# Analytic Number Theory

## Exploring the Anatomy of Integers

**Jean-Marie De Koninck**
**Florian Luca**

**Graduate Studies in Mathematics**
**Volume 134**

**American Mathematical Society**

# Analytic Number Theory

## Exploring the Anatomy of Integers

Jean-Marie De Koninck
Florian Luca

Graduate Studies
in Mathematics
Volume 134

American Mathematical Society
Providence, Rhode Island

2010 *Mathematics Subject Classification.* Primary 11A05, 11A41, 11B05, 11K65, 11N05, 11N13, 11N35, 11N37, 11N60, 11B39.

---

For additional information and updates on this book, visit
**www.ams.org/bookpages/gsm-134**

---

**Library of Congress Cataloging-in-Publication Data**

Koninck, J.-M. de, 1948–
Analytic number theory: exploring the anatomy of integers / Jean-Marie De Koninck, Florian Luca.
p. cm. – (Graduate studies in mathematics ; v. 134)
Includes bibliographical references and index.
ISBN 978-0-8218-7577-3 (alk. paper)
1. Number theory. 2. Euclidean algorithm. 3. Integrals. I. Luca, Florian. II. Title.

QA241.K6855 2012
512.7′4–dc23 2011051431

---



10 9 8 7 6 5 4 3 2 1 17 16 15 14 13 12

# Contents

# Preface

Number theory is one of the most fascinating topics in mathematics, and there are various reasons for this. Here are a few:

- Several number theory problems can be formulated in simple terms with very little or no background required to understand their statements.
- It has a rich history that goes back thousands of years when mankind was learning to count (even before learning to write!).
- Some of the most famous minds of mathematics (including Pascal, Euler, Gauss, and Riemann, to name only a few) have brought their contributions to the development of number theory.
- Like many other areas of science, but perhaps more so with this one, its development suffers from an apparent paradox: giant leaps have been made over time, while some problems remain as of today completely impenetrable, with little or no progress being made.

All this explains in part why so many scientists and so many amateurs have worked on famous problems and conjectures in number theory. The long quest for a proof of Fermat's Last Theorem is only one example.

And what about "analytic number theory"? The use of analysis (real or complex) to study number theory problems has brought light and elegance to this field, in particular to the problem of the distribution of prime numbers. Through the centuries, a large variety of tools has been developed to grasp a better understanding of this particular problem. But the year 1896 saw a turning point in the history of number theory. Indeed, that was the year when two mathematicians, Jacques Hadamard and Charles Jean de la Vallée Poussin, one French, the other Belgian, independently used complex analysis

to prove what we now call the Prime Number Theorem, namely the fact that "$\pi(x)$ is asymptotic to $x/\log x$" as $x$ tends to infinity, where $\pi(x)$ stands for the number of prime numbers not exceeding $x$. This event marked the birth of analytic number theory.

At first one might wonder how analysis can be of any help in solving problems from number theory, which are after all related to the study of positive integers. Indeed, while integers "live" in a discrete world, analysis "lives" in a continuous one. This duality goes back to Euler, who had observed that there was a connection between an infinite product running over the set of all prime numbers and an infinite series which converges or diverges depending on the value of real variable $s$, a connection described by the relation

$$\left(1-\frac{1}{2^s}\right)^{-1}\left(1-\frac{1}{3^s}\right)^{-1}\left(1-\frac{1}{5^s}\right)^{-1}\cdots=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\cdots,$$

which holds in particular for all real $s>1$. Approximately one century later, Riemann studied this identity for complex values of $s$ by carefully exhibiting the analytic properties of the now famous *Riemann Zeta Function*

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}\qquad(\mathrm{Re}(s)>1).$$

By extending this function to the entire complex plane, he used it to establish in 1859 a somewhat exceptional but nevertheless incomplete proof of the Prime Number Theorem. Thirty-seven years later, Hadamard and de la Vallée Poussin managed to complete the proof initiated by Riemann.

The methods put forward by Riemann and many other 20th-century mathematicians have helped us gain a better understanding of the distribution of prime numbers and a clearer picture of the complexity of the multiplicative structure of the integers or, using a stylistic device, a better comprehension of the anatomy of integers.

In this book, we provide an introduction to analytic number theory. The choice of the subtitle "Exploring the Anatomy of Integers" was coined at a CRM workshop held at Université de Montréal in March 2006 which the two of us, along with Andrew Granville, organized. For the workshop as well as for this book, the terminology "anatomy of integers" is appropriate as it describes the area of multiplicative number theory that relates to the size and distribution of the prime factors of positive integers and of various families of integers of particular interest.

Besides the proof of the Prime Number Theorem, our choice of subjects for this book is very subjective but nevertheless legitimate. Hence, several chapters are devoted to the study of arithmetic functions, in particular those

which provide a better understanding of the multiplicative structure of the integers. For instance, we study the average value of the number of prime factors of an integer, the average value of the number of its divisors, the behavior of its smallest prime factor and of its largest prime factor, and so on. A whole chapter is devoted to sieve methods, and many of their applications are presented in the problem section at the end of that chapter. Moreover, we chose to include some results which are hard to find elsewhere. For instance, we state and prove the very useful Birkhoff-Vandiver primitive divisor theorem and the important Turán-Kubilius inequality for additive functions. We also discuss less serious but nevertheless interesting topics such as the Erdős multiplication table problem.

We also chose to discuss the famous *abc* conjecture, because it is fairly recent (it was first stated in 1985) and also because it is central in the study of various conjectures in number theory. Finally, we devote a chapter to the study of the index of composition of an integer, its study allowing us to better understand the anatomy of an integer.

To help the reader better comprehend the various themes presented in this book, we listed 263 problems along with the solutions to the even-numbered ones.

Finally, we are grateful to our former students who provided important feedback on earlier versions of this book. In particular, we would like to thank Maurice-Etienne Cloutier, Antoine Corriveau la Grenade, Michael Daub, Nicolas Doyon, Ross Kravitz, Natee Pitiwan, and Brian Simanek. We are very appreciative of the assistance of Professor Kevin A. Broughan, who kindly provided mathematical and grammatical suggestions. We would also like to thank the anonymous reviewers of the AMS for their clever suggestions which helped improve the quality of this book.

Jean-Marie De Koninck

Florian Luca

# Notation

We denote respectively by $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ the set of positive integers, the set of integers, the set of rational numbers, the set of real numbers, and the set of complex numbers. At times, we shall let $\mathbb{R}_+$ stand for the set of positive real numbers.

A number $\xi$ is said to be *algebraic* if it is the solution of a polynomial equation, that is, if there exist integers $k \geq 1$ and $a_0 \neq 0, a_1, \ldots, a_k$ such that $a_0\xi^k + a_1\xi^{k-1} + \cdots + a_{k-1}\xi + a_k = 0$. A number $\xi$ is said to be *transcendental* if it is not algebraic.

We let $e$ stand for the *naperian number* and we let $\pi$ stand for the ratio of the circumference of a circle to its diameter. Both $e$ and $\pi$ are transcendental numbers.

We write $\gamma$ for the *Euler constant*, which is defined by

$$\gamma = \lim_{N\to\infty} \left( \sum_{n=1}^{N} \frac{1}{n} - \log N \right) = 0.5772156649\ldots.$$

Most of the time, we use the letters $k$, $\ell$, $m$, $n$, $r$ and $\alpha, \beta$ to designate integers and $x$, $y$ to designate real numbers. The letters $C$ and $c$, with or without subscript, are usually reserved for positive constants, but not necessarily the same at each occurrence. Similarly, the letters $p$ and $q$, with or without subscript, will normally stand for prime numbers. Unless we indicate otherwise, the sequence $\{p_n\}$ stands for the increasing sequence of prime numbers, that is, the sequence 2, 3, 5, 7, 11, 13, 17, ....

By $\lfloor x \rfloor$, we mean the largest integer smaller or equal to $x$. Tied to this function is the fractional part of $x$ defined by $\{x\} = x - \lfloor x \rfloor$.

The expression $p^a \parallel b$ means that $a$ is the largest integer for which $p^a \mid b$.

We write $\mathrm{lcm}[a_1, a_2, \ldots, a_k]$ to denote the least common multiple of the positive integers $a_1, a_2, \ldots, a_k$. Similarly, we write $\gcd(a_1, a_2, \ldots, a_k)$ to denote the greatest common divisor of the positive integers $a_1, a_2, \ldots, a_k$; when the context is clear, we may at times simply write $(a_1, a_2, \ldots, a_k)$ instead of $\gcd(a_1, a_2, \ldots, a_k)$, as well as $[a_1, a_2, \ldots, a_k]$ instead of $\mathrm{lcm}[a_1, a_2, \ldots, a_k]$.

Throughout this book, $\log x$ stands for the natural logarithm of $x$. At times, we also write $\log_2 x$ instead of $\log\log x$ and more generally, for each integer $k \geq 3$, we let $\log_k x$ stand for $\log(\log_{k-1} x)$.

For each integer $k \geq 0$, we denote by $C^k[a, b]$ the set of functions whose $k^{\text{th}}$ derivative exists and is continuous on the interval $[a, b]$. Thus $C^0[a, b]$ stands for the set of continuous functions on $[a, b]$.

It is often convenient to use the notations introduced by Landau, namely $o(\ldots)$ and $O(\ldots)$, to compare the order of magnitude of functions in the neighborhood of a point or of infinity. Unless we indicate otherwise, we shall mean the latter.

Given two functions $f$ and $g$ defined on $[a, \infty)$, where $a \geq 0$ and $g(x) > 0$, we shall write that $f(x) = O(g(x))$ if there exist two constants $M > 0$ and $x_0$ such that $|f(x)| < Mg(x)$ for all $x \geq x_0$. In particular, $f(x) = O(1)$ if $f(x)$ is a bounded function. Moreover, instead of writing $f(x) = O(g(x))$, we shall at times write $f(x) \ll g(x)$.

Thus, we have, as $x \to \infty$,

$$x = O(x^2), \qquad \sin x = O(1), \qquad \log x = O(x^{1/10}),$$

$$\frac{\sin x}{x} = O(1), \qquad x^4 = O(e^x), \qquad e^x \sin x = O(e^x),$$

$$2x^2 + \frac{x}{3} \ll x^2, \quad \tfrac{x^3}{x^3+x^2} + 7 = O(1).$$

Given two functions $f$ and $g$ defined on $[a, \infty)$, where $a \geq 0$ and $g(x) > 0$, we shall write $f(x) = o(g(x))$ as $x \to \infty$ if, for each $\varepsilon > 0$, there exists a constant $x_0 = x_0(\varepsilon)$ such that $|f(x)| < \varepsilon g(x)$ for all $x \geq x_0$.

Thus, we have

$$\tfrac{1}{x} = o(1), \qquad \sin x = o(x), \quad \log x = o(x),$$

$$\tfrac{\sin 1/x}{1/x} = 1 + o(1), \quad x^4 = o(e^x), \qquad xe^x \sin x = o(x^2 e^x).$$

Given two functions $f$ and $g$ defined on $[a,\infty)$ (where $a \geq 0$), we shall write $f(x) \gg g(x)$ if there exist two constants $M > 0$ and $x_0$ such that $|f(x)| > M|g(x)|$ for all $x \geq x_0$.

Thus, we have

$$x \gg \sqrt{x}, \qquad 2 + \sin x \gg 1, \quad \sqrt{x} \gg \log x,$$

$$1 + \tfrac{\sin x}{x} \gg 1, \quad e^x \gg x^4, \qquad xe^x \gg e^x.$$

On the other hand, given two functions $f$ and $g$ defined on $[a,\infty)$ (where $a \geq 0$), we write $f(x) \sim g(x)$ to mean that $\lim\limits_{x\to\infty} \dfrac{f(x)}{g(x)} = 1$.

Thus, as $x \to \infty$,

$$\frac{\sin 1/x}{1/x} \sim 1, \qquad x^2 + x \sim x^2.$$

Finally, we write that $f(x) \asymp g(x)$ if we simultaneously have $f(x) \ll g(x)$ and $g(x) \ll f(x)$. Observe that $f(x) \asymp g(x)$ if and only if

$$0 < \liminf_{x\to\infty} \frac{f(x)}{g(x)} \leq \limsup_{x\to\infty} \frac{f(x)}{g(x)} < \infty.$$

# Frequently Used Functions

$P(n) = \max\{p : p|n\}$, the largest prime factor of $n \geq 2$

$p(n) = \min\{p : p|n\}$, the smallest prime factor of $n \geq 2$

$\Psi(x, y) = \#\{n \leq x : P(n) \leq y\}$

$\Phi(x, y) = \#\{n \leq x : p(n) > y\}$

$\beta(n) = \sum_{p|n} p$, the sum of the prime factors of $n$

$\pi(x) = \sum_{p \leq x} 1$, the number of prime numbers $\leq x$

$\theta(x) = \sum_{p \leq x} \log p$

$\psi(x) = \sum_{\substack{p^\alpha \leq x \\ \alpha \geq 1}} \log p$

$\pi(x; k, \ell) = \sum_{\substack{p \leq x \\ p \equiv \ell \pmod{k}}} 1$, the number of prime numbers $p \leq x$, $p \equiv \ell \pmod{k}$

$\mathrm{li}(x) = \int_0^x \frac{dt}{\log t}$, the logarithmic integral

$\gamma(n) = \prod_{p|n} p$, the product of the prime numbers dividing $n$

$\phi(n) = \sum_{\substack{m \le n \\ (m,n)=1}} 1$, the Euler $\phi$ function

$\sigma(n) = \sum_{d|n} d$, the sum of the (positive) divisors of $n$

$\sigma_k(n) = \sum_{d|n} d^k$, the sum of the $k$-th powers of the divisors of $n$

$d(n) = \sum_{d|n} 1$, the number of divisors of $n$

$\omega(n) = \sum_{p|n} 1$, the number of distinct prime divisors of $n$

$\Omega(n) = \sum_{p^\alpha \| n} \alpha$, the number of prime factors of $n$ counting multiplicity

$\Pi_k(x) = \sum_{\substack{n \le x \\ \omega(n)=k}} 1$, the number of integers $n \le x$ such that $\omega(n) = k$

$\mu(n)$, the Möbius function, defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & p^2 | n \text{ for some prime } p, \\ (-1)^{\omega(n)} & \text{otherwise.} \end{cases}$$

$\lambda(n) = \dfrac{\log n}{\log \gamma(n)}$, the index of composition of the integer $n \ge 2$

*Chapter 1*

# Preliminary Notions

## 1.1. Approximating a sum by an integral

In certain situations, it is useful to replace a sum by an integral. The following result shows when and how this can be done.

**Proposition 1.1.** *Let $a, b \in \mathbb{N}$ with $a < b$ and let $f : [a, b] \to \mathbb{R}$ be a monotonic function on $[a, b]$. There exists a real number $\theta = \theta(a, b)$ such that $-1 \leq \theta \leq 1$ and such that*

$$\sum_{a<n\leq b} f(n) = \int_a^b f(t)\,dt + \theta(f(b) - f(a)). \tag{1.1}$$

**Proof.** Indeed, assume that $f$ is decreasing, in which case, using a geometric approach, it is easy to see that

$$0 < \int_a^b f(t)\,dt - \sum_{a<n\leq b} f(n) < \sum_{a\leq n\leq b-1} f(n) - \sum_{a<n\leq b} f(n) = f(a) - f(b),$$

from which (1.1) follows easily. If on the other hand, $f$ is increasing, the same type of argument yields (1.1). □

One can use this result to estimate $\log n!$. Indeed, setting $f(n) = \log n$ in (1.1), one obtains

$$\log n! = \sum_{i=1}^{n} \log i = \int_1^n \log t\,dt + \theta(\log n - \log 1) = n \log n - n + O(\log n),$$

thus providing a fairly good approximation for $\log n!$. A better estimate is proved in Section 1.9.

One can also obtain a more accurate asymptotic expression in the case where the function $f$ is decreasing. In fact, one can prove that if $f : [1, \infty) \to \mathbb{R}_+$ is continuous, decreasing and such that $\lim_{x\to\infty} f(x) = 0$, then there exists a constant $A$ such that

$$\sum_{1\le n\le x} f(n) = \int_1^x f(t)\,dt + A + O(f(x)). \tag{1.2}$$

To prove this result, compare the areas provided by expressions $\sum_{1\le n\le x} f(n)$ and $\int_1^x f(t)\,dt$. We would like to show that the expression

$$D(N) := \int_1^N f(t)\,dt - \sum_{2\le n\le N} f(n),$$

where $N$ is a positive integer, tends to a positive constant as $N \to \infty$. First, it is clear that $D(N) \ge 0$ for each integer $N \ge 2$. So let

$$R(N) = \sum_{n=N+1}^{\infty} \left( \int_{n-1}^{n} f(t)\,dt - f(n) \right).$$

In order to prove (1.2), it is sufficient to show that $R(N) = O(f(N))$. But for each pair of positive integers $M$ and $N$ with $M \ge N + 3$, we have

$$\sum_{n=N+1}^{M-1} f(n) + f(M) < \int_N^M f(t)\,dt < f(N) + \sum_{n=N+1}^{M-1} f(n),$$

so that

$$0 < \sum_{n=N+1}^{M} \left( \int_{n-1}^{n} f(t)\,dt - f(n) \right) < f(N) - f(M) < f(N).$$

It follows from this that

$$0 \le \sum_{n=N+1}^{\infty} \left( \int_{n-1}^{n} f(t)\,dt - f(n) \right) \le f(N),$$

which implies that $R(N) = O(f(N))$, thereby establishing formula (1.2).

## 1.2. The Euler-MacLaurin formula

We saw in the previous section that one could approximate the sum of a function by an integral, provided this function was monotonic. Here, we will see that if the function has a continuous derivative, then a more precise approximation can be obtained.

**Proposition 1.2.** *(Euler-MacLaurin formula) Let $0 < y < x$ be two real numbers and assume that $f : [y, x] \to \mathbb{R}$ has a continuous derivative on $[y, x]$. Then*

(1.3)

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

**Proof.** Expanding the second integral on the right side of (1.3), we get

$$\begin{aligned} I = \int_y^x (t - \lfloor t \rfloor) f'(t)\,dt &= \left( \int_{\lfloor y \rfloor + 1}^{\lfloor x \rfloor} + \int_{\lfloor x \rfloor}^{x} + \int_{y}^{\lfloor y \rfloor + 1} \right) (t - \lfloor t \rfloor) f'(t)\,dt \\ &= I_1 + I_2 + I_3, \end{aligned}$$

say. Set $a = \lfloor y \rfloor$ and $b = \lfloor x \rfloor$, and let us evaluate separately each of the integrals $I_i$.

$$\begin{aligned} I_1 &= \int_{a+1}^{b} (t - \lfloor t \rfloor) f'(t)\,dt = \sum_{k=a+1}^{b-1} \int_k^{k+1} (t-k) f'(t)\,dt \\ &= \sum_{k=a+1}^{b-1} \int_k^{k+1} t f'(t)\,dt - \sum_{k=a+1}^{b-1} k \int_k^{k+1} f'(t)\,dt \\ &= \sum_{k=a+1}^{b-1} \left( t f(t) \Big|_{t=k}^{t=k+1} - \int_k^{k+1} f(t)\,dt \right) - \sum_{k=a+1}^{b-1} k(f(k+1) - f(k)) \\ &= b f(b) - (a+1) f(a+1) \\ &\qquad - \int_{a+1}^{b} f(t)\,dt + (a+1) f(a+1) - b f(b) + \sum_{n=a+2}^{b} f(n). \end{aligned}$$

Therefore,

$$\sum_{n=a+2}^{b} f(n) = \int_{a+1}^{b} f(t)\,dt + I_1.$$

On the other hand,

$$\begin{aligned} I_2 &= \int_b^x (t-b) f'(t)\,dt = \int_b^x t f'(t)\,dt - b \int_b^x f'(t)\,dt \\ &= t f(t) \Big|_{t=b}^{t=x} - \int_b^x f(t)\,dt - b \int_b^x f'(t)\,dt \\ &= (x - \lfloor x \rfloor) f(x) - \int_{\lfloor x \rfloor}^{x} f(t)\,dt. \end{aligned}$$

Similarly,

$$\begin{aligned} I_3 &= -\left((y-\lfloor y\rfloor)f(y) - f(\lfloor y\rfloor+1) - \int_{\lfloor y\rfloor+1}^{y} f(t)\,dt\right) \\ &= (\lfloor y\rfloor - y)f(y) - \int_{y}^{\lfloor y\rfloor+1} f(t)\,dt + f(\lfloor y\rfloor+1). \end{aligned}$$

Since $I_1 = I - I_2 - I_3$, it follows that

$$\begin{aligned} \sum_{n=a+2}^{b} f(n) &= \int_{a+1}^{b} f(t)\,dt + \int_{y}^{x} (t-\lfloor t\rfloor)f'(t)\,dt - (x-\lfloor x\rfloor)f(x) \\ &\quad + \int_{b}^{x} f(t)\,dt - f(\lfloor y\rfloor+1) - (\lfloor y\rfloor - y)f(y) + \int_{y}^{a+1} f(t)\,dt. \end{aligned}$$

From this, we get that

$$\sum_{n=a+1}^{b} f(n) = \int_{y}^{x} f(t)\,dt + \int_{y}^{x} (t-\lfloor t\rfloor)f'(t)\,dt + (\lfloor x\rfloor - x)f(x) - (\lfloor y\rfloor - y)f(y),$$

which proves (1.3). □

The Euler-MacLaurin formula can be considerably generalized. For instance, one can show the following.

**Proposition 1.3.** *Let $\nu$ be a positive integer. Let $f$ be a function such that the derivatives $f', f'', \ldots, f^{(2\nu)}$ are all continuous on the interval $[M, N]$. Then,*

$$\begin{aligned} \sum_{n=M}^{N} f(n) &= \int_{M}^{N} f(t)\,dt + \frac{1}{2}[f(M)+f(N)] + \frac{B_2}{2!}f'(x)\Big|_{M}^{N} + \frac{B_4}{4!}f'''(x)\Big|_{M}^{N} \\ &\quad + \cdots + \frac{B_{2\nu}}{(2\nu)!}f^{(2\nu-1)}(x)\Big|_{M}^{N} - \frac{1}{(2\nu)!}\int_{M}^{N} B_{2\nu}(t-\lfloor t\rfloor)f^{(2\nu)}(t)\,dt, \end{aligned}$$

*where the $B_i$'s are the Bernoulli numbers defined implicitly by*

$$\sum_{i=0}^{\infty} B_i \frac{y^i}{i!} = \frac{y}{e^y - 1}$$

*and where $B_i(x)$ stands for the $i$-th Bernoulli polynomial which is defined as the unique polynomial of degree $i$ satisfying to*

$$\int_{x}^{x+1} B_i(u)\,du = x^i.$$

*Thus, $B_1(u) = u - \frac{1}{2}$, $B_2(u) = u^2 - u + \frac{1}{6}$, $B_3(u) = u^3 - \frac{3}{2}u^2 + \frac{1}{2}u$, ....*

## 1.3. The Abel summation formula

**Proposition 1.4.** *(Abel summation formula) Let $\{a_n\}_{n\geq 1}$ be a sequence of complex numbers and let $f : [1, +\infty) \longrightarrow \mathbb{C}$. For each real number $x \geq 1$, let*

$$A(x) = \sum_{n\leq x} a_n$$

*and assume that $f(x)$ has a continuous derivative for $x \geq 1$. Then*

$$\sum_{n\leq x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt. \tag{1.4}$$

**Proof.** We first assume that $x = N$, an integer. Then

$$\begin{aligned}\sum_{n\leq N} a_n f(n) &= A(1)f(1) + (A(2) - A(1))f(2) \\ &\quad + \cdots + (A(N) - A(N-1))f(N) \\ &= A(1)(f(1) - f(2)) + \cdots + A(N-1)(f(N-1) - f(N)) \\ &\quad + A(N)f(N).\end{aligned}$$

Next observe that $f(i+1) - f(i) = \int_i^{i+1} f'(t)dt$ for $i = 1, \ldots, N-1$, and that $A(t)$ is constant on the interval $[i, i+1)$. Therefore,

$$\begin{aligned}\sum_{n\leq N} a_n f(n) &= A(N)f(N) - \sum_{i=1}^{N-1} A(i) \int_i^{i+1} f'(t)dt \\ &= A(N)f(N) - \sum_{i=1}^{N-1} \int_i^{i+1} A(t)f'(t)dt \\ &= A(N)f(N) - \int_1^N A(t)f'(t)dt.\end{aligned}$$

This proves relation (1.4) when $x = N$ is an integer. So, let us now assume that $x$ is not an integer. Set $N = \lfloor x \rfloor$. On the other hand, since $A(t)$ is constant on the interval $[N, x]$, the right-hand side of (1.4) can be written as

$$\begin{aligned}A(x)f(x) &- \int_1^x A(t)f'(t)dt \\ &= A(x)f(x) - \int_N^x A(t)f'(t)dt - \int_1^N A(t)f'(t)dt \\ &= A(x)f(x) - A(N) \int_N^x f'(t)dt - \int_1^N A(t)f'(t)dt \\ &= A(x)f(x) - A(N)(f(x) - f(N)) - \int_1^N A(t)f'(t)dt\end{aligned}$$

$$\begin{aligned} &= A(N)f(N) - \int_1^N A(t)f'(t)dt \\ &= \sum_{n\le N} a_n f(n), \end{aligned}$$

where the last equality holds since we just proved that (1.4) holds when $x$ is an integer. Now, since clearly $\sum_{n\le x} a_n f(n) = \sum_{n\le N} a_n f(n)$, the proof of the proposition is complete. □

Before establishing the next result, we introduce an important constant.

**Definition 1.5.** *Let*

$$\gamma = 1 - \int_1^\infty \frac{t - \lfloor t \rfloor}{t^2}\, dt.$$

*The number $\gamma$ is called Euler's constant. Its numerical value is approximately* $0.57721\ldots$.

**Remark 1.6.** One can easily show that the above definition of the Euler constant is equivalent to the following one (already mentioned in the Notation section on page xiii):

$$\gamma = \lim_{N\to\infty} \left( \sum_{n=1}^{N} \frac{1}{n} - \log N \right)$$

(see Problem 1.4).

It is believed that $\gamma$ is a transcendental number although it is not even known if it is irrational. See J. Havil's excellent book [**78**] for a thorough study of this amazing constant.

As an application of this formula we have the following.

**Theorem 1.7.** *For all $x \ge 1$,*

$$\sum_{n\le x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right). \tag{1.5}$$

**Proof.** Setting $a_n = 1$ and $f(t) = 1/t$ in the Abel summation formula, we easily obtain that

$$A(x) = \sum_{n\le x} 1 = \lfloor x \rfloor,$$

and that $f'(t) = -1/t^2$, yielding

$$\begin{aligned} \sum_{n\le x} \frac{1}{n} &= \frac{\lfloor x \rfloor}{x} + \int_1^x \frac{\lfloor t \rfloor}{t^2}\, dt \\ &= \frac{x - (x - \lfloor x \rfloor)}{x} + \int_1^x \frac{t - (t - \lfloor t \rfloor)}{t^2}\, dt \end{aligned}$$

$$
\begin{aligned}
&= 1 + O\left(\frac{1}{x}\right) + \int_1^x \frac{dt}{t} - \int_1^x \frac{t - \lfloor t \rfloor}{t^2}\, dt \\
&= 1 + O\left(\frac{1}{x}\right) + \left(\log t \Big|_{t=1}^{t=x}\right) - \left(\int_1^\infty \frac{t - \lfloor t \rfloor}{t^2}\, dt - \int_x^\infty \frac{t - \lfloor t \rfloor}{t^2}\, dt\right) \\
&= \log x + \gamma + O\left(\frac{1}{x}\right) + \int_x^\infty \frac{t - \lfloor t \rfloor}{t^2}\, dt \\
&= \log x + \gamma + O\left(\frac{1}{x}\right) + O\left(\int_x^\infty \frac{dt}{t^2}\right) \\
&= \log x + \gamma + O\left(\frac{1}{x}\right),
\end{aligned}
$$

as $x \to \infty$, thus completing the proof of the theorem. □

## 1.4. Stieltjes integrals

At times, it is convenient to write certain finite sums as Stieltjes integrals.

Recall that the *Stieltjes*[1] *integral* $I$ of the function $f$ over the interval $[a, b]$ with respect to the function $g$ is defined as

$$I = \int_a^b f\, dg = \int_a^b f(t)\, dg(t) = \lim_{\|\Delta\| \to 0} \sum_{j=1}^{n} f(\xi_j)(g(t_j) - g(t_{j-1}))$$

with $\Delta = (t_0, \ldots, t_n)$, $a = t_0$, $b = t_n$, $\|\Delta\| = \max_{1 \le j \le n}(t_j - t_{j-1})$ and $\xi_j \in [t_{j-1}, t_j]$ for all $j = 1, \ldots, n$.

If $g(x) = x$, then

$$I = \int_a^b f(t)\, \mathrm{d}\, t$$

is simply the *Riemann integral* of $f$. If

$$g(x) = \begin{cases} 0 & \text{if } a \le x \le c, \\ 1 & \text{if } c < x \le b, \end{cases}$$

then $I = f(c)$.

For instance, assume that we want to estimate the expression

$$\sum_{\substack{a \le x \\ a \in A}} f(a), \tag{1.6}$$

[1] Thomas Stieltjes (1850–1894, Holland) was very much interested in elliptic curves and in number theory. In fact, as Narkiewicz recalls in his book [**110**], Stieltjes was the first to make an attempt at a proof of the Riemann Hypothesis. Indeed, he asserted that the series $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ converges for all $s > 1/2$, a statement which would have implied the Riemann Hypothesis (see Problem 3.13 in Chapter 3).

where $A \subset \mathbb{N}$ and $f \in C^0[1,x]$. Let $A(x)$ be the counting function for the set $A$, that is, let

$$A(x) = \#\{a \le x : a \in A\}.$$

Then it is easy to see that

$$\int_{1-0}^{x} f(t)\,\mathrm{d}\,A(t) = \sum_{n\le x} \int_{n-0}^{n+0} f(t)\,\mathrm{d}\,A(t) = \sum_{\substack{n\le x\\ n\in A}} \int_{n-0}^{n+0} f(t)\,\mathrm{d}\,A(t) = \sum_{\substack{n\le x\\ n\in A}} f(n),$$

which clearly illustrates that the sum (1.6) can be represented by a Stieltjes integral.

## 1.5. Slowly oscillating functions

Very often in number theory, we encounter asymptotic estimates such as

$$\pi(x) \sim \frac{x}{\log x}, \qquad \sum_{p\le x} \frac{1}{p} \sim \log\log x, \qquad \sum_{n\le x} f(n) = x + O\left(\frac{x}{e^{\sqrt{\log x}}}\right).$$

In these statements, the functions $\log x$, $\log\log x$ and $e^{\sqrt{\log x}}$ are all of a particular type: they all belong to the class of slowly oscillating functions.

**Definition 1.8.** *A function $L : [M,+\infty) \to \mathbb{R}$ continuous on $[M,+\infty)$, where $M$ is a positive real number, is said to be a slowly oscillating function if for each positive real number $c > 0$,*

$$\lim_{x\to\infty} \frac{L(cx)}{L(x)} = 1. \tag{1.7}$$

We denote by $\mathcal{L}$ the set of slowly oscillating functions. It is possible to show (see Seneta [**128**]) that a differentiable function $L$ belongs to $\mathcal{L}$ if and only if

$$\frac{xL'(x)}{L(x)} = o(1) \qquad (x\to\infty) \tag{1.8}$$

and, in fact, that $L \in \mathcal{L}$ if and only if there exists $x_0 > 0$ such that

$$L(x) = C(x)\exp\left\{\int_{x_0}^{x} \frac{\eta(t)}{t}\,dt\right\},$$

where $\lim_{x\to\infty} C(x) = C$, for a certain constant $C \neq 0$, and where $\eta(t)$ is a function which tends to 0 as $t \to \infty$. This last result is often called the *Representation theorem* for slowly oscillating functions.

A function $R : [M,+\infty) \to \mathbb{R}$ continuous on $[M,+\infty)$, where $M$ is a positive real number, is said to be *regularly varying* if there exists a real

number $\rho$ such that, for each positive real number $c > 0$,

$$\lim_{x\to\infty} \frac{R(cx)}{R(x)} = c^\rho,$$

in which case we say that the function $R$ is of *index* $\rho$.

One can prove that any regularly varying function of index $\rho$ can be written in the form

$$R(x) = x^\rho L(x),$$

where $L$ is a slowly oscillating function.

A nice result concerning slowly oscillating functions is the following.

**Proposition 1.9.** *Let $L : [M, +\infty) \to \mathbb{R}_+$, where $M > 0$. Assume that $L \in \mathcal{C}^1[M, +\infty)$. Then*

$$L \in \mathcal{L} \iff \int_M^x \frac{dt}{L(t)} = (1 + o(1))\frac{x}{L(x)} \qquad (x \to \infty).$$

(See Problem 1.12.) Various examples and applications are provided in the problems at the end of this chapter.

## 1.6. Combinatorial results

Of frequent use in several arguments is the *Pigeon Hole principle*, which can be stated as follows:

**Proposition 1.10.** *(Pigeon Hole principle) Given $n$ objects which are to be inserted in $n - 1$ distinct boxes, one can always find one particular box containing at least two of these objects.*

The other frequently used combinatorial tool is the *Inclusion-Exclusion principle*, which can be stated as follows:

**Proposition 1.11.** *(Inclusion-Exclusion principle) Denoting by $P(A)$ the probability that an event $A$ occurs, by $P(A \cup B)$ the probability that $A$ or $B$ occurs and by $P(A \cap B)$ the probability that $A$ and $B$ occur, and letting $A_1, A_2, \ldots, A_n$ be events, then*

$$P(A_1 \cup A_2 \cup \ldots \cup A_n) = \sum_{1\le i\le n} P(A_i) - \sum_{1\le i<j\le n} P(A_i \cap A_j)$$
$$+ \sum_{1\le i<j<k\le n} P(A_i \cap A_j \cap A_k) - \cdots + (-1)^{n+1} P(A_1 \cap A_2 \cap \ldots \cap A_n).$$

## 1.7. The Chinese Remainder Theorem

The following theorem is very important in number theory.

**Theorem 1.12.** *(Chinese Remainder Theorem) Let $m_1, \ldots, m_k$ be positive integers with $(m_i, m_j) = 1$ for all $1 \leq i < j \leq k$. Let $a_1, \ldots, a_k$ be arbitrary integers. Then there is an integer $a$ such that*

$$a \equiv a_i \pmod{m_i} \qquad \text{for all } i = 1, \ldots, k. \tag{1.9}$$

**Proof.** Let $M = \prod_{i=1}^{k} m_i$ and $M_i = M/m_i$ for $i = 1, \ldots, k$. Since $(m_i, m_j) = 1$ whenever $i \neq j$, we get that $m_i$ and $M_i$ are coprime for $i = 1, \ldots, k$. In particular, the class $M_i \pmod{m_i}$ is invertible modulo $m_i$. Let $n_i$ be an integer such that $n_i M_i \equiv 1 \pmod{m_i}$. Put

$$a = \sum_{i=1}^{k} a_i n_i M_i. \tag{1.10}$$

One easily checks that the positive integer $a$ given in (1.10) satisfies (1.9). To see this, let $\ell$ be any index in $\{1, \ldots, k\}$. Since $m_\ell \mid M_j$ for $j \neq \ell$, we get that

$$a \equiv \sum_{i=1}^{k} a_i n_i M_i \equiv a_\ell n_\ell M_\ell \equiv a_\ell \pmod{m_\ell},$$

implying that $a$ satisfies (1.9). □

**Corollary 1.13.** *Let $m_1, \ldots, m_k$ be positive integers with $(m_i, m_j) = 1$ for all $1 \leq i < j \leq k$. The map*

$$\psi : \mathbb{Z}/(m_1 \cdots m_k)\mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \tag{1.11}$$

*given by*

$$a \pmod{m_1 \cdots m_k} \longmapsto (a \pmod{m_1}, \ldots, a \pmod{m_k})$$

*is a ring isomorphism.*

**Proof.** One easily checks that $\psi$ is a morphism of rings. To see that $\psi$ is injective, let $a$ be an integer such that $\psi(a \pmod{m_1 \cdots m_k}) = 0$. In particular, $a \equiv 0 \pmod{m_i}$ for each $i = 1, \ldots, k$, so that $m_i \mid a$ for all $i = 1, \ldots, k$. Since $(m_i, m_j) = 1$ for $i \neq j$, we conclude that $m_1 \cdots m_k \mid a$, so that $a \equiv 0 \pmod{m_1 \cdots m_k}$. The fact that $\psi$ is surjective is then an immediate consequence of the Chinese Remainder Theorem. □

## 1.8. The density of a set of integers

Intuitively, it makes sense to say that half of the positive integers are even, while a third are a multiple of 3. Hence, it would be reasonable to say that the density of the subset of even integers is $\frac{1}{2}$, compared with $\frac{1}{3}$ for the set of positive integers which are a multiple of 3. Let us now make this definition of *density* more rigorous. We will say that a subset $A$ of $\mathbb{N}$ has density (or asymptotic density) $\delta$, where $0 \leq \delta \leq 1$, if the proportion of elements of A among all natural numbers from 1 to $N$ is asymptotic to $\delta$ as $N \to \infty$.

More formally, $A \subset \mathbb{N}$ has density $\delta$ if

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n\leq N \\ n\in A}} 1 = \delta.$$

For example, one easily checks that the set of positive integers which are a multiple of the positive integer $k$ is $\frac{1}{k}$. Also, given the integers $a$ and $b$ with $0 \leq b < a$ and setting $A = \{n \in \mathbb{N} : n \equiv b \pmod{a}\}$, it is easy to prove that the density of $A$ is equal to $\frac{1}{a}$. Moreover, one can easily show that it follows from the Prime Number Theorem that the set of prime numbers is of zero density.

Finally, there exist subsets of $\mathbb{N}$ which do not have a density. For example, consider the function $f : \mathbb{N} \to \{0, 1\}$ which is defined by $f(1) = 1$ and, for each integer $n \geq 2$ by

$$f(n) = \begin{cases} 1 & \text{if } 2^{2m} < n \leq 2^{2m+1}, \\ 0 & \text{if } 2^{2m+1} < n \leq 2^{2m+2}. \end{cases}$$

One can easily show that the set $\{n \in \mathbb{N} : f(n) = 1\}$ has no density (see Problem 1.10).

We will study more extensively the notion of asymptotic density in Section 7.5 of Chapter 7.

## 1.9. The Stirling formula

Before proving the Stirling formula $n! \sim n^n e^{-n}\sqrt{2\pi n}$ (as $n \to \infty$), it is interesting to mention its weak form

$$n! > \left(\frac{n}{e}\right)^n, \tag{1.12}$$

which can easily be proved by observing that

$$\begin{aligned}\log(n!) &= \log 2 + \cdots + \log n \\ &> \int_1^2 \log t\, dt + \int_2^3 \log t\, dt + \cdots + \int_{n-1}^n \log t\, dt \\ &= \int_1^n \log t\, dt = t\log t - t\Big|_{t=1}^{t=n} = n\log n - n + 1 \\ &> \log\left(\left(\frac{n}{e}\right)^n\right).\end{aligned} \tag{1.13}$$

We now state Stirling's formula in its traditional form.

**Theorem 1.14.** *(Stirling's formula) As $n \to \infty$,*

$$n! \sim n^n e^{-n}\sqrt{2\pi n}. \tag{1.14}$$

**Proof.** First observe that since the function $\log t$ is increasing for $t > 0$, it is clear that

$$\int_{j-1}^{j} \log t\, dt < \log j < \int_j^{j+1} \log t\, dt.$$

Adding up these inequalities, for $j = 1, 2, \ldots, n$, we obtain

$$\begin{aligned}\int_0^n \log t\, dt &< \log n! < \int_1^{n+1} \log t\, dt, \\ n\log n - n &< \log n! < (n+1)\log(n+1) - n.\end{aligned}$$

Rearranging this last expression, we obtain

$$n\log n - n < \log n! < n\log n - n + \log n + O(1),$$

suggesting that one should consider the expression

$$b_n := n\log n - n + \frac{1}{2}\log n$$

as an approximation of $\log n!$. So, let us consider the difference

$$a_n := \log n! - b_n = \log n! - \left(n + \frac{1}{2}\right)\log n + n.$$

Observe that, setting $\alpha = 1/(2n+1)$ and using the fact that

$$\frac{1}{2}\log\left(\frac{1+\alpha}{1-\alpha}\right) = \alpha + \frac{1}{3}\alpha^3 + \frac{1}{5}\alpha^5 + \cdots,$$

we get that

$$\begin{aligned}0 < a_n - a_{n+1} &= \left(n + \frac{1}{2}\right)\log\left(\frac{n+1}{n}\right) - 1 \\ &= \frac{1}{\alpha}\cdot\frac{1}{2}\cdot\log\left(\frac{1+\alpha}{1-\alpha}\right) - 1\end{aligned}$$

$$\begin{aligned} &= \frac{1}{\alpha}\left(\alpha + \frac{1}{3}\alpha^3 + \frac{1}{5}\alpha^5 + \cdots\right) - 1 \\ &< \frac{1}{3}\left(\alpha^2 + \alpha^4 + \cdots\right) \\ &= \frac{\alpha^2}{3(1-\alpha^2)} = \frac{1}{12n(n+1)}, \end{aligned}$$

thus establishing that the sequence $\{a_n\}_{n\geq 1}$ is decreasing and converges to some positive number $c$. Therefore,

$$\lim_{n\to\infty} e^{a_n} = \lim_{n\to\infty} \frac{n!e^n}{n^{n+\frac{1}{2}}} = e^c.$$

It remains to show that

$$e^c = \sqrt{2\pi}. \tag{1.15}$$

To do so, we call upon the well-known Wallis formula for $\pi$ (proved in 1656), namely

$$\lim_{n\to\infty} \frac{2\cdot 4\cdot 6\cdots(2n)}{1\cdot 3\cdot 5\cdots(2n-1)\sqrt{2n}} = \sqrt{\frac{\pi}{2}},$$

which can be written as

$$\frac{(2^n n!)^2}{(2n)!}\frac{1}{\sqrt{2n}} \sim \sqrt{\frac{\pi}{2}} \quad \text{as } n\to\infty. \tag{1.16}$$

(For an elementary proof of this formula, see Wästlund [**145**].) Using the fact that $n! \sim n^n\sqrt{n}e^{-n}e^c$, we may replace $n!$ by $n^n\sqrt{n}e^{-n}e^c$ in (1.16), to conclude after simplifications that

$$e^c \sim \sqrt{2\pi},$$

which proves (1.15). □

**Remark 1.15.** Note that Stirling's formula was actually proved by Abraham de Moivre (1667–1754, France) and later improved by James Stirling (1692–1770, Scotland), who established the value of the constant $c$. Moreover, note that it is also possible to prove the following bounds:

$$1 \leq \frac{n!}{n^n e^{-n}\sqrt{2\pi n}} \leq e^{1/12n} \qquad (n \geq 1) \tag{1.17}$$

(see Problem 1.15).

## 1.10. Basic inequalities

Two very useful inequalities are the *Arithmetic Geometric Mean inequality* (AGM inequality for short) and the *Cauchy-Schwarz inequality*, which we state respectively as follows.

**Proposition 1.16.** *(AGM inequality) Given positive numbers $x_1, \ldots, x_r$,*

$$\left(\prod_{i=1}^{r} x_i\right)^{1/r} \leq \frac{1}{r}\left(\sum_{i=1}^{r} x_i\right), \tag{1.18}$$

*where equality holds if and only if $x_1 = x_2 = \cdots = x_r$.*

**Proof.** We give here a proof due to Pólya. It is based on the inequality $e^x \geq 1 + x$ which is easily shown to be valid for all $x \in \mathbb{R}$, with equality if and only if $x = 0$. Given $x_1, \ldots, x_r \in \mathbb{R}_+$, let $M$ and $P$ stand for their arithmetic and geometric mean, respectively. If $x_1 = x_2 = \ldots = x_r$, then $M = P$ and we are done with the last claim. Therefore, it remains to prove that $P < M$ if we assume that the $x_i$'s are not all equal. Note that $M > 0$. In the inequality $e^x \geq 1 + x$, replace $x$ by $x_i/M - 1$, so that

$$\exp\left\{\frac{x_i}{M} - 1\right\} \geq \frac{x_i}{M} \qquad \text{for } i = 1, 2, \ldots, r. \tag{1.19}$$

Now, since the $x_i$'s are not all equal, it follows that $x_j > M$ for at least one $j \in [1, r]$, implying that $x_j/M - 1 > 0$. This means that at least one of the inequalities in (1.19) is strict. Therefore, multiplying all the inequalities in (1.19), we get

$$\begin{aligned}
\prod_{i=1}^{r} \exp\left\{\frac{x_i}{M} - 1\right\} &> \prod_{i=1}^{r} \frac{x_i}{M} \quad , \\
\exp\left\{\frac{1}{M}\sum_{i=1}^{r} x_i - \sum_{i=1}^{r} 1\right\} &> \frac{1}{M^r}\prod_{i=1}^{r} x_i \quad , \\
e^{r-r} &> \frac{P^r}{M^r} \quad ,
\end{aligned}$$

implying that $M > P$, which is what we wanted to prove. □

**Proposition 1.17.** *(Cauchy-Schwarz inequality) Given two sets of real numbers $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$,*

$$\left(\sum_{i=1}^{k} a_i b_i\right)^2 \leq \left(\sum_{i=1}^{k} a_i^2\right)\left(\sum_{i=1}^{k} b_i^2\right). \tag{1.20}$$

**Proof.** This result can be proved by noticing that the quadratic polynomial

$$t^2\left(\sum_{i=1}^{k} a_i^2\right) - 2t\left(\sum_{i=1}^{k} a_i b_i\right) + \left(\sum_{i=1}^{k} b_i^2\right) = \sum_{i=1}^{k} (a_i t - b_i)^2$$

is nonnegative for all real $t$, so that its discriminant is $\leq 0$, that is,

$$4\left(\sum_{i=1}^{k} a_i b_i\right)^2 - 4\left(\sum_{i=1}^{k} a_i^2\right)\left(\sum_{i=1}^{k} b_i^2\right) \leq 0,$$

which is precisely what needed to be proved. □

## Problems on Chapter 1

**Problem 1.1.** *Use Proposition* 1.1 *to prove that if* $\alpha \geq 0$, *then*

$$\sum_{n\leq x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O\left(x^\alpha\right).$$

**Problem 1.2.** *Prove that*

$$\lim_{N\to\infty} \frac{1^3+2^3+3^3+4^3+\cdots+N^3}{N^4} = \frac{1}{4}.$$

**Problem 1.3.** *Use relation* (1.1) *to prove that if* $\alpha > 0$, *then*

$$\sum_{n\leq x} n^\alpha \log n = \frac{x^{\alpha+1}}{\alpha+1}\left(\log x - \frac{1}{\alpha+1}\right) + O\left(x^\alpha \log x\right).$$

**Problem 1.4.** *Show that the following two representations of the Euler constant* $\gamma$ *are actually the same:*

$$\lim_{N\to\infty}\left(\sum_{n=1}^{N}\frac{1}{n} - \log N\right) \qquad \textit{and} \qquad 1 - \int_1^\infty \frac{t-\lfloor t\rfloor}{t^2}\,dt.$$

**Problem 1.5.** *Let* $f:\mathbb{N}\to\mathbb{C}$ *be a function for which there exists a positive constant* $A$ *such that* $\lim_{x\to\infty}\frac{1}{x}\sum_{n\leq x} f(n) = A$. *Prove that*

$$\sum_{n\leq x} f(n)\log n = A(1+o(1))x\log x \qquad (x\to\infty).$$

**Problem 1.6.** *Let* $f:[a,b]\to\mathbb{R}$ *be a function which is continuous at* $x=a$. *Define* $g:[a,b]\to\mathbb{R}$ *by*

$$g(x) = \begin{cases} 0 & \text{if } x = a, \\ 1 & \text{if } a < x \leq b. \end{cases}$$

*Prove that*

$$\int_a^b f\,dg = f(a).$$

**Problem 1.7.** *Let $f : [a,b] \to \mathbb{R}$ be a function continuous at the point $c \in (a,b)$. Consider the function $g : [a,b] \to \mathbb{R}$ defined by*

$$g(x) = \begin{cases} 0 & \text{if } a \le x \le c, \\ 1 & \text{if } c < x \le b. \end{cases}$$

*Prove that*

$$\int_a^b f\, dg = f(c).$$

**Problem 1.8.** *Let $a < c_1 < c_2 < c_3 < b$ and let $f : [a,b] \to \mathbb{R}$ be a function which is continuous at the points $c_i$ $(i = 1,2,3)$. Moreover, let $\beta_1, \beta_2, \beta_3, \beta_4 \in \mathbb{R}$ and let $g : [a,b] \to \mathbb{R}$ be defined by*

$$g(x) = \begin{cases} \beta_1 & \text{if } a \le x \le c_1, \\ \beta_2 & \text{if } c_1 < x \le c_2, \\ \beta_3 & \text{if } c_2 < x \le c_3, \\ \beta_4 & \text{if } c_3 < x \le b. \end{cases}$$

*Show that*

$$\int_a^b f\, dg = (\beta_2 - \beta_1) f(c_1) + (\beta_3 - \beta_2) f(c_2) + (\beta_4 - \beta_3) f(c_3).$$

**Problem 1.9.** (a) *Using definition (1.7) or (1.8), prove that the following functions belong to the set of slowly oscillating functions $\mathcal{L}$:*

$$\log x, \quad \log^3 x, \quad e^{\sqrt{\log x}}.$$

(b) *Prove that the following functions do not belong to $\mathcal{L}$:*

$$\frac{1}{x}, \qquad \sin x.$$

(c) *Prove that the following functions are regularly varying:*

$$x^2 \log x, \qquad \frac{x}{\log x}, \qquad x^{1+1/x}.$$

**Problem 1.10.** *Consider the function $f : \mathbb{N} \to \{0,1\}$ defined by $f(1) = 1$ and, for each integer $n \ge 2$, by*

$$f(n) = \begin{cases} 1 & \text{if } 2^{2m} < n \le 2^{2m+1}, \\ 0 & \text{if } 2^{2m+1} < n \le 2^{2m+2}. \end{cases}$$

*Show that the set $A = \{n \in \mathbb{N} : f(n) = 1\}$ does not have a density.*

**Problem 1.11.** *Let $A \subset \mathbb{N}$ be a set of zero density and let $a_1$ be its smallest element. Also, let $L : [a_1, +\infty) \to \mathbb{R}_+$ be an increasing function which is continuous and differentiable on $[a_1, +\infty)$. Assume moreover that $L'(x) = O(1)$. Prove that the following two statements are equivalent:*

(a) $\displaystyle\sum_{\substack{a\le x\\ a\in A}} L(a) = (1+o(1))x \quad \text{as } x\to\infty,$

(b) $\displaystyle A(x) = (1+o(1))\int_{a_1}^{x} \frac{dt}{L(t)} \quad \text{as } x\to\infty.$

**Problem 1.12.** *Let $L : [M,+\infty) \to \mathbb{R}_+$, where $M > 0$. Assume that $L \in \mathcal{C}[M,+\infty)$. Prove that*

$$L \in \mathcal{L} \Longleftrightarrow \int_M^x \frac{dt}{L(t)} = (1+o(1))\frac{x}{L(x)} \quad \text{as } x\to\infty.$$

**Problem 1.13.** *Let $A \subset \mathbb{N}$, with $a_1$ being its smallest element. Let $L : [a_1,+\infty) \to \mathbb{R}_+$ be an increasing slowly oscillating function. Prove that*

$$\lim_{x\to\infty} \frac{1}{x} \sum_{\substack{a\le x\\ a\in A}} L(a) = 1 \Longleftrightarrow \lim_{x\to\infty} \frac{L(x)}{x} \sum_{\substack{a\le x\\ a\in A}} 1 = 1.$$

**Problem 1.14.** *Let $A = \{p : p+2 \text{ is prime}\}$. It is conjectured that $A(x) \sim Cx/\log^2 x$ (as $x\to\infty$) for a certain positive constant $C$. Use the preceding problem to show that this conjecture implies that*

$$\sum_{\substack{p\le x\\ p+2 \text{ prime}}} \frac{1}{C}\log^2 p = (1+o(1))x \qquad (x\to\infty).$$

**Problem 1.15.** *Prove that*

$$1 \le \frac{n!}{n^n e^{-n}\sqrt{2\pi n}} \le e^{1/12n} \qquad (n\ge 1).$$

*Chapter 2*

# Prime Numbers and Their Properties

## 2.1. Prime numbers and their polynomial representations

Let $p_1 < p_2 < \cdots < p_n < \cdots$ be the sequence of all prime numbers. Does there exist a formula which gives the $n$-th prime number? Yes, there is! In fact, there are many! But none of them are interesting. For example, let us examine the following particular formula for the $n$-th prime, namely

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \left\lfloor \frac{n}{1+\pi(m)} \right\rfloor^{1/n} \right\rfloor.$$

(Here, $\pi(x)$ stands for the number of prime numbers $\leq x$.) In the case $n = 2$, we have

$$p_2 = 1 + \left\lfloor \left\lfloor \frac{2}{1+\pi(1)} \right\rfloor^{1/2} \right\rfloor + \left\lfloor \left\lfloor \frac{2}{1+\pi(2)} \right\rfloor^{1/2} \right\rfloor + 0 + 0 = 1 + 1 + 1 = 3.$$

Clearly, this is kind of useless since in order to obtain the value of the $n$-th prime, one must know in advance the values of $\pi(1)$, $\pi(2)$, ..., $\pi(2^n)$.

The "$n$-th prime number" function can also be provided by a polynomial, but not by a polynomial in one variable.

Indeed, one may ask if there exists a nonconstant polynomial $f(X) \in \mathbb{Z}[X]$ such that $f(n)$ represents a prime number for each integer $n \geq 0$. The answer is NO. In order to prove this, assume that $f(X)$ is such a polynomial. Choose your favorite positive integer $n_0$ and compute $p = f(n_0)$. Since

$$f(n_0 + kp) \equiv f(n_0) \pmod{p}$$

for all integers $k \geq 0$, we easily obtain that $p \mid f(n_0+kp)$ for all $k \geq 0$. Since $f$ takes on only prime values, it follows that $f(n_0+kp) = p$. This establishes that the polynomial equation $f(X) - p = 0$ has infinitely many solutions $X$, including the numbers of the form $X = n_0 + kp$, where $k = 0, 1, 2, \ldots$, which is impossible since a nonconstant polynomial can have at most a finite number of zeros. This proves that the polynomial $f(X) - p$ must be the constant polynomial 0, thus implying that $f(X)$ is always $p$, a contradiction.

Building on the ideas of Matijasievič, the mathematicians Jones, Sato, Wada, and Wiens [**90**] found a polynomial of degree 25 in 26 variables conveniently labeled $f(a, b, c, \ldots, z)$ such that when nonnegative integers are substituted for all the variables, the positive values of $f$ coincide exactly with the set of all prime numbers. Here is their polynomial $f(a, b, c, d, \ldots, z)$:

$$\begin{aligned}
& (k+2)\{1 - [wz + h + j - q]^2 - [(gk + 2g + k + 1)(h + j) + h - z]^2 \\
- \ & [2n + p + q + z - e]^2 - [16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2 \\
- \ & [e^3(e+2)(a+1)^2 + 1 - o^2]^2 - [(a^2-1)y^2 + 1 - x^2]^2 \\
- \ & [16r^2y^4(a^2-1) + 1 - u^2]^2 \\
- \ & [((a + u^2(u^2-a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu^2)^2]^2 \\
- \ & [n + l + v - y]^2 - [(a^2-1)l^2 + 1 - m^2]^2 \\
- \ & [ai + k + 1 - l - i]^2 \\
- \ & [p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 \\
- \ & [q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 \\
- \ & [z + pl(a - p) + t(2ap - p^2 - 1) - pm]^2\}.
\end{aligned}$$

Polynomials with the same property but fewer variables (for example, 12) are known although the minimal number of variables needed for such a polynomial is not known.

The number $n^2 + n + 41$ is prime for $n = 0, 1, \ldots, 39$ and in fact $(n - 40)^2 + (n - 40) + 41$ is prime for $n = 0, 1, \ldots, 79$.

Is it true that for each positive integer $k$ there exists a nonconstant polynomial $f(X) \in \mathbb{Z}[X]$ such that $f(n)$ is prime for all $n = 0, 1, \ldots, k-1$? The answer is YES. Is it possible to construct such a polynomial? Green and Tao (who was awarded the Fields Medal in 2006) showed [**70**] that the answer is YES, even with a linear polynomial $f(X)$. More precisely, given $k$, they showed that there exist positive integers $a$ and $b$ such that all of the numbers $a,\ a + b,\ a + 2b,\ \ldots,\ a + (k-1)b$ are prime.

Is $n^2 + 1$ a prime for infinitely many positive integers $n$? The answer is almost certainly YES, but this has not been proved yet. The best result in this direction is that $n^2 + 1$ is a $P_2$ for infinitely many positive integers

$n$. A number $m$ is called a $P_k$ (here, $k$ is a positive integer) if $m = q_1 \cdots q_j$ for some integer $j \leq k$ and some primes $q_1 \leq q_2 \leq \cdots \leq q_j$. There is no polynomial $f(X) \in \mathbb{Z}[X]$ of degree $> 1$ for which it has been proved that the set

$$\mathcal{P}_f = \{n \in \mathbb{N} : f(n) \text{ is prime}\} \tag{2.1}$$

is infinite. Note that it is easy to give examples of polynomials $f(X) \in \mathbb{Z}[X]$ for which the set $\mathcal{P}_f$ appearing in (2.1) is empty (take $f(X) = X^2$, for example). On the other hand, this is known for polynomials of degree 1. Namely, if $a$ and $b$ are coprime positive integers, then there are infinitely many primes of the form $an + b$. This is Dirichlet's theorem. We will prove it in Chapter 14.

## 2.2. There exist infinitely many primes

It has been known for 2300 years that there exist infinitely many primes. The first proof is due to Euclid.

**Theorem 2.1.** *There exist infinitely many prime numbers.*

**Proof.** *(Euclid)* Assume the contrary, that is, that there exist only a finite number of primes, say $p_1 < p_2 < \cdots < p_k$. Then, consider the number

$$N = p_1 p_2 \cdots p_k + 1. \tag{2.2}$$

If $N$ is prime, then we have found a prime number which is larger than $p_k$, thus a contradiction. On the other hand, if $N$ is composite, then $N$ is divisible by a prime number, and since $p_1, p_2, \ldots, p_k$ are the only existing primes, it follows that there exists an index $i$ $(1 \leq i \leq k)$ such that $p_i | N$. But then it follows from (2.2) that $p_i | 1$, which is also a contradiction. □

## 2.3. A first glimpse at the size of $\pi(x)$

Using Euclid's proof, one can already obtain a lower bound for the expression $\pi(x)$. Indeed, let us show that

$$p_k \leq 2^{2^{k-1}} \qquad \text{for } k = 1, 2, \ldots \tag{2.3}$$

To do so, we use induction on $k$. For $k = 1$, it is clear that $2 = p_1 = 2^{2^{1-1}}$, in which case inequality (2.3) is proved. Assume now that $k \geq 1$ and that (2.3) holds for $j = 1, \ldots, k$. Using Euclid's argument, we have, by the induction hypothesis,

$$p_{k+1} \leq p_1 \cdots p_k + 1 \leq 2^{2^0 + 2^1 + \cdots + 2^{k-1}} + 1 = 2^{2^k - 1} + 1 = \frac{2^{2^k}}{2} + 1 < 2^{2^k},$$

which completes the induction and proves (2.3). Now let $x \geq 2$. There exists a positive integer $\ell$ such that

$$2^{2^{\ell-1}} \leq x < 2^{2^{\ell}}.$$

Calling upon inequality (2.3), we have $p_\ell \leq 2^{2^{\ell-1}}$, so that $\pi(x) \geq \ell$. Taking logarithms on both sides of the inequality $2^{2^{\ell}} > x$, we first obtain that

$$2^{\ell} > \frac{\log x}{\log 2},$$

and thereafter that

$$\ell > \frac{\log(\log x/\log 2)}{\log 2} = \frac{1}{\log 2}(\log\log x - \log\log 2).$$

Since $\log 2 < 1$, we obtain that $-\log\log 2 > 0$ and $1/\log 2 > 1$. Therefore,

$$\pi(x) > \log\log x \qquad \text{for all } x \geq 2.$$

A more direct proof of this result is the following. First we observe that

$$2 \geq \frac{p}{p-1} = \left(1 - \frac{1}{p}\right)^{-1} \qquad \text{for all primes } p.$$

Using the well-known fact that

$$\frac{1}{1-z} = 1 + z + z^2 + \cdots \qquad \text{for } |z| < 1,$$

and the *Fundamental theorem of arithmetic* (which establishes the uniqueness of the prime factorization of each integer), we obtain

$$\begin{aligned} 2^{\pi(x)} &\geq \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \leq x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \\ &\geq \sum_{n \leq x} \frac{1}{n} \geq \int_1^{\lfloor x \rfloor + 1} \frac{dt}{t} = \log(\lfloor x \rfloor + 1) > \log x, \end{aligned}$$

so that

$$\pi(x) > \frac{\log\log x}{\log 2} > \log\log x.$$

## 2.4. Fermat numbers

The numbers mentioned in the title of this section were first studied by Pierre de Fermat (1601–1655, France), who originally conjectured that all numbers of the form $2^{2^n} + 1$, where $n = 0,\ 1, \ldots$, are prime numbers. He did indeed verify his statement for $n = 0,\ 1,\ 2,\ 3,\ 4$. Today, numbers of the form $2^{2^n} + 1$ are called *Fermat numbers* and they are denoted by $F_n$.

In 1732, Leonhard Euler (1707–1783, Switzerland) proved that $641 \mid F_5$, thereby disclaiming Fermat's assertion. One can easily check Euler's result without the use of a computer: indeed, first observe that $641 = 2^7 \cdot 5 + 1$, so that $2^7 \cdot 5 \equiv -1 \pmod{641}$; raising both sides of this congruence to the fourth power, we obtain $2^{28} \cdot 5^4 \equiv 1 \pmod{641}$. Using also the fact that $641 = 5^4 + 2^4$, we have that $5^4 \equiv -2^4 \pmod{641}$, from which it follows that $2^{28}(-2^4) \equiv 1 \pmod{641}$, implying that $641 \mid F_5$. We know today that $F_6, \ldots, F_{32}$ as well as many other Fermat numbers are composite. The status of $F_{33}$ is still unknown. Most mathematicians believe that $F_n$ is composite for each $n \geq 5$. Curiously, for certain composite Fermat numbers, no prime factor is known: this is the case for $F_{14}$, a 4933-digit number. In fact, Selfridge offers a \$500 prize to anyone who comes up with a prime factor of $F_{14}$.

Below is a table of the factorizations of the Fermat numbers $F_n = 2^{2^n} + 1$ for $n = 1, 2, \ldots, 11$, namely all those for which the complete factorization is known.

| $k$ | $F_k$ |
|---|---|
| 1 | 5 |
| 2 | 17 |
| 3 | 257 |
| 4 | 65537 |
| 5 | $641 \cdot 6700417$ |
| 6 | $274177 \cdot 67280421310721$ |
| 7 | $59649589127497217 \cdot 5704689200685129054721$ |
| 8 | 1238926361552897 |
| | $\cdot 93461639715357977769163558199606896584051237541638188580280321$ |
| 9 | $2424833 \cdot 7455602825647884208337395736200454918783366342657 \cdot P_{99}$ |
| 10 | $45592577 \cdot 6487031809$ |
| | $\cdot 4659775785220018543264560743076778192897 \cdot P_{252}$ |
| 11 | $319489 \cdot 974849 \cdot 167988556341760475137$ |
| | $\cdot 3560841906445833920513 \cdot P_{564}$ |

(Here $P_k$ stands for a $k$-digit prime number which can be obtained explicitly.)

**Theorem 2.2.** *If $0 \leq n < m$, then $(F_n, F_m) = 1$.*

**Proof.** We will show that $F_n \mid F_m - 2$. Indeed,

$$\begin{aligned} F_m - 2 &= 2^{2^m} - 1 = (2^{2^{m-1}} + 1)(2^{2^{m-1}} - 1) = F_{m-1}(2^{2^{m-1}} - 1) \\ &= F_{m-1}F_{m-2}(2^{2^{m-2}} - 1) = \cdots = F_{m-1}F_{m-2}\cdots F_0, \end{aligned}$$

which certainly implies that $F_n \mid F_m - 2$. It then follows that $F_n$ and $F_m$ are coprime, since if $p$ was one of their common prime divisor, then since

$p \mid F_n \mid F_m - 2$ and $p \mid F_m$, we would obtain that $p \mid 2$, which is impossible since $F_n$ is odd. □

**Remark 2.3.** *Noting that $p_1 = 2$ does not divide any Fermat number, we immediately get that $p_n \le F_{n-2}$ holds for all $n \ge 2$, which easily leads to $p_n \le 2^{2^{n-1}}$ for all $n \ge 1$. For other properties of the Fermat numbers, see* [**93**]*, a book with 3 authors, 17 chapters, 257 pages, etc.*

## 2.5. A better lower bound for $\pi(x)$

We now prove a better lower bound for $\pi(x)$.

**Theorem 2.4.** *For $x \ge 2$ we have*

$$\pi(x) \ge \frac{\log\lfloor x \rfloor}{2\log 2},$$

*and for $n \ge 1$ we have $p_n \le 4^n$.*

**Proof.** Let $x \ge 1$ be an integer and $2 = p_1 < p_2 < \cdots < p_j \le x$ be all the primes $\le x$. Write each integer $n \le x$ as $n = \ell^2 \cdot m$, where $m$ is squarefree and $\ell$ some positive integer. Thus,

$$m = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_j^{\varepsilon_j},$$

where $\varepsilon_i \in \{0, 1\}$ for all $i = 1, \ldots, j$.

There are $x$ possible values for $n$.

Since $\ell^2 \le n \le x$, we get that $\ell \le \sqrt{x}$. Hence, there are at most $\sqrt{x}$ possibilities for $\ell$. On the other hand, there are at most $2^j$ possibilities for $m$. Hence,

$$x \le \sqrt{x}\, 2^j,$$

which leads to $2^j \ge \sqrt{x}$, or $j \ge \log(\sqrt{x})/\log 2 = \log x/(2\log 2)$. All is left to notice is that $j = \pi(x)$. Taking $x = p_n$, we get that $j = n$ and therefore that $2^n \ge \sqrt{p_n}$, which implies the second inequality. □

**Remark 2.5.** Observe that the above proof clearly provides another proof that the number of primes is infinite.

## 2.6. The Chebyshev estimates

As we mentioned in the preface, in 1896, Charles-Jean de la Vallée Poussin (1866–1962, Belgium) and Jacques Hadamard (1865–1963, France) proved

independently the *Prime Number Theorem*. More precisely, they showed that

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1,$$

a result which had previously been suggested by Euler, Gauss, and Legendre.

Indeed, the history of the Prime Number Theorem is quite fascinating. As early as 1762, Leonhard Euler (1707–1783, Switzerland) stated that $\pi(x)$ was approximately equal to $x/\log x$. In 1792, at the age of 15, Carl Friedrich Gauss (1777–1855, Germany) made the same assertion by writing it in a margin of the mathematical tables of Schulze. In 1798, Adrien-Marie Legendre (1752–1833, France) conjectured a fairly good approximation of $\pi(x)$ by claiming that there existed two constants $A$ and $B$ such that

$$\pi(x) \quad \text{is close to} \quad \frac{x}{A\log x + B} \tag{2.4}$$

and he later (in 1808) proposed the constants $A = 1$ and $B = -1.08366$. Mathematicians later discovered that he was not too far off since one can prove that in fact

$$\pi(x) \sim \frac{x}{\log x - 1} \qquad (x \to \infty) \tag{2.5}$$

(see Problem 2.24).

It is often mentioned that Gauss was the first to write that the *logarithmic integral* defined by

$$\mathrm{li}(x) = \lim_{\varepsilon\to 0}\left(\int_0^{1-\varepsilon} + \int_{1+\varepsilon}^{x}\right)\frac{dt}{\log t} = \int_2^x \frac{dt}{\log t} - 1.04\ldots \tag{2.6}$$

was a good approximation for $\pi(x)$. But Narkiewicz writes in his book [**110**] that $\pi(x) \sim \mathrm{li}(x)$ was mentioned for the first time in a letter of F. W. Bessel (1784–1846, Germany) to W. Olbers (1758–1840, Germany), both astronomers, and that Gauss never published anything on that subject[1].

The first significant step towards the proof of the Prime Number Theorem was made by Pafnuty Lvovich Chebyshev (1821–1894, Russia). He proved that if the function $\pi(x)/(x/\log x)$ has a limit as $x \to \infty$, then this limit has to be equal to 1. However, Chebyshev is more famous for having established very accurate lower and upper bounds for $\pi(x)$. More precisely, in 1850, he proved that the inequalities

$$c_1\frac{x}{\log x} \le \pi(x) \le c_2\frac{x}{\log x} \tag{2.7}$$

[1] However, in a letter to his student Johann Franz Encke, dated December 24, 1849, Gauss recalled his belief based on the examination of the table of all primes $\le 3\,000\,000$, made several years earlier, that $\pi(x)$ is well approximated by $x/\log x$ and that even a better approximation is given by $\mathrm{li}(x)$.

hold for all $x \geq 10$, where $c_1 = \log(2^{1/2}3^{1/3}5^{1/5}/30^{1/30}) \approx 0.921292$ and $c_2 = 6c_1/5 \approx 1.1055$. Inequalities (2.7) are called *Chebyshev inequalities*; at times, they are referred to as the *Chebyshev theorem* or the *Chebyshev estimates*. Here, we prove something somewhat weaker than (2.7) by using a method which is easier than Chebyshev's. The following proof is due to Erdős.

**Theorem 2.6.** *For $x \geq 2$,*

$$\left(\frac{3\log 2}{8}\right)\frac{x}{\log x} < \pi(x) < (6\log 2)\frac{x}{\log x}.$$

To prove this theorem we need the following lemma.

**Lemma 2.7.** *Let $p$ be a prime and $e_p(n!)$ be the exponent at which $p$ appears in the factorization of $n!$. Then*

$$e_p(n!) = \sum_{k\geq 1}\left\lfloor \frac{n}{p^k}\right\rfloor.$$

**Proof.** We use induction on $n$. The formula is clearly true if $n = 1$ for all $p$. Assume that it holds for $n$ and write $n+1 = p^u m$, where $p \nmid m$. Then, by the induction hypothesis,

$$e_p((n+1)!) = e_p(n!) + u = \sum_{k=1}^{u}\left(\left\lfloor \frac{n}{p^k}\right\rfloor + 1\right) + \sum_{k>u}\left\lfloor \frac{n}{p^k}\right\rfloor.$$

All is left to observe is that

$$\left\lfloor \frac{n+1}{p^k}\right\rfloor = \left\lfloor \frac{n}{p^k}\right\rfloor + 1 \quad \text{if } 1 \leq k \leq u \quad \text{and} \quad \left\lfloor \frac{n+1}{p^k}\right\rfloor = \left\lfloor \frac{n}{p^k}\right\rfloor \quad \text{if } k > u.$$

□

*Proof of Theorem* 2.6. We first prove the lower bound on $\pi(x)$. We start with the observation that

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \quad \text{divides} \quad \prod_{p<2n} p^{r_p} \tag{2.8}$$

if $n > 1$, where $r_p$ is the unique integer satisfying $p^{r_p} \leq 2n < p^{r_p+1}$. Indeed, to prove divisibility property (2.8), observe that the exponent at which $p$ appears in the binomial coefficient $\binom{2n}{n}$ equals

$$e_p((2n)!) - e_p((n!)^2) \;=\; e_p((2n)!) - 2e_p(n!) = \sum_{k\geq 1}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right).$$

Divisibility relation (2.8) follows now by observing that $\lfloor 2y\rfloor - 2\lfloor y\rfloor \in \{0,1\}$ holds for all real numbers $y$ (when is it zero and when is it 1 ?), together

with the fact that when $k > r_p$, we have $p^k > 2n$, so that both $\lfloor 2n/p^k \rfloor = 0$ and $\lfloor n/p^k \rfloor = 0$ hold for such values of $k$.

The divisibility relation (2.8) certainly implies that

$$\binom{2n}{n} \leq (2n)^{\pi(2n)}.$$

On the other hand, since

$$(1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k}$$

and since

$$\binom{2n}{n} \geq \binom{2n}{k} \qquad \text{for } \ k = 0, 1, \ldots, 2n,$$

we obtain that

$$\binom{2n}{n} > \frac{2^{2n}}{2n+1}.$$

Using induction, one can verify that the inequality

$$\frac{2^{2n}}{2n+1} > 2^n \qquad \text{holds for all } n \geq 3.$$

This is why, if $n \geq 3$, we have

$$2^n < \frac{2^{2n}}{2n+1} < \binom{2n}{n} \leq (2n)^{\pi(2n)},$$

so that taking logarithms on each side, we obtain

$$\pi(2n) > \frac{\log(2^n)}{\log 2n} = \left(\frac{\log 2}{2}\right) \cdot \frac{2n}{\log(2n)}.$$

Assume now that $x \geq 8$ and let $n$ be the unique positive integer satisfying $2n \leq x < 2n+2$. It is clear that $n \geq 3$. Moreover, we have $2n > x-2 \geq 3x/4$ (since $x \geq 8$). The function $y \mapsto y/\log y$ is increasing for $y > e$ (to see this, one only needs to study the sign of its derivative!) and $3x/4 \geq 6 > e$ when $x \geq 8$. Combining these results, we obtain that if $x \geq 8$, we have

$$\pi(x) \geq \pi(2n) \geq \left(\frac{\log 2}{2}\right) \cdot \frac{2n}{\log(2n)} \geq \left(\frac{\log 2}{2}\right) \cdot \frac{3x/4}{\log(3x/4)} > \left(\frac{3\log 2}{8}\right) \cdot \frac{x}{\log x},$$

which is the required lower bound in the case $x \geq 8$. One easily verifies that this bound also holds for $x \in [2, 8)$.

Let us now examine the upper bound. First it is clear that

$$\prod_{n<p\leq 2n} p \,\Big|\, \binom{2n}{n}.$$

Therefore,

$$\prod_{n<p\le 2n} p < (1+1)^{2n} = 2^{2n},$$

so that taking logarithms, we obtain

$$\pi(2n)\log n - \pi(n)(\log(n/2) + \log 2) < 2n\log 2.$$

Hence,

$$\pi(2n)\log n - \pi(n)\log(n/2) < 2n\log 2 + \pi(n)\log 2 \le (3\log 2)n, \tag{2.9}$$

where we used the trivial inequality $\pi(n) \le n$. Now let $f(n) = \pi(2n)\log n$ and observe that inequality (2.9) implies that

$$f(n) - f(n/2) < (3\log 2)n.$$

Let $n = 2^i$ for $i = k, k-1, \ldots 3, 2$. We then have

$$\begin{aligned} f(2^k) - f(2^{k-1}) &< (3\log 2)\,2^k \\ f(2^{k-1}) - f(2^{k-2}) &< (3\log 2)\,2^{k-1} \\ &\vdots \\ f(4) - f(2) &< (3\log 2)\,4. \end{aligned} \tag{2.10}$$

Adding all inequalities (2.10), we obtain

$$\begin{aligned} \pi(2^{k+1})\log(2^k) = f(2^k) &< (3\log 2)(4+8+\cdots+2^k) + f(2) \\ &= (3\log 2)(4+8+\cdots+2^k) + \pi(4)\log 2 \\ &< (3\log 2)(1+4+8+\cdots+2^k) \\ &< (3\log 2)\,2^{k+1}, \end{aligned}$$

so that

$$\pi(2^{k+1}) < (6\log 2)\left(\frac{2^k}{\log(2^k)}\right).$$

Now given $x \ge 2$, choose $k \ge 1$ in such a way that $2^k \le x < 2^{k+1}$. If $x \ge 4$, then $k \ge 2$ and therefore $2^k \ge 4 > e$. Thus, $2^k/\log(2^k) \le x/\log x$ when $x \ge 4$. We have thus obtained

$$\pi(x) \le \pi(2^{k+1}) < (6\log 2)\left(\frac{2^k}{\log(2^k)}\right) < (6\log 2)\frac{x}{\log x}$$

for $x \ge 4$. Finally, one easily verifies that this upper bound also holds for all $x \in [2, 4)$. □

## 2.7. The Bertrand Postulate

In 1845, Joseph Bertrand (1822–1900, France) proved that given any positive integer $n \leq 6 \cdot 10^6$, there exists at least one prime number in the interval $[n, 2n]$. He conjectured that this was true for any positive integer $n$. Chebyshev proved this conjecture in 1850. Here, we give Erdős' proof. We start with two lemmas.

**Lemma 2.8.** *For each $n \in \mathbb{N}$,*

$$\prod_{p \leq n} p < 4^n. \tag{2.11}$$

**Proof.** We establish inequality (2.11) by induction on $n \geq 1$. Obviously, the result holds for $n = 1$ and $n = 2$. Assume that $n \geq 3$ and that the result holds for each $k \in \{1, 2, \ldots, n-1\}$. First observe that one only needs to consider the case when $n$ is odd, because if $n > 2$ is even, then

$$\prod_{p \leq n} p = \prod_{p \leq n-1} p,$$

in which case the result follows by induction.

We write $n = 2m + 1$ and observe that

$$\prod_{m+1 < p \leq 2m+1} p \,\Big|\, \binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}.$$

Noticing that both $\binom{2m+1}{m}$ and $\binom{2m+1}{m+1}$ appear in the binomial expansion of $(1+1)^{2m+1}$ and that $\binom{2m+1}{m} = \binom{2m+1}{m+1}$, we obtain

$$\binom{2m+1}{m} \leq \frac{1}{2}(2^{2m+1}) = 4^m.$$

Thus, in light of these inequalities and of the induction hypothesis, we obtain

$$\prod_{p \leq 2m+1} p = \left( \prod_{p \leq m+1} p \right) \left( \prod_{m+1 < p \leq 2m+1} p \right) < 4^{m+1} \binom{2m+1}{m} \leq 4^{2m+1},$$

which completes the proof. □

**Lemma 2.9.** *If $n \geq 3$ and $p$ is a prime number with $2n/3 < p \leq n$, then $p$ does not divide $\binom{2n}{n}$.*

**Proof.** Assume that $n \geq 3$ and that $2n/3 < p \leq n$. Obviously, $p > 2$. We then have that $p$ and $2p$ are the only multiples of $p$ which are $\leq 2n$ (since $3p > 2n$). Therefore, $p^2 \,\|\, (2n)!$. Moreover, $p \mid n!$ because $p \leq n$. Since $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$, we see that $\binom{2n}{n}$ is not a multiple of $p$. □

**Theorem 2.10.** *(Bertrand Postulate) For each positive integer $n$, there exists a prime number $p$ such that $n < p \leq 2n$.*

**Proof.** First observe that the result is true for $n = 1, 2, 3$. Assume that it is false for a certain $n \geq 4$. Then, in light of Lemma 2.9, each prime number $p$ which divides $\binom{2n}{n}$ is $\leq 2n/3$.

Let $p$ be such a prime number and assume that $p^\alpha \parallel \binom{2n}{n}$. Then, as in the proof of Theorem 2.6, we have $\alpha \leq r_p$, so that $p^\alpha \leq p^{r_p} \leq 2n$. Moreover, it is clear that if $\alpha \geq 2$, then $p^2 \leq p^\alpha \leq 2n$, so that $p \leq \sqrt{2n}$. Thus,

$$\begin{aligned}\binom{2n}{n} &\leq \left(\prod_{p\leq 2n/3} p\right)\left(\prod_{p\leq\sqrt{2n}} p^{r_p-1}\right) \leq \left(\prod_{p\leq 2n/3} p\right)(2n)^{\pi(\sqrt{2n})} \\ &\leq 4^{2n/3}(2n)^{\sqrt{2n}},\end{aligned} \tag{2.12}$$

where again we called upon Lemma 2.9 and the trivial inequality $\pi(\sqrt{2n}) \leq \sqrt{2n}$. However, since $\binom{2n}{n}$ is the largest of the $2n+1$ terms in the binomial expansion of $(1+1)^{2n}$, we also have

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n+1}. \tag{2.13}$$

It then follows from inequalities (2.12) and (2.13) that

$$\frac{4^n}{2n+1} \leq 4^{2n/3}(2n)^{\sqrt{2n}},$$

which implies that

$$4^{n/3} \leq (2n)^{\sqrt{2n}}(2n+1) < (2n)^{\sqrt{2n}+2}.$$

Taking logarithms we find that

$$\frac{2n\log 2}{3} < (\sqrt{2n}+2)\log(2n).$$

Setting $y = \sqrt{2n}$, this last inequality becomes

$$\frac{y^2\log 2}{3} - 2(y+2)\log y < 0. \tag{2.14}$$

Let

$$f(y) = \frac{y^2\log 2}{3} - 2(y+2)\log y.$$

Observe that if $y > 32$, then

$$f'(y) = \frac{2y\log 2}{3} - 2\left(1+\frac{2}{y}\right) - 2\log y > \frac{2y\log 2}{3} - 2.2 - 2\log y.$$

Finally, setting $g(y) = 2y(\log 2)/3 - 2.2 - 2\log y$, so that $g'(y) = 2(\log 2)/3 - 2/y$ and observing that for $y \geq 32$ we have $g'(y) > 0$, we conclude that $g(y)$ is increasing for these values of $y$. Since $g(32) = 64(\log 2)/3 - 2.2 -$

$10\log 2 = 34(\log 2)/3 - 2.2 > 0$, we obtain that $g(y) > 0$ for $y \geq 32$. In particular, $f'(y) \geq 0$ if $y \geq 32$. Thus, $f(y) \geq f(32)$ if $y \geq 32$. Since $f(32) = 2^{10}(\log 2)/3 - 10 \cdot 34 \log 2 = (1024 - 1020)(\log 2)/3 = 4(\log 2)/3 > 0$, we obtain that $f(y) > 0$ for $y \geq 32$. This argument and inequality (2.14) show that $y < 32$, and therefore that $n < 512$.

Finally, $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 557$ being all primes, the result is true in general. □

## 2.8. The distance between consecutive primes

Let $2 = p_1 < p_2 < \cdots < p_n < \cdots$ be the sequence of primes. It follows from Theorem 2.10 that $p_{n+1} \leq 2p_n$, in which case $p_{n+1} - p_n \leq p_n$. By a probabilistic argument, Cramer [**26**] was led in 1936 to conjecture that

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^2} \leq 1.$$

The best-known upper bound for $p_{n+1} - p_n$ is $p_{n+1} - p_n < p_n^{0.525}$ for all $n$ sufficiently large, and it was obtained by Baker, Harman, and Pintz [**5**] in 2001.

What about small gaps between consecutive prime numbers? It is conjectured that there exist infinitely many integers $n$ such that $p_{n+1} - p_n = 2$: this is known as the *twin prime conjecture*. If $p$ and $p + 2$ are both prime numbers, then the pair $p, p + 2$ is called a pair of *twin primes*. Assuming that prime numbers are randomly distributed and that a positive integer $n$ is prime with probability $1/\log n$, then one might hope that the probability that $p$ and $p+2$ are simultaneously prime is $1/(\log p)^2$. However, this is not quite so. Indeed, in checking whether $n$ is prime, we need to check that $n$ is not divisible by any prime $q < \sqrt{n}$. However, given a number $p$, the events that $p$ is not a multiple of a prime $q \leq \sqrt{p+2}$ and $p+2$ is not a multiple of $q$ are not independent. For example, if $q = 2$ and $p$ is odd, then automatically $p+2$ is also odd. However, it is believed that up to a *local factor* $C$, encoding the above dependencies of $p$ and $p + 2$ not being multiples of some prime $q$ over all primes $q$, and whose formula is known and will be mentioned in the following section, the number of primes $p \leq x$ such that $p + 2$ is also prime should be approximately $Cx/(\log x)^2$. This is why we believe that there are approximately $x/(\log x)^2$ prime numbers $p \leq x$ with $p + 2$ also being prime.

Until recently we did not even know if

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

But this result has been proved by Goldston, Pintz, and Yildirim [**65**] in 2005. In fact, they showed a stronger result, namely that

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{(\log p_n)^{1/2}(\log\log p_n)^2} < \infty.$$

It is also interesting to mention that, in 1955, Ricci established that the set of cluster points of the sequence $\{(p_{n+1}-p_n)/\log p_n\}_{n\geq 1}$ is of positive measure. Nevertheless, only two such points are known, that is, 0 and 1.

Twenty years before, in 1935, Erdős [**46**] proved that there exists a positive constant $c$ such that the inequality

$$p_{n+1}-p_n > c\log p_n \frac{\log\log p_n}{(\log\log\log p_n)^2}$$

holds for infinitely many positive integers $n$. A few years later, Rankin [**118**] added a $\log\log\log\log p_n$ factor.

All this is a clear indication that there remains a lot of work to do in this area. One of the reasons is that we know few prime numbers, in the sense that

$$\sum_{p \text{ known prime}} \frac{1}{p} < 4 \qquad \text{whereas} \qquad \sum_{\text{all } p} \frac{1}{p} = \infty.$$

## 2.9. Mersenne primes

In the preface to his 1644 book *Cogitata Physica-Matematica*, the priest Marin Mersenne (1588–1648, France) claimed that the primes $p \leq 257$ for which $2^p-1$ is also prime were precisely 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257. The list was incorrect, since $2^{67}-1$ and $2^{257}-1$ are not primes, and moreover, $2^{61}-1$, $2^{89}-1$ and $2^{107}-1$ are also primes. The correct list was obtained only in 1947. Nevertheless, numbers of the form $2^p-1$ are called *Mersenne numbers* and are generally denoted by $M_p$, while primes of the form $2^p-1$ (where $p$ is a prime) are called *Mersenne primes*.

In 1876, Edouard Lucas [**98**] proved that $M_{127}$ is prime. Observe that $M_{127} = 2^{127}-1 > (2^{10})^{12} = (1024)^{12} > 10^{36}$ has more than 36 digits. Lucas discovered a particular property of the Mersenne numbers which he used to design a primality test for such numbers. The largest Mersenne prime numbers were discovered using this method: it is now called the "Lucas-Lehmer Test". In fact, the largest known prime number is a Mersenne number, namely the number $2^{43\,112\,609}-1$, a 12 978 189 digit number, discovered in 2008 as part of the *Great Internet Mersenne Prime Search* (see `www.mersenne.org`). It is the 47th Mersenne prime. Let us mention that a

$150000 prize is offered to the first person who discovers a 100 million digit prime number and $250000 for a billion digit prime number.

There exist very few Mersenne prime numbers. In fact, only 47 have so far been found. In their book [**27**], Crandall and Pomerance provide a heuristic argument (see Problem 5.13) which yields that the number of Mersenne primes $2^p - 1$ with $p \le x$ should be approximately $\dfrac{e^\gamma}{\log 2} \log x + O(1)$. Thus, even though it is believed that there exist infinitely many Mersenne prime numbers, most believe they are quite rare.

Interestingly, not much is known about the size of the largest prime factor of Mersenne numbers. Nevertheless, recently, Ford, Luca, and Shparlinski [**59**] proved that, if $P(k)$ stands for the largest prime factor of $k$, then the series $\displaystyle\sum_{n=1}^{\infty} \frac{(\log n)^\alpha}{P(2^n - 1)}$ is convergent for each $\alpha < 1/2$. The fact that the above series converges for all positive numbers $\alpha$ follows from a recent result of Stewart [**138**].

## 2.10. Conjectures on the distribution of prime numbers

Let $b_1 < \cdots < b_k$ be positive integers. For each prime number $p$, let $\nu(p)$ be the number of distinct residue classes modulo $p$ occupied by the integers $b_1, \ldots, b_k$. In other words, let

$$\nu(p) = \#\{b_i \pmod p \ : \ i = 1, \ldots, k\}.$$

The following conjecture, due to Dickson [**39**], is known as the *Prime k-tuples conjecture.*

**Conjecture 2.11.** *If $\nu(p) < p$ for all prime numbers $p$, then there exist infinitely many positive integers $n$ such that*

$$n + b_1, \ n + b_2, \ \ldots, \ n + b_k \tag{2.15}$$

*are all prime numbers.*

Setting $k = 2, \ b_1 = 0, \ b_2 = 2$, we obtain the twin prime conjecture. Note that the condition $\nu(p) < p$ is necessary if we require that each number in the list (2.15) to be prime for infinitely many integers $n$. Moreover, it is easy to see that it is sufficient to verify this condition only for $p < k$. Some 30 years later, Hardy and Littlewood [**76**] proposed a quantitative version of this conjecture.

Hardy and Littlewood have also conjectured the following inequality.

**Conjecture 2.12.**

$$\pi(x + y) \le \pi(x) + \pi(y) \qquad \textit{for all } x > 1, \ y > 1. \tag{2.16}$$

At first one might think that this inequality follows naturally from the Prime Number Theorem. Indeed, if one naively replaces the $\pi(x)$ function by the function $x/\log x$, inequality (2.16) would then read as follows:

$$\frac{x+y}{\log(x+y)} < \frac{x}{\log x} + \frac{y}{\log y} \qquad \text{for all } x > 1,\ y > 1,$$

which clearly holds. However, in 1972, Hensley and Richards [**81**] surprised the mathematical community by proving that Conjectures 2.11 and 2.12 are incompatible. Their proof goes as follows.

We say that a sequence of positive integers $b_1 < \cdots < b_k$ is *admissible* if $\nu(p) < p$ for all primes $p$. Let

$$\rho^*(y) = \max\{k \in \mathbb{N} \ : \text{sequence} \ \ x < b_1 < \cdots < b_k \le x + y \text{ is admissible}\}.$$

Thus, $\rho^*(y)$ is the maximal length ($\le y$) of an admissible sequence of positive integers that one can insert inside an interval of length $y$. But Hensley and Richards proved that

$$\lim_{y\to\infty} (\rho^*(y) - \pi(y)) = \infty.$$

Assume that $y$ is such that $\rho^*(y) > \pi(y)$ and that the sequence $x < b_1 < \cdots < b_k \le x + y$ is admissible, where $k = \rho^*(y)$. If Conjecture 2.11 is true, then for a certain $n$ we will have that $n + b_1 < \cdots < n + b_k$ are all primes. Since all these belong to $(n + x, n + x + y]$, we obtain that

$$\rho^*(y) = k \le \pi(x + n + y) - \pi(x + n),$$

so that

$$\pi(x + n + y) \ge \pi(x + n) + \rho^*(y) > \pi(x + n) + \pi(y),$$

contradicting inequality (2.16).

Most mathematicians believe that Conjecture 2.11 is true, which would imply that Conjecture 2.12 is false. Some calculations seem to indicate that indeed Conjecture 2.12 could be false. Indeed, in 1979, Vehka showed that there exists a number $x_0$ such that the interval $I = [x_0, x_0 + 11763]$ contains more prime numbers than the interval $[1, 11763]$, since $I$ contains 1412 prime numbers, while $\pi(11763) = 1409$. How large is that number $x_0$? Most likely, very large!

In 1996, in his master's thesis, N. Jarvis proved that the number "11763" can be replaced by "4930". In 1998, Gordon and Rodemich [**67**] showed that the smallest $y$ for which there exists $x_0$ such that the interval $[x_0, x_0 + y]$ contains more prime numbers than the interval $[1, y]$ must be $\ge 1731$. Recently, S. Wagon was able to show that the number "4930" (of Jarvis) can be replaced by "4893". Hence the smallest number $y$ such that the

interval $[x_0, x_0 + y]$ contains more prime numbers than the interval $[1, y]$ must satisfy

$$1731 \leq y \leq 4893. \tag{2.17}$$

Now it is conjectured that the number of $k$-tuples of prime numbers $\leq x$ is of order

$$\int_0^x \frac{dt}{\log^k t} \sim \frac{x}{\log^k x} \qquad \text{as } x \to \infty.$$

Taking $k = \pi(1731) = 269$, we have that

$$\frac{x}{\log^k x} > 1 \quad \text{if} \quad x > 10^{891}.$$

In the end, it follows that in order for (2.17) to hold, we must have that

$$10^{891} < x < 10^{2454},$$

an indication that the value of the number $x_0$ is out of range of today's computational capabilities.

Conjecture 2.11 was generalized by Schinzel in a paper written jointly with Sierpiński [**132**]: it is now called the *Schinzel Hypothesis* or at times *Schinzel's Hypothesis H.*

**Conjecture 2.13.** *Let $f_1(X), \ldots, f_k(X) \in \mathbb{Z}[X]$ be nonconstant polynomials, each one having a positive leading coefficient. Assume that:*

(i) *$f_i(X)$ is irreducible for all $i = 1, \ldots, k$.*

(ii) *there exists no prime number $p$ such that $p \mid f_1(n)f_2(n)\cdots f_k(n)$ for all $n \geq 0$.*

*Then there exist infinitely many positive integers $n$ such that*

$$f_1(n),\ f_2(n),\ \ldots,\ f_k(n)$$

*are all prime numbers.*

Bateman and Horn [**10**] proposed a quantitative version of this conjecture. More precisely, for each prime number $p$, let

$$\omega(p) = \#\{0 \leq n \leq p-1 \ :\ f_1(n)f_2(n)\cdots f_k(n) \equiv 0 \pmod p\},$$

and set

$$\pi_{f_1,\ldots,f_k}(x) = \#\{n \leq x \ :\ f_1(n),\ \ldots,\ f_k(n) \text{ are all primes}\}.$$

Then $\pi_{f_1,\ldots,f_k}(x)$ should be asymptotically equal to

$$C(f_1, \ldots, f_k)\, \frac{1}{d_1 \cdots d_k}\, \frac{x}{(\log x)^k},$$

where $d_i = \deg(f_i)$, and where the constant $C(f_1, \ldots, f_k)$ is given by

$$C(f_1, \ldots, f_k) = \prod_{p \geq 2} \frac{1 - \omega(p)/p}{(1 - 1/p)^k}. \tag{2.18}$$

It is not even clear that in formula (2.18) the expression $C(f_1, \ldots, f_k)$ represents a product which converges to a positive limit. In any event, one can easily show that this is indeed the case when $f_i(X) = a_i X + b_i$ ($a_i > 0$, $\gcd(a_i, b_i) = 1$) is linear for each $i = 1, \ldots, k$, thereby providing an effective form of the Hardy and Littlewood Conjecture 2.11.

It follows from the argument detailed in this section that there are approximately $2Cx/(\log x)^2$ twin prime pairs not exceeding $x$, where

$$C = \prod_{p > 2} \left(1 - \frac{1}{(p-1)^2}\right) \approx 0.6601618158.$$

In 1920, Viggo Brun [**19**] established an upper bound for the number of twin prime pairs $p, p+2$ with $p \leq x$. In the same paper, he also proved that there exist infinitely many prime numbers $p$ with $p + 2$ a $P_9$. The record belongs to Chen [**23**] who in 1973 proved that there exists a positive constant $c$ such that there are more than $cx/(\log x)^2$ primes $p < x$ such that $p + 2$ is a $P_2$, provided $x$ is sufficiently large.

## Problems on Chapter 2

**Problem 2.1.** *Show that if $n > 1$ is not prime then $n$ has a prime factor $p \leq \sqrt{n}$.*

**Problem 2.2.** *Show that if $n > 1$ then $n^4 + 4^n$ is composite.*

**Problem 2.3.** *Show that the set $S = \{\log p : p \text{ prime}\}$ consists of real numbers which are linearly independent over the rational numbers $\mathbb{Q}$.*

**Problem 2.4.** *Prove that if $f(X) \in \mathbb{Z}[X]$ is nonconstant, then the set*

$$S = \{p : p \text{ is prime and } p \mid f(n) \text{ for some positive integer } n\}$$

*is infinite.*

**Problem 2.5.** *Show that if $P(X_1, \ldots, X_n) \in \mathbb{C}[X_1, \ldots, X_n]$ takes only prime values at all nonnegative integer values $X_i$, then $P$ is constant.*

**Problem 2.6.** *Show that if $P(X) \in \mathbb{Z}[X]$ is a nonconstant polynomial, then there exists $n$ such that $P(n!)$ is composite.*

**Problem 2.7.** *Show that if $2^n + 1$ is prime, then $n$ is a power of 2.*

**Problem 2.8.** *Let $a > 1$ be an integer. Show that $a^n - 1$ divides $a^m - 1$ if and only if $n$ divides $m$.*

**Problem 2.9.** *A positive integer $n$ is a pseudoprime to base 2 if it is composite and if the congruence $2^{n-1} \equiv 1 \pmod{n}$ holds. Show that if $k+1 \le n_1 < n_2 < \cdots < n_s < 2^k$, then $F_{n_1} \cdots F_{n_s}$ is either a prime or a base 2 pseudoprime. Deduce that there are infinitely many base 2 pseudoprimes.*

**Problem 2.10.** *Show that $(n-1)! \equiv -1 \pmod{n}$ if $n$ is prime and $n \mid (n-1)!$ if $n > 4$ is composite. Use this to prove that*

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \left\lfloor \frac{n}{1 + \sum_{j=2}^{m} \left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor} \right\rfloor^{1/n} \right\rfloor.$$

**Problem 2.11.** *Prove that*

$$\operatorname{lcm}[1, 2, \ldots, n] \ge 2^n$$

*holds for all integers $n \ge 9$.*

**Problem 2.12.** *Show that*

$$Li(x) = \int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

**Problem 2.13.** *Let $p_n$ be the $n$-th prime. Show that, for each positive integer $n$,*

$$\frac{2}{9} n \log n < p_n.$$

**Problem 2.14.** *Show that, for each positive integer $n$,*

$$p_n < 12\left(n \log n + \log\left(\frac{12}{e}\right)\right).$$

**Problem 2.15.** *Show that there do not exist polynomials $P(x)$ and $Q(x)$ such that $\pi(n) = P(n)/Q(n)$ for infinitely many positive integers $n$.*

**Problem 2.16.** *Show that for every $n > 1$, there exist $n$ consecutive composite numbers.*

**Problem 2.17.** *Let $S_n = \sum_{i=1}^{n} p_i$. Prove that the interval $[S_n, S_{n+1}]$ contains a perfect square.*

**Problem 2.18.** *Let $p_n$ be the $n$-th prime. Euclid's proof shows that there is always a prime in the interval $(p_n, p_1 \cdots p_n + 1]$. Show, using Chebyshev's estimates, that for any constant $K$, we have*

$$\pi(p_1 p_2 \cdots p_n + 1) \gg n^K.$$

**Problem 2.19.** *Using the Prime k-tuples conjecture, show that for each positive integer $K$, there exists a positive integer $A$ such that $n^2 - n + A$ is prime for all $n = 0,\ 1,\ \ldots, K$. (Hint: Use $b_k = k^2 - k$.)*

**Problem 2.20.** *Assuming the Prime Number Theorem, show that $p_n = n \log n + o(n \log n)$ as $n \to \infty$.*

**Problem 2.21.** *Assume the Prime Number Theorem. Show that the set of ratios of primes $\{p/q\ :\ p, q \text{ primes}\}$ is dense in $[0, \infty)$. Recall that a subset $S$ of the positive real numbers is called dense in $[0, \infty)$ if every positive real number is the limit of a sequence $\{s_n\}_{n \geq 1}$, whose members $s_n$ are in $S$ for all $n \geq 1$. (Hint: Given positive integers $a$ and $b$, examine the limit of the sequence $p_{an}/p_{bn}$.)*

**Problem 2.22.** *Using Chebyshev's theorem, show that there exists a positive constant $C$ such that for each positive integer $x$, there exists a positive integer $K$ (which may depend on $x$) such that*

$$\#\{p \leq x \text{ prime } :\ p = n^2 + K \text{ for some positive integer } n\} > C \frac{\sqrt{x}}{\log x}.$$

**Problem 2.23.** *Show that there exists a positive constant $C$ such that*

$$\int_2^x \frac{\log t}{t^2}\, dt = C + O\left(\frac{1}{x^{1/2}}\right).$$

**Problem 2.24.** *Recall the statement (2.4) made by Legendre in 1798. Prove that it follows from the Prime Number Theorem in the form $\pi(x) \sim \mathrm{li}(x)$ that Legendre's statement is accurate if one chooses $A = 1$ and $B = -1$.*

**Problem 2.25.** *Prove that there exists an interval of the form $[n^2, (n+1)^2]$ which contains at least 1 000 prime numbers. (Hint: Assume the contrary and establish that it would then imply that*

$$+\infty = \sum_p \frac{1}{p} = \sum_{n=1}^{\infty} \sum_{n^2 < p \leq (n+1)^2} \frac{1}{p} < 1\,000 \sum_{n=1}^{\infty} \frac{1}{n^2} < +\infty,$$

*thereby creating a contradiction.)*

**Problem 2.26.** *Charles Hermite (1822–1901, France) provided the following very simple proof of the infinitude of primes: For each integer $n \geq 1$, let $q_n$ be the smallest prime factor of $n! + 1$; since it is clear that $q_n > n$, we have thus generated an infinite sequence of primes. Now, consider the sequence $\{q_n\}_{n \geq 1}$, whose first 40 terms are 2, 3, 7, 5, 11, 7, 71, 61, 19, 11, 39916801, 13, 83, 23, 59, 17, 661, 19, 71, 20639383, 43, 23, 47, 811, 401, 1697, 1088886945041835216076800000 1, 29, 14557, 31, 257, 2281, 67, 67411, 137, 37, 13763753091226345046315979581580902400000001, 14029308060317546154181, 79 and 41. Show that all prime numbers will eventually appear in this sequence.*

*Chapter 3*

# The Riemann Zeta Function

## 3.1. The definition of the Riemann Zeta Function

The Riemann Zeta Function plays a key role in the proof of the Prime Number Theorem, for which we shall give a proof in Chapter 5. We will use Riemann's notation and write the complex number $s$ as $s = \sigma + it$, where $\sigma$ and $t$ are real numbers.

**Definition 3.1.** *For $s \in \mathbb{C}$ with $\sigma > 1$, we define*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

The series $\sum_{n\geq 1} \frac{1}{n^s}$ converges absolutely for $\sigma > 1$. Indeed, given $N \in \mathbb{N}$, we have

$$\left| \sum_{n=1}^{N} \frac{1}{n^s} \right| \leq \sum_{n=1}^{N} \frac{1}{|n^s|} = \sum_{n=1}^{N} \frac{1}{n^\sigma},$$

and the series

$$\zeta(\sigma) = \sum_{n\geq 1} \frac{1}{n^\sigma}$$

is convergent for all $\sigma > 1$. Furthermore, we have the Euler product representation

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s}, \tag{3.1}$$

where the infinite product runs over all primes $p$. To see that the above formula holds, note that

$$\frac{1}{1-z} = 1 + z + z^2 + \cdots = \sum_{n=0}^{\infty} z^n$$

holds for all complex numbers $|z| < 1$. (To prove it, note that if we stop the sum at $N$ we get $\frac{1-z^{N+1}}{1-z}$ which tends to $\frac{1}{1-z}$ when $N$ tends to infinity because $|z| < 1$.) Thus, letting $z = p^{-s}$,

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right),$$

and if we expand the above product, then a typical term is

$$\frac{1}{p_1^{\alpha_1 s} \cdots p_k^{\alpha_k s}} = \frac{1}{(p_1^{\alpha_1} \cdots p_k^{\alpha_k})^s}.$$

Now the conclusion that formula (3.1) holds follows from the Fundamental theorem of arithmetic, which guarantees the uniqueness of the factorization of each integer $n \geq 2$.

## 3.2. Extending the Zeta Function to the half-plane $\sigma > 0$

In the preceding section, we defined $\zeta(s)$ for all $\sigma > 1$. In this section, we will extend this definition in a *nice* way (here, by nice we mean continuous, differentiable, analytic, etc.) to a function defined for all $s \in \mathbb{C}$ with $\sigma > 0$ except at $s = 1$.

**Theorem 3.2.** *The formula*

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{\infty} \frac{x - \lfloor x \rfloor}{x^{s+1}}\, dx \tag{3.2}$$

*is valid for $\sigma > 0$, provided $s \neq 1$.*

**Proof.** Let $x$ be any positive real number and let us first assume that $\sigma > 1$. Using the Abel summation formula (Proposition 1.4) with $a_n = 1$ and $f(t) = t^{-s}$, we obtain $A(x) = \sum_{n \leq x} a_n = \lfloor x \rfloor$ and

$$\sum_{n \leq x} \frac{1}{n^s} = \frac{\lfloor x \rfloor}{x^s} + s \int_1^x \frac{\lfloor u \rfloor}{u^{s+1}}\, du.$$

Letting $x \to \infty$, it follows that

$$\zeta(s) \;=\; 0 + s \int_1^{\infty} \frac{\lfloor u \rfloor}{u^{s+1}}\, du = s \int_1^{\infty} \frac{u - (u - \lfloor u \rfloor)}{u^{s+1}}\, du$$

$$\begin{aligned} &= s\int_1^\infty \frac{du}{u^s} - s\int_1^\infty \frac{u-\lfloor u\rfloor}{u^{s+1}}\,du \\ &= s\left(\frac{u^{1-s}}{1-s}\Big|_{u=1}^{u=\infty}\right) - s\int_1^\infty \frac{u-\lfloor u\rfloor}{u^{s+1}}\,du \\ &= \frac{s}{s-1} - s\int_1^\infty \frac{x-\lfloor x\rfloor}{x^{s+1}}\,dx, \end{aligned}$$

which establishes (3.2) in the case $\sigma > 1$.

Now observe that the improper integral

$$\int_1^\infty \frac{x-\lfloor x\rfloor}{x^{s+1}}\,dx$$

converges absolutely for all $\sigma = \mathrm{Re}(s) > 0$. This means that, by analytic continuation, (3.2) also holds for all $s \in \mathbb{C}$, $s \neq 1$ with $\sigma > 0$. □

**Remark 3.3.** *In the domain $s \in \mathbb{C} \setminus \{1\}$ with $\sigma > 0$, the function $\zeta(s)$ is very nice, since it is continuous and in fact even differentiable everywhere, hence analytic. (For a brief study of analytic functions, see the Appendix.) There are ways to extend the definition of $\zeta(s)$ to all the complex numbers $s \neq 1$ in such a way that it remains continuous and differentiable, but we do not need this.*

One of the most important conjectures in mathematics is the Riemann Hypothesis. Here it is:

**Conjecture 3.4.** *(Riemann Hypothesis) If $\zeta(s) = 0$ for some $s \in \mathbb{C}$ with $\sigma > 0$ and $s \neq 1$, then $\sigma = 1/2$.*

It is easy to see that $\overline{\zeta(s)} = \zeta(\overline{s})$. In particular, if $s$ is real, so is $\zeta(s)$. Thus, the complex zeros of $\zeta(s)$ with $\sigma > 0$ come in pairs consisting of a zero and its conjugate. Thus, it suffices to look at those ones lying in the part of the complex plane for which $t \geq 0$. The Riemann Hypothesis says that all the zeros of the Riemann Zeta Function with $\sigma > 0$ have $\sigma = 1/2$. It has been checked to be true for the first (that is, those with smallest $t$) 1500000000 zeros. It doesn't look like it will be hard to prove, does it ? Well, many tried and failed. If you prove it, not only do you become famous, but you also cash in the prize of $1000000 offered by the Clay Mathematical Institute (go to the website [**24**]). By the way, you get no money if you find a counterexample.

## 3.3. The derivative of the Riemann Zeta Function

**Proposition 3.5.** *The function $\zeta(s)$ has a derivative for all complex numbers $s = \sigma + it$, $s \neq 1$ with $\sigma > 0$.*

**Proof.** In light of Theorem 3.2, it is easily seen that it suffices to show that the function

$$f(s) = \int_1^\infty \frac{\{x\}}{x^{s+1}}\, dx$$

has a derivative everywhere in the complex region $\sigma > 0$, where we put $\{x\} = x - \lfloor x \rfloor$. Fix $s = \sigma + it$. Assume that $|h| < \min\{1, \sigma/2\}$. Then $\mathrm{Re}(s+h) \geq \sigma/2$. We shall show that

$$\lim_{h\to 0} \frac{f(s+h) - f(s)}{h} = -\int_1^\infty \frac{\{x\}\log x}{x^{s+1}}\, dx.$$

We split the integral at $x_h$, where $x_h > e$ will be determined later, and obtain

$$\begin{aligned}
&\left| \frac{f(s+h) - f(s)}{h} + \int_1^\infty \frac{\{x\}\log x}{x^{s+1}}\, dx \right| \\
&\quad \leq \left| \int_1^{x_h} \{x\} \left( \frac{1}{hx^{s+h+1}} - \frac{1}{hx^{s+1}} + \frac{\log x}{x^{s+1}} \right) dx \right| \\
&\quad\quad + \left| \int_{x_h}^\infty \{x\} \left( \frac{1}{hx^{s+h+1}} - \frac{1}{hx^{s+1}} + \frac{\log x}{x^{s+1}} \right) dx \right| \\
&\quad \leq \int_1^{x_h} \frac{\log x}{x^{\sigma+1}} \left| \frac{e^{-h\log x} - 1}{h\log x} + 1 \right| dx \\
&\quad\quad + \frac{3}{|h| {x_h}^{\sigma/4}} \int_{x_h}^\infty \frac{\log x}{x^{\sigma/4+1}}\, dx.
\end{aligned} \tag{3.3}$$

In the above inequalities, we used the absolute value inequality

$$\left| \int_a^b g(x)\, dx \right| \leq \int_a^b |g(x)|\, dx,$$

valid for every integrable complex valued function $g$ defined on the interval $[a, b]$, the fact that $0 \leq \{x\} \leq 1$, that $|x^{s+h}| = x^{\mathrm{Re}(s+h)} > x^{\sigma/2}$, as well as the fact that $\log x \geq \log x_h \geq 1$ in the second range of integration. We now let $x_h$ be defined by $|h|\log(x_h) = 1$. Clearly, $x_h = e^{1/|h|}$. In the range $1 \leq x \leq x_h$, we have that $|h|\log x \leq 1$, so we may apply inequality (17.7) (see the Appendix) and get that

$$\begin{aligned}
\int_1^{x_h} \frac{\{x\}\log x}{x^{s+1}} \left| \frac{e^{-h\log x} - 1}{h\log x} + 1 \right| dx &\leq |h| \int_1^{x_h} \frac{\{x\}(\log x)^2}{x^{\sigma+1}}\, dx \\
&\leq |h| \int_1^\infty \frac{(\log x)^2}{x^{\sigma+1}}\, dx \\
&= O(|h|),
\end{aligned} \tag{3.4}$$

where the constant implied by the above $O$ depends on $\sigma$. For the second range, we use the fact that if $t > 2$ is real, then $e^t > t^2$. Thus, if $h$ is such

that $|h| < \sigma/8$, then $t = \sigma/(4|h|) > 2$, so that

$$x_h^{\sigma/4} = e^{\sigma/(4|h|)} = e^t > t^2 = \frac{\sigma^2}{16|h|^2},$$

implying that

$$\frac{1}{|h|x_h^{\sigma/4}} \int_{x_h}^{\infty} \frac{\log x}{x^{\sigma/4+1}}\, dx < \frac{16|h|}{\sigma^2} \int_1^{\infty} \frac{\log x}{x^{\sigma/4+1}}\, dx = O(|h|), \tag{3.5}$$

where the constant implied by the above $O$ depends also on $\sigma$. Inserting estimates (3.4) and (3.5) into estimate (3.3), we get that

$$\left| \frac{f(s+h) - f(s)}{h} + \int_1^{\infty} \frac{\{x\} \log x}{x^{s+1}}\, dx \right| = O(|h|).$$

Letting $h$ tend to zero yields the desired conclusion. □

## 3.4. The zeros of the Zeta Function

A complex number $s = \sigma + it \neq 1$ with $\sigma > 0$ is called a *zero* of the Riemann Zeta Function if $\zeta(s) = 0$. We now prove the following result about the location of the zeros of $\zeta(s)$.

**Theorem 3.6.** *The function $\zeta(s)$ has no zeros with $\sigma \geq 1$.*

**Proof.** Assume first that $\sigma > 1$. In this case, we have the Euler product representation

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \left(1 + \frac{1}{p^s} + \cdots + \frac{1}{p^{ks}} + \cdots\right).$$

Let

$$a_n = \begin{cases} \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots = \frac{1}{p^s(1-1/p^s)} & \text{if } n = p, \text{ a prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Then $\zeta(s)$ is the limit of the product (17.5). Since $\sigma > 1$, we get that

$$|a_p| = \frac{1}{|p^s|} \left| \frac{1}{1 - 1/p^s} \right| \leq \frac{2}{p^\sigma}$$

for all primes $p$, so that both properties $|a_p| < 1$ and (17.4) (from Lemma 17.1) are fulfilled. Lemma 17.1 now tells us that $\zeta(s)$ cannot be zero.

To treat the case $\sigma = 1$, we shall use a continuity argument. Again assume that $\sigma > 1$. Taking logarithms on both sides of the Euler product representation of $\zeta(s)$, we get

$$\log \zeta(s) = -\sum_p \log\left(1 - \frac{1}{p^s}\right) = \sum_p \sum_{n \geq 1} \frac{1}{n} \frac{1}{p^{sn}}.$$

Note that

$$\mathrm{Re}\left(\frac{1}{p^{sn}}\right) = \mathrm{Re}(e^{-sn\log p}) = e^{-\sigma n\log p}\cos(-tn\log p) = \frac{\cos(tn\log p)}{p^{\sigma n}}.$$

Thus,

$$\mathrm{Re}(\log\zeta(s)) = \sum_p\sum_{n\geq 1}\frac{\cos(tn\log p)}{np^{\sigma n}}.$$

Since $\mathrm{Re}(\log(\zeta(s))) = \log|\zeta(s)|$ (see formula (17.3)), we get

$$\log|\zeta(s)| = \sum_p\sum_{n\geq 1}\frac{\cos(tn\log p)}{np^{\sigma n}}. \tag{3.6}$$

We will now use inequality

$$\begin{aligned} 0 &\leq 2(1+\cos\theta)^2 = 2(1+2\cos\theta+\cos^2\theta)\\ &= 3+4\cos\theta+(2\cos^2\theta-1)\\ &= 3+4\cos\theta+\cos(2\theta), \end{aligned}$$

for $\theta = nt\log p$, to deduce that

$$\frac{3+4\cos(nt\log p)+\cos(2nt\log p)}{np^{\sigma n}} \geq 0 \tag{3.7}$$

for all $n\geq 1$ and all primes $p$. Summing inequalities (3.7) for all $n$ and $p$, and using formula (3.6), we get that

$$3\log|\zeta(\sigma)| + 4\log|\zeta(\sigma+it)| + \log|\zeta(\sigma+2it)| \geq 0,$$

and therefore that

$$|\zeta(\sigma)|^3|\zeta(\sigma+it)^4||\zeta(\sigma+2it)| \geq 1. \tag{3.8}$$

Now assume that $1+it_0$ is a zero of $\zeta(s)$. Clearly, $t_0\neq 0$. Let $\sigma>1$ approach 1 from the right. Using relation (3.2), we get

$$(\sigma-1)\zeta(\sigma) = \sigma - \sigma(\sigma-1)\int_1^\infty \frac{\{x\}}{x^{\sigma+1}}\,dx = O(1)$$

when $\sigma\in(1,2)$, so that $|\zeta(\sigma)| = O((\sigma-1)^{-1})$. Furthermore, since $\zeta(s)$ has a derivative at $s=1+it_0$, we get that

$$\frac{\zeta(\sigma+it_0)-\zeta(1+it_0)}{\sigma-1} = \frac{\zeta(\sigma+it_0)}{\sigma-1}$$

is bounded in a small neighborhood of $1+it_0$. Thus, if $\sigma$ is close to 1, then $\zeta(\sigma+it_0) = O(\sigma-1)$. Finally, $\zeta(\sigma+2it_0)$ is bounded when $\sigma$ is close to 1 (because $\zeta$ is continuous at $\zeta(1+2it_0)$). Combining all these estimates, we get that if $\sigma>1$ is close to 1, then

$$\zeta(\sigma)^3|\zeta(\sigma+it_0)|^4|\zeta(\sigma+2it_0)| = O\left(\frac{1}{(\sigma-1)^3}\cdot(\sigma-1)^4\right) = O(\sigma-1),$$

which contradicts inequality (3.8) once $\sigma-1$ is sufficiently small. □

## 3.5. Euler's estimate $\zeta(2) = \pi^2/6$

Many great mathematicians of the 18th century tried in vain to obtain a closed expression for the series

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots$$

Amongst these were the Bernoulli brothers (Jean and Jacob). They had no problem showing that $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n(n+1)} = 1$, but they didn't have a clue how to go about evaluating $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2}$. A student of Jean Bernoulli, the great Leonhard Euler, discovered the following result:

**Theorem 3.7.** *The sum of the reciprocals of the squares converges to $\pi^2/6$, that is,*

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}. \tag{3.9}$$

Although his reasoning was not quite rigorous, here is how Euler proceeded. Since the zeros of the $\sin z$ function are $z = 0, \pm\pi, \pm 2\pi, \pm 3\pi, \ldots$, then the zeros of the function $\frac{\sin z}{z}$ are $z = \pm\pi, \pm 2\pi, \pm 3\pi, \ldots$, and therefore

$$\begin{aligned} \frac{\sin z}{z} &= \left(1 - \frac{z^2}{\pi^2}\right)\left(1 - \frac{z^2}{4\pi^2}\right)\left(1 - \frac{z^2}{9\pi^2}\right)\cdots \\ &= 1 - z^2\left(\frac{1}{\pi^2} + \frac{1}{4\pi^2} + \frac{1}{9\pi^2} + \cdots\right) \\ &\qquad + z^4(\ldots) - z^6(\ldots) + \cdots \end{aligned} \tag{3.10}$$

On the other hand, since

$$\sin z = z - \frac{z^3}{3!} + \frac{z^5}{5!} + \cdots,$$

it follows that

$$\frac{\sin z}{z} = 1 - \frac{z^2}{3!} + \frac{z^4}{5!} + \cdots \tag{3.11}$$

Comparing the coefficient of $z^2$ in (3.10) with that of $z^2$ in (3.11), Euler concluded that

$$\frac{1}{3!} = \frac{1}{\pi^2} + \frac{1}{4\pi^2} + \frac{1}{9\pi^2} + \cdots,$$

which by multiplying by $\pi^2$ yields (3.9).

**Remark 3.8.** *Euler also obtained the general formula*

$$\zeta(2k) = (-1)^{k+1}\frac{(2\pi)^{2k}B_{2k}}{2(2k)!} \qquad (k = 1, 2, 3, \ldots), \tag{3.12}$$

*where $B_m$ stands for the $m$-th Bernoulli number (see Proposition* 1.3 *for the definition of Bernoulli numbers). Thus, in particular,*

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}, \quad \zeta(8) = \frac{\pi^8}{9450}, \quad \zeta(10) = \frac{\pi^{10}}{93555}.$$

Here, we give a rigorous proof of (3.9) which avoids complex analysis, a proof due to Tom Apostol [**3**]. The argument consists in evaluating the integral

$$I = \int_0^1 \int_0^1 \frac{1}{1-xy} dxdy$$

in two distinct ways. The above integral is improper but we can think of it as

$$I = \lim_{\varepsilon \to 0} \int_0^{1-\varepsilon} \int_0^{1-\varepsilon} \frac{1}{1-xy}\, dxdy.$$

On the one hand, writing

$$\frac{1}{1-xy} = \sum_{n\geq 0} (xy)^n \tag{3.13}$$

and integrating we get

$$\begin{aligned} I &= \int_0^1 \int_0^1 \sum_{n\geq 0} (xy)^n dxdy = \sum_{n\geq 0} \int_0^1 \int_0^1 x^n y^n \, dxdy \\ &= \sum_{n\geq 0} \left( \int_0^1 x^n \, dx \right) \left( \int_0^1 y^n \, dy \right) = \sum_{n\geq 0} \frac{1}{n+1} \cdot \frac{1}{n+1} \\ &= \sum_{n\geq 0} \frac{1}{(n+1)^2} = \sum_{n\geq 1} \frac{1}{n^2} = \zeta(2). \end{aligned} \tag{3.14}$$

The above evaluation also proves that the given double integral is finite. The second way of evaluating $I$ is by first making a change of coordinates. Rotating $45^o$ clockwise, we get

$$u = \frac{y+x}{\sqrt{2}} \qquad \text{and} \qquad v = \frac{y-x}{\sqrt{2}},$$
$$x = \frac{u-v}{\sqrt{2}} \qquad \text{and} \qquad y = \frac{u+v}{\sqrt{2}}.$$

Substituting the new coordinates we get

$$1 - xy = 1 - \frac{u^2 - v^2}{2},$$

which is the same as

$$\frac{1}{1-xy} = \frac{2}{2-u^2+v^2}.$$

The new domain of integration is a rectangle whose vertices are $(0,0)$, $(\sqrt{2}/2, \sqrt{2}/2)$, $(\sqrt{2}, 0)$ and $(\sqrt{2}/2, -\sqrt{2}/2)$. This domain is symmetric with respect to the $u$-axis and the function that is being integrated is also symmetric. Therefore, we only need to find the integral in the region of the domain for which $v \geq 0$, which we split in two pieces as:

$$I = 4\int_0^{\sqrt{2}/2} \left( \int_0^u \frac{dv}{2-u^2+v^2} \right) du + 4\int_{\sqrt{2}/2}^{\sqrt{2}} \left( \int_0^{\sqrt{2}-u} \frac{dv}{2-u^2+v^2} \right) du.$$

Using $\displaystyle\int \frac{dx}{a^2+x^2} = \frac{1}{a}\arctan\frac{x}{a} + C$, we get

$$\begin{aligned} I &= 4\int_0^{\sqrt{2}/2} \frac{1}{\sqrt{2-u^2}} \arctan\left( \frac{u}{\sqrt{2-u^2}} \right) du \\ &\quad + 4\int_{\sqrt{2}/2}^{\sqrt{2}} \frac{1}{\sqrt{2-u^2}} \arctan\left( \frac{\sqrt{2}-u}{\sqrt{2-u^2}} \right) du. \end{aligned}$$

We only need to make two trigonometric substitutions. For the first integral, we let $u = \sqrt{2}\sin\theta$. The interval $0 \leq u \leq \sqrt{2}/2$ gets mapped to $0 \leq \theta \leq \pi/6$. Computing $du = \sqrt{2}\cos\theta d\theta$ and $\sqrt{2-u^2} = \sqrt{2(1-\sin^2\theta)} = \sqrt{2}\cos\theta$, we get

$$\begin{aligned} &4\int_0^{\sqrt{2}/2} \frac{1}{\sqrt{2-u^2}} \arctan\left( \frac{u}{\sqrt{2-u^2}} \right) du \\ &\quad = 4\int_0^{\pi/6} \frac{1}{\sqrt{2}\cos\theta} \arctan\left( \frac{\sqrt{2}\sin\theta}{\sqrt{2}\cos\theta} \right) \sqrt{2}\cos\theta \, d\theta \\ &\quad = 4\int_0^{\pi/6} \theta \, d\theta = 4\left(\frac{1}{2}\right)\left(\frac{\pi}{6}\right)^2 = \left(\frac{1}{3}\right)\frac{\pi^2}{6}. \end{aligned} \tag{3.15}$$

For the second integral we use $u = \sqrt{2}\cos 2\theta$. Here, $\sqrt{2}/2 \leq u \leq \sqrt{2}$ translates into $\pi/6 \geq \theta \geq 0$. Computing $du = -2\sqrt{2}\sin 2\theta \, d\theta$,

$$\sqrt{2-u^2} = \sqrt{2(1-\cos^2(2\theta))} = \sqrt{2}\sin 2\theta = 2\sqrt{2}\sin\theta\cos\theta,$$

and

$$\sqrt{2}-u = \sqrt{2}(1-\cos 2\theta) = 2\sqrt{2}\sin^2\theta,$$

it follows that

$$
\begin{aligned}
&4\int_{\sqrt{2}/2}^{\sqrt{2}} \frac{1}{\sqrt{2-u^2}} \arctan\left(\frac{\sqrt{2}-u}{\sqrt{2-u^2}}\right) du \\
&\quad = 4\int_{\pi/6}^{0} \frac{1}{\sqrt{2}\sin 2\theta} \arctan\left(\frac{2\sqrt{2}\sin^2\theta}{2\sqrt{2}\sin\theta\cos\theta}\right)(-2\sqrt{2})\sin 2\theta\, d\theta \qquad (3.16)\\
&\quad = 4\int_{0}^{\pi/6} 2\theta\, d\theta = 4\left(\frac{\pi}{6}\right)^2 = \left(\frac{2}{3}\right)\frac{\pi^2}{6}.
\end{aligned}
$$

Summing up integrals (3.15) and (3.16), we obtain

$$I = \left(\frac{1}{3}\right)\frac{\pi^2}{6} + \left(\frac{2}{3}\right)\frac{\pi^2}{6} = \frac{\pi^2}{6}.$$

## Problems on Chapter 3

**Problem 3.1.** *Show that it follows from Theorem* 3.2 *that* $\zeta(\sigma) < 0$ *for* $0 < \sigma < 1$.

**Problem 3.2.** *Extend the function*

$$G(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}$$

*defined for all complex numbers* $s$ *with* $\mathrm{Re}(s) > 1$ *to all complex numbers* $s$ *with* $\mathrm{Re}(s) > 0$.

**Problem 3.3.** *Show that for any given positive integer* $N$, *the representation*

$$\zeta(s) = \sum_{n=1}^{N} \frac{1}{n^s} - s\int_{N}^{\infty} \frac{x - \lfloor x \rfloor}{x^{s+1}} dx + \frac{N^{1-s}}{s-1}$$

*holds for* $\mathrm{Re}(s) > 0$.

**Problem 3.4.** *Show that, for* $\mathrm{Re}(s) > 1$,

$$\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s}.$$

**Problem 3.5.** *Show that, for* $Re(s) > 0$,

$$\zeta'(s) = -\frac{1}{(s-1)^2} - \int_{1}^{\infty} \frac{x - \lfloor x \rfloor}{x^{s+1}} dx + s\int_{1}^{\infty} \frac{(x - \lfloor x \rfloor)\log x}{x^{s+1}} dx.$$

**Problem 3.6.** *Show that if* $s = \sigma + it$ *and* $\sigma > 1$, *then*

$$|\zeta(s)| \le \zeta(\sigma)$$

*and*

$$|\zeta'(s)| \le |\zeta'(\sigma)|.$$

**Problem 3.7.** *Show that*

$$(1-2^{1-s})\zeta(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}$$

*for* $\mathrm{Re}(s) > 1$. *Assuming that the above representation is also true for real* $s \in (0,1)$, *deduce that* $\zeta(s) < 0$ *for* $s \in (0,1)$.

**Problem 3.8.** *Show that for each positive constant* $A$, *there exists a positive constant* $M$ *such that*

$$|\zeta(s)| \le M \log t$$

*and*

$$|\zeta'(s)| \le M(\log t)^2$$

*holds for all* $s$ *in the region* $\sigma > 1 - A/\log t$ *and* $t \ge e$. *(Hint: Use the representation given at Problem* 3.3 *and split it at* $N = \lfloor t \rfloor$.*)*

**Problem 3.9.** *Show that*

$$\sum_{n=1}^{\infty} \frac{\mu(n)^2}{n^2} = \frac{\zeta(2)}{\zeta(4)},$$

*where* $\mu$ *stands for the Möbius function (see its definition in the Frequently Used Functions section of this book on page* xviii*). Can this formula be generalized ?*

**Problem 3.10.** *Let* $\{a_n\}_{n\ge1}$ *be some sequence of complex numbers such that* $|a_n| \le 1$ *for all* $n \ge 1$. *Show that the series*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

*converges to a function* $F(s)$ *which is analytic for* $\sigma > 1$.

**Problem 3.11.** *Let* $f(X) \in \mathbb{Z}[X]$ *be a nonconstant polynomial with integer coefficients. Show that there exist infinitely many positive integers* $n$ *such that* $\mu(|f(n)|) = 0$.

**Problem 3.12.** *A positive integer* $n$ *is called squarefull (or powerful) if* $p^2 \mid n$ *whenever* $p$ *is a prime factor of* $n$. *Show that the formula*

$$\sum_{\substack{n\ge1 \\ n \text{ squarefull}}} \frac{1}{n^s} = \frac{\zeta(2s)\zeta(3s)}{\zeta(6s)}$$

*is valid for all* $\sigma > 1/2$. *(Hint: Show that every powerful number* $n$ *has a unique representation as* $n = a^2b^3$, *where* $a$ *and* $b$ *are integers with* $b$ *squarefree.)*

**Problem 3.13.** *As was mentioned in the footnote at the bottom of page 7, Stieltjes claimed that he could prove that the series* $\displaystyle\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}$ *converges for all* $s > 1/2$. *Show that this statement implies the Riemann Hypothesis. (Hint: First show that this series is equal to* $1/\zeta(s)$*; then, show that the statement of Stieltjes provides an analytic continuation of* $1/\zeta(s)$ *to the half-plane* $Re(s) > 1/2$*, and deduce from this the truth of the Riemann Hypothesis.)*

**Problem 3.14.** *Prove Euler's formula (*3.12*). (Hint: Follow the reasoning appearing in Serre's book* [**129**]*, namely by proceeding as follows. Start with the product formula*

$$\frac{\sin z}{z} = \prod_{n=1}^{\infty}\left(1 - \frac{z^2}{n^2\pi^2}\right),$$

*take logarithms on both sides and then differentiate with respect to* $z$*, thus obtaining*

$$z\cot z = 1 + 2\sum_{n=1}^{\infty}\frac{z^2}{z^2 - n^2\pi^2} = 1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{z^{2k}}{(\pi n)^{2k}} = 1 - 2\sum_{k=1}^{\infty}\zeta(2k)\frac{z^{2k}}{\pi^{2k}}.$$

*Then, set* $x = 2iz$ *in the formula* $\displaystyle\frac{x}{e^x - 1} = \sum_{r=0}^{\infty}B_r\frac{x^r}{r!}$ *to obtain*

$$z\cot z = 1 - \sum_{k=1}^{\infty}(-1)^{k+1}\frac{4^k B_{2k}}{(2k)!}z^{2k}.$$

*Compare the above two representations of* $z\cot z$ *in order to derive (*3.12*).)*

*Chapter 4*

# Setting the Stage for the Proof of the Prime Number Theorem

## 4.1. Key functions related to the Prime Number Theorem

The following functions are very important in the study of prime numbers.

**Definition 4.1.** *For each positive integer $n$, let*

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

The function $\Lambda$ is called the *von Mangoldt function.* Furthermore, define, for $x > 0$, the functions

$$\theta(x) = \sum_{p \leq x} \log p = \log \left( \prod_{p \leq x} p \right)$$

and

$$\psi(x) = \sum_{\substack{p^k \leq x \\ k \geq 1}} \log p = \sum_{n \leq x} \Lambda(n).$$

Notice that

$$\psi(x) = \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p.$$

Also observe that since $p^2 \le x$ is equivalent to $p \le x^{1/2}$, $p^3 \le x$ is equivalent to $p \le x^{1/3}$, and so on, we get that

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \cdots . \tag{4.1}$$

Note that $x^{1/m}$ appears in the above sum only if $x^{1/m} \ge 2$, or, equivalently, $m \le \log x/\log 2$, implying that the sum (4.1) contains $\lfloor \log x/\log 2 \rfloor$ terms. Upon noting that

$$\theta(x) \le (\log x)\pi(x) = O(x)$$

(by the Chebyshev theorem), we get that

$$\theta(x^{1/2}) + \theta(x^{1/3}) + \cdots \le \theta(x^{1/2})(\log x/\log 2) = O(x^{1/2}\log x),$$

which, substituted in (4.1), yields

$$\psi(x) = \theta(x) + O(x^{1/2}\log x). \tag{4.2}$$

We now show that $\psi(x) \sim \theta(x)$ as $x \to \infty$. Indeed, observe that if $p \ge x^{1/2}$, then $\log p \ge \log(x^{1/2}) = (\log x)/2 \gg \log x$, so that

$$\begin{aligned} \theta(x) &\ge \sum_{x^{1/2} \le p \le x} \log p \gg (\pi(x) - \pi(\sqrt{x}))\log x \\ &= \pi(x)\log x - \pi(x^{1/2})\log x = \pi(x)\log x + O(x^{1/2}\log x). \end{aligned} \tag{4.3}$$

Since $\pi(x) \gg x/\log x$, we obtain that $\theta(x) \gg x$. Comparing this with estimate (4.2), we immediately get that the difference $O(x^{1/2}\log x)$ between $\psi(x)$ and $\theta(x)$ is $o(\theta(x))$ as $x \to \infty$. Therefore,

$$\psi(x) \sim \theta(x) \qquad (x \to \infty). \tag{4.4}$$

Note incidentally that we have shown that $\pi(x) \asymp \theta(x)/\log x$. As we will show in the next section, these two expressions are asymptotically the same.

## 4.2. A closer analysis of the functions $\theta(x)$ and $\psi(x)$

In this section, we show how the three functions $\pi(x)$, $\theta(x)$ and $\psi(x)$ are related when $x$ is large.

**Theorem 4.2.** *As $x \to \infty$, $\pi(x) \sim \theta(x)/\log x \sim \psi(x)/\log x$.*

**Proof.** It follows from (4.4) that $\theta(x)/\log x \sim \psi(x)/\log x$ as $x \to \infty$. So, let us prove the estimate $\pi(x) \sim \theta(x)/\log x$. It is clear that

$$\theta(x) = \sum_{p \le x} \log p \le \log x \sum_{p \le x} 1 = \pi(x)\log x,$$

so that

$$\limsup_{x \to \infty} \frac{\theta(x)/\log x}{\pi(x)} \le 1. \tag{4.5}$$

We will now show that

$$\liminf_{x\to\infty} \frac{\theta(x)/\log x}{\pi(x)} \geq 1. \tag{4.6}$$

Let $\delta > 0$ be arbitrarily small but fixed. We shall assume that $\delta \in (0, 1/2)$. We split the defining sum for $\theta(x)$ at $x^{1-\delta}$ and keep only the larger range. This is why

$$\begin{aligned} \theta(x) &\geq \sum_{x^{1-\delta}<p\leq x} \log p > \log(x^{1-\delta}) \sum_{x^{1-\delta}<p\leq x} 1 \\ &= (1-\delta)(\log x)(\pi(x) - \pi(x^{1-\delta})) \\ &= (1-\delta)\pi(x)\log x + O(x^{1-\delta}), \end{aligned} \tag{4.7}$$

where we used Chebyshev's estimate to get that

$$\pi(x^{1-\delta}) \ll \frac{x^{1-\delta}}{\log(x^{1-\delta})} < \frac{2x^{1-\delta}}{\log x},$$

which holds because $1 - \delta > 1/2$. Let $c_1$ be the constant implied in the $O$ term of (4.7). Let $c_2 > 0$ be such that $\pi(x)\log x > c_2 x$ (by Theorem 2.6, we can take $c_2 = 3(\log 2)/8$). Hence, in light of (4.7),

$$\frac{\theta(x)/\log x}{\pi(x)} \geq (1-\delta) - \frac{c_1 x^{1-\delta}}{\pi(x)\log x} \geq (1-\delta) - \frac{c_1}{c_2 x^{\delta}}. \tag{4.8}$$

Letting $x$ tend to infinity in estimate (4.8), we get

$$\liminf_{x\to\infty} \frac{\theta(x)/\log x}{\pi(x)} \geq 1 - \delta,$$

and since $\delta > 0$ is arbitrary, (4.6) follows immediately. Combining (4.6) and (4.5) completes the proof of the theorem. □

## 4.3. Useful estimates

**Theorem 4.3.** *As $x \to \infty$,*

$$\sum_{n\leq x} \frac{\Lambda(n)}{n} = \log x + O(1). \tag{4.9}$$

**Proof.** We apply the Abel summation formula (Proposition 1.4) with $a_n = 1$ and $f(t) = \log t$. Then

$$\begin{aligned}\sum_{n\le x}\log n &= \lfloor x\rfloor\log x - \int_1^x \frac{\lfloor t\rfloor}{t}\,dt\\ &= (x-(x-\lfloor x\rfloor))\log x - \int_1^x \frac{t-(t-\lfloor t\rfloor)}{t}\,dt\\ &= x\log x + O(\log x) - \int_1^x dt + \int_1^x \frac{t-\lfloor t\rfloor}{t}dt\\ &= x\log x + O(\log x) - (x-1) + O\left(\int_1^x \frac{dt}{t}\right)\\ &= x\log x - x + O(\log x).\end{aligned} \tag{4.10}$$

On the other hand, using Lemma 2.7, we also have that

$$\begin{aligned}\sum_{n\le x}\log n &= \log(\lfloor x\rfloor!) = \sum_{p\le x}\left(\sum_{k=1}^{\infty}\left\lfloor\frac{x}{p^k}\right\rfloor\right)\log p\\ &= \sum_{\substack{p^k\le x\\ k\ge 1}}\left\lfloor\frac{x}{p^k}\right\rfloor\log p = \sum_{n\le x}\left\lfloor\frac{x}{n}\right\rfloor\Lambda(n)\\ &= \sum_{n\le x}\frac{x}{n}\Lambda(n) - \sum_{n\le x}\left(\frac{x}{n}-\left\lfloor\frac{x}{n}\right\rfloor\right)\Lambda(n)\\ &= x\sum_{n\le x}\frac{\Lambda(n)}{n} + O\left(\sum_{n\le x}\Lambda(n)\right).\end{aligned}$$

Since

$$\sum_{n\le x}\Lambda(n) = \psi(x) = O(x),$$

we get that

$$\sum_{n\le x}\log n = x\sum_{n\le x}\frac{\Lambda(n)}{n} + O(x). \tag{4.11}$$

Comparing estimate (4.11) with estimate (4.10), we obtain

$$x\log x - x + O(\log x) = x\sum_{n\le x}\frac{\Lambda(n)}{n} + O(x),$$

and by dividing both sides by $x$, the desired estimate follows. □

**Theorem 4.4.** *The estimate*

$$\sum_{p\le x}\frac{\log p}{p} = \log x + O(1) \tag{4.12}$$

*holds as* $x \to \infty$.

**Proof.** Clearly,

$$\begin{aligned}\sum_{p\le x}\frac{\log p}{p} &= \sum_{n\le x}\frac{\Lambda(n)}{n} - \sum_{k\ge 2}\sum_{p^k\le x}\frac{\log p}{p^k}\\ &= \log x + O(1) - \sum_{k\ge 2}\sum_{p^k\le x}\frac{\log p}{p^k},\end{aligned}$$

where we used estimate (4.9). However, since

$$\sum_{k\ge 2}\sum_{p^k\le x}\frac{\log p}{p^k} \le \sum_p\left(\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right)\log p = \sum_p \frac{\log p}{p(p-1)} = O(1),$$

the desired estimate follows. □

## 4.4. The Mertens estimate

The following result is often called *Mertens' estimate*.

**Theorem 4.5.** *There exists a constant* $\beta$ *such that the estimate*

$$\sum_{p\le x}\frac{1}{p} = \log\log x + \beta + O\left(\frac{1}{\log x}\right) \tag{4.13}$$

*holds as* $x \to \infty$.

**Proof.** Define

$$a_n = \begin{cases} \frac{\log p}{p} & \text{if } n = p,\\ 0 & \text{otherwise,}\end{cases}$$

and let $f(t) = 1/\log t$. Then $f'(t) = -1/t(\log t)^2$. Moreover,

$$A(x) = \sum_{n\le x} a_n = \sum_{p\le x}\frac{\log p}{p} = \log x + R(x),$$

where $R(x) = O(1)$ by Theorem 4.4. The Abel summation formula (Proposition 1.4) now gives

$$\begin{aligned}\sum_{p\le x}\frac{1}{p} &= \frac{A(x)}{\log x} + \int_2^x \frac{A(t)}{t(\log t)^2}\,dt = 1 + \frac{R(x)}{\log x} + \int_2^x \frac{\log t + R(t)}{t(\log t)^2}\,dt\\ &= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{dt}{t\log t} + \int_2^x \frac{R(t)}{t(\log t)^2}\,dt\\ &= 1 + O\left(\frac{1}{\log x}\right) + (\log\log t)\Big|_{t=2}^{t=x}\end{aligned}$$

$$
\begin{aligned}
&+\int_2^\infty \frac{R(t)}{t(\log t)^2}\,dt - \int_x^\infty \frac{R(t)}{t(\log t)^2}\,dt \\
&= \log\log x + 1 - \log\log 2 + \int_2^\infty \frac{R(t)}{t(\log t)^2}\,dt + O\left(\frac{1}{\log x}\right) \\
&\quad +O\left(\int_x^\infty \frac{dt}{t(\log t)^2}\right) \\
&= \log\log x + \beta + O\left(\frac{1}{\log x} + \left(-\frac{1}{\log t}\right)\Big|_{t=x}^{t=\infty}\right) \\
&= \log\log x + \beta + O\left(\frac{1}{\log x}\right),
\end{aligned}
$$

where

$$\beta = 1 - \log\log 2 + \int_2^\infty \frac{R(t)}{t(\log t)^2}\,dt.$$

This completes the proof of the theorem. □

**Remark 4.6.** *It can be shown that the constant $\beta$ appearing in estimate* (4.13) *is given by*

$$\beta = \gamma + \sum_p \left(\log\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right) \approx 0.26149.$$

## 4.5. The Möbius function

One of the most important functions in analytic number theory is the Möbius function (also written Moebius function) which we already defined in the *Frequently Used Functions* section. Nevertheless, we recall its definition.

**Definition 4.7.** *The Möbius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is given by $\mu(1) = 1$, $\mu(n) = (-1)^r$ if $n$ is a product of $r$ distinct primes and $\mu(n) = 0$ otherwise.*

In particular, $\mu(12) = 0$, $\mu(15) = 1$ and $\mu(30) = -1$. Notice that if $\sigma > 1$, then

$$\frac{1}{\zeta(s)} = \prod_p \left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^\infty \frac{\mu(n)}{n^s}. \tag{4.14}$$

We summarize the most important properties of the Möbius function in the following theorem. Properties (ii) and (iii) below are usually referred to as the *Möbius inversion formulas.*

**Theorem 4.8.** (i) *Let $n \in \mathbb{N}$. Setting*

$$E(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise,} \end{cases}$$

*then*

$$\sum_{d|n} \mu(d) = E(n).$$

(ii) *Let* $f : \mathbb{R}_+ \longrightarrow \mathbb{C}$ *and define* $F : \mathbb{R}_+ \longrightarrow \mathbb{C}$ *by*

$$F(x) = \sum_{n \leq x} f\left(\frac{x}{n}\right).$$

*Then*

$$f(x) = \sum_{n \leq x} \mu(n) F\left(\frac{x}{n}\right).$$

(iii) *Let* $f : \mathbb{N} \longrightarrow \mathbb{C}$ *and define* $F : \mathbb{N} \longrightarrow \mathbb{C}$ *by*

$$F(n) = \sum_{d|n} f(d).$$

*Then*

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

**Proof.** (i) If $n = 1$, the result is obvious. Assume now that $n > 1$. Let $n = p_1^{\ell_1} \cdots p_r^{\ell_r}$ where $p_1, \ldots, p_r$ are distinct primes and $\ell_1, \ldots, \ell_r$ are positive integers. Let $m = p_1 \cdots p_r$. Then it is clear that

$$\sum_{d|n} \mu(d) = \sum_{d|m} \mu(d),$$

and since for each integer $j \in \{1, \ldots, r\}$, there are $\binom{r}{j}$ divisors of $m$ with $j$ prime factors,

$$\sum_{d|m} \mu(d) = 1 - \binom{r}{1} + \binom{r}{2} - \cdots + (-1)^r \binom{r}{r} = 0,$$

the proof of (i) is immediate.

(ii) Using (i),

$$\begin{aligned} f(x) &= \sum_{n \leq x} \left( \sum_{d \,|\, n} \mu(d) \right) f\left(\frac{x}{n}\right) = \sum_{d\ell \leq x} \mu(d) f\left(\frac{x}{d\ell}\right) \\ &= \sum_{d \leq x} \mu(d) \left( \sum_{\ell \leq x/d} f\left(\frac{x}{\ell d}\right) \right) = \sum_{d \leq x} \mu(d) F\left(\frac{x}{d}\right). \end{aligned}$$

(iii) Again by (i),

$$\begin{aligned} f(n) &= \sum_{c\,|\,n} \left( \sum_{d\,|\,(n/c)} \mu(d) \right) f(c) \\ &= \sum_{d\,|\,n} \mu(d) \sum_{c\,|\,(n/d)} f(c) = \sum_{d\,|\,n} \mu(d) F\left(\frac{n}{d}\right), \end{aligned}$$

which completes the proof of the theorem. □

## 4.6. The divisor function

For each positive integer $n$, let $d(n)$ stand for the number of positive integers dividing $n$.

**Theorem 4.9.**

$$\sum_{m=1}^{n} d(m) = \sum_{m=1}^{n} \left\lfloor \frac{n}{m} \right\rfloor = n \log n + (2\gamma - 1)n + O(n^{1/2}).$$

**Proof.** Let $D_n$ be the region in the upper right hand quadrant not containing the $x$ or the $y$ axis and under (and including) the hyperbola $xy = n$. That is,

$$D_n = \{(x, y) \in \mathbb{R}^2 \ : \ x > 0,\ y > 0,\ xy \le n\}.$$

Every point with integer coordinates in $D_n$ is contained in a hyperbola $xy = m$ for some positive integer $m \le n$. Thus, $\sum_{m=1}^{n} d(m)$ is the number of points with integer coordinates in $D_n$. Note that if $x = m$ is fixed, then the number of points in $D_n$ having this value of $x$ is $\lfloor \frac{n}{m} \rfloor$. Hence, the number of points in $D_n$ is also $\sum_{m=1}^{n} \lfloor \frac{n}{m} \rfloor$.

To estimate how many points are in $D_n$, we first observe that the number of points above the line $y = x$ is the same as the number of points below it. Thus,

$$\begin{aligned} \sum_{m=1}^{n} \left\lfloor \frac{n}{m} \right\rfloor &= 2 \sum_{x=1}^{\lfloor \sqrt{n} \rfloor} \left( \left\lfloor \frac{n}{x} \right\rfloor - \lfloor x \rfloor \right) + \lfloor \sqrt{n} \rfloor \\ &= 2 \sum_{k=1}^{\lfloor \sqrt{n} \rfloor} \left( \frac{n}{k} - k + O(1) \right) + \lfloor \sqrt{n} \rfloor \qquad (4.15) \\ &= \left( 2n \sum_{k=1}^{\lfloor \sqrt{n} \rfloor} \frac{1}{k} \right) - 2 \left( \frac{\lfloor \sqrt{n} \rfloor (\lfloor \sqrt{n} \rfloor + 1)}{2} \right) + O\left(\sqrt{n}\right). \end{aligned}$$

By Theorem 1.7,

$$\sum_{k=1}^{\lfloor\sqrt{n}\rfloor} \frac{1}{k} = \log\lfloor\sqrt{n}\rfloor + \gamma + O\left(\frac{1}{\sqrt{n}}\right). \tag{4.16}$$

Inserting estimate (4.16) into (4.15), we get

$$\sum_{m=1}^{n} \left\lfloor \frac{n}{m} \right\rfloor = 2n\left(\log\lfloor\sqrt{n}\rfloor + \gamma + O\left(\frac{1}{\sqrt{n}}\right)\right) - (n+O(\sqrt{n})) + O(\sqrt{n}). \tag{4.17}$$

Since

$$\lfloor\sqrt{n}\rfloor = \sqrt{n} - \{\sqrt{n}\} = \sqrt{n} + O(1),$$

we have

$$\begin{aligned} \log(\lfloor\sqrt{n}\rfloor) &= \log(\sqrt{n} + O(1)) \\ &= \log\left(\sqrt{n}\left(1 + O\left(\frac{1}{\sqrt{n}}\right)\right)\right) \\ &= \log(\sqrt{n}) + \log\left(1 + O\left(\frac{1}{\sqrt{n}}\right)\right) \\ &= \log(\sqrt{n}) + O\left(\frac{1}{\sqrt{n}}\right). \end{aligned} \tag{4.18}$$

Thus, using (4.18) in (4.17), we obtain

$$\sum_{m=1}^{n} \left\lfloor \frac{n}{m} \right\rfloor = n\log n + (2\gamma - 1)n + O(\sqrt{n}),$$

which is what we wanted to prove. □

**Remark 4.10.** *If we define $\Delta(n)$ implicitly by the relation*

$$\sum_{m=1}^{n} d(m) = n\log n + (2\gamma - 1)n + \Delta(n),$$

*we have established in Theorem 4.9 that $\Delta(n) = O(x^{1/2})$. This upper bound was improved along the years; for a survey of the methods used to do so, see Ivić's book* [**87**] *or the classical Titchmarsh book* [**142**] *revised by Heath-Brown. In 2003, Huxley* [**85**] *showed that $\Delta(n) = O(x^{131/416})$. (Note that $131/416 \approx 0.3149$.) This is the best-known upper bound as of today. This bound cannot be lowered very much since Landau showed in 1916 that if $\Delta(n) = O(n^{\theta})$, then $\theta \geq 1/4$. The problem of finding optimal values for the size of $\Delta(n)$ is known as the Divisor Problem.*

## Problems on Chapter 4

**Problem 4.1.** *Assume that* $\{b_n\}_{n\geq 1}$ *is a sequence of real numbers such that*

$$\sum_{n=1}^{\infty} \frac{b_n}{n}$$

*is convergent. Show that* $\sum_{n\leq x} b_n = o(x)$ *as* $x \to \infty$. *(Hint: Apply the Abel summation formula with* $a_n = b_n/n$ *and* $f(t) = t$.*)*

**Problem 4.2.** *Show that there exists a constant* $\delta$ *such that*

$$\sum_{p\leq x} \frac{1}{p \log\log p} = \log\log\log x + \delta + O\left(\frac{1}{\log\log x}\right).$$

**Problem 4.3.** *A palindrome is a positive integer* $n$ *whose string of digits (in base* 10*) reads the same from left and right. For example,* 151, 2332, *and* 12345678987654321 *are all palindromes.*

(i) *Let* $A(x) = \{n \leq x \ : \ n \text{ is a palindrome}\}$. *Show that* $\#A(x) \asymp x^{1/2}$. *(Hint: How many digits does a palindrome* $n$ *in the vicinity of* $x$ *have? How many of them determine* $n$ *completely?)*

(ii) *Deduce from (i) that if* $\alpha > 1/2$ *is any fixed constant, then*

$$\sum_{n \ palindrome} \frac{1}{n^{\alpha}}$$

*is convergent while*

$$\sum_{\substack{n\leq x \\ n \ palindrome}} \frac{1}{n^{1/2}} \asymp \log x.$$

*(Hint: Use the Abel summation formula with* $a_n = 1$ *if* $n$ *is a palindrome and* $a_n = 0$ *otherwise.)*

**Problem 4.4.** *Use Theorem* 4.5 *with Remark* 4.6 *to prove that*

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x}\left(1+O\left(\frac{1}{\log x}\right)\right) \qquad (x\to\infty),$$

*a result often called Mertens' theorem or Mertens' formula.*

**Problem 4.5.** *Use Problem* 4.4 *to show that*

$$\prod_{p\leq x}\left(1+\frac{1}{p}\right) = \frac{6e^{\gamma}}{\pi^2}\log x\left(1+O\left(\frac{1}{\log x}\right)\right) \qquad (x\to\infty).$$

**Problem 4.6.** *Generalize Problem* 4.5 *by showing that for each nonzero real number* $\kappa$*, there exists a positive constant* $c_\kappa$ *such that*

$$\prod_{p\le x}\left(1+\frac{\kappa}{p}\right)=c_\kappa(\log x)^\kappa\left(1+O\left(\frac{1}{\log x}\right)\right)\qquad(x\to\infty).$$

**Problem 4.7.** *Let* $\mathcal{S}$ *be the set of all positive integers of the form* $2^a+b^2$ *for some positive integers* $a$ *and* $b$*. Show that*

$$\sum_{n\in\mathcal{S}}\frac{1}{n}$$

*is convergent.*

*Chapter 5*

# The Proof of the Prime Number Theorem

## 5.1. A theorem of D. J. Newman

**Theorem 5.1.** *(Newman) Suppose that* $a_n \in \mathbb{C}$ *with* $|a_n| \leq 1$ *for* $n = 1, 2, \ldots$. *Form the series*

$$\sum_{n\geq 1} \frac{a_n}{n^s}. \tag{5.1}$$

*The series converges to a function* $F(s)$ *which is analytic for* $\mathrm{Re}(s) > 1$. *Assume that it can be extended analytically to an open set that contains the half plane* $\mathrm{Re}(s) \geq 1$. *Then, series* (5.1) *converges to* $F(s)$ *for all complex numbers* $s$ *with* $\mathrm{Re}(s) \geq 1$.

**Proof.** We essentially follow Newman's 1980 original proof [**112**].

First, fix a number $w \in \mathbb{C}$ chosen in the half-plane $\mathrm{Re}(w) \geq 1$. With such a choice, we certainly have that the function $F(s+w)$ is holomorphic in the half-plane $\mathrm{Re}(s) \geq 0$. Choose a real number $R \geq 1$ and determine a positive number $\delta = \delta(R) \leq 1/2$ and a real number $M = M(R)$ in such a way that the function $F(s+w)$ is holomorphic and bounded by $M$ in the domain $|s| \leq R$, $\mathrm{Re}(s) \geq -\delta$.

Now, consider the counterclockwise contour $\Gamma$ bounded by the line segment $\mathrm{Re}(s) = -\delta$ and the arc $|z| = R$. Moreover, let $\Gamma = A \cup B$, where $A$ and $B$, respectively, are the parts of $\Gamma$ in the right and left half-planes.

By Cauchy's Integral formula, for any positive integer $N$, we have

$$2\pi i F(w) = \int_\Gamma F(s+w)N^s \left(\frac{1}{s} + \frac{s}{R^2}\right) ds. \tag{5.2}$$

Now, on part $A$ of the contour, the function $F(s+w)$ is equal to its power series representation, which we split as

$$F(s+w) = \sum_{n=1}^{N} \frac{a_n}{n^{s+w}} + \sum_{n=N+1}^{\infty} \frac{a_n}{n^{s+w}} = S_N(s+w) + T_N(s+w),$$

say. Again using the Cauchy Integral formula, we get

$$\int_A S_N(s+w)N^s \left(\frac{1}{s} + \frac{s}{R^2}\right) ds = 2\pi i S_N(w) - \int_{-A} S_N(s+w)N^s \left(\frac{1}{s} + \frac{s}{R^2}\right) ds, \tag{5.3}$$

where $-A$ stands for the reflection of $A$ through the origin. Therefore, by changing $s$ into $-s$, (5.3) can be written as

$$\int_A S_N(s+w)N^s \left(\frac{1}{s} + \frac{s}{R^2}\right) ds = 2\pi i S_N(w) - \int_A S_N(w-s)N^{-s} \left(\frac{1}{s} + \frac{s}{R^2}\right) ds. \tag{5.4}$$

Combining (5.2) and (5.4), we obtain

$$\begin{aligned} 2\pi i(F(w) - S_N(w)) &= \int_A \left(T_N(s+w)N^s - \frac{S_N(w-s)}{N^s}\right)\left(\frac{1}{s} + \frac{s}{R^2}\right) ds \\ &\quad + \int_B F(s+w)N^s \left(\frac{1}{s} + \frac{s}{R^2}\right) ds. \end{aligned} \tag{5.5}$$

Our goal is to show that

$$\lim_{N\to\infty} S_N(w) = F(w). \tag{5.6}$$

To do so, we proceed as follows. We write $s = x + iy$, where $x, y \in \mathbb{R}$ and $|s| = R$, so that

$$\frac{1}{s} + \frac{s}{R^2} = \frac{2x}{R^2}, \tag{5.7}$$

$$|T_N(s+w)| \le \sum_{n=N+1}^{\infty} \frac{1}{n^{x+1}} \le \int_N^\infty \frac{du}{u^{x+1}} = \frac{1}{xN^x} \tag{5.8}$$

and

$$|S_N(w-s)| \le \sum_{n=1}^{N} n^{x-1} \le N^{x-1} + \int_0^N u^{x-1} du \le N^{x-1} + \frac{N^x}{x},$$

so that

$$|S_N(w-s)| \le N^x \left(\frac{1}{N} + \frac{1}{x}\right). \tag{5.9}$$

Therefore, combining estimates (5.7), (5.8), and (5.9), we get

$$\begin{aligned}
&\left|\int_A \left(T_N(s+w)N^s - S_N(w-s)N^{-s}\right)\left(\frac{1}{s}+\frac{s}{R^2}\right)ds\right| \\
&\leq \left|\int_A \left(\frac{1}{x}\,\frac{N^x}{N^x} + N^x\left(\frac{1}{N}+\frac{1}{x}\right)N^{-x}\right)\frac{2x}{R^2}ds\right| \\
&\leq \int_A \left(\frac{2}{x}+\frac{1}{N}\right)\frac{2x}{R^2}ds \qquad (5.10)\\
&= \int_A \left(\frac{4}{R^2}+\frac{2x}{NR^2}\right)ds \leq \int_A \left(\frac{4}{R^2}+\frac{2}{NR}\right)ds \\
&= \pi R\left(\frac{4}{R^2}+\frac{2}{NR}\right) = \frac{4\pi}{R}+\frac{2\pi}{N}.
\end{aligned}$$

We now estimate the integral over $B$. First observe that

$$\left|\frac{1}{s}+\frac{s}{R^2}\right| = \left|\frac{1}{s}\right|\left|\frac{\overline{s}}{s}+\frac{s\overline{s}}{R^2}\right| \leq \frac{1}{\delta}\left(1+\frac{|s|^2}{R^2}\right) \leq \frac{2}{\delta}$$

for $\mathrm{Re}(s) = -\delta$ and $|s| \leq R$. Therefore, since $|F(s+w)|$ is at most $M$, we see that

(5.11)

$$\begin{aligned}
\left|\int_B F(s+w)N^s\left(\frac{1}{s}+\frac{s}{R^2}\right)ds\right| &\leq \int_{-R}^{R} M\,\frac{2}{\delta}\,N^{-\delta}dy + 2\left|\int_{-\delta}^{0} MN^x\,\frac{2x}{R^2}\,2dx\right| \\
&\leq \frac{4MR}{\delta N^\delta} + \frac{8M}{R^2}\left|\int_{-\delta}^{0} xN^x dx\right| \\
&< \frac{4MR}{\delta N^\delta} + \frac{8M\delta}{R^2}\left(\frac{1}{\log N} - \frac{1}{N^\delta \log N}\right) \\
&< \frac{4RM}{\delta N^\delta} + \frac{8M\delta}{R^2\log N}.
\end{aligned}$$

Using (5.10) and (5.11) in (5.5), we obtain

$$|2\pi i(F(w) - S_N(w))| \leq \frac{4\pi}{R} + \frac{2\pi}{N} + \frac{4RM}{\delta N^\delta} + \frac{8M\delta}{R^2\log N},$$

so that

$$|F(w) - S_N(w)| \leq \frac{2}{R} + \frac{1}{N} + \frac{RM}{\delta N^\delta} + \frac{2M\delta}{R^2\log N}.$$

Given $\varepsilon > 0$, choose $R = 3/\varepsilon$. Then for $N$ sufficiently large, we have $|F(w) - S_N(w)| < \varepsilon$. Thus, $S_N(w) \longrightarrow F(w)$ as $N \to \infty$, which proves (5.6), thus completing the proof of Newman's theorem. □

## 5.2. An application of Newman's theorem

We can use Newman's theorem to prove the following result.

**Theorem 5.2.**

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0. \tag{5.12}$$

**Proof.** For $\sigma > 1$, we have

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

It follows from Theorems 3.2 and 3.6 that $f(s) = (s-1)\zeta(s)$ is analytic in the region $\sigma > 0$ and that it has no zeros in the region $\sigma \geq 1$. Hence, $1/\zeta(s)$ is analytic in the region $\sigma \geq 1$. In fact, a formula is

$$\frac{1}{\zeta(s)} = \frac{s-1}{s\left(1-(s-1)\int_1^{\infty} \frac{\{x\}}{x^{s+1}}\,dx\right)} \tag{5.13}$$

valid for $\sigma \geq 1$, by Theorem 3.2. By Theorem 5.1, we have that $\sum_{n\geq 1} \frac{\mu(n)}{n^s}$ converges to $\frac{1}{\zeta(s)}$ for all $s$ with $\sigma \geq 1$. In particular, it converges at $s = 1$, so that formula (5.13) implies the desired conclusion. □

**Theorem 5.3.**

$$\sum_{n\leq x} \mu(n) = o(x) \qquad \text{as } x \to \infty. \tag{5.14}$$

**Proof.** The result follows from Theorem 5.2 and Problem 4.1. □

## 5.3. The proof of the Prime Number Theorem

We are now ready to prove the Prime Number Theorem.

**Theorem 5.4.** *As $x \to \infty$,*

$$\pi(x) \sim \frac{x}{\log x}.$$

**Proof.** By Theorem 4.2, it is sufficient to prove that $\psi(x) \sim x$. Put

$$F(x) = \sum_{n\leq x} \left(\psi\left(\frac{x}{n}\right) - \left\lfloor \frac{x}{n} \right\rfloor + 2\gamma\right).$$

By the Möbius inversion formula (Theorem 4.8(ii)), we have

$$\psi(x) - \lfloor x \rfloor + 2\gamma = \sum_{n\leq x} \mu(n) F\left(\frac{x}{n}\right).$$

It remains to show that

$$\sum_{n\leq x} \mu(n) F\left(\frac{x}{n}\right) = o(x) \qquad \text{as } x \to \infty. \tag{5.15}$$

To do this, we first estimate $F(x)$. We have

$$F(x) = \sum_{n \le x} \psi\left(\frac{x}{n}\right) - \sum_{n \le x} \left\lfloor \frac{x}{n} \right\rfloor + 2\gamma \lfloor x \rfloor.$$

On the other hand,

$$\begin{aligned}
\sum_{n \le x} \psi\left(\frac{x}{n}\right) &= \sum_{n \le x} \sum_{m \le x/n} \Lambda(m) = \sum_{m \le x} \Lambda(m) \left( \sum_{n \le x/m} 1 \right) \\
&= \sum_{m \le x} \Lambda(m) \left\lfloor \frac{x}{m} \right\rfloor = \sum_{\substack{p^k \le x \\ k \ge 1}} (\log p) \left\lfloor \frac{x}{p^k} \right\rfloor \\
&= \sum_{p \le x} \left( \left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{x}{p^2} \right\rfloor + \cdots \right) \log p \\
&= \log(\lfloor x \rfloor !) = \sum_{n \le x} \log n,
\end{aligned}$$

and, recalling (4.10), that is,

$$\sum_{n \le x} \log n = x \log x - x + O(\log x),$$

we obtain

$$\sum_{n \le x} \psi\left(\frac{x}{n}\right) = x \log x - x + O(\log x).$$

Furthermore, by Theorem 4.9,

$$\begin{aligned}
\sum_{n \le x} \left\lfloor \frac{x}{n} \right\rfloor &= \sum_{n=1}^{\lfloor x \rfloor} \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor \\
&= \lfloor x \rfloor \log \lfloor x \rfloor + (2\gamma - 1) \lfloor x \rfloor + O(x^{1/2}) \\
&= (x - \{x\}) \log(x - \{x\}) + (2\gamma - 1)(x - \{x\}) + O(x^{1/2}) \\
&= x \log x + x \log\left(1 - \frac{\{x\}}{x}\right) + (2\gamma - 1)x + O(x^{1/2}) \\
&= x \log x + (2\gamma - 1)x + O(x^{1/2}),
\end{aligned}$$

where we used the fact that

$$\log\left(1 - \frac{\{x\}}{x}\right) = \log\left(1 + O\left(\frac{1}{x}\right)\right) = O\left(\frac{1}{x}\right).$$

Therefore,

$$\begin{aligned}
F(x) &= (x \log x - x + O(x^{1/2})) - (x \log x + (2\gamma - 1)x + O(x^{1/2})) \\
&\qquad +(2\gamma x + O(1)) \\
&= O(x^{1/2}).
\end{aligned}$$

This last estimate implies that there is a positive constant $c$ such that

$$|F(x)| \le cx^{1/2} \qquad \text{for all } x \ge 1.$$

Now let $t$ be an integer larger than 1. Then

$$\begin{aligned}\left|\sum_{n<x/t} \mu(n)F\left(\frac{x}{n}\right)\right| &\le \sum_{n<x/t}\left|F\left(\frac{x}{n}\right)\right| \le c\sum_{n<x/t}\left(\frac{x}{n}\right)^{1/2} \\ &\le cx^{1/2}\left(1+\int_1^{x/t}\frac{du}{u^{1/2}}\right) \\ &\le cx^{1/2}\left(1+2u^{1/2}\Big|_{u=1}^{u=x/t}\right) \\ &\le cx^{1/2}\left(1+2\left(\frac{x}{t}\right)^{1/2}-2\right) < \frac{2cx}{t^{1/2}}.\end{aligned} \tag{5.16}$$

Observe that $F$ is a step function. In particular, if $a$ is an integer and $a \le x < a+1$, then $F(x) = F(a)$. Therefore,

$$\begin{aligned}\sum_{x/t<n\le x} \mu(n)F\left(\frac{x}{n}\right) &= F(1)\sum_{x/2<n\le x}\mu(n) + F(2)\sum_{x/3<n\le x/2}\mu(n) \\ &\quad + \cdots + F(t-1)\sum_{x/t<n\le x/(t-1)}\mu(n).\end{aligned}$$

It follows that

$$\begin{aligned}\left|\sum_{x/t<n\le x} \mu(n)F\left(\frac{x}{n}\right)\right| &\le |F(1)|\left|\sum_{x/2<n\le x}\mu(n)\right| \\ &\quad + \cdots + |F(t-1)|\left|\sum_{x/t<n\le x/(t-1)}\mu(n)\right| \\ &\le (|F(1)| + \cdots + |F(t-1)|)\max_{2\le i\le t}\left|\sum_{x/i<n\le x/(i-1)}\mu(n)\right|.\end{aligned} \tag{5.17}$$

But

$$\sum_{x/i<n\le x/(i-1)}\mu(n) = \sum_{n\le x/(i-1)}\mu(n) - \sum_{n\le x/i}\mu(n) = o(x),$$

by Theorem 5.2, if $i \ge 2$ is fixed and $x$ tends to infinity. Now we have all we need. Let $\varepsilon \in (0, 1/4)$. Choose $t = \lfloor 1/\varepsilon^{1/2} \rfloor \ge 1/(2\varepsilon^{1/2})$. There exists $x_\varepsilon$ such that

$$\left|\sum_{n\le y}\mu(n)\right| < \varepsilon y$$

for all $y > x_\varepsilon$. Thus, if $x$ is such that $x > ty_\varepsilon$, then $x/i > y_\varepsilon$ for all $i = 1, \ldots, t$. Therefore,

(5.18)
$$\left| \sum_{x/i < n \le x/(i-1)} \mu(n) \right| \le \left| \sum_{n \le x/(i-1)} \mu(n) \right| + \left| \sum_{n \le x/i} \mu(n) \right| < \varepsilon \left( \frac{x}{i} + \frac{x}{i-1} \right) \le 2\varepsilon x$$

for $i = t, t-1, \ldots, 2$. Now inequalities (5.17) and (5.18) give

$$\left| \sum_{x/t < n \le x} \mu(n) F\left(\frac{x}{n}\right) \right| \le 2\varepsilon x \sum_{i=1}^{t-1} |F(i)| \le 2\varepsilon x \sum_{i=1}^{t-1} c i^{1/2} < 2c\varepsilon t^{3/2} x,$$

which together with estimate (5.16) yields

$$\begin{aligned} \left| \sum_{n \le x} \mu(n) F\left(\frac{x}{n}\right) \right| &< \left| \sum_{n \le x/t} \mu(n) F\left(\frac{x}{n}\right) \right| + \left| \sum_{x/t < n \le x} \mu(n) F\left(\frac{x}{n}\right) \right| \\ &< c\left( \frac{2x}{t^{1/2}} + 2\varepsilon t^{3/2} x \right) < cx\left( 2\sqrt{2}\varepsilon^{1/4} + 2\varepsilon^{1/4} \right) \\ &< 5c\varepsilon^{1/4} x. \end{aligned}$$

We may therefore conclude that

$$\left| \sum_{n \le x} \mu(n) F\left(\frac{x}{n}\right) \right| = o(x) \qquad \text{as } x \to \infty,$$

so that $\psi(x) \sim x$, as required. □

## 5.4. A review of the proof of the Prime Number Theorem

Let us review the major steps of our proof of the Prime Number Theorem. We first used the Chebyshev estimates (Theorem 2.6) to show that the Prime Number Theorem is equivalent to $\psi(x) \sim x$ (Theorem 4.2). Then we introduced the Riemann Zeta Function $\zeta(s)$ for $\sigma > 1$. An application of Abel's summation formula allowed us to write down a different formula for $\zeta(s)$ (Theorem 3.2) which makes sense for all $\sigma > 0$ except at $s = 1$. This function is analytic in the region $\sigma \ge 1$ with $s \ne 1$ (Proposition 3.5) and has no zeros in this region (Theorem 3.6). Thus, $1/\zeta(s)$ is defined everywhere for $\sigma > 0$ (even at $s = 1$ where its value is zero) and is analytic in this region.

The Euler product representation formula (4.14) allowed us to link $1/\zeta(s)$ with the Möbius function when $\sigma > 1$, and a technical result from complex analysis of D. J. Newman allowed us to conclude that this representation

is true on the line $\sigma = 1$ as well. This leads us to the conclusion that the series of general term $\mu(n)/n$ is convergent and that its sum is zero. Then, the Abel summation formula (or Problem 4.1) allowed us to conclude that the summatory function of $\mu(n)$ up to $x$ is $o(x)$ as $x \to \infty$ (Theorem 5.2). Finally, this result in conjunction with a result on the summatory function of the number of divisors function (Theorem 4.9) were put together to finally achieve the holy grail. Do you think that was hard ? Well, if you answered yes, then you are right. Nevertheless, we believe this is the easiest proof to understand of the Prime Number Theorem known today.

## 5.5. The Riemann Hypothesis and the Prime Number Theorem

We have thus proved the Prime Number Theorem using results from complex analysis. But how much complex analysis did we use? Actually, we only used the fact that $\zeta(s)$ has no zeros in the region $\sigma \geq 1$ ($s \neq 1$). What do the zeros of the Riemann Zeta Function have to do with the prime numbers? First of all, there are infinitely many zeros. This was proved by Hadamard [**73**] in 1893. An effective form of it was proved by von Mangoldt [**105**] in 1905. Let $x$ be any positive real number. Let $N(x)$ be the number of zeros $\rho$ of $\zeta(s)$ of the form $\rho = \sigma + it$, where $\sigma \in (0,1)$ and $0 \leq t \leq x$. (Note that $t > 0$ by Problem 3.1.) Then von Mangoldt proved that

$$N(x) = \frac{x}{2\pi} \log\left(\frac{x}{2\pi}\right) - \frac{x}{2\pi} + O(\log x).$$

The connection between the zeros $\rho = \sigma + it$ of the Riemann Zeta Function and the Prime Number Theorem is given by the remarkable formula

$$\psi(x) = x - \sum_{\substack{\rho=\sigma+it \\ |t|\leq x}} \frac{x^\rho}{\rho} + O(\log^2 x) \tag{5.19}$$

valid for all $x \geq 2$ and proved by von Mangoldt [**104**] in 1895. Note that Riemann had already conjectured this formula in his famous 1859 paper [**120**]. If the Riemann Hypothesis is true, the formula implies that

$$\psi(x) - x = O(x^{1/2}(\log x)^2). \tag{5.20}$$

Recall the *logarithmic integral* $\mathrm{li}(x)$ defined in (2.6). Estimate (5.20) implies that

$$\pi(x) - \mathrm{li}(x) = O(x^{1/2} \log x). \tag{5.21}$$

On the other hand, if the Riemann Hypothesis is false, then the error of approximating $\pi(x)$ by $\mathrm{li}(x)$ exceeds $x^{1/2+\delta}$ for some small positive number $\delta$ if $x$ is large. Indeed, assume that $\rho = \sigma + it$ is a zero of $\zeta(s)$ where

$\sigma \neq 1/2$. We may then assume that $\sigma > 1/2$. Indeed, Riemann proved the now famous *functional equation*, namely

$$\Gamma(s/2)\pi^{-s/2}\zeta(s) = \Gamma\left(\frac{1-s}{2}\right)\pi^{-(1-s)/2}\zeta(1-s), \tag{5.22}$$

where

$$\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt \tag{5.23}$$

is the (Euler) Gamma Function. Formula (5.22) shows that the zeros of the Riemann Zeta Function in the region $0 < \sigma < 1$ (called the *critical strip*) are symmetric with respect to the axis $\sigma = 1/2$ (called the *critical line*). This formula is due to Riemann [**120**]. In fact, using formula (5.22) one may extend the Riemann Zeta Function to the whole complex plane except at $s = 1$. Note that formula (5.22) shows that the zeros $\rho$ of $\zeta(s)$ are symmetric with respect to the $t = 0$ axis as well. Thus, if there is a zero away from the line $\sigma = 1/2$, then there is one to the right of it in the first quadrant and the term corresponding to it in von Mangoldt's formula (5.19) will create an error term of size $\gg x^\sigma$. It is known that many zeros are indeed on the critical line. Hardy proved in 1915 that there are infinitely many. Selberg proved that there is a positive proportion of them on the critical line, and Levinson [**96**] showed that this proportion is at least 1/3. The current record holder is Conrey [**25**] with 40%. However, all these results are useless as far as approximation (5.21) is concerned since from what we have seen, even one zero off the critical line will create a large error when approximating $\pi(x)$ by $\mathrm{li}(x)$.

Without the Riemann Hypothesis, the best-known bound for the difference between $\pi(x)$ and $\mathrm{li}(x)$ is given by

$$\pi(x) = \mathrm{li}(x) + O\left(\frac{x}{\exp(c_2(\log x)^{3/5}(\log\log x)^{-1/5})}\right), \tag{5.24}$$

which appears in the book by Walfisz [**144**]. Here $c_2$ is a positive constant, which Popov [**116**] showed in 1994 could be taken as 0.00006888.

## 5.6. Useful estimates involving primes

The following classical explicit formulas are very useful in applications. We shall not prove them. They can be found in Rosser and Schoenfeld [**124**].

**Proposition 5.5.** (i) *The inequality*

$$\frac{x}{\log x - 0.5} < \pi(x) \qquad \textit{holds for all } x \geq 67.$$

(ii) *The inequality*

$$\pi(x) < \frac{x}{\log x - 1.5} \qquad \textit{holds for all } x > e^{3/2}.$$

We already know that the Prime Number Theorem implies that $p_n = n\log n + o(n\log n)$ as $n \to \infty$, where $p_n$ is the $n$-th prime. More specifically, the following result holds. (See also Rosser and Schoenfeld [**124**].)

**Proposition 5.6.** *Let $p_n$ be the $n$-th prime. Then,*

$$n(\log n + \log\log n - 1.5) < p_n \qquad \textit{for all } n \geq 2,$$

*and*

$$p_n < n(\log n + \log\log n - 0.5) \qquad \textit{for all } n \geq 20.$$

Since the Rosser and Schoenfeld paper, there have been several improvements for the above inequalities. For instance see Dusart's paper [**40**].

## 5.7. Elementary proofs of the Prime Number Theorem

At the beginning of the 20th century, it was widely believed that no one would ever establish an elementary proof of the Prime Number Theorem. By "elementary", we mean "without the use of complex variables". After all, the proofs of Hadamard and de la Vallée Poussin established that the Prime Number Theorem was equivalent to the fact that $\zeta(1+it) \neq 0$ for every real number $t$.

But, in 1949, using the Selberg estimate

$$\sum_{p\leq x} \log^2 p + \sum_{pq\leq x} \log p \log q = 2x\log x + O(x),$$

Erdős [**48**] and Selberg [**126**] obtained an elementary proof of the Prime Number Theorem. Since then, the proof has been considerably simplified. In particular, the proof found by H. Daboussi [**28**] in 1984 is particularly elegant.

## Problems on Chapter 5

**Problem 5.1.** *Let $n = q_1^{\ell_1}\cdots q_r^{\ell_r}$, where $q_1, \ldots, q_r$ are distinct primes and the $\ell_i$'s are positive integers. Show that*

$$d(n) = (\ell_1 + 1)\cdots(\ell_r + 1).$$

**Problem 5.2.** *Show that*

$$\sum_{x<p\le 2x}\frac{1}{p}=O\left(\frac{1}{\log x}\right).$$

**Problem 5.3.** *Show that*

$$\sum_{x<p\le x^2}\frac{1}{p}=\log 2+o(1)$$

*as* $x\to\infty$.

**Problem 5.4.** *Show that the Prime Number Theorem is a consequence of the fact that*

$$\lim_{x\to\infty}\left(\sum_{p\le x}\frac{\log p}{p}-\log x\right)$$

*exists. Compare with Theorem* 4.4. *(Hint: Use Abel's summation formula.)*

**Problem 5.5.** *Show that the Prime Number Theorem is equivalent to the fact that*

$$\lim_{x\to\infty}\left(\sum_{n\le x}\frac{\Lambda(n)}{n}-\log x\right)$$

*exists. Compare with Theorem* 4.3.

**Problem 5.6.** *Assume estimate* (5.20) *holds for all positive real numbers* $x$. *Show that estimate* (5.21) *also holds. (Hint: Use Abel's summation formula.)*

**Problem 5.7.** *Show that* $\Gamma(n)=(n-1)!$, *where* $\Gamma(s)$ *is given by formula* (5.23).

**Problem 5.8.** *Show that there exists a constant* $c$ *such that the inequality*

$$\sum_{p\,|\,n}\frac{1}{p}\le\log\log\log n+c$$

*holds for all integers* $n\ge e^{e^e}$. *(Hint: Let* $\omega(n)=k$. *The right-hand side does not change if we replace all the prime factors of* $n$ *by* $p_1,\dots,p_k$. *Now use Mertens' estimate (Theorem* 4.5*) and what is known about* $k$.*)*

**Problem 5.9.** *Let* $k$ *be a positive integer. Let*

$$f_k(n)=\#\{(d_1,\dots,d_k)\ :\ \operatorname{lcm}[d_1,\dots,d_k]=n\}.$$

*Show that* $f_k(n)=n^{O(k/\log\log n)}$.

**Problem 5.10.** *Use approximation* (5.24) *to show that*

$$\pi(2x)<2\pi(x)$$

*if* $x>x_0$, *for some large* $x_0$.

**Problem 5.11.** *Prove that for every integer $k > 1$ there exists an integer $n$ such that $k\pi(n) = n$.* REMARK: *The reader might be interested in consulting De Koninck's book* [**30**] *to appreciate the size of each of the sets $A_k = \{n \in \mathbf{N} : n/\pi(n) = k\}$ for $2 \le k \le 32$ and that, curiously, $A_{11}$ contains only one element, that is, $A_{11} = \{175197\}$; could it be that $A_{11}$ is the only set $A_k$ containing only one element?*

**Problem 5.12.** *Show that $d(n)$ is odd if and only if $n$ is a perfect square.*

**Problem 5.13.** *Provide the details of Crandall and Pomerance's heuristic argument (see their book* [**27**]*) which yields that the number of Mersenne primes $2^p - 1$ with $p \le x$ should be approximately $\dfrac{e^\gamma}{\log 2}\log x + O(1)$.*

*(Hint: First show that if $q$ is a prime factor of $2^p - 1$, then $q \equiv 1 \pmod p$. In particular, if $n = 2^p - 1$, then $n$ has no prime factors smaller than $p > (\log n)/\log 2$. But if we already know that $n$ is free of small primes, then it has an enhanced chance of being prime. That is, the probability of such an $n$ to actually be prime should be $e^\gamma \log\log n/\log n$, where $e^\gamma \log\log n$ comes from the fact that the probability that $n$ is coprime to all primes $q < \log n$ is $\prod_{q<\log n}(1 - 1/q) \sim e^{-\gamma}/\log\log n$ as $n \to \infty$ by Mertens' formula. This implies that the number of Mersenne primes $2^p - 1$ with $p \le x$ should be approximately*

$$\sum_{p\le x} \frac{e^\gamma \log\log(2^p-1)}{\log(2^p-1)} = \frac{e^\gamma}{\log 2}\sum_{p\le x}\frac{\log p}{p} + O(1) = \frac{e^\gamma}{\log 2}\log x + O(1),$$

*where we used Problem* 5.4*, thus proving our claim.)*

**Problem 5.14.** *Let $f : [2,\infty) \to \mathbf{R}^+$ be a continuous function such that $f(n)/\log n$ is decreasing on $[2,\infty)$. Then,*

$$\sum_{p\le x} f(p) = (1 + o(1))\int_2^x \frac{f(t)}{\log t}\,dt + O(1) \qquad (x \to \infty).$$

**Problem 5.15.** *Show that the following estimates hold as $x \to \infty$:*

$$\begin{aligned}
\sum_{p\le x}\frac{\log p}{p} &\sim \int_2^x \frac{dt}{t} + O(1) \sim \log x,\\
\sum_{p\le x}\frac{1}{p} &\sim \int_2^x \frac{dt}{t\log t} + O(1) \sim \log\log x,\\
\sum_{p\le x}\frac{1}{p\log p} &\sim \int_2^x \frac{dt}{t\log^2 t} + O(1) \sim \frac{1}{\log 2} + O(1) = O(1).
\end{aligned}$$

*Chapter 6*

# The Global Behavior of Arithmetic Functions

## 6.1. Dirichlet series and arithmetic functions

An arithmetic function is simply a sequence of complex numbers. In other words, $f$ is an *arithmetic function* if $f : \mathbb{N} \to \mathbb{C}$. The study of arithmetic functions is interesting because it reveals information about the anatomy of the integers. For instance, by establishing that

$$\sum_{n \le x} \omega(n) \sim x \log\log x \qquad (x \to \infty),$$

where $\omega(n)$ stands for the number of distinct prime factors of $n$, we will learn that on average a number $n$ has approximately $\log\log n$ factors. Various other arithmetic functions will also help us gain more information on the multiplicative structure of integers.

The set of arithmetic functions can be subdivided into different classes. For instance, a large class of arithmetic functions share the property of being multiplicative. An arithmetic function $f$ is said to be *multiplicative* if $f(1) = 1$ and if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$; it is said to be *totally multiplicative* (or *completely multiplicative*) if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all positive integers $m, n$. A function $f$ is said to be *strongly multiplicative* if it is multiplicative and if $f(p^a) = f(p)$ for each prime number $p$ and each positive integer $a$. It is easy to show that $\phi(n)/n$ is strongly multiplicative while $\sigma(n)$ is not.

The study of arithmetic functions, and in particular that of multiplicative functions, is highly simplified if one examines their associated Dirichlet

series. Indeed, given an arithmetic function $f$, consider the corresponding series

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \tag{6.1}$$

where $s$ is a complex variable. This series is then called the *generating function* of $f(n)$.

To keep the presentation of Dirichlet series as simple as possible, in this chapter we shall only examine (as did Dirichlet himself!) the case where $s$ is a real variable. We allow ourselves to do so because the results can easily be generalized to the case where $s \in \mathbb{C}$. However, $f(n)$ can be complex.

It is clear that the convergence or divergence of the series (6.1) depends on the nature of the arithmetic function $f(n)$ and on the interval to which $s$ belongs. For instance, the Dirichlet series $\sum_{n=1}^{\infty} n^n/n^s$ diverges for all real $s$, while $\sum_{n=1}^{\infty} n^{-n}/n^s$ converges for all real $s$. On the other hand, one can show that, for a given function $f(n)$, if there exist two real numbers $s_1 < s_2$ such that $\sum_{n=1}^{\infty} f(n)/n^{s_1}$ diverges and $\sum_{n=1}^{\infty} f(n)/n^{s_2}$ converges, then there exists a real number $\alpha_c$ such that $\sum_{n=1}^{\infty} f(n)/n^s$ converges for $s > \alpha_c$ and diverges for $s < \alpha_c$. This number $\alpha_c = \alpha_c(f)$ is called the *abscissa of convergence* of the series $\sum_{n=1}^{\infty} f(n)/n^s$. On the other hand, for most problems, we shall be interested in the *abscissa of absolute convergence*, that is, the unique real number $\alpha_a$ such that $\sum_{n=1}^{\infty} |f(n)|/n^s$ converges if $s > \alpha_a$ and diverges if $s < \alpha_a$; such a number $\alpha_a$ exists if one can find two real numbers $s_1 < s_2$ such that $\sum_{n=1}^{\infty} |f(n)|/n^{s_1}$ diverges and $\sum_{n=1}^{\infty} |f(n)|/n^{s_2}$ converges.

Observe that we don't always have $\alpha_a = \alpha_c$: consider, for example, the series $\sum_{n=1}^{\infty}(-1)^n/n^s$ for which we clearly have $\alpha_c = 0$ and $\alpha_a = 1$.

Series of the form $\sum_{n=1}^{\infty} f(n)/n^s$ are called "Dirichlet series" because Gustav Lejeune Dirichlet (1805–1859, Germany) was the first not only to discover their main properties but also to use them to establish new results in number theory. For instance, in 1837 he established that in any arithmetic progression there exist infinitely many primes, or in other words, given two coprime positive integers $a$ and $b$, there exist infinitely many primes of the form $an + b$. His proof was based on the study of the series

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

commonly called an *L-series*, where $\chi(n)$ is an arithmetic function with values in $\mathbb{C}$ and satisfying the properties $\chi(1) = 1$, $\chi(mn) = \chi(m)\chi(n)$ and $|\chi(n)| \in \{0, 1\}$ for each $n \geq 1$. We shall study this topic in depth in Chapter 14.

The most well-known Dirichlet series is certainly

$$\sum_{n=1}^{\infty} \frac{1}{n^s},$$

that is, the Riemann Zeta Function, which we studied extensively in Chapter 3.

Given an arithmetic function $f(n)$, we denote by $I_a = I_a(f)$ the set of $s \in \mathbb{R}$ for which $\sum_{n=1}^{\infty} |f(n)|/n^s$ converges and by $J_a = J_a(f)$ the set of $s \in \mathbb{R}$ for which $\sum_{n=1}^{\infty} |f(n)|/n^s$ diverges, so that $I_a \cup J_a = \mathbb{R}$.

**Theorem 6.1.** *Let $f(n)$ be an arithmetic function. Assume that $I_a(f) \neq \emptyset$ and that $J_a(f) \neq \emptyset$. Then the Dirichlet series $\sum_{n=1}^{\infty} f(n)/n^s$ has a finite abscissa of absolute convergence.*

**Proof.** Since $J_a$ is a nonempty set bounded from above (actually bounded by each element of $I_a$), it has a least upper bound $b = \sup J_a$. If $s < b$, then $s \in J_a$, and if $s > b$, then $s \in I_a$. It follows from this that $\alpha_a$ exists and that $\alpha_a = b$. □

For convenience, if for a given series $\sum f(n)/n^s$, we have $I_a(f) = \mathbb{R}$, we write $\alpha_a = -\infty$, while in the case where $J_a(f) = \mathbb{R}$, we write $\alpha_a = +\infty$.

**Example 6.2.** *Let $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Then $\alpha_a = 1$.*

**Example 6.3.** *Let $F(s) = \sum_{n=1}^{\infty} \frac{\log n}{n^s}$. Then $\alpha_a = 1$.*

**Example 6.4.** *Let $F(s) = \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}$, where $\phi$ stands for the Euler function. Since $\phi(n) \leq n$, we have $\alpha_a \leq 2$. Since $\phi(p) = p - 1$, we have $\alpha_a \geq 2$. It follows that $\alpha_a = 2$.*

## 6.2. The uniqueness of representation of a Dirichlet series

Let $\sum_{n=1}^{\infty} f(n)/n^s$ be a Dirichlet series with a finite absolute abscissa of convergence $\alpha_a$. It is easy to prove that for each fixed $s > \alpha_a$, the series $\sum_{n=1}^{\infty} f(n)/n^s$ converges uniformly in the interval $[s, +\infty)$. The series

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \tag{6.2}$$

which is the uniform limit of a sequence of continuous functions, is itself a continuous function. The following result is certainly one of the most important results concerning Dirichlet series, since it is the one that guarantees that the function $F(s)$ has a unique representation in the form (6.2).

**Theorem 6.5.** *Let*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{and} \quad G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$$

*be two Dirichlet series with the same abscissa of absolute convergence $\alpha_a$. Assume that there exists a divergent sequence $s_1 < s_2 < \cdots < s_k < \cdots$ such that $F(s_k) = G(s_k)$ for each $k \in \mathbb{N}$. Then $f(n) = g(n)$ for each positive integer $n$.*

**Proof.** Let $h(n) = f(n) - g(n)$ and $H(s) = F(s) - G(s)$. We will show that $h \equiv 0$. To do so, we proceed by contradiction by assuming that there exists $n \in \mathbb{N}$ such that $h(n) \neq 0$. So let $x$ be the smallest positive integer such that $h(x) \neq 0$. We then have, for $s > \alpha_a$,

$$H(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s} = \sum_{n=x}^{\infty} \frac{h(n)}{n^s} = \frac{h(x)}{x^s} + \sum_{n=x+1}^{\infty} \frac{h(n)}{n^s}.$$

From this relation, it follows that

$$h(x) = x^s\, H(s) - x^s \sum_{n=x+1}^{\infty} \frac{h(n)}{n^s}.$$

Since $H(s_k) = 0$, this means that

$$h(x) = -x^{s_k} \sum_{n=x+1}^{\infty} \frac{h(n)}{n^{s_k}}.$$

Let $c > \alpha_a$. Choose $k$ large enough so that $s_k > c$. Then

$$\begin{aligned} |h(x)| &\leq x^{s_k} \sum_{n=x+1}^{\infty} \frac{|h(n)|}{n^{s_k}} = x^{s_k} \sum_{n=x+1}^{\infty} \frac{|h(n)|}{n^{c+(s_k-c)}} \\ &\leq \frac{x^{s_k}}{(x+1)^{s_k-c}} \sum_{n=x+1}^{\infty} \frac{|h(n)|}{n^c} \\ &= \left(\frac{x}{x+1}\right)^{s_k} (x+1)^c \sum_{n=x+1}^{\infty} \frac{|h(n)|}{n^c}. \end{aligned}$$

But since $x$ is fixed, $\left(\frac{x}{x+1}\right)^{s_k} \to 0$ as $k \to \infty$, while the expressions $(x+1)^c$ and $\sum_{n=x+1}^{\infty} \frac{|h(n)|}{n^c}$ remain bounded. This means that $h(x) = 0$, which contradicts the minimal choice of $x$. □

## 6.3. Multiplicative functions

Recall that a function $f : \mathbb{N} \to \mathbb{C}$ is said to be *multiplicative* if $f(1) = 1$ and if $f(mn) = f(m)f(n)$ for all positive integers $m$ and $n$ such that $(m, n) = 1$.

The generating function of a multiplicative function can be represented as an Euler product; indeed, one can easily check that if $f$ is multiplicative, then, if $\mathrm{Re}(s) > \alpha_a(f)$,

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\right).$$

**Example 6.6.** (i) *The Euler function $\phi(n)$ is multiplicative and*

$$\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \prod_p \left(1 + \frac{p-1}{p^s} + \frac{p(p-1)}{p^{2s}} + \cdots\right).$$

*(See Example* 6.11.*)*

(ii) *The Möbius function $\mu(n)$ is multiplicative and*

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right).$$

(iii) *For any complex number $s$, the $s$-th power function $f_s(n) = n^s$ is multiplicative. When $s = 0$, we get the constant function* **1**, *and when $s = 1$ we get the identity function* **id**.

Multiplicative functions can be "multiplied" using a convolution product, the result being also multiplicative. Indeed, given two arithmetic functions $f$ and $g$, define the *Dirichlet product* of $f$ and $g$, which we denote by $f * g$, as the arithmetic function $h$ defined by

$$h(n) = \sum_{ab=n} f(a)\, g(b), \tag{6.3}$$

where the sum runs over pairs of positive integers $(a, b)$ such that $ab = n$. It is clear that this sum is equal to

$$\sum_{d|n} f(d)\, g(n/d) \quad \text{or} \quad \sum_{d|n} f(n/d)\, g(d).$$

**Proposition 6.7.** *Let $f,\ g : \mathbb{N} \longrightarrow \mathbb{C}$ be two multiplicative functions. Define*

$$(f * g)(n) = \sum_{d \,|\, n} f(d)g(n/d).$$

*Then $f * g$ is multiplicative.*

**Proof.** It is clear that $(f * g)(1) = 1$. It is not hard to see that if $m$ and $n$ are coprime, then every divisor $d$ of $mn$ can be written uniquely as $d = d_1 d_2$, where $d_1 \mid m$ and $d_2 \mid n$ (namely, take $d_1 = (d, m)$ and $d_2 = (d, n)$) and vice versa, if $d_1 \mid m$ and $d_2 \mid n$, then $d_1 d_2 \mid mn$. Thus,

$$\begin{aligned}
(f * g)(mn) &= \sum_{d \,|\, mn} f(d)g(mn/d) = \sum_{\substack{d_1 \,|\, m \\ d_2 \,|\, n}} f(d_1 d_2)g(mn/d_1 d_2) \\
&= \sum_{d_1 \,|\, m} \sum_{d_2 \,|\, n} f(d_1)f(d_2)g(m/d_1)g(n/d_2) \\
&= \left( \sum_{d_1 \,|\, m} f(d_1)g(m/d_1) \right) \left( \sum_{d_2 \,|\, n} f(d_2)g(n/d_2) \right) \\
&= (f * g)(m)(f * g)(n),
\end{aligned}$$

which proves that $f * g$ is multiplicative. □

**Example 6.8.** (i) *Since*

$$\phi(n) = \sum_{d \,|\, n} \mu(d)\frac{n}{d} = (\mu * \mathbf{id})(n),$$

*a relation we will prove in Problem* 8.1 *(i), the Euler function $\phi(n)$ is the convolution of the Möbius function $\mu(n)$ and the identity function* **id**.

(ii) *Since*

$$d(n) = \sum_{d \,|\, n} 1 = (\mathbf{1} * \mathbf{1})(n),$$

*the number of divisors function $d(n)$ is the convolution of the constant function* **1** *with itself.*

(iii) *If $s \in \mathbb{C}$ is any complex number, then the sum of the $s$-th powers of the divisors of $n$*

$$\sigma_s(n) = \sum_{d \,|\, n} d^s = (f_s * \mathbf{1})(n)$$

*is the convolution of the $s$-th power function $f_s(n) = n^s$ with the constant function* **1**. *Note that (ii) is the particular case $s = 0$. When $s = 1$, we simply write $\sigma(n)$ and refer to it as the sum of divisors of $n$.*

If $f$ is multiplicative, then

$$f(\prod_{i=1}^{k} q_i^{\alpha_i}) = \prod_{i=1}^{k} f(q_i^{\alpha_i})$$

whenever $q_1, \ldots, q_k$ are distinct primes and $\alpha_i$ are positive integers for all $i = 1, \ldots, k$.

## 6.4. Generating functions and Dirichlet products

We now give some theorems and examples which provide a fairly good sample of the applications that can be obtained from the preceding theorems.

Generating functions proves very useful when one multiplies together two Dirichlet series to produce a third one, since we then recognize the link with the Dirichlet product.

**Theorem 6.9.** *Let $F(s) = \sum f(n)/n^s$ and $G(s) = \sum g(n)/n^s$ be two Dirichlet series whose abscissa of absolute convergence are $\alpha_a(f)$ and $\alpha_a(g)$ respectively. Then if $s > \max(\alpha_a(f), \alpha_a(g))$,*

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s},$$

*where $h = f * g$.*

**Proof.** Since the variable $s$ is located inside the domain of absolute convergence which is common to both series, one can in the process of multiplication rearrange the terms at will. This is why

$$\begin{aligned} F(s)G(s) &= \sum_{m=1}^{\infty} \frac{f(m)}{m^s} \cdot \sum_{n=1}^{\infty} \frac{g(n)}{n^s} = \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{f(m)g(n)}{(mn)^s} \\ &= \sum_{r=1}^{\infty} \frac{\sum_{mn=r} f(m)g(n)}{r^s} = \sum_{r=1}^{\infty} \frac{h(r)}{r^s}, \end{aligned}$$

where $h(r) = \sum_{mn=r} f(m)g(n) = (f * g)(r)$. □

**Example 6.10.** *Recall that $E(1) = 1$ and $E(n) = 0$ if $n > 1$. Since $\sum_{d|n} \mu(d) = E(n)$ (see Theorem 4.8 (i)), in other words $\mathbf{1} * \mu = E$, it follows from Theorem 4.8 that for $s > 1$,*

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1 * \mu(n)}{n^s} = \sum_{n=1}^{\infty} \frac{E(n)}{n^s} = 1,$$

*so that*

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}.$$

**Example 6.11.** *It is easy to establish that* $\sum_{d|n} \phi(d) = n$. *(See, for instance, De Koninck and Mercier's book* [**34**] *or Problem* 8.1 *below). It follows that*

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \cdot \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{n}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^{s-1}} = \zeta(s-1).$$

*From this, we obtain that*

$$\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} \qquad (s > 2).$$

**Remark 6.12.** *The Möbius inversion formula (Theorem* 4.8 *(iii)) can be stated and proved using Dirichlet products. Indeed, the statement of this result can be written as follows:*

$$g = \mathbf{1} * f \Longleftrightarrow f = \mu * g.$$

*To prove* ($\Rightarrow$), *multiply both sides of* $g = \mathbf{1} * f$ *by* $\mu$, *which yields* $\mu * g = \mu * \mathbf{1} * f = E * f = f$, *and the result follows. To prove* ($\Leftarrow$), *multiply* $f = \mu * g$ *on both sides by* $\mathbf{1}$, *so that* $\mathbf{1} * f = \mathbf{1} * \mu * g = E * g = g$, *which completes the proof. Notice that we used the fact that* $*$ *is associative, which follows easily from the definition of* $*$.

## 6.5. Wintner's theorem

The "global" behavior of arithmetic functions turns out in general to be fairly easy to study. By global behavior of an arithmetic function, we mean its average behavior on a large set of positive integers. More precisely, given an arithmetic function $f(n)$, we shall be interested in the behavior of

$$M_x(f) = \frac{1}{x} \sum_{n \le x} f(n), \tag{6.4}$$

that is, the average of $f$ over the interval $[1, x]$. If $\lim_{x\to\infty} M_x(f)$ exists, we say that the *asymptotic mean value* of $f$ exists, in which case we write

$$M(f) = \lim_{x\to\infty} M_x(f). \tag{6.5}$$

The asymptotic mean value of an arithmetic function $f$ can, in some cases, be studied using information provided by the generating function of $f$, that is, by examining the representation $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$.

We start by giving a result which turns out to be very useful in revealing the asymptotic behavior of certain multiplicative arithmetic functions.

**Theorem 6.13.** *(Wintner) Let $f(n)$ and $g(n)$ be arithmetic functions such that*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \zeta(s) \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \qquad (s > 1), \tag{6.6}$$

*where $\displaystyle\sum_{n=1}^{\infty} \frac{g(n)}{n}$ converges absolutely. Then $M(f)$ exists and is equal to $\displaystyle\sum_{n=1}^{\infty} \frac{g(n)}{n}$.*

**Remark 6.14.** *In other words, if the generating function of $f(n)$ is a "multiple" of $\zeta(s)$ and if this multiple is bounded when $s = 1$, then this is sufficient to conclude that the asymptotic mean value of $f$ exists.*

**Proof.** From (6.6) and Theorem 6.9, we have $f = 1 * g$. Hence,

$$\begin{aligned} \sum_{n \le x} f(n) &= \sum_{n \le x} \sum_{d \mid n} g(d) = \sum_{d \le x} g(d) \left\lfloor \frac{x}{d} \right\rfloor \\ &= x \sum_{d \le x} \frac{g(d)}{d} - \sum_{d \le x} g(d) \left( \frac{x}{d} - \left\lfloor \frac{x}{d} \right\rfloor \right) \\ &= x \sum_{d \le x} \frac{g(d)}{d} + O\left( \sum_{d \le x} |g(d)| \right) \\ &= x S_1(x) + O(S_2(x)), \end{aligned} \tag{6.7}$$

say. On the one hand,

$$S_1(x) = \sum_{n=1}^{\infty} \frac{g(d)}{d} + O\left( \sum_{d > x} \frac{g(d)}{d} \right) = \sum_{n=1}^{\infty} \frac{g(d)}{d} + o(1), \tag{6.8}$$

because of the absolute convergence of $\displaystyle\sum_{n=1}^{\infty} \frac{g(n)}{n}$. On the other hand,

$$\begin{aligned} S_2(x) &= \sum_{d \le \sqrt{x}} \frac{|g(d)|}{d} \cdot d + \sum_{\sqrt{x} < d \le x} \frac{|g(d)|}{d} \cdot d \\ &\le x^{1/2} \sum_{d \le \sqrt{x}} \frac{|g(d)|}{d} + x \sum_{\sqrt{x} < d \le x} \frac{|g(d)|}{d} \\ &= O(x^{1/2}) + o(x) = o(x), \end{aligned} \tag{6.9}$$

where again we used the absolute convergence of $\sum_{n=1}^{\infty} \frac{g(n)}{n}$.

Substituting (6.8) and (6.9) in (6.7), the theorem is proved. □

Applications of Wintner's theorem are numerous. The following two examples are among the classical ones.

**Example 6.15.** *The density of the set of squarefree numbers is equal to* $6/\pi^2$*, that is approximately* 0.61*. More precisely, one can show that*

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} \mu^2(n) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}. \tag{6.10}$$

*Indeed,*

$$\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} = \prod_p \left(1 + \frac{1}{p^s}\right) = \frac{\prod_p \left(1 - \frac{1}{p^{2s}}\right)}{\prod_p \left(1 - \frac{1}{p^s}\right)} = \frac{\zeta(s)}{\zeta(2s)}.$$

*But*

$$\zeta(2) = \prod_p \left(1 - \frac{1}{p^2}\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^2},$$

*a series which converges absolutely. Applying Wintner's theorem, one immediately obtains* (6.10) *by observing that* $\zeta(2) = \pi^2/6$.

**Example 6.16.** *The density of the set of positive integers whose exponents in the factorization* $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$ *are all smaller or equal to* 2*, that is,* $\alpha_i \le 2$ *for* $i = 1, 2, \ldots, r$*, is equal to* $1/\zeta(3)$*. Indeed, if* $\chi(n)$ *is the characteristic function of this set of integers, then*

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}}\right) = \frac{\prod_p \left(1 - \frac{1}{p^{3s}}\right)}{\prod_p \left(1 - \frac{1}{p^s}\right)} = \frac{\zeta(s)}{\zeta(3s)}.$$

*Applying Wintner's theorem, the result follows.*

In Hardy's famous book *Divergent Series* [**75**], one will find Axer's theorem, which is essentially a strengthening of Wintner's theorem.

**Theorem 6.17.** *(Axer) Let* $f(n)$ *and* $g(n)$ *be arithmetic functions such that*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \zeta(s) \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \qquad (s > 1),$$

*where* $\sum_{n=1}^{\infty} \frac{g(n)}{n}$ *converges and* $\sum_{d\le x} |g(d)| = O(x)$. *Then* $M(f)$ *exists and is equal to* $\sum_{n=1}^{\infty} \frac{g(n)}{n}$.

**Proof.** An elegant proof of Axer's theorem is given in Posnikov's book [**117**]. □

## 6.6. Additive functions

An arithmetic function $f$ is said to be *additive* if $f(mn) = f(m) + f(n)$ whenever $(m, n) = 1$. It follows from this definition that if $f$ is additive, then $f(1) = 0$ (since $f(1) = f(1) + f(1)$).

The obvious natural example of such a function is $f(n) = \log n$. The following additive functions are of particular interest in number theory:

$$\begin{aligned}
\omega(n) &= \sum_{p|n} 1 \\
&= \text{ the number of distinct prime factors of } n, \\
\Omega(n) &= \sum_{p^a \| n} a \\
&= \text{the total number of prime factors of } n \text{ counting their multiplicity}, \\
g(n) &= \log f(n), \\
&\quad \text{where } f \text{ is any multiplicative function such that } f(n) > 0.
\end{aligned}$$

It is easy to prove that if $f$ is additive and if $c$ is an arbitrary fixed real number, then $g(n) = cf(n)$ is also an additive function.

On the other hand, an arithmetic function $f$ is said to be *totally additive* (or *completely additive*) if $f(mn) = f(m) + f(n)$ for every pair of positive integers $m, n$. This is the case, for instance, of the function $f(n) = \log n$. One can easily establish that the function $\Omega(n)$ is totally additive while $\omega(n)$ is not.

A function $f$ is said to be *strongly additive* if it is additive and if moreover $f(p^a) = f(p)$ for each prime number $p$ and each positive integer $a$. It is obvious that $\omega(n)$ is strongly additive while the functions $\log n$ and $\Omega(n)$ are not.

While the Dirichlet series associated with a multiplicative function $f$ proved to be of great use to study the average behavior of $f(n)$ for $1 \le n \le x$, it does not provide the right information to study an additive function $f$.

Indeed, as we shall now see, various elementary methods end up being very useful to study the behavior of $\sum_{n\le x} f(n)$ when the function $f$ is additive.

## 6.7. The average orders of $\omega(n)$ and $\Omega(n)$

Given an arithmetic function $f(n)$, if one can find an increasing function $\rho(n)$ such that

$$\frac{1}{x}\sum_{n\le x} f(n) \sim \frac{1}{x}\sum_{n\le x} \rho(n) \qquad (x\to\infty),$$

we say that the *average order* of $f(n)$ is $\rho(n)$. We showed in the preceding chapter that the average order of $d(n)$ is $\log n$.

We first examine the average order of the functions $\omega(n)$ and $\Omega(n)$. A naive approach goes as follows:

$$\begin{aligned}\sum_{n\le x}\omega(n) &= \sum_{n\le x}\sum_{p\mid n} 1 = \sum_{p\le x}\left\lfloor\frac{x}{p}\right\rfloor\\ &= x\sum_{p\le x}\frac{1}{p} + \sum_{p\le x}\left(\left\lfloor\frac{x}{p}\right\rfloor - \frac{x}{p}\right)\\ &= x\sum_{p\le x}\frac{1}{p} + O(\pi(x)).\end{aligned}$$

Using Theorem 4.5 and the fact that $\pi(x) = O(x/\log x)$, we obtain

$$\begin{aligned}\sum_{n\le x}\omega(n) &= x\left(\log\log x + \beta + O\left(\frac{1}{\log x}\right)\right) + O\left(\frac{x}{\log x}\right)\\ &= x\log\log x + \beta x + O\left(\frac{x}{\log x}\right),\end{aligned} \tag{6.11}$$

where $\beta$ is the constant appearing in Remark 4.6.

Can one conclude from (6.11) that the average order of $\omega(n)$ is $\log\log n$? The answer is YES, since using (1.3), we have

$$\sum_{n\le x}\log\log n \sim x\log\log x \qquad (x\to\infty).$$

Now, how can we evaluate $\sum_{n\le x}\Omega(n)$? To do so, we proceed as follows:

$$\sum_{n\le x}\Omega(n) = \sum_{n\le x}\sum_{\substack{p^k\mid n\\ k\ge 1}} 1 = \sum_{\substack{p^k\le x\\ k\ge 1}}\left\lfloor\frac{x}{p^k}\right\rfloor = \sum_{p\le x}\left\lfloor\frac{x}{p}\right\rfloor + \sum_{\substack{p^k\le x\\ k\ge 2}}\left\lfloor\frac{x}{p^k}\right\rfloor$$

$$\begin{aligned} &= x\sum_{p\le x}\frac{1}{p}+\sum_{p\le x}\left(\left\lfloor\frac{x}{p}\right\rfloor-\frac{x}{p}\right)+x\sum_{\substack{p^k\le x\\ k\ge 2}}\frac{1}{p^k}+\sum_{\substack{p^k\le x\\ k\ge 2}}\left(\left\lfloor\frac{x}{p^k}\right\rfloor-\frac{x}{p^k}\right)\\ &= x\left(\log\log x+\beta+O\left(\frac{1}{\log x}\right)\right)+O\left(\pi(x)\right)\\ &\qquad +x\sum_{p}\sum_{k\ge 2}\frac{1}{p^k}-x\sum_{k\ge 2}\sum_{p^k>x}\frac{1}{p^k}+O\left(\sum_{\substack{p^k\le x\\ k\ge 2}}1\right). \end{aligned}$$

Using Problems 6.8 and 6.9 as well as the fact that

$$\pi(x^{1/2})+\pi(x^{1/3})+\cdots\ll\log x\cdot\pi(x^{1/2})\ll x^{1/2},$$

we conclude that

$$\sum_{n\le x}\Omega(n)=x\log\log x+\left(\beta+\sum_{p}\frac{1}{p(p-1)}\right)x+O\left(\frac{x}{\log x}\right). \tag{6.12}$$

**Remark 6.18.** *Even though $\Omega(n)\ge\omega(n)$, comparing formulas* (6.11) *and* (6.12)*, we observe that the two functions $\omega(n)$ and $\Omega(n)$ have the same mean value. It is also interesting to observe that one can deduce from* (6.11) *and* (6.12) *that the function $f(n)=\Omega(n)-\omega(n)$ does indeed have an asymptotic mean value, namely $\displaystyle\sum_{p}\frac{1}{p(p-1)}$.*

## 6.8. The average order of an additive function

Let $f$ be an arbitrary additive function. Then we have

$$\begin{aligned} \sum_{n\le x}f(n) &= \sum_{n\le x}\sum_{p^a\|n}f(p^a)=\sum_{n\le x}\sum_{\substack{p^a\mid n\\ a\ge 1}}\left(f(p^a)-f(p^{a-1})\right)\\ &= \sum_{\substack{p^a\le x\\ a\ge 1}}\left(f(p^a)-f(p^{a-1})\right)\left\lfloor\frac{x}{p^a}\right\rfloor. \end{aligned}$$

Removing the brackets, we can write

$$\begin{aligned} \sum_{n\le x}f(n) &= x\sum_{p\le x}\frac{f(p)}{p}+x\sum_{\substack{p^a\le x\\ a\ge 2}}\frac{f(p^a)-f(p^{a-1})}{p^a}+\sum_{p\le x}f(p)\left(\left\lfloor\frac{x}{p}\right\rfloor-\frac{x}{p}\right)\\ &\qquad +\sum_{\substack{p^a\le x\\ a\ge 2}}\left(f(p^a)-f(p^{a-1})\right)\left(\left\lfloor\frac{x}{p^a}\right\rfloor-\frac{x}{p^a}\right). \end{aligned} \tag{6.13}$$

In the case where $f$ is strongly additive, it follows from (6.13) that

$$\sum_{n\le x} f(n) = x\sum_{p\le x}\frac{f(p)}{p} + \sum_{p\le x} f(p)\left(\left\lfloor\frac{x}{p}\right\rfloor - \frac{x}{p}\right). \tag{6.14}$$

Hence, setting $f=\omega$, relation (6.11) follows almost immediately from (6.14).

It follows from (6.13) that if $f$ is an additive function such that $f(p)=1$ and $f(p^a)-f(p^{a-1})$ stays bounded, the average value of $f(n)$ is the same as that of the function $\omega(n)$, that is, $\log\log n$. This is made explicit in the following result.

**Theorem 6.19.** *Let $f$ be an additive function such that $f(p)=1$ for each prime number $p$ and such that $f(p^a)-f(p^{a-1})=O(1)$ uniformly for $p$ prime and $a\ge 2$. Then*

$$\sum_{n\le x} f(n) = x\log\log x + D_1 x + O\left(\frac{x}{\log x}\right), \tag{6.15}$$

*where*

$$D_1 = \sum_{a\ge 2}\sum_{p}\frac{f(p^a)-f(p^{a-1})}{p^a} + \gamma + \sum_{p}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right).$$

Wintner's theorem has been improved by many. A key improvement was otained by Delange in 1961. Here we state the result without proof.

**Theorem 6.20.** *(Delange [**37**]) Let $f(n)$ be a multiplicative function such that $|f(n)|\le 1$ for all $n\in N$ and such that $\sum_p(1-f(p))/p$ converges. Then the limit*

$$M(f) := \lim_{x\to\infty}\frac{1}{x}\sum_{n\le x} f(n)$$

*exists and*

$$M(f) = \prod_p\left(1-\frac{1}{p}\right)\left(1+\sum_{k=1}^{\infty}\frac{f(p^k)}{p^k}\right).$$

## 6.9. The Erdős-Wintner theorem

The first chapter of Wintner's 1944 book [**148**] is devoted to the study of arithmetic functions $f(n)$ and $g(n)$ connected by the relation $f=1*g$.

We say that a function $F:\mathbb{R}\to[0,1]$ is a *distribution function* if it is nondecreasing, continuous from the right, and if it satisfies $F(-\infty)=0$ and $F(+\infty)=1$.

A sequence of distribution functions $\{F_k\}_{k\geq 1}$ is said to *converge weakly* to a function $F$ if $\lim_{k\to\infty} F_k(z) = F(z)$ for each point of continuity of $F$.

Finally, we say that a real arithmetic function $f$ *has a distribution function* $F$ if the sequence $\{F_k\}_{k\geq 1}$ defined by

$$F_k(z) := \frac{1}{k}\#\{n \leq k : f(n) \leq z\}$$

converges weakly to $F$.

**Theorem 6.21.** *(Erdős-Wintner* [**53**]*) Let $f(n)$ be a real additive function. The convergence of the three series*

$$\sum_{|f(p)|\geq 1} \frac{1}{p}, \qquad \sum_{|f(p)|<1} \frac{f(p)}{p}, \qquad \sum_{|f(p)|<1} \frac{f^2(p)}{p}$$

*is necessary and sufficient for the weak convergence of the sequence of distribution functions*

$$F_k(z) = \frac{1}{k} \sum_{\substack{n\leq k \\ f(n)\leq z}} 1$$

*as $k \to \infty$.*

## Problems on Chapter 6

**Problem 6.1.** *Let $f(1) = 1$ and, for each integer $n \geq 2$, let $f(n)$ be the product of the exponents in the factorization of $n$; in other words, for $n > 1$, if we write $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$, $r \geq 1$, $\alpha_i \in \mathbb{N}$, $q_i$ distinct primes, then $f(n) = \prod_{i=1}^{r} \alpha_i$. Prove that the asymptotic mean of $f(n)$ exists and is equal to $\dfrac{\zeta(2)\zeta(3)}{\zeta(6)}$.*

**Problem 6.2.** *Let $\beta(1) = 1$ and, for each $n \geq 2$, set $\beta(n) = \prod_{i=1}^{r} \dfrac{3+(-1)^{\alpha_i}}{2}$ if $n = q_1^{\alpha_1} \cdots q_r^{\alpha_r} > 1$. Prove that the asymptotic mean of $\beta(n)$ exists and is equal to $\dfrac{\zeta(2)}{\zeta(3)}$.*

**Problem 6.3.** *Prove that under the hypothesis of Wintner's theorem with the additional condition that $\sum_{n=1}^{\infty} \dfrac{g(n)}{n^s}$ converges absolutely for $s = \frac{1}{2} + \delta$ for*

*some $\delta > 0$, then it follows that*

$$\sum_{n\le x} f(n) = cx + O\left(x^{\frac{1}{2}+\delta}\right),$$

*where* $c = \sum_{n=1}^{\infty} \frac{g(n)}{n}$.

**Problem 6.4.** *Deduce from Problems* 6.2 *and* 6.3 *that for each $\varepsilon > 0$,*

$$\sum_{n\le x} \beta(n) = cx + O\left(x^{\frac{1}{2}+\varepsilon}\right),$$

*where* $c = \frac{\zeta(2)}{\zeta(3)} \approx 1.36843$.

**Problem 6.5.** *Let $\gamma(1) = 1$ and, for $n \ge 2$, let $\gamma(n) = \prod_{p|n} p$. Prove that*

$$\sum_{n\le x} \frac{\gamma(n)}{n} = (1 + o(1))cx \qquad (x \to \infty),$$

*where* $c = \prod_p \left(1 - \frac{1}{p(p+1)}\right)$.

**Problem 6.6.** *Is the sum of two additive functions always additive? What about the product of two additive functions?*

**Problem 6.7.** *Let $f$ be an additive function. Assume that for each positive integer $n$, $\lim_{k\to\infty} \frac{f(n^k)}{k}$ exists. Prove that the function $g$ defined by $g(n) = \lim_{k\to\infty} \frac{f(n^k)}{k}$ is totally additive.*

**Problem 6.8.** *Prove that* $\sum_{p>x} \frac{1}{p^2} \ll \frac{1}{x \log x}$.

**Problem 6.9.** *Prove that* $\sum_{a\ge 2} \sum_{p^a>x} \frac{a}{p^a} \ll \frac{1}{x^{1/2} \log x}$.

**Problem 6.10.** *Let $f$ be an additive function such that*

$$\sum_p \frac{|f(p) - 1|}{p} < +\infty$$

*and such that $f(p^a) - f(p^{a-1}) = O(1)$ uniformly for $p$ prime and $a \ge 2$. Prove that*

$$\sum_{n\le x} f(n) = x \log\log x + D_2 x + o(x),$$

*where*

$$D_2 = D_1 + \sum_p \frac{f(p)-1}{p} + \gamma$$

*and $D_1$ is the constant appearing in Theorem* 6.19.

**Problem 6.11.** *Let $f$ be an additive function such that*

$$\sum_{p>x} \frac{|f(p)-1|}{p} \ll \frac{1}{\log x}$$

*and such that $f(p^a)-f(p^{a-1}) = O(1)$ uniformly for all primes $p$ and integers $a \geq 2$. Prove that*

$$\sum_{n\leq x} f(n) = x\log\log x + D_2 x + O\left(\frac{x}{\log x}\right),$$

*where*

$$D_2 = D_1 + \sum_p \frac{f(p)-1}{p} + \gamma$$

*and $D_1$ is the constant appearing in Theorem* 6.19.

**Problem 6.12.** *Prove that*

$$\sum_{n\leq x} \log d(n) = (\log 2)x\log\log x + Ax + o(x) \qquad (x\to\infty),$$

*where*

$$A = \log 2\left\{\gamma + \sum_p \left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)\right\} + \sum_p \sum_{r\geq 2} \frac{\log(1+\frac{1}{p})}{p^r}.$$

*Chapter 7*

# The Local Behavior of Arithmetic Functions

## 7.1. The normal order of an arithmetic function

As proved by estimate (6.11), the average order of $\omega(n)$ is $\log\log n$. Does this mean that $\omega(n)$ is usually close to $\log\log n$ for most integers $n$? YES and NO. One can say NO because by choosing $n = 2^a$ (with $a$ very large), then $\omega(n) = 1$, while $\log\log n$ is obviously very large! On the other hand, one can say YES because, as we will show, the number of times that $\omega(n)$ is "far" from $\log\log n$ is negligible (in the sense given by Theorem 7.4 stated below).

To settle this apparent paradox, we introduce the notion of *normal order*. Given an arithmetic function $f(n)$, we say that $f(n)$ has a *normal order* if there exists a nonnegative nondecreasing function $\rho(n)$ such that, for each real number $\varepsilon > 0$,

$$\lim_{x\to\infty} \frac{1}{x} \# \left\{ n \le x : \left| \frac{f(n)}{\rho(n)} - 1 \right| < \varepsilon \right\} = 1.$$

We shall at times use the notation

$$f(n) = (1 + o(1))\rho(n) \qquad \text{a.e.}$$

to signify that, in fact, the function $f(n)$ is asymptotically equal to $\rho(n)$ almost everywhere, that is, for all (positive) integers $n$ except for a set of integers of zero density.

To establish that $\omega(n)$ has normal order $\log\log n$, the Turán-Kubilius inequality described below will turn out to be a great asset.

## 7.2. The Turán-Kubilius inequality

Recall that $f(n)$ is strongly additive if $f(p^a) = f(p)$ for all integers $a \geq 1$ and all primes $p$.

**Theorem 7.1.** *(Turán-Kubilius inequality) Let $f$ be a strongly additive function. Then there exists an absolute constant $C > 0$ such that*

$$\frac{1}{x}\sum_{n\leq x}\left|f(n)-\sum_{p\leq x}\frac{f(p)}{p}\right|^2 \leq C\sum_{p\leq x}\frac{|f(p)|^2}{p}.$$

We will only prove this theorem in the particular case $f(n) = \omega(n)$, which we also state as a theorem.

**Theorem 7.2.** *As $x \to \infty$,*

$$\sum_{n\leq x}(\omega(n)-\log\log x)^2 = O(x\log\log x). \tag{7.1}$$

**Proof.** First of all, it follows from (6.11) that

$$\sum_{n\leq x}\omega(n) = x\log\log x + O(x). \tag{7.2}$$

Assume for now that

$$\sum_{n\leq x}\omega(n)^2 = x(\log\log x)^2 + O(x\log\log x) \tag{7.3}$$

and write

$$\sum_{n\leq x}1 = \lfloor x\rfloor = x + O(1). \tag{7.4}$$

Multiply estimate (7.4) by $(\log\log x)^2$, multiply estimate (7.2) by $-2\log\log x$, and then copy estimate (7.3) once again to get the three estimates

$$\begin{aligned}
\sum_{n\leq x}(\log\log x)^2 &= x(\log\log x)^2 + O((\log\log x)^2),\\
\sum_{n\leq x}(-2\omega(n)\log\log x) &= -2x(\log\log x)^2 + O(x\log\log x),\\
\sum_{n\leq x}\omega(n)^2 &= x(\log\log x)^2 + O(x\log\log x).
\end{aligned}$$

Summing these three estimates, we get

$$\sum_{n\leq x}(\omega(n)-\log\log x)^2 = O(x\log\log x),$$

which is what we wanted to prove.

It remains to prove (7.3). To do so, we proceed as follows. Observe that

$$\sum_{n\le x}\omega(n)^2=\sum_{n\le x}\left(\sum_{p\,|\,n}1\right)^2=\sum_{n\le x}\left(\sum_{p\,|\,n}1+2\sum_{\substack{p<q\\ pq\,|\,n}}1\right)=S_1+2S_2, \tag{7.5}$$

where

$$S_1=\sum_{n\le x}\sum_{p\,|\,n}1$$

and

$$S_2=\sum_{n\le x}\sum_{\substack{p<q\\ pq\,|\,n}}1.$$

It is easy to see that

$$S_1=\sum_{n\le x}\omega(n)=O(x\log\log x) \tag{7.6}$$

by estimate (7.2). Hence, we set our attention on $S_2$. Changing the order of summation, we obtain

$$\begin{aligned} S_2&=\sum_{\substack{p<q\\ pq\le x}}\sum_{\substack{n\le x\\ pq\,|\,n}}1=\sum_{\substack{p<q\\ pq\le x}}\left\lfloor\frac{x}{pq}\right\rfloor=\sum_{\substack{p<q\\ pq\le x}}\left(\frac{x}{pq}+O(1)\right)\\ &=x\sum_{\substack{p<q\\ pq\le x}}\frac{1}{pq}+O\left(\sum_{\substack{p<q\\ pq\le x}}1\right). \end{aligned} \tag{7.7}$$

Let $N(x)$ be the number of numbers $n\le x$ of the form $n=pq$ with $p<q$. Note that $N(x)$ represents the sum which is in the above error term. To bound $N(x)$, note that $p^2<pq\le x$, so that $p\le x^{1/2}$. Therefore,

$$\begin{aligned} N(x)&\le\sum_{p\le x^{1/2}}\pi\left(\frac{x}{p}\right)\ll\sum_{p\le x^{1/2}}\frac{x}{p\log(x/p)}\le\sum_{p\le x^{1/2}}\frac{x}{p\log(x^{1/2})}\\ &=\frac{2x}{\log x}\sum_{p\le x^{1/2}}\frac{1}{p}\ll\frac{x\log\log(x^{1/2})}{\log x}=o(x)\qquad\text{as } x\to\infty, \end{aligned}$$

where in the above estimates we used the fact that $p<x^{1/2}$ to conclude that $1/\log(x/p)\le 1/\log(x^{1/2})=2/\log x$ together with Mertens' estimate (Theorem 4.5). Hence, (7.7) becomes

$$S_2=x\sum_{\substack{p<q\\ pq\le x}}\frac{1}{pq}+o(x). \tag{7.8}$$

We now note that

$$\sum_{\substack{p<q\\ pq\le x}} \frac{1}{pq} = \frac{1}{2}\left\{ \left(\sum_{p\le x}\frac{1}{p}\right)^2 - \sum_{p\le x}\frac{1}{p^2} - 2\sum_{\substack{p<q\le x\\ pq>x}}\frac{1}{pq}\right\} = \frac{1}{2}(S_3^2 - S_4 - 2S_5), \tag{7.9}$$

where

$$S_3 = \sum_{p\le x}\frac{1}{p}, \qquad S_4 = \sum_{p\le x}\frac{1}{p^2} \qquad \text{and} \qquad S_5 = \sum_{\substack{p<q\le x\\ pq>x}}\frac{1}{pq}.$$

By Mertens' estimate (Theorem 4.5), we have

$$S_3 = \log\log x + O(1),$$

so that

$$S_3^2 = (\log\log x + O(1))^2 = (\log\log x)^2 + O(\log\log x). \tag{7.10}$$

Clearly,

$$S_4 = \sum_{p\le x}\frac{1}{p^2} < \sum_{p}\frac{1}{p^2} = O(1). \tag{7.11}$$

Finally, to estimate $S_5$, first observe that $q > x^{1/2}$. Thus,

$$\begin{aligned} S_5 &\le \left(\sum_{p\le x}\frac{1}{p}\right)\left(\sum_{x^{1/2}<q\le x}\frac{1}{q}\right) \\ &\le (\log\log x + O(1))(\log 2 + o(1)) \\ &= O(\log\log x), \end{aligned} \tag{7.12}$$

where we used Problem 5.3 to conclude that

$$\sum_{x^{1/2}<q\le x}\frac{1}{q} = \log 2 + o(1) \qquad \text{as } x\to\infty.$$

Substituting estimates (7.10), (7.11), and (7.12) into (7.9), we get that

$$\sum_{\substack{p<q\\ pq\le x}}\frac{1}{pq} = \frac{1}{2}(\log\log x)^2 + O(\log\log x),$$

which substituted in estimate (7.8) yields

$$S_2 = \frac{1}{2}x(\log\log x)^2 + O(x\log\log x).$$

Inserting the above estimate for $S_2$ together with estimate (7.6) into (7.5) establishes (7.3), thus completing the proof of Theorem 7.2. □

**Remark 7.3.** *Inequality (7.1) was first proved by Turán* [**143**] *in 1934; he used it to prove that* $\omega(n)$ *has a normal order (see the next theorem). Turán's inequality was generalized by Kubilius* [**94**] *in 1964 to additive functions. In Elliott's book* [**42**] *(page 147), one can find the following general statement of the Turán-Kubilius inequality:*

*"Given a complex-valued additive function* $f(n)$ *and any real* $x > 0$*, define*

$$E(x) = \sum_{p^k \le x} \frac{f(p^k)}{p^k}\left(1 - \frac{1}{p}\right) \quad \text{and} \quad D(x) = \left(\sum_{p^k \le x} \frac{|f(p^k)|^2}{p^k}\right)^{1/2} \ge 0.$$

*Then, the inequality*

$$\sum_{n \le x} |f(n) - E(x)|^2 \le 32xD^2(x) \tag{7.13}$$

*holds uniformly for all additive functions* $f(n)$ *and positive real numbers* $x$*."*

*This result implies in particular that*

$$\sum_{n \le x} \big(\Omega(n) - \log\log x\big)^2 = O(x \log\log x). \tag{7.14}$$

**Theorem 7.4.** *The functions* $\omega(n)$ *and* $\Omega(n)$ *each have normal order* $\log\log n$*.*

**Proof.** We proved in Theorem 7.2 that

$$\frac{1}{x}\sum_{n \le x} (\omega(n) - \log\log x)^2 \le C \log\log x. \tag{7.15}$$

For $x^{1/2} \le n \le x$, it is clear that

$$\log\log x - 1 < \log\log x - \log 2 = \log\log x^{1/2} \le \log\log n \le \log\log x,$$

which implies that relation (7.15) can be replaced by

$$\frac{1}{x}\sum_{n \le x} (\omega(n) - \log\log n)^2 \le C_1 \log\log x \tag{7.16}$$

for some appropriate constant $C_1$. Indeed, using the fact that $\omega(n) \ll \log x$ for all $n \le x$, it follows that

$$\sum_{n \le x} (\omega(n) - \log\log n)^2 = \sum_{x^{1/2} \le n \le x} (\omega(n) - \log\log n)^2 + \sum_{n < x^{1/2}} (\omega(n) - \log\log n)^2$$

$$
\begin{aligned}
&= \sum_{x^{1/2}\le n\le x} (\omega(n) - \log\log x + O(1))^2 \\
&\qquad + O(x^{1/2}(\log x)^2) \\
&= \sum_{x^{1/2}\le n\le x} (\omega(n) - \log\log x)^2 \\
&\qquad + \; O\Big(\sum_{n\le x}(\omega(n) + \log\log x)\Big) + O(x^{1/2}(\log x)^2) \\
&= O(x\log\log x) + O\Big(\sum_{n\le x}\omega(n)\Big) = O\Big(x\log\log x\Big),
\end{aligned}
$$

which proves (7.16).

In order to show that $\omega(n)$ has normal order $\log\log n$, it is certainly sufficient to prove that, if $\delta > 0$ is arbitrarily small, then

(7.17)

$$h_\delta(x) = \#\{n \le x : |\omega(n) - \log\log n| > (\log\log n)^{\frac{1}{2}+\delta}\} = o(x) \qquad (x\to\infty).$$

Now assume the contrary, that is, that $h_\delta(x) \ge \alpha x$, for a certain number $\alpha > 0$. Then

$$
\begin{aligned}
\sum_{n\le x}(\omega(n) - \log\log n)^2 &\ge \sum_{\substack{x^{1/2}<n\le x \\ |\omega(n)-\log\log n|>(\log\log n)^{\frac{1}{2}+\delta}}} (\omega(n) - \log\log n)^2 \\
&\ge \alpha x(\log\log x)^{1+2\delta},
\end{aligned}
$$

which contradicts (7.16), thus establishing (7.17).

With the same reasoning, one can easily show that $\Omega(n)$ also has normal order $\log\log n$. □

**Remark 7.5.** *The only multiplicative functions with a normal order are the functions $f(n) = n^c$, where $c$ is any fixed real number. This result was proved by Birch* [**12**] *in 1967. As a consequence of this result, $d(n)$ has no normal order, even though we know that it has an average order, namely $\log n$, as was shown by Theorem* 4.9. *In fact, one can show that $\log d(n)$ has normal order $(\log 2)\log\log n$ and that the "normal behavior" of $d(n)$ is $(\log n)^{\log 2}$, as is reflected by the next theorem.*

Before we state the next result, we introduce another notation.

**Definition 7.6.** *We say that $f(n) = g(n)$ almost everywhere and write*

$$f(n) = g(n) \quad a.e.$$

*if the set of positive integers $n$ such that $f(n) \ne g(n)$ is of density zero.*

**Theorem 7.7.** *We have*

$$d(n) = (\log n)^{\log 2 + o(1)} \qquad a.e.$$

**Proof.** First observe that

$$2^{\omega(n)} \le d(n) \le 2^{\Omega(n)}. \tag{7.18}$$

We proved in (7.17) that if $\delta > 0$ is a fixed arbitrarily small number, then

$$\#\{n \le x : |\omega(n) - \log\log n| > (\log\log n)^{\frac{1}{2}+\delta}\} = o(x) \quad (x \to \infty).$$

The same result holds when the function $\omega(n)$ is replaced by the function $\Omega(n)$.

Hence, let $A$ be the set of positive integers $n$ such that

$$|\Omega(n) - \log\log n| \le (\log\log n)^{\frac{1}{2}+\delta}.$$

This set has density 1. Therefore, if $n \in A$,

$$\begin{aligned} 2^{\Omega(n)} &= 2^{\log\log n + \Omega(n) - \log\log n} = 2^{\log\log n + O\left((\log\log n)^{\frac{1}{2}+\delta}\right)} \\ &= 2^{\log\log n\left(1 + O\left(\frac{1}{(\log\log n)^{\frac{1}{2}-\delta}}\right)\right)} = 2^{\log\log n(1+o(1))} \\ &= e^{(\log\log n)(1+o(1))\log 2} = (\log n)^{(1+o(1))\log 2}. \end{aligned}$$

Combining this result with (7.18), we have thus obtained that

$$d(n) \le 2^{\Omega(n)} = (\log n)^{(1+o(1))\log 2} \qquad a.e.$$

Similarly we can show that

$$(\log n)^{(1+o(1))\log 2} = 2^{\omega(n)} \le d(n) \qquad a.e.$$

From these two sets of inequalities, it follows that

$$d(n) = (\log n)^{(1+o(1))\log 2} \qquad a.e.,$$

thus proving our claim. □

## 7.3. Maximal order of the divisor function

**Definition 7.8.** *Let $f : \mathbb{N} \to \mathbb{C}$ and $g : [1, \infty) \to \mathbb{R}_+$. We say that $g$ is a maximal order of $f$ if*

$$\limsup_{n\to\infty} \frac{f(n)}{g(n)} = 1,$$

*or, equivalently, if for every $\varepsilon > 0$ there exists $n_\varepsilon$ such that*

$$\frac{f(n)}{g(n)} < 1 + \varepsilon \qquad \text{holds for all } n > n_\varepsilon$$

*with*

$$\frac{f(n)}{g(n)} > 1-\varepsilon \qquad \textit{holding for infinitely many } \ n.$$

In particular, if $g(n)$ is a maximal order of $f(n)$, then $f(n) = O(g(n))$ holds for all $n$.

In the rest of this chapter, we shall be interested in how large the functions $\Omega(n)$, $\omega(n)$ and $d(n)$ can be.

**Proposition 7.9.** *The inequality* $\Omega(n) \le (\log n)/\log 2$ *holds for all positive integers* $n$*, with equality holding when* $n$ *is a power of 2.*

**Proof.** Since

$$n = q_1^{\ell_1} \cdots q_r^{\ell_r} \ge 2^{\ell_1+\cdots+\ell_r} = 2^{\Omega(n)},$$

the desired inequality follows by taking logarithms. □

**Proposition 7.10.** *The function* $g(n) = \log n/\log\log n$ *defined for all* $n \ge 2$ *is a maximal order for the function* $\omega(n)$*.*

**Proof.** As usual, let $p_k$ stand for the $k$-th prime number. Let $n = q_1^{\ell_1} \cdots q_r^{\ell_r}$. Then $q_i \ge p_i$ for all $i = 1, \ldots, r$, and therefore

$$n = \prod_{i=1}^{r} q_i^{\ell_i} \ge \prod_{i=1}^{r} p_i = \exp\left(\sum_{i\le r} \log p_i\right),$$

so that

$$\log n \ge \sum_{i=1}^{r} \log p_i = \sum_{p\le p_r} \log p = \theta(p_r) = p_r(1+o(1)),$$

where the last estimate is the Prime Number Theorem. Since

$$p_r = (1+o(1))r\log r \qquad \text{as} \ \ r\to\infty$$

(see Proposition 5.6), we get that

$$\log n \ge (1+o(1))r\log r.$$

Thus, for each fixed $\varepsilon > 0$ there exists $r_\varepsilon$ such that

$$\log n \ge (1-\varepsilon)r\log r \qquad \text{whenever } r > r_\varepsilon.$$

If $r > (\log n)^{1-\varepsilon}$, we get that

$$\log n > (1-\varepsilon)^2 r\log\log n,$$

and therefore that

$$r < \frac{1}{(1-\varepsilon)^2}\,\frac{\log n}{\log\log n}. \tag{7.19}$$

Otherwise, if $r \le (\log n)^{1-\varepsilon}$, then it is clear that if $n$ is sufficiently large,

$$(\log n)^{1-\varepsilon} < \frac{1}{(1-\varepsilon)^2}\frac{\log n}{\log\log n},$$

in which case (7.19) holds. Since $y^{1-\varepsilon} < y/\log y$ holds for all $y > y_\varepsilon$, we get that if both $r$ and $n$ are sufficiently large (note that it suffices that $r$ is sufficiently large because then $n$ is also large, at least as large as the product of the first $r$ primes), then

$$\omega(n) = r < \frac{1}{(1-\varepsilon)^2}\,\frac{\log n}{\log\log n}.$$

Since $\varepsilon$ was chosen to be arbitrarily small, we get the upper bound.

The lower bound follows by taking $n = \prod_{i=1}^{r} p_i$, where $p_i$ stands for the $i$-th prime, and again using the Prime Number Theorem. □

**Remark 7.11.** *The last part of the proof of Proposition* 7.10 *can be summarized by saying that if* $r\log r \le (1+o(1))f(n)$ *as* $n\to\infty$, *where* $f : \mathbb{N}\to[1,+\infty)$ *is some function tending to infinity with* $n$ *(in our case,* $f(n)=\log n$*), then* $r \le (1+o(1))\log f(n)/\log\log f(n)$. *We will encounter this process of "inverting" inequalities several times in what follows.*

## 7.4. An upper bound for $d(n)$

**Proposition 7.12.** *The inequality*

$$d(n) = n^{O(1/\log\log n)}$$

*holds for all integers* $n \ge 3$.

**Proof.** Note that, for $n = \prod_{i=1}^{r} q_i^{\ell_i}$, we have

$$\begin{aligned}\log d(n) &= \sum_{i=1}^{r}\log(\ell_i+1)\\ &= \sum_{i=1}^{r}\left(\log((\ell_i+1)\log(i+1)) - \log\log(i+1)\right)\\ &= \sum_{i=1}^{r}\log((\ell_i+1)\log(i+1)) - \sum_{i=1}^{r}\log\log(i+1)\\ &= S_1 - S_2,\end{aligned} \tag{7.20}$$

say. To estimate $S_1$, we use the AGM inequality (see (1.18)) in its logarithmic form,

$$\frac{1}{r}\left(\sum_{i=1}^{r}\log x_i\right) \le \log\left(\frac{1}{r}\sum_{i=1}^{r} x_i\right)$$

with $x_i = (\ell_i+1)\log(i+1)$ and get

$$\begin{aligned} S_1 &= \sum_{i=1}^{r}\log((\ell_i+1)\log(i+1)) \le r\log\left(\frac{1}{r}\sum_{i=1}^{r}(\ell_i+1)\log(i+1)\right) \\ &\le r\log\left(\frac{2\log n}{r}\right), \end{aligned}$$

where the last inequality holds because $i+1 \le p_i \le q_i$ (where $p_i$ stands for the $i$-th prime) and therefore,

$$\sum_{i=1}^{r}(\ell_i+1)\log q_i = \log\left(\prod_{i=1}^{r} q_i^{\ell_i+1}\right) \le \log(n^2) = 2\log n.$$

Thus,

$$S_1 \le r\log(2(\log n)/r) = r\log\log n - r\log r + O(r). \tag{7.21}$$

To estimate $S_2$, we use the Abel summation formula with $x = r$, $a_n = 1$ and $f(t) = \log\log(t+1)$ to get that

$$\begin{aligned} S_2 &= \sum_{i=1}^{r}\log\log(i+1) = r\log\log(r+1) - \int_1^r \frac{\lfloor t\rfloor}{(t+1)\log(t+1)}dt \\ &= r\log\log(r+1) + O\left(\int_1^r \frac{dt}{\log t}\right) = r\log\log(r+1) + O(r). \end{aligned} \tag{7.22}$$

Thus, gathering (7.21) and (7.22) in (7.20), and using the fact that

$$r = \omega(n) \ll \frac{\log n}{\log\log n},$$

we have

$$\log d(n) \le r\log\log n - r\log r - r\log\log(r+1) + O(r) = f(r) + O\left(\frac{\log n}{\log\log n}\right), \tag{7.23}$$

where

$$f(r) = r\log\log n - r\log r - r\log\log(r+1).$$

The derivative of $f(r)$ is

$$f'(r) = \log\log n - 1 - \log r - \log\log(r+1) - \frac{r}{(r+1)\log(r+1)},$$

which is easily seen to have a maximum at $r = r_0(n)$ for large $n$. The point $r_0$ can be found by solving $f'(r_0) = 0$, which is equivalent to

$$\log\log n = \log r_0 + \log\log(r_0+1) + \frac{r_0}{(r_0+1)\log(r_0+1)}. \tag{7.24}$$

Now equation (7.24) gives

$$\begin{aligned} f(r) \le f(r_0) &= r_0(\log\log n - \log r_0 - \log\log(r_0+1)) \\ &= r_0\left(1 + \frac{r_0}{(r_0+1)\log(r_0+1)}\right) = O(r_0). \end{aligned} \tag{7.25}$$

Since estimate (7.24) gives $\log\log n \ge \log r_0 + \log\log r_0$, we have that $n \ge r_0 \log r_0$, so that $r_0 \ll \log n/\log\log n$. Therefore, estimates (7.25) and (7.23) lead to

$$\log d(n) \le f(r_0) \ll r_0 \ll \frac{\log n}{\log\log n},$$

which is the desired estimate. □

## 7.5. Asymptotic densities

We introduced the notion of *asymptotic density* in Section 1.8 of Chapter 1. Let us now give another (equivalent) definition.

**Definition 7.13.** *We say that a set of positive integers $A$ has asymptotic density $\lambda$ if*

$$\lambda = \lim_{x\to\infty} \frac{\#(A \cap [1,x])}{x}.$$

**Example 7.14.** *Let $A$ be the set of even numbers. Then*

$$\#(A \cap [1,x]) = \lfloor x/2 \rfloor = x/2 + O(1),$$

*so that*

$$\frac{\#(A \cap [1,x])}{x} = \frac{1}{2} + O\left(\frac{1}{x}\right) \qquad (x \to \infty),$$

*from which it follows that the set of even numbers has asymptotic density $1/2$.*

**Example 7.15.** *The set of primes $\wp$ has asymptotic density zero since*

$$\frac{\#(\wp \cap [1,x])}{x} = \frac{\pi(x)}{x} \ll \frac{1}{\log x}.$$

We say that a set of positive integers *contains almost all integers* if its asymptotic density is 1.

**Proposition 7.16.** *Let*

$$A = \{n : p^2 \mid n \text{ for some prime } p > \log\log n\}.$$

*Then $A$ is of asymptotic density zero.*

**Proof.** Let $x$ be a large positive real number. Let $n \le x$. We may assume that $n > x/\log x$ since there are at most $x/\log x = o(x)$ positive integers $n \le x/\log x$ as $x \to \infty$. Then

$$\log\log n > \log\log(x/\log x) = \log\log x + \log\left(1 - \frac{\log\log x}{\log x}\right) > \frac{1}{2}\log\log x$$

if $x > x_0$. Let $n \in A \cap [x/\log x, x]$. Then $p^2 \mid n$ for some $p > (\log\log x)/2$. Fix $p$. Then the number of such $n$ is at most $\lfloor x/p^2 \rfloor \le x/p^2$. Thus,

$$\begin{aligned} \#(A \cap [x/\log x, x]) &\le \sum_{p > (\log\log x)/2} \frac{x}{p^2} \le x \int_{(\log\log x)/2 - 1}^{\infty} \frac{dt}{t^2} \\ &= \frac{x}{\frac{\log\log x}{2} - 1} = o(x) \qquad \text{as } x \to \infty, \end{aligned}$$

which leads to the desired conclusion. □

**Proposition 7.17.** *The set $A = \{n : d(n) \mid n\}$ is of asymptotic density zero.*

We need the following lemma.

**Lemma 7.18.** *Let $\delta > 0$. Let*

$$A_\delta = \left\{ n : \left| \frac{\omega(n)}{\log\log n} - 1 \right| > \delta \right\}.$$

*Then $A_\delta$ is of asymptotic density zero.*

**Proof.** Let $x$ be a large positive real number. We may assume that $n > x/\log x$ since there are only $O(x/\log x) = o(x)$ positive integers $n \le x/\log x$ as $x \to \infty$. So, let $A(x) = \#(A_\delta \cap [x/\log x, x])$. We look at $n \in A_\delta \cap [x/\log x, x]$. For such $n$,

$$\begin{aligned} \log\log n &> \log\log(x/\log x) = \log(\log x - \log\log x) \\ &= \log\log x + \log\left(1 - \frac{\log\log x}{\log x}\right) > \log\log x - 1 \end{aligned}$$

for $x > x_\delta$. Hence, $\log\log n \in [\log\log x - 1, \log\log x]$. Since

$$|\omega(n) - \log\log n| > \delta \log\log n,$$

it follows easily that

$$\begin{aligned} |\omega(n) - \log\log x| &\ge |\omega(n) - \log\log n| - 1 > \delta\log\log n - 1 \\ &> \delta(\log\log x - 1) - 1 > (\delta/2)\log\log x \end{aligned}$$

for all $x > x_\delta$ and all $n \in A_\delta \cap [x/\log x, x]$. By the Turán-Kubilius inequality, we have

$$((\delta/2)\log\log x)^2\, A(x) \le \sum_{n\le x} (\omega(n) - \log\log x)^2 = O(x\log\log x).$$

Therefore,

$$A(x) \ll \frac{x}{\log\log x} = o(x) \qquad \text{as } x \to \infty,$$

where the constant implied by the above $\ll$ depends on $\delta$. The conclusion is then immediate. □

*Proof of Proposition* 7.17. By Lemma 7.18 with $\delta = 1/2$, the inequality $\omega(n) > (\log\log n)/2$ holds for almost all positive integers $n$. Furthermore, by Proposition 7.16, almost all positive integers $n$ have no prime factor $p > \log\log n$ such that $p^2 \mid n$. Thus, for almost all positive integers $n$, the number of primes $p \| n$ is

$$\ge (\log\log n)/2 - \pi(\log\log n) > (\log\log n)/3.$$

Now let $x$ be a large positive integer, and $n$ be one of the above integers $> x/\log x$. Then

$$(\log\log n)/3 > (\log\log(x/\log x))/3 > (\log\log x)/4$$

for $x > x_0$, say. Thus, such an integer $n$ has at least $K = \lfloor (\log\log x)/4 \rfloor$ prime factors $p \| n$. But then $2^K \mid d(n) \mid n$, so that $n \le x$ is a multiple of $2^K$. The number of such $n \le x$ is

$$\le \frac{x}{2^K} \ll \frac{x}{2^{(\log\log x)/4}} = \frac{x}{(\log x)^c} = o(x) \qquad \text{as } x \to \infty,$$

where $c = (\log 2)/4 > 0$. □

We now discuss a solution to the *Erdős Multiplication Table Problem.*

**Proposition 7.19.** *Let $N$ be a large positive integer, and let $A(N)$ be the number of distinct positive integers $n \le N^2$ which are the result of a multiplication $\kappa \cdot \ell$ of two positive integers $\kappa$ and $\ell$, where $\kappa \le N$ and $\ell \le N$. Then $A(N) = o(N^2)$ as $N \to \infty$.*

**Proof.** Proceeding as in the proof of Proposition 7.16, one can establish that, for each fixed $\varepsilon > 0$, all $\kappa \le N$ are such that $\Omega(\kappa) \in [(1-\varepsilon)\log\log N, (1+\varepsilon)\log\log N]$ except for a set of integers $\kappa$ of cardinality $o(N)$ as $N$ tends to infinity. Thus, the product of two such integers $\kappa$ and $\ell$ satisfies

$$\Omega(\kappa\ell) = \Omega(\kappa) + \Omega(\ell) \in [(2-2\varepsilon)\log\log N, (2+2\varepsilon)\log\log N].$$

However, all most integers $n \le N^2$ have $\Omega(n)$ in $[(1-\varepsilon)\log\log(N^2), (1+\varepsilon)\log\log(N^2)]$. Since

$$\log\log(N^2) = \log(2\log N) = \log\log N + \log 2 = (1+o(1))\log\log N,$$

the interval $[(1-\varepsilon)\log\log(N^2), (1+\varepsilon)\log\log(N^2)]$ is disjoint from $[(2-2\varepsilon)\log\log N, (2+2\varepsilon)\log\log N]$ say if $\varepsilon < 1/4$ and $N$ is sufficiently large. Thus, we conclude that numbers of the form $\kappa\ell$ for $\kappa \le N$, $\ell \le N$ form a set of cardinality $o(N^2)$ as $N$ tends to infinity. □

## 7.6. Perfect numbers

A positive integer $n$ is called *perfect* if $\sigma(n) = 2n$. Two distinct positive integers $m$ and $n$ are called *amicable* if $\sigma(n) - n = m$ and $\sigma(m) - m = n$. For example, $m = 220$ and $n = 284$ are amicable. Note that if $n$ and $m$ are amicable, then $m = \sigma(n) - n$, and $n + m = \sigma(n) = \sigma(m) = \sigma(\sigma(n) - n)$, so that $n$ is perfect or part of an amicable pair if and only if $\sigma(n) = \sigma(\sigma(n)-n)$.

The following characterization of even perfect numbers is due to Euler.

**Proposition 7.20.** *An even positive integer $n$ is perfect if and only if $n = 2^{p-1}(2^p - 1)$, where $p$ and $2^p - 1$ are both primes.*

**Proof.** Write $n = 2^\alpha m$, where $m$ is odd. Then $\sigma(n) = (2^{\alpha+1}-1)\sigma(m) = 2n = 2^{\alpha+1}m$, so we get that $2^{\alpha+1} - 1 \mid m$. Write $m = (2^{\alpha+1}-1)k$. Then

$$2^{\alpha+1}(2^{\alpha+1}-1)k = 2n = \sigma(n) = (2^{\alpha+1}-1)\sigma((2^{\alpha+1}-1)k). \tag{7.26}$$

Note now that $k$ and $(2^{\alpha+1}-1)k$ are divisors of $(2^{\alpha+1}-1)k$ and their sum is $2^{\alpha+1}k$. If $(2^{\alpha+1}-1)k$ would have more divisors, then $\sigma((2^{\alpha+1}-1)k) > 2^{\alpha+1}k$, but in this case the right-hand side of equation (7.26) would exceed the left-hand side of this equation. Thus, $k$ and $(2^{\alpha+1}-1)k$ are the only divisors of $(2^{\alpha+1}-1)k$ leading to the conclusion that $k = 1$ and that $2^{\alpha+1} - 1$ is prime. It follows that $\alpha + 1 = p$ is also prime, so that $n = 2^{p-1}(2^p - 1)$, where $p$ and $2^p - 1$ are both primes. □

## 7.7. Sierpiński, Riesel, and Romanov

An odd number $k$ is called a *Sierpiński number* if $k \cdot 2^n + 1$ is composite for each $n \ge 1$. The reason for this name is that, in 1960, Sierpiński [**131**] proved that there exist infinitely many such numbers $k$, and in particular that 201 446 503 145 165 177 is one of these numbers, without however claiming it was the smallest Sierpiński number (see H.C. Williams [**147**]).

In 1962, Selfridge proved that 78 557 is also a Sierpiński number. To prove that 78 557 is a Sierpiński number, Selfridge showed that at least one of the prime numbers 3, 5, 7, 13, 19, 37, 73 divides $78\,557 \cdot 2^n + 1$ for all integers $n \geq 1$. More precisely he showed that

$$\begin{aligned}
n &\equiv 1 \pmod 3 &&\Longrightarrow 7 | 78557 \cdot 2^n + 1 \\
n &\equiv 11 \pmod{12} &&\Longrightarrow 13 | 78557 \cdot 2^n + 1 \\
n &\equiv 0 \pmod 2 &&\Longrightarrow 3 | 78557 \cdot 2^n + 1 \\
n &\equiv 1 \pmod 4 &&\Longrightarrow 5 | 78557 \cdot 2^n + 1 \\
n &\equiv 15 \pmod{18} &&\Longrightarrow 19 | 78557 \cdot 2^n + 1 \\
n &\equiv 27 \pmod{36} &&\Longrightarrow 37 | 78557 \cdot 2^n + 1 \\
n &\equiv 3 \pmod 9 &&\Longrightarrow 73 | 78557 \cdot 2^n + 1.
\end{aligned}$$

These congruences are respectively equivalent to

$$\begin{aligned}
n &\equiv 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34 \pmod{36}, \\
n &\equiv 11, 23, 35 \pmod{36}, \\
n &\equiv 0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34 \pmod{36}, \\
n &\equiv 1, 5, 9, 13, 17, 21, 25, 29, 33 \pmod{36}, \\
n &\equiv 15, 33 \pmod{36}, \\
n &\equiv 27 \pmod{36}, \\
n &\equiv 3, 12, 21, 30 \pmod{36}.
\end{aligned}$$

Since these congruences cover all congruence classes modulo 36, this establishes that $78557 \cdot 2^n + 1$ is composite for all integers $n \geq 1$.

It is known at this time that the smallest positive integer $k$ which could possibly be a Sierpiński number is $k = 10\,223$; in fact, as of 2008, there remains six numbers smaller than 78 557 which could possibly be Sierpiński numbers: 10 223, 21 181, 22 699, 24 737, 55 459 and 67 607; one of the last "false Sierpiński numbers", namely 19 249, was eliminated in 2007 by K. Agafonov, who proved that $19\,249 \cdot 2^{13\,018\,586} + 1$ is prime.

Let us now formally state and prove Sierpiński's 1960 result.

**Proposition 7.21.** *There exist infinitely many positive integers $k$ such that $2^n k + 1$ is composite for all $n \geq 1$.*

**Proof.** Assume that $(a_i, b_i, q_i)_{i=1}^r$ are triples of integers such that

(i) for each $n$ there exists $i \in \{1, \ldots, r\}$ such that $n \equiv a_i \pmod{b_i}$;

(ii) $q_i$ are distinct primes and $q_i | 2^{b_i} - 1$ for all $i = 1, \ldots, r$.

By the Chinese Remainder Theorem (Theorem 1.12), the system of congruences $2^{a_i}k + 1 \equiv 0 \pmod{q_i}$ for $i = 1, \ldots, r$ has a positive integer solution $k_0$. Furthermore, all the other solutions are precisely the arithmetic progression $k_0 \pmod{q_1 \cdots q_r}$. If $k$ fulfills all these congruences, then for each $n$, the number $2^n k + 1$ is a multiple of $q_i$ for some $i = 1, \ldots, r$. Thus, if $k = k_0 + q_1 \cdots q_r \ell$ with $\ell > 0$, then $k$ fulfills the property that $2^n k + 1$ is composite for all positive integers $n$. It now suffices to observe that

$$(1, 3, 7),\ (11, 12, 13),\ (0, 2, 3),\ (1, 4, 5),\ (15, 18, 19),\ (27, 36, 37),\ (3, 9, 73)$$

fulfill both (i) and (ii), with in this case $k_0 = 78557$. □

In 1956, Riesel [**121**] observed that there are infinitely many positive integers $k$ such that $2^n k - 1$ is composite for all integers $n \geq 1$. Note that this was four years before Sierpiński. Such numbers are called *Riesel numbers*. It is possible to adapt the proof of Proposition 7.21 to show that there are infinitely many Riesel numbers. There is an ongoing quest to find the smallest possible Riesel and Sierpiński numbers. It is conjectured that 509203 and 78557 are the smallest Riesel and Sierpiński numbers, respectively. As of today, there are 61 possible candidates for the smallest Riesel number, and only 6 candidates for the smallest Sierpiński number. See the websites [**122**] and [**134**] for the status of the searches.

In 1934, Romanov [**123**] noted that the set of numbers of the form $\mathcal{R} = \{p + 2^k : p \text{ prime}, k \geq 0\}$ has positive lower density. That is, there exists a positive constant $c$ such that on a sequence $\{x_m\}_{m \geq 1}$ of positive real numbers tending to infinity we have that the inequality

$$\#\left(\mathcal{R} \cap [1, x]\right) > cx$$

holds for all $x = x_m$, $m = 1, 2, \ldots$. Nevertheless, Erdős showed that not all odd positive integers are in $\mathcal{R}$ and in fact exhibited an infinite arithmetic progression of odd positive integers not in $\mathcal{R}$ using again the covering congruences method of Proposition 7.21. We leave the details for the reader.

## 7.8. Some open problems of an elementary nature

In this area, there is no shortage of open problems. We will simply exhibit a few of them.

Until recently, it was not known if there exist infinitely many pairs of positive integers $(m, n)$ such that $\sigma(m) = \phi(n)$. This was resolved in the affirmative in 2010 by Ford, Luca, and Pomerance [**58**].

It is still not known if there are any odd perfect numbers. But one can easily show that the sum of the reciprocals of all the perfect numbers

(including the potential odd ones) is convergent. It is not known whether there exist infinitely many amicable numbers (that is, members of an amicable pair). Pomerance [**115**] showed that the set of $n \le x$ which are part of an amicable pair is of cardinality $O(x \exp(-(\log x)^{1/3}))$ and inferred that the sum of the reciprocals of the members of amicable pairs is convergent. Let $s(n) = \sigma(n) - n$ and for $k \ge 1$, let $s_k(n)$ be the $k$-th fold composition of the function $s(n)$ with itself evaluated at $n$. If $s_k(n) = n$, then $n$ is said to be part of an aliquot cycle of length $k$. For example, perfect numbers are in aliquot cycles of length 1, and amicable numbers are in aliquot cycles of length 2. It is conjectured that every positive integer $n$ belongs to an aliquot cycle of finite length $k$ for some $k$, but we are nowhere near proving anything of this sort. Recent results about aliquot cycles can be found in the paper by Kobayashi, Pollack, and Pomerance [**91**].

In 1907, Carmichael [**21**] announced that whenever $n$ is such that $n = \phi(m)$ for some $m$, then $n = \phi(m)$ for at least two distinct values of $m$. In other words, the set $\phi^{-1}(n) = \{m : \phi(m) = n\}$ never has cardinality 1. However, his proof was flawed and since then this is known as *Carmichael's conjecture*. This is still an open problem, although Kevin Ford [**55**] showed that the smallest counterexample, if any, is larger than $10^{10^{10}}$. (Moral: Don't attempt to find one with your personal computer!)

Mąkowski and Schinzel [**103**] conjectured that the inequality $\sigma(\phi(n)) \ge n/2$ holds for all positive integers $n$. At present, it is only known that $\sigma(\phi(n)) > cn$ holds for all $n$ with $c = 1/39.4$ (see Ford [**56**]) and that for each $\varepsilon > 0$ the inequality $\sigma(\phi(n)) > (c_1 - \varepsilon)n \log\log\log n$ holds for almost all positive integers $n$, where $c_1 = e^{-\gamma}$ (see Luca and Pomerance [**101**]). Lehmer conjectured that if $\phi(n) \mid n - 1$, then $n$ is prime. It is known that the set of counterexamples $n \le x$ to Lehmer's conjecture has cardinality $O(x^{1/2}(\log x)^{-1/2+o(1)})$ (see Luca and Pomerance [**100**]). Křížek and Luca [**92**] modified Lehmer's question and showed that if $\phi^2(n) \mid n^2 - 1$, then $n = 1, 2$ or 3 (see Problem 13.8).

## Problems on Chapter 7

**Problem 7.1.** *Show that the average value of* $\Omega(n) - \omega(n)$ *on* $[1, x]$ *tends to a constant as* $x$ *tends to infinity.*

**Problem 7.2.** *Given a positive integer* $k$*, let*

$$\sigma_k(n) = \sum_{d \mid n} d^k$$

*be the sum of the $k$-th powers of the divisors of $n$. Find the average value of $\sigma_k(n)$ on the interval $[1,x]$. (Hint: Find the average value of $\sigma_k(n)/n^k$ by first proving that $\sigma_k(n)/n^k = \sum_{d\,|\,n} 1/d^k$. Then use Abel's summation formula.)*

**Problem 7.3.** *Show that $2^{\omega(n)} \le d(n) \le 2^{\Omega(n)}$ for all positive integers $n$.*

**Problem 7.4.** *Show that $d(mn) \le d(m)d(n)$ for all positive integers $m$ and $n$.*

**Problem 7.5.** *Show that the conclusion of Proposition* 7.16 *remains valid if we replace* $\log\log n$ *by $f(n)$, where $f : \mathbb{R}_+ \to \mathbb{R}_+$ is any function which is increasing for $x > x_0$ and tends to infinity with $x$.*

**Problem 7.6.** *Prove the following strengthening of Lemma* 7.18*: The set*

$$A = \{n : |\omega(n) - \log\log n| > (\log\log n)^{2/3}\}$$

*is of asymptotic density zero. (Hint: Show that if $x$ is large and $n \in A \cap [x/\log x, x]$, then $|\omega(n) - \log\log x|^2 > (\log\log x)^{4/3}$. Now use the Turán-Kubilius inequality in order to get that the number of such positive integers $n \le x$ is $\ll x/(\log\log x)^{1/3} = o(x)$ as $x \to \infty$.)*

**Problem 7.7.** *Show that almost all positive integers $n$ have a prime factor $p > \log n$.*

**Problem 7.8.** *Consider the set $A$ of those positive integers which do not contain the digit 7 in their decimal expansion.*

(i) *Show that $A$ is of zero density.*

(ii) *Use (i) to show that almost all integers contain each of the digits 0,1,...,9.*

(iii) *Show that the sum of the reciprocals of the elements of $A$ converges.*

**Problem 7.9.** *Let $0 < a_1 < a_2 < \cdots$ be a sequence of positive integers. Let $A$ be the set of elements of this sequence and assume that it is of density $\delta > 0$. Show that the "average distance" between consecutive elements of $A$ is equal to $1/\delta$, in the sense that*

$$\lim_{x\to\infty} \frac{1}{A(x)} \sum_{\substack{a_n \le x \\ n \ge 2}} \frac{a_n - a_{n-1}}{1/\delta} = 1.$$

**Problem 7.10.** *Let $A$ be a set of positive integers for which the counting function $A(x) = \#\{n \le x : n \in A\}$ satisfies the asymptotic relation*

$$A(x) = \frac{x}{L(x)}(1 + o(1)) \qquad (x \to \infty),$$

*where $L(x)$ is a function satisfying $L(x) \gg (\log x)^{1+\eta}$ for some positive constant $\eta > 0$. Prove that*

$$\sum_{n\in A} \frac{1}{n} < +\infty.$$

**Problem 7.11.** *Let $A$ be a set of positive integers for which the counting function $A(x) = \#\{n \le x : n \in A\}$ satisfies*

$$A(x) = \frac{x}{L(x)}(1 + o(1)) \qquad (x \to \infty),$$

*where $L(x)$ is a function satisfying $L(x) \ll \log x$. Prove that*

$$\sum_{n\in A} \frac{1}{n} = +\infty.$$

**Problem 7.12.** *Show that the set $A = \{n : \omega(n) \mid n\}$ is of asymptotic density zero. (Hint: Let $x$ be a large positive real number and set $y = \log\log x$. Use Problem 7.6 to infer that all $n \le x$ have $\omega(n) \in I = [y - y^{2/3}, y + y^{2/3}]$ with at most $o(x)$ exceptions. So, if such an integer $n$ is in $A$, then $k \mid n$ for some $k \in I$. The number of such $n \le x$ for a fixed $k$ is $\le x/k$. Thus, the set in question has at most*

$$x \sum_{y-y^{2/3}\le k\le y+y^{2/3}} \frac{1}{k}$$

*elements. Now use Theorem 1.7 to deduce that the above sum is $o(1)$ as $y \to \infty$.)*

**Problem 7.13.** *Show that*

$$2\zeta(3) = \int_0^1 \int_0^1 \frac{-\log(xy)}{1-xy} dxdy.$$

*(Hint: Use the method used in the proof of $\zeta(2) = \pi^2/6$ in Chapter 3, that is, set*

$$I(\sigma) = \int_0^1 \int_0^1 \frac{(xy)^\sigma}{1-xy} dxdy.$$

*Then take derivatives with respect to $\sigma$ and evaluate the result at $\sigma = 0$.)*

**Problem 7.14.** *Show that if $\sigma(n)$ is odd, then $n = m^2$ or $n = 2m^2$ for some integer $m$.*

**Problem 7.15.** *Show that if $n$ is an odd perfect number, then $n = p^{2\alpha+1}m^2$, where $p$ is prime and coprime to $m$.*

**Problem 7.16.** *Show that the sum of the reciprocals of the perfect numbers is convergent. (Hint: Let $A$ be the set of all odd perfect numbers. Show, using the previous problem, that $\#(A \cap [1, x]) = O(x^{1/2}\log x)$ by noting that if $n = p^{2\alpha+1}m^2$, then $p \mid \sigma(m^2)$. Then use Abel's summation formula.)*

**Problem 7.17.** *Show that if $n > 2$ then $2^{2^n} - 1$ is not of the form $p + 2^a + 2^b$, where $p$ is prime and $b > a \geq 0$ are integers. (Hint: Start by noting that if $r$ is such that $2^r \| b - a$, then $2^{2^r} + 1 \mid 2^{2^n} - 1 - 2^a - 2^b$.)*

**Problem 7.18.** *It is not known if there exist infinitely many multiperfect numbers, that is, positive integers $n$ such that $n | \sigma(n)$. (See, for instance, Guy's book [**71**].) Prove that if $s \geq 2$ is a fixed integer, then there exist infinitely many positive integers $n$ such that $n \mid \sigma_s(n)$, where $\sigma_s(n) = \sum_{d|n} d^s$.*

**Problem 7.19.** *Show that there are infinitely many positive integers $k$ such that $2^n k - 1$ is composite for all $n \geq 0$.*

**Problem 7.20.** *Prove that there are infinitely many odd positive integers $k$ not of the form $2^n + p$ for any positive integer $n$ and odd prime $p$. Is it easier to show that there are infinitely many odd positive integers $k$ not of the form $10^n + p$ for any positive integer $n$ and prime $p$?*

**Problem 7.21.** *Let $a > b$ be coprime positive integers, and let $x > a$. Show that*

$$\sum_{n<x} \omega(an + b) \ll x \log\log x.$$

*(Hint: Note first that $an + b < (x + 1)^2$, so that for each $n$ there is at most one prime factor $p > x + 1$ of $an + b$. Thus, we may reduce the problem to estimating the contribution coming from primes $p < x$. Write the remaining sum on the left as a double sum and change the order of summation. Then use the fact that there are at most $\lfloor x/p \rfloor + 1 \leq 2x/p$ values of $m \leq x$ such that $p \mid am + b$.)*

**Problem 7.22.** *Let $a > b$ be coprime positive integers, and let $x > a$. Show that*

$$\sum_{n<x} d(an + b) \ll x \log x.$$

**Problem 7.23.** *Let $n > 1$ and $1 = d_1 < d_2 < \cdots < d_{d(n)} = n$ be all the $d(n)$ divisors of $n$. Prove that*

$$\sum_{1 \leq i < j \leq d(n)} \frac{1}{d_j - d_i} \ll d(n).$$

**Problem 7.24.** *Show that the sequence $\{\sigma(n)/n\}_{n \geq 1}$ is dense in $[1, \infty)$.*

**Problem 7.25.** *Let $k \geq 2$ be a fixed positive integer. Show that the inequalities*

$$\omega(n + 1) < \omega(n + 2) < \cdots < \omega(n + k)$$

*hold for infinitely many positive integers $n$.*

**Problem 7.26.** *Show that the sequence* $\{\omega(n+1)/\omega(n)\}_{n\geq 1}$ *is dense in* $[0,\infty)$. *(Hint: Let* $\alpha$ *be any positive real number. Choose a very large* $x$ *and write* $\pi(x) = a+b$, *where* $a/b$ *is near* $\alpha$. *Split the set of all primes* $p \leq x$ *into two disjoint sets* $\mathcal{P}$ *and* $\mathcal{Q}$, *one of cardinality* $a$ *and the other of cardinality* $b$. *Then use the Chinese Remainder Theorem to find* $n_0$ *such that* $n_0 \equiv -1 \pmod{n_{\mathcal{P}}}$ *and* $n_0 \equiv 0 \pmod{n_{\mathcal{Q}}}$, *where* $n_{\mathcal{P}} = \prod_{p\in\mathcal{P}} p$ *and* $n_{\mathcal{Q}} = \prod_{q\in\mathcal{Q}} q$. *Let* $n \in [e^{3x}, e^{4x}]$ *be such that* $n \equiv n_0 \pmod{n_{\mathcal{P}} \cdot n_{\mathcal{Q}}}$. *Deduce that* $n+1$ *is divisible by the prime factors in* $\mathcal{P}$ *and (perhaps) some other primes larger than* $x$ *and* $n$ *by the prime factors in* $\mathcal{Q}$ *and (perhaps) some other prime larger than* $x$. *Now show that for most such* $n$, *both* $n+1$ *and* $n$ *have only few prime factors larger than* $x$, *no more than* $o(x)$ *as* $x \to \infty$, *by using, for example, Problem* 7.21. *Conclude that* $\omega(n+1)/\omega(n) = (a/b)(1+o(1))$ *as* $x \to \infty$.*)*

**Problem 7.27.** *Show that the sequence* $\{\Omega(n+1)/\Omega(n)\}_{n\geq 1}$ *is dense in* $[0,\infty)$.

**Problem 7.28.** *Prove that there exist infinitely many positive integers* $k$ *not of the form* $n - \omega(n)$ *for any* $n \geq 1$. *(Hint: Let* $\ell$ *be large, let* $P_1 = p_1p_2$, $P_2 = p_3p_4p_5$, $P_3 = p_6p_7p_8p_9$, $\ldots$, $P_\ell = p_{t_\ell}\cdots p_{t_{\ell+1}-1}$, *where* $t_\ell = \ell(\ell-1)/2$ *is the* $\ell$*-th triangular number. Set* $x = P_1\cdots P_\ell$ *and let* $k \in [x^2, x^3]$ *be in the arithmetical progression* $k \equiv -i \pmod{P_i}$ *for* $i = 1,\ldots,\ell$. *Show, using the Prime Number Theorem, that* $\ell^2 \log\ell \asymp \log x$, *so that* $\ell \gg (\log x/\log\log x)^{1/2}$. *Now show that if* $k = n - \omega(n)$ *for some* $n$, *then* $\omega(n) = t \in \mathcal{I} = [\ell+1, \lfloor \log x \rfloor]$. *Thus,* $n$ *should have a lot of prime factors with respect to its size. Afterwards, use Problem* 7.21 *to show that for most such* $k$ *in* $[x^2, x^3]$, *there is no corresponding* $t$ *in* $\mathcal{I}$ *such that* $n+t$ *has more than* $t$ *prime factors.)*

*Chapter 8*

# The Fascinating Euler Function

## 8.1. The Euler function

Recall that for a positive integer $n$, the Euler function $\phi(n)$ counts the number of positive integers $m \leq n$ which are coprime to $n$, that is,

$$\phi(n) = \#\{1 \leq m \leq n \ : \ (m,n) = 1\}.$$

Let $\mathbb{Z}/n\mathbb{Z}$ be the set of congruence classes $a \pmod n$. The set $\mathbb{Z}/n\mathbb{Z}$ is a ring with the usual addition and multiplication:

$$a \bmod n + b \bmod n = a + b \bmod n,$$

and

$$\Big(a \bmod n\Big) \cdot \Big(b \bmod n\Big) = a \cdot b \bmod n.$$

The invertible elements in $\mathbb{Z}/n\mathbb{Z}$ are precisely those congruence classes $a \bmod n$ with $(a,n) = 1$. These elements form a group $U(\mathbb{Z}/n\mathbb{Z})$ whose cardinality is $\phi(n)$. Lagrange's theorem from group theory tells us that the order of every element in a finite group is a divisor of the order of the group. In the particular case of the group $U(\mathbb{Z}/n\mathbb{Z})$, this theorem implies that the congruence

$$a^{\phi(n)} \equiv 1 \pmod n$$

holds for all integers $a$ coprime to $n$. The above relation is known as the Euler theorem. The following relation, bearing a striking typographical resemblance to Euler's theorem, is also true.

**Proposition 8.1.** *(Euler) Given integers $a > 1$ and $n \geq 1$, then $n | \phi(a^n - 1)$.*

**Proof.** Let $M = a^n - 1$. Note that $a$ is coprime to $M$, $a^n \equiv 1 \pmod{M}$ and if $0 < k < n$ then $0 < a^k - 1 < M$, so that $a^k \not\equiv 1 \pmod{M}$. Thus, $n$ is the exact multiplicative order of $a$ modulo $M$, implying that $n \mid \phi(M)$, which is what we wanted. □

Since the function $\psi$ (defined in (1.11)) is a ring isomorphism, it follows that $\psi$ induces an isomorphism of the multiplicative groups of the two rings. In particular, if we compare the orders of these groups, we get that

$$\#U(\mathbb{Z}/(m_1 \cdots m_k)\mathbb{Z}) = \prod_{i=1}^{k} \#U(\mathbb{Z}/m_i\mathbb{Z}),$$

that is,

$$\phi(m_1 \cdots m_k) = \prod_{i=1}^{k} \phi(m_i).$$

**Proposition 8.2.** *If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ where $p_1, \ldots, p_k$ are distinct primes and $\alpha_i$ are positive integers for all $i = 1, \ldots, k$, then*

$$\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1).$$

*Moreover,*

$$\sigma(n) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right) \cdots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}\right).$$

**Proof.** If $n = p^\alpha$ is a prime power, then $\{p, 2p, 3p, \ldots, (p^{\alpha-1})p\}$ are the only positive integers $m \le p^\alpha$ which are not coprime to $p^\alpha$ and there are $p^{\alpha-1}$ of them. Thus, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Furthermore, the only divisors of $p^\alpha$ are of the form $p^\beta$ with some $\beta \in \{0, 1, \ldots, \alpha\}$, so that

$$\sigma(p^\alpha) = 1 + p + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

Now the results for both the Euler function $\phi$ and the sum of divisors function $\sigma$ follow because both $\phi$ and $\sigma$ are multiplicative. □

Here is an observation attributed to P. Erdős.

**Proposition 8.3.** *For each $n \ge 1$, there exists $m$ such that $\phi(m) = n!$.*

**Proof.** Note that

$$\prod_{p \le n} (p - 1) \mid n!.$$

Furthermore, $n! = \prod_{p \le n} p^{\alpha_p}$ for some positive integers $\alpha_p$. Thus,

$$\frac{n!}{\prod_{p \le n}(p - 1)} = \prod_{p \le n} p^{\beta_p}$$

holds with some integers $\beta_p \geq 0$. Now the number

$$m = \prod_{p \leq n} p^{\beta_p + 1}$$

is such that

$$\phi(m) = \prod_{p \leq n} (p-1) \cdot \prod_{p \leq n} p^{\beta_p} = n!,$$

which proves the existence of an integer $m$ satisfying $\phi(m) = n!$. □

## 8.2. Elementary properties of the Euler function

In this section, we will use what we learned so far about prime numbers and the Chinese Remainder Theorem to prove some fascinating properties of the Euler function and of the sum of the divisors function.

**Proposition 8.4.** *The inequality $\phi(n) \gg n/\log\log n$ holds for all $n \geq 3$.*

**Proof.** Assume that $n = q_1^{\ell_1} q_2^{\ell_2} \cdots q_k^{\ell_k}$ where $q_1 < q_2 < \cdots < q_k$ are prime numbers and $\ell_1, \ell_2, \ldots, \ell_k$ are positive integers. Let $p_i$ be the $i$-th prime for all $i \geq 1$. Then

$$\phi(n) = n \prod_{i=1}^{k} \Big(1 - \frac{1}{q_i}\Big) \geq n \prod_{i=1}^{k} \Big(1 - \frac{1}{p_i}\Big) = n \prod_{p \leq p_k} \Big(1 - \frac{1}{p}\Big).$$

Problem 4.4 now shows that

$$\phi(n) \gg \frac{n}{\log p_k}.$$

Since $k = \omega(n) \ll \log n$ (see Proposition 7.10) and since $p_k \ll k^2$, we get that

$$\phi(n) \gg \frac{n}{\log p_k} \gg \frac{n}{\log(k^2)} \gg \frac{n}{\log k} \gg \frac{n}{\log\log n},$$

which is the desired estimate. □

**Proposition 8.5.** *The inequality $\sigma(n) \ll n \log\log n$ holds for all $n \geq 3$.*

**Proof.** Writing $n = q_1^{\ell_1} \cdots q_k^{\ell_k}$ where $q_1 < \cdots < q_k$ are prime numbers and $\ell_1, \ldots, \ell_k$ are positive integers, we have

$$\begin{aligned} \frac{\sigma(n)}{n} &= \prod_{i=1}^{k} \Big(1 + \frac{1}{q_i} + \cdots + \frac{1}{q_i^{\ell_i}}\Big) < \prod_{i=1}^{k} \Big(\sum_{\ell=0}^{\infty} \frac{1}{q_i{}^{\ell}}\Big) \\ &= \prod_{i=1}^{k} \Big(1 + \frac{1}{q_i - 1}\Big) = \frac{n}{\phi(n)} \ll \log\log n, \end{aligned}$$

where the last inequality follows from Proposition 8.4. □

## 8.3. The average order of the Euler function

**Theorem 8.6.** *The estimate*

$$\sum_{n\le x}\phi(n)=\frac{3}{\pi^2}x^2+O(x\log x)$$

*holds for all $x$.*

**Proof.** Using the formula

$$\frac{\phi(n)}{n}=\sum_{d\,|\,n}\frac{\mu(d)}{d},$$

(see Problem 8.1 (i)), we get, by changing the order of summation,

$$\begin{aligned}
B(x)&=\sum_{n\le x}\frac{\phi(n)}{n}=\sum_{n\le x}\sum_{d\,|\,n}\frac{\mu(d)}{d}\\
&=\sum_{d\le x}\frac{\mu(d)}{d}\sum_{\substack{n\le x\\ n\equiv 0 \pmod d}}1\\
&=\sum_{d\le x}\frac{\mu(d)}{d}\left\lfloor\frac{x}{d}\right\rfloor=\sum_{d\le x}\frac{\mu(d)}{d}\left(\frac{x}{d}+O(1)\right)\\
&=x\sum_{d\le x}\frac{\mu(d)}{d^2}+O\left(\sum_{d\le x}\frac{1}{d}\right)\\
&=x\left(\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}-\sum_{d>x}\frac{\mu(d)}{d^2}\right)+O\left(\sum_{d\le x}\frac{1}{d}\right)\\
&=x\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O\left(x\left(\sum_{d>x}\frac{1}{d^2}\right)+\sum_{d\le x}\frac{1}{d}\right).
\end{aligned}\tag{8.1}$$

Theorem 1.7 tells us that

$$\sum_{d\le x}\frac{1}{d}\ll\log x,\tag{8.2}$$

while formula (4.14) tells us that

$$\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}=\frac{1}{\zeta(2)}=\frac{6}{\pi^2},\tag{8.3}$$

where we used the fact that $\zeta(2)=\pi^2/6$ (see Theorem 3.7). Finally,

$$\sum_{d>x}\frac{1}{d^2}\le\int_{x-1}^{\infty}\frac{dt}{t^2}=-\frac{1}{t}\Big|_{t=x-1}^{\infty}=\frac{1}{x-1}.\tag{8.4}$$

Inserting the estimates (8.2), (8.3), and (8.4) in the last of estimates (8.1), we get

$$B(x) = \frac{6}{\pi^2}x + O(\log x). \tag{8.5}$$

To get to the desired estimate, we now apply the Abel summation formula with $a_n = \phi(n)/n$ and $f(t) = t$. Noting that $A(x)$ becomes $B(x)$ given by (8.5), we finally obtain

$$\begin{aligned}
\sum_{n\le x}\phi(n) &= \sum_{n\le x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt \\
&= \left(\frac{6}{\pi^2}x + O(\log x)\right)x - \int_1^x \left(\frac{6}{\pi^2}t + O(\log t)\right)dt \\
&= \frac{6}{\pi^2}x^2 + O(x\log x) - \frac{6}{\pi^2}\int_1^x t\,dt + O\left(\int_1^x \log t\,dt\right) \\
&= \frac{6}{\pi^2}x^2 + O(x\log x) - \frac{3}{\pi^2}t^2\Big|_{t=1}^{x} + O(x\log x) \\
&= \frac{3}{\pi^2}x^2 + O(x\log x),
\end{aligned}$$

which is the desired estimate. □

## 8.4. When is $\phi(n)\sigma(n)$ a square?

The following appears in Guy and Nowakowski [**72**].

**Proposition 8.7.** *There are infinitely many positive integers $n$ such that $\phi(n)\sigma(n)$ is a square.*

**Proof.** Actually, we will prove more, namely that for large $x$, the number of positive integers $n \le x$ such that $\phi(n)\sigma(n)$ is a square is $\ge x^{c_1/\log\log x}$, for some positive constant $c_1$.

Indeed, let $y > 0$ and define the two sets

$$\mathcal{A} = \{p \le y\} \qquad \text{and} \qquad \mathcal{B} = \{p \le (y+1)/2\}.$$

For each subset $\mathcal{P}$ of $\mathcal{A}$, set $n_{\mathcal{P}} = \prod_{p\in\mathcal{P}} p$. Observe that

$$\phi(n_{\mathcal{P}})\sigma(n_{\mathcal{P}}) = \prod_{p\in\mathcal{P}}(p-1)(p+1) = m_{\mathcal{P}}t_{\mathcal{P}}^2$$

holds with some positive integers $m_{\mathcal{P}}$ and $t_{\mathcal{P}}$, where $m_{\mathcal{P}}$ is squarefree and made up only of primes belonging to $\mathcal{B}$. There are $2^{\pi(y)}$ subsets of $\mathcal{A}$ and only $2^{\pi((y+1)/2)}$ subsets of $\mathcal{B}$. So, by the Pigeon-Hole principle, there is a squarefree positive integer $m$ made up only of primes from $\mathcal{B}$, such that the relation

$$\phi(n_{\mathcal{P}})\sigma(n_{\mathcal{P}}) = mt_{\mathcal{P}}^2$$

holds for a family $\mathcal{F}$ of subsets $\mathcal{P}$ of $\mathcal{A}$ of cardinality at least

$$2^{\pi(y)-\pi((y+1)/2)} = 2^{\frac{y}{2\log y}(1+o(1))} \qquad \text{as } y \to \infty. \tag{8.6}$$

Let $\mathcal{Q}$ be some fixed element of $\mathcal{F}$ and let $\mathcal{P}$ be an arbitrary element of $\mathcal{F}$. Write

$$\mathcal{P}\Delta\mathcal{Q} = (\mathcal{P}\backslash\mathcal{Q}) \cup (\mathcal{Q}\backslash\mathcal{P}).$$

Then, on the one hand,

$$\phi(n_{\mathcal{P}})\sigma(n_{\mathcal{P}})\phi(n_{\mathcal{Q}})\sigma(n_{\mathcal{Q}}) = \phi(n_{\mathcal{P}\Delta\mathcal{Q}})\sigma(n_{\mathcal{P}\Delta\mathcal{Q}})\big(\phi(n_{\mathcal{P}\cap\mathcal{Q}})\sigma(n_{\mathcal{P}\cap\mathcal{Q}})\big)^2,$$

while on the other hand,

$$\phi(n_{\mathcal{P}})\sigma(n_{\mathcal{P}})\phi(n_{\mathcal{Q}})\sigma(n_{\mathcal{Q}}) = (mt_{\mathcal{P}}t_{\mathcal{Q}})^2.$$

From these last two formulas, we get that

$$\phi(n_{\mathcal{P}\Delta\mathcal{Q}})\sigma(n_{\mathcal{P}\Delta\mathcal{Q}}) = \Big(\frac{mt_{\mathcal{P}}t_{\mathcal{Q}}}{\phi(n_{\mathcal{P}\cap\mathcal{Q}})\sigma(n_{\mathcal{P}\cap\mathcal{Q}})}\Big)^2.$$

In particular, all numbers of the form $n_{\mathcal{P}\Delta\mathcal{Q}}$ for $\mathcal{P} \in \mathcal{F}$ have the desired property. Note also that the map

$$\mathcal{P} \mapsto \mathcal{P}\Delta\mathcal{Q}$$

is injective (simply because $\mathcal{A}$ together with the operation $\Delta$ is a group, whose identity element is the empty set $\emptyset$ and in which every element different from $\emptyset$ is of order 2), so by unique factorization, we get that the application $\mathcal{P} \longmapsto n_{\mathcal{P}\Delta\mathcal{Q}}$ is also injective. In particular, there are at least

$$|\mathcal{F}| \geq 2^{\pi(y)-\pi((y+1)/2)} = 2^{\frac{y}{2\log y}(1+o(1))} \qquad (\text{as } y \to \infty)$$

squarefree positive integers $n$ made up only of primes from $\mathcal{A}$ such that $\phi(n)\sigma(n)$ is a square. Let $x$ be an upper bound for the maximal integer of this form. Since

$$\prod_{p\leq y} p = e^{y(1+o(1))},$$

we get

$$x = e^{y(1+o(1))}.$$

Thus,

$$y = (1+o(1))\log x \qquad \text{as } x \to \infty.$$

Since furthermore

$$|\mathcal{F}| \geq 2^{\frac{y}{2\log y}(1+o(1))} = 2^{\frac{\log x}{2\log\log x}(1+o(1))} = x^{\frac{\log 2}{2\log\log x}(1+o(1))},$$

we see that for large $x$ the number of numbers $n \leq x$ such that $\phi(n)\sigma(n)$ is a square is $\geq x^{c_1/\log\log x}$, where $c_1$ to be any positive number smaller than $\dfrac{\log 2}{2}$. □

## 8.5. The distribution of the values of $\phi(n)/n$

First, let us show that the multiplicative function $\phi(n)/n$ has a distribution function. To do so, we first observe that the strongly additive function $f(n) := \log(\phi(n)/n)$ has itself a distribution function. Indeed, it is clear that $|f(p)| < 1$ for each prime $p$, thus implying that the series $\sum_{|f(p)|\geq 1} \frac{1}{p}$ is trivially convergent. On the other hand,

$$\begin{aligned}\sum_{|f(p)|<1} \frac{f(p)}{p} &= \sum_p \frac{\log(1-1/p)}{p} \ll \sum_p \frac{1}{p^2} = O(1),\\ \sum_{|f(p)|<1} \frac{f^2(p)}{p} &= \sum_p \frac{\log^2(1-1/p)}{p} \ll \sum_p \frac{1}{p^3} = O(1).\end{aligned}$$

Hence it follows from the Erdős-Wintner theorem (Theorem 6.21) that the sequence of distribution functions

$$G_N(z) := \frac{1}{N} \sum_{\substack{n\leq N\\ \log(\frac{\phi(n)}{n})\leq z}} 1 \qquad (N = 1, 2, \ldots)$$

converges weakly to a limit function $G(z)$. Thus, letting $F_N(z) = G_N(\log z)$ and $F(z) = G(\log z)$, it is clear that the sequence $\{F_N(z)\}_{N\geq 1}$ converges weakly to $F(z)$, with $F(0) = 0$ and $F(1) = 1$, thus establishing our claim.

The sequence of values of $\phi(n)/n$, for $n = 1, 2, \ldots$, also have an interesting feature, namely the one given in the following theorem.

**Proposition 8.8.** *The set $\{\phi(n)/n\}_{n\geq 1}$ is dense in $[0, 1]$.*

**Proof.** We only sketch the main ideas. Write $\frac{n}{\phi(n)} = \prod_{p|n}\Big(1 + \frac{1}{p-1}\Big)$. Taking logarithms and using the continuity of the function log, it suffices to prove that any number in the interval $(0, \infty)$ is a limit of a sequence of numbers of the form

$$\sum_{p\in\mathcal{P}} \log\Big(1 + \frac{1}{p-1}\Big),$$

where $\mathcal{P}$ is some finite set of primes. Observe that $\log(1 + 1/(p-1))$ is positive and tends to zero as $p$ tends to infinity, while the series

$$\sum_p \log\Big(1 + \frac{1}{p-1}\Big)$$

is divergent. Now, it is easy to see that if $\{a_n\}_{n\geq 1}$ is a sequence of nonnegative real numbers with $a_n \to 0$ as $n \to \infty$, but such that the series

$$\sum_{n\geq 1} a_n$$

is divergent, then for each $a \in (0,\infty)$, $N$ and $\varepsilon > 0$, there exist positive integers $n_1 < n_2 < \cdots < n_s$ with $n_1 > N$ such that

$$|a - \sum_{i=1}^{s} a_{n_i}| < \varepsilon,$$

which is what needed to be proved. □

## 8.6. The local behavior of the Euler function

**Proposition 8.9.** *Let $k \geq 2$ be a fixed integer. Then the inequalities*

$$\phi(n+1) < \phi(n+2) < \cdots < \phi(n+k) \tag{8.7}$$

*hold for infinitely many positive integers $n$.*

**Proof.** Again, we only sketch the main ideas. Let $K = (k!)^2$, $n = Km$, where $m \geq 1$ is an integer. Then $n + i = in_i$, where $n_i = \dfrac{K}{i}m + 1$ is coprime to $k!$ for each $i = 1, \ldots, k$. Dividing inequality (8.7) by $n$, we get

$$\Big(1+\frac{1}{n}\Big)\frac{\phi(n+1)}{n+1} < \Big(1+\frac{2}{n}\Big)\frac{\phi(n+2)}{n+2} < \cdots < \Big(1+\frac{k}{n}\Big)\frac{\phi(n+k)}{n+k},$$

which is the same as

$$\Big(1+\frac{1}{n}\Big)\frac{\phi(1)}{1}\frac{\phi(n_1)}{n_1} < \Big(1+\frac{2}{n}\Big)\frac{\phi(2)}{2}\frac{\phi(n_2)}{n_2} < \cdots < \Big(1+\frac{k}{n}\Big)\frac{\phi(k)}{k}\frac{\phi(n_k)}{n_k}. \tag{8.8}$$

Let $c_i = \phi(i)/i$ for $i = 1, \ldots, k$. Choose numbers $d_1, \ldots, d_k$ in $(0,1)$ and $\varepsilon > 0$ such that

$$\begin{aligned} c_1(d_1+\varepsilon) &< c_2(d_2-\varepsilon) < c_2(d_2+\varepsilon) < c_3(d_3-\varepsilon) \\ &< \cdots < c_i(d_i+\varepsilon) < c_{i+1}(d_{i+1}-\varepsilon) < \cdots < c_k(d_k-\varepsilon). \end{aligned}$$

Using the method from the proof of Proposition 8.8, we choose disjoint sets of primes $\mathcal{P}_i$ for $i = 1, \ldots, k$, in such a way that all the primes $p \in \cup_{i=1}^{k}\mathcal{P}_i$ have $p > k$, and furthermore if we write $m_i = \prod_{p\in\mathcal{P}_i} p$, then $\phi(m_i)/m_i \in (d_i - \varepsilon/2, d_i+\varepsilon/2)$. Let $M$ be the largest prime in the union of the $\mathcal{P}_i$'s. Let $x > M$ be a very large real number, $\mathcal{Q}(x)$ be the complement of $\{p \leq k\} \cup (\cup_{i=1}^{k}\mathcal{P}_i)$ in $\{p \leq x\}$, and $Q(x)$ the product of all the primes in $\mathcal{Q}(x)$. We then examine the congruences $n \equiv 0 \pmod{K}$, $n \equiv Q(x) \pmod{Q(x)^2}$, $n + i \equiv m_i \pmod{m_i^2}$. By the Chinese Remainder Theorem, these congruences have

an integer solution $n_0$, and all $n$ which fulfill these congruences are precisely those $n$ with $n \equiv n_0 \pmod N$, where $N = KQ(x)^2 \prod_{i=1}^{k} m_i^2$. Clearly,

$$N \ll \prod_{p \le x} p^2 = e^{2(1+o(1))x} \qquad \text{as } x \to \infty,$$

so that $N < e^{3x}$ for $x > x(k)$ (the implied constant in $\ll$ depends on $k$). Thus, we have a number $\gg \dfrac{(e^{4x} - e^{3x})}{N} \gg e^x$ of such integers $n$ in the interval $[e^{3x}, e^{4x}]$ if $x$ is large. Now observe that each such $n$ fulfills $n + i = im_i n_i'$, where the minimal prime dividing $n_i'$ is $> x$. The inequalities (8.8) can then be written as

$$\begin{aligned}\Big(1+\frac{1}{n}\Big)c_1\frac{\phi(m_1)}{m_1}\frac{\phi(n_1')}{n_1'} &< \cdots < \Big(1+\frac{i}{n}\Big)c_i\frac{\phi(m_i)}{m_i}\frac{\phi(n_i')}{n_i'} \\ &< \cdots < \Big(1+\frac{k}{n}\Big)c_k\frac{\phi(m_k)}{m_k}\frac{\phi(n_k')}{n_k'}.\end{aligned}$$

Let us prove that $\phi(n_i')/n_i' \to 1$ as $x$ tends to infinity. This. together with the fact that $1 + i/n \to 1$ as $x$ tends to infinity, tells us that when $x$ is sufficiently large, the inequalities (8.7) are indeed satisfied for our $n$. But since $n_i' < e^{4x}$, we get, by Proposition 7.10, that

$$\omega(n_i') \ll \log(e^{4x})/\log\log(e^{4x}) \ll x/\log x.$$

Thus,

$$\frac{\phi(n_i')}{n_i'} = \prod_{p \mid n_i'}\Big(1-\frac{1}{p}\Big) = \exp\Big(-\sum_{p \mid n_i'}\frac{1}{p} + O\Big(\sum_{p>x}\frac{1}{p^2}\Big)\Big). \tag{8.9}$$

Since

$$\sum_{p>x}\frac{1}{p^2} < \sum_{n \ge x}\frac{1}{n^2} \ll \int_x^\infty \frac{dt}{t^2} = \frac{1}{x}$$

and

$$\sum_{p \mid n_i'}\frac{1}{p} \le \frac{\omega(n_i')}{x} \ll \frac{1}{\log x},$$

we get, by formula (8.9), that

$$\frac{\phi(n_i')}{n_i'} = \exp(o(1)) = 1 + o(1) \qquad \text{as } x \to \infty,$$

which does show that $\phi(n_i')/n_i' \to 1$ as $x \to \infty$. □

## Problems on Chapter 8

**Problem 8.1.** *Let $\phi(n)$ be the Euler function.*

(i) *Show that*
$$\phi(n) = \sum_{d\,|\,n} \mu(d)\frac{n}{d}.$$

(ii) *Deduce from (i) that $\phi(mn) = \phi(m)\phi(n)$ whenever $m$ and $n$ are coprime.*

(iii) *Prove that*
$$\sum_{d\,|\,n} \phi(d) = n.$$

**Problem 8.2.** *Show that if $n$ is composite, then $\phi(n) \le n - \sqrt{n}$.*

**Problem 8.3.** *Show that $\phi(n)$ is even if $n \ge 3$.*

**Problem 8.4.** *Find all positive integers $n > 6$ such that if $1 = a_1 < a_2 < \cdots < a_{\phi(n)} = n - 1$ are all the $\phi(n)$ positive integers smaller than $n$ and coprime to $n$, then the numbers $a_i$, for $i = 1, \ldots, \phi(n)$, form an arithmetic progression.*

**Problem 8.5.** *Show that if $\phi(n)|n$, then $n = 2^\alpha \cdot 3^\beta$ for some nonnegative integers $\alpha$ and $\beta$.*

**Problem 8.6.** *Explain how to adapt the proof of Proposition 8.9 to get the following statement: For each integer $k > 1$ and permutation $a_1, a_2, \ldots, a_k$ of the set of integers $1, 2, \ldots, k$, there exist infinitely many positive integers $n$ such that*
$$\phi(n + a_1) < \phi(n + a_2) < \cdots < \phi(n + a_k).$$

**Problem 8.7.** *Let $k \ge 2$ be a fixed positive integer. Show that the inequalities*
$$\sigma(n + 1) < \sigma(n + 2) < \cdots < \sigma(n + k)$$
*hold for infinitely many positive integers $n$.*

**Problem 8.8.** *Show that*
$$\sum_{n\le x} \frac{1}{\phi(n)} = (C + o(1)) \log x \qquad (x \to \infty),$$
*where* $C = \prod_p \left(1 + \frac{1}{p(p-1)}\right) = \frac{\zeta(2)\zeta(3)}{\zeta(6)}$.

**Problem 8.9.** (i) *Use the argument from the proof of Proposition 8.7 to*

*show that there exist infinitely many squarefree positive integers $n$ such that $\phi(n)$ is a square.*

(ii) *Show that there exist infinitely many positive integers $n$ such that $\sigma(n)$ is a square.*

**Problem 8.10.** *Use Wintner's theorem (Theorem* 6.13*) to show that there exist two positive constants $C_1$ and $C_2$ such that, as $x \to \infty$,*

$$\sum_{n \le x} \left( \frac{\phi(n)}{n} \right)^2 = (C_1 + o(1))x$$

*and*

$$\sum_{n \le x} \left( \frac{\sigma(n)}{n} \right)^2 = (C_2 + o(1))x.$$

*Chapter 9*

# Smooth Numbers

## 9.1. Notation

Given an integer $n \geq 2$ whose factorization is given by

$$n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_r^{\alpha_r},$$

where $q_1 < q_2 < \cdots < q_r$ are primes, $\alpha_i \in \mathbb{N}$, $i = 1, 2, \ldots, r$, we denote by $p(n)$ the smallest prime factor of $n$, so that $p(n) = q_1$, and by $P(n)$ the largest prime factor of $n$, so that $P(n) = q_r$. Similarly, given an integer $n \geq 2$ and an integer $1 \leq i \leq \Omega(n)$, we let $p_i(n)$ stand for the $i$-th smallest prime factor of $n$ and by $P_i(n)$ the $i$-th largest prime factor of $n$, so that

$$p(n) = p_1(n) \leq p_2(n) \leq \cdots \leq P_2(n) \leq P_1(n) = P(n).$$

Hence, for $n = 24176295 = 3^2 \cdot 5 \cdot 11 \cdot 13^2 \cdot 17^2$, we have $p_1(n) = p_2(n) = 3$, $p_3(n) = 5$, $p_4(n) = 11$, and so on, while $P_3(n) = 13$, $P_2(n) = 17$ and $P(n) = P_1(n) = 17$.

For convenience, we write $p(1) = P(1) = 1$.

The functions $p(n)$ and $P(n)$, as well as the function $P_2(n)$, are often used to study and even at times solve number theory problems, in particular some related to the factorization of large numbers, a central problem in cryptography.

## 9.2. The smallest prime factor of an integer

We first study the function $p(n)$ whose behavior is somewhat less complex than that of $P(n)$.

Let $x$ be a large positive real number. How many integers $n \le x$ have the number 2 as their smallest prime factor? Clearly the answer to that question is $\lfloor x/2 \rfloor$. We have thus established, without any difficulty, the formula

$$\sum_{\substack{n \le x \\ p(n)=2}} 1 = \left\lfloor \frac{x}{2} \right\rfloor = \frac{x}{2} + O(1). \tag{9.1}$$

Replacing $p(n) = 2$ by $p(n) = 3$, can one obtain a similar formula? Clearly, the positive integers $n \le x$ such that $p(n) = 3$ are those which are divisible by 3, but not by 2. Thus,

$$\begin{aligned} \sum_{\substack{n \le x \\ p(n)=3}} 1 &= \sum_{\substack{n \le x \\ 3 \mid n}} 1 - \sum_{\substack{n \le x \\ 3 \mid n \text{ and } 2 \mid n}} 1 \\ &= \sum_{\substack{n \le x \\ 3 \mid n}} 1 - \sum_{\substack{n \le x \\ 6 \mid n}} 1 = \left\lfloor \frac{x}{3} \right\rfloor - \left\lfloor \frac{x}{6} \right\rfloor \\ &= \frac{x}{3} - \frac{x}{6} + O(1) = \frac{x}{6} + O(1). \end{aligned}$$

Replacing $p(n) = 3$ by $p(n) = 5$, things become more complicated, while in the general case $p(n) = p_0$, this approach becomes too complicated.

So let $p_0 \ge 3$ be a fixed prime and consider the functions

$$f(n) = \begin{cases} 1 & \text{if } p(n) = p_0, \\ 0 & \text{otherwise} \end{cases} \tag{9.2}$$

and

$$g(n) = \begin{cases} 1 & \text{if } p(n) \ge p_0, \\ 0 & \text{otherwise.} \end{cases} \tag{9.3}$$

Then,

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{f(n)}{n^s} &= \sum_{\substack{m=1 \\ p(m) \ge p_0}}^{\infty} \frac{1}{(p_0 m)^s} = \frac{1}{p_0^s} \left( 1 + \sum_{\substack{m=2 \\ p(m) \ge p_0}}^{\infty} \frac{1}{m^s} \right) = \frac{1}{p_0^s} \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \\ &= \frac{1}{p_0^s} \prod_{p \ge p_0} \left( 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots \right) = \frac{1}{p_0^s} \prod_{p \ge p_0} \left( 1 - \frac{1}{p^s} \right)^{-1} \\ &= \frac{1}{p_0^s} \prod_{p < p_0} \left( 1 - \frac{1}{p^s} \right) \zeta(s). \end{aligned}$$

It is clear that the expression $\dfrac{1}{p_0^s} \displaystyle\prod_{p < p_0} \left( 1 - \frac{1}{p^s} \right)$ converges absolutely when $s = 1$. In light of Wintner's theorem (Theorem 6.13), we may conclude that,

as $x \to \infty$,

$$\sum_{n\le x} f(n) = \sum_{\substack{n\le x\\ p(n)=p_0}} 1 = (1+o(1))\left(\frac{1}{p_0}\prod_{p<p_0}\left(1-\frac{1}{p}\right)\right)x. \tag{9.4}$$

Observe that if $p_0$ is sufficiently large (but fixed), using Mertens' theorem, expression

$$\frac{1}{p_0}\prod_{p<p_0}\left(1-\frac{1}{p}\right) \quad \text{is close to} \quad \frac{e^{-\gamma}}{p_0\log p_0}.$$

Unfortunately, formula (9.4) does not hold uniformly for $p_0 \le x$. Indeed, we need to consider only the case where $p_0$ is a large prime with $x = p_0^2 - 1$, in which case there exists only one positive integer $n \le x$ such that $p(n) = p_0$, namely $n = p_0$, while there should be approximately $\dfrac{1}{p_0\log p_0}x \approx \dfrac{\sqrt{x}}{\log x}$, a nonsense.

The Dirichlet series approach has its limits. The study of the following function leads the way to great results. For $1 < y \le x$, let

$$\Phi(x,y) = \sum_{\substack{n\le x\\ p(n)>y}} 1.$$

Consider the function $h(n)$ defined by

$$h(n) = \begin{cases} 1 & \text{if } p(n) > y,\\ 0 & \text{otherwise,}\end{cases}$$

so that $\Phi(x,y) = \sum_{n\le x} h(n)$. Now

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{h(n)}{n^s} &= \prod_{p>y}\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots\right)\\ &= \prod_{p>y}\left(1-\frac{1}{p^s}\right)^{-1} = \prod_{p\le y}\left(1-\frac{1}{p^s}\right)\zeta(s).\end{aligned}$$

Using Wintner's theorem, we obtain that, if $y$ is fixed, then, as $x \to \infty$,

$$\Phi(x,y) = (1+o(1))\prod_{p\le y}\left(1-\frac{1}{p}\right)x.$$

Does this formula remain valid when $y = y(x) \to \infty$? We choose an elementary approach, one which uses the Inclusion-Exclusion principle. So let $2 \le y \le x$. Then it is clear that

$$\Phi(x,y) = \lfloor x\rfloor - \sum_{p\le y}\sum_{\substack{n\le x\\ p\mid n}} 1 + \sum_{p<q\le y}\sum_{\substack{n\le x\\ pq\mid n}} 1 - \cdots + (-1)^r \sum_{\substack{n\le x\\ q_1q_2\cdots q_r\mid n}} 1$$

$$= \lfloor x \rfloor - \sum_{p \le y} \left\lfloor \frac{x}{p} \right\rfloor + \sum_{p<q \le y} \left\lfloor \frac{x}{pq} \right\rfloor - \cdots + (-1)^r \left\lfloor \frac{x}{q_1 q_2 \cdots q_r} \right\rfloor,$$

where $r = \pi(y)$. By eliminating the brackets in this last formula, we introduce some errors, and this is why we have

$$\begin{aligned} \Phi(x,y) &= x - x \sum_{p \le y} \frac{1}{p} + x \sum_{p<q \le y} \frac{1}{pq} - \cdots + (-1)^r \frac{x}{q_1 q_2 \cdots q_r} + O(2^r) \\ &= x \prod_{p \le y} \left(1 - \frac{1}{p}\right) + O\left(2^{\pi(y)}\right). \end{aligned} \tag{9.5}$$

We notice right away that this error term can cause some problems. Indeed it would be very annoying if it became larger than the main term $x \prod_{p \le y} \left(1 - \frac{1}{p}\right)$.

Since $\pi(y) \sim y/\log y$ as $y \to \infty$, it is easy to see that formula (9.5) remains valid when $y = y(x) \to \infty$ with $y = y(x) \le \log x$. Indeed, in this case, we have $y/\log y < \varepsilon \log x$ and this is why the error term $R(y) = O(2^{\pi(y)})$ satisfies

$$R(y) \ll 2^{\pi(y)} < 2^{\varepsilon \log x} < x^{\varepsilon}.$$

We have thus established that

$$\Phi(x,y) = x \prod_{p \le y} \left(1 - \frac{1}{p}\right) + O(x^{\varepsilon}) \qquad (x \to \infty), \tag{9.6}$$

uniformly for $2 \le y \le \log x$.

It is possible to improve (9.6), that is to extend the range of its validity. For instance, one can show, using the Brun pure sieve (see Section 12.2 of Chapter 12), that

$$\Phi(x,y) = x \prod_{p \le y} \left(1 - \frac{1}{p}\right) \left(1 + O\left(\frac{1}{\log y}\right)\right) \qquad \left(2 \le y \le e^{\frac{1}{10} \frac{\log x}{\log\log x}}\right). \tag{9.7}$$

In the previous chapters, we studied the behavior of $\sum_{n \le x} f(n)$ for various multiplicative or additive functions $f(n)$. But the function $p(n)$ is neither multiplicative nor additive; hence, the methods we have developed to estimate $\sum_{n \le x} f(n)$ do not apply when $f(n) = p(n)$. We must therefore find a different approach.

What is the average order of $p(n)$ ? In fact, the estimation of $\sum_{n \le x} p(n)$ is almost trivial. Indeed, we will see that this sum is dominated by the prime

numbers $p \le x$. Separating the sum into two parts, we obtain

$$\sum_{n\le x} p(n) = \sum_{p\le x} p + \sum_{\substack{n\le x\\ \Omega(n)\ge 2}} p(n) = \Sigma_1 + \Sigma_2,$$

say. On the one hand,

$$\begin{aligned}\Sigma_1 &= \int_{2-0}^{x} t\,d\pi(t) = t\pi(t)\Big|_{2-0}^{x} - \int_2^x \pi(t)\,dt\\ &= x\pi(x) - \int_2^x \frac{t}{\log t}\,dt + O\left(\int_2^x \frac{t}{\log^2 t}\,dt\right)\\ &= \frac{1}{2}\frac{x^2}{\log x} + O\left(\frac{x^2}{\log^2 x}\right).\end{aligned} \tag{9.8}$$

On the other hand,

$$\Sigma_2 \le \sum_{n\le x} n^{1/2} < x^{3/2}.$$

Combining these estimates of $\Sigma_1$ and $\Sigma_2$, we obtain

$$\sum_{n\le x} p(n) = \frac{1}{2}\frac{x^2}{\log x} + O\left(\frac{x^2}{\log^2 x}\right). \tag{9.9}$$

The average order of $p(n)$ is therefore $n/\log n$, which by the way does not mean that $p(n)$ is "close" to $n/\log n$ most of the time. On the contrary, most of the time, $p(n)$ is small in the sense that the number of times that $p(n) \le y$ among the integers $n \le x$ (for $y \le \log x$) is equal to

$$x - \Phi(x,y) \approx x - \frac{x}{\log y} = x\left(1 - \frac{1}{\log y}\right) \to x \qquad (y\to\infty).$$

In closing this section, let us mention the useful uniform upper bound

$$\Phi(x,y) \ll \frac{x}{\log y} \qquad (2 \le y \le x), \tag{9.10}$$

a proof of which can be found in Tenenbaum's book [**140**].

## 9.3. The largest prime factor of an integer

As we will now see, the study of the function $P(n)$ turns out to be slightly more difficult than that of $p(n)$.

We begin with the study of the global behavior of $P(n)$, namely by establishing the value of $\sum_{2\le n\le x} P(n)$. For this, we will need the estimate

$$\sum_{p\le x} p = \frac{1}{2}\frac{x^2}{\log x} + O\left(\frac{x^2}{\log^2 x}\right), \tag{9.11}$$

a result which we have already proved (see (9.8)).

Let us now introduce the function

$$\Psi(x,y) = \#\{n \le x : P(n) \le y\},$$

defined for all $x > 0$, $y > 0$.

**Definition 9.1.** *Let $x$ be large and $y \le x$. A positive integer $n \le x$ is called $y$-smooth (or friable) if $P(n) \le y$.*

The following result will be helpful in the study of the $\Psi(x,y)$ function.

**Theorem 9.2.** *As $x \to \infty$,*

$$\sum_{2 \le n \le x} P(n) = \frac{\pi^2}{12} \frac{x^2}{\log x} + O\left(\frac{x^2}{\log^2 x}\right). \tag{9.12}$$

**Proof.** It is clear that

$$\begin{aligned}
\sum_{2 \le n \le x} P(n) &= \sum_{p \le x} p \sum_{\substack{n \le x \\ P(n)=p}} 1 = \sum_{p \le x} p \sum_{\substack{pm \le x \\ P(m) \le p}} 1 = \sum_{p \le x} p \sum_{\substack{m \le x/p \\ P(m) \le p}} 1 \\
&= \sum_{p \le x} p\Psi\left(\frac{x}{p}, p\right) = \sum_{p \le x^{1/2}} p\Psi\left(\frac{x}{p}, p\right) + \sum_{x^{1/2} < p \le x} p\Psi\left(\frac{x}{p}, p\right) \\
&= \Sigma_1 + \Sigma_2,
\end{aligned}$$

say. On the one hand, it is trivial that

$$\Sigma_1 \ll \sum_{p \le x^{1/2}} p\left(\frac{x}{p}\right) = x\pi(x^{1/2}) \le x^{3/2}.$$

On the other hand, for $p > x^{1/2}$, we have $\Psi(x/p, p) = \lfloor x/p \rfloor$, from which it follows that

$$\begin{aligned}
\Sigma_2 &= \sum_{x^{1/2} < p \le x} p\left\lfloor \frac{x}{p} \right\rfloor = \sum_{p \le x} p\left\lfloor \frac{x}{p} \right\rfloor - \sum_{p \le x^{1/2}} p\left\lfloor \frac{x}{p} \right\rfloor \\
&= \sum_{p \le x} p \sum_{n \le x/p} 1 + O(x^{3/2}) = \sum_{np \le x} p + O(x^{3/2}) = \sum_{n \le x} \sum_{p \le x/n} p + O(x^{3/2}) \\
&= \Sigma_3 + O(x^{3/2}),
\end{aligned}$$

for example. We now call upon (9.11) to estimate $\Sigma_3$. We first write

$$\Sigma_3 = \sum_{n \le \log x} \sum_{p \le x/n} p + \sum_{\log x < n \le x} \sum_{p \le x/n} p = \Sigma_4 + \Sigma_5,$$

for example. For $n \le \log x$, we have

$$\frac{1}{\log(x/n)} = \frac{1}{\log x - \log n} = \frac{1}{\log x}\left(1 + O\left(\frac{\log n}{\log x}\right)\right),$$

so that, in light of (9.11),

$$\Sigma_4 = \frac{1}{2}\frac{x^2}{\log x}\sum_{n\le \log x}\frac{1}{n^2}\left(1+O\left(\frac{\log n}{\log x}\right)\right).$$

Now

$$\sum_{n\le \log x}\frac{1}{n^2} = \sum_{n=1}^{\infty}\frac{1}{n^2} - \sum_{n>\log x}\frac{1}{n^2} = \zeta(2)+O\left(\int_{\log x}^{\infty}\frac{1}{t^2}\,dt\right) = \frac{\pi^2}{6}+O\left(\frac{1}{\log x}\right),$$

while

$$\frac{1}{\log x}\sum_{n\le \log x}\frac{\log n}{n^2} \ll \frac{1}{\log x}.$$

Therefore,

$$\Sigma_4 = \frac{\pi^2}{12}\frac{x^2}{\log x}+O\left(\frac{x^2}{\log^2 x}\right).$$

Finally, it is easy to show that in comparison $\Sigma_5$ is negligible. Indeed,

$$\Sigma_5 = \sum_{\log x<n\le x^{1/2}}\sum_{p\le x/n} p + \sum_{x^{1/2}<n\le x}\sum_{p\le x/n} p = \Sigma_6+\Sigma_7,$$

say. But

$$\Sigma_7 < \sum_{x^{1/2}<n\le x}\frac{x}{n}\sum_{p\le x^{1/2}} 1 \ll x\pi(x^{1/2})\sum_{x^{1/2}<n\le x}\frac{1}{n} \ll x\cdot\frac{x^{1/2}}{\log x}\cdot\log x = x^{3/2}$$

and since for $n\le x^{1/2}$ we have $x/n\ge x^{1/2}$, we can use estimate (9.11), that is the fact that $\sum_{p\le X} p \ll \dfrac{X^2}{\log X}$ when $X\to\infty$; this is why (with $X=x/n$) we have

$$\begin{aligned}\Sigma_6 &\ll \sum_{\log x<n\le x^{1/2}}\left(\frac{x}{n}\right)^2\frac{1}{\log(x/n)} \ll \frac{x^2}{\log x}\sum_{\log x<n\le x^{1/2}}\frac{1}{n^2}\\ &\ll \frac{x^2}{\log x}\cdot\frac{1}{\log x} = \frac{x^2}{\log^2 x}.\end{aligned}$$

Collecting the above estimates, we easily obtain (9.12), thus completing the proof of Theorem 9.2. □

We will first try to estimate $\Psi(x,y)$ for a fixed $y$. Let us start with $y=2$. In this case, we have

$$\Psi(x,2) = \sum_{\substack{2^m\le x\\ m\ge 0}} 1 = \sum_{0\le m\le \frac{\log x}{\log 2}} 1 = \left\lfloor\frac{\log x}{\log 2}\right\rfloor + 1 = \frac{\log x}{\log 2}+O(1).$$

For $y = 3$, we have

$$\begin{aligned}
\Psi(x,3) &= \sum_{\substack{2^m 3^k \le x \\ m\ge 0,\ k\ge 0}} 1 = \sum_{0\le m\le \frac{\log x}{\log 2}} \ \sum_{0\le k\le \frac{\log x - m\log 2}{\log 3}} 1 \\
&= \sum_{0\le m\le \frac{\log x}{\log 2}} \left( \left\lfloor \frac{\log x - m\log 2}{\log 3} \right\rfloor + 1 \right) \\
&= \sum_{0\le m\le \frac{\log x}{\log 2}} \left( \frac{\log x}{\log 3} - \left(\frac{\log 2}{\log 3}\right) m + O(1) \right) \\
&= \frac{\log^2 x}{\log 2 \log 3} - \frac{\log 2}{\log 3} \sum_{0\le m\le \frac{\log x}{\log 2}} m + O(\log x) \\
&= \frac{\log^2 x}{\log 2 \log 3} - \frac{\log 2}{\log 3} \frac{\log^2 x}{2\log^2 2} + O(\log x) \\
&= \frac{\log^2 x}{2\log 2 \log 3} + O(\log x).
\end{aligned}$$

Following the same reasoning, one can show that

$$\Psi(x,5) = \frac{\log^3 x}{3!\log 2\log 3\log 5} + O(\log^2 x).$$

In Section 9.6, we will give a general estimate for $\Psi(x,y)$ which holds uniformly for $2 \le y \le \sqrt{\log x}$. But what if $y$ is larger, say $y \ge \log x$?

The following is probably the most important result concerning the $\Psi(x,y)$ function.

**Theorem 9.3.** *For each $y \ge 2$ and $x \ge 2$, set $u := \log x/\log y$. Then,*

$$\Psi(x,y) = (1+o(1))x\rho(u) \qquad (x\to\infty),$$

*where $\rho(u)$ is the Dickman function defined by the initial condition $\rho(u) = 1$ $(0 \le u \le 1)$ and thereafter as the solution to the differential equation with shift differences*

$$u\rho'(u) + \rho(u-1) = 0 \qquad (u > 1). \tag{9.13}$$

**Proof.** Let us start with the case $y \ge x$. Clearly, in that case, we have

$$\Psi(x,y) = \lfloor x \rfloor = x + O(1).$$

We now examine the case where $\sqrt{x} \le y \le x$, or in terms of $u$ the case $1 \le u \le 2$. We then have

$$\begin{aligned}\Psi(x,y) &= \Psi(x,x^{1/u}) = \lfloor x \rfloor - \sum_{x^{1/u}<p\le x} \sum_{\substack{n\le x\\ p\mid n}} 1 = \lfloor x \rfloor - \sum_{x^{1/u}<p\le x} \left\lfloor \frac{x}{p} \right\rfloor \\ &= x + O(1) - x \sum_{x^{1/u}<p\le x} \frac{1}{p} - \sum_{x^{1/u}<p\le x} \left( \left\lfloor \frac{x}{p} \right\rfloor - \frac{x}{p} \right).\end{aligned}$$

Using the estimate $\sum_{x^{1/u}<p\le x} 1/p = \log u + O(1/\log x)$ and the fact that $\sum_{x^{1/u}<p\le x} 1 = O(x/\log x)$, we obtain

(9.14)
$$\Psi(x,x^{1/u}) = x\left(1 - \log u + O\left(\frac{1}{\log x}\right)\right) = x(1-\log u) + O\left(\frac{x}{\log x}\right).$$

We have thus established that, for $0 \le u \le 2$,

$$\Psi(x,x^{1/u}) = (1+o(1))x\rho(u) \qquad (x \to \infty), \tag{9.15}$$

where

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

Now, our goal is to prove (9.15) for each $u \ge 0$.

We will adopt the particular induction approach used by Granville [**68**]. Assuming that (9.15) holds for all $u \in [0, N]$, we will now prove that it must also hold for all $u \in [N, N+1]$. For this, we will need the Buchstab-de Bruijn identity, that is,

$$\Psi(x,y) = 1 + \sum_{p\le y} \Psi\left(\frac{x}{p}, p\right). \tag{9.16}$$

(See Problem 9.10 for the more general Buchstab identity.)

Using (9.16), we have

$$\begin{aligned}\Psi(x,x^{1/N}) &= 1 + \sum_{p\le x^{1/N}} \Psi\left(\frac{x}{p},p\right) \\ \Psi(x,x^{1/u}) &= 1 + \sum_{p\le x^{1/u}} \Psi\left(\frac{x}{p},p\right).\end{aligned}$$

Subtracting these two equations, we obtain

$$\Psi(x,x^{1/u}) = \Psi(x,x^{1/N}) - \sum_{x^{1/u}<p\le x^{1/N}} \Psi\left(\frac{x}{p},p\right). \tag{9.17}$$

Now, since $p > x^{1/u}$ and $u \in [N, N+1]$, we have

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

implying that (9.15) holds, say with $u' = \frac{\log(x/p)}{\log p}$ instead of $u$, thus allowing us to replace (9.17) by

$$\begin{aligned}
\Psi(x, x^{1/u}) &= (1+o(1))x\rho(N) - (1+o(1)) \sum_{x^{1/u} < p \le x^{1/N}} \frac{x}{p} \rho\left(\frac{\log x}{\log p} - 1\right) \\
&= (1+o(1))x\rho(N) - (1+o(1))x \int_{x^{1/u}}^{x^{1/N}} \rho\left(\frac{\log x}{\log v} - 1\right) \frac{dv}{v \log v} \\
&= (1+o(1))x \left(\rho(N) - \int_N^u \frac{\rho(t-1)}{t}\, dt\right) \\
&= (1+o(1))\rho(u),
\end{aligned}$$

(where we used Problem 5.14), thus showing that (9.15) also holds for $u \in [N, N+1]$ if we set

$$\rho(u) = \rho(N) - \int_N^u \rho(v-1)\, \frac{dv}{v} \qquad (N < u \le N+1),$$

thus completing the induction argument and the proof of the theorem. □

The Dickman function is an interesting function in its own right.

**Theorem 9.4.** *The Dickman function $\rho(u)$ has the following four properties:*

(i) $u\rho(u) = \int_{u-1}^u \rho(v)\, dv \quad (u \ge 1)$;
(ii) $\rho(u) > 0 \quad (u > 0)$;
(iii) $\rho'(u) < 0 \quad (u > 1)$;
(iv) $\rho(u) \le \frac{1}{\Gamma(u+1)} \quad (u \ge 0)$.

**Proof.** We sketch only the proofs. First, we let $f(u) = u\rho(u)$ and $g(u) = \int_{u-1}^u \rho(v)\, dv$. It is easy to verify, using (9.13), that $f'(u) = g'(u)$. Hence, $f(u) = g(u) + c$ for a certain constant $c$. But $f(1) = g(1)$. Therefore, $c = 0$. This proves (i).

It is clear that (ii) follows from (i).

One easily sees that (iii) follows from (ii) and (9.13).

Finally, to prove (iv), we use induction on $k = \lfloor u \rfloor$. The property is satisfied for $k = 0$, since $\rho(u) = 1$ for $0 \le u \le 1$. On the other hand, for all

$u \geq 1$, we have, because of (i) and (iii),

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

Therefore, by the induction hypothesis, if $k = \lfloor u \rfloor \geq 1$, we have

$$\rho(u) \leq \frac{1}{u\Gamma(u)} = \frac{1}{\Gamma(u+1)},$$

thus completing the proof of (iv). □

## 9.4. The Rankin method

In 1938, Rankin [**118**] proved that uniformly for $x \geq y \geq 3$,

$$\Psi(x,y) \ll xe^{-u}\log y. \tag{9.18}$$

To do so, he used a very original strategy, now known as the *Rankin method*. Here is how it goes. First of all, it is clear that for each real number $\sigma > 0$, we have

$$\begin{aligned}\Psi(x,y) &= \sum_{\substack{n\leq x\\ P(n)\leq y}} 1 \leq \sum_{\substack{n\geq 1\\ P(n)\leq y}} \left(\frac{x}{n}\right)^{\sigma} = x^{\sigma}\prod_{p\leq y}\left(1+\frac{1}{p^{\sigma}}+\frac{1}{p^{2\sigma}}+\cdots\right)\\ &= x^{\sigma}\prod_{p\leq y}\left(1-\frac{1}{p^{\sigma}}\right)^{-1}.\end{aligned}$$

Choosing $\sigma = 1 - \frac{1}{\log y}$, we derive

$$\Psi(x,y) \leq x^{1-\frac{1}{\log y}}\prod_{p\leq y}\left(1-\frac{1}{p^{1-\frac{1}{\log y}}}\right)^{-1} \ll xe^{-u}\log y,$$

since

$$\prod_{p\leq y}\left(1-\frac{1}{p^{1-\frac{1}{\log y}}}\right)^{-1} \ll \log y. \tag{9.19}$$

Indeed, if we set $\sigma = 1 - \frac{1}{\log y}$, we can write

$$\begin{aligned}\prod_{p\leq y}\left(1-\frac{1}{p^{\sigma}}\right)^{-1} &= \exp\left\{-\sum_{p\leq y}\log\left(1-\frac{1}{p^{\sigma}}\right)\right\} = \exp\left\{\sum_{p\leq y}\frac{1}{p^{\sigma}}+O(1)\right\}\\ &= \exp\left\{\sum_{p\leq y}\frac{1}{p}+\sum_{p\leq y}\frac{p^{\frac{1}{\log y}}-1}{p}+O(1)\right\}\\ &= \exp\left\{\log\log y + O(1) + R(y)\right\},\end{aligned}$$

where

$$R(y) = \sum_{p \le y} \frac{e^{\frac{\log p}{\log y}} - 1}{p} \ll \frac{1}{\log y} \sum_{p \le y} \frac{\log p}{p} \ll 1.$$

We have therefore found that

$$\prod_{p \le y} \left(1 - \frac{1}{p^\sigma}\right)^{-1} \ll \log y,$$

which proves (9.19) and thereby (9.18).

It is possible to improve estimate (9.18). As a matter of fact, we can prove the following remarkable result.

**Theorem 9.5.** *For all $x \ge y \ge 2$,*

$$\Psi(x, y) \ll x\, e^{-u/2}. \tag{9.20}$$

To prove this result, we first prove two lemmas which are of independent interest.

**Lemma 9.6.** *Let $f$ be a multiplicative function such that $f(n) \ge 0$ for all $n$, and such that there exist constants $A$ and $B$ such that for all $x > 1$ both inequalities*

$$\sum_{p \le x} f(p) \log p \le Ax \tag{9.21}$$

*and*

$$\sum_{p} \sum_{\alpha \ge 2} \frac{f(p^\alpha)}{p^\alpha} \log p^\alpha \le B \tag{9.22}$$

*hold. Then, for $x > 1$, we have*

$$\sum_{n \le x} f(n) \le (A + B + 1) \frac{x}{\log x} \sum_{n \le x} \frac{f(n)}{n}. \tag{9.23}$$

**Proof.** Let $S(x)$ be the sum which appears on the left-hand side of (9.23) and $L(x)$ be the sum that appears on the right-hand side of (9.23). Observe that $S(x) \le xL(x)$. It is clear that

$$\begin{aligned} S(x) \log x &= \sum_{n \le x} f(n) \log x = \sum_{n \le x} f(n) \log\Big(\frac{x}{n}\Big) + \sum_{n \le x} f(n) \sum_{p \| n} \log p \\ &+ \sum_{n \le x} f(n) \sum_{\substack{\alpha \ge 2 \\ p^\alpha \| n}} \log p^\alpha = S_1 + S_2 + S_3, \end{aligned}$$

say. Since $x/n > \log(x/n)$ for all $n \le x$, we get that

$$S_1 \le \sum_{n\le x} f(n)\frac{x}{n} = xL(x). \tag{9.24}$$

Writing $n = mp$ with $p \nmid m$ in $S_2$, changing the order of summation, and using inequality (9.21), we get

$$S_2 = \sum_{m\le x} f(m) \sum_{\substack{p\le x/m \\ p\nmid m}} f(p)\log p \le A\sum_{m\le x} f(m)\frac{x}{m} = AxL(x). \tag{9.25}$$

Making, for each $\alpha \ge 2$ and $p^\alpha || n$, the change of variable $n = mp^\alpha$ with $p \nmid m$ in $S_3$, changing the order of summation, and using inequality (9.22), we get

$$\begin{aligned} S_3 &= \sum_p \sum_{\alpha\ge 2} f(p^\alpha)\log(p^\alpha) \sum_{\substack{m\le x/p^\alpha \\ p\nmid m}} f(m) \\ &\le \sum_p \sum_{\alpha\ge 2} f(p^\alpha)\log(p^\alpha) S\Big(\frac{x}{p^\alpha}\Big) \\ &\le \sum_p \sum_{\alpha\ge 2} f(p^\alpha)\log(p^\alpha)\cdot\Big(\frac{x}{p^\alpha}\Big)\cdot L\Big(\frac{x}{p^\alpha}\Big) \\ &\le xL(x)\sum_p \sum_{\alpha\ge 2} \frac{f(p^\alpha)}{p^\alpha}\cdot\log(p^\alpha) \le BxL(x). \end{aligned} \tag{9.26}$$

Inequality (9.23) now follows from (9.24), (9.25), and (9.26). □

**Lemma 9.7.** *Let $\lambda_1, \lambda_2$ be constants such that $\lambda_1 > 0$ and $0 \le \lambda_2 < 2$. If $f$ is a multiplicative function with $0 \le f(p^\alpha) \le \lambda_1\lambda_2^{\alpha-1}$ for all primes $p$ and integers $\alpha \ge 1$, then for all $x \ge 1$ we have*

$$\sum_{n\le x} f(n) \ll x\prod_{p\le x}\Big((1-p^{-1})\sum_{\alpha=0}^{\infty} f(p^\alpha)p^{-\alpha}\Big). \tag{9.27}$$

**Proof.** Since

$$\prod_{p\le x}(1-p^{-1}) \gg \frac{1}{\log x}$$

(see Problem 4.4) and

$$\prod_{p\le x}\sum_{\alpha\ge 0}\frac{f(p^\alpha)}{p^\alpha} \ge \sum_{n\le x}\frac{f(n)}{n},$$

it suffices to prove, via Lemma 9.6, that inequalities (9.21) and (9.22) are fulfilled for the function $f$. Clearly,

$$\sum_{p\le x} f(p)\log p \le \lambda_1\sum_{p\le x}\log p = \lambda_1\theta(x) \ll x.$$

Furthermore,

$$\begin{aligned}\sum_p \sum_{\alpha\ge 2} \frac{f(p^\alpha)}{p^\alpha}\cdot \log(p^\alpha) &\le \lambda_1 \sum_p \frac{\log p}{p} \sum_{\alpha\ge 2} \alpha\Big(\frac{\lambda_2}{p}\Big)^{\alpha-1} \le 2\lambda_1\lambda_2 \sum_{p\ge 2} \frac{\log p}{(p-\lambda_2)^2}\\ &\le \frac{2\lambda_1\lambda_2}{(2-\lambda_2)^2} + \sum_{n\ge 3} \frac{\log n}{(n-\lambda_2)^2} \ll 1,\end{aligned}$$

where we used the fact that for $r = \lambda_2/p < 1$,

$$\sum_{\alpha\ge 2} \alpha r^{\alpha-1} = \frac{r(2-r)}{(1-r)^2} \le \frac{2r}{(1-r)^2},$$

which completes the proof of (9.27). □

We are now ready to prove Theorem 9.5.

**Proof.** We may assume that $y \ge 11$, since otherwise, as we have only four primes smaller than 11, it follows easily that $\Psi(x,y) \ll \log^4 x$, while the right-hand side of inequality (9.20) is at least $\gg \dfrac{x}{\exp\big(\frac{\log x}{2\log 2}\big)} = x^{1-1/2\log 2}$. Using Rankin's method with $\gamma \ge 0$, we have

$$\Psi(x,y) \le x^{3/4} + \sum_{n\le x} \Big(\frac{n}{x^{3/4}}\Big)^\gamma \chi(n,y), \tag{9.28}$$

where we write $\chi(n,y) = 1$ if $P(n) \le y$ and 0 otherwise. With $\gamma = 2/(3\log y)$, the multiplicative function $n \longmapsto n^\gamma \chi(n,y)$ fulfills the conditions of Lemma 9.7 with $\lambda_1 = \lambda_2 = e^{2/3}$, so that by inequality (9.27), we get

$$\sum_{n\le x} n^\gamma \chi(n,y) \ll x \prod_{p\le y} \Big((1-p^{-1}) \sum_{\alpha=0}^{\infty} p^{\alpha(\gamma-1)}\Big). \tag{9.29}$$

Note that

$$\begin{aligned}(1-p^{-1}) \sum_{\alpha=0}^{\infty} p^{\alpha(\gamma-1)} &= \Big(\frac{p-1}{p}\Big)\Big(\frac{p^{1-\gamma}}{p^{1-\gamma}-1}\Big) = \frac{p-1}{p^\gamma(p^{1-\gamma}-1)}\\ &= \frac{p-1}{p-p^\gamma} = 1 + \frac{p^\gamma-1}{p-p^\gamma} = 1 + O\Big(\frac{p^\gamma-1}{p}\Big)\\ &= 1 + O\Big(\frac{e^{\gamma\log p}-1}{p}\Big) = 1 + O\Big(\frac{\gamma\log p}{p}\Big),\end{aligned}$$

where we used the fact that $1 < p^\gamma \ll 1$ holds for all $2 \le p \le y$. Thus, (9.29) becomes

$$\begin{aligned}\sum_{n\le x} n^\gamma \chi(n,y) &\ll x \prod_{p\le y}\Big(1 + O\Big(\frac{\gamma \log p}{p}\Big)\Big) \\ &\ll x \exp\left\{ O\Big(\sum_{p\le y} \frac{\gamma \log p}{p}\Big)\right\} \\ &= x \exp(O(1)) \ll x,\end{aligned} \tag{9.30}$$

where we used the fact that $\gamma \ll 1/\log y$ and again that

$$\sum_{p\le y} \frac{\log p}{p} \ll \log y,$$

which is Theorem 4.4. Since $\frac{1}{4}\log x > \frac{1}{2}u$ for $y \ge 11$ (because $\log 11 > 2$), we get, by inequalities (9.28) and (9.30), that

$$\Psi(x,y) \ll x^{3/4} + \frac{x}{x^{3\gamma/4}} = \frac{x}{\exp(\frac{1}{4}\log x)} + \frac{x}{\exp(\frac{3\gamma}{4}\log x)} \le \frac{2x}{\exp(u/2)},$$

which completes the proof of Theorem 9.5. □

As a consequence of Theorem 9.5, we have the following.

**Corollary 9.8.** *If $\varepsilon(x)$ is any positive function of $x$ which tends to zero as $x$ tends to infinity, then*

$$\Psi(x, x^{\varepsilon(x)}) = o(x)$$

*as $x \to \infty$.*

**Proof.** This follows immediately from Theorem 9.5, by observing that for $y = x^{\varepsilon(x)}$,

$$u = \frac{\log x}{\log y} = \frac{\log x}{\log(x^{\varepsilon(x)})} = \frac{1}{\varepsilon(x)} \to \infty$$

as $x \to \infty$. □

## 9.5. An application to pseudoprimes

The base 2 pseudoprimes were defined in Problem 2.9. We can define them for all bases as follows.

**Definition 9.9.** *Let $a > 1$ be a given integer. A composite integer $n > 1$ coprime to $a$ is called pseudoprime with respect to $a$ if $a^{n-1} \equiv 1 \pmod n$. A natural number $n$ which is composite and such that the congruence $a^n \equiv a \pmod n$ holds for all integers $a$ is called a Carmichael number.*

**Example 9.10.** *The integer* $n = 561 = 3 \times 11 \times 17$ *is a Carmichael number.*

There are infinitely many Carmichael numbers. This result was proved in 1994 by Alford, Granville, and Pomerance [**1**]. Some evidence for it is as follows.

Consider the numbers $p = 3 + 40k,\ q = 11 + 200k$, and $r = 17 + 320k$. Let $n = pqr$. Then

$$n-1 = (3+40k)(11+200k)(17+320k)-1 = 80(1+20k)(1600k^2+213k+7),$$

while $p-1 = 2(1+20k),\ q-1 = 10(1+20k)$ and $r-1 = 16(1+20k)$. Thus, $p-1,\ q-1,\ r-1$ all divide $n-1$. If $p,\ q,\ r$ were all prime numbers, then each element in the multiplicative group

$$U(\mathbb{Z}/n\mathbb{Z}) = U(\mathbb{Z}/(pqr)\mathbb{Z}) = U(\mathbb{Z}/p\mathbb{Z}) \times U(\mathbb{Z}/q\mathbb{Z}) \times U(\mathbb{Z}/r\mathbb{Z})$$

would have its order dividing $\operatorname{lcm}[p-1, q-1, r-1]$, which in turn divides $n-1$. Hence, $a^{n-1} \equiv 1 \pmod{n}$ for all positive integers $a$ coprime to $n$. Thus, $a^n \equiv a \pmod{n}$ for any such $a$. Now, it is easy to see that this last congruence actually holds even for all positive integers $a$, regardless of whether they are coprime to $n$ or not. Now, the Prime $k$-tuple conjecture (Conjecture 2.11) suggests that there should be infinitely many values of $k$ such that $p = 3+40k,\ q = 11+200k$ and $r = 17+320k$ are all simultaneously primes.

However, the pseudoprimes to base 2 are not very abundant, as the following result suggests.

**Proposition 9.11.** *The sum of the reciprocals of the base* 2 *pseudoprimes is convergent.*

**Proof.** Let

$$\mathcal{P}^{(2)} = \{n \in \mathbb{N} : n \text{ is a base 2 pseudoprime}\}.$$

Let us first find an upper bound for the counting function $\mathcal{P}^{(2)}(x) = \#(\mathcal{P}^{(2)} \cap [1, x])$ of the set $\mathcal{P}^{(2)}$.

Let $x$ be large and let $y$ be some function of $x$ which tends to infinity with $x$ and which will be made more precise later. Let

$$\mathcal{A}_1(x) = \{n \le x \mid P(n) \le y\}.$$

By Theorem 9.5, we know that

$$\#\mathcal{A}_1(x) = \Psi(x, y) \ll \frac{x}{\exp(u/2)}, \tag{9.31}$$

where $u = \log x / \log y$.

Let $\mathcal{A}_2(x)$ be the set of those $n \le x$ which are not in $\mathcal{A}_1(x)$ but such that $P(n)^2|n$. For each such $n$, we have $P(n) = p > y$ and $p^2|n$. For $p$ fixed, the number of such $n \le x$ is $\le x/p^2$. Thus,

$$\#\mathcal{A}_2(x) \le \sum_{p>y} \frac{x}{p^2} \ll x \sum_{n>y} \frac{1}{n^2} \ll \frac{x}{y}. \tag{9.32}$$

For each $p > 2$, let $t_p$ be the multiplicative order of 2 modulo $p$, that is, the smallest positive integer $k$ such that $2^k \equiv 1 \pmod p$. Let

$$\mathcal{P} = \{p \ : \ t_p < p^{1/4}\},$$

and for $x$ large let $\mathcal{P}(x) = \mathcal{P} \cap [1, x]$. Let us bound $a(x) = \#\mathcal{P}(x)$. On the one hand, as $x \to \infty$,

$$\prod_{p\in\mathcal{P}(x)} p \ge \prod_{k=1}^{a(x)} p_k = \exp\left(\sum_{p\le p_{a(x)}} \log p\right) = \exp((1+o(1))a(x)\log(a(x))), \tag{9.33}$$

by the Prime Number Theorem. On the other hand,

$$\prod_{p\in\mathcal{P}(x)} p \ \Big| \ \prod_{t<x^{1/4}} (2^t - 1),$$

so that

$$\prod_{p\in\mathcal{P}(x)} p < \prod_{t<x^{1/4}} 2^t = \exp\Big(\log 2 \sum_{t<x^{1/4}} t\Big) = \exp(O(x^{1/2})), \tag{9.34}$$

implying that by inequalities (9.33) and (9.34), we have

$$(1+o(1))a(x)\log a(x) \ll x^{1/2},$$

which leads to the conclusion that the inequality

$$a(x) < x^{1/2} \tag{9.35}$$

holds for all sufficiently large $x$.

Let $\mathcal{A}_3(x)$ be the set of those $n \le x$ which are not in $\mathcal{A}_1(x) \cup \mathcal{A}_2(x)$, but for which $P(n) \in \mathcal{P}$. Given $n \in \mathcal{A}_3(x)$, we write $n = pm$, where $p = P(n) > y$ and $p \in \mathcal{P}$. Fix $m$. Then $p < x/m$, and since $x/m > y$ is large if $x$ is large, we get that $p \in \mathcal{P}(x/m)$, and, by inequality (9.35), we get that the number of values that $p$ can take is $< (x/m)^{1/2}$. Thus,

$$\#\mathcal{A}_3(x) < \sum_{m<x/y} \left(\frac{x}{m}\right)^{1/2} \ll x^{1/2} \int_1^{x/y} \frac{dt}{t^{1/2}} \ll x^{1/2} \cdot \left(\frac{x}{y}\right)^{1/2} = \frac{x}{y^{1/2}}. \tag{9.36}$$

Finally, let $\mathcal{A}_4(x)$ be the set of those $n \le x$ which are not in $\mathcal{A}_1(x) \cup \mathcal{A}_2(x) \cup \mathcal{A}_3(x)$ but which are pseudoprimes to the base 2. Let $n \in \mathcal{A}_4(x)$

and write $n = mp$, where $p = P(n)$. Then $t_p \geq p^{1/4} > y^{1/4}$. Since $2^{n-1} \equiv 1 \pmod{n}$, we get that $2^{n-1} \equiv 1 \pmod{p}$. Thus, $n \equiv 1 \pmod{t_p}$, which can be written as $pm \equiv 1 \pmod{t_p}$. By Fermat's little theorem, $p \equiv 1 \pmod{t_p}$, which together with the previous congruence leads to the conclusion that $m \equiv 1 \pmod{t_p}$. Thus, $t_p | m-1$. Note that $n$ is composite so that $m > 1$. So, if $n = mp \in \mathcal{A}_4(x)$, then there exists a divisor $t_p$ of $m-1$, with $t_p > p^{1/4} > y^{1/4}$, such that $p \equiv 1 \pmod{t_p}$. Fix $m > 1$ and a divisor $d > y^{1/4}$ of $m-1$. Since $p < x/m$, the number of such primes $p$ is

$$\leq \Big\lfloor \frac{x}{dm} \Big\rfloor + 1 \leq \frac{x}{dm} + 1.$$

Summing over all divisors $d$ of $m-1$ with $d > y^{1/4}$, we get that the number of such $n$ for a fixed $m$ is

$$\ll \frac{x}{y^{1/4}} \cdot \frac{d(m-1)}{m} + d(m-1). \tag{9.37}$$

Summing up inequalities (9.37) over all the $m$ with $2 \leq m < x/y$, we get

$$\#\mathcal{A}_4(x) \ll \frac{x}{y^{1/4}} \sum_{k<x} \frac{d(k)}{k+1} + \sum_{k<x/y} d(k) \ll \frac{x \log^2 x}{y^{1/4}} + \frac{x}{y} \log(x/y) \ll \frac{x \log^2 x}{y^{1/4}}, \tag{9.38}$$

where we used Theorem 4.9 (for the second sum) as well as the fact that, by Abel's summation formula,

$$\sum_{k<x} \frac{d(k)}{k+1} = \frac{x \log x}{x+1} + \int_1^x \frac{t \log t}{(t+1)^2}\, dt \ll \log^2 x.$$

Comparing inequalities (9.31), (9.32), (9.36), and (9.38), the best upper bound that comes out of our argument is obtained if one chooses $y$ such that

$$\frac{\log^2 x}{y^{1/4}} = \frac{1}{\exp(u/2)},$$

which is equivalent to

$$\frac{\log y}{4} - 2 \log\log x = \frac{\log x}{2 \log y},$$

which gives $\log y = \sqrt{2}(1+o(1))\sqrt{\log x}$ as $x \to \infty$. With this $y$, we therefore obtain that

$$\mathcal{P}^{(2)}(x) \ll \frac{x}{\exp\big(\frac{1}{2\sqrt{2}}(1+o(1))\sqrt{\log x}\big)} < \frac{x}{\exp(c\sqrt{\log x})}, \tag{9.39}$$

where we can choose $c$ to be any constant $< \dfrac{1}{2\sqrt{2}}$, in which case inequality (9.39) holds for all large values of $x$. In particular, inequality (9.39) implies

that for each $\delta > 1$, the inequality

$$\mathcal{P}^{(2)}(x) < \frac{x}{\log^{\delta} x}$$

holds for $x > x(\delta)$. Then it is clear that this last inequality implies (via the Abel summation formula) that the sum of the reciprocals of all the pseudoprimes to base 2 is convergent. □

It follows from (9.39) that there are much fewer base 2 pseudoprimes (up to $x$) than primes up to $x$, since we know that $\pi(x) \sim x/\log x$. Thus, probabilistically speaking, if an $n$ satisfies $2^{n-1} \equiv 1 \pmod{n}$, then it is quite likely that $n$ is prime and not pseudoprime. This observation is the base of several fast *probabilistic primality tests* (i.e., which return the certificate "$n$ is prime" with a high probability of being correct).

## 9.6. The geometric method

For fixed values of $y$ as well as for values $y = y(x)$ which do not grow too fast with $x$, one can use a geometric approach to estimate the size of $\Psi(x, y)$.

Let $a_1, a_2, \ldots$ be a sequence of positive real numbers, and set

$$N_k(z) \stackrel{\text{def}}{=} \#\{(\nu_1, \nu_2, \ldots, \nu_k) \in \mathbb{Z}^k : \nu_1 \geq 0, \ldots, \nu_k \geq 0,\ \sum_{i=1}^{k} \nu_i a_i \leq z\}.$$

Then, one can show the following two results (for a detailed proof, see Tenenbaum [**140**]).

**Theorem 9.12.** *For $k \geq 1$, $z \geq 0$,*

$$\frac{z^k}{k!} \prod_{i=1}^{k} \frac{1}{a_i} < N_k(z) \leq \frac{(z + \sum_{i=1}^{k} a_i)^k}{k!} \prod_{i=1}^{k} \frac{1}{a_i}.$$

**Corollary 9.13.** *(Ennola [**45**], 1969). Uniformly for $2 \leq y \leq \sqrt{\log x}$,*

$$\Psi(x, y) = \frac{1}{\pi(y)!} \prod_{p \leq y} \left(\frac{\log x}{\log p}\right) \left\{1 + O\left(\frac{y^2}{\log x \cdot \log y}\right)\right\}. \tag{9.40}$$

**Proof.** We use Theorem 9.12 by setting $k = \pi(y)$, $z = \log x$, $a_i = \log p_i$, so that $N_k(z) = \Psi(x, y)$ and $\sum_{i=1}^{k} a_i = \theta(y) \ll y$. □

## 9.7. The best known estimates on $\Psi(x,y)$

**Theorem 9.14.** *Uniformly for $x \geq y \geq 2$,*

$$\Psi(x,y) = x\rho(u) + O\left(\frac{x}{\log y}\right). \tag{9.41}$$

**Sketch of proof.** We need to prove (9.41) for $u \leq \log\log y$. Indeed, assuming the contrary, the error term $O(\frac{x}{\log y})$ is larger than that of $x\rho(u)$, in which case estimate (9.41) follows trivially from Theorem 9.5. Now we prove (9.41) by induction on $k = [u] \leq \log\log y$. We first consider the case $1 \leq u \leq 2$. We use the Buchstab identity with $z = x$, in which case we have

$$\Psi(x,y) = \lfloor x \rfloor - \sum_{y<p\leq x} \left\lfloor \frac{x}{p} \right\rfloor = x(1-\log u) + O(\pi(x)) = x\rho(u) + O\left(\frac{x}{\log x}\right).$$

Since $y \leq x$, the result follows. The proof is then easily completed using an induction argument. □

**Theorem 9.15.** *(Hildebrand, [**82**]) Let $\varepsilon > 0$. Then*

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

*uniformly for $x \geq 3$, $\exp\{(\log\log x)^{\frac{5}{3}+\varepsilon}\} \leq y \leq x$.*

Hildebrand's result also asserts that for every fixed $\varepsilon > 0$,

$$\Psi(x,y) = x\rho(u)\left(1 + O\left(\frac{1}{\log(2x)}\right)\right)$$

holds uniformly in the region $\exp((\log\log x)^{5/3+\varepsilon}) < y \leq x$. The same estimate in a somewhat smaller range was proved a few years before by Canfield, Erdős, and Pomerance in [**20**]. A weaker result which is valid uniformly in the range $2 \leq y \leq x$ was obtained by de Bruijn [**16**] and later improved by Tenenbaum (see Theorem III.5.2 in [**140**] or the survey paper by Hildebrand and Tenenbaum [**84**]), which asserts that

$$\log\Psi(x,y) = Z\left(1 + O\left(\frac{1}{\log y} + \frac{1}{\log\log x}\right)\right), \tag{9.42}$$

where

$$Z = \frac{\log x}{\log y}\log\left(1 + \frac{y}{\log x}\right) + \frac{y}{\log y}\log\left(1 + \frac{\log x}{y}\right). \tag{9.43}$$

This result is remarkable for two reasons: first of all, relation (9.42) holds in the whole range $2 \leq y \leq x$; secondly, the proof is completely elementary, since its upper bound can be obtained from the Rankin method (see Section

9.4) while the lower bound rests on the simple inequality $\Psi(x,y) \geq \binom{k+\ell}{\ell}$, where $\ell = \min\{n \in \mathbb{N} : n \geq \log x/\log y\}$ and $k = \pi(x^{1/\ell})$.

Before stating the next result, we need to introduce the following notations.

$$\zeta(s,y) = \prod_{p \leq y} \left(1 - \frac{1}{p^s}\right)^{-1}, \qquad \phi_y(\sigma) = -\frac{\zeta'(\sigma,y)}{\zeta(\sigma,y)} = \sum_{p \leq y} \frac{\log p}{p^\sigma - 1}.$$

Let $\alpha = \alpha(x,y)$ be the unique solution to the equation

$$\phi_y(\alpha) = \log x.$$

One can show that

$$\alpha(x,y) = \beta(x,y)\left(1 + O\left(\frac{\log\log y}{\log y}\right)\right) \qquad (x \geq y \geq 2),$$

where $\beta = \beta(x,y)$ is the solution of $\dfrac{y}{y^\beta - 1} = \log x$, so that

$$\beta(x,y) = \frac{\log(1 + y/\log x)}{\log y}.$$

**Theorem 9.16.** *(Hildebrand-Tenenbaum* [**83**]*, 1986) Uniformly for $x \geq y \geq 2$,*

$$\Psi(x,y) = \frac{x^\alpha \zeta(\alpha,y)}{\alpha\sqrt{2\pi\phi_y'(\alpha)}}\left(1 + O\left(\frac{1}{u} + \frac{\log y}{y}\right)\right),$$

*where*

$$\phi_y'(\alpha) = \left(1 + \frac{\log x}{y}\right)\log x \log y\left(1 + O\left(\frac{1}{\log(u+1)} + \frac{1}{\log y}\right)\right).$$

## 9.8. The Dickman function

In Section 9.3, we introduced the Dickman function and easily established its basic properties. However, exploring its asymptotic behavior is not an easy task. We describe here (without proof) a result due to de Bruijn [**15**] and later improved by Alladi [**2**].

First, some notations.

- Define $\xi = \xi(u)$ as the unique real number satisfying the equation

$$e^\xi = 1 + u\xi \quad \text{for } u > 0, u \neq 1 \text{ and } \xi(1) = 0.$$

- For each $s \geq 0$, set

$$I(s) = \int_0^s \frac{e^t - 1}{t}\, dt.$$

**Theorem 9.17.** *For $u \geq 1$, we have*

$$\rho(u) = \left(1 + O\left(\frac{1}{u}\right)\right) \sqrt{\frac{\xi'(u)}{2\pi}} \exp\{\gamma - u\xi + I(\xi)\}.$$

Using the fact that

$$\xi'(u) \sim \frac{1}{u} \tag{9.44}$$

(see Problem 9.31) as well as the identity

$$u\xi(u) - I(\xi(u)) = \int_1^u \xi(t)\, dt \tag{9.45}$$

(see Problem 9.32), the following result is then a consequence of Theorem 9.17.

**Corollary 9.18.** *As $u \to \infty$,*

$$\rho(u) = \exp\left\{-u\left(\log u + \log\log u - 1 + O\left(\frac{\log\log u}{\log u}\right)\right)\right\}.$$

**Proof.** Using Theorem 9.17 as well as (9.44), (9.45), and Problem 9.28, we obtain that, if $u_0 \geq 2$ is fixed, then, as $u \to \infty$,

$$\begin{aligned} \exp\{-u\xi(u) + I(\xi(u))\} &= \exp\left\{-\int_1^u \xi(t)\, dt\right\} \\ &= \exp\left\{O(1) - \int_{u_0}^u \left(\log t + \log\log t + O\left(\frac{\log\log t}{\log t}\right)\right) dt\right\} \\ &= \exp\left\{-\left(u\log u - u + u\log\log u + O\left(u\frac{\log\log u}{\log u}\right)\right)\right\}. \end{aligned} \tag{9.46}$$

Now, in light of (9.44), it is clear that

$$\xi'(u) \sim \frac{1}{u} = e^{-\log u} = e^{-u\frac{\log u}{u}} = e^{-uO\left(\frac{\log\log u}{\log u}\right)}.$$

Combining this with (9.46), the result follows. □

## 9.9. Consecutive smooth numbers

The next result is due to A. Balog and T. Wooley [**7**].

**Proposition 9.19.** *Let $\varepsilon > 0$ and $k \geq 2$ be fixed. Then there exist infinitely many positive integers $n$ such that*

$$P((n+1)\cdots(n+k)) < n^{\varepsilon}.$$

**Proof.** Again we sketch only the ideas. We let $\mathcal{Q}_1, \ldots, \mathcal{Q}_k$ be disjoint sets of odd primes exceeding $k$ such that

$$\prod_{p \in \mathcal{Q}_i} \left(1 - \frac{1}{p}\right) < \varepsilon/2 \qquad (i = 1, \ldots, k).$$

It is clear that we can choose such sets because

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \to 0 \qquad \text{as} \qquad x \to \infty.$$

For each $i = 1, \ldots, k$, let $Q_i = \prod_{q \in \mathcal{Q}_i} q$. Note that the $Q_i$'s are mutually coprime for $i = 1, \ldots, k$. Let $p_1 < p_2 < \cdots < p_s \leq k$ be all the $s = \pi(k)$ primes $p \leq k$. Write

$$i = \prod_{j=1}^{s} p_j^{\ell_j(i)} \qquad (i = 1, \ldots, k),$$

for some nonnegative integers $\ell_j(i)$. Construct $L_j$ for $j = 1, \ldots, s$ in such a way that

$$L_j \equiv \ell_j(i) \pmod{Q_i} \qquad \text{for all } i = 1, \ldots, k. \tag{9.47}$$

This is possible by the Chinese Remainder Theorem. Let

$$n = \prod_{j=1}^{s} p_j^{L_j}.$$

Then

$$n + i = i \left( \prod_{j=1}^{s} p_j^{L_j - \ell_j(i)} + 1 \right) = i \left( u_i^{Q_i} + 1 \right),$$

where

$$u_i = \prod_{j=1}^{s} p_j^{(L_j - \ell_j(i))/Q_i}$$

is an integer because of the way we chose the exponents $L_1, \ldots, L_k$ (see congruences (9.47)). Since $Q_i$ is odd, we easily get that if we put $X = -u_i$, then

$$u_i^{Q_i} + 1 = -(X^{Q_i} - 1) = -\prod_{d \mid Q_i} \Phi_d(X),$$

where

$$\Phi_n(Y) = \prod_{\substack{1\le k\le n\\(k,n)=1}} (Y - e^{2\pi ik/n}) \in \mathbb{Z}[Y]$$

is the $n$-th cyclotomic polynomial. This polynomial has as its roots all the primitive roots of unity of order $n$ and its degree is $\phi(n)$, the Euler function of $n$. The fact that it has integer coefficients follows easily by induction from the formula

$$Y^n - 1 = \prod_{d\,|\,n} \Phi_d(Y).$$

Thus, $u_i^{Q_i} + 1$ splits into a product of factors, each one of size at most

$$\begin{aligned}\max_{d\,|\,Q_i}\{|\Phi_d(X)|\} &\le \max_{d\,|\,Q_i}\{||X|+1|^{\phi(d)}\} \le (u_i+1)^{\phi(Q_i)}\\ &= u_i^{\phi(Q_i)}\left(1+\frac{1}{u_i}\right)^{\phi(Q_i)} \ll u_i^{\phi(Q_i)}\\ &\ll n^{\phi(Q_i)/Q_i} \ll n^{\varepsilon/2},\end{aligned}$$

where the constants implied in the above symbols depend at most on $k$ and the numbers $Q_i$ for $i = 1, \dots, k$. Choosing $L_j$ to be sufficiently large in the arithmetical progression (9.47), we get the desired conclusion. □

**Remark 9.20.** *While the above theorem shows that there are arbitrarily long strings of consecutive smooth numbers, two consecutive numbers cannot both be too smooth. Indeed, there is a deep theorem in diophantine analysis which asserts that if $f(x) \in \mathbb{Z}\lfloor x\rfloor$ is a polynomial with at least two distinct roots, then $P(f(n)) \gg \log\log n$ if $n > n_0$, where the constant implied by the above symbol depends on the polynomial $f$. (See, for example, the nice book by Shorey and Tijdeman* [**130**]*.) With $f(x) = (x+1)(x+2)$, we get that*

$$P((n+1)\cdots(n+k)) \ge P((n+1)(n+2)) \gg \log\log n.$$

*We will see this later in Problem* 13.15.

## Problems on Chapter 9

**Problem 9.1.** *Find the value of the constant $C$ in the following formula:*

$$\lim_{x\to\infty} \frac{1}{x}\#\{n \le x : p(n) \le 5\} = C.$$

**Problem 9.2.** *Are the functions $f(n)$ and $g(n)$ defined in* (9.2) *and* (9.3) *multiplicative ?*

**Problem 9.3.** *What about the convergence or divergence of each of the following products ?*

$$\prod_{p\geq 17}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right),\quad \prod_{p<101}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right),\quad \prod_{p\geq 101}\left(1-\frac{1}{p}\right)^{-1}.$$

**Problem 9.4.** *Evaluate the following two sums:*

$$\sum_{n\leq x}\frac{1}{p(n)^2},\qquad \sum_{n\leq x} f(n),$$

*where $f(n)$ is defined by*

$$f(n)=\begin{cases}1 & \text{if } p(n)\leq 3,\\ \sqrt{\log p(n)} & \text{if } p(n)\geq 5.\end{cases}$$

**Problem 9.5.** *Prove that*

$$\sum_{n\leq x} p(n(n+1))=2\lfloor x\rfloor.$$

**Problem 9.6.** *Prove that*

$$\sum_{2\leq n\leq x}\frac{1}{p(n)}=Cx+O\left(\frac{x}{(\log\log x)^2}\right),\quad \text{where } C=\sum_p\frac{1}{p(p-1)}\prod_{q<p}\left(1-\frac{1}{q}\right).$$

**Problem 9.7.** *Compute the value of the constant $C$ appearing in Problem* 9.6 *with a precision of four decimals.*

**Problem 9.8.** *Prove that*

$$1+\sum_{\substack{p^k\leq x\\ k\geq 1}}\Phi(x/p^k,p)=\lfloor x\rfloor.$$

**Problem 9.9.** *Let $y\geq 2$ be fixed. Is it true that*

$$\Phi(2x,y)\sim 2\Phi(x,y)\qquad (x\to\infty)?$$

**Problem 9.10.** *Prove the Buchstab identity*

$$\Psi(x,y)=\Psi(x,z)-\sum_{y<p\leq z}\Psi\left(\frac{x}{p},p\right)\qquad (x\geq 1,\ z\geq y>0).$$

*(Hint: Use the fact that*

$$\Psi(x,z)=\sum_{p\leq z}\sum_{\substack{pm\leq x\\ P(m)\leq p}}1=\sum_{p\leq z}\Psi\left(\frac{x}{p},p\right)$$

*for all $2\leq z\leq x$.)*

**Problem 9.11.** *Show that*

$$\Psi(x,y) \le \left(1+\frac{\log x}{\log 2}\right)^{\pi(y)}.$$

*(Hint: If $n$ is counted by $\Psi(x,y)$, then $n = p_1^{a_1}\cdots p_k^{a_k}$, where $k=\pi(y)$, $2 = p_1 < p_2 < \cdots$ is the increasing sequence of primes and $a_i$ are nonnegative integers. Now count the number of possible values of the exponents.)*

**Problem 9.12.** *Is the series* $\displaystyle\sum_{m=2}^{\infty} \frac{1}{m\log^2 P(m)}$ *convergent?*

**Problem 9.13.** *Evaluate the expression*

$$\sum_{2\le n\le x} \sqrt{P(n)}.$$

**Problem 9.14.** *Use Theorem* 9.5 *in order to prove that if $y < A$ for a fixed $A$, then*

$$\Psi(x,y) \ll x^{1-\eta},$$

*for some real number $\eta > 0$.*

**Problem 9.15.** *Use Theorem* 9.5 *in order to prove that if $y \le e^{\sqrt{\log x}}$, then*

$$\Psi(x,y) \ll \frac{x}{e^{\frac{1}{2}\sqrt{\log x}}}.$$

**Problem 9.16.** *Let $\mathcal{P}^{(2)}$ be the set of base* 2 *pseudoprimes. Using the construction of pseudoprimes from Problem* 2.9*, show that the series*

$$\sum_{n\in\mathcal{P}^{(2)}} \frac{1}{\log n}$$

*is divergent.*

**Problem 9.17.** *Show that the inequality $P(n) < P(n+1) < P(n+2)$ holds for infinitely many positive integers $n$.*

**Problem 9.18.** *Prove that there are infinitely many positive integers $n$ such that $2^{\sigma(n)} \equiv 1 \pmod{n}$. (Hint: Start with $n = 3$ and build up larger $n$'s by multiplying it with appropriate primes.)*

**Problem 9.19.** *Show that the sum of the reciprocals of the numbers appearing in Problem* 9.18 *is convergent.*

**Problem 9.20.** *Let $F_n$ be the $n$-th Fermat number. Let $\mathcal{P}$ be the set of all primes that divide $F_n$ for some positive integer $n$. Show that the series*

$$\sum_{p\in\mathcal{P}} \frac{1}{p}$$

*is convergent. (Hint: Show that* $\omega(F_n) \le 2^n$ *and that each prime factor of* $F_n$ *is congruent to* 1 *modulo* $2^{n+1}$*. Use this information to get a reasonably small bound on* $\sum_{p \mid F_n} 1/p$*.)*

**Problem 9.21.** *Prove that* $P(F_n) \gg n2^n$*.*

**Problem 9.22.** *Use de Bruijn's estimates* (9.42) *and* (9.43) *to show that if* $A = \{n : P(n) < \log n\}$*, then* $\#(A \cap [1, x]) = x^{o(1)}$ *as* $x \to \infty$*.*

**Problem 9.23.** *Let* $y$ *be a large but fixed number. Set* $r = \pi(y)$*. Using Ennola's result (Corollary* 9.13*), show that, for large values of* $r$*, the function* $\Psi(x, y)$ *is larger than* $\dfrac{1}{r!}u^r$*.*

**Problem 9.24.** *Use Theorem* 9.5 *in order to prove that*

$$\sum_{\substack{n>x \\ P(n)\le y}} \frac{1}{n} \ll e^{-\frac{1}{2}u} \log y.$$

**Problem 9.25.** *Use Theorem* 9.14 *in order to prove that*

$$\sum_{\substack{n\le x \\ P(n)\le y}} \frac{1}{n} = \log y \int_0^u \rho(v)\, dv + O(u).$$

**Problem 9.26.** *Combine the results of Problems* 9.24 *and* 9.25 *to prove that*

$$\int_0^u \rho(v)\, dv = e^\gamma + O\left(\frac{u}{\log y} + e^{-\frac{1}{2}u}\right).$$

*(Hint: Use Mertens' theorem.)*

**Problem 9.27.** *By a clever choice of* $y = y(x)$*, prove, using Problem* 9.26*, that*

$$\int_0^\infty \rho(v)\, dv = e^\gamma.$$

*Also prove, using Theorem* 9.4*, that*

$$\sum_{n=1}^{\infty} n\rho(n) = e^\gamma.$$

**Problem 9.28.** *Let* $\xi = \xi(u)$ *be the function defined in Section 8. By first establishing that*

$$1 \ll \xi(u) \ll \log u,$$

*prove that for* $u \ge 3$*,*

$$\xi(u) = \log(u \log u) + O\left(\frac{\log\log u}{\log u}\right).$$

**Problem 9.29.** *Prove that* $I(\xi(u)) \sim u$ *as* $u \to \infty$*.*

**Problem 9.30.** *Prove that*

$$\xi'(u) = \frac{\xi(u)}{1 + u(\xi(u) - 1)}.$$

**Problem 9.31.** *Use Problem* 9.30 *to prove that*

$$\xi'(u) \sim \frac{1}{u} \qquad (u \to \infty).$$

**Problem 9.32.** *Prove the identity*

$$u\xi(u) - I(\xi(u)) = \int_1^u \xi(t)\, dt.$$

**Problem 9.33.** *Use Theorem* 9.14 *to prove that*

$$\sum_{n \le x} \log P(n) = Cx \log x + O(x \log\log x),$$

*where* $C = 1 - \displaystyle\int_1^\infty \frac{\rho(v)}{v^2}\, dv \approx 0.62433.$

**Problem 9.34.** *Let* $A = \{a_k\}_{k \ge 1}$ *be the sequence of positive integers defined by* $a_k = 4k^4$, $k = 1, 2, 3, \ldots$

(i) *Show that* $A$ *contains a subsequence* $B$ *such that*

$$\max\left(P(n-1), P(n), P(n+1)\right) < \sqrt{n} \qquad \text{for all } n \in B.$$

(ii) *Show that there exists a positive constant* $C$ *such that*

$$\#\{n \le x : n \in B\} > Cx^{1/4}.$$

*(Hint: Observe that the identities*

$4k^4 - 1 = (2k^2+1)(2k^2-1)$ *and* $4k^4+1 = (2k^2+2k+1)(2k^2-2k+1)$

*are true for all positive integers* $k$. *Observe also that*

$$\begin{aligned} 2k^2 + 1 &\equiv 0 \pmod 3 \quad \text{if} \quad k \equiv 1 \pmod 3, \\ 2k^2 - 1 &\equiv 0 \pmod 7 \quad \text{if} \quad k \equiv 2 \pmod 7, \\ 2k^2 + 2k + 1 &\equiv 0 \pmod 5 \quad \text{if} \quad k \equiv 1 \pmod 5, \\ 2k^2 - 2k + 1 &\equiv 0 \pmod{13} \quad \text{if} \quad k \equiv 3 \pmod{13}. \end{aligned}$$

*Use these relations to obtain upper bounds for* $P(4k^4 - 1)$, $P(4k^4)$ *and* $P(4k^4 + 1)$, *respectively.)*

**Problem 9.35.** *Show that the set of integers* $A = \{6^6 k^{12} : k = 2, 3, \ldots\}$ *has the interesting property that*

$$\max(P(n-1), P(n), P(n+1)) < 2n^{1/3} \qquad \text{for all } n \in A.$$

*(Hint: Observe that, for each* $k \in \mathbb{N}$,

$6^6 k^{12} + 1 \;=\; (36k^4 + 1)(36k^4 + 36k^3 + 18k^2 + 6k + 1)(36k^4 - 36k^3 + 18k^2 - 6k + 1)$

$$6^6k^{12}-1 \;=\; (6k^2+1)(36k^4-6k^2+1)(6k^2-1)(36k^4+6k^2+1)$$

*and then set* $n=6^6k^{12}$.*)*

**Problem 9.36.** *Let* $p_i$ *stand for the* $i$*-th prime. For each integer* $k\ge 2$*, consider the polynomials* $P_k(x)=x^{p_2p_3\cdots p_k}-1$ *and* $Q_k(x)=x^{p_2p_3\cdots p_k}+1$ *to establish that, given any small number* $\varepsilon>0$*, there exists a positive integer* $n$ *such that*

$$\max(P(n-1),P(n),P(n+1))<n^{\varepsilon}.$$

*(Hint: Show that* $P_k(x)$ *(as well as* $Q_k(x)$*) can be written as a product of polynomials each of degree at most* $(p_2-1)(p_3-1)\cdots(p_k-1)$*, from which it will follow that the largest prime factor of* $2^{3\cdot 5\cdots p_k}-1$ *(and similarly of* $2^{3\cdot 5\cdots p_k}+1$*) is* $\ll 2^{(3-1)(5-1)\cdots(p_k-1)}$*, implying that choosing* $k$ *large enough so that*

$$\frac{(p_2-1)(p_3-1)\cdots(p_k-1)}{p_2p_3\cdots p_k}<\varepsilon,$$

*that is,*

$$\prod_{2\le i\le k}\left(1-\frac{1}{p_i}\right)<\varepsilon,$$

*the proof will be complete.)*

*Chapter 10*

# The Hardy-Ramanujan and Landau Theorems

## 10.1. The Hardy-Ramanujan inequality

In this section, we study the function

$$\Pi_k(x) = \#\{n \le x : \omega(n) = k\},$$

where $k > 0$ is either fixed or depends on $x$, and we prove the Hardy-Ramanujan inequality, which can be stated as follows.

**Theorem 10.1.** *There exist positive constants $x_0$, $c_0$, and $c_1$ such that uniformly for $1 \le k \le 10 \log\log x$,*

$$\Pi_k(x) \le c_0 \frac{x}{\log x} \frac{1}{(k-1)!} (\log\log x + c_1)^{k-1} \tag{10.1}$$

*for all $x > x_0$.*

**Proof.** We follow a method similar to the one used in the proof of Lemma 9.6. We may assume that $k \ge 2$, because for $k = 1$ the inequality follows from Chebyshev's estimate. Using the fact that

$$\frac{(\log\log x + c_1)^{k-1}}{(k-1)!} > \left(\frac{2\log\log x}{10\log\log x}\right)^{10\log\log x} = \frac{1}{(\log x)^A},$$

for $x > e^{e^{c_1}}$, where $A = 10\log 5$ (because $c_1 > 0$ and $(k-1)! < (k-1)^{k-1}$), it follows that if $\Pi_k(x) < 3x/(\log x)^{A+1}$, then there is nothing to prove (simply

take $c_0 > 3$). Hence, we shall assume that $\Pi_k(x) \geq \dfrac{3x}{(\log x)^{A+1}}$. Now

$$\begin{aligned}\Pi_k(x)\log x &= \sum_{\substack{n\leq x\\ \omega(n)=k}} \log x = \sum_{\substack{n\leq x\\ \omega(n)=k}} \log(x/n) + \sum_{\substack{n\leq x\\ \omega(n)=k}} \log n \\ &= \sum_{\substack{n\leq x\\ \omega(n)=k}} \log(x/n) + \sum_{\substack{n\leq x\\ \omega(n)=k}} \sum_{p^a \| n} \log(p^a) \\ &= S_1 + S_2,\end{aligned} \tag{10.2}$$

say. To compute $S_1$, we split it at $y = x/(\log x)^{A+1}$ and get $S_1 = S_1' + S_1''$, say. First

$$S_1' = \sum_{\substack{n<y\\ \omega(n)=k}} \log(x/n) \leq \sum_{n<y} \log x < y \log x = \frac{x}{(\log x)^A}.$$

If $y \leq n \leq x$, then $x/n \leq x/y = (\log x)^{A+1}$, so that $\log(x/n) \leq (A+1)\log\log x$, which implies that

$$S_1'' = \sum_{\substack{y\leq n\leq x\\ \omega(n)=k}} \log(x/n) \leq (A+1)\log\log x \sum_{\substack{n\leq x\\ \omega(n)=k}} 1 = (A+1)(\log\log x)\Pi_k(x).$$

Thus,

$$S_1 = S_1' + S_1'' \leq \frac{x}{(\log x)^A} + (A+1)(\log\log x)\Pi_k(x). \tag{10.3}$$

For $S_2$, we write $n = p^a m$, where $\omega(m) = k-1$, and we change the order of summation, thus obtaining

$$\begin{aligned}S_2 &= \sum_{\substack{n\leq x\\ \omega(n)=k}} \sum_{p^a \,\|\, n} \log(p^a) \\ &= \sum_{\substack{m\leq x\\ \omega(m)=k-1}} \sum_{p^a \leq x/m} \log(p^a) \\ &\ll \sum_{\substack{m\leq x\\ \omega(m)=k-1}} \frac{x}{m} = x \sum_{\substack{m\leq x\\ \omega(m)=k-1}} \frac{1}{m}.\end{aligned} \tag{10.4}$$

But by unique factorization, the multinomial formula and Mertens' formula, we immediately obtain that

$$\sum_{\substack{m\leq x\\ \omega(m)=k-1}} \frac{1}{m} \leq \frac{1}{(k-1)!}\left(\sum_{p^a\leq x} \frac{1}{p^a}\right)^{k-1} \leq \frac{1}{(k-1)!}(\log\log x + c_1)^{k-1}. \tag{10.5}$$

Combining (10.3), (10.4), and (10.5), we obtain from (10.2) that

$$\Pi_k(x)\log x \le \frac{x}{(\log x)^A}+(A+1)\Pi_k(x)\log\log x+c_0x\frac{1}{(k-1)!}(\log\log x+c_1)^{k-1},$$

where $c_0$ is the constant implicit in (10.4). Since $\Pi_k(x) \ge 3x/(\log x)^{A+1}$, we get that $x/(\log x)^A \le (1/3)\Pi_k(x)\log x$ for $x > e$. We also have that $(A+1)\log\log x < (\log x)/3$ for $x > x_0$ sufficiently large. Hence,

$$\Pi_k(x)\log x < \frac{2}{3}\Pi_k(x)\log x + c_0x\frac{1}{(k-1)!}(\log\log x + c_1)^{k-1},$$

which implies that

$$\Pi_k(x) \le 3c_0\frac{x}{\log x}\,\frac{1}{(k-1)!}\,(\log\log x + c_1)^{k-1},$$

which is precisely what we wanted to prove. □

**Remark 10.2.** *In fact, Hardy and Ramanujan* [**77**] *proved that inequality* (10.1) *holds uniformly for all possible $k$ (that is, without the restriction that $k \le 10\log\log x$). Their proof is by induction on the value of $k$. We limited ourselves to the range $k \le 10\log\log x$ because this suffices for most interesting applications.*

## 10.2. Landau's theorem

In 1900, 17 years before Hardy and Ramanujan proved Theorem 10.1, Landau had already proved the next theorem.

But first, some notations. For a fixed positive integer $k$ and a positive real number $x$, let $\tau_k(x) = \{n \le x : \Omega(n) = k\}$ and $\pi_k(x) = \{n \le x : \omega(n) = \Omega(n) = k\}$.

**Theorem 10.3.** *Let $k$ be a fixed positive integer. Then*

$$\tau_k(x) \sim \pi_k(x) \sim \frac{1}{(k-1)!}\frac{x}{\log x}(\log\log x)^{k-1} \qquad (x\to\infty).$$

**Proof.** We introduce the following functions:

$$L_k(x) = \sum_{p_1\cdots p_k\le x}{}^{*}\ \frac{1}{p_1\cdots p_k},$$

$$P_k(x) = \sum_{p_1\cdots p_k\le x}{}^{*}\ 1$$

and

$$\Theta_k(x) = \sum_{p_1\cdots p_k\le x}{}^{*}\ \log(p_1\cdots p_k),$$

where $^*$ means that the sum is taken over all $k$-tuples of primes $(p_1, \dots, p_k)$ with $p_1 \cdots p_k \le x$. Note that different $k$-tuples may correspond to the same product $p_1 \cdots p_k$.

For each positive integer $n$, let $c_n = c_n^{(k)}$ be the number of $k$-tuples $(p_1, \dots, p_k)$ for which $p_1 \cdots p_k = n$. Note that $c_n = 0$ if $n$ is not the product of $k$ primes, while $c_n = k!$ if $n$ is squarefree and $\omega(n) = k$. Thus, we have

$$k!\pi_k(x) \le P_k(x) \le k!\tau_k(x). \tag{10.6}$$

Note also that $P_k(x) = \sum_{n \le x} c_n$ and $\Theta_k(x) = \sum_{n \le x} c_n \log n$.

For $k \ge 2$, note that the number of positive integers up to $x$ which are products of $k$ prime factors and are divisible by the square of a prime is $\tau_k(x) - \pi_k(x)$. Hence,

(10.7)

$$\tau_k(x) - \pi_k(x) \le \sum_{\substack{p_1 \cdots p_k \le x \\ p_i = p_j \text{ for some } i \ne j}} 1 \le \binom{k}{2} \sum_{p_1 \cdots p_{k-1} \le x} 1 = \binom{k}{2} P_{k-1}(x).$$

We shall prove that

$$P_k(x) \sim k \frac{x(\log\log x)^{k-1}}{\log x} \qquad (x \to \infty), \tag{10.8}$$

after which, in light of (10.6) and (10.7), the proof of the theorem will be complete.

Note that for $k \ge 1$,

$$L_k(x) \sim (\log\log x)^k \qquad (x \to \infty),$$

since

$$\left( \sum_{p \le x^{1/k}} \frac{1}{p} \right)^k \le L_k(x) \le \left( \sum_{p \le x} \frac{1}{p} \right)^k,$$

and since by Mertens' estimate (Theorem 4.5), as $x \to \infty$,

$$\begin{aligned} \left( \sum_{p \le x^{1/k}} \frac{1}{p} \right)^k &\sim \left( \log\log(x^{1/k}) \right)^k = \left( \log \left( \frac{\log x}{k} \right) \right)^k \\ &= (\log\log x - \log k)^k \sim (\log\log x)^k, \end{aligned}$$

while

$$\left( \sum_{p \le x} \frac{1}{p} \right)^k \sim (\log\log x)^k.$$

From Abel's summation formula with $a_n = c_n$ and $f(t) = \log t$, we get

$$\Theta_k(x) = \sum_{n \le x} c_n \log n = P_k(x) \log x - \int_1^x \frac{P_k(t)}{t} dt.$$

From (10.6), we have

$$P_k(x) \le k! \tau_k(x) \le k! x,$$

implying that $P_k(t) = O(t)$, so that $\Theta_k(x) = P_k(x) \log x + O(x)$.

Thus, instead of proving (10.8), it is clear that we need to prove only that

$$\Theta_k(x) \sim kx(\log\log x)^{k-1} \qquad \text{for } k \in \mathbb{N}. \tag{10.9}$$

We will prove this by induction on $k$.

For $k = 1$, it holds by the Prime Number Theorem. Now assume that (10.9) holds for some positive integer $k$. We will show that it holds for $k+1$. Since $L_k(x) \sim (\log\log x)^k$, we have that

$$\Theta_{k+1}(x) - (k+1)x(\log\log x)^k = \Theta_{k+1}(x) - (k+1)xL_k(x) + o(x(\log\log x)^k),$$

and

$$\begin{aligned} k\Theta_{k+1}(x) &= \sum\nolimits^*_{p_1 \cdots p_{k+1} \le x} (\log(p_2 \cdots p_{k+1}) \\ &\qquad + \log(p_1 p_3 \cdots p_{k+1}) + \cdots + \log(p_1 \cdots p_k)) \\ &= (k+1) \sum\nolimits^*_{p_2 \cdots p_{k+1} \le x/p_1} \log(p_2 \cdots p_{k+1}) \\ &= (k+1) \sum_{p_1 \le x} \Theta_k(x/p_1). \end{aligned}$$

Next, put $L_0(x) = 1$ and observe that

$$L_k(x) = \sum_{p_1 \cdots p_k \le x}{}^* \frac{1}{p_1 \cdots p_k} = \sum_{p_1 \le x} \frac{1}{p_1} L_{k-1}\left(\frac{x}{p_1}\right).$$

Thus,

$$k(\Theta_{k+1}(x) - (k+1)xL_k(x)) = (k+1) \sum_{p_1 \le x} \left(\Theta_k\left(\frac{x}{p_1}\right) - \frac{kx}{p_1} L_{k-1}\left(\frac{x}{p_1}\right)\right).$$

By the induction hypothesis,

$$\Theta_k(y) - kyL_{k-1}(y) = o(y(\log\log y)^{k-1}) \qquad \text{as } y \to \infty.$$

Thus, given $\varepsilon > 0$, there exists $x_0 = x_0(\varepsilon, k)$ such that for $y > x_0$,

$$\left|\Theta_k(y) - kyL_{k-1}(y)\right| \le \varepsilon y(\log\log y)^{k-1}.$$

Moreover, there exists a positive real number $c = c(\varepsilon, k)$ such that for all $y \le x_0$,

$$\Big|\Theta_k(y) - kyL_{k-1}(y)\Big| \le c.$$

Thus, for $x$ sufficiently large,

$$\begin{aligned}
&|\Theta_{k+1}(x) - (k+1)xL_k(x)| \\
&\quad \le \left(1+\frac{1}{k}\right)\left(\sum_{x/x_0<p_1\le x} c + \sum_{p_1\le x/x_0} \varepsilon\frac{x}{p_1}\left(\log\log\left(\frac{x}{p_1}\right)\right)^{k-1}\right) \\
&\quad \le 2\left(cx + \varepsilon x(\log\log x)^{k-1}\sum_{p_1\le x/x_0}\frac{1}{p_1}\right) \\
&\quad \le 2cx + 4\varepsilon x(\log\log x)^k < 5\varepsilon x(\log\log x)^k.
\end{aligned}$$

From this last inequality, it follows that

$$\Theta_{k+1}(x) - (k+1)xL_k(x) = o(x(\log\log x)^k) \qquad \text{as } x\to\infty,$$

thus completing the induction and therefore the proof of (10.9). □

Using powerful analytic tools, very precise estimates have been established for $\Pi_k(x)$ and $\tau_k(x)$. The following three theorems along with their proofs can be found in Tenenbaum's recent book [**141**].

**Theorem 10.4.** *Let $A > 0$. There exist positive constants $c_1 = c_1(A)$ and $c_2 = c_2(A)$ such that uniformly for $x \ge 3$, $1 \le k \le A\log\log x$, $N \ge 0$,*

$$\Pi_k(x) = \frac{x}{\log x}\left\{\sum_{0\le j\le N}\frac{P_{j,k}(\log\log x)}{\log^j x} + O\left(\frac{(\log\log x)^k}{k!}R_N(x)\right)\right\},$$

*where $P_{j,k}(X)$ is a polynomial of degree at most $k-1$ and where*

$$R_N(x) := e^{-c_1\sqrt{\log x}} + \left(\frac{c_2N+1}{\log x}\right)^{N+1}. \tag{10.10}$$

*In particular,*

$$P_{0,k}(X) = \sum_{m+\ell=k-1}\frac{1}{m!\ell!}\lambda^{(m)}(0)X^\ell,$$

*where*

$$\lambda(z) := \frac{1}{\Gamma(z+1)}\prod_p\left(1+\frac{z}{p-1}\right)\left(1-\frac{1}{p}\right)^z.$$

*Moreover, under the same conditions,*

$$\Pi_k(x) = \frac{x}{\log x}\frac{(\log\log x)^{k-1}}{(k-1)!}\left\{\lambda\left(\frac{k-1}{\log\log x}\right) + O\left(\frac{k}{(\log\log x)^2}\right)\right\}.$$

A similar result holds for $\tau_k(x)$ but with a smaller range for $k$, as is shown by the following theorem.

**Theorem 10.5.** *Let $0 < \delta < 1$. There exist positive constants $c_1 = c_1(\delta)$ and $c_2 = c_2(\delta)$ such that uniformly for $x \geq 3$, $1 \leq k \leq (2-\delta)\log\log x$, $N \geq 0$,*

$$\tau_k(x) = \frac{x}{\log x}\left\{\sum_{0\leq j\leq N}\frac{Q_{j,k}(\log\log x)}{\log^j x} + O\left(\frac{(\log\log x)^k}{k!}R_N(x)\right)\right\},$$

*where $Q_{j,k}(X)$ is a polynomial of degree at most $k-1$ and where $R_N(x)$ is defined as in (10.10). In particular,*

$$Q_{0,k}(X) = \sum_{m+\ell=k-1}\frac{1}{m!\ell!}\nu^{(m)}(0)X^\ell,$$

*where*

$$\nu(z) := \frac{1}{\Gamma(z+1)}\prod_p\left(1-\frac{z}{p}\right)^{-1}\left(1-\frac{1}{p}\right)^z.$$

*Moreover, under the same conditions,*

$$\tau_k(x) = \frac{x}{\log x}\frac{(\log\log x)^{k-1}}{(k-1)!}\left\{\nu\left(\frac{k-1}{\log\log x}\right) + O\left(\frac{k}{(\log\log x)^2}\right)\right\}.$$

Theorems 10.4 and 10.5 were proved by Selberg [**127**] in 1954 in the case $N = 0$. For each fixed integer $N \geq 0$, they are particular cases of results established by Delange [**38**] in 1971.

The next theorem reveals a different behavior of $\tau_k(x)$ as $k$ exceeds $2\log\log x$.

**Theorem 10.6.** *Let $0 < \delta < 1$ and $A > 0$. Uniformly for $x \geq 3$, $(2+\delta)\log\log x \leq k \leq A\log\log x$,*

$$\tau_k(x) = C\frac{x\log x}{2^k}\left(1 + O\left(\frac{1}{(\log x)^{\delta^2/5}}\right)\right), \tag{10.11}$$

*where* $C = \dfrac{1}{4}\displaystyle\prod_{p>2}\left(1+\frac{1}{p(p-2)}\right) \approx 0.378694.$

In 1984, by elementary methods, Nicolas [**113**] extended the above estimate for $\tau_k(x)$ for a much wider range for $k$, namely by showing that, uniformly for $x \geq 3$, $(2+\delta)\log\log x \leq k \leq \log x/\log 2$,

$$\tau_k(x) = C\frac{x}{2^k}\log\left(\frac{x}{2^k}\right)\left(1 + O\left(\frac{1}{\log^\eta x}\right)\right)$$

for some positive number $\eta$ that depends on $\delta$. Four years later, Balazard, Delange, and Nicolas [**6**] provided an estimate for $\tau_k(x)$ when $k$ is close to $2\log\log x$, namely by proving that, for $|k-2\log\log x| \le A\sqrt{\log\log x}$,

$$\tau_k(x) = C\Phi\left(\frac{k-2\log\log x}{\sqrt{2\log\log x}}\right)\frac{x\log x}{2^k}\left(1+O_A\left(\frac{1}{\sqrt{\log\log x}}\right)\right),$$

where $\Phi(z) = \dfrac{1}{\sqrt{2\pi}}\displaystyle\int_{-\infty}^{z} e^{-t^2/2}\,dt$.

**Remark 10.7.** *Theorem* 10.4 *can have unexpected applications. For instance, De Koninck and Tenenbaum* [**36**] *used this result to estimate the probability that an integer $n \le x$ verifies $\Omega(n) \le \log\log x$. More precisely, they proved that*

$$\sum_{\substack{n\le x\\ \Omega(n)\le \log\log x}} 1 = \frac{1}{2}x - x\frac{C+\{\log\log x\}}{\sqrt{2\pi\log\log x}} + O\left(\frac{x}{\log\log x}\right),$$

*(here $\{y\}$ stands for the fractional part of $y$) where*

$$C = \gamma - \frac{2}{3} + \sum_p \left(\frac{1}{p-1} - \log\left(\frac{1}{1-1/p}\right)\right) \approx 0.36798.$$

## Problems on Chapter 10

We know by the Turán-Kubilius inequality that the number of positive integers $n \le x$ for which $|\omega(n)/\log\log x - 1| > \delta$ is $O(x/(\log\log x))$ for any fixed $\delta > 0$. (See, for example, Lemma 7.18.)

In the following problems, we will see that the Hardy-Ramanujan inequalities give us better upper bounds on the cardinality of the sets of such positive integers $n$.

For the following problems, one might need the more precise form of Stirling's formula given in (1.17).

**Problem 10.1.** *Use the fact that $1 \le x/n$ for all $n \le x$ to show that if $k > 10\log\log x$, then*

$$\Pi_k(x) \ll \frac{x}{k!}(\log\log x + c_0)^k.$$

*(Hint: First write $\Pi_k(x) \le \sum_{\substack{n\le x\\ \omega(n)=k}} x/n$. Then use the multinomial formula and Mertens' formula, as in the proof of Theorem* 10.1*.)*

**Problem 10.2.** *Use Theorem* 10.1*, Problem* 10.1*, and Stirling's formula to show that*

$$\max_k\{\Pi_k(x)\} \ll \frac{x}{\sqrt{\log\log x}}.$$

*(Hint: If $k < 10\log\log x$, use Theorem* 10.1 *and Stirling's formula to conclude that*

$$\Pi_k(x) \ll \frac{x}{(k-1)^{1/2}\log\log x}\left(\frac{e\log\log x + c_1}{k-1}\right)^{k-1}.$$

*Then show that for any fixed $A > 0$, the function $t \mapsto (A/t)^t$ is increasing for $t \le A/e$ and decreasing for $t \ge A/e$.)*

**Problem 10.3.** *Let $\delta \in (0,1)$ be fixed. Show, using the Hardy-Ramanujan inequality, that*

$$\#\{n \le x : \omega(n) \le \lfloor \delta\log\log x\rfloor\} \le \frac{x}{(\log x)^{1-\delta\log(e/\delta)+o(1)}}$$

*as $x \to \infty$. (Hint: Let $k \le K = \lfloor \delta\log\log x\rfloor$. Use the fact that for any fixed $A > 1$, the function $t \mapsto (A/t)^t$ is increasing for $t \le A/e$ and decreasing for $t \ge A/e$ to conclude that it suffices to look more closely at $\Pi_K(x)$. Then use Stirling's formula to get a good understanding of the upper bound given by Theorem* 10.1 *with this value of $K$.)*

**Problem 10.4.** *Let $\eta > 1$ be fixed. Show, using the Hardy-Ramanujan inequality, that*

$$\#\{n \le x : \omega(n) \ge \lfloor \eta\log\log x\rfloor\} \le \frac{x}{(\log x)^{1-\eta\log(e/\eta)+o(1)}}$$

*as $x \to \infty$. (Hint: Reduce the problem to that of studying $\Pi_K(x)$, where $K = \lfloor \eta\log\log x\rfloor$. One might want to use Problem* 10.1 *for excessively large values of $k$.)*

**Problem 10.5.** *Show that*

$$\#\{n \le x : \omega(n) > (\log\log x)^2\} \le x\exp\left(-(1+o(1))(\log\log x)^2(\log\log\log x)\right)$$

*as $x \to \infty$.*

*Chapter 11*

# The *abc* Conjecture and Some of Its Applications

## 11.1. The *abc* conjecture

The subject of this chapter concerns a deep conjecture linking the multiplicative and additive structures of the set of positive integers. It is the outcome of a discussion between David W. Masser (Basel University, Switzerland) and Joseph Oesterlé (Université de Paris VI, France) held in Bonn in 1985. Oesterlé was wondering if it was possible to determine the smallest possible exponent $\alpha$ such that, for every triplet of positive coprime integers $a, b, c$, satisfying $a + b = c$, one would have

$$c < \left( \prod_{p|abc} p \right)^{\alpha},$$

where the product runs over the set of prime factors $p$ of $abc$. From this discussion, the now very famous *abc conjecture* was born in 1985.

First, some notation.

Let $\gamma(1) = 1$ and, for $n \geq 2$, let

$$\gamma(n) = \prod_{p \,|\, n} p.$$

The number $\gamma(n)$ is sometimes called the *algebraic radical* of $n$ (or the *kernel* of $n$). It is the generator of the radical of the ideal $n\mathbb{Z}$ generated by $n$ inside the ring of integers $\mathbb{Z}$. (Recall that if $R$ is a commutative ring and $I$ is an ideal, then the radical ideal of $I$ denoted $\mathrm{rad}(I)$ is the ideal consisting

of all $x \in R$ such that $x^k \in I$ for some positive integer $k$.) The following statement is generally called the *abc*-conjecture.

**Conjecture 11.1.** *(The abc conjecture). For every $\varepsilon > 0$ there exists a constant $M = M(\varepsilon) > 0$ such that whenever $a$, $b$, and $c$ are coprime nonzero integers with $a + b = c$,*

$$\max\{|a|, |b|, |c|\} \leq M \cdot \gamma(abc)^{1+\varepsilon}. \tag{11.1}$$

Essentially, the *abc* conjecture tells us that if three large numbers are tied by an additive relation, their prime factors cannot all be small. This is why, as we will see, the *abc* conjecture can shed much light on certain important problems, such as Fermat's last theorem.

In this chapter, we mainly examine some applications of this conjecture.

## 11.2. The relevance of the condition $\varepsilon > 0$

One might naively ask why in inequality (11.1) we cannot take $\varepsilon = 0$.

Before we provide an answer to that question, let us first examine some numerical examples. First consider an example provided by Nitaj [**114**], namely the sequence of triplets of positive integers $a_n, b_n, c_n$ defined by

$$a_n = 1, \qquad b_n = 5^{2^n} - 1, \qquad c_n = 5^{2^n} \qquad (n = 1, 2, 3, \ldots). \tag{11.2}$$

Clearly the numbers $a_n, b_n, c_n$ are coprime and

$$a_n + b_n = c_n \qquad (n = 1, 2, 3, \ldots).$$

According to the *abc* conjecture, we must have

$$\begin{aligned}
5^2 &< M \cdot \left( \prod_{p | a_1 b_1 c_1} p \right)^{1+\varepsilon} = M \cdot (2 \cdot 3 \cdot 5)^{1+\varepsilon} = M \cdot 30^{1+\varepsilon}, \\
5^4 &< M \cdot \left( \prod_{p | a_2 b_2 c_2} p \right)^{1+\varepsilon} = M \cdot (2 \cdot 3 \cdot 5 \cdot 13)^{1+\varepsilon} = M \cdot 390^{1+\varepsilon}, \\
5^8 &< M \cdot \left( \prod_{p | a_3 b_3 c_3} p \right)^{1+\varepsilon} = M \cdot (2 \cdot 3 \cdot 5 \cdot 13 \cdot 313)^{1+\varepsilon} = M \cdot 122070^{1+\varepsilon},
\end{aligned}$$

and so on.

It follows from the *abc* conjecture that

$$M(\varepsilon) \geq \frac{5^{2^n}}{[5 \cdot \gamma(5^{2^n} - 1)]^{1+\varepsilon}}. \tag{11.3}$$

Hence, setting $\varepsilon = 1/100$, we observe that the right-hand side of (11.3) is equal to 1.5 if $n = 2$, to 2.84 if $n = 3$, 5.03 if $n = 4$ and to 7.84 if $n = 5$. Therefore, for this particular case, it is clear that $M = M(1/100) \geq 7.84$.

Now instead of considering the triplet (11.2), let us consider the triplet

$$a_n = 1, \qquad b_n = 7^{2^n} - 1, \qquad c_n = 7^{2^n} \qquad (n = 1, 2, 3, \ldots), \tag{11.4}$$

which also satisfies the conditions of the *abc* conjecture. We find that, for $n = 5$,

$$\begin{aligned} M(\varepsilon) &\geq \frac{7^{32}}{[7 \cdot \gamma(7^{32} - 1)]^{1+\varepsilon}} \\ &= \frac{7^{32}}{[7 \cdot \gamma(2^8 \cdot 3^2 \cdot 5^2 \cdot 17 \cdot 353 \cdot 1201 \cdot 169553 \cdot 47072139617)]^{1+\varepsilon}}, \end{aligned}$$

which implies that $M(1/100) \geq 51.317\ldots$.

Our imagination can certainly create other examples allowing for large lower bounds for $M(1/100)$. In any event, we will now show that $M = M(\varepsilon)$ tends to infinity as $\varepsilon$ tends to zero.

**Theorem 11.2.** *We have*

$$\liminf_{\varepsilon \to 0} M(\varepsilon) = +\infty. \tag{11.5}$$

**Proof.** To obtain this result we shall examine the solutions of the famous Fermat-Pell equation $x^2 - 2y^2 = 1$. It is well known that this equation has infinitely many solutions provided by the expansion of the continuous fraction of $\sqrt{2}$. In any event, using the fact that the smallest positive solution of $x^2 - 2y^2 = 1$ is $(x_1, y_1) = (3, 2)$, one can easily show that all the other solutions $(x_n, y_n)$ are given implicitly by the relation

$$x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n \qquad (n = 1, 2, \ldots). \tag{11.6}$$

Now let us take a closer look at those subscripts $n$ which are powers of 2. We first prove by induction that

$$2^{m+1} | y_{2^m} \qquad (m = 0, 1, 2, \ldots). \tag{11.7}$$

It is clear that (11.7) is true for $m = 0$. It remains to prove that $2^{m+1} | y_{2^m}$ implies that $2^{m+2} | y_{2^{m+1}}$. We have by hypothesis that there exists a positive integer $A$ such that $y_{2^m} = A2^{m+1}$. On the other hand, it follows from (11.6) that, for all $n \geq 1$,

$$x_{2n} + y_{2n}\sqrt{2} = ((3 + 2\sqrt{2})^n)^2 = (x_n + y_n\sqrt{2})^2 = x_n^2 + 2y_n^2 + (2x_n y_n)\sqrt{2},$$

so that $y_{2n} = 2x_n y_n$. Thus, choosing $n = 2^m$, we have

$$y_{2^{m+1}} = 2x_{2^m} y_{2^m} = 2x_{2^m} 2^{m+1} A = 2^{m+2} x_{2^m} A,$$

which means that $2^{m+2} | y_{2^{m+1}}$, thereby proving (11.7).

We now apply the *abc* conjecture to the equation

$$1 + 2y_n^2 = x_n^2 \quad \text{for} \quad n = 2^m \qquad (m = 0, 1, 2, \ldots),$$

which gives, using (11.7) and the fact that $y_n < x_n$,

$$\begin{aligned} x_n^2 &\leq M(\varepsilon)\,(\gamma(2x_n y_n))^{1+\varepsilon} \leq M(\varepsilon)\left(x_n \cdot 2 \cdot \frac{y_n}{2^{m+1}}\right)^{1+\varepsilon} \\ &= M(\varepsilon)\left(x_n \cdot \frac{y_n}{2^m}\right)^{1+\varepsilon} < M(\varepsilon)\frac{x_n^{2(1+\varepsilon)}}{2^{m(1+\varepsilon)}}. \end{aligned}$$

It follows that

$$M(\varepsilon) > \frac{2^{m(1+\varepsilon)}}{x_n^{2\varepsilon}}.$$

Therefore, keeping $n$ fixed (and thus also $m$ fixed) and letting $\varepsilon$ tend to 0, we may conclude that

$$\liminf_{\varepsilon \to 0} M(\varepsilon) \geq 2^m,$$

which proves (11.5). □

The second question one might ask is "What type of upper bound can we really obtain rigourously for $c$?" Here are two results to that effect.

In 1986, C. L. Stewart and R. Tijdeman obtained the following result:

> *There exists a computable constant $k > 0$ such that for each triplet of positive integers $a, b, c$ verifying $(a, b, c) = 1$ and $a + b = c$, we have*

$$c < \exp\{k \cdot \gamma(abc)^{15}\}. \tag{11.8}$$

A somewhat better result was obtained in 1996 by C. L. Stewart and K. Yu (see [**136**]):

> *For each $\varepsilon > 0$, there exists a computable constant $C_1 = C_1(\varepsilon) > 0$ such that for each triplet of positive integers $a, b, c$ verifying $(a, b, c) = 1$ and $a + b = c$, we have*

$$c < \exp\{C_1 \gamma(abc)^{\frac{1}{3}+\varepsilon}\}. \tag{11.9}$$

**Remark 11.3.** *The best example known to challenge inequality* (11.9) *is the one with $a = 1$, $b = 2 \cdot 3^7$ and $c = 5^4 \cdot 7$ which gives*

$$\frac{\log\log c}{\log \gamma(abc)} = 0.39765\ldots.$$

## 11.3. The Generalized Fermat Equation

Fermat's last theorem asserts that the equation

$$x^n + y^n = z^n$$

has no solution in positive integers $x,\ y,\ z$ and $n$ with $n \geq 3$. It was proved in 1995 by A. Wiles [**139**], [**146**]. Here is a more general conjecture:

**Conjecture 11.4.** *The Diophantine equation*

$$x^m + y^n = z^t \tag{11.10}$$

*has only finitely many integer solutions* $|x| > 1,\ |y| > 1,\ |z| > 1,\ m > 0,\ n > 0,\ t > 0$, *with* $\gcd(x, y) = 1$ *and* $1/m + 1/n + 1/t < 1$.

We note that when $x = 1$, we get $z^t - y^n = 1$. Catalan conjectured in 1844 that the only solution in integers $z,\ y,\ t \geq 2,\ n \geq 2$ is $3^2 - 2^3 = 1$. For many years this was known as the *Catalan conjecture*. It was proved by Mihăilescu in 2002 [**106**]. Here, we prove Conjecture 11.4 under the *abc* conjecture.

**Proposition 11.5.** *The abc conjecture implies Conjecture* 11.4.

**Proof.** It is easy to see that there exists $c_0 < 1$ such that if $m,\ n,\ t$ are positive integers with $1/m + 1/n + 1/t < 1$, then $1/m + 1/n + 1/t < c_0$; in fact, one can choose any real number $c_0$ satisfying $41/42 < c_0 < 1$. Now assume that $x,\ y,\ z,\ m,\ n,\ t$ is a solution of equation (11.10). Apply the *abc* conjecture with $a = x^m,\ b = y^n,\ c = z^t$ (note that $abc \neq 0$ and $\gcd(a, b) = 1$) and some fixed $\varepsilon > 0$ such that $c_0(1 + \varepsilon) < 1$ and obtain

$$\max\{|x|^m, |y|^n, |z|^t\} \ll \gamma(xyz)^{1+\varepsilon} \leq |xyz|^{1+\varepsilon}.$$

Let $N = |xyz|$. Then the above implies that

$$|x| \ll N^{(1+\varepsilon)/m}, \qquad |y| \ll N^{(1+\varepsilon)/n}, \qquad |z| \ll N^{(1+\varepsilon)/t},$$

and multiplying these relations we get

$$N \ll N^{(1+\varepsilon)(1/m+1/n+1/t)} < N^{(1+\varepsilon)c_0},$$

so that $N^{1-(1+\varepsilon)c_0} \ll 1$, and since $1 - (1 + \varepsilon)c_0 > 0$ is a fixed positive constant, we get that $N \ll 1$. Hence, $\max\{|x|, |y|, |z|\} = O(1)$. Since $|x| \geq 2$, the inequality $|x| \ll N^{(1+\varepsilon)/m}$ shows that $m = O(1)$, and similarly $n = O(1)$ and $t = O(1)$. □

## 11.4. Consecutive powerful numbers

Recall that a positive integer is called powerful if $p^2 \mid n$ whenever $p \mid n$. Observe that if $n$ is powerful, then $\gamma(n) \leq n^{1/2}$.

**Proposition 11.6.** *Under the abc conjecture, there exist only finitely many positive integers $n$ such that $n-1,\ n,\ n+1$ are all powerful.*

**Proof.** Let $n$ be a number with the desired property. Applying the *abc* conjecture with $\varepsilon = 1/5$ to the equation $n^2 = (n-1)(n+1)+1$, we obtain

$$n^2 \ll \gamma(n(n^2-1))^{6/5} \ll \left(n^{1/2}(n^2-1)^{1/2}\right)^{6/5} < n^{3/2\cdot 6/5} = n^{9/5},$$

which certainly yields $n \ll 1$. □

## 11.5. Sums of $k$-powerful numbers

One can generalize the notion of powerful numbers in the following manner.

**Definition 11.7.** *Given an integer $k \geq 2$, we say that an integer $n \geq 2$ is $k$-powerful if $\gamma(n)^k | n$.*

These numbers raise interesting questions. For instance, we all know that the Diophantine equation $x^2 + y^2 = z^2$ has infinitely many nonzero solutions, meaning in particular that the equation $x + y = z$ has infinitely many solutions in powerful numbers. Now even though we have known (since Euler) that the equation $x^3 + y^3 = z^3$ has no solution in positive integers $x, y, z$, is there a chance for the equation $x + y = z$ to have some solutions in 3-powerful numbers, and why not infinitely many such solutions ?

YES, since, for instance, we have $919^3 = 271^3 + 2^3 \cdot 3^5 \cdot 73^3$. And here is another example:

$$37^3 \cdot 197^3 \cdot 307^3 = 2^7 \cdot 3^4 \cdot 5^3 \cdot 7^3 \cdot 2287^3 + 17^3 \cdot 106219^3.$$

And another one:

$$2^7 \cdot 5^4 \cdot 353^3 = 3^4 \cdot 29^3 \cdot 89^3 + 7^3 \cdot 11^3 \cdot 167^3.$$

In fact, it is possible to show that equation $x^3 + y^3 = 6z^3$ has infinitely many solutions in nonzero integers $x, y, z$ with $6|z$ (see Problem 11.3), thereby implying that $x + y = z$ has infinitely many solutions in 3-powerful integers.

Is such a phenomenon possible with 4-powerful numbers ? Probably not ! Here is a conjecture concerning that possibility.

**Conjecture 11.8.** *(*Erdős*). Equation $x + y = z$ has at most a finite number of solutions in coprime 4-powerful numbers $x, y, z$.*

Nevertheless we can prove the following.

**Theorem 11.9.** *The abc conjecture implies Conjecture* 11.8.

**Proof.** Assume that $x, y, z$ are three 4-powerful numbers, that they are coprime, and that they verify $x + y = z$. Applying the *abc* conjecture with $\varepsilon = 1/3$, we get

$$z \le M \cdot (\gamma(xyz))^{1+\varepsilon} \le M \cdot (xyz)^{(1+\varepsilon)/4} \le M \cdot z^{3(1+\varepsilon)/4}.$$

It follows that

$$z^{(1-3\varepsilon)/4} \le M,$$

thereby implying that $z$ is bounded, as well as $x$ and $y$. □

## 11.6. The Erdős-Woods conjecture

Erdős and Woods conjectured that there exists some positive integer $k$ (sometimes called the *Erdős-Woods number*) such that every positive integer $n$ is uniquely determined by the set of prime factors of $n+1,\ n+2,\ \dots,\ n+k$. Here, we give a proof of this conjecture under the *abc* conjecture.

**Proposition 11.10.** *Under the abc conjecture, there is a positive integer $k$ such that every positive integer $n$ is uniquely determined by the prime factors of $n+1,\ n+2,\ \dots,\ n+k$.*

**Proof.** We first show that under the *abc* conjecture there exist only finitely many pairs of positive integers $n < m$ such that

$$\gamma(n+i) = \gamma(m+i) \qquad \text{for } i = 1, 2, 3, 4. \tag{11.11}$$

Indeed, assume that (11.11) holds. Then, applying the *abc* conjecture with some small $\varepsilon > 0$ to the relation $(n+1)-1 = n$ with $a = n+1,\ b = -1,\ c = n$, we obtain that

$$n < n+1 \ll \gamma(n(n+1))^{1+\varepsilon} = \gamma(n)^{1+\varepsilon}\gamma(n+1)^{1+\varepsilon}, \tag{11.12}$$

and a similar relation holds for $m$. Now $0 < m - n = (m+i) - (n+i)$, so that (11.11) implies that $m - n$ is divisible by $\gamma(m+i)$ for $i = 1, 2, 3, 4$. Since $(m+i, m+j) \le j - i = O(1)$ for $1 \le i < j \le 4$, and since $\gamma(m+i)$ is squarefree for $i = 1, 2, 3, 4$, it follows that

$$\operatorname{lcm}[\gamma(m+1), \dots, \gamma(m+4)] \gg \gamma(m+1) \cdots \gamma(m+4).$$

Hence, in light of (11.12) with $m$ in place of $n$,

$$\gamma(m+1)\cdots\gamma(m+4) \ll m-n \le m+1 \ll \gamma(m+1)^{1+\varepsilon}\gamma(m+2)^{1+\varepsilon},$$

giving

$$\gamma(m+3)\gamma(m+4) \ll \gamma(m+1)^{\varepsilon}\gamma(m+2)^{\varepsilon}.$$

Applying inequality (11.12) with $n$ replaced by $m+3$ we get

$$\begin{aligned} m &< m+3 < (\gamma(m+3)\gamma(m+4))^{1+\varepsilon} \\ &\ll (\gamma(m+1)\gamma(m+2))^{\varepsilon(1+\varepsilon)} \\ &\le ((m+1)(m+2))^{\varepsilon(1+\varepsilon)} \ll m^{8/9}, \end{aligned}$$

provided we choose $\varepsilon = 1/3$. This shows that $m = O(1)$. Thus, there exists $c_0$ such that if $m > c_0$, then $m$ is uniquely determined by the prime factors of $m+1,\ m+2,\ m+3$, and $m+4$. For the pairs $n < m \le c_0$, let $k = k(m,n)$ be such that $m+k$ has a prime factor not dividing $n+k$ for each $n$ with this property. (We may choose $k$ such that $m+k = p$ is a prime and then $p = m+k > n+k$, so that $p$ does not divide $n+k$.) This shows that the Erdős-Woods conjecture holds with $k = \max_{1\le n<m\le c_0}(5, k(m,n))$. □

## 11.7. A problem of Gandhi

Let $n \ge 3$ be a fixed integer. J. M. Gandhi was interested in the coprime integer solutions $x, y, z$ and to the equation

$$x^n + y^n = n!z^n. \tag{11.13}$$

First observe that if $n = 2$, equation (11.13) has infinitely many solutions. Indeed, setting $x_1 = y_1 = 1$ and defining implicitly $x_k$ and $y_k$ for each integer $k \ge 2$ by the relation

$$x_k + y_k\sqrt{2} = (1+\sqrt{2})^k,$$

it is easy to see that for each integer $k \ge 1$, $x_k^2 - 2y_k^2 = (-1)^k$ so that if $k$ is odd, we have $1 + x_k^2 = 2y_k^2$, thereby yielding infinitely many solutions to (11.13) for the case $n = 2$.

In the case $n = 3$, one can construct infinitely many solutions using the following recurrence:

$$\begin{aligned} &x_0 = 37, \quad y_0 = 17, \quad z_0 = 21, \\ &x_{k+1} = x_k(x_k^3 + 2y_k^3), \\ &\quad y_{k+1} = -y_k(2x_k^3 + y_k^3), \quad z_{k+1} = z_k(x_k^3 - y_k^3) \qquad (k \ge 0). \end{aligned}$$

No solution is known for the cases $n \ge 4$. Hence, the following result is perhaps not so surprising.

**Theorem 11.11.** *If the abc conjecture holds, then equation (*11.13*) has at most a finite number of solutions in coprime positive integers $x, y, z$ and $n \geq 4$.*

**Proof.** Assume that such a solution $x, y, z$ with $n \geq 4$ exists. Without any loss of generality, we can assume that $(x, y, z) = 1$. Observe that $d = (x^n, n!) = 1$; indeed, if $d > 1$, since $x$ and $z$ are coprime, it follows that $d = (x^n, y^n) = d_0^n$ with $d_0 = (x, y) > 1$, which is not possible. We may therefore apply the *abc* conjecture to the equation $x^n + y^n = n!z^n$, thus obtaining

$$n!z^n \leq M \cdot (xyz)^{1+\varepsilon}\gamma(n!)^{1+\varepsilon}.$$

Using the trivial upper bounds $x, y, z \leq (n!z^n)^{1/n}$, it follows that

$$n!z^n \leq M \cdot (n!z^n)^{3(1+\varepsilon)/n}\gamma(n!)^{1+\varepsilon}.$$

Using inequality (1.12) and Lemma 2.8, we obtain

$$(nz/e)^{n(1-3(1+\varepsilon)/n)} \leq (n!z^n)^{1-3(1+\varepsilon)} \leq M \cdot 4^{n(1+\varepsilon)},$$

that is,

$$(nz/e)^{1-3(1+\varepsilon)/n} \leq M_0 \cdot 4^{1+\varepsilon},$$

for a certain constant $M_0 = M_0(\varepsilon)$. It follows from this relation that $n$ and $z$ are bounded and therefore that equation (11.13) has at most a finite number of solutions with $n \geq 4$. □

## 11.8. The *k-abc* conjecture

It is interesting to mention that the *abc* conjecture can be generalized to a sum of more than three numbers:

**Conjecture 11.12.** *(The k-abc conjecture) Let $k \geq 3$ be an integer. Then, for each $\varepsilon > 0$, there exists a constant $M_k(\varepsilon) > 0$ such that, if $a_1, \ldots, a_k$ are integers verifying the three conditions*

(i) $a_1 + a_2 + \cdots + a_k = 0$,

(ii) $\gcd(a_1, a_2, \ldots, a_k) = 1$,

(iii) *no sub-sum is 0,*

*then*

$$\max(|a_1|, |a_2|, \ldots, |a_k|) \leq M_k(\varepsilon) \cdot \gamma(a_1 a_2 \cdots a_k)^{2k-5+\varepsilon}.$$

For more details on this conjecture, see J. Browkin and J. Brzezinski [**18**].

## Problems on Chapter 11

**Problem 11.1.** *How is it that the example given in Remark* 11.3 *does not contradict relation (*11.9*) ?*

**Problem 11.2.** *According to Catalan's conjecture, the only two consecutive powers are* $2^3$ *and* $3^2$*. Prove that the abc conjecture implies that there can be only a finite number of consecutive powers.*

**Problem 11.3.** *Prove that there exist infinitely many triplets of 3-powerful integers* $a, b, c$ *with* $\gcd(a, b) = 1$*, such that* $a + b = c$*.*

**Problem 11.4.** *Let* $a \geq 1$ *be a fixed integer. Assuming that the abc conjecture is true, show that the diophantine equation*

$$ax^3 + y^3 = z^4$$

*can have only a finite number of solutions* $x, y, z$ *with* $(x, y) = 1$*.*

**Problem 11.5.** *Find an infinite set of integers* $a$ *such that*

$$ax^3 + y^3 = z^4$$

*has at least one solution in positive integers* $x, y, z$*.*

**Problem 11.6.** *Does the abc conjecture necessarily imply that the diophantine equation*

$$2x^2 + y^3 = z^4$$

*cannot have any solutions in positive integers* $x, y, z$ *?*

**Problem 11.7.** *A prime number* $p$ *is called a Wieferich prime if* $p^2 \mid 2^{p-1} - 1$*. Only two prime numbers, namely 1093 and 3511, are known to be Wieferich primes; there are no other* $< 1.25 \times 10^{15}$*. These primes are of historical interest because of Kummer's proof that the so-called first case of Fermat's last theorem is possible only for Wieferich primes. Show that the abc conjecture implies that there are infinitely many primes which are not Wieferich primes (Hint: Show first that if we let* $f_p$ *stand for the multiplicative order of* 2 *modulo* $p$*, then* $p$ *is a Wieferich prime if and only if* $p^2 \mid 2^{f_p} - 1$*. Then show that if all but finitely many primes are Wieferich, then* $2^n - 1 = dm$*, where* $d = O(1)$ *and* $m$ *is powerful. Then use the abc conjecture.)*

**Problem 11.8.** *Show heuristically that the number of Wieferich primes* $\leq x$ *is of order* $\log\log x$*.*

**Problem 11.9.** *For each positive integer* $n$*, write* $X_n, Y_n$ *for the integers for which* $X_n + \sqrt{2}Y_n = (3 + 2\sqrt{2})^n$*.*

(i) *Show that for each* $n \geq 1$*,* $X_n^2 - 2Y_n^2 = 1$*.*

(ii) *Show that* $2^{n+1} \mid Y_{2^{n+1}}$ *for each* $n \geq 1$*.*

(iii) *Use (i) and (ii) to deduce that the abc conjecture is false for* $\varepsilon = 0$.

**Problem 11.10.** *Let* $a > 1$ *and* $b > 1$ *be positive integers. Show, using the abc conjecture, that if* $\gamma(a^n - 1) = \gamma(b^n - 1)$ *for all* $n \geq 1$, *then* $a = b$.

**Problem 11.11.** *Use the abc conjecture to show that the Diophantine equation* $(x^n - 1)(y^n - 1) = z^2$ *has only finitely many integer solutions* $y > x > 1, z > 0, n \geq 6$. *(Hint: Show first that* $x^n - 1 = du^2$, $y^n - 1 = dv^2$ *for some integers* $d$, $u$, $v$. *Use the abc conjecture to infer that* $u$ *and* $v$ *are very small with respect to* $x^n$ *and* $y^n$ *respectively. Then eliminate* $d$ *to get* $x^n v^2 - y^n u^2 = (v^2 - u^2)$. *Argue that you can apply the abc conjecture to this equation and complete the argument.)*

**Problem 11.12.** *Let* $\{F_n\}_{n\geq 1}$ *be the Fibonacci sequence* $F_1 = 1$, $F_2 = 1$ *and* $F_{n+2} = F_{n+1} + F_n$ *for all* $n \geq 1$. *Show that the abc conjecture implies that* $F_n$ *is powerful only for finitely many* $n$. *(Hint: First prove that if* $\{L_n\}_{n\geq 1}$ *denotes the sequence* $L_1 = 1$, $L_2 = 3$, *and* $L_{n+2} = L_{n+1} + L_n$ *for all* $n \geq 1$, *then* $L_n^2 - 5F_n^2 = \pm 4$.*)*

*Chapter 12*

# Sieve Methods

## 12.1. The sieve of Eratosthenes

The Inclusion-Exclusion principle, or the Möbius inversion formula, can be used—at least theoretically—to calculate $\pi(x)$. For a sufficiently large $x$, let us write

$$P = \prod_{p \le \sqrt{x}} p.$$

Then an integer $n$ with $\sqrt{x} < n < x$ is prime if and only if $(n, P) = 1$. Thus, we can write

$$\begin{aligned} \pi(x) - \pi(\sqrt{x}) + 1 &= \sum_{n \le x} E((n, P))) = \sum_{n \le x} \sum_{\substack{d \mid n \\ d \mid P}} \mu(d) \\ &= \sum_{d \mid P} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor, \end{aligned} \tag{12.1}$$

where, as we have seen,

$$E(n) = \sum_{d \mid n} \mu(d)$$

is 1 if $n = 1$ and 0 otherwise (see Theorem 4.8(i)). If at this stage we insert the simple estimate

$$\left\lfloor \frac{x}{d} \right\rfloor = \frac{x}{d} + O(1)$$

in (12.1), we obtain

$$\pi(x) - \pi(\sqrt{x}) + 1 = x \prod_{p \le \sqrt{x}} \left(1 - \frac{1}{p}\right) + O(2^{\pi(\sqrt{x})}). \tag{12.2}$$

By the estimate of Problem 4.4, the first term of the right-hand side of (12.2) is

$$\sim 2e^{-\gamma}\frac{x}{\log x} \qquad \text{as } x \to \infty,$$

while by Chebyshev's estimates, the error term in (12.2) can be seen to be larger than any power of $x$, thus showing that the error term in (12.2) can in fact be larger than the main term, thereby spoiling our goal of obtaining something worthwhile by this approach.

The above calls for two comments. On the one hand, the exact formula (12.1)—called the *sieve formula of Eratosthenes* or at times the *Legendre formula*—involves too many terms for any reasonable practical estimate. On the other hand, the estimate of the main term itself shows, taking into account the Prime Number Theorem and the fact that $e^{-\gamma} \neq 1$, that the "error terms" created by replacing $\lfloor x/d \rfloor$ by $x/d$ have made a global contribution of the same order of magnitude as the "main term". This suggests that this method, even suitably adapted, will never allow for a proof of the Prime Number Theorem. However, it can provide Chebyshev type estimates in a wide context.

In order to obtain a nontrivial result starting from formula (12.1), one may introduce a parameter $y$, $2 \le y \le x$, and bound $\pi(x) - \pi(y) + 1$ by the number of integers $n \le x$ having no prime factor $p \le y$. With the same calculations we get

$$\begin{aligned} \pi(x) &\le x \prod_{p \le y} \left(1 - \frac{1}{p}\right) + O(2^y) \\ &= \frac{x(e^{-\gamma} + o(1))}{\log y} + O(2^y) \ll \frac{x}{\log\log x}, \end{aligned} \tag{12.3}$$

where we chose $y = \log x$.

With the aim of improving the efficiency of the above method, Viggo Brun invented the combinatorial sieve between 1917 and 1924.

## 12.2. The Brun sieve

The Eratosthenes sieve rests on the identity

$$\mu * \mathbf{1} = E.$$

Brun's idea was to introduce two auxiliary functions $\mu_1$ and $\mu_2$ satisfying

$$\mu_1 * \mathbf{1} \le E \le \mu_2 * \mathbf{1} \tag{12.4}$$

and vanishing often enough so that the number of nonzero terms in the resulting formula analogous with (12.1) is not overwhelming. Brun's initial choice led to what is now called *Brun's pure sieve* and is the following.

**Theorem 12.1.** *Denote by $\chi_t$ the characteristic function of the set of integers $n$ such that $\omega(n) \le t$. Then for each integer $h \ge 0$, the functions defined by*

$$\mu_i(n) = \mu(n)\chi_{2h+2-i}(n) \qquad (i = 1, 2)$$

*satisfy inequalities* (12.4).

**Proof.** Since $\mu_i * 1(n)$ depends only on the kernel of $n$, we may assume that $\mu(n) \neq 0$. If $\omega(n) = k$, then, for each $r$ with $0 \le r \le k$, it is clear that $n$ has exactly $\binom{k}{r}$ divisors $d$ with $\omega(d) = r$. For any given $t \ge 0$, we can thus write

$$\chi_t * 1(n) = \sum_{\substack{d \mid n \\ \omega(d) \le t}} \mu(d) = \sum_{0 \le r \le t} (-1)^r \binom{k}{r} = (-1)^t \binom{k-1}{t},$$

where the last equality is easily obtained by induction over $t$. □

The above result immediately yields the following corollary.

**Corollary 12.2.** *Let $\mathcal{A}$ be a finite set of integers and let $\mathcal{P}$ be a set of prime numbers. Write*

$$\begin{aligned} \mathcal{A}_d &= \#\{a \in \mathcal{A} : a \equiv 0 \pmod d\}, \\ P(y) &= \prod_{\substack{p \le y \\ p \in \mathcal{P}}} p, \\ \mathcal{S}(\mathcal{A}, \mathcal{P}, y) &= \#\{a \in \mathcal{A} : (a, P(y)) = 1\}. \end{aligned}$$

*Then, for each integer $h \ge 0$,*

$$\sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h+1}} \mu(d)\mathcal{A}_d \le \mathcal{S}(\mathcal{A}, \mathcal{P}, y) \le \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} \mu(d)\mathcal{A}_d.$$

Let us see how the above result helps us to considerably improve the upper bound of $\pi(x)$ obtained by the Eratosthenes sieve (see (12.3)).

In Corollary 12.2, we chose $\mathcal{A} = \{n : n \le x\}$, $\mathcal{P} = \{\text{all primes}\}$ and $P = P(y) = \prod_{p \le y} p$. Then $\mathcal{S}(\mathcal{A}, \mathcal{P}, y)$ is the number of positive integers

$n \le x$ having no prime factor $p \le y$, so that

$$\begin{aligned}\mathcal{S}(\mathcal{A},\mathcal{P},y) &\le \sum_{\substack{d\mid P(y)\\ \omega(d)\le 2h}} \mu(d)\left\lfloor \frac{x}{d}\right\rfloor \\ &= x\sum_{\substack{d\mid P(y)\\ \omega(d)\le 2h}} \frac{\mu(d)}{d} + O\left(\sum_{\substack{d\mid P(y)\\ \omega(d)\le 2h}} 1\right) \qquad (12.5)\\ &= x\prod_{p\le y}\left(1-\frac{1}{p}\right) + O\left(\sum_{\substack{d\mid P(y)\\ \omega(d)\le 2h}} 1 + x\sum_{\substack{d\mid P(y)\\ \omega(d)> 2h}}\frac{1}{d}\right),\end{aligned}$$

and similarly

$$\begin{aligned}\mathcal{S}(\mathcal{A},\mathcal{P},y) &\ge \sum_{\substack{d\mid P(y)\\ \omega(d)\le 2h+1}} \mu(d)\left\lfloor \frac{x}{d}\right\rfloor \\ &= x\prod_{p\le y}\left(1-\frac{1}{p}\right) + O\left(\sum_{\substack{d\mid P(y)\\ \omega(d)\le 2h+1}} 1 + x\sum_{\substack{d\mid P(y)\\ \omega(d)> 2h+1}}\frac{1}{d}\right). \qquad (12.6)\end{aligned}$$

The first of the two error terms appearing either at (12.5) or at (12.6) does not exceed $y^{2h+1}$ since this is an upper bound for all integers $d$ such that $d \mid P(y)$ and $\omega(d) \le 2h+1$. The $d$-sums arising in the second error terms are bounded, in light of the arguments already used in Chapter 11, namely, for example, for the second error term in (12.5), by

$$\sum_{\substack{d\mid P(y)\\ \omega(d)>2h}} \frac{1}{d} \le \sum_{k>2h}\frac{1}{k!}\left(\sum_{p\le y}\frac{1}{p}\right)^k \le \sum_{k>2h}\frac{1}{k!}(\log\log y + c_0)^k.$$

Using the weak form of Stirling's formula (see 1.12), together with $y < x$, we get

$$\sum_{\substack{d\mid P(y)\\ \omega(d)>2h}} \frac{1}{d} \le \sum_{k>2h}\frac{1}{k!}\left(\log\log x + c_0\right)^k \le \sum_{k>2h}\left(\frac{e\log\log x + ec_0}{k}\right)^k.$$

Choosing the smallest integer $h \ge e\log\log x + ec_0$, we obtain

$$\sum_{\substack{d\mid P(y)\\ \omega(d)>2h}} \frac{1}{d} \le \left(\frac{1}{2}\right)^{2h}\left(1+\frac{1}{2}+\frac{1}{4}+\cdots\right) \ll \frac{1}{(\log x)^{2e\log 2}} \ll \frac{1}{(\log x)^2},$$

because $2e\log 2 = e\log 4 > e > 2$. For this choice of $h$, we impose that $y^{2h+1} \le x/(\log x)^2$, which for $h > 1$ is implied by

$$y \le \frac{x^{1/(2h+1)}}{\log x} \le \exp\left(\frac{\log x}{2e\log\log x + c_1} - \log\log x\right),$$

where we can take $c_1 = 2ec_0 + 1$. Since $1/2e > 1/10$, it follows that we may choose

$$y = \exp\left(\frac{\log x}{10\log\log x}\right), \tag{12.7}$$

in which case the inequality $y^{2h+1} \ll x/(\log x)^2$ holds for all $x$. With this choice of $y$, we have that

$$\prod_{p\le y}\left(1-\frac{1}{p}\right) \asymp \frac{1}{\log y} \asymp \frac{\log\log x}{\log x},$$

while the error terms in (12.5) and (12.6) are $O(x/(\log x)^2)$. Thus, we have proved that

$$\mathcal{S}(\mathcal{A},\mathcal{P},y) = x\prod_{p\le y}\left(1-\frac{1}{p}\right)\left(1+O\left(\frac{1}{\log y}\right)\right). \tag{12.8}$$

Since

$$\mathcal{S}(\mathcal{A},\mathcal{P},y) \ge \pi(x) - \pi(y) \ge \pi(x) - y \ge \pi(x) + O(x^{1/2}),$$

we immediately deduce that

$$\pi(x) \ll x^{1/2} + x\prod_{p\le y}\left(1-\frac{1}{p}\right) \ll \frac{x\log\log x}{\log x},$$

which, although much weaker than Chebyshev's estimate, is remarkable because of the simplicity and generality of the argument.

To summarize, we have just proved a result announced earlier (see (9.7)):

**Theorem 12.3.** *Letting*

$$\Phi(x,y) = \#\{n \le x : p(n) > y\},$$

*then, for* $y \le \exp\left(\dfrac{\log x}{10\log\log x}\right)$,

$$\Phi(x,y) = x\prod_{p\le y}\left(1-\frac{1}{p}\right)\left\{1+O\left(\frac{1}{\log y}\right)\right\}.$$

## 12.3. Twin primes

Now we expose another remarkable application of Brun's pure sieve, namely, the fact that the sum of the reciprocal of the twin primes is convergent.

**Proposition 12.4.** *Let* $\mathcal{J} = \{p : \ p \text{ and } p+2 \text{ are both primes}\}$ *and set* $\mathcal{J}(x) = \#\{p \le x : p \in \mathcal{J}\}$. *Then*

$$\mathcal{J}(x) \ll \frac{x(\log\log x)^2}{(\log x)^2}.$$

**Proof.** In Corollary 12.2, set $\mathcal{A} = \{n(n+2) : n \le x\}$. Again, let $\mathcal{P}$ stand for the set of all primes and let $y$ be a parameter to be chosen later. To understand $\#\mathcal{A}_d$, we look at

$$\rho(d) = \#\{0 \le n \le d-1 \ : \ n(n+2) \equiv 0 \pmod d\}.$$

Let us first show that $\rho(d)$ is multiplicative. Indeed, if $u$ and $v$ are coprime and $c \pmod{uv}$ is some congruence class modulo $uv$ such that $n(n+2) \equiv 0 \pmod{uv}$, then certainly $c \pmod u$ ($c \pmod v$, respectively) is a congruence class modulo $u$ (modulo $v$, respectively) such that $n(n+2) \equiv 0 \pmod u$ ($n(n+2) \equiv 0 \pmod v$, respectively). Conversely, if $a \pmod u$ and $b \pmod v$ are congruence classes for $n$ modulo $u$ and $v$ which are solutions to $n(n+2) \equiv 0 \pmod u$ and $n(n+2) \equiv 0 \pmod v$, respectively, then by the Chinese Remainder Theorem, there exists a class $c \pmod{uv}$ (which is unique) such that $c \equiv a \pmod u$ and $c \equiv b \pmod v$. Hence, $n(n+2) \equiv 0 \pmod u$ and $n(n+2) \equiv 0 \pmod v$, and since $u$ and $v$ are coprime, we get that $n(n+2) \equiv 0 \pmod{uv}$. This shows that $\rho(uv) = \rho(u)\rho(v)$. Note that $\rho(2) = 1,\ \rho(4) = 2,\ \rho(2^k) = 4$ for $k \ge 3$ and $\rho(p^k) = 2$ if $p > 2$ is odd. In particular, if $d$ is squarefree, then $\rho(d) = 2^{\omega(d)}$ if $d$ is odd and $\rho(d) = 2^{\omega(d)-1}$ if $d$ is even. Since there are precisely $\rho(d)$ solutions $n$ to the congruence $n(n+2) \equiv 0 \pmod d$ in any interval of length $d$, and since the interval $[1, x]$ is made up of $\lfloor x/d \rfloor$ intervals of length $d$ and (maybe) one shorter interval, we get that

$$\begin{aligned} \mathcal{A}_d &= \#\{n \le x \ : \ d \mid n(n+2)\} = \rho(d)\left(\left\lfloor \frac{x}{d} \right\rfloor + O(1)\right) \\ &= \frac{x\rho(d)}{d} + O(\rho(d)) = \frac{x\rho(d)}{d} + O(2^{\omega(d)}). \end{aligned}$$

Upon noting that if $p, p+2$ are twin primes, then either $p \le y$ or $p \in \mathcal{S}(\mathcal{A}, \mathcal{P}, y)$, we have, by Corollary 12.2, that

(12.9)

$$\begin{aligned}
\mathcal{J}(x) &\le \pi(y) + \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} \mu(d)\mathcal{A}_d \\
&= \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} \mu(d) \left( \frac{x\rho(d)}{d} + O(2^{\omega(d)}) \right) + O(y) \\
&= x \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} \frac{\mu(d)\rho(d)}{d} + O\left( y + \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} 2^{\omega(d)} \right) \\
&= x \sum_{d \mid P(y)} \frac{\mu(d)\rho(d)}{d} + O\left( y + 2^{2h} \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} 1 + x \sum_{\substack{d \mid P(y) \\ \omega(d) > 2h}} \frac{2^{\omega(d)}}{d} \right) \\
&= x \prod_{p \le y} \left( 1 - \frac{\rho(p)}{p} \right) + O\left( y + 2^{2h} \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} 1 + x \sum_{\substack{d \mid P(y) \\ \omega(d) > 2h}} \frac{2^{\omega(d)}}{d} \right) \\
&= \frac{x}{2} \prod_{3 \le p \le y} \left( 1 - \frac{2}{p} \right) + O\left( y + (2y)^{2h} + x \sum_{\substack{d \mid P(y) \\ \omega(d) > 2h}} \frac{2^{\omega(d)}}{d} \right).
\end{aligned}$$

Using the combinatorial fact that

$$\sum_{\substack{d \mid P(y) \\ \omega(d) > 2h}} \frac{2^{\omega(d)}}{d} \le \sum_{k > 2h} \sum_{\substack{d \mid P(y) \\ \omega(d) = k}} \frac{2^k}{d} \le \sum_{k > 2h} \frac{1}{k!} \left( \sum_{p \le y} \frac{2}{p} \right)^k,$$

together with Mertens' formula and estimate (1.12), we get

$$\sum_{\substack{d \mid P(y) \\ \omega(d) > 2h}} \frac{2^{\omega(d)}}{d} < \sum_{k > 2h} \frac{1}{k!} (2 \log\log x + 2c_0)^k < \sum_{k > 2h} \left( \frac{2e \log\log x + c_1}{k} \right)^k,$$

where $c_1 = 2ec_0$. Hence, we see that if we choose $h$ to be twice as large as in the proof of Theorem 12.3, that is, the minimal positive integer $h$ larger

than $2e\log\log x + c_1$, we then get

$$\sum_{\substack{d\,|\,P(y)\\ \omega(d)>2h}} \frac{2^{\omega(d)}}{d} < \frac{1}{2^{2h}}\left(\sum_{l\ge 0}\frac{1}{2^l}\right) = \frac{2}{2^{2h}} \ll \frac{1}{(\log x)^{4e\log 2}} < \frac{1}{(\log x)^2}. \tag{12.10}$$

Choosing $y = \exp(\log x/(20\log\log x))$, we obtain that

$$(2y)^{2h} = 2^{2h}\exp\left(\frac{2h\log x}{20\log\log x}\right) = \exp\left(\frac{(1+o(1))4e\log x}{20}\right) \ll \frac{x}{(\log x)^2}. \tag{12.11}$$

Inserting estimates (12.10) and (12.11) into (12.9), we get

$$\mathcal{J}(x) \ll x\prod_{3\le p\le y}\left(1-\frac{2}{p}\right) + \frac{x}{(\log x)^2}.$$

Finally, using Problem 4.6 with $\kappa = -2$, we have that

$$\begin{aligned}\prod_{3\le p\le y}\left(1-\frac{2}{p}\right) &= \frac{c_2}{(\log y)^2}(1+o(1)) = c_2\left(\frac{20\log\log x}{\log x}\right)^2(1+o(1))\\ &= (1+o(1))\frac{400c_2(\log\log x)^2}{(\log x)^2},\end{aligned}$$

so that

$$\mathcal{J}(x) \ll \frac{x(\log\log x)^2}{(\log x)^2},$$

which is what we wanted to prove. □

**Corollary 12.5.** *The series*

$$\sum_{p,\ p+2\ \text{primes}}\frac{1}{p} < \infty.$$

**Proof.** Since

$$\mathcal{J}(n) - \mathcal{J}(n-1) = \begin{cases} 1 & \text{if } n \text{ and } n+2 \text{ are both primes,}\\ 0 & \text{otherwise,}\end{cases}$$

then, in light of Proposition 12.4,

$$\begin{aligned}\sum_{p,p+2\ \text{primes}}\frac{1}{p} &= \sum_{n=2}^{\infty}\frac{\mathcal{J}(n)-\mathcal{J}(n-1)}{n} = \sum_{n=1}^{\infty}\mathcal{J}(n)\left(\frac{1}{n}-\frac{1}{n+1}\right)\\ &= \sum_{n=1}^{\infty}\frac{\mathcal{J}(n)}{n(n+1)} \ll \sum_{n\ge e}\frac{n(\log\log n)^2}{(\log^2 n)\,n(n+1)}\\ &< \sum_{n\ge e}\frac{(\log\log n)^2}{n(\log n)^2} \ll \int_e^{\infty}\frac{(\log\log t)^2}{t\log^2 t}\,dt < \infty,\end{aligned}$$

as requested. □

## 12.4. The Brun combinatorial sieve

The theory described in the previous sections of this chapter was later refined by partitioning the interval $[1, y]$ into suitable subintervals $[y_j, y_{j+1}]$, where $1 = y_0 < y_1 < \cdots < y_k = y$ and selecting for $i = 1,\ 2$, $\mu_i(d) = \mu(d)\chi_i^*(d)$, where $\chi_i^*(d)$ is the characteristic function of the set of those positive integers $n$ having exactly $2h_j+2-i$ prime factors in $[y_j, y_{j+1})$ for $j = 0,\ 1,\ \ldots,\ k-1$. We shall not provide any proof, but we will nevertheless state some of the basic results of the theory, which is known as the *Brun combinatorial sieve* or sometimes simply as the *Brun sieve*.

**Theorem 12.6.** *With the notations of Corollary* 12.2*, assume that there exists a nonnegative multiplicative function $w$, some real number $X$ and positive constants $\kappa$ and $A$ such that*

$$\text{(i)}\ \ \mathcal{A}_d = X\frac{w(d)}{d} + R_d \qquad (d \mid P(y)),$$

$$\text{(ii)}\ \ \prod_{\eta\le p\le\zeta}\left(1-\frac{w(p)}{p}\right)^{-1} < \left(\frac{\log\zeta}{\log\eta}\right)^{\kappa}\left(1+\frac{A}{\log\eta}\right) \qquad (2\le\eta\le\zeta).$$

*Then, uniformly for $\mathcal{A}, X, y, u \ge 1$,*

$$\text{(12.12)}\ \ \mathcal{S}(\mathcal{A},\mathcal{P},y) = X\prod_{\substack{p\le y\\ p\in\mathcal{P}}}\left(1-\frac{w(p)}{p}\right)\{1+O(u^{-u/2})\}+O\left(\sum_{\substack{d\le y^u\\ d\mid P(y)}}|R_d|\right).$$

In the rest of this chapter, we shall give several applications of Theorem 12.6.

## 12.5. A Chebyshev type estimate

Choose $\mathcal{A} = \{n \le x\}$, $\mathcal{P}$ to be the set of all primes and $X = x$. Then (i) of Theorem 12.6 holds with $w(d) = 1$ for all $d \mid P(y)$ and $|R_d| \le 1$. To see that (ii) holds, use the fact that

$$\prod_{p\le z}\left(1-\frac{1}{p}\right) = \frac{c}{\log z}\left(1+O\left(\frac{1}{\log z}\right)\right)$$

for some constant $c > 0$ with $z = \eta$ and then with $z = \zeta$ and divide the two resulting relations to get that

(12.13)
$$\begin{aligned}\prod_{\eta\le p\le\zeta}\left(1-\frac{w(p)}{p}\right)^{-1} &= \prod_{\eta\le p\le\zeta}\left(1-\frac{1}{p}\right)^{-1}\\ &= \frac{(c/\log\eta)^{-1}}{(c/\log\zeta)^{-1}}\left(1+O\left(\frac{1}{\log\eta}\right)\right)^{-1}\left(1+O\left(\frac{1}{\log\zeta}\right)\right)\\ &= \frac{\log\zeta}{\log\eta}\left(1+O\left(\frac{1}{\log\eta}\right)\right)\left(1+O\left(\frac{1}{\log\zeta}\right)\right)\\ &= \frac{\log\zeta}{\log\eta}\left(1+O\left(\frac{1}{\log\eta}+\frac{1}{\log\zeta}\right)\right)\\ &= \frac{\log\zeta}{\log\eta}\left(1+O\left(\frac{1}{\log\eta}\right)\right),\end{aligned}$$

so that condition (ii) holds for some $A > 0$ with $\kappa = 1$. Now let $c_1$ be the constant implied by the $O$ in (12.12) and let $u > 0$ be a constant such that $u^{u/2} > 2c_1$. Then the quantity $O(u^{-u/2})$ in (12.12) is in absolute value at most $c_1/u^{u/2} < 1/2$, so that the main term in (12.12) is $> \frac{x}{2}\prod_{p\le y, p\in\mathcal{P}}(1 - 1/p)$. Now choose $y$ such that $y^u \le x^{1/2}$. Clearly, we may choose $y = x^{1/2u}$. Then the error term is $\ll y^u \le x^{1/2}$, and so we get that

$$\mathcal{S}(\mathcal{A},\mathcal{P},y) = x\prod_{p\le x^{1/2u}}\left(1-\frac{1}{p}\right)+O(x^{1/2}).$$

Since

$$\prod_{p\le x^{1/2u}}\left(1-\frac{1}{p}\right) = \frac{c}{\log(x^{1/2u})}\left(1+O\left(\frac{1}{\log(x^{1/2u})}\right)\right) = \frac{2cu}{\log x}(1+o(1))$$

as $x\to\infty$ and since $u$ is a constant, we get, in particular, that

$$\pi(x) \le \pi(y) + \mathcal{S}(\mathcal{A},\ \mathcal{P}, y) \ll \frac{x}{\log x},$$

a Chebyshev type estimate (see Section 2.6 in Chapter 2).

## 12.6. The Brun-Titchmarsh theorem

Let $1 \le a < b$ be integers with $(a, b) = 1$. Let $\pi(x; b, a) = \#\{p \le x : p \equiv a \pmod b\}$. The following inequality is known as the *Brun-Titchmarsh inequality* or at times as the *Brun-Titchmarsh theorem.*

**Theorem 12.7.** *The inequality*

$$\pi(x;b,a) - \pi(x-z;b,a) \ll \frac{z}{\phi(b)\log(z/b)}$$

*holds uniformly for* $1 \le b < z \le x$ *and* $1 \le a < b$ *such that* $(a,b) = 1$. *The implied constant in the above* $\ll$ *symbol is absolute.*

**Proof.** We choose $\mathcal{A} = \{bm + a \in [x-z, x]\}$. We note that the numbers in $\mathcal{A}$ are always coprime with the primes $p \mid b$. We let $\mathcal{P} = \{p \le y : \ p \nmid b\}$, where $y < z$ will be chosen later. Since $x - z > 0$, it follows that any number $m \in [x-z, x]$ which is congruent to $a \pmod b$ is in $\mathcal{A}$, and if it is prime then it is coprime with all the primes $p \in \mathcal{P}$. Note that if $q \in \mathcal{P}$, then there is only one number $m \in \{0, 1, \dots, q-1\}$ such that $bm + a \equiv 0 \pmod q$. (This $m$ is the congruence class of $-ab^{-1} \pmod q$.) Thus, $w(d) = 1$ if $d \mid P(y)$. Furthermore, if $d$ is coprime to $m$ and $d \mid bm + a$, then $m = m_0 + d\ell$, where $m_0 \in \{0, 1, \dots, d-1\}$ is the smallest nonnegative solution of the congruence $bm + a \equiv 0 \pmod d$. Thus, $bm + d = bd\ell + (bm_0 + a)$. The number of such numbers which are also in the interval $[x-z, x]$ is $\lfloor z/bd \rfloor + O(1)$. Hence, by applying Theorem 12.6(i),

$$\mathcal{A}_d = \frac{z}{b}\frac{w(d)}{d} + R_d,$$

where $|R_d| \le 1$ and this is true for all $d \mid P(y)$. Thus, we may choose $X = z/b$. Clearly,

$$\begin{aligned}\prod_{\substack{\eta \le p \le \zeta \\ p \in \overline{\mathcal{P}}}} \left(1 - \frac{w(p)}{p}\right)^{-1} &= \prod_{\substack{\eta \le p \le \zeta \\ p \nmid b}} \left(1 - \frac{1}{p}\right)^{-1} \le \prod_{\eta \le p \le \zeta} \left(1 - \frac{1}{p}\right)^{-1} \\ &\le \frac{\log \zeta}{\log \eta}\left(1 + O\left(\frac{1}{\log \eta}\right)\right),\end{aligned}$$

where the last inequality follows from (12.13). Thus, we may apply Theorem 12.6. Again, we choose some sufficiently large $u$ such that the expression $1 + O(u^{-u/2})$ is in $(1/2, 3/2)$. Fixing the value of $u$ in this range, we choose $y$ such that $y^u \le X^{1/2}$. This means that we may choose $y = X^{1/(2u)} = (z/b)^{1/2u}$. With these choices, the error term in Theorem 12.6 is $\ll X^{1/2} \ll (z/b)^{1/2}$, while the main term is

$$\begin{aligned}\mathcal{S}(\mathcal{A}, \mathcal{P}, y) &\ll X \prod_{p \in \mathcal{P}(y)} \left(1 - \frac{1}{p}\right) \\ &= \frac{z}{b} \prod_{p \le y} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \le y \\ p \mid b}} \left(1 - \frac{1}{p}\right)^{-1} \\ &\ll \frac{z}{b}\frac{b}{\phi(b)}\frac{1}{\log y} = \frac{z}{\phi(b)}\frac{2u}{\log(z/b)} \\ &\ll \frac{z}{\phi(b)\log(z/b)}.\end{aligned}$$

To summarize,

$$\pi(x;b,a) - \pi(x-z;b,a) \ll \frac{z}{\phi(b)\log(z/b)} + \Big(\frac{z}{b}\Big)^{1/2}.$$

Let $c_0$ be such that $t^{1/2} > \log t$ for $t > c_0$. If $z/b > c_0$, then, since $\phi(b) \le b$, we have

$$\frac{z}{\phi(b)\log(z/b)} \ge \frac{z}{b\log(z/b)} \ge \Big(\frac{z}{b}\Big)^{1/2},$$

so that

$$\pi(x;b,a) - \pi(x-z;b,a) \ll \frac{z}{\phi(b)\log(z/b)},$$

which is what we wanted to prove. If on the other hand $z/b \le c_0$, then $[x, x-z]$ contains at most $z/b+1 \le c_0+1$ numbers congruent to $a \pmod b$, implying that the desired inequality is true with some appropriate implied constant anyway. This completes the proof of the theorem. □

## 12.7. Twin primes revisited

Again let $\mathcal{J}(x) = \#\{p \le x \ : \ p,\ p+2 \text{ are both primes}\}$. Brun's combinatorial sieve gives the following result.

**Theorem 12.8.** *The estimate*

$$\mathcal{J}(x) \ll \frac{x}{(\log x)^2}$$

*holds.*

**Proof.** We only sketch the proof. Again we choose $\mathcal{A} = \{n(n+2) \ : \ n \le x\}$, we let $y \le x$ be a number which will be chosen later and we set $\mathcal{P} = \{p \le y\}$. From the proof of Proposition 12.4, we know that

$$\mathcal{A}_d = x\frac{w(d)}{d} + R_d,$$

where $w(d)$ is the multiplicative function with $w(2) = 1$ and $w(p) = 2$ if $p$ is an odd prime and $|R(d)| \le 2^{\omega(d)}$. It is easy to check that (ii) holds with $\kappa = 2$. We then apply the Brun combinatorial sieve. Note that the error term is $O(y^{2u})$, because $|R_d| \le 2^{\omega(d)} \ll d$ for all $d \le y^u$. Thus, we may choose $y = x^{1/4u}$, where $u > 0$ is an absolute constant and the error term is $O(x^{1/2})$. Hence, we get that

$$\mathcal{J}(x) \ll x\prod_{p\le y}\left(1 - \frac{2}{p}\right) + x^{1/2},$$

and the calculation used in the proof of Proposition 12.4 shows that

$$\prod_{p\le y}\left(1-\frac{2}{p}\right) \ll \frac{1}{(\log y)^2} = \frac{1}{(\log(x^{1/4u}))^2} \ll \frac{1}{(\log x)^2},$$

which completes the proof of the theorem. □

## 12.8. Smooth shifted primes

In this section, we prove the following result.

**Theorem 12.9.** *There exists a positive number $\rho < 1$ such that*

$$\#\{p \le x : P(p-1) < x^\rho\} \gg \frac{x}{\log x}.$$

**Proof.** Let $\rho = 1-\varepsilon$, where $\varepsilon > 0$ is fixed and assume that $P(p-1) > x^\rho$. Then $p-1 = aq$, where $q$ is a prime and $a < x^\varepsilon$. Fix $a$. Then $q < x/a$ is a prime such that $aq+1$ is also a prime. We use the Brun sieve to estimate the number of such primes $q$. Take $\mathcal{A}_a = \{n(an+1) \ : \ n \le x/a\}$ and $\mathcal{P} = \{p \le y\}$, where $y$ will be suitably chosen. It is easy to show (and we already did it several times by now) that if we write $w(d)$ for the number of solutions of $n(an+1) \equiv 0 \pmod d$ in $\{0,1,\dots,d-1\}$, then $w(d)$ is a multiplicative function (see, for example, Problem 12.4). When $d$ is a prime, we have that $w(p) = 2$ if $p \nmid a$ and $w(p) = 1$ otherwise. Thus, condition (i) of Theorem 12.6 is satisfied with $|R_d| \le 2^{\omega(d)}$. One easily checks that condition (ii) is also satisfied with $\kappa = 2$ uniformly in $a$. Thus, one may apply Theorem 12.6 and get that, choosing $y < (x^{1/2})^{1/2u} < (x/a)^{1/2u}$ if $\varepsilon < 1/2$,

$$\begin{aligned}
\mathcal{S}(\mathcal{A}_a,\mathcal{P},y) &\ll \frac{x}{a}\prod_{2\le p\le y}\left(1-\frac{w(p)}{p}\right)\\
&\ll \frac{x}{a}\left(\frac{a}{\phi(a)}\right)\prod_{2\le p\le y}\left(1-\frac{1}{p}\right)^2\\
&\ll \frac{x}{\phi(a)}\frac{1}{(\log(x/a))^2}.
\end{aligned}$$

Since $a < x^{1/2}$, or $x/a > x^{1/2}$, it follows that

$$\mathcal{S}(\mathcal{A}_a,\mathcal{P},y) \ll \frac{x}{\phi(a)}\frac{1}{(\log x)^2}.$$

Summing up over all $a \le x^\varepsilon$, we get

$$\#\{p \le x \ : \ P(p-1) > x^{1-\varepsilon}\} \le \sum_{a\le x^\varepsilon}\mathcal{S}(\mathcal{A}_a,\mathcal{P},y) \ll \frac{x}{(\log x)^2}\sum_{a\le x^\varepsilon}\frac{1}{\phi(a)}.$$

Using the estimate (see Problem 12.9)

$$\sum_{a\le t}\frac{1}{\phi(a)} \ll \log t, \tag{12.14}$$

which is valid for all $t \ge 2$, we get that

$$\#\{p \le x \ : \ P(p-1) > x^{1-\varepsilon}\} \ll \frac{x\log(x^{\varepsilon})}{(\log x)^2} \ll \frac{\varepsilon x}{\log x}.$$

Hence, let $c$ be the constant implied above. Then there are at most $c\varepsilon x/\log x$ primes $p \le x$ such that $P(p-1) > x^{1-\varepsilon}$. Choosing $\varepsilon = 1/2c$, we get that there are $\pi(x) - x/(2\log x) \ge x/(3\log x)$ primes $p \le x$ (for $x > x_0$) such that $P(p-1) < x^{1-1/2c}$, which is what we wanted to prove, with $\rho = 1 - 1/2c$.

□

The result proved in Theorem 12.9 has a rich history. Under the present form it was proved by Erdős [**47**] in 1935. He was 25 years old. Subsequently, many mathematicians obtained specific values of $\rho$ for which Theorem 12.9 holds. These include C. Pomerance ($\rho = 0.48$), J. Friedlander [**61**] ($\rho = 1/2\sqrt{e} \approx 0.303$), and others. The current record-holders are Baker and Harman [**4**] with $\rho = 0.2936$. It is believed that Theorem 12.9 holds with any $\rho > 0$. In the opposite direction, Fouvry [**60**] showed that

$$\#\{p \le x \ : \ P(p-1) \ge x^{2/3}\} \gg \frac{x}{\log x}.$$

It is believed that the above estimate holds with $2/3$ replaced by $1-\varepsilon$ for any fixed $\varepsilon > 0$.

## 12.9. The Goldbach conjecture

Goldbach conjectured that every even positive integer $\ge 4$ is a sum of two primes. This problem is called the *Goldbach conjecture* and at times the *Goldbach problem*. Let $n$ be an even positive integer and write

$$T(n) = \#\{p \le n \ : \ n-p \text{ is prime}\}. \tag{12.15}$$

While we cannot prove that $T(n) > 0$ for all each integer $n > 2$, we can, however, obtain an upper bound for $T(n)$.

**Theorem 12.10.** *The inequality*

$$T(n) \ll \frac{n}{(\log n)^2}\prod_{p\,|\,n}\left(1+\frac{1}{p}\right)$$

*holds.*

**Proof.** We apply the Brun combinatorial sieve to the set $\mathcal{A} = \{m(n-m) \ : \ m \le n\}$. Let $X = n$. It is easy to check that one can take $w(p) = 2$ if $p \nmid n$ and $w(p) = 1$ if $p \mid n$. Hence, by the Brun sieve, one gets

$$T(n) \ll n \left(\frac{n}{\phi(n)}\right) \frac{1}{(\log n)^2},$$

and noticing that

$$\frac{n}{\phi(n)} = \frac{\gamma(n)}{\phi(\gamma(n))} \ll \frac{\sigma(\gamma(n))}{\gamma(n)} = \prod_{p \mid n} \left(1 + \frac{1}{p}\right),$$

the proof of the theorem is complete. □

It is conjectured that there exists a positive constant $C_2$ such that

$$\begin{aligned} T(N) &= \#\{p, q \ : \ p + q = N\} = 2C_2(1 + o(1)) \left(\prod_{\substack{p \mid N \\ p > 2}} \frac{p-1}{p-2}\right) \int_2^N \frac{dt}{(\log t)^2} \\ &= 2C_2(1 + o(1)) \frac{N}{(\log N)^2} \left(\prod_{\substack{p \mid N \\ p > 2}} \frac{p-1}{p-2}\right) \end{aligned}$$

as $N \to \infty$. It is known that this is true for all even $N \le x$ with a set of possible exceptions (called the exceptional Goldbach set) of cardinality $O(x^\delta)$ for some constant $\delta > 0$. Recent work of Li [**97**] shows that $\delta = 0.921$ is acceptable. As far as statements which are valid for all integers go, Chen [**23**] proved that every sufficiently large even integer $n$ can be written in the form $n = p + q$, where $p$ is prime and $q \in P_2$ (recall that a positive integer $m$ is a $P_k$ if $\Omega(m) \le k$). In fact, Chen proved much more. Here is a widely applicable version of Chen's theorem.

**Theorem 12.11.** *(Chen Theorem) Given an arbitrary positive even integer $a$, there exists $x_0 = x_0(a)$ such that for each $x > x_0(a)$, the interval $[x/2, x]$ contains a number $\gg x/(\log x)^2$ of primes $p$ such $(p+1)/2a$ is an integer which is either a prime or a product of two primes each exceeding $x^{1/10}$.*

In fact, Chen proved it for $(p+1)/(2a)$ replaced by $N - p$, where $N = x$ is an even integer.

## 12.10. The Schnirelman theorem

**Definition 12.12.** *Let $\mathcal{A} = \{a_1, a_2, \ldots\}$ be a set of nonnegative integers and let $\mathcal{A}(x) = \#(\mathcal{A} \cap [1, x])$. Then*

$$\sigma(\mathcal{A}) = \inf_{n \geq 1} \frac{\mathcal{A}(n)}{n}$$

*is called the Schnirelman density of $\mathcal{A}$.*

If $\mathcal{A}$ and $\mathcal{B}$ are subsets of the set of real numbers, we let $\mathcal{A} + \mathcal{B} = \{a + b \ : \ a \in \mathcal{A},\ b \in \mathcal{B}\}$.

**Lemma 12.13.** *If $\mathcal{A}$ and $\mathcal{B}$ are sets of nonnegative integers with $1 \in \mathcal{A}$ and $0 \in \mathcal{B}$, then*

$$\sigma(\mathcal{A} + \mathcal{B}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B}).$$

**Proof.** Our proof is the one attributed to Schnirelman and appearing in Nathanson's book [**111**] (Theorem 7.5, page 193).

Let $n$ be a fixed positive integer, let $a_1 < a_2 < \cdots$ be all the elements of $\mathcal{A}$, and assume that $\mathcal{A}(n) = r$. Divide $[1, n]$ into intervals $[a_i, a_{i+1})$ for $i = 1, \ldots, r-1$ and $[a_r, n]$. All numbers of the form $a_i + t$ with $1 \leq t \leq a_{i+1} - a_i - 1$ are in $\mathcal{A} \cap [a_i, a_{i+1})$ together with the numbers $a_i$ since $0 \in \mathcal{B}$. Thus,

$$\begin{aligned}
(\mathcal{A} + \mathcal{B})(n) &\geq \sum_{i=1}^{r-1} (\mathcal{B}(a_{i+1} - a_i - 1) + 1) + \mathcal{B}(n - a_r) + 1 \\
&\geq r + \left( \sum_{i=1}^{r-1} (a_{i+1} - a_i - 1) + n - a_r \right) \sigma(\mathcal{B}) \\
&= r + (n - r)\sigma(\mathcal{B}) = \mathcal{A}(n)(1 - \sigma(\mathcal{B})) + n\sigma(\mathcal{B}) \\
&\geq n(\sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B})),
\end{aligned}$$

which implies the desired inequality. □

**Lemma 12.14.** *Let $\mathcal{A}$ and $\mathcal{B}$ be sets of nonnegative integers such that $0 \in \mathcal{A} \cap \mathcal{B}$ and $\sigma(\mathcal{A}) + \sigma(\mathcal{B}) \geq 1$. Then $\sigma(\mathcal{A} + \mathcal{B}) = 1$, that is, $\mathcal{A} + \mathcal{B}$ is the set of all nonnegative integers.*

**Proof.** If $1 \notin \mathcal{A}$ then $\sigma(\mathcal{A}) = 0$, so that $\sigma(\mathcal{B}) = 1$ and we are done. Thus, assume that $1 \in \mathcal{A}$. Assume that there exists a natural number $n \notin \mathcal{A} + \mathcal{B}$. Since $0 \in \mathcal{B}$, we get that $n \notin \mathcal{A}$. But then

$$\mathcal{A}(n-1) = \mathcal{A}(n) \geq n\sigma(\mathcal{A}) > (n-1)\sigma(\mathcal{A})$$

and

$$\mathcal{B}(n-1) \geq (n-1)\sigma(\mathcal{B}),$$

so that

$$\mathcal{A}(n-1)+\mathcal{B}(n-1) > (n-1)(\sigma(\mathcal{A})+\sigma(\mathcal{B})) \geq n-1,$$

giving

$$\mathcal{A}(n-1)+\mathcal{B}(n-1) \geq n.$$

Let $a_1 < \cdots < a_r$ and $b_1 < \cdots < b_s$ be all the members of $\mathcal{A}$ and of $\mathcal{B}$ that are $\leq n-1$, respectively. Then the $r+s$ integers $a_1, \ldots, a_r, n-b_1, \ldots, n-b_s$ are all positive and $< n$. Since there are $r+s \geq n$ of these numbers, by the Pigeon Hole principle, two of them must coincide, so that there must exist $i$ and $j$ such that $a_i = n-b_j$. Thus, $n = a_i + b_j \in \mathcal{A}+\mathcal{B}$, which is the desired contradiction. □

**Definition 12.15.** *A set $\mathcal{A}$ consisting of some positive integers and 0 is called a base of order $c$ if*

$$\underbrace{\mathcal{A}+\cdots+\mathcal{A}}_{c \text{ times}}$$

*consists of all the nonnegative integers. That is, every positive integer is a sum of at most $c$ terms from $\mathcal{A}$.*

**Lemma 12.16.** *If $\sigma(\mathcal{A}) > 0$, then $\mathcal{A}$ is a base of finite order.*

**Proof.** Let $\mathcal{A}_2 = \mathcal{A}+\mathcal{A}$ and define recursively $\mathcal{A}_r = \mathcal{A}+\mathcal{A}_{r-1}$ for all $r \geq 3$. Let $\alpha = \sigma(\mathcal{A})$. By Lemma 12.13,

$$\sigma(\mathcal{A}_2) \geq 2\alpha - \alpha^2 = 1-(1-\alpha)^2.$$

By induction, one can show that, for all integers $r \geq 2$,

$$\sigma(\mathcal{A}_r) \geq 1-(1-\alpha)^r,$$

where the induction step is based on Lemma 12.13 with $\mathcal{B} = \mathcal{A}_r$. Since $\alpha > 0$, there exists $r$ such that $(1-\alpha)^r < 1/2$. Then $\sigma(\mathcal{A}_r) > 1/2$, so that Lemma 12.14 shows that $\mathcal{A}_{2r} = \mathcal{A}_r + \mathcal{A}_r$ contains all the nonnegative integers. □

We can now prove Schnirelman's theorem.

**Theorem 12.17.** *(Schnirelman) There exists a constant $c > 0$ such that every integer $n \geq 2$ is a sum of at most $c$ primes.*

**Proof.** We start by showing that the set $\mathcal{Q}$ consisting of 0, 1 and the numbers which are a sum of two primes has a positive Schnirelman density. Let

$$\mathcal{Q}(x) = \{m \leq x \ : \ m \in \mathcal{Q}\}.$$

By the Cauchy-Schwarz inequality (see (1.20)), we get that, with $T(n)$ defined in (12.15),

(12.16)
$$\left(\sum_{n\le x} T(n)\right)^2 \le \left(\sum_{n\le x} T^2(n)\right)\left(\sum_{m\in\mathcal{Q}(x)} 1\right) \le \left(\sum_{n\le x} T^2(n)\right) \times \#\mathcal{Q}(x).$$

Note that for $x \ge 4$,

$$\sum_{n\le x} T(n) \ge \sum_{p_1,p_2\le x/2} 1 = \pi(x/2)^2 \gg \frac{x^2}{(\log x)^2}, \tag{12.17}$$

while by Theorem 12.10 and the inequality

$$[d_1,d_2]^2 \ge [d_1,d_2](d_1,d_2) = d_1d_2,$$

which implies that $[d_1,d_2] \ge (d_1d_2)^{1/2}$, we have

$$\begin{aligned}\sum_{n\le x} T^2(n) &\ll \frac{x^2}{(\log x)^4}\sum_{n\le x}\prod_{p\mid n}\left(1+\frac{1}{p}\right)^2\\ &\ll \frac{x^2}{(\log x)^4}\sum_{n\le x}\left(\sum_{d\,\mid\, n}\frac{1}{d}\right)^2\\ &= \frac{x^2}{(\log x)^4}\sum_{n\le x}\left(\frac{\sigma(n)}{n}\right)^2\\ &\ll \frac{x^3}{(\log x)^4},\end{aligned} \tag{12.18}$$

where we used the second estimate of Problem 8.10.

Inserting both the lower bound (12.17) and the upper bound (12.18) into inequality (12.16), we get

$$\frac{x^4}{(\log x)^4} \ll \#\mathcal{Q}(x)\frac{x^3}{(\log x)^4},$$

giving $\#\mathcal{Q}(x) \gg x$. Now Lemma 12.16 tells us that there exists a constant $c$ such any positive integer $n$ is of the form $a_1+\cdots+a_i$ for some $i \le c' \le c$, where $a_i = 1$ or $a_i$ is a prime. Now let $m \ge 2$ be an integer. Applying what we concluded above for $m-2$, we get

$$m-2 = \sum_{i\le k} 1 + \sum_{k<i\le c'} p_i,$$

where the $p_i$'s are some primes. If $k = 0$ or $k = 1$, then

$$m = p + \sum_{k<i\le c'} p_i,$$

where $p = 2,\ 3$, while if $k \ge 2$, we then write

$$k = \underbrace{2 + \cdots + 2}_{\kappa \text{ times}} + \underbrace{3 + \cdots + 3}_{\ell \text{ times}}$$

for some nonnegative integers $\kappa,\ \ell$ with $\kappa + \ell < k$, and we still get that

$$m = \underbrace{2 + \cdots + 2}_{\kappa+1 \text{ times}} + \underbrace{3 + \cdots + 3}_{\ell \text{ times}} + \sum_{k<i\le c'} p_i$$

is a sum of at most $c' \le c$ primes, which is what we wanted to prove. □

Schnirelman showed that $c = 300\,000$ is acceptable in Theorem 12.17. While the Goldbach problem is out of reach, Vinogradov proved in 1937 the following remarkable theorem.

**Theorem 12.18.** *Let $r(N)$ be the number of prime triplets $(p, q, r)$ such that $N = p + q + r$. Then, as $N \to \infty$,*

$$r(N) = \frac{C_3}{2}(1 + o(1))\frac{N^2}{(\log N)^3} \prod_{p \mid N} \left(1 - \frac{1}{p^2 - 3p + 3}\right),$$

*where*

$$C_3 = \prod_{p \ge 2} \left(1 + \frac{1}{(p-1)^3}\right).$$

Hence, in particular, every large odd positive integer is a sum of three primes.

As we mentioned before, it is not known that both $p$ and $p+2$ are primes infinitely often. It is also not known that $n^2 + 1$ is prime infinitely often. Each prime $p \equiv 1 \pmod 4$ is a sum of two squares, so that $a^2 + b^2$ is a prime infinitely often. A few years ago, J. Friedlander and H. Iwaniec [**62**] obtained the following fascinating result:

**Theorem 12.19.** *There exists a constant $\kappa > 0$ such that*

$$\#\{n \le x \ :\ n = a^2 + b^4 \text{ for some integers } a \text{ and } b\} = \kappa(1 + o(1))\frac{x^{3/4}}{\log x}$$

*as $x \to \infty$.*

In particular, the polynomial $X^2 + Y^4$ represents infinitely many primes. The method of Friedlander and Iwaniec was suitably adapted by Heath-Brown [**79**] to yield infinitely many primes of the form $X^3 + 2Y^3$. Before this, it was unknown if there were infinitely many primes of the form $a^3 + b^3 + c^3$ with positive integers $a$, $b$ and $c$. These theorems are among the highest achievements nowadays in sieve methods. We will not prove any of them, but rather discuss another elementary sieve, namely Selberg's sieve.

## 12.11. The Selberg sieve

The Selberg sieve is an upper bound sieve which is remarkable by the simplicity of its basic idea. Assume, for simplicity, that $\mathcal{A} = \{h(n) : n \le x\}$ where $h(X) \in \mathbb{Z}[X]$ is a nonconstant polynomial. Let $w(d) = \#\{0 \le n \le d-1 \ : \ h(n) \equiv 0 \pmod d\}$, let $\mathcal{P}$ be a set of primes and put $P(y) = \prod_{\substack{p \le y \\ p \in \mathcal{P}}} p$. Assume that $1 \le w(p) < p$ for all $p \mid P(y)$. Let

$$\mathcal{A}_d = x\frac{w(d)}{d} + R(d),$$

where $|R_d| \le w(d)$. Recall that in order to get an upper bound on $\mathcal{S}(\mathcal{A}, \mathcal{P}, y)$ we need to find some multiplicative function $\lambda(d)$, such that

$$\sum_{d|(n,P(y))} \mu(d) \le \sum_{d|(n,P(y))} \lambda(d) \tag{12.19}$$

and once the above inequality is true for all positive integers $n$, the arguments from Section 1 (the sieve of Eratosthenes) show that

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, y) \le x \sum_{d \,|\, P(y)} \frac{\lambda(d)w(d)}{d} + \sum_{d \,|\, P(y)} \lambda(d)R(d). \tag{12.20}$$

Selberg's idea was to let $\Phi$ be some multiplicative function and to define $\lambda(d)$ via

$$\sum_{d \,|\, (n,P(y))} \lambda(d) = \left( \sum_{d \,|\, (n,P(y))} \Phi(d) \right)^2, \tag{12.21}$$

in which case inequality (12.19) holds because its right-hand side is always $\ge 0$ and it is 1 if $(n, P(y)) = 1$ because $\Phi(1) = 1$. This suggests defining

$$\lambda(d) = \sum_{\substack{d_1, d_2 | P(y) \\ d = [d_1, d_2]}} \Phi(d_1)\Phi(d_2)$$

and $\lambda(p) = 0$ if $p \nmid P(y)$, in which case identity (12.21) is clearly satisfied. In order to optimize the result, Selberg went on to find $\Phi$ in such a way that the main term in (12.20) is optimal, that is, is as small as possible. Remarkably, the function $\Phi$ that optimizes this problem exists, is unique, and can be computed. For this, put $f(d) = d/w(d)$ for all $d \mid P(y)$ and let

$$g(k) = f(k) \prod_{p \,|\, k} \left(1 - \frac{w(p)}{p}\right) \qquad (k \mid P(y)).$$

Note that $g(k) > 0$ for all $k \mid P(y)$, and since all $k$'s under scrutiny are squarefree and $f$ is multiplicative, we get that if $d \mid k$, then $d$ and $k/d$ are

coprime, so that $f(k) = f(d(k/d)) = f(d)f(k/d)$, and therefore

$$g(k) = f(k)\prod_{p\,|\,k}\left(1 - \frac{1}{f(p)}\right) = \sum_{d\,|\,k}\mu(d)\frac{f(k)}{f(d)} = \sum_{d\,|\,k}\mu(d)f\left(\frac{k}{d}\right).$$

Thus, $g = \mu * f$, that is,

$$f(k) = \sum_{d\,|\,k} g(d).$$

Note also that since $(d_1, d_2)[d_1, d_2] = d_1 d_2$, we have that

$$f([d_1, d_2]) = f\left(d_1\left(\frac{d_2}{(d_1, d_2)}\right)\right) = f(d_1)f\left(\frac{d_2}{(d_1, d_2)}\right) = \frac{f(d_1)f(d_2)}{f((d_1, d_2))},$$

so that

$$\frac{1}{f([d_1, d_2])} = \frac{1}{f(d_1)f(d_2)}f((d_1, d_2)) = \frac{1}{f(d_1)f(d_2)}\sum_{d|(d_1,d_2)} g(d).$$

Selberg then sets

$$Q = \sum_{d\,|\,P(y)}\frac{1}{g(d)} = \sum_{d\,|\,P(y)}\frac{w(d)}{d}\prod_{p\,|\,d}\left(1 - \frac{w(p)}{p}\right)^{-1},$$

and proves the following theorem.

**Theorem 12.20.** *Let $\Phi$ be a multiplicative function with $\Phi(p) = 0$ if $p \nmid P(y)$. Set*

$$\lambda(d) = \sum_{\substack{d_1, d_2 | P(y)\\ [d_1,d_2]=d}} \Phi(d_1)\Phi(d_2)$$

*and let $\lambda(d) = 0$ if $d \nmid P(y)$. Then*

$$\sum_{d\,|\,P(y)}\frac{\lambda(d)}{f(d)} \geq \frac{1}{Q}, \tag{12.22}$$

*with equality if and only if*

$$\Phi(d) = \frac{1}{Q}\mu(d)f(d)\sum_{t|d}\frac{1}{g(t)} \qquad (d \mid P(y)).$$

**Proof.** Let $H(\Phi)$ be the expression appearing on the left-hand side of inequality (12.22). Then

$$\begin{aligned} H(\Phi) &= \sum_{d_1,d_2|P(y)}\frac{\Phi(d_1)\Phi(d_2)}{f([d_1, d_2])} = \sum_{d_1,d_2|P(y)}\frac{\Phi(d_1)}{f(d_1)}\frac{\Phi(d_2)}{f(d_2)}\sum_{t|(d_1,d_2)} g(t)\\ &= \sum_{t\,|\,P(y)} g(t)\sum_{\substack{d_1\,|\,P(y),\ d_2\,|\,P(y)\\ t\,|\,d_1,\ t\,|\,d_2}}\frac{\Phi(d_1)\Phi(d_2)}{f(d_1)f(d_2)} \end{aligned}$$

$$= \sum_{t \mid P(y)} g(t) \left( \sum_{\substack{d \mid P(y) \\ t \mid d}} \frac{\Phi(d)}{f(d)} \right)^2 .$$

Choose

$$y(t) = \sum_{\substack{d \mid P(y) \\ t \mid d}} \frac{\Phi(d)}{f(d)}$$

and observe that

$$\Phi(d) = f(d) \sum_{\substack{t \mid P(y) \\ d \mid t}} \mu\left(\frac{t}{d}\right) y(t). \tag{12.23}$$

Setting $d = 1$, we get $1 = \sum_{t \mid P(y)} \mu(t) y(t)$. Hence,

$$\begin{aligned} H(\Phi) &= \sum_{t \mid P(y)} g(t) y^2(t) \\ &= \sum_{t \mid P(y)} g(t) y^2(t) - \frac{2}{Q} \sum_{t \mid P(y)} \mu(t) y(t) + \frac{1}{Q^2} \sum_{t \mid P(y)} \frac{\mu^2(t)}{g(t)} + \frac{1}{Q} \qquad (12.24) \\ &= \sum_{t \mid P(y)} \frac{1}{g(t)} \left( g(t) y(t) - \frac{\mu(t)}{Q} \right)^2 + \frac{1}{Q}. \end{aligned}$$

Thus, $H(\Phi) \geq 1/Q$, which is what we wanted to prove. It remains to be seen when the minimum is achieved. In fact, it is clear from (12.24) that the minimum is obtained precisely when

$$y(t) = \frac{\mu(t)}{Q g(t)}.$$

Substituting this value in (12.23), we get

$$\Phi(d) = \frac{f(d)}{Q} \sum_{\substack{t \mid P(y) \\ d \mid t}} \frac{\mu(t)}{g(t)} \mu\left(\frac{t}{d}\right) = \frac{f(d)\mu(d)}{Q} \sum_{\substack{t \mid P(y) \\ d \mid t}} \frac{1}{g(t)}, \tag{12.25}$$

which is the other result we needed to prove. □

Using the above result, we get the following sieving result.

**Theorem 12.21.** *With the notations from the preceding theorem,*

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, y) \leq \frac{x}{Q} + y^2 \prod_{p \mid P(y)} \left(1 - \frac{w(p)}{p}\right)^{-2}.$$

**Proof.** The main term is easy to obtain. It remains to bound

$$R = \sum_{d_1,d_2|P(y)} |\Phi(d_1)\Phi(d_2)R([d_1,d_2])|.$$

But, in light of (12.25),

$$|\Phi(d)| = \frac{f(d)}{Q} \sum_{\substack{t|\,P(y)\\ d\,|\,t}} \frac{1}{g(t)} \le \frac{f(d)}{g(d)Q} \sum_{k\,|\,P(y)} \frac{1}{g(k)} \le \frac{f(d)}{g(d)}$$

and since

$$|R([d_1,d_2])| \le \frac{[d_1,d_2]}{f([d_1,d_2])} = \frac{d_1d_2}{(d_1,d_2)} \cdot \frac{f((d_1,d_2))}{f(d_1)f(d_2)} \le \frac{d_1}{f(d_1)} \frac{d_2}{f(d_2)},$$

we get that

$$\begin{aligned} R &\le \sum_{d_1,d_2\,|\,P(y)} \frac{f(d_1)}{g(d_1)} \frac{f(d_2)}{g(d_2)} \frac{d_1}{f(d_1)} \frac{d_2}{f(d_2)} \\ &\le \left( \sum_{d\,|\,P(y)} \frac{d}{g(d)} \right)^2 \le y^2Q^2, \end{aligned}$$

while it is clear that

$$Q \le \prod_{p\le y} \left(1 + \frac{1}{g(p)}\right).$$

Finally, since

$$1 + \frac{1}{g(p)} = 1 + \frac{1}{f(p)-1} = \left(1 - \frac{1}{f(p)}\right)^{-1} = \left(1 - \frac{w(p)}{p}\right)^{-1},$$

the desired estimate follows. □

## 12.12. The Brun-Titchmarsh theorem from the Selberg sieve

At this point, it is illuminating to explain how one can deduce the Brun-Titchmarsh theorem from the Selberg sieve. Let $h(n) = a + bn$, and assume that $bn + a \le x$. Then $n \le \lfloor x/b \rfloor + 1 \le 2x/b$ for $b < x$. Let $y$ be a parameter to be fixed later. Note that $\mathcal{P} = \{p : p \nmid b\}$ and that $w(p) = 1$ for all $p \mid P(y)$. Thus, $f(d) = d$ and therefore

$$g(d) = d \prod_{p\,|\,d} \left(1 - \frac{1}{p}\right) = \phi(d).$$

Hence,

$$Q = \sum_{d \mid P(y)} \frac{1}{\phi(d)} = \sum_{\substack{d \le y \\ (d,b)=1}} \prod_{p \mid d} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \ge \sum_{\substack{d \le y \\ (d,b)=1}} \frac{1}{d}.$$

Since

$$\begin{aligned} \prod_{p \mid b} \left(1 - \frac{1}{p}\right)^{-1} \left(\sum_{\substack{d \le y \\ (d,b)=1}} \frac{1}{d}\right) &= \prod_{p \mid b} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \left(\sum_{\substack{d \le y \\ (d,b)=1}} \frac{1}{d}\right) \\ &\ge \sum_{m \le y} \frac{1}{m} > \log y, \end{aligned}$$

we get that

$$Q > (\log y) \prod_{p \mid b} \left(1 - \frac{1}{p}\right) = \frac{\phi(b)}{b} \log y.$$

We also have that

$$y^2 \prod_{p \le y} \left(1 - \frac{1}{p}\right)^{-2} \ll y^2 (\log y)^2.$$

Thus,

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, y) \ll \frac{x}{b} \left(\frac{b}{\phi(b)}\right) \frac{1}{\log y} + y^2 (\log y)^2 = \frac{x}{\phi(b) \log y} + y^2 (\log y)^2.$$

Choosing $y = (x/b)^{1/3}$, it follows that

$$\pi(x; b, a) \ll \frac{x}{\phi(b) \log(x/b)},$$

which is precisely the Brun-Titchmarsh theorem (Theorem 12.7).

## 12.13. The Large sieve

The Large sieve was invented in 1941 by Linnik and thereafter improved by Bombieri [**14**], Montgomery-Vaughan [**107**], and others. Here we state without proof its most modern version.

Let $\{a_n\}_{n=1,\dots,N}$ be a sequence of complex numbers and let

$$w(p) = \#\{h : 0 \le h \le p-1 \ \text{ and } \ n \equiv h \bmod p \Longrightarrow a_n = 0\},$$

and again assume that $w(p) < p$ for all primes $p$. Set

$$g(d) = \mu(d)^2 \prod_{p \mid d} \frac{w(p)}{p - w(p)}. \tag{12.26}$$

Then the Large sieve is the following result.

**Theorem 12.22.** *If* $L = \sum_{d \le Q} g(d)$, *then*

$$\left| \sum_{n=1}^{N} a_n \right|^2 \le \frac{N - 1 + Q^2}{L} \sum_{n=1}^{N} |a_n|^2. \tag{12.27}$$

## 12.14. Quasi-squares

We now give an application of the Large sieve. A positive integer $n$ is called a *quasi-square* if the congruence $n \equiv x^2 \pmod{p}$ has an integer solution $x$ for each prime number $p \le n^{1/2}$. Clearly, all squares are quasi-squares, but are there more quasi-squares than squares? The next result shows that the number of quasi-squares up to $x$ is of the same order of magnitude as the number of squares up to $x$.

**Proposition 12.23.** *Let* $\mathcal{Q} = \{n : n \text{ is quasi-square}\}$. *Then* $\#(\mathcal{Q} \cap [1, x]) \ll x^{1/2}$.

**Proof.** Let $\mathcal{Q}_1(x)$ be the set of quasi-squares in $[x/2, x]$. Let $a_n = 1$ if $n \in \mathcal{Q}_1(x)$ and $a_n = 0$ otherwise. For each prime $p \le (x/2)^{1/2}$, there are precisely $(p-1)/2$ congruence classes $h \pmod{p}$ which are not quadratic residues modulo $p$. For such classes $h \pmod{p}$, the congruence $a \equiv h \pmod{p}$ is impossible for all $a \in \mathcal{Q}_1(x)$. Thus, we may take $w(p) = (p-1)/2$, $N = x$ and $Q = (x/2)^{1/2}$ in the Large sieve and get

$$(\#\mathcal{Q}_1(x))^2 = \left| \sum_{n \le x} a_n \right|^2 \le \frac{x - 1 + x/2}{L} \sum_{n \le x} |a_n|^2 < \frac{3x}{2L} \#\mathcal{Q}_1(x),$$

leading to $\#\mathcal{Q}_1(x) \ll x/L$. Note that $w(p)/(p - w(p)) = (p-1)/(p+1)$, so that if $\mu(d) \ne 0$, then $g(d)$ defined in (12.26) satisfies

$$\begin{aligned} g(d) &\gg \prod_{p \mid d} \left( \frac{p-1}{p+1} \right) = \prod_{p \mid d} \left( 1 - \frac{2}{p+1} \right) \\ &= \prod_{p \mid d} \left( 1 - \frac{1}{p} \right)^2 \prod_{p \mid d} \left( 1 - \frac{2}{p+1} \right) \left( 1 - \frac{1}{p} \right)^{-2} \\ &= \left( \frac{\phi(d)}{d} \right)^2 \prod_{p \mid d} \left( 1 - \frac{1}{p^2} \right)^{-1}. \end{aligned} \tag{12.28}$$

Since the product

$$\prod_p \left(1 - \frac{1}{p^2}\right)^{-1}$$

converges (to $\zeta(2)$), it follows from formula (12.28) that $g(d) \gg (\phi(d)/d)^2$. Thus,

$$L = \sum_{d \le Q} g(d) \gg \sum_{d \le Q} \left(\frac{\phi(d)}{d}\right)^2 \gg Q,$$

where we used the first estimate of Problem 8.10.

Thus,

$$\mathcal{Q}_1(x) \ll \frac{x}{Q} \ll x^{1/2}.$$

Changing $x$ to $x/2$, then to $x/4$, and so on, we then get that the total number of quasi-squares $n \le x$ is

$$\begin{aligned} \#(\mathcal{Q} \cap [1,x]) &\ll \sum_{0 \le k \le \log x/\log 2} \#\mathcal{Q}_1(x/2^k) \\ &\ll \sum_{0 \le k \le \log x/\log 2} \left(\frac{x}{2^k}\right)^{1/2} \le x^{1/2} \sum_{k \ge 0} \frac{1}{2^{k/2}} \ll x^{1/2}, \end{aligned}$$

which completes the proof of the proposition. □

**Remark 12.24.** *The Large sieve is very useful because it is very general. It allows us to sieve off large chunks of the residue classes modulo $p$, as in the problem of the quasi-squares where we sieved off half of the residue classes modulo $p$ for all primes $p$ up to almost $x^{1/2}$. It is also very useful in conjunction with classical estimates like the Chebyshev estimates, the Brun-Titchmarsh estimates and the counting function of the twin primes where it gives small values for the implied constants. We shall not enter into the details or discuss the Large sieve inequalities that have been designed.*

## 12.15. The smallest quadratic nonresidue modulo $p$

Given an integer $a$ and an odd prime $p$, we define the *Legendre symbol* of $a$ with respect to $p$ as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ for some integer } x, \\ -1 & \text{otherwise.} \end{cases} \tag{12.29}$$

We now give the following application (due to Linnik) that allows us to estimate the least quadratic nonresidue modulo $p$, that is, the smallest

positive integer $q(p)$ such that $\left(\frac{q(p)}{p}\right) = -1$. Notice that $q(p)$ is prime. It is conjectured that

$$q(p) \ll p^{\varepsilon} \tag{12.30}$$

for any $\varepsilon > 0$ with the implied constant depending on $\varepsilon$, but the best-known estimate is that the inequality (12.30) holds only for $\varepsilon > 1/(4\sqrt{e}) \approx 0.1516$.

**Theorem 12.25.** *The number of primes $p \le x$ such that $q(p) > x^{\varepsilon}$ is bounded by a constant depending on $\varepsilon$.*

**Proof.** Let

$$\mathcal{P} = \{p \le x^{1/2} : (n/p) = 1 \text{ for all } n \le x^{\varepsilon}\}$$

and observe that it is enough to show that $\#\mathcal{P} = O_{\varepsilon}(1)$, since afterwards the conclusion will follow by replacing $\varepsilon$ with $\varepsilon/2$ and $x$ by $x^2$. For every prime $p$, let

$$\Omega_p = \{\nu \pmod p) : (\nu/p) = -1\},$$

and let $\{a_n\}_{n \le x}$ be the characteristic function of the set

$$X = \{1 \le n \le x : (n/p) = 1 \text{ for all } p \in \mathcal{P}\}.$$

Then inequality (12.27) with $N = \lfloor x \rfloor$ and $Q = \sqrt{x}$ implies that

$$L \le \frac{N - 1 + Q^2}{\#X} < \frac{2x}{\#X}. \tag{12.31}$$

Observe that if $d = p \in \mathcal{P}$ is odd, then $w(p) = \#\Omega_p = (p-1)/2$, so that

$$g(p) = \frac{(p-1)/2}{p - (p-1)/2} = \frac{p-1}{p+1} \ge \frac{1}{2} \qquad \text{for all} \quad p \in \mathcal{P}.$$

Hence, inequality (12.31) yields

$$\#\mathcal{P} \le 2 \sum_{p \in \mathcal{P}} g(p) \le 2L \le \frac{4x}{\#X},$$

meaning that it suffices to prove that $\#X \gg_{\varepsilon} x$. Since $X$ contains the set $\{n \le x : P(n) \le x^{\varepsilon}\}$, we can write that

$$\#X \ge \Psi(x, x^{\varepsilon}) \ge \frac{1}{2}\rho(1/\varepsilon)x \qquad \text{for} \quad x > x_{\varepsilon},$$

where the last inequality follows from Theorem 9.3, thus completing the proof of the theorem. □

## Problems on Chapter 12

**Problem 12.1.** *Let $x$ be large and set $y = \log x$.*

(i) *By observing that the number of positive integers $n \le x$ divisible by $p^2$ is $\le x/p^2$, show that the set of positive integers $n \le x$ which are multiples of $p^2$ for some prime $p > y$ is $O(x/y)$.*

(ii) *Use the Inclusion-Exclusion principle to show that the number of $n \le x$ which are not divisible by $p^2$ for any prime $p \le y$ is*

$$x \prod_{p \le y} \left(1 - \frac{1}{p^2}\right) + O(2^y).$$

(iii) *Let $\mathcal{S}(x) = \{n \le x : \mu(n) \neq 0\}$. Deduce from (i) and (ii) that*

$$\#\mathcal{S}(x) = \frac{6x}{\pi^2} + O\left(\frac{x}{\log x}\right).$$

**Problem 12.2.** *Let $A = \{n = |u^w \pm v!| \text{ for some integers } u,\ v,\ w > 1\}$. Let $x$ be a large positive real number.*

(i) *Put $y = \log x/(\log\log x)^2$. Show that if $x$ is large, then the set of $n \in A \cap [1, x]$ such that $v \le y$ is of cardinality $x^{1/2+o(1)}$ as $x \to \infty$.*

(ii) *From now on, assume that $v > y$. By noting that if $m > 2p$, then $p^2 \mid m!$, prove that if $n = |u^w \pm v!|$ with $w > 1$ and $p < y/2$, then either $p$ is coprime to $n$ or $p^2 \mid n$.*

(iii) *Let $z = \log\log x$. Show that the number of positive integers $n \le x$ divisible by $p^2$ for some $p > z$ is $O(x/\log\log x)$.*

(iv) *Show that if $n \in A \cap [1, x]$ is not as in (i) or (iii), then $n$ is coprime with all the primes in $[z, y/2]$. Then use the Eratosthenes sieve to show that the number of such $n \le x$ is $O(x \log\log\log x/\log\log x) = o(x)$ as $x \to \infty$.*

(v) *Deduce that $A$ is of asymptotic density zero.*

**Problem 12.3.** *Here is a more general version of the Eratosthenes sieve. Let $m_1, \dots, m_k$ be coprime positive integers. For each $i \in \{1, \dots, k\}$, let $\mathcal{A}_j = \{a_{i_1} \pmod{m_j}, \dots, a_{i_{\omega_j}} \pmod{m_j}\} \subset \mathbb{Z}/m_j\mathbb{Z}$ be a set of $\omega_j < m_j$ congruence classes modulo $m_j$. Put $\Omega = \max\{\omega_j : j = 1, \dots, k\}$. Let*

$$\mathcal{N} = \{n \le x : n \notin \mathcal{A}_j \pmod{m_j} \text{ for all } j = 1, \dots, k\}.$$

*Show, using the Chinese Remainder Theorem and the Inclusion-Exclusion principle, that*

$$\#\mathcal{N} = x \prod_{j=1}^{k} \left(1 - \frac{\omega_j}{m_j}\right) + O((\Omega + 1)^k).$$

**Problem 12.4.** *Let $f(X) \in \mathbb{Z}[X]$ be a nonconstant polynomial of degree $D$ without double roots. Let*

$$\rho(d) = \#\{0 \le n \le d-1 \ : \ f(n) \equiv 0 \pmod{d}\}.$$

(i) *Show that $\rho$ is a multiplicative function.*

*Now, assume that*

$$f(X) = \prod_{i=1}^{D}(a_i X + b_i),$$

*where $a_i > 0$ and $b_i$ are integers for $i = 1, \dots, D$.*

(ii) *Show that the condition that $f(X)$ does not have double roots is equivalent to*

$$\Delta(f) = \prod_{i=1}^{D} \prod_{1 \le i < j \le D} (a_i b_j - a_j b_i) \neq 0.$$

(iii) *Show that $\rho(p) = D$ is equivalent to $gcd(p, \Delta(f)) = 1$.*

**Problem 12.5.** *Adapt the proof of Theorem 12.3 to show that if $f(X) \in \mathbb{Z}[X]$ is of degree $D$ and such that $\rho(p) < p$ for every prime number $p$, then the set $\mathcal{A}_f = \{n \le x \ : \ p(f(n)) > y\}$ has cardinality*

$$x \prod_{p \le y} \left(1 - \frac{\rho(p)}{p}\right)\left(1 + O\left(\frac{1}{\log y}\right)\right),$$

*provided that $x > x_D$ and $y \le \exp(\log x/(10D \log\log x))$.*

**Problem 12.6.** *Let $L_i(X) = a_i X + b_i$, $i = 1, \dots, k$, be distinct linear forms with integer coefficients. Assume that $\gcd(a_i, b_i) = 1$ for $i = 1, \dots, k$, and that $a_i > 0$ for all $i = 1, \dots, k$. Moreover, for each prime $p$, let*

$$\nu(p) = \#\{0 \le n \le p-1 : a_i n + b_i \equiv 0 \pmod{p} \ \text{ for some } i = 0, 1, \dots, k\}.$$

(i) *Show that if we choose $f(X) = \prod_{i=1}^{k} L_i(X)$, then $\nu(p)$ coincides with $\rho(p)$ defined in Problem 12.4.*

(ii) *Use Problem 12.5 to show that*

$$\begin{aligned} &\#\{n \le x : a_i n + b_i \text{ is prime for all } i = 1, \dots, k\} \\ &\quad \le c(k)\left(\frac{\Delta(f)}{\phi(\Delta(f))}\right)^k \frac{x(\log\log x)^k}{(\log x)^k}, \end{aligned}$$

*for $x > x(k)$ (some initial value depending only on $k$), where $c(k)$ is a constant that depends only on $k$. (Hint: Use Problem 12.5 with*

$y = \exp(\log x/(10k \log\log x))$. *As for the main term, note that, by Problem* 12.4, *it is*

$$\leq \prod_{\substack{p\leq y \\ p>k,\ p\nmid \Delta(f)}} \left(1-\frac{k}{p}\right).$$

*Prove first that if we put* $a_k(p) = (1-k/p)/(1-1/p)^k$, *then* $\prod_{p>k} a_k(p)$ *converges to a positive number, so that the above product is bounded by*

$$c_1(k) \prod_{\substack{p\leq y \\ p>k,\ p\nmid \Delta(f)}} \left(1-\frac{1}{p}\right)^k,$$

*where* $c_1(k)$ *depends only on* $k$. *Finally observe that this last product runs over all the primes* $p$ *with* $k < p \leq y$, *a contribution depending only on* $k$, *and the possible primes dividing* $\Delta(f)$. *What does the product of these eliminated factors have to do with* $\Delta(f)/\phi(\Delta(f))$? *Use also known results about the full product* $\prod_{p\leq y}(1-1/p)^k$.)

**Problem 12.7.** *Let* $\mathcal{A}$ *be the set of all positive integers* $n$ *such* $d + n/d$ *is a prime for all divisors* $d$ *of* $n$. *For example,* $n = 10$ *has this property because* $d + n/d \in \{1+10, 2+5\} = \{11, 7\}$. *Show that the sum of the reciprocals of the members of* $\mathcal{A}$ *is convergent. (Hint: Note that if* $n > 2$ *then* $n+1 = p$ *is prime, implying that* $n$ *is even. Thus,* $2 + n/2 = q$ *is also prime. What is the relation between* $p$ *and* $q$?)

**Problem 12.8.** *The following problem appeared as a conjecture in a recent paper of Elliott and Richner* [**44**]: *Show that the set* $\mathcal{A} = \{n \ : \ n = p^2 - q^2$ *with primes* $p,\ q\}$ *is of asymptotic density zero. Prove this result in the following way:*

(i) *Show that if* $n \in \mathcal{A}$, *then* $n = uv$, *where* $v < u$ *are positive integers, and that there exists a prime* $q$ *such that* $p = q + v$ *is prime and* $u = p + q = 2q + v$. *Deduce that* $n \leq x$ *is determined by a positive integer* $v \leq x^{1/2}$ *and a prime* $q < x/v$ *such that* $p = q + v$ *is also a prime.*

(ii) *Use Problem* 12.6, *or adapt the proof of Proposition* 12.4, *to deduce that the number of primes* $q \leq x/v$ *such that* $q + v$ *is also a prime is*

$$\ll \left(\frac{v}{\phi(v)}\right) \frac{x}{v} \frac{(\log\log(x/v))^2}{(\log(x/v))^2}.$$

(iii) *Show that the above upper bound is*

$$\ll \frac{x(\log\log x)^3}{v(\log x)^2}.$$

*(Hint: Use the maximal order of the function $m/\phi(m)$ in the interval $[1,x]$ and remember that $v \le x^{1/2}$.)*

(iv) *Now sum up over $v \le x^{1/2}$ and conclude.*

**Problem 12.9.** *Prove the estimate* $\displaystyle\sum_{n\le t}\frac{1}{\phi(n)} \ll \log t$ *in the following way:*

(i) *First recall that $n/\phi(n) \ll \sigma(n)/n$ and deduce that*

$$\sum_{n\le x}\frac{1}{\phi(n)} \ll \sum_{n\le x}\frac{\sigma(n)}{n^2}.$$

(ii) *To compute the sum appearing on the right-hand side of the above estimate, use the known average value of $\sigma(n)/n$ in the interval $[1,x]$ (Problem 7.2) with the Abel summation formula for $a_n = \sigma(n)/n$ and $f(t) = 1/t$ to conclude that the sum appearing on the right-hand side of the above estimate is $\ll \log x$.*

**Problem 12.10.** *Use the Brun-Titchmarsh theorem and Abel's summation formula to show that*

$$\sum_{\substack{p\le x\\ p\equiv a \pmod b}}\frac{1}{p} \ll \frac{1}{p_{a,b}} + O\left(\frac{\log\log x}{\phi(b)}\right)$$

*uniformly for $x \ge e^e$ and $1 \le a < b$, where $a$ and $b$ are coprime and $p_{a,b}$ is the smallest prime congruent to $a$ modulo $b$, and where the constant implied by the above $O$ is absolute.*

The purpose of the following two problems is to learn something interesting about the distance between consecutive primes.

**Problem 12.11.** *Let $f(x) > 0$ be an increasing function which tends to infinity with $x$ arbitrarily slowly. Let*

$$\mathcal{P} = \{p_n \ : \ p_{n+1} - p_n > f(n)\log n\}.$$

*Show that $\#(\mathcal{P}\cap[1,x]) = o(\pi(x))$ as $x$ tends to infinity. (Hint: Look only at primes $p \in [x/\log x, x]$. Then $f(n)\log n > g(x)\log x$, where you can take $g(x) = \frac{1}{2}f(x/\log x)$ for $x > x_0$. Now construct an interval of length $g(x)\log x$ starting at each prime in $\mathcal{P}\cap[x/\log x, x]$ and deduce that these intervals are disjoint. Hence, each such interval contains only one prime in $\mathcal{P}\cap[x/\log x, x]$. But how many disjoint intervals each of length $g(x)\log x$ can one pack in $[x/\log x, x]$ ?)*

**Problem 12.12.** *Let $f(x) > 0$ be as in the preceding problem. Let*

$$\mathcal{Q} = \{p_n : p_{n+1} - p_n \le (\log n)/f(n)\}.$$

*Show that $\#(\mathcal{Q} \cap [1, x]) = o(\pi(x))$ as $x \to \infty$ in the following way:*

(i) *Observe that if $p \in \mathcal{Q} \cap [x/\log x, x]$, then there exists $k \le (\log x)/g(x)$ such that $p$ and $p + k$ are both primes, where $g(x) = f(x/\log x)$.*

(ii) *Fix $k$. Show, using the Brun sieve, that the number of $p \le x$ such that $p$ and $p + k$ are both primes is*

$$\ll \frac{k}{\phi(k)} \frac{x}{(\log x)^2}.$$

(iii) *Deduce that*

$$\#\left(\mathcal{Q} \cap [x/\log x, x]\right) \ll \frac{x}{(\log x)^2} \sum_{k \le (\log x)/g(x)} \frac{k}{\phi(k)}.$$

(iv) *Use the fact that $k/\phi(k) \ll \sigma(k)/k$ and Problem 7.2 to conclude that the estimate*

$$\sum_{k \le y} \frac{k}{\phi(k)} \ll y$$

*holds for all $y \ge 1$.*

(v) *Use (iv) with $y = (\log x)/g(x)$ in the conclusion of (iii) to conclude that $\#(\mathcal{Q} \cap [x/\log x, x]) \ll \pi(x)/g(x) = o(\pi(x))$ as $x \to \infty$.*

**Problem 12.13.** *Repeat Problem 12.6 but this time using Brun's combinatorial sieve instead of the pure sieve to show that the inequality asserted at (ii) holds without the factor $(\log\log x)^k$. (Hint: Show that instead of stopping with the sieving parameter $y$ at $y = \exp(\log x/10k \log\log x)$, we can stop at $y = x^{1/ku}$, where $u$ is absolute.) Compare your answer with the Bateman-Horn conjectures (see page 35).*

**Problem 12.14.** *Reconsider Problem 12.6 but now deduce that if $\nu(p) < p$ for all $p$, then there exists a number $t$, which depends on $k$, but not on $a_i$ and $b_i$ for $i = 1, \dots, k$, such that there exist infinitely many positive integers $n$ with $\omega(L_i(n)) \le t$ for all $i = 1, \dots, k$. (Hint: Use the Brun sieve as a lower bound sieve and show that the main term is $> 0$ and dominates the error term if we sieve with $y = x^{1/ku}$. Then deduce that one can take $t = ku - 1$.) Note that, for $k = 2$ and $L_1(n) = n$, $L_2(n) = n + 2$, Brun showed that one can take $t = 9$.*

**Problem 12.15.** *Let $\mathcal{T}(x, y) = \{n \in [x, x + y] \ : \ n \text{ is powerful}\}$. Show that $\#\mathcal{T}(x, y) = o(y)$ as $y \to \infty$ uniformly in $x$. (Hint: Organize the powerful numbers $n \in [x, x + y]$ in two groups, the ones coprime to all primes $q \in [\log y, y]$ and the ones divisible by a prime in that interval. For*

*the first set, use the Brun sieve to conclude that the number of such numbers is* $\ll y\prod_{\log y\le p\le y}(1-1/p)\ll y\log\log y/\log y=o(y)$ *as* $y\to\infty$ *regardless of* $x$*. For the second group, note that if* $q\mid n$ *then* $q^2\mid n$ *since* $n$ *is powerful. Deduce that for a fixed* $q$*, the number of such* $n$ *is at most* $y/q^2+1$*. Now sum up over all the primes* $q\in[\log y,y]$*.)*

**Problem 12.16.** *Regarding the preceding problem, show that the abc conjecture implies that* $\#\mathcal{T}(x,y)\le 2$ *if* $x$ *is large. (Hint: Assume that* $1\le i_1<i_2\le y$ *are such that* $n$*,* $n+i_1$ *and* $n+i_2$ *are powerful and apply the abc conjecture to the equation* $(n+i_1)(n+i_2)-n^2=(i_1+i_2)n+i_1i_2$ *to deduce that* $n$ *is bounded in terms of* $y$*.) Deduce that if* $1=a_1<a_2<\cdots$ *is the increasing sequence of all the powerful numbers, then the abc conjecture implies that* $a_{n+2}-a_n\to\infty$*. Does* $a_{n+1}-a_n$ *tend to infinity? (Hint: The answer is NO and can be inferred by using Problem* 12.4*.)*

**Problem 12.17.** *Let* $\mathcal{P}=\{p\ :\ p+1=\phi(n)$ *for some positive integer* $n\}$*. Show that*

$$\sum_{p\in\mathcal{P}}\frac{1}{p}<\infty$$

*using the following steps.*

(i) *Let* $x$ *be large. If* $p+1=\phi(n)$*, show that* $n<c_0x\log\log x:=x_1$*. (Hint: Use the minimal order of the Euler function.)*

(ii) *Let* $v=\left\lfloor\frac{1}{2}\log\log x\right\rfloor$*. If* $\omega(n)>v$*, deduce that* $2^{v-1}\mid p+1$ *and apply the Brun-Titchmarsh theorem to deduce that the number of such primes* $p$ *is*

$$\ll x/(2^v\log(x/2^v))\ll x/(\log x)^{c_1},$$

*where* $c_1=1+\frac{1}{2}\log 2>1$*.*

(iii) *Let* $z=10\log\log x$*, put* $y=x_1^{1/z}$ *and use Theorem* 9.5 *to deduce that if* $p+1=\phi(n)$ *for some* $n$ *with* $P(n)<y$*, then the number of such* $p$ *is at most* $\Psi(x_1,y)\le x_1/\exp(u/2)\ll x/(\log x)^{c_2}$*, where one can take* $c_2=4$*. (Hint: Note that* $u=z$*.)*

(iv) *If* $p$ *is a prime not accounted at (ii) or at (iii), then* $p+1=(q-1)\phi(m)$ *for some positive integer* $m<x_1/y$ *with* $\omega(m)\le v$*. Interpret this as saying that* $q\le x_1/\phi(m)$ *is some prime such that* $\phi(m)q+(\phi(m)+1)=p$ *is also a prime. Now use the Brun sieve to show that the number of such* $q$ *is*

$$\ll\frac{x_1}{\phi(m)}\left(\frac{T(m)}{\phi(T(m))}\right)\frac{1}{(\log(x/\phi(m)))^2},$$

*where* $T(m)=\phi(m)(\phi(m)+1)$*.*

(v) *Use the minimal order of the Euler function to deduce that both inequalities*

$$T(m)/\phi(T(m)) \ll \log\log x \quad \text{and} \quad x/\phi(m) \geq x/m \gg y/\log\log x$$

*hold. Infer that the last upper bound at (iv) is bounded as*

$$\ll \frac{x(\log\log x)^4}{(\log x)^2}\frac{1}{\phi(m)}.$$

(vi) *Use the multinomial coefficient approach to deduce that*

$$\sum_{\substack{m\leq x\\ \omega(m)\leq v}} \frac{1}{\phi(m)} \leq \sum_{k\leq v}\frac{1}{k!}\left(\sum_{p\leq x}\frac{1}{p-1}+O(1)\right)^k \ll \left(\frac{e\log\log x+O(1)}{v}\right)^v.$$

(vii) *Deduce that the number of primes $p$ not accounted at (ii) or (iii) but such that $p+1=\phi(n)$ is $\ll x/(\log x)^{c_3+o(1)}$ as $x\to\infty$, where* $c_3 = 2-\frac{1}{2}\log(2e) > 1$.

(viii) *Conclude.*

**Problem 12.18.** *Note that $p-1=\phi(p)=\phi(2p)$ if $p>2$. Let $\mathcal{P}=\{p \,:\, p-1=\phi(n)$ has at least 3 solutions $n\}$. Prove that*

$$\sum_{p\in\mathcal{P}}\frac{1}{p}<\infty.$$

*(Hint: Follow the same approach as for Problem* 12.17*.)*

**Problem 12.19.** *Adapt the argument used in the proof of Theorem* 12.9 *to show that there exists $\delta<1$ such that*

$$\#\{p\leq x \,:\, P((p-1)(p+1))<x^\delta\} \gg \frac{x}{\log x}.$$

**Problem 12.20.** *Adapt the proof of Proposition* 8.7 *(or Problem* 8.9*) to show that there exists a constant $c_0>0$ such that*

$$\#\{n\leq x \,:\, \phi(n) \text{ is a perfect square}\} \geq x^{c_0}$$

*if $x>x_0$. (Hint: Let $y$ be some parameter and $\delta$ the number appearing in Theorem* 12.9*. Let $\mathcal{P}$ be the set of primes $p\in[y/\log y, y]$ such that $P(p-1)<p^\delta$. Choose subsets $S$ of such primes $p$ of exactly $\lfloor p^\delta\rfloor$ elements and let $n_S=\prod_{p\in S}p$. Then $\phi(n_S)=u_S v_S^2$, where $P(u_S)\leq y^\delta$ so that $u_S$ can take only at most $2^{\pi(y^\delta)}$ values. Now use the Pigeon Hole principle as in the proof of Proposition* 8.7 *to get a lower bound for the number of squarefree numbers $n$ made up of primes from $\mathcal{P}$ for which $\phi(n)$ is a square and compare this lower bound with $x=y^{y^\delta}$, which is the upper bound for such $n$'s.)*

**Problem 12.21.** *Show that the same conclusion as in the preceding problem is valid if one replaces $\phi(n)$ either by $\sigma(n)$ or by $\phi(n)\sigma(n)$.*

**Problem 12.22.** *Let*

$$p_a(n) = \frac{1}{\omega(n)} \sum_{p|n} p$$

*be the average prime factor of $n$. Use Vinogradov's three primes theorem (Theorem 12.18) to show that there exist infinitely many squarefree composite positive integers $n$ for which $p_a(n)$ is a prime factor of $n$. For example, $105 = 3 \times 5 \times 7$ and the average of $3, 5, 7$ is $5$ which is a prime factor of $105$. (Hint: Let $r$ be a large prime. Apply Vinogradov's theorem to $3r$ to deduce that there are many triples $(p_1, p_2, p_3)$ such that $3r = p_1 + p_2 + p_3$. Then use an analogue of Theorem 12.10 to show that most of those representations have $p_i \neq p_j$ and $p_i \neq r$. Then choose $n = rp_1p_2p_3$.)*

**Problem 12.23.** *Let $\beta(n) = \sum_{p \mid n} p$. Construct infinitely many squarefree composite integers $n$ such that $\beta(n) \mid n$. For example, $\beta(30) = 2 + 3 + 5 = 10 \mid 30$ is such a number. (Hint: Apply an argument similar to the one used in Problem 12.22 to deduce the existence of equations of the form $r - 2 = p_1 + p_2 + p_3$, where $r$ is a large prime and $p_1$, $p_2$, $p_3$ are odd distinct primes. Then look at $n = 2rp_1p_2p_3$.)*

**Problem 12.24.** *First show that $\sigma(\sigma(p))/p \geq 3/2$ for all primes $p$. Then use Chen's theorem (Theorem 12.11) to deduce that $\{\sigma(\sigma(p))/p : p \text{ prime}\}$ is dense in $[3/2, \infty)$. (Hint: Let $a$ be an odd integer. Use the Chen Theorem to conclude that there are arbitrarily large primes $p$ with $(p+1)/(2a)$ either a prime or a product of two large primes. Deduce that $\sigma(\sigma(p))/p = (3/2)(\sigma(a)/a)(1 + o(1))$ as $p \to \infty$ over such primes and conclude using known results about the numbers $\sigma(a)/a$ as $a$ runs through the odd positive integers.)*

**Problem 12.25.** *Show that the set of positive integers $n$ such that $p_a(n) \in \mathbb{Z}$, where $p_a$ is defined above in Problem 12.22, is of asymptotic density zero.*

(i) *Let $x$ be large and $n \leq x$. Argue that one may assume that $P(n) > x^{1/u}$, where $u = \log\log\log x$, that $P(n) \| n$, and that $\omega(n) \in [y - y^{2/3}, y + y^{2/3}]$, where $y = \log\log x$. Problem 7.12 might prove to be of interest.*

(ii) *Write $n = mp$, where $p = P(n)$ and $m < x/x^{1/u}$. Fix $m$. Then $p_a(n) \in \mathbb{Z}$ means that $p \equiv -\beta(m) \pmod{\omega(m)+1}$ and $p \leq x/m$. Use Brun-Titchmarsh (check first that it is applicable) to conclude that the number of such choices for $p$ is*

$$\ll \frac{x}{m\phi(\omega(m)+1)} \frac{1}{\log(x/m(\omega(m)+1))}.$$

(iii) *Show that* $\log(x/(m(\omega(m)+1))) \gg (\log x)/u$ *for large* $x$ *and then use the minimal order of the Euler function for numbers close to* $y$ *to conclude that the bound shown at (ii) is*

$$\ll \frac{x(\log\log\log x)^2}{m\omega(m)\log x}.$$

(iv) *Sum up over* $m$ *to conclude that the number of such integers* $n \le x$ *is*

$$\ll \frac{x(\log\log\log x)^2}{\log x}\left(\sum_{m\le x}\frac{1}{m}\right)\left(\sum_{y-y^{2/3}\le k\le y+y^{2/3}}\frac{1}{k}\right)$$

*and use the calculation done at the end of Problem* 7.12 *to show that the above bound is*

$$\ll \frac{x(\log\log\log x)^2}{(\log\log x)^{1/3}} = o(x) \qquad \text{as } x\to\infty.$$

**Problem 12.26.** *Positive integers* $n$ *with* $\beta(n)=\beta(n+1)$ *are called Ruth-Aaron numbers (recall that* $\beta(n)=\sum_{p\mid n}p$*). One can check that* $n=714$ *is such a number. It is not known if there are infinitely many such numbers* $n$*. Do you have an heuristic? What does your heuristic predict? You should back it up with known conjectures such as the abc conjecture or Schinzel's Hypothesis H.*

**Problem 12.27.** *Show that for all* $2\le y\le x$*,*

$$\#\{n\le x \ : \ pq\mid n \text{ for some primes } y\le p<q<p\log p\} \ll \frac{x\log\log y}{\log y}.$$

*(Hint: Note that if* $y\le p\le q\le p\log p$*, then the number of* $n$ *which are multiples of* $pq$ *is* $\le x/pq$*. Then use Mertens' estimate to show that for fixed* $p$*,*

$$\sum_{p\le q\le p\log p}\frac{1}{q} = \log\log(p\log p)-\log\log p+O\left(\frac{1}{\log p}\right)\ll\frac{\log\log p}{\log p}.$$

*It then remains to estimate*

$$\sum_{p\ge y}\frac{\log\log p}{p\log p}$$

*which can be done using Abel's summation formula and the Prime Number Theorem to finally conclude that it is* $\ll(\log\log y)/\log y$*).*

**Problem 12.28.** *Show that the Ruth-Aaron numbers introduced in Problem* 12.26 *form a set of asymptotic density zero in the following way:*

(i) *Let $x$ be large. Argue that one may assume that none of $n$ is not $x^{1/u}$-smooth where $u = \log\log x$, that $P(n)\|n$ and that if $P_2(n)$ is the second largest prime factor of $n$, then $P(n) > P_2(n)(\log x)^3$ and that the same is true for $n+1$.*

(ii) *Let $p$ and $q$ be the largest prime factors of $n$ and $n+1$ respectively. Deduce from $\beta(n) = \beta(n+1)$ and (i) above that $|p-q| < p/(\log x)^2$ if $x > x_0$.*

(iii) *If $pq \le x$, then the number of $n \le x$ such that $p \mid n$ and $q \mid n+1$ is $\le x/pq + 1 \le 2x/pq$. Now sum up over all pairs of primes $p$, $q$ larger than $x^{1/u}$ with $|p-q| = O(p/(\log x)^2)$.*

(iv) *Write $n = pa$, $n+1 = qb$. If $pq > x$, deduce that $ab \le x$ and $|a-b| \ll a/(\log x)^2$.*

(v) *For fixed $a$ and $b$ with $ab \le x$, there are at most $x/ab + 1 \le 2x/ab$ positive integers $n \le x$ such that $a \mid n$ and $b \mid n+1$.*

(vi) *Show that for fixed $a$,*

$$\sum_{a<b<a+O(a/(\log x)^2)} \frac{1}{b} \ll \int_a^{a+O(a/(\log x)^2)} \frac{dt}{t} \ll \frac{1}{(\log x)^2}.$$

(vii) *Conclude that the number of Ruth-Aaron numbers $n \le x$ with $ab \le x$ is*

$$\ll \frac{x}{(\log x)^2} \sum_{a \le x} \frac{1}{a} \ll \frac{x}{\log x} = o(x) \qquad \text{as } x \to \infty.$$

**Problem 12.29.** *For an odd $d$, let $t_d$ be the multiplicative order of 2 modulo $d$. Show that*

$$\sum_{d \text{ odd}} \frac{1}{dt_d} < \infty.$$

*(Hint: Go through the proof of Proposition 9.11 and read off the fact that all odd $n \le x$ have $t_n > (\log x)^2$ except for a possible number of exceptions of cardinality $O(x/(\log x)^2)$. Hence, the odd $n$'s with $t_n < (\log n)^2$ form a set whose counting function is $O(x/(\log x)^2)$ so that the sum of their reciprocals converges, while for the remaining $n$'s we have $1/(nt_n) \le 1/(n(\log n)^2)$, and the series of general term $1/(n(\log n)^2)$ converges.)*

**Problem 12.30.** *Let $r(n) = \#\{(p,k) \ : \ n = p + 2^k\}$.*

(i) *Show that*

$$\sum_{n \le x} r(n) \gg x.$$

(ii) *Show that*

$$\sum_{n \le x} r(n)^2 = \#\{(p_1,k_1,p_2,k_2) \ : \ p_1 + 2^{k_1} = p_2 + 2^{k_2}\}.$$

*If $k_1 = k_2$, then $p_1 = p_2$, implying that the number of such diagonal quadruples $(p_1, k_1, p_2, k_2)$ is $\le \pi(x)(\log x/\log 2) \ll x$.*

(iii) *Show, using the Brun sieve, that the number of nondiagonal quadruples is*

$$\sum_{k\le \log x/\log 2} \frac{x}{\log x} \prod_{p\mid 2^k-1}\left(1+\frac{1}{p}\right) \ll \frac{x}{\log x}\sum_{\substack{d\le x\\ d\ odd}}\frac{1}{d}\sum_{\substack{k\le \log x/\log 2\\ t_d\mid k}} 1$$
$$\ll \frac{x}{\log x}\sum_{d\ odd}\frac{\log x}{dt_d},$$

*where $t_d$ is the multiplicative order of 2 modulo $d$, and now use Problem* 12.29 *to conclude that $\sum_{n\le x} r(n)^2 \ll x$.*

(iv) *Use the Cauchy-Schwarz inequality as in the proof of Theorem* 12.17 *to show that the set of numbers $n = p + 2^k$ has positive lower asymptotic density. (Yet remember that its complement also has positive lower asymptotic density, for example from Problem* 7.20*.)*

**Problem 12.31.** *The aim of this problem is to show that*

$$\sum_{n\ge 1}\frac{p_n}{n!} \notin \mathbb{Q}, \tag{12.32}$$

*where as usual $p_n$ stands for the $n$-th prime. Assume for a contradiction that the series appearing at* (12.32) *is rational.*

(i) *Using the fact that $p_n = n(\log n + O(\log\log n))$, deduce that if the number shown at* (12.32) *is rational then for each $n$ there exist integers $a$ and $b$ of the size $\log n + O(\log\log n)$ such that $p_n = na - b$.*

(ii) *Use the Pigeon Hole Principle to show that there exist integers $a$ and $b$ of the sizes shown in (i) such that $p_k = ka - b$ holds for a set of $k \in [n, 2n]$ of cardinality $\gg n/(\log\log n)^2$.*

(iii) *Use the Brun-Tichmarsh theorem to get an upper bound on the set of primes $p \in [p_n, p_{2n}]$ which are congruent to $-b \pmod a$. Can you see that you reached a contradiction?*

**Problem 12.32.** *The number $n = 113$ has the property that if we delete any of its digits, the number that remains is prime. Show that the number of $n \le x$ with this property is smaller than $x^c$ for some positive constant $c$ as $x \to \infty$. Are there infinitely many such positive integers ?*

**Problem 12.33.** *Show that the Fermat number $F_m = 2^{2^m} + 1$ with $m > 0$ is prime if and only if $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$. This result is known as Pépin's test, named after the French mathematician Théophile Pépin who discovered this primality test in 1877.*

*Chapter 13*

# Prime Numbers in Arithmetic Progression

## 13.1. Quadratic residues

We have already seen that given an odd prime $p$, there are $(p-1)/2$ nonzero congruence classes $a$ modulo $p$ for which the equation $x^2 \equiv a \pmod{p}$ has no solution $x$. Such congruence classes are called *quadratic nonresidues*. The nonzero residue classes $a$ for which $x^2 \equiv a \pmod{p}$ has an integer solution $x$ are called *quadratic residues*. For the sake of completeness, let us quickly review the main properties of quadratic residues.

Let $p$ be any prime. Any polynomial $f(X) \pmod{p}$ of degree $d$ which is not the constant zero polynomial can have at most $d$ roots modulo $p$. Fermat's little theorem tells us that every nonzero residue class $a$ modulo $p$ satisfies $a^{p-1} \equiv 1 \pmod{p}$. To prove this result, first note that the classes $a \cdot 1,\ a \cdot 2,\ \ldots,\ a \cdot (p-1)$ are a permutation of the classes $1,\ 2,\ \ldots,\ (p-1)$ modulo $p$, so that their product is the same. This gives

$$\prod_{i=1}^{p-1} (ai) \equiv \prod_{i=1}^{p-1} i \pmod{p},$$

that is,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Since $(p-1)!$ is invertible modulo $p$ (in fact, it is $-1$ modulo $p$ by Wilson's theorem), we get that $a^{p-1} \equiv 1 \pmod{p}$. Let $d$ be the order of $a$ modulo $p$, that is, $d$ is the smallest positive integer such that $a^d \equiv 1 \pmod{p}$. Fermat's little theorem, or Lagrange's theorem for the group $(\mathbb{Z}/p\mathbb{Z})^*$, shows that $d|p-1$.

Let $d \mid p-1$ be arbitrary and look at the polynomial $X^d - 1 \pmod p$. If there is an element $a \pmod p$ of order $d$, then $1,\ a,\ a^2,\ \ldots, a^{d-1}$ are all distinct modulo $p$ and roots of $X^d - 1 \pmod p$. Since this last polynomial cannot have more than $d$ roots modulo $p$, it follows that $1,\ a,\ \ldots,\ a^{d-1}$ are the only classes $b \pmod p$ which are the roots of the above polynomial. In particular, if $a'$ is any other element of order $d$, it must then be the case that $a' = a^k$, for some $k$ coprime to $d$. (If $k$ is not coprime to $d$, then $(a')^{d/(d,k)} \equiv a^{kd/(d,k)} \equiv 1 \pmod p$, and the fact that $(d,k) > 1$ contradicts the assumption that the order of $a'$ is $d$.) To summarize, if there is an element of order $d$ modulo $p$, then there are precisely $\phi(d)$ such elements. Thus, the total number of elements in $(\mathbb{Z}/p\mathbb{Z})^*$ is

$$\sum\nolimits^{*}_{d \mid p-1} \phi(d),$$

where $^*$ means that the sum is taken only over such $d \mid p-1$ for which there exist elements of order $d$ modulo $p$. Since the number of elements in the group is obviously $p-1$ and since

$$\sum_{d \mid n} \phi(d) = n$$

(see Problem 8.1), we get that $\sum^* = \sum$. In particular, there exists an element $a \pmod p$ of multiplicative order $p-1$. Such an element is called a *primitive root*. To summarize, we proved the following result.

**Theorem 13.1.** *For every prime $p$, there exists a primitive root $\rho \pmod p$.*

Now let $p$ be odd and let $\rho$ be a fixed primitive root modulo $p$. Given a nonzero congruence class $a$ modulo $p$, we can write it as $a = \rho^n \pmod p$ for some $n \in \{0, 1, \ldots, p-1\}$. This representation allows us to decide quickly if $a$ is a quadratic residue or not. Indeed, if $n$ is even, then $a \equiv (\rho^{n/2})^2 \pmod p$, so that $a$ is definitely a quadratic residue modulo $p$. Conversely, if $a$ is a quadratic residue modulo $p$, then $a \equiv x^2 \pmod p$ for some $x$. Writing $x \equiv \rho^m \pmod p$, we get that $a \equiv \rho^{2m} \pmod p$, so that $n \equiv 2m \pmod{p-1}$, in which case $n$ is even because $p-1$ is even. Thus, $a$ is a quadratic residue modulo $p$ if and only if $a \equiv \rho^n \pmod p$ for some even integer $n$. Since there are $(p-1)/2$ even numbers in $\{0, 1, \ldots, p-1\}$, we get that exactly $(p-1)/2$ of the nonzero residue classes modulo $p$ are quadratic residues and $(p-1)/2$ are quadratic nonresidues. Another characterization of the quadratic residues modulo $p$ is as follows.

**Proposition 13.2.** *Let $a \not\equiv 0 \pmod p$. Then $a$ is a quadratic residue modulo $p$ if and only if $a^{(p-1)/2} \equiv 1 \pmod p$.*

**Proof.** First observe that $X^{p-1} - 1 = (X^{(p-1)/2} - 1)(X^{(p-1)/2} + 1)$. Note also that if $a$ is not divisible by $p$ and $a \equiv x^2 \pmod p$, then $a^{(p-1)/2} \equiv$

$x^{p-1} \pmod p$, so that by Fermat's little theorem we get that $a^{(p-1)/2} \equiv 1 \pmod p$, which tells us two things. First it gives us the "if part" of the proposition we want to prove. Secondly, it tells us that $a$ is a root of $X^{(p-1)/2} - 1$. Hence, every quadratic residue is a root of $X^{(p-1)/2} - 1$, a nonzero polynomial of degree $(p-1)/2$, and since there are already $(p-1)/2$ quadratic residues, it follows that the above polynomial cannot have other roots. Hence, $a^{(p-1)/2} \equiv 1 \pmod p$ implies that $a$ is a quadratic residue modulo $p$ as well. □

Proposition 13.2 tells us immediately that

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p, \tag{13.1}$$

where $\left(\frac{a}{p}\right)$ stands for the Legendre symbol defined in Chapter 12 (see relation (12.29)).

**Example 13.3.**

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod p,$$

*and since both sides of the above congruence are* $\pm 1$ *and* $p$ *is odd, we get that the two sides are actually equal. Thus,* $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$*, so that* $-1$ *is a quadratic residue if and only if* $p \equiv 1 \pmod 4$.

Congruence (13.1) also immediately implies that

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p, \tag{13.2}$$

which, in particular, tells us that the product of two quadratic residues is a quadratic residue (intuitively clear), that the product of a residue and a nonresidue is a nonresidue (intuitively almost clear) but also that the product of two nonresidues is a residue (intuitively less clear).

Here is a way to compute the Legendre symbol. Call a residue $a \pmod p$ reduced if $a \in \{0, 1, \ldots, p-1\}$. The following result is known as Gauss's Lemma.

**Lemma 13.4.** *(Gauss's Lemma) Let* $a$ *be coprime to* $p$ *and let* $s$ *be the number of reduced residues among* $a \cdot 1,\ a \cdot 2,\ \ldots,\ a \cdot (p-1)/2$ *which are in the interval* $[(p+1)/2, p-1]$*. Then*

$$\left(\frac{a}{p}\right) = (-1)^s \pmod p.$$

**Proof.** Write each $a \cdot i = \varepsilon_i r_i$, where $r_i \in \{1, \ldots, (p-1)/2\}$ and $\varepsilon_i \in \{-1, 1\}$. Note that $r_i$ and $r_j$ are distinct for $i \neq j \in \{1, \ldots, (p-1)/2\}$. Indeed, if they are equal, then $ai \equiv \pm aj \pmod{p}$, so that $p \mid a(i \pm j)$. Since $p \nmid a$, $i \not\equiv j \pmod{p}$ and $0 < |i \pm j| \leq (p-1)/2 + (p-1)/2 < p$, we get a contradiction. Thus, the residues $r_i$ are distinct and there are precisely $(p-1)/2$ of them. Hence, $r_1, \ldots, r_{(p-1)/2}$ is a permutation of $1, \ldots, (p-1)/2$. By hypothesis, $s$ of the $\varepsilon_i$'s are $-1$ and the other $(p-1)/2 - s$ are $+1$. Multiplying all of the above relations, we get

$$\prod_{i=1}^{(p-1)/2} (a \cdot i) = \prod_{i=1}^{(p-1)/2} (\varepsilon_i r_i) \pmod{p},$$

or

$$a^{(p-1)/2}((p-1)/2)! \equiv (-1)^s((p-1)/2)! \pmod{p},$$

which yields $a^{(p-1)/2} \equiv (-1)^s \pmod{p}$. Calling upon relation (13.1) completes the proof. □

**Example 13.5.** *We use the Gauss Lemma with $a = 2$. Among the numbers $2, 4, \ldots, (p-1)$, there are precisely $k = \lfloor (p-1)/4 \rfloor$ of them whose reduced residues are $\leq (p-1)/2$. Indeed, these are the numbers $i$ for which $2i \leq (p-1)/2$ or $i \leq k$. Thus, $s = (p-1)/2 - \lfloor (p-1)/4 \rfloor$. One checks, by considering each of the four possibilities modulo 8, that*

$$\frac{p^2-1}{8} \equiv \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor \pmod{2},$$

*and now formula (13.1) tells us that*

$$\left(\frac{2}{p}\right) \equiv (-1)^{(p^2-1)/8} \pmod{p}.$$

*In particular, 2 is a quadratic residue modulo $p$ if and only if $p \equiv \pm 1 \bmod 8$.*

## 13.2. The proof of the Quadratic Reciprocity Law

The next result is known as the *Quadratic Reciprocity Law*. It was first discovered by Euler (by numerical evidence) and its first proof was given by Gauss in 1796, who later on gave five more different proofs (see Gauss [**64**]).

**Theorem 13.6.** *Let $p$ and $q$ be odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}}.$$

**Proof.** We first start by writing

$$ja = p\left\lfloor \frac{ja}{p} \right\rfloor + r'_j, \qquad j = 1, \ldots, (p-1)/2,$$

where $r'_j \in \{0, 1, 2, \ldots, p-1\}$. Summing up these relations we get

$$\sum_{j=1}^{(p-1)/2} ja = pT(a,p) + \sum_{j=1}^{(p-1)/2} r'_j, \tag{13.3}$$

where

$$T(a,p) = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor.$$

Note that $r'_j = r_j$ if $\varepsilon_j = 1$ and $r'_j = p - r_j$ if $\varepsilon_j = -1$, where these numbers have been defined in the proof of Gauss' Lemma (Lemma 13.4). Since $r_1, \ldots, r_{(p-1)/2}$ are all the residues modulo $p$, we get that

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{(p-1)/2} r_j = \sum_{\substack{1 \le j \le (p-1)/2 \\ \varepsilon_j = 1}} r'_j + \sum_{\substack{1 \le j \le (p-1)/2 \\ \varepsilon_j = -1}} (p - r'_j),$$

and reducing this modulo 2 we get that

$$\sum_{j=1}^{(p-1)/2} j \equiv s + \sum_{j=1}^{(p-1)/2} r'_j \pmod 2. \tag{13.4}$$

Reducing also equation (13.3) modulo 2 and inserting (13.4) in it, we get that

$$a \sum_{j=1}^{(p-1)/2} j \equiv \sum_{j=1}^{(p-1)/2} j + T(a,p) + s \pmod 2,$$

so that

$$(a-1) \sum_{j=1}^{(p-1)/2} j \equiv T(a,p) + s \pmod 2.$$

When $a$ is odd, we have that $2 \mid a - 1$, and we thus get that $T(a,p) \equiv s \pmod 2$. Gauss's Lemma now shows that

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)}.$$

Thus, in order to complete the proof of the Quadratic Reciprocity Law, it suffices to show that

$$T(q,p) + T(p,q) \equiv \frac{(p-1)}{2} \cdot \frac{(q-1)}{2} \pmod 2,$$

if $p$ and $q$ are odd primes. But this is easy to do. Indeed, $T(q,p)$ counts the number of lattice points (points with integer coefficients) in the triangle bounded below by the horizontal axis $y = 0$, the vertical line $x = (p-1)/2$ (points on this line are also counted) and the line $y = qx/p$. The points on the horizontal line $y = 0$ are not being counted. Similarly, $T(p,q)$ counts

the number of integer points in the triangle to the right of the vertical axis $x = 0$, bounded above by the horizontal line $y = (q-1)/2$ (points on this line are being counted) and to the left of the diagonal $x = yp/q$. Since there are no lattice points on the diagonal (because $p$ and $q$ are primes and both $x$ and $y$ are at most $(p-1)/2$ and $(q-1)/2$ respectively), no point gets counted twice, so that $T(p,q) + T(q,p)$ is the number of lattice points in the rectangle $0 < x \leq (p-1)/2$ and $0 < y \leq (q-1)/2$, which is obviously $\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}$, thus completing the proof. □

## 13.3. Primes in arithmetic progressions with small moduli

The very first important result which we presented in this book is Euclid's proof of the fact that the set of prime numbers is infinite. Euclid's proof can be slightly strengthened to yield the following result.

**Theorem 13.7.** *Let*

$$f(X) = a_d X^d + \cdots + a_0 \in \mathbb{Z}[X]$$

*be a nonconstant polynomial with integer coefficients. Let $\mathcal{P}$ be a set of primes such that $a_0$ is coprime to the primes in $\mathcal{P}$ and for all sufficiently large $n \in \mathbb{N}$, $f(n)$ has a prime factor in $\mathcal{P}$. Then $\mathcal{P}$ is infinite.*

**Proof.** Assuming that this were not so, let $p_1 < \cdots < p_s$ be all the primes in $\mathcal{P}$, and let $n$ go to infinity through numbers of the form $n = mp_1 \cdots p_s$, where $m$ is a positive integer. If $m$ is sufficiently large, then $f(n)$ will have a prime factor in $\mathcal{P}$, by hypothesis. Thus, it must be one of the $p_i$'s. However, this is impossible since all the $p_i$'s divide $n$ and none of them divides $a_0$. □

The above straightforward extension of Euclid's argument allows one to deduce that various sets of primes $\mathcal{P}$ are infinite. We list a few examples.

**1.** *There are infinitely many primes $p \equiv 3 \pmod 4$.* To see this, choose $\mathcal{P} = \{p \equiv 3 \pmod 4\}$ and $f(X) = 4X - 1$. One easily checks that the hypothesis of Theorem 13.7 are fulfilled (note that every positive integer of the form $4n - 1$ must have a prime factor $p \equiv 3 \pmod 4$), so that $\mathcal{P}$ is infinite.

**2.** *There are infinitely many primes $p \equiv 1 \pmod 4$.* Choose $\mathcal{P} = \{p \equiv 1 \pmod 4\}$ and $f(X) = 4X^2 + 1$. If $n > 0$ is an integer and $p \mid f(n)$, then $p$ is odd and $(2n)^2 \equiv -1 \pmod p$. Thus, $-1$ is a quadratic residue modulo $p$ leading to $p \equiv 1 \pmod 4$.

**3.** *There are infinitely many primes $p \equiv 2 \pmod 3$.* Here, we choose $\mathcal{P} = \{p \equiv 2 \pmod 3\}$ and $f(X) = 3X - 1$.

**4.** *There are infinitely many primes* $p \equiv 1 \pmod 3$. Here, we choose $\mathcal{P} = \{p \equiv 1 \pmod 3\}$ and $f(X) = 9X^2 + 3X + 1$. If $p$ divides $f(n)$ for some $n$, then $(3n)^2 + (3n) + 1 \equiv 0 \pmod p$, so that $(3n)^3 \equiv 1 \pmod p$. Thus, the order of $3n$ modulo $p$ is either 1 or 3. If it is 1, we get that $3n \equiv 1 \pmod p$, so that $f(n) \equiv 1^2 + 1 + 1 \pmod p \equiv 3 \pmod p$. Thus, $p \mid 3$, leading to $p = 3$, which is impossible because $f(n) \equiv 1 \pmod 3$. Thus, the order of $3n$ modulo $p$ is 3, and therefore $3 \mid p - 1$.

**5.** *There are infinitely many primes* $p \equiv 7 \pmod 8$. Here, we choose $\mathcal{P} = \{p \equiv 7 \pmod 8\}$ and $f(X) = 8X^2 - 1$. If $p \mid f(n)$, then $2(2n)^2 \equiv 1 \pmod p$, and therefore 2 is a quadratic residue modulo $p$. Thus, $p \equiv \pm 1 \pmod 8$. But since $f(n) \equiv 3 \pmod 4$, there must exist a prime factor $p \equiv 3 \pmod 4$ of $f(n)$. This prime must also satisfy $p \equiv \pm 1 \pmod 8$, and therefore $p \equiv 7 \pmod 8$.

**6.** *There are infinitely many primes* $p \equiv 1 \pmod 8$. Here, we choose $\mathcal{P} = \{p \equiv 1 \pmod 8\}$ and $f(X) = (2x)^4 + 1$. If $p \mid f(n)$, then $p$ is odd and $(2n)^4 \equiv -1 \pmod p$. It follows easily that the order of $2n$ modulo $p$ is 8, so that $8 \mid p - 1$.

**7.** *There are infinitely many primes* $p \equiv 3 \pmod 8$. We choose $\mathcal{P} = \{p \equiv 3 \pmod 8\}$ and $f(X) = X^2 + 2$. If $n$ is odd, then $f(n)$ is odd. Moreover, $f(n) \equiv 3 \pmod 8$, and therefore there exists a prime factor $p \equiv 3 \pmod 4$ of $f(n)$. Since also $n^2 = -2 \pmod p$, we get that $-2$ is a quadratic residue modulo $p$. Since $p \equiv 3 \pmod 4$, we get that $-1$ is not a quadratic residue modulo $p$, so that 2 is not a quadratic residue modulo $p$. We conclude that $p \equiv \pm 3 \pmod 8$ and since $p \equiv 3 \pmod 4$, we get that $p \equiv 3 \pmod 8$.

**8.** *There are infinitely many primes* $p \equiv 5 \pmod 8$. Take $\mathcal{P} = \{p \equiv 5 \pmod 8\}$ and $f(X) = 9(2X^2 - 1)^2 + 64X^2$. If $n$ is odd and not a multiple of 3, then $f(n)$ is coprime to 6. Moreover, $9(2n^2 - 1)$ and $64n^2$ are coprime. If $p \mid f(n)$, then $(3(2n^2 - 1))^2 \equiv -(8n)^2 \pmod p$, and since $8n$ is coprime to $p$, we deduce that $-1$ is a quadratic residue modulo $p$. Thus, $p \equiv 1 \pmod 4$. But note that

$$f(n) = (2n^2 - 1)^2 + 8((2n^2 - 1)^2 + 8n^2) = (2n^2 - 1)^2 + 8(2n^2 + 1)^2,$$

implying that $(2n^2 - 1)^2 \equiv -8(2n^2 + 1)^2 \pmod p$. Again, $p$ and $2n^2 - 1$ are coprime, so that $-8$ is a quadratic residue modulo $p$. Thus, $-2$ is a quadratic residue modulo $p$. We now get that $p \equiv 3, 5 \pmod 8$ and since $p \equiv 1 \pmod 4$, we get that $p \equiv 5 \pmod 8$.

By now one might perhaps be wondering whether it is true that for all coprime $a$ and $b$ there exist infinitely many primes $p \equiv a \pmod b$. The

answer is YES and it is a famous theorem of Dirichlet, which can be stated as follows.

**Theorem 13.8.** *(Dirichlet) Let $a < b$ be fixed coprime positive integers. Then the estimate*

$$\pi(x; b, a) = (1 + o(1))\frac{\pi(x)}{\phi(b)}$$

*holds as $x \to \infty$.*

The above result is not surprising. Note that given $b$, there are precisely $\phi(b)$ numbers $a$ coprime to $b$ in $\{1, \ldots, b\}$. In a fair world, each one of the progressions $a \pmod b$ as $a$ runs over the $\phi(b)$ residue classes coprime to $b$ should contain about the same number of primes. Since there are $\pi(x)$ primes up to $x$, it follows that in a fair world $\pi(x; b, a)$ should be about $\pi(x)/\phi(b)$, and this is exactly what Dirichlet's theorem says.

Throughout the rest of this chapter, we will concentrate on proving Dirichlet's theorem and presenting several of its applications.

## 13.4. The Primitive Divisor theorem

At the beginning of the 1900's, Birkhoff and Vandiver [**13**] came up with a completely elementary proof, much in the spirit of Theorem 13.7, stating that for every fixed positive integer $n$, the set of primes $p \equiv 1 \pmod n$ is infinite. In the remainder of this section, we will present their result.

Let $a$ and $b$ be fixed coprime integers. Let $u_n = a^n - b^n$ and let $p$ be a prime factor of $u_n$. Then $a^n \equiv b^n \pmod p$, and both $a$ and $b$ are coprime to $p$, so that $n$ is a multiple of the multiplicative order of $ab^{-1} \pmod p$. If $n$ equals this order, then $p$ is called a *primitive prime factor* of $u_n$. More generally, $p$ is a *primitive divisor* of $u_n$ if $p \mid u_n$ but $p \nmid u_m$ for each positive integer $m < n$. It is easy to see that this implies that the order of $ab^{-1}$ modulo $p$ is $n$. Since the order of every element modulo $p$ divides $p - 1$, we get that $p \equiv 1 \pmod n$. Thus, if we want to create prime factors $p \equiv 1 \pmod n$, it suffices to prove that $u_n$ has primitive divisors. This is exactly what Birkhoff and Vandiver proved. The next statement is sometimes called the *Primitive Divisor theorem* or the Birkhoff-Vandiver's theorem, even though it was proved by Zsigmondy [**149**] more than 10 years earlier.

**Theorem 13.9.** *(Primitive Divisor theorem) For each pair of coprime integers $a$ and $b$, $u_n = a^n - b^n$ has a primitive prime factor for $n > 6$.*

Note that the above lower bound 6 is best possible since $2^6 - 1 = 63 = (2^2 - 1)^2(2^3 - 1)$, so that for $a = 2,\ b = 1$, we have that $u_6$ does not have primitive divisors.

Before we prove Theorem 13.9, we need to prove a lemma which summarizes some of the relevant arithmetical properties of the sequence $\{u_n\}_{n\geq 0}$ used in the proof of the Primitive Divisor theorem.

**Lemma 13.10.** (i) $\gcd(u_n, u_m) = u_{\gcd(n,m)}$;

(ii) *if* $d \mid n$ *and* $p$ *is a prime such that* $p \mid \gcd(u_d, u_n/u_d)$, *then* $p \mid n/d$;

(iii) *if* $p \mid u_d$ *and* $p$ *is odd, then* $p \| u_{pd}/u_d$.

**Proof.** (i) follows by suitably adapting the argument from the solution of Problem 2.8. For (ii), note that if $a^d \equiv b^d \pmod{p}$, then

$$\begin{aligned}\frac{u_n}{u_d} &= \frac{(a^d)^{n/d} - (b^d)^{n/d}}{a^d - b^d} = (a^d)^{n/d-1} + (a^d)^{n/d-2}b^d + \cdots + (b^d)^{n/d-1} \\ &\equiv (a^d)^{n/d-1} + (a^d)^{n/d-2}(a^d) + \cdots + (a^d)^{n/d-1} \pmod{p} \\ &\equiv a^{n-d}(n/d) \pmod{p},\end{aligned}$$

and since $p \mid u_n/u_d$, but $p \nmid ab$, we get that $p \mid n/d$. Finally, for (iii), let $b^d = a^d + p\lambda$ for some integer $\lambda$. Then, redoing the above computation a little bit more carefully we get

$$\begin{aligned}\frac{u_{pd}}{u_d} &= \sum_{k=0}^{p-1}(a^d)^{p-k-1}(b^d)^k = \sum_{k=0}^{p-1}(a^d)^{p-k-1}(a^d + p\lambda)^k \\ &\equiv \sum_{k=0}^{p-1}(a^d)^{p-k-1}\left((a^d)^k + k\lambda p(a^d)^{k-1}\right) \pmod{p^2} \\ &\equiv \sum_{k=0}^{p-1}\left(a^{d(p-1)} + kp\lambda a^{dp-2d}\right) \pmod{p^2} \\ &\equiv pa^{d(p-1)} + \frac{p^2(p-1)}{2}\lambda a^{dp-2d} \pmod{p^2} \equiv pa^{d(p-1)} \pmod{p^2},\end{aligned}$$

where we used the binomial formula

$$\begin{aligned}(a^d + p\lambda)^k &= (a^d)^k + \binom{k}{1}(a^d)^{k-1}p\lambda + \binom{k}{2}(a^d)^{k-2}(p\lambda)^2 + \cdots + (p\lambda)^k \\ &\equiv a^{dk} + kp\lambda a^{dk-d} \pmod{p^2},\end{aligned}$$

and the fact that $p$ is odd (that is, that $(p-1)/2$ is an integer). □

**Proof of the Primitive Divisor theorem.** Assume that $n$ is large and that $a > b > 0$. We shall only prove that $u_n$ has a primitive prime factor for $n > n_0$, where $n_0$ is some absolute constant. Let

$$\Phi_n(X, Y) = \prod_{\substack{1\leq k\leq n \\ \gcd(k,n)=1}} (X - e^{2\pi ik/n}Y) \in \mathbb{Z}[X, Y]$$

be the homogenized cyclotomic polynomial for $n$, which we have already encountered in the proof of the Balog–Wooley theorem (Proposition 9.19). Recall that the homogenized polynomial

$$f(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0$$

is simply the homogeneous polynomial

$$f(X, Y) = a_d X^d + a_{d-1} X^{d-1} Y + \cdots + a_0 Y^d.$$

The formula

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X)$$

homogenizes to

$$X^n - Y^n = \prod_{d \mid n} \Phi_d(X, Y). \tag{13.5}$$

We write $\Phi_n(a, b) = AB$, where each prime $p \mid B$ is primitive for this value of $n$ and the primes $q \mid A$ are not primitive. Let $p \mid A$. Then $p \mid u_n$ and $p \mid u_d$ for some $d < n$. By Lemma 13.10 (i), we may assume that $d \mid n$ (otherwise, replace $d$ by $\gcd(d, n)$). Since $p \mid A \mid \Phi_n(a, b) \mid u_n/u_d$, where the last divisibility relation follows from equation (13.5) with $(X, Y) = (a, b)$, we get that $p \mid \gcd(u_d, u_n/u_d)$, so that by Lemma 13.10 (ii), we get that $p \mid n/d$. Thus, $d \mid n/p$, implying that $p \mid u_d \mid u_{n/p}$. But $A \mid \Phi_n(a, b) \mid u_n/u_{n/p}$. By Lemma 13.10 (iii) with $d = n/p$, we get that $p \| A$ if $p$ is odd. When $p = 2$, then $u_n$ is odd when $a$ and $b$ have different parities or when $n$ is odd. If $2 \| n$, then $A \mid u_n/u_2 = ((a^2)^{n/2} - (b^2)^{n/2})/(a^2 - b^2)$ is again odd, and if $4 \mid n$, then $A \mid u_n/u_{n/2} = a^{n/2} + b^{n/2} = (a^{n/4})^2 + (b^{n/4})^2$, and since $a$ and $b$ are odd, we have that the above sum of two odd squares is congruent to 2 (mod 4). Thus, the exponent of 2 in the factorization of $A$ is at most 1 also. This shows that $A \mid \gamma(n)$, so that $A \le n$. But note that, by the Inclusion-Exclusion principle,

$$\Phi_n(a, b) = \frac{a^n - b^n}{\prod_{p \mid n} (a^{n/p} - b^{n/p})} \cdot \frac{\prod_{\substack{p<q \\ pq \mid n}} (a^{n/pq} - b^{n/pq})}{\prod_{\substack{p<q<r \\ pqr \mid n}} (a^{n/pqr} - b^{n/pqr})} \cdots . \tag{13.6}$$

Since

$$a^d > a^d - b^d = (a - b)(a^{d-1} + \cdots + b^{d-1}) \ge a^{d-1}, \tag{13.7}$$

it follows that a lower bound on $\Phi_n(a, b)$ is obtained by replacing each factor $a^d - b^d$ from the numerator of the fraction appearing in (13.6) by $a^{d-1}$ and each factor $a^d - b^d$ from the denominator of the fraction in (13.6) by $a^d$, we get

$$\Phi_n(a, b) \ge a^{n - \sum_{p \mid n} \frac{n}{p} + \sum_{pq \mid n} \frac{n}{pq} - \cdots - 2^{\omega(n)-1}} \ge a^{\phi(n) - d(n)/2}.$$

Since $A \le n$, we get that

$$B \ge \frac{a^{\phi(n)-d(n)/2}}{n} \ge \frac{2^{\phi(n)-d(n)/2}}{n}, \tag{13.8}$$

and since $\phi(n) \gg n/\log\log n$ and $d(n) = n^{O(1/\log\log n)}$, we get that the lower bound in (13.8) is $> 1$ for $n > n_0$. Thus, $B > 1$ when $n > n_0$, implying that $u_n$ has a primitive prime factor for $n > n_0$, thereby completing the proof of the Primitive Divisor theorem. □

## 13.5. Comments on the Primitive Divisor theorem

First of all, there is no need to assume that $a$ and $b$ are positive in the statement of the Primitive Divisor theorem. We may assume just that $a$ is positive and that $1 \le |b| < a$ and that $a$ and $b$ are coprime. The same method of proof applies, except that now the bounds in (13.7) are

$$a^{d+1} \ge 2a^d > |a^d - b^d| \ge a^d - |b|^d = (a - |b|)(a^{d-1} + \cdots + |b|^{d-1}) \ge a^{d-1},$$

and the only tiny difference is that the expression "$-d(n)/2$" from the exponent of 2 in the lower bound (13.8) on $B$ will now be $-d(n)$. There are even more general versions of the Primitive Divisor theorem available, such as the following.

Let $P$ and $Q$ be coprime integers with $P^2 + 4Q \ne 0$, and let $\alpha,\ \beta$ be nonzero complex numbers such that $\alpha + \beta = P,\ \alpha\beta = -Q$. That is, $\alpha,\ \beta$ are the roots of the equation $x^2 - Px - Q = 0$. Assume also that $\alpha/\beta$ is not a root of unity. Set

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad n = 0,\ 1,\ \ldots$$

The sequence $\{u_n\}_{n\ge 0}$ is called a Lucas sequence and $\alpha,\ \beta$ its roots.

**Example 13.11.** *Let $P = 1,\ Q = 1$. Then $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. The resulting Lucas sequence $\{u_n\}_{n\ge 0}$ is the sequence of Fibonacci numbers $\{F_n\}_{n\ge 0}$.*

A prime factor $p$ of $u_n$ is called primitive if $p \mid u_n$ but $p \nmid u_m$ for any positive $m < n$ and $p \nmid \Delta = (\alpha - \beta)^2$, the discriminant of the sequence $\{u_n\}_{n\ge 0}$. It is known that if $p$ is primitive for $u_n$, then $p \equiv \pm 1 \pmod{n}$. In particular, $p \ge n - 1$. Then the more general Primitive Divisor theorem says the following.

**Theorem 13.12.** *With the above notations, $u_n$ has a primitive divisor if $n > 31$.*

Note that the Birkoff-Vandiver theorem is a particular case (up to the small values of $n$) of the Primitive Divisor theorem (indeed, take $P = a + b,\ Q = -ab$). With real $\alpha$ and $\beta$, the above theorem was proved by Carmichael in 1913 [**22**]. It has been rediscovered many times since then. The worst case (exception with highest index) is the Fibonacci sequence for which $F_{144} = 12^2 = 2^4\,3^2$, and $2 \mid F_3,\ 3 \mid F_4$. If $n > 12$ and $\alpha,\ \beta$ are real, then the $n$-th general term $u_n$ of any such Lucas sequence has a primitive divisor. Finally, for the complex case, $n = 31$ is optimal, and the worst case is the sequence $u_n$ with $\alpha = (1 + i\sqrt{7})/2,\ \beta = (1 - i\sqrt{7})/2$ having $P = 1,\ Q = -2$, which lacks primitive divisors at $n = 30$. The proof of the theorem for this case was achieved only in 2001 by Y. Bilu, G. Hanrot, and P. M. Voutier [**11**] and involved more than one year of computer calculations and resolutions of Diophantine equations with cyclotomic polynomials of very large degrees.

## Problems on Chapter 13

**Problem 13.1.** *Let $a_1, \dots, a_s$ be squarefree positive integers such that for each $i$ there exists at least one prime $p_i \mid a_i$ but $p_i \nmid a_j$ for all $j \neq i$. Then, let $\varepsilon_1, \dots, \varepsilon_i \in \{-1, +1\}$ be fixed and set $A = \operatorname{lcm}[a_1, \dots, a_s]$. Show that if $p > A$ is a prime such that*

$$\left(\frac{a_i}{p}\right) = \varepsilon_i \qquad i = 1, \dots, s,$$

*then $p \pmod A$ belongs to a subset of congruence classes of cardinality $\phi(4A)/2^s$ of the $\phi(4A)$ possible congruence classes $a \pmod{4A}$, with $a$ coprime to $A$, which can contain prime numbers.*

**Problem 13.2.** *Show that in Problem* 12.33, 3 *can be replaced by* 5 *for $m > 2$. Following Aigner, call a prime $p$ elite if $\left(\dfrac{F_n}{p}\right) = 1$ holds only for finitely many $n$. For example, $p = 3$ and $p = 5$ are elite. The rest of this problem will guide you through a proof of the fact that the sum of the reciprocals of the elite primes is convergent.*

(i) *Let $x$ be large, $v = \lfloor 10 \log\log\log x \rfloor$. Show, using the Brun-Titchmarsh theorem, that the set of primes $p \le x$ for which $2^v \mid p - 1$ has cardinality $O(x/2^v \log x) = O(x/(\log x (\log\log x)^2))$ for large $x$.*

(ii) *Set $y = x^{1/(10 \log\log x)}$. Follow the proof of Proposition* 9.11 *to show that the set of primes $p \le x$ such that either $P(p-1) < y$ or $t_p < y^{1/4}$ is of cardinality $O(x/(\log x)^2)$. Here, $t_p$ is as usual the order of* 2 *modulo $p$.*

(iii) *Let $k$ be such that $2^k \| p-1$. Show that the sequence $F_n \pmod p$ is periodic for $n \geq k$ with period $\gg \log t_p$. In particular, if $p$ satisfies (i) and (ii), then its period is $> v$ for large $x$.*

(iv) *Deduce that $F_m$ is a quadratic residue modulo $p$ for all $m = k, k+1, \ldots, k+v$.*

(v) *Let $i \leq v$ be fixed and let $F_i = M_i x_i^2$, where $M_i$ is squarefree. Show that $M_i > 1$. Further show, using the preceding problem, that if $p$ is elite, then, $p$ can be in at most $\phi(M)/2^{\lfloor v/2 \rfloor}$ of all the possible congruence classes $a \pmod M$ with $\gcd(a, M) = 1$, where $M = \prod_{i=1}^{k} M_i$.*

(vi) *Show that $M = \exp((\log\log x)^{O(1)}) = x^{o(1)}$ as $x \to \infty$ and conclude using the Brun-Titchmarsh theorem with primes in congruence classes modulo $M$, that the number of elite primes $p \leq x$ such that $2^k \| p-1$ is $\ll x/(2^{v/2} \log x)$.*

(vii) *Deduct from the above that the counting function of the elite primes is $O(x/(2^{v/2}\log x)) = O(x/(\log x(\log\log x)^2))$. Now use Abel's summation formula to conclude that the sum of the reciprocals of the elite primes is convergent.*

**Problem 13.3.** *Find all nonnegative integers $x$, $y$, and $z$ such that*

$$2^x + 3^y = 5^z.$$

For the remaining of these problems, we will use $F_n$ for the $n$-th Fibonacci number.

**Problem 13.4.** *Show that if $n$ is sufficiently large, then $F_n$ has a prime factor $p \equiv 1 \pmod 4$. (Hint: If $k$ is coprime to 6, then $L_k^2 - 5F_k^2 = -4$. Observe that $F_k$ is odd and reduce the above relation modulo any prime factor $p$ of $F_k$. Then reduce the problem to $F_{2^\alpha}$ and $F_{3^\beta}$ and show that these numbers have prime factors $p \equiv 1 \pmod 4$ as well, provided $\alpha$ and $\beta$ are sufficiently large.)*

**Problem 13.5.** *Let $p$ be a prime congruent to $17 \pmod{20}$. Show that $p | F_{(p+1)/2}$. Deduce that if there exist infinitely many primes $p \equiv 17 \pmod{20}$ such that $p+1 = 2q$, where $q$ is also a prime, then there exist infinitely many primes $q$ such that $F_q$ is composite (this is not known unconditionally). Primes $p$ such that $p+1 = 2q$, where $q$ is also a prime, are called Sophie Germain primes.*

**Problem 13.6.** *This problem is essentially a guide through a proof of the fact that $0, 1, 144$ are the only squares in the Fibonacci sequence.*

(i) *If $F_n$ is a square, $F_n$ is odd and $n$ is even, show that $F_{n/2}$ is a square.*

(ii) *If $F_n$ is a square, $F_n$ is even and $n$ is odd, show that $F_{n/3}$ is a square.*

(iii) *If $F_n$ is a square, $n$ is even and $F_n$ is also even, show that $12 \mid n$ and that either $F_{n/4}$ or $F_{n/12}$ is a square.*

(iv) *If $\gcd(n,6)=1$ and $F_n$ is a square, show that $n \equiv \pm 1 \pmod{12}$.*

(v) *Assume $n = 12m \pm 1 > 1$. Use the formula $2F_{m+n} = F_m L_n + F_n L_m$ to conclude that $F_n \equiv -1 \pmod{L_{2m}}$.*

(vi) *Show that $L_{2k}$ is divisible by a prime number $p \equiv 3 \pmod 4$ for all $k \geq 1$.*

(vii) *Conclude from (i)-(vi) that $F_0 = 0$, $F_1 = F_2 = 1$ and $F_{12} = 144$ are the only square Fibonacci numbers.*

**Problem 13.7.** (i) *Show that there are only finitely many $n$ such that $n! \mid \sigma(n!)$ (Hint: Let $2^m \parallel n!$. Then $2^{m+1} - 1 \mid \sigma(n!)$. How much of the primitive part of $2^{m+1}-1$ can be in $n!$? Use the Primitive Divisor theorem and compare with the known bound $\sigma(n!)/n!$ from Proposition 8.5.)*

(ii) *Show that there are only finitely $n$ such that $n! \mid \sigma(\sigma(n!))$ (Hint: Use a procedure similar to that used in (i), but start with the primes $p \in [n/2, n]$ to deduce that $\sigma(n!)$ is divisible by a reasonably large power of 2.)*

**Problem 13.8.** *Show that there are only finitely many positive integers $n$ such that $\phi^2(n) \mid n^2 - 1$. (Hint: Write $n^2 - d\phi(n)^2 = 1$ and let $k = \omega(n)$. Justify that $\sqrt{d} \ll \log k$. Compare $2^k$ to the power of 2 dividing $Y_1$, where $Y_1$ is the first solution of the Pell equation $X^2 - dY^2 = 1$. Use the fact that $\phi(n) = Y_\ell$ is a number divisible by $2^{k-1}$, to show that $\ell$ is divisible by $2^{k+O((\log k)^2)}$. Conclude that all prime factors of $n$ are congruent to $\pm 1 \pmod{2^{k+O((\log k)^2)}}$, and then show that $\sqrt{d} \ll \exp(2^{-k+O((\log k)^2)})$. Deduce from this that both $d$ and $k$ are bounded. Then write $\ell = q_1 \cdots q_s$ with increasing primes $q_1 < \cdots < q_s$ and show by induction that each of the $q_i$'s is bounded.)*

**Problem 13.9.** *Recall that a number $n$ is called multiply perfect if $n \mid \sigma(n)$. Let $\mathcal{A}$ be the set of all multiply perfect numbers. Show that if $\mathcal{A}$ is assumed to be infinite, then*

$$\lim_{\substack{n\to\infty \\ n\in\mathcal{A}}} P(n) = \infty.$$

**Problem 13.10.** *Given positive integers $n$ and $k$, show that there exists a positive integer $m$ such that $\phi(m+i) \equiv 0 \pmod n$ for $i = 1, 2, \ldots, k$.*

**Problem 13.11.** *Show that $\omega(2^n - 1) \geq d(n) + O(1)$.*

**Problem 13.12.** *Show that the inequality* $P(2^n - 1) > n \log n / \log\log n$ *holds for almost all positive integers* $n$. *(Hint: Let* $p$ *be a primitive divisor of* $2^n - 1$. *If* $p < n \log n / \log\log n$, *then* $kn + 1 = p$ *is a prime for some* $k < \log n / \log\log n$. *Show, using the Brun sieve, that the number of such* $n \le x$ *is* $o(x)$ *as* $x \to \infty$.*)*

**Problem 13.13.** *Find all positive integer solutions of the equation* $F_m = n!$, *where* $\{F_n\}_{n\ge 0}$ *stands for the Fibonacci sequence.*

The following two problems are essentially a guide through a proof of the fact that $P(n(n+1)) \gg \log\log n$, an estimate mentioned at the very end of Chapter 9. For this, the following two known facts about solutions to Pell equations will prove helpful.

Let $d > 1$ be an integer which is not a square. The equation $X^2 - dY^2 = 1$, called the Pell equation, always has positive integer solutions $(X, Y)$. Let $(X_1, Y_1)$ be the minimal such solution, that is, with $X_1$ minimal. Then,

(i) All other solutions in positive integers $(X, Y) = (X_k, Y_k)$ of the Pell equation are of the form $X_k + \sqrt{d}Y_k = (X_1 + \sqrt{d}Y_1)^k$.

(ii) $X_1 = \exp(O(\sqrt{d}\log d))$.

Both these facts are standard known properties of continued fractions.

**Problem 13.14.** *Show that* $Y_1 \mid Y_k$ *for all* $k \ge 1$ *and that* $Y_k/Y_1$ *is a Lucas sequence corresponding to some pair of roots. What are the roots? Deduce that* $Y_k$ *has a prime factor* $p \ge k - 1$ *if* $k > 31$.

**Problem 13.15.** *The inequality* $P(n(n+1)) \gg \log\log n$ *holds. (Hint: Assume that* $P(n(n+1)) < \varepsilon \log\log n$ *for some fixed* $\varepsilon > 0$ *very small. Write* $n = au^2$, $n + 1 = bv^2$, *where* $a$ *and* $b$ *are squarefree and let* $d = ab$. *Show that* $ab = (\log n)^{O(\varepsilon)}$. *Then show that* $X^2 - dY^2 = 1$, *where* $X = (2n+1)$, $Y = 2uv$. *Deduce that if* $Y = Y_k$, *then* $k = O(\log\log n)$. *Show that it follows that*

$$n^2 \ll X = X_k \le (2X_1)^k \le \exp(O(kd^{1/2}\log d)) = \exp((\log n)^{O(\varepsilon)}\log\log n),$$

*and conclude that in fact* $\varepsilon \gg 1$.*)*

*Chapter 14*

# Characters and the Dirichlet Theorem

## 14.1. Primitive roots

In the last chapter, we showed that there exist primitive roots modulo $p$ for any given prime $p$. Here, we start by proving a slightly more general result.

**Theorem 14.1.** *If $q = p^\alpha$ is a power of an odd prime, then the multiplicative group $U(\mathbb{Z}/q\mathbb{Z})$ of invertible congruence classes modulo $q$ is cyclic. In particular, there exists a primitive root modulo $q$, that is, a congruence class modulo $q$ whose order is $\phi(q)$.*

**Proof.** Let $a$ be an integer whose order modulo $p$ is $p-1$. Such an integer exists by Theorem 13.1. If $a^{p-1} \equiv 1 \pmod{p^2}$, then we replace $a$ by $a+p$ and note that

$$\begin{aligned}(a+p)^{p-1} &= a^{p-1} + p(p-1)a^{p-2} + \sum_{k=2}^{p} \binom{p}{k} a^{p-k}p^k \\ &\equiv a^{p-1} + p(p-1)a^{p-2} \pmod{p^2} \equiv 1 - pa^{p-2} \pmod{p^2}.\end{aligned}$$

Thus, up to replacing $a$ by $a+p$ we have that $p \| a^{p-1} - 1$. We claim that $a$ is a primitive root modulo $p^\alpha$ for all positive integers $\alpha$. We prove this by induction. Assume that $a^k \equiv 1 \pmod{p^{\alpha-1}}$ implies that $p^{\alpha-1}(p-1) \mid k$ for some $\alpha \geq 2$ and we will prove it replacing $\alpha - 1$ by $\alpha$. Assume that $a^k \equiv 1 \pmod{p^\alpha}$. In particular, $p^{\alpha-1} \mid a^k - 1$, so that by the induction hypothesis, $p^{\alpha-1}(p-1) \mid k$. Write $k = p^{\alpha-1}(p-1)\ell$ and observe that, with the notation

$u_m = a^m - 1$,

$$u_k = \frac{u_{p^{\alpha-1}(p-1)\ell}}{u_{p^{\alpha-1}(p-1)}} \cdot \frac{u_{p^{\alpha-1}(p-1)}}{u_{p^{\alpha-2}(p-1)}} \cdots \frac{u_{p(p-1)}}{u_{p-1}} \cdot u_{p-1}. \tag{14.1}$$

By hypothesis, $p \| u_{p-1}$ and by Lemma 13.10 (iii), we have that

$$p \| u_{p^i(p-1)}/u_{p^{i-1}(p-1)} \qquad \text{for } \ i = 1, \dots, \alpha - 2.$$

Thus, counting the powers of $p$ in the left- and right-hand sides of equation (14.1), we get that

$$p \mid \frac{u_{p^{\alpha-1}(p-1)\ell}}{u_{p^{\alpha-1}(p-1)}},$$

and since certainly $p \mid u_{p^{\alpha-1}(p-1)}$, Lemma 13.10 (ii) tells us that $p \mid \ell$, which is what we wanted to prove. □

When $p = 2$, the group of invertible classes modulo $p^\alpha$ is cyclic when $\alpha = 1,\ 2$, but not when $\alpha \geq 3$. However, it is almost cyclic in the sense of the following result.

**Theorem 14.2.** *If $\alpha \geq 3$, then the order of 5 modulo $2^\alpha$ is $2^{\alpha-2}$. Furthermore, every invertible class modulo $2^\alpha$ is of the form $\varepsilon 5^t$, for some uniquely determined $\varepsilon \in \{-1, 1\}$ and $t \in \{0, 1, \dots, 2^{\alpha-2} - 1\}$.*

**Proof.** We show that $5^k \equiv 1 \pmod{2^\alpha}$ for some $\alpha \geq 3$ if and only if $2^{\alpha-2} | 5^k - 1$. When $\alpha = 3$, we have that $5^k - 1 = 4(5^{k-1} + \cdots + 1)$ and since the second factor is congruent to $k \pmod 2$, we get that $8 \mid 5^k - 1$ if and only if $k$ is even. Assume now that $k = 2^\beta m$, where $m$ is odd and note that

$$5^k - 1 = 4\frac{5^m - 1}{4}(5^m + 1)(5^{2m} + 1) \cdots (5^{2^{\beta-1}} + 1),$$

and $(5^m - 1)/4 = 5^{m-1} + \cdots + 1$ is odd for odd $m$, while $5^n + 1 \equiv 2 \pmod 4$ for all non-negative integers $n$. Thus, the exponent of 2 in the factorization of $5^k - 1$ is precisely $2 + \beta$ and in particular it is $\geq \alpha$ if and only if $\beta \geq \alpha - 2$. Hence, both sets of congruence classes

$$\{5^t \bmod 2^\alpha : t = 0, \dots, 2^{\alpha-2} - 1\} \ \text{ and } \ \{-5^t \bmod 2^\alpha : t = 0, \dots, 2^{\alpha-2} - 1\}$$

each contain exactly $2^{\alpha-2}$ invertible congruence classes modulo $2^\alpha$. Note also that they do not share any element in common since the elements in the first set are all congruent to $1 \pmod 4$ while the ones in the second set are all congruent to $-1 \pmod 4$. Thus, their union contains $2^{\alpha-1} = \phi(2^\alpha)$ distinct invertible congruence classes modulo $2^\alpha$, hence all of them. □

There are many interesting questions concerning the primitive roots for prime moduli. For example, Hua proved that there exists $a < 2^{\omega(p-1)}\sqrt{p}$ which is a primitive root modulo $p$. Artin conjectured that if $a \neq -1$ is an integer which is not a square, then $a$ is a primitive root modulo $p$ for

infinitely many primes $p$. This is unknown. The best-known result in this direction is that one of 2, 3, 5 is a primitive root modulo $p$ for infinitely many primes $p$. Here is some evidence for the truth of Artin's conjecture.

**Example 14.3.** *Assume that $q \equiv 1 \pmod 8$ is a prime number such that $p = 2q+1$ is also a prime. Then 2 is a primitive root modulo $p$. Indeed, the only divisors of $p-1$ in this case are $\{1, 2, (p-1)/2, p-1\}$. The order of 2 modulo $p$ cannot be 1 or 2 (because $p > 3$) and it cannot be $(p-1)/2$, for otherwise 2 would be a quadratic residue modulo $p$, but this is not the case since $p \equiv 3 \pmod 8$. Thus, the order of 2 modulo $p$ is $p-1$. Incidentally, the Prime $k$-tuples conjecture suggests that there should be infinitely many such primes $q$.*

## 14.2. Characters

A *character* of an abelian group $G$ is simply a group homomorphism from $G$ into $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. We write this as $\chi : G \to \mathbb{C}^*$. There is a well-developed theory of characters for all finite groups, even for the non-abelian ones. Here, we will illustrate this theory only in the case when the group $G$ is the group of invertible congruence classes modulo $k$ for some positive integer $k$. In this case, the character $\chi$ is said to be a *character modulo $k$*. We think of $\chi$ as a function defined on the invertible classes $n \pmod k$ whose values are nonzero complex numbers such that $\chi(n_1 n_2 \pmod k) \equiv \chi(n_1 \pmod k)\chi(n_2 \pmod k)$ whenever $n_1 \pmod k$ and $n_2 \pmod k$ are invertible congruence classes modulo $k$. It is convenient to extend this definition and consider $\chi : \mathbb{N} \to \mathbb{C}$, such that $\chi(n)$ is the value of $\chi$ on the residue class of $n$ modulo $k$, if $n$ is invertible modulo $k$ and $\chi(n) = 0$ if $(n, k) > 1$. With this definition, we have that a character modulo $k$ is simply a function $\chi : \mathbb{N} \to \mathbb{C}$ such that

(i) $\chi(1) = 1$;

(ii) $\chi(n_1) = \chi(n_2)$ if $n_1 \equiv n_2 \pmod k$;

(iii) $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$;

(iv) $\chi(n) = 0$ if and only if $(n, k) > 1$.

The so-called principal character is denoted by $\chi_0(n)$ and is defined by $\chi_0(n) = 1$ if $(n, k) = 1$ and $\chi_0(n) = 0$ otherwise. The important question is, of course, to understand the properties of the non-principal characters. Before moving on to the theorems, let us examine some examples of characters.

**Example 14.4.** *For $k = 2$, the principal character is the only one. For $k = 3$, there are two characters, namely*

$$\chi_0(n) = \begin{cases} 1 & \text{if } n \equiv 1,\ 2 \mod 3, \\ 0 & \text{if } n \equiv 0 \mod 3, \end{cases} \qquad \chi_1(n) = \begin{cases} 1 & \text{if } n \equiv 1 \mod 3, \\ -1 & \text{if } n \equiv -1 \mod 3, \\ 0 & \text{if } n \equiv 0 \mod 3. \end{cases}$$

**Example 14.5.** *For $k = 4$, there are again two characters, namely*

$$\chi_0(n) = \begin{cases} 1 & \text{if } n \text{ is odd}, \\ 0 & \text{if } n \text{ is even}, \end{cases} \qquad \chi_1(n) = \begin{cases} 1 & \text{if } n \equiv 1 \mod 4, \\ -1 & \text{if } n \equiv -1 \mod 4, \\ 0 & \text{if } n \text{ is even}. \end{cases}$$

**Example 14.6.** *For $k = 5$, there are four characters given in the following table:*

| $n \pmod 5$ | 1 | 2 | 3 | 4 | 0 |
|---|---|---|---|---|---|
| $\chi_0(n)$ | 1 | 1 | 1 | 1 | 0 |
| $\chi_1(n)$ | 1 | $i$ | $-i$ | $-1$ | 0 |
| $\chi_2(n)$ | 1 | $-1$ | $-1$ | 1 | 0 |
| $\chi_3(n)$ | 1 | $-i$ | $i$ | $-1$ | 0 |

We shall see that in all of the above examples, we have provided the complete lists of all the group characters.

## 14.3. Theorems about characters

For now, let us take for granted the existence of non-principal characters. This will later be proved in Theorem 14.9.

**Theorem 14.7.** *If $\chi$ is not the principal character, then*

$$\sum_{n=1}^{k} \chi(n) = 0.$$

**Proof.** Since $\chi$ is not the principal character $\chi_0$, there exists an integer $a$ coprime to $k$ such that $\chi(a) \neq 1$. Then

$$\sum_{n=1}^{k} \chi(n) = \sum_{n=1}^{k} \chi(an),$$

since as $n$ runs through all the residue classes coprime to $k$, so does $an$. But we have $\chi(an) = \chi(a)\chi(n)$. Thus,

$$\sum_{n=1}^{k} \chi(n) = \chi(a) \sum_{n=1}^{k} \chi(n),$$

or

$$(1-\chi(a))\sum_{n=1}^{k}\chi(n)=0,$$

which implies the desired conclusion since $1-\chi(a)\neq 0$. □

When $\chi=\chi_0$ is the principal character, we of course have

$$\sum_{n=1}^{k}\chi_0(n)=\phi(k).$$

**Theorem 14.8.** *The characters modulo $k$ form a finite abelian group.*

**Proof.** There are only finitely many of them since $\chi(n)$ can take only values which are $\phi(k)$-th roots of unity whenever $n$ is invertible modulo $k$. Thus, there cannot be more than $\phi(k)^{\phi(k)}$ characters. The product of two characters is a character since it satisfies conditions (i)–(iv) stated at the beginning of Section 14.2. The associativity of the multiplication is inherent, the identity of the group is just the principal character $\chi_0$ since

$$\chi_0(n)\chi(n)=\chi(n)$$

for all characters $\chi$ modulo $k$ and integers $n$, and the inverse of a character is its complex conjugate $\overline{\chi}$ since $\chi(n)\overline{\chi}(n)=\chi_0(n)$. □

We notice that if $d\mid k$ and $\chi$ is a known character modulo $d$, then we may construct a character $\chi^*$ modulo $k$ by setting

$$\chi^*(n)=\chi(n)\qquad\text{if } (n,k)=1,$$

and $\chi^*(n)=0$ otherwise. It is easy to verify that $\chi^*$ satisfies the mentioned conditions (i)–(iv). We refer to this process as the *extension* of the character $\chi$ of modulus $d$ to the modulus $k$.

We now come to the existence of non-principal characters.

**Theorem 14.9.** *If $(a,k)=1$ and $a\not\equiv 1 \pmod{k}$, then there exists a character $\chi$ modulo $k$ such that $\chi(a)\neq 1$.*

**Proof.** Let $k=2^{\alpha}p_1^{\beta_1}\cdots p_s^{\beta_s}$, where $p_1<\cdots<p_s$ are odd primes and the $\beta_i$'s positive integers. By our assumption and the Chinese Remainder Theorem, not all congruences $a\equiv 1 \pmod{2^{\alpha}}$ and $a\equiv 1 \pmod{p_i^{\beta_i}}$ can be fulfilled. Assume first that $a\not\equiv 1 \pmod{p^{\beta}}$ for some odd prime factor $p=p_i$, where $\beta=\beta_i$. Let $g$ be a primitive root modulo $p^{\beta}$, which exists by Theorem 14.1. Let $\chi$ be the character modulo $p^{\beta}$ given by $\chi(g)=e^{2\pi i/\phi(p^{\beta})}$. Clearly, $a=g^{\lambda} \pmod{p^{\beta}}$ for some $\lambda\in\{1,\ldots,p^{\beta}-1\}$. Thus, $\chi(a)=e^{2\pi\lambda/\phi(p^{\beta})}\neq 1$. Let $\chi^*$ be the extension of $\chi$ from $p^{\beta}$ to $k$. Then $\chi^*(a)=\chi(a)$ since $(a,k)=1$, so that $\chi^*(a)\neq 1$ and $\chi^*$ is a character modulo $k$.

Assume now that $a \not\equiv 1 \pmod{2^\alpha}$. The case $\alpha = 1$ is impossible since it leads to 2 dividing both $a$ and $k$, which is not possible. If $\alpha = 2$, then $a \equiv -1 \pmod 4$. Let $\chi = \chi_1$ be the character modulo 4 that we have constructed. We see that $\chi(a) = -1 \neq 1$. Since $4 \mid k$, we can extend $\chi$ to $\chi^*$, a character modulo $k$ for which we still have that $\chi^*(a) = \chi(a) = -1$, because $(a, k) = 1$. Finally, assume that $\alpha > 2$. If $a \equiv -1 \pmod{2^\alpha}$, then $a \equiv -1 \pmod 4$, and we can proceed as in the previous case. Finally, assume that $a \not\equiv -1 \pmod{2^\alpha}$. Let $\chi$ be a character modulo $2^\alpha$ such that $\chi(-1) = 1$ and $\chi(5) = e^{2\pi i/2^{\alpha-2}}$. The fact that this is well defined follows from Theorem 14.2. Since $a \not\equiv \pm 1 \pmod{2^\alpha}$, it follows that $a \equiv \pm 5^v$ for some $v \in \{1, 2, \ldots, 2^{\alpha-2} - 1\}$. Clearly, $\chi(a) = e^{2\pi i v/2^{\alpha-2}} \neq 1$. The extension $\chi^*$ of $\chi$ to $k$ has again the property that $\chi^*(a) = \chi(a) \neq 1$. This completes the proof of the theorem. □

**Theorem 14.10.** *If $a \not\equiv 1 \pmod k$, then*

$$\sum_\chi \chi(a) = 0,$$

*where the sum runs over all the characters $\chi$ modulo $k$.*

**Proof.** Let $\chi^*$ be a character modulo $k$ with $\chi^*(a) \neq 1$ whose existence was proved in Theorem 14.9. When $\chi$ runs over all the characters modulo $k$, so does $\chi^*\chi$ since all these characters form a group. Therefore,

$$\sum_\chi \chi(a) = \sum_\chi (\chi^*\chi)(a) = \sum_\chi \chi^*(a)\chi(a),$$

implying that

$$(1 - \chi^*(a)) \sum_\chi \chi(a) = 0,$$

which gives the desired conclusion since $1 - \chi^*(a) \neq 0$. □

**Theorem 14.11.** *There are $\phi(k)$ distinct characters modulo $k$.*

**Proof.** By rearranging summands of the double sums we get

$$\sum_\chi \sum_{n=1}^{k} \chi(n) = \sum_{n=1}^{k} \sum_\chi \chi(n). \tag{14.2}$$

The inner sum on the left-hand side is

$$\sum_{n=1}^{k} \chi(n) = \begin{cases} \phi(k) & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise,} \end{cases}$$

by Theorem 14.7. The inner sum on the right-hand side is, by Theorem 14.10, 0 for $n \not\equiv 1 \pmod k$ and it obviously equals the number $c$ of characters modulo $k$ when $n \equiv 1 \pmod k$ since in that case each summand contributes

a 1. Thus, equation (14.2) yields $\phi(k) = c$, which is what we wanted to prove. □

The above theorem shows that our tables for characters modulo $k$ for $k = 2, 3, 4, 5$ were complete since in each case the list contained $\phi(k)$ characters.

An important consequence of Theorem 14.11 is the following equation.

$$\sum_{\chi} \overline{\chi}(a)\chi(n) = \begin{cases} \phi(k) & \text{if } a \equiv n \pmod{k}, \\ 0 & \text{otherwise.} \end{cases} \tag{14.3}$$

Indeed, $\overline{\chi}(a)$ is the reciprocal of $\chi(a)$, so that

$$\overline{\chi}(a) = \chi(a)^{-1} = \chi(a'),$$

where $a'$ is the inverse of $a$ modulo $k$. Thus, the given sum on the left-hand side of (14.3) reduces to

$$\sum_{\chi} \chi(a'n),$$

and this can be handled by Theorems 14.10 and 14.11.

The last theorem that we need to prove about characters is the following one.

**Theorem 14.12.** *For $(a, k) = 1$, let $f$ be the smallest positive exponent such that $a^f \equiv 1 \pmod{k}$. Then $\chi(a)$ is an $f$-th root of unity and all $f$-th roots of unity appear equally often as $\chi(a)$ if $\chi$ runs over all the characters modulo $k$.*

**Proof.** Since $\chi(a)^f = \chi(a^f) = 1$, the first assertion about $\chi(a)$ is clear. If moreover, $a \equiv 1 \pmod{k}$, then $\chi(a) = 1$ for all $\chi$ and there is nothing else to prove. Thus, we may assume that $a \not\equiv 1 \pmod{k}$ so that $f > 1$. Let $\varepsilon$ be a fixed $f$-th root of 1. We want to know how often $\chi(a) = \varepsilon$ among the values of $\chi(a)$ as $\chi$ runs over all the characters and to show that this frequency does not depend on $\varepsilon$. We consider the following sum:

$$S = \sum_{\chi} \{\varepsilon^{-1}\chi(a) + \varepsilon^{-2}\chi(a^2) + \cdots + \varepsilon^{-f}\chi(a^f)\},$$

which we write in two ways as

$$\sum_{\chi} \sum_{\ell=1}^{f} (\varepsilon^{-1}\chi(a))^{\ell} = \sum_{\ell=1}^{f} \varepsilon^{-\ell} \sum_{\chi} \chi(a^{\ell}).$$

The inner sum on the right-hand side is 0 if $a^{\ell} \not\equiv 1 \pmod{k}$, that is, for $\ell = 1, 2, \ldots, f-1$, and it is $\phi(k)$ for $\ell = f$. Moreover, $\varepsilon^{-f} = 1$. Hence,

$S = \phi(k)$. In the inner sum on the left-hand side, we set $\eta = \varepsilon^{-1}\chi(a)$, which is a certain $f$-th root of 1. Hence, this inner sum becomes

$$\sum_{\ell=1}^{f} \eta^{\ell} = \begin{cases} f & \text{for } \eta = 1, \\ 0 & \text{otherwise.} \end{cases}$$

This means that $S = e \cdot f$, where $e$ is the number of times $\eta = 1$, meaning that $e$ is the number of times $\chi(a) = \varepsilon$. Consequently, we have $e = \phi(k)/f$, a number which is independent of the particular choice of $\varepsilon$. □

## 14.4. $L$-series

Here, we initiate the proof of Dirichlet's theorem. It is fair to say that its proof was the greatest achievement of number theory in the mid 19th century. Recall that the goal is to show the following result, but observe that its proof will not be complete until the end of section 14.7.

**Theorem 14.13.** *If $a$ and $k > 0$ are coprime integers, then there exist infinitely many primes $p \equiv a \pmod{k}$.*

Let $\chi$ be any character modulo $k$. The Dirichlet series for $\chi$ is

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

for any real $s > 1$. Throughout this section, $s > 1$ is a real number which will eventually tend to 1.

Clearly, $L(s, \chi)$ is absolutely convergent since it is bounded above by $\zeta(s) = \sum_{n \geq 1} 1/n^s$. The Euler product representation unfolds immediately as a consequence of absolute convergence, unique factorization, and the multiplicative property of $\chi$:

(14.4)
$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \cdots\right) = \prod_{p} \frac{1}{1 - (\chi(p)/p^s)}.$$

When $\chi = \chi_0$ is the principal character,

(14.5)
$$\begin{aligned} L(s, \chi_0) &= \sum_{\substack{n \geq 1 \\ (n,k)=1}} \frac{1}{n^s} = \prod_{p \nmid k} \frac{1}{1 - (1/p^s)} \\ &= \prod_{p} \frac{1}{1 - (1/p^s)} \cdot \prod_{p \,|\, k} \left(1 - \frac{1}{p^s}\right) = \zeta(s) \prod_{p | k} \left(1 - \frac{1}{p^s}\right). \end{aligned}$$

If we take logarithms in (14.4), we have

$$\begin{aligned}\log L(s,\chi) &= -\sum_p \log\left(1-\frac{\chi(p)}{p^s}\right) = \sum_p \sum_{m\geq 1} \frac{1}{m}\frac{\chi(p)^m}{p^{ms}} \\ &= \sum_p \frac{\chi(p)}{p^s} + \sum_{m\geq 2}\frac{1}{m}\sum_p \frac{\chi(p)^m}{p^{ms}}.\end{aligned} \tag{14.6}$$

Now let $a$ be any number coprime to $k$. Multiplying relation (14.6) by $\overline{\chi}(a)$, summing up the resulting relations over all characters $\chi$ modulo $k$ and using the fact that

$$\sum_\chi \overline{\chi}(a)\chi(n) = \begin{cases} \phi(k) & \text{if } a \equiv n \pmod k, \\ 0 & \text{otherwise} \end{cases}$$

(see relation (14.3)), we get that

$$\frac{1}{\phi(k)}\sum_\chi \overline{\chi}(a)\log L(s,\chi) = \sum_{p\equiv a \pmod k} \frac{1}{p^s} + H_a(s), \tag{14.7}$$

where

$$H_a(s) = \frac{1}{\phi(k)}\sum_\chi \overline{\chi}(a)\sum_{m\geq 2}\frac{1}{m}\sum_p \frac{\chi(p^m)}{p^{ms}},$$

so that

$$\begin{aligned}|H_a(s)| &\leq \sum_{m\geq 2}\frac{1}{m}\sum_p \frac{1}{p^{ms}} < \sum_{m\geq 2}\sum_{n\geq 2}\frac{1}{n^{ms}} \\ &= \sum_{n\geq 2}\sum_{m\geq 2}\frac{1}{n^{ms}} = \sum_{n\geq 2}\frac{1}{n^{2s}}\frac{1}{1-(1/n^s)} \ll \sum_{n\geq 2}\frac{1}{n^{2s}} \leq \zeta(2) < \infty\end{aligned}$$

for all $s \geq 1$. Hence, in order to prove Dirichlet's theorem, we need to show that

$$\sum_{p\equiv a \pmod k}\frac{1}{p^s} \longrightarrow \infty$$

as $s \to 1$. Since $H_a(s)$ remains bounded, this will be accomplished, via relation (14.7), if we can prove that

$$\sum_\chi \overline{\chi}(a)\log L(s,\chi) \to \infty \qquad \text{as} \qquad s \to 1. \tag{14.8}$$

Notice that the above sum is real. Proving (14.8) is now our goal.

One of the summands, namely the one corresponding to $\chi = \chi_0$, does go to infinity when $s \to 1$. Indeed, estimate (14.5) together with formula (3.2) gives

$$(s-1)L(s,\chi_0) = (s-1)\zeta(s)\prod_{p\,|\,k}\left(1-\frac{1}{p^s}\right) \longrightarrow \frac{\phi(k)}{k} \qquad \text{as} \qquad s \to 1,$$

so that $L(s,\chi_0)\to\infty$ as $s\to 1$. This shows that the term $\chi_0(a)\log L(s,\chi_0(a))$ tends to infinity as $s\to 1$. Thus, in order to prove that the sum appearing on the left-hand side of (14.8) tends to infinity, it is sufficient to show that no mutual compensation among the terms of that sum might render a finite quantity. Thus, it will be sufficient to show that no other term goes to infinity in absolute value. But in order to show that $|\log L(s,\chi)|$ does not tend to infinity, we need to show that $L(s,\chi)$ does *not go to* $\infty$ *or to* 0.

## 14.5. $L(1,\chi)$ is finite if $\chi$ is a non-principal character

This part of the task is relatively easy. First $L(s,\chi)\neq 0$ for $s>1$ because in this range $L(s,\chi)$ is an absolutely convergent product for which no factor vanishes. We now show that $L(s,\chi)$, for $\chi\neq\chi_0$, is continuous and differentiable for $s>0$. For this purpose, we use again Abel's summation formula. Let $x$ be any positive real number and consider the auxiliary sum

$$S(\chi,x)=\sum_{n\le x}\chi(n).$$

Given that $\sum_{n=1}^{k}\chi(n)=0$ (see Theorem 14.7), it follows that $\sum_{n=1}^{k}\chi(k\ell+n)=0$ for all integers $\ell\ge 0$. Thus,

$$\begin{aligned}|S(\chi,x)| &= \left|\sum_{\ell=0}^{\lfloor x/k\rfloor-1}\sum_{n=1}^{k}\chi(k\ell+n)+\sum_{k\lfloor x/k\rfloor\le n\le x}\chi(n)\right| \le \sum_{\substack{\lfloor x/k\rfloor\le n\le x\\(n,k)=1}}1\\ &\le \phi(k)=O(1).\end{aligned}$$

Hence, for $s>0$ and $N>M$, we have, by Abel's summation formula with $f(t)=1/t^s$, that

$$\begin{aligned}S(\chi,M,N)=\sum_{n=M+1}^{N}\frac{\chi(n)}{n^s} &= \sum_{n\le N}\frac{\chi(n)}{n^s}-\sum_{n\le M}\frac{\chi(n)}{n^s}\\ &= \frac{S(\chi,N)}{N^s}-\frac{S(\chi,M)}{M^s}-\int_M^N S(\chi,t)\frac{(-s)}{t^{s+1}}dt\\ &= O\left(\frac{1}{M^s}\right)+O\left(s\int_M^N\frac{1}{t^{s+1}}dt\right)\ll\frac{1}{M^s}.\end{aligned}\tag{14.9}$$

Cauchy's convergence criterion ensures the convergence of the series $L(s,\chi)$ for all $s>0$ and uniform convergence for all $s\ge\delta$, where $\delta>0$ is fixed. The formal derivative of $L(s,\chi)$ is

$$-\sum_{n=1}^{\infty}\frac{\chi(n)\log n}{n^s},\tag{14.10}$$

and the same argument will show uniform convergence of this derivative for all $s \geq \delta > 0$. Thus, $L(s,\chi)$ is differentiable for all $s > 0$ and has (14.10) as its derivative. Note that the arguments at this step can be replaced by Newman's theorem (Theorem 5.1), or we can rework from scratch and show that for all $s > 0$ fixed,

$$\left| \frac{L(s+h,\chi) - L(s,\chi)}{h} + \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \right| \to 0 \qquad \text{as} \qquad h \to 0,$$

in the same way as we did in the proof of Proposition 3.5. The important result that we will retain from these arguments is that $L(s,\chi)$ is continuous at $s > 0$ and therefore that $L(1,\chi)$ is finite. Moreover, $L(s,\chi)$ has a derivative at $s = 1$, so that

$$\frac{L(s,\chi) - L(1,\chi)}{s-1} = L'(1,\chi) + \eta_1(s),$$

for some number $L'(1,\chi)$ and some function $\eta_1(s) \to 0$ as $s \to 1$. In particular, if $L(1,\chi) = 0$, then we would have that

$$L(s,\chi) = (s-1)(L'(1,\chi) + \eta_1(s))$$

as $s \to 1$.

## 14.6. The nonvanishing of $L(1,\chi)$: first step

We now show that $L(1,\chi) \neq 0$ for all non-principal characters $\chi$. We achieve this in two steps. In the first step, we form the product of all $L(s,\chi)$:

$$F(s) = \prod_{\chi} L(s,\chi) = \prod_{p \nmid k} \prod_{\chi} \frac{1}{1 - (\chi(p)/p^s)} \qquad \text{for all } s > 1.$$

We now apply Theorem 14.12 to $\chi(p)$. If $f$ is the smallest positive integer such that $p^f \equiv 1 \pmod{k}$, then $\chi(p)$ is an $f$-th root of unity, say $\varepsilon$. All such $\varepsilon$ occur with the same multiplicity $e = \phi(k)/f$ as $\chi$ runs over all the characters modulo $k$. This means that

$$\prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right) = \prod_{\varepsilon} \left(1 - \frac{\varepsilon}{p^s}\right)^e,$$

where $\varepsilon$ runs over all the $f$-th roots of unity. Now since

$$\prod_{\varepsilon} (x - \varepsilon) = x^f - 1,$$

we have that

$$\prod_{\varepsilon} \left(1 - \frac{\varepsilon}{x}\right) = 1 - \frac{1}{x^f}.$$

Therefore

$$\prod_{\varepsilon}\left(1-\frac{\varepsilon}{p^s}\right)=1-\frac{1}{p^{fs}},$$

so that

$$\prod_{\chi}\left(1-\frac{\chi(p)}{p^s}\right)=\left(1-\frac{1}{p^{fs}}\right)^e\le 1-\frac{1}{p^{efs}}.$$

Here we used the inequality $(1-x)^n\le 1-x^n$, which is clearly valid for all $n\ge 1$ and $x\in[0,1]$. Setting $h=\phi(k)=ef$, we thus have

$$F(s)=\prod_{\chi}L(s,\chi)\ge\prod_{p\nmid k}\frac{1}{1-(1/p^{hs})}=\zeta(hs)\prod_{p\,|\,k}\left(1-\frac{1}{p^{hs}}\right),$$

which implies that for $s>1$,

$$F(s)=\prod_{\chi}L(s,\chi)\ge\zeta(hs)\prod_{p\,|\,k}\left(1-\frac{1}{p}\right)>\frac{\phi(k)}{k}. \tag{14.11}$$

We shall show that the above fact precludes that two or more of the $L(1,\chi)$'s vanish. Indeed, assume that $L(1,\chi_1)=L(1,\chi_2)=0$ for two characters $\chi_1$ and $\chi_2$. Clearly, $\chi_1,\ \chi_2\ne\chi_0$. Then $F(s)$ would contain, besides other factors that are continuous (thus bounded) at $s=1$, the factor

$$L(s,\chi_0)L(s,\chi_1)L(s,\chi_2)=L(s,\chi_0)(s-1)^2(L'(1,\chi_1)+\eta_1(s))(L'(1,\chi_2)+\eta_2(s)),$$

where $\eta_1(s)\to 0$ and $\eta_2(s)\to 0$ as $s\to 1$. But since $(s-1)L(s,\chi_0)\to\phi(k)/k$, we would get that $F(s)\to 0$ as $s\to 1$, which would contradict inequality (14.11).

If now $L(1,\chi)=0$ for some complex character $\chi$ (that is, which assumes complex non-real values), then $\overline{\chi}$ is also a character of $k$ which is distinct from $\chi$, and clearly $L(1,\overline{\chi})=\overline{L(1,\chi)}=0$. But we have just seen that this is impossible.

Thus, if $L(s,\chi)=0$ for some $\chi$, then $\chi$ is unique and real (it assumes only the values $\pm1$). In order to complete the proof of this nice theorem, we will show that $L(1,\chi)\ne 0$ for all real non-principal characters as well.

## 14.7. The completion of the proof of the Dirichlet theorem

Recall that all we are left with is to show that if $\chi$ is a real non-principal character modulo $k$, then

$$L(1,\chi)\ne 0. \tag{14.12}$$

The following argument is due to Mertens.

Note that $\chi : \mathbb{N} \to \{0, \pm 1\}$ is, in particular, a multiplicative function. So, if we let

$$f(n) = \sum_{d|n} \chi(d) = 1 * \chi,$$

then $f$ is also multiplicative (see Proposition 6.7). Note further that since $\chi(p) = \pm 1$, we get that

$$f(p^\ell) = \chi(1) + \chi(p) + \cdots + \chi(p^\ell) \geq 0$$

for all $\ell$, and, in fact, $f(p^\ell) \geq 1$ whenever $\ell$ is even. Using the fact that $f$ is multiplicative, we get that $f(m^2) \geq 1$. Thus,

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^{1/2}} \geq \sum_{m \geq 1} \frac{f(m^2)}{m} \geq \sum_{m \geq 1} \frac{1}{m}$$

which diverges. Let us take a closer look at this divergence. We have

$$G(x) = \sum_{n \leq x} \frac{f(n)}{n^{1/2}} = \sum_{n \leq x} \frac{1}{n^{1/2}} \sum_{d \,|\, n} \chi(d) = \sum_{td \leq x} \frac{\chi(d)}{(td)^{1/2}}.$$

In this last sum, we are summing over the lattice points $(t, d)$ under the hyperbola $td \leq x$ in the $(t, d)$-plane, where $x$ is an integer. We now use the argument previously used in the proof of Theorem 4.9. Namely, we break the lattice points under the hyperbola in two sets, according to whether $d \leq \sqrt{x}$ or $d > \sqrt{x}$. We then have

$$\begin{aligned} G(x) = & \sum_{1 \leq d \leq \sqrt{x}} \frac{\chi(d)}{d^{1/2}} \sum_{1 \leq t \leq x/d} \frac{1}{t^{1/2}} + \sum_{t \leq \sqrt{x}} \frac{1}{t^{1/2}} \sum_{\sqrt{x+1} \leq d \leq x/t} \frac{\chi(d)}{d^{1/2}} \\ = & G_1(x) + G_2(x), \end{aligned} \tag{14.13}$$

say. By Abel's summation formula, we have that

$$\begin{aligned} \sum_{1 \leq t \leq y} \frac{1}{t^{1/2}} &= \frac{\lfloor y \rfloor}{y^{1/2}} - \int_1^t \lfloor t \rfloor \frac{d}{dt}\left(\frac{1}{t^{1/2}}\right) dt = \frac{y - \{y\}}{y^{1/2}} + \frac{1}{2}\int_1^y \frac{t - \{t\}}{t^{3/2}} dt \\ &= y^{1/2} + O\left(\frac{1}{y^{1/2}}\right) + \frac{1}{2}\int_1^y \frac{dt}{t^{1/2}} - \frac{1}{2}\int_1^y \frac{\{t\}}{t^{3/2}} dt \\ &= y^{1/2} + \left(t^{1/2}\Big|_{t=1}^{t=y}\right) - \frac{1}{2}\left(\int_1^\infty \frac{\{t\}}{t^{3/2}} dt - \int_y^\infty \frac{\{t\}}{t^{3/2}} dt\right) \\ &\qquad + \; O\left(\frac{1}{y^{1/2}}\right) \\ &= 2y^{1/2} + \left(-1 - \frac{1}{2}\int_1^\infty \frac{\{t\}}{t^{3/2}} dt\right) + O\left(\frac{1}{y^{1/2}} + \int_y^\infty \frac{dt}{t^{3/2}}\right) \\ &= 2y^{1/2} + C + O\left(\frac{1}{y^{1/2}}\right), \end{aligned}$$

where $C$ is the constant

$$C = -1 - \frac{1}{2}\int_1^\infty \frac{\{t\}}{t^{3/2}}dt.$$

Hence,

$$\begin{aligned} G_1(x) &= \sum_{1\le d\le\sqrt{x}} \frac{\chi(d)}{d^{1/2}}\left(2\sqrt{\frac{x}{d}} + C + O\left(\sqrt{\frac{d}{x}}\right)\right) \\ &= 2\sqrt{x}\sum_{1\le d\le\sqrt{x}}\frac{\chi(d)}{d} + C\sum_{1\le d\le\sqrt{x}}\frac{\chi(d)}{d^{1/2}} + O\left(\frac{\sqrt{x}}{\sqrt{x}}\right) \\ &= 2\sqrt{x}\left(\sum_{d=1}^{\infty}\frac{\chi(d)}{d} - \sum_{d>\sqrt{x}}\frac{\chi(d)}{d}\right) + O(1), \end{aligned} \tag{14.14}$$

where we used the fact that

$$\sum_{1\le d\le\sqrt{x}}\frac{\chi(d)}{d^{1/2}} = L(1/2,\chi) + o(1) = O(1).$$

Finally, the estimate (14.9) with $N=\infty$, $M = x^{1/2}$ and $s=1$, shows that

$$\sum_{d>\sqrt{x}}\frac{\chi(d)}{d} = O\left(\frac{1}{\sqrt{x}}\right).$$

Hence, estimate (14.14) tells us that

$$G_1(x) = 2\sqrt{x}L(1,\chi) + O(1).$$

We are left with examining the size of

$$G_2(x) = \sum_{1\le t\le\sqrt{x}}\frac{1}{t^{1/2}}\sum_{\sqrt{x+1}\le d\le x/t}\frac{\chi(d)}{d^{1/2}}.$$

Again applying formula (14.9) with $M = \lfloor\sqrt{x+1}\rfloor$, $N = \lfloor x/t\rfloor$ and $s=1/2$, we get that the inner sums are bounded by

$$\left|\sum_{\sqrt{x+1}\le d\le x/t}\frac{\chi(d)}{d^{1/2}}\right| \ll \frac{1}{x^{1/4}}$$

and therefore that

$$\begin{aligned} G_2(x) &\ll \frac{1}{x^{1/4}}\sum_{1\le t\le x^{1/2}}\frac{1}{t^{1/2}} \le \frac{1}{x^{1/4}}\left(1 + \int_1^{\sqrt{x}}\frac{dt}{t^{1/2}}\right) \\ &= \frac{1}{x^{1/4}}\left(1 + 2t^{1/2}\Big|_{t=1}^{t=x^{1/2}}\right) \ll 1, \end{aligned}$$

so that $G_2(x) = O(1)$. Combining the above estimates, we obtain

$$G(x) = G_1(x) + G_2(x) = 2\sqrt{x}L(1,\chi) + O(1).$$

Since we know that $G(x)$ tends to infinity with $x$ and, plainly, that this can happen only if $L(1,\chi) \neq 0$, thus proving (14.12) and completing the proof of Dirichlet's theorem.

## Problems on Chapter 14

**Problem 14.1.** *Find all characters modulo* 8.

**Problem 14.2.** *Show that if $p$ is an odd prime, then the Legendre symbol $\left(\frac{n}{p}\right)$ is a character modulo $p$. Then prove the following statements:*

(i) $\displaystyle\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right) = 0 \qquad$ *if* $p \equiv 1 \pmod 4$;

(ii) $\displaystyle\sum_{\substack{1\le r\le p-1\\ \left(\frac{r}{p}\right)=1}} r = \frac{p(p-1)}{4} \qquad$ *if* $p \equiv 1 \pmod 4$;

(iii) $\displaystyle\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right) = p\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right) \qquad$ *if* $p \equiv 3 \pmod 4$;

(iv) $\displaystyle\sum_{r=1}^{p-1} r^3\left(\frac{r}{p}\right) = \frac{3p}{2}\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right) \qquad$ *if* $p \equiv 1 \pmod 4$;

(v) $\displaystyle\sum_{r=1}^{p-1} r^4\left(\frac{r}{p}\right) = 2p\sum_{r=1}^{p-1} r^3\left(\frac{r}{p}\right) - p^2\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right) \qquad$ *if* $p \equiv 3 \pmod 4$.

**Problem 14.3.** *Let $f(x) = x(ax+b)$, where $(a,p) = (b,p) = 1$, $a,\ b,\ x,\ p$ are integers with $p$ an odd prime. Show that*

$$\sum_{x=1}^{p-1}\left(\frac{f(x)}{p}\right) = -\left(\frac{a}{p}\right).$$

**Problem 14.4.** *For a character $\chi$ modulo $k$ and a positive integer $n$, let*

$$G(n,\chi) = \sum_{m=1}^{k} \chi(m)e^{2\pi imn/k}.$$

*This is called the Gauss sum associated to $\chi$. Assume that $(n,k) = 1$.*

(i) *Show that*

$$G(n,\chi) = \overline{\chi}(n)G(1,\chi).$$

(ii) *Show that* $|G(1,\chi)|^2 = p$, *where* $k = p$ *is a prime. (Hint: Use the fact that* $|z|^2 = z \cdot \overline{z}$ *for any complex number* $z$*.)*

**Problem 14.5.** *A character is called primitive modulo* $k$ *if it is not induced from any divisor* $d < k$, *or in other words, if for every divisor* $d$ *of* $k$ *there is a number* $a \equiv 1 \pmod{d}$, *with* $(a,k) = 1$ *and* $\chi(a) \neq 1$. *Show that if* $\chi$ *is primitive modulo* $k$, *then we can write*

$$\chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{m} \overline{\chi}(n) e^{-2\pi i n m/k},$$

*where*

$$\tau_k(\chi) = \frac{G(1,\chi)}{\sqrt{k}},$$

*and* $G(1,\chi)$ *is defined in Problem* 14.4.

**Problem 14.6.** *Prove Polya's inequality to the effect that*

$$\left| \sum_{m \leq x} \chi(m) \right| < \sqrt{k} \log k$$

*is valid for all primitive characters* $\chi$ *modulo* $k$ *and all* $x \geq 1$. *(Hint: Use the representation of* $\chi$ *given in Problem* 14.5 *to transform a sum into a double sum; then change the order of summation.)*

In what follows, we will assume a known result, namely that if $a$ and $k$ are coprime, then

$$\sum_{p \equiv a \pmod{k}} \frac{1}{p} = \infty. \tag{14.15}$$

**Problem 14.7.** *Show that the series*

$$\sum_{n \geq 1} \frac{\cos n}{\sqrt{n}}$$

*converges.*

**Problem 14.8.** *Use the examples of Chapter* 14 *to verify on a case-by-case basis that* $L(1,\chi) \neq 0$ *for all non-principal characters* $\chi$ *modulo* 3, 4, *and* 5.

**Problem 14.9.** *Use Theorem* 13.8 *to show that for each positive integer* $k$, *there exist infinitely many primes* $p$ *which written in base* 10 *look like*

$$\underbrace{11\ldots1}_{k \text{ times}} \ldots \underbrace{11\ldots1}_{k \text{ times}}.$$

*(Of course, they also have some unspecified digits in the middle.) (Hint: Look for primes in a certain arithmetic progression modulo* $10^k$ *in the interval* $[x, (1+1/10^k)x]$*, where* $x = \underbrace{11\ldots1}_{k \text{ times}} \cdot 10^L$ *for some large positive integer* $L$*.)*

**Problem 14.10.** *Use the Brun sieve to show that the set* $\{n : \phi(n) \not\equiv 0 \pmod{k}\}$ *is of asymptotic density zero. (Hint: Let* $\mathcal{P}$ *be the set of primes* $p \equiv 1 \pmod{k}$*. Use the Brun sieve to show that the set of integers* $n \le x$ *with* $\phi(n) \not\equiv 0 \pmod{k}$ *is contained in the set of integers* $n \le x$ *which are not divisible by any* $p \in \mathcal{P}$ *and that the number of such integers is* $\ll x \prod_{p\in\mathcal{P}}(1-1/p)$*. Finally, use estimate* (14.15) *to conclude.)*

**Problem 14.11.** *A positive integer is called a Niven number if it is a multiple of the sum of its digits. For example,* 280 *is a multiple of* $2+8+0=10$*, so it is a Niven number. Show that there are infinitely many non-Niven Fibonacci numbers. (Hint: Show first that the sum of the digits of* $F_n$ *is* $O(n)$*. Then note that, by the Primitive Divisor theorem, if* $p$ *is prime, any prime factor* $q$ *of* $F_p$ *is* $\equiv \pm 1 \pmod{p}$*. Now choose* $p$ *to be a prime such that* $2p-1 \equiv 0 \pmod{3}$*,* $2p+1 \equiv 0 \pmod{5}$*,* $4p-1 \equiv 0 \pmod{7}$ *and so on up to* $2kp-1 \equiv 0 \pmod{p_{2k}}$ *and* $2kp+1 \equiv 0 \pmod{p_{2k+1}}$*, where* $p_i$ *is the* $i$*-th prime. Justify that for each* $k$ *there exist infinitely many such primes* $p$ *and conclude that if* $k$ *is sufficiently large, then every prime factor of* $F_p$ *is larger than the sum of the digits of* $F_p$*, thereby implying that* $F_p$ *cannot be a Niven number.)*

**Problem 14.12.** *Show that the density of the set of positive integers* $n$ *for which* $F_n$ *has a prime factor* $p \equiv 3 \pmod{4}$ *is equal to* $1/2$*. Here,* $F_n$ *is the* $n$*-th Fibonacci number. (Hint: Show first that the set in question does not contain any odd number. Problem* 13.4 *is relevant here. Thus the density of the set in question is at most* $1/2$*. To show that it is* $1/2$*, let* $n = 2m$ *be an even number. If* $p \mid m$ *and* $p \equiv 2 \pmod{3}$*, then* $2p \mid 2m$ *and* $2p \equiv 4 \pmod{6}$*. Now* $F_{2p} \mid F_n$*. Justify that* $F_{2p} \equiv 3 \pmod{4}$*, so that* $F_{2p}$ *has a prime factor* $q \equiv 3 \pmod{4}$*. Conclude that if* $n$ *has a prime factor* $p \equiv 2 \pmod{3}$ *and it is even, then* $F_n$ *has a prime factor* $q \equiv 3 \pmod{4}$*. To justify that most even numbers have a prime factor* $p \equiv 2 \pmod{3}$*, use the Brun sieve as in Problem* 14.10*, together with the fact that the sum of the reciprocals of all the primes* $p \equiv 2 \pmod{3}$ *is divergent.)*

*Chapter 15*

# Selected Applications of Primes in Arithmetic Progression

## 15.1. Known results about primes in arithmetical progressions

Recall that, given a real number $x > 0$ and coprime integers $a$ and $b \geq 2$, and setting $\pi(x; b, a) = \#\{p \leq x : p \equiv a \pmod{b}\}$, we established Theorem 13.8, which we restate here.

**Theorem 15.1.** *If $a$ and $b$ are coprime, then*

$$\pi(x; b, a) = (1 + o(1))\frac{\pi(x)}{\phi(b)} \qquad (x \to \infty). \tag{15.1}$$

An important issue here is to make estimate (15.1) uniform in $b$ and $x$. Namely, it is clear that (15.1) cannot be valid for all $a$ coprime to $b$ if $b$ is very close to $x$, but it is known that estimate (15.1) is valid if $b$ is not very large with respect to $x$.

Here are some important results.

**Theorem 15.2.** *The inequality*

$$\pi(x; b, a) \leq \frac{2x}{\phi(b)\log(x/b)}$$

*holds for all $1 \leq a < b$ with $(a, b) = 1$ and $b \leq x$.*

For a proof, see Halberstam and Richert's book [**74**]. Note that this theorem is simply the Brun-Titchmarsh theorem, which is already familiar to us as Theorem 12.7 (up to the specific factor 2) but which we state again here for completeness. The next result is called the Siegel-Walfisz theorem, although it was Page who first proved it when $A$ is very small.

**Theorem 15.3.** *(Siegel-Walfisz theorem) Let $A > 0$ be any fixed constant. Then there exists a positive constant $B = B(A)$ depending on $A$, such that*

$$\pi(x;b,a) = \frac{\pi(x)}{\phi(b)} + O\Big(\frac{x}{\exp(B\sqrt{\log x})}\Big)$$

*holds for large values of $x$ uniformly for $1 \le a < b$ with $(a,b) = 1$ and $b < (\log x)^A$.*

For a proof, see Tenenbaum's book [**140**].

The next result is called the Bombieri-Vinogradov theorem. Bombieri won the Fields Medal for this result in 1974.

**Theorem 15.4.** *(Bombieri-Vinogradov theorem) For every constant $A > 0$, there exists a positive constant $B = B(A)$ depending on $A$, such that for large values of $x$, the following estimate holds:*

$$\sum_{b<\sqrt{x}/(\log x)^B} \max_{\substack{1\le a<b\\(a,b)=1\\y\le x}} \Big|\pi(y;b,a) - \frac{\pi(y)}{\phi(b)}\Big| < \frac{x}{\log^A x}.$$

For a proof, see Iwaniec and Kowalski's book [**89**].

By Abel's summation formula, the above results imply the following theorem.

**Theorem 15.5.** *The estimate*

$$\sum_{\substack{p\le x\\ p\equiv a \pmod b}} \frac{1}{p} = \frac{\log\log x}{\phi(b)} + \frac{1}{p_{a,b}} + O\Big(\frac{\log(2b)}{\phi(b)}\Big)$$

*holds for all $1 \le a < b \le x$ with $(a,b) = 1$ where $p_{a,b}$ is the smallest prime congruent to $a$ modulo $b$.*

The above theorem is in fact an improvement of the result stated in Problem 12.10.

**Corollary 15.6.** *If $A$ is any fixed constant and $b \le (\log x)^A$, then*

$$\sum_{\substack{p\le x\\ p\equiv a \pmod b}} \frac{1}{p} \ll \frac{A\log\log x}{\phi(b)} \tag{15.2}$$

*and*

$$\sum_{\substack{p\le x\\ p\equiv a \pmod b}} \frac{\log p}{p} \ll \frac{A\log x}{\phi(b)}. \tag{15.3}$$

*Finally, if $b$ is fixed, then these two estimates can be sharpened to*

$$\sum_{\substack{p\le x\\ p\equiv a \pmod b}} \frac{1}{p} = \frac{\log\log x}{\phi(b)} + O_b(1) \tag{15.4}$$

*and*

$$\sum_{\substack{p\le x\\ p\equiv a \pmod b}} \frac{\log p}{p} = \frac{\log x}{\phi(b)} + O_b(1). \tag{15.5}$$

Corollary 15.6 can be proved using Theorem 15.3 and Abel summation and is left as an exercise for the reader.

Here are some unproved statements about primes in arithmetical progressions which are largely believed to be true. The first one is the famous *Generalized Riemann Hypothesis*, or GRH for short.

**Conjecture 15.7.** *(GRH) Let $\varepsilon > 0$ be fixed. Then the estimate*

$$\pi(x;b,a) = \frac{\pi(x)}{\phi(b)} + O\left(bx^{1/2+\varepsilon}\right)$$

*holds for all integers $1 \le a < b$ with $(a,b) = 1$ as $x \to \infty$.*

The next conjecture is known as the *Elliott-Halberstam conjecture* and it asserts that the Bombieri-Vinogradov theorem holds in a range much larger than the one guaranteed by Theorem 15.4.

**Conjecture 15.8.** *(Elliott-Halberstam conjecture) Let $\varepsilon > 0$ be fixed. Then*

$$\sum_{b<x^{1-\varepsilon}} \max_{\substack{1\le a<b\\ (a,b)=1\\ y\le x}} \left|\pi(y;b,a) - \frac{\pi(y)}{\phi(b)}\right| = o(x) \qquad \text{as } x\to\infty.$$

The function $\pi(x;3,1) - \pi(x;3,2)$ changes signs infinitely many times as $x \to \infty$. This result is part of the topic often called the *Prime Number Race*. For more on this subject, the reader is encouraged to examine the recent paper of Granville and Martin [**69**].

Finally, one may ask how large is $p_{a,b}$, the smallest prime number $p \equiv b \pmod a$. The answer to this is given by a theorem of Linnik.

**Theorem 15.9.** *(Linnik theorem) There exist positive constants $A$ and $B$ such that $p_{a,b} \le Ab^B$ for all coprime integers $a$ and $b > 1$.*

Heath-Brown [**80**] showed that one can take $B = 5.5$. Under GRH, $B$ can be taken to be $2 + \varepsilon$. It is conjectured that $B$ can be taken to be $1 + \varepsilon$.

## 15.2. Some Diophantine applications

We now move on to some applications of these theorems on the distribution of primes in arithmetical progressions.

Erdős and Obláth ([**50**]) proved that the Diophantine equation

$$x^p + y^p = n! \tag{15.6}$$

where $x$ and $y$ are coprime, $\max\{|x|, |y|\} > 1$ and $p \geq 3$ is a prime, does not have any integer solution $(x, y, p, n)$. We will prove only the following weak version of their result.

**Proposition 15.10.** *The Diophantine equation* (15.6) *has only a finite number of integer solutions* $(x, y, p, n)$ *with* $x$ *and* $y$ *coprime,* $\max\{|x|, |y|\} > 1$ *and* $p \geq 3$ *prime.*

**Proof.** Assume that $|x| > |y|$. Since $n! > 0$, we have that $x$ is positive. Observe that the condition that $x$ and $y$ are coprime implies that no prime $q \leq n$ divides either $x$ or $y$. Thus, $x \geq n + 1$, and both $x$ and $y$ are odd. If $y > 0$, then $n^n > n! > x^p \geq (n + 1)^p$, while if $y < 0$,

$$n^n > n! = x^p - |y|^p = (x - |y|)(x^{p-1} + x^{p-2}|y| + \cdots + |y|^{p-1}) > x^{p-1} \geq (n+1)^{p-1}.$$

In both cases, $p \leq n$. Also note that

$$x^p + y^p = (x + y)\Big(\frac{x^p + y^p}{x + y}\Big). \tag{15.7}$$

Lemma 13.10 and Fermat's little theorem show that

$$\frac{x^p + y^p}{x + y} = \delta m,$$

where $\delta \in \{1, p\}$ and all primes $q \mid m$ have the property that $q \equiv 1 \pmod{p}$. If $y > 0$, then

$$m = \frac{x^p + y^p}{\delta(x + y)} > \frac{x^p}{2xp} = \frac{x^{p-1}}{2p},$$

while if $y < 0$, then

$$m = \frac{1}{\delta}\Big(\frac{x^p - |y|^p}{x - |y|}\Big) = \frac{1}{\delta}(x^{p-1} + x^{p-2}|y| + \cdots + |y|^{p-1}) > \frac{x^{p-1}}{p} > \frac{x^{p-1}}{2p}.$$

Thus, the inequality

$$m > \frac{x^{p-1}}{2p} > \frac{(2x^p)^{(p-1)/p}}{4p} > \frac{(n!)^{(p-1)/p}}{4p} \tag{15.8}$$

holds, where we used the fact that $n! = x^p + y^p < 2x^p$. Now let $M$ be the largest divisor of $n!$ amongst those composed only of prime factors $q \equiv 1 \pmod{p}$. Then $m \mid M$ and, by inequality (15.8),

$$\log M > \left(\frac{p-1}{p}\right) \log n! - \log(4p) > \left(\frac{p-1}{p}\right) n \log\left(\frac{n}{e}\right) - \log(4p), \tag{15.9}$$

where we used version (1.17) of Stirling's formula. Since for each prime $q \le n$, the exponent of $q$ in $n!$ is

$$\left\lfloor \frac{n}{q} \right\rfloor + \left\lfloor \frac{n}{q^2} \right\rfloor + \cdots < n \sum_{i \ge 1} \frac{1}{q^i} = \frac{n}{q-1}$$

(see Lemma 2.7), we have

$$\log M < n \sum_{\substack{q \le n \\ q \equiv 1 \pmod{p}}} \frac{\log q}{q-1}. \tag{15.10}$$

Comparing estimates (15.9) and (15.10), we get that

$$\left(\frac{p-1}{p}\right) \log n - \frac{p-1}{p} - \frac{\log 4p}{n} < \sum_{\substack{q \le n \\ q \equiv 1 \pmod{p}}} \frac{\log q}{q-1},$$

which implies, using the inequality $p \le n$, that

$$\left(\frac{p-1}{p}\right) \log n \le \sum_{\substack{q \le n \\ q \equiv 1 \pmod{p}}} \frac{\log q}{q-1} + O(1). \tag{15.11}$$

Using the trivial inequality

$$\sum_{\substack{q \le n \\ q \equiv 1 \pmod{p}}} \frac{\log q}{q-1} \ll \frac{\log n}{p} \sum_{t \le n/p} \frac{1}{t} \ll \frac{\log^2 n}{p},$$

we get that

$$\frac{2}{3} \log n \le \left(\frac{p-1}{p}\right) \log n \ll \frac{\log^2 n}{p} + O(1),$$

so that $p \ll \log n$. In light of relation (15.3) of Corollary 15.6, we get that for $p \ll \log n$,

$$\sum_{\substack{q \le n \\ q \equiv 1 \pmod{p}}} \frac{\log q}{q-1} \ll \frac{\log n}{p},$$

so that estimate (15.11) leads to

$$\frac{2}{3} \log n \le \left(\frac{p-1}{p}\right) \log n \ll \frac{\log n}{p} + O(1),$$

which implies that $p \ll 1$. Now since $p$ is bounded, using relation (15.5) of Corollary 15.6, we get

$$\sum_{\substack{q \le n \\ q \equiv 1 \pmod p}} \frac{\log q}{q-1} = \frac{\log n}{p-1} + O(1),$$

so that inequality (15.11) implies that

$$\left(\frac{p-1}{p}\right) \log n \le \frac{\log n}{p-1} + O(1),$$

which tells us that

$$\Big(\frac{p-1}{p} - \frac{1}{p-1}\Big) = O\Big(\frac{1}{\log n}\Big),$$

which in turn has only finitely many solutions $p$ and $n$ with $p \ge 3$, because

$$\frac{p-1}{p} - \frac{1}{p-1} = \frac{p^2 - 3p + 1}{p(p-1)} \ge \frac{1}{6}$$

for $p \ge 3$. Finally, since $n^n > x^{p-1}$ and since $n$ and $p$ are both bounded, we get that $x$ is also bounded. □

**Proposition 15.11.** *The Diophantine equation* $x^k = m! + n!$ *has only finitely many positive integer solutions* $(x, k, m, n)$ *with* $\min\{k, m, n\} > 1$.

**Proof.** We sketch only the proof. Assume that $x^k = m! + n!$ with $k > 1$ and $m \ge n \ge 2$. By Bertrand's postulate (Theorem 2.10), there exists a prime $p \in (n/2, n]$. In particular, $p \| n!$. Since $n \le m$, we get that $p \mid (m! + n!)$, so that $p | x^k$. Since $k \ge 2$, we get that $p^2$ does not divide $m!$, so that $m \le 2p \le 2n$. From what is known about the distance between consecutive primes (see Section 8 of Chapter 2), if $n > n_0$, there is a prime $q$ in the interval $(n/2, n/2 + n^{2/3})$. By the above argument, $m \le 2\left(n/2 + n^{2/3}\right) = n + 2n^{2/3}$. Thus,

$$1 + (n+1) \cdots m = \exp\{O\left((m-n)\log m\right)\} = O\left(n^{2/3} \log n\right). \tag{15.12}$$

Since $1 + (n+1) \cdots m$ is a multiple of each prime appearing in the interval $(n/2, n)$, we get that its size is

$$1 + (n+1) \cdots m \ge \exp\{(\pi(n) - \pi(n/2)) \log(n/2)\} > \exp\left(n/3\right), \tag{15.13}$$

provided $n$ is large enough. Comparing inequalities (15.12) and (15.13), we get that $n \ll 1$, and since $m \le 2n$, we obtain that $x^k = m! + n!$ admits only a finite number of solutions. □

## 15.3. Primes $p$ with $p-1$ squarefree

For each positive real number $x$, let

$$\pi_1(x) = \#\{p \le x \mid p-1 \text{ is squarefree}\}.$$

**Proposition 15.12.** *As $x \to \infty$,*

$$\pi_1(x) = \pi(x)(C + o(1)), \tag{15.14}$$

*where*

$$C = \prod_p \Big(1 - \frac{1}{p(p-1)}\Big) \approx 0.373956. \tag{15.15}$$

First observe that since the series

$$\sum_p \frac{1}{p(p-1)}$$

converges, the product $C$ appearing in formula (15.15) converges as well. The constant $C$ is sometimes called *the Artin constant*.

**Proof.** Let $x$ be large and $z$ be a function of $x$ tending to infinity with $x$ which we will make more precise later. Observe that if $p-1$ is not squarefree, then $p \in \mathcal{P}_1(x) \cup \mathcal{P}_2(x)$, where $\mathcal{P}_1(x) = \{p \le x \mid q^2 | p-1 \text{ for some } q > z\}$ and $\mathcal{P}_2(x) = \{p \le x \mid q^2 | p-1 \text{ for some } q \le z\}$. Clearly,

$$\#\mathcal{P}_1(x) \le \sum_{z<q<x^{1/2}} \pi(x; q^2, 1). \tag{15.16}$$

If $q \le x^{1/4}$, then $x/q^2 \ge x^{1/2}$, so that by the Brun-Titchmarsh theorem (Theorem 15.2) and the Chebyshev inequalities, we have that

$$\pi(x; q^2, 1) \le \frac{2x}{q(q-1)\log(x/q^2)} \le \frac{4x}{q(q-1)\log x} \ll \frac{\pi(x)}{q^2}.$$

On the other hand, if $q > x^{1/4}$, then trivially,

$$\pi(x; q^2, 1) \le \frac{x}{q^2},$$

so that

$$\begin{aligned} \#\mathcal{P}_1(x) &\ll \pi(x) \sum_{z<q\le x^{1/4}} \frac{1}{q^2} + x \sum_{q>x^{1/4}} \frac{1}{q^2} \\ &\le \pi(x) \sum_{n>z} \frac{1}{n^2} + x \sum_{n>x^{1/4}} \frac{1}{n^2} \ll \frac{\pi(x)}{z} + x^{3/4} = o(\pi(x)) \end{aligned} \tag{15.17}$$

as $x \to \infty$. To estimate $\#\mathcal{P}_2(x)$, observe that

$$\mathcal{P}_2(x) = \bigcup_{q\le z} \mathcal{A}_q(x),$$

where $\mathcal{A}_q(x) = \{p \le x \mid p \equiv 1 \pmod{q^2}\}$. It is clear that if $q_1 < q_2 < \cdots < q_s \le z$ are distinct primes, then

$$\bigcap_{i=1}^{s} \mathcal{A}_{q_i}(x) = \Big\{p \le x \mid p \equiv 1 \pmod{\prod_{i=1}^{s} q_i^2}\Big\}.$$

By the Inclusion-Exclusion principle, we get that

$$\begin{aligned} \#\mathcal{P}_2(x) &= \Big|\bigcup_{q\le z} \mathcal{A}_q(x)\Big| \\ &= \sum_{s\ge 1}(-1)^{s-1} \sum_{q_1<q_2<\cdots<q_s\le z} \Big|\bigcap_{i=1}^{s} \mathcal{A}_{q_i}(x)\Big| \qquad (15.18) \\ &= -\sum_{\substack{d>1\\ P(d)\le z}} \mu(d)\pi(x;d^2,1). \end{aligned}$$

The maximal value of $d$ appearing in (15.18) satisfies

$$d \le \prod_{q\le z} q = e^{z(1+o(1))} < e^{2z}$$

for large values of $z$. Choose $z$ so that $e^{4z} < x^{1/3}$. The choice $z = \left\lfloor \dfrac{\log x}{12} \right\rfloor$ is appropriate. With $A = 2$, let $B = B(A)$ be the constant appearing in the Bombieri-Vinogradov theorem (Theorem 15.4). Since

$$d^2 < e^{4z} < x^{1/3} < \frac{\sqrt{x}}{\log^B x}$$

for all large $x$, we have that (15.18) can be written as

$$\begin{aligned} \#\mathcal{P}_2(x) &= -\pi(x) \sum_{\substack{d>1\\ P(d)\le z}} \frac{\mu(d)}{\phi(d^2)} + O\Big(\frac{x}{\log^2 x}\Big) \\ &= -\pi(x) \sum_{\substack{d>1\\ P(d)\le z}} \frac{\mu(d)}{\phi(d^2)} + o(\pi(x)) \qquad (15.19) \end{aligned}$$

as $x \to \infty$. From estimates (15.17) and (15.19), we have that

$$\begin{aligned} \pi_1(x) &= \pi(x) - \#(\mathcal{P}_1(x) \cup \mathcal{P}_2(x)) \\ &= \pi(x) \sum_{\substack{d\ge 1\\ P(d)\le z}} \frac{\mu(d)}{\phi(d^2)} + o(\pi(x)) \\ &= \pi(x) \prod_{p\le z}\Big(1 - \frac{1}{p(p-1)}\Big) + o(\pi(x)) \end{aligned}$$

$$= \pi(x)(C + o(1)) + o(\pi(x)) = \pi(x)(C + o(1)),$$

as $x \to \infty$, which is what we wanted to prove. □

## 15.4. More applications of primes in arithmetic progressions

First, recall that for $k \geq 1$ and large $x$, it is convenient to denote by $\log_k x$ the $k$-th iterate of the log function evaluated at $x$.

**Proposition 15.13.** *For large $x$, let $f(x) = \log_3 x / \log_4 x$. Then, for all $n \leq x$, $\phi(n)$ is a multiple of all the prime powers $p^a < f(x)$ except for at most $o(x)$ such integers $n$ as $x \to \infty$.*

**Proof.** For each prime power $q < f(x)$, let $\mathcal{A}_q(x) = \{n \leq x : n$ is not divisible by any prime $p \equiv 1 \pmod q\}$. It is clear that if $n \leq x$ and $n \notin \cup_{q<f(x)} \mathcal{A}_q(x)$, then $n$ has the property that $\phi(n)$ is a multiple of $q$ for all prime powers $q < f(x)$. Thus, it suffices to prove that

$$\sum_{q<f(x)} \#\mathcal{A}_q(x) = o(x) \tag{15.20}$$

as $x \to \infty$. We now fix $q$ and write $\mathcal{B}_q(x)$ for the complement of $\mathcal{A}_q(x)$ in $\{n \ : \ 1 \leq n \leq x\}$. Observe that

$$\mathcal{B}_q(x) \supseteq \bigcup_{\substack{p \leq z \\ p \equiv 1 \pmod q}} \mathcal{C}_{p,q}(x), \tag{15.21}$$

where $\mathcal{C}_{p,q}(x) = \{n \leq x : p|n\}$ and $z$ is a parameter depending on $x$ tending to infinity with $x$ which we will specify later. It is clear that if $p_1 < p_2 < \cdots < p_s \leq z$ are primes congruent to 1 modulo $q$, then

$$\bigcap_{i=1}^{s} \mathcal{C}_{p_i,q}(x) = \Big\{ n \leq x \ : \ n \equiv 0 \pmod{\prod_{i=1}^{s} p_i} \Big\},$$

so that

$$\begin{aligned} \#\bigcap_{i=1}^{s} \mathcal{C}_{p_i,q}(x) &= \left\lfloor \frac{x}{\prod_{i=1}^{s} p_i} \right\rfloor \\ &= \frac{x}{\prod_{i=1}^{s} p_i} - \left\{ \frac{x}{\prod_{i=1}^{s} p_i} \right\} \\ &= \frac{x}{\prod_{i=1}^{s} p_i} + O(1). \end{aligned} \tag{15.22}$$

By the Inclusion-Exclusion principle and estimates (15.21) and (15.22), we get

(15.23)
$$\begin{aligned}\#\mathcal{A}_q(x) = \lfloor x\rfloor - \#\mathcal{B}_q(x) &\le x - \#\Big(\bigcup_{\substack{p\le z\\ p\equiv 1 \pmod q}} \mathcal{C}_{p,q}(x)\Big)\\ &\le x - \#\sum_{s\ge 1}(-1)^{s-1} \sum_{\substack{p_1<p_2<\cdots<p_s\le z\\ p_i\equiv 1 \pmod q,\ i=1,\dots,s}} \Big(\frac{x}{\prod_{i=1}^s p_i} + O(1)\Big)\\ &= x \prod_{\substack{p\le z\\ p\equiv 1 \pmod q}} \Big(1-\frac{1}{p}\Big) + O(2^{\pi(z;q,1)}).\end{aligned}$$

Now choose $z = \log x$. Then $\pi(z;q,1) \le \pi(z) < z = \log x$, so that

$$2^{\pi(z;q,1)} < 2^{\log x} = x^{\log 2}.$$

In light of this inequality, it follows from (15.23) that

$$\begin{aligned}\#\mathcal{A}_q(x) &\ll x \prod_{\substack{p\le z\\ p\equiv 1 \pmod q}} \Big(1-\frac{1}{p}\Big) + O(x^{\log 2})\\ &\le x\exp\left(-\sum_{\substack{p\le z\\ p\equiv 1 \pmod q}} \frac{1}{p} + O\left(\sum_{p\ge 2}\frac{1}{p^2}\right)\right) + O(x^{\log 2}) \qquad (15.24)\\ &\ll x\exp\left(-\sum_{\substack{p\le z\\ p\equiv 1 \pmod q}} \frac{1}{p}\right) + x^{\log 2},\end{aligned}$$

where we used the fact that

$$\sum_p \frac{1}{p^2} \ll 1.$$

Since $q < f(x) = o(\log\log z)$ as $x\to\infty$, and $p_{1,q} > q$, we get, using Corollary 15.6, that

$$\sum_{\substack{p\le z\\ p\equiv 1 \pmod q}} \frac{1}{p} = \frac{\log\log z}{\phi(q)} + O(1) = \frac{\log_3 x}{\phi(q)} + O(1) > \log_4 x + O(1), \qquad (15.25)$$

where we used the fact that the inequality

$$\frac{\log_3 x}{\phi(q)} > \frac{\log_3 x}{q} > \frac{\log_3 x}{f(x)} = \log_4 x$$

holds for all prime powers $q < f(x)$. From inequalities (15.24) and (15.25), we get that

$$\#\mathcal{A}_q(x) \ll x\exp\Big(-\log_4 x + O(1)\Big) + x^{\log 2} \ll \frac{x}{\log_3 x} + x^{\log 2} \ll \frac{x}{\log_3 x},$$

so that

$$\sum_{q<f(x)} \#\mathcal{A}_q(x) \ll \frac{xf(x)}{\log_3 x} = \frac{x}{\log_4 x} = o(x),$$

which is precisely the inequality (15.20) that we wanted to prove. □

**Remark 15.14.** *As it will be seen in Problem* 15.11*, the function $f(x)$ from the statement of Proposition* 15.13 *can be improved to be $c_0 \log_2 x/\log_3 x$ for some appropriate constant $c_0$.*

## 15.5. Probabilistic applications

The following version of the Turán-Kubilius inequality (see Theorem 7.2) for prime factors in arithmetic progressions might be useful in some situations.

**Proposition 15.15.** *If $b > 1$ is fixed and $a$ is coprime to $b$, where $1 \le a < b$, then for large $x$ we have*

$$\sum_{n\le x}\Big(\omega_{a,b}(n) - \frac{\log\log x}{\phi(b)}\Big)^2 = O(x\log\log x),$$

*where $\omega_{a,b}(n) = \#\{p \mid n \ : \ p \equiv a \pmod b\}$ and the constant implied by the above $O$ depends on $b$.*

We will not prove this proposition, but the idea of the proof is as follows. A close look at the arguments used in the proof of Theorem 7.2 shows that the proof of the Turán-Kubilius inequality was based on changing the order of summation in $\sum_{n\le x}\omega(n)$ in order to expose $\sum_{p\le x} 1/p$, and then using Mertens' estimate (Theorem 4.5) to provide the estimate that $\sum_{p\le x} 1/p$ is $\log\log x + O(1)$. The proof of Proposition 15.15 follows the same method of proof reducing $\sum_{n\le x}\omega_{a,b}(n)$ to $\sum_{\substack{p\le x\\ p\equiv a \pmod b}} 1/p$, which by Corollary 15.6 is $(\log\log x)/\phi(b) + O(1)$. The rest of the argument is then similar.

Theorem 7.2 says that almost all $n$ have roughly about $\log\log n$ prime factors. Proposition 15.15 says that if $b$ is fixed, then almost all $n$ have the property that their prime factors are *equidistributed* in the $\phi(b)$ arithmetical progressions $a \pmod b$ with $1 \le a < b$ and $a$ coprime to $b$.

**Proposition 15.16.** *The set of positive integers $n$ such that $d(n) \mid \phi(n)$ is of asymptotic density* 1.

**Proof.** It is enough to show that if $x$ is large, then $d(n) \mid \phi(n)$ for all $n \le x$ with at most $o(x)$ exceptions as $x \to \infty$.

Set $z = \lfloor \log_5 x \rfloor$ and let $\mathcal{A}_1(x) = \{n \le x \ : \ p^2 \mid n \text{ for some } p > z\}$. For fixed $p$, the number of $n \le x$ with $p^2 \mid n$ is $\le x/p^2$. Thus,

$$\#\mathcal{A}_1(x) \le \sum_{p>z} \frac{x}{p^2} < x \sum_{n>z} \frac{1}{n^2} \ll \frac{x}{z} = o(x)$$

as $x \to \infty$. Let $\mathcal{A}_2(x)$ be the set of those $n \le x$ not in $\mathcal{A}_1(x)$ and such that there exists a prime $p$ with $p^z \mid n$. For a fixed $p$, the number of such integers $n$ is $\le x/p^z \le x/2^z$, and since $n \notin \mathcal{A}_1(x)$, we have that $p \le z$. Thus, by our choice of $z$,

$$\#\mathcal{A}_2(x) \le \frac{x\pi(z)}{2^z} \ll \frac{x \log_5 x}{(\log_4 x)^{\log 2}} = o(x)$$

as $x \to \infty$.

Let $f(x)$ be the function appearing in Proposition 15.13, and let $\mathcal{A}_3(x)$ be the set of those $n \le x$ such that $\phi(n)$ is not a multiple of all prime powers $p^a < f(x)$. By Proposition 15.13, $\#\mathcal{A}_3(x) = o(x)$ as $x \to \infty$.

Let $b = 4$ and $a \in \{1, 3\}$. Let $\mathcal{A}_4(x)$ be the set of those integers $n \le x$ for which

$$\omega(n) > \frac{11 \log\log x}{10}$$

or for which

$$\omega_{a,b}(n) < \frac{2 \log\log x}{5}$$

holds with $b = 4$ and some $a \in \{1, 3\}$. By the Turán-Kubilius theorem and Proposition 15.15, we have that $\#\mathcal{A}_4(x) = o(x)$ as $x \to \infty$.

Let $n \le x$ with $n \notin \cup_{i=1}^4 \mathcal{A}_i(x)$. For such an $n$, we write

$$n = \prod_{p^{a_p} || n} p^{a_p}.$$

Then,

$$d(n) = \prod_{p^{a_p} || n} (a_p + 1) = A(n) \cdot B(n),$$

where $A(n) = \prod_{p \le z}(a_p + 1)$ and $B(n) = \prod_{p>z}(a_p + 1)$. Clearly,

$$A(n) \le (z+1)^{\pi(z)} = \exp(\pi(z) \log(z+1)) < \exp(2z) < \log_4^2 x$$

holds for large $z$ (that is for large $x$) by the Prime Number Theorem, and since $n \in \mathcal{A}_1(x)$ and $B(n) | 2^{\omega(n)}$. In particular, the odd prime powers that divide $d(n)$ also divide $A(n)$. And if $p^a$ is such a prime power, then $p^a < \log_4^2 x < f(x)$ holds for all large $x$. Since $n \notin \mathcal{A}_3(x)$, we get that all prime powers that divide $d(n)$ divide $\phi(n)$ also.

Thus, it is enough to examine the exponent of 2 in $d(n)$ and $\phi(n)$. The exponent of 2 in $\phi(n)$ is

$$\geq 2\omega_{1,4}(n) + \omega_{3,4}(n) > \left(2 \cdot \frac{2}{5} + \frac{2}{5}\right) \log\log x = \frac{6 \log\log x}{5},$$

while the exponent of 2 in $d(n)$ is

$$\begin{aligned} &\leq \omega(n) + \frac{\log A(n)}{\log 2} \leq \omega(n) + O(\log_5 x) \leq \frac{11 \log\log x}{10} + O(\log_5 x) \\ &= \left(\frac{11}{10} + o(1)\right) \log\log x. \end{aligned}$$

Since $6/5 > 11/10$, these last two inequalities show that if $x$ is large, then the power of 2 that divides $d(n)$ divides $\phi(n)$ as well. □

## Problems on Chapter 15

**Problem 15.1.** *Let $p_1 = 2$, $p_2 = 3$ and, for each integer $k \geq 2$, let $p_k$ be the smallest prime such that $(p_k - 1)/2$ is coprime to $p_1 \cdots p_{k-1}$. The first twelve elements of the sequence $\{p_k\}_{k\geq 1}$ are 2, 3, 11, 47, 59, 71, 83, 107, 131, 179, 191, 227. Show that this sequence is infinite. Erdős proved that $\#\{k : p_k \leq x\} \gg x/(\log x \log\log x)$, implying that the sum of the reciprocals of these primes is divergent.*

**Problem 15.2.** *Show, using the Linnik theorem, that there is a constant $c > 0$ such that for infinitely many primes $p$, all numbers $\leq c \log p$ are quadratic residues modulo $p$. (Hint: Fix $x$. For each odd prime $q \leq x$, let $a_q$ be a quadratic residue modulo $q$. Then, let $p \equiv 1 \pmod 8$ and $p \equiv a_q \pmod q$. Show, using the Quadratic Reciprocity Law, that $q$ is a quadratic residue modulo $p$ for all $q \leq x$. Now use the Linnik theorem to bound $p$ in terms of $x$.)*

**Problem 15.3.** *Let $s(n) = \sigma(n) - n$. Show, using the Linnik theorem, that there exists a constant $c > 0$ such that if $x$ is large and $p \| n$ for all $p < x$, then $p \| s(n)$ for all $p < x^c$. Deduce also that if this is the case, then $s(n) > n$. Iterate the above argument to deduce that for each $k$ there exist infinitely many $n$ such that*

$$n < s(n) < s(s(n)) < \cdots < \underbrace{s(s(\ldots s(n)))}_{k \ \ times}.$$

**Problem 15.4.** *Show, using the Bombieri-Vinogradov theorem and the Siegel-Walfisz theorem, that*

$$\omega(\sigma(n!)) \gg n^{1/2+o(1)}$$

*as $n \to \infty$. (Hint: Use the Bombieri-Vinogradov theorem to obtain that there exists a number $B$ such that the primes $q < n^{1/2}/(\log n)^B$ which do*

*not divide $p+1$ for any prime $p \in (n/2, n)$ have the property that the sum of their reciprocals is $< 1$. Then use the Siegel-Walfisz theorem to conclude that each one of these primes is $> (\log n)^{B+2}$ for large $n$. Deduce that the number of such primes is $\ll n^{1/2}/(\log n)^{B+2} = o(\pi(n^{1/2}/(\log n)^B))$ as $n \to \infty$.)*

**Problem 15.5.** *Solve the so-called Titchmarsh divisor problem*

$$\sum_{p \le x} d(p-1) \ll x.$$

*(Hint: Observe that $d(p-1) \le 2d_1(p-1)$, where $d_1(n)$ is the number of divisors $\le \sqrt{n}$ of $n$. Then change the order of summation and use the Brun-Titchmarsh theorem to estimate the inner sums.)*

**Problem 15.6.** *Show that $\sigma(\sigma(n))/n$ is dense in $[1, \infty)$. (Hint: First show that $\sigma(m)/m$ is dense in $[1, \infty)$ as $m$ runs through numbers all of whose prime factors are $\equiv 1 \pmod 3$. Then show that for each such $m$, there exists a residue class $p_0 \pmod m$ such that $p_0^2 + p_0 + 1 \equiv 0 \pmod m$. Use the Chinese Remainder Theorem and the Linnik theorem to show that if $x$ is large, then there exists such a prime $p$ on the scale of $x^{O(1)}$ such that $m \mid (p^2+p+1)$ with $(p^2+p+1)/m$ being free of primes $q = O(\log x)$. Deduce that $\sigma(p^2) = ma$, where $a$ is free of small primes. Deduce furthermore that $\sigma(\sigma(p^2)) = \sigma(m)\sigma(a) = \sigma(m)(a + o(1))$ and therefore that $\sigma(\sigma(p^2))/p^2 = (1 + o(1))\sigma(m)/m$.)*

**Problem 15.7.** *Show that there exists $\delta > 0$ such that for large $x$,*

$$\#\{p \le x \ : \ \mu(p-1) \ne 0 \text{ and } P(p-1) < x^\delta\} \gg \pi(x).$$

*(Hint: Check the proof of Theorem 12.9.)*

**Problem 15.8.** *Show that there exists a constant $c_0 > 0$ such that for large $x$, the cardinality of the set of positive integers $n \le x$ such that $n^2 + 1$ is squarefree is $c_0(1 + o(1))x$ as $x \to \infty$.*

**Problem 15.9.** *Prove that there exists a constant $c_1 > 0$ such that*

$$\frac{1}{\pi(x)} \sum_{p \le x} \frac{\phi(p-1)}{p-1} = c_1(1 + o(1)) \qquad \text{as } x \to \infty.$$

**Problem 15.10.** *Prove that there exists a constant $c_2 > 0$ such that*

$$\sum_{p \le x} d(p-1) = c_2(1 + o(1))x \qquad \text{as } x \to \infty.$$

**Problem 15.11.** *Repeat the argument used in the proof of Proposition 15.13, but this time using the Brun sieve instead of the Inclusion-Exclusion principle to show that the function $f(x)$ from the statement of Proposition 15.13 (slightly modified in Remark 15.14) can be taken to be $c_0 \log_2 x / \log_3 x$ for some appropriate constant $c_0$.*

**Problem 15.12.** *Use the argument from the proof of Proposition* 15.13*, taking into account Remark* 15.14*, to show that if $x$ is large, then $\sigma(n)$ is a multiple of all the prime powers $p^a < f(x)$ for all $n \leq x$ with at most $o(x)$ exceptions as $x \to \infty$.*

**Problem 15.13.** *Prove that*

$$\sum_{p \leq x} (\omega(p-1) - \log\log x)^2 = O(\pi(x)\log\log x).$$

*Prove that the same estimate holds when $\omega$ is replaced by $\Omega$.*

**Problem 15.14.** *Prove that there exists some function $g : \mathbb{R}_+ \to \mathbb{R}_+$ with $\lim_{x\to\infty} g(x) = \infty$ such that inequality $\sigma(\phi(n))/n > g(n)$ holds for almost all $n$. (Hint: Use the result of Proposition* 15.13*, taking into account Remark* 15.14*.)*

**Problem 15.15.** *Prove that for almost all positive integers $n$, the arithmetic mean of the divisors of $n$ is an integer.*

**Problem 15.16.** *For almost all $n$, which one is larger, $\phi(\sigma(n))$ or $\sigma(\phi(n))$ ?*

**Problem 15.17.** *Use Problem* 15.11 *to show that for most $n$, $\omega(n) \mid \phi(n)$. (Hint: Use the fact that for most $n$, $\omega(n) \leq 2\log\log n$ and $\phi(n)$ is a multiple of all prime powers up to $\ll \log\log n/\log\log\log n$. See Remark* 15.14*.) Thus, if $\omega(n)$ does not divide $\phi(n)$, then $\omega(n)$ has an excessively large prime power in it. Now use the Turán-Kubilius inequality to corner $\omega(n)$ in an interval of the form $[\log\log n - \sqrt{\log\log n}\delta(n), \log\log n + \sqrt{\log\log n}\delta(n)]$ for some $\delta(n)$ tending to infinity very slowly and then use Problem* 10.2 *to conclude that it suffices to count the number of positive integers in the above interval which have an excessively large prime power in them. For this last step, use the Brun-Titchmarsh theorem.*

**Problem 15.18.** *Show that $\limsup_{n\to\infty} \sigma(2^n-1)/(2^n-1) = \infty$.*

**Problem 15.19.** *Show that there exist infinitely many positive integers $k$ not of the form $\sigma(n) - n$ for any $n \geq 1$. (Hint: Look at the positive integers $k$ which are multiples of* 30*.)*

*Chapter 16*

# The Index of Composition of an Integer

## 16.1. Introduction

While studying the *abc* conjecture, Browkin [**17**] suggested that an integer $n > 1$ is *very composite* if the expression $\dfrac{\log n}{\log \gamma(n)}$ is "large". Here, as before, $\gamma(n)$ stands for the *kernel function* introduced in Chapter 11. This motivated De Koninck and Doyon [**35**] to introduce the notion of *index of composition* of an integer $n \geq 2$ as the quantity $\lambda(n) = \dfrac{\log n}{\log \gamma(n)}$. Formulated in another way, the index of composition $\lambda(n)$ of an integer $n \geq 2$ is the real number to which one must raise the number $\gamma(n)$ in order to obtain $n$. In other words, it is the solution of

$$\gamma(n)^{\lambda(n)} = n.$$

For convenience, we set $\lambda(1) = 1$.

The index of composition of an integer can be thought of as a measure of the average weighted multiplicity of its prime factors.

It is easy to see that for a given integer $n > 1$,

$$\lambda(n) = 1 \Longleftrightarrow n \text{ is squarefree.}$$

On the other hand, perfect squares larger than 1 have an index of composition larger than or equal to 2, which is also the case for powerful numbers.

In 2001, Ribenboim [**119**] studied this function, calling it the *radical index* of an integer.

Before examining the global and local behavior of the $\lambda$ function, let us become familiar with it by displaying some of its basic properties.

## 16.2. Elementary results

Ribenboim [**119**] has established that the index of composition of an integer is either an integer or an irrational number, and moreover that the set $\{\lambda(n) : n = 1, 2, \ldots\}$ is dense in the set of real numbers $\geq 1$.

Although the $\lambda$ function is neither additive nor multiplicative, it does satisfy some interesting inequalities as shown in the following lemma.

**Lemma 16.1.** *The function $\lambda$ has the following properties:*

(a) $\lambda(mn) \leq \lambda(m) + \lambda(n)$ *for all positive integers $m$ and $n$;*

(b) $\lambda(mn) \leq \lambda(m)\lambda(n)$ *for all coprime integers $m$ and $n$.*

**Proof.** It is clear that each of these inequalities is satisfied if one of $m$ or $n$ is equal to 1. Hence, we can assume that both $m$ and $n$ are larger than 1. Part (a) follows from the fact that

$$\begin{aligned}\lambda(mn) &= \frac{\log m + \log n}{\log \gamma(mn)} \leq \frac{\log m + \log n}{\max(\log \gamma(m), \log \gamma(n))} \\ &= \frac{\log m}{\max(\log \gamma(m), \log \gamma(n))} + \frac{\log n}{\max(\log \gamma(m), \log \gamma(n))} \\ &\leq \frac{\log m}{\log \gamma(m)} + \frac{\log n}{\log \gamma(n)} = \lambda(m) + \lambda(n).\end{aligned}$$

To prove (b), we proceed as follows. We want to show that if $\gcd(m, n) = 1$, then (since $\gamma(mn) = \gamma(m)\gamma(n)$)

$$\lambda(mn) = \frac{\log m + \log n}{\log \gamma(m) + \log \gamma(n)} \leq \frac{\log m}{\log \gamma(m)} \times \frac{\log n}{\log \gamma(n)}. \tag{16.1}$$

But this last relation is true if one can show that, for any real positive numbers $a, b, c, d$ with $c \leq a$ and $d \leq b$,

$$\frac{a+b}{c+d} \leq \frac{a}{c} \times \frac{b}{d}. \tag{16.2}$$

To prove this last relation, set $r = \frac{a}{c} \geq 1$ and $s = \frac{b}{d} \geq 1$, in which case

$$\frac{a+b}{c+d} = \frac{rc+sd}{c+d} \leq \frac{rsc+rsd}{c+d} = rs = \frac{a}{c} \times \frac{b}{d},$$

which proves (16.2) and consequently (16.1) as well. □

**Lemma 16.2.** *Given an arbitrary real number $\delta > 0$, the sum of the reciprocals of all the positive integers whose index of composition is $\geq 1+\delta$ converges. In particular, the sum of the reciprocals of the powerful numbers converges to $\zeta(2)\zeta(3)/\zeta(6) \approx 1.9436$.*

**Proof.** First, we examine the sum of the reciprocals of the powerful numbers. Here, for convenience, 1 is considered to be a powerful number. It is clear that each powerful number $n$ can be written in a unique way as

$$n = m^2 r^3, \tag{16.3}$$

for some positive integer $m$ and some squarefree number $r$. Hence,

$$\sum_{\substack{n=1\\ n \text{ powerful}}}^{\infty} \frac{1}{n} = \sum_{r=1}^{\infty} \frac{\mu^2(r)}{r^3} \sum_{m=1}^{\infty} \frac{1}{m^2} = \prod_p \left(1 + \frac{1}{p^3}\right) \times \zeta(2) = \frac{\zeta(3)}{\zeta(6)} \times \zeta(2),$$

where $\mu$ stands for the Möbius function. Similarly, it is easy to see that

$$\sum_{\substack{n=1\\ n \text{ powerful}}}^{\infty} \frac{1}{n^\alpha} < +\infty \tag{16.4}$$

for every fixed real number $\alpha > 1/2$.

For the general case, we first observe that each positive integer $n$ such that $\lambda(n) \geq 1+\delta$ can be written as $n = \nu s$, where $\nu \geq 4$ is a powerful number and $s$ is a squarefree number coprime to $\nu$, in which case

$$\lambda(\nu s) = \frac{\log \nu + \log s}{\log \gamma(\nu) + \log s} \geq 1 + \delta,$$

which is equivalent to

$$s \leq \frac{\nu^{1/\delta}}{\gamma(\nu)^{1+1/\delta}}.$$

It follows that

$$\begin{aligned} \sum_{\substack{n=1\\ \lambda(n)\geq 1+\delta}}^{\infty} \frac{1}{n} &= \sum_{\substack{\nu=4\\ \nu \text{ powerful}}}^{\infty} \frac{1}{\nu} \sum_{\substack{(s,\nu)=1\\ s \leq \frac{\nu^{1/\delta}}{\gamma(\nu)^{1+1/\delta}}}} \frac{\mu^2(s)}{s} \\ &\leq \sum_{\substack{\nu=4\\ \nu \text{ powerful}}}^{\infty} \frac{1}{\nu} \sum_{s \leq \nu^{1/\delta}} \frac{1}{s} < \frac{1}{\delta} \sum_{\substack{\nu=4\\ \nu \text{ powerful}}}^{\infty} \frac{1+\log \nu}{\nu}. \end{aligned}$$

But this last series converges in light of (16.4), since it is trivial that $\log \nu \ll \nu^{1/4}$, for example. □

## 16.3. Mean values of $\lambda$ and $1/\lambda$

**Theorem 16.3.** *The asymptotic mean value of the $\lambda$ function is 1. More precisely, as $x \to \infty$, we have*

$$\sum_{n\le x} \lambda(n) = x + c\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),$$

*with* $c = \displaystyle\sum_p \frac{\log p}{p(p-1)} \approx 0.75536.$

**Proof.** Using formula (2.11) of De Koninck and Sitaramachandrarao [**31**], one can prove that there exist positive constants $b_0$ and $b_1$ such that

$$S(x) = \sum_{2\le n\le x} \frac{1}{\log \gamma(n)} = b_0\frac{x}{\log x} + b_1\frac{x}{\log^2 x} + O\left(\frac{x}{\log^3 x}\right), \tag{16.5}$$

namely with $b_0 = G(0)$ and $b_1 = -G'(0)$, where we define, for each real number $t > -1$,

$$\begin{aligned} G(t) &= \frac{1}{\zeta(2)}\frac{1}{t+1}\sum_{n=1}^{\infty}\frac{\chi(n)}{\psi(n)}\left(\frac{\gamma(n)}{n}\right)^t \\ &= \frac{1}{\zeta(2)}\frac{1}{t+1}\prod_p\left(1 + \frac{1}{p^2(1+\frac{1}{p})p^t} + \frac{1}{p^3(1+\frac{1}{p})p^{2t}} + \cdots\right), \end{aligned} \tag{16.6}$$

where $\gamma(1) = \psi(1) = \chi(1) = 1$ and for $n \ge 2$,

$$\psi(n) = n\prod_{p\mid n}\left(1+\frac{1}{p}\right), \qquad \chi(n) = \begin{cases} 1 & \text{if } n \text{ is powerful,} \\ 0 & \text{otherwise.} \end{cases}$$

It follows from these relations that

$$b_0 = 1 \tag{16.7}$$

and

$$b_1 = 1 + \sum_p \frac{\log p}{p(p-1)}. \tag{16.8}$$

Indeed, the functions $\chi$ and $\psi$ being multiplicative, we have

$$\begin{aligned} b_0 = G(0) &= \frac{1}{\zeta(2)}\sum_{n=1}^{\infty}\frac{\chi(n)}{\psi(n)} \\ &= \frac{1}{\zeta(2)}\prod_p\left(1 + \frac{1}{p^2(1+\frac{1}{p})} + \frac{1}{p^3(1+\frac{1}{p})} + \cdots\right) \\ &= \frac{1}{\zeta(2)}\prod_p\left(1-\frac{1}{p^2}\right)^{-1} = 1, \end{aligned}$$

which proves (16.7). On the other hand, using (16.6),

$$\begin{aligned}\log G(t) &= \log(1/\zeta(2)) - \log(t+1) \\ &\quad + \sum_p \log\left(1 + \frac{1}{p^2(1+\frac{1}{p})p^t} + \frac{1}{p^3(1+\frac{1}{p})p^{2t}} + \cdots\right),\end{aligned}$$

so that, differentiating on both sides with respect to $t$,

$$\frac{G'(t)}{G(t)} = -\frac{1}{t+1} + \sum_p \frac{-\frac{\log p}{p^2(1+\frac{1}{p})p^t} - \frac{2\log p}{p^3(1+\frac{1}{p})p^{2t}} - \frac{3\log p}{p^4(1+\frac{1}{p})p^{3t}} - \cdots}{1 + \frac{1}{p^2(1+\frac{1}{p})p^t} + \frac{1}{p^3(1+\frac{1}{p})p^{2t}} + \cdots},$$

which implies that

$$\begin{aligned}G'(0) &= -1 - \sum_p \log p \left(\frac{\frac{1}{p^2(1+\frac{1}{p})} + \frac{2}{p^3(1+\frac{1}{p})} + \frac{3}{p^4(1+\frac{1}{p})} + \cdots}{1/(1-\frac{1}{p^2})}\right) \\ &= -1 - \sum_p \frac{\log p}{p(p-1)},\end{aligned}$$

which proves (16.8), since $b_1 = -G'(0)$.

Relation (16.5) can thus be written as

$$S(x) = \frac{x}{\log x} + (1+c)\frac{x}{\log^2 x} + O\left(\frac{x}{\log^3 x}\right), \tag{16.9}$$

where the constant $c$ is defined in the statement of the theorem.

Using (16.9) and the Abel summation formula, we obtain

$$\begin{aligned}\sum_{2\le n\le x} \frac{\log n}{\log \gamma(n)} &= S(x)\log x - S(2)\log 2 - \int_2^x \frac{S(u)}{u}\,du \\ &= x + (1+c)\frac{x}{\log x} - \int_2^x \left(\frac{1}{\log u} + (1+c)\frac{1}{\log^2 u}\right) du \\ &\qquad + O\left(\frac{x}{\log^2 x}\right) \\ &= x + (1+c)\frac{x}{\log x} - \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right) \\ &= x + c\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),\end{aligned}$$

which completes the proof of the theorem. □

**Remark 16.4.** It is easy to prove that it follows from Theorem 16.3 that for each positive integer $k$ and each real number $\delta > 0$, there exist infinitely

many positive integers $n$ satisfying

$$k \le \lambda(n) + \lambda(n+1) + \cdots + \lambda(n+k-1) < k + \delta.$$

**Theorem 16.5.** *The asymptotic mean value of the function $1/\lambda$ is 1. More precisely, as $x \to \infty$,*

$$\sum_{n \le x} \frac{1}{\lambda(n)} = x + O\left(\frac{x}{\log x}\right).$$

**Proof.** If we let $R(x) = \sum_{2 \le n \le x} \log \gamma(n)$, then

$$\begin{aligned} R(x) &= \sum_{2 \le n \le x} \sum_{p \mid n} \log p = \sum_{p \le x} \log p \left\lfloor \frac{x}{p} \right\rfloor \\ &= x \sum_{p \le x} \frac{\log p}{p} - \sum_{p \le x} \log p \left( \frac{x}{p} - \left\lfloor \frac{x}{p} \right\rfloor \right). \end{aligned} \tag{16.10}$$

On the other hand, it follows from the Chebyshev inequalities that

$$\sum_{p \le x} \log p = O(x) \tag{16.11}$$

and from the Prime Number Theorem that

$$\sum_{p \le x} \frac{\log p}{p} = \log x + O(1). \tag{16.12}$$

Substituting (16.11) and (16.12) in (16.10), we obtain

$$R(x) = x \log x + O(x).$$

Using the Abel summation formula, it then follows that

$$\begin{aligned} \sum_{2 \le n \le x} \frac{1}{\lambda(n)} &= \sum_{2 \le n \le x} \frac{\log \gamma(n)}{\log n} \\ &= \frac{R(x)}{\log x} - \frac{R(2)}{\log 2} + \int_2^x \frac{R(t)}{t \log^2 t}\, dt = x + O\left(\frac{x}{\log x}\right), \end{aligned}$$

as required. □

**Remark 16.6.** *Recently, De Koninck and Kátai* [**32**] *improved the estimates for the mean values of $\lambda$ and $1/\lambda$. In particular, they showed that, given any fixed integer $k \ge 2$, there exist constants $c_1, c_2, \ldots, c_k$ such that*

$$\sum_{n \le x} \lambda(n) = x + c_1 \frac{x}{\log x} + c_2 \frac{x}{\log^2 x} + \cdots + c_k \frac{x}{\log^k x} + O\left(\frac{x}{\log^{k+1} x}\right)$$

*and that a similar estimate holds for* $\displaystyle\sum_{n \le x} \frac{1}{\lambda(n)}$.

## 16.4. Local behavior of $\lambda(n)$

**Theorem 16.7.** *Given an integer $k \geq 2$ and an arbitrary $\varepsilon > 0$, there exist infinitely many positive integers $n$ such that*

$$Q_k(n) = \min\left(\lambda(n), \lambda(n+1), \ldots, \lambda(n+k-1)\right) > \frac{k}{k-1} - \varepsilon.$$

Before we prove this theorem, let us state without proof a lemma, which is essentially a consequence of the Chebyshev inequalities (see Problem 16.3).

**Lemma 16.8.** *Let $k \geq 2$ be an integer and $\varepsilon > 0$ an arbitrary real number smaller than 1. Then, there exists a prime number $q_1$ such that the sequence of consecutive prime numbers $q_1 < q_2 < \cdots < q_k$ satisfies $q_1 > q_k^{1-\varepsilon}$.*

**Proof of Theorem 16.7.** Let $k \geq 2$ and let $0 < \varepsilon < 1$ be fixed. Also let $q_1 < q_2 < \cdots < q_k$ be consecutive prime numbers, and let $a$ be a positive integer yet to be determined. It follows from the Chinese Remainder Theorem that the system of congruences

$$\begin{aligned} x &\equiv 0 \pmod{q_1^a} \\ x &\equiv -1 \pmod{q_2^a} \\ &\vdots \quad\quad \vdots \\ x &\equiv -(k-1) \pmod{q_k^a} \end{aligned}$$

has a unique solution $x = n < q_1^a q_2^a \cdots q_k^a$.

It remains to choose $q_1$ and $a$ appropriately.

First observe that, since $\gamma(rs) \leq \gamma(r)\gamma(s)$ for all positive integers $r$ and $s$, and since $\dfrac{n}{q_1^a} < q_2^a \cdots q_k^a$,

$$\begin{aligned} \lambda(n) = \lambda(q_1^a \cdot \frac{n}{q_1^a}) &= \frac{a\log q_1 + \log(n/q_1^a)}{\log \gamma(n)} \geq \frac{a\log q_1 + \log(n/q_1^a)}{\log q_1 + \log \gamma(n/q_1^a)} \\ &\geq \frac{a\log q_1 + \log(n/q_1^a)}{\log q_1 + \log(n/q_1^a)} \geq \frac{a\log q_1 + \log(q_2^a q_3^a \cdots q_k^a)}{\log q_1 + \log(q_2^a q_3^a \cdots q_k^a)} \\ &\geq \frac{a\log q_1 + \log(q_k^{a(k-1)})}{\log q_1 + \log(q_k^{a(k-1)})} = \frac{a\log q_1 + a(k-1)\log q_k}{\log q_1 + a(k-1)\log q_k}. \end{aligned}$$

Similarly, for each positive integer $i \leq k-1$, we derive

$$\lambda(n+i) = \lambda(q_i^a \cdot \frac{n+i}{q_i^a}) \geq \frac{a\log q_i + a(k-1)\log q_k}{\log q_i + a(k-1)\log q_k} \geq \frac{a\log q_1 + a(k-1)\log q_k}{\log q_1 + a(k-1)\log q_k},$$

so that

$$Q_k(n) \geq \frac{a\log q_1 + a(k-1)\log q_k}{\log q_1 + a(k-1)\log q_k}.$$

This is why, to complete the proof, it is enough to show that it is possible to choose $a$ and $q_1$ in such a way that

$$\frac{a\log q_1 + a(k-1)\log q_k}{\log q_1 + a(k-1)\log q_k} > \frac{k}{k-1} - \varepsilon,$$

an inequality which can be written as

$$\begin{aligned}\left(a - \frac{k}{k-1} + \varepsilon\right)\log q_1 &> a(k-1)\left(\frac{k}{k-1} - \varepsilon - 1\right)\log q_k \\ &= a\,(1 - k\varepsilon + \varepsilon)\log q_k,\end{aligned}$$

which is equivalent to

$$q_1 > q_k^{(a-ak\varepsilon+a\varepsilon)/(a-\frac{k}{k-1}+\varepsilon)} = q_k^{1-\delta},$$

where

$$\delta = \frac{ak\varepsilon - a\varepsilon - \frac{k}{k-1} + \varepsilon}{a - \frac{k}{k-1} + \varepsilon}.$$

To have $\delta > 0$, we need to make sure only that $ak\varepsilon - a\varepsilon - \frac{k}{k-1} + \varepsilon > 0$, that is, that $a > \dfrac{-\varepsilon + k/(k-1)}{(k-1)\varepsilon}$. With such a choice of $a$, we now call upon Lemma 16.8, which guarantees the existence of a sequence of consecutive prime numbers $q_1 < q_2 < \cdots < q_k$ satisfying $q_1 > q_k^{1-\varepsilon}$, thus completing the proof of the theorem. □

**Remark 16.9.** *In the case $k = 3$, this result means that, for any arbitrary small $\varepsilon > 0$,*

$$Q_3(n) = \min\left(\lambda(n), \lambda(n+1), \lambda(n+2)\right) > \frac{3}{2} - \varepsilon \tag{16.13}$$

*for infinitely many numbers $n$. We conjecture, however, that the right-hand side of this last inequality can be replaced by $\frac{3}{2}$, which would represent in a certain way an optimal result, because, according to the abc conjecture, there can exist only a finite number of positive integers $n$ such that*

$$Q_3(n) > \frac{3}{2} + \varepsilon. \tag{16.14}$$

*Indeed assume that the abc conjecture holds and that there exist infinitely many positive integers $n$ verifying* (16.14)*. Then, given an arbitrary number $\delta > 0$ and taking $a = 1$, $b = n(n+2)$ and $c = (n+1)^2$ in (11.1), there would exist a positive constant $M = M(\delta)$ such that, for each of the integers $n$ satisfying* (16.14)*,*

$$\begin{aligned}(n+1)^2 &= n(n+2) + 1 < M(\delta)\left(\gamma(n(n+1)(n+2))\right)^{1+\delta} \\ &\le M(\delta)\left(\gamma(n)\gamma(n+1)\gamma(n+2)\right)^{1+\delta} \\ &= M(\delta)\left(n^{1/\lambda(n)}(n+1)^{1/\lambda(n+1)}(n+2)^{1/\lambda(n+2)}\right)^{1+\delta}\end{aligned}$$

$$\begin{aligned} &< M(\delta)\,(n(n+1)(n+2))^{\frac{2}{3}(1-\frac{2}{3}\varepsilon+\frac{4}{9}\varepsilon^2)(1+\delta)} \\ &< M(\delta)\cdot(n+2)^{2(1-\frac{2}{3}\varepsilon+\frac{4}{9}\varepsilon^2)(1+\delta)}, \end{aligned}$$

*so that*

$$n+1 < \sqrt{M(\delta)}\cdot(n+2)^{(1-\frac{2}{3}\varepsilon+\frac{4}{9}\varepsilon^2)(1+\delta)},$$

*which is impossible if $\delta$ is sufficiently small and $n$ sufficiently large.*

*It is interesting to observe that there exist 40 numbers $n < 10^9$ for which*

$$Q_3(n) = \min\left(\lambda(n), \lambda(n+1), \lambda(n+2)\right) > \frac{3}{2},$$

*the smallest three being $n = 48$, 1375 and 13375 (with respectively $Q_3(n) = 1.698\ldots$, 1.622... and 1.512...), while $Q_3(85016574) = 1.72085\ldots$ is the largest value of $Q_3(n)$ obtained from the numbers $n < 10^9$, and possibly the maximal value of $Q_3(n)$ obtained from all $n \in \mathbb{N}$.*

*Finally, let us mention that De Koninck and Luca* [**33**] *have generalized the above result, namely by showing that given any integer $k \geq 4$ and any arbitrarily small $\varepsilon > 0$, it follows from the abc conjecture that there can exist only a finite number of positive integers $n$ such that*

$$Q_k(n) > \frac{k}{k-1} + \varepsilon.$$

## 16.5. Distribution function of $\lambda(n)$

Given a real number $z > 1$, consider the distribution function

$$F(z,x) = \#\{n < x : \lambda(n) > z\} \qquad (x \geq 2).$$

It is possible to show the following result.

**Theorem 16.10.** *Let $1 < z < 2$ be a fixed real number. Then, for each $\varepsilon > 0$, there exists $x_0 = x_0(\varepsilon) \geq e^e$ such that, if $x \geq x_0$,*

$$\begin{aligned} &\exp\left\{2(1-\varepsilon)\sqrt{\frac{2(1-1/z)\log x}{\log\log x}}\right\} \\ &\qquad < \frac{F(z,x)}{x^{1/z}} < \exp\left\{2(1+\varepsilon)\sqrt{\frac{2(1-1/z)\log x}{\log\log x}}\right\}. \end{aligned} \tag{16.15}$$

*Moreover, the upper bound also holds for each $z \geq 2$.*

**Proof.** The complete proof of this result can be found in De Koninck and Doyon [**35**]. Nevertheless, here are the highlights of the proof of the right-hand side inequality (the lower bound is discussed in Problem 16.4). We

first establish that, given an arbitrary real $z > 1$, then, for all real $x \geq 2$, we have

$$F(z,x) < x^{1/z} + x^{1/z} \sum_{n<x^{1-1/z}L(x)} \frac{1}{\gamma(n)}, \tag{16.16}$$

where $L(x) = \sum_{n<x} \frac{1}{\gamma(n)}$.

Then, the right-hand side inequality of Theorem 16.10 is a consequence of the following result of de Bruijn [**29**]:

$$\log L(x) = 2(1+o(1))\sqrt{\frac{2\log x}{\log\log x}}. \tag{16.17}$$

Indeed, it follows from (16.17) that for all $\varepsilon_1 > 0$, there exists $x_1 = x_1(\varepsilon_1) \geq e^e$ such that

(16.18)

$$L(x) < x^{\varepsilon_1} \quad \text{and} \quad \log L(x) < 2(1+\varepsilon_1)\sqrt{\frac{2\log x}{\log\log x}} \qquad (x \geq x_1).$$

Using (16.17) and (16.18), we get that, for $x \geq x_1$,

$$\begin{aligned} x^{1/z} &\sum_{n<x^{1-1/z}L(x)} \frac{1}{\gamma(n)} \\ &< x^{1/z} \sum_{n<x^{1-1/z+\varepsilon_1}} \frac{1}{\gamma(n)} \\ &= x^{1/z} L(x^{1-1/z+\varepsilon_1}) = x^{1/z} \exp\{\log L(x^{1-1/z+\varepsilon_1})\} \\ &< x^{1/z} \exp\left\{2(1+\varepsilon_1)\sqrt{\frac{2(1-1/z+\varepsilon_1)\log x}{\log\log x + \log(1-1/z+\varepsilon_1)}}\right\}. \end{aligned}$$

Since this last quantity is smaller than

$$x^{1/z} \exp\left\{2(1+\varepsilon)\sqrt{\frac{2(1-1/z)\log x}{\log\log x}}\right\}$$

for all $x \geq x_1$ provided $\varepsilon_1$ is small enough, the right-hand side inequality of (16.15) then follows from (16.16). □

## 16.6. Probabilistic results

We will now use Theorem 16.10 to show that some unproven common sense results are "probably" true.

To obtain our conclusions, we shall take for granted the following *independence hypothesis*: *For each positive $k$, the values of $\lambda(n), \lambda(n+1), \ldots, \lambda(n+k-1)$ are independent random variables.*

Let $z > 1$. It is clear that, for any given positive integer $n$, the probability $P(\lambda(n) > z)$ is equal to $\dfrac{F(z,n)}{n}$. Hence, it follows from Theorem 16.10 that for $1 < z < 2$, there exists a positive integer $n_0$ such that

$$P(\lambda(n) > z) > n^{\frac{1}{z}-1} \qquad (n \geq n_0). \tag{16.19}$$

Moreover, it follows from (16.16) that for all $z > 1$,

$$F(z,n) < n^{1/z} + n^{1/z} \sum_{m<n^{1-1/z}L(n)} \frac{1}{\gamma(m)} < n^{1/z} + n^{1/z} L(nL(n)) \qquad (n \geq 1),$$

where $L(n) = \sum_{m<n} 1/\gamma(m)$. Setting $G(n) = L(nL(n)) + 1$, we then have

$$P(\lambda(n) > z) < n^{\frac{1}{z}-1} G(n) \qquad (n \geq 1). \tag{16.20}$$

On the other hand, in light of the first of the inequalities (16.18), we have that for each $\varepsilon > 0$, there exists $n_1 = n_1(\varepsilon)$ such that $G(n) < n^{\varepsilon}$ for all $n \geq n_1$. This is why, for any fixed $z > 1$,

$$P(\lambda(n) > z) < n^{\frac{1}{z}-1+\varepsilon} \qquad (n \geq n_1). \tag{16.21}$$

**Theorem 16.11.** *For each integer $k \geq 2$, the probability that there exist only a finite number of positive integers $n$ such that*

$$Q_k(n) = \min\left(\lambda(n), \lambda(n+1), \ldots, \lambda(n+k-1)\right) > \frac{k}{k-1} \tag{16.22}$$

*is zero.*

**Proof.** First consider the case $k = 2$. We know that there exist infinitely many powerful numbers $n$ such that $n + 1$ is also powerful; this is an observation made by Golomb [**66**]. (See also Ivić and Shiu [**88**].) However, this result does not guarantee the strict inequality required by (16.22). But that inequality can be established by considering the solutions $(x_\ell, y_\ell)$ of the Fermat-Pell equation $x^2 - 2y^2 = 1$ (with $(x_1, y_1) = (3, 2)$), whose rank $\ell$ satisfies $\ell \equiv 3 \pmod 6$, and by observing that we then have $\min\left(\lambda(2y_\ell^2), \lambda(x_\ell^2)\right) > 2$, since on the one hand we always have that $8|2y_\ell^2$ and on the other hand we have that $9|x_\ell$, a result which can be easily proved by induction.

We may therefore assume that $k \geq 3$. First of all, it follows from (16.19) that, for each nonnegative integer $i \leq k-1$,

$$P\left(\lambda(n+i) > \frac{k}{k-1}\right) > (n+k)^{\frac{k-1}{k}-1} = \frac{1}{(n+k)^{1/k}} \qquad (n \geq n_0).$$

By our *independence hypothesis*, the probabilities $P(\lambda(n+i) > \frac{k}{k-1})$ and $P(\lambda(n+j) > \frac{k}{k-1})$ are independent for $i \neq j$. This is why, for each integer $n \geq n_0$,

$$P\left(Q_k(n) > \frac{k}{k-1}\right) = \prod_{i=0}^{k-1} P\left(\lambda(n+i) > \frac{k}{k-1}\right) > \left(\frac{1}{(n+k)^{1/k}}\right)^k = \frac{1}{n+k}.$$

We therefore have that

$$P\left(Q_k(n) \leq \frac{k}{k-1}\right) \leq 1 - \frac{1}{n+k}. \tag{16.23}$$

Hence, assume that there exist only a finite number of positive integers $n$ such that $Q_k(n) > \dfrac{k}{k-1}$, in which case there exists $N$ such that, for all $n \geq N$, we have $Q_k(n) \leq \frac{k}{k-1}$. Hence, in light of (16.23), it follows that the probability $P^*$ that $Q_k(n) \leq \frac{k}{k-1}$ for all $n \geq N$ satisfies

$$P^* \leq \prod_{n \geq N} \left(1 - \frac{1}{n+k}\right).$$

Since this last product diverges to 0 (because $\sum_{n \geq N} \frac{1}{n+k} = +\infty$), the proof is complete. □

Before we state our next theorem, we mention a classical result from probability theory.

**Lemma 16.12.** *Assume that a given random variable $Y \geq 0$ has an expected value, denoted by $E[Y]$, which is finite. Then, for all $t > 0$,*

$$P(Y \geq tE[Y]) \leq \frac{1}{t},$$

*so that, in particular,*

$$P(Y = +\infty) = 0.$$

**Proof.** See Galambos ([**63**], p. 150). □

**Theorem 16.13.** *Given an integer $k \geq 2$ and an arbitrary real number $\delta > 0$, the probability that there exists an infinite number of integers $n$ such that*

$$Q_k(n) > \frac{k}{k-1} + \delta \tag{16.24}$$

*is zero.*

**Proof.** Let $k \geq 2$ and $\delta > 0$ be fixed. Set $\delta_1 = \delta \times (k-1)$, so that

$$\frac{k}{k-1} + \delta = \frac{k+\delta_1}{k-1}.$$

Let also $\varepsilon > 0$ be a real number satisfying

$$\varepsilon < \frac{\delta_1}{3(k+\delta_1)}.$$

It follows from inequality (16.21) that, if $n \geq n_1$,

$$P\left(\lambda(n+i) > \frac{k+\delta_1}{k-1}\right) < n^{(k-1)/(k+\delta_1)-1+\varepsilon} \qquad (0 \leq i \leq k-1),$$

so that, since $\frac{k-1}{k+\delta_1} - 1 + \varepsilon < \frac{-1-2\delta_1/3}{k+\delta_1}$,

$$P\left(\lambda(n+i) > \frac{k+\delta_1}{k-1}\right) < n^{(-1-2\delta_1/3)/(k+\delta_1)} \qquad (0 \leq i \leq k-1; n \geq n_1).$$

Using our *Independence hypothesis*, we obtain that, for $n \geq n_1$,

$$P\left(Q_k(n) > \frac{k+\delta_1}{k-1}\right) = \prod_{i=0}^{k-1} P\left(\lambda(n+i) > \frac{k+\delta_1}{k-1}\right) < n^{(-k-2k\delta_1/3)/(k+\delta_1)}.$$

Given $x > n_1$, the expected value of the number of integers $n < x$ satisfying (16.24) is therefore smaller than

$$\sum_{n<x} n^{(-k-2k\delta_1/3)/(k+\delta_1)} < n_1 - 1 + \sum_{n=n_1}^{\infty} \frac{1}{n^{(k+2k\delta_1/3)/(k+\delta_1)}},$$

a series which is convergent because $\dfrac{k+2k\delta_1/3}{k+\delta_1} > 1$. Calling upon Lemma 16.12, the proof is complete. □

In light of Theorems 16.7, 16.11, and 16.13, we are now justified in stating the following conjecture.

**Conjecture 16.14.** *For each integer $k \geq 2$,*

$$\limsup_{n\to\infty} Q_k(n) = \frac{k}{k-1}.$$

## Problems on Chapter 16

**Problem 16.1.** *Derive Ribenboim's result to the effect that the set $\{\lambda(n) : n = 1, 2, 3, \ldots\}$ is dense in the set of real numbers $\geq 1$.*

**Problem 16.2.** *Prove that the index of composition of an integer is either an integer or an irrational number.*

**Problem 16.3.** *Use the Chebyshev inequalities to prove Lemma* 16.8.

**Problem 16.4.** *According to Theorem* 16.10*, the distribution function*

$$F(z,x) = \#\{n \le x : \lambda(n) > z\}$$

*satisfies the inequality*

$$F(z,x) > x^{1/z} \cdot \exp\left\{2(1-\varepsilon)\sqrt{\frac{2(1-1/z)\log x}{\log\log x}}\right\}$$

*for all* $1 < z < 2$*. Show that this inequality holds as well for all* $z \ge 2$*. (Hint: First establish that*

$$F(z,x) = \sum_{\substack{ms\le x\\ m \text{ powerful},\ (m,s)=1\\ \lambda(ms)>z}} \mu^2(s) = \sum_{\substack{m\le x\\ m \text{ powerful}}} \sum_{\substack{s<\min\left(\frac{x}{m},\left(\frac{m}{\gamma(m)^z}\right)^{1/(z-1)}\right)\\ (s,m)=1}} \mu^2(s)$$

*and then examine for which positive integers* $m$*, one has*

$$\left(\frac{m}{\gamma(m)^z}\right)^{1/(z-1)} < \frac{x}{m}$$

*and use this to split the inner sum into two sums.)*

# Appendix: Basic Complex Analysis Theory

### 17.1. Basic definitions

A complex number $z$ is a number of the form

$$z = x + iy,$$

where $x$ and $y$ are real numbers and $i = \sqrt{-1}$. The exponential function $e^z$ can be defined in terms of its series, that is,

$$e^z = 1 + z + \frac{z^2}{2} + \cdots + \frac{z^n}{n!} + \cdots = \sum_{n\geq 0} \frac{z^n}{n!}. \tag{17.1}$$

More precisely, one can check, using the ratio test or the root test that the series appearing on the right-hand side converges absolutely for all complex numbers $z$. Thus, this series defines a function which we denote by $e^z$. When $z = x$ is real, we recognize on the right-hand side of formula (17.1) the Taylor expansion of the usual exponential function $e^x$, so that it coincides with it. When $z = iy$ and $y$ is real, we have

$$\begin{aligned} e^{iy} &= \sum_{n\geq 0} \frac{(iy)^n}{n!} = \sum_{k\geq 0} \frac{(iy)^{2k}}{(2k)!} + \sum_{k\geq 0} \frac{(iy)^{2k+1}}{(2k+1)!} \\ &= \sum_{k\geq 0} (-1)^k \frac{y^{2k}}{(2k)!} + i \sum_{k\geq 0} (-1)^k \frac{y^{2k+1}}{(2k+1)!} \end{aligned} \tag{17.2}$$

and on the right-hand side of (17.2) we recognize the familiar Taylor expansions of $\cos y$ and $\sin y$, respectively. Thus, we get

$$e^{iy} = \cos y + i \sin y.$$

The exponential function on the real numbers satisfies the important property $e^{x+y} = e^x \cdot e^y$. The same is true for the complex exponential function since

$$\begin{aligned} e^{z_1+z_2} &= \sum_{n\geq 0} \frac{1}{n!}(z_1+z_2)^n = \sum_{n\geq 0} \frac{1}{n!} \left( \sum_{k=0}^{n} \binom{n}{k} z_1^k z_2^{n-k} \right) \\ &= \sum_{n\geq 0} \sum_{k=0}^{n} \frac{z_1^k}{k!} \frac{z_2^{n-k}}{(n-k)!} = \sum_{u\geq 0} \sum_{v\geq 0} \frac{z_1^u}{u!} \frac{z_2^v}{v!} \\ &= \left( \sum_{u\geq 0} \frac{z_1^u}{u!} \right) \left( \sum_{v\geq 0} \frac{z_2^v}{v!} \right) = e^{z_1} \cdot e^{z_2}, \end{aligned}$$

where in the above calculations we used the binomial formula, the change in the order of summation $u = k,\ v = n - k$ (for all $n \geq 0$ and $0 \leq k \leq n$ whose inverse is $k = u,\ n = u + v$), as well as the fact that we can rearrange the order of the terms any way we want since the series we are working with are absolutely convergent.

In particular,

$$e^{x+iy} = e^x \cdot e^{iy} = e^x(\cos y + i \sin y).$$

If $a > 0$ is any real number, then we can use the fact that $a = e^{\log a}$ and thus define

$$a^z = e^{(\log a)z}.$$

If $z = x + iy$, then

$$a^z = e^{(\log a)(x+iy)} = e^{(\log a)x}\, e^{i(\log a)y} = a^x(\cos(y \log a) + i \sin(y \log a)).$$

In particular, $|a^z| = a^x$.

We now define the logarithm function. As in the real case, it should be the inverse of the exponential function. However, since $e^{2\pi i} = \cos(2\pi) + i \sin(2\pi) = 1 = e^0$, we get that the exponential function is not invertible. Nevertheless, something can still be done. Let $L$ be the semi-axis of all real numbers $x \leq 0$ and let $z \in \mathbb{C} \backslash L$. Write

$$z = \rho(\cos\theta + i \sin\theta),$$

where $\rho > 0$ and $\theta$ are real. We may assume that $\theta \in (-\pi, \pi)$ because $z \notin L$. Then define

$$\log z = \log \rho + i\theta. \tag{17.3}$$

Note that

$$e^{\log z} = e^{\log \rho + i\theta} = e^{\log \rho} \cdot e^{i\theta} = \rho(\cos\theta + i \sin\theta) = z,$$

and that if $\theta = 0$ (that is, $z$ is a positive real number), we get that $\log z$ coincides with the natural logarithm. If $|z| < 1$, then $1 + z$ is a number whose real part is positive, and in particular it is in $\mathbb{C}\backslash L$. Here, although we will not prove it, we have the representation

$$\log(1+z) = z - \frac{z^2}{2} + \cdots + (-1)^{n-1}\frac{z^n}{n} + \cdots,$$

which is similar to the Taylor expansion of the logarithm in the real case.

## 17.2. Infinite products

As one encounters infinite products of complex numbers, the following result will be very useful.

**Lemma 17.1.** *Assume that $\{a_n\}_{n\geq 1}$ is a sequence of complex numbers with $|a_n| < 1$ and such that*

$$\sum_{n\geq 1} |a_n| < \infty. \tag{17.4}$$

*Then*

$$\prod_{n=1}^{N} (1 + a_n) \tag{17.5}$$

*has a finite nonzero limit as $N \to \infty$.*

**Proof.** Let us prove it for the case when $a_n$ are real numbers. Choose $n_0$ such that $|a_n| < 1/2$ for all $n > n_0$. It is easy to check that $|t|/2 \leq |\log(1+t)| \leq 2|t|$ for $|t| < 1/2$. In particular, $\log(1 + a_n) \asymp a_n$ for $n > n_0$. Since the series in (17.4) converges, we get that

$$\sum_{n\geq 1} \log(1 + a_n)$$

converges also. Let $L$ be its limit. Then it is easy to see that the product in (17.5) converges to $e^L \neq 0$.

Assume now that the $a_n$ are complex numbers. If the product in (17.5) tends to zero, then

$$\prod_{n\geq 1} |1 + a_n| = 0.$$

Note that $|1+a_n| = 1+b_n$, where $b_n = |1+a_n|-1$. Writing $a_n = x_n + iy_n$, we get

$$b_n = \sqrt{(1+x_n)^2+y_n^2} - 1 = \frac{x_n^2+y_n^2+2x_n}{1+\sqrt{(1+x_n)^2+y_n^2}},$$

so that $|b_n| \leq 2|x_n| + |a_n|^2 \leq 2|a_n| + |a_n|^2 = O(|a_n|)$ because $|a_n|$ tends to zero and is therefore bounded. Since the series (17.4) converges, so does the series obtained from it by replacing $|a_n|$ by $|b_n|$. Since $b_n$ is real, we get that

$$\prod_{n\geq 1} |1+a_n| = \prod_{n\geq 1}(1+b_n) \neq 0,$$

which is the desired contradiction. □

## 17.3. The derivative of a function of a complex variable

In order to be able to analyze some of the properties of the Riemann Zeta Function studied in Chapter 3, one needs to know that certain functions of a complex variable have a *derivative*.

**Definition 17.2.** *Let $f$ be a function defined everywhere in some open disk $D(z;\delta) = \{w \ : \ |w-z| < \delta\}$ centered at $z$ and of radius $\delta$. Then $f$ has a derivative in $z$ if*

$$\lim_{h\to 0} \frac{f(z+h)-f(z)}{h}$$

*exists. In this case, it is denoted by $f'(z)$. If $f$ has a derivative everywhere in $D(z;\delta)$, then $f$ is called analytic or analytic in $D(z;\delta)$. The term holomorphic is also used instead of analytic.*

As an example, let us show that the exponential function $e^z$ has a derivative at each complex number $z$.

**Example 17.3.** *We show here that the derivative of $e^z$ exists and is itself. For this, it suffices to show that for all fixed $z$, we have*

$$\lim_{h\to 0} \frac{e^{z+h}-e^z}{h} = e^z.$$

*Note that*

$$\frac{e^{z+h}-e^z}{h} - e^z = e^z\left(\frac{e^h-1}{h}-1\right).$$

*Since $z$ is fixed, it suffices to prove that*

$$\lim_{h\to 0}\left(\frac{e^h-1}{h}-1\right) = 0. \tag{17.6}$$

*Assume $|h| < 1$. Then,*

$$\frac{e^h-1}{h} - 1 = \frac{h}{2!} + \frac{h^2}{3!} + \cdots + \frac{h^{n-1}}{n!} + \cdots,$$

*so that*

$$\left|\frac{e^h-1}{h}-1\right| \le |h|\left(\sum_{n\ge 2}\frac{|h|^{n-2}}{n!}\right) < |h|\left(\sum_{n\ge 0}\frac{1}{n!}\right) = e|h|, \tag{17.7}$$

*which clearly implies* (17.6).

All known rules about derivatives apply here: sum rule, product rule, chain rule, etc. We shall not mention them.

## 17.4. The integral of a function along a path

Let $\gamma$ be a path in the complex plane on the interval $[\alpha,\beta]$. This means that $\gamma(t)=u(t)+iv(t)$, where $u(t)$ and $v(t)$ are functions defined on $[\alpha,\beta]$ with real values. We assume there exist points $\alpha=t_0<t_1<\cdots<t_n=\beta$ such that $\gamma$ restricted to $[t_i,t_{i+1}]$ is a continuously differentiable function of $t$. At the points $t_i$, the derivative $\gamma'$ need not exist. We write $\gamma^*=\{\gamma(t): t\in[\alpha,\beta]\}$ for the image of $\gamma$ in $\mathbb{C}$.

Assume that $f:\gamma^*\to\mathbb{C}$ is continuous. Then $(f\circ\gamma)\gamma'$ is piecewise continuous, and hence, integrable on $[\alpha,\beta]$. We define

$$\int_\gamma f(z)dz=\int_\alpha^\beta f(\gamma(t))\gamma'(t)\,dt.$$

**Example 17.4.** *Consider the case when $\gamma$ is the line segment from $a$ to $b$ with interval parameter $t\in[0,1]$. Hence, $\gamma(t)=bt+a(1-t)$. Then $f(\gamma)\gamma'=f(bt+a(1-t))(b-a)$. Thus, if we take, for example, $f(z)=z^n$, with $n\ne -1$, then*

$$\begin{aligned}\int_\gamma z^n dz &= \int_0^1 (tb+a(1-t))^n(b-a)dt = \frac{(bt+a(1-t))^{n+1}}{n+1}\Big|_{t=0}^{t=1}\\ &= \frac{1}{n+1}(b^{n+1}-a^{n+1}).\end{aligned}$$

**Example 17.5.** *Consider now the case when $\gamma$ is the circumference of the circle centered at $a$ of radius $r$. We may take the positively oriented (counterclockwise) parametrization $\gamma(t)=a+re^{it}$, where $t\in[0,2\pi)$. We denote this path by $\gamma(a;r)$. Let $f(z)=(z-a)^n$. Then $\gamma'(t)=ire^{it}$ and $f(\gamma(t))=r^ne^{int}$, so that*

$$\begin{aligned}\int_\gamma (z-a)^n dz &= \int_0^{2\pi} r^n e^{int}(ire^{it})dt = \int_{-\pi}^{\pi} ir^{n+1}e^{i(n+1)t}dt\\ &= \begin{cases} 0 & \text{if } n\ne -1,\\ 2\pi i & \text{if } n=-1.\end{cases}\end{aligned}$$

Given a path $\gamma : [\alpha, \beta] \to \mathbb{C}$, we put $-\gamma(t) = \gamma(\alpha + \beta - t)$. Letting $-\gamma$ stand for the curve $\gamma$ in the opposite direction, and making the change of variable $t \mapsto \beta + \alpha - t$, one easily gets that

$$\int_{-\gamma} f(z)dz = -\int_{\gamma} f(z)dz. \tag{17.8}$$

Given two paths $\gamma_1,\ \gamma_2$, defined on $[\alpha_1, \beta_1]$ and $[\alpha_2, \beta_2]$ respectively, such that the end point of the first one is the starting point of the second, that is, $\gamma_2(\alpha_2) = \gamma_1(\beta_1)$, we can form the path $\gamma_1 \cup \gamma_2$ by setting

$$\gamma(t) = \begin{cases} \gamma_1(t), & \text{if } t \in [\alpha_1, \beta_1], \\ \gamma_2(t + \alpha_2 - \beta_1), & \text{if } t \in [\beta_1, \beta_1 + \beta_2 - \alpha_2], \end{cases}$$

which is now defined on $[\alpha_1, \beta_1 + \beta_2 - \alpha_2]$. To avoid technical difficulties, the parameter intervals in the definition of a path can be arbitrary. The importance of this joined path is, of course, that

$$\int_{\gamma_1 \cup \gamma_2} f(z)dz = \int_{\gamma_1} f(z)dz + \int_{\gamma_2} f(z)dz \tag{17.9}$$

as one can easily verify by breaking up the integral from the left in two pieces and performing a change of variable on the second piece.

An important but not unexpected result is the following.

**Theorem 17.6.** *(Estimation theorem)*

$$\left| \int_{\gamma} f(z)dz \right| \leq \int_{\alpha}^{\beta} |f(\gamma(t))\gamma'(t)|dt. \tag{17.10}$$

**Proof.** We know that if $g : [\alpha, \beta] \to \mathbb{R}$ is integrable, then

$$\left| \int_{\alpha}^{\beta} g(t)dt \right| \leq \int_{\alpha}^{\beta} |g(t)|dt. \tag{17.11}$$

Now clearly,

$$\left| \int_{\gamma} f(z)dz \right| = \left| \int_{\alpha}^{\beta} f(\gamma(t))\gamma'(t)dt \right| = e^{i\phi} \int_{\alpha}^{\beta} f(\gamma(t))\gamma'(t)dt$$

for some angle $\phi \in [0, 2\pi)$. Putting $i\phi$ inside the integral and taking real parts we get

$$\left| \int_{\alpha}^{\beta} f(\gamma(t))\gamma'(t)dt \right| = \int_{\alpha}^{\beta} \mathrm{Re}\left( e^{i\phi} f(\gamma(t))\gamma'(t) \right) dt.$$

Now the desired inequality follows by applying inequality (17.11) with the function $g(t) = \mathrm{Re}\left( e^{i\phi} f(\gamma(t))\gamma'(t) \right)$. □

## 17.5. The Cauchy theorem

Let $a$, $b$, and $c$ be three complex numbers. Assume now that $f(z)$ is analytic in some open connected subset of $\mathbb{C}$ which contains the triangle $[a, b, c]$ of vertexes $a$, $b$, and $c$; that is, the closed curve obtained by joining the segments from $a$ to $b$, $b$ to $c$, and $c$ to $a$. The following result is called the Cauchy theorem for a triangle.

**Theorem 17.7.** *(Cauchy) Assume that $f$ is analytic on an open set containing a triangle $\gamma$. Then $\int_\gamma f(z)dz = 0$.*

**Proof.** Let the triangle be $\gamma = [a, b, c]$ and let $a'$, $b'$, $c'$ denote the midpoints of the edges $[b, c]$, $[c, a]$ and $[a, b]$ respectively. Consider the triangles $\gamma^0 = [a', b', c']$, $\gamma^1 = [a, b', c']$, $\gamma^2 = [b, c', a']$ and $\gamma^3 = [c, a', b']$, respectively. It is easy to see that the integral of $f(z)$ on $[a, b, c]$ is the same as the sum of the integrals of $f(z)$ on each of $\gamma^i$ for $i = 0, 1, 2, 3, 4$. (Indeed, one uses first formula (17.9) to break the integral on a triangle on the sum of the integrals on its three edges and then one notices that the contributions from the three edges of $\gamma^0$ cancel with the contributions from the inner edges of the $\gamma^i$'s for $i = 1, 2, 3$ via formula (17.8), because of opposite orientations.) Thus,

$$I = \int_\gamma f(z)dz = \sum_{i=0}^{4} \int_{\gamma^i} f(z)dz. \tag{17.12}$$

The formula (17.12) implies that for at least one value of $k \in \{0, 1, 2, 3\}$, we must have

$$\left| \int_{\gamma^k} f(z)dz \right| \geq \frac{|I|}{4}.$$

Relabel this $\gamma^k$ as $\gamma_1$. Now continue with $\gamma_1$ in place of $\gamma$. Proceeding in this way we generate a sequence $\gamma_0, \gamma_1, \ldots$ of triangles such that

(i) $\gamma_0 = \gamma$;

(ii) for each $n$, $\Delta_{n+1} \subset \Delta_n$, where $\Delta_n$ is the closed triangular area having $\gamma_n^*$ as its boundary;

(iii) $\text{length}(\gamma_n) = L/2^n$, where $L = \text{length}(\gamma)$;

(iv) $4^{-n}|I| \leq |\int_{\gamma_n} f(z)dz|$.

The set $\cap_{n=0}^{\infty} \Delta_n$ contains a point Z. (To see this, select $z_n$ from each $\Delta_n$. Since $(z_n)_{n\geq 0}$ is bounded, because all points are in $\Delta_0$, it contains a convergent subsequence. Call the limit point of that convergent subsequence $Z$. For each $n$, $Z$ is the limit point of the subsequence of $(z_m)_{m\geq n}$ all of whose terms are in $\Delta_n$, which is closed, so that $Z \in \Delta_n$ for all $n \geq 0$.) Fix $\varepsilon > 0$.

Since $f$ has a derivative in $Z$, it follows that if $r$ is sufficiently small, then

$$\left|\frac{f(z)-f(Z)}{z-Z}-f'(Z)\right|<\varepsilon \qquad \text{for } z\in D(Z;r).$$

Thus,

$$|f(z)-f(Z)-(z-Z)f'(Z)|<\varepsilon|z-Z|, \qquad \text{whenever } |z-Z|<r. \tag{17.13}$$

Choose $N$ such that $\Delta_N \subset D(Z;r)$. For such $N$,

$$|z-Z|\le \frac{L}{2^N} \qquad \text{for all } z\in\Delta_N, \tag{17.14}$$

by (iii), and

$$\int_{\gamma_N}(f(Z)+(z-Z)f'(Z))dz=0, \tag{17.15}$$

by Example 17.4 for the functions $f(z)=1$ and $f(z)=z$ respectively (because the end points of the three edges cancel each other). Thus,

$$\begin{aligned}\left|\int_{\gamma_N}f(z)dz\right| &\le \left|\int_{\gamma_N}(f(Z)+(z-Z)f'(Z))dz\right| \\ &\quad+\left|\int_{\gamma_N}(f(z)-f(Z)-(z-Z)f'(Z))dz\right| \\ &\le \int_{\gamma_N}|f(z)-f(Z)-(z-Z)f'(Z)|dz \\ &\le \varepsilon\times(L/2^N)\times \text{length}(\gamma_N) \\ &= \varepsilon\times(L/2^N)^2,\end{aligned} \tag{17.16}$$

where in the above inequalities we used formula (17.15), estimates (17.13), and (17.14) as well as the estimation in Theorem 17.6. Comparing inequality (17.16) with the one in (iv), we get that $|I|\le\varepsilon L^2$, and since $\varepsilon>0$ was arbitrary, we obtain the desired conclusion. □

In complex analysis, it is very useful to integrate analytic functions on contours. A *contour* is a continuous path $\gamma:[\alpha,\beta]\to\mathbb{C}$ such that $\alpha=t_0<t_1<\cdots<t_k=\beta$ such that $\gamma$ restricted to $[t_i,t_{i+1}]$ is either a line segment or an arc of a circle for all $i=0,\ldots,k-1$. It is called *closed* if $\gamma(\beta)=\gamma(\alpha)$ and it is called a *polygon* if the arcs of circles are not present. Recall that a domain (open connected subset) $D$ in the complex plane is *convex* if whenever it contains two complex numbers $z_1$ and $z_2$, then the segment $[z_1,z_2]$ is contained in $D$. Cauchy's theorem 17.7 can thus be generalized as follows.

**Theorem 17.8.** *Let $D$ be a convex open domain in the plane whose boundary is a contour $\gamma$. Assume that $f$ is analytic in $D$ and its boundary $\gamma$. Then $\int_\gamma f(z)dz=0$.*

We shall not prove it. If the contour $\gamma$ is just a convex polygon, the proof follows immediately from Theorem 17.7 by triangulating $D$. (For example, if the boundary of $\gamma$ has vertexes $P_0, P_1, \ldots, P_k$, we then let $\gamma^i = [P_0, P_i, P_{i+1}]$ for all $i = 1, \ldots, k-1$ and then observe, using formulas (17.8) and (17.9), that the integral of $f$ over $\gamma$ equals the integral of $f$ over the path joining the $\gamma^i$'s for $i = 1, \ldots, k-1$, which in turn is the sum of the integrals of $f$ over the $\gamma^i$'s and each such integral is zero by Theorem 17.7.) We omit the case when some of the edges are arcs of circles. It can be proved to follow from the convex polygon result by a continuity argument (that is, by approximating an arc of a circle by polygonal lines).

In applications, one also needs the following Deformation theorem.

**Theorem 17.9.** *(Deformation theorem) Suppose that $\gamma$ is a positively oriented (counterclockwise) contour, which is the boundary of an open connected subset $D$ containing $\overline{D(a;r)} = \{z : |z-a| \le r\}$. Assume that $f$ is a complex function analytic everywhere in $D$, except possibly at $a$. Then*

$$\int_\gamma f(z)dz = \int_{\gamma(a;r)} f(z)dz,$$

*where $\gamma(a;r) = \{z : |z-a| = r\}$.*

**Proof.** Take a line $\ell$ passing through $a$ with no corner point on $\gamma$ and which is nowhere tangent to $\gamma$. Let $z_1$ and $z_2$ be the points where $\ell$ meets the circle $\gamma(a;r)$ and $w_1$ and $w_2$ be the points where $\ell$ meets $\gamma$ such that for each $k = 1,\ 2$, $z_k$ sits between $w_k$ and $a$ and $|w_k - a|$ is as small as possible. Form the two new contours having boundaries $[w_k, z_k]$ for $k = 1,\ 2$, half of the circle $\gamma(a;r)$, and the parts on $\gamma$ between $w_1$ and $w_2$ positively oriented such that $a$ is not in the interior of the open subset bounded by each of these contours. Let them be $\gamma^1$ and $\gamma^2$. By Theorem 17.8, the integral of $f(z)$ on each of $\gamma^1$ and $\gamma^2$ is zero and summing them up, we easily get that this sum is plus or minus $\int_\gamma f(z)dz - \int_{\gamma(a;r)} f(z)dz$ because the line segment integrals cancel for orientation reasons. □

## 17.6. The Cauchy integral formula

An important application of Cauchy's theorem 17.8 is Cauchy's integral formula.

**Proposition 17.10.** *(Cauchy integral formula) Let $f$ be analytic inside and on the positively (counterclockwise) oriented contour $\gamma$. Then, if $z$ is inside $\gamma$,*

$$f(z) = \frac{1}{2\pi i} \int_\gamma \frac{f(w)}{w - z} dw.$$

**Proof.** There exists $r > 0$ such that $\overline{D(z;r)}$ is contained in the interior of the region bounded by $\gamma$. Thus, $\gamma(z;\varepsilon)$, the circle of center $z$ and radius $\varepsilon$, is also contained in the interior of the region bounded by $\gamma$ for all $\varepsilon < r$. Now using Example 17.5 and the Deformation theorem 17.9, we have

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_\gamma \frac{f(w)}{w-z}dw - f(z)\right| &= \left|\frac{1}{2\pi i}\int_{\gamma(z;\varepsilon)} \frac{f(w)-f(z)}{w-z}dw\right| \\ &= \left|\frac{1}{2\pi i}\int_0^{2\pi} \frac{f(z+\varepsilon e^{i\theta})-f(z)}{\varepsilon e^{i\theta}}\, i\varepsilon e^{i\theta}d\theta\right| \\ &\leq \frac{1}{2\pi}(2\pi)\sup_{\theta\in[0,2\pi]}|f(z+\varepsilon e^{i\theta})-f(z)|,\end{aligned}$$

and since the right-hand side tends to zero when $\varepsilon \to 0$ by continuity, the result follows. □

# Solutions to Even-Numbered Problems

## Solutions to problems from Chapter 1

**Problem 1.2.** *Prove that*

$$\lim_{N\to\infty} \frac{1^3+2^3+3^3+4^3+\cdots+N^3}{N^4} = \frac{1}{4}.$$

*Solution.* It is sufficient to apply the result of the preceding problem with $\alpha = 3$. □

**Problem 1.4.** *Show that the following two representations of the Euler constant $\gamma$ are actually the same:*

$$\lim_{N\to\infty} \left( \sum_{n=1}^{N} \frac{1}{n} - \log N \right) \qquad \textit{and} \qquad 1 - \int_1^\infty \frac{t-\lfloor t \rfloor}{t^2}\, dt.$$

*Solution.* We will show that the second representation can be transformed into the first one. Indeed, given an integer $N \geq 2$, we have

$$\int_1^N \frac{t-\lfloor t \rfloor}{t^2}\, dt = \int_1^N \frac{dt}{t} - \int_1^N \frac{\lfloor t \rfloor}{t^2}\, dt. \tag{18.1}$$

This last integral can be written as

$$\begin{aligned}\int_1^N \frac{\lfloor t\rfloor}{t^2}\,dt &= \sum_{i=1}^{N-1} i\int_i^{i+1}\frac{dt}{t^2} = \sum_{i=1}^{N-1} i\left(-\frac{1}{t}\Big|_{t=i}^{t=i+1}\right)\\ &= \sum_{i=1}^{N-1} i\left(\frac{1}{i}-\frac{1}{i+1}\right) = \sum_{i=1}^{N-1} i\frac{1}{i(i+1)}\\ &= \sum_{i=1}^{N-1}\frac{1}{i+1} = \sum_{j=2}^{N}\frac{1}{j} = \sum_{j=1}^{N}\frac{1}{j} - 1.\end{aligned}$$

Using this in (18.1) and letting $N$ tend to infinity, we obtain that

$$\begin{aligned}1-\int_1^\infty \frac{t-\lfloor r\rfloor}{t^2}\,dt &= 1-\lim_{N\to\infty}\int_1^N \frac{t-\lfloor t\rfloor}{t^2}\,dt\\ &= 1-\lim_{N\to\infty}\left(\log N - \sum_{j=1}^{N}\frac{1}{j}+1\right)\\ &= \lim_{N\to\infty}\left(\sum_{n=1}^{N}\frac{1}{n}-\log N\right),\end{aligned}$$

as requested. □

**Problem 1.6.** *Let $f:[a,b]\to\mathbb{R}$ be a function which is continuous at $x=a$. Define $g:[a,b]\to\mathbb{R}$ by*

$$g(x)=\begin{cases}0 & \text{if } x=a,\\ 1 & \text{if } a<x\le b.\end{cases}$$

*Prove that* $\displaystyle\int_a^b f\,dg = f(a)$.

*Solution.* Given an arbitrary partition $\{x_0,x_1,x_2,\dots,x_k\}$ of the interval $[a,b]$ (where $x_0=a$ and $x_k=b$), the corresponding quantity (which approximates the integral in question)

$$S_k=\sum_{i=1}^{k} f(\xi_i)\,(g(x_i)-g(x_{i-1}))$$

is equal to $f(\xi_1)(g(x_1)-g(x_0)) = f(\xi_1)$, since $g(x_i)-g(x_{i-1})=0$ for each $i\ge 2$. It follows that

$$\int_a^b f\,dg = \lim_{k\to\infty} S_k = \lim_{\xi_1\to a} f(\xi_1) = f(a),$$

as requested. □

**Problem 1.8.** *Let $a < c_1 < c_2 < c_3 < b$ and let $f : [a, b] \to \mathbb{R}$ be a function which is continuous at the points $c_i$ ($i = 1, 2, 3$). Moreover, let $\beta_1, \beta_2, \beta_3, \beta_4 \in \mathbb{R}$ and let $g : [a, b] \to \mathbb{R}$ be defined by*

$$g(x) = \begin{cases} \beta_1 & \text{if } a \le x \le c_1, \\ \beta_2 & \text{if } c_1 < x \le c_2, \\ \beta_3 & \text{if } c_2 < x \le c_3, \\ \beta_4 & \text{if } c_3 < x \le b. \end{cases}$$

*Show that*

$$\int_a^b f\, dg = (\beta_2 - \beta_1) f(c_1) + (\beta_3 - \beta_2) f(c_2) + (\beta_4 - \beta_3) f(c_3).$$

*Solution.* The proof is similar to the one of the preceding problem. □

**Problem 1.10.** *Consider the function $f : \mathbb{N} \to \{0, 1\}$ defined by $f(1) = 1$ and, for each integer $n \ge 2$, by*

$$f(n) = \begin{cases} 1 & \text{if } 2^{2m} < n \le 2^{2m+1}, \\ 0 & \text{if } 2^{2m+1} < n \le 2^{2m+2}. \end{cases}$$

*Show that the set $A = \{n \in \mathbb{N} : f(n) = 1\}$ has no density.*

*Solution.* We will show that the two expressions

$$\frac{A(2^{2r+1})}{2^{2r+1}} \quad \text{and} \quad \frac{A(2^{2r+2})}{2^{2r+2}}$$

do not have the same limit as $r \to \infty$; it will follow from this contradiction that the limit of $A(x)/x$ does not exist and therefore that the set $A$ has no density.

First, we easily see that

$$\begin{aligned} A(2^{2r+1}) &= \sum_{\substack{a \in A \\ a \le 2^{2r+1}}} 1 = 1 + 4 + 16 + \cdots + 2^{2r} = 4^0 + 4^1 + 4^2 + \cdots + 4^r \\ &= \frac{4^{r+1} - 1}{4 - 1} = \frac{4^{r+1} - 1}{3}, \end{aligned}$$

so that

$$\frac{A(2^{2r+1})}{2^{2r+1}} = \frac{4^{r+1} - 1}{3 \cdot 2^{2r+1}} \sim \frac{2}{3} \quad \text{as } r \to \infty.$$

Since we also have that $A(2^{2r+2}) = A(2^{2r+1})$, it follows that

$$\frac{A(2^{2r+2})}{2^{2r+2}} = \frac{A(2^{2r+1})}{2^{2r+2}} = \frac{4^{r+1} - 1}{3 \cdot 2^{2r+2}} \sim \frac{1}{3} \quad \text{as } r \to \infty,$$

which provides the desired contradiction. □

**Problem 1.12.** *Let $L : [M, +\infty) \to \mathbb{R}_+$, where $M > 0$. Assume that $L \in \mathcal{C}[M, +\infty)$. Prove that*

$$L \in \mathcal{L} \Longleftrightarrow \int_M^x \frac{dt}{L(t)} = (1 + o(1))\frac{x}{L(x)} \quad \text{as } x \to \infty.$$

*Solution.* First let $L \in \mathcal{L}$. Integrating by parts, we have

$$\int_M^x \frac{dt}{L(t)} = \frac{t}{L(t)}\Big|_M^x + \int_M^x \frac{tL'(t)}{L^2(t)}\,dt = \frac{x}{L(x)} + O(1) + \int_M^x \frac{\eta(t)}{L(t)}\,dt,$$

where $\eta(t) = tL'(t)/L(t)$. Hence, it follows easily from this relation that, since $\eta(t) = o(1)$ as $t \to \infty$,

$$\int_M^x \frac{dt}{L(t)} = (1 + o(1))\frac{x}{L(x)} \qquad (x \to \infty).$$

To prove the reciprocal, it is sufficient to prove that if $L : [M, +\infty) \to \mathbb{R}_+$ is a continuous function, then

$$\int_M^x L(t)\,dt = (1 + o(1))xL(x) \Longrightarrow L \in \mathcal{L}.$$

We first set

$$I(x) = \int_M^x L(t)\,dt, \qquad \xi(x) = \frac{xL(x)}{I(x)}, \tag{18.2}$$

so that

$$I'(x) = L(x) \tag{18.3}$$

and, by hypothesis,

$$\lim_{x\to\infty} \xi(x) = 1. \tag{18.4}$$

Let $y$ be a real number satisfying $M < y \le x$. Then, for each $y \le u \le x$, it follows from (18.2) and (18.3) that

$$\frac{\xi(u)}{u} = \frac{1}{I(u)/I(y)} \cdot \frac{I'(u)}{I(y)}.$$

Integrating with respect to $u$ between $y$ and $x$, we obtain

$$\int_y^x \frac{\xi(u)}{u}\,du = \int_y^x \frac{1}{I(u)/I(y)} \frac{d}{du}\left(\frac{I(u)}{I(y)}\right) du = \log\left(\frac{I(u)}{I(y)}\right)\Big|_{u=y}^{u=x} + c_0,$$

for a certain constant $c_0$. Setting $y = x$, we have that $c_0 = 0$. It follows from this and (18.2) that

$$e^{\int_y^x \frac{\xi(u)}{u}\,du} = \frac{I(x)}{I(y)} = \frac{1}{I(y)}\frac{xL(x)}{\xi(x)}. \tag{18.5}$$

On the other hand, it is clear that

$$e^{\int_y^x \frac{\xi(u)-1}{u}\,du} = e^{\int_y^x \frac{\xi(u)}{u}\,du - \log x + \log y} = \frac{y}{x}e^{\int_y^x \frac{\xi(u)}{u}\,du}. \tag{18.6}$$

Combining (18.5) and (18.6), we obtain

$$e^{\int_y^x \frac{\xi(u)-1}{u}\,du} = \frac{y}{x}\frac{1}{I(y)}\frac{xL(x)}{\xi(x)} = (1+o(1))\frac{y}{I(y)}L(x) \qquad (x\to\infty),$$

where we used (18.4). If we set $\eta(u) = \xi(u) - 1$, we have thus obtained that

$$L(x) = (C(y) + o(1))e^{\int_y^x \frac{\eta(u)}{u}\,du}$$

for a certain constant $C(y) = \frac{I(y)}{y}$ and a function $\eta(u)$ which tends to 0 (in light of (18.4)). This is why, because of the Representation theorem (see Chapter 1, Section 1.5), we may conclude that $L \in \mathcal{L}$. □

**Problem 1.14.** *Let $A = \{p : p+2$ is prime$\}$. It is conjectured that $A(x) \sim Cx/\log^2 x$ (as $x\to\infty$) for a certain positive constant $C$. Use the preceding problem to show that this conjecture implies that*

$$\sum_{\substack{p\le x\\ p+2 \text{ prime}}} \frac{1}{C}\log^2 p = (1+o(1))x \qquad (x\to\infty).$$

*Solution.* This result is an immediate consequence of the preceding problem. □

## Solutions to problems from Chapter 2

**Problem 2.2.** *Show that if $n > 1$, then $n^4 + 4^n$ is composite.*

*Solution.* If $n$ is even, then $n^4 + 4^n > 4$ is even, implying that the given number cannot be prime. If $n$ is odd, then

$$n^4 + 4^n = (n^2)^2 + (2^n)^2 = (n^2+2^n)^2 - 2^{n+1}n^2 = (n^2+2^n)^2 - (2^{(n+1)/2}n)^2$$
$$= (n^2 + 2^n - 2^{(n+1)/2}n)(n^2 + 2^n + 2^{(n+1)/2}n).$$

It remains to show that both these factors are $> 1$. This is clear for the one with $+$. For the one with $-$, it suffices to prove that

$$2^n > 2^{(n+1)/2}n,$$

which is equivalent to $2^{n-1} > n^2$. This is true for $n = 7$. Assume that it is true for some $n \geq 7$. By induction,

$$2^{(n+1)-1} = 2 \cdot 2^{n-1} > 2n^2,$$

and it suffices to show that $2n^2 > (n+1)^2$. This is equivalent to $n^2 > 2n+1$, that is, $n(n-2) > 1$, which is certainly true for $n \geq 7$.

The above argument proves that $n^4 + 4^n$ is composite for all even $n$ and for all odd $n \geq 7$. For $n = 3,\ 5$, we get that the numbers $3^4 + 4^3 = 81 + 64 = 145 = 5 \cdot 29$ and $5^4 + 4^5 = 625 + 1024 = 1649 = 17 \cdot 97$ are both composite. □

**Problem 2.4.** *Prove that if $f(X) \in \mathbb{Z}[X]$ is nonconstant, then the set*

$$S = \{p \ : \ p \text{ is prime and } p | f(n) \ \text{ for some positive integer } n\}$$

*is infinite.*

*Solution.* We will give two solutions. For the first one, we let

$$f(X) = a_0X^d + \cdots + a_{d-1}X + a_d.$$

If $a_d = 0$, then $f(X) = Xg(X)$, where $g(X) = a_0X^{d-1} + \cdots + a_{d-1}$. In this case, $n \mid f(n)$ for all positive integers $n$. Taking $n = p$ to be an arbitrary prime (there are infinitely many of them), we get that $p$ is in $S$. Assume then that $a_d \neq 0$. Assume that $S$ is finite and that $p_1 < p_2 < \cdots < p_k$ are all the members of $S$. Let $n = (p_1 \cdots p_k)a_dt$, where $t > 0$ is an arbitrary integer. Then

$$f(n) = ng(n) + a_d = g(n)p_1 \cdots p_ka_dt + a_d = a_d(g(p_1 \cdots p_ka_dt)tp_1 \cdots p_k + 1).$$

Note that the number $g(p_1 \cdots p_ka_dt)p_1 \cdots p_kt + 1$ is coprime to $p_1p_2 \cdots p_k$ (it differs by 1 from a multiple of this integer). Thus, if $t$ is such that

$$|g(p_1 \cdots p_ka_dt)tp_1 \cdots p_k + 1| > 1,$$

then this last number will have a prime factor $p$, which obviously divides $f(n)$ and which is none of $p_1, \ldots, p_k$; a contradiction. We claim that this last inequality holds for all $t$ except possibly for finitely many of them. Indeed, otherwise the inequality

$$|g(p_1 \cdots p_ka_dt)tp_1 \cdots p_k + 1| \leq 1$$

will have infinitely many integer solutions $t$. Thus, this shows that for some $c \in \{-1, 0, 1\}$, there are infinitely many solutions $t$ to the polynomial

equation $g(p_1 \cdots p_k a_d t) t p_1 \cdots p_k + 1 = c$, which implies that the equation $f(x) = ca_d$ has infinitely many solutions $x$, which is impossible since $f$ is not constant.

We now provide the second solution. Assume again that $S = \{p_1, \ldots, p_k\}$. Let $x$ be large. The number of positive integers $n \le x$ is $\lfloor x \rfloor$. On the other hand, if $n \le x$, then

$$|f(n)| \le c_1 x^d,$$

where we can take $c_1 = \sum_{i=0}^{d} |a_i|$. Since $f(n) = \pm p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, we get

$$p_i^{\alpha_i} \le c_1 x^d.$$

Hence

$$\alpha_i \le \frac{\log(c_1 x^d)}{\log p_i} \le \frac{\log c_1 + d \log x}{\log 2} < \frac{(d+1)\log x}{\log 2} \qquad \text{if } x > c_1.$$

Thus, $\alpha_i$ can take only at most

$$\left\lfloor \frac{(d+1)\log x}{\log 2} \right\rfloor + 1 < c_2 \log x$$

values for large $x$, where we can take $c_2 = 2(d+1)/\log 2$. Thus, the number of elements belonging to the set $\{f(n) : n \le x\}$ is at most

$$2(c_2 \log x)^k,$$

where the above factor 2 accounts for the signs. For each $m \in \{f(n) : n \le x\}$, the nonconstant polynomial equation $f(n) = m$ can have at most $d$ solutions $n$. Thus, the number of $n \le x$ for which $f(n) = \pm p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is at most

$$2d(c_2 \log x)^k.$$

Since there are $\lfloor x \rfloor$ positive integers $n \le x$, we get

$$\lfloor x \rfloor \le 2d(c_2 \log x)^k$$

for all large $x$, which is obviously a contradiction. □

**Problem 2.6.** *Show that if $P(X) \in \mathbb{Z}[X]$ is a nonconstant polynomial, then there exists $n$ such that $P(n!)$ is composite.*

*Solution.* Let $p$ be a prime and $k < p$ an even number. We note that $(p-k)!(k-1)! \equiv (-1)^{k-1}(p-k)!(p-k+1)\cdots(p-1) = (-1)^{k-1}(p-1)! \equiv 1 \pmod{p}$ by Wilson's theorem. Therefore,

$$(k-1)!^n P((p-k)!) = \sum_{i=0}^{n} a_i [(k-1)!]^{n-i} [(p-k)!(k-1)!]^i$$

$$\equiv \sum_{i=0}^{n} a_i[(k-1)!]^{n-i} = S((k-1)!) \pmod{p},$$

where $S(x) = a_n + a_{n-1}x + \cdots + a_0x^n$. Hence, $p|P((p-k)!)$ if and only if $p|S((k-1)!)$. Note that $S((k-1)!)$ depends only on $k$. Let $k > 2a_n+1$. Then, $s = (k-1)!/a_n$ is an integer which is divisible by all primes smaller than $k$. Hence, $S((k-1)!) = a_nb_k$ for some $b_k \equiv 1 \pmod{s}$. It follows that $b_k$ is divisible only by primes larger than $k$. For large enough $k$, we have $|b_k| > 1$. Thus for every prime divisor $p$ of $b_k$, we have $p|P((p-k)!)$. It remains to select a large enough $k$ for which $|P((p-k)!)| > p$. We take $k = (q-1)!$, where $q$ is a large prime. All the numbers $k+i$ for $i = 1, 2, \ldots, q-1$ are composite (by Wilson's theorem, $q|k+1$). Thus $p = k+q+r$, for some $r \geq 0$. We now have $|P((p-k)!)| = |P((q+r)!)| > (q+r)! > (q-1)! + q + r = p$, for large enough $q$, since $n = \deg(P) \geq 1$. This completes the proof. □

**Problem 2.8.** *Let $a > 1$ be an integer. Show that $a^n - 1$ divides $a^m - 1$ if and only if $n$ divides $m$.*

*Solution.* If $n \mid m$, then $m = nd$. Thus,

$$a^m - 1 = a^{nd} - 1 = (a^n)^d - 1 = (a^n - 1)((a^n)^{d-1} + \cdots + 1),$$

so that $a^n - 1 \mid a^m - 1$. Assume now that $a^n - 1 \mid a^m - 1$. Write $m = nq + r$, where $0 \leq r \leq n-1$. Then

$$a^m - 1 = a^{nq+r} - a^{nq} + a^{nq} - 1 = a^{nq}(a^r - 1) + (a^{nq} - 1).$$

Since clearly $a^n - 1 | a^{nq} - 1$, it follows that $a^n - 1 | a^m - 1$ if and only if $a^n - 1 | a^{nq}(a^r - 1)$. Since $a^n - 1$ and $a^{nq}$ are coprime, it follows that $a^n - 1 | a^r - 1$, which can happen only if $r = 0$, which is what needed to be proved. □

**Problem 2.10.** *Show that $(n-1)! \equiv -1 \pmod{n}$ if $n$ is prime and $n \mid (n-1)!$ if $n > 4$ is composite. Use this to prove that*

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \left\lfloor \frac{n}{1 + \sum_{j=2}^{m} \left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor} \right\rfloor^{1/n} \right\rfloor. \tag{18.7}$$

*Solution.* Let $p$ be prime. The first part is the well-known Wilson's theorem. It is based on the following two observations:

(i) For every number $a \in \{1, 2, \ldots, p-1\}$, there exists a number $a' \in \{1, 2, \ldots, p-1\}$ such that $aa' \equiv 1 \pmod{p}$.

(ii) If $a = 1, p-1$, then $a = a'$. Otherwise, $a \neq a'$.

Both observations are clear. Assume now that $p > 3$. It is easy to see that

$$\prod_{a=2}^{p-2} a \equiv 1 \pmod{p}. \tag{18.8}$$

To see this, group 2 with $2'$. Note that there are $p-3-2 = p-5$, an even number of elements left, and with each $a$ we also have $a'$ and $a \not\equiv a' \pmod{p}$. Now group another pair of elements in this way, and so on. This proves equation (18.8) which implies that $(p-1)! \equiv -1 \pmod{p}$ (just multiply both sides of congruence (18.8) by $p-1$, for example).

Now assume that $n$ is composite. Write $n = ab$, where $1 < a \leq b$. If $a < b$, then $b < n$, so that $b \leq n-1$, implying that

$$(n-1)! = 1 \cdot 2 \cdot \cdots \cdot a \cdots b \cdot \cdots \cdot (n-1)$$

is a multiple of $ab = n$. If $a = b$, but $2 < a$, then $2a < a^2 = n$, so that $(n-1)! = 1 \cdot \cdots \cdot a \cdot \cdots \cdot (2a) \cdot \cdots \cdot (n-1)$ is also a multiple of $a^2 = n$. Finally if $n = 4$, it is not true that $4 \mid (3)!$.

As for formula (18.7), we apply the above results to note that if $j$ is a prime, then $((j-1)!+1)/j$ is an integer; otherwise, it isn't. Thus,

$$\left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor = \begin{cases} 1 & \text{if } j \text{ is prime,} \\ 0 & \text{if } j \text{ is composite.} \end{cases}$$

In turn, this shows that

$$1 + \sum_{j=2}^{m} \left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor = \pi(m) + 1.$$

Thus, if $m$ is such that $\pi(m) + 1 \leq n$, then

$$1 = \left\lfloor \frac{n}{n} \right\rfloor \leq \frac{n}{1 + \sum_{j=2}^{m} \left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor} \leq n < 2^n,$$

so that the integer part of the $n$-th root of the above middle terms is always 1. However, if $\pi(m) + 1 > n$, then the ratio $n/(\pi(m)+1)$ is in $(0,1)$, so that the integer part of the $n$-th roots is 0. Note further that $\pi(m) \leq n-1$ if and only if $m \leq p_n - 1$. This argument shows that the right sum in the statement of the problem is

$$1 + \sum_{m=1}^{\min\{p_n - 1, 2^n\}} 1 = 1 + \min\{p_n - 1, 2^n\}.$$

All that is left is to prove that $p_n \leq 2^n + 1$. But this follows by induction from Bertrand's postulate (that is, $p_1 \leq 2$, $p_2 < 2p_1 = 4$, and assuming that $p_n < 2^n$, we get $p_{n+1} < 2p_n < 2^{n+1}$). □

**Problem 2.12.** *Show that*

$$\int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right).$$

*Solution.* Integrate by parts once and then split at $t = \sqrt{x}$. We then get (18.9)

$$\int_2^x \frac{dt}{\log t} = \frac{t}{\log t}\Big|_{t=2}^{t=x} + \int_2^x \frac{dt}{(\log t)^2} = \frac{x}{\log x} + O(1) + \int_2^{\sqrt{x}} \frac{dt}{(\log t)^2} + \int_{\sqrt{x}}^x \frac{dt}{(\log t)^2}.$$

In the smaller range $2 \le t \le x^{1/2}$, we have that $\log t \ge \log 2$, so that

$$\int_2^{\sqrt{x}} \frac{dt}{(\log t)^2} \le \frac{1}{(\log 2)^2} \int_2^{\sqrt{x}} dt \ll \sqrt{x} \ll \frac{x}{(\log x)^2}. \tag{18.10}$$

In the larger range $\sqrt{x} \le t \le x$, we have $\log t \ge \log(\sqrt{x}) = (\log x)/2$, so that

$$\int_{\sqrt{x}}^x \frac{dt}{(\log t)^2} \le \frac{4}{(\log x)^2} \int_{\sqrt{x}}^x dt < \frac{4x}{(\log x)^2} = O\left(\frac{x}{(\log x)^2}\right). \tag{18.11}$$

The desired estimate follows by inserting estimates (18.10) and (18.11) into (18.9). □

**Problem 2.14.** *Show that, for each positive integer $n$,*

$$p_n < 12\left(n \log n + \log\left(\frac{12}{e}\right)\right).$$

*Solution.* Let us first check this inequality for the small values. Since

$$12 \log(12/e) = 17.8 > p_7,$$

it follows that we may assume that $n \ge 8$. Since

$$12(8 \log 8 + \log(12/e)) > 217 > p_{47},$$

we may assume that $n \ge 48$. To prove it in this range, it suffices to check that

$$\pi(12(n \log n + \log(12/e))) > n.$$

By Chebyshev's estimate,

$$\pi(12(n \log n + \log(12/e))) > \left(\frac{3 \log 2}{8}\right) \frac{12n \log n}{\log n + \log 12 + \log(\log n + (\log(12/e))/n)},$$

and it suffices to show that the above rightmost expression is $> n$. Since $36(\log 2)/8 > 3$, it suffices to show that

$$3\log n > \log n + \log 12 + \log(\log n + (\log(12/e))/n),$$

which is implied by

$$2\log n > \log 12 + \log(\log n + 1/12),$$

because when $n > 48$ we have $(\log(12/e))/n < 1/12$. This last inequality is equivalent to

$$n^2 > 12\log n + 1.$$

The derivative of the function $f(x) = x^2 - 12\log x - 1$ is $2x - 12/x > 0$ when $x \geq 48$. Thus, $f(x)$ is increasing for $x \geq 48$. Since $f(48) = 48^2 - 12\log 48 - 1 = 2256.54\ldots > 0$, we get that $f(n) > 0$ for $n \geq 48$, which yields the desired conclusion. □

**Problem 2.16.** *Show that for every $n > 1$, there exist $n$ consecutive composite numbers.*

*Solution.* Taking a close look at the numbers

$$(n+1)! + 2,\ (n+1)! + 3,\ \ldots,\ (n+1)! + (n+1)$$

provides the solution at once. □

**Problem 2.18.** *Let $p_n$ stand for the $n$-th prime. Euclid's proof shows that there is always a prime in the interval $(p_n, p_1 \cdots p_n + 1)$. Prove that for any constant $K$,*

$$\pi(p_1 p_2 \cdots p_n + 1) \gg n^K.$$

*Solution.* Since $p_i \geq 2$ for $i = 1, \ldots, n$, we have that $\pi(p_1 \ldots p_n + 1) \geq \pi(2^n)$. By Chebyshev's estimates, $\pi(2^n) \gg 2^n/\log(2^n) > 2^n/n$. Now the result follows since if $K$ is any fixed constant, then $2^n/n \gg n^K$. □

**Problem 2.20.** *Assuming the Prime Number Theorem, prove that $p_n = n\log n + o(n\log n)$ as $n \to \infty$.*

*Solution.* By the Prime Number Theorem, $\pi(x) = x/\log x + o(x/\log x)$ as $x \to \infty$. Take $x = p_n$. Then

$$n = \frac{p_n}{\log p_n} + o\left(\frac{p_n}{\log p_n}\right) \qquad \text{as } n \to \infty. \tag{18.12}$$

However, we already know (see, for instance, Problems 2.13 and 2.14) that $p_n \asymp n \log n$. That is, $c_1 n \log n < p_n < c_2 n \log n$ holds for all large $n$ with some positive constants $c_1$ and $c_2$. Taking logarithms we obtain that $\log n + \log\log n + \log c_1 < \log p_n < \log n + \log\log n + \log c_2$, so that $\log p_n = \log n + \log\log n + O(1) = (1 + o(1)) \log n$. Thus,

$$\frac{p_n}{\log p_n} = \frac{p_n}{\log n + o(\log n)} = \frac{p_n}{\log n} + o\left(\frac{p_n}{\log n}\right) \qquad (n \to \infty). \tag{18.13}$$

From estimates (18.12) and (18.13), we get

$$n = \frac{p_n}{\log n} + o\left(\frac{p_n}{\log n}\right)$$

as $n \to \infty$, and if we multiply both sides of the above estimate by $\log n$, we obtain $n \log n = p_n + o(p_n)$ as $n \to \infty$, which is equivalent to the desired estimate. □

**Problem 2.22.** *Using Chebyshev's theorem, show that there exists a positive constant $C$ such that for each positive integer $x$, there exists a positive integer $K$ (which may depend on $x$) such that*

$$\#\{p \le x \text{ prime } : \ p = n^2 + K \text{ for some positive integer } n\} > C\frac{\sqrt{x}}{\log x}.$$

*Solution.* Let $m \le x$ be an arbitrary positive integer. Then,

$$0 \le m - \lfloor\sqrt{m}\rfloor^2 < (\lfloor\sqrt{m}\rfloor + 1)^2 - \lfloor\sqrt{m}\rfloor^2 = 2\lfloor\sqrt{m}\rfloor + 1 \le 2\sqrt{x} + 1.$$

Clearly, the set $T = \{k \in \mathbb{Z} : 0 \le k \le 2\sqrt{x} + 1\}$ contains at most $2\sqrt{x} + 2$ integers. Each positive integer $r \le x$ can thus be written as $r = m^2 + k$ for some $k \in T$. In particular, each prime $p \le x$ can also be written in this way. Since there are $\pi(x)$ primes, by the Pigeon Hole principle, there exists $K \in T$ such that the representation $p = n^2 + K$ for some positive integer $n$ holds for at least $\pi(x)/(2\sqrt{x} + 2)$ values of $p$. The conclusion then follows from Chebyshev's estimate. □

**Problem 2.24.** *Recall the statement (2.4) made by Legendre in 1798. Prove that it follows from the Prime Number Theorem in the form $\pi(x) \sim \mathrm{li}(x)$, as $x \to \infty$, that Legendre's statement is accurate if one chooses $A = 1$ and $B = -1$.*

*Solution.* Integration by parts shows that

$$\mathrm{li}(x) = \frac{x}{\log x} + \frac{x}{\log^2 x} + O\left(\frac{x}{\log^3 x}\right)$$

(see, for instance, the method used in Problem 2.12). On the other hand,

$$\frac{x}{\log x - 1} = \frac{x}{\log x}\left(1 + \frac{1}{\log x} + O\left(\frac{1}{\log^2 x}\right)\right) = \frac{x}{\log x} + \frac{x}{\log^2 x} + O\left(\frac{x}{\log^3 x}\right).$$

Comparing these two estimates proves our result. □

**Problem 2.26.** *The French mathematician Charles Hermite (1822–1901) provided the following very simple proof of the infinitude of primes: For each integer $n \geq 1$, let $q_n$ be the smallest prime factor of $n!+1$; since it is clear that $q_n > n$, we have thus generated an infinite sequence of primes. Now, consider the sequence $\{q_n\}_{n\geq 1}$, whose first 40 terms are 2, 3, 7, 5, 11, 7, 71, 61, 19, 11, 39916801, 13, 83, 23, 59, 17, 661, 19, 71, 20639383, 43, 23, 47, 811, 401, 1697, 10888869450418352160768000001, 29, 14557, 31, 257, 2281, 67, 67411, 137, 37, 13763753091226345046315979581580902400000001, 1402930806031754615418 1, 79 and 41. Show that all prime numbers will eventually appear in this sequence.*

*Solution.* Let $p$ be an arbitrary prime number. According to Wilson's theorem, this prime $p$ divides $(p-1)!+1$. But since the smallest prime factor of $(p-1)!+1$ is $\geq p$, it follows that $q_{p-1} = p$. □

## Solutions to problems from Chapter 3

**Problem 3.2.** *Extend the function*

$$G(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}$$

*defined for all complex numbers $s$ with $\mathrm{Re}(s) > 1$ to all complex numbers $s$ with $\mathrm{Re}(s) > 0$.*

*Solution.* Let $f(t) = \sum_{n\leq t}(-1)^{n-1}$. Clearly, $f(t) = O(1)$. Then, by Abel's summation formula,

$$\sum_{n\leq x} \frac{(-1)^{n-1}}{n^s} = \frac{f(x)}{x^s} - 1 - \int_1^x f(t)\frac{d}{dt}\left(\frac{1}{t^s}\right)dt = \frac{f(x)}{x^s} - 1 + s\int_1^x \frac{f(t)}{t^{s+1}}dt.$$

We now let $x$ tend to infinity and note that the resulting improper integral converges for $\mathrm{Re}(s) > 0$. □

**Problem 3.4.** *Show that, for* $\mathrm{Re}(s) > 1$,

$$\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s}.$$

*Solution.* Fix $s = \sigma + it$. Write $\sigma = 1 + \delta$, where $\delta > 0$. Assume that $|h| < \min\{1, \delta/2\}$ and assume that it is fixed. Then $\mathrm{Re}(s+h) \geq 1 + \delta/2$. We will show that

$$\zeta'(s) = -\sum_{n\geq 1} \frac{\log n}{n^s}$$

by proving that

$$\lim_{h\to 0} \frac{\zeta(s+h) - \zeta(s)}{h} = -\sum_{n=1}^{\infty} \frac{\log n}{n^s}.$$

We split the sum at $n_h$, where $n_h > 3$ will be determined later. We get (18.14)

$$\begin{aligned}\Big|\frac{\zeta(s+h)-\zeta(s)}{h} + \sum_{n=1}^{\infty}\frac{\log n}{n^s}\Big| &\leq \left|\sum_{n=1}^{n_h}\left(\frac{1}{hn^{s+h}} - \frac{1}{hn^s} + \frac{\log n}{n^s}\right)\right| \\ &\quad + \frac{1}{|h|}\sum_{n=n_h}^{\infty}\left(\frac{1}{|n^{s+h}|} + \frac{1}{|n^s|} + \frac{\log n}{|n^s|}\right) \\ &\leq \sum_{n=1}^{n_h}\frac{\log n}{n^{\delta+1}}\left|\frac{e^{-h\log n}-1}{h\log n} + 1\right| \\ &\quad + \frac{3}{|h|{n_h}^{\delta/4}}\sum_{n=n_h}^{\infty}\frac{\log n}{n^{\delta/4+1}}.\end{aligned}$$

In the above inequalities, we used that $|n^{s+h}| = n^{\mathrm{Re}(s+h)} \geq n^{1+\delta/2}$, as well as the fact that $\log n \geq \log n_h \geq 1$ in the second range of summation. We now let $n_h$ be defined by $|h|\log(n_h) = 1$. Clearly, $n_h = e^{1/|h|}$. In the range $1 \leq n \leq n_h$, we have that $|h|\log n \leq 1$, so that we may apply inequality (17.7) and get that

$$\begin{aligned}\sum_{n=1}^{n_h}\frac{\log n}{n^{1+\delta}}\left|\frac{e^{-h\log n}-1}{h\log n} + 1\right| &\leq |h|\sum_{1}^{n_h}\frac{(\log n)^2}{n^{\delta+1}} \\ &\leq |h|\sum_{n=1}^{\infty}\frac{(\log n)^2}{n^{\delta+1}} = O(|h|),\end{aligned} \tag{18.15}$$

where the constant implied by the above $O$ depends on $\sigma$. For the second range, we use the fact that if $t > 2$ is real then $e^t > t^2$. Thus, if $h$ is such

that $|h| < \delta/8$, then $t = \delta/(4|h|) > 2$. It follows that

$$n_h^{\delta/4} = e^{\delta/(4|h|)} = e^t > t^2 = \frac{\delta^2}{16|h|^2},$$

so that

$$\frac{1}{|h| n_h^{\delta/4}} \sum_{n=n_h}^{\infty} \frac{\log n}{n^{\delta/4+1}} < \frac{16|h|}{\delta^2} \sum_{n=1}^{\infty} \frac{\log n}{n^{\delta/4+1}} = O(|h|), \tag{18.16}$$

where the constant implied by the above $O$ depends also on $\sigma$. Inserting estimates (18.15) and (18.16) into estimate (18.14), we get that

$$\left| \frac{\zeta(s+h) - \zeta(s)}{h} + \sum_{n=1}^{\infty} \frac{\log n}{n^{s+1}} \right| = O(|h|).$$

Letting $h$ tend to zero yields the desired conclusion. □

**Problem 3.6.** *Show that if $s = \sigma + it$ and $\sigma > 1$, then*

$$|\zeta(s)| \le \zeta(\sigma)$$

*and*

$$|\zeta'(s)| \le |\zeta'(\sigma)|.$$

*Solution.* The first inequality is immediate since

$$|\zeta(s)| = \left| \sum_{n \ge 1} \frac{1}{n^s} \right| \le \sum_{n \ge 1} \frac{1}{|n^s|} = \sum_{n \ge 1} \frac{1}{n^\sigma} = \zeta(\sigma).$$

The second one follows in a similar way, this time using Problem 3.4. □

**Problem 3.8.** *Show that for each positive constant $A$, there exists a positive constant $M$ such that*

$$|\zeta(s)| \le M \log t$$

*and*

$$|\zeta'(s)| \le M(\log t)^2$$

*hold for all $s$ in the region $\sigma > 1 - A/\log t$ and $t \ge e$. (Hint: Use the representation given at Problem 3.3 and split it at $N = \lfloor t \rfloor$.)*

*Solution.* If $\sigma \ge 2$, we have that $|\zeta(s)| \le \zeta(2)$ and $|\zeta'(s)| \le |\zeta'(2)|$, so that the desired inequalities are obviously true. Assume that $\mathrm{Re}(s) < 2$ and $t \ge e$. We then have

$$|s| \le \sigma + t < 2 + t \le 2t \qquad \text{and} \qquad |s-1| \ge t,$$

implying that $1/|s-1| \le 1/t$. Using the representation of $\zeta(s)$ given by Problem 3.3, we find

$$|\zeta(s)| \le \sum_{n=1}^{N} \frac{1}{n^\sigma} + 2t \int_N^\infty \frac{dt}{t^{\sigma+1}} + \frac{N^{1-\sigma}}{t} = \sum_{n=1}^{N} \frac{1}{n^\sigma} + \frac{2t}{\sigma N^\sigma} + \frac{N^{1-\sigma}}{t}.$$

Now let $N = \lfloor t \rfloor$. Then $N \le t < N+1$ and $\log n \le \log t$ if $n \le N$. Thus, inequality $\sigma > 1 - A/\log t$ gives $1 - \sigma < A/\log t$, so that

$$\frac{1}{n^\sigma} = \frac{n^{1-\sigma}}{n} = \frac{1}{n} e^{(1-\sigma)\log n} < \frac{1}{n} e^{(A \log n)/\log t} \le \frac{e^A}{n} = O\left(\frac{1}{n}\right).$$

Therefore

$$\frac{2t}{\sigma N^\sigma} = O\left(\frac{N+1}{N}\right) = O(1)$$

and

$$\frac{N^{1-\sigma}}{t} = \frac{N}{t}\frac{1}{N^\sigma} = O\left(\frac{1}{N}\right) = O(1),$$

so that collecting the above estimates yields

$$|\zeta(s)| = O\left(\sum_{n=1}^{N} \frac{1}{n}\right) + O(1) = O(\log N) + O(1) = O(\log t).$$

This proves the desired inequality for $|\zeta(s)|$. To obtain the one for $|\zeta'(s)|$, we apply the same type of argument to the derivative of the representation of $\zeta(s)$ given by Problem 3.3. The only essential difference is that an extra factor of $\log N$ appears on the right. But $\log N = O(\log t)$, so we get $|\zeta'(s)| = O((\log t)^2)$ in this specified region. □

**Problem 3.10.** *Let $\{a_n\}_{n\ge1}$ be some sequence of complex numbers such that $|a_n| \le 1$ for all $n \ge 1$. Show that the series*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

*converges to a function $F(s)$ which is holomorphic for $\sigma > 1$.*

*Solution.* Note that this is the first part of Newman's theorem which will be proved in Chapter 5. We use the method described in the solution of Problem 3.4. Fix $s = \sigma + it$. Write $\sigma = 1 + \delta$, where $\delta > 0$. Assume that $|h| < \min\{1, \delta/2\}$ and assume that it is fixed. Then $\mathrm{Re}(s+h) \ge 1 + \delta/2$. We shall show that if we set

$$G(s) = -\sum_{n\ge1} \frac{a_n \log n}{n^s},$$

then $F'(s) = G(s)$ by proving that

$$\lim_{h\to 0} \frac{F(s+h) - F(s)}{h} = G(s).$$

We split the sum at integer $n_h$, where $n_h > 3$ will be determined later. We get

(18.17)

$$\begin{aligned}\left| \frac{F(s+h) - F(s)}{h} + \sum_{n=1}^{\infty} \frac{\log n}{n^s} \right| &\le \left| \sum_{n=1}^{n_h} \left( \frac{1}{hn^{s+h}} - \frac{1}{hn^s} + \frac{\log n}{n^s} \right) \right| \\ &\quad + \frac{1}{|h|} \sum_{n=n_h}^{\infty} \left( \frac{1}{|n^{s+h}|} + \frac{1}{|n^s|} + \frac{\log n}{|n^s|} \right) \\ &\le \sum_{n=1}^{n_h} \frac{\log n}{n^{\delta+1}} \left| \frac{e^{-h\log n} - 1}{h \log n} + 1 \right| \\ &\quad + \frac{3}{|h| {n_h}^{\delta/4}} \sum_{n=n_h}^{\infty} \frac{\log n}{n^{\delta/4+1}}.\end{aligned}$$

In the above inequalities, we used the fact that $|n^{s+h}| = n^{\mathrm{Re}(s+h)} \ge n^{1+\delta/2}$, as well as the fact that $\log n \ge \log n_h \ge 1$ in the second range of summation. We now let $n_h$ be defined by $|h| \log(n_h) = 1$. Clearly, $n_h = e^{1/|h|}$. In the range $1 \le n \le n_h$, we have that $|h| \log n \le 1$, so that we may apply inequality (17.7) of the Appendix and get that

(18.18)

$$\sum_{n=1}^{n_h} \frac{\log n}{n^{1+\delta}} \left| \frac{e^{-h\log n} - 1}{h \log n} + 1 \right| \le |h| \sum_{n=1}^{n_h} \frac{(\log n)^2}{n^{\delta+1}} \le |h| \sum_{n=1}^{\infty} \frac{(\log n)^2}{n^{\delta+1}} = O(|h|),$$

where the constant implied by the above $O$ depends on $\sigma$. For the second range, we use the fact that if $t > 2$ is real, then $e^t > t^2$. Thus, if $h$ is such that $|h| < \delta/8$, then $t = \delta/(4|h|) > 2$, so that

$$n_h^{\delta/4} = e^{\delta/(4|h|)} = e^t > t^2 = \frac{\delta^2}{16|h|^2},$$

implying that

$$\frac{1}{|h| n_h^{\delta/4}} \sum_{n=n_h}^{\infty} \frac{\log n}{n^{\delta/4+1}} < \frac{16|h|}{\delta^2} \sum_{n=1}^{\infty} \frac{\log n}{n^{\delta/4+1}} = O(|h|), \tag{18.19}$$

where the constant implied by the above $O$ depends also on $\sigma$. Inserting estimates (18.18) and (18.19) into estimate (18.17), we get that

$$\left| \frac{F(s+h) - F(s)}{h} + \sum_{n=1}^{\infty} \frac{\log n}{n^{s+1}} \right| = O(|h|),$$

and now letting $h$ tend to zero, we get the desired conclusion. □

**Problem 3.12.** *A positive integer $n$ is called squarefull (or powerful) if $p^2 \mid n$ whenever $p$ is a prime factor of $n$. Show that the formula*

$$\sum_{\substack{n\geq 1\\ n \text{ squarefull}}} \frac{1}{n^s} = \frac{\zeta(2s)\zeta(3s)}{\zeta(6s)}$$

*is valid for all $\sigma > 1/2$. (Hint: show that every powerful number $n$ has a unique representation as $n = a^2b^3$, where $a$ and $b$ are integers with $b$ squarefree.)*

*Solution.* It is not hard to see that if $n$ is squarefull, then $n = a^2b^3$ for some $a$ and $b$ where $b$ is squarefree and this representation is unique. Indeed, write $n = \prod_{i=1}^{s} p_i^{\ell_i}$, where $p_1, \ldots, p_s$ are distinct primes and $\ell_i \geq 2$. We let $b$ be the product of all $p_i$'s such that $\ell_i$ is odd, and then it is easy to see that $b^3 \mid n$ and that $n/b^3$ is a square. To check uniqueness, assume $a^2b^3 = a'^2b'^3$ for some pairs $(a, b)$, $(a', b')$ of positive integers with $b$ and $b'$ squarefree. By looking at the parity of the exponents on the left- and right-hand sides and using the Fundamental theorem of arithmetic, we get that every prime dividing $b$ divides also $b'$ and vice versa and since $b$ and $b'$ are positive and squarefree, we get that $b = b'$, which implies that $a = a'$ also. Now it is clear that

$$\sum_{n \text{ squarefull}} \frac{1}{n^s} = \sum_{\substack{a\geq 1\\ b \text{ squarefree}}} \frac{1}{(a^2b^3)^s} = \left(\sum_{a\geq 1} \frac{1}{a^{2s}}\right)\left(\sum_{b \text{ squarefree}} \frac{1}{b^{3s}}\right). \tag{18.20}$$

The first of these last two sums is $\zeta(2s)$. For the second one, we note that every positive integer $n$ can be written uniquely as $bc^2$, where $b$ is squarefree. Hence,

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \sum_{\substack{b \text{ squarefree}\\ c\geq 1}} \frac{1}{(bc^2)^s} = \left(\sum_{b \text{ squarefree}} \frac{1}{b^s}\right)\left(\sum_{c\geq 1} \frac{1}{c^{2s}}\right),$$

and in the last sum above, we recognize $\zeta(2s)$. Thus, we have just shown that

$$\sum_{b \text{ squarefree}} \frac{1}{b^s} = \frac{\zeta(s)}{\zeta(2s)}. \tag{18.21}$$

Finally, using (18.21) in (18.20) (with $s$ replaced by $3s$), we get the desired result. □

**Problem 3.14.** *Prove Euler's formula (3.12). (Hint: Follow the reasoning appearing in Serre's book* [**129**]*, namely by proceeding as follows. Start with*

*the product formula*

$$\frac{\sin z}{z} = \prod_{n=1}^{\infty}\left(1 - \frac{z^2}{n^2\pi^2}\right),$$

*take logarithms on both sides, and then differentiate with respect to $z$, thus obtaining*

$$z\cot z = 1 + 2\sum_{n=1}^{\infty}\frac{z^2}{z^2 - n^2\pi^2} = 1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{z^{2k}}{(\pi n)^{2k}} = 1 - 2\sum_{k=1}^{\infty}\zeta(2k)\frac{z^{2k}}{\pi^{2k}}.$$

*Then, set $x = 2iz$ in the formula $\dfrac{x}{e^x - 1} = \displaystyle\sum_{r=0}^{\infty} B_r\frac{x^r}{r!}$ to obtain*

$$z\cot z = 1 - \sum_{k=1}^{\infty}(-1)^{k+1}\frac{4^k B_{2k}}{(2k)!}z^{2k}.$$

*Compare the above two representations of $z\cot z$ to conclude.)*

*Solution.* We simply follow the hint recalling that $B_{2r+1} = 0$ for each integer $r \geq 1$. □

## Solutions to problems from Chapter 4

**Problem 4.2.** *Show that there exists a constant $\delta$ such that*

$$\sum_{p\leq x}\frac{1}{p\log\log p} = \log\log\log x + \delta + O\left(\frac{1}{\log\log x}\right).$$

*Solution.* We use the same method as the one used in deducing Mertens' estimate

$$\sum_{p\leq x}\frac{1}{p} = \log\log x + \beta + O\left(\frac{1}{\log x}\right)$$

from the estimate

$$\sum_{p\leq x}\frac{\log p}{p} = \log x + O(1). \tag{18.22}$$

We start the sum at 3. So, let $a_n = \frac{\log n}{n}$ if $n$ is an odd prime and 0 otherwise, and let $f(t) = 1/(\log t\log\log t)$. Then $A(x) = \sum_{p\leq x}\frac{\log p}{p} = \log x + \tau(x)$, where $\tau(x) = O(1)$ by estimate (18.22). Applying Abel's summation formula, we get

$$\sum_{3\leq p\leq x}\frac{1}{p\log\log p} = \frac{A(x) + O(1)}{\log x\log\log x}$$

$$
\begin{aligned}
&\quad + \int_3^x \frac{\log t + \tau(t)}{t(\log t)^2(\log\log t)} \left(1 + \frac{1}{\log\log t}\right) dt \\
&= O\left(\frac{1}{\log\log x}\right) + \int_3^x \frac{dt}{t\log t\log\log t} \\
&\quad + \int_3^x \frac{(1 + \tau(t) + \tau(t)/\log\log t)}{t(\log t)^2\log\log t}\, dt,
\end{aligned}
$$

where we used the fact that

$$
f'(t) = -\left(\frac{1}{t(\log t)^2\log\log t} + \frac{1}{t(\log t)^2(\log\log t)^2}\right).
$$

The above first integral is, via the substitution $u = \log\log t$, equal to $\log\log\log x - \log\log\log 3$, while the second integral converges as $x$ tends to infinity, since $1 + \tau(t) + \tau(t)/\log\log t = O(1)$. Thus,

$$
\begin{aligned}
\sum_{3\le p\le x} \frac{1}{p\log\log p} &= \log\log\log x - \log\log\log 3 + O\left(\frac{1}{\log\log x}\right) \\
&\quad + \int_3^\infty \frac{1 + \tau(t) + \tau(t)/\log\log t}{t(\log t)^2(\log\log t)}\, dt \\
&\quad - \int_x^\infty \frac{1 + \tau(t) + \tau(t)/\log\log t}{t(\log t)^2(\log\log t)}\, dt \\
&= \log\log\log x + \delta + O\left(\frac{1}{\log\log x}\right) \\
&\quad + O\left(\frac{1}{\log\log x}\int_x^\infty \frac{dt}{t(\log t)^2}\right) \\
&= \log\log\log x + \delta + O\left(\frac{1}{\log\log x}\right),
\end{aligned}
$$

where we used the fact that the improper integral $\int_3^\infty \frac{dt}{t(\log t)^2}$ converges. □

**Problem 4.4.** *Use Theorem* 4.5 *with Remark* 4.6 *to prove that*

$$
\prod_{p\le x}\left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x}\left(1 + O\left(\frac{1}{\log x}\right)\right) \qquad (x \to \infty),
$$

*a result often called Mertens' theorem.*

*Solution.* Let $U(x)$ be the left-hand side of the above estimate. Taking logarithms we get

(18.23)
$$\begin{aligned}\log U(x) &= \log \prod_{p\le x}\left(1-\frac{1}{p}\right) = \sum_{p\le x}\log\left(1-\frac{1}{p}\right)\\ &= -\sum_{p\le x}\frac{1}{p}+\sum_{p\le x}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)\\ &= -\log\log x-\beta+O\left(\frac{1}{\log x}\right)+\sum_{p\le x}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right),\end{aligned}$$

where we used Theorem 4.5. Since

$$\left|\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right| \ll \frac{1}{p^2},$$

we get that the last series appearing in (18.23) is convergent, so let us set

$$S=\sum_{p}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right).$$

We then get

(18.24)
$$\begin{aligned}\sum_{p\le x}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right) &= S-\sum_{p>x}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)\\ &= S+O\left(\sum_{p>x}\frac{1}{p^2}\right)=S+O\left(\sum_{n\ge x}\frac{1}{n^2}\right)\\ &= S+O\left(\int_{\lfloor x\rfloor-1}^{\infty}\frac{dt}{t^2}\right)\\ &= S+O\left(\frac{1}{\lfloor x\rfloor-1}\right)=S+O\left(\frac{1}{x}\right).\end{aligned}$$

Combining estimates (18.23) and (18.24), we get

$$\log U(x) = -\log\log x-\beta+S+O\left(\frac{1}{\log x}\right),$$

and exponentiating we get

$$U(x)=e^{-\log\log x}e^{-\beta+S}e^{O(1/\log x)}.$$

The result then follows in light of Remark 4.6. □

**Problem 4.6.** *Generalize Problem* 4.5 *by showing that for each nonzero real number* $\kappa$*, there exists a positive constant* $c_\kappa$ *such that*

$$\prod_{p\le x}\left(1+\frac{\kappa}{p}\right)=c_\kappa(\log x)^\kappa\left(1+O\left(\frac{1}{\log x}\right)\right)\qquad(x\to\infty).$$

*Solution.* Let $V_\kappa(x)$ denote the left-hand side. An argument similar to the one used in Problem 4.4 shows that

$$\log V_\kappa(x)=\kappa\log\log x+\beta+S_\kappa+O\left(\frac{1}{\log x}\right),$$

where now

$$S_\kappa=\sum_{p\ge 2}\left(\log\left(1+\frac{\kappa}{p}\right)-\frac{\kappa}{p}\right).$$

Exponentiate it and the result will follow. □

## Solutions to problems from Chapter 5

**Problem 5.2.** *Show that*

$$\sum_{x<p\le 2x}\frac{1}{p}=O\left(\frac{1}{\log x}\right).$$

*Solution.* Using Mertens' estimate, we get

$$\begin{aligned}\sum_{x<p\le 2x}\frac{1}{p} &= \sum_{p\le 2x}\frac{1}{p}-\sum_{p\le x}\frac{1}{p}\\ &= \left(\log\log(2x)+\beta+O\left(\frac{1}{\log(2x)}\right)\right)\\ &\qquad -\left(\log\log x+\beta+O\left(\frac{1}{\log x}\right)\right)\\ &= \log(\log 2+\log x)-\log\log x+O\left(\frac{1}{\log x}\right)\\ &= \log\left(1+\frac{\log 2}{\log x}\right)+O\left(\frac{1}{\log x}\right)=O\left(\frac{1}{\log x}\right),\end{aligned}$$

which proves our claim. □

**Problem 5.4.** *Show that the Prime Number Theorem is a consequence of the fact that*

$$\lim_{x\to\infty}\left(\sum_{p\le x}\frac{\log p}{p}-\log x\right)$$

*exists. Compare with Theorem* 4.4. *(Hint: Use Abel's summation formula.)*

*Solution.* Assume that there exists a constant $\delta$ such that

$$\sum_{p\le x}\frac{\log p}{p}=\log x+\delta+o(1)\qquad\text{as } x\to\infty. \tag{18.25}$$

Apply the Abel summation formula with $a_p=\frac{\log p}{p}$ for $p$ prime and $a_n=0$ for $n$ composite and $f(t)=t$. Then

$$\sum_{p\le x}\log p=\sum_{n\le x}a_nf(n)=A(x)x-\int_1^x A(t)dt, \tag{18.26}$$

where $A(t)=\log t+\delta+o(1)$ by (18.25) as $t\to\infty$. Clearly,

$$A(x)x=(\log x+\delta+o(1))x=x\log x+\delta x+o(x)\qquad\text{as } x\to\infty. \tag{18.27}$$

We split the integral at $\sqrt{x}$. In the smaller range, $A(t)=O(\log t)$, implying that, as $x\to\infty$,

(18.28)
$$\int_1^{\sqrt{x}}A(t)dt=O\left(\int_1^{\sqrt{x}}\log t\,dt\right)=O\left(\log x\int_1^{\sqrt{x}}dt\right)=O(\sqrt{x}\log x)=o(x).$$

In the larger range, $A(t)=\log t+\delta+o(1)$ for all $t\in[\sqrt{x},x]$. Note that to write "$o(1)$" we need the parameter to tend to infinity. This is why we split it at $\sqrt{x}$, although we could have equally well split it at $y(x)$, where $y(x)$ is any function of $x$ which is $o(x/\log x)$, and the result would have been the same. We then have

(18.29)
$$\begin{aligned}\int_{\sqrt{x}}^x A(t)dt&=\int_{\sqrt{x}}^x(\log t+\delta+o(1))dt\\&=(t\log t-t+\delta t)\Big|_{t=\sqrt{x}}^{t=x}+o\left(\int_{\sqrt{x}}^x dt\right)\\&=(x\log x-x+\delta x)-(\sqrt{x}\log(\sqrt{x})-\sqrt{x}+\delta\sqrt{x})+o(x)\\&=x\log x-x+\delta x+o(x)\qquad\text{as } x\to\infty,\end{aligned}$$

which together with estimate (18.28) gives

$$\int_1^x A(t)dt=x\log x-x+\delta x+o(x)\qquad(x\to\infty).$$

Using this last formula and (18.27) in estimate (18.26), we get

$$\theta(x) = \sum_{p \le x} \log p = x \log x + \delta x + o(x) - (x \log x - x + \delta x + o(x)) = x + o(x)$$

as $x \to \infty$, which is equivalent to the Prime Number Theorem. □

**Problem 5.6.** *Assume estimate* (5.20) *holds for all positive real numbers* $x$. *Show that estimate* (5.21) *also holds. (Hint: Use Abel's summation formula.)*

*Solution.* From formula (4.2) and estimate (5.20), we have

$$\theta(x) = \sum_{p \le x} \log p = \psi(x) + O(x^{1/2} \log x) = x + O(x^{1/2} (\log x)^2). \tag{18.30}$$

Write $g(x) = \theta(x) - x$. Apply the Abel summation formula with $a_n = \log n$ if $n$ is prime and $a_n = 0$ otherwise and $f(t) = 1/\log t$. Then

$$\pi(x) = \sum_{p \le x} 1 = \sum_{n \le x} a_n f(n) = A(x) f(x) - \int_2^x A(t) f'(t) dt.$$

Note that $A(x) = \theta(x) = x + g(x)$ while $f'(t) = -1/(t(\log t)^2)$. Thus,

$$\begin{aligned} \pi(x) &= \frac{x + g(x)}{\log x} + \int_2^x \frac{t + g(t)}{t(\log t)^2} dt \\ &= \left( \frac{x}{\log x} + \int_2^x \frac{dt}{(\log t)^2} \right) + \frac{g(x)}{\log x} + \int_2^x \frac{g(t)}{t(\log t)^2}\, dt. \end{aligned} \tag{18.31}$$

Estimate (18.30) shows that

$$\frac{g(x)}{\log x} = O(x^{1/2} \log x). \tag{18.32}$$

We split the integral of $g(t)/(t(\log t)^2)$ at $t = x^{1/2}$. In the low range, $g(t) = O(1/t^{1/2}) = O(1)$, so that

$$\int_2^{x^{1/2}} \frac{g(t) dt}{t(\log t)^2} = O\left( \int_2^{x^{1/2}} dt \right) = O(x^{1/2}). \tag{18.33}$$

In the upper range $t \in [x^{1/2}, x]$, we have that $g(t) = O(1/t^{1/2})$, which implies that

$$\int_{x^{1/2}}^x \frac{g(t) dt}{t(\log t)^2} = O\left( \int_{x^{1/2}}^x \frac{dt}{t^{1/2}} \right) = O\left( 2t^{1/2} \Big|_{t=x^{1/2}}^{t=x} \right) = O(x^{1/2}). \tag{18.34}$$

Combining estimates (18.33) and (18.34), we get

$$\int_2^x \frac{g(t)}{t(\log t)^2}\, dt = O(x^{1/2}). \tag{18.35}$$

Finally, it remains to observe that, by partial integration,

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t} = \frac{t}{\log t}\Big|_{t=2}^{t=x} + \int_2^x \frac{dt}{(\log t)^2} = \frac{x}{\log x} + \int_2^x \frac{dt}{(\log t)^2} + O(1),$$

so that

$$\frac{x}{\log x} + \int_2^x \frac{dt}{(\log t)^2} = \mathrm{li}(x) + O(1). \tag{18.36}$$

Now the desired estimate

$$\pi(x) = \mathrm{li}(x) + O(x^{1/2}\log x)$$

follows immediately from estimate (18.31) together with estimates (18.32), (18.35), and (18.36). □

**Problem 5.8.** *Show that there exists a constant $c$ such that the inequality*

$$\sum_{p\,|\,n} \frac{1}{p} \le \log\log\log n + c$$

*holds for all integers $n \ge e^{e^e}$. (Hint: Let $\omega(n) = k$. The right-hand side does not change if we replace all prime factors of $n$ by $p_1, \dots, p_k$. Now use Mertens' estimate and what is known about $k$.)*

*Solution.* Let $q_1 < q_2 < \cdots < q_k$ be all the distinct prime factors of $n$ and $p_1 < p_2 < \cdots < p_k$ be the first $k$ primes. Clearly, $q_i \ge p_i$ for all $i = 1, \dots, k$, so that

$$\sum_{p\,|\,n} \frac{1}{p} = \sum_{i=1}^{k} \frac{1}{q_i} \le \sum_{i=1}^{k} \frac{1}{p_i} = \sum_{p \le p_k} \frac{1}{p} = \log\log p_k + O(1). \tag{18.37}$$

However, $p_k \ll k\log k$ while $k \ll \log n$. Thus, $k\log k \ll (\log n)(\log\log n) < \log^2 n$, and therefore $p_k \ll \log^2 n$. It follows that

(18.38)

$$\begin{aligned}\log\log p_k &\le \log(\log\log n + O(1)) = \log\left((\log\log n)\left(1 + O\left(\frac{1}{\log\log n}\right)\right)\right)\\ &= \log\log\log n + \log\left(1 + O\left(\frac{1}{\log\log n}\right)\right)\\ &= \log\log\log n + O(1).\end{aligned}$$

Now the desired inequality follows from inequalities (18.37) and (18.38). □

**Problem 5.10.** *Use approximation* (5.24) *to show that*

$$\pi(2x) < 2\pi(x)$$

*if $x > x_0$, for some large $x_0$.*

*Solution.* Approximation (5.24) certainly implies that

$$\pi(x) = \mathrm{li}(x) + O\left(\frac{x}{\exp(\sqrt{\log x})}\right).$$

Thus,

$$\begin{aligned}
2\pi(x) - \pi(2x) &= 2\mathrm{li}(x) - \mathrm{li}(2x) + O\left(\frac{x}{\exp(\sqrt{\log x})}\right) \\
&= 2\int_2^x \frac{dt}{\log t} - \int_2^{2x} \frac{dt}{\log t} + O\left(\frac{x}{\exp(\sqrt{\log x})}\right) \\
&= \int_2^x \frac{dt}{\log t} - \int_x^{2x} \frac{dt}{\log t} + O\left(\frac{x}{\exp(\sqrt{\log x})}\right) \\
&= \int_2^x \frac{dt}{\log t} - \int_{x+2}^{2x} \frac{dt}{\log t} - \int_x^{x+2} \frac{dt}{\log t} + O\left(\frac{x}{\exp(\sqrt{\log x})}\right) \\
&= \int_2^x \frac{dt}{\log t} - \int_2^x \frac{dt}{\log(t+x)} + O\left(\frac{1}{\log x}\right) \\
&\qquad + O\left(\frac{x}{\exp(\sqrt{\log x})}\right) \\
&= \int_2^x \left(\frac{1}{\log t} - \frac{1}{\log(t+x)}\right) dt + O\left(\frac{x}{\exp(\sqrt{\log x})}\right) \\
&= \int_2^x \frac{\log(1+x/t)}{\log t \log(x+t)}\, dt + O\left(\frac{x}{\exp(\sqrt{\log x})}\right).
\end{aligned}$$

To arrive at the desired conclusion, it suffices to show that the error appearing in the $O$ above is in fact $o$ of the main term. Note that for the main term, we have that $x + t \le 2x$, implying that $\log(x+t) \ll \log x$ for all $t \in [2, x]$. We get a lower bound on the main term by considering the integral only up to $x/\log x$. Then $x/t \ge \log x$, and

$$\begin{aligned}
\int_2^x \frac{\log(1+x/t)}{\log t \log(x+t)}\, dt &\gg \frac{1}{\log x} \int_2^x \frac{\log(1+x/t)}{\log t}\, dt \\
&\ge \frac{1}{\log x} \int_2^{x/\log x} \frac{\log(1+x/t)}{\log t} dt \\
&\ge \frac{\log\log x}{\log x} \int_2^{x/\log x} \frac{dt}{\log t} \\
&= \frac{\log\log x}{\log x} \mathrm{li}\left(\frac{x}{\log x}\right) \gg \frac{\log\log x}{\log x} \pi\left(\frac{x}{\log x}\right) \\
&\gg \frac{\log\log x}{\log x} \left(\frac{x}{\log x}\right) \left(\frac{1}{\log(x/\log x)}\right)
\end{aligned}$$

$$\gg \frac{x \log\log x}{(\log x)^3},$$

and since

$$\frac{x}{\exp(\sqrt{\log x})} = o\left(\frac{x \log\log x}{(\log x)^3}\right) \qquad \text{as } x \to \infty,$$

we easily get that $2\pi(x) - \pi(2x)$ is positive for $x > x_0$. □

**Problem 5.12.** *Show that $d(n)$ is odd if and only if $n$ is a perfect square.*

*Solution.* From Problem 5.1 (or the displayed formula for $d(n)$), we have that if $n = q_1^{\ell_1} \cdots q_k^{\ell_k}$, where $q_1 < \cdots < q_k$ are primes and $\ell_1, \ldots, \ell_k$ are positive integers, then

$$d(n) = (\ell_1 + 1) \cdots (\ell_k + 1).$$

Clearly, the above number is odd if and only if $\ell_i + 1$ is odd for all $i = 1, \ldots, k$. This is equivalent to the fact that $\ell_i$ is even for all $i = 1, \ldots, k$, which obviously is equivalent, via unique factorization, to the fact that $n$ is a perfect square. □

**Problem 5.14.** *Let $f : [2, +\infty[ \to \mathbf{R}^+$ be a continuous function such that $f(n)/\log n$ is decreasing on $[2, +\infty[$. Then,*

$$\sum_{p \le x} f(p) = (1 + o(1)) \int_2^x \frac{f(t)}{\log t}\, dt + O(1) \qquad (x \to \infty).$$

*Solution.* We use the Prime Number Theorem in the form

$$\theta(x) = x + x\varepsilon(x) \qquad \text{with } \varepsilon(x) = o(1), \tag{18.39}$$

where $\theta(x) = \sum_{p \le x} \log p$. First, let us assume that $x = N$, an integer; it is clear that the more general case $x \notin \mathbf{N}$ will easily follow. Since, for each integer $n \ge 2$,

$$\frac{\theta(n) - \theta(n-1)}{\log n} = \begin{cases} 1 & \text{if } n \text{ is prime,} \\ 0 & \text{otherwise} \end{cases}$$

and since $\theta(n) - \theta(n-1) = 1 + n\varepsilon(n) - (n-1)\varepsilon(n-1)$, we may write

$$\begin{aligned} \sum_{p \le N} f(p) &= \sum_{2 \le n \le N} \frac{\theta(n) - \theta(n-1)}{\log n} f(n) \\ &= \sum_{2 \le n \le N} \frac{f(n)}{\log n} + \sum_{2 \le n \le N} (n\varepsilon(n) - (n-1)\varepsilon(n-1)) \frac{f(n)}{\log n} \end{aligned}$$

$$\begin{aligned} &= \sum_{2\le n\le N} \frac{f(n)}{\log n} + \sum_{2\le n\le N-1} n\varepsilon(n)\left(\frac{f(n)}{\log n} - \frac{f(n+1)}{\log(n+1)}\right) \\ &\qquad + N\varepsilon(N)\frac{f(N)}{\log N} - \varepsilon(1)\frac{f(2)}{\log 2} \\ &= S_1 + S_2, \end{aligned}$$

say. We now estimate $S_1$ and $S_2$ separately. For the estimation of $S_1$, we use (1.2) and obtain

$$\sum_{2\le n\le N} \frac{f(n)}{\log n} = \int_2^x \frac{f(t)}{\log t}\,dt + C + O\left(\frac{f(N)}{\log N}\right) = \int_2^x \frac{f(t)}{\log t}\,dt + O(1).$$

Here we used a weak form of (1.5), that is, without the constant $A$ which normally appears in (1.2), because we do not have the hypothesis "$f(N)/\log N$ tends to 0 as $N \to \infty$": indeed, we know only that $f(N)/\log N = O(1)$. Let $\delta > 0$ be an arbitrarily small number. The proof will be complete if we succeed in showing that

$$|S_2| < \delta \sum_{2\le n\le N} \frac{f(n)}{\log n} + O(1).$$

But it follows from (18.39) that there exists a positive integer $N_0 = N_0(\delta) > 2$ such that $|\varepsilon(n)| < \delta$ if $n \ge N_0$. But

$$|S_2| \le O(1) + \delta\left\{\sum_{N_0\le n\le N-1} n\left|\frac{f(n)}{\log n} - \frac{f(n+1)}{\log(n+1)}\right| + N\frac{f(N)}{\log N}\right\}.$$

Since the function $f(n)/\log n$ is decreasing, we can eliminate the absolute values and rearrange the terms and obtain

$$|S_2| \le O(1) + \delta \sum_{N_0\le n\le N} \frac{f(n)}{\log n}(n-(n-1)) = O(1) + \delta \sum_{N_0\le n\le N} \frac{f(n)}{\log n},$$

which is the result we were looking for. □

## Solutions to problems from Chapter 6

**Problem 6.2.** *Let $\beta(1) = 1$ and, for each $n \ge 2$, set $\beta(n) = \prod_{i=1}^{r} \frac{3+(-1)^{\alpha_i}}{2}$ if $n = q_1^{\alpha_1}\cdots q_r^{\alpha_r} > 1$. Prove that the asymptotic mean of $\beta(n)$ exists and is equal to $\frac{\zeta(2)}{\zeta(3)}$.*

*Solution.* Observe that

$$\sum_{n=1}^{\infty} \frac{\beta(n)}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{2}{p^{2s}} + \frac{1}{p^{3s}} + \frac{2}{p^{4s}} + \cdots\right) = \frac{\zeta(s)\zeta(2s)}{\zeta(3s)}.$$

The result then follows from applying Wintner's theorem. □

**Problem 6.4.** *Deduce from Problems* 6.2 *and* 6.3 *that for each* $\varepsilon > 0$,

$$\sum_{n \le N} \beta(n) = cN + O\left(N^{\frac{1}{2}+\varepsilon}\right),$$

*where* $c = \dfrac{\zeta(2)}{\zeta(3)} \approx 1.36843$.

*Solution.* The result does indeed follow immediately from Problems 6.2 and 6.3. □

**Problem 6.6.** *Is the sum of two additive functions always additive? What about the product of two additive functions?*

*Solution.* It is easy to establish that if $f$ and $g$ are both additive, then the function $f + g$ is also additive, while the product $fg$ is not necessarily additive; simply take $f(n) = g(n) = \log n$. □

**Problem 6.8.** *Prove that* $\displaystyle\sum_{p>N} \frac{1}{p^2} \ll \frac{1}{N \log N}$.

*Solution.* Since $\pi(n) - \pi(n-1) = 1$ or 0, depending if $n$ is prime or not, we have that

$$\begin{aligned}
\sum_{p>N} \frac{1}{p^2} &= \sum_{n>N} \frac{\pi(n) - \pi(n-1)}{n^2} \\
&< \sum_{n>N} \pi(n) \left(\frac{1}{n^2} - \frac{1}{(n+1)^2}\right) < 3 \sum_{n>N} \frac{\pi(n)}{n(n+1)^2} \\
&\ll \sum_{n>N} \frac{1}{(n+1)^2 \log n} < \frac{1}{\log N} \sum_{n>N} \frac{1}{(n+1)^2} \\
&\ll \frac{1}{\log N} \int_N^{\infty} \frac{1}{(t+1)^2}\, dt \ll \frac{1}{N \log N},
\end{aligned}$$

where we used Chebyshev's estimate. □

**Problem 6.10.** *Let $f$ be an additive function such that*

$$\sum_p \frac{|f(p)-1|}{p} < +\infty$$

*and such that $f(p^a) - f(p^{a-1}) = O(1)$ uniformly for $p$ prime and $a \geq 2$. Prove that*

$$\sum_{n\leq N} f(n) = N\log\log N + D_2 N + o(N),$$

*where*

$$D_2 = D_1 + \sum_p \frac{f(p)-1}{p} + \gamma$$

*and $D_1$ is the constant appearing in Theorem* 6.19.

*Solution.* First observe that

$$\begin{aligned}\sum_{n\leq N} f(n) &= N\sum_{p\leq N}\frac{f(p)}{p} + N\sum_{\substack{p^a\leq N\\ a\geq 2}}\frac{f(p^a)-f(p^{a-1})}{p^a}\\ &\quad + \sum_{p\leq N} f(p)\left(\left\lfloor\frac{N}{p}\right\rfloor - \frac{N}{p}\right)\\ &\quad + \sum_{\substack{p^a\leq N\\ a\geq 2}}\left(f(p^a)-f(p^{a-1})\right)\left(\left\lfloor\frac{N}{p^a}\right\rfloor - \frac{N}{p^a}\right).\end{aligned}$$

We shall now focus our attention on two expressions, namely

$$\begin{aligned}S_1 &= \sum_{p\leq N}\frac{f(p)}{p},\\ S_2 &= \sum_{p\leq N} f(p)\left(\left\lfloor\frac{N}{p}\right\rfloor - \frac{N}{p}\right),\end{aligned}$$

since the ones tied to the other terms are clearly of smaller order.

First, in light of Theorem 4.5, we have

$$\begin{aligned}S_1 &= \sum_{p\leq N}\frac{f(p)-1}{p} + \sum_{p\leq N}\frac{1}{p}\\ &= \sum_p \frac{f(p)-1}{p} - \sum_{p>N}\frac{f(p)-1}{p} + N\log\log N + C_1 N + o(N) \qquad (18.40)\\ &= \sum_p \frac{f(p)-1}{p} + o(1) + N\log\log N + C_1 N + o(N)\end{aligned}$$

as $N \to \infty$. To estimate $S_2$, we first set

$$S(N) = \sum_{p \le N} \frac{|f(p) - 1|}{p}$$

and observe that

$$S(N) = \sum_{p} \frac{|f(p) - 1|}{p} + o(1) = C_0 + o(1), \tag{18.41}$$

for some constant $C_0$, as $N \to \infty$. Using Abel's Lemma and (18.41), we obtain that

$$\begin{aligned} S_2 &\ll \sum_{p \le N} |f(p)| \le \sum_{p \le N} |f(p) - 1| + \pi(N) \\ &= \sum_{p \le N} \frac{|f(p) - 1|}{p}\, p \quad + \; O\left(\frac{N}{\log N}\right) \\ &= S(N) \cdot N - \int_1^N S(t)\, dt + O\left(\frac{N}{\log N}\right) \\ &= C_0 N + o(N) - \int_1^N (C_0 + o(1))\, dt + O(N/\log N) \\ &= o(N) \end{aligned} \tag{18.42}$$

as $N \to \infty$. Combining relations (18.40) and (18.42), the result follows. □

**Problem 6.12.** *Prove that*

$$\sum_{n \le N} \log d(n) = (\log 2) N \log\log N + AN + o(N) \qquad (N \to \infty),$$

*where*

$$A = \log 2 \left\{ \gamma + \sum_{p} \left( \log\left(1 - \frac{1}{p}\right) + \frac{1}{p} \right) \right\} + \sum_{p} \sum_{r \ge 2} \frac{\log(1 + \frac{1}{p})}{p^r}.$$

*Solution.* Let $f(n) = \frac{\log \tau(n)}{\log 2}$ and apply Theorem 6.19. □

## Solutions to problems from Chapter 7

**Problem 7.2.** *Given a positive integer $k$, let*

$$\sigma_k(n) = \sum_{d \,|\, n} d^k$$

*be the sum of the k-th powers of the divisors of n. Find the average value of $\sigma_k(n)$ on the interval $[1, x]$. (Hint: Find the average value of $\sigma_k(n)/n^k$ by first proving that $\sigma_k(n)/n^k = \sum_{d\,|\,n} 1/d^k$. Then use Abel's summation formula.)*

*Solution.* Since

$$\frac{\sigma_k(n)}{n^k} = \sum_{d\,|\,n} \frac{d^k}{n^k} = \sum_{d\,|\,n} \frac{1}{(n/d)^k} = \sum_{d\,|\,n} \frac{1}{d^k},$$

we have that

$$\begin{aligned} A(x) &= \sum_{n\le x} \frac{\sigma_k(n)}{n^k} = \sum_{n\le x}\sum_{d\,|\,n} \frac{1}{d^k} = \sum_{d\le x} \frac{1}{d^k} \sum_{\substack{n\le x \\ n\equiv 0 \pmod d}} 1 = \sum_{d\le x} \frac{1}{d^k} \left\lfloor \frac{x}{d} \right\rfloor \\ &= \sum_{d\le x} \frac{1}{d^k} \left( \frac{x}{d} + O(1) \right) = x \sum_{d\le x} \frac{1}{d^{k+1}} + O\left( \sum_{d\le x} \frac{1}{d} \right) \\ &= x \left( \zeta(k+1) - \sum_{d>x} \frac{1}{d^{k+1}} \right) + O(\log x) = x\zeta(k+1) + O(\log x), \end{aligned}$$

where we used the estimate

$$\sum_{d>x} \frac{1}{d^{k+1}} \le \int_{x-1}^{\infty} \frac{dt}{t^{k+1}} = -\frac{1}{k}\frac{1}{t^k}\Big|_{t=x-1}^{t=\infty} \ll \frac{1}{x^k} \ll \frac{1}{x}.$$

By Abel's summation formula with $a_n = \sigma_k(n)/n^k$ and $f(t) = t^k$, we get

$$\begin{aligned} \sum_{n\le x} \sigma_k(n) &= \sum_{n\le x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt \\ &= (\zeta(k+1)x + O(\log x))x^k - k\int_1^x (\zeta(k+1)t + O(\log t))t^{k-1}dt \\ &= \zeta(k+1)x^{k+1} + O(x^k \log x) \\ &\qquad -k\int_1^x (\zeta(k+1)t^k + O(t^{k-1}\log t))dt \\ &= \zeta(k+1)x^{k+1} + O(x^k \log x) - \frac{k\zeta(k+1)}{k+1}x^{k+1} \\ &\qquad + O\left( \log x \int_1^x t^{k-1}dt \right) \\ &= \frac{\zeta(k+1)}{k+1}x^{k+1} + O(x^k \log x), \end{aligned}$$

so that the desired average value is

$$\frac{1}{x}\sum_{n\le x}\sigma_k(n) = \frac{\zeta(k+1)}{k+1}x^k + O(x^{k-1}\log x) \sim \frac{\zeta(k+1)}{k+1}x^k$$

as $x \to \infty$. □

**Problem 7.4.** *Show that $d(mn) \le d(m)d(n)$ for all positive integers $m$ and $n$.*

*Solution.* The function

$$\{d_1 : d_1 \mid m\} \times \{d_2 : d_2 \mid n\} \longrightarrow \{d : d \mid mn\}; \qquad (d_1, d_2) \mapsto d_1 d_2$$

is certainly surjective, because if $d \mid mn$, then putting $d_1 = \gcd(d, m)$, we have that $d/d_1 \mid (m/d_1)n$, and since $d/d_1$ and $m/d_1$ are coprime, we get that $d/d_1 \mid n$. Hence, $d = d_1 d_2$, where $d_1$ and $d_2 = d/d_1$ are divisors of $m$ and $n$, respectively. But if $f : A \longrightarrow B$ is a surjection, then $\#A \le \#B$. Thus,

$$\begin{aligned} d(mn) &= \#\{d : d \mid mn\} \le \#\left(\{d_1 : d_1 \mid m\} \times \{d_2 : d_2 \mid n\}\right) \\ &= \#\{d_1 : d_1 \mid m\} \cdot \#\{d_2 : d_2 \mid n\} = d(m)d(n), \end{aligned}$$

which is the desired inequality. □

**Problem 7.6.** *Prove the following strengthening of Lemma* 7.18*: The set*

$$A = \{n : |\omega(n) - \log\log n| > (\log\log n)^{2/3}\}$$

*is of asymptotic density zero. (Hint: Show that if $x$ is large and $n \in A \cap [x/\log x, x]$, then $|\omega(n) - \log\log x|^2 > (\log\log x)^{4/3}$. Now use the Turán-Kubilius inequality to obtain that the number of such positive integers $n \le x$ is $\ll x/(\log\log x)^{1/3} = o(x)$ as $x \to \infty$.)*

*Solution.* Let $x$ be large and $n \in B = A \cap [x/\log x, x]$. Then $\log\log n < \log\log x$, while

$$\log\log n > \log\log(x/\log x) = \log\log x + \log\left(1 - \frac{\log\log x}{\log x}\right) > \log\log x - 1$$

for $x > x_0$. Thus,

$$\begin{aligned} |\omega(n) - \log\log x| &= |\omega(n) - \log\log n| + O(1) > (\log\log n)^{2/3} + O(1) \\ &> \frac{1}{2}(\log\log x)^{2/3} \end{aligned}$$

for all $n \in B$ and $x > x_0$. Hence, by the Turán-Kubilius inequality, we have

$$\#B \cdot (1/2)^2(\log\log x)^{4/3} < \sum_{n\in B}(\omega(n) - \log\log x)^2 = O(x\log\log x),$$

giving

$$\#B \ll \frac{x}{(\log\log x)^{1/3}}.$$

Thus,

$$\#(A \cap [1,x]) \le \#B + \#\{n \le x/\log x\} \ll \frac{x}{(\log\log x)^{1/3}} + \frac{x}{\log x} = o(x)$$

as $x \to \infty$, which implies the desired conclusion. □

**Problem 7.8.** *Consider the set $A$ of those positive integers which do not contain the digit 7 in their decimal expansion.*

(i) *Show that $A$ is of zero density.*

(ii) *Show that most integers contain each of the digits 0,1,...,9.*

(iii) *Show that the sum of the reciprocals of the elements of $A$ converges.*

*Solution.* Given a positive integer $n$, let $\ell(n)$ stand for the number of its digits. For each integer $k \ge 1$, let $A_k = \{n \in A : \ell(n) = k\}$. It is easy to see that $\#A_1 = 8$, that $\#A_2 = 8 \times 9$ and more generally that, for each integer $k \ge 1$, $\#A_k = 8 \times 9^{k-1}$. Let $A(x) = \#\{n \le x : n \in A\}$.

To prove (i), we need to show that

$$\lim_{x\to\infty} \frac{A(x)}{x} = 0. \tag{18.43}$$

First consider the case when $x = 10^r$ for some positive integer $r$. In this case, we have

$$\begin{aligned} \frac{A(x)}{x} &= \frac{A(10^r)}{10^r} = \frac{1}{10^r}\left(1 + \sum_{k=1}^{r} \#A_k\right) \\ &= \frac{1}{10^r}\left(1 + \sum_{k=1}^{r} 8 \times 9^{k-1}\right) = \frac{1}{10^r}\left(1 + 8\sum_{j=0}^{r-1} 9^j\right) = \frac{9^r}{10^r} = \left(\frac{9}{10}\right)^r, \end{aligned}$$

a quantity which tends to 0 as $r \to \infty$, thus establishing (18.43) in the case $x = 10^r$. It is now an easy matter to prove that (18.43) holds in the general case, thus establishing (i).

Denoting by $B_j$, for $j = 0, 1, 2, \ldots, 9$, the set of those positive integers which do not contain the digit $j$, it follows from (i) that each $B_j$ is of zero density, which indeed implies that most integers contain each of the digits $0, 1, 2, \ldots, 9$, thus establishing (ii).

Finally, observing that

$$\sum_{n\in A}\frac{1}{n}=\sum_{k=1}^{\infty}\sum_{\substack{n\in A\\ \ell(n)=k}}\frac{1}{n}\le\sum_{k=1}^{\infty}\frac{1}{10^{k-1}}\sum_{\substack{n\in A\\ \ell(n)=k}}1=\sum_{k=1}^{\infty}\frac{8\times 9^{k-1}}{10^{k-1}}=80,$$

(iii) follows immediately. □

**Problem 7.10.** *Let $A$ be a set of positive integers for which the counting function $A(x)=\#\{n\le x : n\in A\}$ satisfies*

$$A(x)=\frac{x}{L(x)}(1+o(1))\qquad (x\to\infty),$$

*where $L(x)$ is a function satisfying $L(x)\gg(\log x)^{1+\delta}$ for a certain real number $\delta>0$. Prove that*

$$\sum_{n\in A}\frac{1}{n}<+\infty.$$

*Solution.* It is easy to establish that

$$\sum_{\substack{n\le x\\ n\in A}}\frac{1}{n}=\sum_{n\le x}\frac{A(n)}{n(n+1)}+\frac{A(x)}{\lfloor x\rfloor+1}.$$

Using this relation, we obtain that

$$\sum_{\substack{n\le x\\ n\in A}}\frac{1}{n}\ll\sum_{n\le x}\frac{1}{nL(n)}+\frac{1}{L(x+1)}\ll\sum_{2\le n\le x}\frac{1}{n(\log n)^{1+\delta}},$$

a sum which is easily shown to be bounded. □

**Problem 7.12.** *Show that the set $A=\{n : \omega(n)\mid n\}$ is of asymptotic density zero. (Hint: Let $x$ be a large positive real number and set $y=\log\log x$. Use Problem 7.6 to infer that all $n\le x$ have $\omega(n)\in I=[y-y^{2/3},y+y^{2/3}]$ with $o(x)$ exceptions. So, if such an integer $n$ is in $A$, then $k\mid n$ for some $k\in I$. The number of such $n\le x$ for a fixed $k$ is $\le x/k$. Thus, the set in question has at most*

$$x\sum_{y-y^{2/3}\le k\le y+y^{2/3}}\frac{1}{k}$$

*elements. Now use Theorem 1.7 to deduce that the above sum is $o(1)$ as $y\to\infty$.)*

*Solution.* By Problem 7.6, we know that all $n\le x$ have $\omega(n)\in[y-y^{2/3},y+y^{2/3}]$, where $y=\log\log x$, with the possible exception of a set of integers

$n$ of cardinality not exceeding $o(x)$ as $x \to \infty$. If $\omega(n) \mid n$, and $n$ is one of these numbers, then $k \mid n$ for some integer $k \in [y - y^{2/3}, y + y^{2/3}]$. The number of such integers $n \le x$ is $\le \lfloor x/k \rfloor \le x/k$. So, the number of such $n$ is bounded by

$$x \sum_{y-y^{2/3} \le k \le y+y^{2/3}} \frac{1}{k}.$$

Now, by Theorem 1.7,

$$\begin{aligned}
\sum_{y-y^{2/3} \le k \le y+y^{2/3}} \frac{1}{k} &= \sum_{k \le y+y^{2/3}} \frac{1}{k} - \sum_{k < y-y^{2/3}} \frac{1}{k} \\
&= \left( \log(y + y^{2/3}) + \gamma + O\left(\frac{1}{y}\right) \right) \\
&\quad - \left( \log(y - y^{2/3}) + \gamma + O\left(\frac{1}{y}\right) \right) \\
&= \log\left( \frac{y + y^{2/3}}{y - y^{2/3}} \right) + O\left(\frac{1}{y}\right) \\
&= \log\left( 1 + \frac{2y^{2/3}}{y - y^{2/3}} \right) + O\left(\frac{1}{y}\right) \\
&= \log\left( 1 + O\left(\frac{1}{y^{1/3}}\right) \right) + O\left(\frac{1}{y}\right) \\
&= O\left(\frac{1}{y^{1/3}}\right) = o(1) \qquad \text{as } y \to \infty,
\end{aligned}$$

so that indeed the number of $n \le x$ for which $\omega(n) \mid n$ is $o(x)$ as $x \to \infty$. □

**Problem 7.14.** *Show that if $\sigma(n)$ is odd, then $n = m^2$ or $n = 2m^2$ for some integer $m$.*

*Solution.* Assume $n > 1$. Let $n = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$, where $q_1, \ldots, q_k$ are distinct primes. If $q_i$ is odd and $\alpha_i$ is odd, then

$$\sigma(q_i^{\alpha_i}) = 1 + q_i + q_i^2 + \cdots + q_i^{\alpha_i}$$

is a sum of $\alpha_i + 1$ (= even) odd terms, implying that it is even. Since $\sigma(q_i^{\alpha_i}) \mid \sigma(n)$, we get that $\sigma(n)$ is also even in this case. Therefore, the conclusion is that if $\sigma(n)$ is even, then $\alpha_i$ is even whenever $q_i$ is an odd prime factor of $n$. Thus, $n = m^2$ or $2m^2$ according to whether the exponent at which the prime 2 appears in the factorization of $n$ is even or odd. Note that the condition from the problem is actually an "if and only if" statement (that is, if $n = m^2$ or $2m^2$, then $\sigma(n)$ is odd). □

**Problem 7.16.** *Show that the sum of the reciprocals of the perfect numbers is convergent. (Hint: Let $A$ be the set of all odd perfect numbers. Show, using the previous problem, that $\#(A \cap [1,x]) = O(x^{1/2}\log x)$ by noting that if $n = p^{2\alpha+1}m^2$, then $p \mid \sigma(m^2)$. Then use Abel's summation formula.)*

*Solution.* Let $A$ be the set of odd perfect numbers. Let $n \in A \cap [1,x]$. Then $n = p^{2\alpha+1}m^2$, where $p$ is a prime coprime to $m$. Then

$$2n = 2p^{2\alpha+1}m^2 = \sigma(n) = \sigma(p^{2\alpha+1})\sigma(m^2) = (1 + p + \cdots + p^{2\alpha+1})\sigma(m^2).$$

From the above relation, we see that $p^{2\alpha+1} \mid \sigma(m^2)$. To count those integers $n$, note first that since $n \le x$, we get that $m^2 \le x$, so that $m \le x^{1/2}$. For each fixed $m$, we have that $p^{2\alpha+1}$ is a prime power divisor of

$$\sigma(m^2) < \sum_{k \le m^2} k < m^4.$$

Hence, once $m$ is fixed, $p^{2\alpha+1}$ can be chosen in at most

$$\Omega(\sigma(m^2)) \ll \log(\sigma(m^2)) \le \log(m^4) \ll \log x$$

ways. Thus, $A(x) = \#(A \cap [1,x]) \ll \sqrt{x}\log x$. Then, by Abel's summation formula with $a_n = 1$ if $n$ is odd perfect and $a_n = 0$ otherwise, and $f(t) = 1/t$, we have that

$$\begin{aligned}
\sum_{\substack{n \le x \\ n \in A}} \frac{1}{n} &= \sum_{n \le x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f(t)dt \\
&= O\left(\frac{\sqrt{x}\log x}{x}\right) + O\left(\int_1^x \frac{\sqrt{t}\log t}{t^2}\,dt\right) \\
&= o(1) + O\left(\int_1^x \frac{\log t}{t^{3/2}}\,dt\right) = O(1)
\end{aligned}$$

because this last integral clearly converges to a finite limit as $x \to \infty$. To estimate the sum of the reciprocals of the even perfect numbers, note that by Proposition 7.20, it is at most

$$\sum_{p \ge 2} \frac{1}{2^{p-1}(2^p - 1)},$$

which also converges. □

**Problem 7.18.** *It is not known if there exist infinitely many multiperfect numbers, that is, positive integers $n$ such that $n \mid \sigma(n)$. (See, for instance, Guy's book* [**71**]*.) Prove that if $s \ge 2$ is a fixed integer, then there exist infinitely many positive integers $n$ such that $n \mid \sigma_s(n)$, where $\sigma_s(n) = \sum_{d \mid n} d^s$.*

*Solution.* Start with the prime number $q_1 = 2$, and let $q_2$ be any prime divisor of $\sigma_s(2) = 1 + 2^s$. Clearly, $n_1 = 2q_2$ has the property that $\sigma_s(n_1) = (1 + 2^s)(1 + q_2^s)$ is a multiple of $n_1$ because $q_2 \mid (1 + 2^s)$ and $2 \mid (1 + q_2^s)$. To continue, we look at the expression $1 + q_2^s$. Since $q_2$ is odd and $s \geq 2$, it follows that $1 + q_2^s \geq 1 + 3^2 = 10$. Thus, either $2^3 \mid (1 + q_2^s)$, or there exists some odd prime $q_3$ such that $q_3 \mid (1 + q_2^s)$. Note that in the latter case $q_3$ is distinct from $q_2$. In the former case, $n_2 = 2^3 q_2$ has the property that $\sigma_s(n_2) = (1 + 2^s + 2^{2s} + 2^{3s})(1 + q_2^s) = (1 + 2^s)(1 + 2^{2s})(1 + q_2^s)$ is a multiple of $n_2$ because $2^3 \mid (1 + q_2^s)$ and $q_2 \mid (1 + 2^s)$. In the latter case, $n_2 = 2q_2q_3$ has the property that $\sigma_s(n_2) = (1 + 2^s)(1 + q_2^s)(1 + q_3^s)$ is a multiple of $n_2$ because $2 \mid (1 + q_2^s)$, $q_2 \mid (1 + 2^s)$ and $q_3 \mid (1 + q_2^s)$.

We now use induction to construct infinitely many positive integers $n_1, n_2, \ldots$, all of which are larger than 1, and such that they all satisfy $n_\ell \mid \sigma_s(n_\ell)$ for $\ell \geq 1$. Assume that $\ell \geq 2$ and that $n_\ell$ has been constructed.

If there exists a prime number $q$ such that $q \mid \sigma_s(n_\ell)$ but $q \nmid n_\ell$, we then let $n_{\ell+1} = qn_\ell$ and observe that $\sigma_s(n_{\ell+1}) = (1 + q^s)\sigma_s(n_\ell)$. We further note that since both $n_\ell$ and $q$ divide $\sigma_s(n_\ell)$ and $q$ and $n_\ell$ are coprime, it follows that $n_{\ell+1} \mid \sigma_s(n_\ell)$, implying that $n_{\ell+1} \mid \sigma_s(n_{\ell+1})$.

Assume now that every prime factor of $\sigma_s(n_\ell)$ is also a prime factor of $n_\ell$. Write

$$n_\ell = \prod_{i=1}^{t} q_i^{\alpha_i} \quad \text{and} \quad \sigma_s(n_\ell) = \prod_{i=1}^{t} q_i^{\beta_i},$$

where $q_1, q_2, \ldots, q_t$ are distinct primes, and $\alpha_i$ and $\beta_i$ are positive integers for $i = 1, \ldots, t$, with $\beta_i \geq \alpha_i$. Since

$$\sigma_s(n_\ell) > n_\ell^s \geq n_\ell^2,$$

it follows that there exists $i \in \{1, \ldots, t\}$ such that $\beta_i \geq 2\alpha_i + 1$. By relabeling the primes, we may assume that $\beta_1 \geq 2\alpha_1 + 1$. Consider the number

$$n_{\ell+1} = q_1^{2\alpha_1+1} \cdot \prod_{i=2}^{t} q_i^{\alpha_i}.$$

Then,

$$\begin{aligned} \sigma_s(n_{\ell+1}) &= \sigma_s(q_1^{2\alpha_1+1}) \cdot \prod_{i=2}^{t} \sigma_s(q_i^{\alpha_i}) \\ &= (1 + q_1^{(\alpha_1+1)s})\sigma_s(q_1^{\alpha_1}) \cdot \prod_{i=2}^{t} \sigma_s(q_i^{\alpha_i}) \\ &= (1 + q_1^{(\alpha_1+1)s})\sigma_s(n_\ell). \end{aligned} \tag{18.44}$$

From (18.44), it is immediate that $n_{\ell+1} \mid \sigma_s(n_{\ell+1})$. Indeed, if $i \geq 2$, then $q_i^{\alpha_i} \mid n_\ell$, $n_\ell \mid \sigma_s(n_\ell)$ and $\sigma_s(n_\ell) \mid \sigma_s(n_{\ell+1})$, and we have that $q_i^{\alpha_i} \mid \sigma_s(n_{\ell+1})$ for $i = 2, \ldots, t$. For $i = 1$, $q_1^{2\alpha_1+1} \mid q_1^{\beta_1}$, $q_1^{\beta_1} \mid \sigma_s(n_\ell)$ and $\sigma_s(n_\ell) \mid \sigma_s(n_{\ell+1})$, so that $q_1^{2\alpha_1+1} \mid \sigma_s(n_{\ell+1})$, which concludes the proof of the fact that $n_{\ell+1} \mid \sigma_s(n_{\ell+1})$. □

**Remark.** Let $x$ be a large positive real number. The above argument shows that

$$n_1 \leq 2(1 + 2^s) < e^{s+1}, \tag{18.45}$$

and

$$n_{\ell+1} \leq \sigma_s(n_\ell) = \sum_{d \mid n_\ell} d^s < n_\ell^{s+1}. \tag{18.46}$$

Now estimates (18.45) and (18.46), and induction on $\ell$, show that the inequality

$$n_\ell < e^{(s+1)^\ell}$$

holds for all $\ell \geq 1$. Thus, for the inequality $n_\ell \leq x$ to hold, it suffices that

$$e^{(s+1)^\ell} \leq x$$

holds, which is equivalent to

$$\ell \leq \frac{\log\log x}{\log(s+1)}.$$

In particular, the number of positive integers $n \leq x$ such that the relation $n \mid \sigma_\ell(n)$ holds is at least

$$\left\lfloor \frac{\log\log x}{\log(s+1)} \right\rfloor + 1 > \frac{\log\log x}{\log(s+1)}.$$

(Note that the number $n = 1$ fulfills the above property as well.) It would be interesting to find a larger lower bound on the cardinality of the set

$$\{n \leq x \ : \ n \mid \sigma_s(n)\}.$$

**Problem 7.20.** *Prove that there are infinitely many odd positive integers $k$ not of the form $2^n + p$ for any positive integer $n$ and odd prime $p$. Is it easier to show that there are infinitely many odd positive integers $k$ not of the form $10^n + p$ for any positive integer $n$ and prime $p$ ?*

*Solution.* Let $(a_i, b_i, p_i)_{i=1}^u$ be as in the beginning of the proof of Proposition 7.21. Now choose $k$ in the arithmetical progressions

$$k \equiv 2^{a_i} \pmod{p_i}$$

for all $i = 1, \dots, u$. This creates a progression $k \equiv k_0 \pmod{P}$, where $k_0$ is some positive integer and $P = p_1 \cdots p_u$. Let $x$ be a large positive real number. The number of positive integers $k \le x$ in this arithmetical progression is $\ge \lfloor (x - k_0)/P \rfloor \gg x$. Assume that $k = 2^n + p$ for some prime $p$. Since $n \equiv a_i \pmod{b_i}$ for some $i = 1, \dots, u$, we get that $n = a_i + b_i t$ for some nonnegative integer $t$. Then

$$2^n = 2^{a_i + b_i t} = 2^{a_i}((2^{b_i} - 1) + 1)^t \equiv 2^{a_i} \pmod{p_i} \equiv k \pmod{p_i}.$$

Thus, $k - 2^n$ is a multiple of $p_i$. Since it is prime, we get that $p = p_i$. Thus, at best $k = 2^n + p_i$ for some $i = 1, \dots, u$ and some integer $n$. For each fixed $p_i$, the number of positive integers $m \le x$ of the form $2^n + p_i$ is $\le \lfloor \log(x - p_i)/\log 2 \rfloor \ll \log x$, and since we have only $u = O(1)$ primes $p_i$, we get that the number of numbers $\le x$ of the form $2^n + p_i$ for some natural number $n$ and $i \in \{1, \dots, u\}$ is $O(\log x)$. Removing these numbers from the $\lfloor (x - k_0)/P \rfloor$ numbers $k \le x$ in the progression $k_0 \pmod{P}$, we end up with a number of numbers of size

$$\gg x + O(\log x) \gg x$$

of positive integers $k \le x$, none of which is of the form $2^n + p$ for any natural number $n$ and prime $p$. Letting $x$ go to infinity, we get the desired conclusion.

Yes, it is easier for numbers not of the form $10^n + p$. Namely, let $A$ be the set of odd positive integers $m \le x$. Clearly, $\#A = \lfloor x/2 \rfloor \ge (1 + o(1))x/2$ as $x \to \infty$. If $m = 10^n + p$, then $p \le x$, so that there are at most $\pi(x) = (1 + o(1))x/\log x$ possibilities for $p$ as $x \to \infty$. Moreover, since $10^n \le x$, we get that $n \le \log x/\log 10$, so there are at most $(\log x)/\log 10$ possibilities for $n$. Multiplying the above two bounds, we get that the number of numbers of the form $10^n + p$ which do not exceed $x$ is at most $(1 + o(1))x/\log 10$ as $x \to \infty$. Since $\log 10 > 2$, we get that for very large $x$, there are at least

$$(1 + o(1)) \left( \frac{1}{2} - \frac{1}{\log 10} \right) x$$

odd positive integers $m \le x$ not of the form $10^n + p$ for any prime $p$ and natural number $n$. Note that this argument would not have worked if 10 had been replaced by 2 because $\log 2$ is not larger than 2. □

**Problem 7.22.** *Let $a > b$ be coprime positive integers, and let $x > a$. Show that*

$$\sum_{n \le x} d(an + b) \ll x \log x.$$

*Solution.* We use a similar argument to the one used in the previous problem. Since $an+b<(x+1)^2$, it follows that if $x$ is large and $d\geq x+1$ is a divisor of $an+b$, then its complementary divisor $(an+b)/d$ is $\leq x+1$. So, if we write $d_{x+1}(m)$ for the number of divisors of $m$ which are $\leq x+1$, then

$$d(an+b)\leq 2d_{x+1}(an+b).$$

It follows that

$$\begin{aligned}\sum_{n\leq x} d(an+b) &\leq 2\sum_{n\leq x} d_{x+1}(an+b)\leq 2\sum_{n\leq x}\sum_{\substack{d\mid an+b\\ d\leq x+1}} 1\\ &\leq 2\sum_{d\leq x+1}\sum_{\substack{n\leq x\\ d\mid an+b}} 1.\end{aligned}\tag{18.47}$$

Note that there exists $n$ such that $d\mid an+b$ if and only if $d$ and $a$ are coprime (again because $a$ and $b$ are coprime) and in this case $n\equiv -a^{-1}b \pmod d$, where $a^{-1}$ stands for the multiplicative inverse of $a$ modulo $d$. Clearly, the number of such $n\leq x$ does not exceed $\lfloor x/d\rfloor+1<(x+1)/d+1\leq 2(x+1)/d$ because $d\leq x+1$. Hence, from (18.47), we obtain that

$$\begin{aligned}\sum_{n\leq x} d(an+b) &\leq 2\sum_{d\leq x+1}\sum_{\substack{n\leq x\\ d\mid an+b}} 1\\ &\leq 2\sum_{d\leq x+1}\frac{2(x+1)}{d}=4(x+1)\sum_{d\leq x+1}\frac{1}{d}\ll x\log x,\end{aligned}$$

which is what we wanted to prove. □

**Problem 7.24.** *Show that the sequence* $\{\sigma(n)/n\}_{n\geq 1}$ *is dense in* $[1,\infty)$.

*Solution.* Look at the sequence $a_p=\log(1+1/p)$ as $p$ runs over all primes $p$. It is decreasing to zero, but its sum is divergent since

$$\sum_{p\geq 2} a_p=\sum_{p\geq 2}\log\left(1+\frac{1}{p}\right)=\sum_{p\geq 2}\left(\frac{1}{p}+O\left(\frac{1}{p^2}\right)\right)=\sum_{p\geq 2}\frac{1}{p}+O(1),$$

which diverges. Now, for each $\alpha\geq 0$, each $\varepsilon>0$ and each $N$, there exist $N<p_1<\cdots<p_m$ such that $\sum_{i=1}^m \log(1+1/p_i)\in(\alpha-\varepsilon,\alpha+\varepsilon)$. Exponentiating we get that with $n=p_1\cdots p_m$,

$$\frac{\sigma(n)}{n}=\exp\left\{\sum_{i=1}^m\log\left(1+\frac{1}{p_i}\right)\right\}\in(e^{\alpha-\varepsilon},e^{\alpha+\varepsilon})$$

and since $\varepsilon>0$ is arbitrary, and $e^\alpha$ is arbitrary in $[1,\infty)$, we get the desired result. □

**Problem 7.26.** *Show that the sequence* $\{\omega(n+1)/\omega(n)\}_{n\geq 1}$ *is dense in* $[0,\infty)$. *(Hint: Let* $\alpha$ *be any positive real number. Choose a very large* $x$ *and write* $\pi(x) = a + b$, *where* $a/b$ *is near* $\alpha$. *Split the set of all primes* $p \leq x$ *into two disjoint sets* $\mathcal{P}$ *and* $\mathcal{Q}$, *one of cardinality* $a$ *and the other of cardinality* $b$. *Then use the Chinese Remainder Theorem to find* $n_0$ *such that* $n_0 \equiv -1 \pmod{n_{\mathcal{P}}}$ *and* $n_0 \equiv 0 \pmod{n_{\mathcal{Q}}}$, *where* $n_{\mathcal{P}} = \prod_{p\in\mathcal{P}} p$ *and* $n_{\mathcal{Q}} = \prod_{q\in\mathcal{Q}} q$. *Let* $n \in [e^{3x}, e^{4x}]$ *be such that* $n \equiv n_0 \pmod{n_{\mathcal{P}} \cdot n_{\mathcal{Q}}}$. *Deduce that* $n+1$ *is divisible by the prime factors in* $\mathcal{P}$ *and (perhaps) some other primes larger than* $x$ *and* $n$ *by the prime factors in* $\mathcal{Q}$ *and (perhaps) some other prime larger than* $x$. *Now show that for most such* $n$, *both* $n+1$ *and* $n$ *have only few prime factors larger than* $x$, *in other words, no more than* $o(x)$ *as* $x \to \infty$, *by using, for example, Problem* 7.21. *Conclude that* $\omega(n+1)/\omega(n) = (a/b)(1+o(1))$ *as* $x \to \infty$.*)*

*Solution.* We follow the hint. Let $\alpha \in (0,\infty)$. Let $x$ be large and set $a = \lfloor \alpha\pi(x)/(\alpha+1) \rfloor$ and $b = \lfloor \pi(x)/(\alpha+1) \rfloor$. Clearly,

$$\frac{a}{b} = \frac{\frac{\alpha\pi(x)}{\alpha+1} + O(1)}{\frac{\pi(x)}{\alpha+1} + O(1)} = \alpha + o(1)$$

as $x \to \infty$, implying that $a/b$ converges to $\alpha$ with such a choice. We now construct integers $n$ such that $\omega(n+1) = (1+o(1))a$ and $\omega(n) = (1+o(1))b$ as $n \to \infty$ in the following way. Let $\mathcal{P} \cup \mathcal{Q}$ be a partition of the set of all primes $p \leq x$ into two disjoint subsets with $a$ and $b$ elements respectively, and set $n_{\mathcal{P}} = \prod_{p\in\mathcal{P}} p$ and $n_{\mathcal{Q}} = \prod_{q\in\mathcal{Q}} q$. Let $n$ be such that $n+1 \equiv p \pmod{p^2}$ for all $p \in \mathcal{P}$ and $n \equiv q \pmod{q^2}$ for all $q \in \mathcal{Q}$. Let $M = \prod_{p\leq x} p^2 = e^{(2+o(1))x} < e^{4x}$. The Chinese Remainder Theorem guarantees the existence of an integer $n$ such that $n = Mm + n_0$, where $n_0$ is the first integer in this progression and $m \in [M, 2M]$. Then $n = n_{\mathcal{Q}}\ell_{\mathcal{Q}}$ and $n+1 = n_{\mathcal{P}}\ell_{\mathcal{P}}$, where $(n_{\mathcal{P}}, \ell_{\mathcal{P}}) = (n_{\mathcal{Q}}, \ell_{\mathcal{Q}}) = 1$. Observe that

$$\omega(n+1) = \omega(n_{\mathcal{P}}) + \omega(\ell_{\mathcal{P}}) = a + \omega(\ell_{\mathcal{P}})$$

and

$$\omega(n) = \omega(n_{\mathcal{Q}}) + \omega(\ell_{\mathcal{Q}}) = b + \omega(\ell_{\mathcal{Q}}).$$

Note also that since $n+1 = Mm + n_0 + 1$, we get that $\ell_{\mathcal{P}} = M_1 m + n_{0,1}$, where $M_1 = M/m_{\mathcal{P}}^2$ and $n_{0,1} = (n_0+1)/m_{\mathcal{P}}^2$ and $M_1$ and $n_{0,1}$ are coprime. Moreover, observe that $M_1 \leq M \leq m$. Thus, Problem 7.21 (or, more precisely, the argument from the proof of the preceding problem) shows that for all $m \in [M, 2M]$ except for at most $o(M)$ of them, we have that

$$\omega(\ell_{\mathcal{P}}) \leq (\log\log M)^2 = O((\log x)^2) = o(\pi(x)) = o(a)$$

as $x \to \infty$. Similarly, for all $m \in [M, 2M]$, except for at most $o(M)$ of them, we also have that $\omega(\ell_{\mathcal{Q}}) = o(b)$. Thus, for almost all choices of $m$ in

$[M, 2M]$, the number $n$ satisfies

$$\omega(n+1) = a + o(a) = a(1+o(1)) \qquad \text{and} \qquad \omega(n) = b + o(b) = b(1+o(1))$$

as $x \to \infty$, so that indeed $\omega(n+1)/\omega(n)$ can get arbitrarily close to the rational number $a/b$. □

**Problem 7.28.** *Prove that there exist infinitely many positive integers $k$ not of the form $n - \omega(n)$ for any $n \geq 1$. (Hint: Let $\ell$ be large, let $P_1 = p_1p_2$, $P_2 = p_3p_4p_5$, $P_3 = p_6p_7p_8p_9$, $\ldots$, $P_\ell = p_{t_\ell} \cdots p_{t_{\ell+1}-1}$, where $t_\ell = \ell(\ell-1)/2$ is the $\ell$-th triangular number. Set $x = P_1 \cdots P_\ell$ and let $k \in [x^2, x^3]$ be in the arithmetical progression $k \equiv -i \pmod{P_i}$ for $i = 1, \ldots, \ell$. Show, using the Prime Number Theorem, that $\ell^2 \log \ell \asymp \log x$, so that $\ell \gg (\log x/\log\log x)^{1/2}$. Afterwards, show that if $k = n - \omega(n)$ for some $n$, then $\omega(n) = t \in \mathcal{I} = [\ell+1, \lfloor \log x \rfloor]$. Thus, $n$ should have a lot of prime factors with respect to its size. Afterwards, use Problem 7.21 to show that for most such $k$ in $[x^2, x^3]$, there is no corresponding $t$ in $\mathcal{I}$ such that $n+t$ has more than $t$ prime factors.)*

*Solution.* Follow the hint and look at the numbers $k$ from this arithmetical progression. One can see that $k = n - \omega(n)$ is impossible for those $n$ satisfying $\omega(n) \leq \ell$. Indeed, if $\omega(n) = i$ for some $i \leq \ell$, we then get that $n = k + i$. But from the way we chose $k$, the integer $k + i$ is divisible by at least $i + 1$ primes, which is impossible. So if $n - \omega(n) = k$ for some $n$, then $\omega(n) > \ell$. Clearly,

$$x = P_1 \cdots P_\ell = \prod_{p \leq p_{t_{\ell+1}-1}} p = e^{(1+o(1))t_\ell \log(t_\ell)} \qquad (x \to \infty),$$

implying that $\log x = (1 + o(1))t_\ell \log(t_\ell)$. Inverting this as we did, for instance, at the maximal order of the $\omega$ function, we get that $t_\ell = (1 + o(1)) \log x/\log\log x$, and since $t_\ell \sim \ell^2/2$, we get that

$$\ell = (c_0 + o(1))(\log x/\log\log x)^{1/2}$$

for some constant $c_0$ (here, $c_0 = \sqrt{2}$) as $x \to \infty$. In particular, $\ell > y = (\log x)^{1/3}$. Recall that $n - \omega(n) = k$. Clearly, $n \leq 2k \leq 2x^3$, and therefore $\omega(n) \leq T$, where $T$ is of the order of $O(\log x/\log\log x)$. Fix $\omega(n) = i > \ell$. Then $k + i$ is in an arithmetical progression with the first term coprime to the ratio and $\omega(k + i)$ has a very large number of prime factors, that is, at least $y$. For such numbers, $d(k + i) > 2^y$, and now since $k \in [x^2, 2x^2]$ takes about $x$ values (recall that $k = xm + n_0$ where $m \in [x, 2x]$), the number of such $k \in [x^2, 2x^2]$ is $O(x \log x/2^y)$. We do this for each $i = \ell + 1, \ldots, T$, and get a total of at most $O(xT \log x/2^y) = O(x(\log x)^2/2^y) = o(x)$ numbers as

$x \to \infty$ since $y > (\log x)^{1/3}$, which implies that

$$\frac{(\log x)^2}{2^y} = \exp(2 \log\log x - (\log 2)(\log x)^{1/3}),$$

which tends to zero because it is easy to see that the argument inside the exponential tends to $-\infty$. □

## Solutions to problems from Chapter 8

**Problem 8.2.** *Show that if $n$ is composite, then $\phi(n) \le n - \sqrt{n}$.*

*Solution.* Let $q_1$ be the smallest prime factor of $n$. It is clear that $q_1 \le n^{1/2}$. Moreover, note that the $n/q_1$ numbers

$$q_1,\ 2q_1,\ \ldots,\ \frac{n}{q_1}q_1$$

are all $\le n$ and none is coprime to $n$. It follows that

$$\phi(n) \le n - n/q_1 \le n - \sqrt{n},$$

thus proving our claim. □

**Problem 8.4.** *Find all positive integers $n > 6$ such that if $1 = a_1 < a_2 < \cdots < a_{\phi(n)} = n - 1$ are all the $\phi(n)$ positive integers smaller than $n$ and coprime to $n$, then the numbers $a_i$, for $i = 1, \ldots, \phi(n)$, form an arithmetic progression.*

*Solution.* Assume that $n$ is such a number. Note that $a_1 = 1$ and that $a_2 = r$ is the smallest prime that does not divide $n$. So, if $a_1, \ldots, a_{\phi(n)}$ form an arithmetical progression, then this arithmetical progression is

$$1,\ 1 + (r-1),\ \ldots,\ 1 + (r-1)(\phi(n) - 1).$$

The last term $a_{\phi(n)}$ is obviously $n - 1$. Thus, $n = 2 + (r-1)(\phi(n) - 1)$.

If $r = 2$, we get $n = \phi(n) + 1$, or $\phi(n) = n - 1$. Hence, $n$ is prime, and in this case $a_i = i$ for all $i = 1, \ldots, \phi(n) = n - 1$.

If $r = 3$, then $n = 2 + 2\phi(n) - 2 = 2\phi(n)$. It then follows that $n$ is a power of 2. Indeed, if not, with $p$ being the largest odd prime factor of $n$, and letting $\alpha$ be its exponent in the factorization of $n$, we easily see that the exponent of $p$ in the factorization of $2\phi(n)$ is $\alpha - 1 \ne \alpha$, which is a contradiction. Thus, $n = 2^\alpha$ for some positive integer $\alpha$ and in this case $a_i = 1 + 2(i-1)$ for all $i = 1, \ldots, \phi(n)$.

Let us show that these are the only possibilities. Since $n > 6$, $n = 7,\ 8$ are already in the categories treated above, while for $n = 9$ we get that the sequence of $a_i$'s is $1,\ 2,\ 4,\ 5,\ 7,\ 8$, which is obviously not an arithmetic progression, we may assume that $n \geq 10$.

If $r \geq 11$, then both 3 and 7 divide $n$. Thus, $3 \mid \phi(7) \mid \phi(n)$. Reducing the relation

$$n = 2 + (r-1)(\phi(n) - 1)$$

modulo 3, we then get $0 \equiv 2-(r-1) \pmod 3$, and therefore $r \equiv 3 \pmod 3$, which is impossible. If $r = 7$, then $3 \mid r-1$ and $3 \mid n$, in which case $3 \mid (n-(r-1)(\phi(n)-1)) = 2$, which is again impossible. Finally, if $r = 5$, we then get that $a_1 = 1,\ a_2 = 5$ and $a_3 = 9$. But this is impossible since on the one hand $a_2 = 5$ shows that $3 \mid n$, while on the other hand $a_3 = 9$ shows that $3 \nmid n$.

In conclusion, the only $n$'s with the desired property are powers of 2 and primes. □

**Problem 8.6.** *Explain how to adapt the proof of Proposition* 8.9 *to get the following statement: For each integer $k > 1$ and permutation $a_1, a_2, \ldots, a_k$ of the integers $1, 2, \ldots, k$, there exist infinitely many positive integers $n$ such that*

$$\phi(n + a_1) < \phi(n + a_2) < \cdots < \phi(n + a_k).$$

*Solution.* As in the proof of Proposition 8.9, let $c_i = \phi(i)/i$ but this time choose the $d_i$'s in $(0, 1)$ such that, denoting by $\tau$ the function that permutes the $a_i$'s,

$$c_{\tau(1)}d_{\tau(1)} < c_{\tau(2)}d_{\tau(2)} < \cdots < c_{\tau(k)}d_{\tau(k)}.$$

Let $\varepsilon > 0$ be so small that

$$c_{\tau(i)}(d_{\tau(i)} + \varepsilon) < c_{\tau(i+1)}(d_{\tau(i+1)} - \varepsilon)$$

holds for all $i = 1, \ldots, k-1$. Now again choose $K = (k!)^2$, finite disjoint sets $\mathcal{P}_i$ of primes $p > k$ such that if we set $m_i = \prod_{p \in \mathcal{P}_i} p$, then $\phi(m_i)/m_i \in (d_i - \varepsilon/2, d_i + \varepsilon/2)$, a large number $x$ exceeding both $k$ and all primes $p \in \cup_{i=1}^{k} \mathcal{P}_i$ and $\mathcal{Q}$ for the set of all primes $p \in (k, x)$ which are not in any of the $\mathcal{P}_i$'s. Again select $n \in [e^{3x}, e^{4x}]$ such that $n \equiv 0 \pmod K,\ n \equiv q \pmod{q^2}$ for all $q \in \mathcal{Q}$ and $n \equiv -i + m_i \pmod{m_i^2}$. This exists for $x > x_0$ by the Chinese Remainder Theorem, observing that the resulting modulus is

$$\leq (k!)^2 \prod_{k < q \leq x} q^2 \prod_{i=1}^{k} m_i^2 \ll \left( \prod_{p \leq x} p \right)^2 = e^{(2+o(1))x}.$$

As in the proof of Proposition 8.9, we have that $n+i$ is composed of the following primes:

(i) $p \mid i$ (in fact, $i \mid (n+i)$ and $(n+i)/i$ is free of primes $p \le k$);

(ii) primes $p \in \mathcal{P}_i$ (and in fact $p \| (n+i)$ if $p \in \mathcal{P}_i$);

(iii) primes $p > x$; but observe that there are only

$$O\left(\frac{\log n}{\log\log n}\right) = O\left(\frac{\log(e^{4x})}{\log\log(e^{4x})}\right) = O\left(\frac{x}{\log x}\right)$$

of them.

Thus,

$$\begin{aligned}
\frac{\phi(n+i)}{n} &= \frac{n+i}{n}\cdot\frac{\phi(n+i)}{n+i} \\
&= \left(1+\frac{i}{n}\right)\prod_{p\mid i}\left(1-\frac{1}{p}\right)\prod_{p\in\mathcal{P}_i}\left(1-\frac{1}{p}\right)\prod_{\substack{p>x\\ p\mid n+i}}\left(1-\frac{1}{p}\right) \\
&\ll (1+o(1))\frac{\phi(i)}{i}\frac{\phi(m_i)}{m_i}\left(1+O\left(\frac{1}{x}\right)\right)^{O(x/\log x)} \\
&= (1+o(1))c_i\frac{\phi(m_i)}{m_i} \in (c_i(d_i-\varepsilon), c_i(d_i+\varepsilon))
\end{aligned}$$

provided that $x$ is sufficiently large. Ordering the $c_i d_i$'s appropriately, the desired inequality follows immediately. □

**Problem 8.8.** *Show that*

$$\sum_{n\le x}\frac{1}{\phi(n)} = (C+o(1))\log x \qquad (x\to\infty),$$

*where* $C = \prod_p\left(1+\frac{1}{p(p-1)}\right) = \frac{\zeta(2)\zeta(3)}{\zeta(6)}$.

*Solution.* We first compute the generating series of $n/\phi(n)$. We have

$$\begin{aligned}
\sum_{n=1}^{\infty}\frac{n/\phi(n)}{n^s} &= \prod_p\left(1+\frac{(1-\frac{1}{p})^{-1}}{p^s}+\frac{(1-\frac{1}{p})^{-1}}{p^{2s}}+\cdots\right) \\
&= \zeta(s)\prod_p\left(1-\frac{1}{p^s}\right)\prod_p\left(1+\frac{(1-\frac{1}{p})^{-1}}{p^s}+\frac{(1-\frac{1}{p})^{-1}}{p^{2s}}+\cdots\right) \\
&= \zeta(s)\prod_p\left(1+\frac{1}{p^s(p-1)}\right),
\end{aligned}$$

which by Wintner's theorem yields

$$\sum_{n\le x}\frac{n}{\phi(n)} = (C+o(1))x \qquad (x\to\infty), \tag{18.48}$$

where

$$C = \prod_p \left(1+\frac{1}{p(p-1)}\right).$$

Then, using partial summation, we get

$$\sum_{n\le x}\frac{1}{\phi(n)} = C + o(1) + \int_1^x (C+o(1))\frac{dt}{t} = (C+o(1))\log x,$$

as required. One can easily check that $C = \dfrac{\zeta(2)\zeta(3)}{\zeta(6)}$. □

**Problem 8.10.** *Use Wintner's theorem (Theorem* 6.13*) to show that there exist two positive constants $C_1$ and $C_2$ such that, as $x\to\infty$,*

$$\sum_{n\le x}\left(\frac{\phi(n)}{n}\right)^2 = (C_1+o(1))x$$

*and*

$$\sum_{n\le x}\left(\frac{\sigma(n)}{n}\right)^2 = (C_2+o(1))x.$$

*Solution.* For $\mathrm{Re}(s)>1$, we have

$$\begin{aligned}
\sum_{n=1}^{\infty}\frac{(\phi(n)/n)^2}{n^s} &= \prod_p\left(1+\frac{(1-\frac{1}{p})^2}{p^s}+\frac{(1-\frac{1}{p})^2}{p^{2s}}+\cdots\right)\\
&= \zeta(s)\prod_p\left(1-\frac{1}{p^s}\right)\prod_p\left(1+\frac{(1-\frac{1}{p})^2}{p^s}+\frac{(1-\frac{1}{p})^2}{p^{2s}}+\cdots\right)\\
&= \zeta(s)\prod_p\left(1+\frac{(1-\frac{1}{p})^2-1}{p^s}\right)\\
&= \zeta(s)\prod_p\left(1+\frac{\frac{1}{p^2}-\frac{2}{p}}{p^s}\right).
\end{aligned}$$

Since this last infinite product converges absolutely at $s=1$, we may apply Wintner's theorem to conclude that

$$\sum_{n\le x}\left(\frac{\phi(n)}{n}\right)^2 = (C_1+o(1))x \qquad (x\to\infty),$$

where

$$C_1 = \prod_p \left(1 + \frac{\frac{1}{p^2} - \frac{2}{p}}{p}\right) = \prod_p \left(1 - \frac{2}{p^2} + \frac{1}{p^3}\right).$$

Similarly, we easily establish that, for $\mathrm{Re}(s) > 1$,

$$\begin{aligned}
&\sum_{n=1}^{\infty} \frac{(\sigma(n)/n)^2}{n^s} \\
&\quad = \prod_p \left(1 + \frac{(1+\frac{1}{p})^2}{p^s} + \frac{(1+\frac{1}{p}+\frac{1}{p^2})^2}{p^{2s}} + \cdots\right) \\
&\quad = \zeta(s) \prod_p \left(1 - \frac{1}{p^s}\right) \prod_p \left(1 + \frac{(1+\frac{1}{p})^2}{p^s} + \frac{(1+\frac{1}{p}+\frac{1}{p^2})^2}{p^{2s}} + \cdots\right) \\
&\quad = \zeta(s) \prod_p \left(1 + \frac{(1+\frac{1}{p})^2 - 1}{p^s} + \frac{(1+\frac{1}{p}+\frac{1}{p^2})^2 - (1+\frac{1}{p})^2}{p^{2s}} + \cdots\right).
\end{aligned}$$

And again, as above, one can easily check that this last infinite product converges absolutely at $s = 1$, allowing us to use Wintner's theorem and conclude that

$$\sum_{n \le x} \left(\frac{\sigma(n)}{n}\right)^2 = (C_2 + o(1))x \qquad (x \to \infty),$$

where $C_2 = \displaystyle\prod_p \left(1 + \frac{2}{p^2} + \frac{1}{p^3} + \sum_{k=2}^{\infty} \frac{\left(\sum_{i=0}^{k} \frac{1}{p^i}\right)^2 - \left(\sum_{i=0}^{k-1} \frac{1}{p^i}\right)^2}{p^k}\right)$. □

## Solutions to problems from Chapter 9

**Problem 9.2.** *Are the functions $f(n)$ and $g(n)$ defined in* (9.2) *and* (9.3) *multiplicative?*

*Solution.* The function $g(n)$ is multiplicative, while the function $f(n)$ is not. □

**Problem 9.4.** *Evaluate the following two sums:*

$$\sum_{n \le x} \frac{1}{p(n)^2}, \qquad \sum_{n \le x} f(n),$$

*where $f(n)$ is defined by*

$$f(n) = \begin{cases} 1 & \text{if } p(n) \le 3, \\ \sqrt{\log p(n)} & \text{if } p(n) \ge 5. \end{cases}$$

*Solution.* Letting $\alpha_p = \lfloor \log x / \log p \rfloor$, we have

$$\begin{aligned}
\sum_{n\le x} \frac{1}{p(n)^2} &= \sum_{p\le x} \frac{1}{p^2} \sum_{\substack{n\le x \\ p(n)=p}} 1 \\
&= \sum_{p\le x} \frac{1}{p^2} \left( \sum_{\substack{pm\le x \\ p(m)>p}} 1 + \sum_{\substack{p^2 m\le x \\ p(m)>p}} 1 + \cdots + \sum_{\substack{p^{\alpha_p} m\le x \\ p(m)>p}} 1 \right) \\
&= \sum_{p\le x} \frac{1}{p^2} \left( \Phi\left(\frac{x}{p}, p\right) + \Phi\left(\frac{x}{p^2}, p\right) + \cdots + \Phi\left(\frac{x}{p^{\alpha_p}}, p\right) \right) \\
&= \sum_{p\le \log x} \frac{1}{p^2} \left( \Phi\left(\frac{x}{p}, p\right) + \Phi\left(\frac{x}{p^2}, p\right) + \cdots + \Phi\left(\frac{x}{p^{\alpha_p}}, p\right) \right) \\
&\quad + \sum_{\log x < p\le x} \frac{1}{p^2} \left( \Phi\left(\frac{x}{p}, p\right) + \Phi\left(\frac{x}{p^2}, p\right) + \cdots + \Phi\left(\frac{x}{p^{\alpha_p}}, p\right) \right) \\
&= \Sigma_1 + \Sigma_2,
\end{aligned}$$

say. Using estimate (9.6) (with $\varepsilon = \frac{1}{2}$), it follows that

$$\begin{aligned}
\Sigma_1 &= \sum_{p\le \log x} \frac{1}{p^2} \left\{ \sum_{j=1}^{\alpha_p} \frac{x}{p^j} \prod_{q<p} \left(1 - \frac{1}{p}\right) + O\left( \sum_{j=1}^{\alpha_p} \left(\frac{x}{p^j}\right)^{1/2} \right) \right\} \\
&= x \sum_{p\le \log x} \sum_{j=1}^{\alpha_p} \frac{1}{p^{j+2}} \prod_{q<p} \left(1 - \frac{1}{q}\right) + O(x^{1/2}) \\
&= x \sum_{p\le \log x} \frac{1}{p(p-1)} \prod_{q<p} \left(1 - \frac{1}{q}\right) + O(x^{1/2}),
\end{aligned}$$

since $\sum_{j>\alpha_p} 1/p^{j+2} \ll \frac{1}{x}$ for all $p \ge 2$. Moreover, since

$$\sum_{p>\log x} \frac{1}{p^3} \ll \int_{\log x}^{\infty} \frac{1}{t^3}\, dt \ll \frac{1}{\log^2 x},$$

we obtain, using the trivial estimate $\Phi(x/p,p) \le x/p$, that

$$\begin{aligned}\Sigma_2 &\ll x \sum_{\log x < p \le x} \left(\frac{\log x}{\log p}\right) \frac{1}{p^3} \ll x \log x \sum_{p > \log x} \frac{1}{p^3} \\ &\ll x \log x \int_{\log x}^{\infty} \frac{dt}{t^3} \ll \frac{x}{\log x},\end{aligned}$$

so that

$$\sum_{n \le x} \frac{1}{p(n)^2} = Cx + O\left(\frac{x}{\log x}\right),$$

where $C = \displaystyle\sum_p \frac{1}{p(p-1)} \prod_{q<p} \left(1 - \frac{1}{q}\right)$.

For the second sum, we first write

$$\sum_{n \le x} f(n) = \sum_{\substack{n \le x \\ p(n) \le 3}} 1 + \sum_{\substack{n \le x \\ p(n) \ge 5}} \sqrt{\log p(n)} = S_1 + S_2,$$

say. It is clear that

$$S_1 = \left[\frac{x}{2}\right] + \left[\frac{x}{6}\right] = \frac{2x}{3} + O(1). \tag{18.49}$$

On the other hand,

$$\begin{aligned}S_2 &= \sum_{5 \le p \le x} \sqrt{\log p} \sum_{\substack{n \le x \\ p(n) = p}} 1 \\ &= \sum_{5 \le p \le x} \sqrt{\log p} \left\{ \sum_{\substack{pm \le x \\ p(m) > p}} 1 + \sum_{\substack{p^2 m \le x \\ p(m) > p}} 1 + \cdots + \sum_{\substack{p^{\alpha_p} m \le x \\ p(m) > p}} 1 \right\} \\ &= \sum_{5 \le p \le x} \sqrt{\log p} \left\{ \Phi\left(\frac{x}{p}, p\right) + \Phi\left(\frac{x}{p^2}, p\right) + \cdots + \Phi\left(\frac{x}{p^{\alpha_p}}, p\right) \right\} \\ &= \sum_{5 \le p \le \log x} \cdots + \sum_{\log x < p \le x} \cdots = S_3 + S_4,\end{aligned}$$

say. Now,

(18.50)

$$\begin{aligned} S_3 = \sum_{5\le p\le \log x} \sqrt{\log p}\, \Bigg\{ & \frac{x}{p}\prod_{q<p}\left(1-\frac{1}{q}\right) + O\left(\left(\frac{x}{p}\right)^{1/2}\right) \\ & + \frac{x}{p^2}\prod_{q<p}\left(1-\frac{1}{q}\right) + O\left(\left(\frac{x}{p^2}\right)^{1/2}\right) \\ & + \cdots + \frac{x}{p^{\alpha_p}}\prod_{q<p}\left(1-\frac{1}{q}\right) + O\left(\left(\frac{x}{p^{\alpha_p}}\right)^{1/2}\right)\Bigg\} \\ = x \sum_{5\le p\le \log x} \sqrt{\log p} \sum_{j=1}^{\alpha_p} \frac{1}{p^j} \prod_{q<p}\left(1-\frac{1}{q}\right) & + \left(x^{1/2} \sum_{5\le p\le \log x} \frac{\sqrt{\log p}}{p^{1/2}}\right) \\ = x \sum_{5\le p\le \log x} \frac{\sqrt{\log p}}{p-1} \prod_{q<p}\left(1-\frac{1}{q}\right) & + O(x^{1/2}\sqrt{\log x}), \end{aligned}$$

where we used the fact that

$$\sum_{j=1}^{\alpha_p} \frac{1}{p^j} = \sum_{j\ge 1} \frac{1}{p^j} + O\left(\frac{1}{x}\right) = \frac{1}{p-1} + O\left(\frac{1}{x}\right).$$

On the one hand,

(18.51)

$$\sum_{5\le p\le \log x} \frac{\sqrt{\log p}}{p-1} \prod_{q<p}\left(1-\frac{1}{q}\right) = \sum_{p\ge 5} \frac{\sqrt{\log p}}{p-1} \prod_{q<p}\left(1-\frac{1}{q}\right) + O\left(\frac{1}{\sqrt{\log\log x}}\right),$$

where we used the fact that

$$\begin{aligned} \sum_{p>\log x} \frac{\sqrt{\log p}}{p-1} \prod_{q<p}\left(1-\frac{1}{q}\right) &\ll \int_{\log x}^{\infty} \frac{\sqrt{\log t}}{(t-1)\log^2 t} dt \ll \int_{\log x}^{\infty} \frac{dt}{t(\log t)^{3/2}} \\ &= -\frac{2}{\sqrt{\log t}}\Big|_{t=\log x}^{t=\infty} \ll \frac{1}{\sqrt{\log\log x}}. \end{aligned}$$

On the other hand, using the uniform bound (9.10), we have

$$\begin{aligned} \sum_{\log x<p\le x} \sqrt{\log p}\, \Phi\left(\frac{x}{p}, p\right) &\ll x \sum_{p>\log x} \frac{\sqrt{\log p}}{p\log p} \ll x\int_{\log x}^{\infty} \frac{dt}{t\log^{3/2} t} \\ &= x\int_{\log\log x}^{\infty} \frac{dv}{v^{3/2}} \ll \frac{x}{\sqrt{\log\log x}}, \end{aligned}$$

implying that

$$S_4 = \sum_{\log x<p\le x} \sqrt{\log p} \sum_{j=1}^{\alpha_p} \Phi\left(\frac{x}{p^j}, p\right) \ll \frac{x}{\sqrt{\log\log x}}. \tag{18.52}$$

Combining (18.49), (18.50), (18.51), and (18.52), we then obtain

$$\sum_{n\le x} f(n) = C_0 x + O\left(\frac{x}{\sqrt{\log\log x}}\right),$$

where $C_0 = \dfrac{2}{3} + \displaystyle\sum_{p\ge 5} \frac{\sqrt{\log p}}{p-1} \prod_{q<p}\left(1-\frac{1}{q}\right)$. □

**Problem 9.6.** *Prove that*

$$\sum_{2\le n\le x} \frac{1}{p(n)} = Cx + O\left(\frac{x}{(\log\log x)^2}\right), \quad \textit{where } C = \sum_p \frac{1}{p(p-1)} \prod_{q<p}\left(1-\frac{1}{q}\right).$$

*Solution.* Proceeding as in Problem 9.4, we easily establish, using the notation $\alpha_p = \lfloor \log x/\log p \rfloor$,

$$\sum_{2\le n\le x} \frac{1}{p(n)} = \sum_{p\le x} \frac{1}{p} \sum_{j=1}^{\alpha_p} \Phi\left(\frac{x}{p^j}, p\right) = \sum_{p\le \log x} \cdots + \sum_{\log x < p\le x} \cdots = S_1 + S_2,$$

say. On the one hand,

$$\begin{aligned} S_2 &\ll \sum_{\log x < p\le x} \frac{1}{p}\left(\frac{\log x}{\log p}\right)\frac{x}{p} < x\log x \sum_{p>\log x} \frac{1}{p^2\log p} \\ &\ll x\log x \int_{\log x}^{\infty} \frac{dt}{t^2\log^2 t} \ll \frac{x\log x}{(\log\log x)^2}\int_{\log x}^{\infty}\frac{dt}{t^2} \ll \frac{x}{(\log\log x)^2}. \end{aligned}$$

Now, using (9.6) with $\varepsilon = \frac{1}{2}$, we obtain, proceeding essentially as in Problem 9.4,

$$S_1 = x\sum_{j=1}^{\infty} \frac{1}{p^{j+1}} \prod_{q<p}\left(1-\frac{1}{q}\right) + O\left(\frac{x}{\log x}\right).$$

Since $\sum_{j=1}^{\infty} 1/p^{j+1} = 1/p(p-1)$, the result follows. □

**Problem 9.8.** *Prove that*

$$1 + \sum_{\substack{p^k\le x \\ k\ge 1}} \Phi(x/p^k, p) = \lfloor x \rfloor.$$

*Solution.* We have

$$\begin{aligned}\lfloor x\rfloor &= \sum_{n\le x} 1 = 1+\sum_{p\le x}\sum_{\substack{n\le x\\ p(n)=p}} 1\\ &= 1+\sum_{p\le x}\sum_{\substack{pm\le x\\ p(m)>p}} 1+\sum_{p^2\le x}\sum_{\substack{p^2m\le x\\ p(m)>p}} 1+\sum_{p^3\le x}\sum_{\substack{p^3m\le x\\ p(m)>p}} 1+\cdots\\ &= 1+\sum_{p\le x}\Phi\left(\frac{x}{p},p\right)+\sum_{p^2\le x}\Phi\left(\frac{x}{p^2},p\right)+\sum_{p^3\le x}\Phi\left(\frac{x}{p^3},p\right)+\cdots,\end{aligned}$$

where each of the above sums is finite, since all terms are 0 as soon as $p^k > x$. Hence, the result. □

**Problem 9.10.** *Prove the Buchstab identity*

$$\Psi(x,y)=\Psi(x,z)-\sum_{y<p\le z}\Psi\left(\frac{x}{p},p\right)\qquad (x\ge 1,\ z\ge y>0).$$

*(Hint: Use the fact that*

$$\Psi(x,z)=\sum_{p\le z}\sum_{\substack{pm\le x\\ P(m)\le p}} 1=\sum_{p\le z}\Psi\left(\frac{x}{p},p\right)$$

*for all $2\le z\le x$.)*

*Solution.* The result follows easily using the hint. □

**Problem 9.12.** *Is the series* $\displaystyle\sum_{m=2}^{\infty}\frac{1}{m\log^2 P(m)}$ *convergent?*

*Solution.* Yes. Indeed,

$$\begin{aligned}\sum_{m=2}^{\infty}\frac{1}{m\log^2 P(m)} &= \sum_p\sum_{\substack{m\ge 2\\ P(m)=p}}\frac{1}{m\log^2 P(m)}=\sum_p\frac{1}{p\log^2 p}\sum_{\substack{n\ge 1\\ P(n)\le p}}\frac{1}{n}\\ &= \sum_p\frac{1}{p\log^2 p}\prod_{q\le p}\left(1+\frac{1}{q}+\frac{1}{q^2}+\cdots\right)\\ &= \sum_p\frac{1}{p\log^2 p}\prod_{q\le p}\left(1-\frac{1}{q}\right)^{-1}\\ &\ll \sum_p\frac{1}{p\log^2 p}\log p\ll\int_2^{\infty}\frac{dt}{t\log^2 t}=O(1),\end{aligned}$$

where we used Mertens' theorem. □

**Problem 9.14.** *Use Theorem* 9.5 *to prove that if* $y < A$ *for a fixed* $A$*, then*

$$\Psi(x,y) \ll x^{1-\eta},$$

*for some real number* $\eta > 0$*.*

*Solution.* Indeed, in light of Theorem 9.5, we obtain

$$\Psi(x,y) \ll xe^{-\frac{1}{2}\frac{\log x}{\log y}} < xe^{-\frac{1}{2}\frac{\log x}{\log A}} = x^{1-\frac{1}{2\log A}} = x^{1-\eta},$$

if we choose $\eta = 1/(2\log A)$. □

**Problem 9.16.** *Let* $\mathcal{P}^{(2)}$ *be the set of base* 2 *pseudoprimes. Using the construction of pseudoprimes from Problem* 2.9*, show that the series*

$$\sum_{n\in\mathcal{P}^{(2)}} \frac{1}{\log n}$$

*is divergent.*

*Solution.* Let $k$ be a positive integer. We know, from Problem 2.9, that if $s > 1$ and

$$k+1 < n_1 < n_2 < \cdots < n_s < 2^k,$$

then $F_{n_1}\cdots F_{n_k}$ is a pseudoprime to base 2. (Here, $F_r$ is the $r$-th Fermat number.) Let $k$ be large and $m$ be any fixed number in the interval $(2k, 2^k)$. We look at the pseudoprimes $n = F_{n_1}\cdots F_{n_s}$, where $n_1 < \cdots < n_s = m$ and $s > 1$. The interval $(k+1, m)$ contains $m-(k+1)-1 = m-k-2$ integers. The number of nonempty subsets $\{n_1, \ldots, n_{s-1}\}$ of $(k+1,m)\cap\mathbb{Z}$ is $2^{m-k-2} \gg 2^{m-k}$. For each such subset, we have that

$$n = F_{n_1}\cdots F_{n_s} \le 2^{2^{n_s+1}} - 1 = 2^{2^{m+1}} - 1,$$

implying that $\log n \ll 2^m$. Thus, for a fixed $m$, the subsum

$$\sum_{\substack{n=F_{n_1}\cdots F_{n_s}\\ n_s=m}} \frac{1}{\log n} \gg \frac{2^{m-k-2}}{2^m} \gg \frac{1}{2^k}.$$

Since $m$ can be any number in $(2k, 2^k)$, it follows that $m$ can take $2^k - 2k - 1 \gg 2^k$ values. Summing up as well over all the possible values of $m$, we get that

$$\sum_{m\in(2k,2^k)} \sum_{\substack{n=F_{n_1}\cdots F_{n_s}\\ n_s=m}} \frac{1}{\log n} \gg 1.$$

This is true for all $k > k_0$ sufficiently large. Now let $k$ go to infinity through the sequence $k = k_t$, where $k_t = 2^{k_{t-1}}$ for each $t \geq 1$ and note that the set of numbers $n$ constructed for some $k_i$ is disjoint from the set of numbers $n$ constructed for $k_j$ with $j \neq i$ (that is, because at step $i$, $n$ is a product of Fermat numbers, all whose indices are in $(2k_i, k_{i+1})$). This shows that

$$\sum_{\substack{n \in \mathcal{P}^{(2)} \\ n \leq k_t}} \frac{1}{\log n} = \sum_{\ell=0}^{t-1} \sum_{m \in (2k_\ell, k_{\ell+1})} \sum_{\substack{n = F_{n_1} \cdots F_{n_s} \\ n_s = m}} \frac{1}{\log n} \gg \sum_{\ell=0}^{t-1} 1 = t,$$

and since $t$ is arbitrary, the given sum diverges. □

**Problem 9.18.** *Prove that there are infinitely many positive integers $n$ such that $2^{\sigma(n)} \equiv 1 \pmod{n}$. (Hint: Start with $n = 3$ and build up larger $n$'s by multiplying it with appropriate primes.)*

*Solution.* For each $i = 1, 2, \ldots$, let $q_i$ be some prime factor of $F_{i-1}$, where $F_i$ is the $i$-th Fermat number. For example, $q_1 = 3$, $q_2 = 5$, $q_3 = 17$, and so on. Note that the $q_i$'s are distinct since $F_i$ and $F_j$ are coprime if $i \neq j$. Let

$$n = \prod_{i=1}^{k} q_i.$$

Then $\sigma(n) = (q_1 + 1) \cdots (q_k + 1)$ is a multiple of $2^k$. Thus, $2^{2^k} - 1$ divides $2^{\sigma(n)} - 1$, and since $F_j \mid 2^{2^k} - 1$ for all $j = 0, \ldots, k-1$, we get that $q_i \mid F_{i-1} \mid 2^{2^k} - 1 \mid 2^{\sigma(n)} - 1$ for all $i = 1, \ldots, k$. Hence, $n \mid 2^{\sigma(n)} - 1$. □

**Problem 9.20.** *Let $F_n$ be the $n$-th Fermat number. Let $\mathcal{P}$ be the set of all primes that divide $F_n$ for some positive integer $n$. Show that the series*

$$\sum_{p \in \mathcal{P}} \frac{1}{p}$$

*is convergent. (Hint: Show that $\omega(F_n) \ll 2^n$ and that each prime factor of $F_n$ is congruent to 1 modulo $2^{n+1}$. Use this information to get a reasonably small bound on $\sum_{p \mid F_n} 1/p$.)*

*Solution.* Let $p$ be a prime dividing $F_n$. Then $2^{2^n} \equiv -1 \pmod{p}$ so that $2^{2^{n+1}} \equiv 1 \pmod{p}$. So, $p \mid 2^{2^{n+1}} - 1$. But also $p \mid 2^{p-1} - 1$ by Fermat's little theorem. Since $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$, we get that $p \mid 2^{\gcd(2^{n+1}, p-1)} - 1$. Note that $\gcd(2^{n+1}, p-1) = 2^k$ for some $k \leq n+1$. If $k \leq n$, then $2^k \mid 2^n$ so that $p \mid 2^{2^k} - 1 \mid 2^{2^n} - 1 = F_n - 2$, which is false

because $p \mid F_n$. So, $k = n+1$, which implies that $2^{n+1} \mid p-1$. Clearly, $\omega(F_n) \ll \log F_n \ll 2^n$. Thus,

$$\sum_{p|F_n} \frac{1}{p} \le \sum_{i=1}^{\omega(F_n)} \frac{1}{2^{n+1}i+1} \le \frac{1}{2^{n+1}} \sum_{i=1}^{\omega(F_n)} \frac{1}{i} \ll \frac{\log(\omega(F_n))}{2^{n+1}} \ll \frac{n}{2^n}.$$

Summing up over all $n$, we get

$$\sum_{p\in\mathcal{P}} \frac{1}{p} \le \frac{1}{3} + \sum_{n\ge 1} \sum_{p \mid F_n} \frac{1}{p} \ll \sum_{n\ge 1} \frac{n}{2^n} = O(1),$$

which proves that the series converges. □

**Problem 9.22.** *Use de Bruijn's estimates* (9.42) *and* (9.43) *to show that if* $A = \{n : P(n) < \log n\}$, *then* $\#(A \cap [1,x]) = x^{o(1)}$ *as* $x \to \infty$.

*Solution.* Clearly,

$$\sum_{\substack{n\le x \\ P(n)\le \log n}} 1 < \sum_{\substack{n\le x \\ P(n)\le \log x}} 1 = \Psi(x, \log x). \tag{18.53}$$

Using (9.42) with $y = \log x$, we get

$$Z = \frac{\log x}{\log\log x}\log(1+1) + \frac{\log x}{\log\log x}\log(1+1) = 2\log 2 \frac{\log x}{\log\log x},$$

which, when substituted in (9.43), yields

$$\log \Psi(x, \log x) = (2\log 2)\frac{\log x}{\log\log x}\left(1 + O\left(\frac{1}{\log\log x}\right)\right),$$

so that

$$\Psi(x, \log x) = \exp\left\{(2\log 2)\frac{\log x}{\log\log x}\left(1 + O\left(\frac{1}{\log\log x}\right)\right)\right\} = x^{o(1)}$$

as $x \to \infty$, an estimate that concludes the solution, in light of (18.53). □

**Problem 9.24.** *Use Theorem* 9.5 *to prove that*

$$\sum_{\substack{n>x \\ P(n)\le y}} \frac{1}{n} \ll e^{-\frac{1}{2}u} \log y.$$

*Solution.* Writing this sum as a Stieltjes integral and integrating by parts, we obtain, using Theorem 9.3,

$$\begin{aligned}\sum_{\substack{n>x\\P(n)\le y}}\frac{1}{n}=\int_x^\infty\frac{1}{t}\,d\Psi(t,y) &= \frac{\Psi(t,y)}{t}\Big|_{t=x}^{t=\infty}+\int_x^\infty\frac{\Psi(t,y)}{t^2}\,dt\\ &\ll e^{-\frac{1}{2}\frac{\log t}{\log y}}\Big|_{t=x}^{t=\infty}+\int_x^\infty\frac{1}{t}e^{-\frac{1}{2}\frac{\log t}{\log y}}\,dt.\end{aligned}$$

To estimate this last integral, we set $w=\frac{\log t}{\log y}$, thereby allowing us to write

$$\begin{aligned}\sum_{\substack{n>x\\P(n)\le y}}\frac{1}{n} &\ll e^{-\frac{1}{2}u}+\log y\int_u^\infty e^{-\frac{1}{2}w}\,dw=e^{-\frac{1}{2}u}+\log y\,\frac{e^{-\frac{1}{2}w}}{-\frac{1}{2}}\Big|_{w=u}^{w=\infty}\\ &\ll e^{-\frac{1}{2}u}+2\log y\,e^{-\frac{1}{2}u}\ll e^{-\frac{1}{2}u}\log y,\end{aligned}$$

as requested. □

**Problem 9.26.** *Combine the results of Problems* 9.24 *and* 9.25 *to prove that*

$$\int_0^u\rho(v)\,dv=e^\gamma+O\left(\frac{u}{\log y}+e^{-\frac{1}{2}u}\right).$$

*(Hint: Use Mertens' theorem.)*

*Solution.* Using the estimates from the last two problems, we obtain

$$\begin{aligned}\sum_{\substack{n\ge1\\P(n)\le y}}\frac{1}{n}&=\sum_{\substack{n\le x\\P(n)\le y}}\frac{1}{n}+\sum_{\substack{n>x\\P(n)\le y}}\frac{1}{n}\\ &=\log y\int_0^u\rho(v)\,dv+O(u)+O\left(e^{-\frac{1}{2}u}\log y\right).\end{aligned}\tag{18.54}$$

Using Mertens' theorem, we have

$$\begin{aligned}\sum_{\substack{n\ge1\\P(n)\le y}}\frac{1}{n}&=\prod_{p\le y}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)\\ &=\prod_{p\le y}\left(1-\frac{1}{p}\right)^{-1}=e^\gamma\log y\left(1+O\left(\frac{1}{\log y}\right)\right).\end{aligned}\tag{18.55}$$

Combining (18.54) and (18.55), and dividing by $\log y$, we obtain

$$\int_0^u\rho(v)\,dv+O\left(\frac{u}{\log y}\right)+O\left(e^{-\frac{1}{2}u}\right)=e^\gamma\left(1+O\left(\frac{1}{\log y}\right)\right),$$

thus establishing the result. □

**Problem 9.28.** *Let $\xi = \xi(u)$ be the function defined in Section 8. By first establishing that*

$$1 \ll \xi(u) \ll \log u,$$

*prove that for $u \geq 3$,*

$$\xi(u) = \log(u \log u) + O\left(\frac{\log\log u}{\log u}\right).$$

*Solution.* First, using the basic relation $e^{\xi} = 1 + u\xi$, we have

$$1 \ll \xi(u) = \log(e^{\xi(u)}) = \log(1 + u\xi(u)) \ll \log u.$$

By iteration, we get

$$\begin{aligned}
\xi(u) &= \log u + \log\left(\xi + \frac{1}{u}\right) = \log u + \log\left(\log u + \log\left(\xi + \frac{1}{u}\right) + \frac{1}{u}\right) \\
&= \log u + \log\left\{\log u\left(1 + \frac{\log\left(\xi + \frac{1}{u}\right)}{\log u} + \frac{1}{u\log u}\right)\right\} \\
&= \log(u\log u) + O\left(\frac{\log\left(\xi + \frac{1}{u}\right)}{\log u}\right) \\
&= \log(u\log u) + O\left(\frac{\log\xi}{\log u}\right) = \log(u\log u) + O\left(\frac{\log\log u}{\log u}\right),
\end{aligned}$$

thus proving our claim. □

**Problem 9.30.** *Prove that*

$$\xi'(u) = \frac{\xi(u)}{1 + u(\xi(u) - 1)}.$$

*Solution.* Differentiating with respect to $u$ both sides of the relation $e^{\xi(u)} = 1 + u\xi(u)$, we obtain

$$e^{\xi(u)}\xi'(u) = u\xi'(u) + \xi(u).$$

It follows that

$$e^{\xi(u)}\xi'(u) - u\xi'(u) = \xi(u),$$

so that

$$\xi'(u) = \frac{\xi(u)}{e^{\xi(u)} - u} = \frac{\xi(u)}{1 + u\xi(u) - u} = \frac{\xi(u)}{1 + u(\xi(u) - 1)},$$

as claimed. □

**Problem 9.32.** *Prove the identity*

$$u\xi(u) - I(\xi(u)) = \int_1^u \xi(t)\,dt.$$

*Solution.* Let $f(u) = u\xi(u) - I(\xi(u))$ and $g(u) = \int_1^u \xi(t)\,dt$. We have that

$$\begin{aligned} f'(u) &= u\xi'(u) + \xi(u) - \frac{d}{du}\int_0^{\xi(u)} \frac{e^t - 1}{t}\,dt \\ &= u\xi'(u) + \xi(u) - \frac{e^{\xi(u)} - 1}{\xi(u)} \cdot \xi'(u) \\ &= u\xi'(u) + \xi(u) - u\xi'(u) = \xi(u) \end{aligned}$$

and that $g'(u) = \xi(u)$. It follows that $f'(u) = g'(u)$ and therefore that $f(u) = g(u) + c$ for a certain constant $c$. Now, $f(1) = \xi(1) - I(\xi(1)) = 0 - I(0) = 0$ and $g(1) = \int_1^1 \xi(t)\,dt = 0$. This establishes that $c = 0$ and thus that $f(u) = g(u)$. This proves the result. □

**Problem 9.34.** *Let $A = \{a_k\}_{k\geq 1}$ be the sequence of positive integers defined by $a_k = 4k^4$, $k = 1, 2, 3, \ldots$*

(i) *Show that $A$ contains a subsequence $B$ such that*

$$\max\left(P(n-1), P(n), P(n+1)\right) < \sqrt{n} \qquad \text{for all } n \in B.$$

(ii) *Show that there exists a positive constant $C$ such that*

$$\#\{n \leq x : n \in B\} > Cx^{1/4}.$$

*(Hint: Observe that the identities*

$$4k^4 - 1 = (2k^2+1)(2k^2-1) \qquad \text{and} \qquad 4k^4+1 = (2k^2+2k+1)(2k^2-2k+1)$$

*are true for all positive integers $k$. Observe also that*

$$\begin{aligned} 2k^2 + 1 &\equiv 0 \pmod 3 \quad \text{if} \quad k \equiv 1 \pmod 3, \\ 2k^2 - 1 &\equiv 0 \pmod 7 \quad \text{if} \quad k \equiv 2 \pmod 7, \\ 2k^2 + 2k + 1 &\equiv 0 \pmod 5 \quad \text{if} \quad k \equiv 1 \pmod 5, \\ 2k^2 - 2k + 1 &\equiv 0 \pmod{13} \quad \text{if} \quad k \equiv 3 \pmod{13}. \end{aligned}$$

*Use these relations to obtain upper bounds for $P(4k^4 - 1)$, $P(4k^4)$ and $P(4k^4 + 1)$, respectively.)*

*Solution.* Clearly, for each $k \geq 2$, setting $n = 4k^4$, we have that $P(n) = P(k) \leq k < n^{1/4}$. Hence we need to concentrate only on $P(n-1) = P(4k^4 - 1)$ and $P(n+1) = P(4k^4 + 1)$.

In light of the identities and the congruences displayed in the hint, choosing $k$ so that $k \equiv 1 \pmod 3$ and $k \equiv 2 \pmod 7$, we get that

$$\begin{aligned} P(4k^4-1) &\le \max\big(P(2k^2+1), P(2k^2-1)\big) \\ &\le \max\left(\frac{2k^2+1}{3}, \frac{2k^2-1}{7}\right) \\ &\le \frac{2k^2+1}{3}. \end{aligned}$$

While choosing $k$ so that it also satisfies $k \equiv 1 \pmod 5$ and $k \equiv 3 \pmod{13}$, we get that

$$\begin{aligned} P(4k^4+1) &\le \max\big(P(2k^2+2k+1), P(2k^2-2k+1)\big) \\ &\le \max\left(\frac{2k^2+2k+1}{5}, \frac{2k^2-2k+1}{13}\right) \\ &\le \frac{2k^2+2k+1}{5}. \end{aligned}$$

In any event, we get that $\max(P(4k^4-1), P(4k^4), P(4k^4+1)) < k^2 \le \sqrt{n/4}$, thus establishing (i). To prove (ii), we need to observe only that, using the Chinese Remainder Theorem, one easily finds that the minimum solution $k = k_0$ of the four congruences $k \equiv 1 \pmod 3$, $k \equiv 2 \pmod 7$, $k \equiv 1 \pmod 5$, and $k \equiv 3 \pmod{13}$ is $k_0 = 16$, so that all the solutions $k$ to these congruences are given by $k = 16 + 1365j$, $j = 0, 1, 2, 3, \ldots$, implying that the number of integers $n = 4k^4 = 4(16+1365j)^4 \le x$ belonging to $B$ is $\gg x^{1/4}$, as claimed, thus proving (ii). □

**Problem 9.36.** *Let $p_i$ stand for the $i$-th prime. For each integer $k \ge 2$, consider the polynomials $P_k(x) = x^{p_2 p_3 \cdots p_k} - 1$ and $Q_k(x) = x^{p_2 p_3 \cdots p_k} + 1$ to establish that, given any small number $\varepsilon > 0$, there exists a positive integer $n$ such that*

$$\max(P(n-1), P(n), P(n+1)) < n^{\varepsilon}.$$

*(Hint: Show that $P_k(x)$ (as well as $Q_k(x)$) can be written as a product of polynomials each of degree at most $(p_2-1)(p_3-1)\cdots(p_k-1)$, from which it will follow that the largest prime factor of $2^{3\cdot 5\cdots p_k} - 1$ (and similarly of $2^{3\cdot 5\cdots p_k} + 1$) is $\ll 2^{(3-1)(5-1)\cdots(p_k-1)}$, implying that choosing $k$ large enough so that*

$$\frac{(p_2-1)(p_3-1)\cdots(p_k-1)}{p_2 p_3 \cdots p_k} < \varepsilon,$$

*that is,*

$$\prod_{2 \le i \le k} \left(1 - \frac{1}{p_i}\right) < \varepsilon,$$

*the proof will be complete.)*

*Solution.* The hint says it all. □

## Solutions to problems from Chapter 10

**Problem 10.2.** *Use Theorem* 10.1*, Problem* 10.1*, and Stirling's formula, to show that*

$$\max_k\{\Pi_k(x)\} \ll \frac{x}{\sqrt{\log\log x}}.$$

*(Hint: If $k < 10\log\log x$, use Theorem* 10.1 *and Stirling's formula to conclude that*

$$\Pi_k(x) \ll \frac{x}{(k-1)^{1/2}\log\log x}\left(\frac{e\log\log x + c_1}{k-1}\right)^{k-1}.$$

*Then show that for any fixed $A > 1$, the function $t \mapsto (A/t)^t$ is increasing for $t \le A/e$ and decreasing for $t \ge A/e$.)*

*Solution.* If $k > 10\log\log x$, then $\omega(n) - \log\log x > 9\log\log x$. Thus, by the Turán–Kubilius, we get

$$81(\log\log x)^2\Pi_k(x) \le \sum_{n\le x}(\omega(n) - \log\log x)^2 = O(x\log\log x),$$

showing that $\Pi_k(x) \ll x/(\log\log x)$. Hence, if $k > 10\log\log x$, we get a better (smaller) upper bound. For $k \le 10\log\log x$, we use Stirling's formula and the Hardy-Ramanujan inequality to get that

$$\begin{aligned}\Pi_k(x) &\ll \frac{x}{\sqrt{k}\log x}\left(\frac{e\log\log x + ec_0}{k-1}\right)^{k-1}\\ &\ll \frac{x}{(\log\log x)^{1/2}\log x}\left(\frac{e\log\log x + ec_0}{k-1}\right)^{k-1}.\end{aligned} \tag{18.56}$$

We now follow the hint. Fix $A > 1$ and look at $f(t) = (A/t)^t$. Taking logarithms and then taking derivatives, we get

$$\frac{d}{dt}\left(t\log(A/t)\right) = \log A - \log t - 1,$$

and this is $\ge 0$ if $t \le A/e$ and $< 0$ if $t > A/e$. Hence, the maximum of $f(t)$ is obtained when $t = A/e$ in which case $f(A/e) = e^{A/e}$. With $A = e\log\log x + ec_0$, we get that

$$\left(\frac{e\log\log x + ec_0}{k-1}\right)^{k-1} \le e^{\log\log x + c_0} \ll \log x. \tag{18.57}$$

Inserting (18.57) into (18.56), we get

$$\Pi_k(x) \ll \frac{x}{(\log\log x)^{1/2}},$$

which is what we wanted to prove. □

**Problem 10.4.** *Let $\eta > 1$ be fixed. Show, using the Hardy-Ramanujan inequality, that*

$$\#\{n \le x : \omega(n) \ge \lfloor \eta \log\log x \rfloor\} \le \frac{x}{(\log x)^{1-\eta\log(e/\eta)+o(1)}}$$

*as $x \to \infty$. (Hint: Reduce the problem to that of studying $\Pi_K(x)$, where $K = \lfloor \eta \log\log x \rfloor$. One might want to consider using Problem 10.1 for excessively large values of $k$.)*

*Solution.* First we extend the Hardy-Ramanujan inequality to the range $k \le 10\eta \log\log x$. A close investigation of the arguments used in its proof show that it is still true in this somewhat larger range. (As we mentioned in Remark 10.2, Hardy and Ramanujan proved their inequality without any restriction on $k$.) Now set $K = \lfloor \eta \log\log x \rfloor$ and split the set $\{n \le x : \omega(n) > \eta \log\log x\}$ into two subsets, namely when $\omega(n) \le 10\eta \log\log x$ and when $\omega(n) > 10\eta \log\log x$, respectively. Let $N_1$ and $N_2$ be the cardinalities of the first and second subset, respectively. On the first range, we have, by the Hardy-Ramanujan inequality

$$N_1 \le \sum_{k>K} \frac{x}{\log x} a_k,$$

where

$$a_k = \frac{1}{(k-1)!}(\log\log x + c_0)^{k-1}.$$

Now notice that

$$\frac{a_{k+1}}{a_k} = \frac{\log\log x + c_0}{k} \le \frac{\log\log x + c_0}{K} = \frac{1}{\eta} + o(1)$$

as $x \to \infty$, and that $\eta > 1$, implying that for some $c_1 \in (1/\eta, 1)$ we have $a_{k+1}/a_k < c_1$ for all $x > x_0$. Thus,
(18.58)

$$N_1 \le \frac{x}{\log x} a_K \sum_{\ell \ge 0} c_1^\ell \ll \frac{x}{\log x} a_K \ll \frac{x}{K^{1/2}\log x} \left(\frac{e\log\log x + c_0}{K-1}\right)^{K-1}.$$

One then easily shows that

$$\begin{aligned}\left(\frac{e\log\log x + c_0}{K-1}\right)^{K-1} &\ll \left(\frac{e}{\eta}\right)^{\eta\log\log x}\left(1 + O\left(\frac{1}{\log\log x}\right)\right)^{O(\log\log x)} \\ &\ll (\log x)^{\eta\log(e/\eta)},\end{aligned}$$

which together with estimate (18.58) gives

$$N_1 \le \frac{x}{(\log x)^{1-\eta\log(e/\eta)+o(1)}} \qquad \text{as } x \to \infty.$$

For $N_2$, we use Problem 10.1 and a similar argument and get that if $L = \lfloor 10\eta\log(e/(10\eta))\rfloor$, then

$$\begin{aligned} N_2 &\le x\sum_{k>L} a_k \ll xa_L \\ &\ll x\left(\frac{e\log\log x + ec_0}{L}\right)^{10\eta\log\log x} \\ &\ll \frac{x}{(\log x)^{-10\eta\log(e/(10\eta))}} \end{aligned}$$

(that is, a similar type of bound as for $N_1$ with $\eta$ replaced by $10\eta$ but with an exponent of $\log x$ smaller by 1). However, note that

$$-10\eta\log(e/(10\eta)) > 1 - \eta\log(e/\eta),$$

because this is equivalent to

$$10\eta\log 10 + 10\eta\log\eta - 10\eta > 1 - \eta + \eta\log\eta,$$

or

$$\eta(10\log 10 - 9) + 9\eta\log\eta > 1,$$

which is certainly true because $\eta > 1$ and $10\log 10 - 9 > 1$. □

## Solutions to problems from Chapter 11

**Problem 11.2.** *According to Catalan's conjecture, the only consecutive powers are $2^3$ and $3^2$. Prove that the abc conjecture implies that there can be only a finite number of consecutive powers.*

*Solution.* Let $n^\alpha$ and $m^\beta$, with $\alpha \ge 2$ and $\beta \ge 2$, be two consecutive powers. It is clear that we can exclude the possibility that $\alpha = \beta = 2$ (since it is impossible to have two consecutive squares). If $\alpha > \beta \ge 2$, let us assume that $n^\alpha + 1 = m^\beta$ (the case $n^\alpha - 1 = m^\beta$ being similar) and choose $\varepsilon = 1/10$. Then, according to the *abc* conjecture, there exists a constant $M = M(1/10)$ such that

$$m^\beta = n^\alpha + 1 < M\cdot\gamma(n^\alpha m^\beta)^{1+1/10} < M\cdot(nm)^{11/10} < Mm^{(1+\beta/\alpha)\cdot(11/10)},$$

which is impossible if $m$ is sufficiently large. □

**Problem 11.4.** *Let $a \geq 1$ be a fixed integer. Assuming that the abc conjecture is true, show that the diophantine equation*

$$ax^3 + y^3 = z^4 \tag{18.59}$$

*can have only a finite number of solutions.*

*Solution.* Indeed, if $x, y, z$ are three coprime positive integers satisfying (18.59), then for each $\varepsilon > 0$, there exists a constant $M(\varepsilon) > 0$ such that

$$z^4 < M(\varepsilon) \cdot (axyz)^{1+\varepsilon}.$$

Choose $\varepsilon = 1/1000$. By hypothesis, $x < z^{4/3}$ and $y < z^{4/3}$, so that

$$\begin{aligned} z^4 &< M(\varepsilon) \cdot (a \cdot z^{11/3})^{1+\varepsilon} \\ z &< M(1/1000)^{1/4} \cdot a^{\frac{1+\varepsilon}{4}} \cdot z^{\frac{11}{12}(1+1/1000)} \\ z &< C \cdot z^{\frac{11}{12}\cdot\frac{1001}{1000}} < C \cdot z^{\frac{12}{13}}, \end{aligned}$$

for a certain positive constant $C$. But this is impossible if $z$ is sufficiently large.

On the other hand, choosing $x = 1$, equation (18.59) can be written as

$$a + y^3 = z^4,$$

an equation which always has a solution $y, z$ for certain positive integers $a$: simply take $y = z = b$ and then choose $a = b^4 - b^3$. □

**Problem 11.6.** *Does the abc conjecture necessarily imply that the diophantine equation*

$$2x^2 + y^3 = z^4$$

*cannot have any solutions in positive integers $x, y, z$ ?*

*Solution.* The answer is NO. In fact, it has many. For instance, here are two of them: $x = 34$, $y = 89$, $z = 29$ and $x = 831$, $y = 79$, $z = 37$. □

**Problem 11.8.** *Show heuristically that the number of Wieferich primes $\leq x$ is of order* $\log\log x$.

*Solution.* By Fermat's little theorem, $(2^{p-1} - 1)/p$ is an integer for each prime number $p \geq 3$. From a heuristic point of view, the probability that the integer $(2^{p-1} - 1)/p$ is divisible by $p$ is equal to $1/p$. Therefore, the expected number of times that $(2^{p-1} - 1)/p^2$ is an integer is

$$\sum_{3 \leq p \leq x} \frac{1}{p} \sim \log\log x \qquad (x \to \infty),$$

which proves the claim. □

**Problem 11.10.** *Let $a > 1$ and $b > 1$ be positive integers. Show, using the abc conjecture, that if $\gamma(a^n - 1) = \gamma(b^n - 1)$ for all integers $n \geq 1$, then $a = b$.*

*Solution.* Assume that $b > a > 1$ are fixed integers. Clearly, applying the *abc* conjecture to the equation $b^n - 1 = m$, we obtain that for any fixed $\varepsilon > 0$,

$$b^n \ll \gamma(bm)^{1+\varepsilon} \ll \gamma(b^n - 1)^{1+\varepsilon} = \gamma(a^n - 1)^{1+\varepsilon} \ll (a^n)^{1+\varepsilon}.$$

Since $b > a$, we get that $\log b > \log a$. Choose $\varepsilon$ such that $c_0 = \log b - (1 + \varepsilon) \log a > 0$. Then, with this $\varepsilon$, we have

$$e^{n \log b} \ll e^{(1+\varepsilon) n \log a},$$

and therefore $e^{c_0 n} \ll 1$, so that $n \ll 1$, because $c_0 > 0$. □

**Problem 11.12.** *Let $\{F_n\}_{n \geq 1}$ be the Fibonacci sequence $F_1 = 1,\ F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 1$. Show that the abc conjecture implies that $F_n$ is powerful only for finitely many $n$. (Hint: First prove that if $(L_n)_{n \geq 1}$ denotes the sequence $L_1 = 1,\ L_2 = 3$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 1$, then $L_n^2 - 5F_n^2 = \pm 4$.)*

*Solution.* Let $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. First, observe that, for each $n \in \mathbb{N}$, we have $F_n = (\alpha^n - \beta^n)/(\alpha - \beta)$. Indeed, this formula is definitely true at $n = 1,\ 2$. Furthermore, given any constants $c$ and $d$, the sequence of general term $u_n = c\alpha^n + d\beta^n$ satisfies the equation $u_{n+2} = u_{n+1} + u_n$ for all $n \geq 0$. Indeed, multiplying

$$\alpha^2 = \alpha + 1$$

by $c\alpha^n$ and $\beta^2 = \beta + 1$ by $d\beta^n$, and then summing, we get

$$c\alpha^{n+2} + d\beta^{n+2} = (c\alpha^{n+1} + d\beta^{n+1}) + (c\alpha^n + d\beta^n);$$

that is, $u_{n+2} = u_{n+1} + u_n$. Thus, with $c = 1/(\alpha - \beta)$ and $d = -1/(\alpha - \beta)$, the sequence of general term $(\alpha^n - \beta^n)/(\alpha - \beta)$ satisfies the same recurrence relation as the Fibonacci sequence and coincides with it at $n = 1$ and $n = 2$. Thus, by induction, it coincides for all $n \geq 1$. Now put $L_n = \alpha^n + \beta^n$. It satisfies the same relation as the Fibonacci sequence, but it starts with $L_1 = 1,\ L_2 = 3$. Now observe that

$$L_n^2 - 5F_n^2 = (\alpha^n + \beta^n)^2 - 5\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)^2 = 4(\alpha\beta)^n = \pm 4,$$

because $(\alpha-\beta)^2=5$. Now, if we assume that $F_n$ is powerful and apply the *abc* conjecture, with some small $\varepsilon>0$, to the equation $L_n^2-5F_n^2=\pm 4$ which we just proved, we then get that

$$L_n^2 \ll \gamma(L_nF_n)^{1+\varepsilon} \ll \left(L_nF_n^{1/2}\right)^{1+\varepsilon} \ll L_n^{(3/2)(1+\varepsilon)}.$$

Choosing $\varepsilon=1/4$, we get that $L_n^2 \ll L_n^{15/8}$, and therefore $L_n^{1/8}\ll 1$. Since $L_n \gg \alpha^n$ (note that $|\beta|<1$), we get that $n$ is bounded, thus proving our claim. □

## Solutions to problems from Chapter 12

**Problem 12.2.** *Let $A=\{n=|u^w\pm v!|$ for some integers $u,\ v,\ w>1\}$. Let $x$ be a large positive real number.*

(i) *Let $y=\log x/(\log\log x)^2$. Show that if $x$ is large, then the set of $n\in A\cap[1,x]$ such $v\le y$ is of cardinality $x^{1/2+o(1)}$ as $x\to\infty$.*

(ii) *From here on, assume that $v>y$. By observing that if $m>2p$, then $p^2\mid m!$, prove that if $n=|u^w\pm v!|$ with $w>1$ and $p<y/2$, then either $p$ is coprime to $n$ or $p^2\mid n$.*

(iii) *Let $z=\log\log x$. Show that the number of positive integers $n\le x$ divisible by $p^2$ for some $p>z$ is $O(x/\log\log x)$.*

(iv) *Show that if $n\in A\cap[1,x]$ is not as in (i) or (iii) above, then $n$ is coprime with all primes in $[z,y/2]$. Then use the Eratosthenes sieve to show that the number of such $n\le x$ is $O(x\log\log\log x/\log\log x)=o(x)$ as $x\to\infty$.*

(v) *Deduce that $A$ is of asymptotic density zero.*

*Solution.* Clearly, $v!<v^v$. Hence, if $v<y$, then

$$v!<y^y=\exp(y\log y)<\exp\left(\frac{\log x}{(\log\log x)^2}\log\log x\right)=x^{1/\log\log x}<x^{1/2}$$

for large $x$. Thus, if $u^w\pm v!=n$, $0\le n\le x$ and $v<y$, then $u^w<x+x^{1/2}<2x$. Thus, either $u^w=1$ or $u\ge 2$, in which case $2^w\le 2x$, implying that $w\ll\log x$. Moreover, since $w\ge 2$, we get that $u^2\le u^w\le 2x$, so that $u\ll x^{1/2}$. Thus, the number of possibilities for $u,w,v$ (with the $\pm$ sign) is

$$\ll x^{1/2}(\log x)y=x^{1/2+o(1)}$$

as $x\to\infty$, which proves (i). From here on let $v>y$. If $p<y/2$ is a prime, then $p<2p$ are integers less than $v$, implying that $v!$ is divisible by $(p)\cdots(2p)$ and therefore by $p^2$. Now if $n=u^w\pm v!$ and such a prime $p$

divides $n$, then since it divides $v!$, we get that $p \mid u$. Since $w \geq 2$, we get that $p^2 \mid u^w$ and that $p^2 \mid v!$, implying that $p^2 \mid n$, thus establishing (ii). Part (iii) is similar to part (i) from the preceding problem. Indeed, for each fixed prime $p$, the number of positive integers $n \leq x$ which are multiples of $p^2$ is $\lfloor x/p^2 \rfloor \leq x/p^2$. Thus, the total number of positive integers $n \leq x$ divisible by $p^2$ for some prime $p > z$ is

$$\leq \sum_{p>z} \frac{x}{p^2} \ll x \int_z^\infty \frac{dt}{t^2} = \frac{x}{z}.$$

Letting $z = \log\log x$ completes the proof of (iii).

Finally, for (iv), let $P = \prod_{z \leq p \leq y/2} p$. By the Eratosthenes sieve, we have that the number $S$ of positive integers $n \leq x$ coprime to $P$ satisfies

$$\begin{aligned} S &\leq \sum_{d \mid P} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor = \sum_{d \mid P} \mu(d) \left( \frac{x}{d} + O(1) \right) \\ &= x \sum_{d \mid P} \frac{\mu(d)}{d} + O\left( \sum_{d \mid P} 1 \right) = x \prod_{z \leq p \leq y/2} \left( 1 - \frac{1}{p} \right) + O(2^y) \\ &\ll \frac{x \log z}{\log(y/2)} + x^{o(1)} \ll \frac{x \log\log\log x}{\log\log x}, \end{aligned}$$

where in the above estimate we used the fact that

$$\begin{aligned} \prod_{z \leq p \leq y/2} \left( 1 - \frac{1}{p} \right) &\ll \frac{\prod_{p \leq y/2} \left( 1 - \frac{1}{p} \right)}{\prod_{p < z} \left( 1 - \frac{1}{p} \right)} \\ &= (1 + o(1)) \frac{1/\log(y/2)}{1/\log z} = (1 + o(1)) \frac{\log z}{\log(y/2)} \end{aligned}$$

as $x \to \infty$, by Problem 4.4. □

**Problem 12.4.** *Let $f(X) \in \mathbb{Z}[X]$ be a nonconstant polynomial of degree $D$ without double roots. Let*

$$\rho(d) = \#\{0 \leq n \leq d-1 \ : \ f(n) \equiv 0 \pmod{d}\}.$$

(i) *Show that $\rho$ is a multiplicative function.*

*Now, assume that*

$$f(X) = \prod_{i=1}^{D} (a_i X + b_i),$$

*where $a_i > 0$ and $b_i$ are integers for $i = 1, \ldots, D$.*

(ii) *Show that the condition that $f(X)$ does not have double roots is equivalent to*

$$\Delta(f) = \prod_{i=1}^{D} \prod_{1 \le i < j \le D} (a_i b_j - a_j b_i) \neq 0.$$

(iii) *Show that $\rho(p) = D$ is equivalent to $gcd(p, \Delta(f)) = 1$.*

*Solution.* (i) Let $u$ and $v$ be coprime. If $x \pmod{uv}$ is a solution to $f(x) \equiv 0 \pmod{uv}$, it follows that both $u$ and $v$ divide $f(n)$ for every integer $n \equiv x \pmod{uv}$. Since $f(n) \pmod{u}$ depends only on $n \pmod{u}$, it follows that the class of $x \pmod{u}$ and the class $x \pmod{v}$ are solutions to $f(x) \equiv 0 \pmod{u}$ and $f(x) \equiv 0 \pmod{v}$. Thus, setting

$$\mathcal{F}_d = \{n \pmod{d} \ : \ f(n) \equiv 0 \pmod{d}\},$$

we get that the map

$$F_{f,u,v} : \mathcal{F}_{uv} \longrightarrow \mathcal{F}_u \times \mathcal{F}_v, \qquad n \pmod{uv} \longmapsto (n \pmod{u}, n \pmod{v})$$

is well-defined (that is, not only does it not depend on the representative chosen from the congruence class but it also takes a solution modulo $uv$ to a pair of solutions modulo $u$ and modulo $v$, respectively), and it is clearly injective. The fact that it is surjective follows from the Chinese Remainder Theorem. More precisely, if $a \pmod{u}$ and $b \pmod{v}$ are such that $f(a) \equiv 0 \pmod{u}$ and $f(b) \equiv 0 \pmod{v}$, then there exists $n \pmod{uv}$ such that $n \equiv a \pmod{u}$ and $n \equiv b \pmod{v}$, and certainly $f(n) \equiv f(a) \equiv 0 \pmod{u}$ and $f(n) \equiv f(b) \equiv 0 \pmod{v}$. Hence, both $u$ and $v$ divide $f(n)$ for such values of $n$, and since $u$ and $v$ are coprime, we conclude that $uv \mid f(n)$. This shows that $F_{f,u,v}$ is surjective. Hence, $F_{f,u,v}$ is a bijection, implying that its domain and its range have the same cardinalities. Thus, $\rho(uv) = \#\mathcal{F}_{uv} = \#(\mathcal{F}_u \times \mathcal{F}_v) = \rho(u)\rho(v)$. We also remark that $\rho(1) = 1$ is obvious since there is only one class modulo 1 and 1 certainly divides $f(n)$ for all $n \in \mathbb{N}$.

For (ii), note that since $a_i \neq 0$, we get that $x = -b_i/a_i$ are the roots of $f(X)$. A root is double if $-b_i/a_i = -b_j/a_j$ for some $i \neq j$. This is equivalent to $a_i b_j - a_j b_i = 0$. Thus, if $f(X)$ has a double root, then $\Delta(f) = 0$.

For (iii), assume that $\Delta(f) \neq 0$. We will show that $f(X) \pmod{p}$ is such that $\rho(p) = D$ if and only if $p \mid \Delta(f)$. Indeed, let $x \pmod{p}$ be a double root of $f(X)$ modulo $p$, where $f$ is given by

$$f(X) = \prod_{i=1}^{D} (a_i X + b_i). \tag{18.60}$$

Then there must exist $i < j$ such that $p \mid a_i x + b_i$ and $p \mid a_j x + b_j$. If $p \mid a_i$ or $p \mid a_j$, then we already have that $p \mid \Delta(f)$, which is what we

wanted. If $p \nmid a_i a_j$, then $a_i x \equiv -b_i \pmod p$ and $a_j x \equiv -b_j \pmod p$. Multiplying the first congruence by $a_j$ and the second by $a_i$ and subtracting the resulting congruences, we get $a_i a_j x \equiv -b_i a_j \equiv -b_j a_i \pmod p$, implying that $p \mid a_i b_j - a_j b_i$; thus, $p \mid \Delta(f)$ again. From the above arguments, we get that $f(x) \pmod p$ has no double root if $p > P(\Delta(f))$. Since for each $i = 1, \dots, D$, $x \equiv -b_i a_i^{-1} \pmod p$ is a solution of $f(x) \equiv 0 \pmod p$ (note that we can invert $a_i$ modulo $p$ since $p > P(\Delta(f))$ and $a_i$ divides $\Delta(f)$), we conclude that $\rho(p) = D$. □

**Problem 12.6.** *Let $L_i(X) = a_i X + b_i$, $i = 1, \dots, k$, be distinct linear forms with integer coefficients. Assume that $\gcd(a_i, b_i) = 1$ for $i = 1, \dots, k$, and that $a_i > 0$ for all $i = 1, \dots, k$. Moreover, for each prime $p$, let*

$$\nu(p) = \#\{0 \le n \le p-1 : a_i n + b_i \equiv 0 \pmod p \text{ for some } i = 0, 1, \dots, k\}.$$

(i) *Show that if we choose $f(X) = \prod_{i=1}^k L_i(X)$, then $\nu(p)$ coincides with $\rho(p)$ defined in Problem* 12.4.

(ii) *Use Problem* 12.5 *to show that*

$$\#\{n \le x : a_i n + b_i \text{ is prime for all } i = 1, \dots, k\} \le c(k) \left(\frac{\Delta(f)}{\phi(\Delta(f))}\right)^k \frac{x(\log\log x)^k}{(\log x)^k}$$

*for $x > x(k)$ (some initial value depending only on $k$), where $c(k)$ is a constant that depends only on $k$. (Hint: Use Problem* 12.5 *with $y = \exp(\log x/(10k \log\log x))$. As for the main term, note that, by Problem* 12.4, *it is*

$$\le \prod_{\substack{p \le y \\ p > k,\ p \nmid \Delta(f)}} \left(1 - \frac{k}{p}\right).$$

*Prove first that if we put $a_k(p) = (1 - k/p)/(1 - 1/p)^k$, then $\prod_{p>k} a_k(p)$ converges to a positive number, so that the above product is bounded by*

$$c_1(k) \prod_{\substack{p \le y \\ p > k,\ p \nmid \Delta(f)}} \left(1 - \frac{1}{p}\right)^k,$$

*where $c_1(k)$ depends only on $k$. Finally observe that this last product runs over all the primes $p$ with $k < p \le y$, a contribution depending only on $k$, and the possible primes dividing $\Delta(f)$. What does the product of these eliminated factors have to do with $\Delta(f)/\phi(\Delta(f))$? Use also known results about the full product $\prod_{p \le y}(1 - 1/p)^k$.)*

*Solution.* We use the previous two problems. In particular, we use the notations from these problems; hence, we work with $D$ instead of $k$ and with the polynomial $f(X)$ shown at (18.60). Note that $\rho(p) = D$ if $p \nmid \Delta(f)$. Thus, by Problem 12.5, we have, for $y = \exp(\log x/10D \log\log x)$ and $x > x_D$,

$$\begin{aligned} \mathcal{S}(\mathcal{A}, \mathcal{P}, y) &\ll x \prod_{\substack{D<p\le y \\ p\nmid\Delta(f)}} \left(1 - \frac{D}{p}\right) \\ &\le x \prod_{D<p\le y} \left(1 - \frac{D}{p}\right) \prod_{p \mid \Delta(f)} \left(1 - \frac{\rho(p)}{p}\right)^{-1}. \end{aligned} \tag{18.61}$$

The first of the above products is

$$\begin{aligned} \prod_{D<p\le y} \left(1 - \frac{D}{p}\right) &\le \exp\left(\sum_{D<p\le y} \log\left(1 - \frac{D}{p}\right)\right) \\ &= \exp\left(-D \sum_{D<p\le y} \frac{1}{p} + O\left(\sum_{p>D} \sum_{\alpha\ge 2} \left(\frac{D}{p}\right)^{\alpha}\right)\right). \end{aligned} \tag{18.62}$$

For the first part above, we have

$$\begin{aligned} -D \sum_{D<p\le y} \frac{1}{p} &= -D \sum_{p\le y} \frac{1}{p} + D \sum_{p\le D} \frac{1}{p} \\ &= -D(\log\log y + O(1)) + O(D \log\log D), \end{aligned}$$

while for the second part,

$$\sum_{\alpha\ge 2} \left(\frac{D}{p}\right)^{\alpha} = \left(\frac{D}{p}\right)^2 \left(\sum_{\beta\ge 0} \left(\frac{D}{p}\right)^{\beta}\right) = \left(\frac{D}{p}\right)^2 \frac{1}{1 - D/p} = \frac{D^2}{p(p-D)},$$

which implies that

$$\sum_{p>D} \sum_{\alpha\ge 2} \left(\frac{D}{p}\right)^{\alpha} \le D^2 \sum_{p>D} \frac{1}{p(p-D)} \ll D^2 \sum_{p>D} \frac{1}{p^2} \ll D. \tag{18.63}$$

Combining (18.62), (18.63), and (18.63), we get that

$$\begin{aligned} \prod_{D<p\le y} \left(1 - \frac{D}{p}\right) &\le \exp(-D \log\log y + O(D \log\log D)) \le \frac{c_1(D)}{(\log y)^D} \\ &= c_1(D)(10D)^D \frac{(\log\log x)^D}{(\log x)^D}, \end{aligned} \tag{18.64}$$

where $c_1(D)$ is some constant depending on $D$ only.

We now look at the product over the primes dividing $\Delta(f)$. We start by observing that

$$\begin{aligned}\left(1-\frac{\rho(p)}{p}\right)^{-1}\left(1-\frac{1}{p}\right)^{\rho(p)} &= \exp\left(-\log\left(1-\frac{\rho(p)}{p}\right)+\rho(p)\log\left(1-\frac{1}{p}\right)\right)\\ &= \exp\left(\frac{\rho(p)}{p}+O\left(\left(\frac{\rho(p)}{p}\right)^2\right)\right.\\ &\qquad \left.+\quad \rho(p)\left(-\frac{1}{p}+O\left(\frac{1}{p^2}\right)\right)\right)\\ &= \exp\left(O\left(\left(\frac{\rho(p)}{p}\right)^2\right)\right)=\exp\left(O\left(\frac{D^2}{p^2}\right)\right)\end{aligned}$$

for $p > D$, because $\rho(p) \le D$. Hence, it follows easily that

$$\prod_{p>D}\left(1-\frac{\rho(p)}{p}\right)^{-1}\left(1-\frac{1}{p}\right)^{\rho(p)} < \exp\left(O\left(D^2\sum_{p>D}\frac{1}{p^2}\right)\right) < c_2(D),$$

where $c_2(D)$ is some constant depending on $D$. Thus, again using the fact that $\rho(p) \le D$, we have

$$\begin{aligned}\prod_{\substack{p>D\\ p\,|\,\Delta(f)}}\left(1-\frac{\rho(p)}{p}\right)^{-1} &\le c_2(D)\prod_{\substack{p>D\\ p|\Delta(f)}}\left(1-\frac{1}{p}\right)^{-\rho(p)}\\ &\le c_2(D)\prod_{\substack{p>D\\ p\,|\,\Delta(f)}}\left(\frac{p}{p-1}\right)^{\rho(p)}\\ &\le c_2(D)\left(\frac{\Delta(f)}{\phi(\Delta(f))}\right)^D.\end{aligned}\tag{18.65}$$

Using estimates (18.64) and (18.65) in (18.61) yields

$$\mathcal{S}(\mathcal{A},\mathcal{P},y) \le c_3(D)x\left(\frac{\Delta(f)}{\phi(\Delta(f))}\right)^D\frac{(\log\log x)^D}{(\log x)^D},$$

which is uniform in the coefficients $a_i$ and $b_i$ for $i = 1, \dots, k$. □

**Problem 12.8.** *The following problem appeared as a conjecture in a recent paper by Elliott and Richner* [**44**]*: Show that the set* $\mathcal{A} = \{n : n = p^2 - q^2$ *with primes* $p,\ q\}$ *is of asymptotic density zero, by proceeding in the following way:*

(i) *Show that if* $n \in \mathcal{A}$*, then* $n = uv$*, where* $v < u$ *are positive integers, and that there exists a prime* $q$ *such that* $p = q + v$ *is prime and*

$u = p + q = 2q + v$. *Deduce that* $n \le x$ *is determined by a positive integer* $v \le x^{1/2}$ *and a prime* $q < x/v$ *such that* $p = q + v$ *is also a prime.*

(ii) *Use Problem* 12.6*, or adapt the proof of Proposition* 12.4*, to deduce that the number of primes* $q \le x/v$ *such that* $q + v$ *is also a prime is*

$$\ll \left(\frac{v}{\phi(v)}\right) \frac{x}{v} \frac{(\log\log(x/v))^2}{(\log(x/v))^2}.$$

(iii) *Show that the above upper bound is*

$$\ll \frac{x(\log\log x)^3}{v(\log x)^2}.$$

*(Hint: Use the maximal order of the function* $m/\phi(m)$ *in the interval* $[1, x]$ *and remember that* $v \le x^{1/2}$*.)*

(iv) *Now sum up over* $v \le x^{1/2}$ *and conclude.*

*Solution.* Let $x$ be large and look at $n \in \mathcal{A} \cap [1, x]$. Then $n = p^2 - q^2 = (p - q)(p + q)$ for some primes $p > q$. Writing $p - q = v,\ p + q = u$, we get that $n = uv,\ v < u$, so that $v < n^{1/2} < x^{1/2}$ and $q$ and $p = q + v$ are both primes, and $u = 2q + v$. This means that $n$ is determined by the pair $(v, q)$. This completes (i). Now fix $v$. Let $\mathcal{A}_v$ be the set of such integers $n$ belonging to $\mathcal{A}$. Let $\mathcal{A}(x) = \#\{n \le x : n \in \mathcal{A}\}$ and $\mathcal{A}_v(x) = \#\{n \le x : n \in \mathcal{A}_v\}$. Since $pv < (p + q)v = uv = n < x$, we get that $p = q + v < x/v$. Therefore, fixing $v$, we have that $q < x/v$ is a prime such that $q + v$ is also prime. Let $\mathcal{B} = \{n(n + v) \ : \ n \le x/v\}$ and let $\mathcal{P}$ be the set of all primes. Let $y < x/v$ to be fixed later. Note that $x/v > x^{1/2}$, because $v < x^{1/2}$. Clearly $\rho(r) = 1$ if $r \nmid v$ and $\rho(r) = 2$ otherwise. We then get, as in the proof of Proposition 12.4, that

$$\mathcal{A}_v(x) \le \pi(y) + \mathcal{S}(\mathcal{B}, \mathcal{P}, y) \ll \frac{x}{v} \prod_{p \le y} \left(1 - \frac{\rho(p)}{p}\right)$$

is valid for $y \le \log(x/v)/(20 \log\log(x/v))$. Since $x/v > x^{1/2}$, it follows that we may choose $y = \log x/(40 \log\log x)$ for large $x$. It is easily checked, as in the deduction of the Brun-Titchmarsh theorem from the combinatorial sieve, that

$$\begin{aligned} \prod_{p \le y} \left(1 - \frac{\rho(p)}{p}\right) &\ll \prod_{p \le y} \left(1 - \frac{1}{p}\right)^2 \prod_{p \mid v} \left(1 - \frac{1}{p}\right)^{-1} \\ &\ll \frac{v}{\phi(v)(\log y)^2} \ll \frac{v(\log\log x)^2}{\phi(v)(\log x)^2}. \end{aligned}$$

Thus,

$$\mathcal{A}_v(x) \ll \frac{x(\log\log x)^2}{\phi(v)(\log x)^2},$$

which establishes (ii). Since $\phi(v)/v \gg 1/\log\log v > 1/\log\log x$ (see Proposition 8.4), we get that

$$\mathcal{A}_v(x) \ll \frac{x(\log\log x)^3}{v(\log x)^2},$$

which proves (iii). Summing up over all $v$'s, we get

$$\mathcal{A}(x) \ll \sum_{v\le x^{1/2}} \frac{x(\log\log x)^3}{v(\log x)^2} = \frac{x(\log\log x)^3}{(\log x)^2} \sum_{v\le x^{1/2}} \frac{1}{v} \ll \frac{x(\log\log x)^3}{\log x} = o(x)$$

as $x \to \infty$. This completes the proof of (iv). □

**Problem 12.10.** *Use the Brun-Titchmarsh theorem and Abel's summation formula to show that*

$$\sum_{\substack{p\le x\\ p\equiv a \pmod b}} \frac{1}{p} \ll \frac{1}{p_{a,b}} + O\left(\frac{\log\log x}{\phi(b)}\right)$$

*uniformly for $x \ge 3$ and $1 \le a < b$, where $a$ and $b$ are coprime and $p_{a,b}$ is the smallest prime congruent to $a$ modulo $b$, and where the constant implied by the above $O$ is absolute.*

*Solution.* We may assume that $b \ge 3$, since otherwise the desired estimate follows from Mertens' formula. We set $a_n = 1$ if $n$ is a prime $> 3b$ that is congruent to $a$ modulo $b$ and 0 otherwise. Then the Brun-Titchmarsh theorem shows that

$$\sum_{n\le x} a_n \le \pi(x;a,b) \ll \frac{x}{\phi(b)\log(x/b)}.$$

If $3 \le x \le 3b$, then

$$\sum_{\substack{p\le x\\ p\equiv a \pmod b}} \frac{1}{p} < \frac{1}{p_{a,b}} + \frac{1}{b} + \frac{1}{2b} = \frac{1}{p_{a,b}} + O\left(\frac{\log\log x}{\phi(b)}\right),$$

since $\phi(b) \le b$ and $\log\log 3 > 0$. Assume that $x > 3b$. Then the Abel summation formula with $f(t) = 1/t$ yields

$$\begin{aligned}\sum_{\substack{p\le x\\ p\equiv a \pmod b}} \frac{1}{p} &\le \frac{1}{p_{a,b}} + \sum_{\substack{b<p\le x\\ p\equiv a \pmod b}} \frac{1}{p}\\ &< \frac{1}{p_{a,b}} + \frac{1}{b} + \frac{1}{2b} + \sum_{n\le x} a_n f(n)\\ &= \frac{1}{p_{a,b}} + \frac{3}{2b} + \frac{A(x)}{x} + \int_1^x \frac{A(t)}{t^2}dt\\ &= \frac{1}{p_{a,b}} + O\left(\frac{1}{\phi(b)\log(x/b)} + \frac{1}{b}\right)\\ &\qquad + O\left(\frac{1}{\phi(b)}\int_{3b}^x \frac{1}{t\log(t/b)}dt\right).\end{aligned} \tag{18.66}$$

Clearly,

$$\frac{1}{\phi(b)\log(x/b)} + \frac{1}{b} = O\left(\frac{1}{\phi(b)}\right).$$

As for the integral, we make the change of variable $u = t/b$, getting $dt = bdu$, so that

$$\begin{aligned}\int_{3b}^x \frac{1}{t\log(t/b)}dt &= \int_3^{x/b} \frac{du}{u\log u} = \log\log u\Big|_{u=3}^{u=x/b}\\ &= \log\log(x/b) - \log(\log 3) < \log\log(x/b)\\ &< \log\log x.\end{aligned} \tag{18.67}$$

The desired estimate in the range $x \ge 3b$ now follows from estimates (18.66) and (18.67). □

**Problem 12.12.** *Let $f(x) > 0$ be as in the preceding problem. Let*

$$\mathcal{Q} = \{p_n : p_{n+1} - p_n \le (\log n)/f(n)\}.$$

*Show that $\#(\mathcal{Q} \cap [1, x]) = o(\pi(x))$ as $x \to \infty$ in the following way:*

(i) *Observe that if $p \in \mathcal{Q} \cap [x/\log x, x]$, then there exists $k \le (\log x)/g(x)$ such that $p$ and $p + k$ are both primes, where $g(x) = f(x/\log x)$.*

(ii) *Fix $k$. Show, using the Brun sieve, that the number of $p \le x$ such that $p$ and $p + k$ are both primes is*

$$\ll \frac{k}{\phi(k)}\frac{x}{(\log x)^2}.$$

(iii) *Deduce that*

$$\#\left(\mathcal{Q}\cap[x/\log x,x]\right)\ll\frac{x}{(\log x)^2}\sum_{k\le(\log x)/g(x)}\frac{k}{\phi(k)}.$$

(iv) *Use the fact that* $k/\phi(k)\ll\sigma(k)/k$ *and Problem* 7.2 *to conclude that the estimate*

$$\sum_{k\le y}\frac{k}{\phi(k)}\ll y$$

*holds for all* $y\ge 1$.

(v) *Use (iv) with* $y=(\log x)/g(x)$ *in the conclusion of (iii) to conclude that* $\#(\mathcal{Q}\cap[x/\log x,x])\ll\pi(x)/g(x)=o(\pi(x))$ *as* $x\to\infty$.

*Solution.* Again, it suffices to look only at the primes $p\in\mathcal{Q}\cap[x/\log x,x]$, since there are only $\pi(x/\log x)\ll x/(\log x)^2=o(\pi(x))$ primes $q\le x/\log x$ as $x\to\infty$. Then, for large $x$, the next prime $q$ larger than $p$ is in the interval $[p,p+(\log x)/g(x)]$, where we take $g(x)=f(x/\log x)$. Furthermore, $q-p$ is even. Set $y=(\log x)/g(x)$ and let $k\le y$ be a fixed even integer. Then, $p\le x$ is such that $q=p+k$ is also a prime. We apply the Brun sieve with $\mathcal{A}=\{n(n+k)\}$. It is easy to check that we have $w(r)=2$ for all primes $r\nmid k$, while $w(r)=1$ if $r\mid k$. Furthermore, in Theorem 12.6, we may let $X=x$, $\kappa=2$ and $u$ be some appropriate (absolute) constant, and deduce that the cardinality of the set $\mathcal{Q}_k$ of such primes satisfies

$$\#\mathcal{Q}_k\ll x\prod_{p\le x^u}\left(1-\frac{w(p)}{p}\right)\ll x\left(\frac{k}{\phi(k)}\right)\frac{1}{(\log x)^2}.$$

We now sum these estimates for all possible values of $k$, thus obtaining

$$\sum_{k\le y}\#\mathcal{Q}_k\ll\frac{x}{(\log x)^2}\sum_{k\le y}\frac{k}{\phi(k)}.$$

First observe that $k/\phi(k)\ll\sigma(k)/k$. From the solution to Problem 7.2, we have that

$$\sum_{k\le y}\frac{\sigma(k)}{k}\ll y,$$

so that

$$\sum_{k\le y}\#\mathcal{Q}_k\ll\frac{xy}{(\log x)^2}=\frac{x}{g(x)\log x}=o(\pi(x))$$

as $x\to\infty$, because $g(x)\to\infty$ as $x\to\infty$. Since $\mathcal{Q}\cap[x/\log x,x]\subset\cup_{k\le y}\mathcal{Q}_k$, we get that

$$\#\left(\mathcal{Q}\cap[x/\log x,x]\right)\le\sum_{k\le y}\#\mathcal{Q}_k=o(\pi(x))$$

as $x\to\infty$, thus completing the solution of this problem. □

**Problem 12.14.** *Reconsider Problem* 12.6 *but now deduce that if* $\nu(p) < p$ *for all* $p$*, then there exists a number* $t$*, which depends on* $k$*, but not on* $a_i$ *and* $b_i$ *for* $i = 1, \dots, k$*, such that there exist infinitely many positive integers* $n$ *with* $\omega(L_i(n)) \le t$ *for all* $i = 1, \dots, k$*. (Hint: Use the Brun sieve as a lower bound sieve and show that the main term is* $> 0$ *and dominates the error term if we sieve with* $y = x^{1/ku}$*. Then deduce that one can take* $t = ku - 1$*.) Note that, for* $k = 2$ *and* $L_1(n) = n$*,* $L_2(n) = n + 2$*, Brun showed that one can take* $t = 9$*.*

*Solution.* Actually, this follows from the preceding problem and from the Brun sieve. Indeed, recall that the Brun sieve can be used as a lower bound too. That is, if $u$ is such that $1 + O(u^{-u/2}) \in [1/2, 3/2]$ and $(Dy)^u < x^{1/2}$, then we actually get that relation (12.12) reveals that

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, y) \ge \frac{x}{2} \prod_{p \le x^{1/(4uD)}} \left(1 - \frac{w(p)}{p}\right) - c(D)x^{1/2},$$

where $c(D)$ is a constant depending on $D$ only. For large $x$ and fixed $f$, we have that the product appearing in the main term is

$$> c_1 \frac{x}{(\log x)^D}, \tag{18.68}$$

where $c_1$ now depends on $D$ and also on the polynomial $f$, but for large $x$, the above lower bound (18.68) takes over the number $c(D)x^{1/2}$. And we simply retain from here the modest conclusion that

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, y) \to \infty$$

as $x \to \infty$. But recall that the number on the left above counts the number of $n \le x$ such that $f(n)$ is not divisible by any prime up to $y = x^{1/4uD}$. This shows that all prime factors of $a_i n + b_i$ exceed $x^{1/4uD}$, and since $n \le x$, we get that for large $x$, each of the numbers $a_i n + b_i$ for $i = 1, \dots, D$, which are factors of $f(n)$, can have at most $4uD$ prime factors. (For if it would have more, then $a_i n + b_i > y^{4uD+1} = x^{1+1/4ud}$ which is false for large $x$, since $a_i n + b_i \ll x$.) This completes the solution of the problem. □

**Problem 12.16.** *Regarding the preceding problem, show that the abc conjecture implies that* $\#\mathcal{T}(x, y) \le 2$ *if* $x$ *is large. (Hint: Assume that* $1 \le i_1 < i_2 \le y$ *are such that* $n$*,* $n + i_1$ *and* $n + i_2$ *are powerful and apply the abc conjecture to the equation* $(n + i_1)(n + i_2) - n^2 = (i_1 + i_2)n + i_1 i_2$ *to deduce that* $n$ *is bounded in terms of* $y$*.) Deduce that if* $1 = a_1 < a_2 < \cdots$ *is the increasing sequence of all the powerful numbers, then the abc conjecture implies that* $a_{n+2} - a_n \to \infty$*. Does* $a_{n+1} - a_n$ *tend to infinity? (Hint: The answer is NO and can be inferred by using Problem* 12.4*.)*

*Solution.* Call a form an homogeneous polynomial

$$a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d \in \mathbb{C}[X, Y]$$

of degree $d$ in two variables where not all coefficients are zero. As with polynomials, forms can be factored as $\prod_{i=1}^{d}(\alpha_i X + \beta_i Y)$ for some complex numbers $\alpha_i,\ \beta_i$. (To see this, think of the above form as $Y^d f(X/Y)$, where $f(T) = a_0T^d + \cdots + a_d$ and factor $f$ in linear factors over the complex numbers.) State that $f$ is squarefree as a form, if $(\alpha_i, \beta_i)$ and $(\alpha_j, \beta_j)$ are not parallel for any $i \neq j$ (equivalently, if $f$ has degree at least $d-1$ and has no double roots). Then the *abc* conjecture together with a theorem of Belyi implies that if $f(X, Y) \in \mathbb{Z}[X, Y]$ is a homogeneous form with integer coefficients which is squarefree as a form, then for any positive coprime integers $m, n$ we have

$$\gamma(f(m, n)) \gg_\varepsilon \max\{m, n\}^{d-2-\varepsilon},$$

where the implied constant might depend on the form and on $\varepsilon$. To see what this has to do with the *abc* conjecture, note that *abc* itself is the above statement for $f(X, Y) = XY(X+Y)$. This deduction is due to Noam Elkies [**41**]. Now assume that $y$ is fixed, that $0 < i < j \leq y$ and that $m > y$ is large and such that $m,\ m + i,\ m + j$ are all powerful. Since $y$ is fixed, we may assume that $i$ and $j$ are fixed. Apply the Elkies version of the *abc* conjecture to

$$f(X, Y) = (Y - X)XY((i - j)X + jY)$$

with $X = m/\gcd(m, i),\ Y = (m + i)/(\gcd(m, i))$ (note that $X$ and $Y$ are coprime positive integers) and get that $f(X, Y) \mid ijm(m + i)(m + j)$, so that $\gamma(f(X, Y)) \ll y^2m^{3/2}$, because each of $m,\ m + i,\ m + j$ is powerful. But the Elkies version of the *abc* conjecture tells us that $\gamma(f(X, Y)) \gg \max\{X, Y\}^{2-\varepsilon} \gg (m/y)^{2-\varepsilon}$. Choosing a small $\varepsilon$, we get that $m$ is bounded in terms of $y$. You should attempt to prove the stronger *abc* conjecture at least for forms of degree 4 which are a product of linear forms in $\mathbb{Z}[X, Y]$ (the first case not trivially following from the *abc* conjecture).

As for the second part of the problem, it is well known that the Fermat-Pell equation

$$X^2 - 8Y^2 = 1$$

has infinitely many positive integer solutions $X$ and $Y$. Thus, $8Y^2$ and $8Y^2 + 1 = X^2$ are consecutive powerful numbers, so that clearly $a_{n+1} - a_n$ does not tend to infinity with $n$. □

**Problem 12.18.** *Note that $p-1=\phi(p)=\phi(2p)$ if $p>2$. Let $\mathcal{P}=\{p\ :\ p-1=\phi(n)$ has at least 3 solutions $n\}$. Prove that*

$$\sum_{p\in\mathcal{P}}\frac{1}{p}<\infty.$$

*(Hint: Follow the hint suggested to solve Problem* 12.17*.)*

*Solution.* We sketch only the argument. If $n$ is divisible by at least $v$ primes, or if $n$ is very smooth, the same arguments as in (i), (ii) and (iii) of the statement of Problem 12.17 apply. Now let $n=qm$, where $q=P(m)$ is larger than $y$. Then $p-1=\phi(n)=(q-1)\phi(m)$ so that $q$ and $q\phi(m)+(\phi(m)-1)$ are primes. Note that if $m=1,2$, then $q\phi(m)+(\phi(m)-1)=q$, which gives us no extra information. But if $m>2$, then $q\phi(m)+(\phi(m)-1)=aq+b$, where $a$ and $b$ are coprime and $b$ is not zero. The same argument then applies as in the preceding problem and gives the same final bounds. □

**Problem 12.20.** *Adapt the proof of Proposition* 8.7 *(or Problem* 8.9*) to show that there exists a constant $c_0>0$ such that*

$$\#\{n\le x\ :\ \phi(n)\ \textit{is a perfect square}\}\ge x^{c_0}$$

*if $x>x_0$. (Hint: Let $y$ be some parameter and $\delta$ the number appearing in Theorem* 12.9*. Let $\mathcal{P}$ be the set of primes $p\in[y/\log y,y]$ such that $P(p-1)<p^\delta$. Choose subsets $S$ of such primes $p$ of exactly $\lfloor p^\delta\rfloor$ elements and let $n_S=\prod_{p\in S}p$. Then $\phi(n_S)=u_Sv_S^2$, where $P(u_S)\le y^\delta$ so that $u_S$ can take only at most $2^{\pi(y^\delta)}$ values. Now use the Pigeon Hole principle as in the proof of Proposition* 8.7 *to get a lower bound for the number of squarefree number $n$'s made up of primes from $\mathcal{P}$ for which $\phi(n)$ is a square and compare this lower bound with $x=y^{y^\delta}$, which is the upper bound for such $n$'s.)*

*Solution.* As the hint is trying to suggest, modify the proof of Proposition 8.7. Let $\delta<1$, a number for which Theorem 12.9 applies, and let $y$ be a large prime. Let $\mathcal{P}=\{p\le y\ :\ P(p-1)<y^\delta\}$ and assume that $\#\mathcal{P}>c_1\pi(y)$ for some $c_1>0$ (which is guaranteed by Theorem 12.9). Choose subsets $S$ of $\mathcal{P}$ with $K=\lfloor y^\delta\rfloor$ elements. The numbers $n_S=\prod_{p\in S}p$ then do not exceed $y^{y^\delta}$. Therefore, $n_{S\Delta T}\le y^{2y^\delta}=\exp(2y^\delta\log y):=x$ for any two such subsets $S$ and $T$. Now $\phi(n_S)=u_Sv_S^2$, where $P(u_S)\le y^\delta$ and $u_S$ is squarefree and can therefore be chosen in at most $V\le 2^{\pi(y^\delta)}=\exp(o(y^\delta))$ ways as $y\to\infty$. But the number $U$ of subsets $S$ of cardinality $K$ in $\mathcal{P}$ satisfies

$$U\ge\binom{\#\mathcal{P}}{K}\ge\left(\frac{c_1\pi(y)}{y^\delta}\right)^{\lfloor y^\delta\rfloor}=\exp((1-\delta+o(1))y^\delta\log y)\qquad\text{as } y\to\infty.$$

Thus, by the Pigeon Hole principle, there are subsets $S$ of size at least as large as

$$\begin{aligned}\frac{U}{V} &= \exp((1-\delta+o(1))y^\delta \log y + o(y^\delta)) \\ &= \exp((1-\delta+o(1))y^\delta \log y) = x^{(1-\delta+o(1))/2}\end{aligned}$$

as $x \to \infty$ for which $u_S$ has the same value. Now the construction from the end of the proof of Proposition 8.7 guarantees $x^{(1-\delta+o(1))/2}$ numbers $n \le x$ for which the Euler function is a square as $x \to \infty$. □

**Problem 12.22.** *Let*

$$p_a(n) = \frac{1}{\omega(n)} \sum_{p|n} p$$

*be the average prime factor of $n$. Use Vinogradov's three primes theorem (Theorem* 12.18*) to show that there exist infinitely many squarefree composite positive integers $n$ for which $p_a(n)$ is a prime factor of $n$. For example,* $105 = 3 \times 5 \times 7$ *and the average of* $3, 5, 7$ *is* $5$ *which is a prime factor of* $105$*. (Hint: Let $r$ be a large prime. Apply Vinogradov's theorem to $3r$ to deduce that there are many prime triplets $(p_1, p_2, p_3)$ such that $3r = p_1 + p_2 + p_3$. Then use an analogue of Theorem* 12.10 *to show that most of these representations have $p_i \neq p_j$ and $p_i \neq r$. Then choose $n = rp_1p_2p_3$.)*

*Solution.* Let $N = 3r$, where $r$ is a large prime. Vinogradov's theorem gives a number $\gg N^2/(\log N)^3$ of triples $(p_1, p_2, p_3)$ of primes such that $p_1 + p_2 + p_3 = 3r$. For any such triple with distinct $p_1, p_2, p_3, r$, the number $n = rp_1p_2p_3$ has $p_a = (p_1 + p_2 + p_3 + r)/4 = r \mid n$. To guarantee that we have triples $(p_1, p_2, p_3)$ with $p_1, p_2, p_3$ distinct and different from $r$, assume that $p_1 = r$. Then, $2r = p_2 + p_3$ and the number of choices $(p_2, p_3)$ is, by Theorem 12.10, $T(2r) \ll 2r/(\log(2r))^2 \ll N/(\log N)^2 = o(N^2/(\log N)^3)$ as $N \to \infty$. Thus, for large $r$ most of the triples of primes under scrutiny have their components different from $r$. Similarly, if $p_1 = p_2$, we get $3r = 2p_1 + p_2$. With $N = 3r$ fixed, this means that we count primes $p_1 < N/2$ such that $p_1$ and $N - 2p_1 = p_2$ are both primes. The same argument as the one used in the proof of Theorem 12.10 shows that the number of such triples is $\ll N/(\log N)^2 = o(N^2/(\log N)^3))$ as $r \to \infty$, so that indeed most triples of primes $(p_1, p_2, p_3)$ have distinct components which are unequal to $r$. Letting $r$ tend to infinity, we get infinitely many examples. □

**Problem 12.24.** *First show that $\sigma(\sigma(p))/p \ge 3/2$ for all primes $p$. Then use Chen's theorem (Theorem* 12.11*) to deduce that* $\{\sigma(\sigma(p))/p : p \text{ prime}\}$

*is dense in* $[3/2, \infty)$. *(Hint: Let* $a$ *be an odd integer. Use Chen's theorem to conclude that there are arbitrarily large primes* $p$ *with* $(p+1)/(2a)$ *either a prime or a product of two large primes. Deduce that* $\sigma(\sigma(p))/p = (3/2)(\sigma(a)/a)(1+o(1))$ *as* $p \to \infty$ *over such primes and conclude using known results about the numbers* $\sigma(a)/a$ *as* $a$ *runs through the odd positive integers.)*

*Solution.* Clearly, $\sigma(\sigma(p))/p > \sigma(\sigma(p))/\sigma(p)$ and $\sigma(p) = p+1$ is even, implying that $\sigma(\sigma(p))/\sigma(p) > 1 + 1/2 = 3/2$. For the density argument, let $a$ be odd. Chen's theorem gives primes $p$ such that $(p+1)/(2a)$ is prime or has two prime factors each exceeding $p^{1/10}$. Thus, if $p > (2a)^{10}$, $(p+1)/(2a)$ is coprime to $2a$. Thus, $p+1 = 2am$ with $(2a, m) = 1$, so that $\sigma(p+1) = \sigma(2a)\sigma(m) = 3\sigma(a)\sigma(m)$. If $m$ is prime, then $\sigma(m) = m+1$; otherwise, $\sigma(m) = m + O(m/p^{1/10}) = m + O(m^{9/10})$. Thus,

$$\begin{aligned} \frac{\sigma(\sigma(p))}{p} &= \left(1 + \frac{1}{p}\right) \frac{\sigma(\sigma(p))}{\sigma(p)} \\ &= \frac{3}{2}\frac{\sigma(a)}{a}\left(1 + O\left(\frac{1}{m^{1/10}}\right)\right)\left(1 + \frac{1}{p}\right), \end{aligned}$$

so that, as $p$ tends to infinity over these "Chen primes", $\sigma(\sigma(p))/\sigma(p)$ tends to $(3/2)\sigma(a)/a$. Now by Problem 7.24, we have that $\sigma(a)/a$ is dense in $[1, \infty)$ as $a$ varies through odd integers, thus completing the proof. □

**Problem 12.26.** *Positive integers* $n$ *with* $\beta(n) = \beta(n+1)$ *are called Ruth-Aaron numbers (recall that* $\beta(n) = \sum_{p|n} p$*). One can check that* $n = 714$ *is such a number. It is not known if there are infinitely many such numbers* $n$*. Do you have an heuristic? What does your heuristic predict? You should back it up with known conjectures such as the abc conjecture or the Schinzel Hypothesis H.*

*Solution.* Here we can give many examples. In fact, we will exhibit a large family of solutions to $\beta(n) = \beta(n+1)$. Choose $n = qb,\ n+1 = pa$, where $q \| n,\ p \| n+1$. Then $\beta(n+1) = \beta(n)$ is equivalent to $q + \beta(b) = p + \beta(a)$ so that $p - q = \beta(b) - \beta(a)$. But also $pa - qb = 1$. Treat these as two equations in two unknowns $p$ and $q$ and solve to get $p = (b(\beta(b) - \beta(a)) - 1)/(b-a)$ and $q = (a(\beta(b) - \beta(a)) - 1)/(b-a)$. Choose $b = 2(30\lambda + 23),\ a = 15(4\lambda + 3)$, where $30\lambda + 23$ and $4\lambda + 3$ are primes. Then $b - a = 1$, $\beta(b) - \beta(a) = 2 + 30\lambda + 23 - 3 - 5 - 4\lambda - 3 = 26\lambda + 14 = 2(13\lambda + 7)$. Now $p$ and $q$ are given by $p = 4(30\lambda + 23)(13\lambda + 7) - 1$ and $q = 30(4\lambda + 3)(13\lambda + 7) - 1$. Note that all these numbers are odd; if $\lambda \equiv 2 \pmod 3$ none is a multiple of 3, and if $\lambda \equiv 1 \pmod 5$, none is a multiple of 5. Therefore, if we choose

$f_1(\lambda) = 30\lambda + 23$, $f_2(\lambda) = 4\lambda + 3$, $f_3(\lambda) = 4(30\lambda + 23)(13\lambda + 7) - 1$ and $f_4(\lambda) = 30(4\lambda + 3)(13\lambda + 7) - 1$, for each of $p = 2, 3, 5$, there exists a class $\lambda \pmod p$ such that $\prod_{i=1}^4 f_i(\lambda) \not\equiv 0 \pmod p$. If $p \geq 7$, this is also true since $\prod_{i=1}^4 f_i(X)$ has degree 6 so it cannot have more than 6 roots modulo any prime $p$. Now Schinzel's Hypothesis H suggests that perhaps there should be infinitely many Ruth-Aaron numbers. □

**Problem 12.28.** *Show that the Ruth-Aaron numbers introduced in Problem* 12.26 *form a set of asymptotic density zero in the following way:*

(i) *Let $x$ be large. Argue that one may assume that none of $n$ is not $x^{1/u}$-smooth where $u = \log\log x$, that $P(n) \| n$ and that if $P_2(n)$ is the second largest prime factor of $n$, then $P(n) > P_2(n)(\log x)^3$ and that the same is true for $n + 1$.*

(ii) *Let $p$ and $q$ be the largest prime factors of $n$ and $n+1$ respectively. Deduce from $\beta(n) = \beta(n+1)$ and (i) above that $|p-q| < p/(\log x)^2$ if $x > x_0$.*

(iii) *If $pq \leq x$, then the number of $n \leq x$ such that $p \mid n$ and $q \mid n + 1$ is $\leq x/pq + 1 \leq 2x/pq$. Now sum up over all pairs of primes $p$, $q$ larger than $x^{1/u}$ with $|p - q| = O(p/(\log x)^2)$.*

(iv) *Write $n = pa$, $n + 1 = qb$. If $pq > x$, deduce that $ab \leq x$ and $|a - b| \ll a/(\log x)^2$.*

(v) *For fixed $a$ and $b$ with $ab \leq x$, there are at most $x/ab + 1 \leq 2x/ab$ positive integers $n \leq x$ such that $a \mid n$ and $b \mid n + 1$.*

(vi) *Show that for fixed $a$,*

$$\sum_{a<b<a+O(a/(\log x)^2)} \frac{1}{b} \ll \int_a^{a+O(a/(\log x)^2)} \frac{dt}{t} \ll \frac{1}{(\log x)^2}.$$

(vii) *Conclude that the number of Ruth-Aaron numbers $n \leq x$ with $ab \leq x$ is*

$$\ll \frac{x}{(\log x)^2} \sum_{a \leq x} \frac{1}{a} \ll \frac{x}{\log x} = o(x) \qquad \text{as } x \to \infty.$$

*Solution.* Let $x$ be large. By a calculation done several times by now, choosing $y = x^{1/\log\log x}$, we obtain that $\Psi(x, y) \ll x/\exp(u/2) \ll x/(\log x)^{1/2}$. So, we eliminate $n \leq x$ such that either $P(n) \leq y$ or $P(n + 1) \leq y$. Let $P_2(n)$ be the second largest prime factor of $n$. If $P_2(n)(\log x)^3 \geq P(n)$, we get that $P_2(n) \geq y/(\log x)^3 > y^{1/2}$ for large values of $y$, so that $P(n) \leq P_2(n)(\log x)^3 < P_2(n)(\log P_2(n))^4$, because $P_2(n) > y^{1/2}$ and $(\log x)^3 < (\log y^{1/2})^4$ for large values of $x$. Let $p = P_2(n)$. Then $pq \mid n$,

where $p > y^{1/2}$ and $q \in [p, p(\log p)^4]$. then, one can show that for fixed $p$, the number of such $n$ is up to a multiplicative constant

$$\begin{aligned}\frac{x}{p}\sum_{p\le q\le p(\log p)^4}\frac{1}{q} &\le \frac{x}{p}\left(\log\log(p(\log p)^4) - \log\log p + O\left(\frac{1}{\log p}\right)\right)\\ &\ll \frac{x\log\log p}{p\log p},\end{aligned}$$

where we used the fact that

$$\log\log(p(\log p)^4) - \log\log p = \log\left(1 + \frac{4\log\log p}{\log p}\right) \ll \frac{\log\log p}{\log p}.$$

It follows that the number of such $n$ is $\ll x(\log\log(y^{1/2})/(\log(y^{1/2})) \ll x(\log\log x)^2/\log x = o(x)$ as $x \to \infty$. Clearly, the same applies to $n+1$. This completes the proof of (i). (The numbers $n$ for which $p^2 \mid n$ for some prime $p > y$ give again a total contribution of at most $O(x/y) = o(x)$ cases as $x \to \infty$, so that we may assume that $P(n) \| n$.) From (i), if $\beta(n) = \beta(n+1)$ and $n$ has not already been accounted for in (i), then $n = pa,\ n+1 = qb$, where $P(a) < p/(\log x)^3$ and $P(b) < q/(\log x)^3$. Since $p + \beta(a) = q + \beta(b)$, we get that

$$|p - q| \le \max\{\omega(n), \omega(n+1)\}\max\{P(a), P(b)\} \le \frac{\max\{p,q\}}{(\log x)^2},$$

where we use the fact that $\max\{\omega(n), \omega(n+1)\} \ll \log x$. In particular, for large $x$, $p$ and $q$ are very close (say if $p < q$ then $q < 2p$). Assume that $pq < x$. Then $n+1 \equiv 0 \pmod p$ and $n \equiv 0 \pmod q$ puts $n$ into a congruence class modulo $pq$ and the number of such $n \le x$ is $\le x/pq + 1 \le 2x/pq$, because we are assuming that $pq \le x$. Thus, the number of such $n \le x$ is up to a multiplicative constant

$$\ll x\sum_{p>y}\sum_{p\le q\le 2p}\frac{1}{pq} \ll \frac{x(\log\log y)}{\log y} \ll \frac{x(\log\log x)^2}{\log x} = o(x) \qquad \text{as } x \to \infty.$$

If $pq > x$, then since $n(n+1) < x^2$ (consider $n < x - 1$) we get that $ab < x^2/(pq) < x$. Since $pa - qb = 1$ and $p/q$ is close to 1, then $a/b$ is close to 1. That is, $p/q = b/a + O(1/y)$ and since $|p/q - 1| = O(1/(\log x)^2)$, we get that $|b/a - 1| = O(1/(\log x)^2)$. Assume only that $a < b$ since the other case is similar. Then $a$ and $b$ are coprime (as divisors of the coprime positive integers $n+1$ and $n$, respectively), and for fixed $a < b < a + O(a/(\log x)^2)$, we have that $n+1 \equiv 0 \pmod a$ and $n \equiv 0 \pmod b$ puts $n$ into a certain congruence class modulo $ab$. The number of such $n \le x$ is $\le x/(ab) + 1 \le 2x/(ab)$, because $ab \le x$. Summing up over all possible $a$ and $b$, we get that

the number of such $n \le x$ is

$$\ll x \sum_{a \le x} \frac{1}{a} \sum_{a < b < a + O(a/(\log x)^2)} \frac{1}{b}. \tag{18.69}$$

The inner sum is

$$\le \int_a^{a+O(a/(\log x)^2)} \frac{dt}{t} = \log\left(1 + O\left(\frac{1}{(\log x)^2}\right)\right) \ll \frac{1}{(\log x)^2}. \tag{18.70}$$

Combining (18.69) and (18.70), we obtain that the number of such integers $n \le x$ is

$$\ll \frac{x}{(\log x)^2} \sum_{a \le x} \frac{1}{a} \ll \frac{x}{\log x} = o(x)$$

as $x \to \infty$. □

**Remark.** This problem was the subject of the first joint paper by Paul Erdős and Carl Pomerance [**51**]. They wrote 21 joint papers.

**Problem 12.30.** *Let* $r(n) = \#\{(p,k) \ : \ n = p + 2^k\}$.

(i) *Show that*

$$\sum_{n \le x} r(n) \gg x.$$

(ii) *Show that*

$$\sum_{n \le x} r(n)^2 = \#\{(p_1,k_1,p_2,k_2) \ : \ p_1 + 2^{k_1} = p_2 + 2^{k_2}\}.$$

*If* $k_1 = k_2$, *then* $p_1 = p_2$, *implying that the number of such diagonal quadruples* $(p_1,k_1,p_2,k_2)$ *is* $\le \pi(x)(\log x/\log 2) \ll x$.

(iii) *Show, using the Brun sieve, that the number of non-diagonal quadruples is*

$$\begin{aligned} \sum_{k \le \log x/\log 2} \frac{x}{\log x} \prod_{p \mid 2^k - 1} \left(1 + \frac{1}{p}\right) &\ll \frac{x}{\log x} \sum_{\substack{d \le x \\ d \ odd}} \frac{1}{d} \sum_{\substack{k \le \log x/\log 2 \\ t_d \mid k}} 1 \\ &\ll \frac{x}{\log x} \sum_{d \ odd} \frac{\log x}{dt_d}, \end{aligned}$$

*where* $t_d$ *is the multiplicative order of 2 modulo* $d$, *and now use Problem* 12.29 *to conclude that* $\sum_{n \le x} r(n)^2 \ll x$.

(iv) *Use the Cauchy-Schwarz inequality as in the proof of Theorem* 12.17 *to show that the set of numbers* $n = p + 2^k$ *has positive lower asymptotic density. (Yet remember that its complement also has positive lower asymptotic density, for example, from Problem* 7.20.*)*

*Solution.* We start with (i). First, we write $\sum_{n\le x} r(n) = \sum_{\substack{(p,2^k)\\ p+2^k\le x}} 1$. Note that if $p \le x/2$ is prime and $2^k \le x/2$, then $p + 2^k \le x$. This argument shows that the above sum is $\ge \pi(x/2)\cdot \lfloor \log(x/2)/\log 2\rfloor \gg x$, by the Prime Number Theorem (or Chebyshev's estimates), thus establishing (i).

For (ii), it is clear that

$$\sum_{n\le x} r(n)^2 = \sum_{n\le x}\left(\sum_{(p,k):p+2^k=n} 1\right)^2 = \sum_{n\le x}\sum_{\substack{(p_1,k_1,p_2,k_2)\\ p_1+2^{k_1}=p_2+2^{k_2}=n}} 1.$$

A diagonal term has $k_1 = k_2$, so that $p_1 = p_2$. There are at most

$$\pi(x)\lfloor \log x/\log 2\rfloor \ll x$$

pairs $(p,k)$ with $p + 2^k \le x$. Let us look at the non-diagonal pairs. Assume $k_1 < k_2$. Then $p_2 + 2^{k_1}(2^{k_2-k_1} - 1) = p_1$. Thus, we need to count the number of primes $p_2 \le x$ such that $p_2 + 2^{k_1}(2^{k_2-k_1} - 1)$ is also prime. Let $a_{k_1,k_2} = 2^{k_1}(2^{k_2-k_1} - 1)$. By the Brun sieve, with $\kappa = 2$, $X = x$, $w(r) = 1$ if $r \mid 2(2^{k_2-k_1} - 1)$ and $w(r) = 2$ otherwise, we get that the number of primes $p \le x$ such that $p + a_{k_1,k_2}$ is also a prime is, as in the proof of Theorem 12.10,

$$\ll \frac{x}{(\log x)^2}\prod_{p\mid 2^{k_2-k_1}-1}\left(1+\frac{1}{p}\right).$$

Note that $k_2 \le \log x/\log 2$ and $k_2 - k_1 \ll \log x/\log 2$. We therefore obtain that

$$\sum_{n\le x} r(n)^2 \ll \frac{x}{(\log x)^2}\cdot(\log x)\cdot \sum_{1<\ell\le \lfloor \log x/\log 2\rfloor}\prod_{p\mid 2^\ell-1}\left(1+\frac{1}{p}\right).$$

Observe that

$$\prod_{p\mid 2^\ell-1}\left(1+\frac{1}{p}\right) = \sum_{\substack{d:\mu(d)\ne 0\\ t_d\mid \ell}}\frac{1}{d}.$$

Thus, summing up the above bounds and changing the order of summation, we get

$$\begin{aligned}\sum_{1<\ell\le \lfloor \log x/\log 2\rfloor}\prod_{p\mid 2^\ell-1}\left(1+\frac{1}{p}\right) &\le \sum_{1<\ell\le \log x/\log 2}\sum_{d:t_d\mid \ell}\frac{1}{d}\\ &= \sum_{d:t_d\le \log x/\log 2}\frac{1}{d}\sum_{\substack{\ell\le \log x/\log 2\\ t_d\mid \ell}} 1\end{aligned}$$

$$= \sum_{d: t_d \le \log x/\log 2} \frac{1}{d} \left\lfloor \frac{\log x}{(\log 2) t_d} \right\rfloor$$
$$\ll \log x \sum_d \frac{1}{dt_d} \ll \log x,$$

where we used the previous problem, which states that $\sum_{d \text{ odd}} \frac{1}{dt_d} < \infty$. Collecting all these estimates, we obtain that $\sum_{n \le x} r(n)^2 \ll x$. By the Cauchy-Schwarz inequality, we get that if we write $\mathcal{N}$ for the set of $n \le x$ of the form $n = p + 2^k$ and set $a_n = 1$ if $n \in \mathcal{N}$ and $a_n = 0$ otherwise, we have that

$$\left( \sum_{n \le x} r(n) \right)^2 = \left( \sum_{n \le x} a_n (a_n r(n)) \right)^2$$
$$\le \left( \sum_{n \le x} a_n r(n)^2 \right) \left( \sum_{n \le x} a_n^2 \right) \le \left( \sum_{n \le x} r(n)^2 \right) \#\mathcal{N},$$

and since the left-hand side above is $\gg x^2$ while the right-hand side is $\ll x \cdot \#\mathcal{N}$, we get that $\#\mathcal{N} \gg x$. □

**Problem 12.32.** *The number $n = 113$ has the property that if we delete any of its digits, the number that remains is prime. Show that the number of $n \le x$ with this property is smaller than $x^c$ for some positive constant $c$ as $x \to \infty$. Are there infinitely many such positive integers?*

*Solution.* This is actually much easier than it sounds and no sieve is necessary. Indeed, let $n$ be such a number and let $S$ be its digit sum. If $n$ has digits of all three congruence classes modulo 3, then by eliminating appropriate digits we get numbers whose digits sums are congruent to $S$, $S-1$ and $S-2$ modulo 3, respectively, and one of those numbers is a multiple of 3. Since $n$ is large (it has at least 3 digits), the resulting multiple of 3 is not 3 itself, and so it is not prime. This shows that there exists some congruence class modulo 3 such that no digit of $n$ belongs to that congruence class. Since each congruence class modulo 3 has at least 3 digits in it, it follows that the digits of $n$ belong to a set with at most seven digits, and there are only 3 such sets (according to the congruence class modulo 3 that we are forbidding). Now if $x$ is large and $n \le x$, then the number of digits of $n$ is $\le \log x/\log 10 + 1$ and since there are only seven possibilities, we get that

the number of such $n$ is $\leq 3 \cdot 7^{\log x/\log 10+1} \ll x^c$, where $c = \log 7/\log 10 < 1$, which certainly implies the desired estimate. As to whether there should be infinitely many, the answer is perhaps yes. In the same way as one conjectures $2^p - 1$ to be prime for infinitely many primes $p$, perhaps in the same way $q = (10^p - 1)/9 = \underbrace{11\ldots1}_{p \text{ times}}$ is prime for infinitely many primes $p$. For such primes $p$, the number

$$n = (10^{p+1} - 1)/9 = \underbrace{11\ldots1}_{p+1 \text{ times}}$$

has the property that whatever digit we are eliminating we get $q = (10^p - 1)/9$, which we are assuming to be prime. Thus, perhaps there are infinitely many such numbers $n$. □

**Remark.** The following table lists all the prime numbers $< 10^{10}$ with this property

| Number of digits | Primes with the property |
|---|---|
| 2 | 23, 37, 53, 73 |
| 3 | 113, 131, 137, 173, 179, 197, 311, 317, 431, 617, 719 |
| 4 | 1013, 1031, 1097, 1499, 1997, 2239, 2293,<br>3137, 4019, 4919, 6173, 7019, 7433, 9677 |
| 5 | 10193, 10613, 11093, 19973, 23833, 26833, 30011, 37019,<br>40013, 47933, 73331, 74177, 90011, 91733, 93491, 94397 |
| 6 | 111731, 166931, 333911, 355933, 477797, 477977,<br>633317, 633377, 665293, 700199, 719333, 746099,<br>779699, 901499, 901997, 944777, 962233, 991733 |
| 7 | 1367777, 1440731, 1799999, 2668999, 3304331, 3716633,<br>4437011, 5600239, 6666437, 6913337, 7333331, 7364471, 7391117 |
| 8 | 13334117, 22255999, 33771191, 38800999, 40011197,<br>40097777, 44333339, 49473377, 79994177, 86000899,<br>93361493, 94400477, 99396617, 99917711 |
| 9 | 110499911, 144170699, 199033997, 222559399, 333904433, 461133713,<br>469946111, 640774499, 679774391, 680006893, 711110111, 716664317,<br>743444477, 889309999, 900117773, 982669999, 999371099, 999444431 |
| 10 | 1113399311, 1133333777, 1176991733, 1466664677, 1667144477,<br>1716336911, 2350000999, 3336133337, 3355522333, 3443339111,<br>3973337999, 4111116011, 4900001111, 6446999477, 6666116411,<br>6689899999, 6914333711, 7463333477, 8555555599, 8888333599,<br>8936093833, 9746666477 |

## Solutions to problems from Chapter 13

**Problem 13.2.** *Show that in Problem* 12.33, 3 *can be replaced by* 5 *for* $m > 2$. *Following Aigner, call a prime* $p$ *elite if* $\left(\frac{F_n}{p}\right) = 1$ *holds only for finitely many* $n$. *Here* $F_n$ *stands for the* $n$*-th Fermat number. For example,* $p = 3$ *and* $p = 5$ *are elite. The rest of this problem will guide us through a proof of the fact that the sum of the reciprocals of the elite primes is convergent.*

(i) *Let* $x$ *be large,* $v = \lfloor 10 \log\log\log x \rfloor$. *Show, using the Brun-Titchmarsh theorem, that the set of primes* $p \le x$ *for which* $2^v \mid p-1$ *has cardinality* $O(x/2^v \log x) = O(x/(\log x (\log\log x)^2))$ *for large* $x$.

(ii) *Set* $y = x^{1/(10\log\log x)}$. *Follow the proof of Proposition* 9.11 *to show that the set of primes* $p \le x$ *such that either* $P(p-1) < y$ *or* $t_p < y^{1/4}$ *is of cardinality* $O(x/(\log x)^2)$. *Here,* $t_p$ *is as usual the order of* 2 *modulo* $p$.

(iii) *Let* $k$ *be such that* $2^k \| p-1$. *Show that the sequence* $F_n \pmod p$ *is periodic for* $n \ge k$ *with period* $\gg \log t_p$. *In particular, if* $p$ *satisfies (i) and (ii), then its period is* $> v$ *for large* $x$.

(iv) *Deduce that* $F_m$ *is a quadratic residue modulo* $p$ *for all* $m = k, k+1, \dots, k+v$.

(v) *Let* $i \le v$ *be fixed and let* $F_i = M_i x_i^2$, *where* $M_i$ *is squarefree. Show that* $M_i > 1$. *Further show, using the preceding problem, that if* $p$ *is elite, then,* $p$ *can be in at most* $\phi(M)/2^{\lfloor v/2 \rfloor}$ *of all the possible congruence classes* $a \pmod M$ *with* $\gcd(a, M) = 1$, *where* $M = \prod_{i=1}^{k} M_i$.

(vi) *Show that* $M = \exp((\log\log x)^{O(1)}) = x^{o(1)}$ *as* $x \to \infty$ *and conclude using the Brun-Titchmarsh theorem with primes in congruence classes modulo* $M$, *that the number of elite primes* $p \le x$ *such that* $2^k \| p-1$ *is* $\ll x/(2^{v/2} \log x)$.

(vii) *Deduct from the above that the counting function of the elite primes is* $O(x/(2^{v/2} \log x)) = O(x/(\log x (\log\log x)^2))$. *Now use Abel's summation formula to conclude that the sum of the reciprocals of the elite primes is convergent.*

*Solution.* Let $x$ be large and let $p \le x$ be an elite prime. We may assume that $p \ge x/\log x$, since there are only $\pi(x/\log x) \ll x/(\log x)^2$ primes $p \le x/(\log x)$. If $2^v \mid p-1$, then $p \equiv 1 \pmod{2^v}$. By the Brun-Titchmarsh

theorem with $a = 1$ and $b = 2^v$, we get that the number of such primes is

$$\leq \pi(x; 1, 2^v) \ll \frac{x}{\phi(2^v)\log(x/2^v)}.$$

Since $x/2^v > x/(\log\log x)^{10\log 2} > x^{1/2}$ for large $x$, and $\phi(2^v) = 2^{v-1}$, we get that the above upper bound is

$$\leq \frac{4x}{2^v \log x} \ll \frac{x}{\log x(\log\log x)^{10\log 2}}.$$

For (ii), we put $y = x^{1/(10\log\log x)}$. We now follow the proof of Proposition 9.11. We have $u = 10\log\log x$, so that $\exp(u/2) = (\log x)^5$. The bound (9.31) is therefore $x/\exp(u/2) = x/(\log x)^5$ and the bound (9.32) is certainly $x/y^2 = o(x/(\log x)^2)$ as $x \to \infty$. Finally, the number of primes $p \leq x$ such that $t_p < p^{1/4}$ is $O(x^{1/2})$, by relation (9.35) of the proof of Proposition 9.11, implying that the number of exceptions is at most $O(x/(\log x)^2)$. This clears (ii). Now let $2^k \| p-1$ and look at $F_n$ with $n \geq k$. Then $F_n = 2^{2^k(2^{n-k})} + 1$. The sequence $\{2^{n-k}\}_{n\geq k}$ is periodic modulo $(p-1)/2^k$. If $\ell$ is this period, then $2^{n-k+u\ell} = 2^{n-k} \pmod{(p-1)/2^k}$, so that $2^{k+(n-k)+u\ell} \equiv 2^{k+(n-k)} \pmod{p-1}$. Thus, $2^{2^{n+u\ell}} + 1 \equiv 2^{2^n} + 1 \pmod p$ for $n \geq k$, which implies that $F_{n+u\ell} \equiv F_n \pmod p$ for $n \geq k$ and all $u \geq 0$. Thus, if for some $n$, we have that $F_n$ is a quadratic residue modulo $p$, then $F_{n+u\ell}$ is also a quadratic residue modulo $p$ for all $u \geq 0$, which contradicts the fact that $p$ is elite. Thus, all $n \geq k$ are such that $F_n$ is not a quadratic residue modulo $p$. Moreover, if $0 \leq i < j < v$, then $F_{n+i} \not\equiv F_{n+j} \pmod p$. Indeed, if it were not the case, then $p \mid 2^{2^{n+i}(2^{j-i}-1)} - 1$, so that $(2^{j-i}-1)$ would be a multiple of the odd part of $t_p$, which is $> p^{1/4}/2^k > y^{1/4}/2^v$. Thus, $j - i > \log(y^{1/4}/2^v)/\log 2 = (\log x + O(\log\log\log x))/(\log\log\log x) > v$ for large $x$. Therefore, the numbers $F_{n+i}$ for $i = 1, \ldots, v$ are all distinct modulo $p$. They are also coprime (by Theorem 2.2) and they are all of the form $u^2 + 1$, implying that they are not perfect squares. Let $F_{n+i} = M_i u_i^2$ with $M_i$ squarefree. It follows that $M_i \geq 1$, that they are all coprime and that $(M_i/p) = 1$ for $i = 1, \ldots, v$. The preceding problem tells us that $p$ is in only $\phi(M)/2^v$ of all the $\phi(M)$ possible progressions modulo $M$. Note that

$$\begin{aligned} M &\leq 2^{\sum_{i=1}^{v} 2^{k+i}} \leq 2^{2^{2v}} = 2^{(\log\log x)^{O(1)}} \\ &= \exp((\log\log x)^{O(1)}) = \exp(o(\log x)) = x^{o(1)} \end{aligned}$$

as $x \to \infty$. For each $a \pmod M$, the number of primes $p \leq x$ in that progression is by Brun-Titchmarsh $\ll x/(\phi(M)\log(x/M)) \ll x/(\phi(M)\log x)$. Summing up over all the $\phi(M)/2^v$ progressions, we get that the total number of such primes is

$$\ll \frac{x}{2^v(\log x)} \ll \frac{x}{(\log x)(\log\log x)^{10\log 2}}.$$

Since $10 \log 2 > 2$, we get that the counting function is $O(x/(\log x(\log\log x)^2)$. We now use Abel's summation formula with $a_n = 1$ if $n$ is an elite prime and $a_n = 0$ otherwise, and choose $f(t) = 1/t$, which leads to the conclusion that the sum of the reciprocals of the elite primes is convergent, using the fact that the improper integral $\int_3^\infty \frac{dt}{t(\log t)(\log\log t)^2}$ converges (do the substitution $u = e^{e^t}$). □

**Problem 13.4.** *Show that if $n$ is sufficiently large, then the Fibonacci number $F_n$ has a prime factor $p \equiv 1 \pmod 4$. (Hint: If $k$ is coprime to 6, then $L_k^2 - 5F_k^2 = -4$. Observe that $F_k$ is odd and reduce the above relation modulo any prime factor $p$ of $F_k$. Then reduce the problem to $F_{2^\alpha}$ and $F_{3^\beta}$ and show that these numbers have prime factors $p \equiv 1 \pmod 4$ as well, provided $\alpha$ and $\beta$ are sufficiently large.)*

*Solution.* If $k > 1$ is coprime to 6, then $F_k > 1$ and $F_k$ is odd. (By looking at $\{F_n\}_{n\ge 0}$ modulo 2, one notices that $F_n$ is even if and only if $n$ is a multiple of 3.) Reducing $L_k^2 - 5F_k^2 = 4(-1)^k = -4$ (see the solution to Problem 11.12 for this identity, where $\{L_n\}_{n\ge 0}$ is the Lucas sequence given by $L_0 = 2$, $L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \ge 0$) modulo a prime divisor $p$ of $F_k$ (necessarily odd), we get that $L_k^2 \equiv -4 \pmod p$. Thus, $(-4/p) = 1$, implying that $(-1/p) = 1$ because $(4/p) = (2/p)^2 = 1$. Thus, $p \equiv -1 \pmod 4$. Now note that $F_a \mid F_b$ whenever $a \mid b$. This can be shown by induction, observing first that $F_a \mid F_a$ and $F_{2a} = F_a L_a$, so that $F_a \mid F_{2a}$, and later proving that

$$F_{(n+2)a} = L_a F_{(n+1)a} + (-1)^{a-1} F_{na}$$

is valid for all positive integers $n$ and $a$, allowing one to use an induction argument with the basis that $F_a \mid F_{na}$ and $F_a \mid F_{(n+1)a}$ implies that $F_a \mid F_{(n+2)a}$. All these formulas can be checked by using the representations $F_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ and $L_n = \alpha^n + \beta^n$, where $\alpha = (1 + \sqrt{5})/2$, $\beta = (1 - \sqrt{5})/2$ mentioned in the solution to Problem 11.12. From an algebra point of view, $F_n \mid F_m$ is an easy consequence of the fact that

$$\begin{aligned} F_m &= \frac{\alpha^m - \beta^m}{\alpha - \beta} \\ &= \frac{(\alpha^n)^{m/n} - (\beta^n)^{m/n}}{\alpha - \beta} \\ &= \frac{\alpha^n - \beta^n}{\alpha - \beta}((\alpha^n)^{m/n-1} + \cdots + (\beta^n)^{m/n-1}) \\ &= F_n((\alpha^n)^{m/n-1} + \cdots + (\beta^n)^{m/n-1}), \end{aligned}$$

provided one observes that the long messy factor above is an integer. The easiest way to notice this is to observe that it is both a rational number (that is, $F_m/F_n$)) and an algebraic integer (as a sum of products of algebraic integers). Hence, it is an integer.

The above small excursion in the divisibility properties of the Fibonacci numbers, together with what we showed at the beginning of this solution, shows that if $n = 2^\alpha 3^\beta k$ with some $k > 1$ coprime to 6, then $p \mid F_k \mid F_n$ for some prime $p \equiv 1 \pmod 4$. All we need to show is that if $\alpha$ and $\beta$ are large, then $F_{2^\alpha}$ and $F_{3^\beta}$ are also divisible by a prime $p \equiv 1 \pmod 4$. One easily checks that $17 \mid F_9$ and that $F_{64}$ has a prime factor $p \equiv 1 \pmod 4$. □

**Problem 13.6.** *This problem is essentially a guide through a proof of the fact that* $0, 1, 144$ *are the only squares in the Fibonacci sequence.*

(i) *If* $F_n$ *is a square,* $F_n$ *is odd and* $n$ *is even, then show that* $F_{n/2}$ *is a square.*

(ii) *If* $F_n$ *is a square,* $F_n$ *is even and* $n$ *is odd, then show that* $F_{n/3}$ *is a square.*

(iii) *If* $F_n$ *is a square,* $n$ *is even and* $F_n$ *is also even, then show that* $12 \mid n$ *and that either* $F_{n/4}$ *or* $F_{n/12}$ *is a square.*

(iv) *If* $\gcd(n, 6) = 1$ *and* $F_n$ *is a square, show that* $n \equiv \pm 1 \pmod{12}$.

(v) *Assume* $n = 12m \pm 1 > 1$. *Use the formula* $2F_{m+n} = F_m L_n + F_n L_m$ *to conclude that* $F_n \equiv -1 \pmod{L_{2m}}$.

(vi) *Show that* $L_{2k}$ *is divisible by a prime number* $p \equiv 3 \pmod 4$ *for all* $k \geq 1$.

(vii) *Conclude from (i)–(vi) that* $F_0 = 0$, $F_1 = F_2 = 1$ *and* $F_{12} = 144$ *are the only square Fibonacci numbers.*

*Solution.* Assume that $F_n$ is odd. Then $n$ is not a multiple of 3. Moreover, $F_n = F_{n/2} L_{n/2}$ and $L_{n/2}^2 - 5_{n/2}^2 = \pm 4$. Since $F_n$ is odd, so are $F_{n/2}$ and $L_{n/2}$, and the above relation shows that they are coprime. Since their product is a square, each one of them is a square, which completes part (i).

For (ii), $2 \mid F_n$ so that $n$ is a multiple of 3. Write $n = 3m$, where $m$ is odd. One checks that $F_{3m} = F_m(5F_m^2 - 3)$, so that the greatest common divisor of $F_m$ and $5F_m^2 - 3$ is 1 or 3. But if $3 \mid F_m$, then $4 \mid m$ (one can check this by listing down a few of the residues of $\{F_n\}_{n \geq 0}$ modulo 3), and this is not possible because $m$ is odd. Thus, $F_m$ and $5F_m^2 - 3$ and coprime and their product is a square, so each of them is a square. In particular, $F_{n/3}$ is a square.

For (iii), note that since $F_n$ is even, $n$ is a multiple of 3. Since it is also a multiple of 2, it is a multiple of 6. One checks that $F_6 = 8$ and that $8 \| F_{6k}$ if $k$ is odd. This can be done by looking at the period of $\{F_n\}_{n \geq 0}$ modulo 16 (which is 24). Thus, $4 \mid n$ and $F_n = L_{n/2} L_{n/4} F_{n/4}$. Now $n/2$ is a multiple of 6, so that $L_{n/2}$ is 2 (mod 4). (This can be done by looking at the period of $\{L_n\}_{n \geq 1}$ modulo 4.) The greatest common divisor of $L_{n/2}$ and $F_{n/2}$ is 2, so that $F_{n/2} = 2u^2$. This gives $F_{n/4} L_{n/4} = 2u^2$. Therefore, either $F_{n/4}$ is a square or $L_{n/4}$ is a square. If $2 \mid (n/4)$, then $6 \mid (n/4)$ and again $2 \| L_{n/4}$, implying that the square must be $F_{n/4}$. Otherwise, $n/4$ is odd and $F_{n/4} = 2u^2$. Write $n/4 = 3m$, where $m$ is odd. Then $F_{n/4} = F_m(5F_m^2 - 3)$, as in a previous argument. Since $n/4$ is odd, $F_m$ and $5F_m^2 - 3$ are coprime. Thus, either $F_m$ is square, which is what we need, or $5F_m^2 - 3 = v^2$ is a square. But this last relation is impossible since upon reduction modulo 5 it leads to $(-3/5) = 1$, which is false. This takes care of (iii).

To summarize, if $F_n$ is a square and $n$ is not coprime to 6, then there is a divisor $d$ of $n$ of the form $n/2,\ n/3,\ n/4,\ n/12$ such that $F_d$ is a square. Reducing it in this way, we get to a square $F_n$, where we may assume that $n$ is coprime to 6. Then $F_n \equiv 1 \pmod 8$, and now looking at $(F_n)_{n \geq 0}$ modulo 8, one gets that $n = 12m \pm 1$. It follows that

$$2F_n = F_{12m} L_{\pm 1} + L_{12m} F_{\pm 1},$$

where we can extend the Fibonacci and Lucas sequences in the negative indices in the natural way. Let $12m = 2^\alpha t$ for some odd $t$ and look at $L_{2^{\alpha-1}}$. Obviously, $L_{2^{\alpha-1}} \mid F_{2^\alpha} \mid F_{12m}$. Moreover, $L_{12m} = L_{6m}^2 - 2$ and now one checks that since $6m/2^{\alpha-1}$ is odd, one has $L_{2^{\alpha-1}} \mid L_{6m}$. Thus, $L_{12m} \equiv -2 \pmod{L_{2^\alpha}}$. Since $F_{\pm 1} = 1$, we get that

$$2F_n \equiv -2 \pmod{L_{2^{\alpha-1}}},$$

and since $L_{2^{\alpha-1}}$ is odd, we get that $F_n \equiv -1 \pmod{L_{2^{\alpha-1}}}$. By induction, one proves that $L_{2^k}$ is congruent to 3 (mod 4) for all $k \geq 1$, so that $L_{2^{\alpha-1}}$ must have a prime factor $p \equiv 3 \pmod 4$. We thus get that $F_n \equiv -1 \pmod p$ and since $(-1/p) = -1$, $F_n$ cannot be a square. To conclude, we showed that if $(n, 6) = 1$ and $F_n$ is a square, then $n = 1$. Working now backwards through (i)–(iii), one gets the desired conclusion by checking $F_n$ for all divisors $n$ of 144. □

**Problem 13.8.** *Show that there are only finitely many positive integers $n$ such that $\phi^2(n) \mid n^2 - 1$. (Hint: Write $n^2 - d\phi(n)^2 = 1$ and let $k = \omega(n)$. Justify that $\sqrt{d} \ll \log k$. Compare $2^k$ to the power of 2 dividing $Y_1$, where $Y_1$ is the first solution of the Pell equation $X^2 - dY^2 = 1$. Use the fact that $\phi(n) = Y_\ell$ is a number divisible by $2^{k-1}$ to show that $\ell$ is divisible*

*by $2^{k+O((\log k)^2)}$. Conclude that all prime factors of $n$ are congruent to $\pm 1 \pmod{2^{k+O((\log k)^2)}}$ and then show that $\sqrt{d} \ll \exp(2^{-k+O((\log k)^2)})$. Deduce from this that both $d$ and $k$ are bounded. Then write $\ell = q_1 \cdots q_s$ with increasing primes $q_1 < \cdots < q_s$ and show by induction that each of the $q_i$'s is bounded.)*

*Solution.* First observe that

$$\sqrt{d} \asymp \frac{n}{\phi(n)} \le \prod_{p \le p_k} \left(1 + \frac{1}{p-1}\right) \ll \log k,$$

where $k = \omega(n)$ and $p_i$ is the $i$-th prime. This shows that $k > \exp(c_1\sqrt{d})$ for some constant $c_1 > 0$. From the size of the fundamental solution, we have that $\sqrt{d} \log d \gg \log X_1$, so that certainly $\sqrt{d} > (\log X_1)^{1/2}$. Thus, $\log X_1 < (\log k)^2$. Writing $Y_1 = 2^\alpha m$, where $m$ is odd, the above calculation shows that $\alpha = O((\log k)^2)$. Now it is known (and easy to prove by induction) that $2^\beta \mid Y_\ell/Y_1$ if and only if $2^\beta \mid \ell$. Thus, writing $n = Y_\ell$, since $2^{k+O((\log k)^2)} \mid (Y_\ell/Y_1)$, we get that $2^\beta \mid \ell$. Thus, $\ell \equiv 0 \pmod{2^{k+O((\log k)^2)}}$. But now every prime factor $p$ of $X_\ell$ is congruent to $\pm 1 \pmod{2^{k+O((\log k)^2)}}$. But then the sum of their reciprocals is

$$\sum_{p \mid X_\ell} \frac{1}{p} \ll \frac{k}{2^{k+O((\log k)^2)}}.$$

Since

$$\begin{aligned} \sqrt{d} &\le \left(1 + O\left(\frac{1}{X}\right)\right) \prod_{i=1}^{k} \left(1 + \frac{1}{p_i - 1}\right) \\ &\le \exp\left(\sum_{i=1}^{k} \frac{1}{p_i - 1}\right) = \exp\left(O\left(\frac{k}{2^{k+O((\log k)^2)}}\right)\right), \end{aligned}$$

we get immediately that both $k$ and $d$ are bounded. Since $k$ is bounded, the power of 2 in $\ell$ is bounded and $d(\ell)$ is bounded (by the Primitive Divisor theorem), implying that the number of prime factors of $\ell$ and their multiplicities is bounded. Now one uses induction to bound $q_1 < q_2 < \cdots < q_s$, the odd primes that divide $\ell$. Here is how this is done. Assume that $q_1 < \cdots < q_i$ are known but that $q_{i+1}$ is excessively large. Then let $u = q_1 \cdots q_i$ and $v = \ell/u$. Then $X_\ell = X_u(X_\ell/X_u)$, and $X_u$ and $X_\ell/X_u$ are coprime (if not, one can show that $\ell/u$ is divisible by some prime factor of $Y_u$). Thus,

$$X_u^2(X_\ell/X_u)^2 - \sqrt{d}\phi(X_u^2)\phi(X_\ell/X_u)^2 = 1.$$

Dividing this last inequality by $T^2 = (X_\ell/X_u)^2$, we obtain that

$$n_1^2 - d\phi(n_1)^2 \left(\frac{\phi(T)}{T}\right)^2 = \frac{1}{T^2},$$

where $n_1 = X_u$. Since $T$ has no small prime factors and has $O(1)$ prime factors, $T/\phi(T)$ tends to 1. Therefore, if the above relation holds with very large $T$, we must have that $n_1^2 = d\phi(n_1)^2$, which is impossible. It follows that knowledge of small prime factors $q_i$ of $\ell$ determines knowledge of all its prime factors. Hence, there are only finitely many such integers $n$. □

**Problem 13.10.** *Given positive integers $n$ and $k$, show that there exists a positive integer $m$ such that $\phi(m+i) \equiv 0 \pmod{n}$ for $i = 1, 2, \ldots, k$.*

*Solution.* From the Birkhoff-Vandiver theorem, it follows that we can choose primes $k < p_1 < \cdots < p_k$ which are all $\equiv 1 \pmod{n}$. Now use the Chinese Remainder Theorem to find $m$ such that $m \equiv -i \pmod{p_i}$ for $i = 1, \ldots, k$. It follows that $p_i \mid m+i$, which implies that $n \mid (p_i - 1) \mid \phi(m+i)$ for all $i = 1, \ldots, k$. □

**Problem 13.12.** *Show that the inequality $P(2^n - 1) > n \log n / \log\log n$ holds for almost all positive integers $n$. (Hint: Let $p$ be a primitive divisor of $2^n - 1$. If $p < n \log n / \log\log n$, then $kn + 1 = p$ is a prime for some $k < \log n / \log\log n$. Show, using the Brun sieve, that the number of such $n \le x$ is $o(x)$ as $x \to \infty$.)*

*Solution.* Any primitive divisor of $2^n - 1$ is a prime congruent to 1 $\pmod{n}$. Assume that it is $kn + 1$, where $k < n/\log n$. Let $x$ be large and let $n \in [x/\log x, x]$. Then $k < n/\log n < x/\log x$. Fix $k \le x/\log x$. Then $n \le x$ is such that $kn + 1$ is prime. But if $p = kn + 1$ is such a prime, then $p \le kx$ and $p \equiv 1 \pmod{k}$. Thus, the number of such primes $p$ is, by the Brun-Titchmarsh theorem, $\le \pi(kx; 1, k) \ll kx/(\phi(k)\log x)$. Summing this up for all $k \le \log x/\log\log x$, we get that the set of such $n \le x$ has cardinality

$$\ll \frac{x}{\log x} \sum_{k \le \log x/\log\log x} \frac{k}{\phi(k)} \ll \frac{x}{\log\log x} = o(x)$$

as $x \to \infty$. □

**Problem 13.14.** *Show that $Y_1 \mid Y_k$ for all $k \ge 1$ and that $Y_k/Y_1$ is a Lucas sequence corresponding to some pair of roots. What are the roots? Deduce that $Y_k$ has a prime factor $p \ge k - 1$ if $k > 31$.*

*Solution.* Letting $\alpha = (X_1 + \sqrt{d}Y_1)$ and $\beta = X_1 - \sqrt{d}Y_1$, we have that $X_k + \sqrt{d}Y_k = \alpha^k$ and $X_k - \sqrt{d}Y_k = \beta^k$. Thus, $X_k = (\alpha^k + \beta^k)/2$ and

$Y_k = (\alpha^k - \beta^k)/(2\sqrt{d})$. Since $\alpha - \beta = 2\sqrt{d}Y_1$, we get that $Y_k/Y_1 = (\alpha^k - \beta^k)/(\alpha - \beta)$. Thus, $Y_k/Y_1 = u_k$ is a Lucas sequence. In particular, by the Primitive Divisor theorem, $Y_k$ has a prime factor $p \geq k-1$ for all $k \geq 13$. □

## Solutions to problems from Chapter 14

**Problem 14.2.** *Show that if $p$ is an odd prime, then the Legendre symbol $\left(\frac{n}{p}\right)$ is a character modulo $p$. Then prove the following statements:*

(i) $\displaystyle\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right) = 0$ *if* $p \equiv 1 \pmod 4$;

(ii) $\displaystyle\sum_{\substack{1\leq r\leq p-1\\ \left(\frac{r}{p}\right)=1}} r = \frac{p(p-1)}{4}$ *if* $p \equiv 1 \pmod 4$;

(iii) $\displaystyle\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right) = p\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right)$ *if* $p \equiv 3 \pmod 4$;

(iv) $\displaystyle\sum_{r=1}^{p-1} r^3\left(\frac{r}{p}\right) = \frac{3p}{2}\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right)$ *if* $p \equiv 1 \pmod 4$;

(v) $\displaystyle\sum_{r=1}^{p-1} r^4\left(\frac{r}{p}\right) = 2p\sum_{r=1}^{p-1} r^3\left(\frac{r}{p}\right) - p^2\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right)$ *if* $p \equiv 3 \pmod 4$.

*Solution.* To prove that $\chi(n) = \left(\frac{n}{p}\right)$ is a character, there is not really much to show. The definition (12.29) shows that $\chi(n) \neq 0$ if and only if $n$ is coprime to $p$, and relation (13.2) shows that it has the multiplicativity property. We now prove (i)–(v). If $p \equiv 1 \pmod 4$, then $p - r$ is a quadratic residue whenever $r$ is a quadratic residue. Moreover, $r \neq p - r$, and there are precisely $(p-1)/2$ such quadratic residues. Thus, they can be grouped into $(p-1)/4$ disjoint sets of two elements $\{a, b\}$, for each of which we have $a + b = p$. This shows that

$$\sum_{\substack{1\leq r\leq p-1\\ \left(\frac{r}{p}\right)=1}} r = p\left(\frac{p-1}{4}\right),$$

thus establishing (ii). From (ii) and the fact that

$$\sum_{1\le r\le p-1} r = \frac{p(p-1)}{2} = 2p\left(\frac{p-1}{4}\right),$$

we get that

$$\sum_{\substack{1\le r\le p-1\\ \left(\frac{r}{p}\right)=-1}} r = \sum_{1\le r\le p-1} r - \sum_{\substack{1\le r\le p-1\\ \left(\frac{r}{p}\right)=1}} r = 2p\left(\frac{p-1}{4}\right) - p\left(\frac{p-1}{4}\right) = p\left(\frac{p-1}{4}\right),$$

so that clearly

$$\sum_{1\le r\le p-1} r\left(\frac{r}{p}\right) = \sum_{\substack{1\le r\le p-1\\ \left(\frac{r}{p}\right)=1}} r - \sum_{\substack{1\le r\le p-1\\ \left(\frac{r}{p}\right)=-1}} r = p\left(\frac{p-1}{4}\right) - p\left(\frac{p-1}{4}\right) = 0.$$

For (iii), we let $S$ be the desired sum and note that

$$\begin{aligned} S &= \sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right) = \sum_{r=1}^{p-1}(p-r)^2\left(\frac{p-r}{p}\right) \\ &= -\sum_{r=1}^{p-1}(p^2-2pr+r^2)\left(\frac{r}{p}\right) \\ &= -p^2\left(\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)\right) + 2p\left(\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right)\right) - \left(\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right)\right) \\ &= 2\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right) - S, \end{aligned}$$

leading to

$$2S = 2\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right),$$

which is equivalent to (iii). In the above equation we also used the fact that there are as many quadratic residues as non-quadratic residues, which means that

$$\sum_{r=1}^{p-1}\left(\frac{r}{p}\right) = 0. \tag{18.71}$$

For (iv), we let again $S$ be the desired sum and note that

$$\begin{aligned} S &= \sum_{r=1}^{p-1} r^3 \left(\frac{r}{p}\right) = \sum_{r=1}^{p} (p-r)^3 \left(\frac{p-r}{p}\right) \\ &= \sum_{r=1}^{p-1} (p^3 - 3p^2 r + 3pr^2 - r^3) \left(\frac{r}{p}\right) \\ &= p^3 \left(\sum_{r=1}^{p-1} \left(\frac{r}{p}\right)\right) - 3p^2 \left(\sum_{r=1}^{p-1} r \left(\frac{r}{p}\right)\right) \\ &\qquad +3p \left(\sum_{r=1}^{p-1} r^2 \left(\frac{r}{p}\right)\right) - \left(\sum_{r=1}^{p-1} r^3 \left(\frac{r}{p}\right)\right) \\ &= 3p \left(\sum_{r=1}^{p-1} r^2 \left(\frac{r}{p}\right)\right) - S, \end{aligned}$$

where we used (18.71) and (i) to conclude that the first two sums above are zero. Clearly, the above calculation shows that

$$2S = 3p \sum_{r=1}^{p-1} r^2 \left(\frac{r}{p}\right),$$

which is equivalent to (iv). Finally, (v) follows in the same way by noting that if $S$ is the given sum, then

$$\begin{aligned} S &= \sum_{r=1}^{p-1} r^4 \left(\frac{r}{p}\right) = \sum_{r=1}^{p-1} (p-r)^4 \left(\frac{p-r}{p}\right) \\ &= -\sum_{r=1}^{p-1} (p^4 - 4p^3 r + 6p^2 r^2 - 4pr^3 + r^4) \left(\frac{r}{p}\right) \\ &= -p^4 \left(\sum_{r=1}^{p-1} \left(\frac{r}{p}\right)\right) + 4p^3 \left(\sum_{r=1}^{p-1} r \left(\frac{r}{p}\right)\right) \\ &\qquad -6p^2 \left(\sum_{r=1}^{p-1} r^2 \left(\frac{r}{p}\right)\right) + 4p \left(\sum_{r=1}^{p-1} r^3 \left(\frac{r}{p}\right)\right) - S \\ &= 4p^3 \left(\sum_{r=1}^{p-1} r \left(\frac{r}{p}\right)\right) - 6p^2 \left(\sum_{r=1}^{p-1} r^2 \left(\frac{r}{p}\right)\right) + 4 \left(p \sum_{r=1}^{p-1} r^3 \left(\frac{r}{p}\right)\right) - S. \end{aligned}$$

From (iii), we know that $p$ times the first of the above sums equals the second of the above sums. Therefore, we get

$$2S = -2p^2 \left( \sum_{r=1}^{p-1} r^2 \left( \frac{r}{p} \right) \right) + 4p \left( \sum_{r=1}^{p-1} r^3 \left( \frac{r}{p} \right) \right),$$

which implies the desired relation. □

**Problem 14.4.** *For a character $\chi$ modulo $k$ and a positive integer $n$, let*

$$G(n, \chi) = \sum_{m=1}^{k} \chi(m) e^{2\pi i m n/k}.$$

*This is called the Gauss sum associated to $\chi$. Assume that $(n, k) = 1$.*

(i) *Show that*

$$G(n, \chi) = \overline{\chi}(n) G(1, \chi).$$

(ii) *Show that $|G(1, \chi)|^2 = p$, when $k = p$ is a prime. (Hint: Use the fact that $|z|^2 = z \cdot \overline{z}$ for any complex number $z$.)*

*Solution.* If $(n, k) = 1$, the numbers $nr$ run through a complete residue system as $r$ runs through a complete residue system. Also $|\chi(n)|^2 = \chi(n)\overline{\chi}(n) = 1$, so that

$$\chi(r) = \overline{\chi}(n)\chi(n)\chi(r) = \overline{\chi}(n)\chi(nr).$$

Thus, the sum $G(n, \chi)$ can be written as

$$\begin{aligned} G(n, \chi) &= \sum_{r \bmod k} \chi(r) e^{2\pi i n r/k} = \overline{\chi}(n) \sum_{r \bmod k} \chi(nr) e^{2\pi i (nr)/k} \\ &= \overline{\chi}(n) \sum_{r \bmod k} \chi(r) e^{2\pi i r/k} = \overline{\chi}(n) G(1, \chi), \end{aligned}$$

which takes care of (i). As for (ii), we have

$$\begin{aligned} |G(1, \chi)|^2 &= G(1, \chi)\overline{G}(1, \chi) = G(1, \chi) \sum_{r=1}^{p} \overline{\chi}(r) e^{-2\pi i r/p} \\ &= \sum_{r=1}^{p} \overline{\chi}(r) G(1, \chi) e^{-2\pi i r/p} \\ &= \sum_{r=1}^{p} G(r, \chi) e^{-2\pi i r/p} \\ &= \sum_{r=1}^{p} \sum_{m=1}^{p} \chi(m) e^{2\pi i m r/p} e^{-2\pi i r/p} \end{aligned}$$

$$= \sum_{m=1}^{p} \chi(m) \sum_{r=1}^{p} e^{2\pi i r(m-1)/p} = p\chi(1) = p,$$

since the last inner sum is geometric of ratio $e^{2\pi i(m-1)/p}$, implying that it vanishes when summed from 1 to $p$ unless $m = 1$, in which case it is equal to $p$. □

**Problem 14.6.** *Prove Polya's inequality to the effect that*

$$\left| \sum_{m \le x} \chi(m) \right| < \sqrt{k} \log k$$

*is valid for all primitive characters $\chi$ modulo $k$ and all $x \ge 1$. (Hint: Use the representation of $\chi$ given in Problem* 14.5 *to transform a sum into a double sum; then change the order of summation.)*

*Solution.* Express $\chi(m)$ as in Problem 14.5, namely

$$\chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k} \overline{\chi}(n) e^{-2\pi i m n/k}$$

and sum over all $m \le x$ to get

$$\sum_{m \le x} \chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k-1} \overline{\chi}(n) \sum_{m \le x} e^{-2\pi i m n/k},$$

where we used the fact that $\chi(k) = 0$. Taking absolute values and multiplying by $\sqrt{k}$, we obtain

$$\sqrt{k} \left| \sum_{m \le x} \chi(m) \right| \le \sum_{n=1}^{k-1} \left| \sum_{m \le x} e^{-2\pi i m n/k} \right| = \sum_{n=1}^{k} |f(n)|,$$

where

$$f(n) = \sum_{m \le x} e^{-2\pi i m n/k}.$$

Now $f(k-n) = \sum_{m \le x} e^{-2\pi i m(k-n)/k} = \sum_{m \le x} e^{2\pi i m n/k} = \overline{f(n)}$, so that $|f(k-n)| = |f(n)|$. Hence,

$$\sqrt{k} \left| \sum_{m \le x} \chi(m) \right| \le 2 \sum_{n < k/2} |f(n)| + |f(k/2)|,$$

the term $f(k/2)$ appearing only for even values of $k$. But $f(n)$ is a geometric sum of the form

$$f(n) = \sum_{m=1}^{r} y^m,$$

where $r = \lfloor x \rfloor$ and $y = e^{-2\pi i n/k}$. Here, $y \neq 1$ since $1 \leq n \leq k-1$. Writing $z = e^{-\pi i n/k}$, we have $y = z^2$ and $z^2 \neq 1$ when $n < k/2$. Hence, we have

$$f(n) = y\frac{y^r - 1}{y - 1} = z^2\left(\frac{z^{2r} - 1}{z^2 - 1}\right) = z^{r+1}\left(\frac{z^r - z^{-r}}{z - z^{-1}}\right),$$

so that

$$|f(n)| = \left|\frac{z^r - z^{-r}}{z - z^{-1}}\right| = \left|\frac{\sin(\pi r n/k)}{\sin(\pi n/k)}\right| \leq \frac{1}{\sin(\pi n/k)}.$$

Using the inequality $\sin t \geq 2t/\pi$, valid for all $0 \leq t \leq \pi/2$, with $t = \pi n/k$, one gets

$$|f(n)| \leq \frac{1}{(2/\pi)(\pi n/k)} = \frac{k}{2n}.$$

If $k$ is odd, the inequality becomes

$$\sqrt{k}\left|\sum_{m \leq x} \chi(m)\right| \leq k \sum_{n < k/2} \frac{1}{n} < k \log k,$$

where we used the fact that the inequality

$$\sum_{n < k/2} \frac{1}{n} < \log k$$

holds for all odd integers $k > 1$. But if $k$ is even, then $|f(k/2)| \leq 1$, so that the inequality is

$$\sqrt{k}\left|\sum_{m \leq x} \chi(m)\right| \leq k\left\{\sum_{n < k/2} \frac{1}{n} + \frac{1}{k}\right\} < k \log k,$$

implying that the desired inequality holds in this case as well, where, again, we used the fact that the inequality

$$\sum_{n < k/2} \frac{1}{n} + \frac{1}{k} < \log k$$

holds provided $k \geq 2$ is an even integer. □

**Problem 14.8.** *Use the examples of Chapter* 14 *to verify on a case-by-case basis that* $L(1, \chi) \neq 0$ *for all non-principal characters* $\chi$ *modulo* 3, 4, *and* 5.

*Solution.* When $\chi$ is non-principal modulo 3, the value of the $L$-series is

$$L(1,\chi) = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \cdots + \frac{1}{3k+1} - \frac{1}{3k+2} + \cdots$$

and since $1 > 1/2,\ 1/4 > 1/5$, etc., it is clear that the value of the sum is positive. Similarly, modulo 4, we have that

$$L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots + \frac{1}{4k+1} - \frac{1}{4k+3} + \cdots$$

is again positive. Finally, if $\chi$ is real modulo 5, we then get

$$L(1,\chi) = 1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{5k+1} - \frac{1}{5k+2} - \frac{1}{5k+3} + \frac{1}{5k+4} + \cdots$$

and certainly

$$\frac{1}{5k+1} - \frac{1}{5k+2} - \frac{1}{5k+3} + \frac{1}{5k+4} = \frac{1}{(5k+1)(5k+2)} - \frac{1}{(5k+3)(5k+4)} > 0$$

for all $k = 0, 1, \ldots$, so that $L(1,\chi) > 0$, while when $\chi$ is the character $\chi_1$ appearing on page 236, then the imaginary part of $L(1,\chi)$ is

$$\frac{1}{2} - \frac{1}{3} + \frac{1}{7} - \frac{1}{8} + \cdots + \frac{1}{5k+2} - \frac{1}{5k+3},$$

which is a positive number and therefore nonzero (and $L(1,\chi_3) = \overline{L(1,\chi_1)}$). □

**Problem 14.10.** *Use the Brun sieve to show that the set* $\{n : \phi(n) \not\equiv 0 \pmod{k}\}$ *is of asymptotic density zero. (Hint: Let* $\mathcal{P}$ *be the set of primes* $p \equiv 1 \pmod{k}$*. Use the Brun sieve to show that the set of integers* $n \le x$ *with* $\phi(n) \not\equiv 0 \pmod{k}$ *is contained in the set of integers* $n \le x$ *which are not divisible by any* $p \in \mathcal{P}$ *and that the number of such integers is* $\ll x \prod_{p\in\mathcal{P}}(1 - 1/p)$*. Finally, use estimate* (14.15) *to conclude.)*

*Solution.* Let $x$ be large, $y = x^u$, where $u$ is sufficiently small and let $\mathcal{P}$ be the set of primes $p \le y$, $p \equiv 1 \pmod{k}$. If $\phi(n) \not\equiv 0 \pmod{k}$, then certainly $n$ is not divisible by any prime in $\mathcal{P}$, since otherwise if $n$ were a multiple of such a prime $p$, then $k \mid (p-1) \mid \phi(n)$. Thus, $n \le x$ is contained in the set of those positive integers $n \le x$ free of primes $p \in \mathcal{P}$. By the Brun sieve with $w(p) = 1$ for $p \in \mathcal{P}$ and $w(p) = 0$ otherwise, we get that the number of such integers $n$ is

$$\ll\ x \prod_{\substack{p\in\mathcal{P}\\ p\le y}} \left(1 - \frac{1}{p}\right) = x \exp\left(\sum_{\substack{p\in\mathcal{P}\\ p\le y}} \log\left(1 - \frac{1}{p}\right)\right)$$

$$= \quad x \exp\left( -\sum_{\substack{p\in\mathcal{P}\\ p\le y}} \frac{1}{p} + O\left(\sum_{p\ge 2} \frac{1}{p^2}\right)\right) = x\exp\left( -\sum_{\substack{p\in\mathcal{P}\\ p\le y}} \frac{1}{p} + O(1)\right).$$

As $x \to \infty$, we have that $y = x^u$ also tends to infinity, so that

$$\sum_{\substack{p\in\mathcal{P}\\ p\le y}} \frac{1}{p} = \sum_{p\equiv 1 \pmod k} \sum_{\substack{\\ p\le y}} \frac{1}{p}$$

tends to infinity. We conclude that the count on our $n \le x$ is $o(x)$ as $x \to \infty$, which is what we wanted to prove. □

**Problem 14.12.** *Show that the density of the set of positive integers $n$ for which $F_n$ has a prime factor $p \equiv 3 \pmod 4$ is equal to $1/2$. Here, $F_n$ is the $n$-th Fibonacci number. (Hint: Show first that the set in question does not contain any odd number. Problem* 13.4 *is relevant here. Thus the density of the set in question is at most $1/2$. To show that it is $1/2$, let $n = 2m$ be an even number. If $p \mid m$ and $p \equiv 2 \pmod 3$, then $2p \mid 2m$ and $2p \equiv 4 \pmod 6$. Now $F_{2p} \mid F_n$. Justify that $F_{2p} \equiv 3 \pmod 4$, so that $F_{2p}$ has a prime factor $q \equiv 3 \pmod 4$. Conclude that if $n$ has a prime factor $p \equiv 2 \pmod 3$ and it is even, then $F_n$ has a prime factor $q \equiv 3 \pmod 4$. To justify that most even numbers have a prime factor $p \equiv 2 \pmod 3$, use the Brun sieve as in Problem* 14.10*, together with the fact that the sum of the reciprocals of all the primes $p \equiv 2 \pmod 3$ is divergent.)*

*Solution.* We already know that if $n \ge 5$ is prime, then every prime factor of $F_n$ is congruent to 1 modulo 4. It follows that the set of integers $n$ such that $F_n$ has a prime factor $p \equiv 3 \pmod 4$ is contained in the set of even numbers. Let $n = 2m$ be an even number. Let $p \equiv 2 \pmod 3$ be an odd prime. If $p \mid n$, then $2p \mid n$ so that $F_{2p} \mid F_n$. The sequence $\{F_\ell\}_{\ell\ge 1}$ is periodic modulo 4 with period six and since $2p \equiv 4 \pmod 6$, we get that $F_{2p} \equiv F_4 \pmod 4 \equiv 3 \pmod 4$. This shows that $F_{2p}$ has a prime factor $q$ such that $q \equiv 3 \pmod 4$. Thus, $F_n$ has a prime factor $q \equiv 3 \pmod 4$ provided that $n$ has a prime factor which is 2 modulo 3. Therefore, it suffices to show that the set of integers $n$ having no prime factor $\equiv 2 \pmod 3$ is of asymptotic density zero. Using the Brun sieve, if $x$ is large, $u > 0$ is sufficiently small (but absolute), and $\mathcal{P}$ is the set primes $p \equiv 2 \pmod 3$, we may conclude that the number of positive integers $n \le x$ such that $n$ is not a multiple of

any prime $p \in \mathcal{P} \cap [1, y]$ with $y = x^u$ is

$$\ll x \prod_{\substack{p \in \mathcal{P} \\ p \le y}} \left(1 - \frac{1}{p}\right) \ll x \exp\left(- \sum_{\substack{p \equiv 2 \pmod 3 \\ p \le y}} \frac{1}{p} + O(1)\right),$$

and this last expression is $o(x)$ as $x \to \infty$, since

$$\sum_{\substack{p \equiv 2 \pmod 3 \\ p \le y}} \frac{1}{p} \to \infty \qquad \text{as} \qquad x \to \infty,$$

which completes the solution. □

## Solutions to problems from Chapter 15

**Problem 15.2.** *Show, using the Linnik theorem, that there is a constant $c > 0$ such that for infinitely many primes $p$, all numbers $\le c \log p$ are quadratic residues modulo $p$. (Hint: Fix $x$. For each odd prime $q \le x$, let $a_q$ be a quadratic residue modulo $q$. Then, let $p \equiv 1 \pmod 8$ and $p \equiv a_q \pmod q$. Show, using the Quadratic Reciprocity Law, that $q$ is a quadratic residue modulo $p$ for all $q \le x$. Now use the Linnik theorem to bound $p$ in terms of $x$.)*

*Solution.* Let $x$ be large. Let $q_1 < q_2 < \cdots < q_k$ be all the primes $q \le \log x$. Let $p$ be a prime such that $p \equiv 1 \pmod 8$ and $p \equiv 1 \pmod{q_i}$ for all $i = 2, \ldots, k$. Then $(p/q_i) = (1/q_i) = 1$ for all $i = 2, \ldots, k$. By the Quadratic Reciprocity Law and the fact that $p \equiv 1 \pmod 4$, we get that $(q_i/p) = 1$ for all $i = 2, \ldots, k$. The same is true for $i = 1$ since $p \equiv 1 \pmod 8$, and this is why $(2/p) = 1$. Now if $n \le \log x$, then $n = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ for some nonnegative integers $\alpha_1, \ldots, \alpha_k$. Since $(q_i/p) = 1$ for $i = 1, \ldots, k$, we get that $\prod_{i=1}^k (q_i^{\alpha_i}/p) = 1$, so that $(n/p) = 1$. Thus, all $n \le \log x$ are quadratic residues modulo $p$. Now $p \equiv 1 \pmod M$, where $M = 8 \prod_{i=2}^k q_i = 4 \prod_{q \le \log x} q = \exp((1 + o(1)) \log x) < x^2$ for large values of $x$. By the Linnik theorem, we may choose $p < x^{2L}$, so that $\log p < 2L \log x$. Writing $c_1 = 1/(2L)$, we get that all numbers $n \le c_1 \log p$ are quadratic residues modulo $p$, which is what needed to be shown. □

**Problem 15.4.** *Show, using the Bombieri-Vinogradov theorem and the Siegel-Walfisz theorem, that*

$$\omega(\sigma(n!)) \gg n^{1/2 + o(1)}$$

*as $n \to \infty$. (Hint: Use the Bombieri-Vinogradov theorem to obtain that there exists a number $B$ such that the primes $q < n^{1/2}/(\log n)^B$ which do not divide $p+1$ for any prime $p \in (n/2, n)$ have the property that the sum of their reciprocals is $< 1$. Then use the Siegel-Walfisz theorem to conclude that each one of these primes is $> (\log n)^{B+2}$ for large $n$. Deduce that the number of such primes is $\ll n^{1/2}/(\log n)^{B+2} = o(\pi(n^{1/2}/(\log n)^B))$ as $n \to \infty$.)*

*Solution.* Let $A = 3$, $B$ be the corresponding constant for $A$ in the Bombieri-Vinogradov theorem, and $\mathcal{Q}$ be the set of primes $\le n^{1/2}/(\log n)^B$ such that there exists a prime $p \in (n/2, n]$ with $q \mid p+1$. Note that since $p \in (n/2, n]$, we have that $p \| n!$ so that $(p+1) \mid \sigma(n!)$, which implies that $q \mid \sigma(n!)$. Thus, $\omega(\sigma(n!)) \ge \#\mathcal{Q}$. To estimate $\#\mathcal{Q}$, we look at the primes $q_1 \notin \mathcal{Q}$. Applying the Bombieri-Vinogradov theorem with $n$ and then $n/2$, we get

$$\sum_{q \le n^{1/2}/(\log n)^B} \left| \pi(n; -1, q) - \frac{\pi(n)}{\phi(q)} \right| \ll \frac{n}{(\log n)^3}$$

and

$$\sum_{q \le n^{1/2}/(\log n)^B} \left| \pi(n/2; -1, q) - \frac{\pi(n/2)}{\phi(q)} \right| \ll \frac{n}{(\log n)^3}.$$

Hence,

$$\sum_{q \le n^{1/2}/(\log n)^B} \left| (\pi(n; -1, q) - \pi(n/2; -1, q) - \frac{\pi(n) - \pi(n/2)}{\phi(q)} \right| \ll \frac{n}{(\log n)^3}.$$

If $q \notin \mathcal{Q}$, then $\pi(n; -1, q) - \pi(n/2; -1, q) = 0$, so that the above inequality implies in particular that

$$\sum_{\substack{q \le n^{1/2}/(\log n)^B \\ q \notin \mathcal{Q}}} \left| \frac{\pi(n) - \pi(n/2)}{\phi(q)} \right| \ll \frac{n}{(\log n)^3},$$

and since $\pi(n) - \pi(n/2) \gg n/\log n$, while $\phi(q) = q - 1 \asymp q$, we get that

$$\sum_{\substack{q \le n^{1/2}/(\log n)^B \\ q \notin \mathcal{Q}}} \frac{1}{q} \ll \frac{1}{(\log n)^2}.$$

Thus,

$$\sum_{\substack{q \le n^{1/2}/(\log n)^B \\ q \notin \mathcal{Q}}} \frac{n^{1/2}}{q(\log n)^B} \ll \frac{n^{1/2}}{(\log n)^{B+2}}.$$

Since each of the numbers $n^{1/2}/(q(\log n)^B)$ on the left-hand side above is $> 1$, we get that

$$\#\{q \le n^{1/2}/(\log n)^B : q \notin \mathcal{Q}\} \ll \frac{n^{1/2}}{(\log n)^{B+2}} = o(\pi(n^{1/2}/(\log n)^B))$$

as $n \to \infty$. Thus,

$$\pi(n^{1/2}/(\log n)^B) - \#\mathcal{Q} = o(\pi(n^{1/2}/(\log n)^B)) \qquad \text{as } n \to \infty,$$

so that

$$\#\mathcal{Q} = (1 + o(1))\pi(n^{1/2}/(\log n)^B) = n^{1/2+o(1)} \qquad \text{as } n \to \infty,$$

which implies the desired conclusion. □

**Problem 15.6.** *Show that $\sigma(\sigma(n))/n$ is dense in $[1, \infty)$. (Hint: First show that $\sigma(m)/m$ is dense in $[1, \infty)$ as $m$ runs through numbers all of whose prime factors are $\equiv 1 \pmod 3$. Then show that for each such $m$, there exists a residue class $p_0 \pmod m$ such that $p_0^2 + p_0 + 1 \equiv 0 \pmod m$. Use the Chinese Remainder Theorem and the Linnik theorem to show that if $x$ is large, then there exists such a prime $p$ on the scale of $x^{O(1)}$ such that $m \mid (p^2+p+1)$ with $(p^2+p+1)/m$ being free of primes $q = O(\log x)$. Deduce that $\sigma(p^2) = ma$, where $a$ is free of small primes. Deduce furthermore that $\sigma(\sigma(p^2)) = \sigma(m)\sigma(a) = \sigma(m)(a + o(1))$ and therefore that $\sigma(\sigma(p^2))/p^2 = (1 + o(1))\sigma(m)/m$.)*

*Solution.* We follow the hint. Let $\mathcal{P}$ be the set of all primes $\equiv 1 \pmod 3$. Since $\sum_{p\in\mathcal{P}} \frac{1}{p}$ diverges, it follows that $\sum_{p\in\mathcal{P}} \log\left(1 + \frac{1}{p}\right)$ diverges as well. A straightforward adaptation of Proposition 8.9 tells us that every number can be approximated arbitrarily well by numbers of the form $\prod_{p\in S}(p+1)/p = \sigma(m_S)/m_S$, where $m_S = \prod_{p\in S} p$ as $S$ runs through finite subsets of $\mathcal{P}$. Now let $m$ be a squarefree number as above. Let $q \mid m$. The congruence $p^2 + p + 1 \equiv 0 \pmod q$ is equivalent to $(2p+1)^2 \equiv -3 \pmod q$. Note that since $q \equiv 1 \pmod 3$, we get that $(-3/q) = (-1)^{(q-1)/2}(3/q) = (-1)^{(q-1)/2}(q/3)(-1)^{(3-1)/2\cdot(q-1)/2} = (q/3) = 1$, and this is why there exists $p_q \pmod q$ such that $p_q^2 + p_q + 1 \equiv 0 \pmod q$. Note that $p_q \not\equiv 0 \pmod q$ since otherwise we would get $1 \equiv 0 \pmod q$, which is false. Now note that $(p_q^2 + p_q + 1)/q$ is coprime to $q$. To see this, note that $p_q < q$, and therefore that $p_q^2+p_q+1 \le (q-1)^2+(q-1)+1 = q^2-q+1 < q^2$, so that $(p_q^2+p_q+1)/q$ is a positive integer $< q$. Since $q$ is prime, $(p_q^2 + p_q + 1)/q$ is not a multiple of $q$. Now let $x$ be large. For each prime $q \le \log x$ congruent to 1 modulo 3, let $p \equiv p_q \pmod{q^2}$ if $q \mid m$, and $p \equiv 1 \pmod q$ otherwise. Let also $p \equiv 2 \pmod 3$. Then $p^2 + p + 1$ is a multiple of $m$ and $(p^2 + p + 1)/m$ is free of

primes $q \le \log x$. Indeed, to see this, observe that by the calculation with the above Legendre symbols, the only primes $q$ that can divide $p^2+p+1$ are $q = 3$ (which is not the case since $p \equiv 2 \pmod 3$, and therefore $p^2+p+1 \equiv 1 \pmod 3$), or $q \mid m$, in which case $p^2+p+1 \equiv p_q^2+p_q+1 \pmod{q^2}$, so that $(p^2+p+1)/q$ is an integer coprime to $q$. Finally, if $q$ does not divide $m$, then $p^2+p+1 \equiv 3 \pmod q$, so that $p^2+p+1$ is not a multiple of such primes $q$. Thus, if $p$ is in the above arithmetical progression, then $(p^2+p+1)/m$ is an integer free of primes $\le \log x$.

Now the ratio of the progression is

$$M = 3\prod_{q\mid m} q^2 \prod_{\substack{q\le \log x, q\nmid m \\ q\equiv 1 \pmod 3}} q \le \prod_{q\le \log x} q^2 < e^{4\log x} = x^4$$

for large values of $x$. Hence, by Linnik's theorem, $p \ll x^{4L}$, and therefore $p^2+p+1 \ll x^{8L}$. Thus, $\omega(p^2+p+1) \ll \log x/\log\log x$. Hence, $p^2+p+1 = ma$, where the smallest prime in $a$ exceeds $\log x$ and the number of primes in $a$ is at most $O(\log x/\log\log x)$. Thus,

$$\sigma(\sigma(p^2)) = \sigma(p^2+p+1) = \sigma(m)\sigma(a),$$

so that

$$\frac{\sigma(\sigma(p^2))}{p^2} = \frac{p^2+p+1}{p^2}\cdot\frac{\sigma(p^2+p+1)}{p^2+p+1} = (1+o(1))\frac{\sigma(m)}{m}\frac{\sigma(a)}{a}.$$

Now,

$$1 \le \frac{\sigma(a)}{a} \le \prod_{p\mid a}\left(1+\frac{1}{q-1}\right) \le \left(1+\frac{1}{\log x}\right)^{O(\log x/\log\log x)} = 1+o(1).$$

Thus,

$$\frac{\sigma(\sigma(p^2))}{p^2} = (1+o(1))\frac{\sigma(m)}{m}.$$

Since we have established that $\sigma(m)/m$ is dense in $[1,\infty)$ when $m$ runs through squarefree integers built up from primes $q \equiv 1 \pmod 3$, the problem is solved. □

**Problem 15.8.** *Show that there exists a constant $c_0 > 0$ such that for large $x$, the cardinality of the set of positive integers $n \le x$ such that $n^2+1$ is squarefree is $c_0(1+o(1))x$ as $x \to \infty$.*

*Solution.* Let $f(X) = X^2+1$ and let $\rho(d)$ be the function defined by

$$\rho(d) = \#\{0 \le n \le d-1 \ : \ f(n) \equiv 0 \pmod d\}.$$

Thus, $\rho(d) = \#\{0 \le k \le d-1 : k^2+1 \equiv 0 \pmod{d}\}$. We know that $\rho$ is multiplicative. If $p \equiv 3 \pmod 4$, then $\rho(p) = 0$, because there can be no integer $k$ such that $k^2 \equiv -1 \pmod p$ for such primes $p$. When $p = 2$, we have that $\rho(p) = \rho(2) = 1$. Finally, $\rho(p) = 2$ if $p \equiv 1 \pmod 4$ (namely, there exists $k$ such that $k^2+1 \equiv 0 \pmod p$ and if $k$ has this property so does $p-k$ and $p-k \not\equiv k \pmod p$). We now note that $\rho(4) = 1$ (there is no odd $k$ such that $k^2+1$ is a multiple of 4) and if $p \equiv 1 \pmod 4$, then $\rho(p^2) = 2$. Indeed, let $k \pmod p$ be such that $k^2+1 = 0 \pmod p$. Fix $k \in \{0, 1, \ldots, p-1\}$. Note that $k \ne 0$. Let $u = k + tp$. Then $u^2+1 \equiv (k^2+1) + 2ktp = p((k^2+1)/p + 2kt) \pmod{p^2}$. Thus, $p^2 \mid u^2+1$ only when $t$ is such that $t \equiv (2k)^{-1}(k^2+1)/p \pmod p$. This is true for each of the two solutions $k \pmod p$ of the congruence $k^2+1 \equiv 0 \pmod p$. We are now ready to give the argument. Let $x$ be large and $z = (\log x)/5$.

Set

$$P = \prod_{\substack{p \le z \\ p \equiv 1 \pmod 4}} p.$$

Let $d \mid P$. Note that $P \le \prod_{p \le z} p \le \exp(2z) = x^{2/5}$, so that $P^2 < x^{4/5} < x$. The number of $n \le x$ such that $n^2+1 \equiv 0 \pmod{d^2}$ is, by the Chinese remainder theorem,

$$\rho(d)(\lfloor x/d^2 \rfloor + 1) = x\rho(d)/d^2 + O(2^{\omega(d)}) = x2^{\omega(d)}/d^2 + O(2^{\pi(z)}).$$

By the Inclusion-Exclusion principle, the number of $n \le x$ such that $n^2+1$ is not a multiple of $q^2$ for any $q \mid P$ is

$$\begin{aligned} &= \sum_{d \mid P} \mu(d) \frac{x2^{\omega(d)}}{d^2} + O(d(P)2^{\pi(z)}) \\ &= x\left(\prod_{\substack{p \equiv 1 \\ (\mathrm{mod}\ 4)}} \left(1 - \frac{2}{p^2}\right) + o(1)\right) + O(2^{4\pi(z)}) \\ &= (c_1 + o(1))x \end{aligned}$$

as $x \to \infty$, where

$$c_1 = \prod_{\substack{p \equiv 1 \\ (\mathrm{mod}\ 4)}} \left(1 - \frac{1}{p^2}\right).$$

We now look at the number of $n \le x$ such that $q^2 \mid n^2+1$ for some prime $q \in [z, \sqrt{x}\log\log x]$. For a fixed $q$, the number of such $n \le x$ is $\le 2(x/q^2 + 1) \le 2(\log\log x)^2 x/q^2$. Thus, the number of such $n \le x$ is

$$x(\log\log x)^2 \sum_{q \ge z} \frac{1}{q^2} \ll \frac{x(\log\log x)^2}{z} \ll \frac{x(\log\log x)^2}{\log x} = o(x)$$

as $x \to \infty$. Finally, if $q > x^{1/2} \log\log x$, then $n^2 + 1 = q^2\lambda$, where $\lambda \ll x/(\log\log x)^2$. Fix $\lambda$. Assume that the equation $n^2 - \lambda q^2 = -1$ has a prime solution $q$. Then $(n, q)$ is a solution of the Pell equation $X^2 - \lambda Y^2 = -1$. Since $q$ is prime, we get that either the first solution has $Y_1 = 1$, so that $X_1 = \lambda - 1$, or $Y_1 = q$. If $Y_1 = q$, then $X_1 = n$ so $(n, q)$ is the first solution of the Pell equation. The number of such $n$'s is therefore at most the number of $\lambda$'s, so $O(x/(\log\log x)^2) = o(x)$ as $x \to \infty$. Finally, if $Y_1 = 1$, then $\lambda - 1$ is a square and the number of such $\lambda$'s is $\ll x^{1/2}$. For each one of them, $n = (\alpha^t - \beta^t)/(\alpha - \beta)$, where $\alpha = \sqrt{\lambda - 1} + \sqrt{\lambda}$ and $\beta = \sqrt{\lambda - 1} - \sqrt{\lambda}$, and $\lambda \geq 2$. For each fixed $\lambda$, the number of $t$'s such that $n \leq x$ is $\ll \log x / \log\alpha \ll \log x$. So the number of $n \leq x$ in this last instance is $O(\sqrt{x}\log x) = o(x)$ also as $x \to \infty$. Thus, the proportion of positive integers $n \leq x$ such that $n^2 + 1$ is squarefree is equal to

$$\prod_{p \equiv 1 \pmod 4} \left(1 - \frac{2}{p^2}\right).$$

□

**Problem 15.10.** *Prove that there exists a constant $c_2 > 0$ such that*

$$\sum_{p \leq x} d(p-1) = c_2(1 + o(1))x \qquad \text{as } x \to \infty.$$

*Solution.* Note first that

$$\sum_{p \leq x/(\log x)^2} d(p-1) \leq \sum_{n \leq x/(\log x)^2 + 1} d(n) \ll \log x \left(\frac{x}{(\log x)^2}\right) \ll \frac{x}{\log x} = o(x)$$

as $x \to \infty$ by Theorem 4.9. Thus, we may look only at the primes $p \geq x/(\log x)^2 + 1$. We let $B > 2$ to be determined later. Let $y = x^{1/2}/(\log x)^B$ and let $d_1(p-1) = \{d \mid p - 1 : d \leq y\}$. Note that since $B > 1$, we have that $p - 1 \geq x/(\log x)^2 > y^2$, so that $d(p-1) = 2d_1(p-1) + d_2(p-1)$, where $d_2(p-1) \leq 2\#\{d \mid p - 1 : y \leq d \leq x^{1/2}\}$. Thus,

$$\begin{aligned}
\sum_{y \leq p \leq x} d(p-1) &= \sum_{y \leq p \leq x} 2d_1(p-1) + d_2(p-1) \\
&= \sum_{y \leq p \leq x} \left(2 \sum_{\substack{d \mid p-1 \\ d \leq y}} 1 + O\left(\sum_{\substack{y \leq d \leq x^{1/2} \\ d \mid p-1}} 1\right)\right)
\end{aligned}$$

$$\begin{aligned} &= 2\sum_{d\le y}\sum_{\substack{p\le x\\ p\equiv 1 \pmod d}} 1 + O\left(\sum_{y\le d\le x^{1/2}}\sum_{\substack{p\le x\\ p\equiv 1 \pmod d}} 1\right) \\ &\qquad +O(x/\log x) \\ &= 2\sum_{d\le y}\pi(x;1,d) + O\left(\sum_{y\le d\le x^{1/2}}\pi(x;1,d)\right) + O(x/\log x). \end{aligned}$$

By the Brun-Titchmarsh theorem, the first error above is

$$\sum_{y\le d\le x^{1/2}}\pi(x;1,d) \ll \sum_{y\le d\le x^{1/2}}\frac{x}{\phi(d)\log(x/d)} \ll \frac{x}{\log x}\sum_{y\le d\le x^{1/2}}\frac{1}{\phi(d)}.$$

Using $1/\phi(d) \ll (\log\log x)/d$ (see Proposition 8.4), we get that the above sum is

$$\begin{aligned} &\ll \frac{x\log\log x}{\log x}\sum_{y\le d\le x^{1/2}}\frac{1}{d} \ll \frac{x\log\log x}{\log x}\left(1+\int_y^{x^{1/2}}\frac{1}{t}\right) \\ &\ll \frac{x\log\log x}{\log x}\left(1+\log\left(\frac{x^{1/2}}{y}\right)\right) \ll \frac{x(\log\log x)^2}{\log x} = o(x) \end{aligned}$$

as $x\to\infty$. Finally, for the main term, we write $\pi(x;1,d) = \pi(x)/\phi(d) + E(x,d)$ and get that

$$2\sum_{d\le y}\pi(x;1,d) = 2\sum_{d\le y}\frac{\pi(x)}{\phi(d)} + O\left(\sum_{d\le y}|E(x,d)|\right).$$

By the Bombieri-Vinogradov theorem, we may choose $B$ in such a way that the above error is $O(x/\log x)$ (that is, take $A=1$ in the Bombieri-Vinogradov theorem). The sum is therefore

$$2\pi(x)\sum_{d\le y}\frac{1}{\phi(d)} + O(\pi(x)).$$

Thus, it suffices to show that

$$\sum_{d\le y}\frac{1}{\phi(d)} = (c_2+o(1))\log y,$$

which is precisely what was shown in Problem 8.8 with $c_2 = \dfrac{\zeta(2)\zeta(3)}{\zeta(6)}$. □

**Problem 15.12.** *Use the argument from the proof of Proposition* 15.13*, taking into account Remark* 15.14*, to show that if $x$ is large, then $\sigma(n)$ is a*

*multiple of all the prime powers $p^a < f(x)$ for all $n \le x$ with at most $o(x)$ exceptions as $x \to \infty$.*

*Solution.* Let $z = \log x$. The number of $n \le x$ such that $p^2 \mid n$ for some $p \ge z$ is at most

$$\sum_{p \ge z} \frac{x}{p^2} \ll x \int_z^\infty \frac{dt}{t^2} = \frac{x}{z} = o(x)$$

as $x \to \infty$. Hence, from now on, we work with $n \le x$ such that $p^2$ is not a divisor of $n$ for any $p \ge z$. Modify the definition of $\mathcal{A}_q(x)$ to

$$\mathcal{A}_q(x) = \{n \le x : n \text{ is not a multiple of any prime } p > z,\ p \equiv -1 \pmod q\}.$$

It suffices to show that

$$\sum_{q \le f(x)} \#\mathcal{A}_q(x) = o(x) \qquad \text{as } x \to \infty.$$

Let $\mathcal{P}$ consist of the primes $p \equiv -1 \pmod q$ in $[z, y]$, where $z = \log x,\ y = x^u$. The number of $n \in \mathcal{A}_q$ is, by the Brun sieve,

$$\ll x \prod_{\substack{z \le p \le y \\ p \equiv -1 \pmod q}} \left(1 - \frac{1}{p}\right) \ll x \exp\left(- \sum_{\substack{z \le p \le y \\ p \equiv -1 \pmod q}} \frac{1}{p}\right).$$

Since $q \le f(x) = O(\log_2 x) = O(\log z)$, it follows, by the Siegel-Walfisz theorem, that

$$\sum_{\substack{z \le p \le y \\ p \equiv -1 \pmod q}} \frac{1}{p} = \frac{\log\log y - \log\log z}{\phi(q)} + O(1) > \frac{\log\log x}{2q},$$

uniformly for large $x$ if $q < \log\log x/(2\log\log\log x)$. Thus,

$$\#\mathcal{A}_q(x) \ll x \exp\left(-\frac{\log_2 x}{2\log_2 x/(2\log_3 x)}\right) = \frac{x}{\log_2 x}.$$

Therefore,

$$\sum_{q \le f(x)} \#\mathcal{A}_q(x) \ll \frac{x f(x)}{\log_2 x} = \frac{x}{\log_3 x} = o(x)$$

as $x \to \infty$, which is what we needed to show. □

**Problem 15.14.** *Prove that there exists some function $g : \mathbb{R}_+ \to \mathbb{R}_+$ with $\lim_{x\to\infty} g(x) = \infty$ such that inequality $\sigma(\phi(n))/n > g(n)$ holds for almost all $n$. (Hint: Use the result of Proposition* 15.13*, taking into account Remark* 15.14.*)*

*Solution.* Let $f(x) = c\log_2 x/\log_3 x$ be the function such that for most $n$, $\phi(n)$ is a multiple of all the primes $p \le f(n)$. Hence, for most $n$,

$$\frac{\sigma(\phi(n))}{\phi(n)} \ge \prod_{p\le f(n)} \left(1+\frac{1}{p}\right) \gg \log(f(n)) \gg \log_3 n.$$

We now show that $\{n \le x : n/\phi(n) > \log_4 x\}$ has cardinality $o(x)$ as $x \to \infty$. Indeed, we know that

$$\sum_{n\le x} \frac{n}{\phi(n)} \ll \sum_{n\le x} \frac{\sigma(n)}{n} \ll x.$$

If $A = \#\{n \le x : n/\phi(n) > \log_4 x\}$, the above inequality tells us that $A \cdot f(x) \ll x$, so that $A \ll x/\log_4 x = o(x)$ as $x \to \infty$. Hence, indeed for most positive integers $n$ we have that $n/\phi(n) < \log_4 n$. Thus, for most $n$,

$$\frac{\sigma(\phi(n))}{n} = \frac{\sigma(\phi(n))}{\phi(n)} \cdot \frac{\phi(n)}{n} \gg \frac{\log_3 n}{\log_4 n},$$

so we can take $g(x) = \log_3 x/\log_4 x$. □

**Problem 15.16.** *For most $n$, which one is larger, $\phi(\sigma(n))$ or $\sigma(\phi(n))$ ?*

*Solution.* For most $n$, both $\sigma(n)$ and $\phi(n)$ are multiples of all primes $p < c\log_2 n/\log_3 n$. Hence,

$$\frac{\sigma(\phi(n))}{\phi(n)} \ge \prod_{p\le c\log_2 n/\log_3 n} \left(1+\frac{1}{p}\right) \gg \log(c\log_2 n/\log_3 n) \gg \log_3 n,$$

where in the above inequalities we used Problem 4.5. Similarly,

$$\frac{\phi(\sigma(n))}{\sigma(n)} \le \prod_{p\le c\log_2 n/\log_3 n} \left(1-\frac{1}{p}\right) \ll \frac{1}{\log_3 n}.$$

Thus, $\sigma(\phi(n))$ has increased the amount $\phi(n)$ by at least $\log_3 n$ and $\phi(\sigma(n))$ has lowered $\sigma(n)$ by at least $\log_3 n$. However, $\phi(n)$ and $\sigma(n)$ have *decreased* and *increased* $n$, respectively. We now show that these increments are very small for most $n$. One can show that if $f(x)$ is any function tending to infinity with $x$, then $\#\{n \le x : \sigma(n)/n > f(x)\} = o(x)$ as $x \to \infty$. Indeed, we know that

$$\sum_{n\le x} \sigma(n)/n \ll x.$$

Thus, if $A$ is the number of positive integers $n \le x$ such that $\sigma(n)/n > f(x)$, the above inequality tells us that $A \cdot f(x) \ll x$, so that $A \ll x/f(x)$. Thus, the number of such integers $n \le x$ is $o(x)$ as $x \to \infty$. The same is true for $\#\{n \le x : n/\phi(n) > f(x)\}$ because $n\phi(n) \asymp \sigma(n)/n$. Take $f(x) = \log_4 x$. Thus, for most $n$, $\phi(n) > n/\log_4 n$, so that $\sigma(n) > \phi(n)\log_3 n >$

$n \log_3 n / \log_4 n$. On the other hand, for most $n$, $\sigma(n) < n \log_4 n$, implying that $\phi(\sigma(n)) \ll \sigma(n)/\log_3 n \ll n(\log_4 n/\log_3 n)$. In conclusion, not only is $\sigma(\phi(n))$ larger than $\phi(\sigma(n))$ for most $n$, but their ratio tends to infinity for most $n$. □

**Problem 15.18.** *Show that* $\limsup_{n\to\infty} \sigma(2^n-1)/(2^n-1) = \infty$.

*Solution.* Take $x$ to be large and $n = \operatorname{lcm}[p-1 : p \le x]$. Then, by Fermat's little theorem, $p \mid 2^{p-1}-1 \mid 2^n-1$ for all odd primes $p$. Thus,

$$\frac{\sigma(2^n-1)}{2^n-1} \ge \sum_{p\le x} \frac{1}{p}.$$

Since this last sum diverges as $x \to \infty$, the result follows. □

## Solutions to problems from Chapter 16

**Problem 16.2.** *Prove that the index of composition of an integer is either an integer or an irrational number.*

*Solution.* By definition, we have $n = \gamma(n)^{\lambda(n)}$. Therefore, if there exists an integer $n \ge 2$ such that $\lambda(n) = a/b$, where $a$ and $b \ge 2$ are coprime positive integers, then

$$n^b = \gamma(n)^a. \tag{18.72}$$

Denoting the smallest prime factor of $n$ by $p$ and letting $\alpha \in \mathbb{N}$ be defined by $p^\alpha \| n$, then relation (18.72) implies that $p^{\alpha b} = p^a$ and therefore that $\alpha b = a$, meaning that $a$ and $b$ are not coprime, thereby contradicting our hypothesis. □

**Problem 16.4.** *According to Theorem* 16.10*, the distribution function*

$$F(z,x) = \#\{n \le x : \lambda(n) > z\}$$

*satisfies the inequality*

$$F(z,x) > x^{1/z} \cdot \exp\left\{2(1-\varepsilon)\sqrt{\frac{2(1-1/z)\log x}{\log\log x}}\right\}$$

*for all $1 < z < 2$. Show that this inequality holds as well for all $z \geq 2$. (Hint: First establish that*

$$F(z,x) = \sum_{\substack{ms \leq x \\ m \text{ powerful}, \ (m,s)=1 \\ \lambda(ms) > z}} \mu^2(s) = \sum_{\substack{m \leq x \\ m \text{ powerful}}} \sum_{\substack{s < \min\left(\frac{x}{m}, \left(\frac{m}{\gamma(m)^z}\right)^{1/(z-1)}\right) \\ (s,m)=1}} \mu^2(s)$$

*and then examine for which positive integers $m$ one has*

$$\left(\frac{m}{\gamma(m)^z}\right)^{1/(z-1)} < \frac{x}{m}$$

*and use this to split the inner sum into two sums.)*

*Solution.* We will prove that for $z \geq 2$,

$$F(z,x) > x^{1/z} \exp\left\{2(1+o(1))\sqrt{\frac{2(1-1/z)\log x}{\log\log x}}\right\} \qquad (x \to \infty). \tag{18.73}$$

First observe that any positive integer $n$ such that $\lambda(n) > z$ can be written as $n = ms$, where $m$ is powerful and $s$ is squarefree, with $(m,s) = 1$, and where $s < (m/\gamma(m)^z)^{1/(z-1)}$. This is why one can write

$$\begin{aligned} F(z,x) &= \sum_{\substack{n \leq x \\ \lambda(n) > z}} 1 = \sum_{\substack{ms \leq x \\ m \text{ powerful}, \ (m,s)=1 \\ \lambda(ms) > z}} \mu^2(s) \\ &= \sum_{\substack{m \leq x \\ m \text{ powerful}}} \sum_{\substack{s < \min\left(\frac{x}{m}, \left(\frac{m}{\gamma(m)^z}\right)^{1/(z-1)}\right) \\ (s,m)=1}} \mu^2(s). \end{aligned} \tag{18.74}$$

Now, it is clear that

$$\left(\frac{m}{\gamma(m)^z}\right)^{1/(z-1)} < \frac{x}{m} \qquad \Longleftrightarrow \qquad \frac{m}{\gamma(m)} < x^{1-\frac{1}{z}}.$$

In light of this observation, it follows from (18.74) that

$$F(z,x) > \sum_{\substack{m < \gamma(m) x^{1-\frac{1}{z}} \\ m \text{ powerful}}} \sum_{\substack{s < \left(\frac{m}{\gamma(m)^z}\right)^{1/(z-1)} \\ (s,m)=1}} \mu^2(s). \tag{18.75}$$

On the other hand, one can easily establish (see, for instance, De Koninck and Kátai [**32**]) that

$$\sum_{\substack{s < y \\ (s,m)=1}} \mu^2(s) = (1+o(1)) \frac{6}{\pi^2} y \prod_{p \mid m} \left(1 + \frac{1}{p}\right)^{-1} \tag{18.76}$$

and that, if $m$ is large enough,

$$\prod_{p|m}\left(1+\frac{1}{p}\right)=\exp\left\{\sum_{p|m}\log\left(1+\frac{1}{p}\right)\right\}<\exp\left\{\sum_{p\le m}\frac{1}{p}\right\} \tag{18.77}$$
$$=\exp\{\log\log m+O(1)\}=O(\log m).$$

Therefore, using (18.76) and (18.77), it follows from (18.75) that there exists an absolute constant $C>0$ such that

$$F(z,x)>\frac{C}{\log x}\sum_{\substack{m<\gamma(m)x^{1-\frac{1}{z}}\\ m \text{ powerful}}}\left(\frac{m}{\gamma(m)^z}\right)^{1/(z-1)}=\frac{C}{\log x}S_1, \tag{18.78}$$

say. We then write $S_1$ as

$$\begin{aligned} S_1&=\sum_{d\le x^{1/z}}\frac{\mu^2(d)}{d^{z/(z-1)}}\sum_{\substack{m<dx^{1-1/z}\\ m \text{ powerful}\\ \gamma(m)=d}}m^{1/(z-1)}\\ &=\sum_{d\le x^{1/z}}\frac{\mu^2(d)}{d^{z/(z-1)}}\sum_{\substack{ud<dx^{1-1/z}\\ ud \text{ powerful}\\ \gamma(u)|d}}(ud)^{1/(z-1)} \qquad (18.79)\\ &=\sum_{d\le x^{1/z}}\frac{\mu^2(d)}{d}\sum_{\substack{u<x^{1-1/z}\\ ud \text{ powerful}\\ \gamma(u)|d}}u^{1/(z-1)}. \end{aligned}$$

But the statement "$ud$ powerful and $\gamma(u)|d$" is identical to the statement "$ud=rd^2$ for a certain positive integer $r$ such that $\gamma(r)|d$". The relation (18.79) can therefore be written as

$$\begin{aligned} S_1&=\sum_{d\le x^{1/z}}\frac{\mu^2(d)}{d}\sum_{\substack{rd\le x^{1-1/z}\\ \gamma(r)|d}}(rd)^{1/(z-1)}\\ &=\sum_{d\le x^{1/z}}\frac{\mu^2(d)}{d^{1-\frac{1}{z-1}}}\sum_{\substack{d\le\frac{x^{1-1/z}}{r}\\ \gamma(r)|d}}r^{1/(z-1)} \qquad (18.80)\\ &=\sum_{r\le x^{1-1/z}}r^{1/(z-1)}\sum_{d<\min\left(x^{1/z},\frac{x^{1-1/z}}{r}\right)}\frac{\mu^2(d)}{d^{1-\frac{1}{z-1}}}. \end{aligned}$$

But it is clear that

$$\frac{x^{1-1/z}}{r}<x^{1/z}\qquad\Longleftrightarrow\qquad r>x^{1-2/z}.$$

By restricting the range of the summation and writing the condition $\gamma(r)|d$ as $d = \alpha\gamma(r)$, it follows from (18.80) that

$$
\begin{aligned}
S_1 &> \sum_{x^{1-2/z}<r<x^{1-1/z}} r^{1/(z-1)} \sum_{\substack{d<\frac{x^{1-1/z}}{r} \\ \gamma(r)|d}} \frac{\mu^2(d)}{d^{1-\frac{1}{z-1}}} \\
&= \sum_{x^{1-2/z}<r<x^{1-1/z}} r^{1/(z-1)} \sum_{\alpha<\frac{x^{1-1/z}}{r\gamma(r)}} \frac{1}{(\alpha\gamma(r))^{1-\frac{1}{z-1}}} \\
&\geq x^{1/z} \sum_{x^{1-2/z}<r<x^{1-1/z}} \frac{1}{\gamma(r)} + O(1) \\
&= x^{1/z} \Big( L(x^{1-1/z}) - L(x^{1-2/z}) \Big) + O(1) \\
&= x^{1/z} \exp\left\{ 2(1+o(1)) \sqrt{\frac{2(1-1/z)\log x}{\log\log x}} \right\}.
\end{aligned}
\tag{18.81}
$$

Substituting (18.81) in (18.78), the estimate (18.73) is thus established for all $z \geq 2$. □

# Bibliography


1. W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. Math. **140** (1994), 703–722.
2. K. Alladi, *The Turán-Kubilius inequality for integers without large prime factors*, J. Reine Angew. Math. **335** (1982), 180–196.
3. T. M. Apostol, *A proof that Euler missed: Evaluating $\zeta(2)$ the easy way*, Math. Intelligencer **5** (1983), 59–60.
4. R. C. Baker and G. Harman, *Shifted primes without large prime factors*, Acta Arith. **83** (1998), 331–361.
5. R. C. Baker, G. Harman, and J. Pintz, *The difference between consecutive primes. II*, Proc. London Math. Soc. (3) **83** (2001), 532–562.
6. M. Balazard, H. Delange, et J. L. Nicolas, *Sur le nombre de facteurs premiers des entiers*, C.R. Acad. Sci. Paris Sér. I Math. **306** (1988), 511–514.
7. A. Balog and T. Wooley, *On strings of consecutive integers with no large prime factors*, J. Austral. Math. Soc. Ser. A **64** (1998), no. 2, 266–276.
8. W. Banks, M. Garaev, F. Luca, and I. E. Shparlinski, *Uniform distribution of the fractional part of the average prime factor*, Forum Mathematicum **17** (2005), 885–903.
9. W. D. Banks and F. Luca, *Composite integers $n$ for which $\phi(n) \mid n-1$*, Acta Math. Sin., English Series 23 (2007), no. 10, 1915–1918.
10. P. T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. **16** (1962), 363–367.
11. Y. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte*, J. Reine Angew. Math. **539** (2001), 75–122.
12. B. J. Birch, *Multiplicative functions with non-decreasing normal order*, J. London Math. Soc. **42** (1967), 149-151.
13. G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of $a^n - b^n$*, Ann. Math. (2) **5** (1904), 173–180.
14. E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque **18**, Société Mathématique de France, Paris, 1974.

15. N. G. de Bruijn, *The asymptotic behaviour of a function occurring in the theory of primes*, J. Indian Math. Soc. (N. S.) **15** (1951), 25–32.
16. N. G. de Bruijn, *On the number of positive integers $\leq x$ and free of prime factors $> y$*, Indag. Math. **28** (1966), 239–247.
17. J. Browkin, *The abc-conjecture*, Number Theory, Trends Math., Birkhäuser, Basel, 2000, 75–105.
18. J. Browkin and J. Brzezinski, *Some remarks on the abc-conjecture*, Math. of Comp. **62** (1994), 931–939.
19. V. Brun, *Le crible d'Eratosthène et le théorème de Goldbach*, Christiania Vidensk. Selsk. Skr. (1920), 36 pp.
20. E. R. Canfield, P. Erdős, and C. Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum"*, J. Number Theory **17** (1983), no. 1, 1–28.
21. R. D. Carmichael, *On Euler's $\phi$-function*, Bull. Amer. Math. Soc. **13** (1907), 241–243.
22. R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. Math. (2) **15** (1913), 30–70.
23. J. R. Chen, *On the representation of a large even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica **16** (1973), 157–176.
24. The Clay Institute, *Millennium Prize Problems: Riemann Hypothesis*, www.claymath.org/millennium/ Riemann_Hypothesis.
25. B. Conrey, *More than two fifths of the zeros of the Riemann Zeta Function are on the critical line*, J. Reine Angew. Math. **399** (1989), 1–26.
26. H. Cramer, *On the Order of Magnitude of the Difference Between Consecutive Prime Numbers*, Acta Arith. **2** (1936), 23–46.
27. R. Crandall and C. Pomerance, *Prime Numbers. A computational perspective*, Second edition, Springer, New York, 2005.
28. H. Daboussi, *Sur le théorème des nombres premiers*, C. R. Acad. Sci. Paris Sér. I. Math. 298 (1984), 161–164.
29. N.G. de Bruijn, *On the number of integers $\leq x$ whose prime factors divide $n$*, Illinois J. Math. **6** (1962), 137–141.
30. J.-M. De Koninck, *Those Fascinating Numbers*, Amer. Math. Soc., Providence, RI, 2009.
31. J.-M. De Koninck and R. Sitaramachandrarao, *Sums involving the largest prime divisor of an integer*, Acta Arith. **48** (1987), 1–8.
32. J.-M. De Koninck and I. Kátai, *On the mean value of the index of composition*, Monatshefte für Mathematik **145** (2005), no. 2, 131–144.
33. J.-M. De Koninck and F. Luca, *On the index of composition of the Euler function*, Colloquium Mathematicum **108** (2007), 31–51.
34. J.-M. De Koninck and A. Mercier, *Approche élémentaire de l'étude des fonctions arithmétiques*, Les Presses de l'Université Laval, Québec, 1982.
35. J.-M. De Koninck and N. Doyon, *À propos de l'indice de composition des nombres*, Monatshefte für Mathematik **139** (2003), 151–167.
36. J.-M. De Koninck and G. Tenenbaum, *Sur la loi de répartition du $k$-ième facteur premier d'un entier*, Math. Proc. Cambridge Philos. Soc. **133** (2002), 191–204.
37. H. Delange, *Sur les fonctions arithmétiques multiplicatives*, Ann. Sci. École Norm. Sup. (3) **78** (1961), 273–304.

38. H. Delange, *Quelques résultats nouveaux sur les fonctions additives*, Mémoires de la Soc. Math. de France **25** (1971), 45–53
39. L. E. Dickson, *A new extension of Dirichlet's theorem on prime numbers*, Messenger of Math. **33** (1904), 155–161.
40. P. Dusart, *The k-th prime is greater than* $k(\log k + \log\log k - 1)$ *for* $k \geq 2$, Math. Comp. **68** (1999), 411–415.
41. N. D. Elkies, *ABC implies Mordell*, Internat. Math. Res. Notices **1991**, no. 7, 99–109.
42. P. D. T. A. Elliott, *Probabilistic Number Theory I. Mean Value Theorems*, Grundlehren der Math. Wiss. 239, Springer-Verlag, New York, Berlin, Heidelberg, 1979.
43. P. D. T. A. Elliott, *Probabilistic Number Theory II. Central Limit Theorems*, Grundlehren der Math. Wiss. 240, Springer-Verlag, New York, Berlin, Heidelberg, 1980.
44. N. E. Elliott and D. Richner, *An investigation of the set of ans numbers*, Missouri Journal of Mathematical Sciences **15** (2003), 189–199.
45. V. Ennola, *On numbers with small prime divisors*, Ann. Acad. Sci. Fenn. Ser. AI **440** (1969), 16 pp.
46. P. Erdős, *On the difference of consecutive primes*, Quart. J. Math. Oxford Ser. **6** (1935), 124–128.
47. P. Erdős, *On the normal number of prime factors of* $p-1$ *and some other related problems concerning Euler's* $\phi$ *function*, Quart. J. Math. Oxford Ser. **6** (1935), 205–213.
48. P. Erdős, *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 374–384.
49. P. Erdős, *On integers of the form* $2^k + p$ *and related problems*, Summa Brasil. Math. **2** (1950), 113–123.
50. P. Erdős and R. Obláth, *Über diophantishe Gleichungen der Form* $n! = x^p \pm y^p$ *und* $n! \pm m! = x^p$, Acta Litt. Sci. Szeged **8** (1937), 241–255.
51. P. Erdős and C. Pomerance, *On the largest prime factors of n and n+1*, Aequationes Math. **17** (1978), 311–321.
52. P. Erdős and C. L. Stewart, *On the greatest and least prime factors of* $n! + 1$, J. London Math. Soc. **13** (1976), 513–519.
53. P. Erdős and A. Wintner, *Additive arithmetical functions and statistical independence*, Amer. J. Math. **61** (1939), 713–721.
54. L. Euler, *Variae observationes circa series infinitas*, Comm. Acad. Sci. Petropolitanae **9** (1737), 222–236.
55. K. Ford, *The distribution of totients*, Ramanujan J. **2** (1998), 67–151.
56. K. Ford, *An explicit sieve bound and small values of* $\sigma(\phi(m))$, Period. Math. Hungar. **43** (2001), no. 1-2, 15–29.
57. A. Granville, *Smooth numbers: Computational number theory and beyond*, Algorithmic Number Theory, MSRI Publications, Vol. 44, 2008, 267–233.
58. K. Ford, F. Luca, and C. Pomerance, *Common values of the arithmetic functions* $\phi$ *and* $\sigma$*,* Bull. London Math. Soc. **42** (2010), 478–488.
59. K. Ford, F. Luca, and I. Shparlinski, *On the largest prime factor of the Mersenne numbers*, Bull. Aust. Math. Soc. **79** (2009), no.3, 455-463.

60. E. Fouvry, *Théorème de Brun-Titchmarsh: Application au théorème de Fermat*, Invent. Math. **79** (1985), 383–407.
61. J. Friedlander, *Shifted primes without large factors*, Number Theory and Applications (R. A. Mollin, ed.), NATO Adv. Sci. Inst. Ser. C. Math. Phys. Sci., Kluwer, Dordrecht, 1989, 393–401.
62. J. Friedlander and H. Iwaniec, *The polynomial $X^2 + Y^4$ captures its primes*, Ann. of Math. (2) **148** (1998), no. 3, 945–1040.
63. J. Galambos, *Introductory Probability Theory*, Marcel Dekker, 1984.
64. C. F. Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986.
65. D. A. Goldston, J. Pintz, and C. Y. Yildirim, *Primes in tuples II*, Acta Mathematica **24** (2010), 1–47.
66. S. W. Golomb, *Powerful numbers*, Amer. Math. Monthly **77** (1970), 848–852.
67. D. Gordon and G. Rodemich, *Dense admissible sets*, Algorithmic number theory (Portland, OR), Lecture Notes in Comput. Sci., 1423, Springer, Berlin, 1998, 216–225.
68. A. Granville, *Smooth numbers: Computational number theory and beyond*, Algorithmic Number Theory, MSRI Publications, Vol. 44, 2008, 267–323.
69. A. Granville and G. Martin, *Prime number races*, Amer. Math. Monthly **113** (2006), 1–33.
70. B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics **167** (2008), 481–547.
71. R. K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, Third edition, 2004.
72. R. K. Guy and R. J. Nowakowski, *Unsolved Problems: Monthly Unsolved Problems*, 1969-1997, Amer. Math. Monthly **104** (1997), no. 10, 967–973.
73. J. Hadamard, *Étude sur les propriétés des fonctions entières et en particulier d'une fonction considérée par Riemann*, J. Math. Pures et Appl. (4) **9** (1893), 171–215.
74. H. H. Halberstam and H. E. Richert, *Sieve Methods*, Academic Press, London, 1974.
75. G. H. Hardy, *Divergent Series*, Clarendon Press, Oxford, 1949.
76. G. H. Hardy and J. E. Littlewood, *Some problems on partitio numerorum III. On the expression of a number as a sum of primes*, Acta Math., **44** (1923), 1–70.
77. G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number $n$*, Quart. J. Math. **48** (1917), 76–92.
78. J. Havil, *Gamma: Exploring Euler's Constant*, Princeton University Press, Princeton, 2003.
79. D. R. Heath-Brown, *Primes represented by $x^3 + 2y^3$*, Acta Math. **186** (2001), no. 1, 1–84.
80. D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) **64** (1992), no. 2, 265–338.
81. D. Hensley and I. Richards, *On the incompatibility of two conjectures concerning primes*, Analytic Number Theory, Proc. Sympos. Pure Math. **24**, St. Louis Univ., Missouri, 1972, 123–127.
82. A. J. Hildebrand, *On the number of positive integers $\leq x$ and free of prime factors $> y$*, J. Number Theory **22** (1986), no. 3, 289–307.
83. A. Hildebrand and G. Tenenbaum, *On integers free of large prime factors*, Trans. Amer. Math. Soc. **296** (1986), 265–290.

84. A. Hildebrand and G. Tenenbaum, *Integers without large prime factors*, Journal de Théorie des Nombres de Bordeaux **5** (1993), 1–74.
85. M. N. Huxley, *Exponential Sums and Lattice Points III*, Proc. London Math. Soc. **87** (2003), 591-609.
86. *Shortlist Problems IMO2005*, http://www.imomath.com/imocomp/sl05_0707.pdf.
87. A. Ivić, *The Riemann Zeta-function*, Wiley, New York, 1985.
88. A. Ivić and P. Shiu, *The distribution of powerful numbers*, Illinois J. Math. **26** (1982), 576–590.
89. H. Iwaniec and E. Kowalski, *Analytic Number Theory*, AMS Colloquium Publications, Vol. 53, Providence, 2004.
90. J. P. Jones, D. Sato, H. Wada, and D. Wiens, *Diophantine representation of the set of prime numbers*, Amer. Math. Monthly **83** (1976), 449–464.
91. M. Kobayashi, P. Pollack, and C. Pomerance, *On the distribution of sociable numbers*, J. Number Theory **129** (2009), 1990–2009.
92. M. Křížek and F. Luca, *On the solutions of the congruence* $n^2 \equiv 1 \pmod{\phi^2(n)}$, Proc. Amer. Math. Soc. **129** (2001), no. 8, 2191–2196.
93. M. Křížek, F. Luca, and L. Somer: *17 Lectures on Fermat Numbers*, CMS Books in Mathematics, vol. 9, Springer, New York, 2002.
94. J. Kubilius, *Probabilistic Methods in the Theory of Numbers*, Amer. Math. Soc. Translations of Math. Monographs, Vol. 11, Providence, 1964.
95. M. Langevin, *Sur quelques conséquences de la conjecture* $(abc)$ *en arithmétique et en logique*, in Symposium on Diophantine Problems (Boulder, CO, 1994), Rocky Mountain J. Math. **26** (1996), no. 3, 1031–1042.
96. N. Levinson, *More than one third of zeros of Riemann's Zeta function are on* $\sigma = 1/2$, Advances Math. **13** (1974), 383–486.
97. H. Li, *The Exceptional Set of Goldbach Numbers*, Quart. J. Math. Oxford Ser. **50** (1999), 471–482.
98. E. Lucas, *Sur la recherche des grands nombres premiers*, Assoc. Française pour l'Avancement des Sciences. Comptes Rendus **5** (1876), 61–68.
99. F. Luca, *On a problem of K.R.S. Sastry*, Mathematics and Computer Education **35** (2001), 125–135.
100. F. Luca and C. Pomerance, *On composite integers* $n$ *for which* $\phi(n) \mid n-1$, Bol. Soc. Mat. Mexicana (to appear).
101. F. Luca and C. Pomerance, *On some problems of Makowski-Schinzel and Erdős concerning the arithmetical functions* $\phi$ *and* $\sigma$, Colloq. Math. **92** (2002), 111–130.
102. F. Luca and I. E. Shparlinski, *Prime factors of shifted factorials*, Bull. London Math. Soc. **37** (2005), 809–817.
103. A. Mąkowski and A. Schinzel, *On the functions* $\phi(n)$ *and* $\sigma(n)$, Colloq. Math. **13** (1964), 95–99.
104. H. von Mangoldt, *Zu Riemann's Abhandlung: "Über die Anzahl der Primzahlen unter einer gegebenen Grösse"*, J. Reine Angew. Math. **114** (1895), 255-305.
105. H. von Mangoldt, *Zur Verteilung der Nullstellen der Riemannscher Funktion* $\xi(t)$, Math. Ann. **60** (1905), 1–19.
106. P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.

107. H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika **20** (1973), 119–134.
108. M. R. Murty and S. Wong, *The ABC conjecture and prime divisors of the Lucas and Lehmer sequences*, Number theory for the millennium, III (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, 43–54.
109. M. Nair, *On Chebyshev-type inequalities for primes*, Amer. Math. Monthly **89** (1982), 126–129.
110. W. Narkiewicz, *The Development of Prime Number Theory*, Springer, 2000.
111. M. B. Nathanson, *Additive number theory. The classical bases*, Graduate Texts in Mathematics, Vol. 164, Springer-Verlag, New York, 1996.
112. D. J. Newman, *Simple analytic proof of the prime number theorem*, Amer. Math. Monthly **87** (1980), 693–696.
113. J. L. Nicolas, *Sur la distribution des nombres premiers ayant une quantité fixée de nombres premiers*, Acta Arith. **44** (1984), 191–200.
114. A. Nitaj, *Conséquences et aspects expérimentaux des conjectures abc et de Szpiro*, thèse de doctorat, Université de Caen, 1994.
115. C. Pomerance, *On the distribution of amicable numbers, II*, J. Reine Angew. Math. **325** (1981), 183–188.
116. O. V. Popov, *A derivation of the modern bound for the zeros of the Riemann zeta function by the Hadamard method*, Vestnik Mosk. Univ., 1994, 42–45.
117. A. G. Postnikov, *Introduction to Analytic Number Theory*, Translations of Mathematical Monographs, Vol. 68, Amer. Math. Soc., Providence, RI, 1988.
118. R. A. Rankin, *The difference between consecutive prime numbers*, J. Lond. Math. Soc. **13** (1938), 242–247.
119. P. Ribenboim, *The ABC conjecture and the radical index of integers*, Acta Arith. **96** (2001), 389–404.
120. G. F. B. Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, Monatsber. Königl. Preuss. Akad. Wiss. Berlin (1859), 671–680.
121. H. Riesel, *Nagara stora primtal*, Elementa **39** (1956), 258–260.
122. Riesel Prime Search: http://www.prothsearch.net/riesel.html.
123. N. P. Romanov, *Über einige Sätze der aditiven Zahlentheorie*, Math. Annalen **101** (1934), 668–678.
124. J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.
125. W. Schwarz and J. Spilker, *Arithmetical Functions*, London Math. Soc. Lecture Notes Series, Vol. 184, Cambridge University Press, 1994.
126. A. Selberg, *An elementary proof of the prime number theorem*, Ann. Math. **50** (1949), 305–313.
127. A. Selberg, *Note on a paper by L.G. Sathe*, J. Indian Math. Soc. **18** (1953), 83–87.
128. E. Seneta, *Regularly varying functions*, Springer-Verlag, Berlin, 1976.
129. J. P. Serre, *Cours d'arithmétique*. Presses Universitaires de France, Paris. Second edition, 1977.
130. T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Tracts in Mathematics **87**, Cambridge University Press, Cambridge, 1986.
131. W. Sierpiński, *Sur une problème concernant les nombres* $k \cdot 2^n + 1$, Elem. Math. **15** (1960), 73–74.

132. A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith., **4** (1958), 185–208; Erratum, Acta Arith., **5** (1959), 259.

133. A. Selberg, *An elementary proof of the Prime Number Theorem*, Ann. Math. **50** (1949), 305–313.

134. Seventeen or Bust: http://www.seventeenorbust.com/.

135. C. L. Stewart, *On the greatest and least prime factors of* $n! + 1$*, II*, Publ. Math. Debrecen **65** (2004), 461–480.

136. C. L. Stewart and K. Yu, *On the abc conjecture. II.* Duke Math. J. **108** (2001), 169–181.

137. C. L. Stewart, *The greatest prime factor of* $a^n - b^n$, Acta Arith. **26** (1975), 427–433.

138. C. L. Stewart, *On divisors of Lucas and Lehmer numbers*, *Preprint*, 2010.

139. R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.

140. G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Studies in Advanced Mathematics **46**, Cambridge University Press, Cambridge, 1995.

141. G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Belin, 2008.

142. E. C. Titchmarsh, *The Theory of the Riemann Zeta-function*, Oxford Science Publications, Oxford, 1986.

143. P. Turan, *On a theorem of Hardy and Ramanujan*, J. London Math. Soc. **9** (1934), 274–276.

144. A. Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie. Deutscher Verlag der Wissenschaften*, Berlin, 1963.

145. J. Wästlund, *An elementary proof of the Wallis product formula for pi*, Amer. Math. Monthly **114** (2007), 914–917.

146. A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

147. H. C. Williams, *Édouard Lucas and Primality Testing*, Canadian Mathematical Society, Wiley, 1998.

148. A. Wintner, *The theory of measure in arithmetical semi-groups*, Waverly Press, Baltimore, MD, 1944.

149. K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. **3** (1892), 265–284.

# Index

The authors assemble a fascinating collection of topics from analytic number theory that provides an introduction to the subject with a very clear and unique focus on the anatomy of integers, that is, on the study of the multiplicative structure of the integers. Some of the most important topics presented are the global and local behavior of arithmetic functions, an extensive study of smooth numbers, the Hardy-Ramanujan and Landau theorems, characters and the Dirichlet theorem, the *abc* conjecture along with some of its applications, and sieve methods. The book concludes with a whole chapter on the index of composition of an integer.

One of this book's best features is the collection of problems at the end of each chapter that have been chosen carefully to reinforce the material. The authors include solutions to the even-numbered problems, making this volume very appropriate for readers who want to test their understanding of the theory presented in the book.

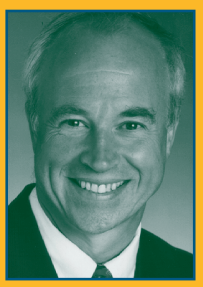

Photo courtesy of Coaching Association of Canada

ISBN 978-0-8218-7577-3

9 780821 875773

GSM/134

For additional information and updates on this book, visit

**www.ams.org/bookpages/gsm-134**

AMS *on the* Web
**www.ams.org**