Anatomy of Integers and Random Permutations
Course Lecture Notes

Kevin Ford

DEPARTMENT OF MATHEMATICS, 1409 WEST GREEN STREET, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, URBANA, IL 61801, USA
E-mail address: ford126@illinois.edu

Contents

1. Notation

1.1. Number Theory. Standard number theory functions:
$\tau(n)$ is the number of positive divisors of n
$\omega(n)$ is the number of distinct prime factors of n
$\omega(n,t)$ is the number of distinct prime factors of n which are $\leqslant t$
$\omega(n;S)$ is the number of distinct prime factors of n that lie in the set S
$\Omega(n)$ is the number of prime factors of n counted with multiplicity
$\mu(n)$ is the Möbius's function; $\mu(n)=(-1)^{\omega(n)}$ if n is squarefree and $\mu(n)=0$ otherwise.
$P^+(n)$ is the largest prime factor of n; $P^+(1)=0$ by convention
$P^-(n)$ is the smallest prime factor of n; $P^-(1)=\infty$ by convention
$\Lambda(n)$ denotes the von Mangoldt function: $\Lambda(p^a)=\log p$ for prime p and $a\in\mathbb{N}$, $\Lambda(n)=0$ otherwise

1.2. Permutations. We adopt the following notation for permutations:
$\mathcal{S}_n$ is the permutation group on a set of n objects (we don't care what the objects are)
$\mathcal{S}_{n,m}$ is the set of permutations in $\mathcal{S}_n$ which have no cycles of length $<m$.
$C_j(\sigma)$ is the number of cycles of length j in the permutation σ
$C(\sigma)$ is the total number of cycles in the permutation σ
$C_I(\sigma)$ is the number of cycles of length $j\in I$ in the permutation σ
$\mathscr{C}(\sigma)$ is the set of cycles in the permutation σ
$\beta|\sigma$ means that β is a *divisor* of the permutation σ, i.e. a product of some subset of the cycles of σ
A *fixed set* I of σ is a subset of $[n]$ which is itself permuted by σ. Equivalently, I is the set of indices permuted by a divisor of σ.
$|\beta|$ is the size of β; β is a divisor of a permutation.

1.3. Order of magnitude notation. Standard Bachman-Landau, Hardy, Vinogradov notations
$f=O(g)$, $f\ll g$ and $g\gg f$ mean that there is a positive constant C so that $|f|\leqslant Cg$ throughout the domain of f. The constant C is independent of any parameters, unless specified by subscripts, e.g. $f(x)=O_\varepsilon(x^\varepsilon)$.
$f\asymp g$ means that both $f\ll g$ and $g\ll f$ hold. Generally makes sense only if f,g are both positive.
$f\sim g$ as $x\to a$ means $\lim_{x\to a} f(x)/g(x)=1$. Here a can be finite, ∞ or $-\infty$.

1.4. Probability. Definitions from probability theory
$\mathbb{P}(X)$ is the probability of the event X
$\mathbb{E}(X)$ is the expectation of the event X
$X\overset{d}{=}Y$ means that X has the same distribution as Y
$\mathrm{Pois}(\lambda)$ is a Poisson random variable with parameter λ

1.5. General. Miscellaneous definitions
$\mathbb{N}=\{1,2,3,\ldots\}$, the set of positive integers ("natural numbers")
$\mathbb{N}_0=\{0,1,2,3,\ldots\}=\mathbb{N}\cup\{0\}$
$\mathrm{e}=2.71828182\ldots$ is the base of the natural logarithm
$\gamma=0.57721566\ldots$ is Euler's constant
$\log$ is the natural logarithm
$\log_k x$ is the $k-$th iterate of the natural logarithm of x
$\lfloor x\rfloor$ is the greatest integer which is $\leqslant x$.
$\mathbf{1}(S)$ is the indicator function of statement S; $\mathbf{1}(S)=\begin{cases}1 & S \text{ is true}\\ 0 & S \text{ is false.}\end{cases}$
$H_n=1+1/2+\cdots+1/n$ is the n-th harmonic sum
$H(I)=\sum_{i\in I}1/i$ is a general harmonic sum, where $I\subset\mathbb{N}$
Z_J is a Poisson random variable with parameter $H(J)$
Variables in boldface type, e.g. $\mathbf{h}$, usually denote vector quantities.

CHAPTER 1

Introduction

1. Overview and brief history

Positive integers factor uniquely into a product of prime numbers, and permutations factor uniquely into a product of cycles. Despite this similarity, the two objects, integers and permutations, look very different on the surface. Deeper inspection, however, reveals that the *distribution* of the two factorizations have many common features, and for much the same underlying reasons.

1.1. Prime factors and divisors. The study of the distribution of prime factors of integers began with the work of Landau, who showed

Theorem (Landau, 1900). For every fixed k,

$$\pi_k(x) := \#\{n \leqslant x : \omega(n) = k\} \sim \frac{x}{\log x} \frac{(\log_2 x)^{k-1}}{(k-1)!}.$$

This already suggests that $\omega(n)$ has a Poisson distribution, although Landau never wrote this explicitly. It was Hardy and Ramanujan in 1917 who analyzed the behavior of $\pi_k(x)$ uniformly in k, showing

Theorem (Hardy-Ramanujan, 1917). Uniformly for $x \geqslant 2$ and $k \geqslant 1$,

$$\pi_k(x) \leqslant C_1 \frac{x}{\log x} \frac{(\log_2 x + C_2)^{k-1}}{(k-1)!},$$

where C_1, C_2 are certain absolute constants.

Summing the upper bound for $k \geqslant (1+\varepsilon)\log_2 x$ and $k \leqslant (1-\varepsilon)\log_2 x$, with $\varepsilon > 0$ fixed, and using standard bounds on the tail of the Poisson distribution (see (1.11) below), one obtains a sum of $o(x)$. Consequently, most $n \leqslant x$ have close to $\log_2 x$ distinct prime factors. This result is sometimes referred to as the birth of probabilistic number theory.

Motivated by the fact that the Poisson distribution tends to the Gaussian as the parameter tends to infinity (see (4.10)), Erdős and Kac proved their celebrated "Central Limit Theorem" for $\omega(n)$ in 1939:

Theorem (Erdős-Kac, 1939 [EK40]). For any real z,

$$\frac{1}{x}\#\left\{n \leqslant x : \frac{\omega(n) - \log_2 x}{\sqrt{\log_2 x}} \leqslant z\right\} \to \Phi(z) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-\frac{1}{2}t^2}\, dt \qquad (x \to \infty).$$

Much further work was done starting in the 1940s, examining the distribution of the entire *sequence of prime factors* of integers (equivalently, studying the distribution of arbitrary *additive functions*). Perhaps the most notable was the work of Kubilius, who developed a probabilistic model of integers which provides a kind of meta-tool for studying al kinds of statistical questions about the distribution of prime factors. A key concept in the theory is *independence*, the idea that if p and q are small primes, then the "events" $p|n$ and $q|n$ are nearly independent, from a probabilistic viewpoint; this idea also played a prominent role in the development of sieve methods. The theory leads to a "Poisson model" of prime factors; namely that the number of prime factors in an interval $(e^{e^a}, e^{e^b}]$ has roughly $\mathrm{Pois}(b-a)$ distribution, with disjoint intervals having independent distributions.

The distribution of divisors of integers has also received much attention, beginning in the 1930s. Much of the study was motivated by two fundamental problems:

(a) (Besicovitch, 1934). Given a quantity y, what is the density of integers that have a divisor in $(y, 2y]$?

(b) (Erdős, 1948). Do almost all integers (that is, a set of density 1) have two divisors in some dyadic interval $(z, 2z]$?

Estimates for the density in Problem (a) were given by Erdős and Tenenbaum, with Ford giving the order of magnitude of the order in 2008 [**For08**]. The solution of Problem (b), in the positive, was given by Maier and Tenenbaum in 1984 [**MT84**].

[MORE – multiplication table, etc..]

1.2. Permutations, cycles and fixed sets. The classical *derangement problem* was posed in 1708 by Pierre Raymond de Montmort. The problem asks how many permutations in $\mathcal{S}_n$ have no fixed points, that is no 1-cycles. Five years later, he found an exact formula, which is approximately $\frac{1}{e}n!$ for large n. In the early 1800s, Cauchy introduced the cycle notation and showed that permutations factor uniquely into a product of cycles. He also developed an exact formula for the number of permutations with a given *cycle type*; that is, the number of cycles of each length. If $\sigma \in \mathcal{S}_n$ has C_j cycles of length j for each j, with $\sum_j C_j = n$, then the number of such permutations equals

$$n! \prod_{j \leqslant n} \left(\frac{1}{j}\right)^{C_j} \frac{1}{C_j!}.$$

This formula suggests that, for random $\sigma \in \mathcal{S}_n$, the quantities $C_1(\sigma), C_2(\sigma), \dots$ behave like independent Poisson random variables, where $C_j(\sigma)$ has distribution $\mathrm{Pois}(1/j)$. This is not precisely true, because of the condition that $\sum_j C_j = n$. Goncharov was the first to make such statements rigorous, and in 1944 proved (among other things) the following:

Theorem (Goncharov, 1944 [Gon44]). We have

- For any fixed j and m, $\frac{1}{n!}\#\{\sigma \in \mathcal{S}_n : C_j(\sigma) = m\}\} \to e^{-1/j}\frac{(1/j)^m}{m!} \quad (n \to \infty)$;
- For any real z, $\frac{1}{n!}\#\left\{\sigma \in \mathcal{S}_n : \frac{C(\sigma) - \log n}{\sqrt{\log n}} \leqslant z\right\} \to \Phi(z) := \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z} e^{-\frac{1}{2}t^2}\,dt \qquad (n \to \infty)$.

The (unsigned) Stirling number of the first kind, $S_1(n, m)$, counts the number of permutations $\sigma \in \mathcal{S}_n$ with exactly m total cycles; that is, $C(\sigma) = m$. Goncharov used careful asymptotic analysis of Stirling numbers to obtain the second part of the theorem above. The first part was deduced from an exact formula which he proved for $\#\{\sigma \in \mathcal{S}_n : C_j(\sigma) = m\}$ (see Exercise 2.1 below). More recently, the Poisson model has been established in great uniformity: Namely,

$$(C_1(\sigma), C_2(\sigma), \dots, C_k(\sigma)) \approx (Z_1, Z_2, \dots, Z_k) \tag{1.1}$$

(meaning the two vectors have distributions which are very close), where $Z_1, \dots, Z_k$ are independent and $Z_j \stackrel{d}{=} \mathrm{Pois}(1/j)$, provided that $k = o(n)$ as $n \to \infty$.

A *fixed set* of a permutation σ is a subset $I \subset [n]$ which is itself permuted by σ. A fixed set is a product of some subset of the cycles in σ (we include both the empty set and the whole set $[n]$ as fixed sets). These play the same role for permutations as divisors do for integers. The existence of fixed sets of a particular size has applications to various questions in combinatorial group theory, such as generation of $\mathcal{S}_n$ by random permutations and the distribution of transitive subgroups of $\mathcal{S}_n$.

2. Background material

2.1. Basic summation estimates.

PROPOSITION 1.1 (HARMONIC SUMS). *The harmonic sums H_n satisfy*
(i) $\log n \leqslant H_n \leqslant 1 + \log n$*;*
(ii) $H_n = \log n + \gamma + O(1/n)$*, where* $\gamma = 0.57721566\dots$ *is Euler's constant.*

PROPOSITION 1.2 (STIRLING'S FORMULA). *We have $n! \geqslant (n/\mathrm{e})^n$ and the asymptotic (Stirling's formula)*

$$n! = \sqrt{2\sigma n}(n/\mathrm{e})^n(1 + O(1/n)).$$

PROPOSITION 1.3 (EULER'S SUMMATION). *Let $f \in C^1(y,x)$. Then*

$$\sum_{y<n\leqslant x} f(n) = \int_y^x f(t)\,dt + \int_y^x \{t\}f'(t)\,dt + \{y\}f(y) - \{x\}f(x),$$

where $\{t\} = t - \lfloor t \rfloor$ is the fractional part of t.

PROPOSITION 1.4 (ABEL SUMMATION). *Let a_n be any sequence of complex numbers with counting function $A(t) = \sum_{1\leqslant n\leqslant t} a_n$. Let $0 < y \leqslant x$ and suppose $f \in C^1(y,x]$. Then*

$$\sum_{y<n\leqslant x} a_n f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)\,dt.$$

2.2. Arithmetic functions. A function $f : \mathbb{N} \to \mathbb{C}$ is called an *arithmetic function*.

An arithmetic function f is *multiplicative* if it is not identically zero, and if $f(mn) = f(m)f(n)$ whenever $(m,n) = 1$. Equivalently, if n has prime factorization $n = p_1^{e_1}\cdots p_k^{e_k}$, then

$$f(n) = f(p_1^{e_1})\cdots f(p_k^{e_k}).$$

In particular (the empty product) $f(1) = 1$.

Important examples:

- (powers) $f(n) = n^c$ for any fixed $c \in \mathbb{C}$. In particular, $1(n) = 1$ for all n (the identically 1 function).
- (one) $e(1) = 1$, $e(n) = 0$ for $n > 1$. This function behaves as a kind of identity function (see below).
- (Divisor function) $f(n) = \tau(n)$, the number of positive divisors of n; $\tau(p_1^{e_1}\cdots p_k^{e_k}) = (e_1+1)\cdots(e_k+1)$.
- (Euler's function) $\phi(n) = \#\{1 \leqslant m \leqslant n : (m,n) = 1\}$; formula $\phi(n) = \prod_{p^a\|n} p^{a-1}(p-1)$.
- (Möbius function) $\mu(n) = (-1)^{\omega(n)}$ for squarefree n; $\mu(n) = 0$ otherwise; in particular, $\mu^2(n)$ is the indicator function for squarefree integers.

Clearly, the product and quotient of multiplicative functions is also multiplicative, as is any fixed power of a multiplicative function.

Ring structure of arithmetic functions. The set of arithmetic functions forms a *commutative ring* with the following operations $(+,\star)$, where

$$f \star g(n) = \sum_{d|n} f(d)g(n/d)$$

(the sum over positive divisors $d|n$). Note that $f \star e = e \star f = f$, that is, e is the identity w.r.t. the $\star$ operation.

Möbius inversion. One of the most important properties of μ is that for any positive integer n,

$$\sum_{d|n} \mu(d) = e(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases} \tag{1.2}$$

A consequence is the **Möbius inversion formula:**

$$f(n) = \sum_{d|n} g(d)\ \forall n \implies g(n) = \sum_{d|n} f(d)\mu(n/d)\ \forall n. \tag{1.3}$$

A sum over divisors of n of a **multiplicative function** f may be written as a product:

$$\sum_{d|n} f(d) = \prod_{p^a\|n} \left(1 + f(p) + f(p^2) + \cdots + f(p^a)\right), \tag{1.4}$$

and an "infinite version"

$$\sum_{d:p|d \implies p\in T} f(d) = \prod_{p\in T} \left(1 + f(p) + f(p^2) + \cdots\right), \tag{1.5}$$

provided each infinite sum converges, and the product also converges. An important special case is $f(n) = 1/n$, which yields the formula

$$\sum_{d:p|d \implies p\in T} \frac{1}{d} = \prod_{p\in T} \left(1 - \frac{1}{p}\right)^{-1}. \tag{1.6}$$

An arithmetic function f is **additive** if $f(ab) = f(a) + f(b)$ whenever $(a, b) = 1$. Examples include

(1) $f(n) = \omega(n)$, the number of distinct prime factors of n;
(2) $f(n) = \Omega(n)$, the number of prime power divisors of n;
(3) $f(n) = \log n$;
(4) $f(n) = \log g(n)$, where $g(n)$ is a positive, multiplicative function.

The von Mangoldt function $\Lambda(n)$, defined by

$$\Lambda(n) = \begin{cases} \log p & n = p^a, p \text{ prime}, \\ 0 & \text{otherwise.} \end{cases}$$

The fundamental theorem of arithmetic (unique factorization of integers into primes) may be expressed as

$$\sum_{d|n} \Lambda(d) = \log n. \tag{1.7}$$

2.3. Prime number estimates. Throughout, p denotes a prime number.

PROPOSITION 1.5 (MERTENS' ESTIMATES). *(i) We have*

$$\sum_{p\leqslant x} \frac{1}{p} = \log\log x + c_1 + O\left(\frac{1}{\log x}\right) \tag{Mertens.sum}$$

for some constant c_1.

(ii) We have

$$\prod_{p\leqslant x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x}\left(1 + O\left(\frac{1}{\log x}\right)\right). \tag{Mertens.product}$$

PROPOSITION 1.6 (CHEBYSHEV'S THEOREM). *(i) We have*

$$x \ll \sum_{n\leqslant x} \Lambda(n) \ll x \qquad (x \geqslant 2).$$

Equivalently, the number of primes which are $\leqslant x$ *is* $\asymp x/\log x$*, for* $x \geqslant 2$.

(ii) (Bertrand's Postulate) For every $x > 1$*, there is a prime between* x *and* $2x$.

PROPOSITION 1.7 (PRIME NUMBER THEOREM). *The number of primes less than* x *equals*

$$\int_2^x \frac{dt}{\log t} + O\left(xe^{-c_2\sqrt{\log x}}\right)$$

for some constant $c_2 > 0$.

2.4. Inclusion-Exclusion. We need a simple version of the inclusion-exclusion principle, with truncation.

LEMMA 1.8 (INCLUSION-EXCLUSION). *Let* a *be a non-negative integer. Then, for any* $k \in \mathbb{N}$,

$$\mathbf{1}(a = 0) = \sum_{r=0}^{\infty} (-1)^r \binom{a}{r} = \sum_{r=0}^{k} \binom{a}{r} + (-1)^{k+1} \binom{a-1}{k}.$$

PROOF. The first equality is trivial from the binomial theorem. For the second, we have

$$\sum_{r=k+1}^{\infty} (-1)^r \binom{a}{r} = \sum_{r=k+1}^{\infty} (-1)^r \left[\binom{a-1}{r-1} + \binom{a-1}{r}\right] = (-1)^{k+1}\binom{a-1}{k}. \qquad \square$$

Often, we need to count a reciprocal weighted sum over integers with a given number of prime factors from a given set.

PROPOSITION 1.9 (SUMS OF k FACTORS). *Let T be a finite set of positive integers, and $k \in \mathbb{N}$. Then*

$$\frac{1}{k!}\Big(H(T)^k - \binom{k}{2} H(T)^{k-2} \sum_{n\in T} \frac{1}{n^2}\Big) \leqslant \sum_{\substack{n_1,\dots,n_k\in T\\ n_1<\dots<n_k}} \frac{1}{n_1\cdots n_k} \leqslant \frac{H(T)^k}{k!}.$$

PROOF. Evidently,

$$H(T)^k = \sum_{n_1,\dots,n_k\in T} \frac{1}{n_1\cdots n_k}.$$

The summands on the right corresponding to distinct, unordered k-tuples $(n_1,\dots,n_k)$ equals

$$k! \sum_{\substack{n_1,\dots,n_k\in T\\ n_1<\dots<n_k}} \frac{1}{n_1\cdots n_k},$$

while the summands corresponding to non-distinct k-tuples $(n_1,\dots,n_k)$ have a total sum of at most

$$\binom{k}{2} \sum_{n\in T} \frac{1}{n^2} H(T)^{k-2}.$$ □

2.5. Probability estimates: general. All random variables lie in $\mathbb{R}$, most are non-negative.
Markov's inequality:

$$\mathbb{P}(X \geqslant w) \leqslant \frac{\mu}{w}, \qquad \mu = \mathbb{E}\, X > 0, w > 0, \tag{Markov}$$

Chebyshev's inequality:

$$\mathbb{P}\left(|X-\mu| \geqslant w\sqrt{\mathbb{E}\,|X-\mu|^2}\right) \leqslant \frac{1}{w^2}, \qquad w > 0, \mu = \mathbb{E}\, X, \mathbb{E}\,|X-\mu|^2 > 0. \tag{Chebyshev}$$

Chernoff's inequality (special case of Markov):

$$\mathbb{P}\,(X \geqslant w) \leqslant \frac{\mathbb{E}\, e^{bX}}{e^{bw}}, \qquad (b \geqslant 0). \tag{Chernoff}$$

2.6. Probability estimates: Poisson random variables. The first Proposition lists basic properties of the Poisson distribution, which are readily verified from the definition.

PROPOSITION 1.10. *Suppose $X \stackrel{d}{=} \mathrm{Pois}(\lambda)$. Then*

$$\mathbb{E}\, X = \lambda, \tag{1.8}$$

$$\mathbb{E}\, c^X = e^{(c-1)\lambda} \quad (c > 0), \tag{1.9}$$

$$\mathbb{E}\binom{X}{m} = \frac{\lambda^m}{m!} \quad (m \geqslant 0). \tag{1.10}$$

If $X_j \stackrel{d}{=} \mathrm{Pois}(\lambda_j)$, $1 \leqslant j \leqslant k$, and $X_1,\dots,X_k$ are independent, then

$$X_1 + \cdots + X_k \stackrel{d}{=} \mathrm{Pois}(\lambda_1 + \cdots + \lambda_k). \tag{1.11}$$

We also record very useful tail bounds:

PROPOSITION 1.11 (POISSON TAILS). *Let $X \stackrel{d}{=} \mathrm{Pois}(\lambda)$. Then*

$$\mathbb{P}(X \leqslant \alpha\lambda) \leqslant e^{-Q(\alpha)\lambda} \quad (0 \leqslant \alpha \leqslant 1), \qquad \mathbb{P}(X \geqslant \alpha\lambda) \leqslant e^{-Q(\alpha)\lambda} \quad (\alpha \geqslant 1),$$

where

$$Q(x) = x\log x - x + 1. \tag{1.12}$$

PROOF. First, using Chernoff's inequality (Chernoff) (with $b = \log \alpha$, $0 < \alpha \leqslant 1$) together with (1.9), we have

$$\mathbb{P}(X \leqslant \alpha\lambda) = \mathbb{P}\left(e^{bX} \geqslant e^{b\alpha\lambda}\right) \leqslant \frac{\mathbb{E}\, e^{bX}}{e^{b\alpha\lambda}} = \frac{e^{(e^b-1)\lambda}}{e^{b\alpha\lambda}} = e^{-Q(\alpha)\lambda}.$$

A second application of Chernoff's inequality (Chernoff) (again with $b = \log \alpha$, $\alpha \geqslant 1$) and (1.9) yields

$$\mathbb{P}(X \geqslant \alpha\lambda) = \mathbb{P}\left(e^{bX} \geqslant e^{b\alpha\lambda}\right) \leqslant \frac{\mathbb{E}\, e^{bX}}{e^{b\alpha\lambda}} = \frac{e^{(e^b-1)\lambda}}{e^{b\alpha\lambda}} = e^{-Q(\alpha)\lambda}.$$

□

We record frequently needed bounds on the function $Q(x)$.

PROPOSITION 1.12 (Q BOUNDS). *We have*

$$Q(x) = \int_1^x \log t \, dt \quad (\textit{all } x) = \sum_{k=2}^{\infty} \frac{(-1)^k}{k(k-1)}(x-1)^k \quad (|x-1| < 1), \tag{1.13}$$

and

$$\frac{x^2}{3} \leqslant Q(1+x) \leqslant x^2 \quad (|x| \leqslant 1). \tag{1.14}$$

PROPOSITION 1.13 (BINOMIAL TAILS). *Let X have binomial distribution according to n trials and parameter $p \in [0,1]$; that is, $\mathbb{P}(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$. If $\beta \leqslant p$ then we have*

$$\mathbb{P}(X \leqslant \beta n) \leqslant \exp\left\{-n\left(\beta \log \frac{\beta}{p} + (1-\beta)\log\frac{1-\beta}{1-p}\right)\right\}. \tag{1.15}$$

PROOF. The proof is an application of Chernoff's inequality (optimizing the parameter c). The right side is also an upper bound for $\mathbb{P}(X \geqslant \beta n)$ for $\beta \geqslant p$ by symmetry.‘ □

CHAPTER 2

The sequence of prime factors of an integer and cycles of a permutation, I

Discussion.

1. Cycles and prime factors from intervals: first nibbles

LEMMA 2.1 (CYCLE LENGTH LEMMA). *Let $m_1, \dots, m_n$ be non-negative integers with $m_1 + 2m_2 + \cdots + nm_n \leqslant n$. Then*

$$\mathbb{E} \prod_{j=1}^{n} \binom{C_j(\sigma)}{m_j} = \prod_{j=1}^{n} \frac{1}{m_j! j^{m_j}}.$$

If $m_1 + 2m_2 + \cdots + nm_n > n$, then the left side is zero.

PROOF. The second assertion is obvious, since the only way for the product to be positive is for σ to have more than n cycles. Now assume that $m_1 + 2m_2 + \cdots + nm_n \leqslant n$. The number of ways of choosing from $[n]$ a disjoint collection of m_1 $1-$element sets, m_2 $2-$element sets, ..., m_n $n-$element sets is equal to

$$\binom{n}{\underbrace{1\cdots 1}_{m_1}\underbrace{2\cdots 2}_{m_2}\cdots\underbrace{n\cdots n}_{m_n}\, t} \frac{1}{m_1!\cdots m_n!} = \frac{n!/t!}{\prod_{j=1}^{n}(j!)^{m_j} m_j!},$$

by the multinomial theorem, where $t = n - (m_1 + 2m_2 + \cdots + nm_n)$. The elements of a k-element set may be arranged into a cycle in $(k-1)!$ ways. Thus, the number of ways to arrange the elements of these sets into cycles is

$$\prod_{j=1}^{n} (j-1)!^{m_j}.$$

Finally, the t elements not used in any of these cycles may be permuted in $t!$ ways, and the claim follows. □

A special case is the well-known formula of Cauchy for the number of permutations with a given cycle type.

LEMMA 2.2 (CAUCHY'S FORMULA). *Let $\mathbf{C}_n(\sigma) = (C_1(\sigma), \dots, C_n(\sigma))$. If $m_1 + 2m_2 + \cdots + nm_n = n$, then*

$$\mathbb{P}\big(\mathbf{C}_n(\sigma) = (m_1, m_2, \cdots, m_n)\big) = \prod_{j=1}^{n} \frac{1}{m_j! j^{m_j}}.$$

PROOF. Apply Lemma 2.1, noting that $\binom{C_j(\sigma)}{m_j} \neq 0$ for all j if and only if $C_j(\sigma) = m_j$ for every j. □

COROLLARY 2.3 (DERANGEMENTS). *We have the exact formula for derangements*

$$\#\{\sigma \in \mathcal{S}_n : C_1(\sigma) = 0\} = n! \sum_{j=0}^{n} \frac{(-1)^j}{j!}.$$

PROOF. Apply Inclusion-Exclusion (Lemma 1.8) with $u = C_1(\sigma)$, followed by the Cycle Length Lemma (Lemma 2.1). We get

$$\begin{aligned}\#\{\sigma \in \mathcal{S}_n : C_1(\sigma) = 0\} &= \sum_{\sigma\in\mathcal{S}_n}\sum_{j=0}^{\infty}(-1)^j\binom{C_1(\sigma)}{j}\\ &= n!\sum_{j=0}^{n}(-1)^j\mathbb{E}\binom{C_1(\sigma)}{j} = n!\sum_{j=0}^{n}\frac{(-1)^j}{j!}. \quad \square\end{aligned}$$

COROLLARY 2.4 (EXPECTED NUMBER OF CYCLES). *We have* $\mathbb{E}\,C(\sigma) = H_n = \log n + \gamma + O(1/n)$.

PROOF. By Lemma 2.1, $\mathbb{E}\,C_j(\sigma) = 1/j$ for every j, and the result follows by linearity of expectation and Proposition 1.1. $\square$

The situation with primes is more complicated (see the lower bound in Proposition 1.9), but we so have a clean upper bound of the same type.

LEMMA 2.5 (PRIME FACTORS LEMMA). *Let* $T_1, \dots, T_k$ *be a nonempty, disjoint subset of the primes in* $[2, x]$, *and let* $m_1, \dots, m_k \geqslant 0$. *Then*

$$\frac{1}{x}\sum_{n\leqslant x}\prod_{j=1}^{k}\binom{\omega(n;T_j)}{m_j} \leqslant \prod_{j=1}^{k}\frac{H(T_j)^{m_j}}{m_j!}.$$

PROOF. The sum in question equals

$$\sum_{\substack{p_{j,1},\dots,p_{j,m_j}\in T_j\\(1\leqslant j\leqslant k)}}\#\{n\leqslant x : p_{1,1}\cdots p_{k,m_k}|n\} = \sum_{\substack{p_{j,1},\dots,p_{j,m_j}\in T_j\\(1\leqslant j\leqslant k)}}\left\lfloor\frac{x}{p_{1,1}\cdots p_{k,m_k}}\right\rfloor.$$

Using $\lfloor y\rfloor \leqslant y$, the desired bound follows immediately from the upper bound in Proposition 1.9. $\square$

Observe that the quantity on the right sides in the Cycle Length Lemma (Lemma 2.1) matches exactly the binomial moments of vectors of independent Poisson random variables with parameters $(1, 1/2, \dots, 1/n)$. Likewise, the quantity on the right sides in Lemma 2.5 (Prime factors in sets, I) matches exactly the binomial moments of vectors of independent Poisson random variables with parameters $(H(T_j) : 1 \leqslant j \leqslant k)$.

LEMMA 2.6. *We have* $\dfrac{1}{x}\displaystyle\sum_{n\leqslant x}\omega(n) = \log\log x + O(1)$.

PROOF. The sum is $\sum_{p\leqslant x}\lfloor x/p\rfloor = x\sum_{p\leqslant x}1/p + O(x)$. Now apply Mertens' sum estimate (Mertens.sum). $\square$

A corollary is a theorem of Turán from 1932:

COROLLARY 2.7 (TURÁN'S VARIANCE THEOREM). *We have*

$$\frac{1}{x}\sum_{n\leqslant x}\big(\omega(n) - \log_2 x\big)^2 \ll \log_2 x.$$

PROOF. Using The Prime Factors Lemma (with $k = 1$, T_1 the set of all primes in $[2, x]$, $m_1 = 2$) and Lemma 2.6, we directly compute

$$\begin{aligned}\frac{1}{x}\sum_{n\leqslant x}\big(\omega(n) - \log_2 x\big)^2 &= \frac{1}{x}\sum_{n\leqslant x}\left(2\binom{\omega(n)}{2} + \omega(n)(1 - 2\log_2 x)\right) + (\log_2 x)^2 + O\left(\frac{1}{x}\right)\\ &\leqslant (\log_2 x + O(1))^2 + (\log_2 x + O(1))(1 - 2\log_2 x) + (\log_2 x)^2\\ &= O(\log_2 x). \qquad \square\end{aligned}$$

We can interpret Corollary 2.7 probabilistically. If $n \leqslant x$ is chosen at random, then Corollary 2.7 gives an upper bound on the variance of $\omega(n)$, telling us that $\omega(n)$ is concentrated near $\log_2 x$. In fact, it follows immediately (see Chebyshev's inequality Chebyshev) that uniformly for $\xi \geqslant 1$,

$$\#\left\{n \leqslant x : |\omega(n) - \log_2 x| \geqslant \xi\sqrt{\log_2 x}\right\} \ll \frac{x}{\xi^2}.$$

An immediate corollary is the following famous result:

THEOREM 2.8 (HARDY-RAMANUJAN, 1917). *The function $\omega(n)$ has normal order $\log\log n$. More specifically, given any function $\psi(n)$ so that $(\log\log n)^{-1/3} < \psi(n) = o(1)$ as $n \to \infty$, we have*

$$|\omega(n) - \log\log n| < \psi(n)\log\log n$$

for almost all integers n (the exceptional set has counting function $o(x)$ as $x \to \infty$).

2. Cycles and prime factors from intervals: general upper bounds

THEOREM 2.9 (CYCLES IN SETS THEOREM). *Let $T_1, \dots, T_r$ be arbitray disjoint, nonempty subsets of $[n]$ and $k_1, \dots, k_r \geqslant 0$. Then*

$$\mathbb{P}\left(C_{T_1}(\sigma) = k_1, \dots, C_{T_r}(\sigma) = k_r\right) \leqslant \mathrm{e}\prod_{j=1}^{r}\left(\frac{H(T_j)^{k_j}}{k_j!}\mathrm{e}^{-H(T_j)}\right)\cdot\left(1 + \frac{k_1}{H(T_1)} + \cdots + \frac{k_r}{H(T_r)}\right).$$

PROOF. Evidently

$$n\#\{\sigma \in \mathcal{S}_n : C_{T_1}(\sigma) = k_1, \dots, C_{T_r}(\sigma) = k_r\} = \sum_{\substack{\sigma\in\mathcal{S}_n \\ C_{T_j}(\sigma)=k_j\ (1\leqslant j\leqslant r)}} \sum_{\substack{\alpha|\sigma \\ \alpha \text{ a cycle}}} |\alpha|.$$

Write $\sigma = \alpha\beta$ and let $h = |a|$. Either $h \in T_j$ for some unique j, or $h \notin T_1 \cup \cdots \cup T_r$. Thus, for some t, $0 \leqslant t \leqslant r$, we have

$$(C_{T_1}(\beta), \dots, C_{T_r}(\beta)) = (m_{t,1}, \dots, m_{t,r}),$$

where

$$m_{t,i} = \begin{cases} k_i - 1 & \text{if } i = t \geqslant 1 \\ k_i & \text{otherwise.} \end{cases} \tag{2.1}$$

It is permissible to think of $\beta \in \mathcal{S}_{n-h}$ and thus

$$\begin{aligned} n\#\{\sigma \in \mathcal{S}_n : C_{T_1}(\sigma) = k_1, \dots, C_{T_r}(\sigma) = k_r\} &\leqslant \sum_{t=0}^{r}\sum_{h=1}^{n} \sum_{\substack{\alpha\in\mathcal{S}_n, |\alpha|=h \\ \alpha \text{ a cycle}}} h \sum_{\substack{\beta\in\mathcal{S}_{n-h} \\ C_{T_i}(\beta)=m_{t,i}\ (1\leqslant i\leqslant r)}} 1 \\ &= \sum_{t=0}^{r}\sum_{h=1}^{n} \frac{n!}{(n-h)!} \sum_{\substack{\beta\in\mathcal{S}_{n-h} \\ C_{T_i}(\beta)=m_{t,i}\ (1\leqslant i\leqslant r)}} 1. \end{aligned}$$

Note that if $k_i = 0$ for some i, then $m_{i,i} = -1$ and the corresponding summand above is ommitted. Now subdivide the sum according the cycle type $(b_1, \dots, b_n)$ of the permutation β, using Cauchy's formula (Lemma 2.2) to count such permutations for each type. It follows that

$$\begin{aligned} n\#\{\sigma \in \mathcal{S}_n : C_{T_j}(\sigma) = k_j\ (1 \leqslant j \leqslant r)\} &\leqslant n!\sum_{t=0}^{r}\sum_{h=1}^{n} \sum_{\substack{b_1,\dots,b_n\geqslant 0 \\ b_1+2b_2+\cdots+nb_n=n-h \\ \sum_{i\in T_j} b_i = m_{t,j}\ (1\leqslant j\leqslant r)}} \frac{1}{\prod_i b_i! i^{b_i}} \\ &\leqslant n!\sum_{t=0}^{r} \sum_{\substack{b_1,\dots,b_n\geqslant 0 \\ \sum_{i\in T_j} b_i = m_{t,j}\ (1\leqslant j\leqslant r)}} \frac{1}{\prod_i b_i! i^{b_i}} := Y, \end{aligned}$$

say. Let $T = T_1 \cup \cdots \cup T_r$ and separately consider the summation over $i \in T$ and $i \notin T$. By the multinomial theorem,

$$\begin{aligned} Y &= n! \sum_{t=0}^{r} \sum_{\substack{b_i \geqslant 0 \ (i \in T) \\ \sum_{i \in T_j} b_i = m_{t,j} \ (1 \leqslant j \leqslant r)}} \frac{1}{\prod_{i \in T} b_i! i^{b_i}} \sum_{b_i \geqslant 0 \ (i \notin T)} \frac{1}{\prod_{i \notin T} b_i! i^{b_i}} \\ &= n! \sum_{t=0}^{r} \prod_{j=1}^{r} \frac{H(T_j)^{m_{t,j}}}{m_{t,j}!} \prod_{i \notin T} e^{1/i} \\ &= n! \prod_{j=1}^{r} \frac{H(T_j)^{k_j}}{k_j!} \left(1 + \sum_{j=1}^{r} \frac{k_j}{H(T_j)}\right) \prod_{i \notin T} e^{1/i}. \end{aligned}$$

The claimed bound now follows using the inequality (from Proposition 1.1)

$$\sum_{i \notin T} \frac{1}{i} = H_n - \sum_{j=1}^{r} H(T_j) \leqslant \log n + 1 - \sum_{j=1}^{r} H(T_j). \qquad \square$$

REMARK 2.10. Whenever r is bounded, and $k_j = O(H(T_j))$ for each j, the right side is

$$\ll \mathbb{P}(\mathrm{Pois}(H(T_1)) = k_1, \ldots, \mathrm{Pois}(H(T_r)) = k_r).$$

Thus, Theorem 2.9 gives an upper bound for counts of cycle lengths in sets $T_1, \ldots, T_r$ of the expected order (up to a constant factor) according to the Poisson model. This is a useful tool for showing that the actual cycle counts cannot vary too much from the expected means.

In the special case $r = 1$, Theorem 2.9 implies that for any $T \subset [n]$ and $k \geqslant 0$,

$$\mathbb{P}\left(C_T(\sigma) = k\right) \leqslant \mathrm{e}^{1-H(T)} \left(\frac{H(T)^{k-1}}{(k-1)!} + \frac{H(T)^k}{k!}\right). \tag{2.2}$$

Specializing to the case of cycle lengths in a single interval $[m]$, we obtain the following very useful corollary:

COROLLARY 2.11 (CYCLES IN INTERVALS). *Uniformly for $1 \leqslant m \leqslant n$ and $0 \leqslant \lambda \leqslant 1$, we have*

$$\mathbb{P}\left(C_{[m]}(\sigma) \leqslant \lambda \log m\right) \ll m^{-Q(\lambda)}.$$

Let $\lambda_0 > 1$. Uniformly for $1 \leqslant m \leqslant n$ and $1 \leqslant \lambda \leqslant \lambda_0$, we have

$$\mathbb{P}\left(C_{[m]}(\sigma) \geqslant \lambda \log m\right) \ll m^{-Q(\lambda)}.$$

In particular, uniformly for $1 \leqslant m \leqslant n$ and $0 \leqslant \psi \leqslant \sqrt{\log m}$, we have

$$\mathbb{P}\left(|C_{[m]}(\sigma) - \lambda \log m| > \psi \sqrt{\log m}\right) \ll e^{-\frac{1}{3}\psi^2}.$$

PROOF. Let $T = T_1 = [m]$, and recall from (1.1) that $H_m = \log m + O(1)$. It follows for $k \leqslant \lambda \log m$ that $H_m^k \ll (\log m)^k$. Applying Theorem 2.9 (see (2.2)), together with the estimate for Poisson tails (1.11), we get that

$$\begin{aligned} \mathbb{P}\left(C_{[m]}(\sigma) \leqslant \lambda \log m\right) &\ll e^{-H_m} \sum_{k \leqslant \lambda \log m} \frac{H_m^k}{k!} \\ &\ll \frac{1}{m} \sum_{k \leqslant \lambda \log m} \frac{(\log m)^k}{k!} \leqslant m^{-Q(\lambda)}. \end{aligned}$$

The proof of the second bound is similar. Again by Theorem 2.9, together with (1.11) and Stirling's formula 1.2, we get that, we get

$$\begin{aligned}\mathbb{P}\left(C_{[m]}(\sigma) \geqslant \lambda \log m\right) &\ll e^{-H_m} \sum_{k \geqslant \lambda \log m - 1} \frac{H_m^k}{k!} \\ &\ll \frac{1}{m}\left(\sum_{\lambda \log m \leqslant k \leqslant 2\lambda_0 \log m} \frac{(\log m)^k}{k!} + \sum_{k > 2\lambda_0 \log m} \frac{(\log m + 1)^k}{k!} \right) \\ &\ll m^{-Q(\lambda)} + \frac{(\log m + O(1))^{\lceil 2\lambda_0 \log m \rceil}}{\lceil 2\lambda_0 \log m \rceil !} \ll m^{-Q(\lambda)} + m^{-Q(2\lambda_0)} \ll m^{-Q(\lambda)}.\end{aligned}$$

The final estimate follows from the bound (1.14) for $Q(u)$. □

In particular, taking $m = n$, we see that $C(\sigma)$ usually does not vary more that $\sqrt{\log n}$ from its mean H_n.

The same proof yields a much more general result:

COROLLARY 2.12. *Let $T \subset [n]$. Uniformly for $0 < \theta \leqslant \sqrt{H(T)}$, we have*

$$\mathbb{P}\left(|C_T(\sigma) - H(T)| > \theta \sqrt{H(T)} \right) \ll e^{-\frac{1}{3}\theta^2}.$$

This is not very useful when $H(T) < 1$, however. In this case, we expect that $C_T(\sigma)$ will rarely be much more than 1. Theorem 2.9 implies a right-tail bound of

$$\mathbb{P}\left(C_T(\sigma) = k\right) \ll \frac{H(T)^{k-1}}{(k-1)!},$$

whereas the Poisson model predicts $H(T)^k/k!$; but see Homework Exercise 2.2 below.

THEOREM 2.13 (PRIME FACTORS IN SETS). *Let $T_1, \dots, T_r$ be arbitrary disjoint, nonempty subsets of the primes $\leqslant x$. For any $k_1, \dots, k_r \geqslant 0$ we have*

$$\#\{n \leqslant x : \omega(n; T_j) = k_j \ (1 \leqslant j \leqslant r)\} \ll x \prod_{j=1}^{r} \left(\frac{H(T_j)^{k_j}}{k_j!} e^{-H(T_j)} \right) \left(1 + \frac{k_1}{H(T_1)} + \cdots + \frac{k_r}{H(T_r)} \right).$$

PROOF. Let

$$L_t(x) = \sum_{\substack{h \leqslant x \\ \omega(h;T_j) = m_{t,j} \ (1 \leqslant j \leqslant r)}} \frac{1}{h},$$

where $m_{t,j}$ are given by (2.1) as in the proof of Theorem 2.9.

Using the basic relation (1.7), we have

$$(\log x)\#\{n \leqslant x : \omega(n; T_j) = k_j \ (1 \leqslant j \leqslant r)\} = \sum_{\substack{n \leqslant x \\ \omega(n;T_j) = k_j \ (1 \leqslant j \leqslant r)}} \log(x/n) + \sum_{\substack{n \leqslant x \\ \omega(n;T_j) = k_j \ (1 \leqslant j \leqslant r)}} \sum_{d \mid n} \Lambda(d).$$

Using the crude bound $\log(x/n) \leqslant x/n$, the first sum is $\leqslant xL_0(x)$. In the double sum, let $n = dh$, note that $d = p^a$ is a prime power, and observe that $\omega(h, T_j) = k_j - 1$ if $p \in T_j$ and $\omega(h, T_j) = k_j$ otherwise. That is, h is counted by $L_t(x)$ for some t, $0 \leqslant t \leqslant r$. Hence

$$(\log x)\#\{n \leqslant x : \omega(n; T_j) = k_j \ (1 \leqslant j \leqslant r)\} \leqslant xL_0(x) + \sum_{t=0}^{r} \sum_{\substack{h \leqslant x \\ \omega(h;T_j) = m_{t,j} \ (1 \leqslant j \leqslant r)}} \sum_{d \leqslant x/h} \Lambda(d).$$

Using Chebyshev's Estimate for primes (Proposition (1.6)), the innermost sum over d is $O(x/h)$ and thus the right side above is $O(x(L_0(x) + \cdots + L_r(x)))$; if $k_j = 0$, then $m_{j,j} = -1$ and the corresponding term is omitted. To bound the sum $L_t(x)$, write the denominator $h = h_1 \cdots h_r h'$, where, for $1 \leqslant j \leqslant r$, h_j is composed only of primes from T_j,

$\omega(h_j;T_j)=m_{t,j}$, and h' is composed of primes in $[2,x]\setminus(T_1\cup\cdots\cup T_r)$. Using the Sums of $k-$ factors Proposition 1.9, (1.6) and Mertens' estimate (Mertens.product), we obtain

$$L_t(x)\leqslant\prod_{j=1}^r\frac{H(T_j)^{m_{t,j}}}{m_{t,j}!}\prod_{\substack{p\leqslant x\\ p\notin T_1\cup\cdots\cup T_r}}\left(1-\frac1p\right)^{-1}\ll(\log x)\prod_{j=1}^r\frac{H(T_j)^{m_{t,j}}}{m_{t,j}!}\prod_{p\in T_1\cup\cdots\cup T_r}\left(1-\frac1p\right).$$

We conclude that

$$\#\{n\leqslant x:\omega(n;T_j)=k_j\ (1\leqslant j\leqslant r)\}\ll x\prod_{j=1}^r\frac{H(T_j)^{k_j}}{k_j!}\left(1+\sum_{j=1}^r\frac{k_j}{H(T_j)}\right)\prod_{p\in T_1\cup\cdots\cup T_r}\left(1-\frac1p\right).$$

Finally, using the elementary inequality $1+y\leqslant e^y$, we see that the product over $p\in S$ is $\leqslant e^{-H(T_1)-\cdots-H(T_r)}$. □

Remark. Theorem 2.13 is similar to [**Tud96**, Theorem 2].

In the special case of a single set of primes, we have

$$\#\{n\leqslant x:\omega(n;T)=k\}\ll xe^{-H(T)}\left(\frac{H(T)^{k-1}}{(k-1)!}+\frac{H(T)^k}{k!}\right),\tag{2.3}$$

similar to (2.2).

Taking as a single set the primes in an interval, we obtain the following very useful corollary.

COROLLARY 2.14 (PRIME FACTORS IN INTERVALS). *Uniformly for $3\leqslant t\leqslant x$ and $0\leqslant\lambda\leqslant1$, we have*

$$\#\{n\leqslant x:\omega(n,t)\leqslant\lambda\log\log t\}\ll x(\log t)^{-Q(\lambda)}.$$

Let $\lambda_0>1$. Uniformly for $3\leqslant t\leqslant x$ and $1\leqslant\lambda\leqslant\lambda_0$, we have

$$\#\{n\leqslant x:\omega(n,t)\geqslant\lambda\log\log t\}\ll_{\lambda_0}x(\log t)^{-Q(\lambda)}.$$

In particular, uniformly for $3\leqslant t\leqslant x$ and $0\leqslant\psi\leqslant\sqrt{\log\log t}$, we have

$$\#\{n\leqslant x:|\omega(n,t)-\log\log t|>\psi\sqrt{\log\log t}\}\ll xe^{-\frac13\psi^2}.$$

PROOF. The proof is identical to the proof of Corollary 2.11, using $T=T_1$ as the set of primes in $[2,t]$, $H(T)=\log\log t+O(1)$ from Mertens' bound (Mertens.sum), and Theorem 2.13. □

Taking as a special case $t=n$, we recover a strong form of the Hardy-Ramanujan Theorem.

3. The sequence of cycles and prime factors from intervals

In this section, we take a first look at the *random sequence* $C_{[m]}(\sigma)$ $(1\leqslant m\leqslant n)$ for $\sigma\in\mathcal{S}_n$, and *random function* $\omega(n,t)$ $(1\leqslant t\leqslant x)$ for integers $n\leqslant x$. As long as m and t are not too small, it is relatively easy to deduce from Corollaries 2.11 and 2.14 that $C_{[m]}(\sigma)$ is **uniformly** close to $\log m$ for most $\sigma\in\mathcal{S}_n$ and $\omega(n,t)$ is **uniformly** close to $\log_2 t$ for most $n\leqslant x$. Here we recall the iterated logarithm notation

$$\log_2 x=\log\log x,\quad \log_3 x=\log\log\log x,\quad etc.$$

THEOREM 2.15 (NORNAMAL SEQUENCE $\omega(n,t)$). *Let $3\leqslant\xi\leqslant x$. For all but $O(x/(\log\log\xi)^{1/3})$ integers $n\leqslant x$, we have*

$$|\omega(n,t)-\log_2 t|<2\sqrt{\log_2 t\log_3 t}\qquad(\xi\leqslant t\leqslant x).$$

THEOREM 2.16 (NORMAL SEQUENCE $C_{[m]}(\sigma)$). *Let $2\leqslant\xi\leqslant n$. With probability $1-O(1/(\log\xi)^{1/3})$, we have*

$$|C_{[m]}-\log m|<2\sqrt{\log m\log_2 m}\quad(\xi\leqslant m\leqslant n).$$

REMARK 2.17. When t is bounded, $\omega(n,t)$ has a discrete distribution and we cannot say anything about almost all n; in fact it takes every possible value with positive probability; e.g. $\omega(n,3)$ takes the values $0,1,2$ with probabilities (as $x\to\infty$) $\frac13$, $\frac12$, $\frac16$, respectively. The same is true for $C_{[m]}$ when m is bounded; see Exercise 2.1.

PROOF. The proof of Theorems 2.15 and 2.16 are nearly identical, the latter being simpler due to the discrete nature of the sequence of values of m in question. Thus, we show full details only for Theorem 2.15. Let

$$k_1 = \lfloor \log_2 \xi \rfloor + 1, \qquad k_2 = \lfloor \log_2 x \rfloor,$$

and for $k_1 \leqslant k \leqslant k_2$, let $t_k = e^{e^k}$. Put $t_{k_1-1} = \xi$ and $t_{k_2+1} = x$. For each k, $k_1 - 1 \leqslant k \leqslant k_2 + 1$, let $N_k(x)$ be the number of $n \leqslant x$ with

$$|\omega(n, t_k) - \log_2 t_k| \geqslant 2\sqrt{(k-1)\log(k-1)} - 1. \tag{2.4}$$

As $\log_2 t_k = k + O(1)$ for all t_k (including the endpoints),

$$2\sqrt{(k-1)\log(k-1)} - 2 = \psi\sqrt{\log_2 t_k}, \quad \psi = 2\sqrt{\log k} + O(1/\sqrt{k}).$$

Hence, by the third part of the Prime Factors in Intervals Corollary (Cor. 2.14),

$$N_k(x) \ll x e^{-\frac{1}{3}\psi^2} \ll \frac{x}{k^{4/3}}.$$

Summing over k, we see that $O(x/(\log_2 \xi)^{1/3})$ integers satisfy (2.4) for some k. Now let $n \leqslant x$ be an integer such that (2.4) fails for every k, $k_1 - 1 \leqslant k \leqslant k_2 + 1$. Let $\xi \leqslant t \leqslant x$ and suppose that $t_k < t \leqslant t_{k+1}$. Evidently,

$$\omega(n, t_k) \leqslant \omega(n, t) \leqslant \omega(n, t_{k+1})$$

and, by the failure of (2.4) at every k,

$$\omega(n, t) \geqslant \log_2 t_k - 2\sqrt{(k-1)\log(k-1)} + 1 \geqslant \log_2 t - 2\sqrt{\log_2 t \log_3 t}$$

and

$$\omega(n, t) \leqslant \log_2 t_{k+1} + 2\sqrt{k \log k} - 1 \leqslant \log_2 t + 2\sqrt{\log_2 t \log_3 t}. \qquad \square$$

Theorems 2.15 and 2.16 also tell us about the normal behavior of $p_j(n)$, the j-th smallest (distinct) prime factor of n, and $D_j(\sigma)$, the length of the j-th smallest cycle of σ (note that $D_j(\sigma) = D_{j+1}(\sigma)$ for some j when σ has cycles of the same length). Since a typical integer has about $\log_2 t$ prime factors $\leqslant t$, we expect $p_j(n) \approx e^{e^j}$. Likewise, a typical permutation $\sigma \in \mathcal{S}_n$ has about $\log m$ cycles of length $\leqslant m$, thus we expect that $D_j(n) \approx e^j$.

THEOREM 2.18 (j-TH SMALLEST PRIME FACTOR). *Let $1 \leqslant \theta \leqslant \log_2 x$. For all but $O(x/\theta^{1/3})$ integers $n \leqslant x$, we have*

$$|\log_2 p_j(n) - j| < 3\sqrt{j \log j} \qquad (\theta \leqslant j \leqslant \omega(n)).$$

THEOREM 2.19 (j-TH SMALLEST CYCLE). *Let $1 \leqslant \theta \leqslant \log n$. With probability $1 - O(\theta^{-1/3})$, we have*

$$|\log D_j(\sigma) - j| < 3\sqrt{j \log j} \qquad (\theta \leqslant j \leqslant C(\sigma)).$$

PROOF. The proof of Corollaries 2.18 and 2.19 are nearly identical, and so we provide details only for Corollary 2.19. We may suppose that $\theta \geqslant \theta_0$, where θ_0 is a sufficiently large, absolute constant, for otherwise the conclusion of the Corollary is trivial if the implied constant is large enough. Let $\xi = \lfloor e^{(2/3)\theta} \rfloor$. By Theorem 2.16, with probability $1 - O(1/\theta^{1/3})$, we have

$$|C_{[m]}(\sigma) - \log m| < 2\sqrt{\log m \log_2 m} \qquad (\xi \leqslant m \leqslant n). \tag{2.5}$$

Also, by exercise 2.2 (c), with probability $1 - O(1/\xi)$ all the cycles of σ of length $\geqslant \xi$ have distinct lengths (Note: this issue does not arise in proving Corollary 2.18, since $p_1(n) < p_2(n) < \cdots$ by definition). Now suppose that σ is a permutation satisfying (2.5), and such that the cycles of σ with lengths $\geqslant \xi$ have distinct lengths. We suppose that θ_0 is so large that the right side of the inequality in (2.5) is at most $\frac{1}{2}\log m$ when $m \geqslant \xi$. In particular,

$$C_{[\xi]}(\sigma) < \frac{3}{2}\log \xi \leqslant \theta,$$

that is, $D_\theta(\sigma) > \xi$. Thus, we may apply (2.5) with $m = D_j(\sigma)$ for all $\theta \leqslant j \leqslant C(\sigma)$. As the cycle lengths $\geqslant \xi$ are distinct, we have $j = C_{[m]}(\sigma) > \frac{1}{2}\log D_j(\sigma)$ and hence

$$|j - \log D_j(\sigma)| < 2\sqrt{\log D_j(\sigma) \log_2 D_j(\sigma)} < 2\sqrt{2j \log(2j)} < 3\sqrt{j \log j}$$

provided that θ_0 is large enough (and hence j is large enough). □

Slightly better bounds than those in Theorems 2.15 and 2.16 are attainable, based on ideas stemming from the 'Law of the Iterated Logarithm' from probability theory. Essentially one can replace the factor $\log_3 t$ (or $\log_2 m$) with $\log_4 t$ (or $\log_3 m$), and this is best possible. See e.g., [**HT88**, Theorem 11] for the statement and proof of the theorem for $\omega(n,t)$.

4. Prime factors counted with multiplicity

When prime factors of an integer are counted with multiplicity, that is, counted by means of the function $\Omega(n)$, the normal behavior is the same as for the function $\omega(n)$. That is, for integers $n \leqslant x$, $\Omega(n)$ is tightly concentrated near $\log_2 x$. However, the behavior changes "out in the right tail" region, owing to the influence of large powers of small primes.

Here, we provide a general use utility for analyzing $\Omega(n)$ and other functions. It is often convenient to use $\Omega(n)$, rather than $\omega(n)$, in applications because $\Omega(n)$ is completely additive ($\Omega(ab) = \Omega(a)+\Omega(b)$ for *every* a, b). It is based on the method of parameters, used to capture tails of the distribution of a random variable (cf. Chernoff's inequality), sometimes referred to as "Rankin's trick" in the literature.

LEMMA 2.20 (HALBERSTAM-RICHERT). *Let f be a non-negative, real valued multiplicative function such that for some constants A, B we have*

(a) $\displaystyle\sum_{p\leqslant y} f(p)\log p \leqslant Ay \quad (y \geqslant 0)$;

(b) $\displaystyle\sum_{p}\sum_{k\geqslant 2} \frac{f(p^k)}{p^k}\log p^k = B.$

Then, for all $x > 1$ we have

$$\sum_{n\leqslant x} f(n) \leqslant (A+B+1)\frac{x}{\log x}\sum_{n\leqslant x}\frac{f(n)}{n} \leqslant (A+B+1)e^B\frac{x}{\log x}\exp\Big(\sum_{p\leqslant x}\frac{f(p)}{p}\Big).$$

PROOF. Let

$$M(x) = \sum_{n\leqslant x} f(n), \qquad L(x) = \sum_{n\leqslant x}\frac{f(n)}{n}.$$

We begin in a similar way to the proof of The Prime Factors in Sets Theorem (Thm. 2.13). Since $\log u \leqslant u$,

$$\begin{aligned} M(x)\log x &= \sum_{n\leqslant x} f(n)\log(x/n) + \sum_{n\leqslant x} f(n)\sum_{p^k\| n}\log p^k \qquad (n = p^k h)\\ &\leqslant xL(x) + \sum_{p^k\leqslant x}\big(\log p^k\big) f(p^k)\sum_{h\leqslant x/p^k} f(h)\\ &\leqslant xL(x) + \sum_{\substack{p^k\leqslant x\\ k\geqslant 2}}\big(\log p^k\big) f(p^k)\frac{x}{p^k}\sum_{h\leqslant x/p^k}\frac{f(h)}{h} + \sum_{p\leqslant x} f(p)\log p\sum_{h\leqslant x/p} f(h). \end{aligned}$$

Recalling (b), the first double sum over p^k and h is bounded by $BxL(x)$. Invoking (a),

$$\sum_{p\leqslant x} f(p)\log p\sum_{h\leqslant x/p} f(h) = \sum_{h\leqslant x} f(h)\sum_{p\leqslant x/h} f(p)\log p \leqslant Ax\sum_{h\leqslant x}\frac{f(h)}{h} \leqslant AxL(x).$$

We obtain

$$M(x)\log x \leqslant (1+B+A)xL(x),$$

which completes the proof of the first asserted inequality. For the second, we invoke (b) again, using (1.5),

$$\begin{aligned} L(x) \leqslant \sum_{P^+(n)\leqslant x} \frac{f(n)}{n} &= \prod_{p\leqslant x} \Big(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots\Big) \\ &\leqslant \exp\left(\sum_{p\leqslant x} \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots\right) \\ &\leqslant \exp\left(B + \sum_{p\leqslant x} \frac{f(p)}{p}\right). \end{aligned}$$

□

COROLLARY 2.21 (SUM OF $y^{\Omega(n,t)}$). *Let T be a subset of the primes in $[2,x]$, and let $1 \leqslant y_0 < \min T$. Uniformly for $1 \leqslant y \leqslant y_0$ we have*

$$\sum_{n\leqslant x} y^{\Omega(n,T)} \ll_{y_0} xe^{(y-1)H(T)}.$$

PROOF. The function $f(n) = y^{\Omega(n,T)}$ is multiplicative, with $f(p^k) = 1$ for $p \notin T$ and $f(p^k) = y^k$ if $p \in T$. Thus,

$$\sum_{p\leqslant u} f(p)\log p \ll y\sum_{p\leqslant u} \log p \ll yu$$

by Chebyshev's inequalities (Proposition 1.6). Also,

$$\sum_p \sum_{k\geqslant 2} \frac{f(p^k)}{p^k}\log p^k = \sum_{p\notin T}\sum_{k\geqslant 2} \frac{\log p^k}{p^k} + \sum_{p\in T}\sum_{k\geqslant 2} \frac{y^k \log p^k}{p^k} \ll 1 + \frac{y^2}{(\min T) - y} \ll_{y_0} 1$$

since $y \leqslant y_0 < \min T$. Hence, the hypotheses of the Halberstam-Richert Lemma (Lem. 2.20) hold, with constants A and B bounded depending on y_0. We conclude that

$$\begin{aligned} \sum_{n\leqslant x} y^{\Omega(n,T)} \ll_{y_0} \frac{x}{\log x}\exp\left(\sum_{p\leqslant x}\frac{f(p)}{p}\right) &= \frac{x}{\log x}\exp\left(\sum_{\substack{p\in T\\ p\leqslant x}}\frac{y}{p} + \sum_{\substack{p\notin T\\ p\leqslant x}}\frac{1}{p}\right) \\ &= \frac{x}{\log x}\exp\left(\sum_{\substack{p\in T\\ p\leqslant x}}\frac{y-1}{p} + \sum_{p\leqslant x}\frac{1}{p}\right) \\ &\leqslant \frac{x}{\log x}\exp\Big((y-1)H(T) + \log_2 x + O(1)\Big), \end{aligned}$$

since $y \geqslant 1$, and where Mertens' bound (Mertens.sum) was used in the last step. □

COROLLARY 2.22 ($\Omega(n,t)$ TAIL). *Let $1 < \lambda_0 < 2$. Uniformly for $1 \leqslant \lambda \leqslant \lambda_0$ and $3 \leqslant t \leqslant x$,*

$$\#\{n \leqslant x : \Omega(n,t) \geqslant \lambda \log_2 t\} \ll_{\lambda_0} x(\log t)^{-Q(\lambda)}.$$

PROOF. Let T be the set of primes in $[2,t]$. By Mertens' bound (Mertens.sum), $H(T) = \log_2 t + O(1)$. By Corollary 2.21,

$$\begin{aligned} \#\{n \leqslant x : \Omega(n,t) \geqslant \lambda\log_2 t\} &\leqslant \sum_{n\leqslant x} \lambda^{\Omega(n,t) - \lambda\log_2 t} \\ &\ll_{\lambda_0} \lambda^{-\lambda\log_2 t} x\mathrm{e}^{(\lambda-1)H(T)} \ll_{\lambda_0} x(\log t)^{-Q(\lambda)}. \end{aligned}$$

□

REMARK 2.23. When $\lambda \geqslant 2$, the behavior of the quantity in Corollary 2.22 is different than that of the quantity in Corollary 2.14. This is due to the behavior of powers of small prime factors, most important being powers of 2, and in fact

$$\#\{n \leqslant x : \Omega(n,t) \geqslant \lambda \log_2 t\} \approx x(\log t)^{-Q(2)-(\log 2)(\lambda-2)} = \frac{x \log t}{2^{\lambda \log_2 t}}. \tag{2.6}$$

See Exercise 2.5 below.

Mimicking the proof of the third part of the Prime Factors in Intervals Corollary (Cor. 2.14) and the proof of the Normal Sequence $\omega(n,t)$ Theorem (Thm. 2.15), we have the following.

COROLLARY 2.24. *(i) Uniformly for $3 \leqslant t \leqslant x$ and $0 \leqslant \psi \leqslant \sqrt{\log\log t}$, we have*

$$\#\{n \leqslant x : |\Omega(n,t) - \log\log t| > \psi\sqrt{\log\log t}\} \ll x\mathrm{e}^{-\frac{1}{3}\psi^2}.$$

(ii) Let $3 \leqslant \xi \leqslant x$. For all but $O(x/(\log\log\xi)^{1/3})$ integers $n \leqslant x$, we have

$$|\Omega(n,t) - \log_2 t| < 2\sqrt{\log_2 t \log_3 t} \qquad (\xi \leqslant t \leqslant x).$$

4.1. Application: Erdős' multiplication table problem. In 1955, Erdős [**Erd55**] posed the following problem: Estimate the number, $A(N)$, of *distinct* products of the form ab with $a \leqslant N$, $b \leqslant N$. Erdős proved that $A(N) = o(N^2)$, and later in 1960 [**Erd60**] refined the estimates to prove that $A(N) = N^2(\log N)^{-\mathcal{E}+o(1)}$, where

$$\mathcal{E} = 1 - \frac{1 + \log\log 2}{\log 2} = 0.08607\ldots.$$

THEOREM 2.25. *We have $A(N) \ll N^2(\log N)^{-\mathcal{E}}$.*

PROOF. Let $k_0 = \frac{\log_2 N}{\log 2}$. By Corollary 2.22 (with $t = N$), the number of distinct products with $\Omega(ab) \geqslant k_0$ is bounded above by

$$\#\{m \leqslant N : \Omega(m,N) \geqslant k_0\} \ll N^2(\log N)^{-Q(1/\log 2)} = N^2(\log N)^{-\mathcal{E}}.$$

If $\Omega(ab) < k_0$, then $\omega(a) = h$, $\omega(b) = j$ with $h + j = k < k_0$. The number of pairs a, b with a fixed h, j is, by the Prime Factors in Sets Theorem (Theorem 2.13) at most

$$\ll \frac{N^2(\log_2 N)^{h+j}}{(\log N)^2 h! j!}.$$

Summing first over all j, h with $h + j = k$ using the binomial theorem, and then over $k < k_0$ we obtain an upper bound for the total number of pairs a, b with $\Omega(ab) < k_0$ of

$$\ll \frac{N^2}{\log^2 N} \sum_{k<k_0} \frac{(2\log_2 N)^k}{k!} \ll N^2(\log^2 N)^{-Q(1/\log 4)} = N^2(\log N)^{-\mathcal{E}}$$

upon invoking the Popisson Tails Proposition (Prop. 1.11). □

5. Number of divisors of integers

The number, $\tau(n)$, of positive divisors of n, is closely related to the distribution of $\omega(n)$. From the formula

$$\tau(n) = \prod_{p^a \| n} (a+1)$$

and the elementary inequality $2 \leqslant a + 1 \leqslant 2^a$, it follows that

$$2^{\omega(n)} \leqslant \tau(n) \leqslant 2^{\Omega(n)}.$$

What is $\tau(n)$ for a "typical" $n \leqslant x$? By Theorem 2.15 and Corollary 2.24 (ii), for almost all $n \leqslant x$ we have

$$\log_2 x - 2\sqrt{\log_2 x \log_3 x} \leqslant \omega(n) \leqslant \Omega(n) \leqslant \log_2 x + 2\sqrt{\log_2 x \log_3 x},$$

and therefore for such n it follows that

$$\tau(n) = (\log x)^{\log 2} \exp\{O(\sqrt{\log_2 x \log_3 x})\} = (\log x)^{\log 2 + o(1)} \quad (x \to \infty).$$

By contrast, $\sum_{n\leqslant x}\tau(n)\sim x\log x$, so the average (mean) of $\tau(n)$ for $n\leqslant x$ is about $\log x$. Hence, the mode is much smaller than the mean.

Further analysis of the sum $\sum_{n\leqslant x}\tau(n)$: As we have just seen, this sum must be dominated by unusual integers, those with an abnormally large number of prime factors. But how large? Heuristically, most integers have few repeated prime factors (see Exercise 2.3), so that $\tau(n)\approx 2^{\omega(n)}$. The number of $n\leqslant x$ with $\omega(n)=k$ has order about $x\frac{(\log_2 x)^k}{k!(\log x)}$, so we get

$$\sum_{n\leqslant x}\tau(n)\approx\sum_k 2^k x\frac{(\log_2 x)^k}{k!(\log x)}=\frac{x}{\log x}\sum_k\frac{(2\log_2 x)^k}{k!}.$$

the sum over k has a peak around $k=2\log_2 x$, so we expect that the sum is dominated by integers with $\omega(n)\sim 2\log_2 x$. Moreover, the distribution is roughly Poisson with parameter $2\log_2 x$, which is well-approximated by a Gaussian (Proposition 4.10). This motivates the next result.

THEOREM 2.26. *Let $1\leqslant\psi\leqslant\sqrt{\log_2 x}$. Then*

$$\sum_{\substack{n\leqslant x\\ |\omega(n)-2\log_2 x|>\psi\sqrt{\log_2 x}}}\tau(n)\ll(x\log x)e^{-\frac{1}{12}\psi^2}.$$

PROOF. Let $\lambda=\frac{\psi}{\sqrt{\log_2 x}}\in[0,1]$. Let $1\leqslant t\leqslant 2$. Then

$$\begin{aligned}\sum_{\substack{n\leqslant x\\ \omega(n)\geqslant(2+\lambda)\log_2 x}}\tau(n)&\leqslant\sum_{n\leqslant x}\tau(n)t^{\omega(n)-(2+\lambda)\log_2 x}\\ &=t^{-(2+\lambda)\log_2 x}\sum_{n\leqslant x}\tau(n)t^{\omega(n)}.\end{aligned}$$

The summand is multiplicative, and satisfies the conditions of the Halberstam-Richert Theorem (Thm. 2.20). Hence

$$\sum_{n\leqslant x}\tau(n)t^{\omega(n)}\ll\frac{x}{\log x}\exp\Big(\sum_{p\leqslant x}\frac{2t}{p}\Big)\ll x(\log x)^{2t-1}$$

and therefore

$$\sum_{\substack{n\leqslant x\\ \omega(n)\geqslant(2+\lambda)\log_2 x}}\tau(n)\ll x(\log x)^{2t-1-(2+\lambda)\log t}.$$

The optimum value of t to minimize the right side is $t=1+\frac{\lambda}{2}$, and then the exponent of $\log x$ is

$$1-Q(1+\frac{\lambda}{2})\leqslant 1-\frac{1}{12}\lambda^2$$

using (1.14).

Similarly, taking $t=1-\frac{\lambda}{2}$, we obtain with a second application of the Halberstam-Richert Theorem (Thm 2.20) we estimate

$$\begin{aligned}\sum_{\substack{n\leqslant x\\ \omega(n)\leqslant(2-\lambda)\log_2 x}}\tau(n)&\leqslant t^{-(2-\lambda)\log_2 x}\sum_{n\leqslant x}\tau(n)t^{\omega(n)}\\ &\ll x(\log x)^{-(2-\lambda)\log t+2t-1}\\ &\ll x(\log x)^{1-2Q(1-\lambda/2)}\ll x(\log x)^{1-\frac{1}{12}\lambda^2}.\end{aligned}$$

Finally, $(\log x)^{\lambda^2}=e^{\psi^2}$ and the proof is complete. □

6. Exercises

EXERCISE 2.1. (a) Derive the following general inclusion-exclusion formula for a non-negative integer u:

$$\mathbf{1}(u=m)=\sum_{j=m}^{\infty}(-1)^{j-m}\binom{j}{m}\binom{u}{j}.$$

(b) Let $1\leqslant j\leqslant n$ be nonempty and $1\leqslant m\leqslant n/m$. Using part (a), derive an exact formula for the number of permutations $\sigma\in\mathcal{S}_n$ with $C_j(\sigma)=m$.

(c) With j,m fixed, evaluate

$$\lim_{n\to\infty}\mathbb{P}(C_j(\sigma)=m).$$

EXERCISE 2.2. (a) Let $I_1,I_2,\dots,I_k$ be disjoint subsets of $[n]$, and let $m_1,\dots,m_k$ be non-negative integers. Prove that

$$\mathbb{E}\binom{C_{I_1}(\sigma)}{m_1}\cdots\binom{C_{I_k}(\sigma)}{m_k}\leqslant\prod_{j=1}^{k}\frac{H(I_j)^{m_j}}{m_j!},$$

with equality if and only if $\sum_{j=1}^{k}m_j\max(I_j)\leqslant n$.

(b) Show that if T is a nonempty susbet of $[n]$, and $k\geqslant 0$, then

$$\mathbb{P}\left(C_T(\sigma)\geqslant k\right)\leqslant\frac{H(T)^k}{k!}.$$

(this is sometimes stronger than Theorem 2.9, especially if $H(T)$ is small).

(c) Show that the probability that a permutation $\sigma\in\mathcal{S}_n$ has two cycles of the same length $j\geqslant\ell$, is $O(1/\ell)$.

EXERCISE 2.3. (a) Show that if T is a nonempty susbet of the primes in $[2,x]$, and $k\geqslant 0$, then

$$\#\{n\leqslant x:\omega(n,T)\geqslant k\}\leqslant x\frac{H(T)^k}{k!}.$$

(this is sometimes stronger than Theorem 2.13, especially if $H(T)$ is small).

(b) Show that the number of $n\leqslant x$ that have two prime factors in some dyadic interval $(z,2z]$ for $z>y$, is $O(x/\log y)$.

EXERCISE 2.4. Show that

$$\sum_{n\leqslant x}2^{\Omega(n)}\gg x\log^2 x.$$

Compare with the upper bound for $\sum_{n\leqslant x}2^{\omega(n)}$.

EXERCISE 2.5 ([HT88], EXERCISE 05). Using Theorem 2.20, prove that for $1\leqslant y<2$,

$$\sum_{n\leqslant x}y^{\Omega(n)}\leqslant x\prod_{p\leqslant x}\left(1+\frac{y-1}{p-y}\right)\ll\frac{x(\log x)^{y-1}}{2-y}.$$

By choosing $y=2-1/k$, prove that

$$\#\{n\leqslant x:\Omega(n)=k\}\ll\frac{xk\log x}{2^k}$$

uniformly for $k\geqslant 1$ and $x\geqslant 2$. (this is not so good when $k<2\log\log x$, but it is close to the true order when $k>2\log\log x$).

EXERCISE 2.6. Let $\phi(n)$ be Euler's "totient" function, i.e., the number of integers $m\in[n]$ that are relatively prime to n. Let V be the image of ϕ, i.e. $V=\{1,2,4,6,8,10,12,16,\cdots\}$, and let $V(x)$ be the number of elements of V that are $\leqslant x$, e.g. $V(15)=7$. Prove that

$$V(x)\ll\frac{x\log\log x}{(\log x)^{c\log 2}},$$

where c is the unique solution of $c \log 2 = Q(c)$ with $0 < c < 1$ ($c = 0.373365\ldots$ according to Mathematica). **Hint:** if $\omega(n) = k$ then $2^{k-1} | \phi(n)$, and if $\phi(n) \leqslant x$ then $n \ll x \log\log x$.

CHAPTER 3

Integers without small/large prime factors and permutations without small/large cycles

Our basic sieve results are based on a method related to the so-called Brun-Hooley sieve [**FH00**].

LEMMA 3.1 (x_iy_i-LEMMA). *Suppose that $0 \leqslant x_j \leqslant y_j$ for $1 \leqslant j \leqslant t$. Then*

$$x_1 \cdots x_t \geqslant y_1 \cdots y_t - \sum_{\ell=1}^{t} (y_\ell - x_\ell) \prod_{\substack{j=1 \\ j\neq \ell}}^{t} y_j.$$

PROOF. The inequality is an equality when $t = 1$, and follows by induction on t using

$$\begin{aligned} y_1 \cdots y_t - x_1 \cdots x_t &= (y_1 \cdots y_{t-1} - x_1 \cdots x_{t-1})y_t + x_1 \cdots x_{t-1}(y_t - x_t) \\ &\leqslant (y_1 \cdots y_{t-1} - x_1 \cdots x_{t-1})y_t + y_1 \cdots y_{t-1}(y_t - x_t). \end{aligned}$$

□

1. Permutations without small cycles

Let $\mathcal{S}_{n,m}$ denote the set of permutations on $[n]$ that have no cycles of length $< m$. In particular, $\mathcal{S}_{n,1} = \mathcal{S}_n$. Based on our heuristic model, the likelihood that $\sigma \in \mathcal{S}_{n,m}$ should be (for m of moderate size) about the probability that $Z_1 = \cdots = Z_m = 0$, where $Z_j \stackrel{d}{=} \mathrm{Pois}(1/j)$, and this is $e^{-H_m} \approx \frac{e^{-\gamma}}{m}$. This cannot be expected to hold for large m, for example the probability is exactly $1/n$ if $m > n/2$ (permutations lacking cycles of length $< m$ must be n-cycles). In fact, when n/m is small, there is an asymptotic formula $\mathbb{P}(\sigma \in \mathcal{S}_{n,m}) \sim \omega(n/m)/m$ ($n \to \infty$, $m \to \infty$) where ω is Buchstab's function and $\omega(u) \to e^{-\gamma}$ as $u \to \infty$ [**Gra06**, Theorem 2.2].

A special case of the Cycles in Intervals Corollary (Cor. 2.11) (with $\lambda = 0$) implies that

$$\mathbb{P}(\sigma \in \mathcal{S}_{n,m}) \ll \frac{1}{m}$$

uniformly for $1 \leqslant m \leqslant n$. Our first result of this section is an explicit version of this bound, together with a corresponding lower estimate.

THEOREM 3.2 (NO SMALL CYCLES, I). *Suppose that m, n are integers with $1 \leqslant m \leqslant n$. Then*

$$\frac{1}{2m} \leqslant \mathbb{P}(\sigma \in \mathcal{S}_{n,m}) \leqslant \frac{1}{m}.$$

PROOF. (See the proof of [**Gra06**, Theorem 2.2]). We proceed by induction on n, the result being trivial when $n = 1$. Let $\mathcal{C}_{k,n}$ denote the set of cycles of length k that may be formed from $[n]$. Using the fact that the sum of lengths of cycles in a permutation in $\mathcal{S}_n$ is n, we get

$$n|\mathcal{S}_{n,m}| = \sum_{\sigma\in\mathcal{S}_{n,m}} n = \sum_{\sigma\in\mathcal{S}_{n,m}} \sum_{\substack{\beta|\sigma \\ \beta \text{ a cycle}}} |\beta| = \sum_{k\geqslant m} k \sum_{\beta\in\mathcal{C}_{k,n}} \sum_{\substack{\sigma\in\mathcal{S}_{n,m} \\ \beta|\sigma}} 1.$$

Write $\sigma = \beta\tau$, and observe that either $\beta = \sigma$ (that is, σ is an n-cycle), or $k = |\beta| \in [m, n-m]$. Therefore,

$$\begin{aligned} n|\mathcal{S}_{n,m}| &= \sum_{m\leqslant k\leqslant n-m} k \sum_{\beta\in\mathcal{C}_{k,n}} |\mathcal{S}_{n-k,m}| + \sum_{\beta\in\mathcal{C}_{n,n}} n \\ &= n! + \sum_{m\leqslant k\leqslant n-m} \frac{n!}{(n-k)!}|\mathcal{S}_{n-k,m}|. \end{aligned}$$

If $\frac{n}{2} < m \leqslant n$, then $|\mathcal{S}_{n,m}| = \frac{n!}{n}$ and the result follows. Otherwise, by the induction hypothesis,

$$n|\mathcal{S}_{n,m}| \leqslant n! + \sum_{m\leqslant k\leqslant n-m} \frac{n!}{m} = n!\left(1 + \frac{n-2m+1}{m}\right) \leqslant \frac{n!\cdot n}{m}$$

and

$$n|\mathcal{S}_{n,m}| \geqslant n! + \sum_{m\leqslant k\leqslant n-m} \frac{n!}{2m} = n!\left(1 + \frac{n-m+1}{m}\right) \geqslant \frac{n!\cdot n}{2m}. \qquad \square$$

When n/m is large, we can refine the prior bound substantially.

THEOREM 3.3 (NO SMALL CYCLES, II). *Let $1 \leqslant m \leqslant n$. Then*

$$\mathbb{P}(\sigma \in \mathcal{S}_{n,m}) = e^{-H_{m-1}}\left(1 + O(1/b!)\right), \quad b = \max\left(1, 2\left\lfloor \frac{n}{4m} - 1\right\rfloor\right).$$

PROOF. We may assume that $n \geqslant 8m$, as the conclusion follows from Lemma 3.2 otherwise (in this case $b = 1$). Partition $[m-1]$ into intervals $I_j = [z_j, z_{j-1})$, where $z_j = m/2^j$, $1 \leqslant j \leqslant \left\lceil \frac{\log m}{\log 2}\right\rceil = t$. Let $k_1, \dots, k_t$ be positive, even integers so that

$$\sum_{j=1}^{t} \frac{k_j m}{2^{j-1}} \leqslant n. \tag{3.1}$$

This implies that

$$\sum_{j=1}^{t} k_j \max I_j \leqslant n. \tag{3.2}$$

Let

$$x_j = \mathbf{1}(C_{I_j}(\sigma) = 0), \quad y_j = \sum_{r=0}^{k_j} (-1)^r \binom{C_{I_j}(\sigma)}{r}.$$

By Inclusion-Exclusion (Prop. 1.8), we have

$$0 \leqslant y_j - x_j = \binom{C_{I_j}(\sigma) - 1}{k_j} \leqslant \binom{C_{I_j}(\sigma)}{k_j}.$$

Thus, by the $x_i y_i$-Lemma (Lemma 3.1),

$$\mathbb{P}(\sigma \in S_{n,m}) = \frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n} x_1\cdots x_t = \frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n}\left[y_1\cdots y_t + O\left(\sum_{\ell=1}^{t}\binom{C_{I_\ell}(\sigma)}{k_\ell}\prod_{j\neq\ell} y_j\right)\right] = M + O(E),$$

say, where M is the "main term" and E is the "error term". Using Exercise 2.2 (a), with the condition (3.2), we find that

$$\begin{aligned} M &= \sum_{\substack{r_1,\dots,r_t\\ 0\leqslant r_j\leqslant k_j\,(1\leqslant j\leqslant t)}} (-1)^{r_1+\cdots+r_t}\mathbb{E}\binom{C_{I_1}(\sigma)}{r_1}\cdots\binom{C_{I_t}(\sigma)}{r_t}\\ &= \sum_{\substack{r_1,\dots,r_t\\ 0\leqslant r_j\leqslant k_j\,(1\leqslant j\leqslant t)}} (-1)^{r_1+\cdots+r_t}\prod_{j=1}^{t}\frac{H(I_j)}{r_j!}\\ &= \prod_{j=1}^{t}\Bigg(\sum_{r_j=0}^{k_j}\frac{(-H(I_j))^{r_j}}{r_j!}\Bigg). \end{aligned}$$

It is easy to see for all j that $\frac{1}{2}\leqslant H(I_j)\leqslant 1$. The alternating series error bound implies that

$$\left|\sum_{r_j=0}^{k_j}\frac{(-H(I_j))^{r_j}}{r_j!}-\mathrm{e}^{-H(I_j)}\right|\leqslant\frac{1}{(k_j+1)!},$$

and we deduce

$$M=\prod_{j=1}^{t}\left(\mathrm{e}^{-H(I_j)}+O\left(\frac{1}{(k_j+1)!}\right)\right)=\mathrm{e}^{-H_{m-1}}\prod_{j=1}^{t}\left(1+O\left(\frac{1}{(k_j+1)!}\right)\right).$$

Similarly, the error term satisfies

$$\begin{aligned} E &= \sum_{\ell=1}^{t}\sum_{\substack{r_j\,(j\neq\ell)\\ 0\leqslant r_j\leqslant k_j\,(j\neq\ell))}} (-1)^{\sum_{j\neq\ell}r_j}\mathbb{E}\binom{C_{I_\ell}(\sigma)}{k_\ell}\prod_{j\neq\ell}\binom{C_{I_j}(\sigma)}{r_j}\\ &= \sum_{\ell=1}^{t}\frac{H(I_\ell)^{k_\ell}}{k_\ell!}\prod_{j\neq\ell}\Bigg(\sum_{r_j=0}^{k_j}\frac{(-H(I_j))^{r_j}}{r_j!}\Bigg)\\ &\leqslant \sum_{\ell=1}^{t}\frac{e^{H(I_\ell)-H(I_\ell)}}{k_\ell!}\prod_{j\neq\ell}\left(\mathrm{e}^{-H(I_j)}+\frac{1}{(k_j+1)!}\right)\\ &\leqslant \mathrm{e}^{1-H_{m-1}}\left(\sum_{\ell=1}^{t}\frac{1}{k_\ell!}\right)\prod_{j\neq\ell}\left(1+\frac{2}{(k_j+1)!}\right). \end{aligned}$$

Taking $k_j=b+2(j-1)$, with $b=2\left\lfloor\frac{n}{4m}-1\right\rfloor$. Since $n\geqslant 8m$, $b\geqslant 2$. Also,

$$\sum_{j=1}^{\infty}\frac{k_j}{2^{j-1}}\leqslant\sum_{h=0}^{\infty}\frac{n/(2m)-2+2h}{2^h}=\frac{n}{m},$$

and thus (3.1) holds. With this choice,

$$\prod_{j=1}^{t}\left(1+O\left(\frac{1}{(k_j+1)!}\right)\right)=1+O\left(\frac{1}{b!}\right),$$

and the claimed estimate follows. □

2. Integers without small prime factors

Let $\Phi(x,z)$ denote the number of positive integers $n\leqslant x$ that have no prime factor $\leqslant z$. Again, a simple heuristic suggests that for small z we should have $\Phi(x,z)\approx x\prod_{p\leqslant z}(1-1/p)$, and this is what we will in fact demonstrate

below. We will also show a uniform bound of the same order of magnitude, valid for all z. A special case of the Prime Factors in Intervals Corollary (Cor. 2.14) (with $\lambda = 0$) implies that

$$\Phi(x,z) = \#\{n \leqslant x : \omega(n,z) = 0\} \ll x(\log z)^{-Q(0)} = \frac{x}{\log z}$$

uniformly for $2 \leqslant z \leqslant x$.

THEOREM 3.4 (NO SMALL PRIME FACTORS). *(i) Uniformly for $x \geqslant 0$, $2 \leqslant z \leqslant y^{1/30}$, we have*

$$\Phi(x+y,z) - \Phi(x,z) = y \prod_{p \leqslant z} \left(1 - \frac{1}{p}\right) \left(1 + O(e^{-u/3})\right), \quad u = \frac{\log y}{\log z};$$

(ii) Uniformly for $x \geqslant 0$ and $2 \leqslant z \leqslant y$, we have

$$\Phi(x+y,z) - \Phi(x,z) \ll \frac{y}{\log z};$$

(iii) Uniformly for $x \geqslant 2z \geqslant 4$ we have

$$\Phi(x,z) \gg \frac{x}{\log z}.$$

PROOF. First, we observe that parts (ii) and (iii) are simple consequences of part (i). By Mertens' estimates (Proposition 1.5),

$$\prod_{p \leqslant z} \left(1 - \frac{1}{p}\right) \asymp \frac{1}{\log z},$$

which proves (ii) for $z \leqslant y^{1/30}$ and (iii) for $z \leqslant x^{\delta}$ if δ is small enough in terms of the implied constants. Part (ii) holds for the remainder of the range using

$$\Phi(x+y,z) - \Phi(x,z) \leqslant \Phi\big(x+y, y^{1/30}\big) - \Phi\big(x, y^{1/30}\big)$$

and $\log z \asymp \log\big(y^{1/30}\big)$ when $y^{1/30} < z \leqslant y$. When $x^{\delta} < z \leqslant x/2$, part (iii) follows from the Prime Number Theorem (Proposition 1.7) for large x, and Bertrand's Postulate (Proposition 1.6 (ii)) for small x.

Next we prove part (i). Following the proof of Lemma 3.3, partition the primes $\leqslant z$ into subsets I_j, the primes in $(z_j, z_{j-1}]$, $1 \leqslant j \leqslant t$, where $z_i = z^{1/2^i}$ (t is the largest index so that the prime 2 is included). Let P_j denote the product of the primes in I_j, and let $k_1, k_2, \dots$ be positive, even integers which satisfy

$$\sum_{j=1}^{t} k_j \log z_{j-1} \leqslant \frac{1}{2} \log y. \tag{3.3}$$

Let

$$x_j = \mathbf{1}(\omega(n; I_j) = 0), \quad y_j = \sum_{r=0}^{k_j} (-1)^r \binom{\omega(n; I_j)}{r}.$$

By Inclusion-Exclusion (Lemma 1.8), we have

$$0 \leqslant y_j - x_j = \binom{\omega(n; I_j) - 1}{k_j} \leqslant \binom{\omega(n; I_j)}{k_j}.$$

Thus, by Lemma 3.1, we have

$$\begin{aligned}\Phi(x+y,z)-\Phi(x,z) &= \sum_{\substack{r_1,\dots,r_t\\ 0\leqslant r_j\leqslant k_j\ (\forall j)}} (-1)^{r_1+\cdots+r_t} \sum_{x<n\leqslant x+y} \binom{\omega(n;I_1)}{r_1}\cdots\binom{\omega(n;I_t)}{r_t} + \\ &\qquad + O\bigg(\sum_{\ell=1}^{t} \sum_{\substack{r_j\ (j\neq\ell)\\ 0\leqslant r_j\leqslant k_j\ (j\neq\ell)}} \sum_{x<n\leqslant x+y} \binom{\omega(n;I_\ell)}{k_\ell} \prod_{j\neq\ell} (-1)^{r_j}\binom{\omega(n;I_j)}{r_j}\bigg) \\ &= \sum_{\substack{d_1\mid P_1,\dots,d_t\mid P_t\\ \omega(d_j)\leqslant k_j (1\leqslant j\leqslant t)}} \mu(d_1)\cdots\mu(d_t)\bigg(\frac{y}{d_1\dots d_t}+O(1)\bigg) + \\ &\qquad + O\bigg(\sum_{\ell=1}^{t} \sum_{\substack{d_1\mid P_1,\dots,d_t\mid P_t\\ \omega(d_j)\leqslant k_j (j\neq\ell)\\ \omega(d_\ell)=k_\ell}} \mu(d_1)\cdots\mu(d_t)\bigg(\frac{y}{d_1\dots d_t}+O(1)\bigg)\bigg).\end{aligned}$$

By (3.3), each product $d_1\cdots d_t\leqslant y^{1/2}$, and each tuple $(d_1,\dots,d_t)$ yields a unique product, thus the aggregate of the $O(1)$ terms is $O(y^{1/2})$. The remaining sums over $d_1,\dots,d_t$ separate into products, and thus we obtain

$$\Phi(x+y,z)-\Phi(x,z)=O(y^{1/2})+y(M+O(E)),$$

where

$$M=\prod_{j=1}^{t}\bigg(\sum_{\substack{d_j\mid P_j\\ \omega(d_j)\leqslant k_j}}\frac{\mu(d_j)}{d_j}\bigg),\qquad E=\sum_{\ell=1}^{t}\bigg(\sum_{\substack{d_\ell\mid P_\ell\\ \omega(d_\ell)=k_\ell}}\frac{\mu(d_\ell)}{d_\ell}\bigg)\prod_{j\neq\ell}\bigg(\sum_{\substack{d_j\mid P_j\\ \omega(d_j)\leqslant k_j}}\frac{\mu(d_j)}{d_j}\bigg). \tag{3.4}$$

We wish to remove the conditions $\omega(d_j)\leqslant k_j$ in the above sums. If d_j is squarefree, and has at least k_j+1 prime factors, let c be the product of the smallest k_j+1 prime factors of d_j, and set $c'=d_j/c$. Using (1.4), we get that

$$\sum_{\substack{d_j\mid P_j\\ \omega(d_j)\geqslant k_j+1}}\frac{\mu(d_j)}{d_j}=\sum_{\substack{c\mid P_j\\ \omega(c)=k_j+1}}\frac{\mu(c)}{c}\sum_{\substack{c'\mid P_j\\ P^-(c')>P^+(c)}}\frac{\mu(c')}{c'}=\sum_{\substack{c\mid P_j\\ \omega(c)=k_j+1}}\frac{(-1)^{k_j+1}}{c}\prod_{\substack{p\mid P_j\\ p>P^+(c)}}(1-1/p).$$

The product is always at most 1, and from the k factors Proposition (1.9), we have

$$\sum_{\substack{d_j\mid P_j\\ \omega(d_j)=k}}\frac{1}{d}\leqslant\frac{H(I_j)^k}{k!}.$$

Thus, we have

$$\bigg|\sum_{\substack{d_j\mid P_j\\ \omega(d_j)\geqslant k_j+1}}\frac{\mu(d_j)}{d_j}\bigg|\leqslant\frac{H(I_j)^{k_j+1}}{(k_j+1)!}. \tag{3.5}$$

Combining (3.5) with the inifinite product formula (1.4) to the corresponding "complete" sum over all $d_j|P_j$, we get

$$M=\prod_{j=1}^{t}\bigg(\prod_{p\in I_j}\Big(1-\frac{1}{p}\Big)+O\Big(\frac{H(I_j)^{k_j+1}}{(k_j+1)!}\Big)\bigg)=\prod_{j=1}^{t}\bigg(1+O\Big(\frac{H(I_j)^{k_j+1}}{(k_j+1)!}\Big)\bigg)\prod_{p\in I_j}\Big(1-\frac{1}{p}\Big).$$

The second inequality follows using Mertens' estimate (Mertens.product) which implies that $\prod_{p\in I_j}(1-1/p)\gg 1$. Likewise we deduce

$$\begin{aligned} E &\ll \sum_{\ell=1}^{t}\frac{H(I_j)^{k_j}}{k_j!}\prod_{j\neq\ell}\left(\prod_{p\in I_j}(1-1/p)+O\left(\frac{H(I_j)^{k_j+1}}{(k_j+1)!}\right)\right)\\ &\ll \left(\sum_{\ell=1}^{t}\frac{H(I_\ell)^{k_\ell}}{k_\ell!}\right)\prod_{j=1}^{t}\left(1+O\left(\frac{H(I_j)^{k_j+1}}{(k_j+1)!}\right)\right)\prod_{p\leqslant z}\left(1-\frac{1}{p}\right). \end{aligned}$$

Let $k_j=b+2(j-1)$ with $b=2\lfloor\frac{u}{8}-2\rfloor$, so that

$$\sum_{j=1}^{t}k_j\log z_{j-1}\leqslant\sum_{j=1}^{\infty}\Big(\frac{u}{4}+2j-6\Big)\frac{\log z}{2^{j-1}}=\frac{\log y}{2},$$

that is, (3.3) holds. Again by Mertens' estimate (Mertens.sum), $H(I_j)\ll 1$, and thus

$$\prod_{j=1}^{t}\left(1+O\left(\frac{H(I_j)^{k_j+1}}{(k_j+1)!}\right)\right)=\exp\left\{\sum_{j=1}^{t}O\left(\frac{H(I_j)^{k_j+1}}{(k_j+1)!}\right)\right\}=\exp\Big\{\frac{e^{O(b)}}{(b+1)!}\Big\}=1+O\Big(\frac{e^{O(b)}}{(b+1)!}\Big).$$

Similarly,

$$\sum_{\ell=1}^{t}\frac{H(I_\ell)^{k_\ell}}{k_\ell!}\ll\frac{e^{O(b)}}{b!}.$$

We conclude that

$$\Phi(x+y,z)-\Phi(x,z)=\Big(1+O\Big(\frac{e^{O(b)}}{b!}\Big)\Big)\,y\prod_{p\leqslant z}\left(1-\frac{1}{p}\right)+O(y^{1/2}).$$

Finally, $e^{O(b)}/b!\ll e^{-u}$ and, using $e^u\leqslant e^{\frac{\log y}{\log 2}}\leqslant y^{1/\log 2}$, we have that

$$y^{1/2}\ll ye^{-u/3}/\log z\ll ye^{-u/3}\prod_{p\leqslant z}\left(1-\frac{1}{p}\right),$$

and the proof is complete. □

REMARK 3.5. The above proof gives a better error term, namely

$$\Phi(x+y,z)-\Phi(x,z)=y\prod_{p\leqslant z}\left(1-\frac{1}{p}\right)\Big(1+O(e^{-(u/4)\log u})\Big),$$

in the restricted range $\log y\leqslant z\leqslant y$. In the full range $2\leqslant z\leqslant y$, one cannot do better than a relative error $O(e^{-(\log 2)u})$ because

$$\Phi(x,2)=\frac{x}{2}+O(1)$$

(the $O(1)$ cannot be improved) and $u=\frac{\log x}{\log 2}$ in this case.

3. Permutations without large cycles, and integers without large prime factors

THEOREM 3.6 (NO LARGE CYCLES). *Choose $\sigma\in\mathcal{S}_n$ at random. Uniformly for $1\leqslant m\leqslant n$ we have*

$$\mathbb{P}(C_{(m,n]}(\sigma)=0)\leqslant e^{-u\log u+u},\quad u=n/m.$$

PROOF. Starting as in the proof of the Theorem on No small Cycles, I (Thm 3.2), we have

$$n\mathbb{P}(C_{(m,n]}(\sigma)=0) = \frac{1}{n!}\sum_{\substack{\sigma\in\mathcal{S}_n\\ C_{(m,n]}(\sigma)=0}}\ \sum_{\substack{\beta|\sigma\\ \beta \text{ a cycle}}} |\beta|$$
$$= \sum_{\ell\leqslant m}\frac{1}{(n-\ell)!}\#\{\tau\in\mathcal{S}_{n-\ell} : C_{(m,n-\ell]}(\tau)=0\}.$$

Let τ have cycle type $(a_1,\dots,a_m)$. By Cauchy's formula 2.2, we have

$$n\mathbb{P}(C_{(m,n]}(\sigma)=0) = \sum_{\ell\leqslant m}\ \sum_{\substack{a_1,\dots,a_m\geqslant 0\\ a_1+2a_2+\cdots+ma_m=n-\ell}}\frac{1}{\prod_{j=1}^m a_j!j^{a_j}}$$
$$= \sum_{\substack{a_1,\dots,a_m\geqslant 0\\ a_1+2a_2+\cdots+ma_m\in[n-m,n-1]}}\frac{1}{\prod_{j=1}^m a_j!j^{a_j}}.$$

Let $w\geqslant 1$ be a parameter, to be chosen later. We have

$$n\mathbb{P}(C_{(m,n]}(\sigma)=0) \leqslant \sum_{a_1,\dots,a_m\geqslant 0}\frac{w^{a_1+\cdots+ma_m-(n-m)}}{\prod_{j=1}^m a_j!j^{a_j}}$$
$$= w^{m-n}\exp\Big\{w+\frac{1}{2}w^2+\cdots+\frac{1}{m}w^m\Big\}.$$

Now let $w=u^{1/m}$, where $u=n/m$. For $c\geqslant 0$ and $0\leqslant z\leqslant 1$ we have

$$e^{cz} = 1+z\sum_{k=1}^{\infty}\frac{c^k z^{k-1}}{k!}\leqslant 1+(e^c-1)z. \tag{e^{cz}}$$

Applying this with $z=j/m$ yields

$$\sum_{j=1}^m\frac{w^j}{j}\leqslant\sum_{j=1}^m\frac{1+(u-1)j/m}{j} = H_m+u-1\leqslant\log m+u$$

and we conclude that

$$\mathbb{P}(C_{(m,n]}(\sigma)=0)\leqslant\frac{1}{n}u^{1-n/m}e^{\log m+u} = e^{-u\log u+u}. \qquad \square$$

Let $\Psi(x,y)=\#\{n\leqslant x : P^+(n)\leqslant y\}$. These are known as *y-smooth*, or *y-friable* numbers.

THEOREM 3.7 (SMOOTH NUMBERS). *Let $2\leqslant y\leqslant x$ and put $u=\frac{\log x}{\log y}$. We have*

(i) $\Psi(x,y)\ll xe^{-u/2}$ *uniformly for* $2\leqslant y\leqslant x$;
(ii) $\Psi(x,y)\ll xe^{-u\log u+O(u)}$ *uniformly for* $(\log x)^3\leqslant y\leqslant x$;
(iii) $\Psi(x,\log x)\ll\exp\{(1+o(1))\frac{\log x\log_3 x}{\log_2 x}\}$ *as* $x\to\infty$.

PROOF. We may assume that x is sufficiently large. If $y<11$, then $\Psi(x,y)\leqslant\Psi(x,7)\ll(\log x)^4$, as every number that is 7-smooth can be written in the form $2^{a_2}3^{a_3}5^{a_5}7^{a_7}$, with $a_p\ll\log x$. On the other hand, $xe^{-u/2}\gg x^{1-1/\log 4}$ when $y\leqslant 7$. Now assume $y\geqslant 11$, and denote by $a(n)$ the indicator function of y-smooth numbers. For any real $\beta\geqslant 0$ we have

$$\Psi(x,y)\leqslant x^{3/4}+\sum_{x^{3/4}<n\leqslant x}\Big(\frac{n}{x^{3/4}}\Big)^{\beta}a(n).$$

Take $\beta = \frac{2}{3\log y} < \frac{1}{3}$ and apply the Halberstam-Richert Lemma (Lemma 2.20) with $f(n) = n^\beta a(n)$; the hypotheses are seen to hold with A, B being absolute constants (since $f(p) = p^\beta \leqslant e^{2/3}$ for $p \leqslant y$). Thus, by (e^{cz}),

$$\begin{aligned}\sum_{n\leqslant x} n^\beta a(n) &\ll \frac{x}{\log x}\exp\left\{\sum_{p\leqslant y}\frac{p^\beta}{p}\right\}\\ &= \frac{x}{\log x}\exp\left\{\sum_{p\leqslant y}\frac{1+O(\beta\log p)}{p}\right\}\\ &\ll \frac{x\log y}{\log x} \ll x.\end{aligned}$$

We conclude that

$$\Psi(x,y) \ll x^{3/4} + x^{1-(3/4)\beta} = x^{3/4} + xe^{-u/2}.$$

Finally, since $y \geqslant 11$, $1 - u/2 > 3/4$, and (i) follows.

To prove (ii), we modify the above argument as follows: when $\log^3 x \leqslant y \leqslant x$, let $\beta = \frac{\log u}{\log y} \in (0, \frac{1}{3}]$, and $1 \leqslant V < x$ be another parameter. We have

$$\begin{aligned}\Psi(x,y) &\leqslant \sum_{n\leqslant V} a(n)\left(\frac{V}{n}\right)^{1-\beta} + \sum_{V<n\leqslant x}\left(\frac{n}{V}\right)^{\beta} a(n)\\ &\leqslant V^{1-\beta}\prod_{P^+(n)\leqslant y}\frac{1}{n^{1-\beta}} + V^{-\beta}\sum_{n\leqslant x} n^\beta a(n).\end{aligned}$$

The first sum equals an infinite product, using (1.5), and we employ the Halberstam-Richert Lemma (Lemma 2.20) on the second sum. Letting $f(n) = a(n)n^\beta$, the hypotheses hold with $A = O(u)$ and B an absolute constant. Thus,

$$\Psi(x,y) \ll \left(V^{1-\beta} + V^{-\beta}\frac{ux}{\log x}\right)\exp\left\{\sum_{p\leqslant y}\frac{p^\beta}{p}\right\}.$$

Using (e^{cz}), $p^\beta = e^{\beta\log p} \leqslant 1 + u\frac{\log p}{\log y}$ and thus, by Mertens' estimates we have

$$\sum_{p\leqslant y}\frac{p^\beta}{p} \leqslant \sum_{p\leqslant y}\frac{1+u\frac{\log p}{\log y}}{p} = \log_2 y + O(u).$$

We conclude that

$$\Psi(x,y) \ll \left(V^{1-\beta} + V^{-\beta}\frac{x}{\log x}\right)(\log y)e^{O(u)}.$$

Finally, take $V = \frac{x}{\log x}$, note that $x^{-\beta} = \exp\{-u\log u\}$, and that $(\log x)^\beta \leqslant e^{(\log u)/3}$.

The proof of (iii) is combinatorial. Let $r = r(x)$ be an integer parameter. Each $n \leqslant x$ with $P^+(n) \leqslant \log x$ may be written uniquely in the form

$$n = m^r \prod_{p\leqslant \log x} p^{a_p}, \quad 0 \leqslant a_p \leqslant r-1.$$

Since $m \leqslant x^{1/r}$ and there are $\pi(\log x) \sim \frac{\log x}{\log_2 x}$ primes in the product, the number of such integers does not exceed

$$x^{1/r} r^{\pi(\log x)} \leqslant \exp\left\{\frac{\log x}{r} + (1+o(1))(\log r)\frac{\log x}{\log_2 x}\right\}.$$

Taking $r = \lfloor \log_2 x \rfloor$ completes the proof. □

REMARK 3.8. The proof of (i) follows [**Ten15**, Theorem III.5.1]. The proof of (i) and (ii) use 'Rankin's method' [**Ran38**], which is partly embodied in the Halberstam-Richert Lemma 2.20; see also [**Pom89**]. The proof of (iii) comes from Erdős [].

Describe what is known for small u, in terms of the Dickman function $\rho(u)$; results of Hildebrand and Mastivičius.

4. Homework

EXERCISE 3.1. (a) Suppose $n/2 \leqslant m \leqslant n$. Show that

$$\mathbb{P}(\sigma \text{ has no cycles of length } > m) = 1 - (H_n - H_m).$$

In particular, when $m = 50, n = 100$, this helps to solve the "100 prisoner's problem".

(b) Suppose $\sqrt{x} \leqslant y \leqslant x$. Show that

$$\#\{n \leqslant x : P^+(n) \leqslant y\} = x \log\left(\frac{\log x}{\log y}\right) + O\left(\frac{x}{\log x}\right).$$

CHAPTER 4

Poisson approximation of small cycle lengths and small prime divisors

1. Small cycles of permutations

Let $1 \leqslant k \leqslant n$ and consider the problem of modeling

$$\mathbf{C}_k = (C_1(\sigma), \dots, C_k(\sigma))$$

by the random vector

$$\mathbf{Z}_k = (Z_1, \dots, Z_k), \quad Z_j \stackrel{d}{=} \mathrm{Pois}(1/j).$$

We especially desire a good approximation when k is large, as opposed to bounded (ref. Theorem 2.9). We express our results in terms of the Total Variational Distance $d_{TV}(X, Y)$ between two random variables X and Y taking values in a discrete space Ω, defined by

$$d_{TV}(X, Y) := \sup_{U \subset \Omega} \Delta(U), \quad \Delta(U) = \mathbb{P}(X \in U) - \mathbb{P}(Y \in U). \tag{4.1}$$

The supremum occurs when $U = U^+ := \{\omega \in \Omega : \mathbb{P}(X = \omega) > \mathbb{P}(Y = \omega)\}$. The infimum occurs at $U = U^- := \{\omega \in \Omega : \mathbb{P}(X = \omega) < \mathbb{P}(Y = \omega)\}$, and since $\Delta(U^+) + \Delta(U^-) = 0$, it follows that

$$d_{TV}(X, Y) = \frac{1}{2}\big(\Delta(U^+) - \Delta(U^-)\big) = \frac{1}{2} \sum_{\omega \in \Omega} \left|\mathbb{P}(X = \omega) - \mathbb{P}(Y = \omega)\right|. \tag{4.2}$$

In comparing $\mathbf{C}_k$ and $\mathbf{Z}_k$, the space of values is $\Omega = \mathbb{N}_0^k$.

LEMMA 4.1. *We have*

$$d_{TV}(\mathbf{C}_k, \mathbf{Z}_k) = \frac{1}{2} \sum_{\mathbf{h} \in \mathbb{N}_0^k} \prod_{j=1}^{k} \frac{1}{j^{h_j} h_j!} \left| e^{-H_k} - \frac{|\mathcal{S}_{n',k+1}|}{(n')!} \mathbf{1}(n' \geqslant 0) \right|,$$

where $n' = n'(\mathbf{h}) = n - \sum_{j=1}^{k} j h_j$.

PROOF. By (4.2), we have

$$d_{TV}(\mathbf{C}_k, \mathbf{Z}_k) = \frac{1}{2} \sum_{\mathbf{h} \in \mathbb{N}_0^k} \left|\mathbb{P}(\mathbf{C}_k = \mathbf{h}) - \mathbb{P}(\mathbf{Z}_k = \mathbf{h})\right|.$$

Clearly,

$$\mathbb{P}(\mathbf{Z}_k = \mathbf{h}) = e^{-H_k} \prod_{j=1}^{k} \frac{1}{j^{h_j} h_j!}.$$

Now suppose that $\mathbf{C}_k = \mathbf{h}$ and write $g = h_1 + 2h_2 + \cdots + kh_k$. If $g > n$, then $\mathbb{P}(\mathbf{C}_k = \mathbf{h}) = 0$. Now suppose that $g \leqslant n$. Write $\sigma = \sigma_1 \sigma_2$, where σ_1 is the product of the cycles of length at most k and permutes a subset I_1 of $[n]$ of size g, and σ_2 is the product of the cycles of length greater than k and permutes $[n] \setminus I$ of size $n' = n - g$. By Cauchy's formula (2.2), applied to σ_1, it follows that

$$\mathbb{P}(\mathbf{C}_k = \mathbf{h}) = \frac{|\mathcal{S}_{n',k+1}|}{(n')!} \prod_{j=1}^{k} \frac{1}{j^{h_j} h_j!},$$

and the lemma follows. □

THEOREM 4.2 (POISSON DISTRIBUTION OF SMALL CYCLES). *Let $1 \leqslant k \leqslant n$. Then*

$$d_{TV}(\mathbf{C}_k, \mathbf{Z}_k) \ll e^{-n/k}.$$

PROOF. The claim is trivial if $k > n/4-4$, as long as the implied constant is large enough. Thus, we may assume that $k \leqslant n/4 - 4$.

Consider a generic vector $\mathbf{h} = (h_1, \cdots, h_k) \in \mathbb{N}_0^k$. The main idea of the proof is to separately consider those vectors which constitue rare events (many h_j large): specifically, let

$$\mathcal{H}_1 = \{\mathbf{h} \in \mathbb{N}_0^k : h_1 + 2h_2 + \cdots + kh_k \leqslant n/2\},$$
$$\mathcal{H}_2 = \{\mathbf{h} \in \mathbb{N}_0^k : h_1 + 2h_2 + \cdots + kh_k > n/2\}.$$

First, consider $\mathbf{h} \in \mathcal{H}_1$ and let $n' = n - (h_1 + 2h_2 + \cdots + kh_k) \geqslant n/2$. By the No Small Cylcles Theorem, II (Thm 3.3),

$$\begin{aligned} \frac{|\mathcal{S}_{n',k+1}|}{(n')!} &= e^{-H_k}\left(1 + O\left(\frac{1}{b!}\right)\right), \quad b = 2\left\lfloor \frac{n/2}{4k} - 1 \right\rfloor \\ &= e^{-H_k}\left(1 + O\left(e^{-n/k}\right)\right), \end{aligned} \tag{4.3}$$

by Stirling's formula (1.2), since $b \geqslant n/4k - 2$. Applying the strong approximation (4.3), it follows that

$$\sum_{\mathbf{h}\in\mathcal{H}_1} \frac{1}{j^{h_j} h_j!}\left| e^{-H_k} - \frac{|\mathcal{S}_{n',k+1}|}{(n')!}\mathbf{1}(n' \geqslant 0)\right| \ll e^{-H_k - n/k} \sum_{\mathbf{h}\in\mathbb{N}_0^k} \frac{1}{j^{h_j} h_j!} = e^{-n/k}. \tag{4.4}$$

For $\mathbf{h} \in \mathcal{H}_2$,

$$e^{-H_k} - \frac{|\mathcal{S}_{n',k+1}|}{(n')!}\mathbf{1}(n' \geqslant 0) = O(1/k)$$

by the No Small Cycles Theorem, I (Thm 3.2) and the bound for the harmonic sum (Proposition (1.1)) (note that if $n' \leqslant k$ then $\mathcal{S}_{n',k+1} = 0$). Using the method of parameters, for any real number $w \geqslant 1$ we have

$$\sum_{\mathbf{h}\in\mathcal{H}_2} \prod_{j=1}^{k} \frac{1}{j^{h_j} h_j!} \leqslant \sum_{\mathbf{h}\in\mathbb{N}_0^k} w^{h_1 + 2h_2 + \cdots + kh_k} \prod_{j=1}^{k} \frac{1}{j^{h_j} h_j!} = w^{-n/2} \exp\left\{ w + \frac{1}{2}w^2 + \cdots + \frac{1}{k}w^k \right\}.$$

We take $w = e^{2/k}$ and note that from inequality (e^{cz}) we get

$$\sum_{j=1}^{k} \frac{w^j}{j} = \sum_{j=1}^{k} \frac{1 + O(j/k)}{j} = H_k + O(1),$$

and hence

$$\sum_{\mathbf{h}\in\mathcal{H}_2} \prod_{j=1}^{k} \frac{1}{j^{h_j} h_j!}\left| e^{-H_k} - \frac{|\mathcal{S}_{n',k+1}|}{(n')!}\mathbf{1}(n' \geqslant 0)\right| \ll \frac{1}{k} e^{-H_k} e^{-n/k} \ll e^{-n/k}. \tag{4.5}$$

Inserting the estimates (4.4) and (4.5) into Lemma 4.1, we conclude the proof. □

REMARK 4.3. By a more strategic choice of parameters in both the proof of Theorem 3.3 (that is, the parameters z_j and k_j) and the proof of Theorem 4.2 (the choice of $\mathcal{H}_1$, $\mathcal{H}_2$, and w), plus a modest amount of additional computation, it is possible to prove that

$$d_{TV}(\mathbf{C}_k, \mathbf{Z}_k) \ll e^{-f(n/k)},$$

where $f(x) \sim x \log x$ as $x \to \infty$. This is the true order (the asymptotics of the logarithm of the left side), and a result of Arratia and Tavaré [**AT92**]. Sharper bounds are known, and are expressed in terms of the Dickman and Buhstab functions (see [**Pet16**]).

We almost immediately obtain the following corollary, by grouping together integers into sets. For any set I of positive integers, let

$$Z_I \stackrel{d}{=} \mathrm{Pois}(H(I)).$$

THEOREM 4.4 (POISSON DISTRIBUTION OF CYCLES). *Let $I_1, \dots, I_m$ be disjoint subsets of $[k]$, with $k \leqslant n$. Then, for any non-negative integers $h_1, \dots, h_m$,*

$$\mathbb{P}\left(C_{I_1}(\sigma) = h_1, \dots, C_{I_m}(\sigma) = h_m\right) = \mathbb{P}\left(Z_{I_1} = h_1, \dots, Z_{I_m} = h_m\right) + O(e^{-n/k}).$$

2. The Kubilius model of small prime factors of integers

We will make formal a kind a probabilistic interpretation of various results about the distribution of integers which have been stated in earlier sections. Let $x \geqslant 2$ be a real number, and select an integer in $[1, x]$ at random. Various probabilities will be denoted using the symbol $\mathbb{P}_x$, and also $\mathbb{E}_x$ for expectations with respect to this probability space. Such an integer n has a canonical prime factorization as

$$n = \prod_{p \leqslant x} n^{v_p}.$$

We regard each of the exponents v_p as random variables; these technically depend no only on p, but also on x. We compute exactly

$$\mathbb{P}_x(v_p = k) = \frac{1}{\lfloor x \rfloor}\left(\left\lfloor \frac{x}{p^k} \right\rfloor - \left\lfloor \frac{x}{p^{k+1}} \right\rfloor\right) = \frac{1}{p^k} - \frac{1}{p^{k+1}} + O\left(\frac{1}{x}\right),$$

the error term being relatively small when p^k is small. Moreover, the variables v_p are quasi-independent; that is, the correlations are small, again provided that the primes are small. The variables v_p corresponding to large p are very dependent on each other, for example the event $(v_p > 0, v_q > 0)$ is impossible if $pq > x$.

The model of Kubilius is a sequence of *idealized* random variables which remove the error terms above, and is thus easier to compute with. For each prime p, define the random variable X_p that has domain $\mathbb{N}_0$ and such that

$$\mathbb{P}(X_p = k) = \frac{1}{p^k} - \frac{1}{p^{k+1}} = \frac{1}{p^k}\left(1 - \frac{1}{p}\right) \qquad (k = 0, 1, 2, \dots).$$

If y is small compared with x, we expect that the random vector

$$\mathbf{X}_y = (X_p : p \leqslant y)$$

has distribution close to that of the random vector

$$\mathbf{V}_{x,y} = (v_p : p \leqslant y).$$

Recall the definition (4.1) of the total variation distance and the basic identity (4.2).

LEMMA 4.5. *We have*

$$d_{TV}(\mathbf{X}_y, \mathbf{V}_{x,y}) = \frac{1}{2} \sum_{P^+(m) \leqslant y} \left| \frac{1}{\lfloor x \rfloor} \Phi\left(\frac{x}{m}, y\right) - \frac{1}{m}\zeta_y \right|, \quad \zeta_y = \prod_{p \leqslant y}\left(1 - \frac{1}{p}\right).$$

PROOF. (cf. Tenenbaum [**Ten99**]). Fix $\mathbf{v} = (v_p : p \leqslant y)$ and write $m = \prod_{p \leqslant y} p^{v_p}$. Then

$$\mathbb{P}(\mathbf{X}_y = \mathbf{v}) = \prod_{p \leqslant y} \mathbb{P}(X_p = v_p) = \prod_{p \leqslant y} \frac{1}{p^{v_p}}\left(1 - \frac{1}{p}\right) = \frac{1}{m}\zeta_y$$

and

$$\mathbb{P}_x\left(\mathbf{V}_{x,y} = \mathbf{v}\right) = \frac{1}{\lfloor x \rfloor} \#\{\ell \in \mathbb{N} : m\ell \leqslant x, P^-(\ell) > y\} = \frac{1}{\lfloor x \rfloor} \Phi\left(\frac{x}{m}, y\right). \qquad \square$$

THEOREM 4.6 (KUBILIUS MODEL APPROXIMATION). *Let $2 \leqslant y \leqslant x$. Then*

$$d_{TV}(\mathbf{X}_y, \mathbf{V}_{x,y}) \ll \exp\Big\{ - \frac{\log x}{6 \log y} \Big\}.$$

PROOF. We begin with Lemma 4.5, and break the summation into two parts, according to $m \leqslant \sqrt{x}$ or $m > \sqrt{x}$. When $m \leqslant \sqrt{x}$, we apply the No Small Prime Factors Theorem (Theorem 3.4) part (i), which implies that

$$\Phi\left(\frac{x}{m}, y\right) = \frac{x}{m}\zeta_y\left(1 + O(e^{-u/3})\right),$$

where $u = u(x, y, m) = \frac{\log(x/m)}{\log y}$. For all such m, we have $u/3 \geqslant w := \frac{\log x}{6 \log y}$, and therefore

$$\sum_{\substack{P^+(m)\leqslant y\\ m\leqslant\sqrt{x}}} \left|\frac{1}{\lfloor x\rfloor}\Phi\left(\frac{x}{m}, y\right) - \frac{1}{m}\zeta_y\right| \ll \zeta_y e^{-w} \sum_{P^+(m)\leqslant y} \frac{1}{m} = e^{-w}.$$

When $m > \sqrt{x}$, we apply the No Small Prime Factors Theorem (Theorem 3.4) part (ii), which implies the less precise bound $\Phi(x/m, y) \ll \frac{x/m}{\log y}$ when $m \leqslant x/y$. When $x/y < m \leqslant x$, $\Phi(x/m, y) = 1$ and when $m > x$, $\Phi(x/m, y) = 0$. Also, by Mertens' bound, $\zeta_y \ll \frac{1}{\log y}$. Therefore

$$\left|\frac{1}{\lfloor x\rfloor}\Phi\left(\frac{x}{m}, y\right) - \frac{1}{m}\zeta_y\right| \ll \frac{1}{m \log y} + \frac{\mathbf{1}(m \leqslant x)}{x}.$$

We sum over m, using the Smooth Number Theorem and partial summation:

$$\sum_{\substack{P^+(m)\leqslant y\\ m>\sqrt{x}}} \frac{1}{m} \leqslant \int_{\sqrt{x}}^{\infty} \frac{\Psi(t, y)}{t^2}\, dt \ll \int_{\sqrt{x}}^{\infty} t^{-1} e^{-\frac{\log t}{2\log y}}\, dt \ll (\log y)(\sqrt{x})^{-\frac{1}{2\log y}} \leqslant (\log y)e^{-1.5w}.$$

Therefore,

$$\sum_{\substack{P^+(m)\leqslant y\\ m>\sqrt{x}}} \left|\frac{1}{\lfloor x\rfloor}\Phi\left(\frac{x}{m}, y\right) - \frac{1}{m}\zeta_y\right| \ll \frac{\Psi(x, y)}{x} + e^{-1.5w} \ll e^{-1.5w},$$

and this completes the proof. □

We next use the Kubilius model to show that prime factors have an approximate Poisson distribution. There are two complications. First, as with permutations, large prime factors (those $> x^c$ for some fixed $c > 0$) cannot be Poisson distributed because they are highly dependent on each other, and the number of such factors is limited (trivially bounded by $1/c$). Secondly, and unlike the case of permutations, the small prime factors also cannot be Poisson distributed (that is, as $x \to \infty$). Take the case $\omega(n, 2)$, which equals 0 or 1, each with probability tending to $\frac{1}{2}$ as $x \to \infty$. Likewise, for fixed t, $\omega(n, t)$ takes only finitely many values and thus cannot approach a Poisson limit as $x \to \infty$. Hence, in the result stated below, the Poisson approximation reveals itself only when "intermediate prime factors" of n are dominant, that is, those in an interval $(y, z]$ where $y \to \infty$ and $\frac{\log z}{\log x} \to 0$ as $x \to \infty$. For each prime p, let Y_p be the Bernouilli random variable which equals

$$Y_p = \mathbf{1}(X_p \geqslant 1).$$

This models when a random integer is divisible by p (ignoring the power of p). For a set T of primes, denote

$$U_T = \sum_{p\in T} Y_p,$$

which, in the Kubilius model, is a model for $\omega(n; T)$.

THEOREM 4.7 (KUBILIUS TO POISSON). *Let T be a subset of the primes. We have*

$$\mathbb{P}\left(U_T = k\right) - \mathbb{P}(Z_T = k) \ll \begin{cases} R_T e^{-H(T)} \frac{H(T)^k}{k!}\left(\frac{1}{k+1} + \left(\frac{k-H(T)}{H(T)}\right)^2\right) & \text{if } 0 \leqslant k \leqslant 2H(T) \\ R_T \frac{e^{H(T)}}{2^k} & \text{if } k > 2H(T), \end{cases}$$

where

$$R_T = \sum_{p\in T} \frac{1}{p^2}.$$

Consequently,

$$d_{TV}(U_T, Z_T) \ll \frac{R_T}{\max(1, H(T))}.$$

PROOF. We work with moment generating functions. For brevity, write $R = R_T$ and $H = H(T)$. For any complex w,

$$\mathbb{E}\, w^{Z_T} = e^{(w-1)H}$$

and if $|w-1| \leqslant 1.9\min(T)$ we have

$$\mathbb{E}\, w^{U_T} = \prod_{p\in T}\left(1 + \frac{w-1}{p}\right) = \exp\Big\{(w-1)H + O(|w-1|^2 R)\Big\}. \tag{4.6}$$

First, suppose that T does not contain 2 or 3. Then, for any $0 < r \leqslant 2$,

$$\begin{aligned}
\mathbb{P}(U_T = k) - \mathbb{P}(Z_T = k) &= \frac{1}{2\pi i}\oint\limits_{|w|=r} \frac{\mathbb{E}\, w^{U_T} - \mathbb{E}\, w^{Z_T}}{w^{k+1}}\, dw \\
&= \frac{1}{r^k}\int_0^1 e(-k\theta)\Big[\mathbb{E}\,(re(\theta))^{U_T} - \mathbb{E}\,(re(\theta))^{Z_T}\Big]\, d\theta \\
&= \frac{1}{r^k}\int_0^1 e(-k\theta)e^{(re(\theta)-1)H}\Big[e^{O(|re(\theta)-1|^2 R)} - 1\Big]\, d\theta \\
&\ll \frac{R}{r^k}\int_0^{1/2} |re(\theta)-1|^2 e^{(r\cos(2\pi\theta)-1)H}\, d\theta.
\end{aligned}$$

Now, for $0 \leqslant \theta \leqslant \frac{1}{2}$,

$$r\cos(2\pi\theta) - 1 = r - 1 - 2r\sin^2(\pi\theta) \leqslant r - 1 - 8r\theta^2$$

and

$$|re(\theta)-1|^2 = (r - 1 - 2r\sin^2(\pi\theta))^2 + \sin^2(2\pi\theta) \ll (r-1)^2 + \theta^2,$$

so we obtain

$$\mathbb{P}(U_T = k) - \mathbb{P}(Z_T = k) \ll R\frac{e^{(r-1)H}}{r^k}\int_0^{1/2} ((r-1)^2 + \theta^2)e^{-8r\theta^2 H}\, d\theta.$$

If $T \cap \{2,3\} \neq \emptyset$, then there is a potential problem with the factors in (4.6) corresponding to $p \in \{2,3\}$ when θ is away from 0. Thus, when $\frac{1}{8} \leqslant \theta \leqslant \frac{7}{8}$, we argue crudely:

$$\mathbb{E}\,(re(\theta))^{U_T} \ll \prod_{\substack{p\in T\\ p>3}} \Big|1 + \frac{re(\theta)-1)}{p}\Big| \ll e^{\Re(re(\theta)-1)} \ll e^{(r/\sqrt{2}-1)}$$

and likewise $\mathbb{E}\,(re(\theta))^{Z_T} = e^{(re(\theta)-1)} \ll e^{(r/\sqrt{2}-1)}$. In this case $R_T \gg 1$, and so in either case we obtain

$$\mathbb{P}(U_T = k) - \mathbb{P}(Z_T = k) \ll R\frac{e^{(r-1)H}}{r^k}\left[\int_0^{1/2} ((r-1)^2 + \theta^2)e^{-8r\theta^2 H}\, d\theta + e^{-0.2rH}\right]. \tag{4.7}$$

When $k = 0$, let $r \to 0^+$ in (4.7) and we obtain the desired bound $O(R_T e^{-H})$. When $1 \leqslant k \leqslant 2H$, we take $r = k/H$ in (4.7) and obtain

$$\begin{aligned}
\mathbb{P}(U_T = k) - \mathbb{P}(Z_T = k) &\ll R\frac{H^k}{k!}e^{k-H}\left(\frac{(k/H-1)^2}{k^{1/2}} + \frac{1}{k^{3/2}} + e^{-0.2k}\right) \\
&\ll R\frac{e^H H^k}{k!}\left(\left(\frac{k-H}{H}\right)^2 + \frac{1}{k}\right).
\end{aligned}$$

When $k > 2H$, take $r = 2$ in (4.7), use $O(1)$ as a trivial bound for the integral, and conclude that

$$PR(U_T = k) - \mathbb{P}(Z_T = k) \ll \frac{Re^H}{2^k}.$$

To prove the last claim, consider two cases. First, if $H \leqslant 1$, we have

$$\sum_{k \geqslant 0} |PR(U_T = k) - \mathbb{P}(Z_T = k)| \ll R_T + \sum_{k > 2H} R_T 2^{-k} \ll R_T.$$

If $H > 1$, we have

$$\sum_{k > 2H} |PR(U_T = k) - \mathbb{P}(Z_T = k)| \ll R_T \sum_{k > 2H} \frac{e^H}{2^k} \ll \frac{R}{(4/\mathrm{e})^H}.$$

Heuristically, $e^{-H} H^k/k!$ is large only for $|k - H| \ll \sqrt{H}$, thus the other terms should sum to $O(1/H)$. To make this rigorous, write $(k-H)^2 = k(k-1) + k - 2kH + H^2$ and get that

$$\begin{aligned}
\sum_{k \leqslant 2H} |PR(U_T = k) - \mathbb{P}(Z_T = k)| &\ll R_T e^{-H} \sum_{k=0}^{\infty} \frac{H^k}{k!} \left[\frac{1}{k+1} + \left(\frac{k-H}{H} \right)^2 \right] \\
&= R_T e^{-H} \sum_{k=0}^{\infty} \left[\frac{H^k}{(k+1)!} + \frac{H^{k-2}}{(k-2)!} + \frac{H^{k-2}}{(k-1)!} - 2\frac{H^{k-1}}{(k-1)!} + \frac{H^k}{k!} \right] \\
&= R_T e^{-H} \left(\frac{e^H - 1}{H} + e^H + \frac{e^H}{H} - 2e^H + e^H \right) \ll \frac{R_T}{H}.
\end{aligned}$$

□

REMARK 4.8. The bound in Theorem 4.7 is good as long as $R_T \to 0$ or $H(T) \to \infty$.

We can use Theorem 4.7 to deal with prime factors in an arbitrary collection of subsets, by a simple combinatorial device. The following is a consequence of Exercise 4.1.

COROLLARY 4.9. *Let $T_1, \dots, T_m$ be disjoint sets of primes. Then*

$$d_{TV}\left((U_{T_1}, \dots, U_{T_m}), (Z_{T_1}, \dots, Z_{T_m})\right) \ll \sum_{j=1}^{m} \frac{R_{T_j}}{\max(1, H(T_j))}.$$

Combining this Corollary with the Kubilius model (Thm. 4.6), we conclude that the "intermediate" (not too small and not too large) prime factors of an integer are "Poisson distributed".

3. Central Limit Theorems

It is well-known that, as $\lambda \to \infty$ that $\mathrm{Pois}(\lambda)$ approaches a Gaussian distribution. This is a special case of the Central Limit Theorem. Below we record a quantitative version with explicit error term, and provide an elementary proof.

PROPOSITION 4.10 (POISSON CLT). *Uniformly for real $\lambda \geqslant 1$, $X \stackrel{d}{=} \mathrm{Pois}(\lambda)$, and real z, we have*

$$\mathbb{P}\left(X \leqslant \lambda + z\sqrt{\lambda} \right) = \Phi(z) + O\left(\lambda^{-1/2} \right),$$

where

$$\Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-\frac{1}{2}t^2}\, dt$$

is the distribution function of the standard Gaussian distribution.

PROOF. Let $h^* = 3\sqrt{\lambda \log(1+\lambda)}$. First observe that by the Poisson Tails Proposition 1.11 and the crude bounds for $Q(x)$ (1.14), we have

$$\mathbb{P}(|X-\lambda| > h^*) \leqslant 2e^{-3\log(1+\lambda)} = \frac{2}{(1+\lambda)^3}.$$

Likewise,

$$\int\limits_{|t|>3\sqrt{\log(1+\lambda)}} e^{-\frac{1}{2}t^2}\, dt \ll \frac{1}{(1+\lambda)^3}. \tag{4.8}$$

Consequently, we may assume that $|z| \leqslant h^*$, and deduce

$$\mathbb{P}\left(X \leqslant \lambda + z\sqrt{\lambda}\right) = e^{-\lambda} \sum_{\lambda - h^* \leqslant k \leqslant \lambda + z\sqrt{\lambda}} \frac{\lambda^k}{k!} + O\left(\frac{1}{\lambda^3}\right).$$

For $|k-\lambda| \leqslant h^*$, Stirling's formula implies that

$$k! = \left(\frac{k}{\mathrm{e}}\right)^k \sqrt{2\pi\lambda}\left(1 + O\left(\frac{|k-\lambda|}{\lambda}\right)\right).$$

Write $k = \lambda + u$. Then, for $|u| \leqslant h^*$, we have

$$\begin{aligned} e^{-\lambda}\frac{\lambda^k}{k!} &= \frac{1+O\left(\frac{|u|+1}{\lambda}\right)}{\sqrt{2\pi\lambda}} e^{-\lambda}\left(\frac{e\lambda}{\lambda+u}\right)^{\lambda+u} = \frac{1+O\left(\frac{|u|+1}{\lambda}\right)}{\sqrt{2\pi\lambda}} \frac{e^u}{(1+u/\lambda)^{\lambda+u}} \\ &= \frac{1+O\left(\frac{|u|+1}{\lambda}\right)}{\sqrt{2\pi\lambda}} \exp\left\{u - (\lambda+u)\left(\frac{u}{\lambda} - \frac{1}{2}\left(\frac{u}{\lambda}\right)^2 + O\left(\left(\frac{u}{\lambda}\right)^3\right)\right)\right\} \\ &= \left(1 + O\left(\frac{1+|u|}{\lambda} + \frac{1+|u|^3}{\lambda^3}\right)\right)\frac{e^{-\frac{u^2}{2\lambda^2}}}{\sqrt{2\pi\lambda}}. \end{aligned}$$

It follows that

$$e^{-\lambda} \sum_{\lambda - h^* \leqslant k \leqslant \lambda + z\sqrt{\lambda}} \frac{\lambda^k}{k!} = M + E,$$

where the "main term" M satisfies

$$M = \frac{1}{\sqrt{2\pi\lambda}} \sum_{\lambda - h^* \leqslant k \leqslant \lambda + z\sqrt{\lambda}} e^{-\frac{(k-\lambda)^2}{2\lambda}}$$

and the "error term" E satisfies

$$\begin{aligned} E &\ll \frac{1}{\sqrt{\lambda}} \sum_k \left(\frac{1+|k-\lambda|}{\lambda} + \frac{|k-\lambda|^3}{\lambda^3}\right) e^{-\frac{|k-\lambda|^2}{2\lambda}} \\ &\ll \sum_{a=1}^{\infty} \left(\frac{a}{\sqrt{\lambda}} + \frac{a^3}{\lambda^{3/2}}\right) e^{-(a-1)^2/2} \ll \frac{1}{\sqrt{\lambda}}. \end{aligned}$$

By Euler summation, the main term satisfies

$$M = \frac{1}{\sqrt{2\pi\lambda}}\left[\int_{\lambda-h^*}^{\lambda+z\sqrt{\lambda}} e^{-\frac{(t-\lambda)^2}{2\lambda}}\, dt - \int_{\lambda-h^*}^{\lambda+z\sqrt{\lambda}} \{t\}\left(\frac{t-\lambda}{\lambda}\right) e^{-\frac{(t-\lambda)^2}{2\lambda}}\, dt + O(1)\right].$$

similar to the estimation of E, the integral involving $\{t\}$ is $O(1)$. The first equals, by (4.8),

$$\sqrt{\lambda}\int_{-3\sqrt{\log(1+\lambda)}}^{z} e^{-\frac{1}{2}u^2}\, du = \sqrt{\lambda}\int_{-\infty}^{z} e^{-\frac{1}{2}u^2}\, du + O(\lambda^{-5/2}),$$

and hence

$$M = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-\frac{1}{2}u^2}\, du + O\left(\frac{1}{\sqrt{\lambda}}\right) = \Phi(z) + O\left(\frac{1}{\sqrt{\lambda}}\right).$$

The proof is complete. □

COROLLARY 4.11 (CYCLES CLT). *Let $I \subset [k]$ with $k \leqslant n$. For any real u,*

$$\mathbb{P}\left(C_{I(\sigma)} \leqslant H(I) + u\sqrt{H(I)}\right) = \Phi(u) + O\left(\frac{1}{\sqrt{H(I)}} + e^{-n/k}\right).$$

PROOF. Combine the Poisson cycles theorem (Theorem 4.4) for a single set and the Poisson CLT theorem (Theorem 4.10). □

We remark that this is only useful when $H(I)$ is large (otherwise $C_I(\sigma)$ is expected to have Poisson distribution with small parameter, and this cannot be approximated by a Gaussian), and when n/k is large. When n/k is small, we may also prove a CLT, provided that the large cycles are "negligible". We illustrate this in the case $I = [n]$. The following is a theorem of Goncharov [**Gon44**].

THEOREM 4.12 (CLT FOR ALL CYCLES). *Let $n \geqslant 100$ and $w \in \mathbb{R}$. Then*

$$P\left(C(\sigma) \leqslant \log n + w\sqrt{\log n}\right) = \Phi(w) + O\left(\frac{\log_2 n}{\sqrt{\log n}}\right).$$

PROOF. Let $A = \log n + w\sqrt{\log n}$, and take $m = \left\lceil \frac{n}{\log_2 n} \right\rceil$. Clearly

$$\mathbb{P}(C(\sigma) \leqslant A) \leqslant C(C_{[m]}(\sigma) \leqslant A).$$

Because $H_m = \log n - \log_3 n + O(1)$, we have

$$A = \log n + w\sqrt{\log n} = H_m + w'\sqrt{H_m}, \quad w' = w + O\left(\frac{\log_3 n}{\sqrt{\log n}}\right).$$

Thus, by the Cycles CLT (Theorem 4.11),

$$\begin{aligned}
\mathbb{P}(C(\sigma) \leqslant A) &\leqslant \mathbb{P}(C_{[m]}(\sigma) \leqslant A) \\
&= \Phi(w') + O\left(H_m^{-1/2} + e^{-n/m}\right) \\
&= \Phi(w') + O(1/\log n) \\
&= \Phi(w) + O\left(\frac{\log_3 n}{\sqrt{\log n}}\right).
\end{aligned}$$

We also have

$$A - \log_2 n = H_m + w''\sqrt{H_m}, \quad w' = w + O\left(\frac{\log_2 n}{\sqrt{\log n}}\right)$$

and it follows from the Cycles CLT (Theorem 4.11) and the upper bound $C_{(m,n]}(\sigma) \leqslant n/m \leqslant \log_2 n$ that

$$\begin{aligned}
\mathbb{P}(C(\sigma) \leqslant A) &\geqslant \mathbb{P}\left(C_{[m]}(\sigma) \leqslant A - \log_2 n \text{ and } C_{(m,n]}(\sigma) \leqslant \log_2 n\right) \\
&= \mathbb{P}\left(C_{[m]}(\sigma) \leqslant A - \log_2 n\right) \\
&= \Phi(w'') + O(1/\log n) \\
&= \Phi(w) + O\left(\frac{\log_2 n}{\sqrt{\log n}}\right).
\end{aligned}$$

The theorem follows by combining the upper and lower bounds. □

THEOREM 4.13 (PRIME FACTORS CLT). *Let $1 \leqslant y \leqslant x$ and suppose that T is a subset of the primes in $[2, x]$. For any real w,*

$$\mathbb{P}_x\left(\omega(n,T) \leqslant H(T) + w\sqrt{H(T)}\right) = \Phi(w) + O\left(e^{-\frac{1}{6}\frac{\log x}{\log y}} + H(T)^{-1/2}\right).$$

PROOF. Assume $H(T) \geqslant 2$, else there is nothing to prove. As $\omega(n,T)$ is a function only of the variables v_p for $p \in T$, and the Kubilius model is U_T, it follows from the Kubilius model Theorem (Thm. 4.6) that

$$\left|\mathbb{P}_x\left(\omega(n,T) \leqslant H(T) + w\sqrt{H(T)}\right) - \mathbb{P}(U_T \leqslant H(T) + w\sqrt{H(T)})\right| \ll e^{-\frac{1}{6}\frac{\log x}{\log y}}.$$

The proof is completed upon invoking the Kubilius to Poisson Theorem (Thm. 4.7) and the Poisson CLT Theorem (Thm. 4.10), noting that $R_T \ll 1$. □

We remark that the error term $H(T)^{-1/2}$ is best possible; in fact, it may be replaced by an asymptotic expansion in powers of $H(T)^{-1/2}$; this is a consequence of a general theory of CLT-type expansions for sums of random variables; see [**GK68**].

As with cycles of permutations, we may extend this to handle the distribution of *all* prime factors of integers, or any function $\omega(n,T)$ where the large prime factors contribute 'negligibly'. The following is a quantitative version of the famous theorem of Erdős and Kac [**EK40**].

THEOREM 4.14 (CLT FOR ALL PRIME FACTORS). *For any real w,*

$$\mathbb{P}_x\left(\omega(n) \leqslant \log_2 x + w\sqrt{\log_2 x}\right) = \Phi(w) + O\left(\frac{\log_3 x}{(\log_2 x)^{1/2}}\right).$$

PROOF. Let $A = \log_2 x + w\sqrt{\log_2 x}$, and let $y = x^{1/(6\log_3 x)}$. We have

$$\log_2 y = \log_2 x - \log_4 x - \log 6$$

and thus

$$A = \log_2 y + w'\sqrt{\log_2 y}, \quad w' = w + O\left(\frac{\log_4 x}{(\log_2 x)^{1/2}}\right).$$

It follows from the Prime Factors CLT (Thm 4.13) that

$$\begin{aligned}\mathbb{P}_x(\omega(n) \leqslant A) &\leqslant \mathbb{P}_x(\omega(n,y) \leqslant A)\\ &\leqslant \Phi(w') + O\left(\frac{1}{(\log_2 y)^{1/2}} + e^{-\frac{1}{6}\frac{\log x}{\log y}}\right)\\ &= \Phi(w) + O\left(\frac{\log_4 x}{(\log_2 x)^{1/2}}\right).\end{aligned}$$

On the other hand, we have

$$A - 6\log_3 x = \log_2 y + w''\sqrt{\log_2 y}, \quad w'' = w + O\left(\frac{\log_3 x}{(\log_2 x)^{1/2}}\right)$$

and it follows from the Prime Factors CLT (Thm 4.13) that

$$\begin{aligned}\mathbb{P}_x(\omega(n) \leqslant A) &\geqslant \mathbb{P}_x\left(\omega(n,y) \leqslant A - 6\log_3 x \text{ and } \omega(n,(y,x]) \leqslant 6\log_3 x\right)\\ &= \mathbb{P}_x\left(\omega(n,y) \leqslant A - 6\log_3 x\right)\\ &= \Phi(w'') + O\left(\frac{1}{(\log_2 x)^{1/2}}\right)\\ &= \Phi(w) + O\left(\frac{\log_3 x}{(\log_2 x)^{1/2}}\right).\end{aligned}$$

Combining the upper and lower bounds completes the proof. □

REMARK 4.15. An error term of $O((\log_2 x)^{-1/2})$ in Theorem 4.14 is best possible (cf. work of Rényi-Turán, Delange and Kubilius in the late 1950s/early 1960s)

4. Exercises

EXERCISE 4.1. (a)Prove that if $X_1, \dots, X_m$ are independent discrete random variables, and $Y_1, \dots, Y_m$ are independent discrete random variables (with Y_j having the same domain as X_j), then

$$d_{TV}((X_1, \dots, X_m), (Y_1, \dots, Y_m)) \leqslant \sum_{j=1}^{m} d_{TV}(X_j, Y_j).$$

(b) Let $X_j \stackrel{d}{=} \mathrm{Pois}(\lambda_j)$ for $1 \leqslant j \leqslant m$, where $0 < \lambda_j \leqslant 1$ for each j. Also suppose that Y_j is a Bernouilli random variable, with $\mathbb{P}(Y_j = 0) = 1 - \lambda_j$, $\mathbb{P}(Y_j = 1) = \lambda_j$ for each j. Show that

$$d_{TV}((X_1, \dots, X_m), (Y_1, \dots, Y_m)) \ll \sum_{j=1}^{m} \lambda_j^2.$$

EXERCISE 4.2. (a) Let $b \mod q$ be a *fixed* arithmetic progression, and let n be large (in terms of q). Prove a central limit theorem for $C_T(\sigma)$, where $T = [n] \cap (b \mod q)$, that is, for the set of cycles of σ whose lengths are $\equiv b \pmod q$.

(b) Let $b \mod q$ be a *fixed* arithmetic progression, with $(b, q) = 1$, and let x be large (in terms of q). Prove a central limit theorem for $\omega(n; T)$, where T is the set of primes that are $\leqslant x$ and in the progression $b \mod q$. You may use standard tools from the theory of primes in progressions (Mertens' theorems for primes in progressions, for example).

Bibliography

[AT92] Richard Arratia and Simon Tavaré. The cycle structure of random permutations. *Ann. Probab.*, 20(3):1567–1591, 1992.

[EK40] P. Erdös and M. Kac. The Gaussian law of errors in the theory of additive number theoretic functions. *Amer. J. Math.*, 62:738–742, 1940.

[Erd55] P. Erdős. Some remarks on number theory. *Riveon Lematematika*, 9:45–48, 1955. (Hebrew. English summary).

[Erd60] P. Erdős. An asymptotic inequality in the theory of numbers. *Vestnik Leningrad. Univ.*, 15(13):41–49, 1960. (Russian).

[FH00] Kevin Ford and H. Halberstam. The Brun-Hooley sieve. *J. Number Theory*, 81(2):335–350, 2000.

[For08] K. Ford. The distribution of integers with a divisor in a given interval. *Ann. Math.*, pages 367–433, 2008.

[GK68] B. V. Gnedenko and A. N. Kolmogorov. *Limit distributions for sums of independent random variables*. Translated from the Russian, annotated, and revised by K. L. Chung. With appendices by J. L. Doob and P. L. Hsu. Revised edition. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills., Ont., 1968.

[Gon44] V. Gontcharoff. Du domaine de l'analyse combinatoire. *Bull. Acad. Sci. URSS Sér. Math. [Izvestia Akad. Nauk SSSR]*, 8:3–48, 1944.

[Gra06] Andrew Granville. Cycle lengths in a permutation are typically Poisson. *Electron. J. Combin.*, 13(1):Research Paper 107, 23, 2006.

[HT88] R. R. Hall and G. Tenenbaum. *Divisors*, volume 90 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1988.

[MT84] H. Maier and G. Tenenbaum. On the set of divisors of an integer. *Invent. Math.*, 76(1):121–128, 1984.

[Pet16] Robertas Petuchovas. *ASYMPTOTIC ANALYSIS OF THE CYCLIC STRUCTURE OF PERMUTATIONS*. PhD thesis, Vilnius University, 2016. arXiv: 1611.02934.

[Pom89] Carl Pomerance. Two methods in elementary analytic number theory. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 135–161. Kluwer Acad. Publ., Dordrecht, 1989.

[Ran38] Robert Rankin. The difference between consecutive prime numbers. *J. London Math. Soc.*, 13:242–247, 1938.

[Ten99] Gérald Tenenbaum. Crible d'ératosthène et modèle de Kubilius. In *Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997)*, pages 1099–1129. de Gruyter, Berlin, 1999.

[Ten15] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion.

[Tud96] Christian Tudesq. Majoration de la loi locale de certaines fonctions additives. *Arch. Math. (Basel)*, 67(6):465–472, 1996.