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
Email address: ford@math.uiuc.edu

Contents

CHAPTER 0

Background material and notation

1. Notation

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

Permutation notation

- $\mathcal{S}_n$ is the permutation group on a set of n objects (we don't care what the objects are)
- $C_j(\sigma)$ 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
- $\beta|\sigma$ 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.

Order of magnitude notation (Bachman-Landau, Hardy, Vinogradov)

- The 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. Equivalently, there are positive constants $C<C'$ such that $Cg\leqslant f\leqslant C'g$ throughout the domain of f.
- $f\sim g$ as $x\to a$ means $\lim_{x\to a} f(x)/g(x)=1$. Here a can be finite, ∞ or $-\infty$.
- $f=o(g)$ as $x\to a$ means $\lim_{x\to a} f(x)/g(x)=0$. Here a can be finite, ∞ or $-\infty$.

Probability

- $\mathbb{P}(X)$ 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
- Pois(λ) is a Poisson random variable with parameter λ

General notational conventions

- $\mathbb{N} = \{1, 2, 3, \ldots\}$, 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 $\leqslant x$.
- $\lceil x \rceil$ is the least integer which is $\geqslant x$.
- $\mathbb{1}(S)$ is the indicator function of statement S; $\mathbb{1}(S) = 1$ if S is true, and $\mathbb{1}(S) = 0$ if S is false.
- $H_n = 1 + 1/2 + \cdots + 1/n$ is the n-th harmonic sum
- $H(I) = \sum_{i \in I} 1/i$ is a general harmonic sum, where $I \subset \mathbb{N}$
- Variables in boldface type, e.g. $\mathbf{h}$, usually denote vector quantities.
- A statement for "almost all integers" means that the number of exceptions below x is $o(x)$ as $x \to \infty$.
- The symbols p, q denote primes unless otherwise noted
- The symbols k, l, m, n denote integers unless otherwise noted

2. Basic summation estimates

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* $\gamma = 0.57721566\ldots$ *is Euler's constant.*

Stirling's formula. *We have the asymptotic (Stirling's formula)*

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

and the strict inequalities

$$1 \leqslant \frac{n!}{\sqrt{2\pi n}(n/\mathrm{e})^n} \leqslant \mathrm{e}^{1/(12n)} \leqslant 1 + \frac{1}{10n} \qquad (n \in \mathbb{N}). \tag{0.1}$$

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.

Roughly speaking, the sum of $f(n)$ is approximated by the corresponding integral of $f(t)$.

Abel summation, also called partial 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*

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

3. 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) $f(1) = 1$. A function is *completely multiplicative* if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$. Important examples include powers n^c (c fixed), $\tau(n)$, the number of positive divisors

of n, Euler's totient function $\phi(n)$, and the Möbius function $\mu(n)$. Clearly, the product and quotient of multiplicative functions is also multiplicative, as is any fixed power of a multiplicative function.

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

$$\sum_{d|n} f(d) = \prod_{p^a \| n} \left(1 + f(p) + f(p^2) + \cdots + f(p^a)\right), \tag{0.2}$$

and an "infinite version"

$$\sum_{d : p|d \implies p \in T} f(d) = \prod_{p \in T} \left(1 + f(p) + f(p^2) + \cdots\right), \tag{0.3}$$

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

$$\sum_{d : p|d \implies p \in T} \frac{1}{d} = \prod_{p \in T} \left(1 - \frac{1}{p}\right)^{-1}. \tag{0.4}$$

Möbius inversion and the Legendre sieve. The Möbius function encodes a number-theoretic version of inclusion-exclusion. For any finite set of primes with product P, and any set $\mathcal{A}$ of positive integers

$$\#\{n \in \mathcal{A} : (n, P) = 1\} = \sum_{d|P} \mu(d) \#\{n \in \mathcal{A} : d|n\}.$$

An arithmetic function f is **additive** if $f(ab) = f(a) + f(b)$ whenever $(a, b) = 1$. A function is *completely additive* if $f(ab) = f(a) + f(b)$ for all $a, b, \in \mathbb{N}$.

Examples include

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

4. Prime number estimates

Throughout, p denotes a prime number.

Prime Number Theorem (PNT).

$$\pi(x) := \#\{p \leqslant x\} = \int_2^x \frac{dt}{\log t} + O\left(x \mathrm{e}^{-\sqrt{\log x}}\right).$$

Also,

$$\sum_{p \leqslant x} \log p = x + O\left(x \mathrm{e}^{-\sqrt{\log x}}\right).$$

We also have the asymptotic

$$\int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + O\left(\frac{x}{\log x}\right).$$

Two consequences are:

Mertens' estimates with strong error terms. *For some constants c_1, c_2 we have*

$$\sum_{p \leqslant x} \frac{1}{p} = \log\log x + c_1 + O\left(\mathrm{e}^{-\sqrt{\log x}}\right), \tag{0.5}$$

$$\sum_{p \leqslant x} \frac{\log p}{p} = \log x + c_2 + O\left(\mathrm{e}^{-\sqrt{\log x}}\right), \tag{0.6}$$

and

$$\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)=\frac{\mathrm{e}^{-\gamma}}{\log x}\left(1+O\left(\mathrm{e}^{-\sqrt{\log x}}\right)\right). \tag{0.7}$$

The original Mertens' estimates had error terms $O(1/\log x)$, and this weak form is sufficient in most of our applications. The best-known form of the error terms above take the form $\exp\{-c(\log x)^{3/5}(\log_2 x)^{-1/5}\}$ for some constant $c>0$.

Oftentimes the more crude bounds of Chebyshev suffice: for positive constants c, c' we have

$$\frac{cx}{\log x}\leqslant \#\{p\leqslant x\}\leqslant \frac{c'x}{\log x}\qquad (x\geqslant 2).$$

The Prime Number Theorem also implies that

$$p_n\sim n\log n\qquad (n\to\infty),$$

where p_n is the n-th smallest prime.

There are similar bounds for primes in a fixed arithmetic progression. Here we fix $1\leqslant a\leqslant b$ with $(a,b)=1$.

Prime number theorem for arithmetic progressions. *We have*

$$\#\{p\leqslant x: p\equiv a \pmod b\}\sim \frac{x}{\phi(b)\log x}\qquad (x\to\infty)$$

There are results which are uniform in b, but they are more complicated to state. We refer the reader to [**10**] for specifics.

Mertens' estimates for primes in arithmetic progressions. *For some constants $c_1(a,b)$ and $c_2(a,b)>0$ we have*

$$\sum_{\substack{p\leqslant x\\ p\equiv a \pmod b}}\frac{1}{p}=\frac{\log\log x}{\phi(b)}+c_1(a,b)+O_b(1/\log x) \tag{0.8}$$

and

$$\prod_{\substack{p\leqslant x\\ p\equiv a \pmod b}}\left(1-\frac{1}{p}\right)=\frac{c_2(a,b)}{(\log x)^{1/\phi(b)}}\left(1+O_b\left(1/\log x\right)\right). \tag{0.9}$$

5. Inclusion-Exclusion

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

Inclusion-exclusion. *Let a be a non-negative integer. Then, for any $k\in\mathbb{N}$,*

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

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 0.1. *Let T be a finite set of positive real numbers, and $k \in \mathbb{N}$. Then*

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

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

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

6. Probability estimates: general

All random variables lie in $\mathbb{R}$, most are non-negative.

Markov's inequality. *We have* $\mathbb{P}(X \geqslant w) \leqslant \dfrac{\mu}{w}, \qquad \mu = \mathbb{E}\, X > 0, w > 0.$

Two easy consequences are Chebyshev's inequality for variances and Chernoff's inequality.

Chebyshev's inequality. *If $w > 0$, $\mu = \mathbb{E}\, X$ and $\mathbb{E}\,|X-\mu|^2 > 0$, then*

$$\mathbb{P}\big(|X-\mu| \geqslant w\sqrt{\mathbb{E}\,|X-\mu|^2}\big) \leqslant \frac{1}{w^2}.$$

Chernoff's inequality. *We have*

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

and

$$\mathbb{P}\,(X \leqslant w) \leqslant \inf_{b\leqslant 0} \frac{\mathbb{E}\,\mathrm{e}^{bX}}{\mathrm{e}^{bw}}.$$

7. Probability estimates: Poisson random variables

The first Proposition lists basic properties of the Poisson distribution, which are readily verified from the definition.

Proposition 0.2. *Suppose $X \stackrel{d}{=} \mathrm{Pois}(\lambda)$. Then*

$$\mathbb{E}\, X = \lambda, \tag{0.10}$$

$$\mathbb{E}\, c^X = \mathrm{e}^{(c-1)\lambda} \quad (c > 0), \tag{0.11}$$

$$\mathbb{E}\binom{X}{m} = \frac{\lambda^m}{m!} \quad (m \geqslant 0). \tag{0.12}$$

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

$$X_1 + \cdots + X_k \stackrel{d}{=} \mathrm{Pois}(\lambda_1 + \cdots + \lambda_k). \tag{0.13}$$

We also record very useful tail bounds on the Poisson distribution, due to Norton [**56**].

Proposition 0.3 (Poisson tails). *Let $X \stackrel{d}{=} \mathrm{Pois}(\lambda)$ where $\lambda > 0$. Then*

$$\mathbb{P}(X \leqslant \alpha\lambda) \leqslant \min\left(1, \frac{1}{(1-\alpha)\sqrt{\alpha\lambda}}\right) \mathrm{e}^{-Q(\alpha)\lambda} \quad (0 \leqslant \alpha \leqslant 1),$$

$$\mathbb{P}(X \geqslant \alpha\lambda) \leqslant \min\left(1, \frac{1}{(1-1/\alpha)\sqrt{2\pi\lambda\alpha}}\right) \mathrm{e}^{-Q(\alpha)\lambda} \quad (\alpha \geqslant 1),$$

where

$$Q(x) = x\log x - x + 1. \tag{0.14}$$

Proof. First, using Chernoff's inequality (with $b = \log\alpha$, $0 < \alpha \leqslant 1$) together with (0.11), we have

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

When α is bounded away from 1 we can do better. Suppose $\alpha < 1$ and let $k_0 = \lfloor\alpha\lambda\rfloor$. Then

$$\mathbb{P}(X \leqslant \alpha\lambda) = \mathrm{e}^{-\lambda} \sum_{k \leqslant k_0} \frac{\lambda^k}{k!}.$$

If $k_0 = 0$ then $Q(\alpha) \leqslant Q(0) = 1$ and $\alpha\lambda < 1$, hence

$$\frac{1}{(1-\alpha)\sqrt{\alpha\lambda}}\mathrm{e}^{-Q(\alpha)\lambda} \geqslant \mathrm{e}^{-\lambda} = \mathbb{P}(X \leqslant \alpha\lambda).$$

Now suppose $k_0 \geqslant 1$. Consecutive summands have ratio $\geqslant 1/\alpha$, and thus by (0.1) and the fact that $\lambda^x/(x/\mathrm{e})^x$ is increasing for $x \leqslant \lambda$, we have

$$\begin{aligned}
\mathbb{P}(X \leqslant \alpha\lambda) &\leqslant \frac{\mathrm{e}^{-\lambda}}{1-\alpha} \cdot \frac{\lambda^{k_0}}{k_0!} \leqslant \frac{\mathrm{e}^{-\lambda}}{1-\alpha} \cdot \frac{\lambda^{k_0}}{(k_0/\mathrm{e})^{k_0}\sqrt{2\pi k_0}} \\
&\leqslant \frac{\mathrm{e}^{-\lambda}}{1-\alpha} \cdot \frac{\lambda^{\alpha\lambda}}{(\alpha\lambda/\mathrm{e})^{\alpha\lambda}\sqrt{2\pi k_0}} = \frac{\mathrm{e}^{-Q(\alpha)\lambda}}{1-\alpha} \cdot \frac{1}{\sqrt{2\pi k_0}} \\
&\leqslant \frac{\mathrm{e}^{-Q(\alpha)\lambda}}{1-\alpha} \cdot \frac{1}{\sqrt{\pi\alpha\lambda}},
\end{aligned}$$

which concludes the proof of the first inequality.

A second application of Chernoff's inequality (again with $b = \log\alpha$, $\alpha \geqslant 1$) and (0.11) yields

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

Now assume $\alpha > 1$ and write $k_1 = \lceil\alpha\lambda\rceil$. We have

$$\mathbb{P}(X \geqslant \alpha\lambda) = \mathrm{e}^{-\lambda} \sum_{k \geqslant k_1} \frac{\lambda^k}{k!}.$$

Consecutive summands have ratio $\leqslant 1/\alpha$. By (0.1) and the fact that $\lambda^x/(x/\mathrm{e})^x$ is decreasing for $x \geqslant \lambda$,

$$\mathbb{P}(X \geqslant \alpha\lambda) \leqslant \frac{1}{1-1/\alpha} \cdot \frac{\lambda^{k_1}}{k_1!} \leqslant \frac{1}{1-1/\alpha} \cdot \frac{\lambda^{k_1}}{(k_1/\mathrm{e})^{k_1}\sqrt{2\pi k_1}} \leqslant \frac{\mathrm{e}^{-Q(\alpha)\lambda}}{1-1/\alpha} \cdot \frac{1}{\sqrt{2\pi k_1}} \leqslant \frac{\mathrm{e}^{-Q(\alpha)\lambda}}{1-1/\alpha} \cdot \frac{1}{\sqrt{2\pi\alpha\lambda}}.$$

This concludes the proof of the 2nd inequality. □

Proposition 0.4 (Q bounds). *We have*

$$Q(x) = \int_1^x \log t\,dt \;\; (\textit{all } x) = \sum_{k=2}^{\infty} \frac{(-1)^k}{k(k-1)}(x-1)^k \;\; (|x-1| < 1), \tag{0.15}$$

and

$$\frac{x^2}{3} \leqslant Q(1+x) \leqslant x^2 \quad (|x| \leqslant 1). \tag{0.16}$$

Proposition 0.5 (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*

$$\mathbb{P}(X \leqslant \beta n) \leqslant \exp\left\{-n\left(\beta \log \frac{\beta}{p} + (1-\beta)\log\frac{1-\beta}{1-p}\right)\right\}. \tag{0.17}$$

Proof. For a proof, see [**3**, Lemma 4.7.2]. The right side is also an upper bound for $\mathbb{P}(X \geqslant \beta n)$ for $\beta \geqslant p$ by symmetry. □

CHAPTER 1

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

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. Prime factors and divisors

Given a random number $n \leqslant x$ and a prime p, the probability that $p|n$ is very close to $1/p$, and moreover these *events* are close to independent for different p (as long as p is "small", in a sense that will be made precise later). In particular, this heuristic suggests that the number of distinct prime factors $\omega(n)$ should be about

$$\sum_{p\leqslant x} \frac{1}{p} = \log_2 x + O(1)$$

on average, using Mertens' sum estimate (0.5). In fact, an easy calculation gives

$$\frac{1}{x}\sum_{n\leqslant x} \omega(n) = \frac{1}{x}\sum_{p\leqslant x} \lfloor x/p \rfloor = \sum_{p\leqslant x} 1/p + O(\pi(x)/x) = \log_2 x + O(1). \tag{1.1}$$

What is the *distribution* of $\omega(n)$ for $n \leqslant x$? One can model the event $p|n$, for a random $n \leqslant x$, by a Bernouilli random variable X_p, which equals 1 with probability $1/p$ and 0 with probability $1 - 1/p$. This in turn is very close to a Poisson random variable Z_p with parameter $1/p$ when p is large. Thus, $\omega(n)$ can be modeled by the random variable $\sum_{p\leqslant x} Z_p$, which is a Poisson variable with parameter $\sum_{p\leqslant x} 1/p = \log_2 x + O(1)$.

The first result in this direction is a classic theorem of Landau from 1900.

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

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

This already suggests that $\omega(n)$ has an approximate Poisson distribution, although Landau never wrote this explicitly. It was Hardy and Ramanujan in 1917 who analyzed the behavior of $\#\{n \leqslant x : \omega(n) = k\}$ uniformly in k, showing

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

$$\#\{n \leqslant x : \omega(n) = k\} \leqslant C_1 \frac{x}{\log x}\,\frac{(\log_2 x + C_2)^{k-1}}{(k-1)!},$$

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 (0.3) 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 Pois(λ) tends to the Gaussian with mean and variance λ as λ tends to infinity, Erdős and Kac proved their celebrated "Central Limit Theorem" for $\omega(n)$ in 1939:

Theorem (Erdős-Kac, 1939 [28]). For any real z,

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

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 $(\mathrm{e}^{\mathrm{e}^a}, \mathrm{e}^{\mathrm{e}^b}]$ 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 **[29]**. The solution of Problem (b), in the positive, was given by Maier and Tenenbaum in 1984 **[52]**. Problem (a) is closely related to the Erdős multiplication table problem: How many *distinct* products are there ab with $1 \leqslant a \leqslant N$ and $1 \leqslant b \leqslant N$?

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 $\sum_j jC_j = n$. Goncharov was the first to make such statements rigorous, and in 1944 proved (among other things) the following:

Theorem (Goncharov, 1944 [39]). We have

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

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 1.1 below). More recently, the Poisson model has been established in great uniformity: Namely,

$$(C_1(\sigma), C_2(\sigma), \dots, C_k(\sigma)) \approx (Z_1, Z_2, \dots, Z_k) \tag{1.2}$$

(meaning the two vectors have distributions which are very close), where $Z_1, \dots, Z_k$ are independent and $Z_j \stackrel{d}{=} \text{Pois}(1/j)$, 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 (i.e., left invariant) by σ. A fixed set corresponds to a *divisor* of σ, that 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). For example, if $\sigma \in \mathcal{S}_6$ has cycle form

$$\sigma = (1)(24)(356)$$

then, e.g., $(1)(356)$ is a divisor with corresponding fixed set $\{1, 3, 5, 6\}$. There 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 statistical group theory, such as generation of $\mathcal{S}_n$ by random permutations, the distribution of transitive subgroups of $\mathcal{S}_n$, and the order of permutations. These in turn have further applications to irreducibility of polynomials over finite fields (with applications to Galois theory) and over global fields.

Since

$$\sum_{e^k < p \leqslant e^{k+1}} \frac{1}{p} \approx \log(1 + 1/k) \approx 1/k$$

when k is large, we can form an approximate *dictionary* between statements about random permutations and the analogous statement about random integers.

Random permutation	Random integer
cycle of length k	prime factor in $(e^k, e^{k+1}]$
divisor of size k	divisor in $(e^k, e^{k+1}]$

3. Cycles and prime factors from intervals: first nibbles

With $n \in \mathbb{N}$ fixed, we consider a random permutation $\sigma \in \mathcal{S}_n$, each permutation occurring with probability $1/n!$. Probability and Expectation with respect to this probability space will be denoted $\mathbb{P}_{\sigma \in \mathcal{S}_n}$ and $\mathbb{E}_{\sigma \in \mathcal{S}_n}$. If the value of n is understood, then often these are abbreviated as $\mathbb{P}_\sigma$ and $\mathbb{E}_\sigma$.

Recall that $C_j(\sigma)$ is the number of cycles of size j in the permutation σ.

The following lemma appears in Watterson [**69**, Theorem 7].

Lemma 1.1 (Cycle length lemma). *Let $m_1, \dots, m_n$ be non-negative integers with*

$$m_1 + 2m_2 + \cdots + nm_n \leqslant n.$$

Then

$$\mathbb{E}_{\sigma \in \mathcal{S}_n} \prod_{j=1}^{n} \binom{C_j(\sigma)}{m_j} = \prod_{j=1}^{n} \frac{(1/j)^{m_j}}{m_j!}.$$

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

Proof. The second assertion is obvious, since the product on the left side is positive if and only if $C_j(\sigma) \geqslant m_j$ for all j, and since $\sum_j jC_j(\sigma) = n$ this implies that $\sum jm_j \leqslant n$. Now assume that $m_1 + 2m_2 + \cdots + nm_n \leqslant n$. The product on the left side in the lemma equals the number of ways to choose from $[n]$ a disjoint collection of m_1 1-cycles, m_2 2-cycles, ..., m_n n-cycles. 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

$$\binom{n}{\underbrace{1\cdots1}_{m_1}\underbrace{2\cdots2}_{m_2}\cdots\underbrace{n\cdots n}_{m_n}\, t} \frac{1}{m_1!\cdots m_n!} = \frac{n!/t!}{\prod_{j=1}^{n}(j!)^{m_j} m_j!},$$

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. Multiplying these quantities together completes the proof. □

We remark that the RHS in Lemma 1.1 equals

$$\prod_{j=1}^{n} \frac{(1/j)^{m_j}}{m_j!} = \mathbb{E} \prod_{j=1}^{n} \binom{Z_j}{m_j},$$

where $Z_j \stackrel{d}{=} \mathrm{Pois}(1/j)$ and $Z_1, \ldots, Z_n$ are independent. This already suggests that the quantities $C_j(\sigma)$ behave like independent Poisson random variables.

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

Lemma 1.2 (Cauchy's formula). *If $m_1 + 2m_2 + \cdots + nm_n = n$, then*

$$\mathbb{P}_\sigma\big\{C_j(\sigma) = m_j \ (1 \leqslant j \leqslant n)\big\} = \prod_{j=1}^{n} \frac{(1/j)^{m_j}}{m_j!}.$$

Proof. Apply Lemma 1.1, 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. This implies that

$$\mathbb{P}_\sigma\big\{C_j(\sigma) = m_j \ (1 \leqslant j \leqslant n)\big\} = \mathbb{E}_\sigma \prod_{j=1}^{n} \binom{C_j(\sigma)}{m_j}.$$ □

Corollary 1.3 (Derangements). *We have the exact formula for derangements*

$$\mathbb{P}_\sigma(C_1(\sigma) = 0) = \sum_{j=0}^{n} \frac{(-1)^j}{j!}.$$

Proof. Apply Inclusion-Exclusion with $u = C_1(\sigma)$, followed by the Lemma 1.1. We get

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

Recall that for a set T os positive integers,

$$C_T(\sigma) = \sum_{j \in T} C_j(\sigma)$$

is the number of cycles in σ with length in T.

Corollary 1.4. *For any nonempty set $T \subseteq [n]$, $\mathbb{E}_\sigma C_T(\sigma) = H(T)$. In particular,*

$$\mathbb{E}_\sigma C(\sigma) = H_n = \log n + \gamma + O(1/n).$$

Proof. By Lemma 1.1, $\mathbb{E}_\sigma C_j(\sigma) = 1/j$ for every j, and the result follows by linearity of expectation and bounds on harmonic sums. □

Corollary 1.5. *For any nonempty set $T \subseteq [n]$,*

$$\mathbb{E}_\sigma (C_T(\sigma) - H(T))^2 \leqslant H(T)$$

with equality in the case $\max T \leqslant n/2$.

Proof. We have

$$C_T(\sigma)^2 = \sum_{\substack{i,j\in T\\ i\neq j}} C_i(\sigma)C_j(\sigma) + 2\sum_{i\in T}\binom{C_i(\sigma)}{2} + \sum_{i\in T} C_i(\sigma).$$

In the double sum over i, j, the summands with $i + j > n$ are zero. Applying Lemma 1.1, we get

$$\mathbb{E}_\sigma C_T(\sigma)^2 \leqslant \sum_{\substack{i,j\in T\\ i\neq j}} \frac{1}{ij} + \sum_{i\in T}\left(\frac{1}{i^2} + \frac{1}{i}\right) = H(T)^2 + H(T),$$

with equality if $\max T \leqslant n/2$. Using Corollary 1.4, we conclude that

$$\mathbb{E}_\sigma (C_T(\sigma) - H(T))^2 = \mathbb{E}_\sigma C_T(\sigma)^2 - 2H(T)\mathbb{E}_\sigma C_T(\sigma) + H(T)^2 \leqslant H(T). \qquad \square$$

Taking $T = [n]$, so that $H(T) = H_n = \log n + O(1)$, and applying Chebyshev's inequality we find that

$$\mathbb{P}_\sigma\Big(|C(\sigma) - H_n| \geqslant \xi\sqrt{\log n}\Big) \leqslant \frac{\mathbb{E}_\sigma |C(\sigma) - H_n|^2}{\xi^2 \log n} \ll \frac{1}{\xi^2} \qquad (\xi \geqslant 1).$$

That is, $C(\sigma)$ is very close to H_n for most σ.

The situation with primes is more complicated (see the lower bound in Proposition 0.1), but we so have a clean upper bound of the same type. **In what follows, we denote $\mathbb{P}_x$ and $\mathbb{E}_x$ the probability and expectation with respect to a random integer in $[1, x]$. Here x may be any real number.**

Lemma 1.6. *Let $T_1, \dots, T_k$ be nonempty, disjoint subsets of the primes in $[2, x]$, and let $m_1, \dots, m_k \geqslant 0$. Then*

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

Proof. We first write

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

Using $\lfloor y/n\rfloor \leqslant \lfloor y\rfloor/n$ for real y and $n \in \mathbb{N}$, Proposition 0.1 then gives

$$\mathbb{E}_x \prod_{j=1}^{k}\binom{\omega(n;T_j)}{m_j} \leqslant \prod_{j=1}^{k}\sum_{\substack{p_{j,1},\dots,p_{j,m_j}\in T_j\\ p_{j,1}<\cdots<p_{j,m_j}}} \frac{1}{p_{j,1}\cdots p_{j,m_j}} \leqslant \prod_{j=1}^{k}\frac{H(T_j)^{m_j}}{m_j!}. \qquad \square$$

A corollary is a theorem of Turán from 1934 **[68]**:

Corollary 1.7 (Turán's variance theorem). *We have*

$$\mathbb{E}_x\big(\omega(n) - \log_2 x\big)^2 \ll \log_2 x.$$

Proof. We directly compute

$$\mathbb{E}_x\big(\omega(n)-\log_2 x\big)^2=\mathbb{E}_x\left(2\binom{\omega(n)}{2}+\omega(n)(1-2\log_2 x)+(\log_2 x)^2\right).$$

Let $T=T_1$ be the set of all primes in $[2,x]$, so that $H(T)=\log_2 x+O(1)$ by Mertens' theorem (0.5). Using Lemma 1.6 with $k=1$ and $m_1=2$, together with (1.1), we obtain

$$\begin{aligned}\mathbb{E}_x\big(\omega(n)-\log_2 x\big)^2&\leqslant H(T)^2+(1-2\log_2 x)\mathbb{E}_x\,\omega(n)+(\log_2 x)^2\\&=O(\log_2 x).\end{aligned}$$

□

We can interpret Corollary 1.7 probabilistically. If $n\leqslant x$ is chosen at random, then Corollary 1.7 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 from Chebyshev's inequality that uniformly for $\xi\geqslant 1$,

$$\mathbb{P}_x\left(|\omega(n)-\log_2 x|\geqslant \xi\sqrt{\log_2 x}\right)\ll\frac{1}{\xi^2}.$$

An immediate corollary is the following famous result of Hardy and Ramanujan [**46**] from 1917. We note that for $\sqrt{x}<n\leqslant x$, $\log_2 x=\log_2 n+O(1)$. That is, we can say that for most n, $\omega(n)$ is close to $\log_2 n$.

Theorem 1.8 (Hardy-Ramanujan). *The function $\omega(n)$ has normal order $\log\log n$, meaning that for any $\varepsilon>0$ we have*

$$(1-\varepsilon)\log\log n\leqslant\omega(n)\leqslant(1+\varepsilon)\log\log n$$

for almost all integers n.

4. Cycles and prime factors from sets: general upper bounds

Theorem 1.9 (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*

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

Proof. Evidently

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

Write $\sigma=\alpha\beta$ and let $h=|\alpha|$. 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

$$m_{t,i}=k_i-\mathbb{1}(i=t\geqslant 1). \tag{1.3}$$

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

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

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 1.2) to count such permutations for each type. It follows that

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

$$\leqslant n! \sum_{\substack{t=0 \\ k_t \neq 0}}^{r} \sum_{\substack{b_1, \dots, b_n \geqslant 0 \\ \sum_{i \in T_j} b_i = m_{t,j} \ (1 \leqslant j \leqslant r)}} \frac{1}{\prod_i b_i! i^{b_i}} := Y,$$

say. Let $T = T_1 \cup \cdots \cup T_r$ and $T_0 = [n] \setminus T$, and separately consider the summation over $i \in T$ and $i \in T_0$. By the multinomial theorem,

$$Y = n! \sum_{\substack{t=0 \\ k_t \neq 0}}^{r} \sum_{\substack{b_i \geqslant 0 \ (i \in T) \\ \sum_{i \in T_j} b_i = m_{t,j} \ (1 \leqslant j \leqslant r)}} \frac{1}{\prod_{i \in T} b_i! i^{b_i}} \sum_{b_i \geqslant 0 \ (i \in T_0)} \frac{1}{\prod_{i \in T_0} b_i! i^{b_i}}$$

$$= n! \sum_{\substack{t=0 \\ k_t \neq 0}}^{r} \prod_{j=1}^{r} \frac{H(T_j)^{m_{t,j}}}{m_{t,j}!} \prod_{i \in T_0} \mathrm{e}^{1/i}$$

$$= n! \prod_{j=1}^{r} \frac{H(T_j)^{k_j}}{k_j!} \left(1 + \sum_{j=1}^{r} \frac{k_j}{H(T_j)}\right) \mathrm{e}^{H(T_0)}.$$

The claimed bound now follows using harmonic sum bounds in the form

$$H(T_0) = H_n - \sum_{j=1}^{r} H(T_j) \leqslant \log n + 1 - \sum_{j=1}^{r} H(T_j). \qquad \square$$

Remark 1.10. Whenever r is bounded, and $k_j = O(H(T_j))$ for each j, the right side is

$$\ll \mathbb{P}(Z_1 = k_1, \dots, Z_r = k_r).$$

where $Z_j \stackrel{d}{=} \mathrm{Pois}(H(T_j))$ for each j, and $Z_1, \dots, Z_r$ are independent. Thus, Theorem 1.9 gives an upper bound for counts of cycle lengths in sets $T_1, \dots, T_r$ 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 1.9 implies that for any $T \subset [n]$ and $k \geqslant 0$,

$$\mathbb{P}_\sigma\left(C_T(\sigma) = k\right) \leqslant \mathrm{e}^{1 - H(T)} \left(\frac{H(T)^{k-1}}{(k-1)!} + \frac{H(T)^k}{k!}\right). \tag{1.4}$$

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

Corollary 1.11 (Cycles in intervals). *Uniformly for $1 \leqslant m \leqslant n$ and $0 \leqslant \lambda \leqslant 1$, we have*

$$\mathbb{P}_{\sigma \in \mathcal{S}_n}\left(C_{[m]}(\sigma) \leqslant \lambda \log m\right) \leqslant \mathrm{e}\, m^{-Q(\lambda)}.$$

Uniformly for $1 \leqslant m \leqslant n$ and $1 \leqslant \lambda$, we have

$$\mathbb{P}_{\sigma \in \mathcal{S}_n}\left(C_{[m]}(\sigma) \geqslant \lambda \log m\right) \leqslant \mathrm{e}\, \lambda^{1+\lambda} m^{-Q(\lambda)}.$$

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

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

PROOF. Let $T = T_1 = [m]$, and recall that $H(T) = H_m \geqslant \log m$. Applying Theorem 1.9 (see (1.4)), together with Proposition 0.3 and the fact that $Q(u)$ is decreasing on $[0,1]$, we get that

$$\mathbb{P}_{\sigma\in\mathcal{S}_n}\left(C_{[m]}(\sigma) \leqslant \lambda \log m\right) \leqslant \mathrm{e}^{1-H_m} \sum_{k\leqslant \lambda\log m} \frac{H_m^k}{k!} \leqslant \mathrm{e}^{1-H_m} \sum_{k\leqslant \lambda H_m} \frac{H_m^k}{k!} \leqslant \mathrm{e}^{1-H_m Q(\lambda)} \leqslant \mathrm{e} m^{-Q(\lambda)}.$$

The proof of the second bound is similar. First we note that the statement is trivial if $m = 1$. Suppose that $m \geqslant 2$. Let $\lambda^* = \lambda - \frac{\lambda+1}{H_m}$. If $\lambda^* < 1$ then the probability in question in $\leqslant 1$ trivially, $\lambda = 1 + O(1/H_m)$ and

$$m^{-Q(\lambda)} = m^{-O(1/H_m^2)} \gg 1,$$

so the desired bound holds. Now suppose that $\lambda^* \geqslant 1$. We have $\lambda \log m \leqslant \lambda(H_m - 1) - 1 = \lambda^* H_m$ and thus by Theorem 1.9, together with Proposition 0.3, we get that

$$\begin{aligned}\mathbb{P}_{\sigma\in\mathcal{S}_n}\left(C_{[m]}(\sigma) \geqslant \lambda \log m\right) &\leqslant \mathrm{e}^{1-H_m} \sum_{k\geqslant \lambda\log m-1} \frac{H_m^k}{k!} \\ &\leqslant \mathrm{e}^{1-H_m} \sum_{k\geqslant \lambda^* H_m} \frac{H_m^k}{k!} \\ &\leqslant \mathrm{e}^{1-H_m Q(\lambda^*)}.\end{aligned}$$

Now $1 \leqslant \lambda^* \leqslant \lambda$, and $Q'(u) = \log u$ implies that

$$Q(\lambda^*) \geqslant Q(\lambda) - \frac{\lambda+1}{H_m}\log\lambda,$$

and, since $\log m \leqslant H_m \leqslant \log m + 1$ we conclude that

$$\mathbb{P}_{\sigma\in\mathcal{S}_n}\left(C_{[m]}(\sigma) \geqslant \lambda \log m\right) \leqslant \mathrm{e}^{1-H_m Q(\lambda)+(\lambda+1)\log\lambda} \leqslant \mathrm{e} m^{-Q(\lambda)}\lambda^{1+\lambda}.$$

The final estimate follows by taking $\lambda = 1 \pm \psi/\sqrt{\log m}$ and using the bound (0.16) for $Q(u)$. Here $0 \leqslant \lambda \leqslant 2$. □

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

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

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 1.9 implies a right-tail bound of

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

whereas the Poisson model predicts that the right side should be smaller, namely $H(T)^k/k!$; but see Homework Exercise 1.2 below.

THEOREM 1.13 (PRIME FACTORS IN SETS). *Let $T_0, T_1, \ldots, T_r$ be a partition of the primes in $[2, x]$ with $T_1, \ldots, T_r$ nonempty. Define*

$$H_j = H(\{p-1 : p \in T_j\}) = \sum_{p\in T_j} \frac{1}{p-1} \qquad (1 \leqslant j \leqslant r).$$

Let $k_1, \dots, k_r \geqslant 0$ and such that if $T_0 = \emptyset$ then $k_1, \dots, k_r$ are not all zero. Then

$$\mathbb{P}_x\{\omega(n;T_j) = k_j \ (1 \leqslant j \leqslant r)\} \ll \prod_{j=1}^{r} \left(\frac{H_j^{k_j}}{k_j!} \mathrm{e}^{-H_j} \right) \left(\eta + \frac{k_1}{H_1} + \cdots + \frac{k_r}{H_r} \right)$$
$$\leqslant \prod_{j=1}^{r} \left(\frac{(H(T_j)+2)^{k_j}}{k_1!} e^{-H(T_j)} \right),$$

where $\eta = 0$ if T_0 is empty, $\eta = 1$ otherwise.

Proof. Let

$$N = \#\{n \leqslant x : \omega(n;T_j) = k_j \ (1 \leqslant j \leqslant r)\},$$

Define $m_{t,j} = k_j - \mathbb{1}(j = t \geqslant 1)$ and let

$$L_t(x) = \sum_{\substack{h \leqslant x \\ \omega(h;T_j) = m_{t,j} \ (1 \leqslant j \leqslant r)}} \frac{1}{h} \qquad (0 \leqslant t \leqslant r).$$

We use the unique factorization of integers into primes, (the "Wirsing trick"), starting with

$$\log x \ll \log n = \sum_{p^a \| n} \log p^a \qquad (x^{1/3} \leqslant n \leqslant x).$$

It follows that

$$(\log x) N \ll \sum_{\substack{n \leqslant x^{1/3} \\ \omega(n;T_j) = k_j \ (1 \leqslant j \leqslant r)}} \log x + \sum_{\substack{n \leqslant x \\ \omega(n;T_j) = k_j \ (1 \leqslant j \leqslant r)}} \sum_{p^a \| n} \log p^a.$$

In the first sum, $\log x \leqslant \frac{x^{1/3} \log x}{n} \ll \frac{x^{1/2}}{n}$, hence the sum is at most $\leqslant x^{1/2} L_0(x)$. In the double sum, let $n = p^a h$ with $p \in T_t$. If $t \geqslant 1$ then $\omega(h, T_t) = k_j - 1$ and $\omega(h, T_j) = k_j$ otherwise. That is, we have $\omega(h;T_j) = m_{t,j}$ for $1 \leqslant j \leqslant t$. Also, $p \in T_0$ is only possible if $\eta = 1$. Hence

$$(\log x) N \ll x^{1/2} L_0(x) + \sum_{t=1-\eta}^{r} \sum_{\substack{h \leqslant x \\ \omega(h;T_j) = m_{t,j} \ (1 \leqslant j \leqslant r)}} \sum_{p^a \leqslant x/h} \log p^a.$$

Using Chebyshev's Estimate for primes or the Prime Number Theorem, the innermost sum over p^a is $O(x/h)$ and thus the double sum over h, p^a is $O(L_t(x))$. Also, if $k_j = 0$ then there is the sum corresponding to $t = j$ is empty. This gives

$$\mathbb{P}_x\Big(\omega(n;T_j) = k_j \ (1 \leqslant j \leqslant r)\Big) \ll \frac{1}{\log x} \Big((\eta + x^{-1/2}) L_0(x) + \sum_{1 \leqslant t \leqslant r : k_t > 0} L_t(x) \Big). \tag{1.5}$$

Now we fix t and bound the sum $L_t(x)$; if $t \geqslant 1$ we may assume that $k_t \geqslant 1$. Write the denominator $h = h_1 \cdots h_r h_0$, where, for $1 \leqslant j \leqslant r$, h_j is composed only of primes from T_j and $\omega(h_j;T_j) = m_{t,j}$, and further that h_0 is composed of primes in T_0. For $1 \leqslant j \leqslant r$ we have

$$\sum_{h_j} \frac{1}{h_j} \leqslant \frac{1}{m_{t,j}!} \Big(\sum_{p \in T_j} \frac{1}{p} + \frac{1}{p^2} + \cdots \Big)^{m_{t,j}} = \frac{H_j^{m_{t,j}}}{m_{t,j}!},$$

and, using Mertens' product estimate (0.7),

$$\sum_{h'} \frac{1}{h'} \leqslant \prod_{p \in T_0} \left(1 - \frac{1}{p}\right)^{-1} \ll (\log x) \prod_{p \in T_1 \cup \cdots \cup T_r} \left(1 - \frac{1}{p}\right).$$

Thus,

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

Using the elementary inequality $1+y \leqslant \mathrm{e}^y$, we see that

$$\prod_{p\in T_1\cup\cdots\cup T_r}\left(1-\frac{1}{p}\right) \leqslant \mathrm{e}^{-H(T_1)-\cdots-H(T_r)}$$

and we obtain

$$L_t(x) \ll (\log x)\prod_{j=1}^{r}\left(\frac{H_j^{m_{t,j}}}{m_{t,j}!}\mathrm{e}^{-H(T_j)}\right) \tag{1.6}$$

Combining estimates (1.5) and (1.6), we conclude that

$$N \ll x\left(\eta + x^{-1/2} + \sum_{j=1}^{r}\frac{k_j}{H_j}\right)\prod_{j=1}^{r}\left(\frac{H_j^{k_j}}{k_j!}\mathrm{e}^{-H(T_j)}\right).$$

By hypothesis, either $\eta = 1$ or $k_j/H_j \geqslant 1/H_j \gg 1/\log\log x$ for some j, and hence the additive term $x^{-1/2}$ may be omitted. This proves the first claim.

Next,

$$\prod_{j=1}^{r}\frac{H_j^{k_j}}{k_j!}\left(\eta+\sum_{j=1}^{r}\frac{k_j}{H_j}\right) \leqslant \prod_{j=1}^{r}\frac{H_j^{k_j}}{k_j!}\prod_{j=1}^{r}\left(1+\frac{1}{H_j}\right)^{k_j} = \prod_{j=1}^{r}\frac{(H_j+1)^{k_j}}{k_j!}$$

and we have

$$H_j = H(T_j) + \sum_{p\in T_j}\frac{1}{p(p-1)} \leqslant H(T_j)+1.$$

This proves the final inequality. □

Remark. A version of Theorem 1.13 is stated in [**67**, Theorem 2], where only the case $r=1$ is proved. The full proof may also be found in [**34**].

Corollary 1.14 (Hardy-Ramanujan inequality, 1917). *Uniformly for $x \geqslant 3$ and $k \in \mathbb{N}$ we have*

$$\mathbb{P}_x\{\omega(n)=k\} \ll \frac{(\log\log x + O(1))^{k-1}}{(k-1)!}.$$

Proof. Let T_1 consist of all primes $\leqslant x$. Then $\eta = 0$ and $H_1 = \log\log x + O(1)$ by Mertens' sum estimate (0.5), and we obtain the desired bound. □

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

Corollary 1.15 (Prime factors in intervals). *Uniformly for $3 \leqslant t \leqslant x$ and $0 \leqslant \lambda \leqslant 1$, we have*

$$\mathbb{P}_x\{\omega(n,t) \leqslant \lambda\log\log t\} \ll (\log t)^{-Q(\lambda)}.$$

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

$$\mathbb{P}_x\{\omega(n,t) \geqslant \lambda\log\log t\} \ll_{\lambda_0} (\log t)^{-Q(\lambda)}.$$

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

$$\mathbb{P}_x\{|\omega(n,t) - \log\log t| > \psi\sqrt{\log\log t}\} \ll \mathrm{e}^{-\frac{1}{3}\psi^2}.$$

Proof. The proof is identical to the proof of Corollary 1.11, using $T = T_1$ as the set of primes in $[2,t]$, $H(T) = \log\log t + O(1)$ from Mertens' bound (0.5), and Theorem 1.13. □

Taking as a special case $t = n$, we recover a strong form of Theorem 1.8.

We can also analyze the distribution of integers composed only of primes factors from a given set.

Corollary 1.16. *Let T be a subset of the primes $\leqslant x$, and let $\mathcal{N}(T)$ denote the set of integers $\leqslant x$ composed only of primes from T. For all $k \geqslant 1$,*

$$\#\{n \in \mathcal{N}(T) : \omega(n) = k\} \ll \frac{x}{\log x} \cdot \frac{(H(T)+1)^{k-1}}{(k-1)!}.$$

Proof. Apply Theorem 1.13 with $T_1 = T$ and T_2 being the set of all primes $\leqslant x$ that are not in T, $k_1 = k$ and $k_2 = 0$. Then $\eta = 0$, $H_1 \leqslant H(T) + 1$ and the result follows. □

Remarks. Applying Theorem 1.13 with T_1 the set of all primes $\leqslant x$ that are *not* in T, and $k_1 = 0$, we see that

$$|\mathcal{N}(T)| \ll \mathrm{e}^{-H(T_1)}x \asymp \mathrm{e}^{H(T)}\frac{x}{\log x}$$

since $H(T) + H(T_1) = \log_2 x + O(1)$ by Mertens' estimate (0.5). Oftentimes we have a corresponding lower bound

$$|\mathcal{N}(T)| \gg \mathrm{e}^{H(T)}\frac{x}{\log x}, \tag{1.7}$$

and this allows us to conclude that, conditionally on $n \in \mathcal{N}(T)$, that $\omega(n)$ has an approximate Poisson distribution with parameter $H(T) + O(1)$. That is, combining (1.7) with Corollary 1.16, we obtain

$$\mathbb{P}_x\{\omega(n) = k | n \in \mathcal{N}(T)\} \ll \mathrm{e}^{-H(T)}\frac{(H(T)+1)^{k-1}}{(k-1)!}.$$

For example, let T be the set of primes $\leqslant x$ that are $1 \mod 4$; in particular, such numbers are the sum of two squares. Then (1.7) follows from a theorem of Landau, and we have $H(T) = \frac{1}{2}\log_2 x + O(1)$ by Mertens' theorem for arithmetic progressions (0.8). We then conclude that

$$\mathbb{P}_x\{\omega(n) = k | n \in \mathcal{N}(T)\} \ll \frac{(\frac{1}{2}\log_2 x + O(1))^{k-1}}{(k-1)!\sqrt{\log x}},$$

what is, conditional on $n \in \mathcal{N}(T)$, $\omega(n)$ has roughly a Poisson distribution with parameter $\frac{1}{2}\log_2 x$.

If we condition on $\omega(n) = k$, the $r = 2$ case of Theorem 1.13 supplies tail bounds for $\omega(n, T)$. If X, Y are independent Poisson random variables with parameters λ_1, λ_2, respectively, then $X + Y \stackrel{d}{=} \mathrm{Pois}(\lambda_1 + \lambda_2)$ and hence, for $0 \leqslant \ell \leqslant k$, we have

$$\begin{aligned}\mathbb{P}(X = \ell | X + Y = k) &= \frac{\mathbb{P}(X = \ell \wedge Y = k - \ell)}{\mathbb{P}(X + Y = k)} \\ &= \frac{\mathrm{e}^{-\lambda_1-\lambda_2}(\lambda_1^\ell/\ell!)(\lambda_2^{k-\ell}/(k-\ell)!)}{\mathrm{e}^{-\lambda_1-\lambda_2}(\lambda_1+\lambda_2)^k/k!} \\ &= \binom{k}{l}\left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right)^\ell\left(\frac{\lambda_2}{\lambda_1+\lambda_2}\right)^{k-\ell}.\end{aligned}$$

Thus, conditional on $\omega(n) = k$ we expect that $\omega(n, T)$ will have roughly a binomial distribution with parameter $\alpha = H(T)/H(S)$, where S is the set of all primes in $[2, x]$.

Theorem 1.17. *Fix $A > 1$ and suppose that $1 \leqslant k \leqslant A\log\log x$. Let T be a nonempty subset of the primes in $[2, x]$ and define let $\alpha = H(T)/H(S)$. For any $0 \leqslant \psi \leqslant \sqrt{\alpha k}$ we have*

$$\mathbb{P}_x\Big(|\omega(n, T) - \alpha k| \geqslant \psi\sqrt{\alpha(1-\alpha)k} \;\Big|\; \omega(n) = k\Big) \ll_A \mathrm{e}^{-\frac{1}{3}\psi^2},$$

the implied constant depending only on A.

We leave the proof as an exercise. It requires the lower bound

$$\mathbb{P}_x(\omega(n) = k) \gg_A \frac{(\log_2 x)^{k-1}}{(k-1)!\log x},$$

which follows, e.g., from the Sathe-Selberg theorem; see also Theorem 1.23 below.

5. 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 1.11 and 1.15 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 $n \leqslant x$.

Theorem 1.18. *Let $3 \leqslant \xi \leqslant x$. With probability $1 - O((\log\log\xi)^{-1/3})$, we have*

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

Theorem 1.19. *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 1.20. 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 $x \to \infty$) $\frac{1}{3}$, $\frac{1}{2}$, $\frac{1}{6}$, respectively. The same is true for $C_{[m]}$ when m is bounded; see Exercise 1.1.

Proof. The proofs of Theorems 1.18 and 1.19 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 1.18. 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 $t_k = \mathrm{e}^{\mathrm{e}^k}$. 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 F_k be the event

$$F_k = \big\{|\omega(n,t_k) - \log_2 t_k| \geqslant 2\sqrt{(k-1)\log(k-1)} - 1\big\}. \tag{1.8}$$

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

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

Hence, by the third part of the Prime Factors in Intervals Corollary (Cor. 1.15),

$$\mathbb{P}F_k \ll \mathrm{e}^{-\frac{1}{3}\psi^2} \ll \frac{1}{k^{4/3}}.$$

Summing over k, we see that F_k holds for some k with probability $O(1/k_1^{1/3})$. Now suppose that F_k fails for every k in the range $k_1 - 1 \leqslant k \leqslant k_2 + 1$. Let $\xi \leqslant t \leqslant x$ and suppose that $t_k < t \leqslant t_{k+1}$. Evidently,

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

By the failure of F_k at every k,

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

and

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

Theorems 1.18 and 1.19 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 $p_j(n) \approx \mathrm{e}^{\mathrm{e}^j}$. Likewise, a typical permutation $\sigma \in \mathcal{S}_n$ has about $\log m$ cycles of length $\leqslant m$, thus we expect that $D_j(n) \approx \mathrm{e}^j$.

Theorem 1.21 (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 1.22 (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 1.21 and 1.22 are nearly identical, and so we provide details only for Theorem 1.22. 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 1.19, with probability $1 - O(1/\theta^{1/3})$, we have

$$|C_{[m]}(\sigma) - \log m| < 2\sqrt{\log m \log_2 m} \qquad (\xi \leqslant m \leqslant n). \tag{1.9}$$

Also, by Exercise 1.2 (b), with probability $1 - O(1/\xi)$ all the cycles of σ of length $\geqslant \xi$ have distinct lengths. Now suppose that σ is a permutation satisfying (1.9), 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 (1.9) 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 (1.9) 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 1.18 and 1.19 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. This is deducible, e.g., from the Kubilius model of integers and the analog for permutations; see Section 4 below.

6. Lower bounds on $\mathbb{P}_x\{\omega(n) = k\}$

Theorem 1.23. *Fix $A \geqslant 1$. For some large constant $x_0(A)$, we have uniformly for $x \geqslant x_0(A)$ and $1 \leqslant k \leqslant A \log_2 x$ that*

$$\mathbb{P}_x\big(\omega(n) = k\big) \asymp_A \frac{(\log_2 x)^{k-1}}{(k-1)! \log x}.$$

Proof. The upper bound follows from the Hardy-Ramanujan inequality (Theorem 1.14), since

$$(\log_2 x + O(1))^{k-1} \ll_A (\log_2 x)^{k-1} \qquad (k \leqslant A \log_2 x).$$

For the lower bound, WLOG suppose that A is sufficiently large. Let $Q = 10A^2 + 1$, $R = x^{1/100A}$ and T the set of all primes in $[Q, R]$. By Mertens' theorem (0.5),

$$H := H(T) = \log_2 x + O_A(1).$$

We assume that x_0 is large enough so that for $x \geqslant x_0(A)$ we have

$$H \geqslant \frac{\log_2 x}{2}. \tag{1.10}$$

Let $\mathcal{N}$ be the set of integers of the form $p_1 \dots p_k \leqslant x$ with $Q \leqslant p_1 < p_2 < \dots < p_{k-1} \leqslant R < p_k$ and such that $p_1 \cdots p_{k-1} \leqslant x^{1/2}$. Clearly $\omega(n) = k$ for each such $n \in \mathcal{N}$. Given $p_1, \dots, p_{k-1}$ with product $\leqslant x^{1/2}$, by the Prime Number Theorem the number of choices for p_k is

$$\pi\left(\frac{x}{p_1 \cdots p_{k-1}}\right) - \pi(R) \gg \frac{x/\log x}{p_1 \cdots p_{k-1}}.$$

Thus,

$$\mathbb{P}_x\left(\omega(n) = k\right) \gg \frac{S_1 - S_2}{\log x},$$

where

$$S_1 = \sum_{Q\leqslant p_1<\ldots<p_{k-1}\leqslant R} \frac{1}{p_1\cdots p_{k-1}}, \qquad S_2 = \sum_{\substack{Q\leqslant p_1<\ldots<p_{k-1}\leqslant R\\ p_1\cdots p_{k-1}>x^{1/2}}} \frac{1}{p_1\cdots p_{k-1}}.$$

We bound S_1 using the lower bound in Proposition 0.1. We note that

$$\sum_{p\geqslant Q}\frac{1}{p^2}\leqslant \sum_{n\geqslant Q}\frac{1}{n^2}\leqslant \frac{1}{Q-1}=\frac{1}{10A^2}.$$

Using (1.10), we have $k\leqslant 2AH$ and hence

$$S_1\geqslant \frac{H^{k-1}}{(k-1)!}\left(1-\frac{k^2}{20H^2A^2}\right)\geqslant 0.8\frac{H^{k-1}}{(k-1)!}.$$

To bound S_2, we use the fact that integers composed of primes below R that are $> x^{1/2}$ are very rare; we will devote the next sections to this type of problem. Let $\alpha=\frac{1}{\log R}=\frac{100A}{\log x}$. Using Proposition 0.1 again,

$$S_2\leqslant \sum_{Q\leqslant p_1<\cdots<p_{k-1}\leqslant R}\frac{1}{x^{\alpha/2}(p_1\cdots p_{k-1})^{1-\alpha}}\leqslant \mathrm{e}^{-50A}\frac{(H')^{k-1}}{(k-1)!},\quad H'=\sum_{Q\leqslant p\leqslant R}\frac{1}{p^{1-\alpha}}.$$

Using the inequality $\mathrm{e}^x\leqslant 1+2x$ for $0\leqslant x\leqslant 1$ and Mertens' estimate (0.6),

$$H'\leqslant \sum_{Q\leqslant p\leqslant R}\frac{1+2\alpha\log p}{p}\leqslant H+2\alpha(\log R-\log Q+O(1))\leqslant H+2$$

if A is large enough. Using (1.10) again yields

$$(H')^{k-1}\leqslant H^{k-1}(1+2/H)^{2AH}\leqslant \mathrm{e}^{4A}H^{k-1}$$

which implies that

$$S_1-S_2\geqslant \frac{H^{k-1}}{(k-1)!}\left(0.8-\mathrm{e}^{4A-50A}\right)\geqslant \frac{H^{k-1}}{2(k-1)!}=\frac{(\log_2 x-O_A(1))^{k-1}}{2(k-1)!}$$

Again, using that $x\geqslant x_0(A)$, we conclude that

$$\mathbb{P}_x(\omega(n)=k)\gg_A \frac{(\log_2 x)^{k-1}}{(k-1)!\log x},$$

as required. □

Much stronger bounds are known for $\mathbb{P}_x(\omega(n)=k)$ in a wide range of uniformity in k. The method are complex-analytic and Chapter II.6 in **[66]** is devoted to this subject.

7. 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 1.24 (Halberstam-Richert). *Let f be a non-negative, real valued multiplicative function and define*

(a) $A(x)=\dfrac{1}{x}\displaystyle\sum_{p\leqslant x} f(p)\log p \quad (x\geqslant 1)$;

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

Then, for all $x > 1$ we have

$$\sum_{n\leqslant x} f(n) \leqslant (A + B(x) + 1)\frac{x}{\log x}\sum_{n\leqslant x}\frac{f(n)}{n} \qquad A := \max_{y\leqslant x} A(y)$$
$$\leqslant (A + B(x) + 1)\mathrm{e}^{B(x)}\frac{x}{\log x}\exp\Big(\sum_{p\leqslant x}\frac{f(p)}{p}\Big).$$

Proof. Fix $x \geqslant 1$, let $A = \max_{y\leqslant x} A(y)$, $B = B(x)$ and also define

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

We begin in a similar way to the proof of The Prime Factors in Sets Theorem (Thm. 1.13). Since $\log u \leqslant u$,

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

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

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

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 (0.3),

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

□

Corollary 1.25. *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*

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

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,

$$\frac{1}{u}\sum_{p\leqslant u} f(p)\log p \leqslant \frac{y}{u}\sum_{p\leqslant u}\log p \ll y$$

by the Prime Number Theorem. Thus, $A(u) \ll y_0 \ll_{y_0} 1$. Also,

$$\begin{aligned} B(x) &\leqslant \sum_p \sum_{k\geqslant 2} \frac{f(p^k)}{p^k} \log p^k = \sum_{p\notin T} \sum_{k\geqslant 2} \frac{\log p^k}{p^k} + \sum_{p\in T} \sum_{k\geqslant 2} \frac{y^k \log p^k}{p^k} \\ &\ll 1 + \sum_{p\in T} (\log p) \sum_{k=2}^{\infty} k \left(\frac{y}{p}\right)^k \\ &= 1 + \sum_{p\in T} (\log p) \frac{(y/p) + (y/p)^2 - (y/p)^3}{(1-y/p)^2} \\ &\ll 1 + \sum_{p\geqslant \min T} \frac{\log p}{p(p-y)} \\ &\ll_{y_0} \frac{1}{(\min T) - y} \ll_{y_0} 1 \end{aligned}$$

since $y \leqslant y_0 < \min T$. Hence, the hypotheses of Lemma 1.24 hold, with bounded $A(x), B(x)$, the bounds 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 (0.5) was used in the last step. □

Corollary 1.26. *Let $1 < \lambda_0 < 2$. Uniformly for $1 \leqslant \lambda \leqslant \lambda_0$ and $3 \leqslant t \leqslant x$,*

$$\mathbb{P}_x\{\Omega(n,t) \geqslant \lambda \log_2 t\} \ll_{\lambda_0} (\log t)^{-Q(\lambda)}.$$

Proof. Let T be the set of primes in $[2,t]$. By Mertens' bound (0.5), $H(T) = \log_2 t + O(1)$. By Corollary 1.25,

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

□

Remark 1.27. When $\lambda \geqslant 2$, the behavior of the quantity in Corollary 1.26 is different than that of the quantity in Corollary 1.15. This is due to the behavior of powers of small prime factors, most important being powers of 2, and in fact

$$\#\{n \leqslant x : \Omega(n,t) \geqslant \lambda \log_2 t\} \approx x(\log t)^{-Q(2) - (\log 2)(\lambda-2)} = \frac{x \log t}{2^{\lambda \log_2 t}}. \tag{1.11}$$

8. Application: Erdős' multiplication table problem

In 1955, Erdős **[25]** 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 **[26]** refined the

estimates to prove that $A(N) = N^2(\log N)^{-\mathcal{E}+o(1)}$, where

$$\mathcal{E} = Q\left(\frac{1}{\log 2}\right) = 1 - \frac{1+\log\log 2}{\log 2} = 0.08607\ldots.$$

Theorem 1.28. *We have $A(N) \ll N^2(\log N)^{-\mathcal{E}}$.*

Proof. Let $k_0 = \frac{\log_2 N}{\log 2}$. By Corollary 1.26 (with $t = N$), the number of distinct products with $\Omega(ab) \geqslant k_0$ is bounded above by

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

There are $O(N)$ products with $a = 1$ or $b = 1$. If $a > 1$, $b > 1$ and $\Omega(ab) < k_0$, then $\omega(a) = h$, $\omega(b) = j$ with $h \geqslant 1$, $j \geqslant 1$ and $h + j = k < k_0$. The number of pairs a, b with a fixed h, j is, by Theorem 1.23,

$$\ll \frac{N^2(\log_2 N)^{h+j-2}}{(\log N)^2(h-1)!(j-1)!}.$$

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

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

upon invoking Proposition 0.3. □

Remarks. The choice of k_0 is motivated by $\lambda = \frac{1}{\log 2}$ being the unique solution of $2Q(\lambda/2) = Q(\lambda)$.

9. 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

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

By a classical theorem of Dirichlet, $\mathbb{E}_x\tau(n) \sim \log x$ as $x \to \infty$, so the average (mean) of $\tau(n)$ for $n \leqslant x$ is about $\log x$.

What is $\tau(n)$ for a "typical" $n \leqslant x$? By Theorem 1.15 and Corollary 1.26, if $\xi = \xi(x) \to \infty$ as $x \to \infty$ then for almost all $n \leqslant x$ we have

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

and therefore for such n it follows that

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

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 1.5), 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 5.1). This motivates the next result.

Theorem 1.29. *Let $1 \leqslant \psi \leqslant \sqrt{\log_2 x}$. Then*

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

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 Lemma 1.24. 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 (0.16).

Similarly, taking $t = 1-\frac{\lambda}{2}$, we obtain with a second application of Lemma 1.24 the 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, $(\log x)^{\lambda^2} = \mathrm{e}^{\psi^2}$ and the proof is complete. □

10. The range of Euler's function

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. $V(15) = 7$. Since $\phi(p) = p-1$ for all primes p, we have $V(x) \geqslant \pi(x+1) \gg x/\log x$ by the Prime Number Theorem. Here we show an upper bound which is very close to this.

Theorem 1.30 (Erdős, 1935 [23]). *We have $V(x) = x(\log x)^{-1+o(1)}$.*

PROOF. Fix an integer $m \geqslant 10$, let $M = p_1 p_2 \cdots p_m$ be the product of the first m primes. Let

$$\mathcal{J}_m = \{1 \leqslant j \leqslant M : (j, M) = 1,\ (j-1, M) \geqslant \log m\}.$$

For each $j \in [M]$ with $(j, M) = 1$ let $\mathcal{P}_j = \{p \leqslant x : p \equiv j \pmod M\}$ and

$$\mathcal{P} = \bigcup_{j \in \mathcal{J}_m} \mathcal{P}_j.$$

We first show that $|\mathcal{J}_m|/\phi(M) \to 1$ as $m \to \infty$. Let $2|\ell|M$. Then

$$\begin{aligned}\#\{1 \leqslant j \leqslant M : (j, M) = 1, (j-1, M) = \ell\} &= \prod_{p | M/\ell} (p-2) \\ &= \phi(M) \prod_{\substack{p|M \\ p>2}} \frac{p-2}{p-1} \prod_{\substack{p|\ell \\ p>2}} \frac{1}{p-2}.\end{aligned}$$

Since $p - 2 > \sqrt{p}$ for $p \geqslant 5$, the inner product is $\leqslant \sqrt{3/\ell}$. The first product is $\ll 1/\log m$ by Mertens. Hence, summing over $\ell < \log m$ we have

$$\phi(M) - |\mathcal{J}_m| = \#\{1 \leqslant j \leqslant M : (j, M) = 1, (j-1, M) < \log m\} \ll \frac{\phi(M)}{\log m} \sum_{\ell < \log m} \frac{1}{\sqrt{\ell}} \ll \frac{\phi(M)}{(\log m)^{1/2}}.$$

Hence,

$$|\mathcal{J}_m| \sim \phi(M) \qquad (m \to \infty). \tag{1.12}$$

Fix $\varepsilon > 0$. By an elementary estimate, for some large constant C, if $\phi(n) \leqslant x$ then $n \leqslant y := Cx \log_2 x$. Let $c_m = |\mathcal{J}_m|/\phi(M)$. By Mertens theorem in arithmetic progressions (0.8),

$$H(\mathcal{P}) = c_m \log_2 x + O_m(1).$$

Let $\delta = 2/\log_2 m$ and suppose m is large enough so that $0 < \delta < 1/2$. Also, $\delta \to 0$ as $m \to \infty$. By Theorem 1.13, followed by (0.3) and Stirling's formula,

$$\begin{aligned}\#\{n \leqslant y : \omega(n; \mathcal{P}) < \delta \log_2 x\} &\ll \frac{y}{(\log x)^{1-c_m}} \sum_{k < \delta \log_2 x} \frac{((1-c_m)\log_2 x + O_m(1))^k}{k!} \\ &\ll \frac{x \log_2 x}{(\log x)^{1-c_m-\delta \log(\mathrm{e}/\delta)}}.\end{aligned}$$

If m is large enough, the exponent of $\log x$ is $> 1 - \varepsilon$.

Now let W be the number of values of Euler's function which have the form $\phi(n)$, where $\omega(n; \mathcal{P}) \geqslant L := \lceil \delta \log_2 x \rceil$. Suppose that $K \geqslant L$ and $\{k_j : j \in \mathcal{J}_m\}$ is a vector of non-negative integers with sum K. If $\omega(n; \mathcal{P}_j) = k_j$ for all $j \in \mathcal{J}_m$ then $\phi(n)$ is divisible by $\prod_{j \in \mathcal{J}_m} (j-1, M)^{k_j}$. Thus,

$$\begin{aligned}W &\leqslant \sum_{K \geqslant L} \sum_{\substack{\{k_j : j \in \mathcal{J}_m\} \\ \sum k_j = K}} \frac{x}{\prod_{j \in \mathcal{J}_m} (j-1, M)} \\ &\leqslant \sum_{K \geqslant L} \sum_{\substack{\{k_j : j \in \mathcal{J}_m\} \\ \sum k_j = K}} \frac{x}{(\log m)^K} \\ &\leqslant \sum_{K \geqslant L} \frac{x(K+1)^{|\mathcal{J}_m|}}{(\log m)^K} \\ &\ll \frac{x(\log_2 x)^{|\mathcal{J}_m|}}{(\log x)^{\delta \log_2 m}} = \frac{x(\log_2 x)^{|\mathcal{J}_m|}}{\log^2 x} \ll_m \frac{x}{\log x}.\end{aligned}$$

This completes the proof. □

11. Exercises

Exercise 1.1. (a) Derive the following general inclusion-exclusion formula, valid for any non-negative integer u:

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

(b) Let $1 \leqslant j \leqslant n$ and $0 \leqslant m \leqslant n/j$. 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

$$\lim_{n\to\infty} \mathbb{P}_{\sigma\in\mathcal{S}_n}(C_j(\sigma) = m).$$

Exercise 1.2. (a) Show that if T is a nonempty susbet of $[n]$, and $k \geqslant 0$, then

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

(this is sometimes stronger than Theorem 1.9, especially if $H(T)$ is small).

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

Exercise 1.3. Show that $\mathbb{E}\, 2^{C(\sigma)} = n + 1$. Contrast this with the behavior of $2^{C(\sigma)}$ for most $\sigma \in \mathcal{S}_n$.

Exercise 1.4. Let $1 \leqslant k \leqslant n$. Show that if T is a nonempty subset of $[n]$ with $\max T \leqslant n/k$, then

$$\mathbb{E}_\sigma C_T(\sigma)^k = \mathbb{E}\, Z^k,$$

where $Z \stackrel{d}{=} \mathrm{Pois}(H(T))$.

Exercise 1.5. (a) Show that if T is a nonempty susbet of the primes in $[2, x]$, and $k \geqslant 0$, then

$$\mathbb{P}_x\{\omega(n, T) \geqslant k\} \leqslant \frac{H(T)^k}{k!}.$$

(this is sometimes stronger than Theorem 1.13, especially if $H(T)$ is small).

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

Exercise 1.6. (a) Prove that $\mathbb{E}_{\sigma\in\mathcal{S}_n} \dfrac{1}{C(\sigma)} \sim \dfrac{1}{\log n}$ as $n \to \infty$.

(b) Prove that $\mathbb{E}_x \left(\dfrac{1}{\omega(n)} \mathbb{1}(n \geqslant 2)\right) \sim \dfrac{1}{\log_2 x}$ as $x \to \infty$.

Exercise 1.7. Provide full details for the proof of Corollary 1.12.

Exercise 1.8. Starting with Lemma 1.24, prove Corollary 1.15 using the method used to prove Corollary 1.26.

Exercise 1.9. Prove Theorem 1.17 using Lemma 0.5 and Theorem 1.23.

Exercise 1.10. Provide full details of the proof of Theorem 1.19.

Exercise 1.11. Provide full details of the proof of Theorem 1.21.

CHAPTER 2

Distribution of the largest cycle and largest prime factor

1. Upper bounds

Theorem 1.9 implies that

$$\nu(n,m) := \mathbb{P}_{\sigma\in\mathcal{S}_n}(C_{(m,n]}(\sigma)=0) \leqslant \mathrm{e}^{1-H_n+H_m} \leqslant \mathrm{e}^2 m/n \qquad 1\leqslant m\leqslant n.$$

When m is small, however, the number of cycles is at least n/m and this is extremely rare by Theorem 1.11. We can argue heuristically as follows: $C_1(\sigma),\dots,C_m(\sigma)$ behaves like a set of independent Poisson variables $Z_1,\dots,Z_m$ with $Z_j \stackrel{d}{=} \mathrm{Pois}(1/j)$. Thus, the event $C_{(m,n]}(\sigma)=0$ can be modeled by the event $Z_1+2Z_2+\cdots+mZ_m=n$. Using the ideas behind Chernoff's inequality, and Proposition 0.2, for any $w\geqslant 1$ we have

$$\begin{aligned}\mathbb{P}_\sigma(Z_1+2Z_2+\cdots+mZ_m=n) &\leqslant \mathbb{E}_\sigma w^{Z_1+2Z_2+\cdots+mZ_m-n}\\ &= w^{-n}\exp\left\{\frac{w-1}{1}+\frac{w^2-1}{2}+\cdots\frac{w^m-1}{m}\right\}.\end{aligned}$$

Optimizing the choice of w will show that the RHS is decaying very rapidly as a function of $u=n/m$. We utilize this idea to show the following.

Theorem 2.1 (No large cycles). *Uniformly for $1\leqslant m\leqslant n$ we have*

$$\nu(n,m)\leqslant \mathrm{e}^{-u\log u+u-1}, \quad u=n/m.$$

Proof. Let $w=u^{1/m}$. Following the heuristic above, we first write

$$\nu(n,m)\leqslant \mathbb{E}_{\sigma\in\mathcal{S}_n} w^{C_1(\sigma)+2C_2(\sigma)+\cdots+mC_m(\sigma)-n}.$$

For each $j\in[m]$, write $w^j=1+(w^j-1)$. By the binomial theorem and Lemma 1.1,

$$\begin{aligned}\nu(n,m) &\leqslant w^{-n}\mathbb{E}_{\sigma\in\mathcal{S}_n}\prod_{j=1}^m\left(\sum_{k_j=0}^\infty (w^j-1)^{k_j}\binom{C_j(\sigma)}{k_j}\right)\\ &= w^{-n}\sum_{k_1,\dots,k_m\geqslant 0}(w-1)^{k_1}\cdots(w^m-1)^{k_m}\mathbb{E}_{\sigma\in\mathcal{S}_n}\binom{C_1(\sigma)}{k_1}\cdots\binom{C_m(\sigma)}{k_m}\\ &\leqslant w^{-n}\sum_{k_1,\dots,k_m\geqslant 0}(w-1)^{k_1}\cdots(w^m-1)^{k_m}\prod_{j=1}^m\frac{(1/j)^{k_j}}{k_j!}\\ &= w^{-n}\exp\left\{\frac{w-1}{1}+\frac{w^2-1}{2}+\cdots\frac{w^m-1}{m}\right\}.\end{aligned}$$

The mean value theorem implies that $w^j=u^{j/m}\leqslant 1+(u-1)j/m$ for $1\leqslant j\leqslant m$ and hence

$$w-1+\frac{w^2-1}{2}+\cdots+\frac{w^m-1}{m}\leqslant\sum_{j=1}^m\frac{(u-1)j/m}{j}=u-1. \tag{2.1}$$

We conclude that

$$\nu(n,m)\leqslant u^{-n/m}\mathrm{e}^{u-1}=\mathrm{e}^{-u\log u+u-1}. \qquad \square$$

Remarks. The upper bound in Theorem 2.1 is reasonably sharp throughout the range on n, m. For example, if $m = 1$ then

$$A(1,n) = \frac{1}{n!} = \frac{1}{u!} = \mathrm{e}^{-u\log u+u-(1/2)\log u+O(1)}$$

by Stirling's formula.

Let $\Psi(x,y) = \#\{n \leqslant x : P^+(n) \leqslant y\}$. These are known as *y-smooth*, or *y-friable* numbers. Applying Theorem 1.13 with T_1 being the set of all primes in $(y,x]$, and $k_1 = 0$, we have $H(T_1) = \log_2 x - \log_2 y + O(1)$ by Mertens' estimate (0.5), and hence

$$\Psi(x,y) \ll x\frac{\log y}{\log x}.$$

When $\log y$ is much smaller than $\log x$, one can do substantially better using the ideas behind the proof of Theorem 2.1.

Theorem 2.2. *Uniformly for $x \geqslant 10$ and $\log x \leqslant y \leqslant x$ we have*

$$\Psi(x,y) \leqslant xe^{-u\log u+O(u)}, \qquad u = \frac{\log x}{\log y}.$$

Remarks. There is a change of behavior around $y = \log x$, due to the fact that for smaller y, if $\prod_{p\leqslant y} p \approx x$, then some of the exponents of primes dividing n must be large.

We note some special cases which we will find useful for applications:

$$\Psi(x,\log x) \leqslant \exp\left\{\frac{(\log x)\log_3 x}{\log_2 x} + O\left(\frac{\log x}{\log_2 x}\right)\right\} = x^{o(1)} \quad (x\to\infty), \tag{2.2}$$

$$\Psi(x,(\log x)^c) \leqslant x^{1-1/c+o(1)} \qquad (x\to\infty) \tag{2.3}$$

for any fixed $c \geqslant 1$, and

$$\Psi(x, x^{c(\log_3 x)/\log_2 x}) \ll \frac{x}{(\log x)^{c+o(1)}} \quad (x\to\infty). \tag{2.4}$$

Proof of Theorem 2.2. Define

$$\alpha = 1 - \frac{\log u}{\log y}.$$

By our hypothesis that $\log x \leqslant y \leqslant x$,

$$1 \leqslant u \leqslant \frac{\log x}{\log_2 x}, \qquad \frac{\log_3 x}{\log_2 x} \leqslant \alpha \leqslant 1, \qquad x^{1-\alpha} = \mathrm{e}^{u\log u}. \tag{2.5}$$

Define

$$S := \sum_{P^+(n)\leqslant y} \frac{1}{n^\alpha} = \prod_{p\leqslant y}\left(1 + \frac{1}{p^\alpha} + \frac{1}{p^{2\alpha}} + \cdots\right) = \prod_{p\leqslant y}\left(1 + \frac{1}{p^\alpha - 1}\right) \leqslant \exp\left\{\sum_{p\leqslant y}\frac{1}{p^\alpha - 1}\right\}. \tag{2.6}$$

In the case $0 < \alpha < 2/3$, we use the simple bound

$$\Psi(x,y) \leqslant \sum_{\substack{n\leqslant x\\ P^+(n)\leqslant y}} \left(\frac{x}{n}\right)^\alpha \leqslant x^\alpha S = x\mathrm{e}^{-u\log u}\, S.$$

We have $y \leqslant u^3 \leqslant \log^3 x$ and $u \asymp \frac{\log x}{\log_2 x}$. When $p \leqslant 2^{1/\alpha}$ we have $p^\alpha - 1 \gg \alpha \log p$, and when $p > 2^{1/\alpha}$ we have $p^\alpha - 1 \geqslant \frac{1}{2} p^\alpha$. Thus, using (2.5) again and ignoring that p is prime,

$$\begin{aligned}\log S \leqslant \sum_{2 \leqslant n \leqslant 2^{1/\alpha}} \frac{O(1)}{\alpha \log n} + \sum_{n \geqslant 2} \frac{2}{n^\alpha} &\ll \frac{1}{\alpha} \int_2^{2^{1/\alpha}} \frac{dt}{\log t} + \int_1^y \frac{dt}{t^\alpha} \\ &\ll 2^{1/\alpha} + \frac{y^{1-\alpha}}{1-\alpha} \\ &\ll (\log x)^{o(1)} + u \ll u.\end{aligned}$$

This completes the proof in the case $0 < \alpha < 2/3$.

Next, assume that $\alpha \geqslant 2/3$. For all $w > 0$, $\log w \leqslant w$ and thus for $n \leqslant x$, $\log(x/n) = \alpha^{-1} \log(x/n)^\alpha \leqslant \alpha^{-1}(x/n)^\alpha$. Hence,

$$\begin{aligned}(\log x)\Psi(x,y) &= \sum_{\substack{n \leqslant x \\ P^+(n) \leqslant y}} \log(x/n) + \log n \\ &\ll x^\alpha S + \sum_{\substack{n \leqslant x \\ P^+(n) \leqslant y}} \sum_{p^k \mid n} \log p,\end{aligned} \tag{2.7}$$

In the double-sum on the right side of (2.7), let $n = p^k m$, and separate into cases depending on $k = 1$ or $k > 1$. The $k = 1$ terms contribute

$$\leqslant \sum_{\substack{m \leqslant x \\ P^+(m) \leqslant y}} \sum_{p \leqslant \min(y, x/m)} \log p \ll \sum_{\substack{m \leqslant x \\ P^+(m) \leqslant y}} \min(y, x/m) \leqslant \sum_{P^+(m) \leqslant y} y^{1-\alpha} \left(\frac{x}{m}\right)^\alpha = u x^\alpha S.$$

The terms with $k \geqslant 2$ contribute

$$\leqslant \sum_{\substack{p \leqslant y \\ 2 \leqslant k \leqslant \frac{\log x}{\log p}}} \log p \sum_{\substack{m \leqslant x/p^k \\ P^+(m) \leqslant y}} 1 \leqslant \sum_{\substack{p \leqslant y \\ 2 \leqslant k \leqslant \frac{\log x}{\log p}}} \log p \sum_{P^+(m) \leqslant y} \left(\frac{x}{p^k m}\right)^\alpha \ll x^\alpha S.$$

Therefore, by (2.5),

$$\Psi(x,y) \ll \frac{u}{\log x} x^\alpha S = \frac{x \mathrm{e}^{-u \log u}}{\log y} S. \tag{2.8}$$

It remains to bound S. Since $\alpha \geqslant 2/3$, $(p^\alpha - 1)^{-1} = p^{-\alpha} + O(1/p^{4/3})$. For any $0 \leqslant x \leqslant 1$, the mean value theorem implies that $u^x \leqslant 1 + (u-1)x$, hence

$$\frac{1}{p^\alpha} = \frac{1}{p} u^{\frac{\log p}{\log y}} \leqslant \frac{1}{p}\left(1 + (u-1)\frac{\log p}{\log y}\right).$$

Thus, by Mertens bounds (0.5) and (0.6),

$$\begin{aligned}\log S &\leqslant O(1) + \sum_{p \leqslant y} \frac{1}{p^\alpha} \\ &\leqslant O(1) + \sum_{p \leqslant y} \frac{1}{p} + \frac{u-1}{\log y} \sum_{p \leqslant y} \frac{\log p}{p} \\ &\leqslant \log_2 y + O(u+1).\end{aligned}$$

Thus, $S \ll (\log y) e^{O(u)}$. Combining this with (2.8), we get the claimed bound in the case $\alpha \geqslant 2/3$. □

When $y \leqslant \log x$, simpler bounds are possible, since $P^+(n) \leqslant y$ implies that $n = \prod_{p \leqslant y} p^{a_p}$. Therefore, we have the equality

$$\Psi(x,y) = \#\Big\{(a_p)_{p\leqslant y} : \sum_{p\leqslant y} a_p \log p \leqslant \log x : 0 \leqslant a_p \ (p \leqslant y)\Big\},$$

and good bounds can be arrived at by combinatorial counting; see, e.g. Section III.5.2 in [**66**].

2. Application: large gaps between primes

Let p_n denote the n^{th} prime, and let

$$G(X) := \max_{p_{n+1}\leqslant X} (p_{n+1} - p_n)$$

denote the the maximum gap between consecutive primes less than X.

In 1931, Westzynthius [**70**] proved that infinitely often the gap between consecutive prime numbers can be an arbitrarily large multiple of the average gap, which is $\sim \log X$ by the PNT. After improvements by Ricci in 1934 and Erdős in 1935, in 1938 Rankin [**59**] proved that

$$G(X) \gg \frac{\log X \log_2 X \log_4 X}{(\log_3 X)^2}. \tag{2.9}$$

This was not improved until August 2014, in two independent papers of Ford-Green-Konyagin-Tao and Maynard. Later, Ford, Green, Konyagin, Maynard, and Tao [**35**] established the current world record

Theorem 2.3 (Ford-Green-Konyagin-Maynard-Tao [35, Theorem 1]). *We have*

$$G(X) \gg \frac{\log X \log_2 X \log_4 X}{\log_3 X}$$

for sufficiently large X.

Here we prove Rankin's bound (2.9) using a very simple argument.

Idea #1. Let x be the largest integer such that $P(x) \leqslant X/3$, where $P(x)$ is the product of primes below x. By the PNT, $x \sim \log X$. Let $J(x)$ be the largest gap between numbers that are coprime to $P(x)$; the set of such numbers is periodic modulo $P(x)$, so $J(x)$ exists. Such a gap occurs between $P(x)$ and $3P(x)$, that is, below X. Each number in the gap has a prime factor $\leqslant x < P(x)$, thus these numbers are composite. Therefore, $G(X) \geqslant J(x)$.

Idea #2. Suppose that the integers coprime to $P(x)$ have a gap $[u, u+y]$ of length y. For each prime $p \leqslant x$, let a_p be the residue class $-u \mod p$. Then the set of residue classes a_p, for $p \leqslant x$, cover all integers in $\{1, 2, \dots, y-1\}$; for all $1 \leqslant j \leqslant y-1$, there is a $p \leqslant x$ with $p|(u+j)$, hence $j \equiv a_p \pmod p$. Conversely, if we can find residue classes a_p, one for each prime $p \leqslant x$, that cover $[1, y-1]$, then $G(X) \geqslant J(x) \geqslant y$.

Rankin's argument, based on earlier work of Westzynthius and Erdős. Suppose that $x < y < x \log x$, let

$$\begin{aligned} z &= y^{(\frac{\log_3 x}{5 \log_2 x})}, \\ \mathcal{P}_1 &= \{p : p \leqslant 2\log x \text{ or } z < p \leqslant x/2\}, \\ \mathcal{P}_2 &= \{p : 2\log x < p \leqslant z\}, \\ \mathcal{P}_3 &= \{p : x/2 < p \leqslant x\}. \end{aligned}$$

First, we set $a_p = 0 \mod p$ for all $p \in \mathcal{P}_1$. These a_p cover all integers in $[1, y-1]$ that have a prime factor from $\mathcal{P}_1$. Let S_0 be the set of uncovered integers $n \in [1, y-1]$. Such n satisfy either $P^+(n) \leqslant z$, or they have a prime factor $> x/2$. In the latter case, as n has no prime factor $< 2\log x$ and $n \leqslant y \leqslant x \log x$, we conclude that n is prime. Let $u = \frac{5\log_2 x}{\log_3 x}$. Then $u \log u > (5 - o(1)) \log_2 x$. By Theorem 2.2 and the PNT,

$$|S_0| \leqslant \Psi(y,z) + \pi(y) \ll \frac{y}{\log^4 x} + \frac{y}{\log x} \ll \frac{y}{\log x}.$$

Secondly, denote by $q_1, \dots, q_k$ the primes in $\mathcal{P}_2$. Let S_j be the set of numbers in $[1, y-1]$ left uncovered by a_p for $p \in \mathcal{P}_1$ and also left uncovered by $a_{q_1}, \dots, a_{q_j}$. For each j, if we are given S_{j-1} we can always find a choice of a_{q_j} (greedy choice) such that $|S_j| \leqslant (1 - 1/q_j)|S_{j-1}|$. In the end, we have

$$|S_k| \leqslant |S_0| \prod_{j=1}^{k} (1 - 1/q_j) = |S_0| \prod_{2 \log x < p \leqslant z} (1 - 1/p) \ll \frac{|S_0| \log_2 x}{\log z} \ll \frac{y (\log_2 x)^2}{(\log_3 x) \log^2 x}$$

using Mertens' product estimate (0.7). Therefore, if $c > 0$ is small enough, and we take

$$y = c \, \frac{x (\log x) \log_3 x}{(\log_2 x)^2}, \tag{2.10}$$

then $|S_k| \leqslant \frac{x}{10 \log x} < \pi(x) - \pi(x/2)$, again using the PNT. Finally, the elements of S_k can be mapped to distinct primes in $\mathcal{P}_3$. Thus, if $\ell \in S_k$ maps to p, take $a_p = \ell \mod p$ to cover ℓ.

In conclusion, if y is given by (2.10), then $G(X) \geqslant J(x) \geqslant y$. As $x \sim \log X$,

$$y \gg (\log X) \frac{(\log_2 X)(\log_4 X)}{(\log_3 X)^2},$$

and this proves (2.9).

3. Asymptotic formulas when u is small

The idea behind the asymptotic formula is to first develop a recurrence formula. For $1 \leqslant \ell \leqslant m$, there are $\binom{n}{\ell}(\ell - 1)!$ ways to form an ℓ–cycle from $[n]$. Hence

$$\begin{aligned} \nu(n,m) = \frac{1}{n!} \sum_{\substack{\sigma \in \mathcal{S}_n \\ C_{(m,n]}(\sigma) = 0}} \frac{1}{n} \sum_{\substack{\tau \mid \sigma \\ \tau \text{ a cycle}}} |\tau| &= \frac{1}{n \cdot n!} \sum_{\ell=1}^{m} \ell \binom{n}{\ell} (\ell - 1)! (n - \ell)! \nu(n - \ell, m) \\ &= \frac{1}{n} \sum_{k=n-m}^{n-1} \nu(k, m). \end{aligned} \tag{2.11}$$

Heuristic. Suppose that $\nu(n,m) \approx f(u)$, where $u = n/m$ and f is continuous. By (2.11),

$$f(u) \approx \frac{1}{n} \sum_{k=n-m}^{n-1} f(k/m) \approx \frac{1}{n} \int_{n-m}^{n} f(t/m) \, dt = \frac{1}{u} \int_{u-1}^{u} f(v) \, dv.$$

Assume we have equality instead of $\approx$. Differentiation gives $u f'(u) = -f(u-1)$. This is known as a *differential-delay equation*. If we add the natural initial conditions $f(u) = 1$ for $0 \leqslant u \leqslant 1$, then there is a unique continuous solution. This motivates the definition of the *Dickman function* $\rho(u)$.

Definition 2.4. The *Dickman function* $\rho : [0, \infty) \to \mathbb{R}$ is the unique continuous solution of

$$\rho(u) = 1 \quad (0 \leqslant u \leqslant 1); \qquad u \rho'(u) = -\rho(u-1) \quad (u > 1). \tag{2.12}$$

Lemma 2.5. *We have*

(a) $u\rho(u) = \int_{u-1}^{u} \rho(v) \, dv$ *for* $u \geqslant 1$*;*
(b) $\rho(u) > 0$ *for all* $u \geqslant 0$*;*
(c) $\rho(u)$ *is decreasing for* $u \geqslant 0$*;*
(d) For $u \geqslant 1$, $-\frac{\rho'(u)}{\rho(u)} \ll 1 + \log u$.

Proof. (a) follows by integrating (2.12) from $u = 1$ to $u = v$ with $v \geqslant 1$. To prove (b), assume that $\tau = \min\{u : \rho(u) = 0\}$ exists. Since $\rho(u) = 1 - \log u$ for $1 \leqslant u \leqslant 2$, $\tau > 2$. By (a),

$$0 = \tau \rho(\tau) = \int_{\tau-1}^{\tau} \rho(v) > 0,$$

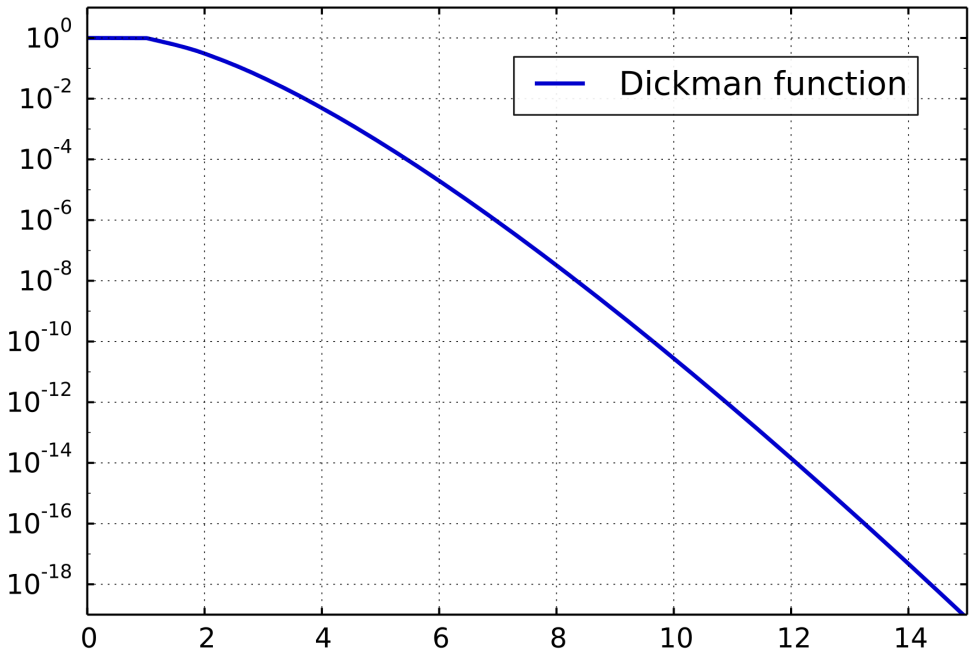

FIGURE 1. Dickman's function from $0 \leqslant u \leqslant 15$.

a contradiction. That $\rho(u)$ is decreasing is clear from (b) and (2.12). This proves (c). From (2.12) and (a),

$$-\frac{\rho'(u)}{\rho(u)} = \frac{\rho(u-1)}{\int_{u-1}^{u} \rho(v)\,dv}. \tag{2.13}$$

Let $B_k = \max_{1<v\leqslant k/2}(-\rho'(v)/\rho(v))$. We have

$$B_4 = \max_{1<v\leqslant 2} \frac{1/v}{1-\log v} = \frac{1}{2(1-\log 2)} = 1.629\ldots.$$

If $k \geqslant 4$ and $k/2 < u \leqslant (k+1)/2$ then the denominator on the right side of (2.13) is at least

$$\int_{u-1}^{u-1/2} \rho(v)\,dv \geqslant \rho(u-1)\int_{u-1}^{u-1/2} \mathrm{e}^{-B_k(v-u+1)}\,dv = \frac{\rho(u-1)(1-\mathrm{e}^{-\frac{1}{2}B_k})}{B_k}.$$

Using that $\mathrm{e}^{-\frac{1}{2}B_k} \leqslant \mathrm{e}^{-\frac{1}{2}B_4} < 1/2$, we infer that

$$B_{k+1} \leqslant \frac{B_k}{1-\mathrm{e}^{-\frac{1}{2}B_k}} \leqslant B_k\left(1+2\mathrm{e}^{-\frac{1}{2}B_k}\right).$$

The function $x(1+2\mathrm{e}^{-x/2})$ is increasing for $x \geqslant 0$, hence if C is large and $B_k \leqslant C\log k$ then $B_{k+1} \leqslant (C\log k)(1+2/k^{C/2}) \leqslant C\log(k+1)$. Therefore, $B_k \ll \log k$ and (d) follows. □

In Figure 3, we plot the Dickman function on a log-scale, and it is evident that ρ decreases rapidly. In fact, $\rho(u) = \mathrm{e}^{-u\log u - u\log_2(2u)+O(u)}$; see **[66]**, Ch. III.5.4 for further asymptotics and proofs.

THEOREM 2.6. *For all $n \geqslant m \geqslant 1$ we have*

$$\rho\left(\frac{n}{m}\right) \leqslant \nu(n,m) \leqslant \rho\left(\frac{n+1}{m+1}\right). \tag{2.14}$$

Consequently, for $\sqrt{n\log n} \leqslant m \leqslant n$ *we have*

$$\nu(n,m) = \rho(u)\left(1 + O\left(\frac{u\log(u+1)}{m}\right)\right), \qquad u = n/m. \tag{2.15}$$

Remarks. Inequality (2.15) recovers Theorem 4 of [**55**], with a much shorter proof, and provides an asymptotic formula for $\nu(n,m)$ as long as $n = o(m^2/\log m)$. When $n \gg m^2/\log m$, $\nu(n,m) \not\sim \rho(n/m)$, the asymptotic having a different shape; see [**58**], Theorem 2.4 or [**55**] for details. Thus the final conclusion is best-possible.

Proof. Suppose $m \leqslant n \leqslant 2m$. As there is at most one cycle of length $> m$, Lemma 1.1 implies

$$\nu(n,m) = 1 - \sum_{k=m+1}^{n} \mathbb{E}\, C_k(\sigma) = 1 - H_n + H_m. \tag{2.16}$$

Since

$$H_n - H_m = \sum_{k=m+1}^{n} \frac{1}{k} \leqslant \sum_{k=m+1}^{n} \int_{k-1}^{k} \frac{dt}{t} = \log\frac{n}{m} = 1 - \rho\left(\frac{n}{m}\right)$$

and

$$H_n - H_m \geqslant \sum_{k=m+1}^{n} \int_{k}^{k+1} \frac{dt}{t} = \int_{m+1}^{n+1} \frac{dt}{t} = \log\left(\frac{n+1}{m+1}\right) = 1 - \rho\left(\frac{n+1}{m+1}\right),$$

the bounds (2.14) hold when $m \leqslant n \leqslant 2m$.

Now fix $m \geqslant 1$, let $N \geqslant 2m+1$ and assume that (2.14) holds when $m \leqslant n \leqslant N-1$. Using (2.11) followed by Lemma 2.5 (a–c),

$$\begin{aligned}\nu(N,m) = \frac{1}{N}\sum_{k=N-m}^{N-1} A(k,m) &> \frac{1}{N}\sum_{k=N-m}^{N-1} \rho(k/m) > \frac{1}{N}\sum_{k=M-n}^{N-1}\int_{k}^{k+1} \rho(t/m)\,dt \\ &= \frac{1}{N}\int_{N-m}^{N} \rho(v/m)\,dv = \frac{1}{N/m}\int_{N/m-1}^{N/m} \rho(v)\,dv = \rho(N/m)\end{aligned}$$

and

$$\begin{aligned}\nu(N,m) &\leqslant \frac{1}{N}\sum_{k=N-m}^{N-1} \rho\left(\frac{k+1}{m+1}\right) \leqslant \frac{1}{N}\sum_{k=N-m}^{N-1}\int_{k-1}^{k} \rho\left(\frac{t+1}{m+1}\right)\,dt \\ &= \frac{m+1}{N}\int_{\frac{N-m}{m+1}}^{\frac{N}{m+1}} \rho(v)\,dv \\ &= \frac{m+1}{N}\int_{\frac{N-m}{m+1}}^{\frac{N+1}{m+1}} \rho(v)\,dv - \frac{m+1}{N}\int_{\frac{N}{m+1}}^{\frac{N+1}{m+1}} \rho(v)\,dv \\ &= \frac{N+1}{N}\rho\left(\frac{N+1}{m+1}\right) - \frac{m+1}{N}\int_{\frac{N}{m+1}}^{\frac{N+1}{m+1}} \rho(v)\,dv.\end{aligned}$$

The final integral on the right side is $\geqslant \frac{1}{m+1}\rho\left(\frac{N+1}{m+1}\right)$ and thus $\nu(n,m) \leqslant \rho\left(\frac{N+1}{m+1}\right)$. The claimed bounds (2.14) now follow by induction on n.

Now we have

$$\frac{n}{m} - \frac{n+1}{m+1} = \frac{n-m}{m(m+1)} \leqslant \frac{n}{m^2}.$$

Thus, by Lemma 2.5 (d),

$$\rho\left(\frac{n+1}{m+1}\right) \leqslant \rho\left(\frac{n}{m}\right)\mathrm{e}^{O((n/m^2)\log(2u))} \leqslant \rho\left(\frac{n}{m}\right)\mathrm{e}^{O(u\log(u+1)/m)}$$

When $\sqrt{n\log n} \leqslant m \leqslant n$, $u\log(u+1)/m \ll 1$ and (2.15) follows. □

Comparing Theorems 2.1 and 2.6, we immediately conclude that

$$\rho(u) \ll \mathrm{e}^{-u\log u+u}. \tag{2.17}$$

The "100 prisoners problem"

Imagine a prison holding 100 prisoners. They are offered to play a game, the reward being freedom for all if they win; but they *all* must win in order for any to go free. The prisoners are numbered 1 to 100. Inside a room are 100 boxes, and the numbers 1 through 100 are placed in these boxes in random order. One by one, the prisoners are led into the room and allowed to open 50 boxes. If a prisoner finds his own number in one of the boxes, he wins. The prisoners are allowed to discuss strategy before the game begins, but then are separated and allowed no communication whatsoever (e.g., one prisoner cannot mark the boxes indicating which number is inside). Is there a strategy that allows all of them to win with large probability?

Naively, if each prisoner chooses 50 boxes at random, then each has a $1/2$ chance of winning, but there is only a $1/2^{100}$ chance that they all win, and go free. There is a much better strategy, based on observing that the number inside the boxes form a permutation of [100] (we can think of the boxes as lying in a row, 1st, 2nd, ...). The strategy for each prisoner number k is thus: first open the k-th box. If the number is k, he wins. Otherwise, if box k contains the number m, next open box m. Continue in this manner until either he finds his own number (win) or has opened 50 boxes without finding his own number (lose). Under what conditions does prisoner k win with this strategy? He is essentially "following the cycle containing k", and if the cycle length is $\leqslant 50$ he will win. Thus, *if there are no cycles of length 50 or more*, then everyone wins! The likelihood of this is $A(100,50)$, and by (2.16) this equals

$$1 - H_{100} + H_{50} \approx 0.31$$

Thus, the prisoners have a 31% chance of all going free.

Next we develop a recursive formula for $\psi(x,y)$ analogous to (2.11) and based on an idea of Hildebrand.

Lemma 2.7. *For $x \geqslant y \geqslant 2$ we have*

$$\Psi(x,y) = \frac{1}{\log x}\sum_{p\leqslant y}(\log p)\Psi\left(\frac{x}{p},y\right) + O\left(\frac{x}{\log x}\right).$$

Proof. We start with

$$\Psi(x,y)\log x = \sum_{\substack{n\leqslant x\\ P^+(n)\leqslant y}}\log(x/n) + \sum_{\substack{n\leqslant x\\ P^+(n)\leqslant y}}\sum_{p^k\mid n}\log p.$$

The first sum is $\ll \sum_{n\leqslant x}(x/n)^{1/2} \ll x$. In the second sum, let $n = mp^k$, so that $P^+(m)\leqslant y$ and $m\leqslant x/p^k$. The terms with $k=1$ have sum

$$\sum_{p\leqslant y}(\log p)\sum_{\substack{m\leqslant x/p\\ P^+(m)\leqslant y}} 1 = \sum_{p\leqslant y}(\log p)\Psi\left(\frac{x}{p},y\right).$$

Likewise, the terms with $k>1$ contribute

$$\sum_{\substack{p\leqslant y\\ k\geqslant 2}}\Psi\left(\frac{x}{p^k},y\right) \leqslant \sum_{\substack{p\leqslant y\\ k\geqslant 2}}\frac{x}{p^k} \ll x.$$ □

Theorem 2.8. *For $x\geqslant y\geqslant 3$ we have $\Psi(x,y) = x\rho(u) + O(x/\log y)$, where $u = \frac{\log x}{\log y}$.*

The proof of Theorem 2.8 is Exercise 2.1 below.

Theorem 2.8 provides an asymptotic formula for $\Psi(x,y)$ as long as $1/\log y = o(\rho(u))$. By Lemma 2.5 (f), this happens only for $u \ll \frac{\log_2 x}{\log_3 x}$. In fact, the asymptotic $\Psi(x,y)\sim x\rho(u)$ is true in a large range of x,y; see [**47**] or [**66**, Ch. III.5] for specific statements.

4. Exercises

Exercise 2.1. For $x \geqslant y \geqslant 2$ let $u = \frac{\log x}{\log y}$.

(a) Show that $\Psi(x,y) = x\rho(u) + O(x/\log x)$ for $y \leqslant x \leqslant y^2$.

(b) Define $\Delta(x,y)$ by $\Psi(x,y) = x(\rho(u) + \Delta(x,y))$. With y fixed, let $\Delta_k := \max_{y \leqslant x \leqslant y2^k} |\Delta(x,y)|$. Use Lemma 2.7 to prove

$$\Delta_k \leqslant \frac{\log y + O(1)}{\log(y2^{k-1})}\Delta_{k-1} + O\left(\frac{1}{\log(y2^{k-1})}\right).$$

(c) use (a) and (b) to prove Theorem 2.8.

Exercise 2.2. Let

$$G = 1 - \int_1^\infty \frac{\rho(u)}{u^2}\,du = 0.624329988\ldots$$

G is known as the "Golomb-Dickman constant", although it was first written down by de Bruijn.

(a) Let $C^+(\sigma)$ denote the length of the largest cycle in σ. Show that $\mathbb{E}_n C^+(\sigma) \sim Gn$ as $n \to \infty$.

(b) Show that $\mathbb{E}_x \log P^+(n) \sim G \log x$ as $x \to \infty$.

Exercise 2.3. Define a function $\rho_2(u)$ by $\rho_2(u) = 1$ for $0 \leqslant u \leqslant 1$ and

$$\rho_2(u) = \rho(u) + \int_0^{u-1} \frac{\rho(w)}{u-w}\,dw \qquad (u \geqslant 1).$$

(a) For a permutation $\sigma \in \mathcal{S}_n$, let $k_2(\sigma)$ denote the length of the 2nd largest cycle (it may equal the length of the largest cycle), and let $k_2(\sigma) = 0$ if σ has only one cycle. Show that, uniformly for $1 \leqslant m \leqslant n$ and $u = n/m$, that

$$\mathbb{P}_\sigma(k_2(\sigma) \leqslant m) = \rho_2(u) + O\left(\frac{1+\log u}{m}\right).$$

(b) Let $q_2(n)$ denote the 2nd largest prime factor of an integer n (it may equal the largest prime factor, if $P^+(n)^2|n$), and define $q_2(n) = 0$ if n is prime. Show that, uniformly for $2 \leqslant y \leqslant x$ and $u = \frac{\log x}{\log y}$,

$$\mathbb{P}_x(q_2(n) \leqslant y) = \rho_2(u) + O\left(\frac{1+\log u}{\log y}\right).$$

(c) Show that $\rho_2(u) \sim c/u$ as $u \to \infty$, where $c = \int_0^\infty \rho(w)\,dw$.

CHAPTER 3

Integers without small prime factors and permutations without small cycles

1. Permutations without small cycles

For $1 \leqslant m \leqslant n$, let

$$U_{n,m} = \mathbb{P}_{\sigma\in\mathcal{S}_n}\big(C_j(n) = 0 \ \ (1 \leqslant j \leqslant m)\big).$$

In particular, $U_{n,0} = 1$. Based on our heuristic model, $U_{n,m}$ 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 $Z_1, \dots, Z_m$ are independent. This probability equals $\mathrm{e}^{-H_m} \approx \frac{\mathrm{e}^{-\gamma}}{m}$. This cannot be expected to hold for large m, for example $U_{n,m} = 1/n$ if $m \geqslant n/2$ (permutations lacking cycles of length $\leqslant n/2$ must be n-cycles). A special case of Corollary 1.11 (with $\lambda = 0$) implies that

$$U_{n,m} \ll \frac{1}{m} \tag{3.1}$$

uniformly for $1 \leqslant m \leqslant n$. Our aim in this section is to prove strong asymptotics for $U_{n,m}$ throughout the range $1 \leqslant m \leqslant n$.

As a first attempt, we'll use inclusion-exclusion, obtaining for any $\ell \geqslant 1$ the formula

$$U_{n,m} = \mathbb{E}_\sigma \mathbb{1}(C_{[m]}(\sigma) = 0) = \sum_{r=0}^{\ell}(-1)^r \mathbb{E}_\sigma \binom{C_{[m]}(\sigma)}{r} + O\left(\binom{C_{[m]}(\sigma)}{\ell+1}\right). \tag{3.2}$$

To evaluate the right side of (3.2) we derive a generalization of Lemma 1.1.

Lemma 3.1. *Let $I \subseteq [n]$ and let $k \geqslant 0$.*

$$\mathbb{E}_\sigma \binom{C_I(\sigma)}{k} \leqslant \frac{H(I)^k}{k!},$$

with equality if and only if $k\,(\max I) \leqslant n$.

Proof. For non-negative integers $x_1, \dots, x_t, k$ we have

$$\binom{x_1 + \cdots + x_t}{k} = \sum_{i_1+\cdots+i_t=k} \prod_{j=1}^{t} \binom{x_j}{i_j}.$$

Thus, since $C_I(\sigma) = \sum_{r\in I} C_r(\sigma)$,

$$\mathbb{E}_\sigma \binom{C_I(\sigma)}{k} = \sum_{\sum_{r\in I} k_r = k} \mathbb{E}_\sigma \prod_{r\in I} \binom{C_r(\sigma)}{k_r}.$$

We apply Lemma 1.1 to the expectation on the right side, followed by the multinomial theorem, obtaining

$$\mathbb{E}_\sigma \binom{C_I(\sigma)}{k} \leqslant \sum_{\sum_{r\in I} k_r = k} \prod_{r\in I} \frac{(1/r)^{k_r}}{k_r!} = \frac{H(I)^k}{k!},$$

with equality if and only if $\sum_{r\in I} rk_r \leqslant n$ for all choices of the k_r. This latter condition clearly holds if $k(\max I) \leqslant n$. On the other hand, if $k(\max I) > n$ then there are terms with $\sum_{r\in I} rk_r > n$, e.g. taking $k_{\max I} = k$, $k_r = 0$ for other r. □

Theorem 3.2. *Let $1 \leqslant m \leqslant n$ and set $u = n/m$. Then*

$$U_{n,m} = \mathrm{e}^{-H_m} + O\bigg(\Big(\frac{\mathrm{e}(\log m+1)}{u}\Big)^u\bigg).$$

Proof. The bound is trivial if $u < \mathrm{e}(\log m+1)$, thus we may assume that $u \geqslant \mathrm{e}(\log m+1)$. Let $\ell = \lfloor u\rfloor = \lfloor n/m\rfloor$. For $0 \leqslant r \leqslant \ell$, $r\max I_1 \leqslant n$, and thus applying Lemma 3.1 to (3.2), we obtain

$$\begin{aligned} U_{n,m} &= \mathbb{E}_\sigma \sum_{r=0}^{\ell} (-1)^r \binom{C_{[m]}(\sigma)}{r} + O\left(\binom{C_{[m]}(\sigma)}{\ell+1}\right) \\ &= \sum_{r=0}^{\ell} (-1)^r \frac{H_m^r}{r!} + O\left(\frac{H_m^{\ell+1}}{(\ell+1)!}\right). \end{aligned}$$

Since $\ell+1 > \mathrm{e}(\log m+1) \geqslant \mathrm{e}H_m$, the sum equals $\mathrm{e}^{-H_m} + O(H_m^{\ell+1}/(\ell+1)!)$. Finally, since $H_m \leqslant \log m+1$ and $(\ell+1)! \geqslant ((\ell+1)/\mathrm{e})^{\ell+1} \geqslant (u/\mathrm{e})^u$ we obtain the claimed bound. □

The inclusion-exclusion identity (3.2) corresponds to the original Brun sieve technique. The bound in Theorem 3.2 is nontrivial only for $u \gg \log m$, that is, when $m \ll n/\log n$. When u is large, however, the error term is very tiny compared to the main term $\mathrm{e}^{-H_m} \asymp 1/m$.

When u is bounded, the behavior of $U_{n,m}$ is more complex. We will derive a recurrence for $U_{n,m}$ in (3.6) below, and use it to obtain an asymptotic for $U_{n,m}$ when u is small. We first must introduce the Buchstab function $\omega(u)$, defined recursively for $u \geqslant 1$ by

$$\omega(u) = \frac{1}{u} \ \ (1 \leqslant u \leqslant 2), \qquad u\omega(u) = 1 + \int_1^{u-1} \omega(v)\,dv \ \ (u > 2). \tag{3.3}$$

An easy induction argument shows that $\omega(u)$ is continuous, differentiable except at the point $u = 2$, and satisfies $1/2 \leqslant \omega(u) \leqslant 1$ for all $u \geqslant 1$. Differentiating the integral equation in (3.3) yields

$$\omega'(u) = \frac{\omega(u-1)-\omega(u)}{u} = -\frac{1}{u}\int_{u-1}^{u} \omega'(v)\,dv \qquad (u > 2). \tag{3.4}$$

Lemma 3.3. *We have $\omega'(u) \ll 1/\lfloor u\rfloor!$. Consequently, for some $C \in [1/2, 1]$ we have*

$$\omega(u) = C + O(1/\lfloor u\rfloor!).$$

Proof. By $1/2 \leqslant \omega(u) \leqslant 1$ for all u, (3.4) gives $|\omega'(u)| \leqslant 1/(2u)$ for $u > 2$. By induction on $k \geqslant 2$ we have

$$|\omega'(u)| \leqslant \frac{1}{2u(u-1)\cdots(u-k+2)} \qquad (u \geqslant k).$$

For any u, let $k = \lfloor u\rfloor \leqslant u$. Then $|\omega'(u)| \leqslant 1/k!$. The second claim follows from the first and

$$\omega(u) - \omega(v) = \int_v^u \omega'(w)\,dw \ll \frac{1}{\lfloor v\rfloor!} \qquad (2 \leqslant v \leqslant u).$$ □

Much more is known about $\omega(u)$, in fact we have $\omega(u) = \mathrm{e}^{-\gamma} + O(1/\lfloor u\rfloor!)$, and $\omega(u) = \mathrm{e}^{-\gamma}$ changes sign infinitely many times (Maier). We will derive such an asymptotic in a indirect way using the next Theorem.

Theorem 3.4. *Suppose that m, n are integers with $1 \leqslant m \leqslant n-1$. Then*

$$\frac{1}{2m+1} \leqslant U_{n,m} \leqslant \frac{1}{m+1} \tag{3.5}$$

and

$$U_{n,m} = \frac{\omega(u)}{m}\left(1 + O\left(\frac{1}{m}\right)\right), \quad u = n/m.$$

The second part provides an asymptotic $U_{n,m} \sim \omega(u)/m$ as long as $m \to \infty$ as $n \to \infty$.

Proof. We follow the method of Granville [**40**, Theorem 2.2], beginning with an analog of the recursion (2.11). If $\sigma \in \mathcal{S}_n$ has no cycles of length $\leqslant m$, then either σ is an n-cycle, or all cycles in σ have length in $[m+1, n-m-1]$. Following the proof of (2.11), we start with

$$U_{n,m} = \frac{1}{n} + \frac{1}{n \cdot n!} \sum_{\substack{\sigma \in \mathcal{S}_n \\ C_{[m]}(\sigma)=0}} \sum_{\substack{\alpha \mid \sigma \\ \alpha \text{ a cycle} \\ |\alpha| \leqslant n-m-1}} |\alpha|.$$

With $\ell = |\alpha|$ fixed, there are $\binom{n}{\ell}(\ell-1)!$ ways to choose α. Writing $\sigma = \alpha\beta$, there are $(n-\ell)!U(n-\ell, m)$ ways to choose β. Letting $k = n - \ell$, we thus we obtain

$$U_{n,m} = \frac{1}{n} + \frac{1}{n} \sum_{m+1 \leqslant k \leqslant n-m-1} U_{k,m}. \tag{3.6}$$

If $m+1 \leqslant n \leqslant 2m+1$, then $U_{n,m} = 1/n$ and thus $\frac{1}{2m+1} \leqslant U_{n,m} \leqslant \frac{1}{m+1}$. Now suppose that $N \geqslant 2m+2$ and that (3.5) holds for $m+1 \leqslant n \leqslant N-1$. By (3.6),

$$NU_{N,m} \leqslant 1 + \sum_{m+1 \leqslant k \leqslant N-m-1} \frac{1}{m+1} = 1 + \frac{N-2m-1}{m+1} \leqslant \frac{N}{m+1}$$

and

$$NU_{N,m} \geqslant 1 + \sum_{m+1 \leqslant k \leqslant N-m-1} \frac{1}{2m+1} = \frac{N}{2m+1}.$$

Thus, (3.5) follows by induction on n.

The second inequality is true when $1 \leqslant u = n/m \leqslant 2$ since then $U_{n,m} = 1/n = \omega(u)/m$. We now proceed by induction on $N = \lfloor u \rfloor$ with m fixed. Let

$$\Delta(n,m) = mU_{n,m} - \omega(n/m), \qquad \Delta_N := \max_{m+1 \leqslant n \leqslant mN} |\Delta(n,m)|$$

In particular, $\Delta_2 = 0$. Now suppose that $N \geqslant 2$ and that $mN < n \leqslant m(N+1)$. By (3.6),

$$\omega(n/m) + \Delta(n,m) = \frac{m}{n} + \frac{1}{n}\sum_{k=m+1}^{n-m-1} \omega\left(\frac{k}{m}\right) + \frac{1}{n}\sum_{k=m+1}^{n-m-1} \Delta(k,m). \tag{3.7}$$

If $m+1 \leqslant k \leqslant n-m-1$, then $n-k \leqslant mN$, and thus the second sum on the right side is bounded in absolute value by $(n-2m-1)\Delta_N$. Writing $u = n/m$ and using Euler's summation formula together with Lemma 3.3, the first sum equals

$$\begin{aligned}
\sum_{k=m+1}^{n-m-1} \omega\left(\frac{k}{m}\right) &= -\omega(u-1) + \sum_{k=m+1}^{n-m} \omega\left(\frac{k}{m}\right) \\
&= -\omega(u-1) + \int_m^{n-m} \omega(t/m)\,dt + \int_m^{n-m} \frac{t - \lfloor t \rfloor}{m} \omega'(t/m)\,dt \\
&= O(1) + m\int_1^{u-1} \omega(v)\,dv.
\end{aligned}$$

By (3.3), the final integral equals $u\omega(u) - 1$, and hence

$$|\Delta(n,m)| \leqslant \left(1 - \frac{2}{N+1}\right)\Delta_N + O\left(\frac{1}{n}\right)$$

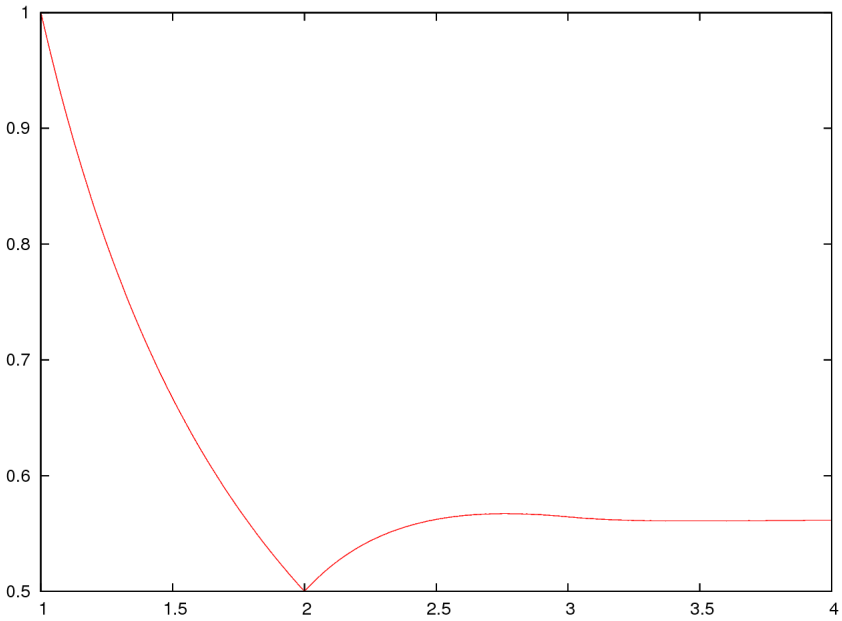

FIGURE 1. Buchstab's function from $1 \leqslant u \leqslant 4$.

and thus

$$\Delta_{N+1} \leqslant \left(1 - \frac{2}{N+1}\right)\Delta_N + O\left(\frac{1}{mN}\right).$$

Iterating this gives

$$\Delta_N \ll \frac{1}{m} \qquad (N \geqslant 2)$$

and the second claim in the theorem follows. □

Combining Theorems 3.2 and 3.4, we derive a strong asymptotic for $\omega(u)$ and a strong uniform asymptotic for $U_{n,m}$. In figure 1 is a graph of $\omega(u)$ for $1 \leqslant u \leqslant 4$. The rapid convergence to $\mathrm{e}^{-\gamma}$ is evident.

THEOREM 3.5. *We have* $\omega(u) = \mathrm{e}^{-\gamma} + O(\mathrm{e}^{-u\log u + O(u)})$.

PROOF. In light of Lemma 3.3 it suffices to evaluate $C = \lim_{u\to\infty}\omega(u)$. Let m be large, $n = m^2, u = m$. By Theorems 3.2 and 3.4, we have

$$U_{m^2,m} = \frac{\omega(m)}{m}\left(1 + O\left(\frac{1}{m}\right)\right) = \mathrm{e}^{-H_m}\left(1 + O\left(m\left(\frac{\mathrm{e}(1+\log m)}{m}\right)^m\right)\right)$$

ad it follows that $C = \mathrm{e}^{-\gamma}$. □

THEOREM 3.6. *For any* $1 \leqslant m \leqslant n-1$ *we have*

$$U_{n,m} = \mathrm{e}^{-H_m}(1 + O(\mathrm{e}^{-u/5})) \qquad (u = n/m).$$

PROOF. When $u > 5\log m$, Theorems 3.2 and 3.5 gives

$$U_{n,m} = \mathrm{e}^{-H_m}(1 + O(\mathrm{e}^{-u/4})).$$

When $u \leqslant 5\log m$, Theorems 3.4 and 3.5 imply

$$U_{n,m} = \frac{\omega(u)}{m}\left(1 + O\left(\frac{1}{m}\right)\right) = \mathrm{e}^{-H_m}(1 + O(\mathrm{e}^{-u/5})).$$

□

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. A special case of Corollary 1.15 (with $\lambda = 0$) implies that

$$\Phi(x,z) = \#\{n \leqslant x : \omega(n,z) = 0\} \ll x(\log z)^{-Q(0)} = \frac{x}{\log z} \asymp x\prod_{p\leqslant z}\Big(1-\frac{1}{p}\Big), \tag{3.8}$$

uniformly for $2 \leqslant z \leqslant x$. Here $\omega(n,z)$ is the number of distinct prime factors of n that are $\leqslant z$.

Following what we did with permutations, we first prove a bound for $\Phi(x,z)$ which is very strong for small z and then by another method work out a bound which is good for large z.

Theorem 3.7. *Uniformly for $x \geqslant 2$, $2 \leqslant z \leqslant x^{1/(4.5\log_2 x)}$ we have*

$$\Phi(x,z) = x\prod_{p\leqslant z}\Big(1-\frac{1}{p}\Big) + O\big(x\mathrm{e}^{-u/2}\big) \quad u = \frac{\log x}{\log z};$$

Proof. We may assume that x is sufficiently large. Following the proof of Lemma 3.2, we apply "Brun's pure sieve". Let $\ell \geqslant 1$, and apply inclusion-exclusion to obtain

$$\mathbb{1}(\omega(n,z)=0) = \sum_{r=0}^{\ell}(-1)^r\binom{\omega(n,z)}{r} + O\left(\binom{\omega(n,z)}{\ell+1}\right).$$

We sum over x and use

$$\sum_{n\leqslant x}\binom{\omega(n,z)}{r} = \sum_{p_1<\cdots<p_r\leqslant z}\Big\lfloor\frac{x}{p_1\cdots p_r}\Big\rfloor = \sum_{p_1<\cdots<p_r\leqslant z}\Big(\frac{x}{p_1\cdots p_r}+O(1)\Big).$$

The totality of the $O(1)$ terms is

$$\ll \sum_{r=0}^{\ell}\#\{d\leqslant z^r : \omega(d)=r\} \leqslant z^\ell.$$

Let T be the set of primes $\leqslant z$, and let $H = H(T)$. By Mertens' sum estimate (0.5), $H(T) = \log_2 z + O(1)$. By Theorem 1.6,

$$\sum_{n\leqslant x}\binom{\omega(n,z)}{\ell+1} \leqslant x\,\frac{H^{\ell+1}}{(\ell+1)!}.$$

We get

$$\Phi(x,z) = x\sum_{r=0}^{\ell}(-1)^r\sum_{p_1<\cdots<p_r\leqslant z}\frac{1}{p_1\cdots p_r} + O\left(z^\ell + x\,\frac{H^{\ell+1}}{(\ell+1)!}\right).$$

Extending the sum on r to all non-negative integers, we have using (0.4)

$$\sum_{r=0}^{\infty}(-1)^r\sum_{p_1<\cdots<p_r\leqslant z}\frac{1}{p_1\cdots p_r} = \sum_{P^+(d)\leqslant z}\frac{\mu(d)}{d} = \prod_{p\leqslant z}\Big(1-\frac{1}{p}\Big).$$

Now assume that $\ell \geqslant 2H$. Using (0.1), we have

$$\left|\sum_{r=\ell+1}^{\infty}(-1)^r\sum_{p_1<\cdots<p_r\leqslant z}\frac{1}{p_1\cdots p_r}\right| \leqslant \sum_{r=\ell+1}^{\infty}\frac{H^r}{r!} \ll \frac{H^{\ell+1}}{(\ell+1)!}.$$

We conclude that

$$\Phi(x,z) = x\prod_{p\leqslant z}\Big(1-\frac{1}{p}\Big) + O\left(z^\ell + x\,\frac{H^{\ell+1}}{(\ell+1)!}\right).$$

If $2 \leqslant z \leqslant \mathrm{e}^{\sqrt{\log x}}$, equivalently $\sqrt{\log x} \leqslant u \leqslant \frac{\log x}{\log 2}$, take $\ell = \lfloor u/5 \rfloor$ so that $\ell \geqslant 2H$ if x is large enough. Then $z^\ell \leqslant x^{1/5} \leqslant x\mathrm{e}^{-u/2}$, and

$$\frac{H^{\ell+1}}{(\ell+1)!} \leqslant \left(\frac{5\mathrm{e}H}{u}\right)^{u/5} \ll \mathrm{e}^{-u/2}.$$

If $\mathrm{e}^{\sqrt{\log x}} \leqslant z \leqslant x^{1/(4.5\log_2 x)}$, equivalently $4.5\log_2 x \leqslant u \leqslant \sqrt{\log x}$, we take $\ell = \lfloor u-1 \rfloor$. Then

$$\ell \geqslant u - 2 \geqslant 4.5\log_2 x - 2 \geqslant 4.5H + 2$$

for large x. Here $z^\ell \leqslant x/z \leqslant x\mathrm{e}^{-u}$ and

$$\frac{H^{\ell+1}}{(\ell+1)!} \leqslant \left(\frac{\mathrm{e}H}{u-1}\right)^{u-1} \ll \left(\frac{\mathrm{e}}{4.5}\right)^{u-1} \ll \mathrm{e}^{-u/2}. \qquad \square$$

When z is large, the asymptotics of $\Phi(x,z)$ are related to the Buchstab function $\omega(u)$ defined in (3.3).

Theorem 3.8. *Uniformly for $2 \leqslant z \leqslant x$ we have*

$$\Phi(x,z) = \frac{x\omega(u) - z}{\log z} + O\left(\frac{x}{\log^2 z}\right), \qquad u = \frac{\log x}{\log z}.$$

This provides an asymptotic formula $\Phi(x,z) \sim \omega(u)\frac{x}{\log z}$ as long as $z \to \infty$ and $x = o(x)$ as $x \to \infty$. Our proof is based on a recurrence formula similar to (3.6).

Lemma 3.9. *(i) When $2 \leqslant z \leqslant x \leqslant z^2$ we have*

$$\Phi(x,z) = \frac{x\omega(u) - z}{\log z} + O\left(\frac{x}{\log^2 x}\right).$$

(ii) When $z \geqslant 2$ and $x \geqslant z^2$ we have

$$(\log x)\Phi(x,z) = x + \sum_{z < p \leqslant x/z} (\log p)\Phi(x/p, z) + O\left(\frac{x}{\log z}\right).$$

Proof. When $z \leqslant x \leqslant z^2$, the Prime Number Theorem gives

$$\Phi(x,z) = 1 + \pi(x) - \pi(z) = \frac{x}{\log x} - \frac{z}{\log z} + O\left(\frac{x}{\log^2 x}\right) = \frac{x\omega(u) - z}{\log z} + O\left(\frac{x}{\log^2 x}\right),$$

proving (i). Here we used that $\omega(u) = 1/u$ for $1 \leqslant u \leqslant 2$.

Now suppose $2 \leqslant z \leqslant x^{1/2}$. We start with the fundamental theorem of arithmetic in the form

$$\log x = \log \frac{x}{n} + \log n = \log \frac{x}{n} + \sum_{p^k \mid n} \log p.$$

Thus,

$$(\log x)\Phi(x,z) = \underbrace{\sum_{\substack{n \leqslant x \\ P^-(n) > z}} \log \frac{x}{n}}_{S_1} + \underbrace{\sum_{\substack{n \leqslant x \\ P^-(n) > z}} \sum_{p^k \mid n} \log p}_{S_2}.$$

In S_1, break up the summands into intervals $x\mathrm{e}^{-j} < n \leqslant x\mathrm{e}^{1-j}$ for integers $j \geqslant 1$. Using (3.8)

$$S_1 \leqslant \sum_{j \geqslant 1} j\Phi(x\mathrm{e}^{1-j}, z) \ll \sum_{j \geqslant 1} \frac{xj\mathrm{e}^{1-j}}{\log z} \ll \frac{x}{\log z}.$$

We have

$$S_2 = \sum_{\substack{p^k \leqslant x \\ p > z}} (\log p)\Phi(x/p^k, z).$$

Using (3.8) again, the terms with $k \geqslant 2$ contribute

$$\ll \sum_{\substack{p^k \leqslant x \\ k \geqslant 2 \\ p > z}} (\log p) \frac{x}{p^k \log z} \ll \frac{x}{\log z} \sum_{p > z} \frac{\log p}{p^2 - p} \ll \frac{x}{z \log z}.$$

The terms with $k = 1$ give, by the Prime Number Theorem,

$$\sum_{z < p \leqslant x/z} (\log p) \Phi(x/p, z) + \sum_{x/z < p \leqslant x} \log p = \sum_{z < p \leqslant x/z} (\log p) \Phi(x/p, z) + x + O\left(\frac{x}{\log z}\right).$$

This completes the proof of (ii). □

Now we argue that Lemma 3.9 (ii) is analogous to the recurrence (3.6). Let

$$V_{n,m} = \frac{\Phi(\mathrm{e}^n, \mathrm{e}^m)}{\mathrm{e}^n}.$$

Assuming that $\Phi(x, z)/x$ is slowly varying in x and in z, we get from Lemma 3.9 (ii)

$$n V_{n,m} \approx \sum_{k=m+1}^{n-m} V_{n-k,m} \sum_{\mathrm{e}^{k-1} < p \leqslant \mathrm{e}^k} \frac{\log p}{p} \approx \sum_{k=m+1}^{n-m} V_{n-k,m}$$

using Mertens' estimate (0.6).

Proof of Theorem 3.8. Let z_0 be a sufficiently large constant. The statement is trivial if $z \leqslant z_0$ and also it follows from (3.8) when $z > x^{1/2}$, thus we may assume that $z_0 \leqslant z \leqslant x^{1/2}$.

We iterate the recurrence in Lemma 3.9 (ii) in a manner similar to the way we analyzed (3.6), however there are more delicate error terms to analyze. Define $\Delta(x, z)$ by

$$\frac{\log z}{x} \Phi(x, z) = \omega(u) - \frac{z}{x} + \Delta(x, z),$$

where $u = \frac{\log x}{\log z}$. With z fixed, define

$$\Delta_N^* = \max_{z \leqslant x \leqslant z^N} |\Delta(x, z)| \qquad (N = 2, 3, \ldots).$$

By Lemma 3.9 (i), we have

$$\Delta_2^* \ll \frac{1}{\log z}.$$

Now suppose that $N \geqslant 3$ and $z^{N-1} < x \leqslant z^N$. Divide Lemma 3.9 (ii) by ux, obtaining

$$\frac{\log z}{x} \Phi(x, z) = \frac{1}{u} + O\left(\frac{1}{u \log z}\right) + \frac{1}{u \log z} \sum_{z < p \leqslant x/z} \frac{\log p}{p} \left(\frac{\log z}{x/p} \Phi(x/p, z)\right).$$

Since $z/x \leqslant 1/\sqrt{x} < \frac{1}{u \log z}$ by our assumptions on z and u, we get

$$\omega(u) + \Delta(x, z) = \frac{1}{u} + O\left(\frac{1}{u \log z}\right) + \frac{1}{u \log z} \sum_{z < p \leqslant x/z} \frac{\log p}{p} \left(\omega\left(\frac{\log(x/p)}{\log z}\right) - \frac{zp}{x} + \Delta\left(\frac{x}{p}, z\right)\right). \tag{3.9}$$

In (3.9), the summands $-zp/x$ contribute, by the Prime Number Theorem,

$$\ll \frac{z/x}{u \log z} \sum_{z < p \leqslant x/z} \log p \ll \frac{1}{u \log z}.$$

Since $x/p < x/z < z^{N-1}$, the summands $\Delta(x/p, z)$ contribute an amount which in absolute value does not exceed

$$\frac{\Delta_{N-1}^*}{u \log z} \sum_{z < p \leqslant x/z} \frac{\log p}{p} = \frac{\Delta_{N-1}^*}{\log x} (\log x - 2 \log z + O(1)) \leqslant (1 - 1/N) \Delta_{N-1}^*$$

if z is large enough, where we used Mertens' estimate (0.6). Using (0.6), partial summation and the rapid decay of $\omega'(u)$ (Theorem 3.3), we obtain

$$\sum_{z<p\leqslant x/z}\frac{\log p}{p}\omega\left(\frac{\log(x/p)}{\log z}\right)=\int_z^{x/z}\frac{1}{t}\omega\left(\frac{\log(x/t)}{\log z}\right)\,dt++\int_z^{x/z}O(\mathrm{e}^{-\sqrt{\log t}})\omega'\left(\frac{\log(x/t)}{\log z}\right)\frac{dt}{t\log z}+O(1)$$
$$=(\log z)\int_1^{u-1}\omega(v)\,dv+O(1).$$

Inserting all of these estimates into (3.9), we find that

$$|\Delta(x,z)|\leqslant\left|-\omega(u)+\frac{1}{u}+\frac{1}{u}\int_1^{u-1}\omega(v)\,dv\right|+\left(1-\frac{1}{N}\right)\Delta_{N-1}^*+O\left(\frac{1}{u\log z}\right)$$
$$=\left(1-\frac{1}{N}\right)\Delta_{N-1}^*+O\left(\frac{1}{N\log z}\right)$$

using the recurrence (3.3) and that $N-1\leqslant u\leqslant N$. Taking a maximum over all $z^{N-1}<x\leqslant z^N$ we get

$$\Delta_N^*\leqslant\max\left(\Delta_{N-1}^*,\left(1-\frac{1}{N}\right)\Delta_{N-1}^*+O\left(\frac{1}{N\log z}\right)\right).$$

Iterating this gives

$$\Delta_N^*\ll\frac{1}{\log z}\qquad(N=2,3,\dots).$$

From the definition of Δ_N^* we conclude that

$$\Delta(x,z)\ll\frac{1}{\log z}\qquad(u\geqslant 2).$$

This completes the proof. □

An unusual application of these theorems is the evaluation of the constant in the Mertens' product formula (0.7). It is rather straightforward to obtain a version of (0.7) where $\mathrm{e}^{-\gamma}$ is replaced by some unspecified constant, and evaluation of the constant is not that easy.

Corollary 3.10. *Assume a weak form of Mertens' product formula*

$$\prod_{p\leqslant z}\left(1-\frac{1}{p}\right)\asymp\frac{1}{\log z}\qquad(z\geqslant 2).\tag{3.10}$$

Then

$$\prod_{p\leqslant z}\left(1-\frac{1}{p}\right)\sim\frac{\mathrm{e}^{-\gamma}}{\log z}\qquad(z\to\infty).$$

Proof. This proof was suggested by Granville. It is easy to check that in the proof of Theorems 3.7 and 3.8, we did not use (0.7) anywhere in the strong form. Fix z and let $x=z^{10\log_2 z}$. Then $u=\frac{\log x}{\log z}=10\log_2 z>5\log_2 x$ if z is large enough. Using (3.10) and Theorem 3.7, we have

$$\Phi(x,z)=x\prod_{p\leqslant z}\left(1-\frac{1}{p}\right)\left(1+O(\mathrm{e}^{-u/2}\log z)\right)=x\prod_{p\leqslant z}\left(1-\frac{1}{p}\right)\left(1+O(1/\log^4 z)\right).$$

On the other hand, using Theorem 3.8, followed by Theorem 3.5,

$$\Phi(x,z)=\frac{x\omega(u)}{\log z}\left(1+O\left(\frac{1}{\log z}\right)\right)=\frac{x\mathrm{e}^{-\gamma}}{\log z}\left(1+O\left(\frac{1}{\log z}\right)\right).$$

The claim follows. □

Theorem 3.11. *Uniformly for $2 \leqslant z \leqslant x$ we have*

$$\Phi(x,z) = x\prod_{p\leqslant z}\left(1-\frac{1}{p}\right)\left(1+O(\mathrm{e}^{-u/5})\right).$$

Proof. When $u \geqslant 4.8\log_2 x$, equivalently, $z \leqslant x^{1/4.8\log_2 x}$, we use Theorem 3.7 and get

$$\Phi(x,z) = x\prod_{p\leqslant z}\left(1-\frac{1}{p}\right)\left(1+O(\mathrm{e}^{-u/2}\log z)\right) = x\prod_{p\leqslant z}\left(1-\frac{1}{p}\right)\left(1+O(\mathrm{e}^{-u/5})\right).$$

When $1 \leqslant u \leqslant 2$, the claim follows from (3.8). Now suppose that $2 \leqslant u \leqslant 4.8\log_2 x$. By Theorem 3.8, followed by Mertens' estimate (0.7), we have

$$\Phi(x,z) = \frac{x\omega(u)}{\log z}\left(1+O\left(\frac{1}{\log z}\right)\right) = x\mathrm{e}^{\gamma}\omega(u)\prod_{p\leqslant z}\left(1-\frac{1}{p}\right)\left(1+O\left(\frac{1}{\log z}\right)\right). \tag{3.11}$$

Now

$$\frac{1}{\log z} = \frac{u}{\log x} \ll \frac{u}{\mathrm{e}^{u/4.8}} \ll \mathrm{e}^{-u/5}$$

and the claim follows from Theorem 3.5. □

3. Exercises

Exercise 3.1. Show that $\Phi(x,z) \asymp x/\log z$ uniformly for $x \geqslant 2z \geqslant 4$. Be careful with the case of small x.

Exercise 3.2. Show that $\Psi(x,y) \ll x\mathrm{e}^{-u}$ uniformly for all $x \geqslant y \geqslant 3$, where $u = \frac{\log x}{\log y}$.

Exercise 3.3 ([45],Exercise 03). (Integers with a large smooth part). For an integer n and $y \geqslant 2$ let n_y be the product of all prime powers dividing n with the prime $\leqslant y$. Define, for $y \leqslant z \leqslant x$ the function

$$\Theta(x,y,z) = \#\{n \leqslant x : n_y > z\}.$$

(a) Show that $\Theta(x,y,z) \leqslant \sum_{\substack{z<a\leqslant x/y\\ P^+(a)\leqslant y}} \Phi(x/a,y) + \Psi(x,y)$.

(b) Show that, for any $2 \leqslant y \leqslant z \leqslant x$ we have

$$\Theta(x,y,z) \ll x\exp\left\{-\frac{\log z}{2\log y}\right\}.$$

Exercise 3.4. (a) Show that for $1 \leqslant m \leqslant n$,

$$1 = \nu(n,m) + \sum_{k=0}^{n-m-1} U_{n-k,m}\nu(k,m),$$

where $\nu(k,m) = 1$ if $m > k$.

(b) Combine (a) with Theorems 2.6 and 3.4 to deduce that

$$\rho(u) + \int_0^{u-1}\rho(v)\omega(u-v)\,dv = 1 \qquad (u \geqslant 1).$$

Remark: This provides a 'combinatorial proof' of a purely analytic statement.

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

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

by the random vector

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

We especially desire a good approximation when k is large, as opposed to bounded (ref. Theorem 1.9). 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

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

The supremum occurs when $U = \{\omega \in \Omega : \mathbb{P}(X = \omega) > \mathbb{P}(Y = \omega)\}$, hence

$$d_{TV}(X, Y) = \sum_{\omega \in \Omega} \max\big(0, \mathbb{P}(X = \omega) - \mathbb{P}(Y = \omega)\big). \tag{4.2}$$

Replacing U by $\Omega \setminus U$, we see that $d_{TV}(X, Y) = d_{TV}(Y, X)$.

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

Lemma 4.1. *We have*

$$d_{TV}(\mathcal{C}_k, \mathcal{Z}_k) = \sum_{\mathbf{h} \in \mathbb{N}_0^k} \prod_{j=1}^{k} \frac{1}{j^{h_j} h_j!} \max\big(0, \mathrm{e}^{-H_k} - U_{n',k}\big),$$

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

Proof. From (4.2) we have

$$d_{TV}(\mathcal{C}_k, \mathcal{Z}_k) = \sum_{\mathbf{h} \in \mathbb{N}_0^k} \max\Big(0, \mathbb{P}(\mathcal{Z}_k = \mathbf{h}) - \mathbb{P}(\mathcal{C}_k = \mathbf{h})\Big).$$

Clearly,

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

Now fix $\mathbf{h}$, write $g = h_1 + 2h_2 + \cdots + kh_k$ and consider $\mathbb{P}(\mathcal{C}_k = \mathbf{h})$. If $g > n$, then $\mathbb{P}(\mathcal{C}_k = \mathbf{h}) = 0$. 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 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 (Theorem 1.2), applied to σ_1, it follows that

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

and the lemma follows. □

Theorem 4.2 (Poisson distribution of small cycles). *Let $1 \leqslant k \leqslant n$. Then*

$$d_{TV}(\mathcal{C}_k, \mathcal{Z}_k) \ll \mathrm{e}^{-n/(5k)}.$$

Proof. Consider a generic vector $\mathbf{h} = (h_1, \cdots, h_k) \in \mathbb{N}_0^k$ and let $n' = n - (h_1 + 2h_2 + \cdots + kh_k)$. If $n' > k$ then By Theorem 3.6,

$$U_{n',k} = \mathrm{e}^{-H_k}\left(1 + O\big(\mathrm{e}^{-n'/(5k)}\big)\right).$$

If $n' \leqslant k$ we'll use the trivial bound $\max(0, \mathrm{e}^{-H_k} - U_{n',k}) \leqslant \mathrm{e}^{-H_k}$, and thus for all $\mathbf{h}$ we have

$$\max\big(0, \mathrm{e}^{-H_k} - U_{n',k}\big) \ll \mathrm{e}^{-H_k - n'/(5k)}.$$

Therefore, and thus

$$\begin{aligned}\sum_{\mathbf{h}\in\mathcal{H}_1}\prod_{j=1}^{k}\frac{(1/j)^{h_j}}{h_j!}\max\big(0, \mathrm{e}^{-H_k} - U_{n',k}\big) &\ll \mathrm{e}^{-H_k - n/(5k)}\sum_{\mathbf{h}\in\mathbb{N}_0^k}\prod_{j=1}^{k}\frac{(1/j)^{h_j}\mathrm{e}^{jh_j/(5k)}}{h_j!}\\ &= \exp\left\{-H_k - \frac{n}{5k} + \sum_{j=1}^{k}\frac{\mathrm{e}^{j/(5k)}}{j}\right\}\\ &\ll \mathrm{e}^{-n/(5k)},\end{aligned}$$

using (2.1) in the last step with $u = \mathrm{e}^{1/5}$ and $w = \mathrm{e}^{1/(5k)}$. The theorem now follows from Lemma 4.1. □

Remarks. By a more sophisticated sieve method than that used to prove Theorem (2.1), see **[33]**, it is possible to prove that

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

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 **[2]**. Sharper bounds are known, and are expressed in terms of the Dickman and Buhstab functions (see **[58]**).

We almost immediately obtain the following corollary, by grouping together integers into sets.

Corollary 4.3. *Let $k \leqslant n$. Then, for any subset $T \subseteq [k]$ and $A \subseteq \mathbb{N}_0$, we have*

$$\mathbb{P}\big(C_T(\sigma) \in A\big) = \mathbb{P}\big(Z_T \in A\big) + O(\mathrm{e}^{-n/(5k)}).$$

where $Z_T \stackrel{d}{=} \mathrm{Pois}(H(T))$.

As long as $k = o(n)$ as $n \to \infty$, the error term is $o(1)$ and this establishes, in a very strong form, the validity of the Poisson model for $\mathcal{C}_k$.

2. The Kubilius model of small prime factors of integers

We will make formal a probabilistic interpretation of various results about the distribution of integers which have been stated in earlier sections. Consider a randomly chosen integers $n \in [1, x]$. Such an integer n has a canonical prime factorization as

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

We regard each of the exponents v_p as random variables (they depend on p and 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

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

Furthermore, the variables X_p are all independent. 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

$$\mathbf{V}_y = (v_p : p \leqslant y).$$

Again, $\mathbf{V}_y$ depends on x as well.

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

Lemma 4.4. *We have*

$$d_{TV}(\mathbf{X}_y, \mathbf{V}_y) = \sum_{P^+(m) \leqslant y} \max\left(0, \frac{\zeta_y}{m} - \frac{1}{\lfloor x \rfloor}\Phi\left(\frac{x}{m}, y\right)\right), \qquad \zeta_y = \prod_{p \leqslant y}\left(1 - \frac{1}{p}\right).$$

Proof. (cf. Tenenbaum [**64**]). Fix $\mathbf{u} = (u_p : p \leqslant y)$ and write $m = \prod_{p \leqslant y} p^{u_p}$. Then

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

and

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

The lemma follows from (4.2).

Theorem 4.5 (Kubilius model approximation). *Let $2 \leqslant y \leqslant x$. Then*

$$d_{TV}(\mathbf{X}_y, \mathbf{V}_y) \ll \exp\Big\{-\frac{\log x}{5\log y}\Big\}.$$

Proof. Let $\delta = 1/(5\log y)$, so that $0 < \delta \leqslant 1/3$. Let m satisfy $P^+(m) \leqslant y$. If $m \leqslant x/y^2$ then Theorem 3.11 implies that

$$\Phi\left(\frac{x}{m}, y\right) = \frac{x}{m}\zeta_y\left(1 + O(\mathrm{e}^{-\delta\log(x/m)})\right).$$

For $m > x/y^2$ we'll just use the trivial bound

$$\max\left(0, \frac{\zeta_y}{m} - \frac{1}{\lfloor x \rfloor}\Phi\left(\frac{x}{m}, y\right)\right) \leqslant \frac{\zeta_y}{m}.$$

Thus, for all m we have

$$\max\left(0, \frac{\zeta_y}{m} - \frac{1}{\lfloor x \rfloor}\Phi\left(\frac{x}{m}, y\right)\right) \ll \frac{\zeta_y}{m}\mathrm{e}^{-\delta\log(x/m)} = \frac{\zeta_y}{x^\delta m^{1-\delta}}.$$

By Lemma 4.4,

$$\begin{aligned} d_{TV}(\mathbf{X}_y, \mathbf{V}_y) &\ll \zeta_y x^{-\delta} \sum_{P^+(m) \leqslant y} m^{-1+\delta} \\ &= \zeta_y x^{-\delta} \prod_{p \leqslant y}\left(1 + \frac{1}{p^{1-\delta}} + \frac{1}{p^{2-2\delta}} + \cdots\right) \\ &\ll \frac{x^{-\delta}}{\log y}\exp\left\{\sum_{p \leqslant y}\frac{p^\delta}{p}\right\}. \end{aligned}$$

Since $p^\delta = 1 + O(\delta \log p)$, Mertens' estimates (0.5) and (0.6) imply that the final sum on p is $\log_2 y + O(1)$. The theorem follows. □

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 a set T of primes, denote

$$U_T = \sum_{p \in T} \mathbb{1}(X_p \geqslant 1), \qquad W_T = \sum_{p \in T} X_p$$

which, in the Kubilius model, are model for $\omega(n; T)$ and $\Omega(n; T)$, respectively. Since $\mathbb{E}\,\mathbb{1}(X_p \geqslant 1) = 1/p$ and $\mathbb{E}\,X_p = 1/(p-1)$ we have

$$\mathbb{E}\,U_T = H(T), \qquad \mathbb{E}\,W_T = H'(T) := \sum_{p \in T} \frac{1}{p-1}. \tag{4.3}$$

Define also

$$H''(T) := \sum_{p \in T} \frac{1}{p^2}.$$

Theorem 4.6. *Let T be a finite subset of the primes, and suppose either $Y = U_T$ or $Y = W_T$. Let $H = \mathbb{E}\,Y$, using the formulas* (4.3). *Let $Z \stackrel{d}{=} \mathrm{Pois}(H)$. Then*

$$\mathbb{P}\,(Y = k) - \mathbb{P}(Z = k) \ll \begin{cases} H''(T) \frac{H^k}{k!} \mathrm{e}^{-H} \left(\frac{1}{k+1} + \left(\frac{k-H}{H} \right)^2 \right) & 0 \leqslant k \leqslant 1.9H \\ H''(T) \mathrm{e}^{0.9H} (1.9)^{-k} & k > 1.9H. \end{cases}$$

Proof. Write $H'' = H''(T)$. When $k = 0$, $\mathbb{P}(Z = 0) = \mathrm{e}^{-H}$ and

$$\mathbb{P}(Y = 0) = \mathbb{P}(\forall p \in T : X_p = 0) = \prod_{p \in T} \left(1 - \frac{1}{p}\right) = \mathrm{e}^{-H + O(H'')} = \mathrm{e}^{-H}(1 + O(H'')),$$

and the desired inequality follows.

For $k \geqslant 1$, we work with moment generating functions. For any complex s, (0.11) implies

$$\mathbb{E}\,s^Z = \mathrm{e}^{(s-1)H}. \tag{4.4}$$

If $Y = U_T$, then $H = H(T)$, and uniformly for complex s with $|s| \leqslant 2$ we have

$$\begin{aligned} \mathbb{E}\,s^{U_T} &= \prod_{p \in T} \mathbb{E}\,s^{\mathbb{1}(X_p \geqslant 1)} = \prod_{p \in T} \left(1 + \frac{s-1}{p}\right) \\ &= \mathrm{e}^{(s-1)H + O(|s-1|^2 H'')} = \mathrm{e}^{(s-1)H} \Big(1 + O\big(|s-1|^2 H''(T)\big)\Big) \end{aligned} \tag{4.5}$$

If $Y = W_T$ then $H = H'(T)$ and uniformly for $|s| \leqslant 1.9$ we have

$$\begin{aligned} \mathbb{E}\,s^{W_T} &= \prod_{p \in T} \mathbb{E}\,s^{X_p} = \prod_{p \in T} \left(1 + \frac{s-1}{p-s}\right) = \prod_{p \in T} \left(1 + \frac{s-1}{p-1} + \frac{(s-1)^2}{(p-1)(p-s)}\right) \\ &= \mathrm{e}^{(s-1)H + O(|s-1|^2 H'')} = \mathrm{e}^{(s-1)H} \big(1 + O(|s-1|^2 H''(T))\big). \end{aligned} \tag{4.6}$$

Then, for any $0 < r \leqslant 1.9$, (4.4), (4.5) and (4.6) imply

$$\begin{aligned}\mathbb{P}(Y=k)-\mathbb{P}(Z=k) &= \frac{1}{2\pi i}\oint\limits_{|s|=r}\frac{\mathbb{E}\,s^Y-\mathbb{E}\,s^Z}{s^{k+1}}\,dz\\ &= \frac{1}{r^k}\int_0^1 \mathrm{e}^{-2\pi i k\theta}\Big[\mathbb{E}\,(r\mathrm{e}^{2\pi i\theta})^Y-\mathbb{E}\,(r\mathrm{e}^{2\pi i\theta})^Z\Big]\,d\theta\\ &\ll \frac{H''}{r^k}\int_0^{1/2}\big|r\mathrm{e}^{2\pi i\theta}-1\big|^2\mathrm{e}^{(r\cos(2\pi\theta)-1)H}\,d\theta.\end{aligned}$$

Now, for $0\leqslant\theta\leqslant\frac12$,

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

and

$$\big|r\mathrm{e}^{2\pi i\theta}-1\big|^2 = (r-1-2r\sin^2(\pi\theta))^2+\sin^2(2\pi\theta)\ll (r-1)^2+\theta^2,$$

so we obtain

$$\begin{aligned}\mathbb{P}(Y=k)-\mathbb{P}(Z=k) &\ll H''\frac{\mathrm{e}^{(r-1)H}}{r^k}\int_0^{1/2}(|r-1|^2+\theta^2)\mathrm{e}^{-8r\theta^2H}\,d\theta\\ &\ll H''\frac{\mathrm{e}^{(r-1)H}}{r^k}\bigg(\frac{|r-1|^2}{\sqrt{1+rH}}+\frac{1}{(1+rH)^{3/2}}\bigg).\end{aligned}\tag{4.7}$$

When $1\leqslant k\leqslant 1.9H$, we take $r=k/H$ in (4.7) and obtain, using Stirling's formula,

$$\begin{aligned}\mathbb{P}(Y=k)-\mathbb{P}(Z=k) &\ll H''\frac{H^k\mathrm{e}^{k-H}}{k^k}\left(\frac{|k/H-1|^2}{k^{1/2}}+\frac{1}{k^{3/2}}\right)\\ &\ll H''\frac{\mathrm{e}^{-H}H^k}{k!}\left(\left|\frac{k-H}{H}\right|^2+\frac1k\right).\end{aligned}$$

This completes the proof when $k\leqslant 1.9H$.

When $k>1.9H$ we take $r=1.9$ and the result follows in this case as well from (4.7). □

Theorem 4.7. *Let T be a finite subset of the primes. Then*

$$d_{TV}\big(U_T,\mathrm{Pois}(H(T))\big)\ll\frac{H''(T)}{1+H(T)}$$

and

$$d_{TV}\big(W_T,\mathrm{Pois}(H'(T))\big)\ll\frac{H''(T)}{1+H(T)},$$

Proof. Let $Y\in\{U_T,W_T\}$. If $Y=U_T$, let $H=H(T)$ and if $Y=W_T$, let $H=H'(T)$. Let $Z\overset{d}{=}\mathrm{Pois}(H)$. Again, write $H''=H''(T)$. From (4.2),

$$d_{TV}(Y,Z)\leqslant\sum_{k=0}^{\infty}\big|\mathbb{P}(Z=k)-\mathbb{P}(Y=k)\big|.$$

Consider two cases. First, if $H\leqslant 2$, we have by Theorem 4.6,

$$d_{TV}(Y,Z)\ll H''+\sum_{k>1.9H}H''(1.9)^{-k}\ll H''.$$

If $H>2$, Theorem 4.6 likewise implies that

$$\sum_{k>1.9H}|\mathbb{P}(Y=k)-\mathbb{P}(Z=k)|\ll H''\sum_{k>1.9H}\frac{\mathrm{e}^{0.9H}}{(1.9)^k}\ll H''\mathrm{e}^{-0.3H}$$

and also

$$\begin{aligned}\sum_{k\leqslant 1.9H}|\mathbb{P}(Y=k)-\mathbb{P}(Z=k)| &\ll H''\mathrm{e}^{-H}\sum_{k=0}^{\infty}\frac{H^k}{k!}\left[\frac{1}{k+1}+\frac{k(k-1)+k-2kH+H^2}{H^2}\right]\\ &= H''\mathrm{e}^{-H}\Bigg[\sum_{k=0}^{\infty}\frac{H^k}{(k+1)!}+\sum_{k=2}^{\infty}\frac{H^{k-2}}{(k-2)!}+\frac{1}{H}\sum_{k=1}^{\infty}\frac{H^{k-1}}{(k-1)!}+\\ &\qquad -2\sum_{k=1}^{\infty}\frac{H^{k-1}}{(k-1)!}+\sum_{k=0}^{\infty}\frac{H^k}{k!}\Bigg]\\ &= H''\mathrm{e}^{-H}\left[\frac{\mathrm{e}^H-1}{H}+\mathrm{e}^H+\frac{\mathrm{e}^H}{H}-2\mathrm{e}^H+\mathrm{e}^H\right]\\ &\ll \frac{H''}{H}.\end{aligned}$$

This proves the bound when $H>2$, upon noting that $H'(T)\asymp H(T)$. □

We can use Theorem 4.6 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. Here $Z_{T_i}\stackrel{d}{=}\mathrm{Pois}(H(T_i))$, and $Z_{T_1},\dots,Z_{T_m}$ are independent.

Corollary 4.8. *Let $T_1,\dots,T_m$ be disjoint sets of primes. Then*

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

Combining this Corollary with the Kubilius model (Thm. 4.5), we conclude that the "intermediate" (not too small and not too large) prime factors of an integer are "Poisson distributed".

Theorem 4.9. *Let $2\leqslant y\leqslant x$, and let $T_1,\dots,T_m$ be disjoint sets of primes $\leqslant y$. Then*

$$d_{TV}\left((\omega(n;T_1),\dots,\omega(n;T_m)),(Z_{T_1},\dots,Z_{T_m})\right)\ll\sum_{j=1}^{m}\frac{H''(T_j)}{\max(1,H(T_j))}+O\left(e^{-\frac{\log x}{5\log y}}\right).$$

Proof. Let $\boldsymbol{\omega}=(\omega(n;T_1),\dots,\omega(n;T_m))$, $\mathbf{U}=(U_{T_1},\dots,U_{T_m})$ and $\mathbf{Z}=(Z_{T_1},\dots,Z_{T_m})$ By the triangle inequality for d_{TV}, which follows easily from the definition (4.1), we have

$$\begin{aligned}d_{TV}(\boldsymbol{\omega},\mathbf{Z}) &\leqslant d_{TV}(\boldsymbol{\omega},\mathbf{U})+d_{TV}(\mathbf{U},\mathbf{Z})\\ &\leqslant d_{TV}(\mathbf{V}_y,\mathbf{X}_y)+d_{TV}(\mathbf{U},\mathbf{Z}).\end{aligned}$$

The theorem now follows by combining Theorem 4.5 with Corollary 4.8. □

3. 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. For each $j \in \mathbb{N}$, let Z_j be Poisson with parameter $1/j$, and $Z_1, Z_2, \dots$ independent.
(a) Show that $\mathbb{P}(Z_j \leqslant 1 \, \forall j) = \mathrm{e}^{-\gamma}$.
(b) Let A_n be the probability that a random $\sigma \in \mathcal{S}_n$ has distinct cycle sizes. Prove that $\lim_{n\to\infty} A_n = \mathrm{e}^{-\gamma}$. (This is a result of Lehmer from 1972).

Exercise 4.3. Let $2 \leqslant y \leqslant x$, and let $T_1, \dots, T_m$ be disjoint sets of primes $\leqslant y$. Then

$$d_{TV}\left((\Omega(n;T_1), \dots, \Omega(n;T_m)), (Z_{T_1}, \dots, Z_{T_m})\right) \ll \sum_{j=1}^{m} \frac{H''(T_j)}{\max(1, H(T_j))} + O\left(e^{-\frac{\log x}{5\log y}}\right).$$

CHAPTER 5

Central Limit Theorems

1. Gaussian approximation of Poisson variables

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 5.1 (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

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

is the distribution function of the standard Gaussian distribution.

Proof. We may assume that λ is sufficiently large. Let $h^* = 3\sqrt{\lambda \log(1+\lambda)}$. First observe that by the Poisson Tails Proposition 0.3 and the crude bounds for $Q(x)$ (0.16), we have

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

Likewise,

$$\int\limits_{|t|>3\sqrt{\log(1+\lambda)}} \mathrm{e}^{-\frac{1}{2}t^2}\, dt \ll \frac{1}{(1+\lambda)^3}. \tag{5.1}$$

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

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

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

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

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

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

It follows that

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

where

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

and

$$E \ll \frac{1}{\sqrt{\lambda}} \sum_k \left(\frac{1+|k-\lambda|}{\lambda} + \frac{|k-\lambda|^3}{\lambda^2} \right) \mathrm{e}^{-\frac{|k-\lambda|^2}{2\lambda}}.$$

For some integer $a \geqslant 1$ we have $(a-1)\sqrt{\lambda} \leqslant |k-\lambda| \leqslant a\sqrt{\lambda}$. Summing over all a gives

$$E \ll \sum_{a=1}^{\infty} \left(\frac{a+a^3}{\sqrt{\lambda}} \right) \mathrm{e}^{-(a-1)^2/2} \ll \frac{1}{\sqrt{\lambda}}.$$

By Euler summation,

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

The integral involving $\{t\}$ is $O(1)$. The first equals, by (5.1),

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

and hence

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

The proof is complete. □

2. Central Limit Theorems for cycles

Combining Theorem 4.3 with the Central Limit Theorem for Poisson variables (Theorem 5.1 below) establishes a Central Limit Theorem for the count of cycles whose lengths lie in an arbitrary set $I \subset [n]$.

Theorem 5.2. *Let $I \subset [n]$. Uniformly for all I and any real w,*

$$\mathbb{P}_{\sigma \in \mathcal{S}_n} \left(C_I(\sigma) \leqslant H(I) + w\sqrt{H(I)} \right) = \Phi(w) + O\left(\frac{\log(2H(I))}{\sqrt{H(I)}} \right).$$

Proof. Let $H = H(I)$. We may assume that $H \geqslant 100$, otherwise the claim is trivial. If $|w| \geqslant \sqrt{3\log H}$ then the result follows from Corollary 1.12, since the left side is thus $O(1/H) = \Phi(w) + O(1/H)$ if $w \leqslant -\sqrt{3\log H}$ and is $1 - O(1/H) = \Phi(w) + O(1/H)$ if $w \geqslant \sqrt{3\log H}$. Suppose now that $|w| < \sqrt{3\log H}$, let

$$A = H + w\sqrt{H}, \qquad m = \left\lceil \frac{n}{5\log H} \right\rceil, \qquad J = I \cap [m].$$

Because

$$H(I \setminus J) = \sum_{\substack{m < k \leqslant n \\ k \in I}} \frac{1}{k} \leqslant H((m,n] \cap \mathbb{N}) \leqslant \log\log H + O(1)$$

we have $H(J) = H + O(\log\log H)$. Thus,

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

Let Y be a Poisson random variable with parameter $H(J)$. Thus, by Theorem 4.3 and Proposition 5.1,

$$\begin{aligned}\mathbb{P}_\sigma(C_I(\sigma) \leqslant A) &\leqslant \mathbb{P}_\sigma(C_J(\sigma) \leqslant A)\\ &= \mathbb{P}(Y \leqslant A) + O(\mathrm{e}^{-n/5m})\\ &= \Phi(w') + O\left(H(J)^{-1/2} + \mathrm{e}^{-n/5m}\right)\\ &= \Phi(w') + O\left(\frac{1}{\sqrt{H}}\right)\\ &= \Phi(w) + O\left(\frac{\log\log H}{\sqrt{H}}\right).\end{aligned}$$

We also have

$$A - 5\log H = H(J) + w''\sqrt{H(J)}, \quad w'' = w + O\left(\frac{\log H}{\sqrt{H}}\right)$$

and it follows that

$$\begin{aligned}\mathbb{P}_\sigma(C_I(\sigma) \leqslant A) &\geqslant \mathbb{P}_\sigma\left(C_J(\sigma) \leqslant A - 5\log H \text{ and } C_{I\setminus J}(\sigma) \leqslant 5\log H\right)\\ &= \mathbb{P}_\sigma\left(C_J(\sigma) \leqslant A - 5\log H\right),\end{aligned}$$

since $\min(I \setminus J) \geqslant m \geqslant n/(5\log H)$ implies that $C_{I\setminus J}(\sigma) \leqslant 5\log H$ always. Hence, by Theorem 4.3 and Lemma 5.1,

$$\begin{aligned}\mathbb{P}_\sigma(C_I(\sigma) \leqslant A) &\geqslant \Phi(w'') + O(1/\sqrt{H})\\ &= \Phi(w) + O\left(\frac{\log H}{\sqrt{H}}\right).\end{aligned}$$

The theorem follows by combining the upper and lower bounds for $\mathbb{P}(C_I(\sigma) \leqslant A)$. □

The special case $I = [n]$ was established by Goncharov [**39**], without a specific rate of convergence. Goncharov analyzed carefully the asymptotics of the Stirling number of the first kind, $s(n,m)$, the absolute value of which counts the number of permutations $\sigma \in \mathcal{S}_n$ with $C(\sigma) = m$. Since $H_n = \log n + O(1)$ and Φ has bounded derivative, we quickly arrive at the following.

Theorem 5.3. *Let $n \geqslant 100$ and w be real. Then*

$$\mathbb{P}_{\sigma\in\mathcal{S}_n}\left(C(\sigma) \leqslant \log n + w\sqrt{\log n}\right) = \Phi(w) + O\left(\frac{\log_2 n}{\sqrt{\log n}}\right).$$

Proof. Letting $\log n + w\sqrt{\log n} = H_n + w'\sqrt{H_n}$, we have

$$w - w' \ll \frac{1}{\sqrt{\log n}}.$$

Hence,

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

The big-O term in Theorem 5.2 cannot be made smaller than $1/\sqrt{H(I)}$ since $C_I(\sigma)$ is integer valued, and thus the left side is constant in intervals of w of length $1/\sqrt{H(I)}$, while $\Phi'(w) \gg 1$ if w is bounded. We remark that when $H(I)$ is bounded, $C_I(\sigma)$ is expected to have Poisson distribution with small parameter, and this cannot be approximated by a Gaussian.

We also derive that the j-th smallest cycle of σ, denoted $D_j(\sigma)$ (with ties allowed), also obeys the Gaussian law, refining Theorem 1.22.

Theorem 5.4. *Uniformly for j in the range*

$$1 \leqslant j \leqslant \log n - \sqrt{(\log n)\log\log n}$$

and for any real w,

$$\mathbb{P}_{\sigma\in\mathcal{S}_n}\Big(\log D_j(\sigma) \leqslant j + w\sqrt{j}\Big) = \Phi(w) + O\left(\frac{\log(2j)}{\sqrt{j}}\right).$$

Proof. We may assume that $j \geqslant 10$ and that n is sufficiently large, the statement being trivial otherwise. We may also assume that $|w| \leqslant \sqrt{\log j}$, since the statement for w outside this range follows from the monotonicity of $\mathbb{P}(\log D_j(\sigma) \leqslant j + w\sqrt{j})$, as a function of w, the statement for the two points $w = \pm\sqrt{\log j}$ and the fact that $\Phi(-\sqrt{\log j}) \ll 1/j^{1/2}$ and $\Phi(\sqrt{\log j}) = 1 - O(1/j^{1/2})$.

Let $k = \left\lfloor \mathrm{e}^{j+w\sqrt{j}} \right\rfloor$, so by hypothesis,

$$\log k \leqslant j + \sqrt{j\log j} \leqslant j + \sqrt{(\log n)\log\log n} \leqslant \log n.$$

Then $D_j(\sigma) \leqslant k$ is equivalent to $C_{[k]}(\sigma) \geqslant j$. As $H_k = \log k + O(1)$ and $\sqrt{H_k} = \sqrt{j} + O(|w| + 1)$, we have

$$j - 1 = H_k - u\sqrt{H_k}, \quad \text{where} \quad u = w + O\left(\frac{w^2+1}{\sqrt{j}}\right).$$

By Theorem 5.2,

$$\begin{aligned}\mathbb{P}_\sigma(D_j(\sigma) \leqslant k) &= \mathbb{P}_\sigma(C_{[k]}(\sigma) \geqslant j)\\ &= 1 - \mathbb{P}_\sigma(C_{[k]}(\sigma) \leqslant j-1)\\ &= 1 - \Phi(-u) + O\left(\frac{\log H_k}{\sqrt{H_k}}\right)\\ &= \Phi(u) + O\left(\frac{\log(2j)}{\sqrt{j}}\right).\end{aligned}$$

Also,

$$\Phi(u) = \Phi(w) + O\left(\frac{w^2+1}{\sqrt{j}}\right) = \Phi(w) + O\left(\frac{\log(2j)}{\sqrt{j}}\right)$$

and the proof is complete. □

3. Central Limit theorems for prime factors

Theorem 5.5 (Prime factors CLT). *Suppose that T is a subset of the primes in $[2, x]$. For any real w,*

$$\mathbb{P}_x\Big(\omega(n;T) \leqslant H(T) + w\sqrt{H(T)}\Big) = \Phi(w) + O\left(\frac{\log(2H(T))}{\sqrt{H(T)}}\right).$$

Proof. Let $H = H(T)$. Assume $H \geqslant 100$, else the conclusion is trivial. As in the proof of Theorem 5.2, the conclusion in the case $|w| \geqslant \sqrt{3\log H}$ follows from Theorem 1.13 and Proposition 0.3.

Suppose now that $|w| < \sqrt{3\log H}$, let

$$A = H + w\sqrt{H}, \qquad y = x^{1/(5\log H)}, \qquad J = T \cap [2, y].$$

Because

$$H(T \setminus J) \leqslant \sum_{y<p\leqslant x}\frac{1}{p} \leqslant \log\log H + O(1)$$

we have $H(J) = H + O(\log\log H)$. Thus,

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

Let Y be a Poisson random variable with parameter $H(J)$. Thus, by Theorem 4.9 and Proposition 5.1,

$$\begin{aligned}\mathbb{P}_x(\omega(n;T)\leqslant A) &\leqslant \mathbb{P}_x(\omega(n;J)\leqslant A)\\ &= \mathbb{P}(Y\leqslant A)+O(1/H)\\ &= \Phi(w')+O\left(\frac{1}{\sqrt{H}}\right)\\ &= \Phi(w)+O\left(\frac{\log\log H}{\sqrt{H}}\right).\end{aligned}$$

We also have

$$A-5\log H = H(J)+w''\sqrt{H(J)},\quad w''=w+O\left(\frac{\log H}{\sqrt{H}}\right)$$

and it follows that

$$\begin{aligned}\mathbb{P}_x(\omega(n;T)\leqslant A) &\geqslant \mathbb{P}_x\big(\omega(n;J)\leqslant A-5\log H \text{ and } \omega(n;T\setminus J)\leqslant 5\log H\big)\\ &= \mathbb{P}_x\left(\omega(n;J)\leqslant A-5\log H\right),\end{aligned}$$

since $\min(T\setminus J)\geqslant y$ implies that $\omega(n;T\setminus J)\leqslant 5\log H$ always. Hence, by Theorem 4.9 and Lemma 5.1,

$$\begin{aligned}\mathbb{P}_x(\omega(n;T)\leqslant A) &\geqslant \Phi(w'')+O(1/\sqrt{H})\\ &= \Phi(w)+O\left(\frac{\log H}{\sqrt{H}}\right).\end{aligned}$$

The theorem follows by combining the upper and lower bounds for $\mathbb{P}(\omega(n;T)\leqslant A)$.

□

We remark that an error term $H(T)^{-1/2}$ is best possible; in fact, the erro term 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 **[38]**.

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 **[28]**.

Theorem 5.6 (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 P be the set of all primes $\leqslant x$, $H=H(P)$, and

$$\log_2 x+w\sqrt{\log_2 x}=H+w'\sqrt{H}.$$

Since $H=\log_2 x+O(1)$, we have $w-w'\ll(\log_2 x)^{-1/2}$. Thus, by Theorem 5.5,

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

An error term of $O((\log_2 x)^{-1/2})$ in Theorem 5.6 is best possible (cf. work of Rényi-Turán, Delange and Kubilius in the late 1950s/early 1960s).

We also derive that the j-th smallest *distinct* prime factor of n, denoted $p_j(n)$, also obeys the Gaussian law, refining Theorem 1.21.

Theorem 5.7. *Uniformly for j in the range*

$$1\leqslant j\leqslant \log_2 x-\sqrt{(\log_2 x)\log_3 x}$$

and for any real w, we have

$$\mathbb{P}_x\Big(\log_2 p_j(n)\leqslant j+w\sqrt{j}\Big)=\Phi(w)+O\left(\frac{\log(2j)}{\sqrt{j}}\right).$$

A version of this, without a rate of convergence, was proved by Galambos [**37**].

4. Exercises

Exercise 5.1. Prove the following variant of Theorem 5.5: Suppose that T is a subset of the primes in $[2,x]$. For any real w,

$$\mathbb{P}_x\left(\Omega(n;T)\leqslant H(T)+w\sqrt{H(T)}\right)=\Phi(w)+O\left(\frac{\log(2H(T))}{\sqrt{H(T)}}\right).$$

Exercise 5.2. Prove Theorem 5.7.

Exercise 5.3. (a) Let T_1,T_2 be disjoint sets of primes $\leqslant x$. Show that, uniformly for all real w_1,w_2,

$$\mathbb{P}_x\left(\omega(n;T_1)\leqslant H(T_1)+w_1\sqrt{H(T_1)},\omega(n;T_1)\leqslant H(T_1)+w_2\sqrt{H(T_1)}\right)=\Phi(w_1)\Phi(w_2)+O\left(\frac{\log(2H(T_1))}{\sqrt{H(T_1)}}+\frac{\log(2H(T_2))}{\sqrt{H(T_2)}}\right).$$

(b) Let T_1 denote the set of primes $\leqslant x$ that are $1 \mod 4$, and let T_2 denote the set of primes $\leqslant x$ that are $3 \mod 4$. Show that

$$\mathbb{P}_x\left(\omega(n;T_1)\leqslant \tfrac12\log_2 x+w_1\sqrt{\tfrac12\log_2 x},\omega(n;T_2)\leqslant \tfrac12\log_2 x+w_2\sqrt{\tfrac12\log_2 x}\right)=\Phi(w_1)\Phi(w_2)+O\left(\frac{\log_3 x}{\sqrt{\log_2 x}}\right).$$

Exercise 5.4. (Galambos, 1976 [**37**]). Fix $\varepsilon>0$ and $z\in\mathbb{R}$. Show that if $j=j(x)\to\infty$ as $x\to\infty$ and $j(x)\leqslant(1-\varepsilon)\log_2 x$, then

$$\mathbb{P}_x\big(\log_2 p_{j+1}(n)-\log_2 p_j(n)\leqslant z\big)\to 1-\mathrm{e}^{-z}\qquad(x\to\infty).$$

Exercise 5.5. Fix $\varepsilon>0$ and $z\in\mathbb{R}$. Show that if $j=j(n)\to\infty$ as $n\to\infty$ and $j(n)\leqslant(1-\varepsilon)\log n$, then

$$\mathbb{P}_{\sigma\in\mathcal{S}_n}\big(\log D_{j+1}(\sigma)-\log D_j(\sigma)\leqslant z\big)\to 1-\mathrm{e}^{-z}\qquad(n\to\infty).$$

This matches the spacing distribution of points in a Poisson process.

CHAPTER 6

The concentration of divisors of integers and permutations

1. Concentration of divisors

Erdős conjectured [**24**] in 1948 that almost all integers have two divisors d and d' with $d < d' < 2d$. This may seem counterintuitive, given that we have already shown (cf. Theorem 1.21) that a typical integer has about 2^j divisors less than e^{e^j}, and hence the k-th smallest divisor of a typical integer, for k large, is about $\exp\{k^{1/\log 2}\}$. Hence, one may be led to believe that $d_{k+1}/d_k \to \infty$ for a typical n, as long as $k \to \infty$ (and $\tau(n) - k \to \infty$ by symmetry). This, however, is faulty reasoning, as (i) as we see in Theorem 5.7, there is a very large "normal" range of deviation for each prime $p_j(n)$, on a log log-scale; however having two close *prime* factors is genuinely rare (see Exercise 1.5). Also, (ii) divisors form from combinations of prime factors in complicated ways, which lack the "independence" of prime divisors. Erdős proved [**24**] that the set $\{n \in \mathbb{N} : \exists d, d' | n \text{ with } d < d' < 2d\}$ has asymptotic density, say δ. Note that $\delta \geqslant 1/6$ because $2 < 3 < 2 \cdot 2$. The question whether $\delta = 1$ would remain open for another 36 years.

Working heuristic: Assume that the set $\{\log(d'/d) : dd' | n, (d, d') = 1\} \subset [-\log n, \log n]$ is well-distributed for a typical integer n. Since $\#\{(d, d') : dd' | n, (d, d') = 1\} \geqslant 3^{\omega(n)}$, we expect that

$$|\{dd' | n : (d, d') = 1, |\log(d'/d)| \leqslant \sigma\}| \approx 3^{\omega(n)} \frac{\sigma}{\log n}.$$

The right hand side above is at least 1 for $\sigma \gtrsim (\log n) 3^{-\omega(n)} \approx (\log n)^{1-\log 3} = o(1)$.

Maier and Tenenbaum proved that this heuristic is in fact close to the truth.

Theorem 6.1 (Maier, Tenenbaum, 1984 [52]). *Fix $\varepsilon > 0$. Then almost all integers n have two divisors d and d' such that*

$$d < d' < d\big(1 + (\log n)^{1-\log 3+\varepsilon}\big).$$

It is possible to show more, that for almost all n there are intervals $(y, ey]$ containing many divisors of n. We define the Erdős-Hooley Δ-function

$$\Delta(n) := \max_t \#\{d | n, \log d \in (t, t+1]\},$$

that is to say the maximum number of divisors n has in any interval of logarithmic length 1. Its normal order (almost sure behavior) has proven quite mysterious. Work on the distibution of $\Delta(n)$ began with Erdős [**18**], Erdős and Nicolas [**20, 21**] and Hooley [**48**] in the 1970s. Further work on the normal and average behavior of $\Delta(n)$ can be found in works of Tenenbaum [**62, 63**], Hall and Tenenbaum [**42, 43, 44**], Maier and Tenenbaum [**52, 53, 54**], and most recently Ford, Green and Koukoulopoulos [**36**]. See also [**45**, Ch. 5,6,7]. Tenenbaum's survey paper [**65**, p. 652–658] includes a history of the function $\Delta(n)$ and description of many applications in number theory.

The best bounds for $\Delta(n)$ for "normal" n currently known were obtained in papers of Maier and Tenenbaum [**54**] (upper bound) and Ford, Green and Koukoulopoulos [**36**] (lower bound). For almost all n we have

$$(\log_2 n)^{\eta - o(1)} \leqslant \Delta(n) \leqslant (\log_2 n)^{\log 2 + o(1)}, \tag{6.1}$$

where $\eta = 0.35332772701323467 11\ldots$ is a specific constant.

In this section, we prove a weaker lower bound, recovering the bound proved by Maier and Tenenbaum [**52**].

Theorem 6.2. *Fix $\varepsilon > 0$. For almost all n we have $\Delta(n) \geqslant (\log\log n)^{\eta_1 - \varepsilon}$, where*

$$\eta_1 = \frac{\log 2}{\log\left(\frac{\log 3}{\log 3 - 1}\right)} = 0.2875404895\ldots$$

The same argument will provide a measure of the concentration of divisors of random permutations.

Theorem 6.3. *For a permutation σ on S_n, denote by*

$$\Delta(\sigma) := \max_r \#\{\tau | \sigma : |\tau| = r\}.$$

Then, for all but $o(n!)$ of the permutations $\sigma \in S_n$, we have

$$\Delta(\sigma) \geqslant (\log n)^{\eta_1 - o(1)}.$$

Here the terms $o(1)$ refer to functions that $\to 0$ as $n \to \infty$.

2. A random model of prime factors and cycle lengths

As we have seen by Theorem 4.2, the number of cycles of size i in a random permutation is well-approximated by a Pois$(1/i)$ variable. Also, by Theorem 4.9, $\omega(n; T)$ is well approximated by Pois$(H(T))$ for a set T of primes which are $\leqslant x^{o(1)}$ and not "too thin". In particular, if i is much larger than K and T is the set of primes in $(e^{i/K}, e^{(i+1)/K}]$ then by Mertens' Theorem (0.5), $H(T) \approx 1/i$ and hence $\omega(n; T)$ is well-approximate by Pois$(1/i)$. In turn, when i is large, by Exercise 4.1 (b), Pois$(1/i)$ is well-approximated by a Bernouilli random variable Y with $\mathbb{P}(Y = 1) = 1/i$. This motivates the following random model.

Definition 6.4. We define $\mathbf{A}$ to be the random set of positive integers such that $\mathbb{P}(i \in \mathbf{A}) = 1/i$ for each i, and the events $i \in \mathbf{A}$ are independent for different values of i. That is, if $Y_1, Y_2, \ldots$ are independent Bernouilli random variables with $P(Y_i = 1) = 1/i$ for each i, then $\mathbf{A} = \{i : Y_i = 1\}$.

The property that an integer has k close divisors can be modeled by the event that $\mathbf{A}$ has k equal subset sums.

Definition 6.5. Let $k \geqslant 2$ be an integer. Let β_k be the supremum of all exponents $c < 1$ for which the following is true with probability $\to 1$ as $D \to \infty$: there are distinct sets $A_1, \cdots, A_k \subset \mathbf{A} \cap [D^c, D]$ with

$$\sum_{a \in A_1} a = \cdots = \sum_{a \in A_k} a.$$

It is not a priori obvious that β_k exists. We will establish this later in Theorem 6.9. In particular, we have $0 < \beta_k < 1/10$ for all k.

Define

$$\zeta_k = \frac{\log k}{\log(1/\beta_k)}. \tag{6.2}$$

Theorem 6.6 ([36]). *Fix $k \geqslant 2$ and $\varepsilon > 0$. For almost every positive integer n, we have*

$$\Delta(n) \gg (\log\log n)^{\zeta_k - \varepsilon}.$$

Theorem 6.7 ([36]). *Fix $k \geqslant 2$ and $\varepsilon > 0$. Then, for all but $o_{n\to\infty}(n!)$ of the permutations $\sigma \in S_n$, we have*

$$\Delta(\sigma) \geqslant (\log n)^{\zeta_k - \varepsilon}.$$

We also prove a more general version of Theorem 6.1. Define α_k be the supremum of all real numbers α such that for almost every $n \in \mathbb{N}$, n has k divisors $d_1 < \cdots < d_k$ with $d_k \leqslant d_1(1 + (\log n)^{-\alpha})$. In 1964, Erdős [**17**] conjectured that $\alpha_2 = \log 3 - 1$, and this was confirmed by Erdős and Hall [**19**] (upper bound) and Maier and Tenenbaum [**52**] (lower bound). Maier and Tenenbaum [**54**] showed that

$$\alpha_k \leqslant \frac{\log 2}{k+1} \qquad (k \geqslant 3)$$

and (this is not stated explicitly in **[54]**)

$$\alpha_k \geqslant \frac{(\log 3-1)^m 3^{m-1}}{(3\log 3-1)^{m-1}} \qquad (2^{m-1}<k\leqslant 2^m, m\in\mathbb{N}). \tag{6.3}$$

See also **[65]**, p. 655–656]. In particular, it is not known if $\alpha_3 > \alpha_4$, although Tenenbaum **[65]** conjectures that the sequence $(\alpha_k)_{k\geqslant 2}$ is strictly decreasing. Ford, Green and Koukoulopoulos connected α_k to the constant β_k from the random model.

It is easy to see that for any $k \geqslant 2$, $\alpha_k \leqslant \alpha_2 \leqslant 1$. Indeed, $\alpha_k \leqslant \alpha_2$ is obvious. Let $\delta = (\log x)^{-1-\varepsilon}$ for arbitrary fixed $\varepsilon > 0$. If n has two divisors d, d' with $d < d' \leqslant d(1+\delta)$, then WLOG there exist two such divisors with $(d, d') = 1$, hence $dd'|n$. Thus, the number of $n \leqslant x$ divisible by two such divisors is at most

$$\sum_{1/\delta\leqslant d\leqslant\sqrt{x}}\ \sum_{d<d'\leqslant d(1+\delta)} \frac{x}{dd'} \leqslant x \sum_{1/\delta<d\leqslant\sqrt{x}} \frac{d\delta}{d^2} \ll \delta x\log x = o(x)$$

as $x\to\infty$. This proves $\alpha_2 \leqslant 1$.

Theorem 6.8 ([36]). *For all $k \geqslant 2$, $\alpha_k \geqslant \beta_k/(1-\beta_k)$.*

The authors in **[36]** conjecture the corresponding upper bound $\alpha_k \leqslant \beta_k/(1-\beta_k)$. The methods of **[36]** allow one to compute β_k for any k using a finite procedure. In particular, we have

$$\beta_3 = \frac{\log 3-1}{\log 3+\frac{1}{\xi}} = 0.02616218797316965133\ldots$$

and

$$\beta_4 = \frac{\log 3-1}{\log 3+\frac{1}{\xi}+\frac{1}{\xi\lambda}} = 0.01295186091360511918\ldots$$

where

$$\xi = \frac{\log 2-\log(e-1)}{\log(3/2)}, \quad \lambda = \frac{\log 2-\log(e-1)}{1+\log 2-\log(e-1)-\log(1+2^{1-\xi})}.$$

In **[36]** it is also proved that

$$\sup_{k\geqslant 2}\zeta_k \geqslant \eta = 0.3533227727\ldots$$

which, combined with Theorem 6.6, gives the lower bound in (6.1). The authors of **[36]** conjecture that $\limsup_{k\to\infty}\zeta_k = \eta$. Most of the paper **[36]** is devoted to relating β_k to a certain combinatorial optimization problem, which grows very complex as k increases.

In these notes we will concentrate on the easiest case $k = 2$ and prove

Theorem 6.9. *We have $\beta_2 = 1-\frac{1}{\log 3} = 0.0897607\ldots$ and, for any $k \geqslant 2$,*

$$\beta_k \geqslant \beta_2^{\left\lceil\frac{\log k}{\log 2}\right\rceil}.$$

Trivially, $\beta_k \leqslant \beta_2$ for all k. Thus, we see that β_k exists for all $k \geqslant 2$ and $0 < \beta_k \leqslant \beta_2 < 1/11$ for all k.

Combining Theorem 6.9 with Theorems 6.6 and 6.7 gives Theorems 6.2 and 6.3. Also, combining Theorems 6.8 and 6.9 gives Theorem 6.1.

It remains to prove Theorems 6.6, 6.7, 6.8, and 6.9.

Further Remarks. The average order of $\Delta(n)$ is also rather mysterious, the best known bounds being

$$\log\log x \leqslant \frac{1}{x}\sum_{n\leqslant x}\Delta(n) \leqslant \mathrm{e}^{c\sqrt{\log\log x}},$$

for some $c > 0$. The lower bound is due to Hall and Tenenbaum (see **[45]**, Theorem 60]) and the upper bound is from an unpublished manuscript of Koukoulopoulos which slightly refines a bound of Tenenbaum **[62]** (see also **[45]**, Theorem 70]).

[1]The factor 3^{m-1} is missing in the stated lower bounds for α_k in **[65]**.

3. Proof of Theorems 6.6, 6.7, and 6.8

In this section we assume Theorem 6.9 and deduce Theorems 6.6, 6.7, and 6.8. In particular, $0 < \beta_k < 1/10$ for all k.

We begin with a simple combinatorial argument, first used in a related context in the work of Maier-Tenenbaum **[52]**, which shows how to use equal subsums in multiple intervals $(u^c, u]$ to create many more common subsums in $\mathcal{A}$. For any finite subset S of positive integers, denote by ΣS the sum of the elements of S.

Lemma 6.10. *Let $k \geqslant 1$ be an integer and fix $\varepsilon > 0$. Let C, D be parameters with $\log u \leqslant (\log v)^{o(1)}$ and $u \to \infty$ as $v \to \infty$. Then, with probability $\to 1$ as $v \to \infty$, there are distinct $A_1, \dots, A_M \subset \mathbf{A} \cap (u, v]$ with $\Sigma A_1 = \dots = \Sigma A_M$ and $M \geqslant (\log v)^{\zeta_k - \varepsilon}$.*

Proof. Fix $\delta \in (0, \beta_k)$, depending on ε, set $\alpha := \beta_k - \delta$ and assume that v is sufficiently large in terms of ε, δ. Set

$$m := \Big\lfloor \frac{\log\log v - \log\log u}{-\log \alpha} \Big\rfloor$$

and consider the intervals $J_i := (v^{\alpha^{i+1}}, v^{\alpha^i}]$, $i = 0, 1, \dots, m-1$. Due to the choice of m, these all lie in $(u, v]$. For each $i \in \{0, 1, \dots, m-1\}$, let E_i be the event that there are distinct $A_{i,1}, \dots, A_{i,k} \subset J_i$ with equal sums. Then, by the definition of β_k, if v is large enough then $\mathbb{P}(E_i) \geqslant 1 - \delta$, uniformly in i. These events E_i are all independent. The Law of Large Numbers then implies that, with probability at least $1-\delta$, at least $(1-2\delta)m$ of them occur. Suppose we are in this event, suppose that E_i occurs for $i \in I$, where $|I| \geqslant (1-2\delta)m$. Then there are numbers s_i, $i \in I$, and sets $A_{i,1}, \dots, A_{i,k} \subset J_i$ all with sum s_i.

It is now clear that for each $\mathbf{j} = \{j_i : i \in I\} \in [k]^I$, the set

$$B_{\mathbf{j}} = \bigcup_{i \in I} A_{i,j_i}$$

lies in $(u, v]$ and has sum $\sum_{i \in I} s_i$. Moreover, these sets are distinct. Let $M = k^{|I|}$, then

$$M \geqslant k^{(1-2\delta)m} \geqslant k^{-1} \left(\frac{\log v}{\log u} \right)^{(1-2\delta)(\log k)/(-\log \alpha)}.$$

Recall the definition (6.2) of ζ_k. By our assumption on u, and if δ is small enough, the right side is $\geqslant (\log v)^{\zeta_k - \varepsilon}$, as required. □

Lemma 6.11. *Let x be a large parameter, suppose that*

$$1 \leqslant K \leqslant (\log x)^{1/2}, \tag{6.4}$$

and let $I = (u, v] \cap \mathbb{N}$, where

$$u = \big\lfloor 100K(\log_2 x)^2 \big\rfloor, \quad v = \left\lfloor \frac{K \log x}{5 \log_3 x} \right\rfloor - 1. \tag{6.5}$$

For $i \in I$, let T_i be the set of primes in $(e^{i/K}, e^{(i+1)/K}]$, and define the random set

$$\mathbf{B} = \{i \in (u, v] : \omega(n; T_i) \geqslant 1\}.$$

Uniformly for any collection $\mathscr{I}$ of subsets of I, we have

$$\mathbb{P}(\mathbf{A} \cap I \in \mathscr{I}) = \mathbb{P}_x(\mathbf{B} \in \mathscr{I}) + O(1/\log_2 x).$$

Proof. For $u < i \leqslant v$, let $\omega_i = \mathbb{1}(\omega(n; T_i) \geqslant 1)$, $P_i \overset{d}{=} \mathrm{Pois}(H(T_i))$ (these being independent for different i) and let $Z_i = \mathbb{1}(P_i \geqslant 1)$. Each T_i is contained in $[\log x, y]$, where $y = x^{1/5 \log_3 x}$. Hence, by Theorem 4.9 and (6.5),

$$d_{TV}(\boldsymbol{\omega}, \mathbf{Z}) \ll \frac{1}{\log_2 x} + \sum_{i \in I} H''(T_i) \ll \frac{1}{\log_2 x}.$$

By the strong form of Mertens' estimate (0.5),

$$H(T_i) = \log\Big(\frac{i+1}{K}\Big) - \log\Big(\frac{i}{K}\Big) + O(e^{-(i/K)^{1/2}}) = \frac{1}{i} + O\Big(\frac{1}{i^2}\Big).$$

Hence, if Y_i is a Bernouilli variable with $\mathbb{P}(Y_i = 1) = 1/i$, then by Exercise 4.1 (b),

$$d_{TV}(\mathbf{Z}, \mathbf{Y}) \leqslant \sum_{i\in I} d_{TV}(Z_i, Y_i) \ll \sum_{i\in I} \frac{1}{i^2} \ll \frac{1}{\log_2 x}.$$

By the triangle inequality,

$$d_{TV}(\boldsymbol{\omega}, \mathbf{Y}) \leqslant d_{TV}(\boldsymbol{\omega}, \mathbf{Z}) + d_{TV}(\mathbf{Z}, \mathbf{Y}) \ll \frac{1}{\log_2 x}$$

and the claim follows. □

Proof of Theorem 6.6. Fix $\varepsilon > 0$, let x be large, let $K = (\log_2 x)^2$ and define u, v by (6.5). Define $\mathbf{B}$ and sets T_i as in Lemma 6.11. Throughout the proof, $o(1)$ means a function $\to 0$ as $x \to \infty$. By Lemma 6.10, with probability $1 - o(1)$, there are distinct sets $A_1, \dots, A_M$ of $\mathbf{A} \cap (u, v]$ with equal sums and $M \geqslant (\log_2 x)^{\zeta_k - \varepsilon}$. We also have that with probability $1 - o(1)$, $|\mathbf{A} \cap (u, v]| \leqslant 2 \log v$. Indeed, by Markov's inequality,

$$\begin{aligned}
\mathbb{P}(|\mathbf{A} \cap (u, v]| > 2\log v) &= \mathbb{P}(2^{|\mathbf{A}\cap(u,v]|} > 2^{2\log v}) \\
&\leqslant v^{-\log 4} \mathbb{E}\, 2^{|\mathbf{A}\cap(u,v]|} \\
&= v^{-\log 4} \prod_{j=u+1}^{D} \Big(1 - \frac{1}{i} + \frac{2}{i}\Big) \\
&= (v/u) v^{-\log 4} = o(1) \quad (v \to \infty).
\end{aligned}$$

Let F be the event that $\mathbf{A} \cap (u, v]$ has at most $2 \log v$ elements and has M distinct subsets with equal sums. By the above discussion, $\mathbb{P}(F) = 1 + o(1)$. By Lemma 6.11, the corresponding event F' for the random set $\mathbf{B}$ also holds with probability $1 - o(1)$; that is, F' is the event that $|\mathbf{B} \cap (u, v]| \leqslant 2 \log v$ and that there are distinct subsets $B_1, \dots, B_M$ of $\mathbf{B}$ with equal sums. If we are in the event F' and n is divisible by $\prod_{b\in\mathbf{B}} p_b$, where $p_b \in T_b$ for each $b \in \mathbf{B}$, then let $d_i = \prod_{b\in B_i} p_b$ for each $i \leqslant M$. For $1 \leqslant i < j \leqslant M$ we have

$$\begin{aligned}
|\log d_i - \log d_j| = \Big|\sum_{b\in B_i} \log p_b - \sum_{b\in B_j} \log p_b\Big| &\leqslant \frac{|B_i| + |B_j|}{K} + \frac{1}{K}\Big|\sum_{b\in B_i} b - \sum_{b\in B_j} b\Big| \\
&= \frac{|B_i| + |B_j|}{K} \leqslant \frac{4\log v}{K} \ll \frac{1}{\log_2 x}.
\end{aligned}$$

Thus, there are M divisors d_i of n whose logarithms all lie in a single interval of length $O(1/\log_2 x) < 1$. It follows that $\mathbb{P}_x(\Delta(n) \geqslant M) = 1 - o(1)$, as required for Theorem 6.6. □

Proof of Theorem 6.7. Fix $\varepsilon > 0$. Let $u = \log n$ and $v = n/\log n$. For each j, let $Z_j \overset{d}{=} \mathrm{Pois}(1/j)$, with $Z_1, Z_2, \dots$ independent. For a random permutation $\sigma \in S_n$, let $\mathbf{C} = \{j : C_j(\sigma) \geqslant 1\}$, and define the random set $\widetilde{\mathbf{A}} = \{j : Z_j \geqslant 1\}$. By Theorem 4.2, Exercise 4.1 (b), and the triangle inequality, we have

$$\begin{aligned}
d_{TV}(\mathbf{A} \cap (u, v], \mathbf{C} \cap (u, v]) &\leqslant d_{TV}(\mathbf{A} \cap (u, v], \widetilde{\mathbf{A}} \cap (u, v]) + d_{TV}(\widetilde{\mathbf{A}} \cap (u, v], \mathbf{C} \cap (u, v]) \\
&= o(1)
\end{aligned}$$

as $n \to \infty$. By Lemma 6.10, with probability $\to 1$ as $n \to \infty$, $\mathbf{A} \cap (u, v]$ has M distinct subsets $A_1, \dots, A_M$ with equal sums, where $M \geqslant (\log v)^{\zeta_k - \varepsilon}$. Hence, $\mathbf{C}$ has distinct subsets $S_1, \dots, S_M$ with equal sums with probability $\to 1$ as $n \to \infty$. Each subset S_j corresponds to a distinct divisor of σ, the size of the divisor being the sum of elements of S_j. As $\varepsilon > 0$ is arbitrary, the result follows. □

PROOF OF THEOREM 6.8. Fix $0 < c < \frac{\beta_k}{1-\beta_k}$, so that $c < 1/10$. Let x be large and set $K = (\log x)^c$. Define u, v by (6.5), let $D = v$ and define c' by $D^{c'} = u$. By assumption,

$$c' \sim \frac{c}{c+1} \qquad (x \to \infty)$$

and therefore there is a $\delta > 0$ so that $c' \leqslant \beta_k - \delta$ for sufficiently large x. Let n be a random integer chosen uniformly in $[1, x]$. With probability $\to 1$ as $x \to \infty$, $\omega(n) \leqslant 2\log_2 x$ (e.g., Theorem 1.8). By the definition of β_k and Lemma 6.11, with probability $1 - o(1)$, the set $\mathbf{B}$ defined in that Lemma has k distinct subsets $B_1, \dots, B_k$ with equal sums. For each $b \in B$, let p_b be a prime factor of n lying in T_b. Let $d_i = \prod_{b \in B_i} p_b$, for $1 \leqslant i \leqslant k$. We have

$$\Big| \sum_{b \in B_i} \log p_b - \sum_{b \in B_j} \log p_b \Big| \leqslant \frac{|B_i| + |B_j|}{K} \leqslant \frac{4\log_2 x}{(\log x)^c}.$$

Thus,

$$\max(d_j) \leqslant \min(d_j) \exp\left\{ O\left(\frac{\log_2 x}{(\log x)^c} \right) \right\} = \min(d_j) \left(1 + O\left(\frac{\log_2 x}{(\log x)^c} \right) \right).$$

Since c is arbitrary subject to $c < \beta_k/(1-\beta_k)$, we conclude that $\alpha_k \geqslant \beta_k/(1-\beta_k)$. □

It remains to prove Theorem 6.9, which we accomplish in the next section.

4. Proof of Theorem 6.9

Our proof use the method introduced by Maier and Tenenbaum in **[52]**, adapted to the random set $\mathbf{A}$. This can be thought of as a 'global-to-local' principle, where the local behavior of divisor ratios is deduced from a result about the global distribution of ratios. A similar principle will be utilized in the study of integers with a divisor in a *given* interval.

It is easy to see the claimed lower bound on β_k given that β_2 exists, following the idea in Lemma 6.10. Indeed, fix very small $\varepsilon > 0$ and $m \in \mathbb{N}$, and set $\alpha = \beta_2 - \varepsilon$. Let D be large and set $I_i = (D^{\alpha^i}, D^{\alpha^{i-1}}]$ for $1 \leqslant i \leqslant m$. By the definition of β_2, with probability $\to 1$ as $D \to \infty$ there are distinct sets $A_{i,j} \in I_i$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant 2$ such that

$$\Sigma A_{i,1} = \Sigma A_{i,2} \qquad (1 \leqslant i \leqslant m).$$

It follows that the 2^m sets $B_{\mathbf{j}} = \bigcup_{i=1}^m A_{i,j_i}$, where $\mathbf{j} = (j_1, \dots, j_m) \in \{1,2\}^m$, all have equal sums. It follows that $\beta_{2^m} \geqslant \alpha^m$. As ε is arbitrary, $\beta_{2^m} \geqslant \beta_2^m$. The claim now follows from the obvious fact that $(\beta_k)_{k=2}^\infty$ is a decreasing sequence ($k+1$ equal subset sums implies k equal subset sums).

It thus remains to establish the value of β_2. First, we show that $|\mathbf{A} \cap I| \approx H(I)$ with high probability.

LEMMA 6.12. *Let I be a finite set of positive integers, and $1 \leqslant \theta \leqslant \sqrt{H(I)}$. Then*

$$\mathbb{P}\Big(\big| |\mathbf{A} \cap I| - H(I) \big| \geqslant \theta \sqrt{H(I)} \Big) \leqslant 2\mathrm{e}^{-\frac{1}{3}\theta^2}.$$

PROOF. Let $H = H(I)$. By hypothesis, $H \geqslant 1$. For any $\lambda > 0$ we have

$$\mathbb{E}\, \lambda^{|\mathbf{A} \cap I|} = \prod_{j \in I} \left(1 + \frac{\lambda - 1}{j} \right) \leqslant \mathrm{e}^{(\lambda-1)H}.$$

Take $\lambda = 1 + \theta/\sqrt{H}$. Then

$$\begin{aligned} \mathbb{P}\big(|\mathbf{A} \cap I| \geqslant H + \theta\sqrt{H} \big) &\leqslant \mathbb{E}\, \lambda_1^{|\mathbf{A} \cap I| - H - \theta\sqrt{H}} \\ &\leqslant \lambda_1^{-H-\theta\sqrt{H}} \mathrm{e}^{(\lambda_1 - 1)H} = \mathrm{e}^{-Q(\lambda_1)} \leqslant \mathrm{e}^{-\frac{1}{3}\theta^2} \end{aligned}$$

using (0.4) at the last step. Similarly, if $\lambda_2 = 1 - \theta/\sqrt{H}$ then

$$\mathbb{P}\big(|\mathbf{A} \cap I| \leqslant H - \theta\sqrt{H} \big) \leqslant \mathbb{E}\, \lambda_2^{|\mathbf{A} \cap I| - H + \psi\sqrt{H}} \leqslant \mathrm{e}^{-Q(\lambda_2)} \leqslant \mathrm{e}^{-\frac{1}{3}\theta^2}.$$ □

Lemma 6.13. *Given $1 \leqslant C < D$, $\psi \geqslant 1$ and $0 < \varepsilon \leqslant 1$, the probability that both*

$$\Big|\#\big(\mathbf{A} \cap (C, v]\big) - \log(v/C)\Big| \leqslant \varepsilon \log(v/C)) \qquad (C\mathrm{e}^{\psi} \leqslant v \leqslant D),$$
$$\Big|\#\big(\mathbf{A} \cap (u, D]\big) - \log(D/u)\Big| \leqslant \varepsilon \log(D/u) \qquad (C \leqslant u \leqslant D\mathrm{e}^{-\psi})$$

is $\geqslant 1 - O_\varepsilon(\mathrm{e}^{-(1/3)\varepsilon^2\psi})$.

Proof. The probability in question is at least 1 minus the probability that

$$\Big|\#\mathbf{A} \cap (\mathrm{e}^k, \mathrm{e}^l] - (l-k)\Big| \geqslant \varepsilon(l-k) - 4 \tag{6.6}$$

for some $k, l \in \mathbb{N}$ with either $k = \lfloor \log C \rfloor$ and $k + \psi - 1 \leqslant l \leqslant \log D + 1$ or $l = \lfloor \log D \rfloor + 1$ and $\log C - 1 \leqslant k \leqslant l - \psi + 2$. This comes from the monotonicity of $\#(\mathbf{A} \cap (C, v])$ as a function of v, and the monotonicity of $\#(\mathbf{A} \cap (u, D])$ as a function of u (cf., the proof of Theorem 1.18). By Lemma 6.12 with $\theta = \varepsilon(l-k)^{1/2} + O((l-k)^{-1/2})$, the probability that (6.6) holds is $O(\mathrm{e}^{-\frac{1}{3}\varepsilon^2(k-l)})$. Summing on k, l gives the lemma. □

To establish the lower bound on β_2, we first analyze the *global* distribution of divisor ratios. For $1 \leqslant C < D$ define the random set

$$\lambda(C, D) = \Big\{\Sigma A_1 - \Sigma A_2 : A_1 \subseteq \mathbf{A} \cap (C, D], A_2 \subseteq \mathbf{A} \cap (C, D], A_1 \cap A_2 = \emptyset, A_1 \neq \emptyset, A_2 \neq \emptyset\Big\},$$

where ΣA is the sum of the elements of A.

Lemma 6.14. *Fix ε satisfying*

$$0 < \varepsilon < \frac{1}{200}.$$

Suppose that $1 \leqslant C < D$ and

$$C \leqslant D^{1 - \frac{1}{\log 3} - \varepsilon}.$$

For any $10 \leqslant \xi \leqslant \log D$, with probability $1 - O_\varepsilon(1/\log \xi)$ we have

$$\#\lambda(C, D) \geqslant D/\xi \quad \textit{and} \quad \Sigma(\mathbf{A} \cap [1, D]) \leqslant \xi D.$$

Proof. We may assume that $\xi \geqslant \mathrm{e}^{20}$, else the lemma is trivial. Firstly, $\mathbb{E}\,\Sigma(\mathbf{A} \cap [1, D]) = D$, hence by Markov's inequality,

$$\mathbb{P}\big(\Sigma(\mathbf{A} \cap [1, D])) > \xi D\big) \leqslant \frac{1}{\xi}. \tag{6.7}$$

We will use a second moment argument. Let V denote the number of quadruples (A_1, A_2, A_3, A_4) with each A_i a nonempty subset of A', $A_1 \cap A_2 = A_3 \cap A_4 = \emptyset$ and

$$\Sigma A_1 - \Sigma A_2 = \Sigma A_3 - \Sigma A_4. \tag{6.8}$$

Our main task is to show that with probability $1 - O_\varepsilon(1/\log \xi)$ we have

$$V \leqslant \xi \cdot \frac{3^{2|A'|}}{2D} \qquad \text{and} \qquad |A'| \geqslant \frac{\log D}{\log 3}. \tag{6.9}$$

Assuming (6.9), let

$$g_m = \#\{(A_1, A_2) : \emptyset \neq A_1 \subseteq A', \emptyset \neq A_2 \subseteq A', A_1 \cap A_2 = \emptyset, \Sigma A_1 - \Sigma A_2 = m\}.$$

In this notation, $V = \sum_m g_m^2$ and $\lambda(C, D) = \{m : g_m > 0\}$. By Cauchy's inequality,

$$(3^{|A'|} - 2^{|A'|+1})^2 = \Big(\sum_m g_m\Big)^2 \leqslant \#\lambda(C, D) \sum_m g_m^2 = \#\lambda(C, D)\, V.$$

The lemma now follows from (6.9), since $(3^{|A'|} - 2^{|A'|+1})^2 \geqslant \frac{1}{2} 3^{2|A'|}$ for large enough D.

To prove (6.9), we first separate off those solutions of (6.8) with $A_1 = A_3$ and $A_2 = A_4$. Thus,

$$V \leqslant 3^{|A'|} + V^*,$$

where V^* counts solutions with $A_1 \neq A_3$ or $A_2 \neq A_4$. Let $\psi = \frac{\log \xi}{3}$. Let E be the event that

$$|\mathbf{A} \cap (B, D)| \geqslant (1-\varepsilon)\log(D/B) \qquad (C \leqslant B \leqslant D\mathrm{e}^{-\psi}).$$

This implies that

$$|\mathbf{A} \cap (B, D)| \geqslant (1-\varepsilon)\log(D/B) - \psi \qquad (C \leqslant B \leqslant D). \tag{6.10}$$

By Lemma 6.13, $\mathbb{P}(\overline{E}) \ll \mathrm{e}^{-(1/3)\varepsilon^2\psi} \ll_\varepsilon 1/\log\xi$. Assume now that we are in event E. In particular, since $\log(D/C) \geqslant (\frac{1}{\log 3} + \varepsilon)\log D$, we have

$$3^{|A'|} \geqslant 3^{(1-\varepsilon)\log(D/C)-\psi} \geqslant D$$

if D is large enough, giving the second part of (6.9). Hence,

$$V \leqslant \frac{\xi}{4} \cdot \frac{3^{2|A'|}}{D} + V^*. \tag{6.11}$$

Our next task is to show that

$$T := \mathbb{E}\left(\frac{V^*\mathbb{1}(E)}{3^{2|A'|}}\right) \ll \frac{\xi^{1/2}}{D}. \tag{6.12}$$

Assuming (6.12), Markov's inequality gives

$$\mathbb{P}\Big(V^* \geqslant \frac{\xi}{4} \cdot \frac{3^{2|A'|}}{D} \text{ and } E\Big) \leqslant \frac{T}{(\xi/4)D^{-1}} \ll \xi^{-1/2},$$

which implies that (6.9) holds with probability $1 - O_\varepsilon(1/\log\xi)$, as required.

It remains to prove (6.12). Assuming E, consider solutions of (6.8) with $A_1 \neq A_3$ or $A_2 \neq A_4$. Elements in $A_1 \cap A_3$ and in $A_2 \cap A_4$ cancel each other. Let n^* be the largest uncancelled element, and write

$$A' = Q \cup \{n^*\} \cup Q', \quad \max Q < n^* < \min Q'.$$

In particular, all elements of Q' cancel out in (6.8), that is,

$$\Sigma A_1 \cap (Q \cup \{n^*\}) - \Sigma A_2 \cap (Q \cup \{n^*\}) = \Sigma A_3 \cap (Q \cup \{n^*\}) - \Sigma A_4 \cap (Q \cup \{n^*\}). \tag{6.13}$$

Also, by (6.10), if $M = \max Q$ then

$$|Q'| = |\mathbf{A} \cap (M, D]| - 1 \geqslant (1-\varepsilon)\log(D/M) - \psi - 1 =: k(M). \tag{6.14}$$

Given Q, the intersections $A_i \cap Q$ for $1 \leqslant i \leqslant 4$, and one of the $O(1)$ possibilities for which sets A_i contain n^* (there are 6 possibilities, namely n^* may lie in a single set A_i, or in A_1 and A_4 or in A_2 and A_3), the element n^* is uniquely determined by (6.13). We will compute T as follows:

- Fix $M \in (C, D]$ and $Q \subset (C, M]$ with $M \in Q$; compute $\mathbb{P}(\mathbf{A} \cap (C, M] = Q)$;
- Fix the sets $A_i \cap Q$, $i = 1, 2, 3, 4$;
- Fix one of the possibilities for n^*; compute $\mathbb{P}(\mathbf{A} \cap (M, n^*] = \{n^*\})$;
- Fix $Q' \subseteq (n^*, D]$ for which (6.14) holds; compute $\mathbb{P}(\mathbf{A} \cap (n^*, D] = Q')$;
- there are then $3^{|Q'|}$ ways to form the sets $A_i \cap Q'$, $1 \leqslant i \leqslant 4$, namely each element of Q' lies in $A_1 \cap A_3$, or in $A_2 \cap A_4$ or neither (it cannot be in both since A_1, A_2 are disjoint).
- By (6.14), we have

$$\frac{3^{|Q'|}}{3^{2|A'|}} = \frac{1}{3^{2+2|Q|+|Q'|}} \leqslant \frac{1}{3^{2+k(M)+2|Q|}}.$$

Following this process, we have

$$T \leqslant \sum_{C<M\leqslant D} \frac{1}{3^{2+k(M)}} \sum_{\substack{Q\subseteq(C,M]\\ M\in Q}} \frac{\mathbb{P}(\mathbf{A}\cap(C,M]=Q)}{3^{2|Q|}} \sum_{A_1\cap Q,\dots,A_4\cap Q} \sum_{n^*} \mathbb{P}\big(\mathbf{A}\cap(M,n^*]=\{n^*\}\big)\times$$
$$\times \sum_{\substack{Q'\subseteq(n^*,D]\\ |Q'|\geqslant k(M)}} \mathbb{P}\big(\mathbf{A}\cap(n^*,D]=Q'\big).$$

The inner sum over Q' is clearly $\leqslant 1$. For each n^*,

$$\mathbb{P}\big(\mathbf{A}\cap(M,n^*]=\{n^*\}\big)\leqslant \frac{1}{n^*}\leqslant \frac{1}{M}.$$

Also, with Q fixed there are $3^{2|Q|}$ ways to choose $A_1\cap Q,\dots,A_4\cap Q$. Thus,

$$T\ll \sum_{C<M\leqslant D}\frac{1}{M\cdot 3^{k(M)}}\sum_{\substack{Q\subseteq(C,M]\\ M\in Q}}\mathbb{P}\big(\mathbf{A}\cap(C,M]=Q\big).$$

The inner sum on Q equals $\mathbb{P}(M\in\mathbf{A})=1/M$. Recalling (6.14), we see that

$$T\ll_\varepsilon 3^\psi \sum_{C<M\leqslant D}\frac{1}{M^2(D/M)^{(1-\varepsilon)\log 3}} = 3^\psi D^{-(1-\varepsilon)\log 3}\sum_{C<M\leqslant D} M^{(1-\varepsilon)\log 3-2}\ll \frac{3^\psi}{D},$$

as required for (6.12). This completes the proof of the lemma. □

Proof that $\beta_2\geqslant 1-\frac{1}{\log 3}$. We use a device from **[52]** to build up a solution of $\Sigma A_1=\Sigma A_2$, starting with Lemma 6.14. Fix $\varepsilon\in(0,\frac{1}{200})$, let N be large and let $\xi=\xi(N)=\log_2 N$, let $D_0=N^{1-\varepsilon}$ and $D_j=D_0(3\xi)^j$ for $j\geqslant 1$. Let $C=D_0^{1-\frac{1}{\log 3}-\varepsilon}$ and put $\lambda_j=\lambda(C,D_j)$ for $j\geqslant 0$. Let $\mathcal{E}_j$ be the event that $0\notin\lambda_j$, and let $\mathcal{E}_j'$ be the event that $\mathcal{E}_j$ holds and also that $|\lambda_j|\geqslant D_j/\xi$ and $\Sigma(\mathbf{A}\cap(C,D_j])\leqslant \xi D_j$. By Lemma 6.14,

$$0\leqslant \mathbb{P}\,\mathcal{E}_j-\mathbb{P}\,\mathcal{E}_j'\ll 1/\log\xi.$$

Let $\mathcal{H}_j$ be the event that there are integers $n,n'\in\mathbf{A}$ with $\xi D_j<n<n'\leqslant 3\xi D_j$ and $n-n'\in\lambda_j$, and define $\mathcal{F}_j=\mathcal{E}_j'\wedge\mathcal{H}_j$. Since $\mathcal{F}_j$ implies that $0\in\lambda_{j+1}$ we have

$$\mathbb{P}\,\mathcal{E}_{j+1}\leqslant \mathbb{P}\,\mathcal{E}_j-\mathbb{P}\,\mathcal{F}_j.$$

With $\mathbf{A}\cap(C,D_j]$ fixed such that $\mathcal{E}_j'$ holds we have

$$\begin{aligned}\mathbb{P}\,\mathcal{H}_j &\geqslant \sum_{\substack{m\in\lambda_j\\ m>0}}\ \sum_{\xi D_j<n\leqslant 2\xi D_j}\mathbb{P}\left(\mathbf{A}\cap(\xi D_j,3\xi D_j]=\{n,n+m\}\right)\\ &= \sum_{\substack{m\in\lambda_j\\ m>0}}\ \sum_{\xi D_j<n\leqslant 2\xi D_j}\frac{1}{n(n+m)}\prod_{\substack{\xi D_j<h\leqslant 3\xi D_j\\ h\neq n,h\neq n+m}}\left(1-\frac{1}{h}\right)\\ &\gg \sum_{\substack{m\in\lambda_j\\ m>0}}\ \sum_{\xi D_j<n\leqslant 2\xi D_j}\frac{1}{n(n+m)}\\ &\gg \frac{|\lambda_j|}{\xi D_j}\gg\frac{1}{\xi^2}.\end{aligned}$$

It follows that

$$\mathbb{P}\,\mathcal{F}_j=\mathbb{P}\,\mathcal{E}_j'\,\mathbb{P}(\mathcal{F}_j\,|\,\mathcal{E}_j')\gg\xi^{-2}\mathbb{P}\,\mathcal{E}_j'.$$

Hence, for some constants $c > 0$ and $c' > 0$, which depend only on ε,

$$\mathbb{P}\,\mathcal{E}_{j+1} \leqslant \mathbb{P}\,\mathcal{E}_j - c\xi^{-2}\mathbb{P}\,\mathcal{E}'_j = (1 - c/\xi^2)\mathbb{P}\,\mathcal{E}_j + \frac{c'}{\log\xi}\,\frac{c}{\xi^2}.$$

Iterating this, starting with $\mathbb{P}\mathcal{E}_0 \leqslant 1$, gives

$$\mathbb{P}\mathcal{E}_j \leqslant (1 - c/\xi^2)^j + \frac{c'c}{\xi^2\log\xi}\sum_{h=0}^{j-1}(1 - c/\xi^2)^h.$$

Taking $J = \lfloor \xi^3 \rfloor$, we conclude that $\mathbb{P}\,\mathcal{E}_J \ll 1/\log\xi$. Since $D_J < N$, it follows that with probability $1 - O(1/\log\xi)$, there are distinct sets $A_1, A_2 \subseteq \mathbf{A} \cap (C, N]$ with $\Sigma A_1 = \Sigma A_2$. As $\varepsilon > 0$ is arbitrary, this proves that

$$\beta_2 \geqslant 1 - \frac{1}{\log 3}. \qquad \square$$

Proof of the upper bound $\beta_2 \leqslant 1 - \frac{1}{\log 3}$. Fix $\varepsilon > 0$ small, let N be large and put $C = N^{1-\frac{1}{\log 3}+\varepsilon}$. It suffices to show that with probability $\to 0$ as $N \to \infty$, $\mathbf{A} \cap (C, N]$ has two disjoint, nomempty subsets with equal sums. Let E be the event that

$$|\mathbf{A} \cap (C, B]| \leqslant \log(B/C) + \frac{\varepsilon}{2}\log N \qquad (C \leqslant B \leqslant N). \tag{6.15}$$

If N is large enough, this occurs if we have

$$|\mathbf{A} \cap (C, B]| \leqslant (1 + \varepsilon/4)\log(B/C) \qquad (C\log N \leqslant B \leqslant N).$$

By Lemma 6.13 with $\psi = \log\log N$, $\mathbb{P}\,\overline{E} = o(1)$ as $N \to \infty$. The probability that there exist distinct nonempty sets $A_1, A_2 \in \mathbf{A} \cap (C, N]$ with $\Sigma A_1 = \Sigma A_2$ is at most $\mathbb{P}(\overline{E}) + \mathbb{E}\,S \cdot \mathbb{1}(E)$, where S is the number of pairs A_1, A_2 of distinct subsets of $\mathbf{A} \cap (C, N]$ with equal sums. For counting S, WLOG let $M = \max A_1 > \max A_2$, $A'_1 = A_1 \setminus \{M\}$ and $M' = \max(A'_1 \cup A_2)$. Given A'_1 and A_2, M is unique determined (if it exists; it must also satisfy $M > M'$). Also, with M' fixed, (6.15) implies that

$$|\mathbf{A} \cap (C, M']| \leqslant \log(M'/C) + \frac{\varepsilon}{2}\log N =: k(M').$$

Then

$$\mathbb{E}\,S \cdot \mathbb{1}(E) \leqslant 2 \sum_{C < M' \leqslant N} \sum_{\substack{A' \subseteq (C, M'] \\ M' \in A' \\ |A'| \leqslant k(M')}} \mathbb{P}(\mathbf{A} \cap (C, M'] = A') \sum_{\substack{A'_1, A_2 \subseteq A' \\ A'_1 \cap A_2 = \emptyset}} \mathbb{P}\big(M \in \mathbf{A} \cap (M', N]\big).$$

The innermost probability is $\frac{1}{M} \leqslant \frac{1}{M'}$, while the number of pairs (A'_1, A_2) equals $3^{|A'|} \leqslant 3^{k(M')}$. Thus,

$$\begin{aligned}
\mathbb{E}\,S \cdot \mathbb{1}(E) &\leqslant 2 \sum_{C < M' \leqslant N} \frac{3^{k(M')}}{M'} \sum_{\substack{A' \subseteq (C, M'] \\ M' \in A'}} \mathbb{P}(\mathbf{A} \cap (C, M'] = A') \\
&\leqslant 2 \sum_{C < M' \leqslant N} \frac{3^{k(M')}}{(M')^2} \\
&\ll \frac{3^{(\varepsilon/2)\log N}}{C^{\log 3}} \sum_{C < M' \leqslant N} (M')^{\log 3 - 2} \\
&\ll_\varepsilon 3^{(\varepsilon/2)\log N} N^{-\varepsilon\log 3} \ll N^{-\varepsilon/2}.
\end{aligned}$$

$\square$

5. Exercises

Exercise 6.1. Let $2 \leqslant \ell \leqslant k$. Show that $\beta_k \geqslant \beta_\ell^{\lceil \frac{\log k}{\log \ell} \rceil}$.

CHAPTER 7

Integers with a divisor in a given interval

1. Exact formulas

For $0 < y < z$, let $\tau(n; y, z)$ be the number of divisors d of n which satisfy $y < d \leqslant z$. Define $H(x, y, z)$ to be the number of positive integers $n \leqslant x$ with $\tau(n; y, z) > 0$, and $H_r(x, y, z)$, the number of $n \leqslant x$ with $\tau(n; y, z) = r$. By inclusion-exclusion,

$$H(x, y, z) = \sum_{k \geqslant 1} (-1)^{k-1} \sum_{y < d_1 < \cdots < d_k \leqslant z} \left\lfloor \frac{x}{\operatorname{lcm}[d_1, \cdots, d_k]} \right\rfloor,$$

but this is not useful for estimating $H(x, y, z)$ unless $z - y$ is small. With y and z fixed, however, this formula implies that the set of positive integers having at least one divisor in $(y, z]$ has an *asymptotic density*, i.e.

$$\varepsilon(y, z) := \lim_{x \to \infty} \frac{H(x, y, z)}{x} = \sum_{k \geqslant 1} (-1)^{k-1} \sum_{y < d_1 < \cdots < d_k \leqslant z} \frac{1}{\operatorname{lcm}[d_1, \cdots, d_k]}.$$

In these notes we primarily focus on the case $y \leqslant x^{3/4}$. Since $d|n$ if and only if $(n/d)|n$, if $n \approx x$ then we expect that

$$H(x, y, z) \approx H(x, x/z, x/y).$$

This has been proved in **[29]**, although the details are rather messy due to the fact that many n are significantly smaller than x, and we actually require short interval versions, that is, estimating $H(x, y, z) - H(x', y, z)$ from below.

2. Easy bounds when z is small or large

When $z - y$ is small compared with y, it is very rare to have more than one divisor in $(y, z]$.

Theorem 7.1. *For $2 \leqslant y + 1 \leqslant x^{3/4}$ with $z = (1 + \eta)y \in [y + 1, 2y]$. Then*

$$H(x, y, z) = x \sum_{y < d \leqslant z} \frac{1}{d} + O\big(\eta y + \eta^2 x \log(2y)\big).$$

Consequently, if $y \to \infty$, $z - y \to \infty$, $z = o(x)$ and $\eta = o(1/\log(2y))$ as $x \to \infty$, then

$$H(x, y, z) \sim \eta x.$$

Remarks. If $y \leqslant \sqrt{x}$ and $z - y = o(y/\log y)$, then the second conclusion follows. Using more sophisticated methods, Tenenbaum **[61]** showed that $H(x, y, z) \sim \eta x$ in the range $z - y \leqslant y/(\log y)^{\log 4 - 1 + \varepsilon}$ for any fixed $\varepsilon > 0$, and the constant $\log 4 - 1$ cannot be replaced by a smaller number. See also **[45**, p. 38–39**]**.

Proof. We start with a simple truncated form of inclusion-exclusion, which implies that

$$\sum_{y < d \leqslant z} \left\lfloor \frac{x}{d} \right\rfloor - \sum_{y < d_1 < d_2 \leqslant z} \left\lfloor \frac{x}{[d_1, d_2]} \right\rfloor \leqslant H(x, y, z) \leqslant \sum_{y < d \leqslant z} \left\lfloor \frac{x}{d} \right\rfloor.$$

The first sum over d equals

$$O(\eta y) + x \sum_{y < d \leqslant z} \frac{1}{d}.$$

In the sum over d_1, d_2, let $m = (d_1, d_2)$, $t_i = d_i/m$ for $i = 1, 2$. We also have $m \leqslant d_2 - d_1 \leqslant z - y = \eta y$. Therefore,

$$\begin{aligned}\sum_{y<d_1<d_2\leqslant z} \left\lfloor \frac{x}{[d_1,d_2]} \right\rfloor &\leqslant x \sum_{m\leqslant \eta y} \frac{1}{m} \sum_{y/m<t_1<t_2\leqslant z/m} \frac{1}{t_1t_2} \\ &\leqslant x \sum_{m\leqslant \eta y} \frac{1}{m}\Big(\log\frac{z}{y} + O\Big(\frac{m}{y}\Big)\Big)^2 \\ &\ll x\eta^2 \sum_{m\leqslant \eta y} \frac{1}{m} \\ &\ll x\eta^2 \log(2y).\end{aligned}$$

The first assertion follows.

To achieve the second conclusion, we use

$$\sum_{y<d\leqslant z} \frac{1}{d} = \log\frac{z}{y} + O(1/y) = \eta + O(\eta^2 + 1/y).$$

Under the hypotheses, $\eta \to 0$ and $\log\min(2y, 2x/y) \to \infty$, and we deduce that $H(x, y, z) \sim \eta x$. □

Theorem 7.2. *(a) Fix $c > 0$. For some $y_0(c)$, if $y \geqslant y_0(c)$ and $y^{1+c} \leqslant z \leqslant x$ then $H(x, y, z) \gg_c x$.*
(b) For all $2 \leqslant y \leqslant z \leqslant x$, we have

$$H(x, y, z) = x\Big(1 + O\Big(\frac{\log y}{\log z}\Big)\Big).$$

Proof. For (a), we will show more, that there are $\gg_c x$ integers $n \leqslant x$ with exactly one *prime* divisor in $(y, z]$. Let T denote the set of primes in $(y, z]$. We may assume without loss of generality that $c \leqslant 1$ and that $z = y^{1+c}$. We have, by Mertens' estimate (0.5),

$$H(T) = \log(1 + c) + O(1/\log y) \in [\tfrac{1}{2}\log(1 + c), 1]$$

if $y_0(c)$ is large enough. By Exercise 1.5,

$$\begin{aligned}\mathbb{P}_x(\omega(n, T) \geqslant 1) &\geqslant \mathbb{E}_x\Big[\omega(n, T) - \binom{\omega(n,T)}{2}\Big] \\ &\geqslant \frac{1}{x}\sum_{y<p\leqslant z} \Big\lfloor \frac{x}{p} \Big\rfloor - \frac{H(T)^2}{2} \\ &\geqslant H(T) - \frac{H(T)^2}{2} - O\Big(\frac{\pi(z)}{x}\Big) \\ &\geqslant \frac{H(T)}{3} \gg_c 1\end{aligned}$$

if $y_0(c)$ is large enough.

The upper bound in (b) is trivial. For the lower bound, we also consider integers with at least one prime factor in $(y, z]$. By Theorem 1.13,

$$\mathbb{P}_x\{\tau(n, y, z) = 0\} \leqslant \mathbb{P}_x\{\omega(n, T) = 0\} \ll \mathrm{e}^{-H(T)} \ll \frac{\log y}{\log z}$$

and (b) follows. □

Remarks. In general, the error term $O(\frac{\log y}{\log z})$ cannot be improved. For example, note that $\tau(n,y,z)=0$ if $n=mh$ with $m\leqslant y$ and $P^-(h)>z$. If $z\leqslant\sqrt{x}$ then by Exercise 3.1,

$$\#\{n\leqslant x:\tau(n,y,z)=0\}\geqslant\sum_{m\leqslant y^{1/2}}\Phi\Big(\frac{x}{m},z\Big)\gg\sum_{m\leqslant y^{1/2}}\frac{x}{m\log z}\asymp x\frac{\log y}{\log z}.$$

3. The critical case $z=2y$

Besicovitch [**6**] showed in 1934 that

$$\liminf_{y\to\infty}\varepsilon(y,2y)=0, \tag{7.1}$$

and used this to construct an infinite set $\mathscr{A}$ of positive integers such that its set of multiples $\mathscr{B}(\mathscr{A})=\{am:a\in\mathscr{A},m\geqslant 1\}$ does not possess asymptotic density. Erdős in 1935 [**22**] showed $\lim_{y\to\infty}\varepsilon(y,2y)=0$ and in 1960 [**26**] gave the further refinement

$$\varepsilon(y,2y)=(\log y)^{-\mathcal{E}+o(1)}\quad(y\to\infty),$$

where

$$\mathcal{E}=1-\frac{1+\log\log 2}{\log 2}=0.086071\ldots.$$

In 1984, Tenenbaum [**61**] refined the bounds to

$$\frac{x}{(\log y)^{\mathcal{E}}\exp\{c\sqrt{\log_2 y\log_3 y}\}}\ll H(x,y,2y)\ll\frac{x}{(\log y)^{\mathcal{E}}(\log_2 y)^{1/2}},$$

valid for $100\leqslant y\leqslant\sqrt{x}$, where $c>0$ is a constant. Hall and Tenenbaum's book *Divisors* [**45**, Ch. 2] gives a simpler proof of Tenenbaum's theorem.

Theorem 7.3 (Ford [29]). *Uniformly for $4\leqslant y\leqslant x^{1/2}$ we have*

$$H(x,y,2y)\asymp\frac{x}{(\log y)^{\mathcal{E}}(\log_2 y)^{3/2}}.$$

Remarks. Theorem 1 of [**29**] establishes the order of $H(x,y,z)$ for all x,y,z, improving upon cruder estimates of Tenenbaum [**61**].

Our proof of the lower bound implicit in Theorem 7.3 gives a somewhat stronger conclusion, where we restrict to integers in an interval which are squarefree and free of small prime factors. We will leave the details as an exercise, Exercise 7.1 below.

Theorem 7.4. *Fix $c'<1<c$, and $w\geqslant 1$. We have, for $4\leqslant y\leqslant x^{1/2}$,*

$$\#\{c'x<n\leqslant x:\mu^2(n)=1,\tau(n,y,cy)\geqslant 1\}\gg_{c,c'}H(x,y,z).$$

Remarks. In Theorem 7.4, we consider c,c',w all fixed. In [**32**], the order of magnitude of $\#\{n\leqslant x:P^-(n)>w,\tau(n,y,2y)\geqslant 1\}$ was determined for all x,y,w. The results change behavior depending on the relative size of y,w.

4. Some applications of Theorem 7.3

1. Distinct products in a multiplication table, a problem of Erdős from 1955 ([**25**], [**26**]). Let $A(x)$ be the number of positive integers $n\leqslant x$ which can be written as $n=m_1m_2$ with each $m_i\leqslant\sqrt{x}$. Earlier, see Theorem 1.28, we showed that $A(x)\ll x/(\log x)^{\mathcal{E}}$.

Theorem 7.5. *We have*

$$A(x)\asymp\frac{x}{(\log x)^{\mathcal{E}}(\log\log x)^{3/2}}.$$

PROOF. Evidently $A(x)$ is at least the number of $n \leqslant x/4$ with a divisor in $(\frac{1}{4}\sqrt{x}, \frac{1}{2}\sqrt{x}]$. Also, if $n = m_1 m_2$ with $m_1 \leqslant \sqrt{x}, m_2 \leqslant \sqrt{x}$ then for some integer $k \geqslant 0$, $2^{-k-1}\sqrt{x} < m_1 \leqslant 2^{-k}\sqrt{x}$, and hence $n \leqslant 2^{-k}x$. Thus,

$$H\left(\frac{x}{4}, \frac{\sqrt{x}}{4}, \frac{\sqrt{x}}{2}\right) \leqslant A(x) \leqslant \sum_{k \geqslant 0} H\left(\frac{x}{2^k}, \frac{\sqrt{x}}{2^{k+1}}, \frac{\sqrt{x}}{2^k}\right).$$

The theorem now follows quickly from Theorem 7.3. For the right side, use Theorem 7.3 when $k \leqslant 10 \log_2 x$ and the trivial upper bound $x/2^k$ when $k > 10 \log_2 x$. □

2. Distribution of Farey gaps (Cobeli, Ford, Zaharescu [**9**]).

THEOREM 7.6. *Let $(\frac{0}{1}, \frac{1}{Q}, \dots, \frac{Q-1}{Q}, \frac{1}{1})$ denote the sequence of Farey fractions of order Q, and let $N(Q)$ denote the number of distinct gaps between successive terms of the sequence. Then*

$$N(Q) \asymp \frac{Q^2}{(\log Q)^{\delta} (\log\log Q)^{3/2}}.$$

PROOF. The distinct gaps are precisely those products qq' with $1 \leqslant q, q' \leqslant Q$, $(q, q') = 1$ and $q + q' > Q$. Thus, $\max(q, q') > Q/2$, so $N(Q) \leqslant H(Q^2, Q/2, Q)$ and the upper bound follows from Theorem 7.3. For the lower bound, consider squarefree $0.3Q^2 < n \leqslant 0.36Q^2$ with a divisor in $(0.5Q, 0.6Q]$. The complementary divisor then lies in $(0.5Q, 0.72Q]$. Hence

$$N(Q) \geqslant \frac{1}{2} \#\{0.3Q^2 < n \leqslant 0.36Q^2 : \mu^2(n) = 1, \tau(n, 0.5Q, 0.6Q) \geqslant 1\}$$

and the lower bound follows from Theorem 7.4. □

3. Density of unions of residue classes. Given moduli $m_1, \dots, m_k$, let $\delta_0(m_1, \dots, m_k)$ be the minimum, over all possible residue classes $a_1 \bmod m_1, \dots, a_k \bmod m_k$, of the density of integers which lie in at least one of the classes. By a theorem of Rogers (see [**41**, p. 242–244]), the minimum is achieved by taking $a_1 = \cdots = a_k = 0$ and thus $\delta_0(m_1, \dots, m_k)$ is the density of integers possessing a divisor among the numbers $m_1, \dots, m_k$. When $m_1, \dots, m_k$ consist of the integers in an interval $(y, z]$, then $\delta_0(m_1, \dots, m_k) = \varepsilon(y, z)$.

4. Partial Möbius divisor sums, which was first studied by Erdős and Hall [**27**]. Define

$$M(n, y) = \sum_{\substack{d \mid n \\ d \leqslant y}} \mu(d).$$

THEOREM 7.7 (K. FORD, UNPUBLISHED). *Let $10 \leqslant y \leqslant \sqrt{x}$. The number of integers $n \leqslant x$ with $M(n, y) \neq 0$ is*

$$\asymp \frac{x}{(\log y)^{\mathcal{E}} (\log_2 y)^{3/2}}.$$

This requires versions of $H(x, y, 2y)$ which count integers free of prime factors $\leqslant w$, uniformly in w, as well as a version counting integers with exactly one divisor in $(y, 2y]$. The former is dealt with in [**32**] and the latter in [**29**].

Here we argue more crudely and show that

$$\#\{n \leqslant x : M(n, y) \neq 0\} \ll \frac{x}{(\log y)^{\mathcal{E}/2}} \qquad (y \leqslant x^{1/3}). \tag{7.2}$$

Let $w = \exp\{(\log y)^{\mathcal{E}/2}\}$. By Theorem 3.8,

$$\#\{n \leqslant x : P^-(n) > w\} = \Phi(x, w) \ll \frac{x}{(\log y)^{\mathcal{E}/2}}.$$

Now consider $n \leqslant x$ with $p = P^-(n) \leqslant w$. If $p^a | n$ with $p^a > w^2$ then for some $d \in \mathbb{N}$ with $d > w$, $d^2 | n$. The number of such n is at most

$$\ll \sum_{d > w} \frac{x}{d^2} \ll \frac{x}{w} \ll \frac{x}{\log y}.$$

Now consider $n \leqslant x$ where $p = P^-(n) \leqslant w$, $p^a \| n$, $p^a \leqslant w^2$, $n = p^a m$. If $\tau(n,y,py) = 0$ then for any squarefree $d|m$, $pd \leqslant y$ and hence

$$M(n,y) = \sum_{\substack{d|m\\ d\leqslant y}} \mu(d) + \mu(pd) = 0.$$

The number of such n is at most

$$\begin{aligned}\sum_{\substack{p\leqslant w\\ p^a\leqslant w^2}} H\Big(\frac{x}{p^a}, y, py\Big) &\ll \sum_{\substack{p\leqslant w\\ p^a\leqslant w^2}} \sum_{0\leqslant k\leqslant \frac{\log p}{\log 2}} H\Big(\frac{x}{p^a}, 2^k y, 2^{k+1}y\Big)\\ &\ll \sum_{\substack{p\leqslant w\\ a\geqslant 1}} \frac{x\log p}{p^a (\log y)^{\mathcal{E}}} \ll \frac{x}{(\log y)^{\mathcal{E}/2}}\end{aligned}$$

by Mertens' estimate (0.6). This proves (7.2).

5. A heuristic for $H(x,y,2y)$

Write $n = n'n''$, where n' is composed only of primes $\leqslant 2y$ and n'' is composed only of primes $> 2y$. For simplicity, assume n' is squarefree and $n' \leqslant y^{100}$. Assume for the moment that the set $D(n') = \{\log d : d|n'\}$ is uniformly distributed in $[0, \log n']$. If n' has k prime factors, then the expected value of $\tau(n', y, 2y)$ should be about $\frac{2^k \log 2}{\log n'} \asymp \frac{2^k}{\log y}$. This is $\gg 1$ precisely when $k \geqslant k_0 + O(1)$, where $k_0 := \Big\lfloor \frac{\log\log y}{\log 2} \Big\rfloor$. Using the fact that, e.g. Theorem 1.13 for the upper bound, the number of $n \leqslant x$ with n' having k prime factors is of order

$$\frac{x}{\log y} \frac{(\log\log y)^k}{k!},$$

we obtain a heuristic estimate for $H(x,y,2y)$ of order

$$\frac{x}{\log y} \sum_{k\geqslant k_0 + O(1)} \frac{(\log\log y)^k}{k!} \asymp \frac{x(\log\log y)^{k_0}}{k_0! \log y} \asymp \frac{x}{(\log y)^{\delta} (\log\log y)^{1/2}}.$$

This is slightly too big, and the reason stems from the uniformity assumption about $D(n')$. In fact, for most n' with about k_0 prime factors, *the set $D(n')$ is far from uniform, possessing many clusters of divisors and large gaps between clusters.* This substantially decreases the likelihood that $\tau(n', y, 2y) \geqslant 1$. If we write $n' = p_1 \cdots p_k$, where $p_1 < p_2 < \ldots < p_k$, then we expect $\log\log p_j \approx \frac{j \log\log y}{k_0} = j \log 2 + O(1)$ for each j. The Central Limit Theorem for prime factors $\leqslant 2y$ (e.g. Theorem 5.7) tell us that with high probability there is a j for which $\log\log p_j \leqslant j\log 2 - c\sqrt{\log\log y}$, where c is a small positive constant. Thus, the 2^j divisors of $p_1 \cdots p_j$ will be clustered in an interval of logarithmic length about $\ll \log p_j \leqslant 2^j \mathrm{e}^{-c\sqrt{\log_2 y}}$. On a logarithmic scale, the divisors of n' will then lie in 2^{k-j} translates of this cluster, the total length of the clusters being $\ll 2^k \mathrm{e}^{-c\sqrt{\log_2 y}}$. A measure of the degree of clustering of the divisors of an integer a is given by

$$\mathscr{L}(a) = \bigcup_{d|a} [-\log 2 + \log d, \log d) \qquad L(a) = \operatorname{meas} \mathscr{L}(a). \tag{7.3}$$

The probability that $\tau(n', y, 2y) \geqslant 1$ should then be about $L(n')/\log y$. Making this precise leads to the upper and lower bounds for $H(x,y,2y)$ given below in Proposition 7.8. The upper bound for $L(a)$ given in Lemma 7.9 (iii) below quantifies how small $L(a)$ must be when there is a j with $\log\log p_j$ considerably smaller than $j\log 2$.

What we really need to count is n for which n' has about k_0 prime factors *and* $L(n') \gg \log n'$. This roughly corresponds to asking for $\log\log p_j \geqslant j\log 2 - O(1)$ for all j. The analogous problem from statistics theory is to ask for the likelihood than given k_0 random numbers in $[0,1]$, there are $\leqslant k_0 x + O(1)$ of them

which are $\leqslant x$, uniformly in $0 \leqslant x \leqslant 1$. Later, we will see that this probability is about $1/k_0 \asymp 1/\log\log y$ and this leads to the correct order of $H(x, y, 2y)$ given in Theorem 7.3.

6. A global-to-local principle

In this section, we estimate $H(x, y, 2y)$ in terms of an average over $L(a)$, as defined in (7.3). As $L(a)$ captures the global distribution of divisors of a, we call this a 'global-to-local' principle. Introduce the notation

$$\mathscr{P}(x) = \{n \in \mathbb{N} : \mu^2(n) = 1, P^+(n) \leqslant x\}.$$

Proposition 7.8. *If y_0 is sufficiently large and $y_0 \leqslant y \leqslant \sqrt{x}$, then*

$$H(x, y, 2y) \asymp \frac{x}{\log^2 y} \sum_{a \in \mathscr{P}(y)} \frac{L(a)}{a}.$$

We first show some basic inequalities for $L(a)$ and then relate sums of the type on the RHS in Proposition 7.8.

Lemma 7.9. *We have*

(i) $L(a) \leqslant \min(\tau(a)\log 2, \log(2a))$;
(ii) If $(a, b) = 1$, *then* $L(ab) \leqslant \tau(b)L(a)$;
(iii) If $p_1 < \cdots < p_k$, *then*

$$L(p_1 \cdots p_k) \leqslant \min_{0 \leqslant j \leqslant k} 2^{k-j}(\log(2p_1 \cdots p_j)).$$

Proof. Part (i) is immediate, since $\mathscr{L}(a)$ is the union of $\tau(a)$ intervals of length $\log 2$, all contained in $[-\log 2, \log a)$. Part (ii) follows from

$$\mathscr{L}(ab) = \bigcup_{d|b} \{u + \log d : u \in \mathscr{L}(a)\}.$$

Combining parts (i) and (ii) with $a = p_1 \cdots p_j$ and $b = p_{j+1} \cdots p_k$ yields (iii). □

Lemma 7.10. *Let $w_2 \geqslant w_1 \geqslant 2$. Then*

$$\sum_{a \in \mathscr{P}(w_2)} \frac{L(a)}{a} \ll \left(\frac{\log w_2}{\log w_1}\right)^2 \sum_{a \in \mathscr{P}(w_1)} \frac{L(a)}{a}.$$

Proof. Given $a \in \mathscr{L}(w_2)$, write a uniquely as $a = a_1 a_2$ where $P^+(a_1) \leqslant w_1 < P^-(a_2)$. By Lemma 7.9 (ii), $L(a) \leqslant \tau(a_2)L(a_1)$. Thus,

$$\sum_{a \in \mathscr{P}(w_2)} \frac{L(a)}{a} = \sum_{a_1 \in \mathscr{P}(w_1)} \frac{L(a_1)}{a_1} \sum_{p|a_2 \Rightarrow w_1 < p \leqslant w_2} \frac{\tau(a_2)\mu^2(a_2)}{a_2}.$$

By Mertens' product estimate (0.7), the sum on a_2 equals

$$\prod_{w_1 < p \leqslant w_2} \left(1 + \frac{2}{p}\right) \leqslant \prod_{w_1 < p \leqslant w_2} (1 - 1/p)^{-2} \ll \left(\frac{\log w_2}{\log w_1}\right)^2.$$ □

For the upper bound we also need the following technical lemma, which is a special case of a result of Koukoulopoulos [**50**, Lemma 2.2].

Lemma 7.11. *We have*

$$\sum_{a \in \mathscr{P}(2y)} \frac{L(a)}{a \log^2(P^+(a) + y^{2/3}/a)} \ll \frac{1}{(\log y)^2} \sum_{a \in \mathscr{P}(2y)} \frac{L(a)}{a}.$$

PROOF. Let $\mathscr{P}_1 = \{a \in \mathscr{P}(y^{1/4}) : a > y^{1/2}\}$. Then clearly

$$\sum_{a\in\mathscr{P}(2y)} \frac{L(a)}{a\log^2(P^+(a)+y^{2/3}/a)} \ll \sum_{a\in\mathscr{P}_1} \frac{L(a)}{a\log^2 P^+(a)} + \frac{1}{(\log y)^2}\sum_{a\in\mathscr{P}(2y)}\frac{L(a)}{a}.$$

For $a \in \mathscr{P}_1$, let $p = P^+(a)$ and $a = pb$, so $b > y^{1/4}$. By Lemma 7.9 (ii), $L(a) \leqslant 2L(b)$ and thus

$$\begin{aligned}\sum_{a\in\mathscr{P}_1}\frac{L(a)}{a\log^2 P^+(a)} &\leqslant 2\sum_{p\leqslant y^{1/4}}\frac{1}{p\log^2 p}\sum_{\substack{b\in\mathscr{P}(p)\\ b>y^{1/4}}}\frac{L(b)}{b}\\ &\leqslant 2\sum_{p\leqslant y^{1/4}}\frac{1}{p\log^2 p}\frac{4^3}{\log^3 y}\sum_{b\in\mathscr{P}(p)}\frac{L(b)\log^3 b}{b}.\end{aligned}$$

Next,

$$\begin{aligned}\sum_{b\in\mathscr{P}(p)}\frac{L(b)\log^3 b}{b} &= \sum_{b\in\mathscr{P}(p)}\frac{L(b)}{b}\sum_{p_1|b,p_2|b,p_3|b}(\log p_1)(\log p_2)(\log p_3)\\ &\leqslant 8\sum_{p_1,p_2,p_3\leqslant p}\frac{(\log p_1)(\log p_2)(\log p_3)}{[p_1,p_2,p_3]}\sum_{t\in\mathscr{P}(p)}\frac{L(t)}{t},\end{aligned}$$

where we have written $b = [p_1, p_2, p_3]t$ and used Lemma 7.9 (ii) again. Considering separately the three cases ($p_1 = p_2 = p_3$, two of the p_i equal, all p_i distinct), we find that

$$\sum_{p_1,p_2,p_3\leqslant p}\frac{(\log p_1)(\log p_2)(\log p_3)}{[p_1,p_2,p_3]} \ll (\log p)^3$$

by Mertens' estimate. Extending the range of t to $t \in \mathscr{P}(2y)$, we get

$$\sum_{a\in\mathscr{P}_1}\frac{L(a)}{a\log^2(P^+(a)+y^{2/3}/a)} \ll \sum_{p\leqslant y^{1/4}}\frac{1}{p\log^2 p}\frac{(\log p)^3}{(\log y)^3}\sum_{t\in\mathscr{P}(2y)}\frac{L(t)}{t}.$$

A final application of Mertens' estimate concludes the proof. □

We are now ready to embark on the proof of Proposition 7.8.

We begin with the lower bound, which is easier. Consider integers $n = ap_1p_2b \leqslant x$ with p_1 and p_2 prime,

$$a \leqslant y^{1/5} < p_1 < p_2 \leqslant \frac{1}{4}y^{4/5} < P^-(b),$$

and with $\log(y/p_1p_2) \in \mathscr{L}(a)$. The last condition implies that there is a divisor $d|a$ with

$$\frac{d}{2} \leqslant \frac{y}{p_1p_2} < d,$$

which is equivalent to $y < dp_1p_2 \leqslant 2y$. Thus, for such n, $\tau(n, y, 2y) \geqslant \tau(ap_1p_2, y, 2y) \geqslant 1$. In particular, $y^{4/5} \leqslant y/a < p_1p_2 \leqslant 2y$, so that $x/ap_1p_2 \geqslant x/(2y^{6/5}) \geqslant \frac{1}{2}y^{4/5}$. Thus, by Exercise 3.1, for each triple a, p_1, p_2, the number of possible b is

$$\geqslant \Phi\left(\frac{x}{ap_1p_2}, \frac{1}{4}y^{4/5}\right) \gg \frac{x}{ap_1p_2\log y}.$$

Now $\mathscr{L}(a)$ is the disjoint union of intervals of length $\geqslant \log 2$, all contained in $[-\log 2, \frac{1}{5}\log y]$. For each such interval $[u, v]$ we have by Mertens' estimae (0.5)

$$\sum_{\substack{u\leqslant\log(y/p_1p_2)\leqslant v\\ y^{1/5}<p_1<p_2<\frac{1}{4}y^{4/5}}}\frac{1}{p_1p_2} \geqslant \sum_{8y^{1/5}<p_1\leqslant y^{2/5}}\frac{1}{p_1}\sum_{ye^{-v}/p_1<p_2\leqslant ye^{-u}/p_1}\frac{1}{p_2} \gg \frac{v-u}{\log y}.$$

Thus, with a fixed, we have

$$\sum_{\log(y/p_1p_2)\in\mathscr{L}(a)} \frac{1}{p_1p_2} \gg \frac{L(a)}{\log y}.$$

Hence,

$$H(x,y,2y) \gg \frac{x}{\log^2 y} \sum_{a\leqslant y^{1/5}} \frac{L(a)}{a}.$$

Next, we replace the sum over a more convenient set, starting with

$$\sum_{a\leqslant y^{1/5}} \frac{L(a)}{a} \geqslant \sum_{\substack{a\leqslant y^{1/5}\\ a\in\mathscr{P}(y^{1/15})}} \frac{L(a)}{a} \geqslant \sum_{a\in\mathscr{P}(y^{1/15})} \frac{L(a)}{a}\left(1-\frac{\log a}{\log(y^{1/5})}\right).$$

Next,

$$\begin{aligned}\sum_{a\in\mathscr{P}(y^{1/15})} \frac{L(a)\log a}{a} &= \sum_{a\in\mathscr{P}(y^{1/15})} \frac{L(a)}{a}\sum_{p|a}\log p\\ &= \sum_{p\leqslant y^{1/15}} \frac{\log p}{p} \sum_{\substack{b\in\mathscr{P}(y^{1/15})\\ p\nmid b}} \frac{L(pb)}{b}\\ &\leqslant \sum_{p\leqslant y^{1/15}} \frac{2\log p}{p} \sum_{b\in\mathscr{P}(y^{1/15})} \frac{L(b)}{b}\\ &= (2\log(y^{1/15})+O(1)) \sum_{b\in\mathscr{P}(y^{1/15})} \frac{L(b)}{b}\end{aligned}$$

using the relation $L(pb)\leqslant 2L(b)$ from Lemma 7.9 (ii) and Mertens' estimate (0.6). Thus,

$$\sum_{a\leqslant y^{1/5}} \frac{L(a)}{a} \geqslant \sum_{a\in\mathscr{P}(y^{1/15})} \frac{L(a)}{a}\left(1-\frac{2\log(y^{1/15})+O(1)}{\log(y^{1/5})}\right) \gg \sum_{a\in\mathscr{P}(y^{1/15})} \frac{L(a)}{a}.$$

Applying Lemma 7.10 with $w_1 = y^{1/15}$ and $w_2 = y$ concludes the proof of the lower bound in Proposition 7.8.

We now prove the upper bound in Proposition 7.8. We will first show that

$$H(x,y,2y) \ll x \sum_{a\in\mathscr{P}(2y)} \frac{L(a)}{a\log^2(y^{2/3}/a+P^+(a))}. \tag{7.4}$$

We may assume that y is sufficiently large (say $y\geqslant y_0$), as (7.4) is trivial for small y. First, we relate $H(x,y,2y)$ to $H^*(x,y,z)$, the number of *squarefree* integers $n\leqslant x$ with $\tau(n,y,z)\geqslant 1$. Let δ be a fixed, small constant. Write $n=n'n''$, where n' is squarefree, n'' is squarefull and $(n',n'')=1$. The number of $n\leqslant x$ with $n''>y^\delta$ is

$$\leqslant x\sum_{n''>y^\delta}\frac{1}{n''} \ll \frac{x}{y^{\delta/2}},$$

since the number of squarefull integers below w is $O(\sqrt{w})$. If $n''\leqslant y^\delta$, then for some $f|n''$, n' has a divisor in $(y/f, 2y/f]$, hence

$$H(x,y,2y) \leqslant \sum_{n''\leqslant y^\delta}\sum_{f|n''} H^*\left(\tfrac{x}{n''},\tfrac{y}{f},\tfrac{2y}{f}\right) + O\left(\frac{x}{y^{\delta/2}}\right). \tag{7.5}$$

For any n'' and f, $y/f \geqslant y^{1-\delta}$. Next, we show that

$$H^*(x_1,y_1,2y_1)-H^*(\tfrac12 x_1,y_1,2y_1)\ll x_1\sum_{a\in\mathscr{P}(2y_1)}\frac{L(a)}{a\log^2\left(y_1^{3/4}/a+P^+(a)\right)}\quad(y^{1-\delta}\leqslant y_1\leqslant x_1^{\frac12+\delta}). \tag{7.6}$$

Consider squarefree $n\in(\frac12 x_1,x_1]$ with a divisor in $(y_1,2y_1]$. Put $z_1=2y_1$, $y_2=\frac{x_1}{4y_1}$, $z_2=\frac{x_1}{y_1}$. Then $n=m_1m_2$ with $y_i<m_i\leqslant z_i$ $(i=1,2)$. For some $j\in\{1,2\}$ we have $p=P^+(m_j)<P^+(m_{3-j})$. Write

$$n=abp,\qquad P^+(a)<p<P^-(b).$$

Then $b>p$ and this is crucial to our argument. Since $\tau(ap,y_j,z_j)\geqslant 1$ and

$$y_2\geqslant\frac14 x_1^{\frac12-\delta}\geqslant\frac14\,y_1^{\frac{1/2-\delta}{1/2+\delta}}\geqslant y_1^{3/4}$$

if δ is small enough, we have

$$p\geqslant y_j/a\geqslant y_1^{3/4}/a.$$

Thus, $p\geqslant Q(a):=\max(P^+(a),y_1^{3/4}/a)$. We also have $p\leqslant\min(z_1,z_2)\leqslant 2y_1$. As noted earlier, $b>p$ and so $ap\leqslant x_1/p$. Hence, by (3.8), given a and p, the number of possible b is

$$\leqslant\Phi\left(\frac{x_1}{ap},p\right)\ll\frac{x_1}{ap\log p}\leqslant\frac{x_1}{ap\log Q(a)},$$

Since a has a divisor in $(y_j/p,z_j/p]$, we have $\log(y_j/p)\in\mathscr{L}(a)$ or $\log(2y_j/p)\in\mathscr{L}(a)$ (the latter case is needed if $j=2$ since $z_2=4y_2$). Since $\mathscr{L}(a)$ is the disjoint union of intervals of length $\geqslant\log 2$ with total measure $L(a)$, by repeated use of Mertens' sum estimate (0.5), we obtain

$$\sum_{\substack{\log(cy_j/p)\in\mathscr{L}(a)\\ p\geqslant P^+(a)}}\frac1p\ll\frac{L(a)}{\log Q(a)}\qquad(c=1,2),$$

and (7.6) follows upon summing over all possible a and over $j=1,2$.

Write $x_2=x/n''$, $y_1=y/f$. Each $n\in(x_2/y_1^\delta,x_2]$ lies in an interval $(2^{-r-1}x_2,2^{-r}x_2]$ for some integer $0\leqslant r\leqslant\frac{\delta\log y_1}{\log 2}$. We note that $y_1\geqslant y^{1-\delta}$ since $f\leqslant n''\leqslant y^\delta$ and also

$$x_1=2^{-r}x_2\geqslant x_2y_1^{-\delta}\geqslant xy^{-2\delta}\geqslant y^{2-2\delta}\geqslant y_1^{2-2\delta},$$

which implies $y_1\leqslant x_1^{\frac{1}{2(1-\delta)}}\leqslant x_1^{\frac12+\delta}$. Applying (7.6) with $x_1=2^{-r}x_2$ and summing over r we find that

$$H^*(x_2,y_1,2y_1)\ll\frac{x_2}{y_1^\delta}+x_2\sum_{a\in\mathscr{P}(2y_1)}\frac{L(a)}{a\log^2\left(y_1^{3/4}/a+P^+(a)\right)}.$$

The first term x_2/y_1^δ may be ignored because $L(1)=\log 2$ and thus the term $a=1$ is $\gg 1/\log^2 y_1$. Thus, by (7.5),

$$H(x,y,2y)\ll\frac{x}{y^{\delta/2}}+x\sum_{n''\leqslant y^\delta}\frac{1}{n''}\sum_{f\mid n''}\sum_{a\in\mathscr{P}(2y/f)}\frac{L(a)}{a\log^2\left((y/f)^{3/4}/a+P^+(a)\right)}.$$

Again, the term $x/y^{\delta/2}$ is negligible and may be omitted. We have $(y/f)^{3/4}\geqslant(y^{1-\delta})^{3/4}\geqslant y^{2/3}$ for any pair (n'',f) and

$$\sum_{n''}\frac{\tau(n'')}{n''}=\prod_p\left(1+\frac{3}{p^2}+\frac{4}{p^3}+\cdots\right)\ll 1.$$

This completes the proof of (7.4).

Combining (7.4) with Lemma 7.11, we find that

$$H(x,y,2y)\ll\frac{1}{\log^2 y}\sum_{a\in\mathscr{P}(2y)}\frac{L(a)}{a}.$$

Finally, applying Lemma 7.10 with $w_1 = y$ and $w_2 = 2y$ completes the proof of the upper bound in Proposition 7.8.

7. Completion of the lower bound in Theorem 7.3

Lemma 7.12. *For any finite set $\mathscr{A}$ of positive integers,*

$$\sum_{a\in\mathscr{A}} \frac{L(a)}{a} \geqslant (\log 2)\, \frac{\Big(\sum_{a\in\mathscr{A}} \frac{\tau(a)}{a}\Big)^2}{\sum_{a\in\mathscr{A}} \frac{W(a)}{a}},$$

where

$$W(a) = |\{(d,d') : d|a, d'|a, |\log d/d'| \leqslant \log 2\}|.$$

Proof. Since

$$\tau(a)\log 2 = \int \tau(a, \mathrm{e}^u, 2\mathrm{e}^u)\, du = \int \mathbb{1}(u \in \mathscr{L}(a))\tau(a, \mathrm{e}^u, 2\mathrm{e}^u)\, du$$

and $\int \mathbb{1}(u \in \mathscr{L}(a))\, du = L(a)$, by the Cauchy-Schwarz inequality,

$$\begin{aligned}\left(\sum_{a\in\mathscr{A}} \frac{\tau(a)}{a}\right)^2 (\log 2)^2 &= \left(\sum_{a\in\mathscr{A}} \frac{1}{a}\int \tau(a, \mathrm{e}^u, 2\mathrm{e}^u)\, du\right)^2 \\ &\leqslant \left(\sum_{a\in\mathscr{A}} \frac{L(a)}{a}\right)\left(\sum_{a\in\mathscr{A}} \frac{1}{a}\int \tau^2(a, \mathrm{e}^u, 2\mathrm{e}^u)\, du\right).\end{aligned}$$

Now

$$\begin{aligned}\int \tau^2(a, e^u, 2e^u)\, du &= \int \#\{d|a, d'|a, \mathrm{e}^u < d, d' \leqslant 2\mathrm{e}^u\}\, du \\ &= \sum_{d|a, d'|a} \max\big(0, \log 2 - |\log(d'/d)|\big) \leqslant (\log 2) W(a)\end{aligned}$$

and the proof is complete. □

We apply Lemma 7.12 with sets $\mathscr{A}$ of integers whose prime factors are localized. To simplify later analysis, partition the primes into sets $D_1, D_2, \ldots$, where each D_j consists of the primes in an interval $(\lambda_{j-1}, \lambda_j]$, with $\lambda_j \approx \lambda_{j-1}^2$. More precisely, let $\lambda_0 = 1.9$ and define inductively λ_j for $j \geqslant 1$ as the largest prime so that

$$\sum_{\lambda_{j-1} < p \leqslant \lambda_j} \frac{1}{p} \leqslant \log 2. \tag{7.7}$$

For example, $\lambda_1 = 2$, $D_1 = \{2\}$, $\lambda_2 = 7$ and $D_2 = \{3, 5, 7\}$. The left side of (7.7) is $= \log 2 + O(1/\lambda_j)$, hence by Mertens' estimate (0.5),

$$\log\log \lambda_j - \log\log \lambda_{j-1} = \log 2 + O(1/\log \lambda_{j-1}). \tag{7.8}$$

We claim that this implies

$$\log \lambda_j = 2^{j+O(1)} \qquad (j \geqslant 0). \tag{7.9}$$

To see (7.9), let $w_j = \log\log \lambda_j$. Since each D_j contains at least one prime, $w_j \to \infty$ as $j \to \infty$ and hence, for some j_0, if $j \geqslant j_0$ then the big-O term in (7.8) is $\leqslant 0.1$ and $w_j - w_{j-1} \geqslant \log 2 - 0.1 \geqslant 1/2$. It then follows that the big-O term is $\ll \mathrm{e}^{-w_j} \ll \mathrm{e}^{-j/2}$, and thus (7.8) implies

$$(w_j - j\log 2) - (w_{j-1} - (j-1)\log 2) \ll \mathrm{e}^{-j/2}.$$

By Cauchy's criterion, $\lim_{j\to\infty}(w_j - j\log 2)$ exists and (7.9) follows.

For a vector $\mathbf{b} = (b_1, \ldots, b_J)$ of non-negative integers, let $\mathscr{A}(\mathbf{b})$ be the set of square-free integers a composed of exactly b_j prime factors from D_j for each j, and having no other prime factors.

Lemma 7.13. *Assume* $\mathbf{b} = (b_1, \dots, b_J)$. *Then*

$$\sum_{a \in \mathscr{A}(\mathbf{b})} \frac{W(a)}{a} \ll \frac{(2\log 2)^{b_1+\cdots+b_J}}{b_1! \cdots b_J!} \sum_{j=1}^{J} 2^{-j+b_1+\cdots+b_j}.$$

Proof. Let $B = b_1 + \cdots + b_J$ and for $j \geqslant 0$ let $B_j = \sum_{i \leqslant j} b_j$. Let $a = p_1 \cdots p_B$, where

$$p_{B_{j-1}+1}, \dots, p_{B_j} \in D_j \qquad (1 \leqslant j \leqslant J) \tag{7.10}$$

and the primes in each interval D_j are unordered. Since $W(p_1 \cdots p_B)$ is the number of pairs $Y, Z \subseteq \{1, \dots, B\}$ with

$$\left| \sum_{i \in Y} \log p_i - \sum_{i \in Z} \log p_i \right| \leqslant \log 2, \tag{7.11}$$

we have

$$\sum_{a \in \mathscr{A}(\mathbf{b})} \frac{W(a)}{a} \leqslant \frac{1}{b_1! \cdots b_J!} \sum_{Y, Z \subseteq \{1, \dots, B\}} \sum_{\substack{p_1, \dots, p_B \\ (7.10), (7.11)}} \frac{1}{p_1 \cdots p_B}. \tag{7.12}$$

By (7.7), we have

$$\sum_{p_i} \frac{1}{p_i} \leqslant \log 2.$$

When $Y = Z$, the inner sum on the right side of (7.12) is $\leqslant (\log 2)^B$, and there are 2^B such pairs Y, Z. When $Y \neq Z$, let $I = \max[(Y \cup Z) - (Y \cap Z)]$. With all the p_i fixed except for p_I, (7.11) implies that $U \leqslant p_I \leqslant 4U$ for some number U. Let $E(I)$ be defined by $B_{E(I)-1} < I \leqslant B_{E(I)}$, i.e. $p_I \in D_{E(I)}$. By Mertens' bound (0.5) and (7.9),

$$\sum_{\substack{U \leqslant p_I \leqslant 4U \\ p_I \in D_{E(I)}}} \frac{1}{p_I} \ll \frac{1}{\max(\log U, \log \lambda_{E(I)-1})} \ll 2^{-E(I)}.$$

Thus, by (7.7) the inner sum in (7.12) is $\ll 2^{-E(I)} (\log 2)^B$. For each I, there are $2^{B-I+1} 4^{I-1} = 2^{B+I-1}$ corresponding pairs Y, Z. Hence, by (7.12),

$$\sum_{a \in \mathscr{A}(\mathbf{b})} \frac{W(a)}{a} \ll \frac{(2\log 2)^B}{b_1! \cdots b_J!} \left[1 + \sum_{I=1}^{B} 2^{I-E(I)} \right] \ll \frac{(2\log 2)^B}{b_1! \cdots b_J!} \left(1 + \sum_{j=1}^{J} 2^{-j} \sum_{B_{j-1} < I \leqslant B_j} 2^I \right).$$

The sum on I on the right side is $\leqslant 2^{B_j+1} = 2^{1+b_1+\cdots+b_j}$. When $j = 1$, $2^{-j+b_1+\cdots+b_j} \geqslant 2^{-1}$ and thus we may remove the additive term 1 on the right side above. The claimed bound follows. □

Now suppose that y is sufficiently large, M is a sufficiently large, fixed positive integer, $b_i = 0$ for $i < M$, and $b_j \leqslant Mj$ for each j (this last constraint is very mild, as we expect that each D_j contains only 1 prime on average). Let $k = b_M + \cdots + b_J$. By (7.9),

$$\begin{aligned} \sum_{a \in \mathscr{A}(\mathbf{b})} \frac{\tau(a)}{a} &= 2^k \prod_{j=M}^{J} \frac{1}{b_j!} \Bigg(\sum_{p_1 \in D_j} \frac{1}{p_1} \sum_{\substack{p_2 \in D_j \\ p_2 \neq p_1}} \frac{1}{p_2} \cdots \sum_{\substack{p_{b_j} \in D_j \\ p_{b_j} \notin \{p_1, \dots, p_{b_j-1}\}}} \frac{1}{p_{b_j}} \Bigg) \\ &\geqslant 2^k \prod_{j=M}^{J} \frac{1}{b_j!} \left(\log 2 - \frac{b_j}{\lambda_{j-1}} \right)^{b_j} \geqslant \frac{(2\log 2)^k}{2 b_M! \cdots b_J!}. \end{aligned} \tag{7.13}$$

Let

$$k = \left\lfloor \frac{\log\log y}{\log 2} - 2M \right\rfloor, \qquad J = M + k - 1.$$

Let $\mathscr{B}$ be the set of vectors $(b_1,\dots,b_J)$ with $b_i=0$ for $i<M$ and $b_1+\cdots+b_J=k$. Let $\mathscr{B}^*$ be the set of $\mathbf{b}\in\mathscr{B}$ with $b_j\leqslant Mj$ for each $j\geqslant M$. If $\mathbf{b}\in\mathscr{B}^*$ and $a\in\mathscr{A}(\mathbf{b})$, then by (7.9),

$$P^+(a)\leqslant\lambda_J\leqslant\exp\left(2^{J+O(1)}\right)\leqslant y$$

if M is large enough. Put

$$f(\mathbf{b}):=\sum_{h=M}^{J}2^{M-1-h+b_M+\cdots+b_h}=\sum_{h=M}^{J}2^{(b_M-1)+\cdots+(b_h-1)}. \tag{7.14}$$

Since

$$(b_M-1)+\cdots+(b_J-1)=k-(J-M+1)=0, \tag{7.15}$$

we have $f(\mathbf{b})\geqslant 1$ and hence, by Lemma 7.13,

$$\sum_{a\in\mathscr{A}(\mathbf{b})}\frac{W(a)}{a}\ll\frac{(2\log 2)^k}{b_M!\cdots b_J!}\left(\sum_{j=1}^{M-1}2^{-j}+2^{1-M}f(\mathbf{b})\right)\ll\frac{(2\log 2)^k}{b_M!\cdots b_J!}f(\mathbf{b}).$$

By Proposition 7.8, Lemma 7.12, plus (7.13), we have for large y

$$H(x,y,2y)\gg\frac{x(2\log 2)^k}{\log^2 y}\sum_{\mathbf{b}\in\mathscr{B}^*}\frac{1}{b_M!\cdots b_J!f(\mathbf{b})}. \tag{7.16}$$

Roughly speaking,

$$f(\mathbf{b})\approx g(\mathbf{b}):=\max_j 2^{(b_M-1)+\cdots+(b_j-1)}.$$

Observe that the product of factorials is unchanged under permutation of $b_M,\dots,b_J$. Given real numbers $z_1,\cdots,z_k$ with zero sum, there is a cyclic permutation $\mathbf{z}'$ of the vector $\mathbf{z}=(z_1,\dots,z_k)$ all of whose partial sums are $\geqslant 0$: let i be the index minimizing $z_1+\cdots+z_i$ and take $\mathbf{z}'=(z_{i+1},\dots,z_k,z_1,\dots,z_i)$. In combinatorics, this fact is know as the *cycle lemma*. Thus, there is a a cyclic permutation $\mathbf{b}'$ of $\mathbf{b}$ with $g(\mathbf{b}')=1$. Thus, we expect that $1/f(\mathbf{b}')$ will be $\gg 1/k$ on average over $\mathbf{b}'$ and that $1/f(\mathbf{b})\gg 1/k$ on average over $\mathbf{b}\in\mathscr{B}$. This is essentially what we prove next; see (7.18) below.

Lemma 7.14. *For positive real numbers $x_1,\dots,x_r$ with product X, let $x_{r+i}=x_i$ for $i\geqslant 1$. Then*

$$\sum_{j=0}^{r-1}\left(\sum_{h=1}^{r}x_{1+j}\cdots x_{h+j}\right)^{-1}\in\left[\frac{1}{\max(1,X)},\frac{1}{\min(1,X)}\right].$$

Proof. Put $y_0=1$ and $y_j=x_1\cdots x_j$ for $j\geqslant 1$. The sum in question is

$$\sum_{j=0}^{r-1}\left(\sum_{h=1}^{r}\frac{y_{h+j}}{y_j}\right)^{-1}=\sum_{j=0}^{r-1}\frac{y_j}{y_{1+j}+\cdots+y_{r+j}}.$$

Since $y_r=X$,

$$\begin{aligned}y_{1+j}+\cdots+y_{r+j}&=X(y_0+\cdots+y_j)+y_{1+j}+\cdots+y_{r-1}\\&\in[\min(1,X)(y_0+\cdots+y_{r-1}),\max(1,X)(y_0+\cdots+y_{r-1})].\end{aligned}$$

□

We have

$$\sum_{\mathbf{b}\in\mathscr{B}^*}\frac{1}{b_M!\cdots b_J!f(\mathbf{b})}\geqslant S_0-\sum_{M\leqslant j<k/M}S_1(j), \tag{7.17}$$

where

$$S_0=\sum_{\mathbf{b}\in\mathscr{B}}\frac{1}{b_M!\cdots b_J!f(\mathbf{b})},\qquad S_1(j)=\sum_{\substack{\mathbf{b}\in\mathscr{B}\\ b_j>Mj}}\frac{1}{b_M!\cdots b_J!f(\mathbf{b})}.$$

Let $x_i = 2^{b_{M-1+i}-1}$ for $1 \leqslant i \leqslant k$, and $x_i = x_{i-k}$ for $i > k$. By (7.14) and (7.15), $x_1 \cdots x_k = 1$ and

$$f(\mathbf{b}) = x_1 + x_1x_2 + \cdots + x_1x_2\cdots x_k.$$

By Lemma 7.14 and the multinomial theorem,

$$S_0 = \sum_{\mathbf{b}\in\mathscr{B}} \frac{1}{b_M!\cdots b_J!}\ \frac{1}{k}\sum_{j=0}^{k-1}\left(\sum_{h=1}^{k} x_{1+j}\cdots x_{h+j}\right)^{-1} = \frac{k^{k-1}}{k!}. \tag{7.18}$$

To bound $S_1(j)$, apply Lemma 7.14 with $x_i = 2^{b_{j+i}-1}$ for $1 \leqslant i \leqslant J-j$. By (7.15) and $b_j > jM$ we have

$$\begin{aligned} X := x_1\cdots x_{J-j} &= 2^{(b_{j+1}-1)+\cdots+(b_J-1)} \\ &= 2^{-(b_M-1)-\cdots-(b_j-1)} \\ &\leqslant 2^{j-M+1-Mj} \\ &< 1. \end{aligned}$$

From the definition of J and our assumption $j \leqslant k/M$, we have $J - j \geqslant k/2$. Write

$$\mathbf{b}' = (b_M, \ldots, b_{j-1}, b_{j+1}, \ldots, b_J),$$

whose sum of components is $k - b_j$. We will sum over cyclic permutations of $(b_{j+1}, \ldots, b_J)$ using Lemma 7.14. Ignoring the terms with $h \leqslant j$ in (7.14), we have

$$\begin{aligned} f(\mathbf{b}) &\geqslant \sum_{h=j+1}^{J} 2^{M-1-h+b_M+\cdots+b_h} \\ &= \sum_{h=j+1}^{J} 2^{M-1-j+b_M+\cdots+b_j+(b_{j+1}-1)+\cdots+(b_J-1)} \\ &= 2^{M-1-j+b_M+\cdots+b_j}(x_1 + x_1x_2 + \cdots x_1\cdots x_{J-j}). \end{aligned}$$

Since the variables b_i are unrestricted for $i \neq j$, and have sum $k - b_j$, we get

$$\begin{aligned} S_1(j) &\leqslant \sum_{b_j > Mj} \frac{1}{b_j!}\sum_{\mathbf{b}'} \frac{1}{\prod_{i\neq j} b_i!\, 2^{M-1-j+b_M+\cdots+b_j}} \cdot \frac{1}{J-j}\sum_{i=0}^{J-j-1}\left(\sum_{h=1}^{J-j} x_{1+i}\cdots x_{h+i}\right)^{-1} \\ &\leqslant \sum_{b_j > Mj} \frac{1}{b_j!}\sum_{\mathbf{b}'} \frac{1}{\prod_{i\neq j} b_i!\, 2^{M-1-j+b_M+\cdots+b_j}} \cdot \frac{1}{(J-j)X} \\ &= \frac{2^k}{J-j}\sum_{b_j > Mj} \frac{1}{2^{b_j}b_j!}\sum_{\mathbf{b}'}\prod_{i\neq j}\frac{2^{-b_i}}{b_i!} \\ &= \frac{2^k}{J-j}\sum_{b_j > Mj} \frac{1}{2^{b_j}b_j!}\,\frac{\left(\frac{k-1}{2}\right)^{k-b_j}}{(k-b_j)!}, \end{aligned}$$

using the multinomial theorem in the last step. We conclude that

$$\begin{aligned} S_1(j) &\leqslant \frac{2}{k} \sum_{b_j > Mj} \frac{(k-1)^{k-b_j}}{b_j!(k-b_j)!} \\ &= \frac{2(k-1)^{k-1}}{k \cdot k!} \sum_{b_j > Mj} \frac{k(k-1)\cdots(k-b_j+1)}{b_j!(k-1)^{b_j-1}} \\ &\leqslant \frac{2(k-1)^{k-1}}{k!} \sum_{b_j > Mj} \frac{1}{b_j!} \\ &\leqslant \frac{k^{k-1}}{k!} \frac{2}{(Mj)!}. \end{aligned}$$

Hence, if $M \geqslant 2$ then

$$\sum_{M \leqslant j < k/M} S_1(j) \leqslant \frac{k^{k-1}}{10k!}. \tag{7.19}$$

By (7.17), (7.18), and (7.19),

$$\sum_{\mathbf{b} \in \mathscr{B}^*} \frac{1}{b_M! \cdots b_J! f(\mathbf{b})} \geqslant \frac{k^{k-1}}{2k!}.$$

The lower bound in Theorem 7.3 for large y now follows from (7.16) and Stirling's formula:

$$H(x,y,2y) \gg \frac{x(2\log 2)^k k^k}{(\log^2 y)k \cdot k!} \gg \frac{x(2\mathrm{e}\log 2)^k}{(\log^2 y)k^{3/2}} \gg \frac{x}{(\log y)^{\mathcal{E}}(\log_2 y)^{3/2}}.$$

8. Bounding $H(x,y,z)$ above in terms of uniform order statistics

We cut up the sum in Proposition 7.8 according to $\omega(a)$. Let

$$T_k = \sum_{\substack{a \in \mathscr{P}(y) \\ \omega(a)=k}} \frac{L(a)}{a}.$$

Recalling Proposition 7.8, our goal is to show that

$$\sum_k T_k \ll \frac{(\log y)^{2-\mathcal{E}}}{(\log_2 y)^{3/2}}.$$

Note the trivial bound $L(a) \leqslant \min(\tau(a)\log 2, \log(2a)) \approx \min(2^k, \log y)$ if $\omega(a) = k$, from Lemma 7.9. There is a transition at the point where $2^k = \log y$, that is, at

$$k_0 = \left\lfloor \frac{\log_2 y}{\log 2} \right\rfloor.$$

When $|k - k_0|$ is relatively large, it is easy to deduce that T_k is small.

Lemma 7.15. *We have*

$$\sum_{|k-k_0| \geqslant 10 \log_3 y} T_k \ll \frac{(\log y)^{2-\mathcal{E}}}{(\log_2 y)^3}.$$

Proof. When $k \leqslant k_0$ we'll use the bound $L(a) \leqslant \tau(a)\log 2 \leqslant 2^k$. Thus,

$$T_k \leqslant 2^k \sum_{\substack{a \in \mathscr{P}(y) \\ \omega(a)=k}} \frac{1}{a} \leqslant \frac{2^k}{k!}(\log_2 y + O(1))^k \ll \frac{(2\log_2 y)^k}{k!}.$$

We have $\frac{2\log_2 y}{k} \geqslant 2\log 2$, hence

$$\begin{aligned}\sum_{k\leqslant k_0-10\log_3 y} T_k &\ll \sum_{k\leqslant k_0-10\log_3 y} (2\log 2)^{k-k_0}\frac{(2\log_2 y)^{k_0}}{k_0!}\\ &\ll (2\log 2)^{10\log_3 y}\frac{(\log y)^{2-\mathcal{E}}}{\sqrt{\log_2 y}}\\ &\ll \frac{(\log y)^{2-\mathcal{E}}}{(\log_3 y)^3}.\end{aligned}$$

Now suppose that $k > k_0$ and use the bound $L(a) \leqslant \log(2a) \ll \log(a)$ (since $a \geqslant 2$). We have

$$\begin{aligned}T_k &\ll \sum_{\substack{a\in\mathscr{P}(y)\\ \omega(a)=k}} \frac{1}{a}\sum_{p\mid a}\log p\\ &\leqslant \sum_{p\leqslant y}\frac{\log p}{p}\sum_{\substack{b\in\mathscr{P}(y)\\ \omega(b)=k-1}}\frac{1}{b}\\ &\ll (\log y)\frac{(\log_2 y+O(1))^{k-1}}{(k-1)!}.\end{aligned}$$

Since $\frac{\log_2 y+O(1)}{k-1} \geqslant 1/\log 2 - o(1) \geqslant 1.3$ for large y, the sum over k is dominated by the smallest term $k = k_1 := k_0 + \lceil 10\log_3 y\rceil$. Hence

$$\begin{aligned}\sum_{k\geqslant k_0+10\log_3 y} T_k &\ll (\log y)\frac{(\log_2 y+O(1))^{k_1-1}}{(k_1-1)!}\\ &\ll (\log y)\frac{(\log_2 y)^{k_1-1}}{(k_1-1)!}\\ &\ll (\log y)\frac{(\log_2 y)^{k_0}}{k_0!}\left(\frac{1}{\log 2}\right)^{k_1-1-k_0}\\ &\ll \frac{(\log y)^{2-\mathcal{E}}}{\sqrt{\log_2 y}}(\log_2 y)^{10\log\log 2}\\ &\ll \frac{(\log y)^{2-\mathcal{E}}}{(\log_2 y)^3}.\end{aligned}$$

□

Remarks. By the same argument applied to all k we deduce

$$\sum_k T_k \ll \frac{(\log y)^{2-\mathcal{E}}}{\sqrt{\log_2 y}},$$

which is too big by a factor $\log_2 y$. The correct order is achieved by using the more sophisticated bound for $L(a)$ given by Lemma 7.9 (iii). In particular, this captures when there are an unusually large number of small prime factors of a, this forcing $L(a)$ to be small.

For k near k_0, we bound T_k in terms of a mutivariate integral. Since $\sum_{p\leqslant z} 1/p = \log\log z + O(1)$, by partial summation we expect for "nice" functions f that

$$\sum_{p_1<\cdots<p_k\leqslant y}\frac{f\left(\frac{\log_2 p_1}{\log_2 y},\dots,\frac{\log_2 p_k}{\log_2 y}\right)}{p_1\cdots p_k} \approx (\log_2 y)^k \int\limits_{0\leqslant\xi_1\leqslant\cdots\leqslant\xi_k\leqslant 1}\cdots\int f(\mathbf{x})\,d\mathbf{x}.$$

For $a = p_1 \dots p_k$, the function $L(a)$ is not very regular as a function of $p_1, \dots, p_k$. However, the most common way for $L(a)$ to be small is for a to have many small prime factors, and the bound in Lemma 7.9 (iii) captures this nicely. Moreover, this bound has the useful property of being monotone in each variable p_i

Lemma 7.16. *Suppose y is large and $k_0/2 \leqslant k \leqslant 2k_0$. Then*

$$T_k \ll (2\log_2 y)^k U_k(k_0), \quad U_k(v) = \int\limits_{0\leqslant\xi_1\leqslant\dots\leqslant\xi_k\leqslant 1} \cdots \int \min_{0\leqslant j\leqslant k} 2^{-j}(1 + 2^{v\xi_1} + \cdots + 2^{v\xi_j})\, d\mathbf{x}.$$

Proof. Recall the definition of λ_i, D_i from the previous section. Consider $a = p_1 \cdots p_k$, where $p_1 < \cdots < p_k \leqslant y$, and define j_i by $p_i \in D_{j_i}$ $(1 \leqslant i \leqslant k)$. By (7.9), $p_i \in D_j$ implies that $\log p_i \ll 2^j$. By (7.9), $0 \leqslant j_i \leqslant k_1$ for each i, where $k_1 = k_0 + O(1)$. By Lemma 7.9 (iii),

$$L(a) \leqslant 2^{k+1} \min_{0\leqslant g\leqslant k} 2^{-g} \log(2p_1 \cdots p_g) \ll 2^k F(\mathbf{j}),$$

where

$$F(\mathbf{j}) = \min_{0\leqslant g\leqslant k} 2^{-g}(1 + 2^{j_1} + \cdots + 2^{j_g}).$$

For each $1 \leqslant j \leqslant k_1$, let $b_j = \#\{i : p_i \in D_j\}$ Then

$$T_k \ll 2^k \sum_{1\leqslant j_1\leqslant\dots\leqslant j_k\leqslant k_1} F(\mathbf{j}) \prod_{j=1}^{k_1} \frac{(\log 2)^{b_j}}{b_1!} \ll \frac{(2\log 2)^k}{b_1! \cdots b_{k_1}!} \sum_{\mathbf{j}} F(\mathbf{j}).$$

Extend the domain of F to include k-tuples of non-negative real numbers. It is clear that if $j_i - 1 \leqslant t_i \leqslant j_i$ for each i, then $F(\mathbf{j}) \leqslant 2F(\mathbf{t})$. Therefore, writing $B_i = b_1 + \cdots + b_i$ as before,

$$\begin{aligned}\frac{1}{b_1! \cdots b_{k_1}!} \sum_{\mathbf{j}} F(\mathbf{j}) &= \sum_{\mathbf{j}} F(\mathbf{j}) \prod_{j=1}^{k_1} \int\limits_{j-1\leqslant t_{B_{j-1}+1}\leqslant\dots\leqslant t_{B_j}\leqslant j} \cdots \int 1 d\mathbf{t} \\ &\leqslant 2 \int\limits_{0\leqslant t_1\leqslant\dots\leqslant t_k\leqslant k_1} \cdots \int F(\mathbf{t})\, d\mathbf{t}.\end{aligned}$$

Making the change of variables $t_i = k_1\xi_i$ for each i, we see that the multiple integral on the right side equals

$$k_1^k \int\limits_{0\leqslant\xi_1\leqslant\dots\leqslant\xi_k\leqslant 1} \cdots \int \min_{0\leqslant g\leqslant k} 2^{-g} \left(1 + 2^{k_1\xi_1} + \cdots + 2^{k_1\xi_g}\right) d\boldsymbol{\xi}.$$

Recalling that $k_1 = k_0 + O(1)$, we conclude that

$$T_k \ll (2k_0 \log 2 + O(1))^k U_k(k_0).$$

Lastly, $(2k_0 \log 2 + O(1))^k \ll (2\log\log y)^k$ since $k \leqslant 2k_0$, and the lemma follows. □

Estimating $U_k(v)$ is the most complex part of the argument. For comparison purposes, observe that the region of integration has volume $1/k!$ and that the integrand is roughly $\ll \min(1, 2^{v-k})$. This leads to an upper bound roughly like

$$U_k(v) \ll \frac{1}{k!(2^{k-v} + 1)}.$$

The next lemma will be proved in the next section. In the case $|k - v|$ small, this improves upon the trivial bound by a factor $1/k$.

Lemma 7.17. *Suppose k, v are integers with $0 \leqslant k \leqslant 2v$. Then*

$$U_k(v) \ll \frac{1 + |v - k|^2}{(k+1)!(2^{k-v} + 1)}.$$

Proof of Theorem 7.3, upper bound, assuming Lemma 7.17. By Lemmas 7.16 and 7.17,

$$\sum_{k_0\leqslant k\leqslant k_0+10\log_3 y} T_k \ll \sum_{k_0\leqslant k\leqslant 2k_0} 2^{k_0}((k-k_0)^2+1)\,\frac{(\log_2 y)^k}{(k+1)!} \ll \frac{(2\log_2 y)^{k_0}}{(k_0+1)!} \asymp \frac{(\log y)^{2-\mathcal{E}}}{(\log_2 y)^{3/2}}.$$

and

$$\sum_{k_0-10\log_3 y\leqslant k\leqslant k_0} T_k \ll \sum_{k\leqslant k_0} \frac{((k_0-k)^2+1)(2\log_2 y)^k}{(k+1)!} \ll \frac{(2\log_2 y)^{k_0}}{(k_0+1)!} \asymp \frac{(\log y)^{2-\mathcal{E}}}{(\log_2 y)^{3/2}}.$$

Combining these with Lemma 7.15 and Proposition 7.8 completes the proof. □

9. Upper bound, part II

The goal of this section is to prove Lemma 7.17, and thus complete the proof of the upper bound in Theorem 7.3.

Let $Y_1,\dots,Y_k$ be independent, uniformly distributed random variables in $[0,1]$. Let ξ_1 be the smallest of the numbers Y_i, let ξ_2 be the next smallest, etc., so that $0\leqslant\xi_1\leqslant\dots\leqslant\xi_k\leqslant 1$. The numbers ξ_i are the *order statistics* for $Y_1,\dots,Y_k$. Then $k!U_k(v)$ is the expectation of the random variable

$$X=\min_{0\leqslant j\leqslant k} 2^{-j}(1+2^{v\xi_1}+\dots+2^{v\xi_j}).$$

Heuristically, we expect that $\xi_i\approx i/k$, and so when $k\approx v$ we guess that

$$\mathbb{E}\,X \ll \mathbb{E}\min_{1\leqslant j\leqslant k} 2^{-j+v\xi_j}. \tag{7.20}$$

It remains to understand the distribution of $\min_{1\leqslant j\leqslant k} v\xi_j-j$. Let $Q_k(u,v)$ be the probability that $\xi_i\geqslant\frac{i-u}{v}$ for every i, that is, $v\xi_i-i\geqslant -u$ for all i. In the special case $v=k$, Smirnov in 1939 showed that

$$Q_k(x\sqrt{k},k)\sim 1-e^{-2x^2}$$

for each fixed x. The corresponding probability estimate for two-sided bounds on the ξ_i was established by Kolmogorov in 1933 and together these limit theorems are the basis of the *Kolmogorov-Smirnov goodness-of-fit statistical tests*.

In the next lemma, we prove a uniform estimate for $Q_k(u,v)$ from **[30]**. Stronger asymptotics are known, e.g. **[31]**. The remainder of the section is essentially devoted to proving (7.20). The details are complicated, but the basic idea is that if $2^{-j}(2^{v\xi_1}+\dots+2^{v\xi_j})$ is much large than $2^{v\xi_j-j}$, then for some large l, the numbers $\xi_{j-l},\dots,\xi_j$ are all very close to one another. As shown below in Lemmas 7.21 and 7.22, this is quite rare.

Lemma 7.18. *Let $w=u+v-k$. Uniformly in $u\geqslant 0$ and $w\geqslant 0$, we have*

$$Q_k(u,v)\ll\frac{(u+1)(w+1)^2}{k}.$$

Proof. Without loss of generality, suppose $k\geqslant 100$, $u\leqslant k/10$ and $w\leqslant\sqrt{k}$. If $\min_{1\leqslant i\leqslant k}(\xi_i-\frac{i-u}{v})<0$, let l be the smallest index with $\xi_l<\frac{l-u}{v}$ and write $\xi_l=\frac{l-u-\lambda}{v}$, so that $0\leqslant\lambda\leqslant 1$. Let

$$R_l(\lambda)=\operatorname{Vol}\left\{0\leqslant\xi_1\leqslant\dots\leqslant\xi_{l-1}\leqslant\frac{l-u-\lambda}{v}:\xi_i\geqslant\frac{i-u}{v}\,(1\leqslant i\leqslant l-1)\right\}.$$

Then we have

$$\begin{aligned}Q_k(u,v)&=1-\frac{k!}{v}\int_0^1\sum_{u+\lambda\leqslant l\leqslant k}R_l(\lambda)\operatorname{Vol}\left\{\frac{l-u-\lambda}{v}\leqslant\xi_{l+1}\leqslant\dots\leqslant\xi_k\leqslant 1\right\}d\lambda\\&=1-\frac{k!}{v}\int_0^1\sum_{u+\lambda\leqslant l\leqslant k}\frac{R_l(\lambda)}{(k-l)!}\left(\frac{k+w+\lambda-l}{v}\right)^{k-l}d\lambda.\end{aligned}$$

Now suppose that $\xi_k \leqslant 1 - \frac{2w+2}{v} = \frac{k-u-w-2}{v}$. Then $\min_{1\leqslant i\leqslant k}(\xi_i - \frac{i-u}{v}) < 0$. Defining l and λ as before, we have

$$\begin{aligned}\left(1-\frac{2w+2}{v}\right)^k &= k!\,\mathrm{Vol}\left\{0\leqslant \xi_1\leqslant\cdots\leqslant\xi_k\leqslant 1-\frac{2w+2}{v}\right\}\\ &= \frac{k!}{v}\int_0^1 \sum_{u+\lambda\leqslant l\leqslant k-w-2+\lambda} \frac{R_l(\lambda)}{(k-l)!}\left(\frac{k-l-w-2+\lambda}{v}\right)^{k-l} d\lambda.\end{aligned}$$

Thus, for any $A > 0$, we have

$$\begin{aligned}Q_k(u,v) = 1 - A\left(1-\frac{2w+2}{v}\right)^k &- \frac{k!}{v}\int_0^1 \sum_{k-w-2+\lambda<l\leqslant k} \frac{R_l(\lambda)}{(k-l)!}\left(\frac{k+w+\lambda-l}{v}\right)^{k-l} d\lambda\\ &+ \frac{k!}{v}\int_0^1 \sum_{u+\lambda\leqslant l\leqslant k-w-2+\lambda} \frac{R_l(\lambda)}{(k-l)!v^{k-l}}\left[A(k-l-w-2+\lambda)^{k-l} - (k-l+w+\lambda)^{k-l}\right] d\lambda.\end{aligned}$$

Noting that $2-\lambda \geqslant \lambda$, we have

$$\begin{aligned}\left(\frac{k-l-w-2+\lambda}{k-l+w+\lambda}\right)^{k-l} &= \left(1-\frac{w+2-\lambda}{k-l}\right)^{k-l}\left(1+\frac{w+\lambda}{k-l}\right)^{-(k-l)}\\ &= \exp\left\{-(2w+2) + \sum_{j=2}^{\infty}\frac{-(w+2-\lambda)^j + (-1)^j(w+\lambda)^j}{j(k-l)^{j-1}}\right\}\\ &\leqslant e^{-(2w+2)}.\end{aligned}$$

Thus, taking $A = e^{2w+2}$, we conclude that

$$\begin{aligned}Q_k(u,v) &\leqslant 1 - e^{2w+2}\left(1-\frac{2w+2}{v}\right)^k\\ &= 1-\exp\left\{\frac{2w+2}{v}\left(v-k+O(w)\right)\right\}\\ &= 1-\exp\left\{\frac{-2uw+O(u+w^2+1)}{v}\right\}\\ &\leqslant \frac{2uw+O(u+w^2+1)}{v} \ll \frac{(u+1)(w+1)^2}{k}.\end{aligned}$$

□

Lemma 7.19 (Abel 1839). *Let $n \in \mathbb{N}$, $a > 0$ and $b > 0$. Then*

$$\sum_{k=0}^{n}\binom{n}{k}(a+k)^{k-1}(b+n-k)^{n-k-1} = \left(\frac{1}{a}+\frac{1}{b}\right)(n+a+b)^{n-1}.$$

Proof. From Riordan[**60**], p. 18–20. Define

$$A_n(x,y;p,q) = \sum_{k=0}^{n}\binom{n}{k}(x+k)^{k+p}(y+n-k)^{n-k+q}$$

where $p, q \in \mathbb{Z}$, $x > 0$ and $y > 0$. The formula in Lemma 7.19 is the case $p = q = -1$. We first observe that replacing k with $n-k$ yields

$$A_n(x,y;p,q) = A_n(y,x;q,p) \tag{7.21}$$

Next, by the Pascal relation $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, we get (setting $h = k-1$ in the first sum)

$$\begin{aligned} A_n(x,y;p,q) &= \sum_{h=0}^{n-1} \binom{n-1}{h} (x+1+h)^{h+p+1} (y+(n-1)-h)^{n-1-h+q} \\ &\qquad + \sum_{k=0}^{n-1} \binom{n-1}{k} (x+k)^{k+p} (y+1+(n-1)-k)^{(n-1)-k+q+1} \\ &= A_{n-1}(x+1,y;p+1,q) + A_{n-1}(x,y+1;p,q+1). \end{aligned} \tag{7.22}$$

Another identity is obtained by splitting off one factor $x+k$, thus

$$\begin{aligned} A_n(x,y;p,q) &= \sum_{k=0}^{n} \binom{n}{k} (x+k)(x+k)^{k-1+p} (y+n-k)^{n-k+q} \\ &= xA_n(x,y;p-1,q) + n \sum_{k=1}^{n} \binom{n-1}{k-1} (x+k)^{k-1+p} (y+n-k)^{n-k+q} \\ &= xA_n(x,y;p-1,q) + nA_{n-1}(x+1,y;p,q). \end{aligned}$$

Applying (7.22) to the first term we get

$$A_n(x,y;p,q) = xA_{n-1}(x,y+1;p-1,q+1) + (x+n)A_{n-1}(x+1,y;p,q). \tag{7.23}$$

For brevity, write $B_n(x,y) = A_n(x,y;-1,0)$. Taking $p=0$, $q=-1$ in (7.23) and applying (7.21) we deduce that

$$\begin{aligned} B_n(x,y) = A_n(y,x;0,-1) &= yA_{n-1}(y,x+1;-1,0) + (y+n)A_n(y+1,x;0,-1) \\ &= yB_{n-1}(y,x+1) + (y+n)B_{n-1}(x,y+1). \end{aligned} \tag{7.24}$$

It follows from (7.24) by an easy induction on $n \in \mathbb{N}$ that

$$B_n(x,y) = x^{-1}(x+y+n)^n \qquad (n \in \mathbb{N}, x>0, y>0).$$

Inserting this into (7.22) and using (7.21) we deduce that

$$\begin{aligned} A_n(x,y;-1,-1) &= A_{n-1}(x+1,y;0,-1) + A_{n-1}(x,y+1;-1,0) \\ &= B_{n-1}(y,x+1) + B_{n-1}(x,y+1) \\ &= (1/x + 1/y)(x+y+n)^{n-1}, \end{aligned}$$

and this completes the proof of the lemma. □

Lemma 7.20. *If $t \geqslant 2$, $b \geqslant 0$ and $t+a+b > 0$, then*

$$\sum_{\substack{1 \leqslant j \leqslant t-1 \\ j+a>0}} \binom{t}{j} (a+j)^{j-1} (b+t-j)^{t-j-1} \leqslant e^4 (t+a+b)^{t-1}.$$

Proof. Let $C_t(a,b)$ denote the sum in the lemma. We may assume that $a > 1-t$, otherwise $C_t(a,b) = 0$. If $a \geqslant -1$, put $A = \max(1,a)$ and $B = \max(1,b)$. By Lemma 7.19,

$$\begin{aligned} C_t(a,b) \leqslant C_t(A,B) &\leqslant \left(\frac{1}{A} + \frac{1}{B}\right)(t+A+B)^{t-1} \\ &\leqslant 2(t+a+b+3)^{t-1} \\ &\leqslant 2e^{\frac{3(t-1)}{t+a+b}} (t+a+b)^{t-1} < e^4 (t+a+b)^{t-1}. \end{aligned} \tag{7.25}$$

Next assume $a < -1$. For $c > 0$, $(1-c/x)^x$ is an increasing function for $x > c$, thus we have

$$(a+j)^{j-1} = (j-1)^{j-1} \left(1 + \frac{a+1}{j-1}\right)^{j-1} \leqslant (j-1)^{j-1} \left(1 + \frac{a+1}{t-1}\right)^{t-1}.$$

Thus, by (7.25),

$$\begin{aligned} C_t(a,b) &\leqslant \left(\frac{t+a}{t-1}\right)^{t-1} C_t(-1,b) \\ &\leqslant e^4 \left(\frac{(t+a)(t+b-1)}{t-1}\right)^{t-1} = e^4 \left(t+a+b+\frac{(a+1)b}{t-1}\right)^{t-1} \\ &\leqslant e^4 (t+a+b)^{t-1}. \end{aligned}$$

□

We now complete the proof of the upper bound for $H(x,y,2y)$ in Theorem 7.3. Recall our heuristic that

$$\min_{1\leqslant j\leqslant k} 2^{-j}\left(2^{v\xi_1}+\cdots+2^{v\xi_j}\right) \approx \min_{1\leqslant j\leqslant k} 2^{-j+v\xi_j}.$$

This is violated if the minimum occurs at $j=j^*$ and there are many ξ_i clustered near ξ_{j^*}. The next lemma captures the likelihood of such an event.

Lemma 7.21. *Suppose $g,k,s,u,v\in\mathbb{Z}$ satisfy*

$$1\leqslant g\leqslant k-1,\ s\geqslant 0,\ v\geqslant k/2,\ u\geqslant 0,\ u+v\geqslant k+1.$$

Let R be the set of $(\xi_1,\dots,\xi_k)$ satisfying

$$0\leqslant \xi_1\leqslant\cdots\leqslant\xi_k\leqslant 1,\quad \xi_i\geqslant \frac{i-u}{v}\ \ (1\leqslant i\leqslant k) \tag{7.26}$$

and such that, for some $l\geqslant \max(g+1,u)$, we have

$$\frac{l-u}{v}\leqslant\xi_l\leqslant\frac{l-u+1}{v},\qquad \xi_{l-g}\geqslant\frac{l-u-s}{v}. \tag{7.27}$$

Then

$$\mathrm{Vol}(R)\ll \frac{g^2(2(s+1))^g}{g!}\,\frac{(u+1)(u+v-k)^2}{(k+1)!}.$$

Proof. Fix l satisfying $\max(u,g+1)\leqslant l\leqslant k$. Let R_l be the subset of $\boldsymbol{\xi}$ satisfying (7.26) and (7.27) for this particular l. We have $\mathrm{Vol}(R_l)\leqslant V_1V_2V_3V_4$, where, by Lemma 7.18,

$$\begin{aligned} V_1 &= \mathrm{Vol}\{0\leqslant\xi_1\leqslant\cdots\leqslant\xi_{l-g-1}\leqslant\tfrac{l-u+1}{v} : \xi_i\geqslant\tfrac{i-u}{v}\ \forall i\} \\ &= \left(\frac{l-u+1}{v}\right)^{l-g-1}\mathrm{Vol}\{0\leqslant\theta_1\leqslant\cdots\leqslant\theta_{l-g-1}\leqslant 1 : \theta_i\geqslant\tfrac{i-u}{l-u+1}\ \forall i\} \\ &= \left(\frac{l-u+1}{v}\right)^{l-g-1}\frac{Q_{l-g-1}(u,l-u+1)}{(l-g-1)!} \\ &\ll \left(\frac{l-u+1}{v}\right)^{l-g-1}\frac{(u+1)g^2}{(l-g)!}, \end{aligned}$$

$$V_2 = \mathrm{Vol}\{\tfrac{l-u-s}{v}\leqslant\xi_{l-g}\leqslant\cdots\leqslant\xi_{l-1}\leqslant\tfrac{l-u+1}{v}\} = \frac{1}{g!}\left(\frac{s+1}{v}\right)^g,$$

$$V_3 = \mathrm{Vol}\{\tfrac{l-u}{v}\leqslant\xi_l\leqslant\tfrac{l-u+1}{v}\} = \frac{1}{v},$$

$$\begin{aligned} V_4 &= \mathrm{Vol}\{\xi_{l+1}\leqslant\cdots\leqslant\xi_k\leqslant 1 : \xi_i\geqslant\tfrac{i-u}{v}\ \forall i\} \qquad (\text{note that } \xi_{l+1}\geqslant\tfrac{l+1-u}{v}) \\ &= \left(\frac{u+v-l-1}{v}\right)^{k-l}\frac{Q_{k-l}(0,u+v-l-1)}{(k-l)!} \\ &\ll \left(\frac{u+v-l}{v}\right)^{k-l}\frac{(u+v-k)^2}{(k-l+1)!}. \end{aligned}$$

Thus

$$\mathrm{Vol}(R) \ll \frac{(s+1)^g(u+1)g^2(u+v-k)^2}{g!v^k(k+1-g)!}\sum_{\substack{l\geqslant g+1\\ l\geqslant u}}\binom{k+1-g}{l-g}(l-u+1)^{l-g-1}(u+v-l)^{k-l}.$$

By Lemma 7.20 (with $t=k+1-g$, $a=g+1-u$, $b=u+v-k-1$, $j=l-g$), the sum on l is

$$\ll (v+1)^{k-g} \ll v^{k-g} = \frac{v^k}{(k+1)^g}\left(\frac{k+1}{v}\right)^g \ll v^k 2^g \frac{(k-g+1)!}{(k+1)!}$$

and the lemma follows. □

To bound $U_k(v)$, we will bound the volume of the set

$$\mathscr{T}(k,v,m) = \{\boldsymbol{\xi}\in\mathbb{R}^k : 0\leqslant\xi_1\leqslant\cdots\leqslant\xi_k\leqslant 1, 2^{v\xi_1}+\cdots+2^{v\xi_j}\geqslant 2^{j-m}\ (1\leqslant j\leqslant k)\}.$$

Lemma 7.22. *Suppose k,v,m are integers with $1\leqslant k\leqslant 2v$ and $m\geqslant 0$. Set $b=k-v$. Then*

$$\mathrm{Vol}(\mathscr{T}(k,v,m)) \ll \frac{Y}{2^{2^{b-m}}(k+1)!}, \qquad Y=\begin{cases} b & \text{if } b\geqslant m+5\\ (m+5-b)^2(m+1) & \text{if } b\leqslant m+4\end{cases}.$$

Proof. Let $r=\max(5,b-m)$ and $\boldsymbol{\xi}\in\mathscr{T}(k,v,m)$. Then either

$$\xi_j > \tfrac{j-m-r}{v} \quad (1\leqslant j\leqslant k) \tag{7.28}$$

or

$$\min_{1\leqslant j\leqslant k}(\xi_j-\tfrac{j-m}{v}) = \xi_l-\tfrac{l-m}{v}\in[\tfrac{-h}{v},\tfrac{1-h}{v}] \text{ for some integers } h\geqslant r+1, 1\leqslant l\leqslant k. \tag{7.29}$$

Let V_1 be the volume of $\boldsymbol{\xi}\in\mathscr{T}(k,v,m)$ satisfying (7.28). If $b\geqslant m+5$, then (7.28) is not possible since (7.28) implies that

$$\xi_k > \frac{k-m-r}{v} = \frac{k-b}{v} = 1.$$

Thus, if (7.28) holds then $b\leqslant m+4$ and $r=5$. By Lemma 7.18,

$$V_1 \leqslant \frac{Q_k(m+5,v)}{k!} \ll \frac{(m+6)(m+5-b)^2}{(k+1)!} \ll \frac{Y}{2^{2^{b-m}}(k+1)!}.$$

If (7.29) holds, then there is an integer t satisfying

$$t\geqslant h-3,\ \xi_{l-2^t}\geqslant\tfrac{l-m-2t}{v}. \tag{7.30}$$

To see (7.30), suppose such an t does not exist. Then

$$\begin{aligned}2^{v\xi_1}+\cdots+2^{v\xi_l} &\leqslant 2^{h-3}2^{v\xi_l}+\sum_{t\geqslant h-3}2^t\cdot 2^{v\xi_{l-2^t}}\\ &\leqslant 2^{h-3}2^{l-m-h+1}+\sum_{t\geqslant h-3}2^t 2^{l-m-2t}\\ &\leqslant 2^{l-m-1},\end{aligned}$$

a contradiction. Let V_2 be the volume of $\boldsymbol{\xi}\in\mathscr{T}(k,v,m)$ satisfying (7.29). Fix h and t satisfying (7.30) and use Lemma 7.21 with $u=m+h$, $g=2^t$, $s=2t$. The volume of such $\boldsymbol{\xi}$ is

$$\ll \frac{(m+h+1)(m+h-b)^2}{(k+1)!}\,\frac{(4t+2)^{2^t}2^{2t}}{(2^t)!} \ll \frac{(m+h+1)(m+h-b)^2}{2^{2^{t+3}}(k+1)!}.$$

The sum of $2^{-2^{t+3}}$ over $t\geqslant h-3$ is $\ll 2^{-2^h}$. Summing over $h\geqslant r+1$ gives

$$V_2 \ll \frac{(m+r+2)(m-b+r+2)^2}{2^{2^{r+1}}(k+1)!} \ll \frac{Y}{2^{2^{b-m}}(k+1)!}.$$

□

PROOF OF LEMMA 7.17. Assume $k \geqslant 1$, since the lemma is trivial when $k = 0$. Put $b = k - v$. For integers $m \geqslant 1$, consider $\boldsymbol{\xi}$ satisfying

$$2^{-m+1} \leqslant \min_{0 \leqslant j \leqslant k} 2^{-j} \left(1 + 2^{v\xi_1} + \cdots + 2^{v\xi_j}\right) < 2^{-m+2}.$$

For such $\boldsymbol{\xi}$ and for $1 \leqslant j \leqslant k$ we have

$$2^{-j} \left(2^{v\xi_1} + \cdots + 2^{v\xi_j}\right) \geqslant \max(2^{-j}, 2^{1-m} - 2^{-j}) \geqslant 2^{-m},$$

so that $\boldsymbol{\xi} \in \mathscr{T}(k, v, m)$. By Lemma 7.22,

$$U_k(v) \leqslant \sum_{m \geqslant 1} 2^{2-m} \operatorname{Vol}(\mathscr{T}(k, v, m)) \ll \frac{1}{(k+1)!} \sum_{m \geqslant 1} \frac{2^{-m} Y_m}{2^{2^{b-m}}},$$

$$Y_m = \begin{cases} b & \text{if } m \leqslant b - 5 \\ (m + 5 - b)^2 (m + 1) & \text{if } m \geqslant b - 4 \end{cases}.$$

Next,

$$\sum_{m \geqslant 1} \frac{2^{-m} Y_m}{2^{2^{b-m}}} \ll \sum_{1 \leqslant m \leqslant b-5} \frac{b}{2^m 2^{2^{b-m}}} + \sum_{m \geqslant \max(1, b-4)} \frac{(m + 5 - b)^2 (m + 1)}{2^m}.$$

The proof is completed by noting that if $b \geqslant 5$, each sum on the right side is $\ll b 2^{-b}$ and if $b \leqslant 4$, the first sum is empty and the second is $\ll (5 - b)^2 \ll 1 + b^2$. This completes the proof of Lemma 7.17. □

10. Counting integers with a given number of divisors in an interval

Recall $\tau(n, y, z) = \#\{d | n : y < d \leqslant z\}$ and define

$$H_r(x, y, z) = \{n \leqslant x : \tau(n, y, z) = r\}.$$

Of particular interest is the case $r = 1$. Similarly, the exact formula

$$H_r(x, y, z) = \sum_{k \geqslant r} (-1)^{k-r} \binom{k}{r} \sum_{y < d_1 < \cdots < d_k \leqslant z} \left\lfloor \frac{x}{\operatorname{lcm}[d_1, \cdots, d_k]} \right\rfloor$$

implies the existence of

$$\varepsilon_r(y, z) = \lim_{x \to \infty} \frac{H_r(x, y, z)}{x}.$$

for every fixed pair y, z.

In [**29**], it is proved that for every $r \geqslant 1$,

$$H_r(x, y, 2y) \gg_r H(x, y, 2y),$$

that is, a positive proportion of all integers $n \leqslant x$ with a divisor in $(y, 2y]$ have exactly r such divisors. In particular, this disproved a 1960 conjecture of Erdős.

11. Exercises

EXERCISE 7.1. Fix $c' < 1 < c$. Suppose that $3 \leqslant y \leqslant \sqrt{x}$. (a) Show that

$$\#\{c'x < n \leqslant x : \mu^2(n) = 1, \tau(n, y, cy) \geqslant 1\} \gg_{c, c'} \frac{1}{\log^2 y} \sum_{a \in \mathscr{P}(y)} \frac{L(a)}{a}.$$

(b) Use (a) to prove Theorem 7.4.

EXERCISE 7.2. If $1 \leqslant y \leqslant x^{1/\log_2 x}$, show that

$$\frac{H(x, y, 2y)}{x} \sim \varepsilon(y, 2y) \qquad (x \to \infty).$$

CHAPTER 8

Permutations with a fixed set of a given size

1. Introduction and notation

Let k, n be integers with $1 \leqslant k \leqslant n/2$. What is $i(n,k)$, the probability that a random $\sigma \in \mathcal{S}_n$ fixes some set of size k? Equivalently, what is the probability that the cycle decomposition of σ contains disjoint cycles with lengths summing to k? This is analogous to the problem of bounding $H(x,y,2y)$ from the previous Chapter, and we will develop a parallel theory based on the same ideas.

The size of $i(n,k)$ has only recently been at all well understood. The lower bound $\lim_{n\to\infty} i(n,k) \gg \log k/k$ is contained in a paper of Diaconis, Fulman and Guralnick [**11**] in 2008, while the upper bound $i(n,k) \ll k^{-1/100}$ is due to Łuczak and Pyber [**51**] in 1993 (These authors did not make any special effort to optimise the constant $1/100$, but their method does not lead to a sharp bound.) Pemantle, Peres, and Rivin [**57**, Theorem 1.7] proved that $\lim_{n\to\infty} i(n,k) = k^{-\mathcal{E}+o(1)}$, where as before,

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

Theorem 8.1 (Eberhard–Ford–Green[14], 2016). *For $1 \leqslant k \leqslant n/2$,*

$$i(n,k) \asymp \frac{1}{k^{\mathcal{E}}(1+\log k)^{-3/2}}.$$

Since $i(n,n-k) = i(n,k)$, Theorem 8.1 establishes the order of $i(n,k)$ for all n,k.

Theorem 8.1 has implications for a conjecture of Cameron related to random generation of the symmetric group. Cameron conjectured that the proportion of $\sigma \in \mathcal{S}_n$ contained in a transitive subgroup not containing $\mathcal{A}_n$ tends to zero: this was proved by Łuczak and Pyber [**51**] using their bound $i(n,k) \ll k^{-1/100}$. Cameron further guessed that this proportion might decay as fast as $n^{-1/2+o(1)}$ (see [**51**, Section 5]). However Theorem 8.1 has the following corollary.

Corollary 8.2. *The proportion of $\sigma \in \mathcal{S}_n$ contained in a transitive subgroup not containing $\mathcal{A}_n$ is $\gg n^{-\mathcal{E}}(\log n)^{-3/2}$, provided that n is even and greater than 2.*

Proof. By Theorem 8.1 the proportion of $\sigma \in \mathcal{S}_n$ fixing a set B_1 of size $n/2$ is $\asymp n^{-\mathcal{E}}(\log n)^{-3/2}$. Such a permutation σ must also fix the set $B_2 = \{1,\dots,n\} \setminus B_1$, and thus preserve the partition $\{B_1, B_2\}$ of $\{1,\dots,n\}$. Since $|B_1| = |B_2|$, the set of all τ preserving this partition is a transitive subgroup not containing $\mathcal{A}_n$. □

In [**16**] by Eberhard, Ford and Koukoulopoulos, it is shown (among other things) that the proportion of $\sigma \in \mathcal{S}_n$ contained in a transitive subgroup not containing $\mathcal{A}_n$ is $\asymp n^{-\mathcal{E}}(\log n)^{-3/2}$, provided that n is even and greater than 2.

Whether or not a permutation σ has a fixed set of size k depends only on the vector

$$\mathbf{C} = (C_1(\sigma), C_2(\sigma), \dots, C_k(\sigma))$$

listing the number of cycles of length $1,2,\dots,k$, respectively, in σ. Crucial to our argument is the fact (e.g., Theorem 4.2) that $\mathbf{C}$ has limiting distribution (as $n \to \infty$) equal to $\mathbf{X}_k = (X_1, X_2, \dots, X_k)$, where the X_i are independent and X_i has Poisson distribution with parameter $1/i$ (for short, $X_i \stackrel{d}{=} \mathrm{Pois}(1/i)$).

A simple corollary is that the limit $i(\infty,k)=\lim_{n\to\infty} i(n,k)$ exists for every k. Define, for any finite list $\mathbf{c}=(c_1,c_2,\dots,c_k)$ of non-negative integers, the quantity

$$\mathscr{L}(\mathbf{c})=\{m_1+2m_2+\cdots+km_k : 0\leqslant m_j\leqslant c_j \text{ for } j=1,2,\dots,k\}. \tag{8.1}$$

We immediately obtain that

$$i(\infty,k)=\mathbb{P}(k\in\mathscr{L}(\mathbf{X}_k)). \tag{8.2}$$

This makes it easy to compute $i(\infty,k)$ for small values of k. For example we have the extremely well known result (derangements) that

$$i(\infty,1)=\mathbb{P}(X_1\geqslant 1)=1-\frac{1}{\mathrm{e}}\approx 0.6321,$$

and the less well known fact that

$$i(\infty,2)=1-\mathbb{P}(X_1=X_2=0)-\mathbb{P}(X_1=1,X_2=0)=1-2\mathrm{e}^{-3/2}\approx 0.5537.$$

When k is allowed to grow with n, the vector $\mathbf{C}$ is still close to being distributed as $\mathbf{X}_k$, the total variation distance between the two distributions decaying rapidly as $n/k\to\infty$ (Theorem 4.2). This fact is, however, not strong enough for our application. We must establish an approximate analog of (8.2), showing that $i(n,k)$ has about the same order as $\mathbb{P}(k\in\mathscr{L}(\mathbf{X}_k))$, uniformly in $k\leqslant n/2$.

Instead of directly estimating the probability of a single number lying in $\mathscr{L}(\mathbf{X}_k)$, however, we apply a global-to-local principle analogous to Proposition 7.8.

Proposition 8.3. *$i(n,k)\asymp\frac{1}{k}\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)|$ uniformly for $40\leqslant k\leqslant n/2$.*

Theorem 8.1 follows immediately from this and the next proposition, when $k\geqslant 40$.

Proposition 8.4. *$\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)|\asymp k^{1-\mathcal{E}}(1+\log k)^{-3/2}$.*

When $1\leqslant k\leqslant 39$, we argue more directly. If $n=2k$ then Cauchy's formula (Lemma 1.2) implies that

$$i(2k,k)\geqslant\mathbb{P}_{\sigma\in\mathcal{S}_n}(C_k(\sigma)=2)=\frac{1}{2k^2}\gg 1.$$

If $n>2k$ then Lemma 8.5 gives

$$i(n,k)\geqslant\mathbb{P}_{\sigma\in\mathcal{S}_n}\big(C_k(\sigma)=1,C_j(\sigma)=0\ (j<k)\big)\geqslant\frac{1}{k(2k+1)}\gg 1.$$

Thus, Theorem 8.1 follows when $k\leqslant 39$ as well.

Question 1. Is there some constant C such that $i(\infty,k)\sim Ck^{-\mathcal{E}}(\log k)^{-3/2}$?

Question 2. Is $i(\infty,k)$ monotonically decreasing in k?

Data collected by Britnell and Wildon [**8**] shows that this is so at least as far as $i(\infty,30)$, and of course a positive answer is plausible just from the fact that $i(\infty,k)\to 0$.

2. The global-to-local principle

In this section we prove Proposition 8.3.

Lemma 8.5. *Let $1\leqslant m<n$ and $c_1,\dots,c_m$ be non-negative integers satisfying*

$$c_1+2c_2+\cdots+mc_m\leqslant n-m-1.$$

Then

$$\frac{1}{2m+1}\prod_{i=1}^{m}\frac{(1/i)^{c_i}}{c_i!}\leqslant\mathbb{P}_\sigma(C_1(\sigma)=c_1,\dots,C_m(\sigma)=c_m)\leqslant\frac{1}{m+1}\prod_{i=1}^{m}\frac{(1/i)^{c_i}}{c_i!}.$$

Proof. Let $t=c_1+2c_2+\cdots+mc_m$. If $C_j(\sigma)=c_j$ for $1\leqslant j\leqslant m$, write $\sigma=\sigma_1\sigma_2$, where all the cycles in σ_1 have length $\leqslant m$ and all the cycles in σ_2 have length $>m$. Applying Cauchy's Theorem (Lemma 1.2) for σ_1 and (3.5) for σ_2 completes the proof. □

As in the introduction, let $X_1, X_2, \dots$ be independent random variables with distribution $X_j \overset{d}{=} \mathrm{Pois}(1/j)$. We record here that

$$\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)| = \sum_{c_1,\dots,c_k \geqslant 0} |\mathscr{L}(\mathbf{c})| \mathbb{P}(X_1 = c_1) \cdots \mathbb{P}(X_k = c_k) = e^{-H_k} \sum_{c_1,\dots,c_k \geqslant 0} \frac{|\mathscr{L}(\mathbf{c})|}{\prod_{i=1}^k c_i! i^{c_i}}. \tag{8.3}$$

Lemma 8.6. *Let $k \in \mathbb{N}$, $c_1, \dots, c_k \geqslant 0$, $I \subset [k]$ and $c_i' = c_i$ for $i \notin I$, $c_i' = 0$ for $i \in I$. then*

$$|\mathscr{L}(\mathbf{c})| \leqslant |\mathscr{L}(\mathbf{c}')| \prod_{i \in I} (c_i + 1).$$

Proof. Clearly, $\mathscr{L}(\mathbf{c})$ is the union of $\prod_{i \in I}(c_i + 1)$ translates of $\mathscr{L}(\mathbf{c}')$. □

Lemma 8.7. *Suppose that $\ell' \leqslant \ell$. Then*

$$\mathbb{E}\,|\mathscr{L}(\mathbf{X}_\ell)| \leqslant \frac{\ell + 1}{\ell' + 1} \mathbb{E}\,|\mathscr{L}(\mathbf{X}_{\ell'})|.$$

Proof. By Lemma 8.6, $|\mathscr{L}(\mathbf{X}_\ell)| \leqslant (1 + X_{\ell'+1}) \cdots (1 + X_\ell) |\mathscr{L}(\mathbf{X}_{\ell'})|$. Thus by independence,

$$\mathbb{E}\,|\mathscr{L}(\mathbf{X}_\ell)| \leqslant \Bigl(\prod_{i=\ell'+1}^{\ell} \mathbb{E}\,(1 + X_i) \Bigr) \mathbb{E}\,|\mathscr{L}(\mathbf{X}_{\ell'})| = \frac{\ell + 1}{\ell' + 1} \mathbb{E}\,|\mathscr{L}(\mathbf{X}_{\ell'})|.$$ □

Lemma 8.8. *For any $j \leqslant k$ we have*

$$\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)| X_j \leqslant \frac{3}{j} \mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)|.$$

Suppose that $j_1, \dots, j_h \leqslant k$ are distinct integers and that $a_1, \dots, a_h$ are positive integers. Then

$$\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)| X_{j_1}^{a_1} \cdots X_{j_h}^{a_h} \ll_{a_1,\dots,a_h} \frac{1}{j_1 \dots j_h} \mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)|.$$

Proof. Define $\mathbf{X}_k'$ by putting $X_{j_1}' = \cdots = X_{j_h}' = 0$ and $X_j' = X_j$ for all other j. By Lemma 8.6, we have

$$|\mathscr{L}(\mathbf{X}_k)| \leqslant |\mathscr{L}(\mathbf{X}_k')| (1 + X_{j_1}) \cdots (1 + X_{j_h}) \leqslant |\mathscr{L}(\mathbf{X}_k)| (1 + X_{j_1}) \cdots (1 + X_{j_h}).$$

Thus by independence

$$\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)| X_{j_1}^{a_1} \cdots X_{j_h}^{a_h} \leqslant \mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)| \prod_{i=1}^{h} (\mathbb{E}\,X_{j_i}^{a_i} + \mathbb{E}\,X_{j_i}^{a_{i+1}}).$$

When $h = a_1 = 1$ and $j_1 = j$, we have

$$\mathbb{E}\,X_j + X_j^2 = 2\mathbb{E} \binom{X}{2} + 2\mathbb{E}\,X = \frac{1}{j^2} + \frac{2}{j} \leqslant \frac{3}{j}.$$

In general, for $X \overset{d}{=} \mathrm{Pois}(\lambda)$ with $\lambda \leqslant 1$ we have $\mathbb{E}\,X^m \ll_m \lambda$ and the lemma follows. □

We turn now to the proof of Proposition 8.3. In what follows write

$$S(\mathbf{X}_\ell) = X_1 + 2X_2 + \cdots + \ell X_\ell = \max \mathscr{L}(\mathbf{X}_\ell).$$

We will treat the lower bound and upper bound in Proposition 8.3 separately, the former being somewhat more straightforward than the latter.

Proof of Proposition 8.3 (Lower bound). When $k \geqslant 40$, let $r = \lfloor k/20 \rfloor$, so that $r \geqslant 2$, and consider the permutations $\sigma = \alpha\sigma_1\sigma_2\beta \in \mathcal{S}_n$, where σ_1 and σ_2 are cycles, $|\alpha| \leqslant 4r < |\sigma_1| < |\sigma_2| < 16r$, all cycles in α have length $\leqslant r$, all cycles in β have length at least $16r$, and α has a fixed set of size $k - |\sigma_1| - |\sigma_2|$. If $C_i(\alpha) = c_i$ for $1 \leqslant i \leqslant r$, then the last condition is equivalent to $k - |\sigma_1| - |\sigma_2| \in \mathscr{L}(\mathbf{c})$. In particular $|\sigma_1| + |\sigma_2| \leqslant k$, and hence

$$n - |\alpha| - |\sigma_1| - |\sigma_2| \geqslant \frac{4}{5} k \geqslant k - 4r \geqslant 16r.$$

Fix $\mathbf{c}$ and ℓ_1, ℓ_2 with $4r < \ell_1 < \ell_2 < 16r$ such that $k - \ell_1 - \ell_2 \in \mathscr{L}(\mathbf{c})$. By Proposition 8.5, the probability that a random $\sigma \in \mathcal{S}_n$ has c_i cycles of length i $(1 \leqslant i \leqslant r)$, one cycle each of length ℓ_1, ℓ_2 and no other cycles of length $< 16r$ is at least

$$\gg \frac{1}{r\ell_1\ell_2 \prod_{i=1}^r c_i! i^{c_i}} \gg \frac{1}{r^3 \prod_{i=1}^r c_i! i^{c_i}}.$$

Now $\mathscr{L}(\mathbf{c}) \subset [0, 4r]$. Hence, for any ℓ_1 satisfying $4r + 1 \leqslant \ell_1 \leqslant 8r - 1$, there are $|\mathscr{L}(\mathbf{c})|$ admissible values of $\ell_2 > \ell_1$ for which $k - \ell_1 - \ell_2 \in \mathscr{L}(\mathbf{c})$. We conclude that

$$i(n,k) \gg \frac{1}{r^2} \sum_{\substack{c_1, \cdots, c_r \geqslant 0 \\ S(\mathbf{c}) \leqslant 4r}} |\mathscr{L}(\mathbf{c})| \prod_{i=1}^r \frac{(1/i)^{c_i}}{c_i!}.$$

As in (8.3), the sum above equals $e^{H_r} \mathbb{E}\, |\mathscr{L}(\mathbf{X}_r)| \mathbb{1}(S(\mathbf{X}_r) \leqslant 4r)$. Hence, by , we see that

$$i(n,k) \gg \frac{1}{r} \mathbb{E}\, |\mathscr{L}(\mathbf{X}_r)| \mathbb{1}(S(\mathbf{X}_r) \leqslant 4r).$$

To estimate this, we use the inequality

$$\mathbb{1}(S(\mathbf{X}_r) \leqslant 4r) \geqslant 1 - \frac{S(\mathbf{X}_r)}{4r}.$$

By Lemma 8.8 (first part) we have

$$\mathbb{E}\, |\mathscr{L}(\mathbf{X}_r)| S(\mathbf{X}_r) = \sum_{j=1}^r \mathbb{E}\, |\mathscr{L}(\mathbf{X}_r)| j X_j \leqslant 3r \mathbb{E}\, |\mathscr{L}(\mathbf{X}_r)|.$$

It follows that

$$i(n,k) \gg \frac{1}{r} \mathbb{E}\, |\mathscr{L}(\mathbf{X}_r)|.$$

Finally, the lower bound in Proposition 8.3 is a consequence of this and Lemma 8.7. □

Proof of Proposition 8.3 (Upper bound). Temporarily impose a total ordering on the set of all cycles fromed from subsets of $[n]$, first ordering them by length, then imposing an arbitrary ordering of the cycles of a given length. Let $\sigma \in \mathcal{S}_n$ have a divisor of size k. Let $k_1 = k$ and $k_2 = n - k$. Then $\sigma = \sigma_1\sigma_2$, where $|\sigma_1 = k_1$ and $|\sigma_2| = k_2$. For some $j \in \{1, 2\}$, the largest cycle in σ, with respect to our total ordering, lies in σ_{3-j}. Let δ be the largest cycle in σ_j, and note that $|\delta| \leqslant \min(k_1, k_2) = k$. Write $\sigma = \alpha\delta\beta$, where α is the product of all cycles dividing σ which are smaller than δ and β is the product of all cycles which are larger than σ. In particular $|\beta| \geqslant |\delta|$ since β contains the largest cycle in σ, and thus

$$|\delta| \leqslant |\beta| = n - |\delta| - |\alpha|. \tag{8.4}$$

By definition of δ and α, α has a divisor of size $k_j - |\delta|$. Suppose $|\delta| = \ell$, $C_j(\alpha) = c_j$ for $j \leqslant \ell$ and $\mathbf{c} = (c_1, c_2, \ldots, c_\ell)$. Then $k_j - \ell \in \mathscr{L}(\mathbf{c})$. For ℓ and $\mathbf{c}$ satisfying this last condition, we count the number of possible pairs α, δ using Lemma 1.2 to first count the number of *products* $\alpha\delta$ (noting that $C_\ell(\alpha\delta) = c_\ell + 1$)) and then counting the number of possible ways to choose δ (which equals $c_\ell + 1$). The total count is

$$\binom{n}{n - |\alpha| - \ell} (|\alpha| + \ell)! \prod_{i<\ell} \frac{(1/i)^{c_i}}{c_i!} \times \frac{1}{(c_\ell + 1)! \ell^{c_\ell + 1}} \times (c_\ell + 1) = \frac{n!}{\ell(n - |\alpha| - \ell)!} \prod_{i \leqslant \ell} \frac{(1/i)^{c_i}}{c_i!}.$$

Given α and δ, (8.4) and (3.5) imply that the number of choices for β is at most $(n - |\alpha| - \ell)!/\ell$. Thus

$$i(n,k) \leqslant \sum_{j=1}^2 \sum_{\ell=1}^k \frac{1}{\ell^2} \sum_{\substack{c_1, \ldots, c_\ell \geqslant 0 \\ k_j - \ell \in \mathscr{L}(\mathbf{c})}} \prod_{i \leqslant \ell} \frac{(1/i)^{c_i}}{c_i!} = \sum_{j=1}^2 \sum_{c_1, \ldots, c_k \geqslant 0} \prod_{i \leqslant k} \frac{(1/i)^{c_i}}{c_i!} \sum_{\substack{m(\mathbf{c}) \leqslant \ell \leqslant k \\ k_j - \ell \in \mathscr{L}(\mathbf{c})}} \frac{1}{\ell^2},$$

where $m(\mathbf{c}) = \max\{i : c_i > 0\} \cup \{1\}$. With $\mathbf{c}$ fixed, note that $\ell \geqslant \max(m(\mathbf{c}), k_j - S(\mathbf{c}))$. Also, the number of ℓ such that $k_j - \ell \in \mathscr{L}(\mathbf{c})$ is at most $|\mathscr{L}(\mathbf{c})|$. Thus, the innermost sum on the right side above is at most

$$\frac{|\mathscr{L}(\mathbf{c})|}{\max\big(m(\mathbf{c}), k_j - S(\mathbf{c})\big)^2}.$$

Like (8.3), using we thus see that

$$i(n,k) \leqslant 2ek\,\mathbb{E}\,\Big(\frac{|\mathscr{L}(\mathbf{X}_k)|}{\max(m(\mathbf{X}_k), k - S(\mathbf{X}_k))^2}\Big). \tag{8.5}$$

To bound this we use the inequality

$$\frac{1}{\max(m, k-S)^2} \leqslant \frac{4}{k^2}\left(1 + \frac{S^2}{m^2}\right),$$

which can be checked in the cases $S \geqslant k/2$ and $S \leqslant k/2$ separately. It follows from this and (8.5) that

$$i(n,k) \leqslant 8\mathrm{e}\frac{1}{k}\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)| + 8\mathrm{e}\frac{1}{k}\mathbb{E}\,\frac{|\mathscr{L}(\mathbf{X}_k)|S(\mathbf{X}_k)^2}{m(\mathbf{X}_k)^2}. \tag{8.6}$$

The first of these two terms is what we want, but the second requires a keener analysis. By conditioning on $m = m(\mathbf{X}_k)$ we have

$$\begin{aligned}
\mathbb{E}\,\frac{|\mathscr{L}(\mathbf{X}_k)|S(\mathbf{X}_k)^2}{m(\mathbf{X}_k)^2} &= \sum_{m=1}^{k}\frac{1}{m^2}\sum_{\substack{c_1,\dots,c_m\geqslant 0\\ c_m\geqslant 1}}|\mathscr{L}(\mathbf{c})|S(\mathbf{c})^2\mathbb{P}(\mathbf{X}_m = \mathbf{c})\mathbb{P}(X_{m+1} = \cdots = X_{k_j} = 0)\\
&= \sum_{m=1}^{k_j}\frac{1}{m^2}\mathbb{E}\,|\mathscr{L}(\mathbf{X}_m)|S(\mathbf{X}_m)^2\mathbb{1}(X_m \geqslant 1)\mathrm{e}^{H_m - H_k}\\
&\leqslant \frac{\mathrm{e}}{k}\sum_{m=1}^{k}\frac{1}{m}\mathbb{E}\,|\mathscr{L}(\mathbf{X}_m)|S(\mathbf{X}_m)^2X_m.
\end{aligned}$$

In the last step we used the crude inequality $\mathbb{1}(X_m \geqslant 1) \leqslant X_m$. Letting $\mathbf{Y}_m = |\mathscr{L}(\mathbf{X}_m)|$, expanding $S(\mathbf{X}_m)^2 = (X_1 + 2X_2 + \cdots + mX_m)^2$ and using (8.6), we arrive at

$$i(n,k) \ll \frac{1}{k}\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)| + \frac{1}{k}\sum_{m=1}^{k}\frac{1}{m}\sum_{i,i'=1}^{m} ii'\mathbb{E}\,\mathbf{Y}_m X_i X_{i'} X_m. \tag{8.7}$$

The innermost sum is estimated using Lemma 8.8, splitting into various cases depending on the set of distinct values among i, i', m.

Case 1: i, i', m all distinct. Then $ii'\mathbb{E}\,\mathbf{Y}_m X_i X_{i'} X_m \ll \frac{1}{m}\mathbb{E}\,\mathbf{Y}_m$.
Case 2: $i = i' \neq m$. Then $ii'\mathbb{E}\,\mathbf{Y}_m X_i X_{i'} X_m \ll \frac{i}{m}\mathbb{E}\,\mathbf{Y}_m \ll \mathbb{E}\,\mathbf{Y}_m$.
Case 3: $i = i' = m$. Then $ii'\mathbb{E}\,\mathbf{Y}_m X_i X_{i'} X_m \ll m\mathbb{E}\,\mathbf{Y}_m$.
Case 4: $i \neq i' = m$ or $i' \neq i = m$. In both cases $ii'\mathbb{E}\,\mathbf{Y}_m X_i X_{i'} X_m \ll \mathbb{E}\,\mathbf{Y}_m$.

Summing over all cases, it follows that

$$\sum_{i,i'=1}^{m} ii'\mathbb{E}\,\mathbf{Y}_m X_i X_{i'} X_m \ll m\mathbb{E}\,\mathbf{Y}_m.$$

Since clearly $\mathbb{E}\,\mathbf{Y}_m \leqslant \mathbb{E}\,\mathbf{Y}_k$ for every $m \leqslant k$ the result follows from this and (8.7). □

3. The lower bound in Proposition 8.4

We begin by noting that from (8.3) and the inequality $H_k \leqslant 1 + \log k$, it follows

$$\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)| \geqslant \frac{1}{\mathrm{e}k} \sum_{c_1,\dots,c_k \geqslant 0} |\mathscr{L}(\mathbf{c})| \prod_{i=1}^{k} \frac{(1/i)^{c_i}}{c_i!}. \tag{8.8}$$

Fix $r = c_1 + \cdots + c_k$. We claim that

$$\sum_{c_1+\cdots+c_k=r} |\mathscr{L}(\mathbf{c})| \prod_{i=1}^{k} \frac{(1/i)^{c_i}}{c_i!} = \frac{1}{r!} \sum_{a_1,\dots,a_r=1}^{k} \frac{|\mathscr{L}^*(\mathbf{a})|}{a_1 \cdots a_r}, \tag{8.9}$$

where

$$\mathscr{L}^*(\mathbf{a}) = \Big\{ \sum_{i \in I} a_i : I \subseteq [r] \Big\}. \tag{8.10}$$

To see (8.9), we start from the right side and set $c_i = |\{j : a_j = i\}|$ for each i. Then $\mathscr{L}(\mathbf{c}) = \mathscr{L}^*(\mathbf{a})$, $\prod_{i=1}^{k} i^{c_i} = a_1 \cdots a_k$, and each $\mathbf{c} = (c_1, \dots, c_k)$ comes from $\frac{r!}{c_1! \cdots c_k!}$ different choices of $a_1, \dots, a_k$.

Now let $J = \left\lfloor \frac{\log k}{\log 2} \right\rfloor$ and suppose that $b_1, \dots, b_J$ are arbitrary non-negative integers with sum r. Consider the part of the sum on the right side of (8.9) in which

$$b_i = \#\{j : 2^{i-1} \leqslant a_j \leqslant 2^i - 1\} \quad (i = 1, 2, \dots, J), \quad a_j \leqslant 2^J - 1 \ \ (\forall\, j).$$

Writing

$$\mathscr{D}(\mathbf{b}) = \prod_{i=1}^{J} \{2^{i-1}, \dots, 2^i - 1\}^{b_i},$$

we have

$$\frac{1}{r!} \sum_{a_1,\dots,a_r=1}^{2^J-1} \frac{|\mathscr{L}^*(\mathbf{a})|}{a_1 \cdots a_r} = \sum_{b_1+\cdots+b_J=J} \frac{1}{b_1! \cdots b_J!} \sum_{\mathbf{d} \in \mathscr{D}(\mathbf{b})} \frac{|\mathscr{L}^*(\mathbf{d})|}{d_1 \cdots d_r}. \tag{8.11}$$

To see this, fix $b_1, \dots, b_J$ and observe that there are $\frac{r!}{b_1! \cdots b_J!}$ ways to choose which b_i of the variables $a_1, \dots, a_r$ lie in $[2^{i-1}, 2^i - 1]$ for $1 \leqslant i \leqslant J$.

We now take only the terms with $r = J$. Combining (8.8), (8.9) and (8.11) gives

$$\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)| \gg \frac{1}{k} \sum_{b_1+\cdots+b_J=J} \frac{1}{b_1! \cdots b_J!} \sum_{\mathbf{d} \in \mathscr{D}(\mathbf{b})} \frac{|\mathscr{L}^*(\mathbf{d})|}{d_1 \cdots d_J}. \tag{8.12}$$

Lemma 8.9. *For any $\mathbf{b} = (b_1, \dots, b_J)$ with $b_1 + \cdots + b_J = J$ we have*

$$\sum_{\mathbf{d} \in \mathscr{D}(\mathbf{b})} \frac{|\mathscr{L}^*(\mathbf{d})|}{d_1 \cdots d_J} \gg \frac{(2 \log 2)^J}{\sum_{i=1}^{J} 2^{b_1+\cdots+b_i-i}}.$$

Proof. Given $\ell \geqslant 0$, let $R(\mathbf{d}, \ell)$ be the number of $I \subseteq [J]$ with $\ell = \sum_{i \in I} d_i$. Also, define

$$\lambda_i = \sum_{j=2^{i-1}}^{2^i-1} \frac{1}{j}.$$

Since $\frac{1}{j} \geqslant \frac{1}{2j} + \frac{1}{2j+1}$ for all j, $\lambda_i \geqslant \lambda_{i+1}$. Also, $\lim_{i\to\infty} \lambda_i = \log 2$. Thus we conclude that

$$\log 2 \leqslant \lambda_i \leqslant 1 \qquad (1 \leqslant i \leqslant J).$$

Since $\sum_\ell R(\mathbf{d},\ell) = 2^J$, By Cauchy-Schwarz,

$$\begin{aligned} 2^{2J}\prod_{j=1}^{J}\lambda_j^{2b_j} &= \Big(\sum_{\mathbf{d}\in\mathscr{D}(\mathbf{b})}\frac{1}{d_1\cdots d_J}\sum_{\ell}R(\mathbf{d},\ell)\Big)^2 \\ &= \Big(\sum_{\mathbf{d}\in\mathscr{D}(\mathbf{b})}\frac{1}{d_1\cdots d_J}\sum_{\ell\in\mathscr{L}^*(\mathbf{d})}R(\mathbf{d},\ell)\Big)^2 \\ &\leqslant \Big(\sum_{\mathbf{d}\in\mathscr{D}(\mathbf{b}),\ell}\frac{R(\mathbf{d},\ell)^2}{d_1\cdots d_J}\Big)\Big(\sum_{\mathbf{d}\in\mathscr{D}(\mathbf{b})}\frac{|\mathscr{L}^*(\mathbf{d})|}{d_1\cdots d_J}\Big). \end{aligned} \tag{8.13}$$

Our next aim is to establish an upper bound for the first sum on the right side. We have

$$\sum_{\mathbf{d}\in\mathscr{D}(\mathbf{b}),\ell}\frac{R(\mathbf{d},\ell)^2}{d_1\cdots d_J} = \sum_{Y,Z\subset[J]}S(Y,Z), \qquad S(Y,Z) = \sum_{\substack{\mathbf{d}\in\mathscr{D}(\mathbf{b})\\ \sum_{i\in Y}d_i=\sum_{i\in Z}d_i.}}\frac{1}{d_1\cdots d_J}. \tag{8.14}$$

If $Y = Z$, then evidently $S(Y,Z) = \lambda_1^{b_1}\cdots\lambda_J^{b_J}$. If Y and Z are distinct, let $j = \max(Y\triangle Z)$ be the largest coordinate at which Y and Z differ. With all of the quantities d_i fixed except for d_j, we see that d_j is uniquely determined by the relation $\sum_{i\in Y}d_i = \sum_{i\in Z}d_i$. If we define $e(j)\in[J]$ uniquely by

$$b_1+\cdots+b_{e(j)-1}+1 \leqslant j \leqslant b_1+\cdots+b_{e(j)},$$

then $d_j \geqslant 2^{e(j)-1}$, regardless of the choice of $d_1,\dots,d_{j-1},d_{j+1},\dots,d_J$ and thus

$$S(Y,Z) \leqslant \prod_{\substack{i=1\\ i\neq j}}^{J}\Big(\sum_{d_i}\frac{1}{d_i}\Big)\cdot\frac{1}{2^{e(j)-1}} = \frac{\lambda_1^{b_1}\cdots\lambda_J^{b_J}\lambda_{e(j)}^{-1}}{2^{e(j)-1}} \ll \frac{\lambda_1^{b_1}\cdots\lambda_J^{b_J}}{2^{e(j)}}.$$

(Here, the sums over d_i are over the appropriate dyadic intervals required so that $\mathbf{d}\in\mathscr{D}(\mathbf{b})$.)

Since the number of pairs of subsets $Y,Z\subset[J]$ with $\max(Y\triangle Z) = j$ is exactly 2^{J+j-1}, we get from this and (8.14) that

$$\begin{aligned} \prod_{j=1}^{J}\lambda_j^{-b_j}\sum_{\mathbf{d}\in\mathscr{D}(\mathbf{b}),\ell}\frac{R(\mathbf{d},\ell)^2}{d_1\cdots d_J} &\ll 2^J + 2^J\sum_{j=1}^{J}2^{j-e(j)} = 2^J + 2^J\sum_{i=1}^{J}2^{-i}\sum_{j:e(j)=i}2^j \\ &\ll 2^J + 2^J\sum_{i=1}^{J}2^{b_1+\cdots+b_i-i} \\ &\ll 2^J\sum_{i=1}^{J}2^{b_1+\cdots+b_i-i}. \end{aligned}$$

Comparing with (8.13), and using again that $\lambda_i \geqslant \log 2$, completes the proof. □

Combining Lemma 8.9 and (8.12), we obtain

$$\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)| \gg \frac{(2\log 2)^J}{k}\sum_{b_1+\cdots+b_J=J}\frac{1}{b_1!\cdots b_J!\sum_{i=1}^{J}2^{b_1+\cdots+b_i-i}}.$$

Applying the Lemma 7.14 with $x_i = 2^{b_i-1}$, $1\leqslant i\leqslant J$, the multiple sum over $b_1,\dots,b_J$ equals

$$\frac{1}{J}\sum_{b_1+\cdots+b_J=J}\frac{1}{b_1!\cdots b_J!} = \frac{1}{J}\cdot\frac{J^J}{J!} \asymp \frac{\mathrm{e}^J}{J^{3/2}},$$

using the multinomial theorem and Stirling's formula. Recalling that $J = \frac{\log k}{\log 2} + O(1)$, the lower bound in Proposition 8.4 now follows.

4. The upper bound in Proposition 8.4

Recall from (8.10) the definition of $\mathscr{L}^*(\mathbf{a})$. From (8.3), the bound $H_k \geqslant \log k$ and (8.9) we obtain

$$\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)| \leqslant \frac{1}{k}\sum_r \frac{1}{r!}\sum_{a_1,\dots,a_r=1}^{k} \frac{|\mathscr{L}^*(\mathbf{a})|}{a_1\cdots a_r}. \tag{8.15}$$

Let $\tilde{a}_1, \tilde{a}_2, \dots$ be the increasing rearrangement of the sequence $\mathbf{a}$, so that $\tilde{a}_1 \leqslant \tilde{a}_2 \leqslant \cdots$. For $0 \leqslant j \leqslant r$,

$$\mathscr{L}^*(\mathbf{a}) \subset \left\{ m + \sum_{i\in I} \tilde{a}_i : 0 \leqslant m \leqslant \sum_{i=1}^{j} \tilde{a}_i,\ I \subset \{j+1,\dots,r\} \right\},$$

from which it follows immediately that

$$|\mathscr{L}^*(\mathbf{a})| \leqslant G(\widetilde{\mathbf{a}}),$$

where, for any real $t_1, \dots, t_r$, we define

$$G(\mathbf{t}) = \min_{0\leqslant j\leqslant r} 2^{r-j}\left(t_1 + \cdots + t_j + 1\right). \tag{8.16}$$

As in the previous chapter, we replace the sum in (8.15) with an integral, using that $G(\mathbf{a})$ is increasing in each coordinate.

Lemma 8.10. *For any $r \geqslant 1$, we have*

$$\frac{1}{r!}\sum_{a_1,\dots,a_r=1}^{k} \frac{|\mathscr{L}^*(\mathbf{a})|}{a_1\cdots a_r} \ll (2H_k)^r \int_{\Omega_r} \min_{0\leqslant j\leqslant r} 2^{-j}(k^{\xi_1} + \cdots + k^{\xi_j} + 1)d\boldsymbol{\xi},$$

where $\Omega_r = \{(\xi_1,\dots,\xi_r) : 0 \leqslant \xi_1 \leqslant \xi_2 \leqslant \ldots \leqslant \xi_r \leqslant 1\}$.

Proof. Motivated by the fact that

$$\frac{1}{a} = \int_{\exp(H_{a-1})}^{\exp(H_a)} \frac{dt}{t},$$

for each $\mathbf{a}$ define the product sets

$$R(\mathbf{a}) = \prod_{i=1}^{r} \left[\exp\left(H_{a_i-1}\right), \exp\left(H_{a_i}\right)\right].$$

By (8.16), we have

$$\sum_{a_1,\dots,a_r=1}^{k} \frac{|\mathscr{L}^*(\mathbf{a})|}{a_1\cdots a_r} \leqslant \sum_{a_1,\dots,a_r=1}^{k} \frac{G(\widetilde{\mathbf{a}})}{a_1\cdots a_r} = \sum_{a_1,\dots,a_r=1}^{k} G(\widetilde{\mathbf{a}}) \int_{R(\mathbf{a})} \frac{d\mathbf{t}}{t_1\cdots t_r}.$$

Consider some $\mathbf{t} \in R(\mathbf{a})$, so that $\exp\{H_{a_i-1}\} \leqslant t_i \leqslant \exp\{H_{a_i}\}$ for $1 \leqslant i \leqslant r$. Let $\tilde{t}_1 \leqslant \cdots \leqslant \tilde{t}_r$ be the increasing rearrangement of $\mathbf{t}$. From $H_m \geqslant \log(m+1)$ we have $\tilde{t}_i \geqslant \tilde{a}_i$ for all i. Hence

$$G(\widetilde{\mathbf{a}}) \leqslant \min_{0\leqslant j\leqslant r} 2^{r-j}(\tilde{t}_1 + \cdots + \tilde{t}_j + 1) = G(\tilde{\mathbf{t}}) \quad \text{for all } \mathbf{t} \in R(\mathbf{a}).$$

This yields

$$\sum_{a_1,\dots,a_r=1}^{k} G(\tilde{\mathbf{a}}) \int_{R(\mathbf{a})} \frac{d\mathbf{t}}{t_1\cdots t_r} \leqslant \sum_{a_1,\dots,a_r=1}^{k} \int_{R(\mathbf{a})} \frac{G(\tilde{\mathbf{t}})}{t_1\cdots t_r} d\mathbf{t} = \int_1^{\exp(H_k)} \cdots \int_1^{\exp(H_k)} \frac{G(\tilde{\mathbf{t}})}{t_1\cdots t_r} d\mathbf{t}.$$

The integrand on the right is symmetric in $t_1, \dots, t_r$. Making the change of variables $t_i = e^{\xi_i H_k}$ yields

$$\sum_{a_1,\dots,a_r=1}^{k} \frac{|\mathscr{L}^*(\mathbf{a})|}{a_1\cdots a_r} \leqslant (2H_k)^r r! \int_{\Omega_r} \min_{0\leqslant j\leqslant r} 2^{-j}\left(\mathrm{e}^{\xi_1 H_k} + \cdots + \mathrm{e}^{\xi_j H_k} + 1\right) d\boldsymbol{\xi}.$$

The lemma follows from the upper bound $H_k \leqslant 1 + \log k$. □

In the notation of Lemma 7.17, we have by Lemma 8.10 the bound

$$\mathbb{E}\,|\mathscr{L}(\mathbf{X}_k)| \ll \frac{1}{k}\sum_r (2H_k)^r U_r(v), \qquad v = \frac{\log k}{\log 2}. \tag{8.17}$$

Now Lemma 7.17 provides the bound

$$U_r(v) \ll \frac{1+|v-r|^2}{(r+1)!(2^{r-v}+1)},$$

uniformly for $0 \leqslant r \leqslant 2v$. Set

$$r_* = \lfloor v \rfloor.$$

In what follows, we will use the observation that $a^n/(n+1)!$ is increasing for $n \leqslant a-2$ and decreasing thereafter. If $r = r_* + m$ with $0 \leqslant m \leqslant v$, then we have

$$\begin{aligned}(2H_k)^r U_r(v) &\ll \frac{(2H_k)^r}{(r+1)!}\cdot\frac{1+m^2}{2^m}\\ &\ll \frac{(2H_k)^{r_*}}{(r_*+1)!}\cdot\left(\frac{2H_k}{r_*}\right)^m\cdot\frac{1+m^2}{2^m}\\ &\ll k^{2-\mathcal{E}}(\log k)^{-3/2}\cdot(1+m^2)(\log 2+0.1)^m,\end{aligned}$$

the $\log 2 + 0.1$ coming from the assumption that $k \geqslant 40$. Summed over m, this gives a total of $\ll k^{2-\mathcal{E}}(\log k)^{-3/2}$.

Next suppose that $r = r_* - m$, $m \in \mathbb{N}$. Then we have

$$\begin{aligned}(2H_k)^r U_r(v) &\ll \frac{(2H_k)^r}{(r+1)!}\cdot(1+m^2)\\ &\ll \frac{(2H_k)^{r_*}}{(r_*+1)!}\cdot\left(\frac{r_*}{2H_k}\right)^m\cdot(1+m^2)\\ &\ll k^{2-\mathcal{E}}(\log k)^{-3/2}\cdot\frac{1+m^2}{(2\log 2)^m}.\end{aligned}$$

Summed over m, we again get a total of $\ll k^{2-\mathcal{E}}(\log k)^{-3/2}$.

There remains the range $r > 2v$. Here, we use the trivial bound $U_r(v) \leqslant 1/r!$ and thus

$$\sum_{r>2v}(2H_k)^r U_r(v) \ll \sum_{r>2v}\frac{(2H_k)^r}{r!} \ll \mathrm{e}^{2H_k(1-Q(1/\log 2))} \ll k^{2-2\mathcal{E}}.$$

We conclude that

$$\sum_r (2H_k)^r U_v(r) \ll k^{2-\mathcal{E}}(\log k)^{-3/2}.$$

Combined with (8.17), this proves the upper bound in Proposition 8.4.

5. Exercises

Exercise 8.1. If $1 \leqslant k \leqslant n/\log n$, show that

$$i(n,k) \sim i(\infty,k) \qquad (n \to \infty).$$

CHAPTER 9

Sets of permutations with equal sized divisors

1. Equal sized divisors of several permutations

Let $\sigma_1, \dots, \sigma_r$ be random permutations in $\mathcal{S}_n$, chosen independently. By Theorem 8.1, the probability that they all have a divisor of size k is

$$i(n,k)^r \asymp_r \frac{1}{(k^{\mathcal{E}}(1+\log k))^r} \qquad (1 \leqslant k \leqslant n/2).$$

For $\sigma \in \mathcal{S}_n$ define

$$D(\sigma) = \{|\beta| : \beta|\sigma\}, \quad \text{the set of sizes of divisors of } \sigma.$$

We note that $\{0, n\} \subseteq D(\sigma)$ always. We wish to also bound the probability that $D(\sigma_1) \cap \cdots \cap D(\sigma_r)$ contains an element in $[k, n/2]$. Crudely, from the above and the fact that $12\mathcal{E} > 1$ this is at most

$$\sum_{k \leqslant m \leqslant n/2} i(n,k)^r \ll_r \frac{k^{1-r\mathcal{E}}}{(1+\log k)^{(3/2)r}} \qquad (r \geqslant 12). \tag{9.1}$$

This estimate is wasteful, since the events $m_1 \in D(\sigma_1) \cap \cdots \cap D(\sigma_r)$ and $m_2 \in D(\sigma_1) \cap \cdots \cap D(\sigma_r)$ are not independent. In fact, if $r \geqslant 4$ then it is rare for $D(\sigma_1) \cap \cdots \cap D(\sigma_r)$ to have a large element, but this is not true for $r = 3$. This ultimately depends on the inequalities

$$3(1 - \log 2) < 1 < 4(1 - \log 2).$$

Theorem 9.1 (Pemantle-Peres-Rivin [57]; 2016). *Let $\sigma_1, \dots, \sigma_4$ be random permutations in $\mathcal{S}_n$, chosen independently. There is a real number $\alpha > 0$ so that*

$$\mathbb{P}\big(D(\sigma_1) \cap \cdots \cap D(\sigma_4) = \{0, n\}\big) \geqslant \alpha.$$

The authors if **[15]** gave a proof of 9.1 which is much simpler than the original proof in **[57]**, and we given an even simpler proof below.

Theorem 9.2 (Eberhard-Ford-Green [15]; 2017). *With probability $\to 1$ as $n \to \infty$, we have*

$$|D(\sigma_1) \cap D(\sigma_2) \cap D(\sigma_3)| \to \infty$$

as $n \to \infty$.

Lemma 9.3. *(a) Suppose that h, m are integers with $h < m < n - h$. Then*

$$\mathbb{P}_\sigma\Big(m \in D(\sigma), C_{[h]}(\sigma) = 0\Big) \ll h^{-2}.$$

(b) If $1 \leqslant \lambda \leqslant 2$, $1 \leqslant h \leqslant k \leqslant n/2$ and $k < m < n - k$ then

$$\mathbb{P}_\sigma\Big(m \in D(\sigma), C_{[h]}(\sigma) = 0, C_{(h,k]}(\sigma) \leqslant \lambda \log(k/h)\Big) \ll h^{-2}(k/h)^{-2Q(\lambda/2)}.$$

Proof. For (a), factor each such σ as $\sigma = \sigma_1\sigma_2$ where $|\sigma_1| = m$ and $|\sigma_2| = n - m$. By By Theorem 1.9, the number of such σ is

$$\ll \binom{n}{m} \cdot \frac{m!}{h} \cdot \frac{(n-m)!}{h} \ll \frac{n!}{h^2},$$

For (b), WLOG $k \geqslant 10$. Fix $\ell \leqslant \lambda \log(k/h)$ and consider permutations σ with $C_{[h]}(\sigma) = 0$, $C_{(h,k]}(\sigma) = \ell$ and such that $m \in D(\sigma)$. Write $\sigma = \sigma_1\sigma_2$ with $|\sigma_1| = m$, $|\sigma_2| = n - m$. Then $C_{(h,k]}(\sigma_1) = \ell_1$ and $C_{(h,k]}(\sigma_2) = \ell_2$, where $\ell_1 + \ell_2 = \ell$. By Theorem 1.9, the number of such σ, for a given choice of ℓ_1, ℓ_2, is

$$\ll \binom{n}{m} \frac{(H_k - H_h)^{\ell_1}}{h \cdot (k/h)\ell_1!} m! \cdot \frac{(H_k - H_h)^{\ell_2}}{h \cdot (k/h)\ell_2!} (n-m)! = n! \frac{(1 + \log(k/h))^{\ell}}{k^2 \ell_1! \ell_2!}.$$

Summing over $\ell_1 + \ell_2 = \ell$, we see that

$$\mathbb{P}_\sigma\big(m \in D(\sigma), C_{[h]}(\sigma) = 0, C_{(h,k]}(\sigma) = \ell\big) \ll \frac{(2\log(k/h) + 2)^{\ell}}{k^2 \ell!}.$$

We sum over $\ell \leqslant \lambda \log(k/h)$, using the bound for Poisson tails (Prop. 0.3) and noting that $(2\log(k/h)+2)^{\ell} \ll (2\log(k/h))^{\ell}$. We get

$$\mathbb{P}_\sigma\left(m \in D(\sigma), C_{[k]}(\sigma) \leqslant (1+\varepsilon)\log k\right) \ll h^{-2} e^{-(2\log(k/h))Q(\lambda/2)} = h^{-2}(k/h)^{-2Q(\lambda/2)}. \qquad \square$$

Lemma 9.4. *Let $1 \leqslant h \leqslant n/10$. There is a real number $c > 0$ so that with probability $\ll h^{-4-c}$, $C_{[h]}(\sigma_i) = 0$ for $1 \leqslant i \leqslant 4$ and $D(\sigma_1) \cap \cdots \cap D(\sigma_4)$ contains an element other than 0 and n.*

Proof. Fix $0 < \varepsilon \leqslant \frac{1}{2}$, to be determined later. WLOG $h \geqslant 10$. Let $k = 2^r h \leqslant n/2$ for a non-negative integer r. Let $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ be random permutations of $\mathcal{S}_n$.

Let F_k be the event that $C_{[h]}(\sigma_i) = 0$ $(1 \leqslant i \leqslant 4)$, and for some i, $C_{(h,k]}(\sigma_i) > (1+\varepsilon)\log(k/h)$. Let G_k be the event that $C_{[h]}(\sigma_i) = 0$ $(1 \leqslant i \leqslant 4)$, and that for some $m \in (k, 2k] \cap (h, n/2]$, we have $m \in D(\sigma_1) \cap \cdots \cap D(\sigma_4)$. Let H_k be the event that G_k holds and that $C_{(h,k]}(\sigma_i) \leqslant (1+\varepsilon)\log(k/h)$ for each i. Evidently, the probability in the lemma is at most

$$\sum_{h \leqslant k \leqslant n/2} \mathbb{P}\, G_k \leqslant \sum_{h \leqslant k \leqslant h^3} \mathbb{P}\, G_k + \sum_{h^3 < k \leqslant n/2} (\mathbb{P}\, F_k + \mathbb{P}\, H_k). \tag{9.2}$$

By Theorem 1.11, if $k > h^3$ then

$$\mathbb{P}\, F_k \ll \frac{1}{h^4 (k/h)^{Q(1+\varepsilon)}}.$$

By Lemma 9.3 (a), we have

$$\mathbb{P}\, G_k \ll \frac{k}{h^8}.$$

Now suppose that $h^3 < k \leqslant n/2$ and consider the event H_k. By Lemma 9.3 (b), we get that

$$\mathbb{P}\, H_k \ll \frac{k}{h^8 (k/h)^{8Q(\frac{1+\varepsilon}{2})}}.$$

Choose ε so $1 - 8Q(\frac{1+\varepsilon}{2}) = -Q(1+\varepsilon)$; the solution is $\varepsilon = 0.08895343\cdots$. Inserting our bounds for F_k, G_k and H_k into (9.2), we see that the probability in the lemma is

$$\ll \frac{h^3}{h^8} + \frac{1}{h^{4+2Q(1+\varepsilon)}} + \frac{1}{h^{5+16Q(\frac{1+\varepsilon}{2})}} \ll \frac{1}{h^{4+2Q(1+\varepsilon)}}. \qquad \square$$

Proof of Theorem 9.1. Let h be a sufficiently large constant and $n_0 = 3h$. If $n \leqslant n_0$, the probability in question is at least the probability that σ_1 is an n-cycle, which is $1/n \geqslant 1/n_0$. Now suppose that $n > n_0$, in particular $n > 3h$. By (3.5) and Lemma 9.4,

$$\mathbb{P}\Big(C_{[h]}(\sigma_i) = 0\ (1 \leqslant i \leqslant 4); D(\sigma_1) \cap \cdots \cap D(\sigma_4) = \{0, n\}\Big) \geqslant \frac{1}{(2h+1)^4} - O\left(\frac{1}{h^{4+c}}\right).$$

Taking h large enough proves the theorem. $\square$

2. Application: Invariable generation of $\mathcal{S}_n$

By Dixon's theorem [**12**], two random elements σ_1, σ_2 of $\mathcal{S}_n$ generate at least the whole alternating group $\mathcal{A}_n$ with probability tending to 1 as $n \to \infty$. It is less clear how large the group generated by σ_1', σ_2' must be when σ_1' and σ_2' are allowed to be arbitrary conjugates of σ_1 and σ_2. Following Dixon [**13**] we say that a list $\sigma_1, \dots, \sigma_r \in \mathcal{S}_n$ has a property P *invariably* if $\sigma_1', \dots, \sigma_r'$ has property P whenever σ_i' is conjugate to σ_i for every i. How many random elements of $\mathcal{S}_n$ must we take before we expect them to invariably generate $\mathcal{S}_n$?

This problem is connected with computational Galois theory. Given a polynomial $f \in \mathbb{Z}[x]$ of degree n with no repeated factors, information about the Galois group can be gained by reducing f modulo various primes p and factorizing the reduced polynomial f_p over $\mathbb{Z}/p\mathbb{Z}$. By classical Galois theory, if f_p has irreducible factors of degrees $n_1, \dots, n_r$ then the Galois group G of f over $\mathbb{Q}$ has an element with cycle lengths $n_1, \dots, n_r$. Moreover by Frobenius's density theorem, if $G = \mathcal{S}_n$ then the frequency with which a given cycle type arises is equal to the proportion of elements in $\mathcal{S}_n$ with that cycle type. Thus if we suspect that $G = \mathcal{S}_n$ then the number of times we expect to have to iterate this procedure before proving that $G = \mathcal{S}_n$ is controlled by the expected number of random elements required to invariably generate $\mathcal{S}_n$.

Łuczak and Pyber [**51**] were the first to prove the existence of a constant C such that C random permutations $\sigma_1, \dots, \sigma_C \in \mathcal{S}_n$ invariably generate $\mathcal{S}_n$ with probability bounded away from zero. Their method does not directly yield a reasonable value of C, but recently Pemantle, Peres, and Rivin [**57**] proved that we may take $C = 4$. The key to their proof is Theorem 9.1.

Theorem 9.5 (Pemantle-Peres-Rivin [57]; 2016). *For some $\alpha > 0$, the probability that random $\sigma_1, \dots, \sigma_4$ invariably generate $\mathcal{S}_n$ is at least α, for any n.*

Theorem 9.6 (Eberhard-Ford-Green [15]; 2017). *With probability $\to 1$ as $n \to \infty$, random $\sigma_1, \sigma_2, \sigma_3$* do not *invarably generate $\mathcal{S}_n$.*

The connection between common size fixed sets of $\sigma_1, \dots, \sigma_r$ and invariable generation is clear: if $m \in D(\sigma_1) \cap \dots \cap D(\sigma_r)$, $0 < m < n$, then there are conjugates $\sigma_1', \dots, \sigma_r'$ each mapping $\{1, 2, \cdots, m\}$ to itself (a *fixed set*). In this case, it is clear that $\sigma_1', \dots, \sigma_r'$ do not generate $\mathcal{S}_n$.

What if $D(\sigma_1) \cap \dots \cap D(\sigma_r) = \{0, n\}$? It is simple to see that $\sigma_1', \dots, \sigma_r'$ generate some *transitive* subgroup of $\mathcal{S}_n$; a subgroup H of $\mathcal{S}_n$ is transitive if for every pair $i, j \in [n]$ there is some element of H which maps i to j. Examples of transitive subgroups include $\mathcal{S}_n$, $\mathcal{A}_n$ as well as *imprimitive transitive subgroups* such as this example when $n = 2k$ is even: Let $I_1 = \{1, 2, \dots, k\}$ and $I_2 = \{k+1, \dots, 2k\}$ amd let

$$G = \{\sigma : \text{ either } \sigma(I_1) = I_1, \sigma(I_2) = I_2 \text{ or } \sigma(I_1) = I_2, \sigma(I_2) = I_1\}.$$

Lemma 9.7. *Suppose that $D(\sigma_1) \cap \dots \cap D(\sigma_r) = \{0, n\}$. Then $\sigma_1, \dots, \sigma_r$ generate a transitive subgroup of $\mathcal{S}_n$.*

Proof. Let G be the group generated by $\sigma_1, \dots, \sigma_r$. Define a relation $\sim$ on $[n]$ by $a \sim b$ if there is a $\sigma \in G$ with $\sigma(a) = b$. This is clearly an equivalence relation, and thus partitions $[n]$. If G is not a transitive subgroup, then there is a non-trivial equivalence class I, $\emptyset \neq I \neq [n]$, and clearly I is a fixed set of each σ_j. □

From Lemma 9.7, Theorem 9.6 now follows from Theorem 9.2. Also, from Theorem 9.1, it follows that for some $\alpha' > 0$, with probability at least α' four random permutations $\sigma_1, \dots, \sigma_4$ generate a transitive subgroup of $\mathcal{S}_n$. It is known (a Theorem of Łuczak-Pyber [**51**], which also uses the theory of permutations) that the probability that a random $\sigma \in \mathcal{S}_n$ lies in a transitive subgroup of S_n other than $\mathcal{S}_n$ or $\mathcal{A}_n$ is $o(1)$ as $n \to \infty$. We will not prove this here. For the latest estimates, see [**16**]. Note that if σ does not lie in a transitive subgroup, then neither do any of its conjugates $\tilde{\sigma}$, since σ and $\tilde{\sigma}$ are indistinguishable in a group-theoretic sense. It follows then that for some $\alpha'' > 0$, with probability at least α'' four random permutations $\sigma_1, \dots, \sigma_4$ generate either $\mathcal{A}_n$ or $\mathcal{S}_n$.

To distinguish $\mathcal{A}_n$ from $\mathcal{S}_n$, it suffices to choose σ_1 to be an *odd* permutation (a permutation which is the product of an odd number of transpositions (ab)) in order to conclude that $\sigma_1', \dots, \sigma_4'$ generates $\mathcal{S}_n$.

Recalling the proof of Theorem 9.1 from the previous section, it suffices to show that if σ is a random odd permutation, then $\mathbb{P}_\sigma(C_{[h]}(\sigma) = 0) \gg 1/h$, i.e., an analog of the lower bound in (3.5).

Lemma 9.8. *Let n be sufficiently large and $1 \leqslant h \leqslant n^{1/3}$. Then*

$$\mathbb{P}(C_{[h]}(\sigma) = 0, \sigma \text{ odd}) \gg \frac{1}{h}.$$

We first establish a general result about random odd permutations.

Lemma 9.9 (Random odd permutations). *Let $\tau \in \mathcal{S}_n$ be a random **odd** permutation, and $1 \leqslant k \leqslant n$. Then $d_{TV}(C_1(\tau), \dots, C_k(\tau), \mathcal{Z}_k) \ll k/n$, where*

$$\mathcal{Z}_k = (Z_1, \dots, Z_k), \qquad Z_i \stackrel{d}{=} \text{Pois}(1/i) \ \ (1 \leqslant i \leqslant k), \quad Z_i \text{ independent.}$$

Proof. WLOG $k \leqslant n/10$. Choose $\sigma \in \mathcal{S}_n$ uniformly at random, and define ρ by putting $\rho = 1$ if σ is odd and $\rho = (12)$ if σ is even. Then $\tau = \sigma\rho$ is uniformly distributed over odd permutations. We will show that with high probability,

$$(C_1(\sigma), \dots, C_k(\sigma)) = (C_1(\sigma\rho), \dots, C_k(\sigma\rho)). \tag{9.3}$$

In particular, (9.3) holds provided that neither of the following holds:

(i) 1 and 2 are in different cycles, each of length $\leqslant k$; or
(ii) 1 and 2 are in the same cycle of σ and there are fewer than k elements in between them (in either direction).

To see this, observe that for any strings of numbers A, B (including the empty strings), if σ has cycles $(1A)$ and $(2B)$ and $\rho = (12)$ then $\sigma\rho$ has a cycle $(1A2B)$. Also, if σ has a cycle $(1A2B)$ and $\rho = (12)$, then $\sigma\rho$ has cycles $(1A)$ and $(2B)$.

We will show that the probability that (9.3) fails is $O(\frac{k}{n})$. Then, by the Poisson distribution of Small Cycles (Theorem 4.3), $d_{TV}(C_1(\sigma), \dots, C_k(\sigma), \mathcal{Z}_k) \ll \mathrm{e}^{-n/5k} \ll k/n$ and the lemma follows.

Consider (i). Given positive $a, b \leqslant k$, the probability that $(1A)$ and $(2B)$ are cycles in σ with $|A| = a, |B| = b$, equals

$$\frac{1}{n!} \cdot \frac{(n-2)!}{a!b!(n-a-b-2)!} a!b!(n-a-b-2)! = \frac{1}{n(n-1)}.$$

Thus, the probability that (i) holds is $O(k^2/n^2)$.

Now consider the probability that 1 and 2 are both contained in the same cycle of σ and are close together. Let this cycle be $(1A2B)$, where $|A| = a$ and $|B| = b$ with $\min(a, b) \leqslant k-1$. The probability of having such a cycle with a, b fixed equals $\frac{1}{n(n-1)}$ by the same logic. Hence, the probability that (ii) holds is $O(k/n)$. □

Proof of Lemma 9.8. By Lemma 9.3,

$$\begin{aligned}
\mathbb{P}_\sigma(C_{[h]}(\sigma) = 0, \sigma \text{ odd}) &= \frac{1}{2}\mathbb{P}_{\tau \in \mathcal{S}_n \setminus \mathcal{A}_n}(C_{[h]}(\tau) = 0) \\
&= \frac{1}{2}\mathbb{P}(Z_1 = \cdots = Z_h = 0) + O(h/n) \\
&= (1/2)\mathrm{e}^{-H_h} + O(1/n^{2/3}) \gg 1/h
\end{aligned}$$

if n is large enough. □

3. Application: Irreducibility of polynomials over $\mathbb{Q}$

A famous conjecture of Odlyzko and Poonen states that a random polynomial

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 1, \tag{9.4}$$

where each $a_i \in \{0,1\}$ is randomly chosen, is irreducible with probability $\to 1$ as $n \to \infty$. Variations on this problem put the coefficients a_j in other finite sets, e.g. $\{-1,1\}$. Here are some highlights of what's known.

- Almost all polynomials of shape (9.4) with $a_n \in \{0,1\}$ have no irreducible factor $\leqslant cn/\log n$, for some $c > 0$ (Konyagin [**49**], 1999). This was improved in Bary-Soroker, Koukoulopoulos and Kozma [**4**] in 2022, where the conclusion is that with probability $\to 1$ as $n \to \infty$, the polynomial has no irreducible factor $\leqslant cn$, for some $c > 0$.
- Almost all polynomials of shape (9.4) with $a_n \in \{1, 2, \dots, 210\}$ are irreducible (Bary-Soroker and Kozma [**5**], 2020). The methods were refined in work of Bary-Soroker, Koukoulopoulos and Kozma [**4**] in 2022, where they show the same conclusion with $a_n \in \{1, 2, \dots, 35\}$ and other finite sets.
- Assuming the GRH for Dedekind zeta-functions, almost all polynomials of shape (9.4) with $a_n \in \{0,1\}$ are irreducible (Bruillard, Varju [**7**], 2019).

Here we discuss the proof of Bary-Soroker and Kozma's "210" theorem, because of its connection to random permutations. The authors consider polynomials

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with each $a_i \in \{1, 2, \dots, 210\}$ chosen uniformly at random. We sketch the proof of

Theorem 9.10. *Let $\xi(n) \to \infty$ as $n \to \infty$. With probability $\to 1$ as $n \to \infty$, $f(x)$ has no factor of degree in $[\xi(n), n-1]$.*

The key idea is that $210 = 2 \cdot 3 \cdot 5 \cdot 7$, and there is a natural bijection between such f and the vector (f_2, f_3, f_5, f_7) of its reduction modulo $2, 3, 5$ and 7. Moreover, each f_p is a random polynomial over $\mathbb{F}_p$ and (this is crucial!) the Chinese Remainder Theorem implies that the random polynomials f_2, f_3, f_5, f_7 are *independent*. Also, if f has a factor or degree k, then so do f_2, f_3, f_5, f_7 (these need not be irreducible!).

The second key idea is the well-known fact that the distribution of the sizes of the irreducible factors of a random polynomial of degree n over $\mathbb{F}_p$ is roughly the same as the distribution of the sizes of cycles of a random permutation $\sigma \in \mathcal{S}_n$. This is relatively easy to establish since we have exact formulas in both cases.

Lemma 9.11. *Let f be a random monic polynomial of degree n over $\mathbb{F}_q$, where q is a prime power. Let $I_f(r)$ be the number of irreducible factors of f of degree r. Then, if $m_1 + 2m_2 + \cdots + nm_n = n$,*

$$\mathbb{P}\big(I_f(1) = m_1, \dots, I_f(n) = m_n\big) = \prod_{i=1}^{n} \alpha(i, m_i),$$

where

$$\alpha(i,1) = \frac{1}{i}\sum_{j|i} \mu(i/j) q^{j-i}, \qquad \alpha(i,m) = \frac{(\alpha(i,1) + q^{-i}(m-1))(\alpha(i,1) + q^{-i}(m-2)) \cdots \alpha(i,1)}{m!}$$

Proof. The main task is to show that $\alpha(i,m)q^{im}$ is the number of m-tuples (duplicates allowed) of monic, irreducible polynomials of degree i over $\mathbb{F}_q$. Once this is established, we follow the idea of Lemma 1.1, getting

$$\mathbb{E}\binom{I_f(1)}{m_1} \cdots \binom{I_f(n)}{m_n} = \prod_{i=1}^{n} \alpha(i, m_i)$$

and then noticing that if $m_1 + 2m_2 + \cdots + nm_n = n$, the product of binomials on the left equals 1 if and only if $I_f(r) = m_r$ for all r. We begin with the interpretation of $\alpha(i,1)$. Let $\pi_q(d)$ be the number of irreducible

polynomials of degree d (all polynomials will be monic and over $\mathbb{F}_q$). Let I denote a generic irreducible polynomial of any degree. Then

$$\begin{aligned} nq^n &= \sum_{\deg F = n} \sum_{I^v | F} \deg(I) \\ &= \sum_{v \cdot \deg I \leqslant n} \deg(I) \cdot |\{F : \deg(F) = n, I^v | F\}| \\ &= \sum_{v \cdot \deg I \leqslant n} \deg(I) \cdot q^{n - v \cdot \deg(I)} \\ &= q^n \sum_{m=1}^{n} q^{-m} \sum_{d|m} d\pi_q(d). \end{aligned}$$

Divide by q^n, then apply this at n and $n-1$ and take the difference. This gives

$$q^n = \sum_{d|n} d\pi_q(d).$$

By Möbius inversion,

$$n\pi_q(n) = \sum_{d|n} \mu(d) q^{n/d} = \sum_{d|n} \mu(n/d) q^d,$$

and therefore

$$\alpha(d, 1) = q^{-d} \pi_q(d),$$

as desired.

Finally, the number of ways one can choose m irreducible polynomials of degree d is

$$\binom{\pi_q(d) + m - 1}{m} = q^{dm} \alpha(d, m).$$

□

For large i we have

$$\alpha(i, 1) = \frac{1}{i} + O(q^{-i/2}) \approx \frac{1}{i}$$

and

$$\alpha(i, m) \approx \frac{\alpha(i, m)^i}{m!} \approx \frac{(1/i)^m}{m!}.$$

Thus, the distribution of $(I_f(1), \ldots, I_f(k))$ is about the same as the distribution of $(C_1(\sigma), \ldots, C_k(\sigma))$. For precise statements, see **[1]**.

Heuristically, the probability that $f_2, \ldots, f_7$ all have a factor of the *same* degree in $[\xi(n), n-1]$ should be approximately the same as the probability that four random permutations each have a divisor of size k for some $k \in [\xi(n), n-1]$. This latter probability is $\to 0$ as $n \to \infty$, essentially the proof of Theorem 9.4. See Exercise 9.1 below.

4. Exercises

Exercise 9.1. Show that for some constant $c > 0$, the probability that $D(\sigma_1) \cap \cdots \cap D(\sigma_4)$ contains an element in $[K, n-K]$ is $O(K^{-c})$.

Bibliography

[1] Richard Arratia, A. D. Barbour, and Simon Tavaré. On random polynomials over finite fields. *Math. Proc. Cambridge Philos. Soc.*, 114(2):347–368, 1993.

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

[3] Robert B. Ash. *Information theory*. Dover Publications, Inc., New York, 1990. Corrected reprint of the 1965 original.

[4] Lior Bary-Soroker, Dimitrios Koukoulopoulos, and Gady Kozma. Irreducibility of random polynomials: general measures.

[5] Lior Bary-Soroker and Gady Kozma. Irreducible polynomials of bounded height. *Duke Math. J.*, 169(4):579–598, 2020.

[6] A. S. Besicovitch. On the density of certain sequences of integers. *Math. Ann.*, 110:336–341, 1934.

[7] Emmanuel Breuillard and Péter P. Varjú. Irreducibility of random polynomials of large degree. *Acta Math.*, 223(2):195–249, 2019.

[8] J. Britnell and M. Wildon. Computing derangement probabilities of the symmetric group acting on k-sets. `http://arxiv.org/abs/1511.04106`.

[9] C. Cobeli, K. Ford, and A. Zaharescu. The jumping champions of the Farey series. *Acta Arith.*, 110(3):259–274, 2003.

[10] Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[11] Persi Diaconis, J. Fulman, and R. Guralnick. On fixed points of permutations. *J. Algebraic Combin.*, 28(1):189–218, 2008.

[12] John D. Dixon. The probability of generating the symmetric group. *Math. Z.*, 110:199–205, 1969.

[13] John D. Dixon. Random sets which invariably generate the symmetric group. *Discrete Math.*, 105(1-3):25–39, 1992.

[14] Sean Eberhard, Kevin Ford, and Ben Green. Permutations fixing a k-set. *Int. Math. Res. Not. IMRN*, (21):6713–6731, 2016.

[15] Sean Eberhard, Kevin Ford, and Ben Green. Invariable generation of the symmetric group. *Duke Math. J.*, 166(8):1573–1590, 2017.

[16] Sean Eberhard, Kevin Ford, and Dimitris Koukoulopoulos. Permutations contained in transitive subgroups. *Discrete Anal.*, pages Paper No. 12, 34, 2016.

[17] Paul Erdős. On some applications of probability to analysis and number theory. *J. London Math. Soc.*, 39:692–696, 1964.

[18] Paul Erdős. On abundant-like numbers. *Canad. Math. Bull.*, 17(4):599–602, 1974.

[19] Paul Erdős and Richard R. Hall. The propinquity of divisors. *Bull. London Math. Soc.*, 11(3):304–307, 1979.

[20] Paul Erdős and Jean-Louis Nicolas. Répartition des nombres superabondants. *Bull. Soc. Math. France*, 103(1):65–90, 1975.

[21] Paul Erdős and Jean-Louis Nicolas. Méthodes probabilistes et combinatoires en théorie des nombres. *Bull. Sci. Math. (2)*, 100(4):301–320, 1976.

[22] P. Erdős. Note on the sequences of integers no one of which is divisible by any other. *J. London Math. Soc.*, 10:126–128, 1935.

[23] Paul Erdős. On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ-function. *Quart. J. Math. Oxford*, pages 205–213, 1935.

[24] Paul Erdös. On the density of some sequences of integers. *Bull. Amer. Math. Soc.*, 54:685–692, 1948.

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

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

[27] Paul Erdős and Richard R. Hall. On the Möbius function. *J. Reine Angew. Math.*, 315:121–126, 1980.

[28] Paul Erdős and Marc Kac. The Gaussian law of errors in the theory of additive number theoretic functions. *Amer. J. Math.*, 62:738–742, 1940.

[29] Kevin Ford. The distribution of integers with a divisor in a given interval. *Ann. of Math. (2)*, 168(2):367–433, 2008.

[30] Kevin Ford. Integers with a divisor in $(y, 2y]$. In *Anatomy of integers*, volume 46 of *CRM Proc. Lecture Notes*, pages 65–80. Amer. Math. Soc., Providence, RI, 2008.

[31] Kevin Ford. Sharp probability estimates for generalized Smirnov statistics. *Monatsh. Math.*, 153(3):205–216, 2008.

[32] Kevin Ford. Rough integers with a divisor in a given interval. *J. Aust. Math. Soc.*, 111(1):17–36, 2021.

[33] Kevin Ford. Cycle type of random permutations: A toolkit. *Discrete Analysis*, 2022.

[34] Kevin Ford. Joint poisson distribution of prime factors in sets. *Math. Proc. Cambridge Phil. Soc*, 2022.

[35] Kevin Ford, Ben Green, Sergei Konyagin, James Maynard, and Terence Tao. Long gaps between primes. *J. Amer. Math. Soc.*, 31(1):65–105, 2018.

[36] Kevin Ford, Ben Green, and Dimitrios Koukoulopoulos. Equal sums in random sets and the concentration of divisors. 2019.

[37] János Galambos. The sequences of prime divisors of integers. *Acta Arith.*, 31(3):213–218, 1976.
[38] 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.
[39] V. Gontcharoff. Du domaine de l'analyse combinatoire. *Bull. Acad. Sci. URSS Sér. Math. [Izvestia Akad. Nauk SSSR]*, 8:3–48, 1944.
[40] Andrew Granville. Cycle lengths in a permutation are typically Poisson. *Electron. J. Combin.*, 13(1):Research Paper 107, 23, 2006.
[41] Heini Halberstam and Klaus F. Roth. *Sequences*. Oxford University Clarendon Press, 1966.
[42] Richard R. Hall and Gérald Tenenbaum. On the average and normal orders of Hooley's Δ-function. *J. London Math. Soc. (2)*, 25(3):392–406, 1982.
[43] Richard R. Hall and Gérald Tenenbaum. The average orders of Hooley's Δ_r-functions. *Mathematika*, 31(1):98–109, 1984.
[44] Richard R. Hall and Gérald Tenenbaum. The average orders of Hooley's Δ_r-functions. II. *Compositio Math.*, 60(2):163–186, 1986.
[45] Richard R. Hall and Gérald Tenenbaum. *Divisors*, volume 90 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1988.
[46] G. H. Hardy and S. Ramanujan. The normal number of prime factors of a number n [Quart. J. Math. **48** (1917), 76–92]. In *Collected papers of Srinivasa Ramanujan*, pages 262–275. AMS Chelsea Publ., Providence, RI, 2000.
[47] Adolf Hildebrand and Gérald Tenenbaum. Integers without large prime factors. *J. Théor. Nombres Bordeaux*, 5(2):411–484, 1993.
[48] Christopher Hooley. On a new technique and its applications to the theory of numbers. *Proc. London Math. Soc. (3)*, 38(1):115–151, 1979.
[49] S. V. Konyagin. On the number of irreducible polynomials with $0, 1$ coefficients. *Acta Arith.*, 88(4):333–350, 1999.
[50] Dimitrios Koukoulopoulos. Localized factorizations of integers. *Proc. London Math. Soc.*, 101:392–426, 2010.
[51] T. Łuczak and L. Pyber. On random generation of the symmetric group. *Combin. Probab. Comput.*, 2(4):505–512, 1993.
[52] Helmut Maier and Gérald Tenenbaum. On the set of divisors of an integer. *Invent. Math.*, 76(1):121–128, 1984.
[53] Helmut Maier and Gérald Tenenbaum. On the normal concentration of divisors. *J. London Math. Soc. (2)*, 31(3):393–400, 1985.
[54] Helmut Maier and Gérald Tenenbaum. On the normal concentration of divisors. II. *Math. Proc. Cambridge Philos. Soc.*, 147(3):513–540, 2009.
[55] Eugenijus Manstavičius and Robertas Petuchovas. Local probabilities for random permutations without long cycles. *Electron. J. Combin.*, 23(1):Paper 1.58, 25, 2016.
[56] Karl K. Norton. On the number of restricted prime factors of an integer. I. *Illinois J. Math.*, 20(4):681–705, 1976.
[57] Robin Pemantle, Yuval Peres, and Igor Rivin. Four random permutations conjugated by an adversary generate $\mathcal{S}_n$ with high probability. *Random Structures Algorithms*, 49(3):409–428, 2016.
[58] Robertas Petuchovas. *ASYMPTOTIC ANALYSIS OF THE CYCLIC STRUCTURE OF PERMUTATIONS*. PhD thesis, Vilnius University, 2016. `arXiv: 1611.02934`.
[59] Robert Rankin. The difference between consecutive prime numbers. *J. London Math. Soc.*, 13:242–247, 1938.
[60] J. Riordan. *Combinatorial identities*. John Wiley & Sons Inc., New York, 1968.
[61] G. Tenenbaum. Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné. *Compositio Math.*, 51(2):243–263, 1984.
[62] Gérald Tenenbaum. Sur la concentration moyenne des diviseurs. *Comment. Math. Helv.*, 60(3):411–428, 1985.
[63] Gérald Tenenbaum. Fonctions Δ de Hooley et applications. In *Séminaire de théorie des nombres, Paris 1984–85*, volume 63 of *Progr. Math.*, pages 225–239. Birkhäuser Boston, Boston, MA, 1986.
[64] 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.
[65] Gérald Tenenbaum. Some of Erdős' unconventional problems in number theory, thirty-four years later. In *Erdös centennial*, volume 25 of *Bolyai Soc. Math. Stud.*, pages 651–681. János Bolyai Math. Soc., Budapest, 2013.
[66] 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.
[67] Christian Tudesq. Majoration de la loi locale de certaines fonctions additives. *Arch. Math. (Basel)*, 67(6):465–472, 1996.
[68] Paul Turán. On a Theorem of Hardy and Ramanujan. *J. London Math. Soc.*, 9(4):274–276, 1934.
[69] G. A. Watterson. The sampling theory of selectively neutral alleles. *Advances in Appl. Probability*, 6:463–488, 1974.
[70] E. Westzynthius. Über die verteilung der zahlen, die zu den n ersten primzahlen teilerfremd sind. *Commentationes Physico–Mathematicae, Societas Scientarium Fennica, Helsingfors*, 5(25):1–37, 1931.