\alpha/(\log x)^2) \qquad (4.8)$$

as $x \to \infty$, for all fixed $\alpha > 1$, where $\sigma_k(\alpha)$ will be defined appropriately below. In principle, the approach we shall use could be extended to obtain an asymptotic formula for $\Psi_k(x^\alpha,x)$ which is good to $O(x^\alpha/(\log x)^r)$ for any fixed r; the method is based on ideas of N. G. de Bruijn [1], who went on to find extremely precise asymptotic expansions of $\Psi_1(N^\alpha,N)$ in an elegant way using Stieltjes integration by parts. (Note: When $k = 1$, the limiting formula (3.2) was first established by V. Ramaswami [11]; K. K. Norton [9] has given a comprehensive survey of the literature relating to this important special case.)

We shall use a strong form of the prime number theorem due to de la Vallée Poussin [2]:

$$\pi(x) = L(x) + O(x\, e^{-C\sqrt{\log x}}) \quad , \qquad (4.9)$$

where C is a positive constant and

$$L(x) = \int_2^x \frac{dt}{\ln t} \quad . \qquad (4.10)$$

Now to the proof, which will be "elementary" except for our use of (4.9). Letting p range over primes and n over positive integers, we have

$$\lfloor x^\alpha \rfloor - \Psi_k(x^\alpha, x) = \sum_{x < p \le x^\alpha} \|\{n \le x^\alpha \mid n_k = p\}\|$$

$$= \sum_{x < p \le x^\alpha} \|\{m \le x^\alpha/p \mid m_k \le p \text{ and } m_{k-1} \ge p\}\|$$

$$= \sum_{x < p \le x^\alpha} (\Psi_k(x^\alpha/p\,,\, p) - \Psi_{k-1}(x^\alpha/p\,,\, p-\varepsilon))$$

where ε is a small positive number and $\Psi_0(x,y) = 0$. The key idea in our derivation will be to replace $\sum_{x < p \le x^\alpha} \Psi_k(x^\alpha/p\,,\, p)$ by $\int_x^{x^\alpha} \Psi_k(x^\alpha/y\,,\, y)dy/(\ln y)$, using the "density" function for primes suggested by (4.10). To justify this, we have

$$\left(\sum_{x < p \le x^\alpha} \Psi_k\left(\frac{x^\alpha}{p}\,,\, p\right)\right) - \int_x^{x^\alpha} \Psi_k\left(\frac{x^\alpha}{y}\,,\, y\right) \frac{dy}{\ln y}$$

$$= \left(\sum_{x < p \le x^\alpha} \; \sum_{n \in S_k(x^\alpha/p,p)} 1\right) - \int_x^{x^\alpha} \left(\sum_{n \in S_k(x^\alpha/y,y)} 1\right) \frac{dy}{\ln y}$$

$$= \sum_{\substack{1 \le n \le x^{\alpha-1} \\ n_k \le x^\alpha/n}} \left(\left(\sum_{\substack{n_k \le p \le x^\alpha/n \\ x < p}} 1\right) - \int_{\max(n_k,x)}^{x^\alpha/n} \frac{dy}{\ln y}\right)$$

$$= \sum_{\substack{1 \le n \le x^{\alpha-1} \\ n_k \le x^\alpha/n}} \left(\pi(x^\alpha/n) - \pi(\max(n_k,x)) + O(1) - L(x^\alpha/n) + L(\max(n_k,x))\right)$$

$$= \sum_{\substack{1 \le n \le x^{\alpha-1} \\ n_k \le x^{\alpha}/n}} O\left(\frac{x^{\alpha}}{n} e^{-C\sqrt{\log x}} \right)$$

$$= O(x^{\alpha}(\log x^{\alpha}) e^{-C\sqrt{\log x}}) \quad . \tag{4.11}$$

A similar estimate applies to $\sum_{x < p \le x^{\alpha}} \Psi_{k-1}(x^{\alpha}/p\,,\, p-\varepsilon)$, so we have

$$\Psi_k(x^{\alpha},x) = x^{\alpha} - \int_x^{x^{\alpha}} \left(\Psi_k\left(\frac{x^{\alpha}}{y}\,,\,y\right) - \Psi_{k-1}\left(\frac{x^{\alpha}}{y}\,,\,y\right)\right) \frac{dy}{\ln y} + O\left(\frac{\alpha x^{\alpha}}{(\log x)^{r}}\right) \tag{4.12}$$

as $x \to \infty$, for all fixed $r \ge 0$. This is the formula we shall use for $\alpha \ge 1$; for $0 \le \alpha < 1$ we have $\Psi_k(x^{\alpha},x) = \lfloor x^{\alpha} \rfloor$. (The brackets $\lfloor\ \rfloor$ in the latter formula turn out to be important, since the integral (4.12) is sensitive to $O(1)$ terms in the vicinity of $y = x^{\alpha}$.)

Our proof of (4.8) is by induction on k , and for fixed k by induction on $\lceil \alpha \rceil$. Actually the first case $k = 1$, $\lceil \alpha \rceil = 2$ seems to be the hardest; when $1 < \alpha \le 2$ we have

$$\Psi_1(x^\alpha,x) = x^\alpha - \int_x^{x^\alpha} \Psi_1\left(\frac{x^\alpha}{y}, y\right) \frac{dy}{\ln y} + O\left(\frac{x^\alpha}{(\log x)^2}\right)$$

$$= x^\alpha - \int_x^{x^\alpha} \left(\frac{x^\alpha}{y} - \left\{\frac{x^\alpha}{y}\right\}\right) \frac{dy}{\ln y} + O\left(\frac{x^\alpha}{(\log x)^2}\right)$$

$$= x^\alpha - x^\alpha \ln \alpha + x^\alpha \int_1^{x^{\alpha-1}} \{u\} \frac{du}{u^2 \ln x^\alpha/u} + O\left(\frac{x^\alpha}{(\log x)^2}\right)$$

$$= x^\alpha \rho_1(\alpha) + \frac{x^\alpha}{\ln x^\alpha} \int_1^{x^{\alpha-1}} \left(\frac{\{u\}du}{u^2} + \frac{\{u\} \ln u \, du}{u^2 \ln(x^\alpha/u)}\right) + O\left(\frac{x^\alpha}{(\log x)^2}\right)$$

$$= x^\alpha \rho_1(\alpha) + \frac{x^\alpha}{\ln x^\alpha} \int_1^\infty \frac{\{u\}du}{u^2} + O\left(\frac{x}{\log x}\right) + O\left(\frac{x^\alpha}{(\log x)^2}\right), \qquad (4.13)$$

where $\{x\}$ denotes $x-\lfloor x \rfloor$. The remaining integral is

$$\int_1^\infty \frac{\{u\}du}{u^2} = \sum_{n \geq 1} \int_n^{n+1} \frac{(u-n)du}{u^2} = \sum_{n \geq 1} \left(\left(\ln \frac{n+1}{n}\right) - \frac{1}{n+1}\right)$$

$$= \lim_{n \to \infty} ((\ln n) - (H_n - 1)) = 1-\gamma \quad , \qquad (4.14)$$

where γ is Euler's constant.

Now suppose we have proved that

$$\Psi_1(x^\alpha,x) = x^\alpha \rho_1(\alpha) + (1-\gamma) \frac{x^\alpha}{\ln x^\alpha} \rho_1(\alpha-1) + O\left(\frac{x}{\log x}\right) + O\left(\frac{x^\alpha}{(\log x)^2}\right) \qquad (4.15)$$

for $1 < \alpha \leq m$, where the bounding constants implied by the O's depend on m but not on x or α . The discussion in the previous paragraph establishes (4.15) for $m = 2$. We can extend it to the next case by analyzing its value for $m < \alpha \le m+1$:

$$\begin{aligned}
\Psi_1(x^\alpha,x) &= x^\alpha - \int_x^{x^\alpha} \Psi_1\left(\frac{x^\alpha}{y}, y\right)\frac{dy}{\ln y} + O\left(\frac{x^\alpha}{(\log x)^2}\right) \\
&= x^\alpha - \int_1^\alpha \Psi_1(x^{\alpha(t-1)/t}, x^{\alpha/t})\, x^{\alpha/t}\,\frac{dt}{t} + O\left(\frac{x^\alpha}{(\log x)^2}\right) \\
&= x^\alpha - \int_1^2 \lfloor x^{\alpha(t-1)/t}\rfloor\, x^{\alpha/t}\,\frac{dt}{t} \\
&\quad - x^\alpha \int_2^\alpha \left(\rho_1(t-1) + \frac{(1-\gamma)\rho_1(t-2)}{\ln x^{\alpha(t-1)/t}} + O\left(\frac{1}{(\alpha/t)\log x}\right)^2\right)\frac{dt}{t} \\
&\quad - \int_2^\alpha x^{\alpha/t}\, O\left(\frac{x^{\alpha/t}}{(\alpha/t)\log x}\right)\frac{dt}{t} + O\left(\frac{x^\alpha}{(\log x)^2}\right) \qquad (4.16)
\end{aligned}$$

by substituting $x^{\alpha/t}$ for y and inserting (4.15). Continuing, we get

$$\begin{aligned}
\Psi_1(x^\alpha,x) &= x^\alpha - x^\alpha\int_1^\alpha \rho_1(t-1)\,\frac{dt}{t} + \int_1^2 \{x^{\alpha(t-1)/t}\}\, x^{\alpha/t}\,\frac{dt}{t} \\
&\quad - \frac{(1-\gamma)x^\alpha}{\ln x^\alpha}\int_2^\alpha \rho_1(t-2)\,\frac{dt}{t-1} + O\left(\frac{1}{\log x}\int_2^\alpha x^{2\alpha/t}\,dt\right) + O\left(\frac{x^\alpha}{(\log x)^2}\right) \\
&= x^\alpha\,\rho_1(\alpha) + x^\alpha\int_1^{x^{\alpha/2}} \frac{\{u\}du}{u^2\,\ln(x^\alpha/u)} - \frac{(1-\gamma)x^\alpha}{\ln x^\alpha}\int_1^{\alpha-1} \rho_1(t-1)\,\frac{dt}{t} \\
&\quad + O\left(\frac{1}{\log x}\int_{2/\alpha}^1 \frac{x^{\alpha u}\,du}{u^2}\right) + O\left(\frac{x^\alpha}{(\log x)^2}\right) \\
&= x^\alpha\,\rho_1(\alpha) + \frac{x^\alpha(1-\gamma)}{\ln x^\alpha}\,\rho_1(\alpha-1) + O\left(\frac{x^\alpha}{(\log x)^2}\right), \qquad (4.17)
\end{aligned}$$

since

$$\int_1^{x^{\alpha/2}} \frac{\{u\}du}{u^2 \ln(x^\alpha/u)} = \frac{1}{\ln x^\alpha}\left(1-\gamma+O\left(\frac{1}{\log x}\right)\right) \tag{4.18}$$

as in (4.13) and (4.14), and

$$\int_{2/\alpha}^1 \frac{x^{\alpha u}\,du}{u^2} = O\left(\int_{2/\alpha}^1 x^{\alpha u}\,du\right) = O\left(\frac{x^\alpha}{\log x}\right) \tag{4.19}$$

with bounding constants depending only on m. This establishes (4.15) for all m, by induction.

We have proved (4.8) for $k = 1$, with

$$\sigma_1(\alpha) = (1-\gamma)\rho_1(\alpha-1) \quad .$$

For larger k, a similar but simpler derivation applies: Assuming that

$$\Psi_k(x^\alpha,x) = x^\alpha \rho_k(\alpha) + \frac{x^\alpha}{\ln x^\alpha}\sigma_k(\alpha) + O\left(\frac{x}{\log x}\right) + O\left(\frac{x^\alpha}{(\log x)^2}\right) \tag{4.20}$$

for $1 < \alpha \le m$ (cf. (4.15)), we extend this to $m < \alpha \le m+1$ by

$$\begin{aligned}
\Psi_k(x^\alpha,x) &= x^\alpha - \int_x^{x^\alpha}\left(\Psi_k\left(\frac{x^\alpha}{y}, y\right) - \Psi_{k-1}\left(\frac{x^\alpha}{y}, y\right)\right)\frac{dy}{\ln y} + O\left(\frac{x^\alpha}{(\log x)^2}\right) \\
&= x^\alpha - \int_1^\alpha \left(\Psi_k(x^{\alpha(t-1)/t}, x^{\alpha/t}) - \Psi_{k-1}(x^{\alpha(t-1)/t}, x^{\alpha/t})x^{\alpha/t}\right)\frac{dt}{t} \\
&\qquad + O\left(\frac{x^\alpha}{(\log x)^2}\right) \\
&= x^\alpha\left(1 - \int_2^\alpha (\rho_k(t-1) - \rho_{k-1}(t-1))\,\frac{dt}{t}\right. \\
&\qquad \left. - \frac{1}{\ln x^\alpha}\int_2^\alpha (\sigma_k(t-1) - \sigma_{k-1}(t-1))\,\frac{dt}{t-1}\right) + O\left(\frac{x^\alpha}{(\log x)^2}\right) \quad ;
\end{aligned} \tag{4.21}$$

the desired relation follows for $k \geq 2$ provided that we define

$$\sigma_k(\alpha) = -\int_2^\alpha (\sigma_k(t-1) - \sigma_{k-1}(t-1)) \frac{dt}{t-1} \quad \text{for} \quad \alpha \geq 2 \quad ; \tag{4.22}$$

$$\sigma_k(\alpha) = 0 \quad \text{for} \quad \alpha < 2 \quad . \tag{4.23}$$

It follows that

$$\sigma_k(\alpha) = (1-\gamma)(\rho_k(\alpha-1) - \rho_{k-1}(\alpha-1)) \tag{4.24}$$

for all $k \geq 1$.

5. Identities satisfied by ρ_k .

The functions $\rho_k(\alpha)$ defined by (4.2), (4.3), (4.4) possess many rather surprising properties, and we shall examine some of them in this section.

Our first goal is to express the ρ_k in terms of the polylogarithm functions L_k , defined by

$$L_0(\alpha) = 0 \quad \text{for} \quad \alpha \leq 0 \ , \quad L_0(\alpha) = 1 \quad \text{for} \quad \alpha > 0 \quad ; \tag{5.1}$$

$$L_k(\alpha) = \int_1^\alpha L_{k-1}(t-1) \frac{dt}{t} \quad . \tag{5.2}$$

Thus $L_1(\alpha) = \ln \alpha$ for $\alpha \geq 1$, and $L_2(\alpha) = \int_2^\alpha \ln(t-1)dt/t$ for $\alpha \geq 2$, etc.; it is not difficult to verify that $L_k(\alpha)$ is $1/k!$ times the integral of $(dx_1 \ldots dx_k)/(x_1 \ldots x_k)$ over all points $x_1,\ldots,x_k$ where $1 \leq x_1,\ldots,x_k \leq \alpha$ and $|x_i - x_j| \geq 1$ for all $i \neq j$. In particular, $L_k(\alpha) = 0$ for $\alpha \leq k$.

By iterating the recurrence for ρ_k we find

$$1 - \rho_1(\alpha) = L_1(\alpha) - L_2(\alpha) + L_3(\alpha) - L_4(\alpha) + L_5(\alpha) - \ldots \ , \tag{5.3}$$

$$1 - \rho_2(\alpha) = L_2(\alpha) - 2L_3(\alpha) + 3L_4(\alpha) - 4L_5(\alpha) + \ldots \ , \tag{5.4}$$

for $\alpha > 0$, and in general

$$1 - \rho_k(\alpha) = \sum_{n \geq 0} \binom{-k}{n} L_{n+k}(\alpha) \quad . \tag{5.5}$$

These infinite sums are actually finite for any particular value of α .

Now let us examine several auxiliary functions:

$$S_k(\alpha,\beta) = \int_0^\alpha \frac{\rho_k(t-1)dt}{\beta-t} \quad \text{for} \quad \beta > \alpha \quad \text{or} \quad \beta < 0 \quad ; \qquad (5.6)$$

$$S_k(\alpha) = S_k(\alpha,\alpha+1) \quad ; \qquad (5.7)$$

$$I_k(\alpha) = \int_0^\alpha \frac{\rho_k(t-1)}{t} \ln(t+1)dt \quad ; \qquad (5.8)$$

$$\sigma_k(\alpha) = \int_0^\alpha \frac{\rho_k(t-1)}{t} dt \quad ; \qquad (5.9)$$

$$e_k(x) = \int_0^\infty \rho_k(t)e^{-tx} dt \quad , \quad x > 0 \quad . \qquad (5.10)$$

(This is a different function $\sigma_k(\alpha)$ from that in Section 4.) It follows immediately from the definition $\rho_k(\alpha) = 1 - \sigma_k(\alpha) + \sigma_{k-1}(\alpha)$ that

$$\sigma_k(\alpha) = k - \rho_1(\alpha) - \dots - \rho_k(\alpha) \quad . \qquad (5.11)$$

Integration by parts enables us to evaluate $I_k(\alpha)$ as follows:

$$I_k(\alpha) - I_{k-1}(\alpha) = -\rho_k(t) \ln(t+1)\Big|_0^\alpha + \int_0^\alpha \frac{\rho_k(t)dt}{t+1}$$

$$= -\rho_k(\alpha) \ln(\alpha+1) + \sigma_k(\alpha+1) \quad . \qquad (5.12)$$

Thus in particular we have

$$I_1(\alpha) = -\rho_1(\alpha) \ln(\alpha+1) + 1 - \rho_1(\alpha+1) \quad , \qquad (5.13)$$

$$I_2(\alpha) = -\rho_1(\alpha) \ln(\alpha+1) - \rho_2(\alpha) \ln(\alpha+1) + 3 - 2\rho_1(\alpha+1) - \rho_2(\alpha+1) \quad , \qquad (5.14)$$

etc. A somewhat surprising consequence of this relation is that $I_k(\infty) = k(k+1)/2$, while $\sigma_k(\infty) = k$; in particular, $I_1(\infty) = \sigma_1(\infty)$.

Integration by parts applied to $S_k(\alpha,\beta)$ yields

$$S_k(\alpha,\beta) - S_{k-1}(\alpha,\beta) = - \left.\frac{t\rho_k(t)}{\beta-t}\right|_0^{\alpha} + \beta \int_0^{\alpha} \frac{\rho_k(t)dt}{(\beta-t)^2}$$

$$= - \frac{\alpha\rho_k(\alpha)}{\beta-\alpha} + \beta \int_1^{\alpha+1} \frac{\rho_k(t-1)dt}{(\beta+1-t)^2} \quad . \tag{5.15}$$

Differentiating the integral which defines $S_k(\alpha) = S_k(\alpha,\alpha+1)$ with respect to α leads to a formula which can be combined with this one:

$$S_k'(\alpha) = \rho_k(\alpha-1) - \int_1^{\alpha} \frac{\rho_k(t-1)dt}{(\alpha+1-t)^2}$$

$$= \rho_k(\alpha-1) - \frac{1}{\alpha}\left((\alpha-1)\rho_k(\alpha-1) + S_k(\alpha-1) - S_{k-1}(\alpha-1)\right)$$

$$= \frac{1}{\alpha}\left(\rho_k(\alpha-1) + S_{k-1}(\alpha-1) - S_k(\alpha-1)\right) \quad . \tag{5.16}$$

Now we are ready to prove an important relation which expresses ρ_{k+1} in terms of ρ_k and ρ_{k-1} :

Lemma.

$$\rho_{k+1}(\alpha) = \rho_k(\alpha) + \frac{1}{k}\left(S_k(\alpha) - S_{k-1}(\alpha)\right) \;, \quad \text{for } k \geq 1 \quad . \tag{5.17}$$

Proof. Since $\rho_{k+1}(\alpha) = \rho_k(\alpha) = 1$ and $S_k(\alpha) = S_{k-1}(\alpha) = 0$ for $0 < \alpha \leq 1$, the result holds for $\lceil\alpha\rceil = 1$; we will show that the derivatives agree, by induction on $\lceil\alpha\rceil$. Since

$$(\alpha+1)\rho'_{k+1}(\alpha+1) = \rho_k(\alpha) - \rho_{k+1}(\alpha) = (S_{k-1}(\alpha) - S_k(\alpha))/k \quad ,$$

$$(\alpha+1)\rho'_k(\alpha+1) = \rho_{k-1}(\alpha) - \rho_k(\alpha) \quad ,$$

$$(\alpha+1)S'_k(\alpha+1) = \rho_k(\alpha) + S_{k-1}(\alpha) - S_k(\alpha) \quad ,$$

$$(\alpha+1)S'_{k-1}(\alpha+1) = \rho_{k-1}(\alpha) + S_{k-2}(\alpha) - S_{k-1}(\alpha) \quad ,$$

the desired result is equivalent to

$$\frac{k-1}{k}\rho_k(\alpha) = \frac{k-1}{k}\rho_{k-1}(\alpha) + \frac{1}{k}(S_{k-1}(\alpha) - S_{k-2}(\alpha)) \quad .$$

For $k = 1$ this is obvious, otherwise it holds by induction. □

By iterating the recurrence in the lemma, it follows that

$$\rho_{k+1}(\alpha) = \rho_1(\alpha) + \frac{1}{2.1}S_1(\alpha) + \ldots + \frac{1}{k(k-1)}S_{k-1}(\alpha) + \frac{1}{k}S_k(\alpha) \quad . \qquad (5.18)$$

Finally let us consider the functions $e_k(x)$ defined in (5.10). Somewhat surprisingly, these can actually be expressed in closed form:

<u>Theorem</u>. $e_k(x) = \dfrac{e^{-E(x)}}{x}\left(1 + \dfrac{E(x)}{1!} + \ldots + \dfrac{E(x)^{k-1}}{(k-1)!}\right)$, where $E(x) = E_1(x)$ is the exponential integral function

$$E(x) = \int_x^\infty e^{-t}\,dt/t = \int_1^\infty e^{-xt}\,dt/t \quad . \qquad (5.19)$$

Proof. Once again we integrate by parts:

$$e_k(x) - e_{k-1}(x) = \int_1^\infty \frac{\rho_k(t-1) - \rho_{k-1}(t-1)}{t} \, t\, e^{-(t-1)x} dt$$

$$= - e^x \int_0^\infty t\, e^{-tx} \, d\, \rho_k(t)$$

$$= e^x \int_0^\infty \rho_k(t)(e^{-tx} - t\, x\, e^{-tx}) dt$$

$$= e^x(e_k(x) + x\; e_k'(x)) \quad .$$

If we let $f_k(x) = xe^{E(x)}\, e_k(x)$, we have therefore

$$f_k'(x) = e^{E(x)}(e_k(x) + x\, e_k'(x) - e^{-x}\, e_k(x))$$

$$= - \frac{e^{-x}}{x} f_{k-1}(x) = E'(x) f_{k-1}(x)$$

and it follows by induction on k that

$$f_k(x) = C + \frac{E(x)}{1!} + \ldots + \frac{E(x)^{k-1}}{(k-1)!} \quad .$$

In order to evaluate C , we integrate by parts in the opposite direction:

$$x\, e_k(x) = - \int_0^\infty \rho_k(t)\, d(e^{-tx}) = - \rho(t) e^{-tx}\Big|_0^\infty + \int_0^\infty e^{-tx}\, d\, \rho_k(t)$$

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

$$= 1 - \int_x^\infty e^{-u}\left(\rho_k\left(\frac{u}{x} - 1\right) - \rho_{k-1}\left(\frac{u}{x} - 1\right)\right) \frac{du}{u} \quad .$$

Hence $C = \lim_{x\to\infty} x\, e_k(x) = \lim_{x\to\infty} f_k(x) = 1$. □

6. Asymptotic formulas.

In this section we shall study the asymptotic behavior of $\rho_k(\alpha)$ for large α. Our starting point is a simple proof that $\rho_1(\alpha)$ is exponentially small: Let us write $\rho(\alpha)$ for $\rho_1(\alpha)$. Then since

$$\begin{aligned} 1+\int_2^{\alpha} \rho(t-1)dt &= \int_1^{\alpha} \rho(t-1)dt \\ &= -t\rho(t)\Big|_1^{\alpha} + \int_1^{\alpha} \rho(t)dt \\ &= 1-\alpha\rho(\alpha)+\int_2^{\alpha+1} \rho(t-1)dt \qquad (6.1) \end{aligned}$$

we have

$$\int_{\alpha}^{\alpha+1} \rho(t-1)dt = \alpha\rho(\alpha) \quad . \qquad (6.2)$$

It follows immediately that $\alpha\rho(\alpha) < \rho(\alpha-1)$ for all $\alpha > 1$, hence by induction

$$\rho(n) \leq 1/n! \qquad (6.3)$$

for all integers $n \geq 1$. Considerably more precise formulas have been obtained by de Bruijn [1] and others, and numerical results have been tabulated by Mitchell [8] and by van de Lune and Wattel [13]; but (6.3) suffices for our purposes in this section.

The rapid decrease of $\rho_1(\alpha)$ simplifies the numerical evaluation of integrals and it also leads to a simple treatment of the asymptotic behavior of $\rho_2(\alpha)$:

Theorem. For all fixed $r \geq 1$ *we have*

$$\rho_2(\alpha) = A\left(\frac{c_0}{\alpha} + \frac{c_1}{\alpha^2} + \dots + \frac{c_{r-1}}{\alpha^r}\right) + O(\alpha^{-r-1}) \tag{6.4}$$

as $\alpha \to \infty$, *where*

$$A = e^\gamma \approx 1.78107\ 24179\ 90197\ 98524 \quad , \tag{6.5}$$

and the coefficients c_k *are defined by*

$$\sum_{k \geq 0} z^k c_k/k! = \exp\left(\int_0^z (e^t - 1)\,dt/t\right) = \exp\left(\sum_{k \geq 1} z^k/k \cdot k!\right) . \tag{6.6}$$

Thus $\langle c_0, c_1, c_2, \dots \rangle = \left\langle 1, 1, \frac{3}{2}, \frac{17}{6}, \frac{19}{3}, \frac{81}{5}, \frac{8351}{180}, \frac{184553}{1260}, \frac{52907}{105}, \frac{1768847}{945}, \dots \right\rangle$. Before proving the theorem, we note that (6.6) implies the recurrence formula

$$c_n = \frac{1}{n} \sum_{1 \leq k \leq n} \binom{n}{k} c_{n-k} \quad , \qquad n \geq 1 . \tag{6.7}$$

Therefore $c_n > \frac{n-1}{2} c_{n-2}$ for $n \geq 2$, and $c_{2n+1} > n!$; the infinite series $\sum c_k/\alpha^k$ diverges for all α . In other words, (6.4) is strictly an asymptotic formula.

Proof. From the lemma in the previous section we have

$$\begin{aligned}
\rho_2(\alpha) &= \rho_1(\alpha) + S_1(\alpha) = \rho(\alpha) + \int_1^\alpha \frac{\rho(t-1)\,dt}{\alpha+1-t} \\
&= \rho(\alpha) + \int_1^\alpha \rho(t-1)\,dt\left(\frac{1}{\alpha} + \frac{t-1}{\alpha^2} + \dots + \frac{(t-1)^r}{\alpha^{r+1}} + \frac{(t-1)^{r+1}}{\alpha^{r+1}(\alpha+1-t)}\right) \\
&= \sum_{0 \leq k \leq r} \int_0^{\alpha-1} \rho(t) t^k\,dt/\alpha^{k+1} + O(\alpha^{-r-1})
\end{aligned} \tag{6.8}$$

since $\int_1^\alpha \rho(t-1)(t-1)^{r+1}\,dt/(\alpha+1-t) < \int_1^\infty \rho(t-1)(t-1)^{r+1}\,dt < \infty$.

Furthermore we have

$$\int_{\alpha-1}^\infty \rho(t)t^k\,dt = O\left(\int_{\alpha-1}^\infty e^{-t}\,t^k\,dt\right) = O\left(e^{-\frac{1}{2}\alpha}\right) \tag{6.9}$$

as $\alpha \to \infty$, by making very crude estimates not even as powerful as (6.3), so we can integrate to ∞ in (6.8):

$$\rho_2(\alpha) = \frac{a_0}{\alpha} + \frac{a_1}{\alpha^2} + \ldots + \frac{a_{r-1}}{\alpha^r} + O(\alpha^{-r-1}) \quad , \tag{6.10}$$

where

$$a_k = \int_0^\infty \rho(t)\,t^k\,dt \quad . \tag{6.11}$$

It remains to evaluate the a_k . We have

$$\sum_{k\geq 0} a_k \frac{(-x)^k}{k!} = \int_0^\infty \rho(t)\,e^{-xt}\,dt = e_1(x) = e^{-E(x) - \ln x} \tag{6.12}$$

by the theorem of Section 5; and it is well known that

$$-E(x) - \ln x = \gamma + \sum_{k\geq 1} (-x)^k/k\cdot k! \quad . \tag{6.13}$$

(See, for example, [7, exercise 5.2.2-43].) This combines with (6.12) and (6.6) to prove that $a_k = e^\gamma c_k$. □

The coefficients c_k have the curious property that

$$\rho_2(\alpha) = A\left(\frac{c_0}{\alpha+1} + \frac{2c_1}{(\alpha+1)^2} + \ldots + \frac{r\,c_{r-1}}{(\alpha+1)^r}\right) + O(\alpha^{-r-1}) \qquad (6.14)$$

is also an asymptotic expansion of ρ_2, but not as accurate when truncated. Another series,

$$\rho_2(\alpha) = A\left(\frac{c_0}{\alpha-1} + \frac{c_1-c_0}{2(\alpha-1)^2} + \frac{c_2-c_1+c_0}{3(\alpha-1)^3} + \ldots\right) + O(\alpha^{-r-1})$$

is, in turn, more accurate than (6.4). These series are obtainable from one another using the relation $\rho_2(\alpha) = -(\alpha+1)\rho_2'(\alpha+1) + \rho_1(\alpha)$.

For $k \geq 3$, we shall content ourselves with establishing the leading term in the asymptotic expansion of ρ_k, namely

$$\rho_k(\alpha) = \frac{A(\ln\alpha)^{k-2}}{(k-2)!\,\alpha} + O\left(\frac{(\ln\alpha)^{k-3}}{\alpha}\right) \qquad \text{for } k \geq 3 \ . \qquad (6.15)$$

[Appendix B contains an asymptotic expansion of ρ_3.] Consider first

$$S_2(\alpha) = \int_1^\alpha \left(\frac{A}{t} + O\left(\frac{1}{t^2}\right)\right)\frac{dt}{\alpha+1-t}$$

and note that

$$\int_1^\alpha \frac{dt}{t(\alpha+1-t)} = \frac{1}{\alpha+1}\left(\int_1^\alpha \frac{dt}{t} + \int_1^\alpha \frac{dt}{\alpha+1-t}\right) = \frac{2\ln\alpha}{\alpha+1} \ ,$$

$$\int_1^\alpha \frac{dt}{t^2(\alpha+1-t)} = \frac{1}{\alpha+1}\int_1^\alpha \frac{dt}{t^2} + \frac{1}{\alpha+1}\int_1^\alpha \frac{dt}{t(\alpha+1-t)}$$

$$= \frac{1}{\alpha+1}\left(1-\frac{1}{\alpha}\right) + \frac{2\ln\alpha}{(\alpha+1)^2} = O(\alpha^{-1}) \ . \qquad (6.17)$$

Hence $S_2(\alpha) = 2A\alpha^{-1}\ln\alpha + O(\alpha^{-1})$, and $\rho_3(\alpha) = A\alpha^{-1}\ln\alpha + O(\alpha^{-1})$ by (5.18). In order to use this approach for larger k, we note that, when $k \geq 1$,

$$\int_1^{\alpha} \frac{(\ln t)^k\, dt}{t(\alpha+1-t)} = \frac{1}{\alpha+1} \int_1^{\alpha} \frac{(\ln t)^k\, dt}{t} + \frac{1}{\alpha+1} \int_1^{\alpha} \frac{(\ln t)^k\, dt}{\alpha+1-t}$$

$$= \frac{1}{(\alpha+1)} \frac{(\ln \alpha)^{k+1}}{(k+1)} + \frac{k}{\alpha+1} \int_1^{\alpha} \frac{(\ln t)^{k-1} \ln(\alpha+1-t)\, dt}{t}$$

$$= \frac{1}{(\alpha+1)} \frac{(\ln \alpha)^{k+1}}{(k+1)} + \frac{\ln(\alpha+1)}{\alpha+1} (\ln \alpha)^k$$

$$+ \frac{k}{\alpha+1} \int_1^{\alpha} \frac{(\ln t)^{k-1} \ln\left(1 - \frac{t}{\alpha+1}\right) dt}{t} \quad .$$

Now $\ln(1-x) = -x\, f(x)$, where f is a function satisfying

$$1 < f\left(\frac{t}{\alpha+1}\right) \le f\left(\frac{\alpha}{\alpha+1}\right) = \frac{\alpha+1}{\alpha} \ln(\alpha+1) \qquad (6.18)$$

when $1 \le t \le \alpha$, hence

$$\int_1^{\alpha} \frac{(\ln t)^{k-1}}{t} \ln\left(1 - \frac{t}{\alpha+1}\right) dt = \frac{1}{\alpha+1} \int_1^{\alpha} (\ln t)^{k-1}\, O(\ln \alpha)\, dt$$

$$= O(\ln \alpha)^k \quad . \qquad (6.19)$$

We have proved that

$$\int_1^{\alpha} \frac{(\ln t)^k\, dt}{t(\alpha+1-t)} = \frac{k+2}{k+1} \frac{(\ln \alpha)^{k+1}}{\alpha} + O\left(\frac{(\ln \alpha)^k}{\alpha}\right) , \qquad (6.20)$$

for all $k \ge 0$. Using (5.18), formula (6.15) now follows by induction, together with

$$S_k(\alpha) = \frac{A\, k(\ln \alpha)^{k-1}}{(k-1)!\, \alpha} + O\left(\frac{(\ln \alpha)^{k-2}}{\alpha}\right) \quad . \qquad (6.21)$$

7. Application to factoring.

The distributions $F_k(x) = \rho_k(1/x)$ can be used to estimate the running time of various algorithms for factorization. For example, Pollard's important new Monte Carlo method [10] takes about $\sqrt{n_2}$ steps, where n_2 is the second-largest prime factor of n, so we can use a table of F_2 to state that Pollard's method will complete the factorization in $O(n^{.106})$ steps at most, about half of the time.

For the simple algorithm of Section 1, we need to analyze the distribution of $\max(n_2, \sqrt{n_1})$, and this does not appear to be expressible directly as an algebraic function of the F_k. However, we can readily carry out the analysis by using the techniques above. Let $G(x)$ be the limiting probability that $\max(n_2, \sqrt{n_1}) \le N^x$, when n is a random integer between 1 and N. Then $G(x) = F_1(x) + G_1(x) = F_2(x) - G_2(x)$, where $G_1(x)$ is the probability that $N^x \le n_1 \le N^{2x}$ and $n_2 \le N^x$, and $G_2(x)$ is the probability that $n_1 > N^{2x}$ and $n_2 \le N^x$. Arguing as above, we find

$$G_1(x) = \int_x^{2x} \frac{dt}{t} F_1\left(\frac{x}{1-t}\right) = \int_x^{2x} \frac{dt}{t} \rho\left(\frac{1-t}{x}\right), \tag{7.1}$$

$$G_1\left(\frac{1}{\alpha}\right) = \int_{1/\alpha}^{2/\alpha} \rho((1-t)\alpha)\, \frac{dt}{t} = \int_{\alpha-1}^{\alpha} \frac{\rho(u-1)du}{\alpha+1-u}, \tag{7.2}$$

$$G_2(x) = \int_{2x}^{1} \frac{dt}{t} F_1\left(\frac{x}{1-t}\right) = \int_{2x}^{1} \frac{dt}{t} \rho\left(\frac{1-t}{x}\right), \tag{7.3}$$

$$G_2\left(\frac{1}{\alpha}\right) = \int_{2/\alpha}^{1} \rho((1-t)\alpha)\, \frac{dt}{t} = \int_{1}^{\alpha-1} \frac{\rho(u-1)du}{\alpha+1-u}. \tag{7.4}$$

(Note that $G_1\left(\frac{1}{\alpha}\right) + G_2\left(\frac{1}{\alpha}\right) = S_1(\alpha) = F_2\left(\frac{1}{\alpha}\right) - F_1\left(\frac{1}{\alpha}\right)$, in agreement with the lemma of Section 5.) It is clear from our asymptotic results that $G_1(1/\alpha)$ decreases exponentially for large α, hence it is numerically better to use the formula $G(x) = F_1(x) + G_1(x)$ than to use $F_2(x) - G_2(x)$; furthermore the integration is over a limited range. On the other hand for $2 \leq \alpha \leq 3$ it is most convenient to use G_2 since $G_2\left(\frac{1}{\alpha}\right) = \ln(\alpha/2)$ in this range.

8. Remarks about the model.

The probability considerations above are for random n between 1 and N, and for relations such as $n_k \leq N^x$; but from an intuitive standpoint we might rather ask for the probability of a relation such as $n_k \leq n^x$, without considering N. Actually it is easy to convert from one model to the other, since most numbers between 1 and N are large.

More precisely, consider how many numbers n between $\frac{1}{2}N$ and N have $n_k \leq N^x$; this is $P_k(x,N) - p_k\left(x, \frac{1}{2}N\right) = \frac{1}{2}N \cdot F_k(x) + O(N/\log N)$, since $P_k(x,N) = N \cdot F_k(x) + O(N/\log N)$. Furthermore, consider how many of these n have $n^x < n_k \leq N^x$: The latter relation implies $N^x \geq n_k > \left(\frac{1}{2}N\right)^x = N^{x - \log 2/\log N}$, and $F_k(x - \log 2/\log N) = F_k(x) + O(1/\log N)$, since F_k is differentiable; so the number of such n is at most $P_k(x,N) - P_k(x - \log 2/\log N, N) = O(N/\log N)$. (The constant implied by the O in (4.7) will be independent of x in a bounded region about x.)

We have shown that $F_k(x) + O(1/\log N)$ of all n between $\frac{1}{2}N$ and N satisfy $n_k \leq n^x$. Therefore if $Q_k(x,N)$ denotes the total number of $n \leq N$ such that $n_k \leq n^x$, we have

$$Q_k(x,N) = \sum_{1 \leq j \leq \log_2 \log N} \frac{1}{2^j} N\left(F_k(x) + O\left(\frac{1}{\log(N/2^j)}\right)\right) + O\left(\frac{N}{\log N}\right)$$

$$= N F_k(x) + O\left(\frac{N}{\log N}\right), \tag{8.1}$$

by dividing the range $N/\log N \leq n \leq N$ into $\log_2 \log N$ parts.

It is customary to define the "probability" of a statement $S(n)$ about the positive integer n by the formula

$$\Pr(S(n)) = \lim_{N\to\infty} \frac{1}{N} \text{(number of } n \le N \text{ such that } S(n) \text{ is true)} , \qquad (8.2)$$

when this limit exists. Thus, we can state well-known facts such as the following: $\Pr(n \text{ is even}) = \frac{1}{2}$; $\Pr(n \text{ is prime}) = 0$; $\Pr(n \text{ is squarefree}) = 6/\pi^2$. Equation (8.1) now yields another result of this type:

$$\Pr(n_k \le n^x) = F_k(x) \quad , \qquad (8.3)$$

for all fixed x .

Another important observation should also be made about the theoretical model we have used to study the factorization algorithm in this paper: We have stated our results in terms of the probability that the running time is $\le N^x$ (or, if we prefer, n^x); this contrasts with the customary approach to the study of average running time, which derives mean values and the standard deviation. The reason for abandoning the traditional approach is that the mean and standard deviation are particularly uninformative for this algorithm. This phenomenon is apparent when we consider that the mean running time over all $n \le N$ will be relatively near the worst case $n^{0.5}$, but in more than 70 per cent of all cases the actual running time will be less than $n^{0.4}$.

In order to understand this rather anomalous situation more fully, let us calculate the asymptotic mean and standard deviation of the largest prime factor n_1 , when all integers $1 \le n \le N$ are considered equally likely. Let $\Phi(t)$ be the probability that $n_1 \le t$, when n is in this range. Then the derivation of Eq. (4.13) allows us to conclude that

$$\Phi(t) = 1 + \ln\ln t - \ln\ln N + \frac{1}{\ln N}\int_1^{N/t} \frac{\{u\}du}{u^2} + O\left(\frac{1}{\log N}\right)^2 , \qquad (8.4)$$

for $\sqrt{N} \leq t \leq N$.

We shall now calculate the asymptotic behavior of the k-th moment of this distribution, namely the asymptotic expected value of n_1^k . [Incidentally, our derivation provides a good example of the use of Stieltjes integration.] The k-th moment is

$$E(n_1^k) = \int_1^N t^k \, d\,\Phi(t) , \qquad (8.5)$$

and since the integral from $1+\sqrt{N}$ is $O\left(N^{k/2}\int_1^{\sqrt{N}} d\,\Phi(t)\right) = O(N^{k/2})$ it can safely be ignored. We are left with

$$\int_{\sqrt{N}}^N t^k \, d\left(1 + \ln\ln t - \ln\ln N + \frac{1}{\ln N}\int_1^{N/t} \frac{\{u\}du}{u^2} + O\left(\frac{1}{\log N}\right)^2\right)$$

$$= \int_{\sqrt{N}}^N t^k \, d(\ln\ln t) + \frac{1}{\ln N}\int_{\sqrt{N}}^1 \left(\frac{N}{v}\right)^k d\int_1^v \frac{\{u\}du}{u^2} + O\left(\frac{N^k}{(\log N)^2}\right) , \qquad (8.6)$$

by replacing t by N/v in the second integral. [The O estimate here is justified by the following general lemma: Let $\int_a^b f(t)\,d\,g(t)$ and $\int_a^b f(t)\,d\,h(t)$ exist, where $h(t) = O(g(t))$, and where both f and g are positive monotone functions on $[a,b]$. Then it is easy to see that

$$\int_a^b f(t)\,d\,O(g(t)) = O(f(a)g(a)) + O(f(b)g(b)) + O\left(\int_a^b f(t)\,d\,g(t)\right) ,$$

if we integrate by parts twice.] The first integral in (8.6) is

$$\int_{\sqrt{N}}^{N} \frac{t^{k-1}dt}{\ln t} = N^k \int_1^{\sqrt{N}} \frac{dv}{v^{k+1}(\ln N - \ln v)} = \frac{N^k}{\ln N}\left(\int_1^{\sqrt{N}} \frac{dv}{v^{k+1}} + \int_1^{\sqrt{N}} \frac{\ln v \; dv}{v^{k+1}(\ln N - \ln v)}\right)$$

$$= \frac{N^k}{k \ln N} + O\left(\frac{N^k}{(\log N)^2}\right) .$$

The second integral is $-N^k/\ln N$ times $\int_1^{\sqrt{N}} \{v\}dv/v^{k+2}$, which is within $O(N^{-(k+1)/2})$ of

$$\int_1^{\infty} \frac{\{v\}dv}{v^{k+2}} = \sum_{j \geq 1} \int_j^{j+1} \frac{(v-j)dv}{v^{k+2}}$$

$$= \sum_{j \geq 1}\left(\frac{1}{k}\left(\frac{1}{j^k} - \frac{1}{(j+1)^k}\right) - \frac{j}{k+1}\left(\frac{1}{j^{k+1}} - \frac{1}{(j+1)^{k+1}}\right)\right)$$

$$= \sum_{j \geq 1}\left(\frac{1}{k(k+1)}\left(\frac{1}{j^k} - \frac{1}{(j+1)^k}\right) - \frac{1}{k+1} \; \frac{1}{(j+1)^{k+1}}\right)$$

$$= \frac{1}{k(k+1)} - \frac{1}{k+1}\left(\zeta(k+1)-1\right) = \frac{1}{k} - \frac{\zeta(k+1)}{k+1} .$$

Thus we have shown that

$$E(n_1^k) = \frac{\zeta(k+1)}{k+1} \; \frac{N^k}{\ln N} + O\left(\frac{N^k}{(\log N)^2}\right) . \qquad (8.7)$$

It follows that the mean value of n_1 is asymptotically $(\pi^2/12)N / \ln N$, and the standard deviation is $(\zeta(3)/3)^{1/2} N / \sqrt{\ln N}$, to within a factor of $1 + O(1/\log N)$. In particular, the ratio

$$\frac{\text{standard deviation}}{\text{mean}} \rightarrow \infty \qquad (8.8)$$

as $N \rightarrow \infty$; this result demonstrates the unsuitability of a traditional "mean and variance" approach to the analysis of such algorithms.

9. Numerical results.

The differential-difference equations for ρ_k are conveniently suited to numerical integration. For example, given internal arrays containing $\rho_1(m + k/n)$, $\rho_2(m + k/n)$, and $\rho_3(m + k/n)$ for $0 \leq k \leq n+t$, where m is some fixed integer and $\delta = 1/n$ is the step size and t depends on the method of integration, one pass over these arrays serves to increase m by 1. When m reaches a suitably large value, the asymptotic formulas derived above provide an excellent check on the accuracy of the calculations. Another excellent check comes from the formula

$$e^{\gamma} = \int_0^{\infty} \rho(t)dt = \rho(1) + 2\rho(2) + 3\rho(3) + \dots \quad ; \qquad (9.1)$$

cf. (6.2), (6.5), and (6.11). (Incidentally, identity (9.1) appears to be new; it was discovered empirically, after noticing that the results of numerical integration seemed to resemble a "familiar" constant. This particular constant came as a surprise, since e^{γ} usually occurs only in connection with infinite products. After the proof of (9.1) was found, the theorem in Section 5 above followed rather quickly. Thus, numerical results indeed suggest theorems.)

The following table gives representative values of ρ_1, ρ_2, ρ_3 and G to 12D :

α	$\rho_1(\alpha)$	$\rho_2(\alpha)$	$\rho_3(\alpha)$	$G(1/\alpha)$
1.0	1.000000 000000	1.000000 000000	1.000000 000000	1.000000 000000
1.5	.594534 891892	1.000000 000000	1.000000 000000	1.000000 000000
2.0	.306852 819440	1.000000 000000	1.000000 000000	1.000000 000000
2.5	.130319 561832	.953389 706294	1.000000 000000	.730246 154979
3.0	.048608 388291	.852779 323041	1.000000 000000	.447314 214932
3.5	.016229 593243	.733481 165219	.997526 273042	.223819 493955
4.0	.004910 925648	.623681 059959	.985113 653272	.096399 005935
4.5	.001370 117741	.533652 572034	.960975 011157	.036573 065077
5.0	.000354 724700	.463222 186987	.927859 653628	.012413 482748
6.0	.000019 649696	.365217 751694	.851107 195638	.001092 266742
7.0	.000000 874567	.301786 010308	.777229 329492	.000071 391673
8.0	.000000 032321	.257435 710831	.712844 794121	.000003 662651
9.0	.000000 001016	.224592 162720	.657959 581954	.000000 153284
10.0	.000000 000028	.199248 208994	.611115 997540	.000000 005383
12.0	.000000 000000	.162638 856635	.535865 613616	.000000 000004
14.0	.000000 000000	.137437 368144	.478221 749442	.000000 000000
16.0	.000000 000000	.119016 453035	.432642 865532	.000000 000000
18.0	.000000 000000	.104958 753569	.395653 753569	.000000 000000
20.0	.000000 000000	.093875 845625	.364991 546696	.000000 000000
25.0	.000000 000000	.074277 803044	.307069 057805	.000000 000000
30.0	.000000 000000	.061453 736517	.266170 912880	.000000 000000
40.0	.000000 000000	.045683 813582	.211838 770538	.000000 000000
50.0	.000000 000000	.036356 095670	.177085 969207	.000000 000000
60.0	.000000 000000	.030192 055732	.152778 425203	.000000 000000

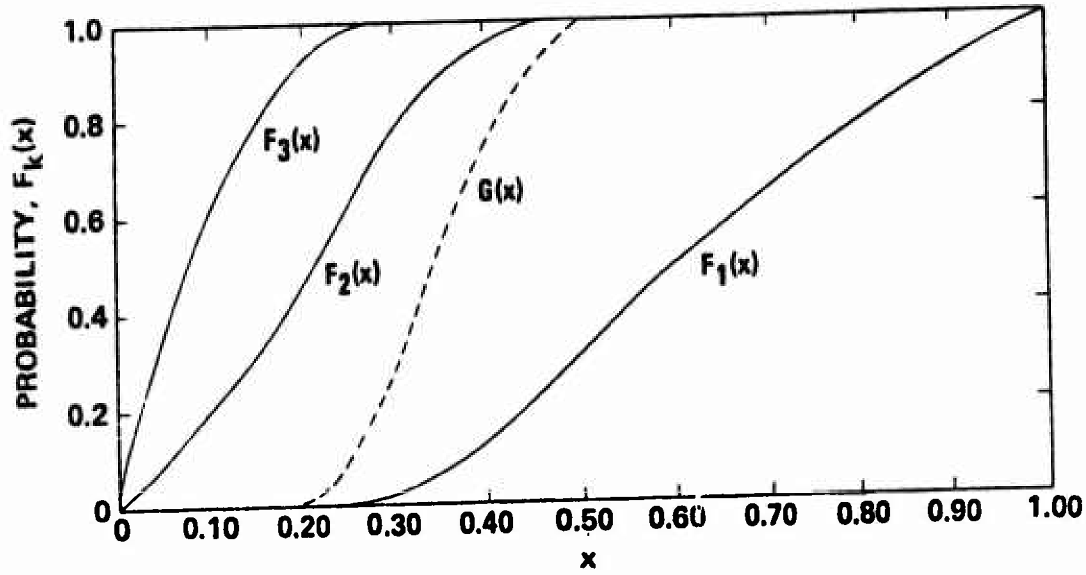

Figure 1. Distributions of the three largest prime factors of a random integer, and the distribution of the simple factorization time.

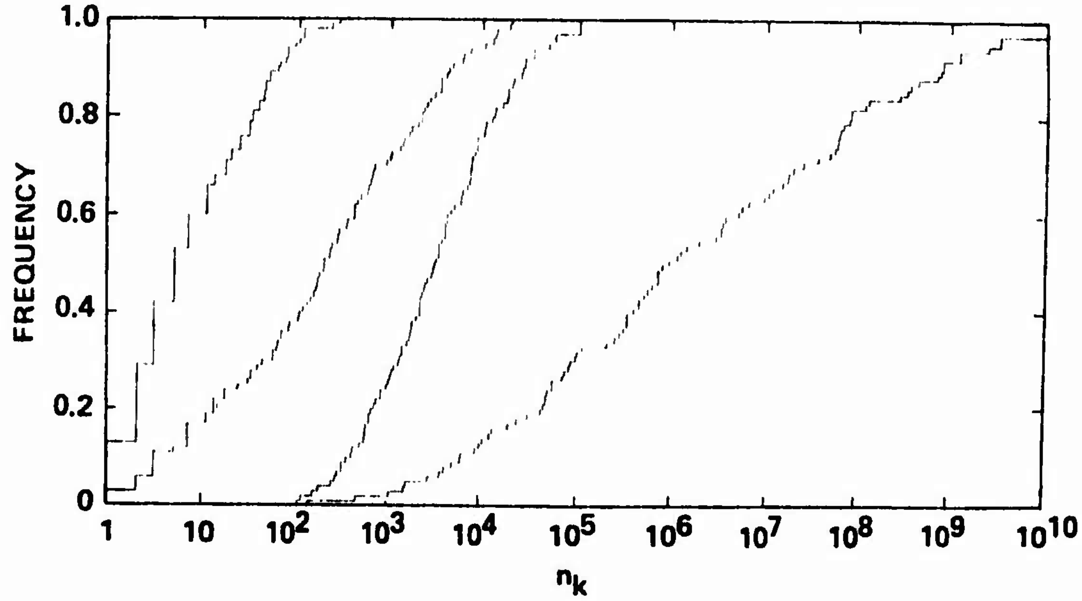

Figure 2. Empirical distribution functions corresponding to Figure 1, based on the factors of the largest 100 10-digit numbers.

(In 1930, Dickman published 8D values of $\rho_1(\alpha)$ for integer $\alpha \leq 8$; his figures were correct except that $\rho_1(7)$ was given as " .0000 0088 ".)

Figure 1 shows these distributions graphically, and illustrates the fact that $F_1'(0) = G'(0) = F_2'\left(\frac{1}{2}\right) = F_3'\left(\frac{1}{2}\right) = 0$, $F_2'(0) = A$, $G'\left(\frac{1}{2}\right) = 2$, $F_1'(1) = 1$, $F_3'(0) = \infty$. Although the graphs of F_1 , F_2 , and F_3 are qualitatively different, the graphs of F_k for $k \geq 4$ will resemble that of F_3 (but they will rise ever more steeply).

The following table shows percentage points of the distributions F_1 , F_2 , F_3 ; for example, the probability is only 10 percent that $n_3 > n^{.18616}$.

p	$F_1^{-1}(p)$	$F_2^{-1}(p)$	$F_3^{-1}(p)$
.01	.26974	.00558	.00068
.02	.29341	.01110	.00149
.03	.31004	.01656	.00239
.04	.32341	.02196	.00334
.05	.33483	.02730	.00435
.10	.37851	.05308	.00995
.15	.41288	.07741	.01629
.20	.44304	.10033	.02327
.25	.47068	.12191	.03079
.30	.49656	.14216	.03882
.40	.54881	.17892	.05636
.50	.60653	.21172	.07584
.60	.67032	.24267	.09745
.70	.74082	.27437	.12165
.75	.77880	.29153	.13506
.80	.81873	.31035	.14972
.85	.86071	.33201	.16627
.90	.90484	.35899	.18616
.95	.95123	.39672	.21377
.96	.96079	.40681	.22141
.97	.97045	.41850	.23054
.98	.98020	.43268	.24224
.99	.99005	.45169	.25954
1.00	1.00000	.50000	.33333

Empirical confirmation of the theory is illustrated in Figure 2, which shows exact empirical distribution functions corresponding to Figure 1 for the 100 numbers $n = 10^{10}-m$, $1 \leq m \leq 100$. As expected, the deviation from $F_k(x)$ is most pronounced for $k = 1$ and $x > \frac{1}{2}$, but the deviations are not severe. This set of numbers contains three primes $(10^{10}-33, 10^{10}-57, 10^{10}-71)$, and ten products of two primes. The smallest values of n_1 occurred for $10^{10}-100 = 137\cdot101\cdot73\cdot11\cdot5^2\cdot3^2\cdot2^2$, $10^{10}-64 = 463\cdot431\cdot29\cdot3^3\cdot2^6$; the largest values of n_2 occurred for $10^{10}-69 = 456767\cdot21893$, $10^{10}-22 = 85021\cdot19603\cdot3\cdot2$; the largest values of n_3 occurred for $10^{10}-51 = 88301\cdot421\cdot269$, $10^{10}-73 = 13879\cdot359\cdot223\cdot3^2$. The smallest values of $\max(\sqrt{n_1}, n_2)$ occurred for $10^{10}-100 = 137\cdot101\cdot73\cdot11\cdot5^2\cdot3^2\cdot2^2$, $10^{10}-25 = 2857\cdot113\cdot59\cdot7\cdot5^2\cdot3$ (so these would be the easiest numbers in the given range to factor by the simple algorithm); the smallest values of n_1 for which $\sqrt{n_1} > n_2$ occurred for $10^{10}-66 = 59417\cdot103\cdot43\cdot19\cdot2$, $10^{10}-68 = 77201\cdot53\cdot47\cdot13\cdot2^2$.

In Dickman's original paper he calculated the "average" value of x such that $n_1 = n^x$, namely the expected value of $\log n_1 / \log n$. This equals

$$D_1 = \int_0^1 x\,d\,F_1(x) = -\int_1^\infty \rho'(t)\ dt/t = \int_1^\infty \rho(t-1)\ dt/t^2 \qquad (9.2)$$

and by Eq. (5.14) we also have

$$\int_1^\infty \rho(t-1)\ dt/t^2 = -S_1(\infty,-1) = \int_1^\infty \rho(t-1)\ dt/(t+1) \quad . \qquad (9.3)$$

In a similar way we can determine the expected value of $\log n_k / \log n$, a number which can be expressed in several ways, namely

$$D_k = \int_0^1 x\, d\, F_k(x) = \int_1^\infty (\rho_k(t-1) - \rho_{k-1}(t-1))\ dt/t^2 = 1 - \int_1^\infty \rho_k(t)\ dt/t^2$$

$$= \int_1^\infty (\rho_k(t-1) - 2\rho_{k-1}(t-1) + \rho_{k-2}(t-1))\ dt/(t+1) . \qquad (9.4)$$

Numerical evaluation (using the asymptotic formulas for ρ_2 and ρ_3) gives

$$D_1 = .62432\ 99885 ; \qquad (9.5)$$

$$D_2 = .20958\ 08743 ; \qquad (9.6)$$

$$D_3 = .08831\ 60989 . \qquad (9.7)$$

(Dickman's value for D_1 was $.624329998$. Note that D_2 is not equal to $D_1(1-D_1)$, although n_2 is the largest prime factor of n/n_1.)

The average value of a logarithm may seem at first to be of limited practical interest, by comparison with the median and other percentiles; however, we can interpret it meanin fully by saying that $D_k m$ is the <u>asymptotic average number of digits</u> in the k-th largest prime factor of an m-digit number. Dickman's constant D_1 arises also in an unexpected way in connection with our simple factoring algorithm: The probability that $n_2 < \sqrt{n_1}$, namely the probability that the algorithm needs to divide by all numbers up to $\sqrt{n_1}$, is

$$\int_0^1 \frac{dt}{t} F_1\left(\frac{t}{2(1-t)}\right) = \int_0^1 \frac{dt}{t} \rho\left(\frac{2(1-t)}{t}\right) = \int_1^\infty \rho(u-1)\ du/(u+1) \qquad (9.8)$$

by substituting $u = 2/t - 1$. So this probability equals D_1 ! In the empirical tests which led to Figure 2, exactly 61 of the 100 numbers had $n_2 < \sqrt{n_1}$.

10. Relation to permutations.

The numerical value of D_1 in (9.5) leads again to a feeling of déjà vu; and sure enough Dickman's constant turns out to be the same as "Golomb's constant", which has been evaluated to 53 places in [6]. Golomb's constant λ is defined to be $\lim_{n\to\infty} \ell_n/n$, where ℓ_n is the average length of the longest cycle in a random permutation. In Golomb's original analysis [5] of this combinatorial problem (which is not obviously related to prime factors at all!), he independently defined a function essentially identical to $\rho(\alpha)$, and he computed $\lambda = \int_1^\infty \rho(t-1)dt/t^2$ numerically. Another expression $\lambda = \int_0^\infty \exp(-x-E(x))\,dx$ was found later by L. Shepp and S. P. Lloyd [12].

In Table 1 of their paper, Shepp and Lloyd list also the limiting values $\ell^{(k)}/n \to \int_0^\infty E(t)^{k-1}\exp(-t-E(t))dt/(k-1)!$ for the average length of the k-th longest cycle; and this agrees numerically with D_k for $1 \leq k \leq 3$. In fact, the Shepp - Lloyd formula yields D_k for all k, since

$$\begin{aligned}\int_0^\infty \frac{E(t)^{k-1}}{(k-1)!}\exp(-t-E(t))dt &= \int_0^\infty t\,e^{-t}(e_k(t)-e_{k-1}(t))dt \\ &= \int_0^\infty t\,e^{-t}\int_0^\infty (\rho_k(u)-\rho_{k-1}(u))e^{-tu}\,du\,dt \\ &= \int_1^\infty (\rho_k(u-1)-\rho_{k-1}(u-1))\int_0^\infty t\,e^{-t(u)}\,dt\,du \\ &= \int_1^\infty (\rho_k(u-1)-\rho_{k-1}(u-1))\,du/u^2 \ . \qquad (10.1)\end{aligned}$$

Therefore, if we are factoring a random m-digit number, the distribution of the number of digits in its prime factors is approximately the same as the distribution of the cycle lengths in a random permutation on m elements! (Note that there are approximately $\ln m$ factors, and approximately $\ln m$ cycles.)

There is a fairly simple explanation for the fact that $\rho_k(\alpha)$ turns up in the study of cycles in permutations. Let $Q_k(n,r)$ be the number of permutations on n objects having less than k cycles of length exceeding r. Then, by considering the permutations on $n+1$ elements $\{0,1,\ldots,n\}$ and considering the $n!/(n-m)!$ possible cycles in which 0 appears with m different elements, we have

$$Q_k(n+1,r) = \sum_{0\le m<r} \frac{n!}{(n-m)!} Q_k(n-m,r) + \sum_{r\le m\le n} \frac{n!}{(n-m)!} Q_{k-1}(n-m,r) \quad . \tag{10.2}$$

Therefore if $q_k(n,r) = Q_k(n,r)/n!$ is the probability that the k-th largest cycle has length $\le r$, we have

$$(n+1)q_k(n+1,r) = \sum_{0\le m<r} q_k(n-m,r) + \sum_{r\le m\le n} q_{k-1}(n-m,r) \quad ; \tag{10.3}$$

replacing n by $n-1$ yields

$$nq_k(n,r) = \sum_{0\le m<r} q_k(n-1-m,r) + \sum_{r\le m\le n} q_{k-1}(n-1-m,r) \quad . \tag{10.4}$$

Subtracting these two equations, we have

$$(n+1)(q_k(n+1,r) - q_k(n,r)) = q_{k-1}(n-r,r) - q_k(n-r,r) \quad , \tag{10.5}$$

and this is analogous to the differential equation

$$\alpha\, \rho_k'(\alpha) = \rho_{k-1}(\alpha-1) - \rho_k(\alpha-1) \quad . \tag{10.6}$$

The connection between the two problems is completed by showing that $q_k(n,r) = \rho_k(n/r) + O(1/r)$.

A similar distribution is obtained for the degrees of the factors of a random polynomial of degree n , over a finite field: The average degree of the k-th "largest" irreducible factor will tend to be approximately $D_k n$.

Let us close by stating an open problem: Are the functions ρ_k algebraically independent? They are linearly independent, because of Eq. (5.5).

Acknowledgments. We wish to thank Marvin Wunderlich and John Pollard for correspondence relating to early drafts of this paper. A letter received from Nathan J. Fine in June, 1965, regarding Golomb's problem, was also very helpfu: for this research.

Appendix A. The number of prime factors.

Following the notation of Hardy and Wright [6], let $\omega(n)$ be the number of distinct prime factors of n , and let $\Omega(n)$ be the total number of prime factors including multiplicity. Thus, $\Omega(n)$ is the quantity T in the analysis of the algorithm above. Clearly $1 \le \Omega(n) \le \log_2 n$, and both of these limits are obtained for infinitely many n ; similarly $\omega(n)$ can get as large as $\ln n / \ln \ln n$. On the other hand these extreme values are relatively rare, and the number of factors is usually near $\ln \ln n$.

P. Erdös and M. Kac [4] proved that the number of n in the range $1 \le n \le N$ such that $\omega(n) < \ln \ln N + c\sqrt{\ln \ln N}$ is

$$\left(\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{c} e^{-t^2/2}\, dt\right) N + o(N) \quad ; \tag{A.1}$$

hence, for example, the probability that $|\omega(n) - \ln \ln N| < c\sqrt{\ln \ln N}$ for fixed $c > 0$ approaches the limiting value

$$\frac{1}{\sqrt{2\pi}} \int_{-c}^{c} e^{-t^2/2}\, dt \quad . \tag{A.2}$$

We might say that $\omega(n)$ behaves essentially like a normally distributed random variable with mean and variance $\ln \ln n$, where n is large.

Erdös and Kac remarked that their methods, which were based on the idea that residues modulo distinct primes are independent, could be extended to the case of prime factors with multiplicities included, but they did not state what the resulting theorem would be. Fortunately it is easy to deduce the asymptotic behavior of $\Omega(n)$ from that of $\omega(n)$, using a method like that in [5]. Let $k(N)$ be the number of n in $1 \le n \le N$ such that

$$\omega(n) < \ln \ln N + c\sqrt{\ln \ln N} \qquad (A.3)$$

and let $K(N)$ be the number such that

$$\Omega(n) < \ln \ln N + c\sqrt{\ln \ln N} + \ln \ln \ln N \ . \qquad (A.4)$$

Then $|k(N) - K(N)|$ is at most the number of n which satisfy (A.3) but not (A.4), or (A.4) but not (A.3), and both of these quantities are $o(N)$: If n satisfies (A.3) but not (A.4), we have $\Omega(n) - \omega(n) > \ln \ln \ln N$; and the number of such n is $O(N / \ln \ln \ln N)$, because

$$\sum_{1 \le n \le N} (\Omega(n) - \omega(n)) = O(N) \qquad (A.5)$$

by [6, Theorem 430]. If n satisfies (A.4) but not (A.3), then

$$\ln \ln N + c\sqrt{\ln \ln N} \le \omega(n) < \ln \ln N + \left(c + \frac{\ln \ln \ln N}{\sqrt{\ln \ln N}}\right)\sqrt{\ln \ln N} \ ,$$

and this is $o(N)$ by the theorem of Erdös and Kac.

We have proved that the number of n in the range $1 \le n \le N$ such that $\Omega(n) < \ln \ln N + c\sqrt{\ln \ln N}$ is asymptotically given by the normal distribution (A.1). But this estimate is insensitive to $O(1)$ terms, so the "average order" [6, Theorem 430] is also relevant:

$$\lim_{N \to \infty} \frac{1}{N} \sum_{1 \le n \le N} (\omega(n) - \ln \ln N)$$

$$= \gamma + \sum_{p \text{ prime}} \left(\log\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right) \approx .26149\ 72128\ 47643 \ ; \qquad (A.6)$$

$$\lim_{N\to\infty} \frac{1}{N} \sum_{1\le n\le N} (\Omega(n) - \ln\ln N)$$

$$= \gamma + \sum_{p\ \mathrm{prime}} \left(\log\left(1 - \frac{1}{p}\right) + \frac{1}{p-1}\right) \approx 1.03465\ 38818\ 97438\ . \qquad \text{(A.7)}$$

(These sums may be evaluated to high precision using the formula

$$\sum_{p\ \mathrm{prime}} \frac{1}{p^s} = \sum_{n\ge 1} \frac{\mu(n)}{n} \ln \zeta(ns) \qquad \text{(A.8)}$$

for $s > 1$.)

Let $S = \{10^{10} - m \mid 1 \le m \le 100\}$ be the numbers used to construct Figure 2 above. For $n \in S$ we have $\ln\ln n \approx 3.1366$, and the following table shows the actual distribution of $\omega(n)$ and $\Omega(n)$.

$k =$	1	2	3	4	5	6	7	8	9	10	11	12
$\lVert\{n\in S \mid \omega(n) = k\}\rVert$	3	14	36	29	14	3	1	0	0	0	0	0
$\lVert\{n\in S \mid \Omega(n) = k\}\rVert$	3	10	27	23	15	11	5	3	1	1	0	1

The respective mean values are 3.50 and 4.27 . The number of square-free n (those with $\omega(n) = \Omega(n)$) was 61 , compared to the expected value $600/\pi^2 = 60.793$.

Appendix B. An asymptotic formula for ρ_3 .

In this appendix we shall sketch the derivation of an asymptotic expression for $\rho_3(\alpha)$ as $\alpha \to \infty$. Our starting point is the formula

$$S_2(\alpha) = \int_0^{\alpha-1} \frac{\rho_2(t)\,dt}{\alpha-t}$$

$$= \sum_{0\le k\le r} \frac{1}{\alpha^{k+1}} \int_0^{\alpha-1} \rho_2(t)\, t^k\, dt + \frac{1}{\alpha^{r+1}} \int_0^{\alpha-1} \frac{\rho_2(t)\, t^{r+1}\, dt}{\alpha-t} \; ; \qquad (\text{B.1})$$

we replace the final term by its asymptotic value

$$\frac{A}{\alpha^{r+1}} \int_0^{\alpha-1} \frac{(c_0 t^r + c_1 t^{r-1} + \ldots + c_{r-1} t)\,dt}{\alpha-t} + O\left(\frac{1}{\alpha^{r+1}} \int_0^{\alpha-1} \frac{dt}{\alpha-t}\right) \quad , \qquad (\text{B.2})$$

so that the remainder is $O(\alpha^{-r-1}\log\alpha)$. The main integral in (B.2) is a linear combination of

$$\int_0^{\alpha-1} \frac{t^k\, dt}{\alpha-t} = \int_1^{\alpha} \frac{(\alpha-t)^k\, dt}{t} = \alpha^k(\ln\alpha - H_k) - \sum_{j\ge1} \binom{k}{j} (-1)^j \frac{\alpha^{k-j}}{j} \quad , \qquad (\text{B.3})$$

and it remains to evaluate $\int_0^{\alpha-1} \rho_2(t)\, t^k\, dt$ to $O(\alpha^{k-r}\log(\alpha))$.

Since $\rho_2 = S_1 + \rho_1$, we have

$$\int_0^{\alpha} \rho_2(t)\, t^k\, dt = \int_0^{\alpha} t^k\, dt \left(\int_0^{t} \frac{\rho(u-1)}{t+1-u}\, du + \rho(t) \right)$$

$$= \left(\int_0^{\alpha} \rho(u-1)\,du \int_u^{\alpha} \frac{t^k}{t+1-u}\, dt \right) + a_k + O(\alpha^{-r-1})$$

$$= \int_1^{\alpha} \rho(u-1)(u-1)^k \ln(\alpha+1-u)\,du$$

$$+ \sum_{j \geq 1} \binom{k}{j} \frac{1}{j} \int_1^{\alpha} \rho(u)(u-1)^{k-j}((\alpha+1-u)^j-1) + a_k + O(\alpha^{-r-1})$$

$$= \sum_{1 \leq j \leq k} \left(\alpha^j - \binom{k}{j}\right) a_{k-j}/j + (\ln \alpha - H_k + 1)a_k$$

$$- \sum_{1 \leq j \leq r} \alpha^{-j} a_{k+j}/j + O(\alpha^{-r-1}) \quad , \qquad \text{(B.4)}$$

where $a_k = \int_0^{\infty} \rho(t)\, t^k\, dt = A\, c_k$. Putting all this together and summing leads to the formula

$$S_2(\alpha) = (2 \ln \alpha + 1)\rho_2(\alpha) - \frac{2b_0}{\alpha} - \frac{2b_1}{\alpha^2} - \cdots - \frac{2b_{r-1}}{\alpha^r} + O(\alpha^{-r-1}) \quad , \qquad \text{(B.5)}$$

where

$$b_k = H_k\, a_k + \sum_{1 \leq j \leq k} \binom{k}{j} a_{k-j}/j \quad . \qquad \text{(B.6)}$$

In particular, $\langle b_0, b_1, b_2, \ldots \rangle = A \left\langle 0 , 2 , \frac{19}{4} , \frac{415}{36} , \frac{551}{18} , \frac{13391}{150} , \frac{1023289}{3600} , \ldots \right\rangle$. Since $\rho_3 = \frac{1}{2}(\rho_1(\alpha) + \rho_2(\alpha) + S_2(\alpha))$, we have the final formula

$$\rho_3(\alpha) = (\ln \alpha + 1)\rho_2(\alpha) - \frac{b_0}{\alpha} - \cdots - \frac{b_{r-1}}{\alpha^r} + O(\alpha^{-r-1}) \quad . \qquad \text{(B.7)}$$

References

[1] N. G. de Bruijn, "On the number of positive integers $\le x$ and free of prime factors $> y$," *Proc. Kon. Nederl. Akad. Wetensch.* **A54** (= *Indag. Math.* **13**) (1951), 50-60.

[2] Charles de la Vallée Poussin, "Sur la fonction $\zeta(s)$ de Riemann et le nombre des nombres premiers inférieurs à une limite donnée," *Mém. Couronnés Acad. Roy. Belgique* **59** (1899), 1-74.

[3] Karl Dickman, "On the frequency of numbers containing prime factors of a certain relative magnitude," *Arkiv för Matematik, Astronomi och Fysik* **22A**, 10 (1930), 1-14.

[4] P. Erdös and M. Kac, "The Gaussian law of errors in the theory of additive number theoretic functions," *Amer. J. Math.* **26** (1940), 738-742.

[5] S. W. Golomb, L. R. Welch, and R. M. Goldstein, "Cycles from nonlinear shift registers," Prog. Report No. 20-389, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, Calif., 1959.

[6] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed. Oxford: Clarendon Press, 1960.

[7] Donald E. Knuth, *Sorting and Searching*, *The Art of Computer Programming*, vol. 3, Addison-Wesley, Reading, Mass., 1973.

[8] William C. Mitchell, "An evaluation of Golomb's constant," *Math. Computation* **22** (1968), 411-415.

[9] K. K. Norton, "Numbers with small prime factors, and the least k-th power non-residue," *Memoirs Amer. Math. Soc.* **106** (1971), 9-27.

[10] J. M. Pollard, "A Monte-Carlo method for factorization," *BIT* **15** (1975), 331-334.

[11] V. Ramaswami, "The number of positive integers $< x$ and free of prime divisors $> x^c$, and a problem of S. S. Pillai," *Duke Math. J.* **16** (1949), 99-109.

[12] L. Shepp and S. P. Lloyd, "Ordered cycle lengths in a random permutation," *Trans. Amer. Math. Soc.* **121** (1966), 340-357.

[13] J. van de Lune and E. Wattel, "On the numerical solution of a differential-difference equation arising in analytic number theory," *Math. Computation* **23** (1969), 417-421.

[14] M. L. Wunderlich and J. L. Selfridge, "A design for a number theory package with an optimized trial division routine," *Comm. ACM* **17** (May 1974), 272-276.