Not Always Buried Deep

Paul Pollack

Department of Mathematics, University of Georgia, Athens, GA 30609

E-mail address: `twonth@gmail.com`

Dedicated to the memory of Arnold Ephraim Ross (1906–2002).

Contents

Foreword

> The gold in 'them there hills' is not always buried deep. Much of it is within easy reach. Some of it is right on the surface to be picked up by any searcher with a keen eye for detail and an eagerness to explore. As in any treasure hunt, the involvement grows as the hunt proceeds and each success whether small or great adds the fuel of excitement to the exploration. – A. E. Ross

Number theory is one of the few areas of mathematics where problems of substantial interest can be described to someone possessing scant mathematical background. It sometimes proves to be the case that a problem which is simple to state requires for its resolution considerable mathematical preparation; e.g., this appears to be the case for Fermat's conjecture regarding integer solutions to the equation $x^n + y^n = z^n$. But this is by no means a universal phenomenon; many engaging problems can be successfully attacked with little more than one's "mathematical bare hands". In this case one says that the problem can be solved in an *elementary* way (even though the elementary solution may be far from simple). Such elementary methods and the problems to which they apply are the subject of this book.

Because of the nature of the material, very little is required in terms of prerequisites: The reader is expected to have prior familiarity with number theory at the level of an undergraduate course. The nececssary background can be gleaned from any number of excellent texts, such as Sierpiński's charmingly discursive *Elementary Theory of Numbers* or LeVeque's lucid and methodical *Fundamentals of Number Theory*. Apart from this, a rigorous course in calculus, some facility with manipulation of estimates (in particular, big-Oh and little-oh notation), and a first course in modern algebra (covering groups, rings, and fields) should suffice for the majority of the text. A course in complex variables is *not* required, provided that the reader is willing to overlook some motivational remarks made in Chapter 8.

Rather than attempt a comprehensive account of elementary methods in number theory, I have focused on topics that I find particularly attractive and accessible:

- Chapters 1, 3, 4, and 8 collectively provide an overview of prime number theory, starting from the infinitude of the primes, moving through the elementary estimates of Chebyshev and Mertens, then the theorem of Dirichlet on primes in prescribed arithmetic progressions, and culminating in an elementary proof of the prime number theorem.
- Chapter 2 contains a discussion of Gauss's arithmetic theory of the roots of unity (*cyclotomy*), which was first presented in the final section of his *Disquisitiones Arithmeticae*. After developing this theory to the extent required to prove Gauss's characterization of constructible regular polygons, we give a cyclotomic proof of the quadratic reciprocity law, followed by a detailed account of a little-known cubic reciprocity law due to Jacobi.
- Chapter 5 is a 12-page interlude containing Dress's proof of the following result conjectured by Waring in 1770 and established by Hilbert in 1909: For each fixed integer $k \geq 2$, every natural number can be expressed as the sum of a bounded number of nonnegative kth powers, where the bound depends only on k.
- Chapter 6 is an introduction to combinatorial sieve methods, which were introduced by Brun in the early twentieth century. The best-known consequence of Brun's method is that if one sums the reciprocals of each prime appearing in a twin prime pair $p, p+2$, then the answer is finite. Our treatment of sieve methods is robust enough to establish not only this and other comparable 'upper bound' results, but also Brun's deeper "lower bound" results. For example, we prove that there are infinitely many n for which both n and $n+2$ have at most 7 prime factors, counted with multiplicity.
- Chapter 9 summarizes what is known at present about *perfect numbers*, numbers which are the sum of their proper divisors.

At the end of each chapter (excepting the interlude) I have included several nonroutine exercises. Many are based on articles from the mathematical literature, including both research journals and expository publications like the *American Mathematical Monthly*. Here, as throughout the text, I have made a conscious effort to document original sources and thus encourage conformance to Abel's advice to "read the masters".

While the study of elementary methods in number theory is one of the most accessible branches of mathematics, the lack of suitable textbooks has been a repellent to potential students. It is hoped that this modest contribution will help to reverse this injustice.

Paul Pollack

Notation

While most of our notation is standard and should be familiar from an introductory course in number theory, a few of our conventions deserve explicit mention: The set $\mathbf{N}$ of natural numbers is the set $\{1, 2, 3, 4, \ldots\}$. Thus 0 is *not* considered a natural number. Also, if $n \in \mathbf{N}$, we write "$\tau(n)$" (instead of "$d(n)$") for the number of divisors of n. This is simply to avoid awkward expressions like "$d(d)$" for the number of divisors of the natural number d. Throughout the book, we reserve the letter p for a prime variable.

We remind the reader that "$A = O(B)$" indicates that $|A| \leq c|B|$ for some constant $c > 0$ (called the *implied constant*); an equivalent notation is "$A \ll B$". The notation "$A \gg B$" means $B \ll A$, and we write "$A \asymp B$" if both $A \ll B$ and $A \gg B$. If A and B are functions of a single real variable x, we often speak of an estimate of this kind holding as "$x \to a$" (where a belongs to the two-point compactification $\mathbf{R} \cup \{\pm\infty\}$ of $\mathbf{R}$) to mean that the estimate is valid on some deleted neighborhood of a. Subscripts on any of these symbols indicate parameters on which the implied constants (and, if applicable, the deleted neighborhoods) may depend. The notation "$A \sim B$" means $A/B \to 1$ while "$A = o(B)$" means $A/B \to 0$; here subscripts indicate parameters on which the rate of convergence may depend.

If S is a subset of the natural numbers $\mathbf{N}$, the (*asymptotic*, or *natural*) *density* of S is defined as the limit

$$\lim_{x \to \infty} \frac{1}{x} \#\{n \in S : n \leq x\},$$

provided that this limit exists. The *lower density* and *upper density* of S are defined similarly, with $\liminf$ and $\limsup$ replacing $\lim$ (respectively). We say that a statement holds for *almost all natural numbers n* if it holds on a subset of $\mathbf{N}$ of density 1.

If f and G are defined on a closed interval $[a, b] \subset \mathbf{R}$, with f' piecewise continuous there, we define

$$\int_a^b f(t)\, dG(t) := G(b)f(b) - G(a)f(a) - \int_a^b f'(t)G(t)\, dt,$$

provided that the right-hand integral exists. (Experts will recognize the right-hand side as the formula for integration by parts for the Riemann–Stieltjes integral, but defining the left-hand side in this manner allows us to avoid assuming any knowledge of Riemann–Stieltjes integration.) We will often apply partial summation in the following form, which is straightforward to verify directly: *Suppose that a and b are real numbers with $a \le b$ and that we are given complex numbers a_n for all natural numbers n with $a < n \le b$. Put $S(t) := \sum_{a<n\le t} a_n$. If f' is piecewise continuous on $[a,b]$, then*

$$\sum_{a<n\le b} a_n f(n) = \int_a^b f(t)\, dS(t).$$

In order to paint an accurate portrait of the mathematical landscape without straying off point, it has been necessary on occasion to state certain theorems without proof; such results are marked with a star (★). For some of these results, proofs are sketched in the corresponding chapter exercises.

Acknowledgements

There are many people without whom this book could not have been written and many others without whom this book would not be worth reading.

Key members of the first group include my middle and high-school teachers Daniel Phelon, Sharon Bellak, and Jeff Miller. It is thanks to their tireless efforts that I was prepared to attend the Ross Summer Mathematics Program at Ohio State University in 1998. There Arnold Ross, assisted by my counselor Noah Snyder and my seminar instructor Daniel Shapiro, impressed upon me the importance of grappling with mathematical ideas for oneself. I regard this as the most important lesson I have learned so far on my mathematical journey. As an undergraduate, I was the fortunate recipient of generous mentoring from Andrew Granville and Matt Baker, and I had the privilege of attending A. J. Hildebrand's 2002 REU in number theory. My subsequent graduate experience at Dartmouth College ranks as one of the happiest times of my life, due in large measure to the wise guidance of my advisor, Carl Pomerance.

My family — my father Lawrence, my mother Lolita, and my brother Michael — has done so much for me over the years that it would be impossible (and inappropriate!) for me to express the extent of my appreciation in this brief space. Another friend for whom I am grateful beyond words is Susan Roth, who for the last decade has accompanied me on many of my (mis)adventures in genre television.

Mits Kobayashi cheerfully donated his time to prepare many of the figures included in the text. Both he and Enrique Treviño pointed out several typographical errors and inaccuracies in earlier versions of the manuscript. I am grateful for both their help and their friendship.

This text served as the basis for a graduate topics course taught by the author during the Spring 2009 semester at the University of Illinois at Urbana-Champaign. I am grateful to the U of I for allowing me this opportunity. Almost concurrently, Carl Pomerance used a preliminary version of these notes to teach a quarter-long course at Dartmouth College. This manuscript is better for his numerous insightful suggestions.

Finally, I would like to thank the American Mathematical Society, especially Ed Dunne, Cristin Zanella, and Luann Cole, for their encouragement of this project at every stage.

Chapter 1

Elementary Prime Number Theory, I

> Prime numbers are more than any assigned multitude of prime numbers. – Euclid
>
> No prime minister is a prime number – A. Plantinga

1. Introduction

Recall that a natural number larger than 1 is called *prime* if its only positive divisors are 1 and itself, and *composite* otherwise. The sequence of primes begins

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \ldots$$

Few topics in number theory attract more attention, popular or professional, than the theory of prime numbers. It is not hard to see why. The study of the distribution of the primes possesses in abundance the very features that draw so many of us to mathematics in the first place: intrinsic beauty, accessible points of entry, and a lingering sense of mystery embodied in numerous unpretentious but infuriatingly obstinate open problems.

Put

$$\pi(x) := \#\{p \le x : p \text{ prime}\}.$$

Prime number theory begins with the following famous theorem from antiquity:

Theorem 1.1. *There are infinitely many primes, i.e., $\pi(x) \to \infty$ as $x \to \infty$.*

The first half of this chapter is a survey of the many proofs that have been given for Theorem 1.1. The second half of this chapter is devoted to the theme of prime-producing formulas and the occurrence of primes in various natural sequences.

2. Euclid and his imitators

We begin with the classic proof from Euclid's *Elements* (circa 300 BC):

Proof. Suppose that $p_1, p_2, \ldots, p_k$ is any finite list of primes. Let P denote the product of the p_i and consider the integer $P+1$. Since $P+1 \equiv 1 \pmod{p_i}$ for each $1 \leq i \leq k$, none of the p_i divide $P+1$. But since $P+1 > 1$, it must have some prime divisor p. It follows that there is always a prime missing from any finite list, or, as Euclid put it, "prime numbers are more than any assigned multitude of primes." $\square$

There are many trivial variants; for instance, we can easily show that for every integer m there is a prime $p > m$ by taking p to be any prime divisor of $m! + 1$.

In this section we collect several Euclidean proofs for Theorem 1.1. All of these start with a finite list of primes and then produce an integer > 1 that is coprime to every prime on the list. Stieltjes's proof is typical:

Stieltjes's proof, 1890. Suppose that $p_1, \ldots, p_k$ is a finite list of distinct primes with product P and let $P = AB$ be any decomposition of P into two positive factors. Suppose that p is one of the p_i. Then $p \mid AB$, so that either $p \mid A$ or $p \mid B$. If p divides both A and B, then p^2 divides P, which is false. Consequently, p divides exactly one of A and B. It follows that $p \nmid A + B$. So $A + B$ is divisible by none of the p_i; but as $A + B \geq 2$, it has some prime divisor. So again we have discovered a prime not on our original list. $\square$

Euler's second proof (published posthumously). This proof is based on the multiplicativity of the Euler totient function: Let $p_1, \ldots, p_k$ be a list of distinct primes with product P. By said multiplicativity,

$$\varphi(P) = \prod_{i=1}^{k} (p_i - 1) \geq 2^{k-1} \geq 2,$$

provided that our list contains at least two primes (as we may assume). It follows that there is an integer in the interval $[2, P]$ that is coprime to P; but such an integer has a prime factor distinct from all of the p_i. $\square$

Proof of Braun (1897), Métrod (1917). Let $p_1, \dots, p_k$ be a list of $k \geq 2$ distinct primes and let $P = p_1 p_2 \cdots p_k$. Consider the integer

$$N := P/p_1 + P/p_2 + \cdots + P/p_k.$$

For each $1 \leq i \leq k$, we have

$$N \equiv P/p_i = \prod\nolimits_{j \neq i} p_j \not\equiv 0 \pmod{p_i},$$

so that N is divisible by none of the p_i. But $N \geq 2$, and so it must possess a prime factor not on our list. □

3. Coprime integer sequences

Suppose we know an infinite sequence of pairwise relatively prime positive integers

$$2 \leq n_1 < n_2 < \cdots .$$

Then we may define a sequence of primes p_i by selecting arbitrarily a prime divisor of the corresponding n_i; the terms of this sequence are pairwise distinct because the n_i are pairwise coprime.

If we can exhibit such a sequence of n_i without invoking the infinitude of the primes, then we have a further proof of Theorem 1.1. An argument of this nature was given by Goldbach:

Proof (Goldbach). Let $n_1 = 3$, and for $i > 1$ inductively define

$$n_i = 2 + \prod_{1 \leq j < i} n_j.$$

The following assertions are all easily verified in succession:

(i) Each n_i is odd.

(ii) When $j > i$, we have $n_j \equiv 2 \mod n_i$.

(iii) We have $\gcd(n_i, n_j) = 1$ for $i \neq j$.

Theorem 1.1 now follows from the above remarks. □

A straightforward induction shows that

$$n_i = 2^{2^{i-1}} + 1, \tag{1.1}$$

and this is how Goldbach presented the proof.

Before proceeding, we pause to note that the above proof implies more than simply the infinitude of the primes. First, it gives us an upper bound for the nth prime, $2^{2^{n-1}} + 1$; this translates into a lower bound of the shape

$$\pi(x) \gg \log\log x \quad (x \to \infty).$$

(Cf. Exercise 1.) Second, it may be used to prove that certain arithmetic progressions contain infinitely many primes. To see this, suppose that $p \mid n_i$ and note that by (1.1), we have

$$2^{2^{i-1}} \equiv -1 \pmod{p}, \quad \text{so that} \quad 2^{2^i} \equiv (2^{2^{i-1}})^2 \equiv 1 \pmod{p}.$$

Hence the order of 2 modulo p is precisely 2^i. Thus $2^i \mid (\mathbf{Z}/p\mathbf{Z})^\times = p-1$, so that $p \equiv 1 \pmod{2^i}$. As a consequence, for any fixed k, there are infinitely many primes $p \equiv 1 \pmod{2^k}$: choose a prime p_i dividing n_i for each $i \geq k$. In §9.1 we will prove the more general result that for each $m \geq 1$, there are infinitely many primes $p \equiv 1 \pmod{m}$.

A related method of proving the infinitude of the primes is as follows: Let $a_1 < a_2 < a_3 < \cdots$ be a sequence of positive integers with the property that

$$\gcd(i,j) = 1 \quad \Longrightarrow \quad \gcd(a_i, a_j) = 1.$$

Moreover, suppose that for some prime p, the integer a_p has at least two distinct prime divisors. Then if $p_1, \dots, p_k$ were a list of all the primes, the integer

$$a_{p_1} a_{p_2} \cdots a_{p_k}$$

would possess at least $k+1$ prime factors: indeed, each factor exceeds 1, the factors are pairwise relatively prime, and one of the factors is divisible by two distinct primes. So there are $k+1 > k$ primes, a contradiction.

It remains to construct such a sequence. We leave to the reader the easy exercise of showing that $a_n = 2^n - 1$ has the desired properties (note that $a_{11} = 23 \cdot 89$). The original version of this argument, where a_n is instead chosen as the nth Fibonacci number, is due to Wunderlich [**Wun65**]. The generalization presented here is that of Hemminger [**Hem66**].

Saidak [**Sai06**] has recently given a very simple argument making use of coprimality. Start with a natural number $n > 1$. Because n and $n+1$ are coprime, the number $N_2 := n(n+1)$ must have at least two distinct prime factors. By the same reasoning,

$$N_3 := N_2(N_2+1) = n(n+1)(n(n+1)+1)$$

must have at least three distinct prime factors. In general, having constructed N_j with at least j different prime factors, the number $N_{j+1} := N_j(N_j+1)$ must have at least $j+1$.

4. The Euler-Riemann zeta function

For complex numbers s with real part greater than 1, define the zeta function by putting

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

(The condition that $\Re(s) > 1$ guarantees convergence of the series.) In the analytic approach to prime number theory, this function occupies a central position. Because of this text's emphasis on elementary methods, the zeta function will not play a large role for us, but it should be stressed that in many of the deeper investigations into the distribution of primes, the zeta function is an indispensable tool.

Riemann introduced the study of $\zeta(s)$ as a function of a complex variable in an 1859 memoir on the distribution of primes [**Rie59**]. But the connection between the zeta function and prime number theory goes back earlier. Over a hundred years prior to Riemann's study, Euler had looked at the same series for real s and had shown that [**Eul37**, Theorema 8]

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}} \quad (s > 1). \tag{1.2}$$

This is often called an analytic statement of unique factorization. To see why, notice that formally (i.e., disregarding matters of convergence)

$$\prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where a_n counts the number of factorizations of n into prime powers. Thus unique factorization, the statement that $a_n = 1$ for all n, is equivalent to the statement that (1.2) holds as a formal product of Dirichlet series.[1] This, in turn, is equivalent to the validity of (1.2) for all real $s > 1$ (or even a sequence of s tending to ∞) by a standard result in the theory of Dirichlet series (see, e.g., [**Apo76**, Theorem 11.3]).

Euler's product expansion of the zeta function is the first example of what is now called an *Euler factorization*. We now prove (following [**Hua82**]) a theorem giving general conditions for the validity of such factorizations.

Theorem 1.2 (Euler factorizations)**.** *Let f be a multiplicative function. Then*

$$\sum_{n=1}^{\infty} f(n) = \prod_p \left(1 + f(p) + f(p^2) + \cdots\right) \tag{1.3}$$

if either of the following two conditions holds:

(i) $\sum_{n=1}^{\infty} |f(n)|$ *converges.*
(ii) $\prod_p \left(1 + |f(p)| + |f(p^2)| + \cdots\right)$ *converges.*

[1] Here a *Dirichlet series* is a series of the form $F(s) = \sum_{n=1}^{\infty} c_n/n^s$, where each c_n is a complex number.

Remark. Without imposing a condition such as (i) or (ii), it is possible for either the series or the product in (1.3) to converge while the other diverges, or for both to converge without being equal. See [**Win43**, §15] for explicit examples.

If f is not merely multiplicative but completely multiplicative, then the factors in (1.3) form a geometric series whose convergence is implied by either of the above conditions. Thus we have the following consequence:

Corollary 1.3. *Let f be a completely multiplicative function. Then*

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \frac{1}{1 - f(p)}$$

subject to either of the two convergence criteria of Theorem 1.2.

The factorization (1.2) of the zeta function is immediate from this corollary: One takes $f(n) = 1/n^s$ and observes that for $s > 1$, condition (i) holds (for example) by the integral test.

Proof of Theorem 1.2. Suppose that condition (i) holds and set $S_0 := \sum_{n=1}^{\infty} |f(n)|$. For each prime p, the series $\sum_{k=0}^{\infty} f(p^k)$ converges absolutely, since $\sum_{k=0}^{\infty} |f(p^k)| \leq S_0$. Therefore

$$P(x) = \prod_{p \leq x} \left(1 + f(p) + f(p^2) + \cdots\right)$$

is a finite product of absolutely convergent series. It follows that

$$P(x) = \sum_{n: p | n \Rightarrow p \leq x} f(n).$$

If we now set $S = \sum_{n=1}^{\infty} f(n)$ (which converges absolutely), we have

$$S - P(x) = \sum_{n: p|n \text{ for some } p > x} f(n),$$

which shows

$$|S - P(x)| \leq \sum_{n > x} |f(n)| \to 0$$

as $x \to \infty$. Thus $P(x) \to S$ as $x \to \infty$, which is the assertion of (1.3).

Now suppose that (ii) holds. We shall show that (i) holds as well, so that the theorem follows from what we have just done. To see this, let

$$P_0 = \prod_{p} \left(1 + |f(p)| + |f(p^2)| + \cdots\right),$$

and let

$$P_0(x) := \prod_{p \le x} \left(1 + |f(p)| + |f(p^2)| + \cdots\right)$$
$$= \sum_{n : p | n \Rightarrow p \le x} |f(n)| \ge \sum_{n \le x} |f(n)|.$$

Since $P_0(x) \le P_0$ for all x, the partial sums $\sum_{n \le x} |f(n)|$ form a bounded increasing sequence. Thus $\sum |f(n)|$ converges, proving (i). □

We can now present Euler's first proof of the infinitude of the primes.

Euler's first proof of Theorem 1.1. Let f be defined by $f(n) = 1/n$ for every n. Assuming that there are only finitely many primes, condition (ii) of Theorem 1.3 is trivially satisfied, as the product in question only has finitely many terms. It follows that

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) < \infty,$$

in contradiction with the well-known divergence of the harmonic series. □

As pointed out by Euler, this proof gives a much stronger result than that asserted in Theorem 1.1.

Theorem 1.4. *The series $\sum \frac{1}{p}$ diverges, where the sum extends over all primes p.*

Proof. Suppose not and let $C = \sum 1/p$. As in the last proof, we take $f(n) = 1/n$ and apply Theorem 1.2. Let us check that condition (ii) of that theorem holds here. First, notice that

$$\prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \prod_{p \le x} \frac{1}{1 - \frac{1}{p}} = \prod_{p \le x} \left(1 + \frac{1}{p-1}\right) \le \prod_{p \le x} \left(1 + \frac{2}{p}\right).$$

Now recall that $e^t \ge 1 + t$ for every nonnegative t; this is clear from truncating the Taylor expansion $e^t = 1 + t + t^2/2! + \ldots$. It follows that

$$\prod_{p \le x} \left(1 + \frac{2}{p}\right) \le \prod_{p \le x} e^{2/p} = \exp\left(\sum_{p \le x} 2/p\right) \le \exp(2C).$$

Consequently, the partial products

$$\prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right)$$

form a bounded, increasing sequence, which shows that we have condition (ii). We conclude that

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p} \frac{1}{1-\frac{1}{p}} \leq \exp(2C),$$

a contradiction. □

Tweaking this argument, it is possible to derive an explicit lower bound on the partial sums $\sum_{p \leq x} 1/p$: Note that for $x \geq 2$,

$$\prod_{p \leq x} \frac{1}{1-\frac{1}{p}} = \sum_{n: p \mid n \Rightarrow p \leq x} \frac{1}{n} \geq \sum_{n \leq x} \frac{1}{n} \geq \log x. \tag{1.4}$$

From the upper bound $(1-1/p)^{-1} = (1+1/(p-1)) \leq \exp((p-1)^{-1})$, we deduce (taking the logarithm of (1.4)) that $\sum_{p \leq x} (p-1)^{-1} \geq \log\log x$. To derive a lower bound for $\sum_{p \leq x} 1/p$ from this, note that

$$\begin{aligned}\sum_{p \leq x} \frac{1}{p} &= \sum_{p \leq x} \frac{1}{p-1} - \sum_{p \leq x} \left(\frac{1}{p-1} - \frac{1}{p}\right) \\ &\geq \sum_{p \leq x} \frac{1}{p-1} - \sum_{n \geq 2} \left(\frac{1}{n-1} - \frac{1}{n}\right) = \left(\sum_{p \leq x} \frac{1}{p-1}\right) - 1 \geq \log\log x - 1.\end{aligned}$$

The next two proofs also make use of the zeta function and its Euler factorization, but in a decidedly different manner.

Proof of J. Hacks. We need the well-known result, also due to Euler, that $\zeta(2) = \pi^2/6$; a proof is sketched in Exercise 6 (for alternative arguments see [**AZ04**, Chapter 7], [**Cha03**]). Plugging $s = 2$ into the Euler factorization (1.2) we obtain

$$\frac{\pi^2}{6} = \zeta(2) = \prod_{p} \frac{1}{1-\frac{1}{p^2}}.$$

If there are only finitely many primes, then the product appearing here is a finite product of rational numbers, so that $\pi^2/6$ must also be a rational number. But this is impossible, since π is well known to be a *transcendental number*, i.e., not the root of any nonzero polynomial with rational coefficients.

The known proofs of the transcendence of π rely fairly explicitly on the infinitude of primes, so it is somewhat dangerous to appeal to this result directly. However, a weaker result which does not rely in an obvious way on this fact, and which nevertheless suffices for the current application, appears as Exercise 7 (cf. [**AZ04**, Chapter 6, Theorem 2]). □

One can give a similar argument avoiding irrationality considerations:

Proof. We use not only that $\zeta(2) = \pi^2/6$ but also that $\zeta(4) = \pi^4/90$. (Again see Exercise 6.) Thus $\zeta(2)^2/\zeta(4) = 5/2$. The Euler factorization (1.2) implies that

$$\frac{5}{2} = \frac{\zeta(2)^2}{\zeta(4)} = \prod_p (1-p^{-4})(1-p^{-2})^{-2} = \prod_p \frac{p^4-1}{p^4}\frac{p^4}{(p^2-1)^2} = \prod_p \frac{p^2+1}{p^2-1},$$

so that

$$\frac{5}{2} = \frac{5}{3}\cdot\frac{10}{8}\cdot\frac{26}{24}\cdots.$$

If there are only finitely many primes, then the product on the right-hand side is a finite one and can be written as M/N, where $M = 5\cdot 10\cdot 26\cdots$ and $N = 3\cdot 8\cdot 24\cdots$. Then $M/N = 5/2$, so $2M = 5N$. Since $3 \mid N$, it must be that $3 \mid M$. But this cannot be: M is a product of numbers of the form k^2+1, and no such number is a multiple of 3. $\square$

Wagstaff has asked whether one can give a more elementary proof that $5/2 = \prod_p \frac{p^2+1}{p^2-1}$. The discussion of this (open) question in [**Guy04**, B48] was the motivation for the preceding proof of Theorem 1.1.

5. Squarefree and smooth numbers

Recall that a natural number n is said to be *squarefree* if it is not divisible by the square of any integer larger than 1. The fundamental theorem of arithmetic shows that there is a bijection

$$\{\text{finite subsets of the primes}\} \longleftrightarrow \{\text{squarefree positive integers}\},$$

given by sending

$$S \longmapsto \prod\nolimits_{p\in S} p.$$

So to prove the infinitude of the primes, it suffices to prove that there are infinitely many positive squarefree integers.

J. Perott's proof, 1881. We sieve out the non-squarefree integers from $1,\dots,N$ by removing those divisible by 2^2, then those divisible by 3^2, etc. The number of removed integers is bounded above by

$$\sum_{k=2}^{\infty} \lfloor N/k^2 \rfloor \le N\sum_{k=2}^{\infty} k^{-2} = N(\zeta(2)-1),$$

so that the number of squarefree integers up to N, say $A(N)$, satisfies

$$A(N) \ge N - N(\zeta(2)-1) = N(2-\zeta(2)). \tag{1.5}$$

At this point Perott uses the evaluation $\zeta(2) = \pi^2/6$. However, it is simpler to proceed as follows: Since t^{-2} is a decreasing function of t on the positive real axis,

$$\zeta(2) = 1 + \sum_{n=2}^{\infty} \frac{1}{n^2} < 1 + \sum_{n=1}^{\infty} \int_n^{n+1} \frac{dt}{t^2} = 1 + \int_1^{\infty} \frac{dt}{t^2} = 2.$$

Referring back to (1.5), we see that $A(N)/N$ is bounded below by a positive constant. In particular, it must be that $A(N) \to \infty$ as $N \to \infty$. $\square$

Remark. As observed by Dressler [**Dre75**], Perott's argument also yields a lower bound on $\pi(N)$. Note that since every squarefree number $\leq N$ is a product of some subset of the $\pi(N)$ primes up to N, we have $2^{\pi(N)} \geq A(N)$. The argument above establishes that $A(N) \geq cN$ for $c = 2 - \zeta(2) > 0$, and so $\pi(N) \geq \log N/\log 2 + O(1)$.

For the next proof we need the following simple lemma:

Lemma 1.5. *Every natural number n can be written in the form rs^2, where r and s are natural numbers and r is squarefree.*

Proof. Choose the positive integer s so that s^2 is the largest perfect square dividing n, and put $r = n/s^2$. We claim that r is squarefree. Otherwise $p^2 \mid r$ for some prime p. But then $(ps)^2 \mid n$, contrary to the choice of s. $\square$

Erdős's proof of Theorem 1.1. Let N be a positive integer. There are at most $\sqrt{N}$ squares not exceeding N and at most $2^{\pi(N)}$ squarefree integers below this bound. So Lemma 1.5 implies that

$$2^{\pi(N)}\sqrt{N} \geq N.$$

Dividing by $\sqrt{N}$ and taking logarithms yields the lower bound $\pi(N) \geq \log N/\log 4$. $\square$

A modification of this argument leads to another proof that $\sum \frac{1}{p}$ diverges:

Erdős's proof of Theorem 1.4. Suppose that $\sum 1/p$ converges. Then we can choose an M for which

$$\sum_{p>M} \frac{1}{p} < \frac{1}{2}. \tag{1.6}$$

Keep this M fixed.

Let N be an arbitrary natural number. The estimate (1.6) implies that most integers up to N factor completely over the primes not exceeding M.

Indeed, the number of integers not exceeding N that have a prime factor $p > M$ is bounded above by

$$\sum_{M<p\leq N} \left\lfloor \frac{N}{p} \right\rfloor \leq N \sum_{p>M} \frac{1}{p} < N/2,$$

so that more than $N/2$ of the natural numbers not exceeding N are divisible only by primes $p \leq M$.

We now show that there are too few integers divisible only by primes $p \leq M$ for this to be possible. There are at most $\sqrt{N}$ squares not exceeding N and at most $C := 2^{\pi(M)}$ squarefree numbers composed only of primes not exceeding M. Thus, there are at most $C\sqrt{N}$ natural numbers $\leq N$ having all their prime factors $\leq M$. But $C\sqrt{N} < N/2$ once $N > 4C^2$. □

In the last argument we needed an estimate for the number of integers up to a given point with only small prime factors. This motivates the following definition: Call a natural number *y-smooth* if all of its prime factors are bounded by y. We let $\Psi(x, y)$ denote the number of y-smooth numbers not exceeding x; i.e.,

$$\Psi(x, y) := \#\{n \leq x : p \mid n \Rightarrow p \leq y\}. \tag{1.7}$$

Smooth numbers are important auxiliary tools in many number-theoretic investigations, and so there has been quite a bit of work on estimating the size of $\Psi(x, y)$ in various ranges of x and y. (For a survey of both the applications and the estimates, see [**Gra08b**].) A trivial estimate yields an easy proof of Theorem 1.1.

Lemma 1.6. *For $x \geq 1$ and $y \geq 2$, we have*

$$\Psi(x, y) \leq \left(1 + \frac{\log x}{\log 2}\right)^{\pi(y)}.$$

Proof. Let $k = \pi(y)$. By the fundamental theorem of arithmetic, $\Psi(x, y)$ is the number of k-tuples of nonnegative integers $e_1, \ldots, e_k$ with

$$p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \leq x.$$

This inequality requires $p_i^{e_i} \leq x$, so that

$$e_i \leq \log x / \log p_i \leq \log x / \log 2,$$

so that there are at most $1 + \lfloor \log x / \log 2 \rfloor$ possibilities for each e_i. □

Since every positive integer not exceeding N is a (possibly empty) product of primes not exceeding N,

$$N = \Psi(N, N) \leq (1 + \log N / \log 2)^{\pi(N)}.$$

It follows that

$$\pi(N) \geq \frac{\log N}{\log(1 + \log N/\log 2)}.$$

Taking some care to estimate the denominator, we obtain the lower bound

$$\pi(N) \geq (1 + o(1))\frac{\log N}{\log\log N},$$

which tends to infinity. Similar proofs of Theorem 1.1 have been given by Thue (1897), Auric (1915), Schnirelmann [**Sch40**, pp. 44–45], Chernoff [**Che65**], and Rubinstein [**Rub93**]. See also Exercise 19.

6. Sledgehammers!

In the spirit of the saying, "nothing is too simple to be made complicated," we finish off the first half of this chapter with three proofs of Theorem 1.1 that dip into the tool chest of higher mathematics.

We start with a proof that uses a bit of analysis, taken from [**Pol11b**]. For an arithmetic function f (i.e., a function $f\colon \mathbf{N} \to \mathbf{C}$), we define its *Möbius transform* $\hat{f}$ by $\hat{f}(n) := \sum_{d|n} \mu(d) f(n/d)$. By the *support* of f, we mean the set of natural numbers n with $f(n) \neq 0$. The key ingredient in our proof is the following "uncertainly principle" for the Möbius transform:

Lemma 1.7. *Suppose that f is an arithmetic function for which both f and $\hat{f}$ are of finite support. Then f vanishes identically.*

Proof. Let $F(z)$ denote the polynomial $\sum_{n=1}^{\infty} f(n) z^n$. From the Möbius inversion formula, we have the identity $f(n) = \sum_{d|n} \hat{f}(d)$. Hence, for $|z| < 1$,

$$\begin{aligned} F(z) = \sum_{n=1}^{\infty} f(n) z^n &= \sum_{n=1}^{\infty} \left(\sum_{d|n} \hat{f}(d) \right) z^n \\ &= \sum_{d=1}^{\infty} \hat{f}(d) \sum_{\substack{n=1 \\ d|n}}^{\infty} z^n = \sum_{d=1}^{\infty} \hat{f}(d) \frac{z^d}{1 - z^d}. \end{aligned}$$

(The interchange of summation is easily justified by our assumption that $\hat{f}$ is of finite support.) We deduce from this alternative expression for F that $\hat{f}$ must vanish identically: Indeed, if there is any d with $\hat{f}(d) \neq 0$, then there is a largest such d. For this d, the function F has a pole at the primitive dth root of unity $z = e^{2\pi i/d}$. But F, being a polynomial function, is entire! So $\hat{f}$ vanishes identically and (by Möbius inversion again) so does f. ☐

Now define f so that $f(1) = 1$ and $f(n) = 0$ for $n > 1$. Then $\hat{f} = \mu$. Since f is of finite support, $\mu = \hat{f}$ cannot be. Thus, there are infinitely many squarefree integers and so also infinitely many primes.

Our second proof uses the language of topology and is due to Furstenberg [**Fur55**]:

Proof. We put a topology on $\mathbf{Z}$ by taking as a basis for the open sets all arithmetic progressions, infinite in both directions. (This is permissible since the intersection of two such progressions is either empty or is itself an arithmetic progression.) Then each arithmetic progression is both open and closed: it is open by choice of the basis, and it is closed since its complement is the union of the other arithmetic progressions with the same common difference. For each prime p, let $A_p = p\mathbf{Z}$, and define $A := \bigcup_p A_p$. The set $\{-1, 1\} = \mathbf{Z} \setminus A$ is not open. (Indeed, each open set is either empty or contains an arithmetic progression, so must be infinite.) It follows that A is not closed. On the other hand, if there are only finitely many primes, then A is a finite union of closed sets, and so it *is* closed. $\square$

Our final argument, due to L. Washington (and taken from [**Rib96**]) uses the machinery of commutative algebra. Recall that a *Dedekind domain* is an integral domain R with the following three properties:

(i) R is *Noetherian*: if $I_1 \subset I_2 \subset I_3 \subset \cdots$ is an ascending chain of ideals of R, then there is an n for which

$$I_n = I_{n+1} = I_{n+2} = \cdots .$$

(ii) R is *integrally closed*: if K denotes the fraction field of R and $\alpha \in K$ is the root of a monic polynomial with coefficients in R, then in fact $\alpha \in R$.

(iii) Every nonzero prime ideal of R is a maximal ideal.

Proof. We use the theorem that a Dedekind domain with finitely many nonzero prime ideals is a principal ideal domain (see, e.g., [**Lor96**, Proposition III.2.12]) and thus also a unique factorization domain. The ring of integers $\mathfrak{O}_K$ of a number field K is always a Dedekind domain; consequently, if K does not possess unique factorization, then $\mathfrak{O}_K$ has infinitely many nonzero prime ideals. Each such prime ideal lies above a rational prime p, and for each prime p there are at most $[K : \mathbf{Q}]$ prime ideals lying above it. It follows that there are infinitely many primes p, provided that there is a single number field K for which $\mathfrak{O}_K$ does not possess unique factorization. And there is: If $K = \mathbf{Q}(\sqrt{-5})$, then

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

is a well-known instance of the failure of unique factorization in $\mathfrak{O}_K = \mathbf{Z}[\sqrt{-5}]$. $\square$

7. Prime-producing formulas

> A mathematician is a conjurer who gives away his secrets. – J. H. Conway

Now that we know there are infinitely many primes, the next question is: Where are they hiding? Or, to ask a question that has ensnared many who have flirted with number theory: Is there a formula for producing primes? This line of inquiry, as natural as it seems, has not been very productive.

The following 1952 result of Sierpiński [**Sie52**] is representative of many in this subject. Let p_n denote the nth prime number. Define a real number ξ by putting

$$\xi := \sum_{n=1}^{\infty} p_n 10^{-2^n} = 0.0203000500000007000000000000000011\ldots.$$

★ **Theorem 1.8.** *We have*

$$p_n = \left\lfloor 10^{2^n}\xi \right\rfloor - 10^{2^{n-1}} \left\lfloor 10^{2^{n-1}}\xi \right\rfloor.$$

This is, in the literal sense, a formula for primes. But while it may have some aesthetic merit, it must be considered a complete failure from the standpoint of utility; determining the number ξ seems to require us to already know the sequence of primes. A similar criticism can be leveled against a result of Mills [**Mil47**], which asserts the existence of a real number $A > 1$ with the property that $\lfloor A^{3^n} \rfloor$ is prime for each natural number n.

A more surprising way of generating primes was proposed by J. H. Conway [**Con87**]. Consider the following list of 14 fractions:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
$\frac{17}{91}$	$\frac{78}{85}$	$\frac{19}{51}$	$\frac{23}{38}$	$\frac{29}{33}$	$\frac{77}{29}$	$\frac{95}{23}$	$\frac{77}{19}$	$\frac{1}{17}$	$\frac{11}{13}$	$\frac{13}{11}$	$\frac{15}{2}$	$\frac{1}{7}$	$\frac{55}{1}$

Now run the following algorithm: Beginning with the number 2, look for the first (leftmost) fraction which can be multiplied by the current number to give an integer. Perform the multiplication and repeat. Whenever you reach a power of 2, output the exponent. The first several (19) steps of the algorithm are

$$\begin{aligned} 2 &\mapsto 15 \mapsto 825 \mapsto 725 \mapsto 1925 \mapsto 2275 \mapsto 425 \mapsto 390 \mapsto 330 \mapsto 290 \mapsto 770 \\ &\mapsto 910 \mapsto 170 \mapsto 156 \mapsto 132 \mapsto 116 \mapsto 308 \mapsto 364 \mapsto 68 \mapsto 4 = 2^2, \end{aligned}$$

and so the first output is 2. Fifty more steps yield

$$2^2 \mapsto 30 \mapsto 225 \mapsto 12375 \mapsto \cdots \mapsto 232 \mapsto 616 \mapsto 728 \mapsto 136 \mapsto 8 = 2^3,$$

and so the second output is 3. After another 212 steps, we arrive at $32 = 2^5$, and so our third output is 5.

★ **Theorem 1.9** (Conway). *The sequence of outputs is exactly the sequence of primes in increasing order.*

This is rather striking; the sequence of primes, which seems random in so many ways, is the output of a deterministic algorithm involving 14 fractions. But perhaps this should not come as such a shock. Most anyone who has experimented with programming knows that the primes are the output of a deterministic algorithm: Test the numbers $2, 3, 4, \ldots$ successively for primality, using (say) trial division for the individual tests. And actually, underneath the surface, this is exactly what is being done in Conway's algorithm. This sequence of 14 fractions encodes a simple computer program: The number n is tested for divisibility first by $d = n - 1$, then $d = n - 2$, etc; as soon as a divisor is found, n is incremented by 1 and the process is repeated. The game is rigged so that a power of 2 arises only when d reaches 1, i.e., when n is prime. Moreover, there is nothing special in Theorem 1.9 about the sequence of primes; an analogue of Theorem 1.9 can be proved for any recursive set. (Here a set of natural numbers S is called *recursive* if there is an algorithm for determining whether a natural number belongs to S.) We conclude that while Conway's result *is* genuinely surprising, the surprise is that one can simulate computer programs with lists of fractions, and is in no way specific to the prime numbers.

8. Euler's prime-producing polynomial

The prime-producing functions we have been considering up to now have all been rather complicated. In some sense this is necessary; one can show that any function which produces only primes cannot have too simple a form. We give only one early example of a result in this direction. (See [**War30**], [**Rei43**] for more theorems of this flavor.)

Theorem 1.10 (Goldbach). *If $F(T) \in \mathbf{Z}[T]$ is a nonconstant polynomial with positive leading coefficient, then $F(n)$ is composite for infinitely many natural numbers n.*

Proof. Suppose F is nonconstant but that $F(n)$ is prime for all $n \geq N_0$, where N_0 is a natural number. Let $p = F(N_0)$; then p divides $F(N_0 + kp)$ for every positive integer k. But since F has a positive leading coefficient, $F(N_0 + kp) > p$ for every sufficiently large integer k, and so $F(N_0 + kp)$ is composite, contrary to the choice of N_0. □

Theorem 1.10 does not forbid the existence of polynomials F which assume prime values over impressively long stretches. And indeed these do exist; a famous example is due to Euler, who observed that if $f(T) = T^2 + T + 41$, then $f(n)$ is prime for all integers $0 \le n < 40$.

It turns out that Euler's observation, rather than being an isolated curiosity, is intimately connected with the theory of imaginary quadratic fields. We will prove the following theorem:

Theorem 1.11. *Let $A \ge 2$, and set $D := 1 - 4A$. Then the following are equivalent:*

(i) $n^2 + n + A$ *is prime for all* $0 \le n < A - 1$,

(ii) $n^2 + n + A$ *is prime for all* $0 \le n \le \frac{1}{2}\sqrt{\frac{|D|}{3}} - \frac{1}{2}$,

(iii) *the ring* $\mathbf{Z}[(-1 + \sqrt{D})/2]$ *is a unique factorization domain.*

The equivalence (i) $\Leftrightarrow$ (iii) is proved by Rabinowitsch in [**Rab13**], and is usually referred to as *Rabinowitsch's theorem.*

Remark. Since $n^2 + n + A = (n + 1/2)^2 + (4A - 1)/4$, (ii) can be rephrased as asserting that $(n + 1/2)^2 + |D|/4$ is prime for every integer n for which $|n + 1/2| \le \frac{1}{2}\sqrt{\frac{|D|}{3}}$. We will use this observation in the proof of Theorem 1.11.

Cognoscenti will recognize that $\mathbf{Z}[(-1 + \sqrt{D})/2]$ is an order in the quadratic field $\mathbf{Q}(\sqrt{D})$. However, the proof of Theorem 1.11 presented here, due to Gyarmati (née Lanczi) [**Lán65**], [**Gya83**] and Zaupper [**Zau83**], requires neither the vocabulary of algebraic number theory nor the theory of ideals.

We begin the proof of Theorem 1.11 by observing that the bound on n in (ii) is always at least as strict as the bound on n in (i), which makes clear that (i) implies (ii). So it is enough to show that (ii) implies (iii) and that (iii) implies (i). To continue we need some preliminary results on the arithmetic of the rings $\mathbf{Z}[(-1 + \sqrt{D})/2]$. These will be familiar to students of algebraic number theory, but we include full proofs for the sake of completeness.

Let $A \ge 2$ be an integer, and fix a complex root η of $x^2 + x + A$, so that (for an appropriate choice of the square root) $\eta = (-1 + \sqrt{D})/2$. Since $\eta^2 = -\eta - A$, it follows that

$$\mathbf{Z}[\eta] = \mathbf{Z} + \mathbf{Z}\eta = \{x + y\eta : x, y \in \mathbf{Z}\}.$$

For $\alpha \in \mathbf{Z}[\eta]$, we denote its complex conjugate by $\overline{\alpha}$. Observe that $\overline{\eta} = -1 - \eta$; consequently, $\mathbf{Z}[\eta]$ is closed under complex-conjugation. We define the *norm* of the element $\alpha = x + y\eta \in \mathbf{Z}[\eta]$ by

$$\begin{aligned} \mathscr{N}(\alpha) &:= |\alpha|^2 \\ &= \alpha\overline{\alpha} = x^2 - xy + Ay^2. \end{aligned}$$

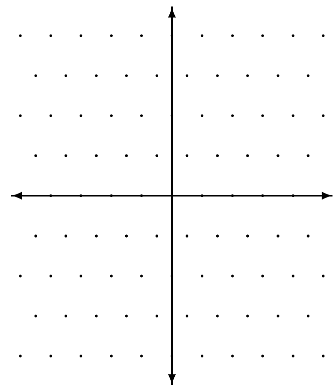

Figure 1. The lattice $\mathbf{Z}+\mathbf{Z}\eta$ sitting inside $\mathbf{C}$. Here $A=2$ so that $D=-7$.

Notice that the norm of $\alpha \in \mathbf{Z}[\eta]$ is always an integer and is positive whenever $\alpha \neq 0$. Moreover, since the complex absolute value is multiplicative, it is immediate that

$$\mathscr{N}(\alpha\beta) = \mathscr{N}(\alpha)\cdot\mathscr{N}(\beta) \quad \text{for all} \quad \alpha,\beta \in \mathbf{Z}[\eta].$$

We now recall the requisite definitions from ring theory: If $\alpha,\beta \in \mathbf{Z}[\eta]$, we say that α *divides* β if $\beta = \alpha\gamma$ for some $\gamma \in \mathbf{Z}[\eta]$. A nonzero element $\alpha \in \mathbf{Z}[\eta]$ is called a *unit* if α divides 1. A nonunit element $\alpha \in \mathbf{Z}[\eta]$ is *irreducible* if whenever $\alpha = \beta\gamma$ with $\beta,\gamma \in \mathbf{Z}[\eta]$, then either β is a unit or γ is a unit. Finally, $\pi \in \mathbf{Z}[\eta]$ is called *prime* if whenever π divides $\beta\gamma$ for $\beta,\gamma \in \mathbf{Z}[\eta]$, then either π divides β or π divides γ.

Lemma 1.12. *An element $\alpha \in \mathbf{Z}[\eta]$ is a unit precisely when $\mathscr{N}(\alpha) = 1$. The only units in $\mathbf{Z}[\eta]$ are ± 1.*

Proof. If α is a unit, then $\mathscr{N}(\alpha)\cdot\mathscr{N}(\alpha^{-1}) = 1$. Moreover, both $\mathscr{N}(\alpha)$ and $\mathscr{N}(\alpha^{-1})$ are positive integers, so that $\mathscr{N}(\alpha) = \mathscr{N}(\alpha^{-1}) = 1$. Conversely, if $\mathscr{N}(\alpha) = 1$, then $\alpha\overline{\alpha} = 1$, and so α is a unit. Finally, notice that if $y \neq 0$, then

$$\mathscr{N}(x+y\eta) = x^2 - xy + Ay^2 = (x-y/2)^2 + \frac{1}{4}(4A-1)y^2 \geq \frac{4A-1}{4} \geq \frac{7}{4} > 1.$$

So $x + y\eta$ can be a unit only when $y = 0$. In this case we must have $\mathscr{N}(x) = x^2 = 1$, and this occurs exactly when $x = \pm 1$. □

Lemma 1.13. *If α is a nonzero, nonunit element of $\mathbf{Z}[\eta]$, then α can be written as a product of irreducible elements of $\mathbf{Z}[\eta]$.*

Proof. If the claim fails, there is a nonzero, nonunit α of smallest norm for which it fails. Clearly α is not irreducible, and so we can write $\alpha = \beta\gamma$, where β and γ are nonzero nonunits. Hence $\mathscr{N}(\alpha) = \mathscr{N}(\beta)\mathscr{N}(\gamma)$. Since $\mathscr{N}(\beta)$ and $\mathscr{N}(\gamma)$ are each larger than 1, both $\mathscr{N}(\beta)$ and $\mathscr{N}(\gamma)$ must be smaller than $\mathscr{N}(\alpha)$. So by the choice of α, both β and γ factor as products of irreducibles, and thus α does as well. This contradicts the choice of α. $\square$

We can now prove one of the two outstanding implications:

Proof that (iii) $\Rightarrow$ (i). Let $\eta = (-1+\sqrt{D})/2$. Suppose $0 \le n < A-1$. We have

$$n^2 + n + A = (n-\eta)(n-\bar{\eta}) = (n-\eta)(n+1+\eta). \tag{1.8}$$

Let p be a prime dividing n^2+n+A. We claim that p is not irreducible in $\mathbf{Z}[\eta]$. Indeed, since $\mathbf{Z}[\eta]$ is a unique factorization domain by hypothesis, if p were irreducible, then p would be prime. So from (1.8), we would have that p divides $n-\eta$ or $n+1+\eta$. But this is impossible, since neither $n/p - \eta/p$ nor $(n+1)/p + \eta/p$ belongs to $\mathbf{Z}[\eta] = \mathbf{Z} + \mathbf{Z}\eta$.

Hence we can write $p = \alpha\beta$, where $\alpha, \beta \in \mathbf{Z}[\eta]$ and neither α nor β is a unit. Taking norms, we deduce that $p^2 = \mathscr{N}(p) = \mathscr{N}(\alpha)\mathscr{N}(\beta)$. Since α and β are not units, we must have $\mathscr{N}(\alpha) = \mathscr{N}(\beta) = p$.

Write $\alpha = x + y\eta$ for integers x, y. Then $y \neq 0$ (since p is a rational prime), and so

$$p = N(\alpha) = x^2 - xy + Ay^2 = (x - y/2)^2 + (A - 1/4)y^2 \ge A - 1/4.$$

Thus (since p is an integer) $p \ge A$. Moreover, since $0 \le n < A-1$,

$$n^2 + n + A < (A-1)^2 + (A-1) + A = (A-1)A + A = A^2.$$

This shows that every prime divisor of n^2+n+A exceeds its square root, so that n^2+n+A is prime. $\square$

The proof of the remaining implication requires one more preliminary result:

Lemma 1.14. *If π is an element of $\mathbf{Z}[\eta]$ whose norm is a rational prime p, then π is prime in $\mathbf{Z}[\eta]$.*

Proof. We claim that $\mathbf{Z}[\eta]/(\pi)$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$. Since $\mathbf{Z}/p\mathbf{Z}$ is a field, this implies that π generates a prime ideal of $\mathbf{Z}[\eta]$, which in turn implies that π is prime. Let $\psi\colon \mathbf{Z} \to \mathbf{Z}[\eta]/(\pi)$ be the ring homomorphism defined by mapping n to $n \bmod \pi$. Since $p = \pi\bar{\pi} \equiv 0 \pmod{\pi}$, the kernel of ψ contains the ideal $p\mathbf{Z}$. Since $p\mathbf{Z}$ is a maximal ideal, either ψ is identically zero or the kernel of ψ is precisely $p\mathbf{Z}$. Since π is not a unit in $\mathbf{Z}[\eta]$, $\psi(1)$ is nonzero, and so the kernel of ψ is precisely $p\mathbf{Z}$. Hence $\mathbf{Z}/p\mathbf{Z}$ is isomorphic to the image of ψ. So the proof will be complete if we show that ψ is surjective.

Write $\pi = r + s\eta$ for integers r and s, and let $x + y\eta$ be an arbitrary element of $\mathbf{Z}[\eta]$. We can choose integers a and b for which

$$m := x + y\eta - \pi(a + b\eta) \in \mathbf{Z}.$$

Indeed, a short computation shows that this containment holds precisely when

$$b(r - s) + as = y,$$

which is a solvable linear Diophantine equation in a and b since $\gcd(r-s, s) = \gcd(r, s) = 1$. Then $m \equiv x + y\eta \pmod{\pi}$, and so $\psi(m) = x + y\eta \bmod \pi$. Since $x + y\eta$ was arbitrary, ψ is surjective as claimed. $\square$

Proof that (ii) $\Rightarrow$ (iii). Suppose that $n^2 + n + A$ is prime for all

$$0 \le n \le \frac{1}{2}\sqrt{\frac{|D|}{3}} - \frac{1}{2}.$$

We are to prove that $\mathbf{Z}[\eta]$ possesses unique factorization. Suppose otherwise, and let α be a nonzero, nonunit of minimal norm with two distinct factorizations into irreducibles, say

$$\alpha = \pi_1 \cdots \pi_k = \rho_1 \cdots \rho_j.$$

(Here *distinct* means that either $k \neq j$, or that $k = j$, but there is no way to reorder the π_i so that each π_i is a unit multiple of ρ_i.) By the minimality of $\mathscr{N}(\alpha)$, it is easy to see that none of the irreducibles in the first factorization can be a unit multiple of an irreducible in the second factorization. Consequently, none of the irreducibles appearing in either factorization can be prime in $\mathbf{Z}[\eta]$.

We can assume that $\mathscr{N}(\pi_1) \le \mathscr{N}(\rho_1)$. (If this does not hold initially, interchange the two factorizations.) For $\xi, \gamma \in \mathbf{Z}[\eta]$ still to be chosen, define

$$\alpha' := (\rho_1\xi - \pi_1\gamma)\rho_2 \cdots \rho_j. \tag{1.9}$$

Then

$$\begin{aligned} \alpha' &= \alpha\xi - \pi_1\frac{\alpha}{\rho_1}\gamma \\ &= \pi_1(\pi_2 \cdots \pi_k\xi - \rho_2 \cdots \rho_j\gamma). \end{aligned}$$

Factoring the parenthetical expression, we deduce that α' has a factorization into irreducibles where one of the irreducibles is π_1. We will choose ξ and γ so that $\pi_1 \nmid \rho_1\xi$. Then $\pi_1 \nmid \rho_1\xi - \pi_1\gamma$, and so we may deduce from (1.9) that α' has a factorization into irreducibles, none of which is a unit multiple of π_1. So α' possesses two distinct factorizations into irreducibles. If further, γ and ξ satisfy

$$\mathscr{N}(\rho_1\xi - \pi_1\gamma) < \mathscr{N}(\rho_1),$$

then $\mathscr{N}(\alpha')$ is smaller than $\mathscr{N}(\alpha)$, and so we have a contradiction to our choice of α.

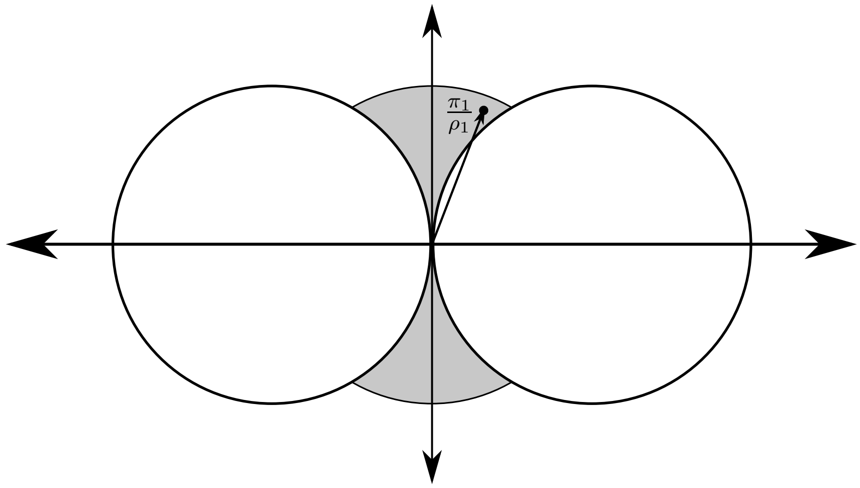

Figure 2. (Based on [**Zau83**].)

So it remains to show that it is possible to choose $\xi, \gamma \in \mathbf{Z}[\eta]$ with the following two properties:

(P1) $\pi_1 \nmid \rho_1\xi$,

(P2) $\mathscr{N}(\rho_1\xi - \pi_1\gamma) < \mathscr{N}(\rho_1)$, or equivalently, $\left|\xi - \frac{\pi_1}{\rho_1}\gamma\right| < 1$.

Since $\mathscr{N}(\pi_1) \le \mathscr{N}(\rho_1)$, the complex number π_1/ρ_1 lies on or inside the unit circle. Suppose first that π_1/ρ_1 lies outside the shaded region indicated in Figure 2. Then for either $\xi = 1$ or $\xi = -1$, we have

$$|\xi - \pi_1/\rho_1| < 1.$$

Then (P1) and (P2) hold if we choose this value of ξ and take $\gamma = 1$. Note that $\pi_1 \nmid \pm\rho_1$, since otherwise π_1 and ρ_1 would be unit multiples of each other, which we have already argued is not the case.

So we may assume that π_1/ρ_1 lies within the shaded region. Let e_1 be the ray from the origin making an angle of 60° with the x-axis, and let e_2 be the ray from the origin making an angle of 120° with that axis. Then the ray e (say) from the origin through π_1/ρ_1 is contained within the 60° angle determined by e_1 and e_2.[2] Let f be the horizontal line consisting of those complex numbers with imaginary part $\sqrt{|D|}/2$; thus f is the first horizontal line above the x-axis containing points of the lattice $\mathbf{Z} + \mathbf{Z}\eta$. Let μ be the complex number corresponding to the intersection of e and f. The angle determined by e_1 and e_2 cuts f into a segment of length $\sqrt{|D|/3} > 1$, and so there is a point of $\mathbf{Z} + \mathbf{Z}\eta$ on f within this angle. We choose such a point ξ for which the distance from ξ to μ is as small as possible. See Figure 3.

[2]Here the *angle determined by* e_1 *and* e_2 means the closed set of points between e_1 and e_2.

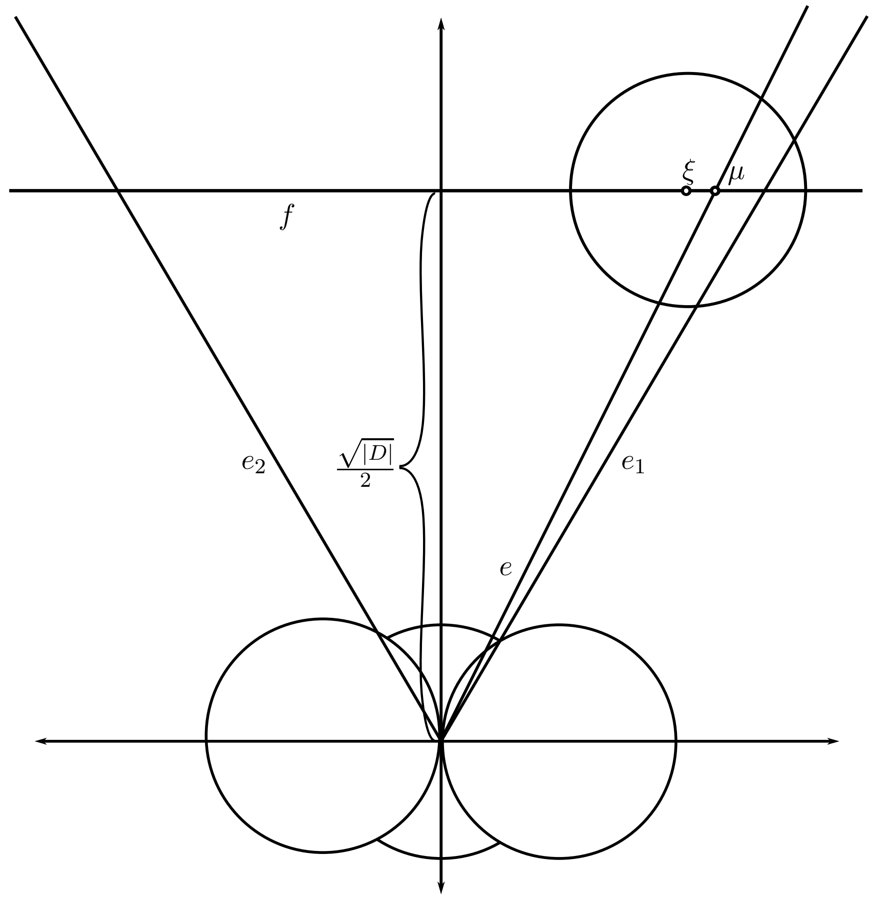

Figure 3. (Based on [**Zau83**].)

We claim that the distance from ξ to e is strictly smaller than $\sqrt{3}/2$. This is clear if both $\xi+1$ and $\xi-1$ fall within the angle determined by e_1 and e_2, since in that case, the distance from ξ to μ must be at most $1/2$. So suppose that $\xi+1$ falls outside this angle; the case when $\xi-1$ falls outside is analogous. Then $\xi-1$ must lie within the given angle. Now, if ξ is to the right of μ, then in order that ξ be at least as close to μ as $\xi-1$, it must be that the distance from ξ to μ is at most $1/2$. So we can assume that ξ falls to the left of μ. This is the scenario depicted in Figure 3. In this case we we use the following argument: Let ν represent the intersection of e_1 and f; then the distance between ξ and ν is smaller than 1. Since e_1 makes an angle of $60°$ with f, elementary trigonometry shows that the distance from ξ to e_1 is strictly smaller than $\sqrt{3}/2$. But the perpendicular line segment from ξ to e_1 meets e. So the distance from ξ to e is also strictly smaller than $\sqrt{3}/2$.

It follows that the unit disc centered at ξ intersects e in a segment of total length > 1. (Indeed, let τ be the point on e for which the line from ξ to τ is perpendicular to e, so that the distance from ξ to τ is strictly smaller than $\sqrt{3}/2$. Then by the Pythagorean theorem, τ divides the segment in question into two parts, each of length $> 1/2$.) Since $|\pi_1/\rho_1| \leq 1$, it follows that we can choose a rational integer γ so that $\gamma\pi_1/\rho_1$ lies within the open unit disc centered at ξ.

We claim that with the above choices of ξ and γ, both (P1) and (P2) hold. Condition (P2) is guaranteed by the choice of γ, so it remains only to verify (P1). For this it is enough to prove that ξ is prime. Indeed, suppose that ξ is prime but (P1) fails. Then

$$\rho_1\xi = \pi_1\kappa$$

for some κ. Since ξ is prime, it must divide either π_1 or κ. But ξ cannot divide π_1; if it did, then since π_1 is irreducible, we would have that π_1 is a unit multiple of ξ. But then π_1 would be prime since ξ is prime. This contradicts the observation made above that none of the π_i are prime. So ξ must divide κ; but then dividing through by ξ we find that π_1 divides ρ_1. That implies that π_1 and ρ_1 are unit multiples of each other, which again contradicts our initial observations.

Why should ξ be prime? Since ξ is a point of the lattice $\mathbf{Z} + \mathbf{Z}\eta$ lying on f, we have $\xi = n + \eta$ for some integer n. Moreover, since ξ belongs to the 60° angle determined by e_1 and e_2, we find that

$$|(n-1) + 1/2| = |n - 1/2| \leq \frac{1}{2}\sqrt{|D|/3}.$$

But now (ii) of Theorem 1.11 implies that

$$\begin{aligned}\mathscr{N}(\xi) &= n^2 - n + A\\ &= (n-1)^2 + (n-1) + A\end{aligned}$$

is prime, so that ξ is a prime element of $\mathbf{Z}[\eta]$ by Lemma 1.14. □

A small amount of computation shows that condition (ii) of Theorem 1.11 holds for the values $A = 2, 3, 5, 11, 17$, and 41. This yields the following corollary:

Corollary 1.15. $\mathbf{Z}[(-1+\sqrt{D})/2]$ *is a unique factorization domain for* $D = -7, -11, -19, -43, -67, -163$.

Checking larger values of A does not appear to yield any more examples satisfying the conditions of Theorem 1.11. Whether or not the list in Corollary 1.15 is complete is known as the *class number* 1 *problem*; an equivalent question appears in Gauss's *Disquisitiones* (see [**Gau86**, Art. 303]). In 1933, Lehmer showed [**Leh33**] that any missing value of A is necessarily large, in that $|D| > 5 \cdot 10^9$. In 1934, Heilbronn & Linfoot [**HL34**] showed that there is at most one missing value of A. Finally, in 1952, Heegner settled the problem, using new techniques from the theory of modular functions:

Theorem 1.16 (Heegner). *If $A > 41$, then $\mathbf{Z}[\eta]$ does not have unique factorization. Hence if $A \geq 2$ is an integer for which $n^2 + n + A$ is prime for all $0 \leq n < A - 1$, then $A \leq 41$.*

For a modern account of Heegner's proof, see [**Cox89**, §12].

9. Primes represented by general polynomials

The result of the previous section leaves a very natural question unresolved: Does Euler's polynomial $T^2 + T + 41$, which does such a marvelous job of producing primes at the first several natural numbers n, represent infinitely many primes as n ranges over the set of all positive integers? More generally, what can one say about the set of prime values assumed by a polynomial $F(T) \in \mathbf{Z}[T]$? In this section we survey the known results in this direction.

9.1. The linear case. Suppose first that $F(T)$ is linear, say $F(T) = a + mT$, where $m > 0$. Asking whether $F(n)$ is prime for infinitely many natural numbers n amounts to asking whether the infinite arithmetic progression

$$a + m, \quad a + 2m, \quad a + 3m, \quad a + 4m, \quad \ldots$$

contains infinitely many primes — or, phrased in terms of congruences, whether or not there are infinitely many primes $p \equiv a \pmod{m}$.

This question is sometimes easy to answer. Let $d = \gcd(a, m)$. If $d > 1$, then there are at most finitely many primes in the above progression, since every term is divisible by d, and so we have a negative answer to our query. So let us suppose that $d = 1$. Then certain special cases can easily be settled in the affirmative. For example, if $a = -1$ and $m = 4$, then we are asking for infinitely many primes $p \equiv -1 \pmod{4}$, and now we can mimic Euclid: If there are only finitely many such primes, say $p_1, \ldots, p_k$, form the number $N := 4p_1 \cdots p_k - 1$. Since $N \equiv -1 \pmod{4}$, it must have at least one prime divisor $p \equiv -1 \pmod{4}$. But p cannot be any of $p_1, \ldots, p_k$, and we have a contradiction. A similar argument works when $a = -1$ and $m = 3$.

The general case of our problem is much more difficult. It turns out that whenever $\gcd(a, m) = 1$, there *are* infinitely many primes $p \equiv a \pmod{m}$. This was proved by Dirichlet in 1837, by analytic methods. (One can view his argument as a far-reaching generalization of Euler's proof that the sum of the reciprocals of the primes diverges.) We will give a proof of Dirichlet's theorem in Chapter 4.

For now we content ourselves with some special cases of Dirichlet's theorem that follow from algebraic arguments. We noted above that an easy variant of Euclid's proof shows that there are infinitely many primes p for which the residue class of p avoids the trivial subgroup of the unit group $(\mathbf{Z}/4\mathbf{Z})^\times$, and similarly for $(\mathbf{Z}/3\mathbf{Z})^\times$. As observed by A. Granville (unpublished), we have the following general result:

Theorem 1.17. *If H is a proper subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$, then there are infinitely many primes p for which $p \bmod m \notin H$.*

Proof. Let $\mathscr{P}$ be the set of primes p for which $p \bmod m \notin H$, and let $\mathscr{P}'$ be the set of such primes not dividing m. Assuming $\mathscr{P}$ is finite, let P be the product of the elements of $\mathscr{P}'$. Fix an integer a coprime to m with $a \bmod m \notin H$ (which is possible since H is a *proper* subgroup), and then choose a positive integer n satisfying the congruences $n \equiv 1 \pmod{P}$ and $n \equiv a \pmod{m}$. (Such a choice of n is possible by the Chinese remainder theorem.) Since n is coprime to mP, none of its prime divisors can come from $\mathscr{P}$, so that every prime p dividing n must be such that $p \bmod m \in H$. But since H is closed under multiplication, this implies that $n \bmod m \in H$. This contradicts the choice of a. □

If $F(T)$ is a nonzero polynomial with integer coefficients, we say that the prime p is a *prime divisor* of F if p divides $F(n)$ for some integer n. The following useful lemma is due to Schur [**Sch12**]:

Lemma 1.18. *Let $F(T)$ be a nonconstant polynomial with integer coefficients. Then F has infinitely many prime divisors.*

Proof. If $F(0) = 0$, then every prime is a prime divisor of F. So we can assume that the constant term c_0 (say) of $F(T)$ is nonzero. Then $F(c_0T) = c_0G(T)$ for some nonconstant polynomial $G(T)$ with constant term 1. It is enough to show that G has infinitely many prime divisors. Suppose that $p_1, \dots, p_k$ is a list of prime divisors of G. For m sufficiently large, we have $|G(mp_1 \cdots p_k)| > 1$, so that there must be some prime p dividing $G(mp_1 \cdots p_k)$. Then p is a prime divisor of G and p is not equal to any of the p_i, since $G(mp_1 \cdots p_k) \equiv 1 \pmod{p_i}$ for each $1 \le i \le k$. So no finite list of prime divisors of G can be complete. □

For example, let $F(T) = T^2 + 1$. If p divides $n^2 + 1$, then $n^2 \equiv -1 \pmod{p}$, and so either $p = 2$ or $p \equiv 1 \pmod{4}$. So Lemma 1.18 implies that there are infinitely many primes $p \equiv 1 \pmod{4}$. Similarly, if $F(T) = T^2+T+1$, then any prime divisor p of F is such that $p \equiv 1 \pmod{3}$, and so there are infinitely many primes $p \equiv 1 \pmod{3}$. Combining this with our earlier results, we have proved Dirichlet's theorem for all progressions modulo 3 and modulo 4.

These examples are special cases of the following construction: Recall that the *mth cyclotomic polynomial* is defined by

$$\Phi_m(T) = \prod_{\substack{1\le k\le m\\ \gcd(k,m)=1}} \left(T - e^{2\pi i k/m}\right),$$

i.e., $\Phi_m(T)$ is the monic polynomial in $\mathbf{C}[T]$ whose roots are precisely the primitive mth roots of unity, each occurring with multiplicity 1. For example, $\Phi_4(T) = T^2+1$ and $\Phi_3(T) = T^2+T+1$.

We will apply Lemma 1.18 to Φ_m to deduce that there are infinitely many primes $p \equiv 1 \pmod{m}$. To apply Lemma 1.18, we need that the coefficients of $\Phi_m(T)$ are not merely complex numbers, but in fact integers.

Lemma 1.19. *For each positive integer m, the polynomial $\Phi_m(T)$ has integer coefficients.*

Proof. For each m we have the factorization

$$T^m - 1 = \prod_{d\mid m} \Phi_d(T). \tag{1.10}$$

To see this, note that $T^m - 1 = \prod_{\zeta^m=1}(T-\zeta)$. Since the set of mth roots of unity is the disjoint union of the primitive dth roots of unity, taken over those d dividing m, we have (1.10). Applying Möbius inversion to (1.10) yields

$$\Phi_m(T) = \prod_{d\mid m}\left(T^d-1\right)^{\mu(m/d)} = \frac{\prod_{d\mid m,\, \mu(m/d)=1}\left(T^d-1\right)}{\prod_{d\mid m,\, \mu(m/d)=-1}\left(T^d-1\right)} = \frac{F}{G},$$

say. Now F and G are *monic* polynomials in $\mathbf{Z}[T]$ with $G \neq 0$, and so we can write

$$F = GQ + R, \tag{1.11}$$

where $Q, R \in \mathbf{Z}[T]$ and $\deg R < \deg Q$. Of course (1.11) remains valid over $\mathbf{C}[T]$ and expresses in that ring one result of division by G. But we know that over $\mathbf{C}[T]$, we have $F = G\Phi_m$, so that G goes into F with no remainder. By the uniqueness of quotient and remainder in the division algorithm for polynomials, we must have $R = 0$ above. Consequently, $\Phi_m = F/G = Q \in \mathbf{Z}[T]$. □

Lemma 1.20. *If p is a prime divisor of Φ_m, then either $p \mid m$ or $p \equiv 1 \pmod{m}$.*

Proof. If p is a prime divisor of Φ_m, then p divides $\Phi_m(n)$ for some integer n. Since the cyclotomic polynomials have integer coefficients, it follows from

(1.10) that $p \mid \prod_{d|m} \Phi_d(n) = n^m - 1$, so that the order of n modulo p is a divisor of m.

Suppose now that p does not divide m. We claim that in this case, m is the precise order of n modulo p. Thus m divides $p-1$, whence $p \equiv 1 \pmod{m}$. To prove the claim, suppose for the sake of contradiction that $f < m$ is the exact order of n mod p. Then f is a proper divisor of m. Moreover, p divides $n^f - 1 = \prod_{e|f} \Phi_e(n)$, so that p divides $\Phi_e(n)$ for some $e \mid f$. Hence the residue class n mod p is a zero of both $\Phi_e(T)$ and $\Phi_m(T)$. The polynomials Φ_e and Φ_m both appear in the factorization (1.10) of $T^m - 1$, so that $T^m - 1$ has a zero of order ≥ 2 over $\mathbf{Z}/p\mathbf{Z}$. But $T^m - 1$ has no multiple roots over $\mathbf{Z}/p\mathbf{Z}$, since $T^m - 1$ has no roots in common with its derivative mT^{m-1}. □

Since only finitely many primes divide m, Lemmas 1.18 and 1.20 have the following corollary:

Corollary 1.21. *For each natural number m, there are infinitely many primes $p \equiv 1 \pmod{m}$.*

This proof of Corollary 1.21 is essentially due to Wendt [**Wen95**].

How far can one take this algebraic approach? The following result is due to Schur (op. cit.).

★ **Theorem 1.22.** *Let m be a positive integer and let H be a subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$. There is a nonconstant polynomial $F(T) \in \mathbf{Z}[T]$ with the following property: Every prime divisor p of F, with finitely many exceptions, satisfies $p \bmod m \in H$. Consequently, there are infinitely many primes p for which $p \bmod m \in H$.*

When H is the trivial subgroup we have just seen that $F := \Phi_m$ satisfies the conclusion of Theorem 1.22.

Schur gave an elementary proof of Theorem 1.22 requiring only familiarity with the theory of finite fields. A less elementary proof is outlined in Exercise 22. When m is a prime number, Theorem 1.22 is contained in the results of Chapter 2 (see, in particular, Theorem 2.12).

Suppose that a and m satisfy $a^2 \equiv 1 \pmod{m}$, where $a \not\equiv 1 \pmod{m}$. Applying Theorem 1.22 to the 2-element subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$ generated by $a \bmod m$, we obtain a polynomial $F(T)$ all of whose prime divisors (with finitely many exceptions) satisfy either $p \equiv 1 \pmod{m}$ or $p \equiv a \pmod{m}$. Schur showed (op. cit.) that if there is a single, suitably large prime $p \equiv a \pmod{m}$, then the polynomial F he constructs cannot have all (or even all but finitely many) of its prime divisors from the progression 1 mod m. (See the first example below for an illustration of how this works.) So F must have infinitely many prime divisors $p \equiv a \pmod{m}$.

Since Dirichlet's theorem is true, there is always a suitably large prime $p \equiv a \pmod{m}$ to be used in Schur's argument, and so in principle, it is possible to give a purely algebraic proof of Dirichlet's theorem for any progression $a \bmod m$ satisfying $a^2 \equiv 1 \pmod{m}$. Moreover, this is best possible in the following sense:

★ **Theorem 1.23** (Murty [**Mur88, MT06**]). *Suppose m is a positive integer. If F is a nonconstant polynomial with the property that every prime divisor p of F, with finitely many exceptions, satisfies $p \equiv 1 \pmod{m}$ or $p \equiv a \pmod{m}$, then $a^2 \equiv 1 \pmod{m}$.*

The proof of Theorem 1.23 rests on rather deep results in algebro-analytic number theory. The principal tool required is the *Chebotarev density theorem*, which is a far-reaching generalization of Dirichlet's theorem. See [**SL96**] for a down-to-earth discussion of Chebotarev's result.

Example. As an easy example of Schur's method, consider the problem of showing that there are infinitely many primes $p \equiv 3 \pmod{8}$. We start by taking $F(T) := T^2+2$. From the elementary theory of quadratic residues we have that each odd prime divisor of $F(T)$ satisfies $p \equiv 1$ or $3 \pmod{8}$. Now we observe that there is at least one prime in the residue class $3 \pmod{8}$, namely 11. We replace T by $4T+3$ and so obtain from F the polynomial

$$G(T) = F(4T+3) = 16T^2 + 24T + 11 = 8(2T^2 + 3T) + 11.$$

Then every prime divisor of G belongs to either the residue class 1 mod 8 or 3 mod 8. Moreover, for each positive integer n, there is at least one prime $p \equiv 3 \pmod{8}$ for which $p \mid G(n)$, since $G(n) \equiv 3 \pmod{8}$. We will show that G (and hence also F) must have infinitely many prime divisors from the residue class 3 mod 8. Suppose otherwise, and let $p_1, p_2, \ldots, p_k$ be a complete list of the prime divisors $p \equiv 3 \pmod{8}$ of G. For each p_i, choose an integer n_i for which $G(n_i) \not\equiv 0 \pmod{p_i}$. (This is possible since G has at most two roots modulo p_i.) If n is a positive integer chosen by the Chinese remainder theorem to satisfy $n \equiv n_i \pmod{p_i}$ for all $1 \le i \le k$, then $G(n)$ cannot be divisible by any of $p_1, \ldots, p_k$. So $G(n)$ must have a prime divisor from the residue class 3 mod 8 other than $p_1, \ldots, p_k$, a contradiction.

Example. Since every integer a coprime to 24 satisfies $a^2 \equiv 1 \pmod{24}$, it is in principle possible to give an algebraic proof of Dirichlet's theorem for progressions with common difference 24. The details in this case have been completely worked out by Bateman & Low [**BL65**]. We leave to the reader the task of showing that 24 is the largest modulus m with the property that $a^2 \equiv 1 \pmod{m}$ for each a coprime to m.

9.2. Hypothesis H.

> I do not mean to deny that there are mathematical truths, morally certain, which defy and will probably to the end of time continue to defy proof, as, *e.g.*, that every indecomposable polynomial function must represent an infinitude of primes. – J. J. Sylvester [**Syl88**]

There are two natural directions we might head in if we hope to generalize Dirichlet's result: First, we might inquire about simultaneous prime values of several linear polynomials. One has to be careful here, of course. For example, we cannot hope that there are infinitely many n for which both n and $n+1$ are prime, because one of these two numbers is always even! However, if instead of n and $n+1$ we consider n and $n+2$, then this obstruction disappears, and we arrive at the following famous conjecture:

Conjecture 1.24 (Twin prime conjecture)**.** *There are infinitely many natural numbers n for which both n and $n+2$ are prime.*

Alternatively, we might accept the restriction of working with a single polynomial, but hope to treat polynomials of higher degree. The following conjecture of Euler, which appears in correspondence with Goldbach, fits nicely into this framework:

Conjecture 1.25 (Euler)**.** *There are infinitely many natural numbers n for which n^2+1 is prime.*

Similarly, it seems reasonable to conjecture that our old friend, T^2+T+41, represents infinitely many primes. Once again, formulating conjectures of this type requires some care; if n^2+1 or n^2+n+41 is replaced by n^2+n+2, then the statement corresponding to Euler's conjecture is false, since n^2+n+2 is always even.

Suppose more generally that $F_1(T), \dots, F_r(T) \in \mathbf{Z}[T]$ are nonconstant polynomials, each with positive leading coefficient. We can ask when it is the case that $F_1(n), \dots, F_r(n)$ are simultaneously prime for infinitely many natural numbers n. Evidently if this is to be the case, then we must suppose that each F_i is irreducible over $\mathbf{Z}$. The example of $r=2$ and $F_1(T)=T$, $F_2(T)=T+1$ shows that this is not sufficient, as does the example of $r=1$ and $F_1(T)=T^2+T+2$. What goes wrong in these examples is that there is a *local obstruction*: If we put $G(T) := \prod_{i=1}^r F_i(T)$, then $G(n)$ is always even. In 1958, Schinzel conjectured (see [**SS58**]) that these are the only remaining obstructions to be accounted for:

Conjecture 1.26 (Schinzel's "Hypothesis H")**.** *Suppose $F_1(T), \dots, F_r(T) \in \mathbf{Z}[T]$ are nonconstant and irreducible and that each F_i has a positive leading coefficient. Put $G(T) := \prod_{i=1}^r F_i(T)$, and suppose that there is no prime p*

which divides $G(n)$ for every integer n. Then $F_1(n)$, $F_2(n)$, $\ldots$, $F_r(n)$ are simultaneously prime for infinitely many natural numbers n.

The hypothesis on G is necessary: Suppose that p is a (fixed) prime which divides $G(n)$ for each n. Then p divides some $F_i(n)$ for each n. But for large n, each $F_i(n) > p$, and so for large n, some $F_i(n)$ is composite.

The twin prime conjecture corresponds to choosing $r = 2$, $F_1(T) = T$, and $F_2(T) = T + 2$ in Hypothesis H. Taking instead $r = 1$ and $F_1(T) = T^2 + 1$, we recover Euler's Conjecture 1.25. Despite substantial attention, both the twin prime conjecture and Conjecture 1.25 remain open. Even more depressing, no case of Hypothesis H has ever been shown to hold except when $r = 1$ and $F_1(T)$ is linear, when Hypothesis H reduces to Dirichlet's theorem!

Sieve methods, which we introduce in Chapter 6, can be used to obtain certain approximations to Hypothesis H. We give two examples: A theorem of Chen [**Che73**] asserts that there are infinitely many primes p for which $p + 2$ is either prime or the product of two primes. Iwaniec [**Iwa78**] has shown that there are infinitely many n for which $n^2 + 1$ is either prime or the product of two primes.

10. Primes and composites in other sequences

We conclude by discussing the occurrence of primes in other sequences of interest. Results in this area are rather thin on the ground, and so we content ourselves with a smattering of problems and results meant to showcase our collective ignorance.

One sequence that has received much attention is that of the *Mersenne numbers* $2^n - 1$. The occurrence of primes in this sequence has long been of interest in view of Euclid's result that if $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is a perfect number. (Here a number is called *perfect* if it is the sum of its proper divisors.) Since $2^d - 1$ divides $2^n - 1$ whenever d divides n, for $2^n - 1$ to be prime it is necessary that n be prime. At first glance it appears that $2^p - 1$ is often prime; 7 of the first 10 primes p have this property. However, the tide quickly turns: Of the 78498 primes p up to 10^6, only 31 yield primes. As of October 2011, there are 47 known primes of the form $2^p - 1$, the largest corresponding to $p = 43112609$. It is not clear from this data whether or not we should expect infinitely many primes of this form, but probabilistic considerations to be discussed in Chapter 3 suggest that we should:

Conjecture 1.27. *For infinitely many primes p, the number $2^p - 1$ is prime.*

Unfortunately, this conjecture seems far beyond reach. In fact, we know disturbingly little about the numbers $2^p - 1$; perhaps the most striking illustration of this is that even the following modest conjecture remains unproved:

Conjecture 1.28. *For infinitely many primes p, the number $2^p - 1$ is composite.*

We may also change the "$-$" sign to a "$+$" and consider primes of the form $2^n + 1$. Since $2^d + 1$ divides $2^n + 1$ when n/d is odd, we see that $2^n + 1$ can be prime only if n is a power of 2. This leads us to consider the *Fermat numbers* $F_m = 2^{2^m} + 1$. The attentive reader will recall that these numbers appeared already in Goldbach's proof of Theorem 1.1. For $m = 0, 1, 2, 3$, and 4, the numbers F_m are prime:

$$2^{2^0} + 1 = 3, \quad 2^{2^1} + 1 = 5, \quad 2^{2^2} + 1 = 17, \quad 2^{2^3} + 1 = 257, \quad 2^{2^4} + 1 = 65537.$$

Fermat was intuitively certain that F_m is prime for all $m \geq 0$, and expressed this belief in letters to his contemporaries; but in 1732 Euler discovered the factorization

$$2^{2^5} + 1 = 641 \cdot 6700417.$$

It is now known that F_m is composite for $5 \leq m \leq 32$, and (for the same probabilistic reasons alluded to above) it is widely believed that F_m is composite for every $m \geq 5$. So much for intuition! Despite this widespread belief, the following conjecture appears intractable:

Conjecture 1.29. *The Fermat number F_m is composite for infinitely many natural numbers m.*

Similarly, for each even natural number a, one can look for primes in the sequence $a^{2^m} + 1$. Again we believe that there should be at most finitely many, but again the analogue of Conjecture 1.29 seems impossibly difficult! Indeed, the only even values of $a > 0$ for which we can prove that $a^{2^m} + 1$ is composite infinitely often are those values of a, like $a = 8$, which have the form b^k for some odd $k > 1$. (In this case $b^{2^m} + 1$ divides $a^{2^m} + 1$ for every m.) This is a somewhat odd state of affairs in view of the following amusing theorem of Schinzel [**Sch63**]:

Theorem 1.30. *Suppose that infinitely many of the Fermat numbers F_j are prime. If $a > 1$ is an integer not of the form 2^{2^r} (where $r \geq 0$), then $a^{2^m} + 1$ is composite for infinitely many natural numbers m.*

Proof. Fix an integer $a > 1$ not of the form 2^{2^r}. Let M_0 be an arbitrary positive integer. We will show that $a^{2^m} + 1$ is composite for some $m \geq M_0$.

Let F_j be a prime Fermat number not dividing $a(a^{2^{M_0}}-1)$. Since a is coprime to F_j, Fermat's little theorem implies that

$$a^{F_j-1} = a^{2^{2^j}} \equiv 1 \pmod{F_j}.$$

Since $F_j \nmid a^{2^{M_0}}-1$, we must have $M_0 < 2^j$. So we can write

$$\begin{aligned} a^{F_j-1}-1 &= a^{2^{2^j}}-1 \\ &= (a^{2^{M_0}}-1)(a^{2^{M_0}}+1)(a^{2^{M_0+1}}+1)(a^{2^{M_0+2}}+1)\cdots(a^{2^{2^j-1}}+1). \end{aligned}$$

Since F_j divides $a^{F_j-1}-1$ but not $a^{2^{M_0}}-1$, it must be that F_j divides $a^{2^m}+1$ for some $M_0 \le m < 2^j$. We cannot have $a^{2^m}+1 = F_j$, since a is not of the form 2^{2^r}, and so $a^{2^m}+1$ is composite. □

In connection with Fermat-type numbers the following result of Shapiro & Sparer [**SS72**] merits attention (cf. [**Sha83**, Theorem 5.1.5]). It shows (in particular) that the doubly exponential sequences $a^{2^m}+1$ are unusually difficult to handle among sequences of the same general shape:

★ **Theorem 1.31.** *Suppose a, b, and c are integers, and that $a, b > 1$. If c is odd, then*

$$a^{b^m}+c$$

is composite for infinitely many $m \in \mathbf{N}$, except possibly in the case when a is even, $c = 1$, and $b = 2^k$ for some $k \ge 1$. If c is even, there are infinitely many such m except possibly when a is odd and $c = 2$.

The reader should note that the Shapiro–Sparer paper contains several other attractive results on composite numbers in various sequences.

We close this section by considering the sequence of shifted factorials $n!+1$. Here we can easily obtain infinitely many composite terms, since Wilson's theorem implies that $(p-1)!+1$ is composite for each $p > 3$. The following pretty theorem of Schinzel [**Sch62b**] generalizes this result:

Theorem 1.32. *Let α be a positive rational number. Then there are infinitely many n for which $\alpha \cdot n!+1$ is composite.*

Lemma 1.33. *Let p be a prime and let r and s be positive integers. Then for $0 \le i \le p-1$, we have*

$$p \mid si! + (-1)^{i+1}r \iff p \mid r(p-1-i)!+s.$$

Proof. By Wilson's theorem,

$$\begin{aligned} -1 \equiv (p-1)! &= (p-1)(p-2)\cdots(p-i)(p-i-1)! \\ &\equiv (-1)^i i!(p-1-i)! \pmod{p}, \end{aligned}$$

so that $(p-1-i)!i! \equiv (-1)^{i+1} \pmod p$. Since p and $(p-1-i)!$ are coprime,

$$\begin{aligned} p \mid si! + (-1)^{i+1}r &\iff p \mid s(p-1-i)!i! + (-1)^{i+1}r(p-1-i)! \\ &\iff p \mid (-1)^{i+1}s + (-1)^{i+1}r(p-1-i)! \\ &\iff p \mid s + r(p-1-i)!. \end{aligned}$$

$\square$

Proof of Theorem 1.32. Write $\alpha = r/s$, where r and s are relatively prime positive integers. Assume $l \in \mathbf{N}$ and $l \geq r/2$. Then $(4l)!\alpha^{-1}$ is an integer divisible by both 4 and r. Since $4 \mid (4l)!\alpha^{-1}$, we can choose a prime $p_l \equiv -1 \pmod 4$ with

$$p_l \mid (4l)!\alpha^{-1} - 1.$$

Because $r \mid (4l)!\alpha^{-1}$, necessarily $p_l \nmid r$. Since

$$p_l \mid r\left((4l)!\alpha^{-1} - 1\right) = s(4l)! - r, \tag{1.12}$$

we must have $p_l > 4l$. From Lemma 1.33 (with $i = 4l$) and (1.12), we find that

$$p_l \mid r(p_l - 4l - 1)! + s. \tag{1.13}$$

Since $p_l \nmid r$, (1.13) implies that $p_l \nmid s$, and so

$$p_l \mid N_l := \alpha(p_l - 4l - 1)! + 1$$

whenever N_l is an integer. This happens for all large l: Indeed, from (1.13) we have $N_l \geq p_l/s \geq 4l/s$, so that $N_l \to \infty$ with l, which is only possible if $p_l - 4l - 1 \to \infty$ with l. But N_l is an integer whenever $p_l - 4l - 1 \geq s$.

Finally, notice that for large l, we cannot have $p_l = N_l$, since $p_l \equiv -1 \pmod 4$ while $N_l \equiv 1 \pmod 4$. Thus N_l is a composite integer of the form $\alpha \cdot n! + 1$. Letting $l \to \infty$, we obtain infinitely many composite numbers of this form. $\square$

Notes

Most of the proofs discussed for the infinitude of the primes may be found in [**Dic66**, Chapter XVIII] or [**Nar00**, §1.1]. For other compilations, see [**Rib96**, Chapter 1], [**FR07**, Chapter 3], and [**Moh79**]. An amusing version of Euclid's proof, couched in the language of nonstandard analysis, is presented in [**Gol98**, pp. 57–58]. Additional elementary proofs of the stronger result that $\sum 1/p$ diverges may be found in [**Bel43**], [**Mos58**], and the survey [**VE80**].

The following result of Matijasevich and Putnam provides an interesting contrast to Goldbach's theorem (Theorem 1.10): *There is a polynomial with integral coefficients such that the set of primes coincides with the set of positive values assumed by this polynomial, as the variables range over the nonnegative integers.* (An explicit example of such a polynomial, in 26 variables, was produced by Jones et al. [**JSWW76**].) Yet upon inspection we realize we are once again looking at a result that properly belongs not to number theory but to computability theory (or logic); an analogous statement is true if we replace the set of primes with any *listable set*. Here a set of positive integers S is called *listable* if there is a computer program which, when left running forever, outputs precisely the elements of S. A very approachable introduction to this circle of ideas is Matijasevich's article [**Mat99**]; for complete details see [**Mat93**].

In connection with the results of §8, we cannot resist pointing out the remarkable identity

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925\ldots,$$

which shows that $e^{\pi\sqrt{163}}$ is very nearly an integer. We sketch the explanation, which comes from the theory of modular functions; for details one may consult [**Cox89**, §11]. Every lattice $L \subset \mathbf{C}$ has a so-called j-invariant $j(L)$, and $j(L_1) = j(L_2)$ precisely when L_1 and L_2 are homothetic, i.e., when one can be obtained from the other by rotation and scaling. We view j as a function on the upper half-plane $\{z \in \mathbf{C} : \Im(z) > 0\}$ by defining $j(\tau)$ as $j(L)$, where L is the lattice spanned by 1 and τ. It turns out that j is then holomorphic on the upper half-plane. Moreover, since 1 and τ determine the same lattice as 1 and $\tau + 1$, we have $j(\tau) = j(\tau + 1)$. This shows that $j(\tau)$ is holomorphic as a function of $q = e^{2\pi i\tau}$ in the punctured disc $0 < |q| < 1$, and so j has a Laurent expansion. It turns out that this expansion starts

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots,$$

so that $j(\tau) \approx 1/q + 744$ for small q. Now for the coup de grâce: One can show that if K is an imaginary quadratic field with integral basis $1, \tau$, then $j(\tau)$ is an algebraic integer of degree exactly $h(K)$, the class number of K. In particular, if K has class number 1, then $j(\tau)$ is a rational integer. The main theorem of §8 implies that $K = \mathbf{Q}(\sqrt{-163})$ has class number 1, and so $j(\tau) \in \mathbf{Z}$ for $\tau = \frac{1+i\sqrt{163}}{2}$. This value of τ corresponds to $q = -1/\exp(\pi\sqrt{163})$, so that

$$e^{\pi\sqrt{163}} \approx j(\tau) - 744 \in \mathbf{Z}.$$

We remark that $e^{\pi\sqrt{163}}$, while close to an integer, is actually a transcendental number. This may be deduced from the following theorem of Gelfond and Schneider (noting that $e^{\pi\sqrt{163}} = (-1)^{i\sqrt{163}}$): *If α and β are algebraic numbers, where $\alpha \neq 0$ and β is irrational, then α^β is transcendental.* Here "α^β" stands for $\exp(\beta \log \alpha)$, and any nonzero value of $\log \alpha$ is permissible. For a proof of the Gelfond–Schneider result, see, e.g., [**Hua82**, §17.9].

There are many sequences not discussed in §10 where it would be of interest to decide if they contain infinitely many primes, or composites. For example, fix a nonintegral rational number $\alpha > 1$, and consider the sequence of numbers $\lfloor \alpha^n \rfloor$. Whiteman has conjectured that this sequence always contains infinitely many primes. If we drop the rationality condition, then from a very general theorem of Harman [**Har97**] we have that each sequence $\lfloor \alpha^n \rfloor$ contains infinitely many primes as long as $\alpha > 1$ avoids a set of measure zero. (Of course since the rational numbers have measure zero, this has no direct consequence for Whiteman's conjecture.) Very little is known about the sequences considered by Whiteman. For the particular numbers $\alpha = 3/2$ and $\alpha = 4/3$, Forman & Shapiro [**FS67**] present ingenious elementary arguments showing that the sequence $\lfloor \alpha^n \rfloor$ contains infinitely many composite numbers. Some extensions of their results have been obtained by Dubickas & Novikas [**DN05**]; e.g., these authors prove that if $\xi > 0$ and $\alpha \in \{2, 3, 4, 6, 3/2, 4/3, 5/4\}$, then the sequence $\lfloor \xi\alpha^n \rfloor$ contains infinitely many composites.

Exercises

1. Let $a_1 = 1$ and if a_n has already been defined, let $a_{n+1} = a_n \cdots a_1 + 1$. Prove that $a_n < 2^{2^n} - 1$ for all n. Use this to show that $\pi(x) \geq \log\log x$ for all $x > 1$.

† 2. (Harris [**Har56**]) Let b_0, b_1, b_2 be positive integers with b_0 coprime to b_2. Define A_k for $k = 0, 1$ and 2 as the numerator when the finite continued fraction
$$b_0 + \cfrac{1}{b_1 + \cfrac{1}{\ddots + \cfrac{1}{b_k}}}$$
is put in lowest terms. For $k = 3, 4, \ldots$, inductively define b_k and A_k by
$$b_k = A_0 A_1 \cdots A_{k-3}$$
and A_k by the rule given above. Prove that the A_i form an increasing sequence of pairwise coprime positive integers.

3. (Aldaz & Bravo [**AB03**]) Let p_i denote the ith prime. Euclid's argument shows that for each r, there is a prime in the interval $(p_r, \prod_1^r p_i + 1]$. Prove that the number of primes in the (smaller) interval $(p_r, \prod_2^r p_i + 1]$ tends to infinity with r. *Suggestion:* With $P = \prod_2^r p_i$, show that $P - 2, P - 2^2, \ldots, P - 2^k$ are > 1 and pairwise coprime for fixed k and large r; then choose a prime factor of each.

† 4. (Chowdhury [**Cho89**]; see also Grundhöfer [**Gru80**]) It is trivial that for $n \geq 1$, the number $n! + 1$ has a prime divisor exceeding n. Show that for $n \geq 6$, the same holds for each of the numbers $n! + k$, where $2 \leq k \leq n$. *Hint:* Reduce to the case when $k = p$ is a prime with $n/2 < p \leq n$ and $n! + p$ is a power of p. Writing $n! = p^m - p$, compare the power of 2 sitting in both sides.

5. (Hegyvári [**Heg93**]) Suppose $a_1 < a_2 < a_3 < \ldots$ is an increasing sequence of natural numbers for which $\sum 1/a_i$ diverges. Show that the real number $\alpha := 0.a_1a_2a_3\ldots$ formed by concatenating the decimal expansions of the a_i is irrational. In particular, $0.235711131719\ldots$ is irrational. *Hint:* First show that every finite sequence of decimal digits appears in the expansion of α.

   Remark. Suppose that in place of our divergence hypotheses, we assume that for each fixed $\theta < 1$, the number of $a_i \leq x$ exceeds x^θ for all sufficiently large x. Then Copeland & Erdős [**CE46**] have proved that the number α constructed above is *normal* (in base 10); in other words, not only does every finite digit string appear in the expansion of α, but each string of length k appears with the expected frequency 10^{-k}.

6. (Euler) In courses in complex analysis, it is often proved that $\sin x$ possesses the following Weierstrass factorization (valid for all $x \in \mathbf{C}$):

$$\sin x = x \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{n^2\pi^2}\right); \tag{1.14}$$

see, e.g., [**Pri01**] for a short, direct proof of this identity. A proof using only real-variable methods appears in [**Kob84**, Chapter II].

   (a) Starting from (1.14), show that

   $$x \cot x = 1 - 2\sum_{m=1}^{\infty} \zeta(2m)\frac{x^{2m}}{\pi^{2m}},$$

   where ζ denotes the Euler-Riemann zeta function. *Hint:* Take the logarithmic derivative of both sides.

   (b) Computing by hand the first few coefficients in the Taylor series for $x \cot x$ about $x = 0$, check that $\zeta(2) = \pi^2/6$ and $\zeta(4) = \pi^4/90$.

7. (J. D. Dixon) We outline Dixon's proof [**Dix62**] that π is not the root of a polynomial over $\mathbf{Z}$ of degree ≤ 2. The method is that employed by Niven to show π is irrational (see [**Niv47**]). Suppose for the sake of contradiction that π is a root of $P(T) = aT^2 + bT + c$, where a, b and c are integers, not all vanishing.

   Given a polynomial $f(T) \in \mathbf{R}[T]$, define

$$F(T) := f(T) - f^{(2)}(T) + f^{(4)}(T) - f^{(6)}(T) + \cdots . \tag{1.15}$$

   Then $F(T) \in \mathbf{R}[T]$. View F as a function of a real variable x.

   (a) Check that

   $$\frac{d}{dx}\left(F'(x)\sin x - F(x)\cos x\right) = f(x)\sin(x),$$

   and conclude that

$$\int_0^{\pi} f(x)\sin x\,dx = F(\pi) + F(0). \tag{1.16}$$

   (b) With n a positive integer to be chosen shortly, let f be the polynomial

   $$f(T) := \frac{1}{n!}P(T)^{2n}(P(T) - P(0))^{2n}.$$

   Show that the left-hand side of (1.16) is strictly between 0 and 1 if n is sufficiently large.

   We now fix such an n and derive a contradiction by showing that the right-hand side of (1.16) is an integer.

   (c) Show that $f^{(r)}(0) = f^{(r)}(\pi) = 0$ for all $0 \le r < 2n$.

(d) If e and r are nonnegative integers and r is even, show that there is an expansion of the form

$$\frac{d^r}{dx^r}\left(P(x)^e\right) = \sum_{j=r/2}^{r} c_j j! \binom{e}{j} P(x)^{e-j}$$

for certain integers c_j.

(e) Use the result of part (d) to show that if e is a nonnegative integer and $r \geq 2n$ is even, then $\frac{1}{n!}\frac{d^r}{dx^r}(P(x)^e)$ is a polynomial in $P(x)$ with integer coefficients. Conclude that $f^{(r)}(0)$ and $f^{(r)}(\pi)$ are integers.

(f) Referring back to definition (1.15), deduce that $F(\pi) + F(0) \in \mathbf{Z}$.

8. In this exercise we present a proof similar to that of J. Hacks (on p. 8) but relying on the irrationality of π in place of π^2. Let

$$\chi(n) = \begin{cases} (-1)^{(n-1)/2} & \text{if } 2 \nmid n, \\ 0 & \text{otherwise.} \end{cases}$$

a) Show that $\chi(n)$ is a completely multiplicative function, i.e.,

$$\chi(ab) = \chi(a)\chi(b)$$

for every pair of positive integers a, b.

b) Assume that there are only finitely many primes. Show that for every $s > 0$,

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

c) Take $s = 1$ and obtain a contradiction to the irrationality of π. You may assume that $\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$.

9. Say that a natural number n is *squarefull* if $p^2 \mid n$ whenever $p \mid n$, i.e., if every prime showing up in the factorization of n occurs with multiplicity > 1. Every perfect power is squarefull, but there are many other examples, such as $864 = 2^5 \cdot 3^3$. Using Theorem 1.2, show that $\sum' n^{-1}$ converges to $\frac{\zeta(2)\zeta(3)}{\zeta(6)}$, where the $'$ indicates that the sum is restricted to squarefull n. Determine the set of real α for which $\sum' n^{-\alpha}$ converges.

10. (Continuation) Show that every squarefull number has a unique representation in the form u^2v^3, where u and v are positive integers with v squarefree. Deduce that for $x \geq 1$,

$$\sum_{\substack{n \leq x \\ n \text{ squarefull}}} 1 = \frac{\zeta(3/2)}{\zeta(3)} x^{1/2} + O(x^{1/3}).$$

11. Let $r \geq 2$. We say that n is *r-full* if $p^r \mid n$ whenever $p \mid n$. Show that every r-full number can be written in the form $u_0^r u_1^{r+1} u_2^{r+2} \cdots u_{k-1}^{2r-1}$. Deduce that the number of r-full numbers in $[1, x]$ is $\ll_r x^{1/r}$.
12. (Ramanujan) Assuming $\zeta(2) = \pi^2/6$ and $\zeta(4) = \pi^4/90$, show that
$$\sum{}' \frac{1}{n^2} = \frac{9}{2\pi^2},$$
where the $'$ indicates that the sum ranges over positive squarefree integers n with an odd number of prime divisors.
13. (Cf. Porubský [**Por01**]) If R is a commutative ring, its *Jacobson radical* $J(R)$ is the intersection of all of its maximal ideals. Show that
$$J(R) = \{x \in R : 1 - xy \text{ is invertible for all } y \in R\}.$$
Deduce that if R is an integral domain with finitely many units, then $J(R) = \{0\}$. Use this to prove that if R is a principal ideal domain with finitely many units, then either R is a field or R contains an infinite set of pairwise nonassociated primes.
14. By carefully examining the proof of Theorem 1.11, show that the theorem remains correct when $A = 1$, provided that in condition (ii) we replace "prime" with "prime or equal to 1".
15. Suppose that $a_1 < a_2 < a_3 < \cdots$ is an increasing sequence of natural numbers, and put $A(x) := \sum_{a_i \leq x} 1$. Prove that if $(\log x)^{-k} A(x) \to \infty$ for each fixed k, then infinitely many primes p divide some a_i. Use this to give another proof of Lemma 1.18.
16. Prove the following theorem of Bauer [**Bau06**]:

    Theorem. *If $F(T) \in \mathbf{Z}[T]$ is a nonconstant polynomial with at least one real root, then for every $m \geq 3$, there exist infinitely many prime divisors p of F with $p \not\equiv 1 \pmod{m}$.*

    Proceed by showing that each of the following conditions on F is sufficient for the conclusion of the theorem to hold:
    (a) F has a positive leading coefficient and constant term -1.
    (b) F has a positive leading coefficient and negative constant term.
    (c) F has a positive leading coefficient and $F(a) < 0$ for some $a \in \mathbf{Z}$.
    (d) F has a positive leading coefficient and $F(a) < 0$ for some $a \in \mathbf{Q}$.
    (e) F has a positive leading coefficient and $F(a) < 0$ for some $a \in \mathbf{R}$.
    (f) F has a positive leading coefficient and $F(a) = 0$ for some $a \in \mathbf{R}$.
    Hint for (f): Reduce to the case when F has no multiple roots.
17. Let F be a field of characteristic not dividing m. By carefully examining the proof of Lemma 1.20, show that the roots of $\Phi_m(T)$ in the algebraic closure of F are precisely the primitive mth roots of unity there, and that all these roots are simple.

18. (Continuation; Kronecker [**Kro88**], Dirichlet, Bauer [**Bau06**]) Define $\Phi_m(X,Y)$ as the homogenization of $\Phi_m(T)$, so that

$$\Phi_m(X,Y) = \prod_{\substack{\zeta^m=1 \\ \zeta^j\neq 1 \text{ if } 1\le j<m}} (X-\zeta Y).$$

   (a) Suppose $m>2$. Show that $\Phi_m(X+Y,X-Y) = G_m(X,Y^2)$ for some polynomial G_m (say) with integer coefficients. Show also that $\prod_{d\mid m} d^{\mu(m/d)}$ is the coefficient of $X^{\varphi(m)}$ in $\Phi_m(X+Y,X-Y)$.

   (b) Let F be a field of characteristic not dividing m. Suppose s is a nonsquare integer, and let $\sqrt{s}$ denote a fixed square root of s from the algebraic closure of F. Show that the roots of $G_m(T,s)\in\mathbf{Z}[T]$ in the algebraic closure of F are precisely the elements

$$\sqrt{s}\frac{\zeta+1}{\zeta-1},$$

   where ζ runs through the primitive mth roots of unity.

   (c) Suppose s is as in (b), and let p be a prime for which $p\nmid 2ms$. Show that p is a prime divisor of $G_m(T,s)$ if and only if $p\equiv\left(\frac{s}{p}\right) \pmod{m}$.

   (d) Show that if $p\equiv -1 \pmod 4$ is a prime divisor of $G_m(T,-1)$ which does not divide m, then $p\equiv -1\pmod{m}$. Use Exercise 16 to show that $G_m(T,-1)$ has infinitely many such prime divisors, and deduce that there are infinitely many primes $p\equiv -1\pmod{m}$.

19. (Hirschhorn [**Hir02**]) Let $p_1<p_2<p_3<\cdots$ denote the sequence of *odd* primes.

   (a) Let $N\in\mathbf{N}$. Prove that the number of odd positive integers $\le N$ which can be written in the form $p_1^{e_1}\cdots p_k^{e_k}$ does not exceed

$$\prod_{i=1}^{k}\left(\frac{\log N}{\log p_i}+1\right) < (\log(p_kN))^k < \sqrt{2k!}\sqrt{p_kN}.$$

   Hint: Show that $(\log u)^k u^{-1/2}\le (2k/e)^k$ whenever $u\ge 1$. Now invoke the inequality $m!\ge (m/e)^m$, valid for every integer $m\ge 0$.

   (b) Supposing that $p_1,\dots,p_k$ exist (i.e., that there are at least k odd primes), prove that p_{k+1} exists and satisfies $p_{k+1}\le 4(2k!)p_k+1$.

20. Suppose that A is a commutative monoid (written multiplicatively) and that P is a system of generators for A, so that each element of A can be written in the form $\prod_{p\in P} p^{e_p}$, where each $e_p\ge 0$ and only finitely many of the e_p are nonzero. (We do *not* require that this representation be unique.) Suppose also that there is a function $\|\cdot\|\colon A\to\mathbf{N}$ with the following two properties:

   (a) $\|\cdot\|$ respects multiplication, i.e., $\|ab\| = \|a\|\|b\|$ for all $a,b\in A$.

(b) For some real number x_0 and constants $c_1, c_2 > 0$, we have

$$c_1 x \leq \#\{a \in A : \|a\| \leq x\} \leq c_2 x \quad \text{for all} \quad x > x_0.$$

Prove that P is infinite, and that in fact $\sum_{p \in P} \frac{1}{\|p\|}$ diverges.

21. (Continuation)
   (a) For each nonzero Gaussian integer α put $\|\alpha\| = |\alpha|^2$. Show that $\sum_\pi \|\pi\|^{-1}$ diverges, where the sum is over all Gaussian primes π. Deduce that $\sum_{p \equiv 1 \pmod 4} p^{-1}$ diverges, where the sum is over rational primes $p \equiv 1 \bmod 4$.
   (b) For each nonzero polynomial $F(T) \in \mathbf{F}_q[T]$, put $\|F\| := q^{\deg F}$. Show that $\sum \|P\|^{-1}$ diverges, where P ranges over the irreducible elements of $\mathbf{F}_q[T]$.

22. This exercise outlines a proof of Theorem 1.22 via algebraic number theory. Let m be a positive integer, and let ζ be a primitive mth root of unity. Put $K = \mathbf{Q}(\zeta_m)$, and identify $\mathrm{Gal}(K/\mathbf{Q})$ with $(\mathbf{Z}/m\mathbf{Z})^\times$. Let H be a subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$, and let $L \subset K$ be the fixed field of H.
   (a) Say that two sets of rational primes $\mathscr{P}_1$ and $\mathscr{P}_2$ *eventually coincide* if their symmetric difference is finite; in this case we write $\mathscr{P}_1 \doteq \mathscr{P}_2$. Prove that $\mathscr{P}_1 \doteq \mathscr{P}_2$, where $\mathscr{P}_1$ is the set of primes for which $p \bmod m \in H$ and $\mathscr{P}_2$ is the set of primes which split completely in L. *Hint:* If p is a prime not dividing m, analyze how the Frobenius element of p in $\mathrm{Gal}(K/\mathbf{Q})$ behaves upon restriction to L.
   (b) Let θ be an algebraic integer for which $L = \mathbf{Q}(\theta)$. Let F be the minimal polynomial of θ. Prove that $\mathscr{P}_2$, and hence also $\mathscr{P}_1$, eventually coincides with the set of prime divisors of F. *Hint:* $L/\mathbf{Q}$ is Galois, so an unramified rational prime splits completely in L exactly when it has a degree 1 prime factor; now apply the Kummer-Dedekind theorem.

23. (Bang [**Ban86**]; cf. Roitman [**Roi97**]) Let $\ell(q)$ denote the order of 2 modulo q. In this exercise and the next, we outline a proof that for each $n > 6$, there is a prime q with $\ell(q) = n$. In other words, for $n > 6$, one can always find a prime q dividing $2^n - 1$ but not any $2^k - 1$ with $1 \leq k < n$. (Note that this fails when $n = 6$, since $2^6 - 1 = 3^2 \cdot 7$, and $3 \mid 2^2 - 1$ while $7 \mid 2^3 - 1$.)
   (a) Let q be an odd prime and a an integer with $a > 1$. Suppose that q divides $a - 1$. Show that if p is a prime, then $q \nmid \frac{a^p - 1}{a - 1}$ unless $q = p$, in which case $q \parallel \frac{a^p - 1}{a - 1}$.
   (b) Let n be an integer with $n > 1$. Show that $\Phi_n(2) > 1$. *Hint:* Write $\Phi_n(2) = \prod_\zeta (2 - \zeta)$, and pair the terms $2 - \zeta$ and $2 - \zeta^{-1}$.
   (c) Suppose that $n > 1$ and that q is a prime divisor of $\Phi_n(2)$. Observe that $\ell(q) \mid n$. Show that if p is a prime divisor of n for which $\ell(q)$

divides n/p, then $p = q$. *Hint:* Use (a), noting that $q \mid \Phi_n(2) \mid \frac{2^n-1}{2^{n/p}-1}$.

(d) Deduce from (c) that if r denotes the largest divisor of n coprime to q, then $r \mid \ell(q) \mid q-1$.

(e) Now make the further assumption that q is a prime divisor of $\Phi_n(2)$ for which $\ell(q) < n$; we call q an *intristic prime divisor of* $\Phi_n(2)$. Show that q divides n and is the largest prime dividing n.

(f) Continuing to assume that q is an intrinsic prime divisor of $\Phi_n(2)$, show that $q \mid 2^{n/q}-1$. Deduce from (a) and the relation $\Phi_n(2) \mid \frac{2^n-1}{2^{n/q}-1}$ that $q \parallel \Phi_n(2)$.

(g) Combining the results of (a)–(f), show that if $n > 1$ and every prime factor of $\Phi_n(2)$ is intrinsic, then $\Phi_n(2) = P(n)$, where $P(n)$ denotes the largest prime factor of n.

(h) We will show in the next exercise that $\Phi_n(2) > 3^{\frac{1}{2}\varphi(n)}$ whenever $n > 6$. Assuming this for now, show that one cannot have $\Phi_n(2) = P(n)$ with $n > 6$, and so complete the proof. *Hint:* $\varphi(n) > 2$ if $n > 6$.

24. (Continuation) In this exercise, we show that $\Phi_n(2) > 3^{\frac{1}{2}\varphi(n)}$ whenever $n > 6$. (Note that this inequality fails when $n = 6$, since $\Phi_6(2) = 3$.)

(a) Prove the following preliminary lemma: If m is a natural number and p is a prime, then

$$\Phi_{mp}(T) = \begin{cases} \frac{\Phi_m(T^p)}{\Phi_m(T)} & \text{if } p \text{ does not divide } m, \\ \Phi_m(T^p) & \text{if } p \text{ divides } m. \end{cases}$$

(b) Suppose that $q^2 \mid n$ for some prime q. Show that

$$\Phi_n(2) = \Phi_{n/q}(2^q) > (2^q-1)^{\varphi(n/q)} = ((2^q-1)^{1/q})^{\varphi(n)},$$

and use this to deduce the desired inequality.

(c) Now suppose that n is squarefree, say $n = p_1 \cdots p_k$ with the p_i in increasing order. Since $n > 6$, we have $p_k > 3$. Prove that

$$\Phi_n(2) = \frac{\Phi_{p_1\cdots p_{k-1}}(2^{p_k})}{\Phi_{p_1\cdots p_{k-1}}(2)} \geq \left(\frac{2^{p_k}-1}{3}\right)^{\varphi(p_1\cdots p_{k-1})},$$

and use this inequality to deduce the stated estimate.

25. Using the result of Exercise 23, show that for each $n > 1$, the least prime $p \equiv 1 \pmod{n}$ satisfies $p < 2^n$. (With some tweaking of the argument, one can improve the exponent n in this result to $1 + \varphi(n)$; see [**TV11**]. See also Exercise 4.11.)

† 26. (Pólya [**Pól21**]; see also [**MS00**]) Suppose that a and b are nonzero integers and $a \neq \pm 1$. Let $\mathscr{P}$ be the set of primes for which the exponential

congruence $a^k \equiv b \pmod{p}$ has a positive integer solution k. In other words, $\mathscr{P}$ is the set of primes which divide some term of the sequence

$$a - b, \quad a^2 - b, \quad a^3 - b, \quad a^4 - b, \dots .$$

This exercise outlines a proof that $\mathscr{P}$ is always an infinite set.

We may suppose that b is not a power of a, as otherwise $\mathscr{P}$ contains every prime. We assume for the sake of contradiction that $\mathscr{P}$ is finite.

(a) For each $p \in \mathscr{P}$ and each $k \geq 1$, define integers $v_{p,k} \geq 0$ by writing

$$a^k - b = \pm \prod_{p \in P} p^{v_{p,k}}.$$

For each $p \in \mathscr{P}$, set $v_p := \sup_{k \geq 1} v_{p,k}$. We let $\mathscr{P}_1 := \{p \in \mathscr{P} : v_p < \infty\}$ and we put $\mathscr{P}_2 := \mathscr{P} \setminus \mathscr{P}_1$. Show that if $p \in \mathscr{P}_2$, then $p \nmid a$.

(b) Suppose $p \in \mathscr{P}_2$, and let l_p be the order of a modulo p. (This exists by part (a).) Define e_p so that $p^{e_p} \parallel a^{l_p} - 1$. Show that if k is a positive integer for which $p^{e_p+1} \mid a^k - b$, then k belongs to a fixed residue class modulo p.

(c) Show that there is an infinite arithmetic progression of integers k which avoid all the residue classes mod p ($p \in \mathscr{P}_2$) determined in (b). Prove that $a^k - b$ is uniformly bounded for such k, contradicting that $|a^k - b| \to \infty$ as $k \to \infty$.

Remark. In the opposite direction, one can ask when the set $\mathscr{P}$ defined above omits infinitely many primes. Using the Chebotarev density theorem, Schinzel [**Sch60**] has shown that this holds unless $b = a^k$ for some nonnegative integer k. See also [**MS00**].

27. (Křížek et al. [**KLS02**]) Let $F_n = 2^{2^n} + 1$ be the nth Fermat number. Suppose $N \in \mathbf{N}$.
   (a) Show that there are fewer than 2^N distinct prime divisors of the product $F_0 \cdots F_{N-1}$.
   (b) Show that for each $x > 0$, the number of primes $p \leq x$ which divide F_n for some $n \geq N$ is at most $x/2^{N+1}$.
   (c) Making an appropriate choice of N, deduce from (a) and (b) that there are at most $2\sqrt{x}$ primes $p \leq x$ which divide a term of the sequence $F_0, F_1, F_2, \dots$.
   (d) Deduce that if $\lambda > 1/2$, then $\sum' p^{-\lambda} < \infty$, where the $'$ indicates that the sum is restricted to primes dividing at least one Fermat number. When $\lambda = 1$, this confirms a conjecture of Golomb [**Gol55**].
28. (Erdős & Turán [**ET34**]) For $n > 1$, write $P(n)$ for the largest prime factor of n. In this exercise we show that if S is an infinite set of natural

numbers, then

$$\{P(a+b) : a, b \in S\} \quad \text{is unbounded.} \tag{1.17}$$

For each prime p, let v_p be the *p-adic valuation*, defined so that $p^{v_p(n)} \parallel n$ for every natural number n.

(a) Let S be an arbitrary infinite set of natural numbers. Show that for each odd prime p, we can determine an infinite subset $S' \subset S$ with the property that whenever $a, b \in S'$,

$$v_p(a+b) = \min\{v_p(a), v_p(b)\}. \tag{1.18}$$

Hint: First treat the case when no element of S is divisible by p.

(b) Suppose, for the sake of contradiction, that S is infinite but (1.17) fails. Using part (a), argue that we may assume (1.18) holds for every pair $a, b \in S$ and every odd prime p. We make this assumption from now on.

(c) Now argue that $v_2(a) = v_2(b)$ for every pair of elements $a, b \in S$. Thus, dividing through by a suitable power of 2, we may (and do) assume that all the elements of S are odd.

(d) Finally, show that for each pair of elements $a, b \in S$, we have

$$a + b = 2^{v_2(a+b)} \prod_{p>2} p^{\min\{v_p(a), v_p(b)\}}.$$

Show that this equation leads to a contradiction if a and b are chosen to be congruent modulo 4.

† 29. Figure 4, based on Conway's article [**Con87**], describes the action of Conway's prime-producing machine. Decipher this figure and explain how it proves Theorem 1.9. For a more detailed explanation of the workings of Conway's prime-producing machine, see Guy's expository article [**Guy83**].

† 30. (Schinzel [**Sch62a**]) In 1857, Bunyakovsky conjectured [**Bun57**] that if $F(T) \in \mathbf{Z}[T]$ is an irreducible polynomial with positive leading coefficient and D is the largest positive integer dividing $F(n)$ for each $n \in \mathbf{Z}$, then $F(n)/D$ is prime for infinitely many natural numbers n. Show that this would follow from Hypothesis H.

31. (Granville; see, e.g., [**Mol97**, Theorem 2.1]) Assume Hypothesis H. Show that for every natural number N_0, one can find a positive integer A with the property that $n^2 + n + A$ assumes prime values for all $0 \le n \le N_0$. *Hint:* Apply Hypothesis H to the N_0 linear polynomials $T, T + (1^2 + 1), T + (2^2 + 2), \ldots, T + (N_0^2 + N_0)$.

32. (Schinzel & Sierpiński [**SS58**]) Assume Hypothesis H. Show that if $n > 1$ and r is a positive integer divisible by all primes $p \le n$, then there

$$
\begin{array}{l}
5^n 7^d 13 \\
\quad \downarrow (AB)^d J \\
2^d 3^d 5^{n-d} 11 \\
\quad \downarrow (EF)^d K \\
2^d 5^{n-d} 7^d 13 \\
\quad \downarrow (AB)^d J \\
2^{2d} 3^d 5^{n-2d} 11 \\
\quad \downarrow (EF)^d K \\
2^{2d} 5^{n-2d} 7^d 13 \\
\quad \downarrow (AB)^d J \\
\quad \vdots \\
\quad \downarrow (EF)^d K \\
2^{qd} 5^r 7^d 13 \\
\quad \downarrow (AB)^r A \\
2^n 3^r 7^{d-r-1} 17
\end{array}
$$

$$
\begin{array}{ll}
(\text{if } r > 0) \swarrow C & I \searrow (\text{if } r = 0) \\
2^n 3^{r-1} 7^{d-r-1} 19 & 2^n 7^{d-1} \\
\quad \downarrow (DG)^n H & \quad \downarrow L^n M^{d-1} N \\
3^{r-1} 5^n 7^{d-r} 11 & 3^n 5^{n+1} 11 \\
\quad \downarrow (EF)^{r-1} K & \quad \downarrow (EF)^n K \\
5^n 7^{d-1} 13 & 5^{n+1} 7^n 13
\end{array}
$$

Figure 4. The action of Conway's prime-producing machine when started with $5^n 7^d 13$, where $0 < d < n$. The variables q and d are defined by the division algorithm: $n = dq + r$ where $0 \le r < d$.

are infinitely many arithmetic progressions of length n and common difference r consisting of consecutive primes.

Remark. The weaker claim that there are arbitrarily long arithmetic progressions of primes has been proved in a tour de force by Green & Tao [**GT08**]. For some striking elementary consequences of the Green–Tao result, see [**Gra08a**].

33. (Cf. Chang & Lih [**CL77**]) Show that for every $N \in \mathbf{N}$, there is a polynomial $F(T) \in \mathbf{Z}[T]$ for which $\{F(k)\}_{k=0}^N$ is a sequence of $N+1$ distinct primes.

    Hint: For $0 \le k \le N$, put $c_k(T) = \prod_{0 \le i \le N, i \ne k}(T - i)$. Using Corollary 1.21, choose integers $r_0, r_1, \dots, r_N$ for which $\{1 + r_k c_k(k)\}_{k=0}^N$ is a sequence of $N+1$ distinct primes. Put $F(T) := 1 + \sum_{i=0}^N r_i c_i(T)$.

† 34. (Clement [**Cle49**], Cucurezeanu [**Cuc68**]) Let k and n be integers with $n > k \ge 2$. Suppose that n has no prime divisors $< k$. Show that n and $n + k$ are simultaneously prime if and only if

$$k \cdot k!((n-1)! + 1) + (k! - (-1)^k)n \equiv 0 \pmod{n(n+k)}.$$

Table 1. Mann-Shanks criterion: Columns containing only bold entries are indexed by prime numbers.

	0	1	**2**	**3**	4	**5**	6	**7**	8	9	10	**11**	12	**13**
0	1													
1			**1**	**1**										
2					1	**2**	1							
3							1	**3**	**3**	1				
4									1	**4**	6	**4**	1	
5											1	**5**	**10**	**10**
6													1	**6**

† 35. (Shanks [**Sha64**]) Let $F(z) = \sum_{n=0}^{\infty} z^{n(n+1)/2}$ and define

$$G(z) := (F(z) - 1)^2 - (F(z) - 1).$$

Prove that there are infinitely many primes of the form $\frac{n^2+1}{2}$ (with $n \in \mathbf{N}$) if and only if the power series expansion of G has infinitely many negative coefficients.

36. Suppose $p \equiv 3 \pmod 4$ is prime. Prove that if $2p+1$ is also prime, then $2p+1 \mid 2^p - 1$. Deduce that Hypothesis H implies Conjecture 1.28.

37. (Selfridge; cf. [**Erd50b**]) Let $n \in \mathbf{N}$. Show that $78557 \cdot 2^n + 1$ is divisible by some prime number from the set $\{3, 5, 7, 13, 19, 37, 73\}$. In particular, $78557 \cdot 2^n + 1$ is always composite.

† 38. (Louisiana State University Problem Solving Group [**PSG02**]) Prove that $5^{4n} + 5^{3n} + 5^{2n} + 5^n + 1$ is composite for every natural number n.

If you know some algebraic number theory, establish the following generalization: If $q > 1$ is a squarefree natural number with $q \equiv 1 \pmod 4$, then $\Phi_q(q^n)$ is composite for every natural number n.

Hint (due to J. A. Rouse): $q^n - \zeta$ is a difference of squares in $\mathbf{Z}[\zeta]$, where ζ denotes a primitive qth root of unity.

† 39. Table 1 illustrates a primality criterion discovered by Mann & Shanks [**MS72**]: Place the rows of Pascal's triangle in an infinite table, where the zeroth row (consisting of the single element 1) is placed in column 0. Each successive row is shifted two units right. An element of the nth row is written in boldface when it is divisible by n. Then the column number is prime exactly when all entries in its column are written in boldface. Prove this!

40. (Hayes [**Hay65**]; cf. Pollack [**Pol11e**]) Suppose that R is a principal ideal domain with infinitely many prime ideals. Show that every nonconstant polynomial A over R can be written as the sum of two irreducible polynomials of the same degree as A. *Hint:* Arrange for both

summands to satisfy the Eisenstein criterion with respect to the same prime.

Chapter 2

Cyclotomy

> The principles upon which the division of the circle depend, and geometrical divisibility of the same into seventeen parts, etc. – C. F. Gauss

1. Introduction

The terse quotation opening this chapter also opens Gauss's mathematical diary, commenced on March 30, 1796, when Gauss was 18 years old. This entry carries more significance for mathematics than a straight reading would suggest; it was his discovery of the constructibility of the regular 17-gon that swayed Gauss to choose mathematics over philology, his other early love.

It has been known since the time of Euclid that the regular n-gon is constructible for any $n \geq 3$ of the form

$$n = 2^a 3^b 5^c \quad \text{where} \quad a \geq 0, \quad b = 0 \text{ or } 1, \quad c = 0 \text{ or } 1.$$

Whether there were other constructible regular polygons remained an open question for 2000 years. The millenia-long silence was broken by the following notice, which appeared in the April 1796 *Allgemeine Literaturzeitung* (see [**Dun04**, p. 28]):

> It is known to every beginner in geometry that various regular polygons, viz., the triangle, tetragon, pentagon, 15-gon and those which arise by the continued doubling of the number of sides of one of them, are geometrically constructible.
>
> One was already that far in the time of Euclid, and, it seems, it has generally been said since then that the field of

> elementary geometry extends no farther: at least I know of no successful attempt to extend its limits on this side.
>
> So much the more, methinks, does the discovery deserve attention... that besides those regular polygons a number of others, e.g., the 17-gon, allow of a geometrical construction. This discovery is really only a special supplement to a theory of greater inclusiveness, not yet completed, and is to be presented to the public as soon as it has reached its completion.
>
> Carl Friedrich Gauss
> Student of Mathematics at Göttingen

This "theory of greater inclusiveness" (which became known as *cyclotomy*; literally, "circle-splitting") appeared five years later in the last of the seven sections of the *Disquisitiones*. There Gauss [**Gau86**, §365] offers a complete characterization of the constructible regular polygons. Recall that a *Fermat prime* is a prime number of the form $2^n + 1$, where n is a positive integer.

Theorem 2.1 (Gauss, Wantzel)**.** *It is possible to construct a regular n-sided polygon in the plane by straightedge and compass if and only if $n = 2^e p_1 \cdots p_k$ for $e \geq 0$ and distinct Fermat primes $p_1, \ldots, p_k$ (where $k \geq 0$).*

Wantzel's name is attached to this result because the *Disquisitiones*, while insisting on the necessity of the condition of Theorem 2.1, proves only its sufficiency. The first published proof that the regular n-gon is constructible only for those n as in Theorem 2.1 is due to Wantzel [**Wan37**].

The first goal of this chapter is to prove the Gauss–Wantzel theorem. The remainder of this chapter discusses two applications of cyclotomy to the study of reciprocity laws.

Recall that when p is an odd prime and a is an integer relatively prime to p, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a square modulo p and -1 otherwise. Gauss was the first to prove the following fundamental result, which to this day forms the capstone of many a course in elementary number theory:

Theorem 2.2 (Law of quadratic reciprocity)**.** *Suppose that p and q are distinct odd primes. Then*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Over the course of his life Gauss worked out eight different proofs of Theorem 2.2. Eight proofs may seem like overkill, but Gauss was hoping that these arguments would shed light on the theory of higher power residues (cubic residues, quartic residues, etc.). Arguably the first significant step in this direction came in September 1796, when Gauss found two proofs of Theorem 2.2, both based on cyclotomy. In §6 we present a "cyclotomic" proof of quadratic reciprocity.

While most students who take any course in number theory will see quadratic reciprocity, the study of higher reciprocity laws is often postponed to postgraduate courses in class field theory. Moreover, it takes substantial effort to relate these modern results, such as *Artin reciprocity*, to anything resembling "reciprocity" in a naive sense. We end this chapter by motivating and proving an early cubic reciprocity law discovered by Jacobi, in an attractive modern formulation due to Z.-H. Sun. While contained in later, deeper results, Jacobi's law has three features which make it a natural candidate for inclusion in this book: (a) It is quite elementary, using only rational integers in its statement, (b) it wears its status as a reciprocity law on its sleeve, and (c) it falls out naturally of our development of cyclotomy.

2. An algebraic criterion for constructibility

Let us review the rudiments of straightedge and compass constructions. (We assume a prior casual acquaintance with these of the type formed in a typical secondary-school geometry course; alternatively, all we need and more can be found in the book of Courant & Robbins [**CR41**, Chapter III, Part I].) We begin with two "constructed points" $O = (0, 0)$ and $P = (0, 1)$ in the plane $\mathbf{R}^2$. There are now three fundamental constructions we can perform:

(i) Given two constructed points, draw the line between them.

(ii) Given two constructed points, draw the line *segment* between them.

(iii) Given a constructed point and a constructed line segment, draw the circle centered at the given point with radius the length of the specified segment.

Each time two distinct lines intersect, or a line and a circle intersect, we add the point(s) of intersection to our set of constructible points. These processes may be continued indefinitely.

The key to proving Theorem 2.1 is to translate "constructibility" into an algebraic notion. Call $x + iy \in \mathbf{C}$ *constructible* if the point $(x, y) \in \mathbf{R}^2$ is constructible (in finitely many steps). Then one can prove:

Lemma 2.3. *The complex number α is constructible if and only if there is a tower of subfields of the complex numbers*

$$\mathbf{Q} := K_0 \subset K_1 \subset \cdots \subset K_m,$$

where $\alpha \in K_m$ *and, for each* $1 \le i \le m$, $K_i = K_{i-1}(\sqrt{\beta_i})$ *for some* $\beta_i \in K_{i-1}$. *The set of constructible complex numbers forms a field under complex addition and multiplication.*

We leave the proof of Lemma 2.3 as Exercise 2.

Lemma 2.3 reduces the Gauss–Wantzel theorem (Theorem 2.1) to an assertion in field theory and allows us to quickly dispense with the necessity half of this result. We take for granted the (easy) fact that the constructibility of the n-gon is equivalent to the constructibility of an arbitrary primitive nth root of unity ζ_n (Exercise 3) and the fact that the cyclotomic polynomials are always irreducible (see Exercise 7).

Lemma 2.4. *If the primitive* n*th root of unity* ζ_n *is constructible, then* n *has the form given in the Gauss–Wantzel Theorem. Moreover, for every* $j \ge 1$, *each primitive* 2^j*th root of unity* ζ_{2^j} *is constructible.*

Proof. Suppose ζ_n is constructible, and let $K_0 \subset \cdots \subset K_m$ be a tower of fields as in Lemma 2.3 ending with $\zeta_n \in K_m$. Then the irreducibility of the cyclotomic polynomial $\Phi_n(T)$ implies

$$[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \varphi(n) \mid [K_m : \mathbf{Q}].$$

But

$$[K_m : K_{m-1}][K_{m-1} : K_{m-2}] \cdots [K_1 : K_0] = 2^r$$

for some $r \ge 0$. Hence $\varphi(n)$ is a power of 2, and it is easy to show (Exercise 1) that this forces n to be of the form described in Theorem 2.1.

The final claim of the lemma follows easily by induction: $1 = \zeta_{2^0}$ is constructible. If all the 2^{j-1}th primitive roots of unity are constructible, then so is an arbitrary primitive 2^jth root of unity ζ_{2^j}, since $(\zeta_{2^j})^2$ is primitive of order 2^{j-1}. □

We can reduce the remaining portion of the Gauss–Wantzel result to the following theorem:

Theorem 2.5 (Gauss)**.** *Let* p *be a Fermat prime, and let* ζ_p *be a primitive* p*th root of unity. Then* ζ_p *is constructible.*

Suppose Theorem 2.5 is proven. Let $n := 2^e p_1 \cdots p_k$ be as in the theorem statement. Since the constructible numbers form a field, it follows that $\zeta_{2^e}\zeta_{p_1} \cdots \zeta_{p_r}$ is constructible (for any choices of the primitive roots of unity in question). But $\zeta_{2^e}\zeta_{p_1} \cdots \zeta_{p_r}$ is a primitive nth root of unity, and as remarked above, the constructibility of a primitive nth root of unity implies the constructibility of the regular n-gon.

Below we will give a proof of Theorem 2.5 in the spirit of Gauss. For this it is first necessary to investigate the arithmetic of $\mathbf{Z}[\zeta_p]$.

3. Much ado about $\mathbf{Z}[\zeta_p]$

Let p be a prime number, and let $\zeta = \zeta_p$ be a complex primitive pth root of unity. In this section we study the arithmetic of $\mathbf{Z}[\zeta]$. Since $\mathbf{Z}[\zeta]$ is the ring of algebraic integers of the cyclotomic field $\mathbf{Q}(\zeta)$, much of this material will be old hat to those versed in algebraic number theory; however, our needs are simple, and we can develop everything that we need from scratch.

Lemma 2.6 (Determination of an integral basis)**.** *Every element of* $\mathbf{Z}[\zeta]$ *(respectively* $\mathbf{Q}(\zeta)$*) can be expressed uniquely in the form* $a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1}$*, with integral (respectively rational) coefficients* a_i*.*

Proof. We prove the claim for $\mathbf{Z}[\zeta]$; the proof for $\mathbf{Q}(\zeta)$ is similar. (Note that $\mathbf{Q}(\zeta) = \mathbf{Q}[\zeta]$, since ζ is algebraic.)

Existence: Since ζ is a primitive pth root of unity, it is a root of the cyclotomic polynomial

$$\Phi_p(T) := \frac{T^p - 1}{T - 1} = T^{p-1} + T^{p-2} + \cdots + T + 1.$$

Substituting ζ for T yields

$$\zeta^{p-1} = -1 - \zeta - \zeta^2 - \cdots - \zeta^{p-2}. \tag{2.1}$$

This relation together with induction implies that every power of ζ can be represented as a $\mathbf{Z}$-linear combination of $1, \zeta, \ldots, \zeta^{p-2}$. It then follows that each element of $\mathbf{Z}[\zeta]$ also has a representation of this form. By (2.1), we can write 1 as an integral linear combination of $\zeta, \zeta^2, \ldots, \zeta^{p-1}$, and the existence half of Lemma 2.6 follows.

Uniqueness (cf. [**Gau86**, Art. 341, end of Art. 346]): This is a consequence of the irreducibility of $\Phi_p(T)$, which in turn follows from the Eisenstein-Schönemann criterion:

$$\Phi_p(T+1) = \frac{1}{T}\left((T+1)^p - 1\right) = \sum_{k=0}^{p-1} \binom{p}{k+1} T^k$$

is a monic polynomial all of whose nonleading coefficients are divisible by p, and whose constant coefficient is equal to p. Hence $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$ are $\mathbf{Q}$-linearly independent, and so are $\zeta \cdot 1, \zeta \cdot \zeta, \ldots, \zeta \cdot \zeta^{p-2}$. $\square$

Remark. See [**Gau86**, Art. 341] for Gauss's original proof of the irreducibility of $\Phi_p(T)$, which was considerably more complicated. In Exercise 7 we show that $\Phi_n(T)$ is irreducible for every n.

Lemma 2.7. *Suppose* $\alpha \in \mathbf{Z}[\zeta] \cap \mathbf{Q}$*. Then* $\alpha \in \mathbf{Z}$*. That is, the only rational elements of* $\mathbf{Z}[\zeta]$ *are the rational integers.*

Proof. By Lemma 2.6, we can write $\alpha = a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$ for integers a_i. Since $\alpha \in \mathbf{Q}$, the expression $\alpha = -\sum_{i=1}^{p-1} \alpha\zeta^i$ is a representation of α as a $\mathbf{Q}$-linear combination of $\zeta, \zeta^2, \dots, \zeta^{p-1}$. By the uniqueness half of Lemma 2.6, it follows that $a_i = -\alpha$ for each i. In particular, $\alpha = -a_1 \in \mathbf{Z}$. □

We turn next to a study of the Galois theory of $\mathbf{Q}(\zeta)/\mathbf{Q}$:

Lemma 2.8 (Description of the automorphisms of $\mathbf{Q}(\zeta)/\mathbf{Q}$)**.** *For each element $a \bmod p \in (\mathbf{Z}/p\mathbf{Z})^\times$, there is an automorphism σ_a of $\mathbf{Q}(\zeta)/\mathbf{Q}$ sending $\zeta \mapsto \zeta^a$. Moreover, every such automorphism is of this form. Consequently, $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ can be identified with $(\mathbf{Z}/p\mathbf{Z})^\times$.*

Proof. The automorphisms of $\mathbf{Q}(\zeta)$ are determined by where they send ζ. The possible images are the roots of Φ_p, which are precisely ζ^a for $(a,p) = 1$. So for each $(a,p) = 1$, there is an automorphism σ_a with $\zeta \mapsto \zeta^a$, and these exhaust the automorphisms. Moreover, $\sigma_a = \sigma_{a'}$ precisely when $a \equiv a' \pmod{p}$. Finally, notice that

$$\sigma_a \circ \sigma_{a'}(\zeta) = \sigma_a(\zeta^{a'}) = \zeta^{aa'} = \sigma_{aa'}(\zeta).$$

Putting everything together, we see that the map $a \bmod p \mapsto \sigma_a$ is an isomorphism between $(\mathbf{Z}/p\mathbf{Z})^\times$ and the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$. □

Lemma 2.9 (Description of the fixed fields; cf. [**Gau86**, Art. 347])**.** *Let H be a subgroup of $(\mathbf{Z}/p\mathbf{Z})^\times$; then H is the set of eth powers for a uniquely defined natural number e dividing $p-1$. Write $p - 1 = ef$.*

Let g be a fixed generator of $(\mathbf{Z}/p\mathbf{Z})^\times$. Then the set of elements of $\mathbf{Q}(\zeta)$ (respectively $\mathbf{Z}[\zeta]$) fixed by σ_a for every $a \in H$ is precisely the set of $\mathbf{Q}$-linear (resp. $\mathbf{Z}$-linear) combinations of $\eta_1, \dots, \eta_e$, where

$$\eta_i := \zeta^{g^i} + \zeta^{g^{e+i}} + \zeta^{g^{2e+i}} + \cdots + \zeta^{g^{e(f-1)+i}} = \sum_{m=0}^{f-1} \zeta^{g^{em+i}}. \tag{2.2}$$

Following Gauss, we refer to the numbers $\eta_1, \dots, \eta_e$ as the *f-nomial periods* (associated to this prime p and this choice of a generator g). Note that the complex numbers $\eta_1, \dots, \eta_e$ are distinct because of Lemma 2.6. It is convenient to take (2.2) as defining η_i for every integer i; then the η_i are periodic in i with minimal period e.

Proof. The assertion that H is the set of eth powers for a unique positive divisor e of $p-1$ follows from the cyclic nature of $(\mathbf{Z}/p\mathbf{Z})^\times$. Since g is a generator of $(\mathbf{Z}/p\mathbf{Z})^\times$, we have $H = \langle g^e \rangle$. Thus an element of $\mathbf{Q}(\zeta)$ is fixed by everything in H once it is fixed by the single automorphism σ_{g^e}.

Suppose α is fixed by σ_{g^e}. Write $\alpha = \sum_{i=1}^{p-1} c_i\zeta^{g^i}$, and extend the indices on the c_i cyclically with period $p-1$ (i.e., set $c_i := c_{i \bmod p-1}$ for all i).

Lemma 2.6 implies that α is fixed by σ_{g^e} if and only if $c_i = c_{i+e}$ for all i. But then

$$\begin{aligned}\alpha = c_1(\zeta^g + \zeta^{g^{e+1}} + \cdots + \zeta^{g^{(f-1)e+1}}) + c_2(\zeta^{g^2} + \zeta^{g^{e+2}} + \cdots + \zeta^{g^{(f-1)e+2}}) \\ + \cdots + c_e(\zeta^{g^e} + \zeta^{g^{2e}} + \cdots + \zeta^{g^{ef}}) = c_1\eta_1 + c_2\eta_2 + \cdots + c_e\eta_e\end{aligned}$$

is a linear combination of the η_i, as claimed.

The converse is clear, since each of the η_i is fixed by σ_{g^e}. □

Corollary 2.10. *Let α be an element of $\mathbf{Z}[\zeta]$ and suppose that $\sigma_a(\alpha) = \alpha$ for every $a \in (\mathbf{Z}/p\mathbf{Z})^\times$. Then α is a rational integer.*

Proof. We apply the lemma with $H = (\mathbf{Z}/p\mathbf{Z})^\times$ (and hence $e = 1$, $f = p-1$) to obtain that α is a $\mathbf{Z}$-linear combination of the $(p-1)$-nomial period

$$\eta_1 = \sum_{m=0}^{p-2} \zeta^{g^{m+1}} = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1. \qquad \square$$

4. Completion of the proof of the Gauss–Wantzel theorem

Suppose that p is a Fermat prime, so that $p-1 = 2^n$ for some positive integer n. Let g be a fixed generator of $(\mathbf{Z}/p\mathbf{Z})^\times$, and write down the 2^n-nomial period

$$\zeta^{g^0} + \zeta^{g^1} + \cdots + \zeta^{g^{p-2}}. \tag{2.3}$$

We split this into two 2^{n-1}-nomial periods by taking every other term,

$$\zeta^{g^0} + \zeta^{g^2} + \zeta^{g^4} + \cdots + \zeta^{g^{p-1}}, \quad \zeta^{g^1} + \zeta^{g^3} + \zeta^{g^5} + \cdots + \zeta^{g^{p-2}}. \tag{2.4}$$

Each of these then splits into two 2^{n-2}-nomial periods in the same manner. Continuing in this way we eventually reach a level with 2^n 1-nomial periods (which are simply the individual 2^n primitive pth roots of unity).

To codify this process, we let $(2^n, g^0)$ denote the 2^n-nomial period (2.3), we let $(2^{n-1}, g^0)$ and $(2^{n-1}, g^1)$ denote the first and second 2^{n-1}-nomial periods indicated in (2.4), and in general we let (f, j) denote the f-nomial period containing ζ^j.

Splitting up the period (2.3) like this yields a binary tree whose first few rows are shown in the following diagram. Here each period is the sum of the two periods from the nodes immediately below:

$$\begin{tikzcd}[column sep=small]
 & & & (2^n, g^0) \arrow[dll, dash] \arrow[drr, dash] & & & \\
 & (2^{n-1}, g^0) \arrow[dl, dash] \arrow[dr, dash] & & & & (2^{n-1}, g^1) \arrow[dl, dash] \arrow[dr, dash] & \\
(2^{n-2}, g^0) & & (2^{n-2}, g^2) & & (2^{n-2}, g^1) & & (2^{n-2}, g^3)
\end{tikzcd}$$

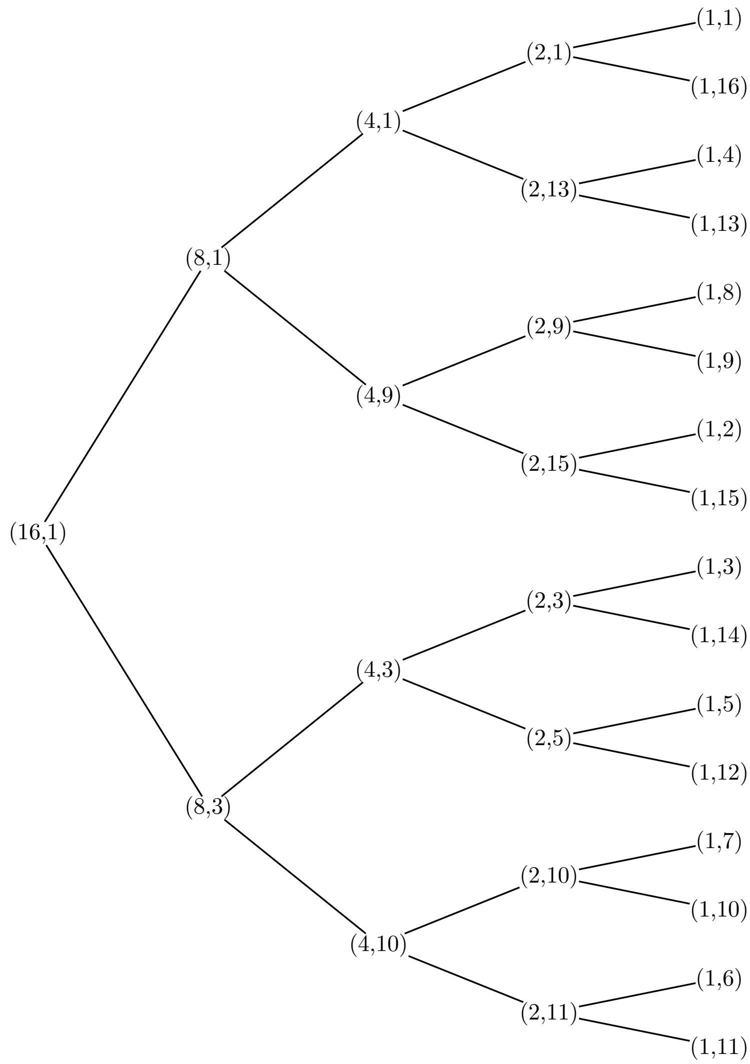

Figure 1. Gauss [**Gau86**, Art. 354]: Binary tree illustrating (for $p = 17$, $g = 3$) the decomposition of the 16-nomial period $\zeta^1 + \zeta^3 + \zeta^9 + \zeta^{10} + \cdots + \zeta^2 + \zeta^6$ into successive half-periods. The correctness of this diagram can be verified with the aid of the following table of powers of 3 (mod 17):

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^n mod 17	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

In general, $(2^{n-r}, g^k)$ branches off (if $r < n$) to yield the two periods $(2^{n-r-1}, g^k)$ and $(2^{n-r-1}, g^{k+2^r})$. Moreover, the 2^r periods of the rth row (numbered starting with $r = 0$) are a complete list of the 2^{n-r}-nomial periods. To see this, let $f = 2^{n-r}$. Then there are $e = (p-1)/f = 2^r$ distinct periods. But the rth row contains 2^r distinct 2^{n-r}-nomial periods by construction (each constructed period is distinct from the others by Lemma 2.6). The claim follows.

We can now prove Gauss's result that ζ_p is constructible. By the remarks in the introduction, this will complete the proof of Theorem 2.1.

Proof of Theorem 2.5. Certainly the (unique) 2^n-nomial period is constructible, being just $\zeta + \cdots + \zeta^{p-2} + \zeta^{p-1} = -1$.

Suppose now that every period in the rth row (i.e., every 2^{n-r}-nomial period) is constructible, for a certain $0 \leq r < n$. Choose a node in the rth row, say $(2^{n-r}, g^k)$, and consider the polynomial

$$\psi_r(T) := (T - (2^{n-(r+1)}, g^k))(T - (2^{n-(r+1)}, g^{k+2^r}))$$

whose roots are the periods beneath this node. Since $\sigma_{g^{2^r}}\left((2^{n-(r+1)}, g^k)\right) = (2^{n-(r+1)}, g^{k+2^r})$ and

$$\sigma_{g^{2^r}}((2^{n-(r+1)}, g^{k+2^r})) = (2^{n-(r+1)}, g^{k+2^{r+1}}) = (2^{n-(r+1)}, g^k),$$

the automorphism $\sigma_{g^{2^r}}$ permutes the factors of $\psi_r(T)$, and so leaves the coefficients of ψ_r fixed. It follows from Lemma 2.9 (with $e = 2^r, f = 2^{n-r}$) that the coefficients of ψ_r are $\mathbf{Z}$-linear combinations of the 2^{n-r}-nomial periods. In particular, they are constructible by the induction hypothesis.

Since the constructible numbers form a field closed under the taking of square roots, the quadratic formula shows that both roots $(2^{n-(r+1)}, g^k)$ and $(2^{n-(r+1)}, g^{k+2^r})$ of ψ_r are constructible.

Proceeding like this for each node in the rth row, we obtain the constructibility of all the periods in the $(r+1)$th row. Theorem 2.5 now follows by induction, since the individual primitive pth roots of unity are the (2^0-nomial) periods of the nth row. $\square$

A detailed treatment of the case $p = 17$ is the subject of Exercise 4.

5. Period polynomials and Kummer's criterion

If $p \equiv 1 \pmod{e}$ is prime, then the *period polynomial* $\phi(T)$ *of degree* e is defined by

$$\phi(T) := (T - \eta_0)(T - \eta_1) \cdots (T - \eta_{e-1}) \in \mathbf{C}[T],$$

and *the reduced period polynomial* $\hat{\phi}(x)$ *of degree* e is defined by

$$\hat{\phi}(T) := (T - (e\eta_0 + 1))(T - (e\eta_1 + 1)) \cdots (T - (e\eta_{e-1} + 1)),$$

where the η_i are the f-nomial periods (and, as usual, $p = ef + 1$). Note that since the choice of a generator g of $(\mathbf{Z}/p\mathbf{Z})^\times$ only impacts the order of the η_i, both ϕ and $\hat{\phi}$ are independent of the choice of g.

At this point ϕ is arguably as natural to introduce as the Gaussian periods themselves. But what is $\hat{\phi}$? We can describe $\hat{\phi}$ by describing its roots: They are

$$e\eta_0 + 1 = 1 + e\sum_{m=0}^{f-1} \zeta^{g^{em}} = 1 + e \sum_{u \bmod p \in (\mathbf{F}_p^\times)^e} \zeta^e = \sum_{v \bmod p \in \mathbf{F}_p} \zeta^{v^e}$$

and its images under the various automorphisms σ_a. For us, the importance of $\hat{\phi}$ rests in the observation that

$$\begin{aligned}\sum_i (e\eta_i + 1) &= e\sum_i \eta_i + e \\ &= e(1 + \zeta + \cdots + \zeta^{p-1}) + e = -e + e = 0,\end{aligned}$$

so that the next-to-leading coefficient of $\hat{\phi}$ automatically vanishes. This makes $\hat{\phi}$ a simpler object to work with.

We now prove that ϕ and $\hat{\phi}$, which *a priori* have complex coefficients, in fact have integer coefficients and are irreducible over the rationals:

Theorem 2.11. *The period polynomial $\phi(T)$ has integer coefficients and is irreducible over the rationals. The same holds for $\hat{\phi}$.*

Of course this agrees with what we already know about the pth cyclotomic polynomial (which corresponds to taking $e = p - 1, f = 1$). Below we will compute the period polynomials and reduced period polynomials of degree 2 and 3.

Proof of Theorem 2.11. It suffices to prove only the statements for ϕ owing to the relation

$$\hat{\phi}(T) = \prod_{i=0}^{e-1} (T - (e\eta_i + 1)) = e^e \prod_{i=0}^{e-1} \left(\frac{T-1}{e} - \eta_i\right) = e^e \phi((T-1)/e). \tag{2.5}$$

The coefficients of $\phi(T)$ belong to $\mathbf{Z}[\zeta]$, so (by Corollary 2.10) to show that they are rational integers, it is enough to check that they are fixed by every σ_a. Assume that the η_i are defined with respect to the generator g of $\mathbf{F}_p^\times$. If the index of a with respect to g is congruent to $i \pmod e$, then $\sigma_a(\eta_j) = \eta_{i+j}$. Since $i + j$ runs through a complete residue system modulo e as j does, it follows that σ_a merely permutes the roots of $\phi(T)$, and so fixes its coefficients.

Irreducibility is surprisingly easy: Given a polynomial over the rationals which vanishes at η_0, we repeatedly apply the automorphism σ_g to see that this polynomial also vanishes at $\eta_1, \eta_2, \ldots$. Since the η_i are distinct, the given polynomial must be divisible by ϕ. This implies that ϕ generates the ideal of polynomials in $\mathbf{Q}[T]$ which vanish at η_0. This is a prime ideal, hence ϕ itself is prime. $\square$

The next theorem provides the link between period polynomials and the study of higher reciprocity. Keeping with tradition, we have attributed it to Kummer (see [**Kum46**]), but it appears to have been known earlier to Gauss (cf. [**Gau65**, Art. 367]):

Theorem 2.12 (Kummer's criterion)**.** *Let $p = ef + 1$ be prime, and let ϕ be the period polynomial of degree e. Let q be a prime distinct from p.*

(i) *If q is an eth power modulo p, then the polynomial $\phi(T)$ has a root mod q.*

(ii) *Conversely, if q is a prime not dividing the discriminant of ϕ for which ϕ has a root mod q, then q is an eth power residue mod p.*

(iii) *Suppose moreover that e is prime. Then every q dividing the discriminant of ϕ is an eth power residue of p.*

When e is prime, statements (i)–(iii) have the following elegant corollary:

Corollary 2.13. *With notation as in Theorem 2.12, q is an eth power residue modulo p if and only if ϕ has a root modulo q.*

The proof of Theorem 2.12 requires the following simple lemma:

Lemma 2.14. *Keep the notation of Theorem 2.12. Suppose that $\eta_i \equiv \eta_j \pmod{q}$, where the congruence is in the ring $\mathbf{Z}[\zeta]$. Then $i \equiv j \pmod{e}$.*

Proof. If $\eta_i \equiv \eta_j \pmod{q}$, then q divides $\eta_i - \eta_j$. Lemma 2.6 then implies that q divides every coefficient of $\eta_i - \eta_j$ when both are expressed as $\mathbf{Z}$-linear combinations of $\zeta, \zeta^2, \dots, \zeta^{p-1}$. But referring to the definition (2.2) of the η_i shows that this is only possible when $\eta_i = \eta_j$, i.e., when $i \equiv j \pmod{e}$. $\square$

Proof of Theorem 2.12. We work modulo q in the ring $\mathbf{Z}[\zeta]$. Fix a generator g of $(\mathbf{Z}/p\mathbf{Z})^\times$, and use this generator to determine the numbering of the periods η_i. Suppose that $q \equiv g^r \pmod{p}$. From the binomial theorem,

$$\eta_k^q = \left(\sum_{m=0}^{f-1} \zeta^{g^{em+k}}\right)^q \equiv \sum_{m=0}^{f-1} \zeta^{g^{em+k+r}} \equiv \eta_{k+r} \pmod{q}.$$

Now let n be an arbitrary integer. Since $y^q - y = \prod_{i=0}^{q-1}(y-i)$ is an identity in every ring of characteristic q, we have

$$\begin{aligned}(n-\eta_k)(n-\eta_k-1)\cdots(n-\eta_k-(q-1)) &\equiv (n-\eta_k)^q - (n-\eta_k)\\ &\equiv \eta_k - \eta_k^q \equiv \eta_k - \eta_{k+r} \pmod{q}.\end{aligned}$$

Multiplying over $k = 0, 1, \ldots, e-1$, we obtain

$$\phi(n)\phi(n-1)\cdots\phi(n-(q-1)) \equiv \prod_{k=0}^{e-1}(\eta_k - \eta_{k+r}) \pmod{q}. \tag{2.6}$$

If q is an eth power modulo p, then e divides r, and so $\eta_{k+r} = \eta_k$ for each k. Hence q divides $\phi(n)\cdots\phi(n-(q-1))$ in $\mathbf{Z}[\zeta]$. By Lemma 2.7, the same divisibility relation holds over $\mathbf{Z}$. Since q is prime in $\mathbf{Z}$, it follows that q divides (over the integers) some value of ϕ, which is the assertion of (i).

The congruence (2.6) also yields a quick proof of (ii): If $q \mid \phi(n)$ and q is not an eth power residue mod p, then $e \nmid r$. Hence, defining

$$P_j := \prod_{k=0}^{e-1}(\eta_k - \eta_{k+j}), \quad \text{we have} \quad q \mid P_r \mid \prod_{j=1}^{e-1} P_j \mid \operatorname{Disc}(\phi)$$

in $\mathbf{Z}[\zeta]$. The same divisibility holds also in $\mathbf{Z}$, and this proves (ii).

We now prove (iii). We suppose that q divides the discriminant of ϕ and show that in this case $e \mid r$, so that $q \equiv g^r$ must be an eth power residue.

Suppose instead that $e \nmid r$. Then r is coprime to e, since e is a rational prime by hypothesis. Now the P_j are rational integers, since they are fixed by every automorphism σ_a. Since

$$q \mid \operatorname{Disc}(\phi) = \pm \prod_{1 \le j \le e-1} P_j,$$

we can choose an index j, $1 \le j \le e-1$, for which $q \mid P_j$. Then

$$\begin{aligned}(\eta_0 - \eta_j)^{\frac{q^e-1}{q-1}} = \prod_{i=0}^{e-1}(\eta_0 - \eta_j)^{q^i} &\equiv \prod_{i=0}^{e-1}(\eta_{ir} - \eta_{ir+j}) \\ &\equiv \prod_{i=0}^{e-1}(\eta_i - \eta_{i+j}) \equiv P_j \pmod{q},\end{aligned}$$

using that r is coprime to e, so that ir runs through a complete residue system modulo e as i does. Since $q \mid P_j$, it follows that

$$q \mid (\eta_0 - \eta_j)^{\frac{q^e-1}{q-1}} \mid (\eta_0 - \eta_j)^{q^e},$$

and so

$$0 \equiv (\eta_0 - \eta_j)^{q^e} \equiv \eta_{0+re} - \eta_{j+re} \equiv \eta_0 - \eta_j \pmod{q},$$

so that $\eta_0 \equiv \eta_j \pmod{e}$. But this contradicts Lemma 2.14. $\square$

6. A cyclotomic proof of quadratic reciprocity

Let p be an odd prime. Then $p-1$ is even, and so it makes sense to consider the period polynomial of degree 2. We will prove quadratic reciprocity by applying Kummer's criterion (Theorem 2.12) with $e=2$. For this we need an explicit determination of the quadratic period polynomial:

Theorem 2.15. *Let p be an odd prime, and put $p^* = (-1)^{(p-1)/2}p$, so that $p^* = p$ if $p \equiv 1 \pmod 4$ and $p^* = -p$ otherwise. The period polynomial of degree $e=2$ is*

$$T^2 + T + \frac{1-p^*}{4}.$$

The reduced period polynomial of degree 2 is $T^2 - p^*$.

The proof of this theorem will be facilitated by means of the following lemma, which allows us to simplify any product of two f-nomial periods (where, as usual, we write $p = ef+1$). Before we can state the lemma, we need to introduce the *cyclotomic numbers*. Fix a generator g of $\mathbf{F}_p^\times$. If $\alpha \in \mathbf{F}_p^\times$, the *index of α (with respect to g)*, denoted $\mathrm{ind}_g\alpha$, is the integer $k \in [0, p-2]$ for which $g^k = \alpha$. The cyclotomic numbers are defined for every pair of integers i and j by

$$(i,j) := \sum_{\substack{\alpha\in\mathbf{F}_p\setminus\{0,-1\} \\ \mathrm{ind}_g\alpha\equiv i \pmod e \\ \mathrm{ind}_g(\alpha+1)\equiv j \pmod e}} 1. \tag{2.7}$$

While we have made this definition for all pairs of i and j, of course i and j really only matter modulo e. (In our contexts there will be no danger of confusing this "(i,j)" with that used to identify the periods of Fermat primes previously.)

Lemma 2.16. *Let $p \equiv 1 \pmod e$ be prime, and write $p = ef+1$. Let $\eta_1, \dots, \eta_e$ denote the f-nomial periods. We assume that both the f-nomial periods and the cyclotomic numbers are indexed with respect to the same fixed generator $g \bmod p$ of $(\mathbf{Z}/p\mathbf{Z})^\times$. Then for every pair of integers i and j, we have*

$$\eta_i\eta_{i+j} = \sum_{m=0}^{e-1} (j,m)\eta_{i+m} + \begin{cases} f & \text{if } j \equiv ef/2 \pmod e, \\ 0 & \text{otherwise.} \end{cases} \tag{2.8}$$

Proof. We have

$$\begin{aligned}\eta_i\eta_{i+j} &= \sum_{m=0}^{f-1}\zeta^{g^{em+i}}\sum_{n=0}^{f-1}\zeta^{g^{en+i+j}} = \sum_{m=0}^{f-1}\sum_{n=0}^{f-1}\zeta^{g^{em+i}(1+g^{e(n-m)+j})}\\ &= \sum_{m=0}^{f-1}\sum_{n=0}^{f-1}\zeta^{g^{em+i}(1+g^{en+j})} = \sum_{n=0}^{f-1}\sum_{m=0}^{f-1}\zeta^{g^{em+i}(1+g^{en+j})},\end{aligned}$$

where in the transition from the first line to the second we use that $n-m$ runs over a complete residue system modulo f as n does (for fixed m).

Suppose n is such that $\operatorname{ind}_g(1+g^{en+j}) \equiv r \pmod{e}$. Then the inner sum over m (for this n) is η_{i+r}. The number of values of n with $0 \le n \le f-1$ for which $\operatorname{ind}_g(1+g^{en+j}) \equiv r \pmod{e}$ is the cyclotomic number (j,r). Adding the contributions from $r = 0, 1, \ldots, e-1$ gives the main term in (2.8).

The secondary term comes from the (unique if it exists) value of n with $0 \le n \le f-1$ for which $1+g^{en+j} \equiv 0 \pmod{p}$; this term appears if and only if $(p-1)/2 = ef/2 \equiv j \pmod{e}$. □

Proof of Theorem 2.15. We have

$$\phi(T) = (T-\eta_0)(T-\eta_1) = T^2 - (\eta_0+\eta_1)T + \eta_0\eta_1.$$

We have

$$\begin{aligned}\eta_0+\eta_1 &= \left(\zeta^{g^0}+\zeta^{g^2}+\cdots+\zeta^{g^{p-1}}\right) + \left(\zeta^{g^1}+\zeta^{g^3}+\cdots+\zeta^{g^{p-2}}\right)\\ &= \sum_{a \bmod p\in(\mathbf{Z}/p\mathbf{Z})^\times}\zeta^a = -\zeta^0 = -1,\end{aligned}$$

and it remains only to compute $\eta_0\eta_1$. By Lemma 2.16 with $e = 2$ and $f = (p-1)/2$, we have

$$\eta_0\eta_1 = (1,0)\eta_0 + (1,1)\eta_1 + \begin{cases} f & \text{if } f \text{ is odd},\\ 0 & \text{if } f \text{ is even}.\end{cases}$$

The automorphism σ_g interchanges η_0 and η_1 and hence leaves $\eta_0\eta_1$ fixed. From the expression just obtained for $\eta_0\eta_1$ and the $\mathbf{Q}$-linear independence of η_0 and η_1 (coming from Lemma 2.6), we must have $(1,0) = (1,1)$. Hence

$$\begin{aligned}2(1,1) = (1,1)+(1,0) &= \sum_{\substack{\alpha\in\mathbf{F}_p\setminus\{0,-1\}\\ \operatorname{ind}_g\alpha\equiv 1 \ (\mathrm{mod}\ 2)}} 1\\ &= \sum_{\substack{1\le a<p-1\\ \left(\frac{a}{p}\right)=-1}} 1 = \frac{p-1}{2} - \frac{1-\left(\frac{-1}{p}\right)}{2},\end{aligned}$$

If $p \equiv 1 \pmod 4$, then f is even and $\left(\frac{-1}{p}\right) = 1$. Hence

$$\begin{aligned}\eta_0\eta_1 = (1,0)\eta_0 + (1,1)\eta_1 &= (\eta_0+\eta_1)(1,1) = -(1,1)\\ &= -\frac{1}{2}\left(\frac{p-1}{2}\right) = \frac{1-p}{4} = \frac{1-p^*}{4}.\end{aligned}$$

If $p \equiv 3 \pmod 4$, then f is odd and $\left(\frac{-1}{p}\right) = -1$, so that

$$\begin{aligned}\eta_0\eta_1 = (1,0)\eta_0 + (1,1)\eta_1 + \frac{p-1}{2} &= -(1,1) + \frac{p-1}{2}\\ &= -\frac{1}{2}\left(\frac{p-3}{2}\right) + \frac{p-1}{2} = \frac{1+p}{4} = \frac{1-p^*}{4}.\end{aligned}$$

This proves the claim about the form of the period polynomial. It follows from (2.5) that the reduced period polynomial is $4\phi(T/2 - 1/2) = T^2 - p^*$, which finishes the proof. □

We are now almost in a position to prove quadratic reciprocity. The only additional ingredient required is the following basic result:

Lemma 2.17 (First supplementary law)**.** *For each odd prime p, we have $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.*

The proof is trivial: A square root of -1 exists modulo p exactly when there is a primitive fourth root of unity in $\mathbf{F}_p^\times$. Since $\mathbf{F}_p^\times$ is cyclic, the latter occurs exactly when $p \equiv 1 \pmod 4$. It is easy to check that this agrees with the answer provided by Lemma 2.17.

Proof of quadratic reciprocity (Theorem 2.2). Let p and q be distinct odd primes. Then q does not divide the discriminant p^* of the period polynomial $T^2 + T + \frac{1}{4}(1-p^*)$. By parts (i) and (ii) of Kummer's criterion (Theorem 2.12),

$$\begin{aligned}\left(\frac{q}{p}\right) = 1 &\iff T^2 + T + \frac{1-p^*}{4} \text{ has a root modulo } q\\ &\iff \operatorname{Disc}\big(T^2 + T + \frac{1-p^*}{4}\big) \text{ is a square mod } q \iff \left(\frac{p^*}{q}\right) = 1.\end{aligned}$$

Thus $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$. From Lemma 2.17 and the multiplicativity of the Legendre symbol, we have

$$\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{(p-1)/2}p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right),$$

which gives Theorem 2.2. □

This proof of quadratic reciprocity most closely resembles the demonstration offered by V.A. Lebesgue [**Leb60**]. However, the same ideas can already be found in Gauss's third and fourth proofs of quadratic reciprocity [**Gau65**, Art. 365-366], which were originally intended to be included in the *Disquisitiones* (see [**Fre07**]).

Using the same method we can classify the primes for which 2 is a square:

Theorem 2.18 (Second supplementary law)**.** *If p is an odd prime, then $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1 \pmod 8$ and $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 3 \pmod 8$.*

Proof of the second supplementary law. Let p be an odd prime. Since $2 \nmid p^*$, Theorem 2.12 implies that

$$\begin{aligned}\left(\frac{2}{p}\right) = 1 &\iff T^2 + T + \frac{1-p^*}{4} \text{ has a root mod } 2\\ &\iff \frac{1-p^*}{4} \equiv 0 \pmod 2 \iff p \equiv \pm 1 \pmod 8. \qquad \square\end{aligned}$$

7. Discovering cubic reciprocity

We now ramp our study of residues and reciprocity up a notch, from quadratic to cubic. If p is prime and $p \equiv 2 \pmod 3$, then 3 is coprime to $p - 1 = \#\mathbf{F}_p^\times$, and so every element of $\mathbf{F}_p^\times$ is a cube. So cubic residues are only interesting for primes $p \equiv 1 \pmod 3$. Before formulating any results for these primes, we need the following elementary lemma:

Lemma 2.19. *Let $p \equiv 1 \pmod 3$ be prime. Then there are integers L and M, uniquely determined up to sign, for which $4p = L^2 + 27M^2$.*

Proof. We first show that p can be written in the form $a^2 + ab + b^2$. Since $p \equiv 1 \pmod 3$ and $(\mathbf{Z}/p\mathbf{Z})^\times$ is a cyclic group, there is an element of order 3 in $(\mathbf{Z}/p\mathbf{Z})^\times$ and hence an integer r satisfying $r^2 + r + 1 \equiv 0 \pmod p$. Let x and y run over pairs of integers with $0 \le x \le \sqrt{p}$ and $0 \le y \le \sqrt{p}$, and consider the difference $x - ry$ modulo p. There are $(\lfloor\sqrt{p}\rfloor + 1)^2 > p$ such pairs, and so by the Pigeonhole principle, we have $x_1 - ry_1 \equiv x_2 - ry_2 \pmod p$ for some x_1, y_1, x_2, y_2 with $(x_1, y_1) \neq (x_2, y_2)$ and $0 \le x_i, y_i < \sqrt{p}$. Then with $a = x_1 - x_2$ and $b = y_1 - y_2$, we have $(a, b) \neq (0, 0)$, $a \equiv rb \pmod p$ and $|a|, |b| < \sqrt{p}$. Moreover,

$$a^2 + ab + b^2 \equiv (r^2 + r + 1)b^2 \equiv 0 \pmod p \quad \text{and} \quad 0 < |a^2 + ab + b^2| < 3p.$$

So $a^2 + ab + b^2 = p$ or $a^2 + ab + b^2 = 2p$. Working modulo 2, we see that $a^2 + ab + b^2$ is even only when both a and b are even, in which case $a^2 + ab + b^2$ is a multiple of 4. Since $4 \nmid 2p$, we must have $a^2 + ab + b^2 = p$, as desired.

If b is a multiple of 3, say $b = 3M$, then the lemma follows quickly: From $p = a^2 + ab + b^2$ we deduce $4p = (2a + b)^2 + 3b^2 = (2a + b)^2 + 27M^2$. So we

Table 1. The first fifty primes $p \equiv 1 \pmod 3$ together with positive values of L and M for which $4p = L^2 + 27M^2$ and the cubic residue status of 2 and 3.

p	L	M	$2 =$ cube?	3?	p	L	M	$2 =$ cube?	3?
7	1	1	N	N	271	29	3	N	Y
13	5	1	N	N	277	26	4	Y	N
19	7	1	N	N	283	32	2	Y	N
31	4	2	Y	N	307	16	6	Y	Y
37	11	1	N	N	313	35	1	N	N
43	8	2	Y	N	331	1	7	N	N
61	1	3	N	Y	337	5	7	N	N
67	5	3	N	Y	349	37	1	N	N
73	7	3	N	Y	367	35	3	N	Y
79	17	1	N	N	373	13	7	N	N
97	19	1	N	N	379	29	5	N	N
103	13	3	N	Y	397	34	4	Y	N
109	2	4	Y	N	409	31	5	N	N
127	20	2	Y	N	421	19	7	N	N
139	23	1	N	N	433	2	8	Y	N
151	19	3	N	Y	439	28	6	Y	Y
157	14	4	Y	N	457	10	8	Y	N
163	25	1	N	N	463	23	7	N	N
181	7	5	N	N	487	25	7	N	N
193	23	3	N	Y	499	32	6	Y	Y
199	11	5	N	N	523	43	3	N	Y
211	13	5	N	N	541	29	7	N	N
223	28	2	Y	N	547	1	9	N	Y
229	22	4	Y	N	571	31	7	N	N
241	17	5	N	N	577	11	9	N	Y

have the lemma with this value of M and $L := 2a + b$. By the symmetry in a and b, the lemma also holds if a is a multiple of 3. So we can suppose that $3 \nmid ab$. In this case, from $a^2 + ab + b^2 \equiv p \equiv 1 \pmod 3$ we deduce that $ab \equiv -1 \pmod 3$, which forces $a \equiv -b \pmod 3$. Put $A = -b$ and $B = a + b$. Then $A^2 + AB + B^2 = a^2 + ab + b^2 = p$; moreover, 3 divides B, and so we can run our previous argument.

We leave the proof of uniqueness as Exercise 8. $\square$

It turns out that the numbers L and M play a pivotal role in the study of cubic residues modulo p. The reader should pause for a few moments to examine Table 1, which collects the values of L and M for small primes p

together with the cubic residue status of 2 and 3. A bit of staring at this table prompts the following guess:

Theorem 2.20 (Gauss [**Gau73a**, §4]). *Let* $p \equiv 1 \pmod 3$, *and write* $4p = L^2 + 27M^2$, *where* L *and* M *are positive. Then*

$$\begin{aligned} 2 \text{ is a cube mod } p &\iff 2 \mid L \text{ and } 2 \mid M \\ &\iff p = L'^2 + 27M'^2 \text{ for some } L', M', \end{aligned}$$

and

$$3 \text{ is a cube mod } p \iff 3 \mid M \iff 4p = L'^2 + 243M'^2 \text{ for some } L', M'.$$

We have labeled this in the style of a theorem, and indeed our guess can be proved correct. We will do this in §8.2 below.

Encouraged by this success, let us attempt to characterize the primes p for which $q = 5$, 7 and 11 are cubic residues. Table 2 shows the results of a computation for primes $p \equiv 1 \pmod 3$ between 10^6 and $10^6 + 10^3$. (This range of primes was motivated by the desire to see reasonably large values of L and M.) In this table we also include the ratio $\frac{L}{3M} \bmod q$, writing ∞ for $\frac{L}{3M} \bmod q$ when $q \mid M$. (Granted, it requires prophetic insight even to consider the ratio of L to M mod q, and a double portion of such to consider the more obscure $\frac{L}{3M}$. Patience; all will be clear in time!)

For $q = 3, 5$ and 7, it appears from Table 2 that q is a cube modulo p precisely when $q \mid LM$ (i.e., when $\frac{L}{3M} = 0$ or ∞). When $q = 11$, it seems that q is a cube modulo p if $\frac{L}{3M} = 0$ or ∞, but also when $\frac{L}{3M} = \pm 5$. These limited examples lead us to conjecture that a fixed prime q is a cubic residue of p if and only if $\frac{L}{3M} \bmod q$ belongs to a certain subset S of $\mathbf{Z}/q\mathbf{Z} \cup \{\infty\}$.

We now state Jacobi's cubic reciprocity law, which vindicates our conjecture and provides an explicit description of the set S:

Theorem 2.21 (Jacobi's cubic reciprocity law). *Let* p *and* q *be distinct primes greater than* 3, *and suppose that* $p \equiv 1 \pmod 3$. Jacobi:

$$q \text{ is a cube modulo } p \iff \frac{L + 3M\sqrt{-3}}{L - 3M\sqrt{-3}} \text{ is a cube in } \mathbf{F}_q(\sqrt{-3}).$$

Z.-H. Sun: *Equivalently (as shown in detail in §8.4), let* $G = G(q)$ *be the group*

$$\{[a, b] : a, b \in \mathbf{F}_q \text{ and } a^2 + 3b^2 \neq 0\},$$

where $[a, b]$ *and* $[c, d]$ *are identified if one is a nonzero scalar multiple of the other, and where multiplication is defined by*

$$[a, b] \odot [c, d] = [ac - 3bd, ad + bc].$$

Table 2. Primes $p \equiv 1 \pmod 3$ between 10^6 and $10^6 + 10^3$, together with the cubic residue status of p with respect to $5, 7$ and 11, and the ratios $\frac{L}{3M}$ with respect to the same moduli.

p	L	M	5?	$\frac{L}{3M}$ mod 5	7?	$\frac{L}{3M}$ mod 7	11?	$\frac{L}{3M}$ mod 11
100003	337	103	N	-2	N	1	N	-4
100057	175	117	Y	0	Y	0	N	1
100069	458	84	N	-1	Y	∞	N	4
100129	562	56	N	-1	Y	∞	N	4
100153	443	87	N	-2	N	1	N	-1
100183	383	97	N	-2	N	3	N	4
100189	209	115	Y	∞	N	3	Y	0
100207	421	91	N	2	Y	∞	N	4
100213	575	51	Y	0	N	-1	N	-3
100237	194	116	N	-2	N	1	N	1
100267	224	114	N	2	Y	0	N	4
100279	137	119	N	1	Y	∞	N	1
100291	491	77	N	1	Y	∞	Y	∞
100297	250	112	Y	0	Y	∞	Y	5
100333	515	71	Y	0	N	-1	Y	5
100357	631	11	N	2	N	3	Y	∞
100363	355	101	Y	0	N	-1	Y	-5
100393	593	43	N	2	N	-3	N	4
100411	179	117	N	-1	N	-3	N	-3
100417	139	119	N	2	Y	∞	N	-3
100447	404	94	N	2	N	-1	N	-2
100459	263	111	N	1	N	1	N	-4
100483	8	122	N	-2	N	-3	N	-1
100501	323	105	Y	∞	Y	∞	N	-1
100519	523	69	N	-1	N	3	N	-3
100537	305	107	Y	0	N	3	N	4
100549	83	121	N	1	N	1	Y	∞
100591	181	117	N	1	N	-1	Y	-5
100609	622	24	N	1	N	3	N	1
100621	574	52	N	-1	Y	0	N	1
100669	626	20	Y	∞	N	-1	N	2
100693	475	81	Y	0	N	-3	N	2
100699	143	119	N	-1	Y	∞	Y	0
100741	509	73	N	1	N	-1	N	-3
100747	605	37	Y	0	N	-3	Y	0
100801	254	112	N	-1	Y	∞	N	2
100927	380	98	Y	0	Y	∞	N	-2
100957	185	117	Y	0	N	3	N	2
100981	457	85	Y	∞	N	3	N	3
100987	595	43	Y	0	Y	0	N	-4
100999	452	86	N	-1	N	3	N	-2

Table 3. Jacobi's criteria for $q = 11, 13, 17, 23, 29, 31$ or 37 to be cubic residues modulo $p = \frac{1}{4}(L^2 + 27M^2)$. In each case it is necessary and sufficient that either $q \mid L$, $q \mid M$, or that one of the given congruences holds.

q	11	13	17	19	23	29	31	37
	$L \equiv \pm 4M$	$L \equiv \pm M$	$L \equiv \pm 3M$	$L \equiv \pm 3M$	$L \equiv \pm 2M$	$L \equiv \pm 2M$	$L \equiv \pm 5M$	$L \equiv \pm 8M$
			$L \equiv \pm 9M$	$L \equiv \pm 9M$	$L \equiv \pm 8M$	$L \equiv \pm M$	$L \equiv \pm 7M$	$L \equiv \pm 3M$
					$L \equiv \pm 11M$	$L \equiv \pm 11M$	$L \equiv \pm 6M$	$L \equiv \pm 9M$
						$L \equiv \pm 13M$	$L \equiv \pm 11M$	$L \equiv \pm 7M$
								$L \equiv \pm 12M$

Then G is a cyclic group of order $q - \left(\frac{-3}{q}\right)$, and

$$q \text{ is a cube modulo } p \Longleftrightarrow [L, 3M] \text{ is a cube in } G.$$

One can use Theorem 2.21 to compute S for any given prime q. For the primes $q \leq 37$, this was carried out by Jacobi ([**Jac27**]; cf. [**Jac69**]); his results for $q = 11$, 13, 17, 23, 29, 31 and 37 are quoted in Table 3. (Jacobi considers the expression $\frac{L}{M}$ instead of $\frac{L}{3M}$, but as we shall see in the proof, the latter arises somewhat more naturally.) We note that Jacobi's law appears (without proof) in Gauss's Nachlass [**Gau73a**, §2].

8. Proving Jacobi's cubic reciprocity law

The proof of Jacobi's cubic reciprocity law is entirely analogous to the proof of the quadratic reciprocity law offered in §6. But each of the corresponding steps is much more difficult; in particular, determining the coefficients of the cubic period polynomial corresponding to a prime $p \equiv 1 \pmod 3$ requires a considerable amount of ingenuity. Here we follow Gauss's treatment [**Gau86**, Art. 358] with minor changes in notation. Along the way we will compute the cyclotomic numbers (i, j) of order 3, which will be used to determine the cubic residue status of 2 and 3.

Even after we can write down the cubic period polynomial, it is not obvious how to determine whether it has a root modulo a prime q; we will tackle this problem by writing down the roots explicitly (in a finite extension of $\mathbf{F}_q$) using Cardano's formulas and then using properties of the qth power map to detect when a root lies in $\mathbf{F}_q$.

8.1. Article 358: The cubic period polynomial.

Theorem 2.22 (Determination of the cubic period polynomial)**.** *Let $p \equiv 1 \pmod 3$ be prime, say $p = 3f + 1$. Write $4p = L^2 + 27M^2$ with integers L and M, where the sign of L is chosen so that $L \equiv 1 \pmod 3$. Put $L = 3k - 2$. Then the cubic period polynomial corresponding to p is*

$$T^3 + T^2 - fT - \frac{f + kp}{9}.$$

Theorem 2.23 (Determination of the cyclotomic numbers of order 3)**.** *The matrix of cyclotomic numbers*

$$\begin{pmatrix} (0,0) & (0,1) & (0,2) \\ (1,0) & (1,1) & (1,2) \\ (2,0) & (2,1) & (2,2) \end{pmatrix} \quad \textit{has the shape} \quad \begin{pmatrix} a & b & c \\ b & c & d \\ c & d & b \end{pmatrix}. \tag{2.9}$$

Here a, b, c and d can be described explicitly as follows: we have

$$a = \frac{f+k}{3} - 1 \quad \textit{and} \quad d = \frac{f+k}{3}.$$

We can choose our generator g of $(\mathbf{Z}/p\mathbf{Z})^\times$ so that either of $b - c = M$ or $b - c = -M$ holds. If g is chosen so that $b - c = M$, then

$$b = \frac{M}{2} + \frac{2f-k}{6} \quad \textit{and} \quad c = -\frac{M}{2} + \frac{2f-k}{6}; \tag{2.10}$$

otherwise these are interchanged.

It appears from Gauss's mathematical diary that he discovered these results on October 1, 1796 [**Gra84**, Entry 39].

We will prove Theorems 2.22 and 2.23 simultaneously. We first need some easy properties of the cubic cyclotomic numbers:

Lemma 2.24. *Let $p \equiv 1 \pmod 3$ and write $p - 1 = 3f$. Then the cyclotomic numbers (i, j) defined in (2.7) have the following properties:*

(i) *For every pair of integers i and j, we have $(i, j) = (j, i)$.*

(ii) *We have*
   (a) $(0,0) + (0,1) + (0,2) = f - 1$,
   (b) $(1,0) + (1,1) + (1,2) = f$,
   (c) $(2,0) + (2,1) + (2,2) = f$.

Proof. Since -1 is a cube in $(\mathbf{Z}/p\mathbf{Z})^\times$, the map $\alpha \mapsto -1 - \alpha$ is a bijection between the set counted by (i, j) and that counted by (j, i). This proves (i). To prove (ii), note that

$$(i,0) + (i,1) + (i,2) = \sum_{\substack{\alpha \in \mathbf{F}_p \setminus \{0,1\} \\ \mathrm{ind}_g(\alpha) \equiv i \pmod 3 \\ \mathrm{ind}_g(\alpha+1) \equiv 0,1, \text{ or } 2 \pmod 3}} 1.$$

That is, $(i,0)+(i,1)+(i,2)$ counts the number of α with $\mathrm{ind}_g(\alpha) \equiv i \pmod 3$ and $\alpha+1 \neq 0$. There are $(p-1)/3 = f$ elements α with $\mathrm{ind}_g(\alpha) \equiv i \pmod 3$. If $i \not\equiv 0 \pmod 3$, then none of these satisfy $\alpha + 1 = 0$. However, if $i \equiv 0 \pmod 3$, then $\alpha := -1$ has index congruent to i mod 3 and $\alpha + 1 = 0$; this explains the anomalous count for $(0,0) + (0,1) + (0,2)$. □

Write the period polynomial $\phi(T)$ in the form

$T^3 - AT^2 + BT - C,$

where $A = \eta_0 + \eta_1 + \eta_2, B = \eta_0\eta_1 + \eta_1\eta_2 + \eta_0\eta_2$ and $C = \eta_0\eta_1\eta_2$

are the elementary symmetric functions of η_0, η_1 and η_2. We have

$$A = \eta_0 + \eta_1 + \eta_2 = \sum_{a \bmod p \in (\mathbf{Z}/p\mathbf{Z})^\times} \zeta^a = -1.$$

By Lemma 2.16,

$$\eta_0\eta_1 = (1,0)\eta_0 + (1,1)\eta_1 + (1,2)\eta_2. \tag{2.11}$$

Applying the automorphism σ_g we obtain the two further relations

$$\eta_1\eta_2 = (1,0)\eta_1 + (1,1)\eta_2 + (1,2)\eta_0, \tag{2.12}$$

$$\eta_2\eta_0 = (1,0)\eta_2 + (1,1)\eta_0 + (1,2)\eta_1. \tag{2.13}$$

Adding (2.11), (2.12), and (2.13) we find that

$$B = \eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_3 = ((1,0) + (1,1) + (1,2))(\eta_0 + \eta_1 + \eta_2) = -f.$$

Lemma 2.16 also yields

$$\eta_0\eta_2 = (2,0)\eta_0 + (2,1)\eta_1 + (2,2)\eta_2.$$

Comparing this with (2.13), we see that $(2,0) = (1,1)$ and $(2,2) = (1,0)$. This, together with the first statement of Lemma 2.24, proves that the matrix of cyclotomic numbers has the form stated in (2.9). Henceforth we refer to the cyclotomic numbers by their letter designation in that matrix.

By Lemma 2.24,

$$a + b + c = (0,0) + (0,1) + (0,2) = f - 1 \quad \text{and} \quad b + c + d = f,$$

and so we obtain the additional relation

$$a = d - 1.$$

From Lemma 2.16 and equations (2.11), (2.12), (2.13), we have

$$\begin{aligned}
\eta_0\eta_0 &= f+(d-1)\eta_0 + b\eta_1 + c\eta_2,\\
\eta_0\eta_1 &= b\eta_0 + c\eta_1 + d\eta_2,\\
\eta_0\eta_2 &= c\eta_0 + d\eta_1 + b\eta_2,\\
\eta_1\eta_2 &= d\eta_0 + b\eta_1 + c\eta_2.
\end{aligned}$$

Hence

$$C = \eta_0(\eta_1\eta_2) = d\eta_0^2 + b\eta_0\eta_1 + c\eta_0\eta_2$$
$$= df + (b^2 + c^2 + d^2 - d)\eta_0 + (bd + bc + cd)\eta_1 + (bd + bc + cd)\eta_2. \tag{2.14}$$

Since C is a rational integer, it is fixed by the automorphism σ_g. This automorphism cyclically permutes η_0, η_1, and η_2, and so the linear independence of the η_i implies that the coefficients of η_0, η_1 and η_2 in (2.14) must coincide. That is,

$$b^2 + c^2 + d^2 - d = bd + bc + cd. \tag{2.15}$$

Hence

$$C = df + (bd + bc + cd)(\eta_0 + \eta_1 + \eta_2)$$
$$= d(b + c + d) - (bd + bc + cd) = d^2 - bc.$$

Relation (2.15) can also be written in the form

$$12d + 12b + 12c + 4$$
$$= 36d^2 + 36b^2 + 36c^2 - 36bd - 36cd - 36bc - 24d + 12b + 12c + 4,$$

or, observing that $12(b + c + d) + 4 = 12f + 4 = 4p$, very concisely as

$$4p = (6d - 3b - 3c - 2)^2 + 27(b - c)^2.$$

(Note that this gives another proof of the existence half of Lemma 2.19.) We began by assuming that $4p = L^2 + 27M^2$. Since L and $6d - 3b - 3c - 2$ both belong to the residue class 1 mod 3, the uniqueness half of Lemma 2.19 implies that

$$L = 3k - 2 = 6d - 3b - 3c - 2 \quad \text{and} \quad b - c = \pm M,$$

so that

$$k = 2d - b - c = 3d - f.$$

Hence

$$d = \frac{f + k}{3} \quad \text{and} \quad b + c = f - d = \frac{2f - k}{3}. \tag{2.16}$$

Consequently,

$$C = d^2 - bc = d^2 - \frac{(b + c)^2}{4} + \frac{(b - c)^2}{4}$$
$$= \frac{(f + k)^2}{9} - \frac{(2f - k)^2}{36} + \frac{M^2}{4}.$$

If we substitute $M^2 = \frac{1}{27}((12f + 4) - (3k - 2)^2)$, this simplifies to

$$\frac{k(3f + 1) + f}{9} = \frac{f + kp}{9},$$

and this finishes the proof of Theorem 2.22.

It is now easy to complete the determination of the cyclotomic numbers. First, replacing g with g^{-1} has the effect of interchanging $b = (0,1)$ and $c = (0,2)$, so that $b - c = \pm M$ can be made to hold for either choice of sign, as was claimed in Theorem 2.23. Next, if g is chosen so that $b - c = M$, then (2.16) yields (2.10). Similar considerations apply if g is chosen so that $b - c = -M$. This completes the proof of Theorem 2.23.

Corollary 2.25. *Let $p \equiv 1 \pmod 3$. Then $T^3 - 3pT - pL$ is the reduced cubic period polynomial corresponding to p.*

Proof. By (2.5) and Theorem 2.22,

$$\hat{\phi}(T) = 3^3\phi(T/3 - 1/3) = T^3 - 3(3f+1)T + 6f - 3kp + 2.$$

The corollary follows once we observe that

$$3f + 1 = p \quad \text{and} \quad 6f - 3kp + 2 = -3kp + 2p = p(2 - 3k) = -pL. \qquad \square$$

8.2. The cubic character of 2 and 3.

Theorem 2.26 (Cubic character of 2)**.** *Let $p \equiv 1 \pmod 3$, and write $4p = L^2 + 27M^2$, where $L \equiv 1 \pmod 3$. Suppose g is a primitive root chosen so that $b - c = M$, where $b = (2,2)$ and $c = (1,1)$ are the cyclotomic numbers of the previous section. Then*

$$\begin{aligned} &2 \text{ is a cube} \Longleftrightarrow 2 \mid L \text{ and } 2 \mid M, \\ &\qquad \operatorname{ind}_g(2) \equiv 1 \pmod 3 \Longleftrightarrow 4 \mid L - M, \\ &\qquad\qquad \operatorname{ind}_g(2) \equiv 2 \pmod 3 \Longleftrightarrow 4 \mid L + M. \end{aligned}$$

In particular, 2 is a cube modulo the prime $p \equiv 1 \pmod 3$ if and only if p can be written in the form $L'^2 + 27M'^2$ for some integers L' and M'.

Proof. Suppose $i \in \{0,1,2\}$. We let S be the set of α counted by the cyclotomic number (i,i). In other words, S is the set of $\alpha \in \mathbf{F}_p \setminus \{0,-1\}$ for which $\operatorname{ind}_g\alpha \equiv \operatorname{ind}_g(\alpha+1) \equiv i \pmod 3$. It is easy to check that the map ψ defined on S by $\psi(\alpha) = -1 - \alpha$ is an involution of S. Since $(i,i) = \#S$,

$$\begin{aligned} (i,i) \text{ is odd} &\Longleftrightarrow \psi \text{ has a fixed point} \\ &\Longleftrightarrow \operatorname{ind}_g(-1/2) \equiv i \pmod 3 \\ &\Longleftrightarrow \operatorname{ind}_g(2) \equiv -i \pmod 3. \end{aligned} \tag{2.17}$$

Since $f = \frac{p-1}{3}$ is even and $L = 3k - 2 \equiv -k - 2 \pmod 4$, Theorem 2.23 implies that

$$(0,0) = a = d - 1 = \frac{f+k}{3} - 1 \equiv k - 1 \equiv L - 1 \pmod 2,$$

$$(1,1) = c, \text{ and } 2c = \frac{2f-k}{3} - M \equiv k - 2f - M \equiv -L - M - 2 \pmod 4,$$

$$(2,2) = b, \text{ and } 2b = M + \frac{2f-k}{3} \equiv M + k - 2f \equiv M - L - 2 \pmod 4.$$

Theorem 7.5 now follows from the equivalences (2.17): For example, taking $i = 0$, we see that

$$\begin{aligned} 2 \text{ is a cube} &\iff \mathrm{ind}_g(2) \equiv 0 \pmod 3 \\ &\iff (0,0) \text{ is odd} \iff L - 1 \text{ is odd} \iff L \text{ is even.} \end{aligned}$$

The other results are proved similarly:

$$\begin{aligned} \mathrm{ind}_g(2) \equiv 1 \pmod 3 &\iff (2,2) \text{ is odd} \\ &\iff 2(2,2) \equiv 2 \pmod 4 \iff M - L \equiv 0 \pmod 4, \end{aligned}$$

and

$$\begin{aligned} \mathrm{ind}_g(2) \equiv 2 \pmod 3 &\iff (1,1) \text{ is odd} \\ &\iff 2(1,1) \equiv 2 \pmod 4 \iff M + L \equiv 0 \pmod 4. \end{aligned}$$

To prove the final assertion of the theorem, notice that if 2 is a cube mod p, so that L and M are even, then $p = L'^2 + 27M'^2$ with $L' := L/2$ and $M' := M/2$. Conversely, if $p = L'^2 + 27M'^2$ for some integers L' and M', then $4p = L^2 + 27M^2$ where $L = 2L'$ and $M = 2M'$. Since the integers L and M in such a representation are uniquely determined up to sign, it follows that L and M are even in all such representations, so that 2 is a cube modulo p. □

Theorem 2.27 (Cubic character of 3)**.** *Under the same assumptions as the previous theorem,*

$$\begin{aligned} 3 \textit{ is a cube modulo } p &\iff 3 \mid M, \\ \mathrm{ind}_g(3) \equiv 1 \pmod 3 &\iff M \equiv -1 \pmod 3, \\ \mathrm{ind}_g(2) \equiv 2 \pmod 3 &\iff M \equiv +1 \pmod 3. \end{aligned}$$

Proof. As β runs through all the elements of $\mathbf{F}_p^\times \setminus \{1\}$, the expression $(\beta - 1)^{-1}$ assumes all the values in $\mathbf{F}_p^\times \setminus \{-1\}$. So by Wilson's theorem, $\prod_{\beta \in \mathbf{F}_p^\times \setminus \{1\}} (\beta - 1)^{-1} = 1$. With g our chosen generator, we put $\omega := g^{(p-1)/3}$ and let $H := \{1, \omega, \omega^2\}$ be the subgroup of $\mathbf{F}_p^\times$ generated by ω. Let $A := \{\gamma_1 = 1, \gamma_2, \ldots, \gamma_{(p-1)/3}\}$ be a complete set of coset representatives for H.

Then we have

$$\prod_{\substack{\beta\in(\mathbf{Z}/p\mathbf{Z})^\times\\ \beta\neq 1}} \frac{1}{\beta-1} = \frac{1}{\omega-1}\frac{1}{\omega^2-1}\prod_{1\neq\gamma\in A}\frac{1}{\gamma-1}\frac{1}{\gamma\omega-1}\frac{1}{\gamma\omega^2-1}$$
$$= \frac{1}{1-\omega}\frac{1}{1-\omega^2}\prod_{1\neq\gamma\in A}\frac{1}{\gamma-1}\frac{1}{\gamma-\omega}\frac{1}{\gamma-\omega^2}$$
$$= \frac{1}{3}\prod_{1\neq\gamma\in A}\frac{1}{\gamma^3-1}.$$

As γ runs through the elements of $A\setminus\{1\}$, the element γ^3-1 runs exactly once through the immediate predecessors of every cube $\neq 1$. It follows that

$$0 = \mathrm{ind}_g(1) \equiv -\mathrm{ind}_g(3) - \sum_{1\neq\gamma\in A}\mathrm{ind}_g(\gamma^3-1) \pmod{p-1};$$

modulo 3 this implies that

$$-\mathrm{ind}_g(3) - 0(0,0) - 1(1,0) - 2(2,0) \equiv 0 \pmod 3,$$

i.e.,

$$\mathrm{ind}_g(3) \equiv -(1,0) - 2(2,0) = -b-2c \equiv c-b \equiv -M \pmod 3,$$

as we sought to show. □

Remark. Gauss's first proof of Theorem 2.27 (which has been preserved in [**Gau73a**, pp. 10-11]) was a good deal more intricate. The elegant argument described above was discovered subsequently by Gauss, and recorded on January 6th, 1809 in his mathematical diary:

> The theorem for the cubic residue 3 is proved with an elegant special method by considering the values of $\frac{x+1}{x}$ where three each always have the values $a, a\epsilon, a\epsilon^2$, with the exception of two which give ϵ, ϵ^2, but these are
>
> $$\frac{1}{\epsilon-1} = \frac{\epsilon^2-1}{3}, \quad \frac{1}{\epsilon^2-1} = \frac{\epsilon-1}{3}$$
>
> with product $\equiv \frac{1}{3}$.

For many years this comment remained obscure. The reconstruction presented here is due to Gröger [**Grö06**].

8.3. Jacobi's rational cubic reciprocity law. We now show how to derive Jacobi's original form of cubic reciprocity from Kummer's criterion (Theorem 2.12) and our determination of the cubic period polynomial. Sun's version of Jacobi's law is treated in §8.4.

First we recall the statement of Jacobi's law:

Theorem 2.28 (Jacobi)**.** *Let p and q be distinct primes with $p, q > 3$ and $p \equiv 1 \pmod 3$. Write $4p = L^2 + 27M^2$. Then*

$$q \text{ is a cube in } \mathbf{F}_p \Longleftrightarrow \frac{L + 3M\sqrt{-3}}{L - 3M\sqrt{-3}} \text{ is a cube in } \mathbf{F}_q(\sqrt{-3}). \tag{2.18}$$

We can (and do) assume for the proof of Theorem 2.28 that the sign of L is chosen so that $L \equiv 1 \pmod 3$. Indeed, replacing L with $-L$ has the effect of replacing the ratio on the right-hand side of (2.18) with its reciprocal, and this new ratio is a cube exactly when the original is.

Let ϕ (respectively $\hat{\phi}$) be the cubic period polynomial (respectively reduced period polynomial) whose coefficients were determined in §8.1. Then

$$\mathrm{Disc}(\hat{\phi}) = 4(3p)^3 - 27(pL)^2 = 27p^2(4p - L^2) = 3^6 p^2 M^2.$$

But $\mathrm{Disc}(\hat{\phi}) = 3^6 \cdot \mathrm{Disc}(\phi)$, so that

$$\mathrm{Disc}(\phi) = p^2 M^2.$$

Since $e = 3$ is prime, part (iii) of Kummer's criterion (Theorem 2.12) yields the following special case of Theorem 2.28. (Note that if $q \mid M$, then the quotient on the right-hand side of (2.18) is $L/L = 1$, which is a cube in $\mathbf{F}_q(\sqrt{-3})$.)

Lemma 2.29. *Let p and q be distinct primes with $p, q > 3$ and $p \equiv 1 \pmod 3$. Write $4p = L^2 + 27M^2$ with $L \equiv 1 \pmod 3$. If q divides M, then q is a cube in $\mathbf{F}_p$.*

It remains to treat the case when $q > 3$ and $q \nmid pM$. Here we use Corollary 2.13:

$$q \text{ is a cube modulo } p \Longleftrightarrow \phi \text{ has a root mod } q \Longleftrightarrow \hat{\phi} \text{ has a root mod } q,$$

the last implication following from (2.5). To analyze when $\hat{\phi}$ has a root in $\mathbf{F}_q$, we use the classical solution of the cubic equation.

★ **Theorem 2.30** (Cardano)**.** *Let $f(T) = T^3 + aT - b$ be a cubic polynomial with coefficients in a field F of characteristic $\neq 2, 3$. Suppose also that $a \neq 0$. Then the roots of f in an algebraic closure of F are given by*

$$w + \frac{-a/3}{w}, \quad \textit{where} \quad w^3 = \frac{b}{2} \pm \sqrt{\frac{b^2}{4} + \frac{a^3}{27}},$$

where w ranges over all six cube roots corresponding to the two choices of sign.

Applied to our situation we find:

Corollary 2.31. *Let $p \equiv 1 \pmod 3$ and let $q > 3$ be a prime not dividing pM. Then the roots of the reduced cubic period polynomial $T^3 - 3pT - pL$ in an algebraic closure of $\mathbf{F}_q$ can be described by*

$$w + \frac{p}{w}, \quad \textit{where} \quad w^3 = p\frac{L \pm 3M\sqrt{-3}}{2}.$$

Let w be one of these cube roots. Since the elements of $\mathbf{F}_q$ can be characterized as the fixed points of the qth power map, for the root corresponding to w we have

$$\begin{aligned} w + p/w \in \mathbf{F}_q &\iff (w + p/w)^q = (w + p/w) \\ &\iff w^q + p/w^q = w + p/w. \end{aligned}$$

To analyze the last of these equivalent statements, we use the following lemma, whose proof is left as Exercise 9.

Lemma 2.32. *Let F be a field of characteristic other than p. If $x, y \in F$ and $x + p/x = y + p/y$, then either $x = y$ or $x = p/y$.*

We conclude that if $w + p/w \in \mathbf{F}_q$, then either $w^q = w$ or $w^q = p/w$. We now show that the first possibility can only occur if $q \equiv 1 \pmod 3$ and that the latter can only occur if $q \equiv 2 \pmod 3$.

Lemma 2.33. *Let p and q be distinct primes with $p, q > 3$ and $p \equiv 1 \pmod 3$. Suppose $q \nmid pM$. Suppose the element w in a fixed algebraic closure of $\mathbf{F}_q$ satisfies*

$$w^3 = p\frac{L \pm 3M\sqrt{-3}}{2} \in \mathbf{F}_q(\sqrt{-3}) \tag{2.19}$$

for some choice of sign. Then

$$w^{3q} = w^3 \textit{ if and only if } q \equiv 1 \pmod 3, \qquad \textit{while} \quad w^{3q} = p^3/w^3 \textit{ if and only if } q \equiv 2 \pmod 3.$$

Consequently, $w^q = w$ implies $q \equiv 1 \pmod 3$ and $w^q = p/w$ implies $q \equiv 2 \pmod 3$.

Proof. We have

$$w^{3q} = (w^3)^q = p^q\left(\frac{L \pm 3M\sqrt{-3}}{2}\right)^q = p\frac{L \pm 3M\left(\frac{-3}{q}\right)\sqrt{-3}}{2}. \tag{2.20}$$

As $M \neq 0$ in $\mathbf{F}_q$ by hypothesis, the right-hand side agrees with w^3 exactly when $\left(\frac{-3}{q}\right) = 1$, i.e., when $q \equiv 1 \pmod 3$. Since

$$p^3/w^3 = \frac{p^3}{p(L \pm 3M\sqrt{-3})/2} = p\frac{p}{(L \pm 3M\sqrt{-3})/2} = p\frac{L \mp 3M\sqrt{-3}}{2},$$

the right-hand side of (2.20) agrees with p^3/w^3 exactly when $\left(\frac{-3}{q}\right) = -1$, i.e., when $q \equiv 2 \pmod 3$. $\square$

We prove Theorem 2.28 by analyzing for which primes $p \equiv 1 \pmod 3$ we have $w^q = w$ and for which primes $p \equiv 2 \pmod 3$ we have $w^q = p/w$. By Lemma 2.29, we can assume in these proofs that $q \nmid M$.

In what follows we let $\sqrt{-3}$ denote a fixed square root of -3 in an algebraic closure of $\mathbf{F}_q$ and we let w be an element of this algebraic closure satisfying (2.19). For notational convenience we also set

$$\pi := \frac{L \pm 3M\sqrt{-3}}{2} \quad \text{and} \quad \pi' := \frac{L \mp 3M\sqrt{-3}}{2},$$

so that $\pi\pi' = p$ and $w^3 = p\pi$.

Proof of the Jacobi law for $q \equiv 1 \pmod 3$. In this case

$$\begin{aligned} w + p/w \in \mathbf{F}_q &\iff w^q = w \iff w^{q-1} = 1 \\ &\iff (p\pi)^{(q-1)/3} = 1 \iff (\pi^2\pi')^{(q-1)/3} = 1. \end{aligned}$$

Since $q \equiv 1 \pmod 3$, we have $\mathbf{F}_q(\sqrt{-3}) = \mathbf{F}_q$. Hence π and π' are elements of $\mathbf{F}_q$ (and are nonzero since they multiply to the nonzero element p). So by Euler's criterion, the above holds

$$\iff \pi^2\pi' \text{ is a cube in } \mathbf{F}_q \iff \frac{\pi^2\pi'}{\pi'^3} = \pi'/\pi \text{ is a cube in } \mathbf{F}_q.$$

If the minus sign holds in the definition of π, then this is exactly the criterion appearing in (2.18). If the plus sign holds, then we have only to note that π/π' is a cube if and only if π'/π is a cube, and we again recover Jacobi's criterion.

Since this computation was valid for any choice of w, we have proved more than required: We have shown that if the right-hand side of (2.18) is a cube in $\mathbf{F}_q(\sqrt{-3})$, then the reduced period polynomial has *all its roots* (not just one) defined modulo q. Conversely, if this quotient is not a cube, then none of the roots of the reduced period polynomial lie in $\mathbf{F}_q$. $\square$

Proof of the Jacobi law for $q \equiv 2 \pmod 3$. In this case

$$w + p/w \in \mathbf{F}_q \iff w^q = p/w \iff w^{q+1} = p.$$

By Lemma 2.33, we have $w^{3(q+1)} = p^3$. Since the cube roots of unity lie outside $\mathbf{F}_q$,

$$w^{q+1} = p \Leftrightarrow w^{q+1} \in \mathbf{F}_q \Leftrightarrow w^{(q+1)(q-1)} = 1 \Leftrightarrow p^{(q^2-1)/3}\pi^{(q^2-1)/3} = 1.$$

But for a nonzero $\alpha \in \mathbf{F}_q(\sqrt{-3})$, we have $\alpha^{(q^2-1)/3} = 1$ precisely when α is a cube. Note that since $q \equiv 2 \pmod 3$, every element of $\mathbf{F}_q$ (in particular, the element p) is a cube in both $\mathbf{F}_q$ and $\mathbf{F}_q(\sqrt{-3})$. Hence

$$\begin{aligned} p^{(q^2-1)/3}\pi^{(q^2-1)/3} = 1 &\iff \pi^{(q^2-1)/3} = 1 \\ &\iff \pi \text{ is a cube in } \mathbf{F}_q(\sqrt{-3}) \\ &\iff \pi^2 \text{ is a cube in } \mathbf{F}_q(\sqrt{-3}) \\ &\iff \pi^2/p = \pi/\pi' \text{ is a cube in } \mathbf{F}_q(\sqrt{-3}). \end{aligned}$$

The proof is now completed as in the case $q \equiv 1 \pmod 3$. □

8.4. Sun's form of Jacobi's law. We now prove Sun's pretty equivalent form of Jacobi's law (see [**Sun98**]), enunciated as the second half of Theorem 2.21 in the introduction. Recall that for each prime $q > 3$ we defined the group $G = G(q)$ by

$$G = \{[a, b] : a, b \in \mathbf{F}_q, a^2 + 3b^2 \neq 0\},$$

where we identify $[a, b]$ and $[c, d]$ if $a = \lambda c, b = \lambda d$ for some nonzero $\lambda \in \mathbf{F}_q$, and where we multiply according to the rule

$$[a, b] \odot [c, d] = [ac - 3bd, ad + bc].$$

All of the group axioms are quickly verified, with $[1, 0]$ as the identity element, except associativity. We leave this to the reader to check by a direct calculation.

Lemma 2.34. *We have* $\#G = q - \left(\frac{-3}{q}\right)$.

Proof. Every element besides $[1, 0]$ can be written uniquely in the form $[a, 1]$ with $a \in \mathbf{F}_q$. We have $[a, 1] \in G$ if and only if $a^2 \neq -3$. Hence

$$\begin{aligned} \#G &= 1 + \#\mathbf{F}_q - \#\{a \in \mathbf{F}_q : a^2 = -3\} \\ &= 1 + q - \left(1 + \left(\frac{-3}{q}\right)\right) = q - \left(\frac{-3}{q}\right). \end{aligned}$$ □

Lemma 2.35. *Let ψ be the map from G to $\mathbf{F}_q(\sqrt{-3})^\times$ defined by*

$$\psi([a, b]) := \frac{a + b\sqrt{-3}}{a - b\sqrt{-3}}.$$

Then ψ is an injective homomorphism. Hence G is cyclic.

Proof. We need to check first that ψ is well-defined: This follows because $a^2 + 3b^2 \neq 0$ and because we are taking a ratio on the right-hand side (so that the ambiguity in $[a, b]$ up to scaling disappears). To see that ψ is a homomorphism, we compute:

$$\begin{aligned}\psi([a,b]\odot[c,d]) &= \psi([ac-3bd, ad+bc])\\ &= \frac{ac-3bd+(ad+bc)\sqrt{-3}}{ac-3bd-(ad+bc)\sqrt{-3}}\\ &= \frac{a+b\sqrt{-3}}{a-b\sqrt{-3}}\cdot\frac{c+d\sqrt{-3}}{c-d\sqrt{-3}} = \psi([a,b])\psi([c,d]).\end{aligned}$$

To see that ψ is injective, it suffices to prove that its kernel is trivial: But

$$\psi([a,b]) = 1 \Longrightarrow \frac{a+b\sqrt{-3}}{a-b\sqrt{-3}} = 1,$$

and this implies that $b = 0$. Hence $[a,b] = [1,0]$ is the identity of G. This proves ψ is an embedding as claimed.

The cyclicity of G is an easy corollary: We can view G as a subgroup of $\mathbf{F}_q(\sqrt{-3})^\times$, and every finite subgroup of the multiplicative group of a field is cyclic. $\square$

We can now prove Sun's form of Jacobi's law:

Theorem 2.36. *Let p and q be distinct primes, with $p, q > 3$ and $p \equiv 1 \pmod 3$. Write $4p = L^2 + 27M^2$ with integers L and M, and let $G = G(q)$ be the group defined above. Then*

$$q \textit{ is a cube modulo } p \Longleftrightarrow [L, 3M] \textit{ is a cube in } G.$$

Proof. Let H be the image of ψ, where ψ is the map of Lemma 2.35 (so that $\#H = \#G$). By Theorem 2.28,

$$\begin{aligned} q \text{ is a cube modulo } p &\Longleftrightarrow \psi([L,3M]) \text{ is a cube in } \mathbf{F}_q(\sqrt{-3})\\ &\Longleftrightarrow \psi([L,3M])^{\#\mathbf{F}_q(\sqrt{-3})^\times/3} = 1\\ &\Longleftrightarrow \psi([L,3M])^{\gcd(\#H, \#\mathbf{F}_q(\sqrt{-3})^\times/3)} = 1\\ &\Longleftrightarrow \psi([L,3M])^{\#H/3} = 1\\ &\Longleftrightarrow \psi([L,3M]^{\#H/3}) = 1.\end{aligned}$$

Since ψ has trivial kernel, the last equality holds precisely when $[L,3M]^{\#H/3}$ is the identity of G. Since $\#H = \#G$, this holds if and only if $[L, 3M]$ is a cube in G. $\square$

As we mentioned in the introduction, Jacobi's cubic reciprocity law implies that whether q is a residue or nonresidue of p depends only on the ratio $L/M \bmod q$. These ratios are the subject of the following two theorems. We leave their proofs as Exercises 16 and 17.

Theorem 2.37 (Cunningham & Gosset [**CG20**]). *Let $p \equiv 1 \pmod 3$ be prime and write $4p = L^2 + 27M^2$ with integers L and M. Let $q > 3$ be a prime distinct from p, and let $n = \frac{1}{3}(q - (\frac{-3}{q}))$. Then q is a cube mod p if and only if*

$$\sum_{\substack{0 \le j \le n \\ j \equiv 1 \ (\mathrm{mod}\ 2)}} 3^j (-3)^{(j-1)/2} \binom{n}{j} L^{n-j} M^j \equiv 0 \pmod q.$$

A more explicit description of these ratios is provided by the next result:

Theorem 2.38 (Sun). *Let $p \equiv 1 \pmod 3$ be prime and write $4p = L^2 + 27M^2$ with integers L and M. Let $q > 3$ be a prime distinct from p. Then q is a cubic residue modulo p if and only if either q divides M or $\frac{L}{3M} \equiv \frac{x^3-9x}{3x^2-3} \pmod q$ for some integer x.*

Notes

Jacobi's law (Theorem 2.21) is an example of a *rational reciprocity law*; the word "rational" is here because the statement of the law refers only to *rational integers*. This is in contrast to Eisenstein's cubic reciprocity law, which is not a statement about rational primes but a statement about primes in the ring $\mathbf{Z}[\omega]$, where ω is a complex primitive cube root of unity.

While Eisenstein's law is harder to state, it has the advantage of being applicable to more problems. To see why Jacobi's law is not the end of the story (even if one is concerned just with $\mathbf{Z}$ and not $\mathbf{Z}[\omega]$), consider the problem of determining the primes $p \equiv 1 \pmod 3$ for which 35 is a cube modulo p. Theorem 2.21 suffices to tell us when 5 is a cube modulo p and when 7 is a cube modulo p. But if neither 5 nor 7 are cubes modulo p, the status of 35 is still undetermined: In this case whether or not 35 is a cube modulo p depends on whether 5 and 7 belong to the same coset or different cosets of $(\mathbf{F}_p^\times)^3$ in $\mathbf{F}_p^\times$.

This suggests the following: Given a prime q different than p, we would like to know not merely when $q^{(p-1)/3} = 1$, but which cube root of unity $q^{(p-1)/3}$ represents in $\mathbf{F}_p$; this is not a question that Jacobi's law answers. However, an answer can be coaxed out of Eisenstein's law. This requires one to translate the problem into the setting of $\mathbf{Z}[\omega]$, where Eisenstein's law operates, work out the answer, and then translate back! Luckily, the heavy lifting has been done by Sun ([**Sun98**, Corollary 2.1, Theorem 2.2]; see also the paper of von Lienen [**vL79**]). He proves the following:

★ **Theorem 2.39.** *Let $p, q > 3$ be distinct primes, and suppose $p \equiv 1 \pmod{3}$. Write $4p = L^2 + 27M^2$. Put*

$$\omega := \frac{-1 - L/3M}{2};$$

by the choice of L and M, this represents a primitive cube root of unity in $\mathbf{F}_p$. Write $\bar{\omega}$ for the element $[1,1]$ of $G(q)$, where $G(q)$ is the group considered in Sun's Theorem 2.36; note that $\bar{\omega}$ is an element of order 3 in $G(q)$. For each $i \in \{0,1,2\}$, we have

$$q^{\frac{p-1}{3}} \equiv \omega^i \pmod{p} \Longleftrightarrow [L, 3M]^{\frac{q - \left(\frac{-3}{q}\right)}{3}} = \bar{\omega}^i \quad \textit{in } G(q).$$

Note that when $i = 0$, this reduces to Theorem 2.36. For an excellent account of Eisenstein's cubic reciprocity law, see Chapter 9 of the text of Ireland & Rosen [**IR90**] or Chapter 7 of Lemmermeyer's beautiful monograph [**Lem00**]. For further discussion of rational reciprocity laws, see [**Lem00**, Chapter 5] and [**BEW98**, Chapters 7 and 8].

Exercises

1. Show that if $\varphi(n)$ is a power of 2, then n has the form $2^e P$, where $e \geq 0$ and P is a product (possibly empty) of distinct Fermat primes.
2. Say that $\alpha \in \mathbf{R}$ is *real-constructible* if it is possible to construct two points a distance $|\alpha|$ apart.
   (a) Prove (or look up) the following (geometric) lemma: If α and β are two real-constructible numbers, then so are
   $$\alpha \pm \beta, \quad \alpha\beta, \quad 1/\alpha \quad (\text{if } \alpha \neq 0), \quad \sqrt{\alpha} \quad (\text{if } \alpha \geq 0).$$
   Hence the real-constructible numbers form a subfield of $\mathbf{R}$, say $\mathrm{Cons}_{\mathbf{R}}$. Show, moreover, that the point (x, y) is constructible if and only if its components x and y are both real-constructible.
   (b) Suppose we have a tower of subfields of the real numbers
   $$\mathbf{Q} := K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m$$
   where $\alpha \in K_m$ and, for $i > 0$, each $K_i = K_{i-1}(\sqrt{\beta_i})$ for some nonnegative $\beta_i \in K_{i-1}$. Using part (a), prove that α is real-constructible.
   (c) Let L be the line described by the equation $ax+by = c$, and let C be the circle described by the equation $(x - x_0)^2 + (y - y_0)^2 = r^2$. Let $K = \mathbf{Q}(a, b, c, x_0, y_0, r)$. Prove that each coordinate of a point of intersection of L and C lies either in K or in a quadratic extension of K.
   (d) Use (c) to prove the converse of (b): If α is real-constructible, then there is such a tower whose last term contains α.
   (e) Prove that the point (x, y) is constructible if and only if $x + iy \in \mathrm{Cons}_{\mathbf{R}}(i)$. Now prove that the elements of (the field!) $\mathrm{Cons}_{\mathbf{R}}(i)$ are exactly the elements described in Lemma 2.3. For one containment you may find helpful the identity
   $$\sqrt{x + iy} = \frac{1}{2}\sqrt{2}\left(\sqrt{\sqrt{x^2 + y^2} + x} + i \ \mathrm{sgn}(y)\sqrt{\sqrt{x^2 + y^2} - x}\right).$$
   Here $\mathrm{sgn}(y) \in \{0, 1, -1\}$ is defined as $y/|y|$ for $y \neq 0$ and defined to be 0 when $y = 0$.
3. Prove that the following are equivalent for every $n \geq 3$:
   (a) It is possible to construct all the vertices of a regular n-gon,
   (b) Some primitive nth root of unity is constructible,
   (c) Every primitive nth root of unity is constructible.

† 4. (Gauss [**Gau86**, Art. 354]) In this exercise we make explicit Theorem 2.5 for the case $p = 17$. We use the notation of Figure 1 for the Gaussian periods.

(a) Using Lemma 2.16, prove the polynomial identities

(i) $(T - (8,1))(T - (8,3)) = T^2 + T - 4$,

(ii) $(T - (4,1))(T - (4,9)) = T^2 - (8,1)T - 1$,

(iii) $(T - (4,3))(T - (4,10)) = T^2 - (8,3)T - 1$,

(iv) $(T - (2,1))(T - (2,13)) = T^2 - (4,1)T + (4,3)$,

(v) $(T - (1,1))(T - (1,16)) = T^2 - (2,1)T + 1$.

(b) Show that one can choose the primitive 17th root of unity ζ so that

$$(8,1) = \frac{-1 + \sqrt{17}}{2} \quad \text{and} \quad (4,1) = \frac{(8,1) + \sqrt{(8,1)^2 + 4}}{2}.$$

Of course the difficulty is in proving that we can make the plus sign hold in both places.

(c) The choices of sign in (b) force a choice of sign for $(4,3)$: To see this, prove that

$$((4,1) - (4,9))\,((4,3) - (4,10)) = 2\,((8,1) - (8,3)) > 0,$$

and deduce that $(4,3) = \frac{1}{2}((8,3) + \sqrt{(8,3)^2 + 4})$.

(d) Prove that we can choose ζ as in (b) so that

$$(2,1) = \frac{(4,1) + \sqrt{(4,1)^2 - 4(4,3)}}{2};$$

again, the nontrivial aspect is to prove that we can force the plus sign. (Note that $(4,1)^2 - 4(4,3) > 0$, as follows from a rough numerical calculation.)

(e) We have

$$(2,1) = \zeta + \zeta^{g^8} = \zeta + \zeta^{-1} = 2\Re(\zeta).$$

Obtain a rough numerical approximation (on a calculator, say) of $(2,1)$ sufficient to prove to pin down ζ to one of the two values $e^{\pm 2\pi i/17}$; hence $(2,1) = 2\cos\frac{2\pi}{17}$.

(f) Prove that $e^{2\pi i/17}$ and $e^{-2\pi i/17}$ are the roots of $T^2 - (2,1)T + 1$.

(g) Combining (a)–(e), show that

$$(2,1) = 2\cos\frac{2\pi}{17} = \frac{1}{8}\sqrt{34 - 2\sqrt{17}} - \frac{1}{8} + \frac{1}{8}\sqrt{17} +$$
$$\frac{1}{8}\sqrt{68 + 12\sqrt{17} - 2\sqrt{34 - 2\sqrt{17}} + 2\sqrt{34 - 2\sqrt{17}}\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}}}.$$

Now use (f) to compute an explicit representation of ζ_{17}. (You may wish to use a computer algebra system for this part.)

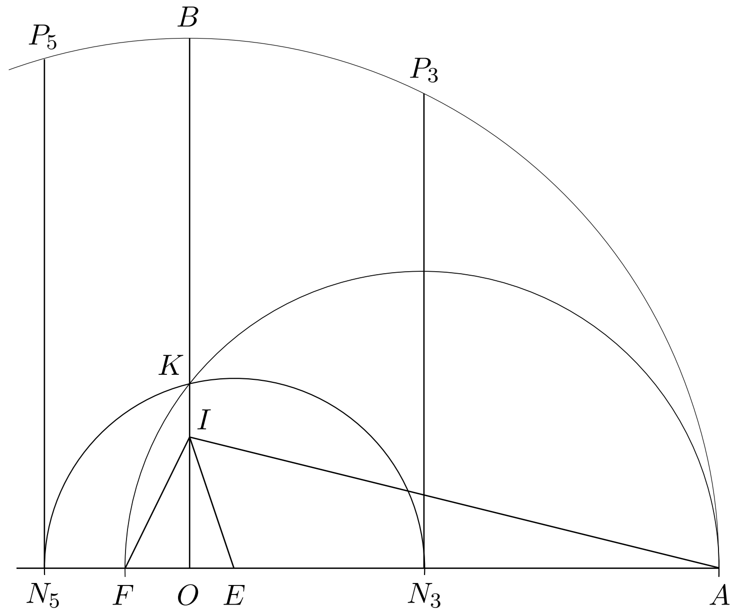

Figure 2. Diagram accompanying Richmond's construction of the 17-gon (see Exercise 5), based on [**HW08**, Fig. 5, p. 76].

Lecture 7 of [**Rad64**] is a self-contained account of the results of this exercise; see also Hardy & Wright [**HW08**, §5.8].

5. The result of the preceding exercise gives us an explicit way of constructing the 17-gon; however, such a direct attack is both inefficient and onerous. In 1893, Richmond proposed the following alternative geometric construction ([**Ric93, Ric09**]):

> Let OA, OB [Figure 2] be two perpendicular radii of a circle. Make OI one-fourth of OB, and the angle OIE one-fourth of OIA; also find in OA produced a point F such that EIF is 45°. Let the circle on AF as diameter cut OB in K, and let the circle whose centre is E and radius EK cut OA in N_3 and N_5; then if ordinates N_3P_3, N_5P_5 are drawn to the circle, the arcs AP_3, AP_5 will be $3/17$ and $5/17$ of the circumference.

   Prove Richmond's assertions. If you have trouble with this, Hardy & Wright [**HW08**, §5.8] present his construction in detail.

† 6. (Luca [**Luc00b**]) Say that the natural number $n \geq 2$ has property (C) if both the regular $(n-1)$-gon and regular n-gon are constructible. Using the Gauss–Wantzel Theorem, show that if n has property (C), then

either n is a Fermat prime or $n \in \{2 \cdot 3, 2^2, 2^{2^2}, 2^{2^3}, 2^{2^4}, 2^{2^5}\}$. Proceed as follows:

(a) Consider a nonempty product of distinct Fermat numbers $F_m = 2^{2^m} + 1$, say

$$F_{n_0} F_{n_1} \cdots F_{n_{k-1}}, \tag{2.21}$$

where $0 \leq n_0 < n_1 < \cdots < n_{k-1}$.

(i) Prove that this product has precisely 2^k nonzero digits in its binary expansion.

(ii) Show that, moreover, there are $1+2^{n_0}+2^{n_1}+\cdots+2^{n_{k-1}}$ total binary digits in this product. Thus, if we start with the number of binary digits in the product, subtract one and compute the binary expansion, we can read off the n_i corresponding to the Fermat number factors.

(b) Using (a), prove that any odd number n with property (C) is a Fermat prime.

(c) Suppose n is even and has property (C). Using (b), show that if $n \equiv 2 \pmod 4$, then $n - 1 = F_1$, and so $n = 6$.

(d) Finally, suppose n has property C where $4 \mid n$. Since $n - 1 \equiv 3 \pmod 4$, if we write $n - 1$ in the form (2.21), then $n_0 = 0$. Suppose that $n_0 = 0$, $n_1 = 1$, $n_2 = 2$, $\ldots$, $n_{k'} = k'$ for a certain $k' \geq 0$ while $n_j \geq k'+2$ for the remaining indices $k' < j < k$. Verify that in this case the binary expansion of $n-1$ ends with precisely $2^{k'+1}$ trailing 1's, and the binary expansion of n contains precisely $2^k - 2^{k'+1} + 1$ nonzero binary digits.
Now obtain a contradiction to (i) unless $k = k' + 1$, i.e., unless $n - 1 = F_0 F_1 \cdots F_{k'}$. Complete the proof making use of Euler's discovery that F_5 is composite.

7. Here we give two proofs for the irreducibility of the cyclotomic polynomials $\Phi_n(T)$: Let ζ be a primitive nth root of unity and let $f(T) \in \mathbf{Q}[T]$ be its minimal polynomial. It is easy to show that $f(T) \in \mathbf{Z}[T]$ and that $f(T)$ divides $\Phi_n(T)$ in $\mathbf{Z}[T]$. We would like to show that $f(T) = \Phi_n(T)$, and for this it suffices to prove that ζ^a is a root of f for each a coprime to n.

(a) Prove that a nonzero element of the ring $\mathbf{Z}[\zeta]$ is divisible by only finitely many rational primes p.

(b) Prove that $p \mid f(\zeta^p)$ in $\mathbf{Z}[\zeta]$ for every prime p not dividing n.

(c) (Grandjot [**Gra23**]) We can now give a simple proof by means of Dirichlet's theorem. Let a be coprime to n. Letting p run through the primes congruent to a mod n, show that the single element $f(\zeta^a)$ has infinitely many rational prime divisors; conclude from part (i) that $f(\zeta^a) = 0$ as desired.

(d) (Landau [**Lan28**]) Here is an alternative argument avoiding Dirichlet's result. Using (a), show that we can choose a number B (depending only on n) so that if $p > B$ is prime and a is coprime to n, then either $f(\zeta^a) = 0$ or $p \nmid f(\zeta^a)$. Fix such a B, and fix a particular integer a coprime to n. Choose a positive integer m with $m \equiv a \pmod{n}$ and m coprime to $\prod_{p \le B} p$. Factor $m = q_1 q_2 \cdots q_j$ as a product of primes, and show successively that all of

$$\zeta^{q_1}, \zeta^{q_1 q_2}, \ldots, \zeta^{q_1 \cdots q_j} = \zeta^a$$

are roots of f.

(e) (Pomerance, private communication) Another argument avoiding Dirichlet's theorem: Let H be the subset of $(\mathbf{Z}/n\mathbf{Z})^\times$ consisting of those residue classes $a \bmod n$ for which $f(\zeta^a) = 0$. Show that H is a subgroup of $(\mathbf{Z}/n\mathbf{Z})^\times$. Assuming H is proper, derive a contradiction from (a), (b), and Theorem 1.17.

8. Let $p \equiv 1 \pmod{3}$. Suppose that $A_1, B_1, A_2, B_2 \in \mathbf{Z}$ and $A_1^2 + 27B_1^2 = A_2^2 + 27B_2^2 = 4p$. Prove that $A_1 = \pm A_2$ and $B_1 = \pm B_2$. *Hint:* Verify the identity

$$16p^2 = (A_1 A_2 \pm 27 B_1 B_2)^2 + 27(A_2 B_1 \mp A_1 B_2)^2.$$

Also, check that

$$p \mid (A_1 A_2 - 27 B_1 B_2)(A_2 B_1 - A_1 B_2)$$

and

$$p \mid (A_1 A_2 + 27 B_1 B_2)(A_2 B_1 + A_1 B_2).$$

Deduce that $p \mid A_2 B_1 \pm A_1 B_2$ for one of the choices of sign, and conclude that $A_1/A_2 = \pm B_1/B_2$.

9. Prove Lemma 2.32.

† 10. (Ankeny; see [**Ank60**]) Fix a prime e. Let p and q be primes distinct from each other and distinct from e with $p \equiv 1 \pmod{e}$. Let ζ_e and ζ_p be fixed primitive eth and pth roots of unity in a fixed algebraic closure $\overline{\mathbf{F}}_q$ of $\mathbf{F}_q$. Let $\chi\colon \mathbf{F}_p^\times \to \overline{\mathbf{F}}_q^\times$ be a homomorphism whose image is precisely the set of eth roots of unity in $\overline{\mathbf{F}}_q^\times$. We define the *Gauss sum* $\tau_a(\chi)$ by

$$\tau_a(\chi) := \sum_{n=1}^{p-1} \chi(n) \zeta_p^{an}.$$

If $a = 1$, we write $\tau_1(\chi) = \tau(\chi)$.

(a) Prove that $\tau_a(\chi)\tau_{-a}(\chi^{-1}) = p$ for every a not divisible by p. So, in particular, $\tau_a(\chi)$ is nonzero for all such a. *Hint:*

$$\tau_a(\chi)\tau_{-a}(\chi^{-1}) = \sum_{n,m \in \mathbf{F}_p^\times} \chi(nm^{-1}) \zeta_p^{a(n-m)} = \sum_{l \in \mathbf{F}_p^\times} \chi(l) \sum_{m \in \mathbf{F}_p^\times} \zeta_p^{am(l-1)}.$$

Table 4. Primes $p = 3 \cdot 2^n + 1$ with $n \le 750000$ which divide some Fermat number F_m.

n	Fermat number F_m	Discoverer	Discovered
41	F_{38}	R. M. Robinson	1956
209	F_{207}	R. M. Robinson	1956
157169	F_{157167}	J. Young	1995
213321	F_{213319}	J. Young	1996
303093	F_{303088}	J. Young	1998
382449	F_{382447}	J. B. Cosgrave & Y. Gallot	1999

(b) Let f be the order of q (mod e). Prove that $\tau(\chi)^{q^f} = \chi(q)^{-f}\tau(\chi)$.

(c) Deduce from (b) that $\tau(\chi)^e$ is fixed by the q^fth power map, and conclude that $\tau(\chi)^e \in \mathbf{F}_q(\zeta_e)$.

(d) Using (a)–(c), show that

$$\begin{aligned} q \text{ is an } e\text{th power mod } p &\iff (\tau(\chi)^e)^{\frac{q^f-1}{e}} = 1 \\ &\iff \tau(\chi)^e \text{ is an } e\text{th power in } \mathbf{F}_q(\zeta_e). \end{aligned}$$

11. (Continuation) Here we consider the cases $e = 2$ and $e = 3$ which correspond to Gauss's quadratic reciprocity law and Jacobi's cubic reciprocity law.

(a) Let $e = 2$, so that the nontrivial character $\chi(\cdot)$ of order 2 can be identified with the Legendre symbol $\left(\frac{\cdot}{p}\right)$. Prove that $\tau_{-1}(\chi) = \chi(-1)\tau_1(\chi)$. Using part (a) of the preceding exercise, show that $\tau(\chi)^2 = \left(\frac{-1}{p}\right)p$, and deduce from part (d) another proof of the law of quadratic reciprocity.

(b) Now suppose $e = 3$. One can show that for any χ as in the preceding exercise, we have $\tau(\chi)^3 = p\pi$, where $\pi = \frac{L+3M\sqrt{-3}}{2}$ for certain integers L, M satisfying $L^2 + 27M^2 = 4p$ and $L \equiv 1 \pmod 3$ (cf. [**Gau86**, footnote to Art. 358], [**IR90**, p. 115]). Assuming this result, deduce another proof of Jacobi's cubic reciprocity law.

12. Give a necessary and sufficient condition in terms of L and M for 6 to be a cubic residue modulo p.

13. (Golomb [**Gol76**])

(a) Suppose $p = 3 \cdot 2^n + 1$ is prime. Show that p divides the jth Fermat number $F_j = 2^{2^j} + 1$ for some j if and only if the order of 3 (mod p) is not divisible by 3. Moreover, show that in this case there is exactly one such j, and $j < n$.

(b) Prove that if $p = 3 \cdot 2^{2m} + 1$ is prime, then the order of 2 modulo p is divisible by 3, and hence no such primes can divide Fermat numbers. *Hint:* Show that 2 is not a cubic residue modulo such a prime.

Table 4 lists all primes of the form $3 \cdot 2^n + 1$ with $n \leq 750000$ which divide a Fermat number.

14. (Kraïtchik, Pellet) Suppose that both $q = 2n + 1$ and $p = 12n + 7$ are prime. Prove that if $p = L'^2 + 27M'^2$ for integers L' and M', then $q \mid 2^p - 1$.

    Prove that if both $q = 12n + 5$ and $p = 72n + 31$ are prime, and $p = L'^2 + 27M'^2$ for integers L' and M', then $q \mid 2^p - 1$.

    Example: Let $n = 18$; then $q = 37$, $p = 223 = 14^2 + 27 \cdot 1^2$, and $2^{37} - 1 = 223 \cdot 616318177$.

    For other results of this kind see the papers of Fueter [**Fue46**], Storchi [**Sto55**] and Golubev [**Gol58**].

15. Use Kummer's criterion to give another proof that 2 is a cube mod p if and only if $2 \mid L$ and $2 \mid M$, and that 3 is a cube mod p if and only if $3 \mid M$. Note that these results are less precise than those of Theorems 2.26 and 2.27. *Hint:* Before tackling the problem of when 3 is a cube, rewrite the final coefficient of the period polynomial in a form more amenable to computations modulo 3.

16. Prove Theorem 2.37. Use Jacobi's law in the form stated in Theorem 2.28 and the binomial theorem.

17. Prove Theorem 2.38, using Sun's form of Jacobi's reciprocity law.

† 18. (Lehmer [**Leh58**]) Let $p \equiv 1 \pmod 3$ be prime, and suppose $q > 3$ is a prime distinct from p. Write $4p = L^2 + 27M^2$. Suppose that $p \equiv \lambda L^2 \pmod q$ for a prime λ which can be written in the form $4\lambda = 1 + 27m^2$ with $q \nmid m$. Show that q is a cube modulo p if and only if q is a cube modulo λ.

    Example (with $\lambda = 7, m = 1$): If $p \equiv 7L^2 \pmod q$ (equivalently, if $L^2 \equiv M^2 \pmod q$), then q is a cubic residue modulo p if and only if $q \equiv \pm 1 \pmod 7$.

† 19. Let $p \equiv 1 \pmod 3$ be prime, and write $4p = L^2 + 27M^2$, where $L \equiv 1 \pmod 3$. For each integer c not divisible by p, let N_c be the number of ordered pairs $(x, y) \in \mathbf{F}_p^2$ with $x^3 + y^3 = c$.
    (a) (Gauss) Show that if c is a cube modulo p, then $N_c = p - 2 + L$.
    (b) (Chowla, Cowles, & Cowles [**CCC80**]) Suppose c is not a cube modulo p. Show that $N_c = p - 2 + \frac{1}{2}(\pm 9M - L)$ and describe how to determine the correct choice of sign.
    (c) Deduce that in every case, $|N_c - (p - 2)| \leq 2\sqrt{p}$. This is a special case of Hasse's *Riemann Hypothesis for elliptic curves.*

(d) Show that if p is any prime with $p > 7$, then every element of $\mathbf{F}_p$ is a sum of two cubes. Show, moreover, that if $p > 13$, then every element of $\mathbf{F}_p$ is a sum of two nonzero cubes.

Hint for (b): Give a criterion for α and $c-\alpha$ to be simultaneously cubes in terms of $c^{-1}\alpha$ and $c^{-1}\alpha - 1$.

Remark. Leep & Shapiro [**LS89**] have shown that if G is a multiplicative subgroup of index 3 in an arbitrary field F, then every element of F can be written as a sum of two elements of G, unless $\#F = 4, 7, 13$, or 16; see also [**BS92**].

† 20. (Gauss [**Gau86**, footnote to Art. 358], Jacobi [**Jac27, Jac69**]) Let $p \equiv 1 \pmod 3$ be prime, say $p = 3f + 1$. Write $4p = L^2 + 27M^2$, where $L \equiv 1 \pmod 3$. Put

$$S := \sum_{\alpha \in \mathbf{F}_p^\times} (\alpha^3 + 1)^{2(p-1)/3}.$$

(a) Using the binomial theorem, prove that $S = -2 - \binom{2f}{f}$.

(b) Let g be a generator of $\mathbf{F}_p^\times$ and let ω be the element of $\mathbf{F}_p^\times$ defined by $\omega := g^{(p-1)/3}$. Show that, with a, b, and c as in Theorem 2.23, we have $S = 3a + 3b\omega^2 + 3c\omega$.

(c) Check that $(\omega^2 - \omega)^2 = -3$.
In what follows we write "$\sqrt{-3}$" as an abbreviation for the element $\omega^2 - \omega \in \mathbf{F}_p^\times$.

(d) Deduce from (b) and the explicit expressions for a, b, and c in Theorem 2.23 that $S = -2 + \frac{L+3M\sqrt{-3}}{2}$.

(e) Conclude that $L + 3M\sqrt{-3} = -2\binom{2f}{f}$ in $\mathbf{F}_p$. Deduce that $L - 3M\sqrt{-3} = 0$ in $\mathbf{F}_p$.

(f) Show that L is the least absolute remainder of $-\binom{2f}{f}$ modulo p. In other words, L is the unique integer in the interval $(-p/2, p/2)$ with $L \equiv -\binom{2f}{f} \pmod p$.
Example: Take $p = 109 = 3 \cdot 36 + 1$. We have $\binom{2\cdot 36}{36} \equiv 2 \pmod{109}$ and $4 \cdot 109 = 2^2 + 27 \cdot 4^2$.

Elementary Prime Number Theory, II

> Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate. – L. Euler

> Even before I had begun my more detailed investigations into higher arithmetic, one of my projects was to turn my attention to the decreasing frequency of primes, to which end I counted the primes in several chiliads [intervals of length 1000]... I soon recognized that behind all of its fluctuations, this frequency is on average inversely proportional to the logarithm, so that the number of primes below a given bound n is approximately equal to
> $$\int \frac{dn}{\log n},$$
> where the logarithm is understood to be hyperbolic. – C. F. Gauss

1. Introduction

We began our study of prime number theory in Chapter 1 with several different proofs that there are infinitely many primes. In this chapter we turn to the question of how these infinitely many primes are distributed on the real number line. Once again, let $\pi(x)$ denote the number of primes

Table 1. Comparison of $\Delta(x)$ and $1/\log x$, rounded to the nearest thousandth.

x	1000	2000	3000	4000	5000	6000	7000	8000	9000	10000
$\Delta(x)$	.144	.128	.122	.121	.115	.117	.108	.109	.118	0.107
$\frac{1}{\log x}$	.145	.132	.125	.121	.117	.115	.113	.111	.110	0.109

$p \leq x$. We would like to understand how quickly and how regularly $\pi(x)$ grows.

1.1. Discovering the prime number theorem. As is the case with much mathematics, the first substantial investigations here were carried out by Gauss. In an 1849 letter to the mathematician and astronomer Encke, Gauss recounted how almost sixty years prior, as a boy of 15 or 16, he had taken an interest in the function $\pi(x)$.

Gauss's study began with an investigation of what we could term the "local density" of primes near a number x. (Some of Gauss's tables have been preserved in [**Gau73b**, p. 435–443].) Here when we say "local density", what we have in mind is the ratio of the count of primes "near x" with the total number of integers "near x". Of course this is somewhat vague; Gauss counted primes in intervals of 1000, which suggests defining

$$\Delta(x) := \frac{\pi(x+500) - \pi(x-500)}{1000}.$$

Thus $\Delta(x)$ is the probability of choosing a prime if one samples an integer uniformly at random from the interval $(x-500, x+500]$. Table 1 displays some values of x vs. $\Delta(x)$. From this limited data it appears that $\Delta(x)$ is generally decreasing, albeit somewhat slowly.

But how slowly? To answer this question, Gauss considered the inverse ratio, $\Delta(x)^{-1}$, and discovered empirically that $\Delta(x) \approx 1/\log x$ (which is also illustrated in Table 1). Since $\Delta(x)$ is the slope of a chord on the graph of $y = \pi(x)$, it is natural to think that one could recover $\pi(x)$ by integrating $1/\log x$. This suggests that

$$\pi(x) \approx \int_2^x \frac{dt}{\log t}. \tag{3.1}$$

We use the notation $\mathrm{Li}(x)$ for the integral appearing on the right-hand side of this approximation; it is known as the *(Eulerian) logarithmic integral*. We refer to (3.1) as the *Gauss approximation to* $\pi(x)$.

Table 2 compares $\pi(x)$ and $\mathrm{Li}(x)$ for powers of 10 from 10^3 through 10^{13}. The last column of this table is the most revealing. It suggests that for larger and larger values of x, the Gauss approximation very quickly approaches 100% accuracy. In other words, it seems that the following is

Table 2. Comparison of $\pi(x)$ and $\mathrm{Li}(x)$, where $\mathrm{Li}(x)$ is rounded to the nearest integer. The last column gives the percentage error, computed as $|\mathrm{Li}(x) - \pi(x)|/\pi(x)$.

x	$\pi(x)$	$\mathrm{Li}(x)$	$\mathrm{Li}(x) - \pi(x)$	% error
10^3	168	177	9	5.4%
10^4	1229	1245	16	1.3%
10^5	9,592	9,629	37	3.8×10^{-1} %
10^6	78,498	78,627	129	1.6×10^{-1} %
10^7	664,579	664,917	338	5.1×10^{-2} %
10^8	5,761,455	5,762,208	753	1.3×10^{-2} %
10^9	50,847,534	50,849,234	1,700	3.3×10^{-3} %
10^{10}	455,052,512	455,055,614	3,102	6.8×10^{-4} %
10^{11}	4,118,054,813	4,118,066,400	11,587	2.8×10^{-4} %
10^{12}	37,607,912,018	37,607,950,280	38,262	1.0×10^{-4} %
10^{13}	346,065,536,839	346,065,645,809	108,970	3.2×10^{-5} %

true:

★ **Theorem 3.1** (Prime number theorem)**.** *$\pi(x) \sim \mathrm{Li}(x)$ as $x \to \infty$.*

In 1859, Riemann outlined a strategy for proving Theorem 3.1 based on viewing the function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, introduced by Euler, as a function of a *complex* variable s. But it took until 1896 for complex analysis to mature to the point where Riemann's outline could be filled in; this was done independently by Hadamard and de la Vallée-Poussin. There are still no simple proofs of Theorem 3.1, although there are short proofs which require only a modicum of familiarity with complex analysis (see, e.g., [**Zag97**]). In Chapter 8, we will give a (long) proof of the prime number theorem completely independent of the theory of complex variables.

1.2. An alternative formulation of the prime number theorem. The prime number theorem is often stated in the following simpler form:

★ **Theorem 3.2** (Prime number theorem, alternative form)**.** *As $x \to \infty$, $\pi(x) \sim x/\log x$.*

It is not difficult to show that Theorems 3.1 and 3.2 are equivalent: If we integrate $1/\log t$ by parts, we find that

$$\begin{aligned}\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} &= \left.\frac{t}{\log t}\right|_2^x + \int_2^x \frac{dt}{(\log t)^2}\\ &= \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{dt}{(\log t)^2}.\end{aligned}$$

Moreover, the final integral is $o(\mathrm{Li}(x))$. Indeed, by L'Hôpital's rule,

$$\lim_{x\to\infty} \frac{\int_2^x \frac{dt}{(\log t)^2}}{\mathrm{Li}(x)} = \lim_{x\to\infty} \frac{1/(\log x)^2}{1/\log x} = 0.$$

Hence $\mathrm{Li}(x) \sim x/\log x$, from which the equivalence of Theorems 3.1 and 3.2 follows.

1.3. What happens now? Since the prime number theorem is not proved until Chapter 8, what is left for us to do here? Prior to the proof of Theorem 3.1, several estimates for quantities related to $\pi(x)$ were obtained by Chebyshev, Mertens, and others. For many applications, these are more than sufficient; the prime number theorem itself is not required. In particular, this comment applies to our treatment of sieve methods in Chapter 6. Moreover, these estimates are necessary preliminaries for our eventual proof of the prime number theorem. We devote most of this chapter to a discussion of these results and their charming, elementary proofs.

In the final section we revisit Gauss's heuristic for the prime number theorem. We explain how Gauss's observation that the "local density" of the primes near x is $\approx 1/\log x$ suggests many other statements about primes. For example, we show how Gauss's idea can be used to formulate a plausible prediction of the number of twin prime pairs up to x.

2. The set of prime numbers has density zero

After a moment's reflection on the definitions, most intelligent laymen can convince themselves that the prime numbers account for at most half of the natural numbers. Indeed, one of the first facts people tend to notice about the primes is that every prime number $p > 2$ is odd. A small elaboration on this trivial observation permits one to establish the following:

Theorem 3.3. *$\pi(x)/x \to 0$ as $x \to \infty$. That is, the set of primes has asymptotic density zero.*

Proof. Let q be any (fixed) natural number. Then every prime p that does not divide q belongs to one of the $\varphi(q)$ invertible residue classes modulo q. The number of natural numbers $n \leq x$ which fall in a given residue class modulo q is at most $1 + x/q$, and so the number of $n \leq x$ which are coprime to q is at most $\varphi(q) + x\varphi(q)/q$. Since only finitely many primes p divide q, this shows that

$$\pi(x) \leq (\varphi(q)/q + o(1))x \quad (x \to \infty).$$

Theorem 3.3 will follow if we can show that $\varphi(q)/q$ can be made arbitrarily small. For each $z > 0$, put $q := q_z = \prod_{p \leq z} p$. From (1.4), we have

$$\frac{\varphi(q_z)}{q_z} = \prod_{p \le z} \left(1 - \frac{1}{p}\right) \le \exp\left(-\sum_{p \le z} \frac{1}{p}\right).$$

Since $\sum_p p^{-1}$ diverges, it follows that $\varphi(q_z)/q_z \to 0$ as $z \to \infty$. $\square$

It is remarkable that a result asserting that there are not too few primes (namely, that $\sum_p p^{-1}$ diverges) is used here to show that there are not too many primes (Theorem 3.3). Amusingly, if we assume (contrary to fact) that $\sum_p p^{-1}$ converges, we can also show easily that $\pi(x)/x \to 0$; see Exercise 1.

3. Three theorems of Chebyshev

> [Chebyshev] was the only man ever able to cope with the refractory character and erratic flow of prime numbers and to confine the stream of their progression with algebraic limits, building up, if I may so say, banks on either side which that stream, devious and irregular as are its windings, can never overflow. – J. J. Sylvester

In 1851 and 1852, Chebyshev published two important papers [**Che51, Che52**] on the behavior of $\pi(x)$. We shall focus our attention on three of his results:

Theorem 3.4. *If* $\frac{\pi(x)}{x/\log x}$ *tends to a limit as* $x \to \infty$*, then that limit is* 1.

Theorem 3.5. *There exist positive constants* c_1, c_2 *and a real number* x_0 *so that*

$$c_1 \frac{x}{\log x} \le \pi(x) \le c_2 \frac{x}{\log x} \quad (\textit{whenever } x > x_0).$$

Theorem 3.5 shows that the prime number theorem at least predicts the correct order of magnitude of $\pi(x)$. Theorem 3.4 shows that if $\pi(x)$ behaves regularly enough that $\pi(x) \sim cx/\log x$ for some constant c, then the prime number theorem holds. (For a more general result of the same character as Theorem 3.4, see Exercises 30 and 31.)

Theorem 3.6 (Bertrand's postulate)**.** *For all sufficiently large* x*, there is a prime in the interval* $(x, 2x]$.

Actually Bertrand conjectured, and Chebyshev proved, that the conclusion of Theorem 3.6 is valid for every real $x \ge 1$. This follows from the argument presented below after a finite computation; cf. Exercises 13–14.

Before proving these results, it is convenient to introduce certain auxiliary functions. Put

$$\theta(x) := \sum_{p \le x} \log p, \qquad \psi(x) := \sum_{n=1}^{\infty} \theta(x^{1/n}).$$

The sum defining ψ appears to be infinite, but is morally finite since $\theta(x^{1/n})$ vanishes once $x^{1/n} < 2$. The functions ψ and θ turn out to be better-behaved and easier to study than $\pi(x)$. Fortunately, estimates for $\pi(x)$ can be easily deduced from estimates for either θ or ψ: By partial summation,

$$\theta(x) = \pi(x) \log x - \int_2^x \frac{\pi(t)}{t}\, dt.$$

Because $\pi(t)/t = o(1)$ (Theorem 3.3), we have $\int_2^x \pi(t)/t\, dt = o(x)$, whence

$$\theta(x) = \pi(x) \log x + o(x),$$

and

$$\frac{\theta(x)}{x} = \frac{\pi(x)}{x/\log x} + o(1). \tag{3.2}$$

The analogue of (3.2) holds with ψ in place of θ, because the difference between ψ and θ is quite small: Indeed, write

$$\psi(x) - \theta(x) = \theta(x^{1/2}) + \theta(x^{1/3}) + \cdots . \tag{3.3}$$

As observed above, $\theta(x^{1/n})$ vanishes whenever $x^{1/n} < 2$, i.e., once $n > \log x / \log 2$. Consequently, only $O(\log x)$ of the terms on the right of (3.3) are nonzero. Because $\theta(t) \le \sum_{n \le t} \log t \le t \log t$ trivially,

$$\psi(x) - \theta(x) \ll x^{1/2} \log x + (x^{1/3} \log x) \log x \ll x^{1/2} \log x. \tag{3.4}$$

Thus replacing θ with ψ in equation (3.2) results in an extra error term of $O((\log x) x^{-1/2})$, which can be absorbed into the existing $o(1)$ error term. Thus we have proved:

Proposition 3.7. *As $x \to \infty$, we have both*

$$\frac{\theta(x)}{x} = \frac{\pi(x)}{x/\log x} + o(1), \tag{3.5}$$

$$\frac{\psi(x)}{x} = \frac{\pi(x)}{x/\log x} + o(1). \tag{3.6}$$

This has the following useful consequence:

Corollary 3.8. *If any of $\frac{\theta(x)}{x}$, $\frac{\psi(x)}{x}$, or $\frac{\pi(x)}{x/\log x}$ tends to a limit as $x \to \infty$, then all of them do, and the limit in each case is the same. In particular, the prime number theorem is equivalent to the estimate $\theta(x) \sim x$ and to the estimate $\psi(x) \sim x$.*

Indeed, (3.5) and (3.6) together imply that

$$\liminf_{x\to\infty} \frac{\theta(x)}{x} = \liminf_{x\to\infty} \frac{\pi(x)}{x/\log x} = \liminf_{x\to\infty} \frac{\psi(x)}{x},$$

and similarly for the lim sup.

The definition of ψ given above is useful for making comparisons with θ, but it masks the arithmetic information that ψ encodes. To get at this, observe that for any fixed positive integer k,

$$\theta(x^{1/k}) = \sum_{p\le x^{1/k}} \log p = \sum_{p^k\le x} \log p.$$

Hence

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \cdots = \sum_{p^k\le x} \log p, \tag{3.7}$$

where the final sum is over *all* pairs (p,k) where p is prime, k is a positive integer and $p^k \le x$. Define the *von Mangoldt function* $\Lambda(n)$ by

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

The fundamental theorem of arithmetic assures us that Λ is well-defined, and from equation (3.7) we can read off the identity

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

Lemma 3.9. *For every positive integer n,*

$$\sum_{d\mid n} \Lambda(n) = \log n.$$

Proof. Write $n = \prod_{p\mid n} p^{e_p}$. Then

$$\sum_{d\mid n} \Lambda(d) = \sum_{p^k\mid n} \log p = \sum_{p\mid n} \sum_{k=1}^{e_p} \log p$$

$$= \sum_{p\mid n} e_p \log p = \sum_{p\mid n} \log p^{e_p} = \log \left(\prod_{p\mid n} p^{e_p} \right) = \log n. \square$$

Following Chebyshev, we now set $T(x) := \sum_{n\le x} \log n$.

Lemma 3.10. *For $x \ge 2$, we have*

$$T(x) = x\log x - x + O(\log x). \tag{3.8}$$

Proof. Since $\log t$ is increasing for $t > 0$, we have $\log n \leq \int_n^{n+1} \log t\,dt \leq \log(n+1)$ for each natural number n. So

$$\sum_{n \leq x} \log n \leq \int_1^{\lfloor x \rfloor + 1} \log t\,dt = (\lfloor x \rfloor + 1)\log(\lfloor x \rfloor + 1) - (\lfloor x \rfloor + 1) + 1$$

and

$$\sum_{n \leq x} \log n = \sum_{2 \leq n \leq x} \log n \geq \int_1^{\lfloor x \rfloor} \log t\,dt = \lfloor x \rfloor \log \lfloor x \rfloor - \lfloor x \rfloor + 1.$$

Both the upper and lower bounds are $x \log x - x + O(\log x)$, and so the lemma follows. $\square$

The link between $T(x)$ and prime number theory is given by the following result, which is the fundamental tool in the proofs of Theorems 3.4–3.6.

Lemma 3.11. *For every $x > 0$, we have $T(x) = \sum_{n \leq x} \psi(x/n)$.*

Proof. Observe that

$$\begin{aligned}\sum_{n \leq x} \psi(x/n) &= \sum_{n \leq x} \sum_{m \leq x/n} \Lambda(m) = \sum_{nm \leq x} \Lambda(m) \\ &= \sum_{N \leq x} \sum_{m \mid N} \Lambda(m) = \sum_{N \leq x} \log N = T(x). \quad \square\end{aligned}$$

3.1. Proof of Theorem 3.4. We begin with a plausibility argument for the prime number theorem: From Lemma 3.11 and (3.8),

$$\sum_{n \leq x} \psi(x/n) \sim x \log x \qquad (x \to \infty). \tag{3.9}$$

This is the same estimate one would obtain if the terms on the left of (3.9) were "x/n" instead of "$\psi(x/n)$", which can be considered evidence for the prime number theorem in the form $\psi(x) \sim x$.

This idea can be used to prove the following proposition, which in view of Proposition 3.7 implies Theorem 3.4.

Proposition 3.12. *We have*

$$\liminf_{x \to \infty} \frac{\psi(x)}{x} \leq 1 \leq \limsup_{x \to \infty} \frac{\psi(x)}{x}.$$

Proof. Put $c := \liminf_{x\to\infty} \psi(x)/x$ and $C := \limsup_{x\to\infty} \psi(x)/x$. Then $\psi(x) \geq cx + g(x)$ for a function $g(x)$ satisfying $g(x) = o(x)$. Hence

$$\begin{aligned}\sum_{n\leq x} \psi(x/n) &\geq cx \sum_{n\leq x} n^{-1} + \sum_{n\leq x} g(x/n) \\ &= cx\log x + o(x\log x) + \sum_{n\leq x} g(x/n).\end{aligned}$$

We claim that the final summand can be absorbed into the error term $o(x\log x)$. This implies that $\sum_{n\leq x}\psi(x/n) \geq (c+o(1))x\log x$, which (by (3.9)) implies $c \leq 1$. A similar argument, with c replaced by C, shows that $C \geq 1$.

To prove the claim about $\sum g(x/n)$, let $\epsilon > 0$ be given and choose N so large that $|g(t)|t^{-1} < \epsilon/2$ whenever $t > N$. Let M be an upper bound for $|g|$ on $[1, N]$. Then

$$\begin{aligned}\left|\sum_{n\leq x} g(x/n)\right| &\leq \sum_{\substack{n\leq x\\ x/n\leq N}} |g(x/n)| + \sum_{\substack{n\leq x\\ x/n>N}} |g(x/n)| \\ &\leq Mx + \frac{\epsilon}{2}x\sum_{n\leq x} n^{-1} < \epsilon x\log x\end{aligned}$$

for sufficiently large x. □

3.2. Proof of Theorem 3.5. Suppose $x \geq 4$. By Lemma 3.10,

$$\begin{aligned}T(x) - 2T(x/2) &= x\log x - x + O(\log x) - 2\left(\frac{x}{2}\log\frac{x}{2} - \frac{x}{2} + O\left(\log\frac{x}{2}\right)\right) \\ &= x\log 2 + O(\log x).\end{aligned}$$

On the other hand, Lemma 3.11 implies that

$$\begin{aligned}T(x) - 2T(x/2) &= \sum_{n\leq x}\psi(x/n) - \sum_{n\leq x} 2\psi(x/2n) \\ &= \sum_{n\geq 1}(-1)^{n-1}\psi(x/n) = \psi(x) - \psi(x/2) + \cdots.\end{aligned}$$

Since ψ is an increasing function, this is an alternating series of decreasing terms. It follows that for any even k,

$$T(x) - 2T(x/2) \geq \psi(x) - \psi(x/2) + \cdots + \psi(x/(k-1)) - \psi(x/k), \tag{3.10}$$

while for any odd k,

$$T(x) - 2T(x/2) \leq \psi(x) - \psi(x/2) + \cdots - \psi(x/(k-1)) + \psi(x/k). \tag{3.11}$$

Taking $k = 1$ in (3.11) gives the lower bound

$$\psi(x) \geq T(x) - 2T(x/2) = x\log 2 + O(\log x).$$

Getting an upper bound on $\psi(x)$ is a tad bit trickier. First take $k = 2$ in (3.10) to find that

$$\psi(x) - \psi(x/2) \leq T(x) - 2T(x/2) = x\log 2 + O(\log x).$$

Now let k be the positive integer for which $x/2^{k-1} \geq 4 > x/2^k$. For each $1 \leq j \leq k$,

$$\psi(x/2^{j-1}) - \psi(x/2^j) \leq \frac{x}{2^{j-1}}\log 2 + O\left(\log\frac{x}{2^{j-1}}\right) = \frac{x}{2^{j-1}}\log 2 + O(\log x).$$

Summing these inequalities for $1 \leq j \leq k$, we have (noting that $k \ll \log x$)

$$\begin{aligned}\psi(x) - \psi(x/2^k) &\leq x\log 2\left(1 + \frac{1}{2} + \cdots + \frac{1}{2^{k-1}}\right) + O((\log x)(\log x)),\\ &\leq 2x\log 2 + O((\log x)^2).\end{aligned}$$

Thus,

$$\psi(x) \leq 2x\log 2 + O((\log x)^2) + \psi(4) \leq 2x\log 2 + O((\log x)^2). \tag{3.12}$$

Collecting our upper and lower bounds on $\psi(x)$, we have proved:

Proposition 3.13. *For $x \geq 4$, we have*

$$x\log 2 + O(\log x) \leq \psi(x) \leq 2x\log 2 + O((\log x)^2). \tag{3.13}$$

From Propositions 3.7 and 3.13, we obtain Theorem 3.5 for any constants c_1 and c_2 satisfying $c_1 < \log 2$ and $c_2 > 2\log 2$. Since $\frac{2\log 2}{\log 2} = 2$, this has the following corollary: For each fixed $\epsilon > 0$, there is a prime in the interval $[x, (2+\epsilon)x]$ for all $x > x_0(\epsilon)$. Said differently, we are an ϵ away from a proof of Bertrand's postulate!

3.3. Proof of Bertrand's postulate. Obviously, if we can produce a nonvanishing sum over the primes $p \in (x, 2x]$, then there must be a prime in $(x, 2x]$. In particular, Bertrand's postulate will follow if we show that

$$\theta(2x) - \theta(x) = \sum_{x<p\leq 2x} \log p > 0$$

for large enough x. We will establish this by first estimating $\psi(2x) - \psi(x)$ from below, and then using (3.4) to translate that estimate into a lower bound on $\theta(2x) - \theta(x)$.

Here one's first instinct is perhaps to take $k = 2$ in (3.10), as this immediately gives us a bound on $\psi(x) - \psi(x/2)$, namely

$$\psi(x) - \psi(x/2) \leq T(x) - 2T(x/2).$$

Unfortunately, the inequality is going the wrong way for our purposes. So instead we take $k = 3$ in (3.11); this gives us that

$$\psi(x) - \psi(x/2) + \psi(x/3) \geq T(x) - 2T(x/2) = x\log 2 + O(\log x). \tag{3.14}$$

This inequality is going the right way but has the extra term $\psi(x/3)$. However, from (3.12),

$$\psi(x/3) \le \frac{2\log 2}{3}x + O((\log x)^2),$$

which in conjunction with (3.14) implies that

$$\psi(x) - \psi(x/2) \ge x\frac{\log 2}{3} + O((\log x)^2).$$

Invoking (3.4), we obtain the lower bound

$$\theta(x) - \theta(x/2) \ge x\frac{\log 2}{3} + O(x^{1/2}\log x) \qquad (x \to \infty). \tag{3.15}$$

Theorem 3.6 is now immediate, since the right-hand side of (3.15) is positive for large x.

In fact, (3.15) yields a lower bound for $\pi(x) - \pi(x/2)$ of the same order of magnitude as the lower bound for $\pi(x)$ in Theorem 3.5. Indeed,

$$\theta(x) - \theta(x/2) = \sum_{x/2<p\le x} \log p \le \log x\,(\pi(x) - \pi(x/2))\,,$$

so that by (3.15),

$$\pi(x) - \pi(x/2) \ge \frac{\log 2}{3}\frac{x}{\log x} + O(x^{1/2}) = \left(\frac{\log 2}{3} + o(1)\right)\frac{x}{\log x} \quad (x \to \infty). \tag{3.16}$$

This proof of Bertrand's postulate is due to Ramanujan [**Ram19**].

4. The work of Mertens

By 1737, Euler was aware not only of the divergence of $\sum_p p^{-1}$, but had assigned the infinite sum the value $\log\log\infty$ [**Eul37**, Theorema 19], showing that he possessed an inkling as to the rate of growth of the partial sums. In Gauss's Nachlass [**Gau73c**, pp. 11-16] one can find the more precise assertion that

$$\text{“}1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots + \frac{1}{x} = (\text{for } x \text{ infinite})\ llx + V.\text{”}$$

Gauss writes that he suspects V to be a constant near 1.266. It seems reasonable to read this as the conjecture that

$$\sum_{p\le x}\frac{1}{p} = \log\log x + V - 1 + o(1).$$

Gauss also claims that

$$\text{“}\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{5}{4}\cdots\frac{x}{x-1} = (x \text{ inf})\ a.lx\text{”}$$

for a constant $a \approx 1.874$, which we can read as the conjecture that

$$\prod_{p \le x} (1 - 1/p)^{-1} \sim a \log x.$$

Mertens observed [**Mer74**] that Chebyshev's results could be used to obtain precise estimates for both $\sum_{p \le x} 1/p$ and $\prod_{p \le x}(1 - 1/p)$. His results vindicate Gauss's claims, apart from small inaccuracies in the numerical values of the constants; the correct values are $V = 1.2614972\dots$ and $a = 1.7810724\dots$.

4.1. Mertens' first theorem. We begin by considering the weighted sum $A(x) := \sum_{p \le x} \log p/p$. From estimates for $A(x)$, results on $\sum_{p \le x} 1/p$ follow by partial summation, and these in turn easily yield theorems about $\prod_{p \le x}(1 - 1/p)$.

Observe that the function $T(x)$ introduced in §3 can be written in the form

$$T(x) = \sum_{n \le x} \log n = \sum_{n \le x} \sum_{d \mid n} \Lambda(d) = \sum_{d \le x} \sum_{\substack{n \le x \\ d \mid n}} \Lambda(d) = \sum_{d \le x} \Lambda(d) \left\lfloor \frac{x}{d} \right\rfloor.$$

If we drop the greatest integer sign, then the error incurred in the sum is $\ll \sum_{d \le x} \Lambda(d) = \psi(x) \ll x$ by (3.13). Now substituting in the estimate $T(x) = x \log x + O(x)$ furnished by Lemma 3.10 and dividing by x, we are led to the important result that

$$\sum_{d \le x} \frac{\Lambda(d)}{d} = \log x + O(1). \tag{3.17}$$

Observe that

$$\sum_{d \le x} \frac{\Lambda(d)}{d} = \sum_{p^k \le x} \frac{\log p}{p^k}. \tag{3.18}$$

So if it were not for the terms corresponding to prime powers p^k with $k \ge 2$, then (3.17) would be an estimate for $A(x)$. But these nuisance terms contribute a bounded amount:

$$\begin{aligned} \sum_{\substack{p^k \le x \\ k \ge 2}} \frac{\log p}{p^k} &\le \sum_{p \le x} \log p \sum_{k=2}^{\infty} p^{-k} \\ &= \sum_{p \le x} \frac{\log p}{p(p-1)} \le \sum_{2 \le n \le x} \frac{\log n}{n(n-1)} = O(1). \end{aligned} \tag{3.19}$$

Combining (3.17), (3.18) and (3.19), we obtain that (for $x \ge 1$)

$$A(x) = \sum_{p \le x} \frac{\log p}{p} = \log x + O(1). \tag{3.20}$$

Theorem 3.14 (Mertens' first theorem)**.** *As $x \to \infty$, we have $\sum_{p\le x} p^{-1} = \log\log x + B_1 + O(1/\log x)$ for a constant B_1. Here $B_1 = 1 - \log\log 2 + \int_2^\infty (A(t) - \log t)/(t(\log t)^2)\, dt$.*

Proof. By partial summation,

$$\sum_{p\le x} \frac{1}{p} = \sum_{p\le x} \frac{\log p}{p} \frac{1}{\log p} = \frac{A(x)}{\log x} + \int_2^x \frac{A(t)}{t(\log t)^2}\, dt.$$

From (3.20) we have that $A(x)/\log x = 1 + O(1/\log x)$. To estimate the integral, we write $A(t) = \log t + (A(t) - \log t)$, so that

$$\begin{aligned}\int_2^x \frac{A(t)}{t(\log t)^2}\, dt &= \int_2^x \frac{1}{t\log t}\, dt + \int_2^x \frac{A(t)-\log t}{t(\log t)^2}\, dt\\ &= \log\log x - \log\log 2 + \int_2^x \frac{A(t)-\log t}{t(\log t)^2}\, dt.\end{aligned}$$

Since $A(t) - \log t$ is bounded, the integral $I := \int_2^\infty \frac{A(t)-\log t}{t(\log t)^2}\, dt$ converges absolutely. Moreover,

$$I - \int_2^x \frac{A(t)-\log t}{t(\log t)^2}\, dt \ll \int_x^\infty \frac{dt}{t(\log t)^2} = \frac{1}{\log x}.$$

Piecing everything together yields the theorem. $\square$

4.2. Mertens' second theorem. The second theorem of Mertens, which is usually the result intended when one sees references to *Mertens' theorem* in the literature, governs the behavior of the product $\prod_{p\le x}(1 - 1/p)$.

Theorem 3.15. *There is an absolute constant C for which $\prod_{p\le x}(1-1/p) = e^{-C}/\log x + O(1/(\log x)^2)$ as $x \to \infty$. Explicitly, $C = B_1 + B_2$, where B_1 is the constant of Theorem 3.14 and $B_2 := \sum_p \sum_{k=2}^\infty (kp^k)^{-1}$.*

Proof. Let $P_x := \prod_{p\le x}(1 - 1/p)$. Since $\log(1 - 1/p) = -\sum_{k\ge 1}(kp^k)^{-1}$,

$$\log P_x = -\sum_{p\le x} \frac{1}{p} - \sum_{p\le x}\sum_{k=2}^\infty \frac{1}{kp^k}.$$

Since

$$\sum_{k=2}^\infty \frac{1}{kp^k} \le \frac{1}{2}\sum_{k=2}^\infty \frac{1}{p^k} = \frac{1}{2p(p-1)} \le \frac{1}{p^2},$$

the infinite sum $\sum_p \sum_{k=2}^\infty (kp^k)^{-1}$ converges absolutely, to B_2, say. Moreover, $B_2 - \sum_{p\le x}\sum_{k=2}^\infty (kp^k)^{-1} \le \sum_{p>x} p^{-2} \ll x^{-1}$. Hence

$$\begin{aligned}\log P_x &= -\log\log x - B_1 + O(1/\log x) - B_2 + O(1/x)\\ &= -\log\log x - B_1 - B_2 + O(1/\log x).\end{aligned}$$

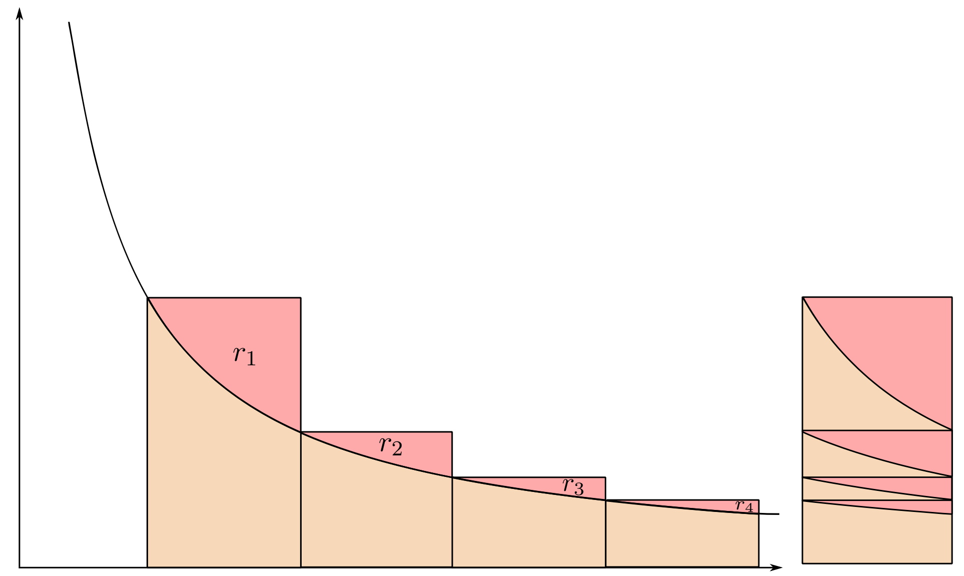

Figure 1.

Exponentiating, we find that

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right)=\frac{\exp(-(B_1+B_2))}{\log x}\exp(O(1/\log x)),$$

and the result follows with $C=B_1+B_2$. $\square$

In the remainder of this section we show that the constant C of Theorem 3.15 admits a much more pleasant description.

Lemma 3.16 (Euler). *For $x\geq 1$, we have $\sum_{n\leq x} n^{-1}=\log x+\gamma+O(1/x)$, where γ is an absolute constant.*

The constant $\gamma = 0.57721566490153286061\ldots$ is known as the *Euler–Mascheroni constant.*

Proof. Let $r_n = n^{-1}-\int_n^{n+1} t^{-1}\,dt$. Then r_n is the area of that part of the rectangle $[n, n+1]\times[0, 1/n]$ that lies above the graph of $y=1/x$. From Figure 1 it is clear that $\sum_{n\geq 1} r_n$ converges to a number γ less than 1. For each natural number N, we have

$$\sum_{n\leq N} r_n=\sum_{n\leq N}\frac{1}{n}-\int_1^{N+1}\frac{dt}{t}.$$

Thus

$$\sum_{n\le N}\frac{1}{n}=\int_1^{N+1}\frac{dt}{t}+\sum_{n\le N}r_n$$
$$=\log(N+1)+\gamma-\sum_{n=N+1}^{\infty}r_n.$$

From Figure 1 it is clear that $\sum_{n=N+1}^{\infty} r_n \le (N+1)^{-1}$. So, taking $N=\lfloor x\rfloor$, we deduce that for $x\ge 1$, we have $\sum_{n\le x} n^{-1}=\log(\lfloor x\rfloor+1)+\gamma+O(1/x)$. Since $\log(\lfloor x\rfloor+1)=\log x+O(1/x)$ for $x\ge 1$, the lemma follows. □

Theorem 3.17. *In the notation of Theorems 3.14 and 3.15, we have* $C = B_1+B_2=\gamma$, *where* γ *is the Euler–Mascheroni constant.*

Proof. For real $s>1$, we let $\zeta(s)=\sum_{n=1}^{\infty} n^{-s}$ be the Euler–Riemann zeta function (introduced in Chapter 1, §4) and we let $Z(s):=\sum_p p^{-s}$. Put $F(s):=\log\zeta(s)-Z(s)$. Since $\zeta(s)=\prod_p(1-p^{-s})^{-1}$, a short calculation shows that $F(s)=\sum'_{k,p}(kp^{ks})^{-1}$, where the $'$ indicates that the sum is over primes p and integers $k\ge 2$. This series for $F(s)$ converges uniformly on each compact subset of $(1/2,\infty)$, and so $F(s)\to\sum'(kp^k)^{-1}=B_2$ as $s\downarrow 1$.

We now derive an alternative representation for $F(s)$ which will make visible that $F(s)\to\gamma-B_1$ as $s\downarrow 1$, thus proving that $\gamma=B_1+B_2$. We start by noting that since t^{-s} is decreasing for $t>0$ (for each fixed $s>1$),

$$\frac{1}{s-1}=\int_1^{\infty}t^{-s}\,dt\le\zeta(s)\le 1+\int_1^{\infty}t^{-s}\,dt=1+\frac{1}{s-1},$$

so that $0\le\zeta(s)-(s-1)^{-1}\le 1$. Hence $\log\zeta(s)=\log((s-1)^{-1})+O(s-1)$. Since $1-e^{-(s-1)}=(s-1)(1+O(s-1))$, it follows that $\log(1-e^{-(s-1)})=\log(s-1)+O(s-1)$, and so

$$\log\zeta(s)=-\log(1-e^{-(s-1)})+O(s-1)$$
$$=\sum_{n=1}^{\infty}e^{-(s-1)n}n^{-1}+O(s-1). \tag{3.21}$$

With $H(x):=\sum_{n\le x}n^{-1}$, the sum in (3.21) is $\int_0^{\infty}e^{-(s-1)t}\,dH(t)$, which (after a short calculation) shows that

$$\log\zeta(s)=(s-1)\int_0^{\infty}H(t)e^{-(s-1)t}\,dt+O(s-1).$$

Let $P(x):=\sum_{p\le x}p^{-1}$. Another application of partial summation shows that

$$Z(s)=(s-1)\int_1^{\infty}t^{-s}P(t)\,dt=(s-1)\int_0^{\infty}e^{-(s-1)t}P(e^t)\,dt.$$

Theorem 3.14 implies that $P(e^t) = \log t + B_1 + O((t+1)^{-1})$ for $t \geq 0$ and Theorem 3.16 gives us that $H(t) = \log t + \gamma + O((t+1)^{-1})$ for $t \geq 1$. So

$$\begin{aligned} F(s) &= \log \zeta(s) - Z(s) \\ &= (s-1) \int_0^\infty e^{-(s-1)t} (H(t) - P(e^t))\, dt + O(s-1) \\ &= (s-1) \int_0^\infty e^{-(s-1)t} \left(\gamma - B_1 + O\left(\frac{1}{t+1} \right) \right) dt + O(s-1). \end{aligned}$$

Here the main term is

$$(s-1) \int_0^\infty e^{-(s-1)t} (\gamma - B_1)\, dt = \gamma - B_1$$

and the error term is

$$\ll (s-1) + (s-1) \int_0^\infty \frac{e^{-(s-1)t}}{t+1}\, dt.$$

Splitting this last integral at $t = (s-1)^{-1}$, we find that

$$\begin{aligned} &(s-1) \int_0^\infty \frac{e^{-(s-1)t}}{t+1}\, dt \\ &\quad \leq (s-1) \int_0^{(s-1)^{-1}} \frac{dt}{t+1} + \frac{s-1}{s} \int_{(s-1)^{-1}}^\infty (s-1) e^{-(s-1)t}\, dt \\ &\qquad = (s-1) \log \frac{s}{s-1} + \frac{s-1}{s} e^{-1}. \end{aligned}$$

It follows that as $s \downarrow 1$, the above error term tends to zero, and so $F(s) \to \gamma - B_1$ as desired. □

5. Primes and probability

> In response to the theory of quantum mechanics, Einstein exclaimed, "God does not play dice with the universe." Though this never happened, I would like to think that Paul Erdős and the great probabilist, Mark Kac, replied, "Maybe so, but something is going on with the primes." – C. Pomerance [**Pom98**]

In §1 we discussed how Gauss was led to the prime number theorem by observing that the "local density" of primes near is x is approximately $1/\log x$. This observation can be used to support many additional statements about primes, the majority of which seem to lie very deep.

We can get a feeling for the reasoning involved in these heuristic arguments by considering a quantitative version of a problem discussed qualitatively in Chapter 1. Suppose that $a \bmod m$ is a (fixed) coprime residue class: How many primes $p \leq x$ are there with $p \equiv a \pmod{m}$? Denote the answer to this question by $\pi(x; m, a)$. In Chapter 1 we mentioned the theorem of Dirichlet that there are always infinitely many such primes, i.e., that $\pi(x; m, a) \to \infty$. Now we would like to know how quickly $\pi(x; m, a)$ tends to infinity.

The numbers not exceeding x from the residue class a mod m have the form $a + mr$, where $r \lessapprox x/m$. The Gauss philosophy says that a number chosen at random near $a + mr$ should be prime with probability about $1/\log(a + mr)$. So, parroting our reasoning in §1, we might conjecture that $\pi(x; m, a) \approx \int_1^{x/m} dt/\log(a + mt)$. But this *cannot* be correct: It is easy to check (e.g., using L'Hôpital's rule) that the integral here is asymptotic to $\mathrm{Li}(x)/m$. But there are only $\varphi(m)$ coprime residue classes modulo m, so if our guess is correct, then summing over the coprime residue classes modulo m accounts for only $\sim (\varphi(m)/m)\mathrm{Li}(x)$ primes $p \leq x$. Since $\varphi(m)/m < 1$ when $m > 1$, this contradicts the prime number theorem.

Where did we go wrong? The answer is in our pretending that $a + mr$ is a typical number of its size. Suppose p is prime. Loosely speaking, the probability that a number near $a + mr$ is a multiple of p is $1/p$. What is the probability that $a + mr$ itself is a multiple of p? If p does not divide m, then the congruence $a + mr \equiv 0 \pmod{p}$ has exactly one solution r modulo p, and so again this probability is $1/p$. But if p does divide m, then p never divides a number of the form $a + mr$, and so $a + mr$ has a leg up on being prime over its neighbors.

To account for this we introduce a correction factor c_p for each prime p, defined as a ratio of two probabilities: In the numerator of c_p we put the probability that $a + mr$ is not divisible by p, and in the denominator we put the probability that a typical number near $a + mr$ is not divisible by p. Then $c_p = 1$ for primes p not dividing m, while $c_p = (1 - 1/p)^{-1}$ when p does divide m. Each c_p measures the leg up that a number of the form $a + mr$ has over its neighbors, as seen from the perspective of p. The Chinese remainder theorem suggests that these effects modulo p should be treated as independent, which in turns suggests that our earlier guesstimate for $\pi(x; m, a)$ should be multiplied by a factor of $\prod_p c_p = m/\varphi(m)$. This leads to the new prediction that when $\gcd(a, m) = 1$, we have

$$\pi(x; m, a) \sim \frac{1}{\varphi(m)}\mathrm{Li}(x) \qquad (x \to \infty).$$

Unlike our former guess, this is no longer obviously false, and in fact it can be proved correct by the same methods used to establish the prime number theorem. It is known as the *prime number theorem for arithmetic progressions.*

Table 3. Comparison of $\pi_2(x)$ and $L_2(x) := 2C_2 \int_2^x \frac{dt}{(\log t)^2}$. The last column gives the percentage error, computed as $|L_2(x) - \pi_2(x)|/\pi_2(x)$.

x	$\pi_2(x)$	$L_2(x) - \pi_2(x)$	% error
10^5	1,224	25	2.0 %
10^6	8,169	79	9.7×10^{-1}%
10^7	58,980	-226	3.8×10^{-1}%
10^8	440,312	56	1.3×10^{-2}%
10^9	3,424,506	802	2.3×10^{-2}%
10^{10}	27,412,679	-1,262	4.6×10^{-3}%
10^{11}	224,376,048	-7,183	3.2×10^{-3}%
10^{12}	1,870,585,220	-25,353	1.4×10^{-3}%
10^{13}	15,834,664,872	-66,567	4.2×10^{-4}%
10^{14}	135,780,321,665	-56,771	4.2×10^{-5}%
10^{15}	1,177,209,242,304	-750,443	6.4×10^{-5}%

Let's try something harder: How many $n \leq x$ are there for which both n and $n+2$ are prime? This quantity is traditionally denoted $\pi_2(x)$. The Gauss philosophy suggests that a random pair of integers "near n" should be simultaneously prime with probability about $1/(\log n)^2$. But n and $n+2$ do not form a typical pair of integers "near n". Indeed, let p be a prime number. The probability that neither element of a pair of random numbers near n is divisible by p is $(1-1/p)^2$. But the probability that neither n nor $n+2$ is divisible by p is $(1-\nu(p)/p)$, where

$$\nu(p) := \#\{n \bmod p : n(n+2) \equiv 0 \pmod{p}\}.$$

For each prime p, put $c_p := (1-\nu(p)/p)(1-1/p)^{-2}$. Then we might expect that $\pi_2(x) \approx \left(\prod_p c_p\right) \int_2^x \frac{dt}{(\log t)^2}$. Noting that $\nu(p) = 1$ if $p = 2$ and $\nu(p) = 2$ if $p > 2$, this conjecture becomes:

Conjecture 3.18 (Twin prime conjecture, quantitative form)**.** *As $x \to \infty$, we have $\pi_2(x) \sim 2C_2 \int_2^x \frac{dt}{(\log t)^2}$, where $C_2 := \prod_{p>2}\left(1-(p-1)^{-2}\right)$.*

The constant C_2 is called the *twin prime constant*. The numerical evidence for Conjecture 3.18 is very persuasive; see Table 3.

As discussed in Chapter 1, the twin prime conjecture can be viewed as a special case of Schinzel's Hypothesis H. We can now formulate a quantitative version of that general conjecture. Suppose that $F_1(T), \ldots, F_r(T) \in \mathbf{Z}[T]$ are r distinct polynomials with integer coefficients, that each $F_i(T)$ has a positive leading coefficient, that each is irreducible over $\mathbf{Z}$, and that

(3.22) there is no prime p dividing $F_1(n) \cdots F_r(n)$ for every $n \in \mathbf{Z}$.

Let d_i denote the degree of F_i. Then $\log|F_i(n)|$ is asymptotic to $d_i \log|n|$ as $n \to \infty$. Our heuristic suggests that

$$\pi_{F_1,\dots,F_r}(x) := \#\{n \le x : F_1(n),\dots,F_r(n) \text{ are simultaneously prime}\}$$

should be asymptotic to

$$C(F_1,\dots,F_r)\frac{1}{d_1\cdots d_r}\int_2^x \frac{dt}{(\log t)^r},$$

where

$$C(F_1,\dots,F_r) := \prod_p \frac{1-\nu(p)/p}{(1-1/p)^r} \tag{3.23}$$

and

$$\nu(p) := \#\{n \bmod p : F_1(n)\cdots F_r(n) \equiv 0 \pmod{p}\}.$$

Notice that the condition (3.22) amounts to the assertion that $\nu(p) < p$ for every prime p.

It is worth taking a step back to see if this conjecture makes sense. Does the infinite product (3.23) even converge? This is not at all obvious, even in the simple case when $r = 1$. Nevertheless, as shown by Bateman & Horn [**BH62**], this is true: The product (3.23) always converges; in fact it always converges to a positive real number. The proof uses some elementary results of Landau on the distribution of prime ideals in algebraic number fields (cf. [**DH09**]). The positivity of the constant $C(F_1,\dots,F_r)$ means that this quantitative formulation of Hypothesis H really does imply the qualitative formulation of Chapter 1.

The basic argument of this section has many other applications. We close this section with two examples that do not fall under the rubric of Hypothesis H.

For a positive integer N, let $R(N)$ be the number of (ordered) pairs of primes p and q for which $p+q=N$. A well-known conjecture of Goldbach asserts that $R(N) > 0$ whenever $N > 2$ is even. The methods of this section suggest much more:

Conjecture 3.19 (Goldbach conjecture, quantitative form)**.** *As $N \to \infty$ through even numbers, we have*

$$R(N) \sim 2C_2\left(\prod_{p\mid N, p>2}\frac{p-1}{p-2}\right)\int_2^N \frac{dt}{(\log t)^2}.$$

Here C_2 is the twin prime constant.

We leave the task of justifying this conjecture as Exercise 4.

For our last example we consider the distribution of Mersenne primes, i.e., primes of the form 2^p-1. A number near 2^p-1 is prime with probability roughly $1/\log(2^p-1) \approx 1/(p\log 2)$. But 2^p-1 is atypical in that we can rule out small prime divisors in advance: If q is a prime divisor of 2^p-1, then 2 has order p modulo q, which implies that $q \equiv 1 \pmod{p}$. In particular, every prime divisor of 2^p-1 is at least p.

Let us make the working assumption that this is the only relevant difference between 2^p-1 and a number typical for its size. Since a typical integer is divisible by a prime q with probability $1/q$, this suggests that we multiply our former probability $1/(p\log 2)$ by $\prod_{q\le p}(1-1/q)^{-1}$. By Mertens' theorem, $\prod_{q\le p}(1-1/q)^{-1} \sim e^\gamma \log p$ (as $p\to\infty$). This suggests that among the primes $p\le x$, we should expect

$$\approx \sum_{p\le x} e^\gamma \frac{\log p}{p\log 2} = \frac{e^\gamma}{\log 2}\sum_{p\le x}\frac{\log p}{p} \sim \frac{e^\gamma}{\log 2}\log x$$

for which 2^p-1 is also prime. (Here we have used (3.20) to estimate the last sum.) So we arrive at the following prediction:

Conjecture 3.20. *There are infinitely many primes p for which 2^p-1 is prime. In fact, the number of such $p\le x$ is asymptotic to $c\log x$ where $c = e^\gamma/\log 2$ and γ is the Euler–Mascheroni constant.*

Notes

The discussion in §1 of Gauss's discovery of the prime number theorem is based on [**LeV96**]. With all due respect to Gauss's ingenuity and industriousness, it must be admitted that Gauss's observations do not provide any explanation for the truth of the prime number theorem. A candidate for such an explanation was proposed by Hawkins [**Haw58**].

To explain Hawkins's idea, we first recall the classical sieve of Eratosthenes for obtaining a list of the prime numbers: Begin with the sequence $2, 3, 4, 5, \dots$ of natural numbers $n > 1$. Circle the first uncircled number m on the list. Now remove from the list every $n > m$ which is divisible by m. If this process is repeated indefinitely, the sequence of circled numbers coincides with the set of primes.

Suppose, following Hawkins, that the deterministic removal step above is replaced with the following random step: Instead of removing each $n > m$ which is divisible by m, remove each $n > m$ with probability $1/m$. That is, for each $n > m$, roll an m-sided die (with faces labeled "1" thru "m"), and remove the number n if the toss comes up "1" and keep the number n otherwise. In this case, indefinite repetition results in a random sequence $\mathscr{P}$. Let $\pi_{\mathscr{P}}(x)$ be the number of terms of $\mathscr{P}$ not exceeding x. The following remarkable theorem was conjectured by Hawkins ([**Haw74**], but see already [**Erd65**, p. 213]) and proved by Wunderlich [**Wun75**]:

Table 4. Comparison of $\pi(x)$ and $E(x) := \mathrm{Li}(x) - \pi(x)$ along powers of 10, from $x = 10^{14}$ through $x = 10^{23}$. $E(x)$ is shown rounded to the nearest integer.

x	$\pi(x)$	$E(x)$
10^{14}	3,204,941,750,802	314,891
10^{15}	29,844,570,422,669	1,052,617
10^{16}	279,238,341,033,925	3,214,631
10^{17}	2,623,557,157,654,233	7,956,588
10^{18}	24,739,954,287,740,860	21,949,554
10^{19}	234,057,667,276,344,607	99,877,774
10^{20}	2,220,819,602,560,918,840	222,744,643
10^{21}	21,127,269,486,018,731,928	597,394,253
10^{22}	201,467,286,689,315,906,290	1,932,355,207
10^{23}	1,925,320,391,606,803,968,923	7,250,186,215

★ **Theorem 3.21.** *With probability* 1*, we have* $\pi_{\mathscr{P}}(x) \sim x/\log x$ *as* $x \to \infty$*.*

Informally, this result says that Eratosthenes-like sieves tend to produce sequences which satisfy the conclusion of the prime number theorem — so maybe it should not come as a shock that the sequence actually produced by the sieve of Eratosthenes has this property. A story with a similar moral is told in [**GLMU56, HB58**].

If we take a careful look at Table 2, we are led to wonder whether the prime number theorem is not too modest an assertion. Put

$$E(x) := \mathrm{Li}(x) - \pi(x).$$

The prime number theorem asserts that $E(x) = o(\pi(x))$, while the data in Table 2 suggests that $E(x)$ is actually of a much smaller order of magnitude than x. In Table 4 we extend the comparison of $\pi(x)$ and $\mathrm{Li}(x)$ up to 10^{23}. Inspecting this table, we find that the numbers in the third column are only about half the length of those in the second, which suggests that perhaps $|E(x)| \lessapprox \sqrt{\pi(x)}$. While nothing of this sort can yet be proved, this behavior is not unexpected: It has been known since Riemann that the size of $E(x)$ is intimately connected with the location of the zeros of $\zeta(s)$. The so-called *Riemann Hypothesis* asserts that all the nonreal zeros of $\zeta(s)$ lie on the line $\Re(s) = 1/2$. As shown by von Koch [**Koc01**] in 1901, the Riemann Hypothesis is equivalent to the bound

$$E(x) = O(\sqrt{x}\log x).$$

Unfortunately, we still cannot even prove that $E(x) = O(x^{1-\epsilon})$ for a fixed positive value of ϵ. The best-known result is (in somewhat rough form) that for each fixed $\alpha < 3/5$, there is a constant $C_\alpha > 0$ with

$$E(x) \ll x \exp(-C_\alpha (\log x)^\alpha). \tag{3.24}$$

That this is the state-of-the-art reflects an embarrassing lack of twentieth century progress, since the result (3.24) with $\alpha = 1/2$ was established by de la Vallée-Poussin [**VP99**] already in 1899.

In the opposite direction, it is known that von Koch's conditional bound on $E(x)$, if correct, is close to best possible:

★ **Theorem 3.22** (Littlewood [**Lit14**]). *There are constants $c^- < 0 < c^+$ for which the following holds: There is a sequence of x tending to infinity along which*

$$E(x) > c^+ x^{1/2} \log\log\log x/\log x$$

and a sequence of x tending to infinity along which

$$E(x) < c^- x^{1/2} \log\log\log x/\log x.$$

Littlewood's theorem is usually quoted in connection with one of its more surprising consequences, namely that $E(x)$ changes sign infinitely often. (Tables 2 and 4 might lead one to the contrary conjecture that $E(x) \to \infty$ as $x \to \infty$.)

Our proofs of the theorems of Chebyshev and Mertens incorporate a number of later simplifications. For a discussion of these authors' original methods, one should consult the beautiful monograph of Narkiewicz [**Nar04**], in particular, Chapter 3. This monograph is the source of much of the historical content throughout this book.

The quantitative forms of the twin prime and Goldbach conjectures which we discussed in §5 are due to Hardy & Littlewood [**HL23**]. Their approach was considerably more complicated than ours; the realization that conjectures of this type could be derived from the "Gauss philosophy" on the local density of primes appears to be due to Selmer [**Sel42**] (see also [**Gol60**]). Bateman & Horn [**BH62**] were the first to suggest, in full generality, the quantitative form of Hypothesis H discussed in §5. Conjecture 3.20 was suggested independently by Pomerance, Selfridge and Wagstaff (see, e.g., [**Wag83**]).

Exercises

1. Let A be a set of natural numbers and let $A(x) := \#\{a \le x : a \in A\}$. Show that if $\sum_{a\in A} a^{-1}$ converges, then A has asymptotic density zero.

† 2. (Golomb [**Gol62**])
   (a) Show that for each integer $k > 1$, there is at least one natural number n for which $n/\pi(n) = k$.
   (b) Show that the set of n for which $\pi(n)$ divides n has asymptotic density zero. (Cf. [**EP90**].)

3. Should one expect that there are infinitely many primes of the form $n! + 1$? What about $p! + 1$, where p itself is prime?

4. Provide a convincing argument suggesting the truth of Conjecture 3.19.

5. Using only the divergence of $\sum_p p^{-1}$, show that $\limsup_{x\to\infty} \frac{\pi(x)}{x/(\log x)^{1+\epsilon}}$ is infinite for each fixed $\epsilon > 0$.

6. (a) Suppose $\{a_n\}_{n\ge 1}$ and $\{b_n\}_{n\ge 1}$ are sequences of real numbers where $a_n \to \infty$ and $a_n \sim b_n$ as $n \to \infty$. Show that $a_n \log a_n \sim b_n \log b_n$ as $n \to \infty$.
   (b) Write p_n for the nth prime number. Taking $a_n := p_n/\log p_n$ and $b_n := n$, deduce from the prime number theorem that $p_n \sim n \log n$ as $n \to \infty$.

7. (Continuation) Prove that $p_{n+1}/p_n \to 1$ as $n \to \infty$. Show also that $\{p/q : p, q \text{ prime}\}$ is a dense subset of $(0, \infty)$.

8. Show that if m is a fixed natural number, then $\mathrm{Li}(x)$ may be estimated as
$$\frac{x}{\log x} + \frac{x}{(\log x)^2} + \frac{2x}{(\log x)^3} + \cdots + \frac{(m-1)!x}{(\log x)^m} + O_m\left(\frac{x}{(\log x)^{m+1}}\right).$$
Assuming (3.24), show that the same expansion is valid for $\pi(x)$ replacing $\mathrm{Li}(x)$.

9. (Landau [**Lan01**]) Let $\pi'(x)$ be the number of primes in the interval $(x, 2x]$. Assuming the prime number theorem, show that $\pi'(x) \sim \pi(x)$ as $x \to \infty$. Assuming (3.24), show that $\pi(x) > \pi'(x)$ for large x, and that in fact $\pi(x) - \pi'(x) \to \infty$ as $x \to \infty$.

   Remark. It is tempting to conjecture, as Hardy & Littlewood did in 1923 (see [**HL23**]), that the interval $(0, x]$ always contains at least as many primes as the interval $(y, x + y]$ whenever $x, y \ge 2$. However, this is probably false; Hensley & Richards [**HR73**] have shown that it contradicts the *prime k-tuples conjecture*, which is a special case of Schinzel's Hypothesis H.

10. (see Sierpiński [**Sie59**]) Using the prime number theorem for arithmetic progressions, show that there are infinitely many primes whose base 26 expansion has the form $\texttt{PROPERTYOF}\cdots\textit{other digits here}\cdots\texttt{EULER}$ (where with $A = 0$, $B = 1$, …, $Z = 25$).

11. (Gelfond & Schnirelmann [**Gel46**]; cf. [**Mon94**, Chapter 10]) Show that for each natural number N,

$$\operatorname{lcm}[1, 2, \ldots, N] = \exp(\psi(N)).$$

Deduce that the expression

$$e^{\psi(2N+1)} \int_0^1 x^N (1-x)^N \, dx$$

represents a positive integer, and use this to give another proof that $\psi(x) \geq x \log 2 + O(\log x)$ as $x \to \infty$.

12. (Brun [**Bru17**]) For $x \geq 2$, let $N = N(x)$ be the number of natural numbers $n \leq x$ divisible by some prime $p \in (\sqrt{x}, x]$.
    (a) Noting that each natural number $n \leq x$ can be divisible by at most one prime $p \in (\sqrt{x}, x]$, show that $N \geq \sum_{\sqrt{x}<p\leq x} \lfloor x/p \rfloor$.
    (b) Deduce from the trivial bound $N \leq x$ that $\sum_{\sqrt{x}<p\leq x} 1/p \leq 2$.
    (c) Use the result of (b) to give another proof that $\sum_{p\leq x} p^{-1} \ll \log\log x$ as $x \to \infty$.

13. In this exercise and the next we establish Bertrand's postulate in its full strength: *For every positive integer n, there is a prime p with $n < p \leq 2n$.* The proof described here is a hybrid of Ramanujan's argument (described in §3.3) and an argument of Erdős [**Erd32**], and can be found in [**Sha83**, §9.3C].
    (a) Check that $\prod_{n+1<p\leq 2n+1} p \mid \binom{2n+1}{n+1}$ for every integer $n \geq 0$.
    (b) Prove that $\binom{2n+1}{n+1} \leq 4^n$ for each integer $n \geq 0$.
    (c) Use (a) and (b) to fashion an inductive proof that $\prod_{p\leq N} p \leq 4^N$ for all nonnegative integers N. Thus $\theta(x) \leq 2x\log 2$ for all $x \geq 0$.
    (d) Check that $\binom{2n+1}{n+1}$ is divisible by every prime $p \leq n+1$ which possesses a power belonging to the interval $(n+1, 2n+1]$. Use this to show that $\exp(\psi(N)) \leq 4^N$ for every natural number $N \geq 0$. Thus $\psi(x) \leq 2x\log 2$ for every $x \geq 0$.

    Remark. The argument of (a)–(c) is due to Erdős & Kalmár (see [**Erd89**]). Erdős's 1932 paper had a more complicated proof of a slightly weaker bound for $\theta(x)$.

14. (Continuation) Recall that for each $x \geq 0$, we have

$$T(x) - 2T(x/2) \leq \psi(x) - \psi(x/2) + \psi(x/3). \tag{3.25}$$

(a) Show that if n is a nonnegative integer, then $\binom{2n}{n} \geq 4^n/(2n+1)$. *Hint:* What does the $2n$th row of Pascal's triangle look like?

(b) Show that

$$\sum_{\substack{n<p^k \leq 2n \\ k \geq 2}} \log p \leq \sqrt{2n} \log \sqrt{2n}.$$

(c) Deduce from (3.25) (with $x = 2n$) and (d) of the last exercise that

$$\theta(2n) - \theta(n) \geq \frac{1}{3} n \log 4 - \log(2n+1) - \sqrt{2n} \log \sqrt{2n}.$$

(d) Conclude from (c) that there is always a prime in the interval $(n, 2n]$ whenever $n \geq 82$.

(e) The primes $2, 3, 5, 7, 13, 23, 43, 83$ form a sequence with each less than twice the next. Use this to argue that there is always a prime in the interval $(n, 2n]$ for $n < 82$ as well.

† 15. (Richert [**Ric49**]) Using the full form of Bertrand's postulate, show that every integer $n > 6$ can be written as a sum of distinct prime numbers. *Hint:* Start by observing that if $6 < n \leq 19$, then n is a sum of distinct primes ≤ 11.

16. Let $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ be the sequence of primes and put $d_n := p_{n+1} - p_n$. Deduce from Theorem 3.5 that $\liminf d_n/\log p_n < \infty$ and $\limsup d_n/\log p_n > 0$.

Remark. The twin prime conjecture says that $d_n = 2$ infinitely often, which of course implies that

$$\liminf_{n \to \infty} d_n/\log p_n = 0. \tag{3.26}$$

In 2005, Goldston, Pintz, and Yıldırım (see [**GPY09, GMPY06**] and the survey [**Sou07**]) proved that (3.26) holds unconditionally, which had been a long-standing open problem. Their method can be elaborated on [**GPY10**] to show that on an infinite set of n,

$$d_n \ll (\log p_n)^{1/2} (\log \log p_n)^2.$$

The principal tool needed in their argument is a theorem of Bombieri and Vinogradov. Roughly speaking, the Bombieri–Vinogradov theorem asserts that the primes are as well-distributed in arithmetic progressions, *on average*, as the Extended Riemann Hypothesis predicts for each individual progression. A plausible strengthening of the Bombieri–Vinogradov conjecture, due to Elliott & Halberstam, would imply that infinitely often $d_n \leq 16$, which would put us agonizingly close to the twin prime conjecture. In fact, any improvement of the Bombieri–Vinogradov theorem in the direction of the Elliott-Halberstam conjecture would imply the existence of a constant C with $d_n \le C$ infinitely often. However, such improvements seem to lie very deep.

In the opposite direction, it was shown by Westzynthius [**Wes31**] already in 1931 that $\limsup_{n\to\infty} \frac{d_n}{\log p_n} = \infty$. The best result in this direction is due to Erdős [**Erd35c**] and Rankin [**Ran38**]: For some constant $c > 0$ and infinitely many n,

$$d_n > c \log p_n \frac{\log\log p_n \log\log\log\log p_n}{(\log\log\log p_n)^2}.$$

According to work of Pintz [**Pin97**], we can take $c = 2e^{\gamma}$. Erdős offered a prize of \$10,000 for a proof that c could be taken arbitrarily large.

† 17. (Continuation; Erdős & Turán [**ET48**])

(a) Prove that $d_n < d_{n+1}$ for infinitely many n.

(b) Prove that $d_n > d_{n+1}$ for infinitely many n. *Hint:* Assume that $d_n \le d_{n+1}$ whenever $n \ge N_0$. Fix $C > 0$ so that $d_m < C \log p_m$ for infinitely many m. Show that there is a $k_0 \in \mathbf{N}$ with the property that if k is a natural number with $k \ge k_0$, then $d_n = k$ can hold for at most k consecutive values of n. Now argue that if $d_m < C \log p_m$, then $p_{m+1} - 2 = \sum_{i=1}^{m} d_i \ll (\log p_m)^3$.

Remark. Open problems about d_n abound; here are two: Is $d_n = d_{n+1}$ for infinitely many n? Is $d_n < d_{n+1} < d_{n+2}$ infinitely often?

18. Show that the series $\sum_{n=1}^{\infty} \frac{1}{n(p_{n+1}-p_n)^{\lambda}}$ diverges when $\lambda = 1$, and give a heuristic argument suggesting that it diverges for every real λ.

19. For each integer $n > 1$, let $P(n)$ denote the largest prime factor of n. Determine the set of real numbers λ for which $\sum_{n>1} \frac{1}{n^{\lambda} P(n)}$ converges.

20. (Sierpiński [**Sie64**]) It is an easy consequence of Hypothesis H that for every positive integer k, there are infinitely many primes of the form $n^2 + k$. Show (unconditionally) that for every natural number N, there is a positive integer k for which there are at least N primes of the form $n^2 + k$. *Hint:* For every p, one can write $p = \lfloor \sqrt{p} \rfloor^2 + k$ for some $k \ll \sqrt{p}$.

21. Show that for every $N \in \mathbf{N}$, there is an even integer $k > 0$ for which there are at least N prime pairs $p, p + k$.

22. (Mertens, Lindqvist & Peetre [**LP97**]) In this exercise we derive an alternative expression for the constant B_1 in Theorem 3.14, namely

$$B_1 = \gamma + \sum_{n=2}^{\infty} \frac{\mu(n)}{n} \log \zeta(n). \tag{3.27}$$

(Using the expansion (3.27) and a table of ζ-values compiled by Legendre, Mertens showed that $B_1 = 0.2614972128\ldots$.) By the results of

§4, in order to prove (3.27) it is enough to show that

$$B_2 = -\sum_{n=2}^{\infty} \frac{\mu(n)}{n} \log \zeta(n). \tag{3.28}$$

(Here $B_2 = \sum_{k\geq 2}\sum_p \frac{1}{kp^k}$, as in the statement of Theorem 3.15.)

(a) Prove that for real $s > 1$, we have $s^{-1}\log\zeta(s) = \int_2^\infty \frac{\pi(t)}{t(t^s-1)}\,dt$. Show also that $B_2 = \int_2^\infty \frac{\pi(t)}{t^2(t-1)}\,dt$.

(b) Prove that for $|x| < 1$,

$$\frac{x^2}{1-x} = -\sum_{m=2}^{\infty} \mu(m) \frac{x^m}{1-x^m}.$$

(c) Taking $x = 1/t$ in part (b), deduce that for $t > 1$,

$$\frac{1}{t^2(t-1)} = -\sum_{m=2}^{\infty} \frac{\mu(m)}{t(t^m-1)}.$$

(d) Use the results of (a)–(c) to prove (3.28).

† 23. (Pomerance [**Pom79**]) Using p_n to denote the nth prime number, let G be the collection of points $(n, p_n) \in \mathbf{R}^2$, where $n \in \mathbf{N}$. We call G the *prime number graph.*

(a) Show that every line in $\mathbf{R}^2$ contains only finitely many points of G.

(b) In the remainder of this exercise we prove that there are lines in the plane which contain arbitrarily many points of G. For this we may replace G by $G' := \{(p_n, n) : n \in \mathbf{N}\}$.
Let $k \in \mathbf{N}$. Put $u = e^k$, $v = u + u/\log u$, and let T be the parallelogram bounded by the vertical lines $x = u$, $x = v$ and the diagonal lines with slope $1/k$ through $(u, \mathrm{Li}(u) + 2u/(\log u)^4)$ and $(u, \mathrm{Li}(u) - 3u/(\log u)^4)$. Prove that there are $\ll ku/(\log u)^4$ lines of slope $1/k$ passing through lattice points contained in T (as $k \to \infty$).

(c) Assuming that $\pi(x) - \mathrm{Li}(x) = o(x/(\log x)^4)$ (which follows from (3.24)), prove that every point (p_n, n) with $u \leq p_n \leq v$ lies inside T once k is sufficiently large.

(d) Show that as $k \to \infty$, there are $\gg u/(\log u)^2$ points (p_n, n) with $u \leq p_n \leq v$. Conclude from (b) and (c) that there is a line of slope $1/k$ passing through $\gg \frac{1}{k}(\log u)^2 = k$ of these points.

† 24. (Hardy & Ramanujan [**HR17**], Turán [**Tur34**]) Write $\omega(n)$ for the number of distinct prime factors of n and $\Omega(n)$ for the number of prime factors of n counted with multiplicity. (Thus, if $n = \prod_{i=1}^k p_i^{e_i}$, where the p_i are distinct primes and each $e_i \geq 1$, then $\omega(n) = k$ and $\Omega(n) = \sum_{i=1}^k e_i$.)

(a) Show that for $x \geq 3$, we have $\sum_{n\leq x}\omega(n) = x\log\log x + O(x)$ and $\sum_{n\leq x}\omega(n)^2 = x(\log\log x)^2 + O(x\log\log x)$. *Suggestion:* First show the second estimate with $\omega(n)$ replaced by $\omega'(n) = \sum_{p|n, p \le x^{1/3}} 1$. Then use that $\omega(n) - \omega'(n) \le 2$ for all $n \le x$.

(b) Deduce from (a) that $\sum_{n \le x} (\omega(n) - \log\log x)^2 = O(x \log\log x)$.

(c) Conclude from (b) that if $B > 0$, then the number of $n \le x$ with $|\omega(n) - \log\log x| > B\sqrt{\log\log x}$ is $\ll x/B^2$, where the implied constant is absolute. Hence $\omega(n)$ is very close to $\log\log x$ for most $n \le x$.

(d) Show that $\sum_{n \le x} (\Omega(n) - \omega(n))^2 = O(x)$, and deduce that the result of (c) holds with ω replaced by Ω.

Remark. For fixed real numbers $B_1 < B_2$, a beautiful theorem of Erdős & Kac [**EK40**] asserts that

$$\frac{1}{x}\#\{n \le x : B_1 \le \frac{\omega(n) - \log\log x}{\sqrt{\log\log x}} \le B_2\} \to \frac{1}{\sqrt{2\pi}} \int_{B_1}^{B_2} e^{-u^2/2}\, du$$

as $x \to \infty$, and the same with ω replaced by Ω. Actually the Erdős–Kac result is far more general and can be viewed as an analogue of the central limit theorem for additive arithmetic functions.[1] The Erdős–Kac theorem stands with the Erdős–Wintner theorem (discussed in the notes to Chapter 9) as one of the foundational results in probabilistic number theory.

† 25. (Continuation; Erdős [**Erd55b, Erd60**]) Suppose N is a natural number. The $N \times N$ *multiplication table* is defined as the $N \times N$ array whose ith row, jth column entry is $i \cdot j$. Since multiplication is commutative, it is clear that the number $A(N)$ of distinct entries in this table is bounded by the number of unordered pairs of integers from $[1, N]$, which is just $\frac{1}{2}N(N+1)$. The following rough argument suggests that $A(N)$ is considerably smaller:

> For most ordered pairs of integers (i, j) with $1 \le i, j \le N$, the number $\Omega(i \cdot j) = \Omega(i) + \Omega(j)$ of prime factors of $i \cdot j$ is very close to $2 \log\log N$ by Exercise 24. But most numbers $n \le N^2$ have about $\log\log(N^2) \sim \log\log N$ prime factors. So the multiplication table contains mostly atypical numbers, and so it cannot contain very many of the numbers $n \le N^2$.

Fill in the details of this argument to construct a rigorous proof that $A(N)/N^2 \to 0$ as $N \to \infty$.

Remark. As a consequence of a detailed study of the distribution of divisors of natural numbers, Ford [**For08a**] (see also [**For08b**]) proved that

$$A(N) \asymp \frac{N^2}{(\log N)^{\delta} (\log\log N)^{3/2}}, \quad \text{where} \quad \delta := 1 - \frac{1 + \log\log 2}{\log 2}.$$

[1] An arithmetic function f is termed *additive* if $f(mn) = f(m) + f(n)$ whenever $\gcd(m, n) = 1$.

† 26. (Erdős [**Erd79**]) Define $\omega(n;z) := \sum_{p\mid n,\ p\le z} 1$, so that $\omega(n) = \omega(n;n)$.

(a) Show that if $x \ge z \ge 3$, then

$$\sum_{n\le x}(\omega(n;z) - \log\log z)^2 \ll x\log\log z.$$

(b) Define a sequence of positive real numbers $\{z_j\}_{j=1}^{\infty}$ by putting $z_j := \exp(\exp(j^4))$. Show that if $x \ge z_j$, then there are $\ll xj^{-2}$ natural numbers $n \le x$ with $|\omega(n;z_j) - \log\log z_j| > (\log\log z_j)^{3/4}$.

(c) Now let $\epsilon > 0$. Show that one can choose a positive real number Z, depending only on ϵ, so that the following holds: If x is sufficiently large, then all but at most ϵx natural numbers $n \le x$ satisfy $|\omega(n;z) - \log\log z| < 40(\log\log z)^{3/4}$ for all $Z < z \le x$.

(d) Prove that all of the assertions of (a)–(c) remain valid if $\omega(n;z)$ is replaced by $\Omega(n;z) := \sum_{p^k\mid n,\ p\le z} 1$.

† 27. (Continuation) For $n \in \mathbf{N}$ and $1 \le k \le \omega(n)$, let $p_k(n)$ denote the kth smallest prime divisor of n. Show that for each $\epsilon > 0$ and $\eta > 0$, there is a natural number K for which the following holds: The set of natural numbers n for which

$$k(1-\epsilon) < \log\log p_k(n) < k(1+\epsilon)$$

for every $K < k \le \omega(n)$ has lower density at least $1-\eta$. Roughly speaking, this says that for large k, the kth prime factor of a typical natural number is approximately e^{e^k}.

† 28. (Besicovitch [**Bes34**], Erdős [**Erd35a**]) For $y \ge 1$, let δ_y denote the asymptotic density of the set of natural numbers with a divisor d in the interval $y < d \le 2y$.

(a) Show that δ_y is well-defined, i.e., that the density of the set in question exists.

(b) Show that $\delta_y \to 0$ as $y \to \infty$. *Hint:* Write $n = de$. Then either $\Omega(d;y) \le \frac{3}{4}\log\log y$, $\Omega(e;y) \le \frac{3}{4}\log\log y$, or $\Omega(n;y) > \frac{3}{2}\log\log y$.

29. The twin prime conjecture illustrates how difficult it can be to control the multiplicative structure of neighboring integers. In this exercise we give an elementary example where this is possible.

(a) Define a sequence of finite subsets $S_i \subset \mathbf{N}$ as follows: Let $S_2 = \{2,3\}$. Assuming S_r has already been defined, let M be the product of all the elements of S_r and put $S_{r+1} := \{M\} \cup \{M - a : a \in S_r\}$. Check that for each r, the set S_r has r elements and $|a_1 - a_2| = \gcd(a_1,a_2)$ for every pair of distinct elements $a_1, a_2 \in S_r$. (This important construction is due to Heath-Brown [**HB87**].)

(b) Suppose that $f\colon \mathbf{N} \to \mathbf{C}^{\times}$ is a completely multiplicative arithmetic function and that its image $f(\mathbf{N})$ is finite. Show that the set of $n \in \mathbf{N}$ for which $f(n) = f(n+1)$ has positive lower density. *Hint:*

Choose a natural number $r > |f(\mathbf{N})|$, and list the elements $a_1 < a_2 < \cdots < a_r$ of S_r. Put $M = \prod_{i=1}^{r} a_i$. Start by observing that for any $k \in \mathbf{N}$, at least two of the values $\{f(kM + a_j)\}_{1\le j\le r}$ must coincide.

(c) Using (b), show that for each fixed $m \in \mathbf{N}$, a positive proportion of natural numbers n satisfy $\Omega(n) \equiv \Omega(n+1) \pmod{m}$.

Remark. For further results on the multiplicative structure of consecutive integers, see Hildebrand's elegant survey [**Hil97**].

† 30. (Montgomery & Wagon [**MW06**]) Suppose that $W(x)$ is a real-valued function of x which is decreasing for $x \ge 2$. Prove that if

$$\int_2^x W(t)\log t\,\frac{dt}{t} \sim \log x,$$

then $W(x) \sim 1/\log x$ as $x \to \infty$. *Hint:* Obtain a lower bound for $\liminf_{x\to\infty} W(x)\log x$ by observing that

$$W(x)\int_x^{x^{1+\epsilon}} \log t\,\frac{dt}{t} \ge \int_x^{x^{1+\epsilon}} W(t)\log t\,\frac{dt}{t} \sim \epsilon\log x.$$

Replacing the limits of integration with $x^{1-\epsilon}$ and x, establish an analogous upper bound for $\limsup_{x\to\infty} W(x)\log x$.

† 31. (Continuation) We now prove that if $\pi(x) \sim x/L(x)$ for a function $L(x)$ which is positive-valued and increasing for $x \ge 2$, then necessarily $L(x) \sim \log x$, so that the prime number theorem holds. Note that this generalizes Theorem 3.4.

Put $f(x) = x^{-1}\log x$, so that $\sum_{p\le x} f(p) \sim \log x$ by (3.20).

(a) Show that $\sum_{p\le x} f(p) \sim -\int_2^x \pi(t)f'(t)\,dt$ as $x \to \infty$.

(b) Prove that $\int_2^x \pi(t)f'(t)\,dt \sim \int_2^x (t/L(t))f'(t)\,dt$.

(c) Deduce from (a), (b), and (3.20) that

$$\int_2^x L(t)^{-1}\log t\,\frac{dt}{t} \sim \log x.$$

(d) Conclude from Exercise 30 that $1/L(x) \sim 1/\log x$, so that $L(x) \sim \log x$.

Remark. See Exercise 8.3 for a different strengthening of Theorem 3.4.

32. In this exercise and the next we explore what can be proved with our present tools about the magnitude of the divisor function $\tau(n)$.

(a) Show that $\sum_{n\le x}\tau(n) = x\log x + O(x)$ for $x \ge 1$. So on average, a natural number $n \le x$ has about $\log x$ divisors.

(b) Show that $2^{\omega(n)} \le \tau(n) \le 2^{\Omega(n)}$ for every natural number n. Deduce from Exercise 24 that for each $B > 0$, all but $O(x/B^2)$ of the natural numbers $n \le x$ satisfy

$$2^{\log\log x - B\sqrt{\log\log x}} \le \tau(n) \le 2^{\log\log x + B\sqrt{\log\log x}}.$$

Since $2^{\log\log x} = (\log x)^{\log 2}$, this shows that most $n \le x$ have significantly fewer divisors than the average.

33. (Continuation; Wigert [**Wig07**]) Let n be a natural number not exceeding x. Let $A := \prod_{p^e \| n, p \le \frac{\log x}{(\log\log x)^2}} p^e$ and put $B := \prod_{p^e \| n, p > \frac{\log x}{(\log\log x)^2}} p^e$.
   (a) Show that $\tau(A) \le 2^{O(\log x/(\log\log x)^2)}$ as $x \to \infty$.
   (b) Show that $\Omega(B) \le (1 + o(1)) \log x/\log\log x$. Deduce that $\tau(B) \le 2^{(1+o(1))\frac{\log x}{\log\log x}}$.
   (c) Conclude from (a) and (b) that $\tau(n) \le 2^{(1+o(1))\frac{\log x}{\log\log x}}$.
   (d) By considering the product of an initial segment of the primes, show that there is a sequence of n tending to infinity along which

$$\tau(n) \ge 2^{(1+o(1))\frac{\log n}{\log\log n}}.$$

   Thus (c) is best possible. You *may* assume the prime number theorem for this part of the exercise, but this is not necessary.

34. Recall that $\Psi(x, y)$ denotes the number of y-smooth $n \le x$, i.e., the number of natural numbers $n \le x$ all of whose prime divisors are $\le y$. Rankin [**Ran38**] observed that for any $\sigma > 0$, one has

$$\Psi(x, y) \le \sum_{\substack{n \le x \\ p \mid n \Rightarrow p \le y}} \left(\frac{x}{n}\right)^{\sigma} = x^{\sigma} \prod_{p \le y} (1 - p^{-\sigma})^{-1}. \tag{3.29}$$

Suppose now that $x \ge y \ge 2$, and put $\sigma := 1 - \frac{1}{2\log y}$. Show that

$$\frac{1}{p^{\sigma}} - \frac{1}{p} \ll \frac{\log p}{p \log y}$$

uniformly for primes $p \le y$, and deduce that the product appearing in (3.29) is $\ll \log y$. Conclude that for $x \ge y \ge 2$,

$$\Psi(x, y) \ll x e^{-u/2} \log y, \quad \text{where} \quad u := \frac{\log x}{\log y}$$

and the implied constant is absolute.

35. (Gauss's polynomial prime number theorem) For each $A(T) \in \mathbf{F}_q[T]$, put $|A| := q^{\deg A}$. Define the *zeta function* $\zeta_q(s)$ *of* $\mathbf{F}_q[T]$ by setting $\zeta_q(s) := \sum_A |A|^{-s}$, where A runs over all monic polynomials in $\mathbf{F}_q[T]$. Let $\pi(q; n)$ denote the number of monic irreducible polynomials of degree n over $\mathbf{F}_q$.
   (a) Show that for $s > 1$, we have $\zeta_q(s) = 1/(1 - q^{1-s})$.

(b) Show that for $s > 1$, there is a product representation of $\zeta_q(s)$, namely $\zeta_q(s) = \prod_P (1 - |P|^{-s})^{-1}$, where P runs over all monic irreducible polynomials in $\mathbf{F}_q[T]$.

(c) From (a) and (b), deduce that with $u = q^{-s}$,

$$\frac{1}{1-qu} = \prod_{j=1}^{\infty} \left(\frac{1}{1-u^j}\right)^{\pi(q;j)}.$$

(d) Starting with the result of (c), show that

$$\sum_{d \geq 1} d\pi(q;d) \frac{u^d}{1-u^d} = \frac{qu}{1-qu}. \tag{3.30}$$

Hint: Take the logarithmic derivative.

(e) By comparing the coefficients of u^n on both sides of (3.30), deduce that $q^n = \sum_{d \mid n} d\pi(q;d)$. Conclude that $\pi(q;n) = \frac{1}{n}\sum_{d\mid n} \mu(d) q^{n/d}$.

(f) Show that $|\pi(q;n) - q^n/n| \leq 2q^{n/2}/n$ for every prime power q and every natural number n.

If we set $X = q^n$, then we have just shown that $\pi(q;n)$ is very close to $X/\log_q X$, where $\log_q$ denotes the logarithm with base q. This is strikingly reminiscent of the prime number theorem.

36. (Mertens' theorem for polynomials) Show that $\prod_{\deg P \leq n}(1 - 1/|P|) = e^{-\gamma}/n + O(1/n^2)$, where γ is the Euler–Mascheroni constant. Here n is a natural number, P runs over the monic irreducible polynomials in $\mathbf{F}_q[T]$ of degree at most n, and the implied constant is understood to be absolute (independent of both q and n). Proceed as follows:

(a) Reduce the proof to the assertion that

$$\sum_{\deg P \leq n} \sum_{k \geq 1} \frac{1}{k|P|^k} = \log n + \gamma + O(1/n).$$

(b) Use the results of Exercise 35 to show that we have the (exact) identity

$$\sum_{P,k\colon\ \deg P^k \leq n} \frac{1}{k|P|^k} = \sum_{m \leq n} \frac{1}{m}.$$

(c) Complete the proof by first estimating $\sum_{m \leq n} m^{-1}$ using Lemma 3.16 and then showing that

$$\sum_{\deg P \leq n} \sum_{k > n/\deg P} \frac{1}{k|P|^k} \ll \frac{1}{n}.$$

This argument is due to K. Conrad (see [**EHM02**]).

37. (A polynomial analogue of the twin prime conjecture) Capelli's theorem (proved, e.g., as [**Lan02**, Theorem 9.1]) asserts that if F is an arbitrary

field, $a \in F$ and $n \in \mathbf{N}$, then the binomial $T^n - a$ is irreducible in $F[T]$ unless one of the following holds:

(i) there is a prime l dividing n for which a is an lth power in F,

(ii) 4 divides n and $a = -4b^4$ for some $b \in F$.

Using this result, show that $T^{3^k} - 3$ and $T^{3^k} - 2$ are both irreducible over $\mathbf{F}_7$ for every integer $k \geq 0$. In particular, there are infinitely many monic polynomials $A(T) \in \mathbf{F}_7[T]$ for which A and $A+1$ are both irreducible.

If you are feeling ambitious, prove that this last claim holds with $\mathbf{F}_7$ replaced by any finite field with more than 3 elements. This result is due to Hall [**Hal03, Hal06**].

Remark. Actually this claim holds even for the field $\mathbf{F}_3$, but a somewhat different argument is required. For this and other generalizations, see [**Pol08a**]. See also [**Eff08**], [**Pol08b**].

Chapter 4

Primes in Arithmetic Progressions

> When Gauss says he has proved something, it is very probable ... when Cauchy says it, you can bet equally well pro or contra, but when Dirichlet says it, it is *certain*. I prefer to leave myself out of this Delikatessen. – C. G. J. Jacobi, letter to von Humboldt

1. Introduction

In this chapter we prove Dirichlet's result [**Dir37, Dir39, Dir41**] that if a and m are integers with $m > 0$ and $\gcd(a, m) = 1$, then there are infinitely many primes $p \equiv a \pmod{m}$. Actually, we shall prove more, namely that for $x \geq 4$,

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{m}}} \frac{\log p}{p} = \frac{1}{\varphi(m)} \log x + O(1), \tag{4.1}$$

where the implied constant may depend on m. The infinitude of primes $p \equiv a \pmod{m}$ is of course an obvious consequence, but (4.1) says much more. In light of (3.20), we can view (4.1) as an equidistribution statement, asserting that (in a peculiar average sense) the fraction of primes falling into a given coprime residue class is exactly $1/\varphi(m)$. Moreover, as shown in Exercise 3, the estimate (4.1) implies that

$$\pi(x; m, a) \gg_{a,m} \frac{x}{\log x},$$

which can be considered an analogue of Chebyshev's lower bound on $\pi(x)$ from Chapter 3.

As an application of Dirichlet's result, we close the chapter with a proof of Legendre's characterization of the integers expressible as a sum of three squares.

2. Progressions modulo 4

We begin by considering the case when $m = 4$. Define a function $\chi\colon \mathbf{Z} \to \mathbf{C}$ by putting

$$\chi(n) := \begin{cases} (-1)^{(n-1)/2} & \text{if } 2 \nmid n, \\ 0 & \text{otherwise.} \end{cases} \tag{4.2}$$

It is straightforward to check that $\chi(ab) = \chi(a)\chi(b)$ for every pair of integers a, b. So, at least formally (i.e., ignoring issues of convergence),

$$\prod_p \left(1 - \frac{\chi(p)}{p}\right)^{-1} = \sum_{n \geq 1} \frac{\chi(n)}{n} \tag{4.3}$$

(cf. Theorem 1.2). Let L denote the right-hand series; then

$$\begin{aligned} L :&= 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \cdots \\ &= (1 - 1/3) + (1/5 - 1/7) + (1/9 - 1/11) + \cdots > 2/3. \end{aligned} \tag{4.4}$$

In particular, $L > 0$. Since

$$\log \frac{1}{1-z} = z + \frac{z^2}{2} + \frac{z^3}{3} + \ldots \qquad (\text{when } |z| < 1),$$

taking the logarithm of both sides of (4.3) shows that as $x \to \infty$,

$$\sum_{\substack{p^k \leq x \\ p^k \equiv 1 \pmod 4}} \frac{1}{kp^k} - \sum_{\substack{p^k \leq x \\ p^k \equiv 3 \pmod 4}} \frac{1}{kp^k} = \log L + o(1).$$

The terms corresponding to $k \geq 2$ contribute a negligible amount to both sums, which implies that

$$\sum_{\substack{p \leq x \\ p \equiv 3 \pmod 4}} \frac{1}{p} - \sum_{\substack{p \leq x \\ p \equiv 1 \pmod 4}} \frac{1}{p}$$

is $O(1)$. Since $\sum_{p \leq x} p^{-1} \sim \log\log x$ (by Mertens' first theorem), both $\sum_{p \leq x, p \equiv 1 \pmod 4} p^{-1}$ and $\sum_{p \leq x, p \equiv 3 \pmod 4} p^{-1}$ are $\sim \frac{1}{2} \log\log x$. In particular, both coprime residue classes modulo 4 contain infinitely many primes.

Unfortunately, it is by no means apparent how to justify the identity (4.3). (Our only tool for establishing a factorization like (4.3) is Theorem

1.2, but its hypotheses do not hold in this case.) There are various ways to work around this; the most common is to replace the series $\sum \chi(n)n^{-1}$ with $\sum \chi(n)n^{-s}$, where $s > 1$. Then $\sum \chi(n)n^{-s}$ is absolutely convergent, and so from Theorem 1.2 we obtain the analogue of (4.3). Following the above argument, we now find that $\sum_p \chi(p)p^{-s}$ remains bounded as $s \downarrow 1$. Since $\sum_p p^{-s}$ diverges to infinity as $s \downarrow 1$, it must be that 1 and -1 both occur as the value of $\chi(p)$ for infinitely many primes p. This again shows that both coprime progressions modulo 4 contain infinitely many primes. We will follow a different route in this text; rather than alter the terms of the series $\sum \chi(n)n^{-1}$, we alter the range of summation, working with the truncations $\sum_{n \le x} \chi(n)n^{-1}$.

Suppose now that m is any natural number and $a \in \mathbf{Z}$. Then

$$\begin{aligned}\sum_{\substack{n \le x\\ n \equiv a \ (\mathrm{mod}\ m)}} \frac{\Lambda(n)}{n} &= \sum_{\substack{p^k \le x\\ p^k \equiv a \ (\mathrm{mod}\ m)}} \frac{\log p}{p^k}\\ &= \sum_{\substack{p \le x\\ p \equiv a \ (\mathrm{mod}\ m)}} \frac{\log p}{p} + \sum_{k \ge 2} \sum_{\substack{p \le x^{1/k}\\ p^k \equiv a \ (\mathrm{mod}\ m)}} \frac{\log p}{p^k}.\end{aligned}$$

By (3.19), the double sum here is absolutely bounded. Consequently,

$$\sum_{\substack{p \le x\\ p \equiv a \ (\mathrm{mod}\ m)}} \frac{\log p}{p} = \sum_{\substack{n \le x\\ n \equiv a \ (\mathrm{mod}\ m)}} \frac{\Lambda(n)}{n} + O(1). \tag{4.5}$$

Thus estimates for $\sum \log p/p$, taken over the primes $p \equiv a \pmod{m}$, follow from estimates for $\sum \Lambda(n)/n$, taken over natural numbers $n \equiv a \pmod{m}$.

Now specialize again to the case $m = 4$. Let χ be as defined in (4.2), and let χ_0 be the indicator function of the odd integers. Then $\chi_0 + \chi$ is twice the characteristic function of the arithmetic progression 1 mod 4, and $\chi_0 - \chi$ is twice the characteristic function of the arithmetic progression 3 mod 4. This suggests studying the summatory functions

$$\sum_{n \le x} \frac{\chi_0(n)\Lambda(n)}{n} \quad \text{and} \quad \sum_{n \le x} \frac{\chi(n)\Lambda(n)}{n}. \tag{4.6}$$

The first of these behaves very much like the sum $\sum_{n \le x} \Lambda(n)/n$ investigated in Chapter 3:

$$\begin{aligned}\sum_{n \le x} \frac{\chi_0(n)\Lambda(n)}{n} &= \sum_{n \le x} \frac{\Lambda(n)}{n} - \sum_{2^k \le x} \frac{\log 2}{2^k}\\ &= \sum_{n \le x} \frac{\Lambda(n)}{n} + O(1) = \log x + O(1),\end{aligned} \tag{4.7}$$

the final equality coming from (3.17). To understand the second sum appearing in (4.6), we notice that L, defined in (4.4), is an alternating series with terms decreasing in absolute value. Thus, if we use N to denote the smallest odd integer exceeding x, then for every $x \geq 1$,

$$\left|\sum_{n>x} \frac{\chi(n)}{n}\right| \leq \left|\frac{\chi(N)}{N}\right| = \frac{1}{N} < \frac{1}{x}.$$

Following Mertens, we observe next that

$$\begin{aligned}
\sum_{n\leq x} \frac{\chi(n)\log n}{n} &= \sum_{n\leq x} \frac{\chi(n)}{n} \sum_{d\mid n} \Lambda(d) \\
&= \sum_{d\leq x} \Lambda(d) \sum_{\substack{n\leq x\\ d\mid n}} \frac{\chi(n)}{n} \\
&= \sum_{de\leq x} \frac{\chi(de)\Lambda(d)}{de} = \sum_{d\leq x} \frac{\chi(d)\Lambda(d)}{d} \sum_{e\leq x/d} \frac{\chi(e)}{e}.
\end{aligned}$$

The inner sum here is equal to $L - \sum_{e>x/d} \chi(e)e^{-1} = L + O(d/x)$. Substituting this above tells us that

$$\begin{aligned}
\sum_{n\leq x} \frac{\chi(n)\log n}{n} &= L \sum_{d\leq x} \frac{\chi(d)\Lambda(d)}{d} + O\left(\frac{1}{x}\sum_{d\leq x} \Lambda(d)\right) \\
&= L \sum_{d\leq x} \frac{\chi(d)\Lambda(d)}{d} + O(1),
\end{aligned}$$

since $\sum_{d\leq x} \Lambda(d) = \psi(x) \ll x$. Also, $\sum_{n\leq x} \chi(n)\log n/n = O(1)$, since

$$\frac{\log 1}{1} - \frac{\log 3}{3} + \frac{\log 5}{5} - \cdots$$

is an alternating series with eventually decreasing terms. Thus

$$L \sum_{d\leq x} \frac{\chi(d)\Lambda(d)}{d} = O(1),$$

and since $L \neq 0$, it follows that

$$\sum_{d\leq x} \frac{\chi(d)\Lambda(d)}{d} = O(1). \tag{4.8}$$

From (4.7) and (4.8), we deduce that

$$\sum_{\substack{n \le x \\ n \equiv 1 \pmod{4}}} \frac{\Lambda(n)}{n} + \sum_{\substack{n \le x \\ n \equiv 3 \pmod{4}}} \frac{\Lambda(n)}{n} = \log x + O(1),$$

$$\sum_{\substack{n \le x \\ n \equiv 1 \pmod{4}}} \frac{\Lambda(n)}{n} - \sum_{\substack{n \le x \\ n \equiv 3 \pmod{4}}} \frac{\Lambda(n)}{n} = O(1).$$

Adding these estimates shows that

$$\sum_{\substack{n \le x \\ n \equiv 1 \pmod{4}}} \frac{\Lambda(n)}{n} = \frac{1}{2} \log x + O(1),$$

and subtracting yields the same result for n restricted to the residue class 3 mod 4. Referring to equation (4.5) shows that the same estimates hold for the sums $\sum \log p/p$. This completes the proof of (4.1) when $m = 4$.

In general, to prove Dirichlet's theorem for all coprime progressions modulo m, we will need to consider $\varphi(m) - 1$ series analogous to the single series L appearing in this proof. The most difficult part of the argument consists of showing that none of these series converges to zero.

Remark. For the remainder of this chapter, up until the exercises, we adopt the convention that **all implied constants may depend on m, unless otherwise stated**. Further dependence will be mentioned explicitly.

3. The characters of a finite abelian group

To carry out the strategy which proved successful for progressions modulo 4, we first need to understand the appropriate analogues of the function χ, as defined in (4.2), for a general modulus m. These turn out to be the Dirichlet characters modulo m, which arise in a natural way from the characters of the unit group $(\mathbf{Z}/m\mathbf{Z})^\times$.

3.1. The classification of characters. Let G be a finite abelian group (written multiplicatively). By a *character* of G we mean a homomorphism

$$\chi \colon G \to \mathbf{C}^\times,$$

i.e., a function from G to the nonzero complex numbers satisfying

$$\chi(ab) = \chi(a)\chi(b) \tag{4.9}$$

for every $a, b \in G$. The set of characters of G is denoted $\hat{G}$. We let χ_0 denote the *trivial* character which is identically 1. Note that if χ is a character of G, then every value which χ assumes is a root of unity. Indeed, if the order of $g \in G$ is n, then $\chi(g)^n = \chi(g^n) = \chi(1) = 1$, so that $\chi(g)$ is an nth root of unity.

Our goal in this section is to classify the characters of an arbitrary finite abelian group G. We first treat the case when G is cyclic. Fix a generator g_0 of G. The value of $\chi(g_0)$ determines $\chi(g)$ for every $g \in G$; indeed, if $g = g_0^k$, then $\chi(g) = \chi(g_0^k) = \chi(g_0)^k$. From the preceding paragraph, $\chi(g_0)$ must be a $|G|$th root of unity, and so G has at most $|G|$ characters. Moreover, we see that there are precisely $|G|$ characters if and only if for every $|G|$th root of unity η, there is a character χ of G with $\chi(g_0) = \eta$. And it is easy to describe a character χ of G for which this holds: Simply define χ by putting $\chi(g_0^k) = \eta^k$ for all k. χ is well-defined, since if $g = g_0^{k_1} = g_0^{k_2}$, then $k_1 \equiv k_2 \pmod{|G|}$, so that $\eta^{k_1} = \eta^{k_2}$. Moreover, it is straightforward to verify (4.9) in this case, so that χ is a genuine character of G. We have thus achieved a complete classification of the characters of a finite cyclic group.

An arbitrary finite abelian group of course need not be cyclic, but according to a well-known classification theorem, every such group is a direct sum of cyclic groups. In other words, one can always find elements $g_1, \dots, g_k \in G$ with respective orders $n_1, \dots, n_k$ (say), with the property that every $g \in G$ has a unique representation in the form

$$g_1^{e_1} g_2^{e_2} \cdots g_k^{e_k}, \quad \text{where } 0 \le e_i < n_i \text{ for each } 1 \le i \le k.$$

If χ is a character of G, then χ is completely determined by $\chi(g_1), \dots, \chi(g_k)$. Since $\chi(g_i)$ must be an n_ith root of unity for each i, we see that there are at most $\prod_{i=1}^k n_i = |G|$ characters of G. Moreover, if for each $1 \le i \le k$ we let η_i be an arbitrary n_ith root of unity, then it is easy to check that putting

$$\chi(g_1^{e_1} \cdots g_k^{e_k}) := \eta_1^{e_1} \eta_2^{e_2} \cdots \eta_k^{e_k} \tag{4.10}$$

gives us a well-defined character χ of G with $\chi(g_i) = \eta_i$ for each $1 \le i \le k$. So there are precisely $|G|$ elements of $\hat{G}$, and we understand them all.

Remark. For the purposes of this chapter, we need not invoke any classification results from group theory. We only need to understand the case when $G = (\mathbf{Z}/m\mathbf{Z})^\times$. In this case the existence of a decomposition into cyclic groups is elementary: Indeed, the Chinese remainder theorem guarantees that if $m = \prod_{i=1}^k p_i^{e_i}$, then $(\mathbf{Z}/m\mathbf{Z})^\times \cong \prod_{i=1}^k (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times$, and we obtain the desired decomposition of G once we recall that (see, e.g., [**IR90**, Theorems 2, 2′])

$$(\mathbf{Z}/p^e\mathbf{Z})^\times \cong \begin{cases} \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2^{e-2}\mathbf{Z} & \text{if } p = 2, e > 2, \\ \mathbf{Z}/((p-1)p^{e-1})\mathbf{Z} & \text{otherwise.} \end{cases}$$

3.2. The orthogonality relations. The characters of a finite abelian group obey certain *orthogonality relations*, which play an essential role in the proof of Dirichlet's theorem. In the situation that concerns us, when $G = (\mathbf{Z}/m\mathbf{Z})^\times$, these relations allow us to express the characteristic function of a coprime residue class modulo m as a linear combination of characters.

Before stating these relations, we note that $\hat{G}$ can be made into a group (called the *dual group of* G) by defining, for $\chi, \psi \in \hat{G}$,

$$(\chi\psi)(g) := \chi(g)\psi(g),$$

i.e., by defining the multiplication pointwise. The trivial character χ_0 now serves as the identity. Associativity and commutativity follow from the corresponding properties of $\mathbf{C}^\times$. And inverses are easy; for each $\chi \in \hat{G}$, define χ^{-1} by putting

$$\chi^{-1}(g) := \chi(g)^{-1}.$$

The right-hand side exists since χ takes values in the *nonzero* complex numbers, and the homomorphism property of χ^{-1} follows from inverting both sides of (4.9). Notice that because the values χ assumes are always roots of unity, we have $\chi^{-1} = \overline{\chi}$, where $\overline{\chi}$ is defined by $\overline{\chi}(g) := \overline{\chi(g)}$ for each $g \in G$.

Now suppose that $\chi \in \hat{G}$ is nontrivial, i.e., $\chi \neq \chi_0$. Then there is an element $h \in G$ with $\chi(h) \neq 1$. Since G is a group, hg runs over the elements of G as g does. Thus, setting $S_\chi = \sum_{g \in G} \chi(g)$, one has

$$\chi(h)S_\chi = \chi(h)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(hg) = \sum_{g\in G}\chi(g) = S_\chi.$$

Since $\chi(h) \neq 1$, we must have $S_\chi = 0$. Thus

$$\sum_{g\in G}\chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise.} \end{cases}$$

Since $\overline{\chi} = \chi^{-1}$ for any character χ, this can be recast as follows: If χ and ψ are two characters of G, then

$$\sum_{g\in G}\overline{\chi}(g)\psi(g) = \begin{cases} |G| & \text{if } \chi = \psi, \\ 0 & \text{otherwise.} \end{cases} \tag{4.11}$$

Equation (4.11) is the first of two orthogonality relations for characters. It was obtained by studying $\sum \chi(g)$, where $\chi \in \hat{G}$ is fixed and g runs over the elements of the group G. To obtain the second orthogonality relation, we investigate the same sum where instead $g \in G$ is fixed and χ runs over the elements of the group $\hat{G}$. To proceed we require the following lemma:

Lemma 4.1. *Let G be a finite abelian group and let $g \neq 1$ be an element of G. Then there exists a character $\chi \in \hat{G}$ with $\chi(g) \neq 1$.*

Proof. Let $g_1, \dots, g_k$ be a system of independent generators for G as in §3.1, so that every element of G admits a unique representation in the form (4.10). Since g is not the identity of G, in its representation in the form (4.10) there is at least one exponent e_i with $0 < e_i < n_i$. Fix such an i, and let χ be the character of G defined by $\chi(g_1^{e_1} \cdots g_k^{e_k}) = \eta_i^{e_i}$, where η_i is a fixed primitive n_ith root of unity. Then $\chi(g) \neq 1$. □

Now let $g \neq 1$ be an element of G and choose $\psi \in \hat{G}$ with $\psi(g) \neq 1$. Set $S_g = \sum_{\chi \in \hat{G}} \chi(g)$. Since $\hat{G}$ forms a group, $\psi\chi$ runs over all elements of $\hat{G}$ as χ does. Consequently,

$$\psi(g) S_g = \psi(g) \sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi \in \hat{G}} (\psi\chi)(g) = \sum_{\chi \in \hat{G}} \chi(g) = S_g.$$

Hence

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Noting that for each $g \in G$,

$$\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)} = \overline{\chi}(g),$$

we find that

$$\sum_{\chi \in \hat{G}} \overline{\chi}(g)\chi(h) = \begin{cases} |G| & \text{if } g = h, \\ 0 & \text{otherwise.} \end{cases} \tag{4.12}$$

This is the second orthogonality relation.

3.3. Dirichlet characters. Let m be a natural number and let $G = (\mathbf{Z}/m\mathbf{Z})^\times$, the group of units modulo m. For each $\chi \in \hat{G}$, we introduce an associated function $\tilde{\chi}$ defined on the set of integers coprime to m by putting

$$\tilde{\chi}(a) := \chi(a \bmod m).$$

We extend $\tilde{\chi}$ to a function defined on all of $\mathbf{Z}$ by setting $\tilde{\chi}(a) := 0$ whenever $\gcd(a, m) > 1$. The functions $\tilde{\chi}$ are known as the *Dirichlet characters modulo* m. Instead of continuing to write "$\tilde{\chi}$", in what follows we adopt a customary abuse of notation and use the same symbol χ for both the function on G and the associated function on $\mathbf{Z}$.

It is easy to see that every Dirichlet character χ modulo m has both of the following properties:

(i) χ is periodic modulo m, i.e., $\chi(a + m) = \chi(a)$ for every $a \in \mathbf{Z}$.

(ii) χ is completely multiplicative, i.e., for every $a, b \in \mathbf{Z}$,

$$\chi(ab) = \chi(a)\chi(b).$$

Moreover, the Dirichlet characters obey the following orthogonality relations:

Theorem 4.2. *Let m be a positive integer and let χ and ψ be two Dirichlet characters modulo m. Then*

$$\sum_{a \bmod m} \overline{\chi}(a)\psi(a) = \begin{cases} \varphi(m) & \text{if } \chi = \psi^{-1}, \\ 0 & \text{otherwise.} \end{cases} \tag{4.13}$$

Theorem 4.3. *Let m be a positive integer. If $a, b \in \mathbf{Z}$ and $\gcd(a, m) = 1$, then*

$$\sum_{\chi} \overline{\chi}(a)\chi(b) = \begin{cases} \varphi(m) & \text{if } a \equiv b \pmod{m}, \\ 0 & \text{otherwise.} \end{cases} \tag{4.14}$$

Here the sum is over all Dirichlet characters χ modulo m.

These results follow from (4.11) and (4.12) if G is taken to be the $\varphi(m)$-element group $(\mathbf{Z}/m\mathbf{Z})^\times$: Theorem 4.2 is immediate from (4.11), since the values of a with $\gcd(a, m) = 1$ do not contribute to the left-hand side of (4.13). To prove Theorem 4.3, notice that (4.14) follows immediately from (4.12) in the case when $\gcd(a, m) = \gcd(b, m) = 1$. If, however, $\gcd(b, m) > 1$, then the left-hand side of (4.14) vanishes because $\chi(b) = 0$. Since $\gcd(b, m) > 1$ implies that $a \not\equiv b \pmod{m}$, the theorem holds in this case as well. (This is where we need the condition in Theorem 4.3 that $\gcd(a, m) = 1$.)

4. The L-series at $s = 1$

To each Dirichlet character χ we associate the *Dirichlet L-series*

$$L(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{4.15}$$

For our purposes, only the series corresponding to nontrivial characters are of interest and these are only of interest at $s = 1$. Nevertheless, because there is no extra difficulty involved, we begin by treating the series corresponding to nontrivial Dirichlet characters whenever $s > 0$.

Lemma 4.4. *Let χ be a nontrivial Dirichlet character modulo m. Then* (4.15) *converges for every $s > 0$. Moreover, for every $s > 0$ and $x \geq 1$,*

$$\left| \sum_{n > x} \frac{\chi(n)}{n^s} \right| \leq 2\varphi(m)x^{-s}.$$

In particular, $\sum_{n>x} \chi(n)n^{-1} \ll x^{-1}$.

Proof. Put $S(x) = \sum_{n\le x} \chi(n)$. Theorem 4.2 implies that $\sum \chi(n)$ vanishes when taken over any block of m consecutive integers, which in turn shows that $|S(x)| \le \varphi(m)$ for every x. By partial summation,

$$\sum_{n\le x} \frac{\chi(n)}{n^s} = \frac{S(x)}{x^s} + \int_1^x s\frac{S(t)}{t^{s+1}}\,dt.$$

As $x \to \infty$, the first term on the right goes to 0, since $S(x)$ remains bounded while x^s tends to infinity. The last factor converges as $x \to \infty$, by comparison with the absolutely convergent integral $\int_1^\infty s\frac{\varphi(m)}{t^{s+1}}\,dt = \varphi(m)$. This proves the first claim.

To bound the tail of $L(s,\chi)$, we apply partial summation once again:

$$\begin{aligned}\sum_{n>x} \frac{\chi(n)}{n^s} &= \left(\frac{S(y)}{y^s} - \frac{S(x)}{x^s} + \int_x^y s\frac{S(t)}{t^{s+1}}\,dt\right)\Bigg]_{y=\infty}\\ &= -\frac{S(x)}{x^s} + \int_x^\infty s\frac{S(t)}{t^{s+1}}\,dt.\end{aligned}$$

The first term is bounded in absolute value by $\varphi(m)x^{-s}$ and the second by $\int_x^\infty s\frac{\varphi(m)}{t^{s+1}}\,dt = \varphi(m)x^{-s}$. The stated estimate now follows from the triangle inequality. $\square$

5. Nonvanishing of $L(1,\chi)$ for complex χ

We say that the Dirichlet character χ is *real* if $\chi(\mathbf{Z}) \subset \mathbf{R}$, i.e., if χ assumes only real values. (In this case, $\chi(\mathbf{Z}) \subset \{0,1,-1\}$, since every nonvanishing value of χ is a root of unity.) Otherwise, we call χ a *complex* character. Our goal in this section is to show that $L(1,\chi)$ is nonvanishing for each complex Dirichlet character χ.

We first connect the vanishing or nonvanishing of $L(1,\chi)$ to the behavior of the partial sums of $\sum \chi(n)\Lambda(n)n^{-1}$.

Lemma 4.5. *Let χ be any nontrivial Dirichlet character modulo m. For $x \ge 4$,*

$$\sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n} = \begin{cases} O(1) & \text{if } L(1,\chi) \ne 0,\\ -\log x + O(1) & \text{otherwise.}\end{cases}$$

Proof when $L(1,\chi) \ne 0$. We mimic the argument of §2, which corresponds to the case when χ is the the nontrivial Dirichlet character modulo 4. We start by writing

$$\sum_{n\le x}\frac{\chi(n)\log n}{n}=\sum_{n\le x}\frac{\chi(n)}{n}\sum_{d\mid n}\Lambda(d)$$
$$=\sum_{de\le x}\frac{\chi(de)\Lambda(d)}{de}=\sum_{d\le x}\frac{\chi(d)\Lambda(d)}{d}\sum_{e\le x/d}\frac{\chi(e)}{e}.$$

From Lemma 4.4, the inner sum is $L(1,\chi)-\sum_{e>x/d}\chi(e)/e = L(1,\chi)+O(d/x)$. Inserting this above shows that

$$\sum_{n\le x}\frac{\chi(n)\log n}{n}=L(1,\chi)\sum_{d\le x}\frac{\chi(d)\Lambda(d)}{d}+O\left(\frac{1}{x}\sum_{d\le x}\Lambda(d)\right)$$
$$=L(1,\chi)\sum_{d\le x}\frac{\chi(d)\Lambda(d)}{d}+O(1), \tag{4.16}$$

since $\sum_{d\le x}\Lambda(d)=\psi(x)\ll x$ by (3.13). But we also have

$$\sum_{n\le x}\frac{\chi(n)\log n}{n}=O(1). \tag{4.17}$$

Indeed, with $S(x):=\sum_{n\le x}\chi(n)$,

$$\sum_{n\le x}\frac{\chi(n)\log n}{n}=\frac{S(x)\log x}{x}-\int_1^x S(t)\frac{1-\log t}{t^2}\,dt,$$

so that (noting that $t^{-1}\log t$ is decreasing for $t\ge e$)

$$\left|\sum_{n\le x}\frac{\chi(n)\log n}{n}\right|\le\varphi(m)\frac{\log 4}{4}+\varphi(m)\int_1^\infty\frac{dt}{t^2}+\varphi(m)\int_1^\infty\frac{\log t}{t^2}\,dt\ll 1.$$

Together, (4.16) and (4.17) imply that

$$L(1,\chi)\sum_{d\le x}\frac{\chi(d)\Lambda(d)}{d}=O(1).$$

Since $L(1,\chi)\neq 0$, the sum here must be bounded (independently of x), which is the statement of the lemma in this case. $\square$

Proof when $L(1,\chi)=0$. Applying Möbius inversion to the relation $\log n=\sum_{d\mid n}\Lambda(d)$, we obtain

$$\Lambda(n)=\sum_{d\mid n}\mu(d)\log\frac{n}{d}=\sum_{d\mid n}\mu(d)\log n-\sum_{d\mid n}\mu(d)\log d$$
$$=\log n\sum_{d\mid n}\mu(d)-\sum_{d\mid n}\mu(d)\log d=-\sum_{d\mid n}\mu(d)\log d,$$

since for every positive integer n, either $\log n = 0$ or $\sum_{d|n} \mu(d) = 0$. So for every $x > 0$,

$$\sum_{d|n} \mu(d) \log \frac{x}{d} = \log x \sum_{d|n} \mu(d) + \Lambda(n)$$
$$= \begin{cases} \log x + \Lambda(n) & \text{if } n = 1, \\ \Lambda(n) & \text{otherwise.} \end{cases}$$

Consequently,

$$\log x + \sum_{n \le x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{n \le x} \frac{\chi(n)}{n} \sum_{d|n} \mu(d) \log \frac{x}{d}$$
$$= \sum_{d \le x} \mu(d) \log \frac{x}{d} \sum_{\substack{n \le x \\ d|n}} \frac{\chi(n)}{n} = \sum_{d \le x} \mu(d) \log \frac{x}{d} \frac{\chi(d)}{d} \sum_{e \le x/d} \frac{\chi(e)}{e}$$
$$= L(1,\chi) \sum_{d \le x} \mu(d) \left(\log \frac{x}{d}\right) \frac{\chi(d)}{d} + R(x), \tag{4.18}$$

where (using the estimate of Lemma 4.4)

$$R(x) \ll \sum_{d \le x} \left(\log \frac{x}{d}\right) \frac{1}{d} \frac{d}{x} = \frac{1}{x} \sum_{d \le x} (\log x - \log d)$$
$$= \frac{1}{x} \left(\lfloor x \rfloor \log x - \log \lfloor x \rfloor !\right) \ll 1. \tag{4.19}$$

(Here we have used Lemma 3.10 to estimate $\log\lfloor x \rfloor !$.) Since $L(1,\chi) = 0$, (4.18) implies that

$$\log x + \sum_{n \le x} \frac{\chi(n)\Lambda(n)}{n} = O(1),$$

which is the assertion of Lemma 4.5 in this case. □

We also require an estimate for $\sum_{n \le x} \chi(n)\Lambda(n)n^{-1}$ when $\chi = \chi_0$.

Lemma 4.6. *Let χ_0 be the trivial character modulo m. Then for $x \ge 4$,*

$$\sum_{n \le x} \frac{\chi_0(n)\Lambda(n)}{n} = \log x + O(1).$$

Proof. Observe that

$$\sum_{n \le x} \frac{\Lambda(n)}{n} - \sum_{n \le x} \frac{\chi_0(n)\Lambda(n)}{n} = \sum_{p|m} \sum_{\substack{p^k \le x \\ k \ge 1}} \frac{\log p}{p^k} \le \sum_{p|m} \frac{\log p}{p-1} \ll 1.$$

The result now follows from (3.17). □

We can now prove the main result of this section.

Theorem 4.7. *Let χ be a complex character modulo m. Then $L(1,\chi) \neq 0$.*

Proof. Lemmas 4.5 and 4.6 together imply that for $x \geq 4$,

$$\sum_{\chi} \sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} = (1-V)\log x + O(1), \tag{4.20}$$

where V denotes the number of nontrivial χ with $L(1,\chi) = 0$, and the sum is taken over all Dirichlet characters χ modulo m. On the other hand, taking $a = 1$ in the orthogonality relation (4.14) shows that

$$\frac{1}{\varphi(m)} \sum_{\chi} \sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{\substack{n \leq x \\ n \equiv 1 \pmod{m}}} \frac{\Lambda(n)}{n} \geq 0. \tag{4.21}$$

If $V > 1$, then (4.20) and (4.21) contradict each other for large enough x. Thus $V \leq 1$, i.e., $L(1,\chi)$ vanishes for at most one nontrivial character χ.

But if $L(1,\chi) = 0$ for some complex character χ, then

$$0 = \overline{L(1,\chi)} = \overline{\sum_{n=1}^{\infty} \frac{\chi(n)}{n}} = \sum_{n=1}^{\infty} \frac{\overline{\chi}(n)}{n} = L(1,\overline{\chi})$$

also. Since χ is complex, $\chi \neq \overline{\chi}$, so that $V \geq 2$, a contradiction. $\square$

Remarks. The reader who is only familiar with the analytic proof of Dirichlet's theorem may find Lemmas 4.5 and 4.6 rather strange, so it is worth saying a word or two about why we might expect results of this type. For $\Re(s) > 1$, we have

$$L(s,\chi) = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1},$$

so that by logarithmic differentiation,

$$-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s}.$$

Our Lemmas 4.5 and 4.6 thus concern the partial sums of the coefficients of $-\frac{L'}{L}(s,\chi)$. An important lesson from analytic combinatorics is that we can often read off information on the coefficients of a generating function from information on the behavior of the associated analytic object.

Assume it has been shown that $\zeta(s)$ and $L(s,\chi)$ admit holomorphic extensions to $\Re(s) > 0$, except for simple poles at $s = 1$ in the cases of $\zeta(s)$ and the functions $L(s,\chi_0)$. (This is a usual first step in the analytic arguments.) If $L(s,\chi)$ is analytic and nonzero at $s = 1$, then $\frac{L'}{L}(s,\chi)$ is analytic at $s = 1$. Suppose, on the other hand, that $L(s,\chi)$ has a zero or pole at $s = 1$ (the latter occurring only when χ is trivial). Let K denote the integer for which $(s-1)^K L(s,\chi)$ is analytic and nonzero at $s=1$. Then $-\frac{L'}{L}(s,\chi) \sim \frac{K}{s-1}$ as $s \to 1$. For s real,

$$\left|\sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s}\right| \leq \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'}{\zeta}(s) \sim \frac{1}{s-1} \quad (\text{as } s \downarrow 1),$$

and so it must be that $K = \pm 1$. From this we easily deduce that

$$\lim_{s\downarrow 1}(s-1)\left(-\frac{L'}{L}(s,\chi)\right) = \begin{cases} 0 & \text{if } \chi \neq \chi_0 \text{ and } L(1,\chi) \neq 0, \\ \text{-1} & \text{if } \chi \neq \chi_0 \text{ and } L(1,\chi) = 0, \\ 1 & \text{if } \chi = \chi_0. \end{cases}$$

The numbers on the right-hand side correspond precisely to the coefficients of $\log x$ in the estimates of Lemmas 4.5 and 4.6. This is not a coincidence! For a theorem that guarantees this must occur, see [**Ten95**, §7.3].

6. Nonvanishing of $L(1,\chi)$ for real χ

Lemma 4.8. *Let χ be a real Dirichlet character modulo m. For every natural number n,*

$$\sum_{d\mid n} \chi(d) \geq \begin{cases} 1 & \textit{if } n \textit{ is a perfect square}, \\ 0 & \textit{in any case.} \end{cases}$$

Proof. Let $F(n) := \sum_{d\mid n} \chi(d)$. Since χ is multiplicative, F is also multiplicative. Hence $F(n) = \prod_{p^e \| n} F(p^e)$. Since χ is real, we have $\chi(p) = 0, 1,$ or -1, so that

$$F(p^e) = 1 + \chi(p) + \cdots + \chi(p^e) = \begin{cases} 1 & \text{if } \chi(p) = 0, \\ e+1 & \text{if } \chi(p) = 1, \\ 0 & \text{if } \chi(p) = -1 \text{ and } 2 \nmid e, \\ 1 & \text{if } \chi(p) = -1 \text{ and } 2 \mid e. \end{cases}$$

Since $F(p^e)$ is always nonnegative and $F(p^e) \geq 1$ when e is even, the lemma follows. □

Suppose now that χ is nontrivial. By partial summation,

$$\sum_{n\leq x} \frac{\chi(n)}{n} = \frac{S(x)}{x} + \int_1^x S(t)\frac{dt}{t^2}, \quad \text{where} \quad S(t) := \sum_{n\leq t} \chi(n). \tag{4.22}$$

Moreover, $S(t)$ is $O(1)$ (in fact, bounded by $\varphi(m)$). Multiplying (4.22) through by x and recalling (Lemma 4.4) that

$$L(1,\chi) - \sum_{n\leq x} \frac{\chi(n)}{n} = O\left(\frac{1}{x}\right),$$

we find that for $x \geq 2$,

$$
\begin{aligned}
xL(1,\chi) &= \int_1^x \left(\sum_{n \leq t} \chi(n) \right) \frac{x}{t^2}\, dt + O(1) \\
&= \int_1^x \left(\sum_{n \leq t} \chi(n) \right) \left\lfloor \frac{x}{t} \right\rfloor \frac{1}{t}\, dt + O(\log x) \\
&= \int_1^x \left(\sum_{n \leq t} \chi(n) \sum_{a \leq x/t} 1 \right) \frac{1}{t}\, dt + O(\log x).
\end{aligned}
$$

This integral may be rewritten as

$$\sum_{an \leq x} \chi(n) \int_n^{x/a} \frac{1}{t}\, dt = \sum_{an \leq x} \chi(n) \log \frac{x}{an} = \sum_{N \leq x} \left(\sum_{d \mid N} \chi(d) \right) \log \frac{x}{N},$$

which by Lemma 4.8 is bounded below by

$$\sum_{M \leq \sqrt{x}} \log \frac{x}{M^2} = 2 \sum_{M \leq \sqrt{x}} \log \frac{\sqrt{x}}{M} \geq 2 \log 2 \left\lfloor \frac{\sqrt{x}}{2} \right\rfloor,$$

where the final bound comes from just considering those values of $M \leq \sqrt{x}/2$. Hence

$$xL(1,\chi) \geq 2 \log 2 \left\lfloor \frac{\sqrt{x}}{2} \right\rfloor + O(\log x).$$

The right-hand side of this inequality is positive for large enough x, which is only possible if $L(1,\chi) > 0$.

7. Finishing up

Let m be a positive integer and let a be any integer coprime to m. We now know that $L(1,\chi)$ is nonvanishing for every nontrivial Dirichlet character χ modulo m. It follows from Lemma 4.5 that for every such χ,

$$\sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} = O(1).$$

We record here also the result of Lemma 4.6 that

$$\sum_{n \leq x} \frac{\chi_0(n)\Lambda(n)}{n} = \log x + O(1).$$

From the orthogonality relation (4.14), we see that

$$\sum_{\substack{n\le x\\ n\equiv a \pmod{m}}} \frac{\Lambda(n)}{n} = \frac{1}{\varphi(m)} \sum_{\chi} \overline{\chi}(a) \sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n}$$

$$= \frac{1}{\varphi(m)} \overline{\chi_0}(a) \log x + O(1) = \frac{1}{\varphi(m)} \log x + O(1), \tag{4.23}$$

since $\chi_0(a) = 1$ (because $\gcd(a, m) = 1$).

But already in the introduction we showed that

$$\sum_{\substack{p\le x\\ p\equiv a \pmod{m}}} \frac{\log p}{p} = \sum_{\substack{n\le x\\ n\equiv a \pmod{m}}} \frac{\Lambda(n)}{n} + O(1),$$

with an absolute implied constant (see (4.5)). So from (4.23),

$$\sum_{\substack{p\le x\\ p\equiv a \pmod{m}}} \frac{\log p}{p} = \frac{1}{\varphi(m)} \log x + O(1).$$

This completes the proof of (4.1) in the general case.

8. Sums of three squares

Our goal in this section is to prove the following theorem, claimed by Legendre (see [**Leg00**, Troisième Partie]) and proved by Gauss [**Gau86**, Art. 291]:

Theorem 4.9. *A natural number n can be written as the sum of three squares of integers if and only if n does not have the form $4^k(8l + 7)$ for nonnegative integers k and l.*

We first dispense with the necessity half of Theorem 4.9.

Lemma 4.10. *Suppose the positive integer n is a sum of three squares of integers. Then n is not of the form $4^k(8l + 7)$.*

Proof. Suppose n has the form $4^k(8l + 7)$ but that n is a sum of three squares, say $n = x^2 + y^2 + z^2$. Since every square is either 0 or 1 modulo 4, if 4 divides n, we must have $x^2 \equiv y^2 \equiv z^2 \equiv 0 \pmod{4}$, so that all of x, y, z are even. Thus $n/4 = (x/2)^2 + (y/2)^2 + (z/2)^2$ is also a sum of three squares. Applying this reasoning k times, we eventually find that $8l + 7$ is a sum of three squares. But this is impossible, since the congruence $x^2 + y^2 + z^2 \equiv 7 \pmod{8}$ has no solutions. □

We can therefore focus our attention on the sufficiency portion of Theorem 4.9. Our proof of this requires another of Legendre's results (see [**Leg00**, Première Partie, §IV]), of independent interest:

Theorem 4.11 (Legendre). *Suppose a, b, and c are squarefree, pairwise coprime nonzero integers, not all of the same sign. In order that there exist a nonzero solution $(x, y, z) \in \mathbf{Z}^3$ to the equation*

$$ax^2 + by^2 + cz^2 = 0 \tag{4.24}$$

it is necessary and sufficient that $-ab$ be a square modulo c, $-ac$ a square modulo b, and $-bc$ a square modulo a.

Before proving Theorem 4.11 we need the following simple but useful lemma, the proof of which is similar to an argument that appeared already in the proof of Lemma 2.19.

Say that two vectors with integer entries are congruent modulo m if every entry in their difference is a multiple of m.

Lemma 4.12 (Brauer & Reynolds [**BR51**]). *Let $A = (a_{ij})_{1\le i\le r, 1\le j\le s}$ be an $r \times s$ matrix with integer entries, and let m be a natural number. Suppose that $\lambda_1, \dots, \lambda_s$ are positive real numbers with $\lambda_1 \cdots \lambda_s > m^r$. Then there is a nonzero column vector $\mathbf{x} = (x_1, \dots, x_s)^T$ with integer entries satisfying $A\mathbf{x} \equiv \mathbf{0} \pmod{m}$ and having each $|x_i| < \lambda_i$.*

Proof. For a real number λ, let $\llbracket\lambda\rrbracket$ be the greatest integer strictly less than λ. Let $\mathbf{x} = (x_1, \dots, x_s)^T$ range over the $s \times 1$ vectors with integer entries x_i satisfying $0 \le x_i < \lambda_i$ for each $1 \le i \le s$. The number of such vectors $\mathbf{x}$ is $\prod_{i=1}^{s}(1 + \llbracket\lambda_i\rrbracket) \ge \prod_{i=1}^{s} \lambda_i > m^r$. This implies that there must be two distinct vectors of this type, say $\mathbf{x}_1$ and $\mathbf{x}_2$, for which $A\mathbf{x}_1 \equiv A\mathbf{x}_2 \pmod{m}$. The theorem follows with $\mathbf{x} := \mathbf{x}_1 - \mathbf{x}_2$. $\square$

Proof of Theorem 4.11. First we prove necessity. Suppose (x, y, z) is a nonzero solution to (4.24). Dividing (4.24) by $\gcd(x, y, z)^2$, we can assume from the start that $\gcd(x, y, z) = 1$. Considering (4.24) modulo c, we find that $ax^2 \equiv -by^2 \pmod{c}$, so that

$$(ax)^2 \equiv (-ab)y^2 \pmod{c}. \tag{4.25}$$

Moreover, y is invertible modulo c: Otherwise, there is a prime p dividing both c and y. From (4.25), this p divides ax; since $\gcd(a, c) = 1$, it follows that p divides x. But then $p^2 \mid ax^2 + by^2 = -cz^2$, and since c is squarefree, we obtain that p divides z. Thus p divides $\gcd(x, y, z)$, a contradiction. So y is invertible modulo c and from (4.25) we get $(axy^{-1})^2 \equiv -ab \pmod{c}$, so that $-ab$ is a square modulo c. The other necessary conditions are established similarly.

Now we turn to sufficiency. We claim that modulo abc, the diagonal form $ax^2 + by^2 + cz^2$ splits into linear factors. That is, there are integers A_1, B_1, C_1 and A_2, B_2, C_2 for which

$$ax^2 + by^2 + cz^2 \equiv (A_1x + B_1y + C_1z)(A_2x + B_2y + C_2z) \pmod{abc}. \tag{4.26}$$

By the Chinese remainder theorem, to prove the claim it is enough to show that a factorization of this type exists modulo each of a, b, and c. Suppose we first look modulo a. By hypothesis, we can choose an integer u with $u^2 \equiv -bc \pmod{a}$. Then, using b^{-1} to denote an integer with $b^{-1}b \equiv 1 \pmod{a}$,

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv by^2 + cz^2 \equiv b^{-1}(b^2y^2 + bcz^2) \\ &\equiv b^{-1}(by - uz)(by + uz) \equiv (y - b^{-1}uz)(by + uz) \pmod{a}, \end{aligned}$$

which is a factorization of the desired form. In exactly the same way we obtain factorizations modulo b and modulo c, proving the claim.

Since a, b, and c are not all of the same sign, we can assume $a, b > 0$ and $c < 0$. We can also assume $|abc| > 1$, since otherwise the theorem is trivial. Put $\lambda_1 := \sqrt{|bc|}$, $\lambda_2 = \sqrt{|ac|}$, and $\lambda_3 := \sqrt{|ab|}$. Since either $|bc|, |ac|$, or $|ab|$ is squarefree and > 1, not every λ_i can be an integer. Pick one that is not, and increase it slightly, without changing $\lfloor\!\lfloor \lambda_i \rfloor\!\rfloor$. Then $\lambda_1\lambda_2\lambda_3 > |abc|$, and so from Lemma 4.12 (with $r = 1$ and $s = 3$), there are integers x, y, z, not all zero, with

$$A_1x + B_1y + C_1z \equiv 0 \pmod{abc}, \quad |x| < \sqrt{|bc|}, |y| < \sqrt{|ac|}, |z| < \sqrt{|ab|}.$$

From (4.26), it follows that $ax^2 + by^2 + cz^2$ is a multiple of abc; moreover,

$$-|abc| < cz^2 \le ax^2 + by^2 + cz^2 \le ax^2 + by^2 < a|bc| + b|ac| = 2|abc|.$$

So either $ax^2 + by^2 + cz^2 = 0$ or $ax^2 + by^2 + cz^2 = |abc| = -abc$. In the first case we are done. In the second case,

$$ax^2 + by^2 + c(z^2 + ab) = 0.$$

Multiplying through by $z^2 + ab$, we find

$$0 = (ax^2+by^2)(z^2+ab)+c(z^2+ab)^2 = a(xz+by)^2+b(yz-ax)^2+c(z^2+ab)^2.$$

Moreover, this is nontrivial since $z^2+ab > 0$. So once again we are done. $\square$

The next lemma reduces our task to showing that a number n meeting the conditions of Theorem 4.9 can be written as a sum of three squares of rational numbers.

Lemma 4.13. *Suppose that the positive integer n is the sum of three squares of rational numbers. Then n is the sum of three squares of integers.*

Proof (Aubry). If n is a sum of three rational squares, then there is a point $\mathbf{a} = (a_1, a_2, a_3)$ with rational coordinates on the sphere $x^2 + y^2 + z^2 = n$. Let d be the least common denominator of a_1, a_2, a_3, so that

$$A_1 := da_1, A_2 := da_2, A_3 := da_3 \quad \text{are integers, and } \gcd(A_1, A_2, A_3, d) = 1.$$

Suppose that the rational point $\mathbf{a}$ is chosen so that d is as small as possible. We shall show that $d = 1$, so that $\mathbf{a}$ has integer coordinates, making n a sum of three integer squares.

Suppose $d > 1$. Let $\mathbf{a}' = (a_1', a_2', a_3')$ be a point of $\mathbf{Z}^3$ closest to $\mathbf{a}$, so that

$$|a_i - a_i'| \leq \frac{1}{2} \text{ for each } 1 \leq i \leq 3, \quad \text{whence} \quad \|\mathbf{a} - \mathbf{a}'\| \leq \frac{\sqrt{3}}{2} < 1. \tag{4.27}$$

Observe that

$$\|\mathbf{a} - \mathbf{a}'\|^2 = \frac{1}{d^2} \sum_{i=1}^{3} (A_i - da_i')^2,$$

while

$$\sum_{i=1}^{3} (A_i - da_i')^2 \equiv A_1^2 + A_2^2 + A_3^2 = d^2 n \equiv 0 \pmod{d}. \tag{4.28}$$

By (4.27) and (4.28),

$$\|\mathbf{a} - \mathbf{a}'\|^2 = \frac{d'}{d} \tag{4.29}$$

for some $1 \leq d' < d$. We shall exhibit a rational point on our sphere with (not necessarily least) common denominator d', contradicting the minimality of d.

This point will be the second intersection point of the line through $\mathbf{a}$ and $\mathbf{a}'$ with the sphere $x^2 + y^2 + z^2 = n$. Put $\mathbf{A} := (A_1, A_2, A_3)$. Since $\mathbf{a} - \mathbf{a}' = (\mathbf{A} - d\mathbf{a}')/d$, the line through $\mathbf{a}$ and $\mathbf{a}'$ can be parameterized by a real parameter λ as

$$\mathbf{a}' + \lambda(\mathbf{A} - d\mathbf{a}').$$

Setting the squared norm of this vector equal to n gives the equation

$$\|\mathbf{a}'\|^2 - n + 2\lambda(\mathbf{a}' \cdot \mathbf{A} - d\|\mathbf{a}'\|^2) + \|\mathbf{A} - d\mathbf{a}'\|^2 \lambda^2 = 0.$$

This is a quadratic equation in λ. We know already that $\lambda = 1/d$ is a root; this corresponds to the point $\mathbf{a}$ on the sphere. Since the roots multiply to

$$\frac{\|\mathbf{a}'\|^2 - n}{\|\mathbf{A} - d\mathbf{a}'\|^2},$$

the root corresponding to the other intersection point is (by (4.29))

$$\lambda = d\frac{\|\mathbf{a}'\|^2 - n}{\|A - d\mathbf{a}'\|^2} = d\frac{\|\mathbf{a}'\|^2 - n}{d'd} = \frac{\|\mathbf{a}'\|^2 - n}{d'}.$$

Thus λ can be written as a fraction with denominator $d' < d$, which implies that the same is true for the coordinates of the corresponding intersection point $\mathbf{a}' + \lambda(\mathbf{A} - d\mathbf{a}')$. $\square$

We now complete the proof of sufficiency.

Lemma 4.14. *Every positive integer not of the form $4^k(8l+7)$ is a sum of three squares.*

Proof. It is enough to prove that every squarefree positive integer $m \not\equiv 7 \pmod 8$ is a sum of three squares. Indeed, suppose this special case is proven, and let n be a positive integer not of the form $4^k(8l+7)$. We can write $n = 2^{2k}a^2m$, where $k \geq 0$, a is odd and m is squarefree. The hypothesis on n implies that

$$m \equiv a^2m \not\equiv 7 \pmod 8.$$

Thus m is a sum of three squares. Since n is a square multiple of m, it follows that n is also a sum of three squares.

To prove this special case we will construct a squarefree positive integer r relatively prime to m with the properties that

(i) r is a sum of two integer squares,

(ii) m is a square modulo r and $-r$ is a square modulo m.

For this r, Legendre's theorem implies that there is are integers x, y, and z, not all zero, with

$$mx^2 - y^2 - rz^2 = 0.$$

If $x = 0$, then $y^2 + rz^2 = 0$. But then also $y = z = 0$, which is a contradiction. So $x \neq 0$, and we can divide through by x^2 to find

$$m = (y/x)^2 + r(z/x)^2.$$

We are supposing that $r = r_1^2 + r_2^2$ for integers r_1 and r_2, and thus

$$m = (y/x)^2 + (r_1z/x)^2 + (r_2z/x)^2.$$

So m is a sum of three rational squares. By Lemma 4.13, m is also a sum of three integer squares.

It remains to construct a suitable value of r. Write $m = 2^e m_1$ where $e = 0$ or 1 and $m_1 = p_1 \cdots p_k$ is odd. Put

$$\beta := \begin{cases} 0 & \text{if } e = 1, \text{ or if } e = 0 \text{ and } m_1 \equiv 1 \pmod 4, \\ 1 & \text{if } e = 0 \text{ and } m_1 \equiv 3 \pmod 8. \end{cases}$$

Use Dirichlet's theorem to pick a prime q with

$$\left(\frac{q}{p_i}\right) = \left(\frac{-2^\beta}{p_i}\right) \quad \text{for all } 1 \leq i \leq k,$$

$$\text{and} \quad q \equiv \begin{cases} 1 \pmod 8 & \text{if } m_1 \equiv 1 \pmod 4, \\ 5 \pmod 8 & \text{if } m_1 \equiv 3 \pmod 4. \end{cases}$$

(These conditions can be enforced by picking q from a suitable residue class modulo $8\prod p_i = 8m_1$.) We put $r := 2^\beta q$. Then classical results of Euler show that r can be written as a sum of two squares. Now $(q,m)=1$; moreover, $\beta>0$ only when m is odd. Thus r is coprime to m. Moreover, since $q\equiv 1 \pmod 4$,

$$\begin{aligned}\left(\frac{m}{q}\right) = \left(\frac{2^e}{q}\right)\left(\frac{m_1}{q}\right) = \left(\frac{2^e}{q}\right)\left(\frac{q}{m_1}\right) = \left(\frac{2^e}{q}\right)\prod_{i=1}^{k}\left(\frac{q}{p_i}\right)\\ = \left(\frac{2^e}{q}\right)\prod_{i=1}^{k}\left(\frac{-2^\beta}{p_i}\right) = \left(\frac{2^e}{q}\right)\left(\frac{-2^\beta}{m_1}\right) = 1.\end{aligned}$$

(The last equality requires some checking of cases, depending on whether $e=0$ or 1 and whether $m_1\equiv 1$ or $3 \pmod 4$.) Hence m is a square modulo q. Since m is trivially a square modulo 2^β, we have by the Chinese remainder theorem that m is a square modulo $r=2^\beta q$. Moreover,

$$\left(\frac{-r}{p_i}\right) = \left(\frac{-2^\beta q}{p_i}\right) = \left(\frac{-2^\beta}{p_i}\right)\left(\frac{q}{p_i}\right) = \left(\frac{-2^\beta}{p_i}\right)^2 = 1.$$

By the Chinese remainder theorem, it follows that $-r$ is a square modulo $\prod p_i = m_1$. Since $-r$ is trivially a square modulo 2^e, we have that $-r$ is also a square modulo $2^e m_1 = m$, as desired. □

Notes

The proof of Dirichlet's theorem given here is a variant due to Gelfond [**Gel56**] of an argument of Shapiro ([**Sha50**], see also [**Sha83**, Chapter 9]). For the most part, our treatment follows that of Gelfond & Linnik [**GL66**, §3.2], but the slick proof of the nonvanishing of $L(1,\chi)$ for real χ is due to Yanagisawa [**Yan98**]. A very different elementary proof of Dirichlet's theorem was given by Selberg [**Sel49a**]. An excellent presentation of the usual complex-analytic proof can be found in the textbook of Ireland & Rosen [**IR90**, Chapter 16]. For a discussion of Dirichlet's original argument, and in particular his remarkable *class number formula*, see the beautiful text of Scharlau & Opolka [**SO85**, Chapter 8].

For certain small moduli it is possible to prove Dirichlet's theorem by arguments analogous to those offered for Chebyshev's theorems in Chapter 3. See, e.g., Bang [**Ban91, Ban37**], Ricci [**Ric33, Ric34**], and Erdős [**Erd35e**]. Erdős's method, which is the most comprehensive, applies to any modulus m for which $\sum_{p\nmid m, p<m} p^{-1} < 1$. (This inequality has only finitely many solutions, the largest being $m=840$, as shown by Moree [**Mor93**].)

Shiu [**Shi00**] has established the following handsome strengthening of Dirichlet's theorem: *If a and m are integers with $m>0$ and $\gcd(a,m)=1$, then for every $k\in\mathbf{N}$ the sequence of primes contains k consecutive terms* *each congruent to a modulo m.* So, for example, there are 10^{100} consecutive primes each of which terminates in the decimal digit “1”.

Recent deep work of Green, Tao, and Ziegler [**GT10, GTZ11**] yields the following multidimensional version of Dirichlet's theorem: Fix an $m \times n$ matrix A with integer entries and a vector $\mathbf{v} \in \mathbf{Z}^m$. Suppose that no two rows of A are linearly dependent. If $A\mathbf{x}$ has all positive entries for some $\mathbf{x} \in \mathbf{N}^n$, and there are no local obstructions (see §1.5), then there are infinitely many vectors $\mathbf{x} \in \mathbf{N}^n$ with the property that all of the entries of $A\mathbf{x} + \mathbf{v}$ are prime. Taking

$$A = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & m-1 \end{bmatrix}^T \quad \text{and} \quad \mathbf{v} = \mathbf{0},$$

we recover the earlier Green–Tao result [**GT08**] that the primes contain arbitrarily long arithmetic progressions. Moreover, the Green–Tao–Ziegler work shows that the count of vectors $\mathbf{x}$ as above agrees with what is expected from the heuristic philosophy of §3.5.

Our proof of Theorem 4.9 characterizing sums of three squares is due to Wójcik [**Wój72**]. The proof of Legendre's Theorem 4.11 is based on the treatment of LeVeque [**LeV96**, Chapter 8]. From a modern perspective, Legendre's theorem is the first nontrivial case of the following important result of Hasse and Minkowski: *If Q is any quadratic form with rational coefficients, then Q has a nontrivial zero over $\mathbf{Q}$ precisely when Q has a nontrivial zero over $\mathbf{R}$ and every p-adic field $\mathbf{Q}_p$.* The Hasse–Minkowski theorem can be used to give a quick proof of Theorem 4.9; see the appendix to [**Ser73**, Chapter IV].

In his *Disquisitiones*, Gauss determined the precise number of representations of an arbitrary natural number as a sum of three squares. For a natural number n, let $r_3(n)$ be the number of triples $(x, y, z) \in \mathbf{Z}^3$ with $x^2 + y^2 + z^2 = n$, and let $R_3(n)$ be the number of such triples with $\gcd(x, y, z) = 1$. It is easy to see that $r_3(n) = \sum_{d^2 \mid n} R_3(n/d^2)$. Gauss showed that $R_3(1) = 6$, $R_3(2) = 12$, $R_3(3) = 8$, and for $n > 3$,

$$R_3(n) = \begin{cases} 12h(-4n) & \text{if } n \equiv 1 \text{ or } 2 \pmod 4, \\ 24h(-n) & \text{if } n \equiv 3 \pmod 8, \\ 0 & \text{otherwise.} \end{cases}$$

Here $h(D)$ is the number of classes of primitive binary quadratic forms of discriminant D — explicitly, $h(D)$ is the number of solutions in integers a, b, and c to $b^2 - 4ac = D$, subject to the constraints that

$$a > 0 \text{ and } c > 0, \quad \gcd(a, b, c) = 1, \quad \text{and}$$
$$|b| \le a \le c, \text{ with } b \ge 0 \text{ if either } |b| = a \text{ or } a = c$$

(cf. [**Gau86**, Art. 291], [**Ven70**, Chapter 4, §16]). For $r_3(n)$ itself one has the following complicated explicit description: Let $T(n)$ denote the number of triples of positive integers d, δ, δ' where d, δ, and δ' are all odd, $d + \delta \equiv 0 \pmod 4$, and $4n + 1 = d\delta + (d + \delta \pm 2)\delta'$ for some choice of sign. Then

$$r_3(n) = \begin{cases} 3T(n) & \text{if } n \equiv 1 \text{ or } 2 \pmod 4, \\ 2T(n) & \text{if } n \equiv 3 \pmod 8, \\ r_3(n/4) & \text{if } n \equiv 0 \pmod 4, \\ 0 & \text{if } n \equiv 7 \pmod 8. \end{cases} \tag{4.30}$$

In Chapter XIII of the classic text of Uspensky & Heaslet [**UH39**], one can find a a completely elementary proof of (4.30) based on certain remarkable identities of Liouville.

Exercises

1. Show that if a and m are integers with $m > 0$ and $\gcd(a, m) = 1$, then for $x \geq 3$,
$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{m}}} \frac{1}{p} = \frac{1}{\varphi(m)} \log\log x + C_{a,m} + O_m(1/\log x),$$
where $C_{a,m}$ is a constant depending on a and m.
2. (Sylvester) Show that for complex z with $|z| < 1$,
$$\sum_{\substack{n \geq 1 \\ p \mid n \Rightarrow p \equiv 3 \pmod{4}}} \mu(n) \frac{z^n}{1 - z^{2n}} = \sum_{\substack{m \geq 1 \\ p \mid m \Rightarrow p \equiv 1 \pmod{4}}} z^m.$$
Suppose that there are only finitely many primes $p \equiv 3 \pmod{4}$. Setting $z = iy$ and letting y tend to 1 from below, show that the left-hand side of this identity tends to a limit while the right-hand side "blows up" (has absolute value tending to infinity).
3. Let $\mathscr{P}$ be a set of primes. Suppose that
$$\sum_{p \leq x, p \in \mathscr{P}} \frac{\log p}{p} = \kappa \log x + O_{\mathscr{P}}(1)$$
for some constant $\kappa > 0$ and every $x \geq 2$.
   (a) Show that for some constant $D > 1$, there are $\gg x/\log x$ elements of $\mathscr{P}$ in the interval $(x, Dx]$ for every $x \geq 2$.
   (b) Put $\pi_{\mathscr{P}}(x) := \#\{p \leq x : p \in \mathscr{P}\}$. Using the result of (a), show that $\pi_{\mathscr{P}}(x) \gg_{\mathscr{P}} x/\log x$ as $x \to \infty$.
   (c) Show that if $\lim_{x \to \infty} \frac{\pi_{\mathscr{P}}(x)}{x/\log x}$ exists, then it equals κ.
4. Show that under the hypotheses of Exercise 3, there is a positive constant $C = C(\mathscr{P})$ for which
$$\prod_{p \leq x, p \in \mathscr{P}} \left(1 - \frac{1}{p}\right) = \frac{C}{(\log x)^{\kappa}} \left(1 + O\left(\frac{1}{\log x}\right)\right)$$
for $x \geq 2$. Here the implied constant may depend on $\mathscr{P}$.

   Remark. When $\mathscr{P}$ is the set of primes $p \equiv a \pmod{m}$ (so that $\kappa = 1/\varphi(m)$), Languasco & Zaccagnini [**LZ07**] have shown that C is the positive solution to
$$C^{\varphi(m)} = e^{-\gamma} \prod_{p} (1 - 1/p)^{\alpha(p;m,a)},$$

where $\alpha(p;m,a) := \varphi(m)-1$ if $p \equiv a \pmod m$ and $\alpha(p;m,a) = -1$ otherwise.

5. Suppose that $\chi\colon \mathbf{Z} \to \mathbf{C}$ has the following three properties:
   (i) χ is periodic with period m,
   (ii) χ is completely multiplicative,
   (iii) $\chi(n) = 0$ if and only if $\gcd(n,m) > 1$.
   Show that χ is a Dirichlet character modulo m.
6. Let G be a finite abelian group and let $\mathbf{C}[G]$ denote the space of functions $f\colon G \to \mathbf{C}$. For $\phi, \psi \in \mathbf{C}[G]$, define
$$(\phi,\psi) = \frac{1}{|G|}\sum_{g\in G}\phi(g)\overline{\psi(g)}.$$
   Show that this is a scalar product on $\mathbf{C}[G]$. Using (4.11) show that the characters of G form an orthonormal basis for $\mathbf{C}[G]$. This explains the name “orthogonality relation”.
7. Let G be a finite abelian group of order n with elements $g_1, g_2, \dots, g_n$ and characters $\chi_1, \chi_2, \dots, \chi_n$. Define the matrix
$$M := \begin{pmatrix} \chi_1(g_1) & \chi_1(g_2) & \dots & \chi_1(g_n) \\ \chi_2(g_1) & \chi_2(g_2) & \dots & \chi_2(g_n) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_n(g_1) & \chi_n(g_2) & \dots & \chi_n(g_n) \end{pmatrix}.$$
   Let M^* denote the conjugate-transpose of M. Using (4.11), show that $MM^* = nI$, where I is the $n\times n$ identity matrix. Linear algebra implies that $M^*M = nI$ as well. Deduce from this that (4.12) holds. That is, the first orthogonality relation implies the second.
8. Let m be a natural number. By an *additive character modulo* m, we mean a function $\psi\colon \mathbf{Z} \to \mathbf{C}^\times$ which is periodic modulo m and which satisfies $\psi(a+b) = \psi(a)\psi(b)$ for every pair of integers a and b. (Equivalently, ψ is a function on $\mathbf{Z}$ induced from a character of the additive group $\mathbf{Z}/m\mathbf{Z}$.) For each real θ, define $e(\theta) := e^{2\pi i\theta}$. Show that for each integer r, the function $\psi_r(n) := e(rn/m)$ is an additive character modulo m. Then show that each additive character mod m arises in this way from some choice of r, with r uniquely determined modulo m.
9. (Sylvester, [**Syl88**]) Let f be a nonnegative, multiplicative arithmetic function. Let χ be a nontrivial character modulo m, and define the arithmetic function g by setting $g(n) := \sum_{d\mid n}\chi(d)f(n/d)$. Using only the convergence of $L(1,\chi)$ (and *not* its nonvanishing), prove that
$$\left|\sum_{n\le x}\frac{g(n)}{n}\right| \ll \prod_{p\le x}\left(1+\frac{f(p)}{p}+\frac{f(p^2)}{p^2}+\cdots\right),$$

where the implied constant depends at most on m.

10. (Continuation) Let χ be a nontrivial real Dirichlet character modulo m. Show that there is a unique choice of f in the preceding exercise with the property that the induced function g is identically 1. Show, moreover, that this f is nonnegative and multiplicative, and that for each prime p and each $k \geq 1$ we have
$$f(p^k) = \begin{cases} 1 & \text{if } \chi(p) = 0, \\ 0 & \text{if } \chi(p) = 1, \\ 2 & \text{if } \chi(p) = -1. \end{cases}$$
Deduce from the preceding exercise that
$$\sum_{\substack{p \leq x \\ \chi(p) = -1}} \frac{1}{p} \geq \frac{1}{2} \log\log x + O(1).$$
As a special case, we see that the sum of the reciprocals of the primes from the residue class 3 mod 4 diverges at least as fast as $\frac{1}{2}\log\log x$.

† 11. (Mertens [**Mer97**]) Suppose that a and m are integers with $m > 0$ and $\gcd(a, m) = 1$.
   (a) Show that if χ is a character modulo m and $x \geq 4$, then
   $$\sum_{d \leq x} \frac{\chi(d)\Lambda(d)}{d} = \begin{cases} \log x + O\left(1 + \sum_{p \mid m} \frac{\log p}{p-1}\right) & \text{if } \chi = \chi_0, \\ O(m|L(1,\chi)|^{-1}) & \text{if } \chi \neq \chi_0, \end{cases}$$
   where the implied constants are absolute.
   (b) Put $M = \sum_{\chi \neq \chi_0} |L(1,\chi)|^{-1}$, where the sum is over all nontrivial Dirichlet characters modulo m. Show that
   $$\sum_{p \leq x} \frac{\log p}{p} = \frac{1}{\varphi(q)} \log x + O\left(M + 1\right),$$
   again with an absolute implied constant.
   (c) By splitting the sum defining $L(1,\chi)$ at $n = m$, show that $L(1,\chi) \ll \log m$ for each nontrivial character χ, so that $M \gg \varphi(m)/\log m$. (Again, both implied constants are supposed to be absolute.)
   (d) Deduce that there is an absolute positive constant C with the property that for every $x \geq 4$, there is a prime $p \equiv a \pmod{m}$ in the interval $[x, x\exp(CmM)]$.

Remark. Let $p(m,a)$ be the least prime $p \equiv a \pmod{m}$. From (d) we have that $p(m,a) \ll \exp(CmM)$. Unfortunately, from (c) this upper bound is quite large, at least $\exp(m^{2+o(1)})$. See Révész [**Rév80**] for an elementary proof that $p(m,a) \ll \exp(cm(\log m)^{11})$ for an absolute constant $c > 0$.

A deep result of Linnik asserts that $p(m,a) \ll m^L$ for an absolute constant L. Heath-Brown has shown [**HB92**] that one may take $L = 5.5$. The so-called Extended Riemann Hypothesis (which asserts that all the "nontrivial" zeros of the functions $L(s,\chi)$ lie on the line $\Re(s) = 1/2$) would imply that $p(m,a) < 2m^2(\log m)^2$ (see [**BS96**]).

12. (Sierpiński [**Sie62**]) Suppose that a and m are coprime integers with $m > 0$. Prove that for every $s \in \mathbf{N}$, there are infinitely many natural numbers $n \equiv a \pmod{m}$ with exactly s prime divisors (counted with multiplicity).
13. (Schinzel [**Sch59**]) Prove that there are no congruence obstructions to the Goldbach conjecture. That is, show that if n is an even integer and m is a (positive) modulus, then the congruence $n \equiv p + q \pmod{m}$ is always solvable in primes p and q.
14. (Sierpiński [**Sie48**]) Prove that for each $M \in \mathbf{N}$, there are infinitely many primes p for which all of $p \pm i$, $i = 1, 2, \ldots, M$, are composite.

† 15. (Powell, Israel [**Isr83**]) Let m and n be natural numbers with $m > 1$. Show that if $(m,n) \neq (2,1)$, then $m^p - n$ is composite for infinitely many primes p.

† 16. (Newman [**New97**]; see also Aldaz et al. [**ABGU01**]) Dov Jarden, in his book *Recurring Sequences* (1973), observed that $\varphi(30n+1) > \varphi(30n)$ for all $n \leq 10,000$.

Prove that contrary to what one might expect from the computational evidence, the reverse inequality,

$$\varphi(30n+1) < \varphi(30n), \tag{4.31}$$

holds for infinitely many n. *Hint*: Consider large primes n for which $30n+1$ has many small prime factors.

Remark. The smallest solution to (4.31), which has over 1000 decimal digits, has been given explicitly by Martin [**Mar99**].

17. This exercise illustrates the utility of (4.1) as an equidistribution statement. Define $n^\diamond$ as that portion of $n!$ composed of primes congruent to 3 (mod 4), i.e., $n^\diamond := \prod_{p^k \| n!, p \equiv 3 \pmod 4} p^k$.
    (a) Using (4.1), show that $\log n^\diamond \sim \frac{1}{2}\log n!$. *Hint:* First show that if p is prime, then $p^k \parallel n!$ for $k = \sum_{i \geq 1} \lfloor n/p^i \rfloor$.
    (b) Suppose that n and y are positive integers with $n! + 1 = y^8$. Using the factorization
    $$n! = y^8 - 1 = \left((y^4+1)(y^2+1)\right)(y^2-1),$$
    prove that $n^\diamond \leq y^2 - 1 \leq (n!)^{1/4}$. Deduce from part (a) that the equation $n! + 1 = y^8$ has only finitely many solutions.

(c) Show that the equation $n! + 1 = x^p$ has at most finitely many solutions (n, x) for each fixed odd prime p.
In combination with the result of (b), this shows that $n! + 1 = x^m$ has only finitely many solutions for each positive integer $m > 1$ except possibly for $m = 2$ and $m = 4$.

Remark. It has been shown that $n! + 1 = y^m$ has *no* solutions for any $m > 2$. See [**EO37**] for the case $m \neq 4$ and [**PS73**] for the case $m = 4$. When $m = 2$, an 1885 conjecture of Brocard asserts that the only solutions correspond to $n = 4, 5$ and 7, but even showing there are at most finitely many solutions remains open.

18. (Continuation; Dąbrowski [**Dąb96**]) Show that if $A \in \mathbf{Z}$ is not a perfect square, then the equation $n! + A = y^2$ has only finitely many integral solutions.

† 19. (Chebyshev, Nagell [**Nag22**, §1]) For each $x \geq 1$, put
$$N_x := \prod_{n \leq x} (n^2 + 1).$$
(a) Show that $\log N_x = 2x \log x + O(x)$.
(b) For each prime p, define $e(p, x)$ by the relation $p^{e(p,x)} \parallel N_x$. Show that
$$e(p, x) \leq \begin{cases} x/2 + O(1) & \text{if } p = 2, \\ 2x/(p-1) + O(\log x/\log p) & \text{if } p \equiv 1 \pmod 4, \\ 0 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$
(c) Show that there is a constant $c > 0$ with the property that the largest prime factor p_x of N_x satisfies $p_x > cx \log x$ for all large x. Conclude that there are infinitely many $n \in \mathbf{N}$ for which $n^2 + 1$ has a prime factor $> cn \log n$. This can be considered an approximation to the conjecture that $n^2 + 1$ is prime infinitely often.

Remark. Deshouillers & Iwaniec [**DI82**], building on earlier work of Hooley, have shown that $p_x > x^{\theta + o(1)}$ infinitely often, where θ is a constant slightly larger than $6/5$.

† 20. (Continuation; Cilleruelo [**Cil08**]) Show that if $e(p, x) \geq 2$, then $p \leq 2x$. Deduce that N_x assumes only finitely many squarefull values for $x \geq 1$. (With a bit more work, it can be shown that $10^2 = (1^2+1)(2^2+1)(3^2+1)$ is the only such value.)

† 21. (Cf. Tulyaganova [**Tul83**])
(a) Show that $p := 2x + 5y + 14$ and $q := 3x - 2y + 1$ are simultaneously prime for infinitely many pairs $(x, y) \in \mathbf{Z}^2$.

(b) Prove the following strengthening of the claim in (a): For every constant C, there is a pair $(x, y) \in \mathbf{Z}^2$ for which both p and q are prime and $p, q > C$.

22. (C. Pomerance; see also Lamzouri et al. [**LPZ11**]) Let $\Phi(N)$ denote the number of *Farey fractions of order* N; in other words, $\Phi(N)$ is the number of reduced fractions $0 \le \frac{a}{b} \le 1$ with denominator $b \le N$. It is not hard to see that

$$\Phi(N) = 1 + \sum_{k=1}^{N} \varphi(k).$$

The first few values of Φ are

$$2, 3, 5, 7, 11, 13, 19, 23, 29, 33, 43, 47, 59, 65, 73, 81, 97, \dots.$$

Probably there are infinitely many primes in the sequence $\{\Phi(N)\}_{N=1}^{\infty}$, but this is presumably very hard. In this exercise we outline a proof that the sequence $\{\Phi(N)\}_{N=1}^{\infty}$ hits every residue class modulo 3 infinitely often. In particular, there are infinitely many composite terms in this sequence.

(a) Let χ be the nontrivial Dirichlet character modulo 3. For real values of x, put $D(x) := \sum_{n \le x} \chi(\varphi(n))$. Show that if some residue class modulo 3 contains only finitely many of the terms $\Phi(N)$, then $D(x)$ is absolutely bounded.

(b) Put $L(s) := \sum_{n=1}^{\infty} \frac{\chi(\varphi(n))}{n^s}$. Show that for real $s > 1$, one has

$$L(s) = \left(1 - \frac{1}{3^s}\right) \prod_{p \equiv 2 \pmod 3} \left(1 + \frac{1}{p^s + 1}\right).$$

(c) Conclude from (b) and the divergence of the series $\sum_{p \equiv 2 \pmod 3} \frac{1}{p}$ that $L(s)$ tends to infinity as s tends to 1 from above.

(d) Use the result of (c) to show that for each $\delta < 1$, there are arbitrarily large values of x with $D(x) > x^{\delta}$. In particular, $D(x)$ is not absolutely bounded.

Remark. The author does not know any proof of the analogous result for residue classes modulo 5, or even a proof that 5 divides infinitely many of the terms $\Phi(N)$.

† 23. Let p be a prime, and let $\zeta_p := e^{2\pi i/p}$, so that ζ_p is a complex primitive pth root of unity. For each nontrivial character χ modulo p, define the *Gauss sum* $\tau(\chi)$ by setting

$$\tau(\chi) := \sum_{n=1}^{p-1} \chi(n) \zeta_p^n$$

(cf. Exercise 2.10, where certain analogous quantities were defined in positive characteristic).

(a) Show that $\tau(\chi)\overline{\tau(\chi)} = p$, so that $|\tau(\chi)| = \sqrt{p}$. You may wish to consult the hint to Exercise 2.10(a).

(b) For each integer a, define $\tau_a(\chi) := \sum_{n=1}^{p-1} \chi(n)\zeta_p^{an}$. (Thus $\tau(\chi) = \tau_1(\chi)$.) Show that $\tau_a(\chi) = \overline{\chi}(a)\tau(\chi)$.

(c) Deduce from the result of (b) that for each natural number N and each nontrivial character χ,

$$\tau(\overline{\chi}) \sum_{a \le N} \chi(a) = \sum_{n=1}^{p-1} \overline{\chi}(n) \sum_{a \le N} \zeta_p^{an}.$$

Show that the right-hand inner sum has absolute value $\frac{|\sin \frac{\pi N n}{p}|}{|\sin \frac{\pi n}{p}|}$.

(d) Check that if $|\theta| \le 1/2$, then $|\sin \pi\theta| \ge 2|\theta|$. Use this to prove the *Pólya–Vinogradov inequality*: For every N,

$$\left| \sum_{a \le N} \chi(a) \right| < \sqrt{p} \log p.$$

† 24. (Continuation) Let p be a prime.

(a) Suppose that d divides $p-1$. Show that for a coprime to p,

$$\frac{1}{d} \sum_{\chi^d = \chi_0} \chi(a) = \begin{cases} 1 & \text{if } a \text{ is a } d\text{th power residue modulo } p, \\ 0 & \text{otherwise.} \end{cases}$$

Here the sum on the left is extended over all characters modulo p whose dth power is the trivial character. *Hint:* The characters with $\chi^d = \chi_0$ can be identified in a natural way with the characters on the group $\mathbf{F}_p^\times/(\mathbf{F}_p^\times)^d$.

(b) Deduce from the Pólya–Vinogradov inequality that if I is a finite interval of measure $\mu(I)$, then the number of dth power residues in I is $\mu(I)/d + O(p^{1/2}\log p)$. (Thus if $\mu(I)$ is significantly larger than $dp^{1/2}\log p$, then I contains roughly the expected number of dth power residues.)

(c) Show that for a coprime to p,

$$\sum_{e \mid p-1} \frac{\mu(e)}{e} \sum_{\chi^e = \chi_0} \chi(a) = \begin{cases} 1 & \text{if } a \text{ is a primitive root modulo } p, \\ 0 & \text{otherwise.} \end{cases}$$

(d) Prove that for each finite interval I, the number of primitive roots contained in I is

$$\mu(I)\frac{\varphi(p-1)}{p-1} + O(2^{\omega(p-1)} p^{1/2} \log p).$$

As a special case, conclude that if we let $g(p)$ denote the least positive primitive root modulo p, then for each $\epsilon > 0$, we have $g(p) \ll_\epsilon p^{1/2+\epsilon}$.

Remark. Burgess [**Bur62**] has shown that $g(p) \ll_\epsilon p^{1/4+\epsilon}$ for each $\epsilon > 0$, which is the best known unconditional upper bound. The Extended Riemann Hypothesis implies (see [**Sho92**]) that $g(p) \ll (\log p)^6$, and it is conjectured that $g(p) \ll_\epsilon (\log p)^{1+\epsilon}$ for each $\epsilon > 0$. In the opposite direction, there are infinitely many primes p for which $g(p) \gg (\log p)(\log\log\log p)$; in fact, the same lower bound holds for the least positive quadratic nonresidue mod p [**GR90**].

25. By imitating the proof of Lemma 4.13, show that if the positive integer n is a sum of two squares of rational numbers, then it is a sum of two squares of integers. Use this and Theorem 4.11 to show that every prime $p \equiv 1 \pmod 4$ is a sum of two squares.
26. (Gauss [**Gra84**, Entry 18], [**Gau86**, Art. 293]) Show that every nonnegative integer n can be written as a sum of three triangular numbers. (Here a *triangular number* is a number of the form $k(k+1)/2$, where k is a nonnegative integer.)
27. Prove that the set of positive integers expressible as a sum of three squares has asymptotic density $5/6$.
28. (Turski [**Tur33**]) Prove that every positive integer is the sum of at most 10 odd squares and that infinitely many require 10.
29. Show that every nonnegative integer n can be written as the sum of four squares of integers, where one of the integers belongs to the set $\{0\} \cup \{2^k : k = 0, 1, 2, \dots\}$.
30. (Sierpiński; extracted from [**Sie88**, Chapter XI]) Let m be an odd positive integer.
    (a) Prove that m can be written as a sum of four squares of integers with two of the integers equal.
    (b) Prove that m can be written as a sum of four squares of integers with two of the integers consecutive.

    Suggestions: For (a), write $2m = x^2 + y^2 + z^2$. Show that we can assume that x and y are odd while z is even. Verify that $m = ((x+y)/2)^2 + ((x-y)/2)^2 + (z/2)^2 + (z/2)^2$.

    For (b), start by writing $2m - 1 = x^2 + y^2 + z^2$. Show that after a rearrangement we can assume x and y are even while $z = 2c+1$ is odd. Now use the identity $c^2 + (c+1)^2 = \frac{1}{2}\left((2c+1)^2 + 1\right)$.

† 31. (Lemmermeyer) In a letter to Goldbach dated June 9, 1750, Euler conjectured that every odd natural number n could be written in the form $x^2 + y^2 + z^2 + w^2$ for integers x, y, z, and w satisfying $x + y + z + w = 1$.

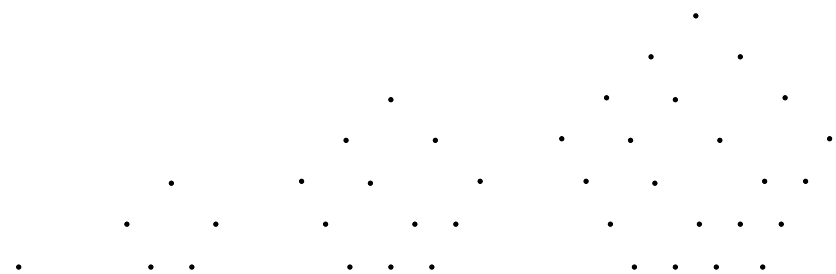

Figure 1. Pictorial representation of the first few nonzero $(m+2)$-gonal numbers when $m = 3$. In this case the jth step in the construction corresponds to adding $1 + 3j$ dots.

Show that Euler's conjecture is equivalent to the result that every positive integer $\equiv 3 \pmod 8$ is a sum of three squares. *Hint:* Put $n = 2m+1$, and consider the equation $2m + 1 = x^2 + y^2 + z^2 + (1 - (x + y + z))^2$. Multiply both sides by 4, subtract 1, and express the right-hand side as a sum of three squares.

32. For each natural number m, the sequence of $(m + 2)$-*gonal numbers* is the sequence with kth term
$$p_m(k) := \sum_{0 \leq j < k} (1 + mj) = \frac{mk^2 - (m-2)k}{2},$$
indexed starting at $k = 0$. Figure 1 explains the geometric origin of the terminology. When $m = 1$ we recover the triangular numbers of Exercise 26, and when $m = 2$ we recover the familiar sequence of square numbers. Fermat recorded the following claim in his copy of Diophantus's *Arithmetica*:

> Every number is either a triangular number or the sum of two or three triangular numbers; every number is a square or the sum of two, three, or four squares; every number is a pentagonal number or the sum of two, three, four or five pentagonal numbers; and so on *ad infinitum*, for hexagons, heptagons, and any polygons whatever ... The proof, which depends on many various and abstruse mysteries of numbers, I cannot give here...

This statement is true; however, no record survives of Fermat's proof. The first published proof of the *polygonal number theorem*, as it has come to be called, is due to Cauchy [**Cau15**]. The argument is technical for uninteresting reasons, and we do not give it here. We can, however, sketch a proof of the following related theorem of Legendre (see [**Leg00**, Sixième Partie, §II]):

★ **Theorem 4.15.** *Fix a natural number m. If m is odd, then every large enough natural number n is a sum of four $(m+2)$-gonal numbers. If m is even, then every large enough n is a sum of five polygonal numbers of order $m+2$, one of which is either 0 or 1.*

Our sketch is based on [**Nat96**, Chapter 1], which also contains a proof of the polygonal number theorem.

The first step towards Theorem 4.15 is proving "Cauchy's lemma": *If a and b are odd positive integers with $3a \le b^2 \le 4a$, then there are nonnegative integers s, t, u, and v with*

$$s+t+u+v = b \quad \text{and} \quad s^2+t^2+u^2+v^2 = a.$$

Proceed as follows:

(a) Deduce from Theorem 4.9 that we can write $4a - b^2 = x^2 + y^2 + z^2$ where x, y, and z are odd integers.

(b) Show that one can choose the signs of x, y, and z in (a) so that

$$s := \frac{b+x+y+z}{4}, \quad t := \frac{b+x-y-z}{4},$$
$$u := \frac{b-x+y-z}{4}, \quad v := \frac{b-x-y+z}{4}$$

are all integers. Check that $s+t+u+v = b$ and $s^2+t^2+u^2+v^2 = a$.

(c) Show that $|x| + |y| + |z| \le b$ and conclude that each of s, t, u, and v is nonnegative.

33. (Continuation) We can suppose for the proof of Theorem 4.15 that $m > 1$, by Exercise 26. Suppose also that m is odd.
    (a) Show that if $n \ge 120m^3$, then there is an odd natural number b with $b \equiv n \pmod{m}$ and $\sqrt{7n/m} \le b \le \sqrt{8n/m}$.
    (b) With b as in (a), put $a := 2\frac{n-b}{m} + b$. (Thus $a \equiv b \equiv 1 \pmod 2$.) Show that (still under the assumption $n \ge 120m^3$) $3a \le b^2 \le 4a$.
    (c) Choose s, t, u, v as in Cauchy's lemma to correspond to the integers a and b. Show that

    $$n = p_m(s) + p_m(t) + p_m(u) + p_m(v).$$

    Thus every natural number $n \ge 120m^3$ is a sum of four polygonal numbers of order $m+2$.

34. (Continuation) Suppose now that m is even. Show that (a)–(c) of the preceding exercise remain correct if we make the extra assumption that n is odd. Now complete the proof of Theorem 4.15.

Remark. Legendre (cf. [**Nat87b**]) actually proved a little bit more than Theorem 4.15: He showed that if $4 \mid m$, then every large enough n is a sum of four polygonal numbers of order $m+2$, while if $2 \parallel m$, then every large enough $n \equiv 2 \pmod 4$ is such a sum. For hexagonal numbers (corresponding to $m = 4$), Duke (see [**Duk97**]) has shown that actually three such numbers suffice for large n; this is easily seen to be best-possible in this case. Some recent results and conjectures in the spirit of Cauchy's polygonal number theorem are discussed by [**Sun**] (see also [**Sun07, GPS07, OS09, KS10, CO09**]).

Interlude: A Proof of the Hilbert–Waring Theorem

Every integer is a cube or the sum of at most nine cubes; every integer is also the square of a square, or the sum of up to nineteen such, and so forth. – E. Waring [**War91**]

It would hardly be possible for me to exaggerate the admiration which I feel for the solution of this historic problem... Within the limits which it has set for itself, it is absolutely and triumphantly successful, and it stands with the work of Hadamard and de la Vallée-Poussin, in the theory of primes, as one of the landmarks in the modern history of the theory of numbers. – G. H. Hardy [**Har20**] on Hilbert's solution of Waring's problem

1. Introduction

Fix an integer $k \geq 2$. Then every natural number n can be written as a sum of nonnegative kth powers, since trivially

$$n = \overbrace{1^k + 1^k + \cdots + 1^k}^{n \text{ terms}}.$$

Of course this way of writing n as a sum of kth powers is usually vastly inefficient. Write $g(k;n)$ for the minimal number of nonnegative kth powers needed to additively represent n. (So, for example, $g(2;5) = 2$, since $5 =$

$2^2 + 1^2$ and 5 is not a perfect square.) Let $g(k)$ be the supremum of the numbers $g(k; n)$ as n ranges over the set of natural numbers. In 1770, Waring asserted that $g(k) < \infty$ for every fixed k, and he conjectured that $g(3) \leq 9$ and $g(4) \leq 19$. (Presumably he believed equality to hold in both cases.)

Waring's claims have engaged the energies of mathematicians throughout the intervening centuries: The same year that Waring announced these conjectures, Lagrange proved his "four squares theorem" asserting that $g(2) = 4$. In 1909, Wieferich [**Wie09**] proved that $g(3) = 9$ (modulo a gap later filled by Kempner [**Kem12**]). Finally, in 1986, Balasubramanian et al. [**BDD86a, BDD86b**] succeeded in showing that $g(4) = 19$. As described in the notes to this chapter, the precise value of $g(k)$ is now known for every k.

Our goals for this chapter are rather modest. We will not determine the exact value of $g(k)$ for even a single value of $k > 2$. Instead, we describe what seems to be the simplest known proof of Waring's claim that all the numbers $g(k)$ are finite:

Theorem 5.1. *$g(k) < \infty$ for each fixed k.*

Theorem 5.1 was first established by Hilbert in 1909 [**Hil09**]. The proof presented here is a variant due to Dress [**Dre71, Dre72a**] of Hilbert's argument.

2. Proof of the Hilbert–Waring theorem (Theorem 5.1)

Fundamental to the proof of Theorem 5.1 is the following lemma which guarantees the existence of polynomial identities of a convenient shape:

Lemma 5.2 (Hilbert–Dress identities)**.** *Let $k \in \mathbf{N}$, and put $N := \binom{2k+4}{4}$. There is a formal identity in indeterminates $X_1, \dots, X_5$ of the form*

$$(5.1) \quad M(X_1^2 + \cdots + X_5^2)^k = \sum_{i=0}^{N} m_i (a_{i1}X_1 + \cdots + a_{i5}X_5)^{2k} + m_{N+1}X_5^{2k},$$

where M and m_{N+1} are positive integers, the m_i $(0 \leq i \leq N)$ are nonnegative integers, and the a_{ij} $(0 \leq i \leq N, 1 \leq j \leq 5)$ are integers.

The rather complicated proof of Lemma 5.2 is deferred to §3. Lemma 5.2 has the following important consequence:

Lemma 5.3. *Fix a natural number k and fix a corresponding identity of the form* (5.1)*. Then with M as in* (5.1)*, one can find a natural number Q with the following property: For every nonnegative integer l and every integer x*

with $|x| \leq \sqrt{l}$*, we have*

$$Ml^k = x^{2k} + \sum_{h=1}^{Q} u_h^{2k},$$

for some integers $u_1, u_2, \dots, u_Q$.

Thus, if we fix an M as in (5.1), then each number of the form Ml^k can be written as the sum of $O_k(1)$ $(2k)$th powers, one of which can be arbitrarily prescribed subject to a constraint on its size.

Proof. If $|x| \leq \sqrt{l}$, then by Lagrange's result on sums of four squares, we may write $l - x^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ where $x_1, \dots, x_4 \in \mathbf{Z}$. Put $x_5 := x$. Evaluating both sides of (5.1) with $X_i = x_i$ for $1 \leq i \leq 5$, we find that

$$\begin{aligned} Ml^k = x^{2k} + &\overbrace{x^{2k} + \cdots + x^{2k}}^{m_{N+1}-1 \text{ terms}} \\ &+ \sum_{i=0}^{N} \left(\overbrace{(a_{i1}x_1 + \cdots + a_{i5}x_5)^{2k} + \cdots + (a_{i1}x_1 + \cdots + a_{i5}x_5)^{2k}}^{m_i \text{ terms}} \right). \end{aligned}$$

This proves the lemma with $Q := m_{N+1} - 1 + \sum_{i=0}^{N} m_i$. □

The next lemma guarantees the existence of another family of polynomial identities; these identities have long been well-known, but their use in the proof of Theorem 5.1 is due to Dress.

Lemma 5.4. *For every natural number* k*, there is a formal identity in the indeterminate* T *of the shape*

$$\sum_{i=1}^{R} (T + a_i)^{2k} - \sum_{j=1}^{R} (T + a'_j)^{2k} = AT + B.$$

Here R *and* A *are natural numbers and* $B, a_1, \dots, a_R, a'_1, \dots, a'_R$ *are integers. In fact, one can take* $R = 2^{2k-2}$ *and* $A = (2k)!$.

Proof. The proof uses two easily-verified properties of the *forward difference operator* $\Delta\colon \mathbf{Z}[T] \to \mathbf{Z}[T]$, defined by

$$(\Delta F)(T) := F(T+1) - F(T).$$

First, if $a_n T^n$ is the leading term of $F(T)$, where $n > 0$, then $(\Delta F)(T)$ has leading term $n a_n T^{n-1}$. The second property concerns repeated application of Δ. Write Δ^r for $\Delta \circ \cdots \circ \Delta$ (r times). Then for each natural number r and each $F(T) \in \mathbf{Z}[T]$,

$$(\Delta^r F)(T) = \sum_{j=0}^{r} \binom{r}{j} (-1)^{r-j} F(T+j).$$

Now take $F(T) := T^{2k}$. Applying the first property $2k-1$ times, we find that $(\Delta^{2k-1}F)(T) = (2k)!T + B$ for some integer B. So by the second property (with $r = 2k-1$), we conclude that

$$(2k)!T + B = \sum_{\substack{0 \le j \le 2k-1 \\ 2 \nmid j}} \binom{2k-1}{j} (T+j)^{2k} - \sum_{\substack{0 \le j \le 2k-1 \\ 2 \mid j}} \binom{2k-1}{j} (T+j)^{2k}.$$

Since

$$\sum_{\substack{0 \le j \le 2k-1 \\ 2 \nmid j}} \binom{2k-1}{j} = \sum_{\substack{0 \le j \le 2k-1 \\ 2 \mid j}} \binom{2k-1}{j} = \frac{1}{2} \sum_{0 \le j \le 2k-1} \binom{2k-1}{j} = 2^{2k-2},$$

the lemma follows with $R = 2^{2k-2}$ and $A = (2k)!$. □

The last result we need is a simple lemma concerning how closely one can approximate a nonnegative real number by a sum of kth powers of nonnegative integers:

Lemma 5.5. *Let k be a natural number and put $\kappa := (k-1)/k$. Then for each $x \ge 0$, we have*

$$0 \le x - \left\lfloor x^{1/k} \right\rfloor^k \le k x^{\kappa}.$$

Consequently, for all $x \ge 0$ and $t \in \mathbf{N}$, there are nonnegative integers $z_1, \dots, z_t$ for which

$$x - z_1^k - z_2^k - \cdots - z_t^k \ll_{k,t} x^{\kappa^t}.$$

Proof. By the mean value theorem, there is an $x' \in (\lfloor x^{1/k} \rfloor, x^{1/k})$ for which

$$0 \le x - \left\lfloor x^{1/k} \right\rfloor^k = \frac{d}{dx}(x^k)\bigg|_{x=x'} = k(x')^{k-1} \le k x^{(k-1)/k} = k x^{\kappa}.$$

Iterating this observation gives the lemma. □

Proof of Theorem 5.1. Fix a natural number k. We wish to show that $g(k;m)$ is bounded independently of m. Clearly it is enough to prove this for large m. To this end, fix an R as in Lemma 5.4 and fix M as in Lemmas 5.2 and 5.3. (Thus R and M depend entirely on k.)

Let m be a large natural number which we seek to write as a sum of nonnegative kth powers, and let l^k be the largest kth power not exceeding m/RM. If m is sufficiently large, then

$$\frac{1}{2}\left(\frac{m}{RM}\right)^{1/k} \leq l \leq \left(\frac{m}{RM}\right)^{1/k}. \tag{5.2}$$

Moreover, by Lemma 5.5 with $x = m/RM$,

$$m = RMl^k + r_1, \quad \text{where} \quad 0 \leq r_1 \leq kRM\left(\frac{m}{RM}\right)^{(k-1)/k}.$$

With $\kappa := (k-1)/k$, let t be the least natural number for which $\kappa^t < \frac{1}{2k}$. By Lemma 5.5 (with $x = r_1$) we can write

$$r_1 = z_1^k + z_2^k + \cdots + z_{t-1}^k + r_t, \quad \text{where} \quad r_t \ll_k r_1^{\kappa^{t-1}} \ll_k m^{\kappa^t} \tag{5.3}$$

and each z_i is a nonnegative integer.

Let $x_1, \dots, x_R$ represent integers of absolute value not exceeding $\sqrt{l}$, whose precise values will be chosen below. By Lemma 5.3, we can write

$$\begin{aligned} Ml^k &= x_1^{2k} + \sum\nolimits_{h=1}^{Q} u_h^{2k}, \\ Ml^k &= x_2^{2k} + \sum\nolimits_{h=Q+1}^{2Q} u_h^{2k}, \\ &\;\;\vdots \\ Ml^k &= x_R^{2k} + \sum\nolimits_{h=(R-1)Q+1}^{RQ} u_h^{2k}, \end{aligned} \tag{5.4}$$

for certain integers $u_1, \dots, u_{RQ}$. Adding equations (5.3) and (5.4), we find that

$$\begin{aligned} m &= RMl^k + r_1 \\ &= \sum_{j=1}^{R} x_j^{2k} + \sum_{h=1}^{QR} u_h^{2k} + z_1^k + z_2^k + \cdots + z_{t-1}^k + r_t. \end{aligned}$$

We appear to have made some progress towards our goal, seeing as we have expressed m as a sum of $R + QR + t - 1$ nonnegative kth powers, up to a small remainder r_t. In particular, it would be an easy task to complete the proof if we knew that r_t was the sum of a bounded number of kth powers; however, this is not at all obvious.

To circumvent this difficulty we make a judicious choice of the numbers x_j. In the notation of Lemma 5.4, we set $x_j := n + a_j'$ for all $1 \leq j \leq R$, where n is an integer which remains to be selected. Then $\sum_{j=1}^{R} x_j^{2k} =$

$\sum_{i=1}^{R} y_i^{2k} - (An + B)$, where each $y_i := n + a_i$. Hence

$$m = \sum_{i=1}^{R} y_i^{2k} + \sum_{h=1}^{QR} u_h^{2k} + z_1^k + z_2^k + \cdots + z_{t-1}^k + r_t - (An + B). \tag{5.5}$$

We now choose n so that

$$0 \leq r_t - (An + B) < A, \quad \text{which amounts to setting} \quad n := \left\lfloor \frac{r_t - B}{A} \right\rfloor.$$

To see that we are permitted to choose n in this way, we must check that each $x_j = n + a_j'$ is at most $\sqrt{l}$ in absolute value. But by (5.3),

$$x_j = \left\lfloor \frac{r_t - B}{A} \right\rfloor + a_j' \ll_k r_t + 1 \ll_k m^{\kappa^t},$$

while by (5.2), $\sqrt{l} \gg_k m^{\frac{1}{2k}}$. Since $\kappa^t < \frac{1}{2k}$, each $|x_j|$ is smaller than $\sqrt{l}$ if m is sufficiently large (as we are assuming).

Since $0 \leq r_t - (An + B) < A$, the integer $r_t - (An + B)$ is a sum of fewer than A terms of the form 1^k. So by (5.5),

$$g(k; m) < R + QR + t - 1 + A = O_k(1).$$

This completes the proof of Theorem 5.1. □

3. Producing the Hilbert–Dress identities

3.1. Prerequisites from convex analysis. The proof of Theorem 5.2 given in this text assumes some familiarity with convex sets. Any number of sources would suffice for the the vocabulary and basic theory that we require; references below are to [**Lay82**].

Suppose that V is a real vector space and that S is a subset of V. We write $\operatorname{Conv} S$ for the convex hull of S. The following two results will be particularly important in what follows:

★ **Lemma 5.6** (Carathéodory's theorem)**.** *Let V be a real vector space of dimension n. If S is an arbitrary subset of V, then every element of* $\operatorname{Conv} S$ *can be written as a convex combination of at most $n+1$ elements of S. That is, if $\mathbf{v} \in \operatorname{Conv} S$, then there is an $m \leq n$ for which $\mathbf{v}$ can be written in the form*

$$\sum_{i=0}^{m} \alpha_i \mathbf{v}_i, \quad \text{where each } \mathbf{v}_i \in S, \quad \text{each } \alpha_i \geq 0, \quad \text{and} \quad \sum_{i=0}^{m} \alpha_i = 1. \tag{5.6}$$

Suppose, moreover, that with respect to some basis of V, not only the vector $\mathbf{v}$ but also all the vectors in S have rational coordinates. Then we can choose a representation (5.6) *of $\mathbf{v}$ where all the α_i are rational.*

Remarks.

1. We can always arrange to have $m = n$ in the representation (5.6). Indeed, if $m < n$, then (5.6) continues to hold with m replaced by n if we pad our representation by setting $\alpha_i := 0$ for $m < i \le n$ and choose $\mathbf{v}_i \in S$ arbitrarily for these indices.
2. The second half of the lemma is often not stated explicitly in discussions of Carathéodory's theorem but is implicit in the usual proof of that result (see, e.g., [**Lay82**, Theorem 2.23]). Indeed, suppose that $\mathbf{v}$ and all the vectors in S have rational coordinates, and write $\mathbf{v}$ in the form (5.6) with m as small as possible. The minimality of m forces $\mathbf{v}_0, \dots, \mathbf{v}_m$ to be affinely independent (in the sense of [**Lay82**, Definition 2.17]). It follows that the real numbers $\alpha_0, \dots, \alpha_m$ appearing in our representation (5.6) are the *unique* real numbers satisfying

$$\mathbf{v} = \sum_{i=0}^{m} \alpha_i \mathbf{v}_i, \quad \text{where} \quad \sum_{i=0}^{m} \alpha_i = 1. \tag{5.7}$$

By hypothesis, (5.7) defines a system of linear equations in the α_i with rational coefficients, so by Gaussian elimination its unique solution $\alpha_0, \dots, \alpha_m$ must consist of rational numbers.

Lemma 5.7. *Let V be an n-dimensional real vector space and let S be a convex subset of V. If the vector $\mathbf{v} \in V$ does not belong to the relative interior of S, then one can pass an $(n-1)$-dimensional hyperplane H through $\mathbf{v}$ so that S is contained entirely in one of the closed half-spaces determined by H.*

Proof (sketch). By [**Lay82**, Corollary 4.6], there is an $(n-1)$-dimensional hyperplane H through $\mathbf{v}$ with the relative interior of S entirely contained in one of the open half-spaces determined by H. So the closure of the relative interior of S, which coincides with the closure of S (cf. [**Lay82**, Exercise 2.13]), belongs to the corresponding closed half-space. □

3.2. Proof of Lemma 5.2. Let V be the space of homogeneous polynomials of degree $2k$ belonging to $\mathbf{R}[X_1, \dots, X_5]$. Then V is a real vector space of dimension $N := \binom{2k+4}{4}$, with a basis given by (an arbitrary ordering of) the monomials

$$X_1^{e_1} X_2^{e_2} X_3^{e_3} X_4^{e_4} X_5^{e_5}, \quad \text{where each} \quad e_i \ge 0 \quad \text{and} \quad \sum_{i=1}^{5} e_i = 2k. \tag{5.8}$$

We put an inner product on V by using (5.8) to identify V with $\mathbf{R}^N$ and then importing the standard dot product on $\mathbf{R}^N$. If $(\alpha_1, \dots, \alpha_5) \in \mathbf{R}^5$, we put

$$\mathbf{v}_{(\alpha_1,\ldots,\alpha_5)} := (\alpha_1 X_1 + \cdots + \alpha_5 X_5)^{2k} \in V.$$

Let $\mathbf{B}$ be the 5-dimensional unit ball $\{(\alpha_1,\ldots,\alpha_5) \in \mathbf{R}^5 : \alpha_1^2+\cdots+\alpha_5^2 \le 1\}$. Define a subset $S_{\mathbf{B}}$ of V by

$$S_{\mathbf{B}} := \{\mathbf{v}_{(\alpha_1,\ldots,\alpha_5)} : (\alpha_1,\ldots,\alpha_5) \in \mathbf{B}\}.$$

Lemma 5.8. *Let $c = c(k)$ be the positive real number given by*

$$c := \frac{\int_{\mathbf{B}} \beta_1^{2k}\, d\beta_1 d\beta_2 \cdots d\beta_5}{\int_{\mathbf{B}} d\beta_1 d\beta_2 \cdots d\beta_5}.$$

Then $f(X_1,\ldots,X_5) := c(X_1^2+\cdots+X_5^2)^k$ belongs to the relative interior of the convex hull of $S_{\mathbf{B}}$.

Proof. The proof proceeds in two stages. First we show that if we put

$$g(X_1,\ldots,X_5) := \frac{\int_{\mathbf{B}} \mathbf{v}_{(\alpha_1,\ldots,\alpha_5)}\, d\alpha_1\cdots d\alpha_5}{\int_{\mathbf{B}} d\alpha_1\cdots d\alpha_5}$$

$$= \frac{\int_{\mathbf{B}} (\alpha_1 X_1 + \cdots + \alpha_5 X_5)^{2k}\, d\alpha_1\cdots d\alpha_5}{\int_{\mathbf{B}} d\alpha_1\cdots d\alpha_5}, \tag{5.9}$$

then $f = g$ in $\mathbf{R}[X_1,\ldots,X_5]$. Then we show that g belongs to the relative interior of the convex hull of $S_{\mathbf{B}}$.

Since two multivariate polynomials with real coefficients are equal if they agree for every assignment of the variables, to show that $f = g$ it is enough to prove that

$$f(x_1,\ldots,x_5) = g(x_1,\ldots,x_5)$$

for all real numbers $x_1,\ldots,x_5$. If all of the x_i vanish, then $f = g = 0$. Otherwise we perform the following change of variables in (5.9): Let

$$\begin{array}{ccccccc} \beta_1 & = & \lambda_{11}\alpha_1 & + & \lambda_{12}\alpha_2 & + \cdots + & \lambda_{15}\alpha_5, \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ \beta_5 & = & \lambda_{51}\alpha_1 & + & \lambda_{52}\alpha_2 & + \cdots + & \lambda_{55}\alpha_5, \end{array}$$

where

$$\lambda_{i1} := \frac{x_i}{\sqrt{x_1^2+x_2^2+\cdots+x_5^2}}$$

and the remaining λ_{ij} are chosen so that the resulting matrix (λ_{ij}) is orthogonal. The orthogonality of the matrix ensures that $\mathbf{B}$ is taken to itself by this linear transformation, and we find that

$$\begin{aligned} g(x_1,\ldots,x_5) &= \left(\frac{\int_{\beta_1^2+\cdots+\beta_5^2\le 1} \beta_1^{2k}\, d\beta_1 d\beta_2\cdots d\beta_5}{\int_{\beta_1^2+\cdots+\beta_5^2\le 1} d\beta_1 d\beta_2\cdots d\beta_5}\right)(x_1^2+\cdots+x_5^2)^k \\ &= f(x_1,\ldots,x_5). \end{aligned}$$

Thus $f = g$ for all choices of the x_i, and so $f = g$ in $\mathbf{R}[X_1, \ldots, X_5]$.

Now we take up the problem of showing that g belongs to the relative interior of the convex hull of $S_{\mathbf{B}}$. Let W be the affine hull of $\operatorname{Conv} S_{\mathbf{B}}$ (or equivalently, of $S_{\mathbf{B}}$). Since $S_{\mathbf{B}}$ contains the zero vector, W coincides with the subspace of V generated by $S_{\mathbf{B}}$. We would like to apply Lemma 5.7 (with $\mathbf{v} = g$ and $V = W$), but the way we have set things up, it is necessary to first verify that g belongs to W. But this is easy: Indeed, if $\mathbf{v}$ is any vector from the orthogonal complement $W^\perp$ of W, then $\mathbf{v} \cdot g = 0$, since $\mathbf{v} \cdot \mathbf{v}_{(\alpha_1,\ldots,\alpha_5)} = 0$ for all $(\alpha_1, \ldots, \alpha_5) \in \mathbf{B}$. So $g \in (W^\perp)^\perp = W$.

So by Lemma 5.7, if g does not belong to the relative interior of $\operatorname{Conv} S_{\mathbf{B}}$, then there is a hyperplane H in W passing through g with $\operatorname{Conv} S_{\mathbf{B}}$ entirely contained in one of the closed half-spaces determined by H. Such a hyperplane corresponds to a nonzero $\mathbf{w} \in W$ with the property that

$$\mathbf{w} \cdot \mathbf{v}_{(\alpha_1,\ldots,\alpha_5)} \geq \mathbf{w} \cdot g$$

for all $(\alpha_1, \ldots, \alpha_5) \in \mathbf{B}$. But then

$$\mathbf{w} \cdot g = \frac{\int_{\mathbf{B}} (\mathbf{w} \cdot \mathbf{v}_{(\alpha_1,\ldots,\alpha_5)})\, d\alpha_1 \cdots d\alpha_5}{\int_{\mathbf{B}} d\alpha_1 \cdots d\alpha_5} \geq \frac{\int_{\mathbf{B}} (\mathbf{w} \cdot g)\, d\alpha_1 \cdots d\alpha_5}{\int_{\mathbf{B}} d\alpha_1 \cdots d\alpha_5} = \mathbf{w} \cdot g,$$

which forces us to have

$$\mathbf{w} \cdot \mathbf{v}_{(\alpha_1,\ldots,\alpha_5)} = \mathbf{w} \cdot g$$

for all $(\alpha_1, \ldots, \alpha_5) \in \mathbf{B}$. Since $\mathbf{B}$ contains $(0,0,0,0,0)$, this implies that $\mathbf{w}$ is orthogonal to $\mathbf{v}_{(\alpha_1,\ldots,\alpha_5)}$ for all $(\alpha_1, \ldots, \alpha_5) \in \mathbf{B}$. Thus $S_{\mathbf{B}}$ is entirely contained within a proper subspace of W (viz. the hyperplane orthogonal to $\mathbf{w}$), contrary to the choice of W. □

Lemma 5.8 is enough to prove the existence of an identity of the form (5.1) but where M, the m_i, and the a_{ij} are real numbers (and not necessarily integers). In order to obtain Theorem 5.2 as stated, it is expedient to introduce the following relatives of S:

$$S_{\mathbf{R}^5} := \left\{\mathbf{v}_{(\alpha_1,\ldots,\alpha_5)} : \alpha_i \in \mathbf{R}\right\} \quad \text{and} \quad S_{\mathbf{Q}^5} := \left\{\mathbf{v}_{(\alpha_1,\ldots,\alpha_5)} : \alpha_i \in \mathbf{Q}\right\}.$$

Theorem 5.2 will follow once we know that the f of Lemma 5.8 belongs not only to the relative interior of $\operatorname{Conv} S_{\mathbf{B}}$ but also to the relative interior of $\operatorname{Conv} S_{\mathbf{Q}^5}$. This is a consequence of the next two lemmas:

Lemma 5.9. *The sets $S_{\mathbf{B}}$ and $S_{\mathbf{R}^5}$ have the same affine hull.*

Proof. Since $\mathbf{0} \in S_{\mathbf{B}} \cap S_{\mathbf{R}^5}$, this amounts to checking that $S_{\mathbf{B}}$ and $S_{\mathbf{R}^5}$ generate the same subspace of V. But this is clear, since $S_{\mathbf{R}^5}$ is a union of dilations of $S_{\mathbf{B}}$. □

Since $S_{\mathbf{B}}$ is contained within $S_{\mathbf{R}^5}$, its convex hull $\operatorname{Conv} S_{\mathbf{B}}$ is contained within $\operatorname{Conv} S_{\mathbf{R}^5}$. So by Lemma 5.9, the relative interior of $\operatorname{Conv} S_{\mathbf{B}}$ is contained in the relative interior of $\operatorname{Conv} S_{\mathbf{R}^5}$. Since f belongs to the relative interior of $\operatorname{Conv} S_{\mathbf{B}}$ by Lemma 5.8, we will have that f belongs to the relative interior of $\operatorname{Conv} S_{\mathbf{Q}^5}$ once we establish the following lemma:

Lemma 5.10. *The relative interior of* $\operatorname{Conv} S_{\mathbf{R}^5}$ *is contained within the relative interior of* $\operatorname{Conv} S_{\mathbf{Q}^5}$.

Proof. We start by observing that, using an overline to denote the closure operator,

$$\operatorname{Conv} S_{\mathbf{R}^5} \subset \overline{\operatorname{Conv} S_{\mathbf{Q}^5}}. \tag{5.10}$$

Indeed, suppose that $\mathbf{v}$ belongs to the convex hull of $S_{\mathbf{R}^5}$ and write $\mathbf{v}$ as a convex combination of vectors $\mathbf{v}_i \in S_{\mathbf{R}^5}$. We can approximate these $\mathbf{v}_i$ arbitrarily closely by elements of $S_{\mathbf{Q}^5}$, and so we can approximate $\mathbf{v}$ arbitrarily closely by elements of $\operatorname{Conv} S_{\mathbf{Q}^5}$. This proves (5.10).

Consequently, the affine hull of $\operatorname{Conv} S_{\mathbf{R}^5}$ is contained within the affine hull of $\overline{\operatorname{Conv} S_{\mathbf{Q}^5}}$. On the other hand, the affine hull of $\operatorname{Conv} S_{\mathbf{R}^5}$ coincides with the affine hull of $S_{\mathbf{R}^5}$ while the affine hull of $\overline{\operatorname{Conv} S_{\mathbf{Q}^5}}$ coincides with the affine hull of $S_{\mathbf{Q}^5}$. Since $S_{\mathbf{Q}^5}$ is contained in $S_{\mathbf{R}^5}$, we conclude that both sides of (5.10) have the same affine hull.

It now follows from (5.10) that the relative interior of $\operatorname{Conv} S_{\mathbf{R}^5}$ is contained in the relative interior of $\overline{\operatorname{Conv} S_{\mathbf{Q}^5}}$. To complete the proof of the lemma we need only recall that a convex set and its closure always have the same relative interior (cf. [**Lay82**, Exercise 2.14]). □

Proof of Theorem 5.2. Since $\mathbf{0} \in S_{\mathbf{Q}^5}$, the affine hull of $S_{\mathbf{Q}^5}$ coincides with the subspace generated by $S_{\mathbf{Q}^5}$. Since X_5^{2k} belongs to this subspace (because $X_5^{2k} = \mathbf{v}_{(0,0,0,0,1)} \in S_{\mathbf{Q}^5}$) and $f(X_1, \dots, X_5)$ is in the relative interior of $\operatorname{Conv} S_{\mathbf{Q}^5}$, it follows that for all sufficiently small $\mu > 0$,

$$f(X_1, \dots, X_5) - \mu X_5^{2k} = c(X_1^2 + X_2^2 + \cdots + X_5^2)^k - \mu X_5^{2k} \in \operatorname{Conv} S_{\mathbf{Q}^5}.$$

Moreover, since $\mathbf{0} \in \operatorname{Conv} S_{\mathbf{Q}^5}$, for each $0 \le \lambda \le 1$,

$$\lambda c(X_1^2 + X_2^2 + \cdots + X_5^2)^k - \lambda\mu X_5^{2k} \in \operatorname{Conv} S_{\mathbf{Q}^5}.$$

We choose $\lambda > 0$ and μ here so that both λc and $\lambda\mu$ are rational. Applying Carathéodory's Theorem (Theorem 5.6), we can write

$$\lambda c(X_1^2 + X_2^2 + \cdots + X_5^2)^k = \lambda\mu X_5^{2k} + \sum_{i=0}^{N} r_i(b_{i1}X_1 + \cdots + b_{i5}X_5)^{2k}$$

where each $r_i \ge 0$ is rational, $\sum_{i=0}^{N} r_i = 1$, and each b_{ij} is rational. The Hilbert–Dress identity follows upon clearing all the denominators. □

Notes

Our proof of Theorem 5.1 is a pure existence argument; it shows that $g(k)$ is bounded above but does not give any finite procedure for determining an upper bound. This is because our proof of Lemma 5.2, due essentially to Hilbert [**Hil09**] and Schmidt [**Sch13**], yields no information on the size of the coefficients in (5.1). An alternative method for proving identities like (5.1) was given by Hausdorff [**Hau09**] (see [**Nat96**, §3.2] for a lucid exposition). This allowed Rieger [**Rie53a, Rie53b**], in his doctoral dissertation, to obtain explicit upper bounds on $g(k)$. Specifically, he proved that for each k,

$$g(k) < (2k+1)^{260(k+3)^{3k+8}}.$$

He later announced in [**Rie56**] the improved bound

$$g(k) < (2k+1)^{260(k+1)^8}.$$

If instead of following Hilbert's original proof, one uses Rieger's method in combination with Dress's argument, then one finds that

$$g(k) < (2k+1)^{2000k^5}$$

(see [**Pol11d**]). This appears to be the best known general upper bound on $g(k)$ so far obtained by elementary methods, although as we shall see shortly, it is quite far from the truth.

Around 1772, J. A. Euler observed that $g(k;n) = 2^k + \lfloor (3/2)^k \rfloor - 2$ when $n := 2^k \lfloor (3/2)^k \rfloor - 1$. (The reader should attempt to verify this for herself; the essential observation is that $n < 3^k$, so that only 0^k, 1^k, and 2^k can enter into a representation of n as a sum of kth powers.) Thus

$$g(k) \geq 2^k + \lfloor (3/2)^k \rfloor - 2. \tag{5.11}$$

In particular, $g(2) \geq 4$, $g(3) \geq 9$, $g(4) \geq 19$, $g(5) \geq 53$, etc. Remarkably, it turns out that the easy lower bound (5.11) is almost always sharp. More precisely, we have the following statement (which combines results of Dickson, Pillai, Rubugunday, Niven, Chen, Balasubramanian, Deshouillers, and Dress): Write $\{x\}$ for the fractional part $x - \lfloor x \rfloor$ of the real number x. If

$$2^k \{(3/2)^k\} + \lfloor (3/2)^k \rfloor \leq 2^k, \tag{5.12}$$

then equality holds in (5.11). If (5.12) fails, define

$$N(k) := \lfloor (3/2)^k \rfloor \cdot \lfloor (4/3)^k \rfloor + \lfloor (3/2)^k \rfloor + \lfloor (4/3)^k \rfloor;$$

then

$$g(k) := \begin{cases} \lfloor (3/2)^k \rfloor + \lfloor (4/3)^k \rfloor + 2^k - 3 & \text{if } 2^k < N(k), \\ \lfloor (3/2)^k \rfloor + \lfloor (4/3)^k \rfloor + 2^k - 2 & \text{if } 2^k = N(k). \end{cases}$$

The inequality (5.12) holds for all $k \leq 471{,}600{,}000$ [**KW90**], and it seems reasonable to conjecture that it always holds. In any event, Mahler [**Mah57**] has shown that (5.12) fails for at most finitely many k.

Much of the modern research on Waring's problem focuses not on $g(k)$, but on the quantity $G(k)$, defined as the smallest number of kth powers needed to additively represent all *sufficiently large* numbers. (Thus $G(k) = \limsup_{n\to\infty} g(k;n)$.) For $k = 2$, we have $g(2) = G(2) = 4$, since no number from the residue class 7 mod 8 is a sum of three squares. But for $k > 2$, it is known that $G(k) < g(k)$. In fact, for large k, $G(k)$ is considerably smaller than $g(k)$; in sharp contrast with (5.11), Wooley [**Woo95**] has proved that

$$G(k) \leq k\log k + k\log\log k + 2k + O(k\log\log k/\log k).$$

The precise determination of $G(k)$ is a very difficult problem which has been solved only for $k = 2$ and $k = 4$ (see [**Dav39**]).

The results of the last two paragraphs rely on the Hardy–Littlewood *circle method* for their proofs. For a gentle introduction to this method in the context of Waring's problem, see [**Nat96**, Chapters 4 and 5]. For further discussion of Waring's problem, see [**HW08**, Chapter XXI] and the surveys of Ellison [**Ell71**] and Vaughan & Wooley [**VW02**].

Chapter 6

Sieve Methods, I

> Brun's [sieve] method ... is perhaps our most powerful elementary tool in number theory. – P. Erdős [**Erd65**]

1. Introduction

In a delightful survey article [**Gra95**], the contemporary number theorist Andrew Granville points out that ancient Greek mathematics bequeathed two results in prime number theory that have proved of first importance in subsequent thought. The first is Euclid's proof of the infinitude of the primes, which was discussed in Chapter 1. The second is the sieve of Eratosthenes.

Eratosthenes' method allows one to determine the primes not exceeding x assuming only knowledge of the primes not exceeding $\sqrt{x}$. In this procedure, one begins with a list of all positive integers in the interval $[2, x]$. For each prime $p \le \sqrt{x}$, we cross out all the multiples of p on the list; the numbers remaining are exactly the primes in the interval $(\sqrt{x}, x]$. We illustrate this with $x = 30$, sieving by the primes $2, 3$, and 5:

	2	3	$\cancel{4}$	5	$\cancel{6}$	7	$\cancel{8}$	$\cancel{9}$	$\cancel{10}$
11	$\cancel{12}$	13	$\cancel{14}$	$\cancel{15}$	$\cancel{16}$	17	$\cancel{18}$	19	$\cancel{20}$
$\cancel{21}$	$\cancel{22}$	23	$\cancel{24}$	$\cancel{25}$	$\cancel{26}$	$\cancel{27}$	$\cancel{28}$	29	$\cancel{30}$

This procedure is remarkable not only insofar as it gives a fast algorithm for listing primes, but also in that it suggests the useful viewpoint of the primes as the integers surviving a "sieving process".

It is natural to hope that the sieve of Eratosthenes might shed light on the behavior of the prime counting function $\pi(x)$. Let us see how this might go, without any attempt at rigor for the time being. For each prime p, the proportion of natural numbers divisible by p is $1/p$. Moreover, if one has several distinct primes p, the events of being divisible by p are mutually independent (by the Chinese remainder theorem). So letting

$$\pi(x,z) := \#\{n \le x : n \text{ has no prime factors} \le z\},$$

we expect that in a reasonable range of parameters x and z,

$$\pi(x,z) \approx x \prod_{p\le z}(1-1/p). \tag{6.1}$$

A number $n \in [2,x]$ survives the sieve of Eratosthenes precisely when n is divisible by no prime $p \le \sqrt{x}$. In terms of $\pi(x,z)$, this says that

$$\pi(x) - \pi(\sqrt{x}) + 1 = \pi(x,\sqrt{x}). \tag{6.2}$$

(The $+1$ on the left-hand side comes from the fact that 1 is counted in $\pi(x,\sqrt{x})$.) Thus, our heuristic suggests that

$$\pi(x) \approx x \prod_{p\le\sqrt{x}}(1-1/p). \tag{6.3}$$

(We ignore the "$\pi(\sqrt{x})+1$" part of (6.2), since this is much smaller than the right-hand side of (6.3).) By Mertens's theorem (see Theorems 3.15, 3.17), the product in (6.3) is asymptotically $2e^{-\gamma}/\log x$, as $x\to\infty$. So the sieve of Eratosthenes suggests the guess that $\pi(x) \approx 2e^{-\gamma}x/\log x \approx 1.1229x/\log x$. On the other hand, the prime number theorem asserts that $\pi(x) \sim x/\log x$. What are we to make of this discrepancy?

Before answering that question, we digress to consider another prototypical sieving scenario. Recall that $\pi_2(x)$ denotes the number of twin prime pairs $p, p+2$ with $p \le x$. If p and $p+2$ form a twin prime pair, then for any choice of $z > 0$, either $p \le z$ or both p and $p+2$ have no prime factors $\le z$. Consequently, with

$$\pi_2(x,z) := \#\{n \le x : n(n+2) \text{ has no prime factors} \le z\}, \tag{6.4}$$

we have the upper bound

$$\pi_2(x) \le z + \pi_2(x,z). \tag{6.5}$$

So an upper bound on $\pi_2(x,z)$ leads to an upper bound on $\pi_2(x)$. In the opposite direction, if $n \le x$ is a natural number for which $n(n+2)$ has no prime factors $\le \sqrt{x+2}$, then n and $n+2$ must both be prime, and so

$$\pi_2(x) \ge \pi_2(x, \sqrt{x+2}).$$

This suggests a natural way of approaching the distribution of the twin primes: Instead of mounting a direct assault on $\pi_2(x)$, attempt to grok the two-parameter function $\pi_2(x,z)$.

From the standpoint of heuristic reasoning, the function $\pi_2(x,z)$ does not present any extra difficulty over $\pi(x,z)$. Notice that if p is an odd prime, the odds that p divides an expression of the form $n(n+2)$ are $2/p$, since this divisibility occurs precisely when n belongs to one of the congruence classes 0 or -2 modulo p. If $p = 2$, the odds are $1/2$. In analogy with our work on $\pi(x, z)$, we are led to predict that in a wide range of x and z,

$$\pi_2(x, z) \approx \frac{1}{2} x \prod_{2<p\leq z} (1 - 2/p).$$

After another appeal to Mertens's theorem and some algebraic fiddling (see Example (ii) in §3 below for details), we can recast this prediction in the form

$$\pi_2(x, z) \approx 2C_2 e^{-2\gamma} \frac{x}{(\log z)^2}, \quad \text{where} \quad C_2 = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right). \tag{6.6}$$

(The "twin-prime constant" C_2 appearing here was introduced already in Chapter 3, §5.) Now up to a $O(\sqrt{x})$ error, we have $\pi_2(x) \approx \pi_2(x, \sqrt{x+2})$, and thus (6.6) suggests that

$$\pi_2(x) \approx 4e^{-2\gamma} \left(2C_2 \frac{x}{(\log x)^2}\right).$$

But the twin prime conjecture, in the quantitative form discussed in Chapter 3, makes the simpler opposing prediction that $\pi_2(x) \sim 2C_2 x/(\log x)^2$. Again, we are off by a constant factor from what we hoped to find. What's going on here?

In this context of failed heuristics, Hardy and Littlewood [**HL23**] expressed the following sentiment:

> Probability is not a notion of pure mathematics, but of philosophy or physics.

In fairness, these authors were writing before Kolmogorov's axiomatization of probability; from a modern perspective, it would appear more balanced to lay the blame for our failures not at the foot of probability but at our own misuse of it. In brief, we have been dealing in half-truths, and our sin has found us out. For example, it is simply not the case that for actual, honest-to-goodness finite values of x, a number $\leq x$ is divisible by p with probability $1/p$; the actual probability is $\lfloor x/p \rfloor / \lfloor x \rfloor$. Nor is it the case that distinct p give rise to mutually independent events; there is only approximate independence. Our predictions, which are off by a constant factor from what we expected, illustrate that enough half-truths lead to one whole lie; the accumulation of error terms is significant enough to lead to predictions with an incorrect main term.

This is a frustrating development for would-be solvers of the twin prime conjecture. But as the saying goes, problems worthy of attack prove their worth by fighting back!

What happens if we try to put the heuristic arguments proposed above on a solid footing? This might seem like a lost cause, given what we have seen. But in fact, quite a bit can be salvaged! It will turn out that our predictions (6.1), (6.6) actually do describe the asymptotic behavior of $\pi(x, z)$ and $\pi_2(x, z)$ in a wide range of x and z – just not wide enough to deduce asymptotic results about $\pi(x)$ or $\pi_2(x)$. And in view of relations like (6.5), even results in a limited range of z can have nontrivial implications. So we solider on, proving what we can.

We will actually work in some generality: We suppose we are given a finite sequence of integers $\mathscr{A}$ and a finite set of primes $\mathscr{P}$, and we seek to estimate the number of terms of $\mathscr{A}$ not divisible by any prime from $\mathscr{P}$. We assume that for each prime $p \in \mathscr{P}$, the proportion of terms of $\mathscr{A}$ divisible by p is approximately $\alpha(p)$ (say), and that the events of being divisible by different $p \in \mathscr{P}$ are close to mutually independent. Under these conditions, we hope to prove a theorem that the proportion of terms of $\mathscr{A}$ remaining after sieving out those divisible by $p \in \mathscr{P}$ is $\approx \prod_{p \in \mathscr{P}}(1 - \alpha(p))$. We know from experience that we should not always expect the "$\approx$" sign in this relation to yield an asymptotic formula, but even weaker interpretations of "$\approx$" will be of interest to us.

This chapter discusses the simplest and historically earliest methods for establishing approximations of this type:

- **Eratosthenes–Legendre sieve**: Using the combinatorial principle of inclusion-exclusion, one can write down a finite sum whose value is the precise number of terms of $\mathscr{A}$ remaining after the sieve process is carried out. The motivating example is due to Legendre, who knew that (cf. [**Leg00**, Quatrième Partie, §XI]))

$$\pi(x, z) = \lfloor x \rfloor - \sum_{p \le z} \left\lfloor \frac{x}{p} \right\rfloor + \sum_{p_1 < p_2 \le z} \left\lfloor \frac{x}{p_1 p_2} \right\rfloor - \cdots + (-1)^{\pi(z)} \sum_{p_1 < p_2 < \cdots < p_{\pi(z)} \le z} \left\lfloor \frac{x}{p_1 \cdots p_{\pi(z)}} \right\rfloor .$$

  Legendre's method has the virtue of giving an exact answer. But as is apparent already in Legendre's example, it is not clear how to understand the magnitude of the result, and this is our chief concern! To obtain something more digestible, one replaces each term in the sum with an approximation, and re-expresses the result as a finite product. (In Legendre's case, this is accomplished by dropping the greatest-integer signs.) This introduces a number of errors, and in fact, the error term in the Eratosthenes–Legendre method dominates except in very special cases. Nevertheless, the sieve of Eratosthenes–Legendre has an important role as an auxiliary tool in a number of investigations.

- **Brun's pure sieve:** Viggo Brun observed that rather than carrying out the full inclusion-exclusion, one has more manageable error terms if one truncates the inclusion-exclusion process at a finite level. One no longer has an exact count of unsieved terms, but depending on whether one cuts off the process after an inclusion of an exclusion, one has either a lower bound or an upper bound. This method has come to be called the "pure sieve", because the approach is purely combinatorial. The name "Brun's pure sieve" also distinguishes the method from the approach taken in Brun's later work (discussed in Chapter 7), which is not so easily interpreted combinatorially.

  Using his pure sieve, Brun [**Bru19a**] showed (as we will do in §4) that the approximation appearing in (6.6) is valid as an asymptotic formula for certain values of z growing almost, but not quite, as fast as a power of x. Using (6.5), he deduced that

$$\pi_2(x) \ll \frac{x(\log\log x)^2}{(\log x)^2}. \tag{6.7}$$

  Since z is smaller than a fixed power of x in this method, there is an an extra factor on the right-hand side (in this case, a power of $\log\log x$) over what is expected to be the truth. This is typical of applications of Brun's pure sieve. Nevertheless, while the upper bound (6.7) on $\pi_2(x)$ given here is not sharp, it still has interesting consequences. The most famous of these (established below as Corollary 6.13) is that the series $\sum_p 1/p$, restricted to primes p which belong to a twin prime pair, is either a finite sum or a convergent infinite series.

Sieve methods are one of the more difficult topics discussed in this book; the technically-sophisticated content and the complicated notation conspire to create a feeling of foreboding in many a novice. By restricting our discussion in this chapter to two comparatively simple sieve methods, we hope to give the reader a fighting chance to acclimate. Still, caution is warranted! The reader is advised to tread slowly and carefully through this chapter, verifying the details in the examples and trying her hand at the exercises.

2. Anatomy of a sieve problem: The basic setup

Let us make precise the anatomy of a general sieve problem. We suppose that we are given a finite sequence of integers $\mathscr{A}$; the order of the sequence is not important, but it is important in some applications to allow multiplicities.[1] We suppose that $\mathscr{P}$ is a finite set of primes, and we seek to estimate the number of terms of $\mathscr{A}$ divisible by no $p \in \mathscr{P}$, i.e., the quantity

$$S(\mathscr{A}, \mathscr{P}) := \#\{a \in \mathscr{A} : \gcd(a, P) = 1\}, \quad \text{where} \quad P := \prod_{p \in \mathscr{P}} p.$$

We write A_d for the number of terms of $\mathscr{A}$ divisible by d, i.e.,

$$A_d := \#\{a \in \mathscr{A} : d \mid a\}.$$

Let X denote an approximation to the size of $\mathscr{A}$. We assume the existence of a multiplicative function α taking values in $[0, 1]$ as well as a real-valued remainder function $r(d)$ for which

$$A_d = X\alpha(d) + r(d) \tag{6.8}$$

for each d dividing P. Equation (6.8) encodes that the proportion of elements of $\mathscr{A}$ divisible by p is approximately $\alpha(p)$; moreover, since α is multiplicative, for distinct primes p, the events of being divisible by p are approximately mutually independent. In practice, we *choose* X and α, and we *define* $r(d)$, for d dividing P, so that (6.8) holds. Of course, any choice of X and α gives rise to *some* remainder function r; the hope is that making natural choices, the resulting remainder terms $r(d)$ are small, either uniformly or on average.

In many situations, the sieving set $\mathscr{P}$ is obtained by truncating an infinite set of primes at a finite height z. Consequently, it is expedient to allow the set $\mathscr{P}$ to be infinite and to introduce special notation indicating that we sieve only by those primes $p \in \mathscr{P}$ with $p < z$. We therefore define

$$S(\mathscr{A}, \mathscr{P}, z) := \#\{a \in \mathscr{A} : \gcd(a, P(z)) = 1\}, \quad \text{where} \quad P(z) := \prod_{\substack{p \in \mathscr{P} \\ p < z}} p.$$

Hence, $S(\mathscr{A}, \mathscr{P}, z) = S(\mathscr{A}, \mathscr{P} \cap [2, z))$.

Examples.

(i) (**Sieving for primes**) Let $\mathscr{A}$ be the set of natural numbers $n \le x$, and let $\mathscr{P}$ be the set of primes $\le z$. Then $S(\mathscr{A}, \mathscr{P})$ is what was denoted in the introduction by $\pi(x, z)$. For each d dividing P, we have $A_d = \lfloor x/d \rfloor$. So if we take $X = x$ and $\alpha(d) = 1/d$, then (6.8) holds with $r(d) = \lfloor x/d \rfloor - x/d$. In particular, $|r(d)| \le 1$ for all d dividing P.

[1] Thus, the term "multiset" would serve us just as well as "sequence". In the sequel, when we speak of the number of $a \in \mathscr{A}$ with a certain property, we always intend that these be counted with multiplicity.

(ii) (**Sieving for twin primes**) Let $\mathscr{A}$ be the sequence of natural numbers $n(n+2)$, with $n \le x$. Let $\mathscr{P}$ be the set of primes $\le z$. Then $S(\mathscr{A}, \mathscr{P})$ is what was denoted in the introduction by $\pi_2(x, z)$. The condition that d divides $n(n+2)$ is a condition on n modulo d, so we set

$$\nu(d) := \#\{n \pmod d : n(n+2) \equiv 0 \pmod d\}.$$

Then each block of d consecutive integers contains precisely $\nu(d)$ solutions of the congruence $n(n+2) \equiv 0 \pmod d$. Hence, $A_d \approx (x/d)\nu(d)$. This suggests that we choose $X = x$ and $\alpha(d) = \nu(d)/d$. (By the Chinese remainder theorem, both ν and α are multiplicative.) Since the interval $[1, x]$ contains the first $\lfloor x/d \rfloor$ blocks of d consecutive natural numbers, and is contained in the first $\lceil x/d \rceil$ such blocks, with this choice of X and α we have

$$\lfloor x/d \rfloor \nu(d) \le A_d \le \lceil x/d \rceil \nu(d),$$

and so $|r(d)| = \left| A_d - x\frac{\nu(d)}{d} \right| \le \nu(d)$ for each d dividing P.

(iii) (**Sieving for primes of the form** n^2+1) Let $\mathscr{A}$ be the sequence of natural numbers n^2+1, with $n \le x$. Let $\mathscr{P}$ be the set of primes for which $n^2+1 \equiv 0 \pmod p$ has a solution, so that $\mathscr{P}$ contains 2 and all primes $\equiv 1 \pmod 4$. Then $S(A, \mathscr{P}, z)$ counts the number of $n \le x$ for which n^2+1 has no prime factors $< z$. This setup is a natural one if one is interested in the function $\pi_{T^2+1}(x)$ counting the number of $n \le x$ for which n^2+1 is prime; indeed, for any choice of positive z,

$$\pi_{T^2+1}(x) \le \sqrt{z} + S(\mathscr{A}, \mathscr{P}, z). \tag{6.9}$$

Now set

$$\nu(d) := \#\{n \pmod d : n^2+1 \equiv 0 \pmod d\}.$$

With $X = x$ and $\alpha(d) = \nu(d)$, the same reasoning as in the previous example shows that $|r(d)| \le \nu(d)$ for each d dividing $P(z)$.

(iv) (**Sieving for Goldbach representations**) Let N be an even natural number. Let $\mathscr{A}$ be the sequence of values $n(N-n)$, with $1 \le n \le N$. Let $\mathscr{P}$ be the set of all primes. Then $S(\mathscr{A}, \mathscr{P}, z)$ is related to the number of ordered representations $R(N)$ of N as a sum of two primes (cf. Conjecture 3.19): Indeed, if $N = p_1 + p_2$ is a representation of N as a sum of two primes, then either $\min\{p_1, p_2\} < z$, or $p_1(N-p_1)$ is coprime to $P(z)$. Thus,

$$R(N) \le 2z + S(\mathscr{A}, \mathscr{P}, z). \tag{6.10}$$

We let

$$\nu(d) := \#\{n \ (\mathrm{mod}\ d) : n(N-n) \equiv 0 \ (\mathrm{mod}\ d)\};$$

then with $X = N$ and $\alpha(d) = \nu(d)/d$, we have that $|r(d)| \le \nu(d)$ for all divisors d of $P(z)$.

3. The sieve of Eratosthenes–Legendre and its applications

3.1. A first sieve result. We start by recalling one of the fundamental theorems of enumerative combinatorics:

Theorem 6.1 (Principle of inclusion-exclusion)**.** *Let X be a nonempty, finite set of N objects, and let $P_1, \dots, P_r$ be properties that elements of X may have. For each subset $I \subset \{1, 2, \dots, r\}$, let $N(I)$ denote the number of elements of X that have each of the properties indexed by the elements of I. Then with N_0 denoting the number of elements of X with none of these properties, we have*

$$\begin{aligned} N_0 &= \sum_{k=0}^{r} (-1)^k \sum_{\substack{I \subset \{1,2,\dots,r\} \\ |I|=k}} N(I) \\ &= \sum_{I \subset \{1,2,\dots,r\}} (-1)^{|I|} N(I). \end{aligned} \tag{6.11}$$

Proof. Suppose that the element $x \in X$ has exactly l of the properties $P_1, \dots, P_r$. If $l = 0$, then x is counted only once in (6.11), in the term $N(\emptyset)$. On the other hand, if $1 \le l \le r$, then the number of k-element sets $I \subset \{1, 2, 3, \dots, r\}$ for which x is counted in $N(I)$ is exactly $\binom{l}{k}$, and the total weight with which x is counted is

$$\sum_{k=0}^{l} (-1)^k \binom{l}{k} = (1-1)^l = 0,$$

by the binomial theorem. □

The principle of inclusion-exclusion can be immediately applied to the general sieve problem as described in §2:

Theorem 6.2 (Sieve of Eratosthenes–Legendre)**.**

$$S(\mathscr{A}, \mathscr{P}) = X \prod_{p \in \mathscr{P}} (1 - \alpha(p)) + \sum_{d \mid P} \mu(d) r(d).$$

Remark. The second term is usually thought of as an error and estimated crudely by the triangle inequality:

$$\left|\sum_{d\mid P}\mu(d)r(d)\right| \le \sum_{d\mid P}|r(d)|.$$

Proof. Let $p_1,\dots,p_r$ be a list of the primes in $\mathscr{P}$, and for each $1\le i\le r$, let P_i be the property of being divisible by p_i. For every d dividing P, there are $X\alpha(d)+r(d)$ terms of $\mathscr{A}$ divisible by d. So by the principle of inclusion-exclusion, the number of $a\in\mathscr{A}$ divisible by none of the primes of $\mathscr{P}$ is

$$\begin{aligned}\sum_{k=0}^{r}(-1)^k \sum_{\substack{I\subset\{1,2,\dots,r\}\\ |I|=k}} N(I) &= \sum_{k=0}^{r}(-1)^k \sum_{\substack{d\mid P\\ \omega(d)=k}} A_d\\ &= \sum_{k=0}^{r}\sum_{\substack{d\mid P\\ \omega(d)=k}} \mu(d)\left(X\alpha(d)+r(d)\right)\\ &= X\sum_{d\mid P}\mu(d)\alpha(d)+\sum_{d\mid P}\mu(d)r(d)\end{aligned}$$

Since $\sum_{d\mid P}\mu(d)\alpha(d)=\prod_{p\in\mathscr{P}}(1-\alpha(p))$, the theorem follows. $\square$

Examples. We return to the examples of sieve problems given in §2.

(i) (**Sieving for primes**) In this example, $\mathscr{A}$ is the sequence of all natural numbers $\le x$ and $\mathscr{P}$ is the set of all primes $\le z$. With X, α, and r as described in §2, we obtain from Theorem 6.2 that

$$\pi(x,z)=x\prod_{p\le z}\left(1-\frac{1}{p}\right)+O\biggl(\sum_{d\mid P}1\biggr).$$

The error term here is $\ll 2^{\pi(z)}\le 2^z$, while the main term is asymptotic to $e^{-\gamma}x/\log z$, whenever z tends to infinity. Choosing $z=\log x$, the error is $\ll 2^{\log x}=x^{\log 2}$, and we deduce that

$$\pi(x,\log x)\sim e^{-\gamma}\frac{x}{\log\log x}\qquad(\text{as } x\to\infty).$$

Since $\pi(x)\le \log x+\pi(x,\log x)$, we recover the result obtained in Chapter 3 that the set of primes has asymptotic density zero. Unfortunately, the upper bound on $\pi(x)$ obtained by this sieve argument is much weaker than Chebyshev's upper bound $\pi(x)\ll x/\log x$ obtained in Chapter 3.

(ii) (**Sieving for twin primes**) In this case, Theorem 6.2 shows that if $x \geq z \geq 2$, then

$$\pi_2(x, z) = \frac{1}{2}x \prod_{p \leq z}\left(1 - \frac{2}{p}\right) + O\left(\sum_{d|P} \nu(d)\right). \tag{6.12}$$

Rewrite

$$\frac{1}{2}\prod_{2<p\leq z}\left(1-\frac{2}{p}\right) = \left(2\prod_{2<p\leq z}\frac{1-2/p}{(1-1/p)^2}\right)\prod_{p\leq z}\left(1-\frac{1}{p}\right)^2.$$

Estimating the final product by Mertens' theorem, we find that the main term in (6.12) is asymptotic to $2C_2e^{-2\gamma}x/(\log z)^2$ whenever $z \to \infty$. Since $\nu(p) \leq 2$ for all primes p, the error in (6.12) is $\ll \prod_{p\leq z}(1+\nu(p)) \leq 3^{\pi(z)} \leq 3^z$. Now choose $z = \frac{1}{2}\log x$ to show that

$$\pi_2(x, \frac{1}{2}\log x) \sim 2C_2e^{-2\gamma}\frac{x}{(\log\log x)^2} \qquad (\text{as } x \to \infty).$$

This result is perhaps of some interest in itself. But it is too weak to say anything novel about twin primes; the corresponding bound on $\pi_2(x)$ obtained via (6.5) is weaker than the trivial upper bound $\pi_2(x) \leq \pi(x) \ll x/\log x$. A more powerful sieve is needed; we will return to this example below, when more sophisticated tools are at our disposal.

(iii) (**Sieving for primes of the form** n^2+1) The congruence $n^2 + 1 \equiv 0 \pmod{p}$ has one solution if $p = 2$ and two solutions if $p \equiv 1 \pmod 4$. Hence, for $x \geq z > 2$,

$$S(\mathscr{A}, \mathscr{P}, z) = \frac{1}{2}x \prod_{\substack{p<z \\ p\equiv 1 \pmod 4}}\left(1-\frac{2}{p}\right) + O\left(\sum_{d|P(z)}\nu(d)\right). \tag{6.13}$$

It is a bit tricky to find an asymptotic for the main term, and so we make do with an upper bound of the correct order. From Exercise 4.1,

$$\sum_{p<z,\ p\equiv 1 \pmod 4}\frac{1}{p} = \frac{1}{2}\log\log z + O(1).$$

Since $1 + x \leq e^x$ for all real x,

$$\prod_{\substack{p<z \\ p\equiv 1 \pmod 4}}\left(1-\frac{2}{p}\right) \leq \exp\left(-2\sum_{\substack{p<z \\ p\equiv 1 \pmod 4}}\frac{1}{p}\right) \ll \frac{1}{\log z}.$$

We have $\nu(p) \leq 2$ for all $p \in \mathscr{P}$, and so (see example (ii) above) the O-error in (6.13) is $\ll 3^z$. Choosing $z = \frac{1}{2}\log x$, we find that $S(\mathscr{A}, \mathscr{P}, \frac{1}{2}\log x) \ll x/\log\log x$. So by (6.9),

$$\pi_{T^2+1}(x) \ll x/\log\log x$$

for $x \geq 3$. In particular, the set of n for which n^2+1 is prime has density zero. This example is due to Nagell [**Nag22**]; see Exercise 2 for a generalization.

(iv) (**Sieving for Goldbach representations**) This is similar to example (ii). Since N is even, we have $\nu(2) = 1$. In general, $\nu(p) = 2$ if $p \nmid N$ and $\nu(p) = 1$ if $p \mid N$. Hence, for even $N > z > 2$,

$$S(\mathscr{A}, \mathscr{P}, z) = \frac{N}{2} \prod_{\substack{p \nmid N \\ 2<p<z}} \left(1 - \frac{2}{p}\right) \prod_{\substack{p \mid N \\ 2<p<z}} \left(1 - \frac{1}{p}\right) + O\Bigg(\sum_{d \mid P(z)} \nu(d)\Bigg).$$

Noting that $\nu(p) \leq 2$ for all p, the O-error is once again $\ll 3^z$. Arguing as in Example (ii), we find that the main term is asymptotic, whenever $z \to \infty$, to

$$2C_2 e^{-2\gamma} \Bigg(\prod_{\substack{p \mid N \\ 2<p<z}} \frac{p-1}{p-2}\Bigg) \frac{N}{(\log z)^2}.$$

If we take $z = \frac{1}{2}\log N$, then the main term dominates and we have an asymptotic formula for $S(\mathscr{A}, \mathscr{P}, \frac{1}{2}\log N)$. Note though that for this value of z, the corresponding upper bound on $R(N)$ implied by (6.10) is worse than the trivial bound $R(N) \leq \pi(N)$. Once again, we need a better sieve!

3.2. Further examples. In order to stress the wide applicability of the sieve of Eratosthenes–Legendre, we give two applications where this sieve plays an auxiliary role. The first of these, concerning sums of two squares, requires the following lemma of independent interest:

Lemma 6.3. *Let $\mathscr{P}$ be an arbitrary set of primes. Then the set of natural numbers n not divisible by any $p \in \mathscr{P}$ possesses an asymptotic density; in fact, the density has the expected value*

$$\delta(\mathscr{P}) := \prod_{p \in \mathscr{P}} (1 - 1/p).$$

In particular, if the sum of the reciprocals of the elements of $\mathscr{P}$ diverges, then the corresponding set of n has asymptotic density zero.

Proof. We let $\mathscr{A}$ be the set of natural numbers $n \le x$ and let $\mathscr{P}$ be the set of primes appearing in the hypothesis of the lemma. If n has no prime factors from $\mathscr{P}$, then n is counted in $S(\mathscr{A}, \mathscr{P}, z)$, for every choice of z.

We take $X = x$ and define $\alpha(d) = 1/d$; then, as in the first example of §2, we have $|r(d)| \le 1$ for each d dividing $P(z)$. So taking $z = \frac{1}{2}\log x$, we derive from the sieve of Eratosthenes–Legendre that

$$S(\mathscr{A}, \mathscr{P}, z) = x \prod_{p \in \mathscr{P} \cap [2,z)} (1 - 1/p) + O(2^{\log x}).$$

Hence, as $x \to \infty$.

$$S(\mathscr{A}, \mathscr{P}, z) = \delta x + o(x). \tag{6.14}$$

If $\delta = 0$, then $S(\mathscr{A}, \mathscr{P}, z) = o(x)$, and so the number of $n \le x$ as in the lemma statement is also $o(x)$. Hence, the lemma holds in this case. So we can assume that $\delta > 0$, or equivalently, that the sum of the reciprocals of the members of $\mathscr{P}$ is convergent.

In view of (6.14), it is enough to show that the number of $n \le x$ with no prime factor from $\mathscr{P}$ differs from $S(\mathscr{A}, \mathscr{P}, z)$ by only $o(x)$, as $x \to \infty$. But if n is counted in $S(\mathscr{A}, \mathscr{P}, z)$ but not in the lemma statement, then n has a prime factor $p \in \mathscr{P}$ with $p \ge z$, and the number of such $n \le x$ is $\le x \sum_{p \in \mathscr{P} \cap [z,\infty)} \frac{1}{p} = o(x)$. □

We note in passing an amusing consequence of Lemma 6.3: a sieve-based proof of Euler's Theorem 1.4. Indeed, if $\mathscr{P}$ is the set of all primes, then the only integer n not divisible by any $p \in \mathscr{P}$ is $n = 1$, and so Lemma 6.3 shows that $\delta(\mathscr{P}) = 0$. Hence, the sum of the reciprocals of the primes diverges. This argument is due to Pinasco [**Pin09**].

Now to our first application. Consider the function $A(x)$ defined as the number of $n \le x$ for which n can be written as a sum of two squares. For example,

$$A(10^{10}) = 1637624156,$$

so that about 16% of the numbers $n \le 10^{10}$ have such a representation. Does $A(x)/x$ tend to a limit? We prove:

Theorem 6.4. *The set of natural numbers n expressible as a sum of two squares has asymptotic density zero.*

Proof. Using Euler's familiar characterization of sums of two squares, we see that each n counted by $A(x)$ can be written in the form

$$m^2 q, \qquad \text{where } q \text{ is the part of } n \text{ supported on primes} \not\equiv 3 \pmod 4. \tag{6.15}$$

Let $B(t)$ count those natural numbers $q \le t$ not divisible by any prime $\equiv 3 \pmod 4$. Since the sum of the reciprocals of the primes $\equiv 3 \pmod 4$ diverges (cf. Exercise 4.1), Lemma 6.3 implies that $B(t) = o(t)$, as $t \to \infty$.

Our strategy is to partition the n counted by $A(x)$ according to the value of m^2 appearing in the decomposition (6.15): Fix a large real z. For each $m \le z$, the number of sums of two squares $n \le x$ corresponding to m^2 is at most $B(x/m^2) = o(x)$. Since z is fixed, we see that only $o(x)$ sums of two squares correspond to some $m \le z$. But the number of $n \le x$ corresponding to some $m > z$ is at most $\sum_{m>z} x/m^2 \ll x/z$. It follows that $\limsup_{x\to\infty} \frac{A(x)}{x} \ll \frac{1}{z}$. Since z was arbitrary, the theorem is proved. □

Remark. Landau [**Lan08**] has proved the sharper result that the number of $n \le x$ expressible as a sum of two squares is

$$\sim \frac{1}{\sqrt{2}} \left(\prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{p^2}\right) \right)^{-1/2} \frac{x}{\sqrt{\log x}}.$$

The simplest proof of Landau's result seems to be that of Selberg [**Sel91**, pp. 183–185].

In our next example, the hard work consists not in the application of the sieve but in establishing suitable estimates for the terms A_d. Call an integer n a *binary pretender in base g* if the base g expansion of n consists only of the digits 0 and 1. In other words, n is a binary pretender if n is a sum of some finite subset of $\{1, g, g^2, g^3, \dots\}$. We prove:

Theorem 6.5. *For each fixed $g \ge 2$, almost all binary pretenders in base g are composite. More precisely,*

$$\frac{\#\{\textit{prime binary pretenders } n \textit{ with } 0 \le n < x\}}{\#\{\textit{binary pretenders with } 0 \le n < x\}} \to 0, \qquad \textit{as } x \to \infty.$$

To each real number θ, associate the point $e(\theta) := e^{2\pi i\theta}$ on the unit circle, and observe that $e(\theta)$ is a periodic function of θ with period 1. The next lemma follows from the orthogonality relations for characters established in Chapter 4 and the classification of additive characters in Exercise 4.8, but it is easy to give a direct proof.

Lemma 6.6. *If a and d are integers with $d > 0$, then*

$$\frac{1}{d}\sum_{m=0}^{d-1} e(am/d) = \begin{cases} 1 & \textit{if } d \textit{ divides } a, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. If d divides a, then every term in the sum is 1, and the result is clear. Otherwise, $e(a/d) \ne 1$, and the formula for the sum of a geometric series shows that the sum has value $\frac{e(a)-1}{e(a/d)-1} = 0$. □

Lemma 6.7. *Let k be a natural number, and let d be a natural number coprime to g. The number of binary pretenders n in the interval $0 \le n < g^k$ which are divisible by d is*

$$2^k/d + r(d), \quad \textit{where} \quad |r(d)| \le 2^k \exp(-k\pi/d^2).$$

Proof. There are exactly 2^k binary pretenders in the interval $0 \le n < g^k$, namely the 2^k subset sums of $\{1, g, g^2, \dots, g^{k-1}\}$. This already shows that when $d = 1$, the lemma holds with $r(d) = 0$. So we assume henceforth that $d \ge 2$. By Lemma 6.6, the number of n as in the lemma statement is precisely

$$\frac{1}{d}\sum_{m=0}^{d-1}\left(\prod_{j=0}^{k-1}\left(1 + e(g^j m/d)\right)\right). \tag{6.16}$$

The term $m = 0$ contributes $2^k/d$ to (6.16). If $0 < m \le d-1$, then

$$\left|1 + e(g^j m/d)\right| = \left|e\left(-g^j\frac{m}{2d}\right) - e\left(g^j\frac{m}{2d}\right)\right| = 2|\cos(g^j m\pi/d)|.$$

Since d is coprime to g and $d \nmid m$, it follows that $d \nmid g^j m$. Since $|\cos(\pi\theta)|$ is an even function of θ, periodic with period 1, and decreasing on $[0, 1/2]$,

$$\left|1 + e(g^j m/d)\right| \le 2\cos(\pi/d).$$

So using $r(d)$ to denote the contribution to (6.16) from those $m \ne 0$, we have

$$|r(d)| \le 2^k\left(\frac{d-1}{d}\right)\cos(\pi/d)^k. \tag{6.17}$$

Since $\sin(\theta) \ge 2\theta/\pi$ for $0 \le \theta \le \pi/2$,

$$1 - \cos(\pi/d) = \int_0^{\pi/d}\sin(\theta)\,d\theta \ge \int_0^{\pi/d}\frac{2}{\pi}\theta\,d\theta = \frac{\pi}{d^2},$$

and so

$$\cos(\pi/d)^k \le (1 - \pi/d^2)^k \le \exp(-k\pi/d^2).$$

Substituting this estimate back into (6.17) proves the lemma. □

Proof of Theorem 6.5. Squeezing x between two consecutive powers of g, it is enough to show that the number of prime binary pretenders with $0 \le n < g^k$ is $o(2^k)$, as $k \to \infty$.

In the sieve, we let $\mathscr{A}$ be the set of binary pretenders with $0 \le n < g^k$, and we let $\mathscr{P}$ be the set of primes not dividing g. We take $X = 2^k$ and

$\alpha(d) = 1/d$; then by Lemma 6.7, $|r(d)| \le 2^k \exp(-k\pi/d^2)$ for all d dividing $P(z)$. So by the sieve of Eratosthenes–Legendre,

$$S(\mathscr{A}, \mathscr{P}, z) = 2^k \prod_{\substack{p<z \\ p\nmid g}} \left(1 - \frac{1}{p}\right) + O\left(2^k \sum_{d|P(z)} \exp(-k\pi/d^2)\right).$$

If $z = z(k)$ is any function tending to infinity, then the main term here is $\asymp_g 2^k/\log z$, for large k. Since $P(z) \le z^z$, the O-error is

$$\ll 2^k \cdot \tau(P(z)) \cdot \max_{d|P} \left\{\exp(-k\pi/d^2)\right\} \le 2^{k+z} \exp(-k\pi/z^{2z}).$$

We choose

$$z := \frac{1}{4} \frac{\log k}{\log\log k}, \quad \text{so that} \quad z^{2z} < k^{1/2} \qquad \text{for large } k.$$

Then the error is

$$\ll 2^k \exp(-\pi\sqrt{k}) \exp(O(\log k/\log\log k)) \ll 2^k \exp(-\sqrt{k}),$$

while the main term is $\asymp_g 2^k/\log\log k$, which dominates. It follows that $S(\mathscr{A}, \mathscr{P}, z) \asymp_g 2^k/\log\log k$.

Now if $n \in \mathscr{A}$ is prime, then either $n < z$ or n is counted by $S(\mathscr{A}, \mathscr{P}, z)$. Consequently, for large k, the number of primes in $\mathscr{A}$ is $\ll_g 2^k/\log\log k$. □

Remark. This example is adapted from a paper of Filaseta & Konyagin [**FK96**]. There is no base $g > 2$ for which the existence of infinitely many prime binary pretenders has been proved. Filaseta & Konyagin (op. cit.) show that one has somewhat better luck counting squarefree binary pretenders; they prove the expected asymptotic formula for $2 \le g \le 5$. When $g > 5$, it is an open problem to establish the weaker claim that there are infinitely many squarefree binary pretenders in base g.

A problem similar in flavor is that of counting prime palindromes in a given base g. No base g is known for which we can prove there are infinitely many such primes, but Banks, Hart & Sakata [**BHS04**] have shown, by arguments in the same spirit as the proof of Theorem 6.5, that almost all palindromes (in any given base) are composite. Sharper results have been obtained by Col [**Col09**], who gets an upper bound in this problem of the expected correct order. Col also shows, using a lower-bound sieve, that there are infinitely many palindromes in base 10 which have at most 372 prime factors (counted with multiplicity).

4. Brun's pure sieve

4.1. Combinatorial foundations. The essence of Brun's pure sieve is the following intuitively plausible result: After every inclusion in the principle of inclusion-exclusion, we have an upper bound for the number of elements we are trying to count, and after each exclusion, we have a lower bound on the same number. Stated formally:

Theorem 6.8 (Bonferroni inequalities)**.** *Let X be a nonempty, finite set of N objects, and let $P_1, \dots, P_r$ be properties that elements of X may have. For each subset $I \subset \{1, 2, \dots, r\}$, let $N(I)$ denote the number of elements of X that have each of the properties indexed by the elements of I. Let N_0 denote the number of elements of X with none of these properties. Then if m is a nonnegative even integer,*

$$N_0 \le \sum_{k=0}^{m} (-1)^k \sum_{\substack{I \subset \{1,2,\dots,r\} \\ |I|=k}} N(I), \tag{6.18}$$

while if m is a nonnegative odd integer,

$$N_0 \ge \sum_{k=0}^{m} (-1)^k \sum_{\substack{I \subset \{1,2,\dots,r\} \\ |I|=k}} N(I). \tag{6.19}$$

The goal of this section is to prove Theorem 6.8. The key is the following lemma, for which we offer two proofs. The first is very short, but the second will be important for our treatment of the Brun–Hooley sieve in Chapter 7.

Lemma 6.9. *Let n be a positive integer. Then the alternating sum*

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k}$$

is nonnegative or nonpositive according to whether m is even or odd.

Proof. By induction on m, one easily finds that

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k} = (-1)^m \binom{n-1}{m}, \tag{6.20}$$

which makes Lemma 6.9 obvious. As an alternative to induction, (6.20) follows by comparing the coefficient of x^m in both sides of the power series identity $(1-x)^{n-1} = (1-x)^{-1}(1-x)^n$. □

Proof of Theorem 6.8. Suppose that $x \in X$ has exactly l of the properties $P_1, \dots, P_r$. If $l = 0$, then x is counted once by both N_0 and the common right-hand side of (6.18) and (6.19) (in the term corresponding to $I = \emptyset$). If $l \ge 1$, then x is not counted at all by N_0, and is counted by this right-hand sum with weight

$$\sum_{k=0}^{m} (-1)^k \binom{l}{k} \begin{cases} \ge 0 & \text{if } m \text{ is even,} \\ \le 0 & \text{otherwise.} \end{cases}$$

Summing over $x \in X$ gives the theorem. □

Our second proof of Lemma 6.9 requires a bit of new notation: If $a_1, \dots, a_n$ is a (possibly empty) sequence of $n \geq 0$ elements belonging to a commutative ring, we define (for $k \geq 0$) the kth elementary symmetric function $\sigma_k(a_1, \dots, a_n)$ as the sum of all possible $\binom{n}{k}$ products of the a_i taken k at a time. We adopt the usual conventions about empty sums and products. Thus, when $n = 0$, we have $\sigma_0 = 1$ and $\sigma_k = 0$ for $k > 0$. To take a less pathological example, when $n = 2$, one has

$$\sigma_0(a_1, a_2) = 1, \quad \sigma_1(a_1, a_2) = a_1 + a_2, \quad \sigma_2(a_1, a_2) = a_1 a_2,$$

and $\sigma_k(a_1, a_2) = 0$ for $k > 2$. The following lemma of Hooley [**Hoo94**] is an elegant generalization of Lemma 6.9:

Lemma 6.10. *Suppose $0 \leq a_1, \dots, a_n \leq 1$, where n is nonnegative. The difference*

$$\sum_{k=0}^{m} (-1)^k \sigma_k(a_1, \dots, a_n) - \prod_{j=1}^{n} (1 - a_j) \tag{6.21}$$

is nonnegative or nonpositive according to whether m is even or odd, respectively.

Remarks.

(i) Observe that (6.21) vanishes when $m \geq n$.

(ii) Let $n \in \mathbf{N}$ and let $a_1 = a_2 = \cdots = a_n = 1$. Then

$$\prod_{i=1}^{n}(1 - a_i) = 0, \quad \text{while} \quad \sigma_k(1, \dots, 1) = \binom{n}{k}.$$

So Lemma 6.9 follows immediately from Lemma 6.10.

Proof. We induct on the length n of the sequence $a_1, \dots, a_n$. When $n = 0$, the product $P := \prod_{i=1}^{n}(1 - a_i)$ appearing in (6.21) is empty, so equal to 1, while

$$\sum_{k=0}^{m} (-1)^k \sigma_k = 1 - 0 + 0 - \cdots \pm 0 = 1.$$

Hence (6.21) vanishes for every m, confirming the result in this case. Now assume that the result holds for each sequence of n real numbers in $[0, 1]$ and each m, and consider an arbitrary sequence $0 \leq a_1, \dots, a_{n+1} \leq 1$ of length

$n+1$. By the induction hypothesis, it suffices to prove that

$$\left(\sum_{k=0}^{m}(-1)^k\sigma_k(a_1,\dots,a_{n+1})-\prod_{i=1}^{n+1}(1-a_i)\right) - \left(\sum_{k=0}^{m}(-1)^k\sigma_k(a_1,\dots,a_n)-\prod_{i=1}^{n}(1-a_i)\right) \tag{6.22}$$

is nonnegative or nonpositive according to whether m is even or odd respectively. This is easily seen to hold for $m=0$, since then (6.22) simplifies to Pa_{n+1}, which is nonnegative. When $m>0$, we can rewrite (6.22) as

$$\begin{aligned}\sum_{k=1}^{m}(-1)^k\left(\sigma_k(a_1,\dots,a_{n+1})-\sigma_k(a_1,\dots,a_n)\right)+Pa_{n+1}&\\ =\sum_{k=1}^{m}(-1)^k a_{n+1}\sigma_{k-1}(a_1,\dots,a_n)+Pa_{n+1}&\\ =a_{n+1}\left(P-\sum_{k=0}^{m-1}(-1)^k\sigma_k(a_1,\dots,a_n)\right).&\end{aligned}$$

The claim in this case now follows from the induction hypothesis. □

4.2. Brun's pure sieve: Statements. As was the case for the principle of inclusion-exclusion (Theorem 6.1), Theorem 6.8 has immediate consequences in the sieve context.

Corollary 6.11 (Brun's pure sieve, general form)**.** *With the notation of §2, we have for every nonnegative even integer m,*

$$\sum_{d\mid P,\ \omega(d)\le m-1}\mu(d)A_d\le S(\mathscr{A},\mathscr{P})\le\sum_{d\mid P,\ \omega(d)\le m}\mu(d)A_d.$$

Proof. As in the proof of Theorem 6.2, let $p_1,\dots,p_r$ be a list of the primes $p\in\mathscr{P}$, and let P_i be the property of being divisible by p_i. We aim to estimate the number $S(\mathscr{A},\mathscr{P})$ of elements of $\mathscr{A}$ possessing none of the P_i. The upper bound for $S(\mathscr{A},\mathscr{P})$ in the corollary is just (6.18). If $m=0$, then the lower bound is trivial, while if $m>0$, then $m-1$ is a nonnegative odd integer and the lower bound follows from (6.19). □

To obtain a result suitable for applications, we substitute above the relation $A_d=X\alpha(d)+r(d)$. With a bit of manipulation, we arrive at the following theorem:

Theorem 6.12 (Brun's pure sieve)**.** *For every even integer* $m \geq 0$*,*

$$S(\mathscr{A}, \mathscr{P}) = X \prod_{p \in \mathscr{P}} (1 - \alpha(p)) + O\Bigg(\sum_{d \mid P,\ \omega(d) \leq m} |r(d)|\Bigg) + O\Bigg(X \sum_{d \mid P,\ \omega(d) \geq m} \alpha(d)\Bigg).$$

Here the implied constants are absolute.

Proof. From Corollary 6.11,

$$\begin{aligned} S(\mathscr{A}, \mathscr{P}) &= \sum_{\substack{d \mid P \\ \omega(d) \leq m}} \mu(d) A_d + O\Bigg(\sum_{\substack{d \mid P \\ \omega(d) = m}} A_d\Bigg) \\ &= \sum_{\substack{d \mid P \\ \omega(d) \leq m}} \mu(d)(X\alpha(d) + r(d)) + O\Bigg(\sum_{\substack{d \mid P \\ \omega(d) = m}} A_d\Bigg) \\ &= X \sum_{\substack{d \mid P \\ \omega(d) \leq m}} \mu(d)\alpha(d) + O\Bigg(\sum_{\substack{d \mid P \\ \omega(d) \leq m}} |r(d)|\Bigg) + O\Bigg(\sum_{\substack{d \mid P \\ \omega(d) = m}} A_d\Bigg). \end{aligned}$$

Writing $A_d = X\alpha(d) + r(d)$, we see that the last of these error terms is

$$\ll X \sum_{d \mid P,\ \omega(d) = m} \alpha(d) + \sum_{d \mid P,\ \omega(d) = m} |r(d)|;$$

hence,

$$(6.23) \quad S(\mathscr{A}, \mathscr{P}) = X \sum_{\substack{d \mid P \\ \omega(d) \leq m}} \mu(d)\alpha(d) + O\Bigg(\sum_{\substack{d \mid P \\ \omega(d) \leq m}} |r(d)|\Bigg) + O\Bigg(X \sum_{\substack{d \mid P \\ \omega(d) = m}} \alpha(d)\Bigg).$$

In order to factor the sum appearing in the main term, we extend the sum to all d dividing P; the main term can then be expressed as $X \prod_{p \in \mathscr{P}} (1 - \alpha(p))$, but we have introduced a new error of

$$\ll X \sum_{d \mid P, \omega(d) > m} \alpha(d).$$

If this is combined with the last error term of (6.23), we find that

$$S(\mathscr{A}, \mathscr{P}) = X \prod_{p \in \mathscr{P}} (1 - \alpha(p)) + O\Bigg(\sum_{d \mid P,\ \omega(d) \leq m} |r(d)|\Bigg) + O\Bigg(X \sum_{d \mid P,\ \omega(d) \geq m} \alpha(d)\Bigg),$$

exactly as the theorem asserts. □

4.3. Applications. In this section, we illustrate the utility of Brun's pure sieve by zeroing in on Example (ii) of §2. Recall that in §3, we showed that

$$\pi_2(x,z) \sim 2C_2 e^{-2\gamma} \frac{x}{(\log z)^2} \qquad \text{as } x \to \infty, \tag{6.24}$$

if $z = \frac{1}{2}\log x$. (In fact, it is clear that the argument goes through whenever $z = z(x) \to \infty$ and $z \le \frac{1}{2}\log x$.) From this, we deduced from (6.5) that $\pi_2(x) \ll x/(\log\log x)^2$. Our goal in this section is to show that, in fact, the asymptotic (6.24) holds whenever $z = z(x) \to \infty$ and

$$z(x) \le x^{\frac{1}{20\log\log x}}. \tag{6.25}$$

This immediately implies, via (6.5), that

$$\pi_2(x) \ll \frac{x(\log\log x)^2}{(\log x)^2}. \tag{6.26}$$

So suppose now that $z = z(x) \to \infty$ but satisfies (6.5). Keeping the notation from Example (ii), Brun's pure sieve (Theorem 6.12) shows that

$$\begin{aligned} &\pi_2(x,z) = \\ &\quad x\prod_{p\le z}(1-\alpha(p)) + O\Bigg(\sum_{d\mid P,\ \omega(d)\le m} 2^{\omega(d)}\Bigg) + O\Bigg(x\sum_{d\mid P,\ \omega(d)\ge m}\alpha(d)\Bigg), \end{aligned} \tag{6.27}$$

for each even number $m \ge 0$. We take

$$m := 10\lfloor \log\log z\rfloor.$$

Note that as x goes to infinity, so does z and hence also m. In §3, we calculated that the main term of (6.27) is $\sim 2C_2e^{-2\gamma}x/(\log z)^2$, as $x \to \infty$. Thus, it is enough to establish the following two estimates:

(i) With $E_1 := \sum_{d\mid P,\ \omega(d)\le m} 2^{\omega(d)}$, we have $E_1 = o(x/(\log z)^2)$.

(ii) With $E_2 := x\sum_{d\mid P,\ \omega(d)\ge m}\alpha(d)$, we have $E_2 = o(x/(\log z)^2)$.

Proof of (i). For large x,

$$\begin{aligned} E_1 = \sum_{d\mid P,\ \omega(d)\le m} 2^{\omega(d)} &= \sum_{k=0}^{m} 2^k\binom{\pi(z)}{k} \le \sum_{k=0}^{m}(2\pi(z))^k \\ &\le \sum_{k=-\infty}^{m}(2\pi(z))^k = (2\pi(z))^m\frac{1}{1-\frac{1}{2\pi(z)}} \le 2(2\pi(z))^m \le 2z^m, \end{aligned}$$

since $\pi(z) \le z/2$ for large x. Hence,

$$E_1 \le 2z^{10\log\log z} \le 2z^{10\log\log x} \le 2x^{1/2}.$$

This upper bound is certainly $o(x/(\log z)^2)$, since as $x \to \infty$,

$$\frac{x^{1/2}}{x/(\log z)^2} \le \frac{x^{1/2}}{x/(\log x)^2} = \frac{(\log x)^2}{x^{1/2}} \to 0. \qquad \square$$

Proof of (ii). We can write $E_2 = x \sum_{k \ge m} \sum_{d|P,\ \omega(d)=k} \alpha(d)$. For the inner sum, we have

$$\sum_{\substack{d|P \\ \omega(d)=k}} \alpha(d) = \sum_{p_1<p_2<\cdots<p_k\le z} \alpha(p_1)\alpha(p_2)\cdots\alpha(p_k) \le \frac{1}{k!}\left(\sum_{p\le z}\alpha(p)\right)^k.$$

Here the upper bound comes from the multinomial theorem: In the expansion of $(\sum_{p\le z}\alpha(p))^k$, every term $\alpha(p_1)\cdots\alpha(p_k)$ appears with coefficient $k!$. From Mertens' first theorem, we have $\sum_{p\le z} p^{-1} \le \log\log z + c$ for $z \ge 3$, where c is an absolute constant. Since $\alpha(p) \le 2/p$ for every prime p,

$$\sum_{k\ge m}\frac{1}{k!}\left(\sum_{p\le z}\alpha(p)\right)^k \le \sum_{k\ge m}\frac{1}{k!}(2\log\log z + 2c)^k. \tag{6.28}$$

The ratio of the $(k+1)$th term in the right-hand series to the kth is given by

$$\frac{2\log\log z + 2c}{k+1} \le \frac{2\log\log z + 2c}{10\lfloor\log\log z\rfloor + 1} \le \frac{1}{2},$$

for large enough z, and hence also for large enough x. For such x, the right-hand sum in (6.28) is bounded above by twice its first term, by comparison with a geometric series. Because

$$e^m = 1 + m + m^2/2! + m^3/3! + \cdots \ge m^m/m!,$$

we have $m! \ge (m/e)^m$, so that

$$\sum_{k\ge m}\frac{1}{k!}(2\log\log z + 2c)^k \le 2\left(\frac{2e\log\log z + 2ce}{m}\right)^m.$$

Since $m = 10\lfloor\log\log z\rfloor$, the parenthetical expression on the right is eventually smaller than any constant exceeding $2e/10$; in particular, it is eventually smaller than $3/5$.

It follows that for large x,

$$\begin{aligned} E_2 \le 2x(3/5)^m &= 2x(3/5)^{10\lfloor\log\log z\rfloor} \\ &\ll x(3/5)^{10\log\log z} \ll x/(\log z)^5, \end{aligned}$$

since $10\log\frac{3}{5} < -5$. So $E_2 = o(x/(\log z)^2)$. $\square$

This proof may appear a bit magical. Why did we choose m the way we did? And why did we need to restrict z by (6.25)? In answer to the first question, a careful study of our analysis of E_2 reveals that we needed m to be at least a bit larger than $2e \log\log z$ in order to guarantee even that E_2 had smaller order than x. We chose $m = 10\lfloor \log\log z \rfloor$ to get the stronger result that $E_2 = o(x/(\log z)^2)$. We can explain the restriction on z similarly: In order to guarantee that E_1 had smaller order than x, our argument required that z^m have smaller order than x. Since m is about $10 \log\log z$, we chose z so that $z^{10 \log\log z}$ was quite a bit smaller than x.

As promised in the introduction, we deduce from (6.26) the convergence of the reciprocal sum of the twin primes:

Corollary 6.13. *If there are infinitely many primes p for which $p+2$ is also prime, then the sum*

$$\sum_p \frac{1}{p},$$

taken over all such primes, converges.

Proof. Weakening (6.26) somewhat, we see that $\pi_2(x) \ll x/(\log x)^{3/2}$ for all $x \geq 3$. Letting p_n denote the nth prime p for which $p+2$ is also prime, we see that for $n \geq 1$,

$$n = \pi_2(p_n) \ll p_n/(\log p_n)^{3/2},$$

so that

$$p_n \gg n(\log p_n)^{3/2} \geq \frac{n+1}{2}(\log(n+1))^{3/2}.$$

The comparison and integral tests together now imply that $\sum_{n=1}^{\infty} p_n^{-1}$ converges, which is the assertion of the corollary. $\square$

Examples. We say a few words about what Brun's pure sieve yields for Examples (i), (iii), and (iv) introduced in §2. In each case, the situation is analogous to what we have just seen with Example (ii).

- In (i), where one is sieving for primes, we can now show that the asymptotic formula $\pi(x,z) \sim e^{-\gamma}\frac{x}{\log z}$ holds for any function $z = z(x) \to \infty$ satisfying $z(x) \leq x^{\frac{1}{10 \log\log x}}$. This implies that $\pi(x) \ll \frac{x}{\log x}\log\log x$, which is nearly as sharp as Chebyshev's upper bound.
- In (iii), where one is sieving for primes of the form n^2+1, one obtains that $S(\mathscr{A}, \mathscr{P}, z) \sim \frac{1}{2}x\prod_{p<z, p\equiv 1 \pmod 4}(1-2/p)$ for any $z = z(x) \to \infty$ with $z(x) \leq x^{\frac{1}{10\log\log x}}$. Consequently, $\pi_{T^2+1}(x) \ll \frac{x}{\log x}\log\log x$.

- In (iv), one can show that

$$S(\mathscr{A},\mathscr{P},z) \sim 2C_2 e^{-2\gamma}\left(\prod_{\substack{p\mid N\\ 2<p<z}} \frac{p-1}{p-2}\right)\frac{N}{(\log z)^2},$$

whenever $z = z(N) \to \infty$ and $z(N) \le N^{\frac{1}{20\log\log N}}$. Consequently,

$$R(N) \ll \left(\prod_{p\mid N,\ p>2} \frac{p-1}{p-2}\right)\frac{N}{(\log N)^2}(\log\log N)^2. \tag{6.29}$$

The reader who wishes to solidify her understanding of Brun's pure sieve should attempt to adapt the argument given in the twin prime case above to treat one or more of these examples.

Notes

For historical reasons, in place of the series appearing in Corollary 6.13 one usually sees the slight variant

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots.$$

Of course this series also converges (by comparison with that of the corollary), and its value B is known as *Brun's constant*. Computing the value of B to any precision seems to be difficult; while constants like π and e are known to billions of decimal digits, the sharpest known bounds on B are (roughly)

$$1.830 < B < 2.347.$$

Thus we do not know B to even one significant digit! The lower bound here is due to Sebah [**SG**], who computed all the twin prime pairs up to 10^{16} and summed their reciprocals. The upper bound is due to Crandall & Pomerance ([**CP05**, pp. 16-17], see also [**Kly07**, Chapter 3]), who bound the reciprocal sum past 10^{16} using an explicit upper estimate of Riesel and Vaughan [**RV83**] for the number of twin prime pairs. Much sharper estimates for Brun's constant are available if one assumes a suitable quantitative version of the twin prime conjecture; e.g., it is plausible that

$$B = 1.902160583121 \pm 4.08\times 10^{-8}.$$

This last estimate is taken from the Ph.D. thesis of Klyve [**Kly07**], which the reader should consult for references to earlier work.

Exercises

1. (Gandhi [**Gan71**], Golomb [**Gol74**]) For each set of natural numbers S, put $w(S) := \sum_{n\in S} 2^{-n}$. For each natural number k, let p_k denote the kth prime.
   (a) If S is the set of natural numbers coprime to $p_1 \cdots p_k$, show that $w(S) = \frac{1}{2} + \frac{1}{2^{p_{k+1}}} + E$ where $0 < E < \frac{1}{2^{p_{k+1}}}$.
   (b) Show that for the set S in (a), we have $w(S) = \sum_{d\mid p_1\cdots p_k} \frac{\mu(d)}{2^d-1}$.
   (c) Deduce that p_{k+1} is the unique integer for which
$$1 < 2^{p_{k+1}}\left(\sum_{d\mid p_1\cdots p_k} \frac{\mu(d)}{2^d-1} - \frac{1}{2}\right) < 2.$$

† 2. (Cf. Nagell [**Nag22**, §3]) This exercise generalizes Example (iii) of §2.
   (a) Let D be an integer that is not a square. Using the law of quadratic reciprocity, prove that there is a collection S (say) of $\frac{1}{2}\varphi(4|D|)$ residue classes modulo $4|D|$ with the property that for each prime $p \nmid 4D$, $\left(\frac{D}{p}\right) = 1 \iff p \bmod 4|D| \in S$.
   (b) Deduce from (a) and the results of Chapter 4 that
$$\sum_{p\le x,\ \left(\frac{D}{p}\right)=1} \frac{\log p}{p} = \frac{1}{2}\log x + O(1),$$
   where the implied constant may depend on D. (Thus, in a certain average sense, D is a square modulo precisely $\frac{1}{2}$ of all primes.)
   (c) Let $F(T)$ be a quadratic polynomial with integer coefficients. Using the sieve of Eratosthenes–Legendre, show that as $x \to \infty$, the number of $n \le x$ with $|F(n)|$ prime is $\ll_F x/\log\log x$.

3. (cf. Hofmeister & Stoll [**HS85**])
   (a) Prove that there are infinitely many natural numbers n for which the equation
$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} \tag{6.30}$$
   has no solution in positive integers x and y.
   (b) Show that if n has a positive divisor of the form $4k-1$, say $n = (4k-1)q$, then
$$\frac{4}{n} = \frac{1}{qk} + \frac{1}{q(4k^2-k)}.$$
   Using Lemma 6.3, deduce that equation (6.30) has a solution for almost all natural numbers n. (For a continuation, see Exercise 14.)

4. Use the inclusion-exclusion principle to establish each of the following assertions about squarefree numbers:
   (a) The number of squarefree $n \le x$ is asymptotic to $\frac{1}{\zeta(2)}x = \frac{6}{\pi^2}x$ as $x \to \infty$.
   (b) The number of pairs of squarefree integers $n, n+2$ with $1 \le n \le x$ is asymptotic to $x \prod_p (1 - 2/p^2)$ as $x \to \infty$.
   (c) The number of ordered representations of a natural number N as a sum of two positive squarefree integers is asymptotic to
$$N \prod_p \left(1 - \frac{2}{p^2}\right) \prod_{p^2 \mid N} \frac{p^2-1}{p^2-2} \qquad (N \to \infty).$$
   Hint: For each of (a)–(c), first sieve out the multiples of p^2 for $p \le z$, where $z = z(x) \to \infty$ slowly enough to keep the error term in check. To conclude, observe that almost no n are divisible by p^2 for some prime $p > z$, since $\sum_{p>z} \frac{1}{p^2}$ is $o(1)$.

† 5. (Rényi [**Rén55**])
   (a) Show that for each fixed integer $j \ge 0$, the set of natural numbers n with $\Omega(n) - \omega(n) = j$ possesses an asymptotic density d_j (say). Check that $\sum_{j=0}^{\infty} d_j = 1$.
   (b) Show that for all complex numbers z with $|z| < 2$, we have
$$\sum_{j=0}^{\infty} d_j z^j = \frac{1}{\zeta(2)} \prod_p \left(1 - \frac{z}{p+1}\right)\left(1 - \frac{z}{p}\right)^{-1}.$$

† 6. (Hooley [**Hoo76**], Rieger [**Rie77**]) If m is an odd natural number, write $l(m)$ for the order of 2 modulo m.
   (a) Suppose $m \in \mathbf{N}$ is odd and squarefree and put $M := \operatorname{lcm}[m, l(m)]$. Show that $n \cdot 2^n$ runs through every residue class modulo m exactly M/m times as n runs over the integers $1, 2, 3, \dots, M$.
   (b) Using the result of (a) and the sieve of Eratosthenes–Legendre, show that the set of $n \in \mathbf{N}$ for which $n \cdot 2^n + 1$ is prime has density zero. (Primes of the form $n \cdot 2^n + 1$ are called *Cullen primes*; the first several examples correspond to $n = 1$, 141, 4713, 5795, 6611, 18496, 32292.)

7. Let A and B be subsets of the natural numbers defined by
$$A = \{n : n \mid 2^k - 1 \text{ for some positive integer } k\},$$
$$B = \{n : n \mid 2^k + 1 \text{ for some positive integer } k\}.$$
   Prove that A has asymptotic density $\frac{1}{2}$ and B has asymptotic density 0.

† 8. (Ballot & Luca [**BL07**]; cf. Luca [**Luc06**, Problem 190]) Let F_n denote the nth Fibonacci number, so that $F_0 = 0$, $F_1 = 1$, and for $n > 1$, $F_n = F_{n-1} + F_{n-2}$. Show that the set of n for which F_n can be written

as a sum of two coprime squares has asymptotic density 1/2. For a challenge, prove the same with the word "coprime" removed.

9. Show that for each $d \in \mathbf{N}$, the set of natural numbers n for which $d \mid \varphi(n)$ has asymptotic density 1. Deduce that the set of n for which $\gcd(n, \varphi(n)) = 1$ has density zero.

† 10. (Continuation; cf. Pillai [**Pil29**]) Let $\mathscr{V} := \{\varphi(m) : m \in \mathbf{N}\}$ be the image of the Euler φ-function, and let $V(x)$ be the number of $n \leq x$ belonging to $\mathscr{V}$. Show that $V(x) = o(x)$. *Hint:* Divide the elements n of $\mathscr{V}$ into two classes, depending on whether or not n has a preimage m with only a "small" number of distinct odd prime divisors.

Remark. Maier & Pomerance [**MP88**] showed in 1988 that

$$V(x) = \frac{x}{\log x} \exp((C + o(1))(\log\log\log x)^2)$$

for a constant $C = 0.81781464640\ldots$. This improved upon earlier results of Erdős, Hall, and Pomerance. The (somewhat complicated) exact order of magnitude of $V(x)$ was subsequently determined by Ford [**For98a, For98b**].

11. Show that the number of triples of primes $p, p+2, p+6$ with $p \leq x$ is $\ll x(\log\log x)^3/(\log x)^3$, for $x \geq 3$.

12. Call a prime p *M-reclusive* if $|q - p| > M$ for every prime $q \neq p$. Show that for every $M > 0$ and every $k \in \mathbf{N}$, there are infinitely many k-tuples of consecutive primes all of which are M-reclusive. (This strengthens the result of Exercise 4.14.)

13. (Blecksmith, Erdős & Selfridge [**BES99**]) Say that a prime p is *a cluster prime* if every even natural number $n < p-2$ can be written in the form $q - q'$, where q and q' are primes $\leq p$.
    (a) Check (perhaps with the aid of a computer) that every prime $p < 97$ is a cluster prime, but that $p = 97$ is not.
    (b) Show that if p is a cluster prime, then for every integer $3 \leq t \leq p-3$, the number of primes in the closed interval $[p-t, p]$ is $\gg \log t$, where the implied constant is absolute. In other words, the primes to the left of p have to "cluster" around p.
    (c) Show that contrary to what one might expect from (a), the cluster primes are comparatively rare: For every k, the number of cluster primes up to x is $O_k(x/(\log x)^k)$, as $x \to \infty$.

14. (Yang [**Yan82**]; see also Webb [**Web70**]) Erdős & Straus [**Erd50a**] conjectured that the equation

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$

has a solution for every $n > 1$; for example, $\frac{4}{301} = \frac{1}{76} + \frac{1}{7626} + \frac{1}{87226188}$. Using the identities

$$\frac{4}{n} = \begin{cases} \frac{1}{n(k+1)k} + \frac{1}{n(k+1)} + \frac{1}{qk} & \text{if } n = (4k-1)q, \\ \frac{1}{nk} + \frac{1}{nqk} + \frac{1}{qk} & \text{if } n+1 = (4k-1)q, \\ \frac{1}{nk} + \frac{1}{nk(qk-1)} + \frac{1}{qk-1} & \text{if } n+4 = (4k-1)q, \\ \frac{1}{nk} + \frac{1}{k(qk-n)} + \frac{1}{n(qk-n)} & \text{if } 4n+1 = (4k-1)q, \end{cases}$$

show that the number of $n \le x$ for which the Erdős–Strauss equation is unsolvable is $\ll \frac{x(\log\log x)^2}{(\log x)^2}$, for $x \ge 3$. Deduce that the sum of the reciprocals of all n of this kind converges.

Remark. Vaughan [**Vau70**] has shown that the number of counterexamples $n \le x$ to the Erdős–Strauss conjecture is $\le x\exp(-c(\log x)^{2/3})$ for a certain constant $c > 0$.

† 15. (Cf. Erdős [**Erd36**]) For each $r \in \mathbf{N}$, define a function $p_r \colon \mathbf{N} \to \{\text{primes}\} \cup \{\infty\}$ by setting $p_r(n)$ equal to the rth smallest prime factor of n if n has at least r distinct prime factors and putting $p_r(n) = \infty$ otherwise. Observe that $p_1(n) < p_1(n+1)$ precisely when n is even. In particular, $p_1(n) < p_1(n+1)$ on a set of asymptotic density $1/2$. Show that for each fixed r, we have $p_r(n) < p_r(n+1)$ on a set of asymptotic density $1/2$.

Remark. For each $n > 1$, put $P(n)$ equal to the largest prime factor of n, and put $P(1) = 0$. In the 1930s, Erdős conjectured that $P(n) < P(n+1)$ on a set of asymptotic density $1/2$. This remains open. Erdős & Pomerance have shown that each of the inequalities $P(n) > P(n+1)$ and $P(n) < P(n+1)$ holds for a positive proportion of the natural numbers [**EP78**].

16. For each even natural number N, let $R^*(N)$ be the number of *unordered* representations of N as a sum of two primes. Then

$$R^*(N) \le \pi(N-2) - \pi((N-1)/2),$$

with equality holding exactly when $N - p$ is prime for each prime p with $N/2 \le p \le N-2$. Use the estimates (3.16) and (6.29) to prove that this upper bound is attained for only finitely many N.

Remark. It has been shown by Deshouillers et al. [**DGNP93**] that $N = 210$ is the largest value for which the upper bound is achieved.

† 17. (Hardy & Littlewood [**HL23**], cf. Landau [**Lan00**]) Let $R(N)$ be the number of ordered representations of N as a sum of two primes. Conjecture 3.19 asserts that as $N \to \infty$ through even numbers,

$$R(N) = (A + o(1)) \left(\prod_{p \mid N} \frac{p-1}{p-2} \right) \frac{N}{(\log N)^2}, \tag{6.31}$$

where

$$A = 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2} \right). \tag{6.32}$$

This differs from what a naive sieve argument would suggest, namely that (6.31) holds with

$$A = 8 \exp(-2\gamma) \prod_{p>2} \left(1 - \frac{1}{(p-1)^2} \right). \tag{6.33}$$

In this exercise we outline a proof that (6.33) cannot be correct. In fact, we show that if an asymptotic relation of the form (6.31) holds, then A must be given by (6.32).

(a) Use the prime number theorem to show that $\sum_{N \le x} R(N) \sim \frac{1}{2} \frac{x^2}{(\log x)^2}$ as $x \to \infty$.

(b) Deduce from (a) that as $x \to \infty$,

$$\sum_{2 \le N \le x} \frac{R(N)}{N/(\log N)^2} \sim x.$$

(c) Put $g(N) := \prod_{p \mid N, p>2} \frac{p-1}{p-2}$ for each N, and define an arithmetic function h by the relation $g(N) = \sum_{d \mid N} h(d)$. Show that h is supported on odd, squarefree positive integers, and that as $x \to \infty$,

$$\frac{1}{x} \sum_{\substack{N \le x \\ N \text{ even}}} g(N) \to \frac{1}{2} \sum_{d \text{ odd}} \frac{h(d)}{d} = \frac{1}{2} \prod_{p>2} \frac{(p-1)^2}{p(p-2)}.$$

(d) Use the result of (c) and the purported relation (6.31) to derive another asymptotic formula for $\sum_{2 \le N \le x} \frac{R(N)}{N/(\log N)^2}$ which, when compared with that of (b), proves (6.32).

Remark. It is now known that the relation (6.31) with A given by (6.32) holds for almost all even natural numbers N (see, e.g, [**Vau97**, §3.2]). More precisely, (6.31) holds (with this A) as $N \to \infty$ through even numbers, provided we exclude a particular set of even numbers N of asymptotic density zero.

Chapter 7

Sieve Methods, II

> When I encountered Brun's sieve for the first time, I was reminded of the legend that Alexander the Great cut with his sword the intricate knot of Phrygian King Gordius, and proceeded to Asia. In fact, in my mind Brun is mightier than the great king, for he cut the enigmatic knot that had survived 2100 years without any sign of wear. – Y. Motohashi [**Mot05**]

1. Introduction

In Chapter 6, we proved that with $\pi_2(x)$ denoting the number of twin prime pairs $p, p+2$ with $p \le x$,

$$\pi_2(x) \ll \frac{x}{(\log x)^2}(\log\log x)^2, \tag{7.1}$$

for $x \ge 3$. A cognate result was also established in the context of Goldbach's conjecture: With $R(N)$ denoting the number of representations of the natural number N as a sum of two primes, we have

$$R(N) \ll \left(\prod_{\substack{p \mid N \\ p>2}} \frac{p-1}{p-2}\right)\frac{N}{(\log N)^2}(\log\log N)^2.$$

These theorems constitute nontrivial progress, on the upper bound side, towards the quantitative forms of the twin prime and Goldbach conjectures discussed in §5 of Chapter 3. But neither is entirely satisfactory; in each case, there is a bothersome extra log log-factor on the right-hand side over and above what we expect to be the truth.

In a seminal 1920 paper [**Bru20**] (announcement in [**Bru19b**]), Brun described how to establish upper bounds in these problems free of the pesky $\log\log$-factors. That is, he proved upper bounds on $\pi_2(x)$ and $R(N)$ agreeing in order of magnitude with the conjectured asymptotics. The same sieve method allowed him to prove the following two *almost-prime* results. In the sequel, we say a number n is an *r-almost prime* if $\Omega(n) \le r$.

- There are infinitely many pairs of 9-almost primes $n, n+2$.
- Every large even integer N is a sum of two 9-almost primes.

These striking results are just out of reach of the techniques detailed in Chapter 6. Recall the way we approached the twin prime problem as a sieve problem, first described in Example (ii) of Chapter 6, §2. Here $\mathscr{A}$ was the sequence of numbers $\{n(n+2)\}_{n\le x}$, $\mathscr{P}$ was the set of primes $\le z$, and our attack on the twin prime problem went through estimates for $S(\mathscr{A},\mathscr{P})$.[1] The naive expectation in this case is that

$$S(\mathscr{A},\mathscr{P}) \approx 2C_2 e^{-2\gamma}\frac{x}{(\log z)^2}. \tag{7.2}$$

We have seen reasons to be suspicious of (7.2) for large values of z (e.g., $z \approx x^{1/2}$), but for small values of z, we saw already in Chapter 6 that this approximation holds good. Indeed, we proved (7.1) by showing that (7.2) is valid as an asymptotic formula whenever

$$z = z(x) \to \infty, \quad \text{and} \quad z(x) \le x^{\frac{1}{20\log\log x}}. \tag{7.3}$$

The upper bound on z in (7.3) has the form $x^{o(1)}$. This is a limit of the method; the reader can convince herself that Brun's pure sieve yields no result if we sieve up to a power of x.

Brun's breakthrough was the realization that formulas like (7.2) retained their validity, suitably interpreted, in a wider range of z than the sort appearing in (7.3). Let $\mathscr{P}$ be the set of all primes. In the twin prime problem, Brun's method shows that the not-quite-asymptotic formula

$$S(\mathscr{A},\mathscr{P},z) \asymp \frac{x}{(\log z)^2} \tag{7.4}$$

holds whenever

$$z = z(x) \to \infty, \quad \text{and} \quad z(x) \le x^{\frac{1}{9.9}}.$$

From this, the aforementioned results follow quickly: For example, taking $z = x^{1/9.9}$ in (7.4), the upper bound aspect of (7.4) yields the $\log\log$-free estimate

$$\pi_2(x) \ll x/(\log x)^2.$$

[1]We could also let $\mathscr{P}$be the set of all primes and write $S(\mathscr{A},\mathscr{P},z)$ here. However, there is then a minor discrepancy with our work in Chapter 6, since our definition of $S(\mathscr{A},\mathscr{P},z)$ stipulates that we sieve only up to primes *strictly less* than z. This is a negligible change and will not be important in what follows.

Suppose now that n is counted in $S(\mathscr{A}, \mathscr{P}, x^{1/9.9})$, so that $n \le x$ and every prime factor of n and $n+2$ exceeds $x^{1/9.9}$. For large x,

$$n < n + 2 < (x^{1/9.9})^{10}.$$

Hence, both n and $n+2$ have at most 9 prime factors. So from the lower bound in (7.4), Brun's almost-prime result towards the twin prime conjecture follows. Brun's results on the Goldbach conjecture are proved analogously, but now one chooses the sieving parameters in accord with Example (iv) of §2.

Euclid is said to have disappointed Ptolemy I with his counsel that "there is no royal road to geometry." To this day, there is no royal road to these theorems of Brun. While the ideas underlying the sieve methods discussed in Chapter 6 comfortably fit in one's brain, Brun's sieve (in its full form) is rather intricate and does not admit an easy combinatorial interpretation. Nevertheless, the reader is owed some account of what is surely one of our most powerful tools. In this chapter, we take a two-pronged approach, aimed at appeasing both theorists and those looking at sieve methods primarily with an eye toward applications. We do not attempt to discuss Brun's original work but instead take full advantage of the streamlining that has occurred over the past several decades.

For application-oriented individuals, we describe in §2 the "fundamental lemma of sieve theory" (but give no proof). Loosely speaking, the fundamental lemma asserts that under widely applicable hypotheses, the naive prediction

$$S(\mathscr{A}, \mathscr{P}, X^{1/u}) \approx X \prod_{\substack{p \in \mathscr{P} \\ p < X^{1/u}}} (1 - \alpha(p))$$

holds up to a multiplicative factor of $1 + o_{u\to\infty}(1)$. In particular, if $z = X^{o(1)}$, so that $u \to \infty$, then $S(\mathscr{A}, \mathscr{P}, z) \sim X \prod_{p \in \mathscr{P} \cap [2,z)} (1 - \alpha(p))$, while if $z = X^{1/u}$ with a large fixed value of u, then $S(\mathscr{A}, \mathscr{P}, z) \asymp X \prod_{p\in\mathscr{P}\cap[2,z)} (1 - \alpha(p))$. This result has many applications; for example, the order-of-magnitude result (7.4) obtained by Brun is an immediate consequence, though with an inexplicit constant $1/u$ in place of the exponent $1/9.9$.

For the theorist, we develop in §3 an alternative to Brun's approach discovered relatively recently by Hooley [**Hoo94**]. Hooley referred to this method as an "almost–pure sieve", but following Ford and Halberstam [**FH00**], we have chosen to refer to it as the *Brun–Hooley sieve*. While simpler than Brun's original approach, there are still many technical intricacies; in the main text, we have chosen to merely state the upper and lower bounds, leaving the proofs to an appendix. As applications, we establish the claims of Brun mentioned above in somewhat stronger form: *There are infinitely many pairs of* 7*-almost primes* $n, n+2$*, and every large even integer* N *is a sum of two* 7*-almost primes.*

Sieve methods are now part of the standard tool chest of analytic number theory. In the years immediately following Brun's work, when only a few theorems had been proved, it was far from clear that this would be the case. A turning point came in the work of Schnirelmann in the 1930s, who showed how to deduce from Brun's sieve that a positive proportion of even numbers could be represented as a sum of two primes. Schnirelmann leveraged this fact, and some easy ideas in additive number theory (developed by him from scratch!) to prove the following dazzling theorem in the direction of Goldbach's conjecture: Every integer > 1 can be written as a sum of $O(1)$ primes. An account of Schnirelmann's ideas is given in §4.

2. Sieves made simple: The fundamental lemma

The following form of the fundamental lemma is extracted from the monograph of Diamond and Halberstam (see [**DH08**, Theorem 4.1] for a somewhat more precise statement). We make free use of the notation introduced in §2 of Chapter 6.

★ **Theorem 7.1** (Fundamental lemma)**.** *Suppose that* $0 \le \alpha(p) < 1$ *for all* $p \in \mathscr{P}$*. Assume also that for certain positive constants* κ *and* A*,*

$$\prod_{\eta \le p < \xi} (1-\alpha(p))^{-1} \le \left(\frac{\log \xi}{\log \eta}\right)^{\kappa} \left(1 + \frac{A}{\log \eta}\right) \qquad (\textit{for all } 2 \le \eta \le \xi). \tag{7.5}$$

Define

$$V(z) := \prod_{\substack{p \in \mathscr{P} \\ p < z}} (1-\alpha(p)).$$

Then for all $z \ge 2$ *and* $v \ge 1$*,*

$$S(\mathscr{A}, \mathscr{P}, z) = XV(z)\left(1 + O_{\kappa,A}(v^{-v})\right) + O\Bigg(\sum_{\substack{d < z^{2v} \\ d \mid P(z)}} 3^{\omega(d)} |r(d)|\Bigg). \tag{7.6}$$

Here the second O*-constant is absolute (in fact, can be taken to be* 1*).*

Below, we describe applications of the fundamental lemma to the following four problems:

- Generalized twins
- Goldbach representations
- Primes in progressions
- Prime k-tuples

The last section discusses a crude but effective result that is often easier to apply than the fundamental lemma itself.

2.1. Generalized twins. Let $\pi_N(x)$ denote the count of natural numbers $n \le x$ for which both n and $n+N$ are prime. As a first application of the fundamental lemma, we prove that for each even number $N > 0$ and all $x \ge 2$,

$$\pi_N(x) \ll \left(\prod_{\substack{p \mid N\\ p>2}} \frac{p-1}{p-2}\right) \frac{x}{(\log x)^2}, \tag{7.7}$$

with an absolute implied constant. Moreover, for each fixed even difference $N > 0$, we show that there are infinitely many natural numbers n for which both n and $n+N$ have $O(1)$ prime factors.

We sieve the sequence $\mathscr{A} = \{n(n+N) : 1 \le n \le x\}$ by the set $\mathscr{P}$ of all primes, truncated at a height z to be determined. Let $\nu(d)$ denote the number of roots of the congruence $n(n+N) \equiv 0 \pmod{d}$. It follows from the Chinese remainder theorem that for each squarefree d, we have

$$\left| A_d - \frac{\nu(d)}{d} x \right| \le \nu(d) \le 2^{\omega(d)}.$$

(Cf. Example (ii) of §2 in Chapter 6.) Motivated by this, we take $X = x$ and $\alpha(d) = \nu(d)/d$, so that $|r(d)| \le 2^{\omega(d)}$ whenever d divides $P(z)$.

It is easy to check the hypotheses of Theorem 7.1 on α: We have $\alpha(p) = \frac{1}{p}$ when $p \mid N$ and $\alpha(p) = \frac{2}{p}$ when $p \nmid N$. Thus, $0 \le \alpha(p) < 1$ for all p (since $2 \mid N$). Also, if $2 \le \eta \le \xi$, then

$$\begin{aligned} \log \prod_{\eta \le p < \xi} (1-\alpha(p))^{-1} &= \sum_{\eta \le p < \xi} (\alpha(p) + O(1/p^2)) \\ &\le \sum_{\eta \le p < \xi} \frac{2}{p} + O(1/\eta) = 2 \log \frac{\log \xi}{\log \eta} + O(1/\log \eta). \end{aligned}$$

Exponentiating gives (7.5) with $\kappa = 2$ and some absolute constant $A > 0$.

Now, fix v large enough that the $1 + O(\cdots)$ factor in (7.6) is $> 1/2$. (Note that v can be chosen as an absolute constant, independent of N.) Then for any choice of $z \ge 2$, the main term in (7.6) is $\gg XV(z)$, and

$$\begin{aligned} XV(z) &\asymp x \prod_{\substack{p<z\\ p \mid N}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p<z\\ p \nmid N}} \left(1 - \frac{2}{p}\right) \\ &\asymp x \prod_{2<p<z} \left(1 - \frac{2}{p}\right) \prod_{\substack{p \mid N\\ 2<p<z}} \frac{p-1}{p-2} \asymp \frac{x}{(\log z)^2} \prod_{\substack{p \mid N\\ 2<p<z}} \frac{p-1}{p-2}. \end{aligned}$$

The second O-term in (7.6), which we think of as an error term, is

$$\ll \sum_{\substack{d<z^{2v}\\ d|P(z)}} 6^{\omega(d)} \le z^{2v} \sum_{\substack{d<z^{2v}\\ d\text{ squarefree}}} \frac{6^{\omega(d)}}{d} \le z^{2v} \prod_{p<z^{2v}} (1+6/p) \ll z^{2v}(\log(z^{2v}))^6.$$

Choosing $z = x^{\frac{1}{4v}}$, the error term is $\ll x^{1/2}(\log x)^6$ while the main term is (crudely) $\gg x/(\log x)^2$. Hence, for all x larger than a certain absolute constant,

$$S(\mathscr{A},\mathscr{P},x^{\frac{1}{4v}}) \asymp \left(\prod_{\substack{p|N\\ 2<p\le x^{\frac{1}{4v}}}} \frac{p-1}{p-2} \right) \frac{x}{(\log x)^2}. \tag{7.8}$$

The product in (7.8) is only increased if extended over all primes dividing N, as in (7.7). Recalling the trivial bound $\pi_N(x) \le z + S(\mathscr{A},\mathscr{P},z)$, we finish the proof of (7.7) for large x. Of course, for absolutely bounded values of $x \ge 2$, the assertion (7.7) is trivial.

Now assume that N is fixed. If n is counted in $S(\mathscr{A},\mathscr{P},x^{\frac{1}{4v}})$, then both n and $n+N$ have no prime factors $\le x^{\frac{1}{4v}}$. Moreover, for large x, both n and $n+N$ are smaller than $2x$. Hence, both n and $n+N$ have at most $4v \ll 1$ prime factors. Since the right-hand side of (7.8) tends to infinity with x, there are infinitely many pairs of $(4v)$-almost primes $n, n+N$.

2.2. Goldbach representations. The situation for $R(N)$ is similar to that for $\pi_2(x)$, except that we set up the sieve as in Example (iv) of §2 from Chapter 6. The function α appearing in this setting is the same one we saw above in the treatment of generalized twins. Thus, the hypotheses on α in Theorem 7.1 hold. Proceeding as above, we find that with the same v as before,

$$S(A,\mathscr{P},N^{1/4v}) \asymp \left(\prod_{\substack{p|N\\ 2<p<N^{1/4v}}} \frac{p-1}{p-2} \right) \frac{N}{(\log N)^2} \tag{7.9}$$

for all large even numbers N. Since $R(N) \le S(\mathscr{A},\mathscr{P},N^{1/4v}) + 2N^{1/4v}$, we obtain Brun's upper bound

$$R(N) \ll \left(\prod_{\substack{p|N\\ p>2}} \frac{p-1}{p-2} \right) \frac{N}{(\log N)^2}.$$

If n is counted by $S(\mathscr{A},\mathscr{P},N^{1/4v})$, then both n and $N-n$ have all their prime factors $> N^{1/4v}$. Since both n and $N-n$ are bounded above by N, it follows that $N = n + (N-n)$ is a sum of two $(4v)$-almost primes. So the lower bound in (7.9) implies that all large even N are the sum of two $(4v)$-almost primes.

2.3. Primes in progressions and the Brun–Titchmarsh inequality. In Chapter 6 (§2, Example (i)), we investigated what sieve methods could tell us about the distribution of $\pi(x)$. This was a purely academic exercise; we knew already that the asymptotic behavior of $\pi(x)$ was governed by the prime number theorem. To make the situation a bit more interesting, we now consider the distribution of primes in progressions. It turns out that here the sieve is capable of establishing rather nontrivial results that do not appear easily accessible by other methods.

Recall that $\pi(x; m, a)$ denotes the number of primes $p \leq x$ with $p \equiv a \pmod{m}$. The prime number theorem for arithmetic progressions asserts that for every *fixed* progression $a \bmod m$ satisfying $\gcd(a, m) = 1$,

$$\pi(x; m, a) \sim \frac{x}{\varphi(m) \log x} \qquad (\text{as } x \to \infty). \tag{7.10}$$

With some effort (see, e.g., [**IK04**, §5.9]), one can show that the estimate (7.10) holds with some uniformity. For example, if $m \leq (\log x)^A$ for some fixed A, then (7.10) remains valid. (This is one form of the *Siegel–Walfisz theorem*.) We expect that much more is true; probably (7.10) holds uniformly for $m \leq x^{1-\epsilon}$, for each fixed $\epsilon > 0$. Such a strong form of the PNT for progressions appears far beyond the reach of present methods; even the powerful Extended Riemann Hypothesis would only guarantee uniformity for m up to about $x^{1/2}$.

Fortunately, in in many applications, it is sufficient to have an upper bound for $\pi(x; m, a)$ of the conjectured correct order. Our next theorem, due essentially to Titchmarsh [**Tit30**], shows that such a bound holds even when m is almost as large as x itself; e.g., $m \leq x^{1-\epsilon}$ is enough.

Theorem 7.2 (Brun–Titchmarsh inequality)**.** *Suppose that a is coprime to m and that $m < x$. Then*

$$\pi(x; m, a) \ll \frac{x}{\varphi(m) \log \frac{x}{m}}.$$

Remark. An elegant result of Montgomery & Vaughan [**MV73**] asserts that the implied constant can be taken equal to 2.

Proof. Let $\mathscr{A}$ be the set of natural numbers $n \leq x$ with $n \equiv a \pmod{m}$, and let $\mathscr{P}$ be the set of all primes. Let z be a positive real parameter to be specified shortly. If $p \equiv a \pmod{m}$ is prime, then either $p < z$ or p is counted in $S(\mathscr{A}, \mathscr{P}, z)$. Hence,

$$\pi(x; m, a) \leq z + S(\mathscr{A}, \mathscr{P}, z). \tag{7.11}$$

To get started estimating $S(\mathscr{A}, \mathscr{P}, z)$, we first estimate the terms A_d for squarefree numbers d. If d is not coprime to m, then $A_d = 0$. On the other hand, if $\gcd(d, m) = 1$, then the simultaneous relations $d \mid n$ and $n \equiv a \pmod{m}$ are equivalent to a single congruence on n modulo dm, and hence $\left|A_d - \frac{x}{dm}\right| \leq 1$. Thus, if we set $X = x/m$ and put $\alpha(d) = 1/d$ or 0 according to whether d is coprime to m or not, then then each remainder term $r(d)$ satisfies $|r(d)| \leq 1$.

Clearly $0 \leq \alpha(p) < 1$ for all primes p. Also, for $2 \leq \eta < \xi$, Mertens' theorem shows that

$$\prod_{\eta \leq p \leq \xi} (1 - \alpha(p))^{-1} \leq \prod_{\eta \leq p < \xi} \left(1 - \frac{1}{p}\right)^{-1} \leq \frac{\log \xi}{\log \eta} \left(1 + O\left(\frac{1}{\log \eta}\right)\right),$$

and thus (7.5) holds with $\kappa = 1$ and a certain absolute constant A. Choose $v = 1$ and $z = X^{1/4}$, and notice that the $1 + O(\cdots)$ term in (7.6) is then $\ll 1$. Hence, by the fundamental lemma and the uniform bound $|r(d)| \leq 1$,

$$S(\mathscr{A}, \mathscr{P}, X^{1/4}) \ll XV(X^{1/4}) + \sum_{\substack{d < X^{1/2} \\ d \text{ squarefree}}} 3^{\omega(d)},$$

assuming for the time being that $z \geq 2$ (equivalently, that $X \geq 16$). Now

$$\begin{aligned} XV(X^{1/4}) &= \frac{x}{m} \prod_{\substack{p \nmid m \\ p < (x/m)^{1/4}}} \left(1 - \frac{1}{p}\right) \\ &= \frac{x}{m} \prod_{p < (x/m)^{1/4}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \mid m \\ p < (x/m)^{1/4}}} \left(1 - \frac{1}{p}\right)^{-1} \\ &\ll \left(\frac{x}{m \log \frac{x}{m}}\right) \prod_{p \mid m} \left(1 - \frac{1}{p}\right)^{-1} = \frac{x}{\varphi(m) \log \frac{x}{m}}. \end{aligned} \tag{7.12}$$

Moreover,

$$\begin{aligned} \sum_{d < X^{1/2}} 3^{\omega(d)} &\leq X^{1/2} \sum_{\substack{d < X^{1/2} \\ d \text{ squarefree}}} \frac{3^{\omega(d)}}{d} \\ &\ll X^{1/2} \prod_{p < X^{1/2}} \left(1 + \frac{3}{p}\right) \ll X^{1/2} (\log X)^3. \end{aligned}$$

This term is dominated by the final expression in (7.12); indeed,

$$\frac{x}{\varphi(m) \log \frac{x}{m}} \gg X / \log X \gg X^{1/2} (\log(X))^3.$$

Hence,

$$S(\mathscr{A}, \mathscr{P}, X^{1/4}) \ll \frac{x}{\varphi(m)\log\frac{x}{m}}.$$

To complete the proof of the Brun–Titchmarsh theorem, we refer back to (7.11). Since

$$z = X^{1/4} \ll \frac{X}{\log X} \ll \frac{x}{\varphi(m)\log\frac{x}{m}},$$

the estimate for $S(\mathscr{A}, \mathscr{P}, X^{1/4})$ established above implies that

$$\pi(x; m, a) \ll \frac{x}{\varphi(m)\log\frac{x}{m}},$$

as desired. Everything so far has been under the assumption that $X \geq 16$. However, if X is absolutely bounded, then $\#\mathscr{A} \ll X \ll X/\log X \ll \frac{x}{\varphi(m)\log\frac{x}{m}}$, and so the theorem is trivial. $\square$

2.4. Prime k-tuples. Suppose that $F_1(T), \dots, F_k(T)$ are k linear polynomials, and write each $F_i(T) = a_iT + b_i$. Suppose that $a_i, b_i \in \mathbf{Z}$ and that each $a_i \neq 0$. Assume also that no F_i is a rational multiple of a different F_j, so that

$$E := \prod_{i=1}^{k} a_i \prod_{1\leq i<j\leq k} (a_ib_j - a_jb_i) \neq 0.$$

Define a multiplicative arithmetic function ν by setting

$$\nu(d) := \#\{n \bmod d : \prod_{i=1}^{k} F_i(n) \equiv 0 \pmod{d}\}.$$

Finally, assume that that there are "no local obstructions" to the simultaneous primality of the $|F_i|$, in the sense that

$$\nu(p) < p$$

for all primes p.

In the case when the F_i are fixed, we expect as a special case of Schinzel's Hypothesis H (cf. Chapter 1, §9.2) that there are infinitely many n for which $|F_1(n)|, \dots, |F_k(n)|$ are simultaneously prime. Moreover, the quantitative form of Hypothesis H developed in Chapter 3, §5 even tells us how many such $n \leq x$ to expect for large x. (This case of Hypothesis H, where all the F_i are linear, was goes back to Dickson [**Dic04**].)

The following upper bound, which does *not* require us to fix the F_i in advance, has numerous applications:

Theorem 7.3. *Assume all of the above conditions on the* F_i*. Let* $x \geq 2$*. The number of* $n \leq x$ *for which all of* $|F_1(n)|, \ldots, |F_2(n)|$ *are prime is*

$$\ll_k \frac{x}{(\log x)^k} \prod_{\substack{p|E \\ p>k}} \left(\left(1 - \frac{\nu(p)}{p}\right) \left(1 - \frac{k}{p}\right)^{-1} \right). \tag{7.13}$$

We emphasize that the implied constant here depends only on k*, and not on the coefficients of the* f_i*.*

Remark. As evidence of the usefulness of Theorem 7.3, we note here that it implies our previous upper bounds on $\pi_N(x)$, $R(N)$, and $\pi(x; m, a)$:

- For $\pi_2(x)$, take $k = 2$ and $F_1(T) = T$, $F_2(T) = T + N$.
- For $R(N)$, take $k = 2$ and $F_1(T) = T$, $F_2(T) = N - T$.
- For $\pi(x; q, a)$ with $0 \leq a < q$, take $k = 1$ and $F_1(T) = q(T-1)+a$.

We leave the reader to check the details (Exercise 3).

Proof. We can assume that x is large (say, $x \geq 16$), since otherwise the upper bound in (7.13) is trivial. As might be expected, we proceed by sieving the sequence

$$\mathscr{A} := \{ \prod_{1 \leq i \leq k} F_i(n) : n \leq x\}$$

by the set of all primes $\mathscr{P}$, truncated at some height z.

By hypothesis, $\nu(p) < p$ for all p; in other words, there is no prime p dividing $\prod_{i=1}^k F_i(n)$ for every integer n. Thus, the reduction mod p of the polynomial $\prod_{i=1}^k F_i(T)$ is a nonzero polynomial of degree $\leq k$ in $\mathbf{F}_p[T]$. Consequently, $\nu(p) \leq k$ for all primes p, and so

$$\nu(p) \leq \max\{p - 1, k\} \tag{7.14}$$

for all primes p. We claim that $\nu(p) = k$ for all primes except possibly those dividing E. To see this, first observe that if $p \nmid \prod_{i=1}^k a_i$, then each F_i has the single root $-\frac{b_i}{a_i}$ mod p. Now

$$-\frac{b_i}{a_i} = -\frac{b_j}{a_j} \quad \text{in } \mathbf{F}_p \Longrightarrow p \mid a_i b_j - a_j b_i.$$

Thus, if $\nu(p) < k$, then either p divides $\prod_{i=1}^k a_i$ or p divides $\prod_{1 \leq i < j \leq k}(a_i b_j - a_j b_i)$. In either case, p divides E.

For each squarefree d, we have $|A_d - x\frac{\nu(d)}{d}| \leq \nu(d)$. So we take $X = x$ and $\alpha(d) = \nu(d)/d$. Then $\alpha(p) < 1$ for all primes p. In fact, by (7.14),

$1-\alpha(p) \geq \frac{1}{k+1}$; in particular, $\alpha(p)$ is bounded away from 1 by a constant depending only on k. Thus, for $2 \leq \xi \leq \eta$,

$$\begin{aligned}\log \prod_{\eta \leq p < \xi} (1-\alpha(p))^{-1} &= \sum_{\eta \leq p < \xi} (\alpha(p) + O_k(1/p^2)) \\ &\leq \sum_{\eta \leq p < \xi} \frac{k}{p} + O_k(1/\eta) = k \log \frac{\log \xi}{\log \eta} + O_k(1/\log \eta),\end{aligned}$$

and so the hypothesis (7.5) of the fundamental lemma (Theorem 7.1) holds with $\kappa = k$ and an A depending only on k.

We take $v = 1$ and $z = X^{1/4}$ in the fundamental lemma. (Then $z \geq 2$, by our opening assumption that x is large.) Imitating the steps in our application to the Brun–Titchmarsh theorem, we find that

$$S(\mathscr{A}, \mathscr{P}, X^{1/4}) \ll_k XV(X^{1/4}) + X^{1/2}(\log X)^{3k}. \tag{7.15}$$

The second term in (7.15) will be negligible for us and we concentrate on the first. Since we seek an upper bound, we may ignore the contribution to $V(X^{1/4})$ from primes $< k$. This gives

$$\begin{aligned}XV(X^{1/4}) &\leq x \prod_{\substack{k<p<X^{1/4} \\ p \mid E}} \left(1 - \frac{\nu(p)}{p}\right) \prod_{\substack{k<p<X^{1/4} \\ p \nmid E}} \left(1 - \frac{k}{p}\right) \\ &\ll x \prod_{k<p<X^{1/4}} \left(1 - \frac{k}{p}\right) \prod_{\substack{k<p<X^{1/4} \\ p \mid E}} \left(\left(1 - \frac{\nu(p)}{p}\right)\left(1 - \frac{k}{p}\right)^{-1}\right) \\ &\ll_k \frac{x}{(\log x)^k} \prod_{\substack{k<p<X^{1/4} \\ p \mid E}} \left(\left(1 - \frac{\nu(p)}{p}\right)\left(1 - \frac{k}{p}\right)^{-1}\right). \end{aligned} \tag{7.16}$$

(Above, we use the estimate

$$\prod_{k<p\leq t} \left(1 - \frac{k}{p}\right) \ll_k \frac{1}{(\log t)^k},$$

valid for all $t \geq 2$.) Since we seek an upper bound, we can extend the product in (7.16) to all primes $p > k$ dividing E; recalling (7.15), we deduce that

$$S(\mathscr{A}, \mathscr{P}, X^{1/4}) \ll_k \frac{x}{(\log x)^k} \prod_{\substack{k<p<X^{1/4} \\ p \mid E}} \left(\left(1 - \frac{\nu(p)}{p}\right)\left(1 - \frac{k}{p}\right)^{-1}\right). \tag{7.17}$$

If all the $|F_i(n)|$ are prime for the natural number $n \leq x$, then either $2 \leq |F_i(n)| \leq X^{1/4}$ for some $1 \leq i \leq k$, or n is counted by $S(\mathscr{A}, \mathscr{P}, X^{1/4})$. The number of n for which the former possibility holds is $< 2kX^{1/4} \ll_k X^{1/4}$, which is negligible in comparison with (7.17). Since the right-hand side of (7.17) is precisely the upper bound claimed in the theorem statement, the proof is complete. □

2.5. As simple as possible, but no simpler. In many problems, even an appeal to the fundamental lemma is more trouble than necessary. A. N. Whitehead opined that "The ultimate goal of mathematics is to eliminate any need for intelligent thought." The following result, very much in the spirit of Whitehead's remark, is often sufficient. In the literature (particularly in papers of Erdős), when an appeal to "Brun's sieve" is made, this is often the result that is intended:

Theorem 7.4 (Brun's sieve). *Let $z \geq 2$. For each prime $p \leq z$, fix a set $\Omega_p \subset \mathbf{Z}/p\mathbf{Z}$ of excluded residue classes modulo p, and put $\nu(p) := \#\Omega_p$. Assume that for some fixed k, we have*

$$0 \leq \nu(p) \leq \min\{k, p-1\}$$

for all primes $p < z$. In other words, we always remove at most k residue classes and never remove every residue class. Let S denote the number of $n \leq x$ not belonging to any excluded residue class.

(i) (Upper bound) *Let u be any positive constant. If $2 \leq z \leq x^{1/u}$, then*

$$S \ll x \prod_{p \leq z} (1 - \nu(p)/p).$$

The implied constant depends at most on k and u.

(ii) (Lower bound) *There are positive constants $u > 0$ and $x_0 > 0$, both depending only on k, so that if $x > x_0$ and $2 \leq z \leq x^{1/u}$, then*

$$S \gg x \prod_{p \leq z} (1 - \nu(p)/p).$$

Note the change in perspective: Instead of starting with an arbitrary sequence $\mathscr{A}$ and sieving out the residue class $0 \bmod p$, we start with an initial segment of the natural numbers and sieve out multiple residue classes modulo each prime.

Proof. By this point, the key components of the proof are old friends. Let $\mathscr{P}$ be the set of primes $< z$ for which Ω_p is nonempty. Choose $F(T) \in \mathbf{Z}[T]$ with the property that for all primes $p \in \mathscr{P}$, the set Ω_p is the set of roots of F modulo p. (Such an F can be constructed by the Chinese remainder theorem.) Put $\mathscr{A} = \{F(n) : n \leq x\}$. Then S is what we have been denoting up to now by $S(\mathscr{A}, \mathscr{P}, z)$.

Table 1. Fix k linear polynomials $F_1, \dots, F_k$ satisfying the conditions of Theorem 7.3. Then there are infinitely many natural numbers n with $\Omega(\prod_{i=1}^{n} |F_i(n)|) \leq \Theta_k$. In fact, for large x, there are $\gg x/(\log x)^k$ such $n \leq x$ having this property and satisfying the additional condition that $\prod_{i=1}^{n} |F_i(n)|$ is squarefree.

k	1	2	3	4	5	6	7	8	9	10
Θ_k	1	3	8	12	16	20	24	29	33	39

For our approximation X to the size of $\mathscr{A}$, we take $X := x$. For each d dividing $P(z)$, put $\nu(d) := \prod_{p \mid d} \nu(p)$, and set $\alpha(d) := \frac{\nu(d)}{d}$. Then

$$|A_d - X\alpha(d)| \leq \nu(d) \leq k^{\omega(d)} \quad (\text{for all } d \mid P(z)).$$

We should check that the hypotheses on α appearing in the fundamental lemma are satisfied, but in fact we have already done the relevant computation in our prior discussion of prime k-tuples. Fix v large enough that the $1 + O(\cdots)$ term in (7.6) is $> \frac{1}{2}$, and take $z = x^{1/4v}$. Then the main term in (7.6) is

$$\asymp XV(z) = x \prod_{p<z} (1 - \nu(p)/p),$$

while the error term is $\ll \sum_{d<x^{1/2},\ \text{squarefree}} (3k)^{\omega(d)} \ll_k x^{1/2} (\log x)^{3k}$. For large x (in terms of k), the main term dominates. This proves the lower bound in the theorem with $u = 4v$. One also obtains the upper bound in the theorem for any $u > 4v$. Technically, we have only established these cases of the upper bound when x is large, but the upper bound is trivial for values of x which are bounded in terms of k.

To complete the proof, it remains only to show that the upper bound is valid also when $0 < u \leq 4v$. But this is easy: If one sieves up to $x^{1/u}$, the number of remaining integers cannot exceed the number which remain if one sieves up to the smaller point $x^{1/4v}$, and so (by the above) is

$$\ll_k \left(x \prod_{p < x^{\frac{1}{4v}}} (1 - \alpha(p)) \right) = \left(x \prod_{p < x^{\frac{1}{u}}} (1 - \alpha(p)) \right) \prod_{x^{1/4v} \leq p < x^{1/u}} (1 - \alpha(p))^{-1}.$$

By (7.5), the final product is $\ll_{k,u} 1$, and so $S \ll_{k,u} x \prod_{p<x^{1/u}} (1 - \alpha(p))$. $\square$

An instructive application is the problem of obtaining almost-prime values of polynomials:

Example. Let $F(T)$ be a polynomial of degree $k \geq 1$ with integer coefficients. Suppose that there is no prime p which divides $F(n)$ for all values of n. Then with $\nu(p)$ denoting the number of roots of F modulo p, we have $\nu(p) < p$ for all primes p. Moreover, the reduction of F modulo p is nonvanishing in $\mathbf{F}_p[T]$, and hence also $\nu(p) \leq k$.

Now apply the lower bound in Theorem 7.4. For a certain large u (depending only on k), we deduce that there are $\gg x/(\log x)^k$ values of $n \leq x$ for which $F(n)$ has no prime factors $< x^{1/u}$ (once $u > x_0(k)$). Since $|F(n)| \asymp n^k$ for large n, it follows that there are infinitely many n for which $|F(n)|$ is a uk-almost prime:

$$\liminf_{n\to\infty} \Omega(|F(n)|) \leq uk \ll_k 1.$$

This upper bound is interesting for at least two reasons which we are already positioned to appreciate:

- Suppose that $F_1, \ldots, F_k$ is a fixed collection of linear polynomials satisfying all the hypotheses of Theorem 7.3. Taking $F = \prod_{i=1}^k F_i$ above gives an almost-prime result for general prime k-tuples analogous to that mentioned in the special case of twin prime pairs at the start of this chapter.

  The best results in this direction for small k are collected in Table 1, without proof (see [**HT06**] and references). (The condition that the $F_i(n)$ all be squarefree is added there, which is convenient for some applications and does not affect the results.) As one example, from the result for $k = 2$ in Table 7.3, we may deduce a famous result of Chen [**Che73**]: *There are infinitely many n for which one of n and $n+2$ is prime and the other is a product of at most two primes.* In fact, Chen's result says a bit more; one can specify which of n and $n+2$ is the guaranteed prime.
- Alternatively, suppose that F is a polynomial which is predicted, by the Hardy–Littlewood conjectures discussed in Chapter 3, to represent infinitely many primes. In this case, the above discussion shows that $|F(n)|$ is a Λ_k-almost prime for infinitely many n for some Λ_k depending only on k. By Dirichlet's theorem on primes in progressions, we can take $\Lambda_1 = 1$. Lemke Oliver [**LO11**], building on earlier work of Iwaniec [**Iwa78**], has shown that we can take $\Lambda_2 = 2$. (Thus, for example, there are infinitely many n for which n^2+1 is either prime or a product of two primes.) Richert [**Ric69**] has proved that $\Lambda_k = k+1$ is admissible for every k.

See Exercise 6 for an upper bound on the number of prime values of a polynomial.

Theorem 7.4 has many applications, but one should not harbor the misconception that all interesting sieve problems are readily treated in this fashion. For example, the problem of counting prime "binary pretenders", considered in Chapter 6, is not amenable to such an approach. Another example (or rather, non-example), similar in spirit but markedly different in details, is discussed in Exercise 8.

3. The Brun–Hooley sieve

We now turn to an account of the Brun–Hooley sieve. Our approach is somewhat discursive. Rather than work in great generality to begin with, we have chosen to concentrate on the two applications mentioned at the start of this chapter: obtaining upper and lower estimates relevant to the the twin prime and Goldbach problems.

A reference for this material that treats the method more systematically is the exposition of Ford & Halberstam [**FH00**]. Note that what those authors call the Brun–Hooley sieve in their main theorem differs slightly from our formulation, which largely follows the introduction of the method by Hooley [**Hoo94**].

Throughout, we assume familiarity with the notation introduced in Chapter 6, §2. It will also be convenient to write

$$V := \prod_{p\in\mathscr{P}} (1-\alpha(p)), \quad \text{and} \quad V(z) := \prod_{\substack{p\in\mathscr{P}\\ p<z}} (1-\alpha(p)).$$

3.1. Statement of the Brun–Hooley sieve. The next theorem is our version of the Brun–Hooley sieve. It is probably not worth committing this rather complicated result to memory. But it is worth taking some time to grasp its basic form, which might be compared with that of the fundamental lemma. Both results assert that if one compares $S(\mathscr{A},\mathscr{P})$ to XV, then the comparison is good up to a multiplicative error, which in applications we hope is $\asymp 1$, and an extra additive error incorporating the remainder terms $|r(d)|$, which we hope to be negligible.

Theorem 7.5 (Brun–Hooley sieve)**.** *Let $\mathscr{P} = \dot{\bigcup}_{j=1}^{r} \mathscr{P}_j$ be a partition of $\mathscr{P}$. Suppose that $\alpha(p) < 1$ for each $p \in \mathscr{P}$. For any choice of nonnegative even integers $m_1, \dots, m_r$, we have*

$$S(\mathscr{A},\mathscr{P}) \le XV \exp\left(\sum_{j=1}^{r}\left(\sum{}^{(j)} \Big/ \prod{}^{(j)}\right)\right) + O\Bigg(\sum_{\substack{d_1,\dots,d_r\\ d_j|P_j,\ \omega(d_j)\le m_j}} |r(d_1\cdots d_r)|\Bigg). \tag{7.18}$$

Here

$$\prod{}^{(j)} := \prod_{p\in\mathscr{P}_j}(1-\alpha(p)), \quad \sum{}^{(j)} := \sum_{\substack{d_j \mid P_j \\ \omega(d_j)=m_j+1}} \alpha(d_j).$$

Also,

$$S(\mathscr{A},\mathscr{P}) \geq XV\left(1-\sum_{j=1}^{r}\left(\sum{}^{(j)}\Big/\prod{}^{(j)}\right)\right) + O\Bigg(\sum_{\substack{d_j \mid P_j\ (1\leq j\leq r)\\ \theta_{d_1,\dots,d_r}}} |r(d_1\cdots d_r)|\Bigg).$$

Here $\theta_{d_1,\dots,d_r}$ denotes the condition that there exist $r-1$ indices j, $1\leq j\leq r$, for which $\omega(d_j)\leq m_j$, while the remaining index satisfies $\omega(d_j)\leq m_j+1$.

3.2. Applications of the upper bound. Let us state formally the sharp upper bound on $R(N)$ already discussed in the introduction:

Theorem 7.6. *For every even natural number N,*

$$R(N) \ll \Bigg(\prod_{\substack{p\mid N\\ p>2}}\frac{p-1}{p-2}\Bigg)\frac{N}{(\log N)^2}.$$

We assume that the sieving parameters are chosen in Example (iv) of Chapter 6, §2. So $\mathscr{A}=\{n(N-n) : 1\leq n\leq N\}$, $\mathscr{P}$ is the set of all primes, $X=N$, and $\alpha(d)$ denotes the number of solutions modulo d to the congruence $n(N-n)\equiv 0 \pmod{d}$.

We think of u as a large, fixed positive number. How large u has to be will be specified in the course of the argument; essentially, we choose it as large as we need in order for our subsequent assertions to be correct. For such a choice of u, we will show that $S(\mathscr{A},\mathscr{P},x^{1/u}) \ll XV(x^{1/u})$ for all large values of X $(=N)$, which will lead quickly to Theorem 7.6.

To apply the Brun–Hooley sieve to this situation we need a partition of $\mathscr{P}\cap[2,z)$. We introduce the notation

$$\eta = \log\log X$$

and the choice of parameters

$$K := 1.57, \quad K_1 := 1.571. \tag{7.19}$$

For the present discussion it is only important that $1<K<K_1$, but this choice will be particularly effective for the lower bound applications of §3.3.

For large X, we have $\eta < z = X^{1/u}$, so that if we define R as the minimal integer with $z^{1/K^R} < \eta$, then $R \geq 1$. (Indeed, $R \to \infty$ with X.) For such X, we define

$$z_j = \begin{cases} z^{1/K^j} & \text{for } 0 \leq j \leq R-1, \\ \eta & \text{for } j = R, \\ 2 & \text{for } j = R+1. \end{cases}$$

We partition $\mathscr{P} \cap [2, z)$ into the $r := R+1$ sets

$$\mathscr{P}_j := \{p \in \mathscr{P} : z_j \leq p < z_{j-1}\} \quad (1 \leq j \leq R+1),$$

and we define the corresponding nonnegative even integers $m_1, \dots, m_{R+1}$ by putting

$$m_j = 2j \quad (j = 1, \dots, R) \quad \text{and} \qquad m_{R+1} = \infty;$$

here "∞" indicates that m_{R+1} is chosen at least as large as the cardinality of $\mathscr{P}_{R+1}$. For definiteness, we take m_{R+1} as the smallest even integer with this property. With this choice of m_{R+1}, the condition on a divisor d of P_{R+1} that it has no more than m_{R+1} prime divisors becomes vacuous.

We now apply the upper bound (7.18) to our problem. By our choice of m_{R+1}, it is trivial that

$$\sum\nolimits^{(R+1)} = \sum_{\substack{d_{R+1} \mid P_{R+1} \\ \omega(d_{R+1}) = m_{R+1}+1}} \alpha(d_{R+1}) = 0. \tag{7.20}$$

Hence, $\sum^{(j)} / \prod^{(j)}$ vanishes at $j = R+1$, and to estimate the main term of (7.18) it suffices to estimate the ratio $\sum^{(j)} / \prod^{(j)}$ for $j = 1, \dots, R$.

Clearly

$$\prod\nolimits^{(j)} = \prod_{z_j \leq p < z_{j-1}} (1 - \alpha(p)) \geq \prod_{z_j \leq p < z_{j-1}} \left(1 - \frac{2}{p}\right).$$

We now invoke the following lemma, whose easy proof is left to the reader:

Lemma 7.7. *For $x \geq 2$, we have*

$$\prod_{x \leq p < y} \left(1 - \frac{2}{p}\right) = \frac{(\log x)^2}{(\log y)^2} \left(1 + O\left(\frac{1}{\log x}\right)\right), \tag{7.21}$$

uniformly for $y \geq x$.

From (7.21) and Lemma 7.7, we deduce that

(7.22)
$$\prod\nolimits^{(j)} \geq \frac{(\log z_j)^2}{(\log z_{j-1})^2} \left(1 + O\left(\frac{1}{\log z_j}\right)\right) \geq \frac{1}{K^2} \left(1 + O\left(\frac{1}{\log \eta}\right)\right) \geq \frac{1}{K_1^2}.$$

Moreover, for $1 \le j \le R$, the multinomial theorem gives that

$$\sum\nolimits^{(j)} = \sum_{\substack{d_j \mid P_j \\ \omega(d_j) = m_j+1}} \alpha(d_j) \le \frac{1}{(m_j+1)!}\left(\sum_{p \in \mathscr{P}_j} \alpha(p)\right)^{m_j+1}$$

$$\le \frac{1}{(m_j+1)!}\left(\sum_{p \in \mathscr{P}_j} \frac{2}{p}\right)^{m_j+1} \le \frac{(2\log K_1)^{m_j+1}}{(m_j+1)!} \tag{7.23}$$

provided X is large enough, since

$$\sum_{z_j \le p < z_{j-1}} \frac{2}{p} = 2\log\frac{\log z_{j-1}}{\log z_j} + O\left(\frac{1}{\log z_j}\right)$$
$$\le 2\log K + O\left(\frac{1}{\log \eta}\right) \le 2\log K_1.$$

Putting (7.22) and (7.23) together and recalling (7.20), we find that for large X,

$$\sum_{j=1}^{R+1}\left(\sum\nolimits^{(j)} \Big/ \prod\nolimits^{(j)}\right) \le K_1^2 \sum_{j=1}^{R} \frac{(2\log K_1)^{2j+1}}{(2j+1)!} \le K_1^2 \exp(2\log K_1).$$

This shows that the main term of (7.18) is bounded above by a constant multiple of $XV(z)$. Now

$$XV(z) \ge \frac{1}{2}X \prod_{2 < p < X^{1/u}} (1 - 2/p) \asymp_u X/(\log X)^2, \tag{7.24}$$

so that to obtain the estimate $S(\mathscr{A}, \mathscr{P}, z) \ll XV(z)$ we need only ensure that the sum appearing in the expression for the remainder term,

$$\sum_{\substack{d_1, \ldots, d_{R+1} \\ d_j \mid P_j,\ \omega(d_j) \le m_j}} |r(d_1 \cdots d_{R+1})|, \tag{7.25}$$

is of smaller order than $X/(\log X)^2$. We will show that if u was initially selected sufficiently large, then (7.25) is $\ll X^{\delta}$ for a certain constant $\delta < 1$.

Observe that any product $d_1 \cdots d_{R+1}$ appearing as an argument of $r(\cdot)$ in the sum (7.25) satisfies

$$d_1 \cdots d_{R+1} \le \left(\prod_{j=1}^{R} z_{j-1}^{m_j}\right)\eta^{\eta}$$
$$= X^{\frac{1}{u}\left(\sum_{j=1}^{R} m_j / K^{j-1}\right)} X^{(\log\log X)(\log\log\log X)/\log X}.$$

Also,

$$\sum_{j=1}^{R} \frac{m_j}{K^{j-1}} \le \sum_{j=1}^{\infty} \frac{2j}{K^{j-1}} = \frac{2K^2}{(K-1)^2} = 15.173\dots.$$

We now suppose that u exceeds $15.173\dots$, say $u = 16$ for definiteness. Then for large enough X, we have $d_1 \cdots d_{R+1} \le X^{15.2/16}$ for every such product $d_1 \cdots d_{R+1}$. For every d dividing $P(z)$,

$$|r(d)| \le \nu(d) = \prod_{p|d} \nu(p) \le 2^{\omega(d)}.$$

As each integer admits at most one representation in the form $d_1 \cdots d_{R+1}$ (since the d_i are supported on disjoint sets of primes), the sum (7.25) above is bounded by

$$\sum_{d \le X^{15.2/16}} 2^{\omega(d)} \le X^{15.2/16} \sum_{d \le X^{15.2/16}} \frac{2^{\omega(d)}}{d} \ll X^{15.2/16} (\log X)^2.$$

Hence, for all large X,

$$\begin{aligned} S(\mathscr{A}, \mathscr{P}, X^{\frac{1}{16}}) &\ll XV(X^{1/16}) \\ &= X \prod_{p < X^{\frac{1}{16}}} \left(1 - \frac{2}{p}\right) \left(\prod_{\substack{p < X^{\frac{1}{16}} \\ p|N}} \frac{p-1}{p-2} \right) \ll \left(\prod_{p|N} \frac{p-1}{p-2} \right) \frac{N}{(\log N)^2}. \end{aligned}$$

(Recall here that $X = N$.) Consequently, for all large even N,

$$\begin{aligned} R(N) &\le S(\mathscr{A}, \mathscr{P}, X^{1/16}) + 2X^{1/16} \\ &\ll \left(\prod_{\substack{p|N \\ p>2}} \frac{p-1}{p-2} \right) \frac{N}{(\log N)^2}. \end{aligned}$$

This gives the assertion of Theorem 7.6 for sufficiently large N, but for bounded N the theorem is trivial.

This argument applies, mutatis mutandis, to the generalized prime twin problem considered in §2.1, i.e., the estimation of $\pi_N(x)$. In this problem, $\mathscr{A} := \{n(n+N) : 1 \le n \le x\}$, but $X = x$, but $\mathscr{P}$ and α are unchanged from above. Choosing z, the z_j, the partition $\mathscr{P}_j$, and the m_j exactly as before, the same proof shows that $S(\mathscr{A}, \mathscr{P}, X^{1/16}) \ll XV(X^{1/16})$ for all large X

(uniformly in N). So for large x.

$$\begin{aligned}\pi_N(x) &\ll X^{1/16} + S(\mathscr{A}, \mathscr{P}, X^{1/16})\\ &\ll x^{1/16} + \left(\prod_{\substack{p\mid N\\ p>2}} \frac{p-1}{p-2}\right)\frac{x}{(\log x)^2} \ll \left(\prod_{\substack{p\mid N\\ p>2}} \frac{p-1}{p-2}\right)\frac{x}{(\log x)^2},\end{aligned}$$

uniformly in N. For absolutely bounded values of x, the upper bound is trivial (with perhaps a different implied constant). So we have proved:

Theorem 7.8. *Let N be a positive even integer. Then for $x \geq 2$,*

$$\pi_N(x) \ll \left(\prod_{\substack{p\mid N\\ p>2}} \frac{p-1}{p-2}\right)\frac{x}{(\log x)^2},$$

where the implied constant is absolute.

3.3. Applications of the lower bound. We now prove the two remarkable theorems of Brun mentioned in the introduction: Every large even integer is a sum of two 9-almost primes, and there exist infinitely many pairs of 9-almost primes differing by 2.

Our setup for attacking these problems is the same as that used in attacking the analogous upper bound problems considered in §3.2. So, for the first of these, we assume N is an even natural number, and we take $\mathscr{A} := \{n(N-n) : 1 \leq n \leq N\}$. As before, we let $\mathscr{P}$ be the set of all primes. We seek to show that for a certain fixed $u > 1$, we have

$$S(\mathscr{A}, \mathscr{P}, N^{1/u}) > 0. \tag{7.26}$$

for all large even N. In this case, N is a sum of two u-almost primes.

We choose X, α, and $\mathscr{P}$ as before. With u a parameter to be chosen later, we define the partition of $\mathscr{P} \cap [2, z)$ into sets $\mathscr{P}_j$ precisely as in §3.2, with K and K_1 defined in (7.19). However, the choice of the corresponding even integers m_j requires more care.

To describe this choice, suppose for the moment that we have constructed a sequence $\{n_i\}_{i=1}^{\infty}$ of nonnegative even integers satisfying the two inequalities

$$\sum_{j=1}^{\infty} \frac{(2\log K_1)^{n_j+1}}{(n_j+1)!} < \frac{1}{K_1^2}, \tag{7.27}$$

$$\Gamma := 1 + \sum_{j=1}^{\infty} \frac{n_j}{K^{j-1}} < \infty, \tag{7.28}$$

where K and K_1 are given by (7.19). We fix $u > \Gamma$ and define (with same meaning of "∞" as in §3.2)

$$m_j = n_j \quad (1 \le j \le R), \qquad m_{R+1} = \infty.$$

Then for all large X, we have (recalling (7.20), (7.22), (7.23))

$$\sum_{j=1}^{R+1} \left({\sum}^{(j)} \Big/ {\prod}^{(j)} \right) = \sum_{j=1}^{R} \left({\sum}^{(j)} \Big/ {\prod}^{(j)} \right)$$
$$\le K_1^2 \sum_{j=1}^{R} {\sum}^{(j)} \le K_1^2 \sum_{j=1}^{R} \frac{(2\log K_1)^{m_j+1}}{(m_j+1)!} \le 1 - \epsilon$$

for a positive constant ϵ, by (7.27). This implies that the main term in the lower bound

$$(7.29) \quad S(\mathscr{A}, \mathscr{P}, z) \ge XV(z) \left(1 - \sum_{1 \le j \le R+1} \left({\sum}^{(j)} \Big/ {\prod}^{(j)} \right) \right) + O\Bigg(\sum_{\substack{d_j | P_j (1 \le j \le R+1) \\ \theta_{d_1, \dots, d_{R+1}}}} |r(d_1 \cdots d_{R+1})| \Bigg)$$

is (cf. (7.24))

$$\gg X \prod_{p < X^{1/u}} (1 - \alpha(p)) \gg X/(\log X)^2 \quad (X \to \infty).$$

The O-term in (7.29) can be treated much as in §3.2: The largest value of $d_1 \cdots d_{R+1}$ appearing as an argument of $r(\cdot)$ is bounded above by

$$X^{\frac{1}{u}\left(1 + \sum_{j=1}^{R} m_j / K^{j-1}\right)} X^{\log\log X \log\log\log X / \log X} \le X^{\Gamma/u + o(1)} \le X^{\delta}$$

for all large X, where $\delta := \frac{1}{2}(1 + \Gamma/u)$. Notice that $\delta < 1$. The argument of §3.2 then shows that the O-term in (7.29) is $\ll X^{\delta}(\log X)^2$, which is $o(X/(\log X)^2)$. So with this choice of parameters, we obtain (7.26) in the stronger form

$$S(\mathscr{A}, \mathscr{P}, X^{1/u}) \gg X/(\log X)^2$$

whenever X is sufficiently large.

It remains to construct a suitable sequence $\{n_i\}$. It is not hard to see that (7.27) and (7.28) will be satisfied with the simple choice $n_i = b + 2(i-1)$ $(i \ge 1)$, if we pick b to be a suitably large even natural number. However, this construction leads to an unnecessarily bloated value of Γ, so that while we still obtain a statement of the form "every large even N is a sum of two numbers with $O(1)$ prime factors", the $O(1)$ term dictating the number of summands is larger than we might like. We do better if we use the greedy algorithm to pick the first several n_i (which play the largest role in determining the size of Γ): Choose as many of the initial n_i to be 2 as (7.27) allows, then as many of the subsequent n_i to be 4 as allowed, etc.

Using a calculator or computer, we find that the sequence obtained in this way begins

$$n_1 = n_2 = n_3 = 2, \quad n_4 = \cdots = n_{10} = 4, \quad n_{11} = \cdots = n_{24} = 6.$$

Instead of continuing in this manner, we make the simple choice

$$n_{25} = 8 + 2(j - 25) \quad (j \geq 25).$$

Then, setting $L := 2\log K_1$,

$$\begin{aligned} &\frac{1}{K_1^2} - \sum_{j=1}^{\infty} \frac{(2\log K_1)^{n_j+1}}{(n_j+1)!} \\ &\qquad \geq \frac{1}{K_1^2} - \sum_{j=1}^{3} \frac{L^3}{3!} - \sum_{j=4}^{10} \frac{L^5}{5!} - \sum_{j=11}^{24} \frac{L^7}{7!} - \sum_{j=25}^{\infty} \frac{L^{9+2(j-25)}}{(9+2(j-25))!} \\ &\qquad \geq \frac{1}{K_1^2} - 3\frac{L^3}{3!} - 7\frac{L^5}{5!} - 14\frac{L^7}{7!} - \frac{L^9/9!}{1 - L^2/(11\cdot 10)} = 0.00003\ldots > 0, \end{aligned}$$

so that (7.27) holds in this case. Also,

$$\begin{aligned} \Gamma &= 1 + \sum_{j=1}^{3} \frac{2}{K^{j-1}} + \sum_{j=4}^{10} \frac{4}{K^{j-1}} + \sum_{j=11}^{24} \frac{6}{K^{j-1}} + \sum_{j=25}^{\infty} \frac{8+2(j-25)}{K^{j-1}} \\ &= 1 + \sum_{j=1}^{3} \frac{2}{K^{j-1}} + \sum_{j=4}^{10} \frac{4}{K^{j-1}} + \sum_{j=11}^{24} \frac{6}{K^{j-1}} + \frac{2(4K-3)}{K^{23}(K-1)^2} = 7.993\ldots. \end{aligned}$$

Thus (7.28) holds. Moreover, we can take

$$u = 7.995,$$

say. Doing so, we obtain an even stronger theorem than that stated in the introduction: Every large enough even N may be represented as a sum of two natural numbers each of which has no more than 7 prime divisors, and the number of such representations is $\gg X/(\log X)^2 = N/(\log N)^2$ as $N \to \infty$. Being slightly more careful, this argument will show that the number of representations is $\gg \frac{N}{(\log N)^2} \prod_{p\mid N,\ p>2} \frac{p-1}{p-2}$; we ask the reader to check this in Exercise 16.

Turning to the generalized twin problem, one can show in exactly the same way that there are $\gg x/(\log x)^2$ positive integers $n \leq x$ for which both n and $n+N$ have no prime divisor $\leq x^{1/7.995}$, uniformly in the choice of the even natural number N. If N is fixed, we get $\gg x/(\log x)^2$ integers $n \leq x$ for which n and $n+N$ have no more than 7 prime divisors, once x is large.

We have thus proved the almost-prime claims attributed to Brun in the introduction, with 9 replaced by the superior constant 7.

Remark. A word is in order about one of the more mysterious aspects of the argument. Why and how did we choose K and K_1? The choices in (7.19) were made to minimize the quantity Γ, which is the limiting factor in how small we are allowed to select u. Their numerical values were found by computer (cf. [**FH00**, pp. 347-348]).

4. Schnirelmann's application to the Goldbach problem

In the monograph of Halberstam & Richert [**HR74**, p. 6], the story is told of how Landau left Brun's manuscript untouched in a drawer for six years until hearing of a striking application made by the Russian mathematician Schnirelmann [**Sch33**]:

Theorem 7.9. *There is an absolute constant S with the following property: Every integer $n > 1$ can be written as a sum of at most S prime numbers.*

Our objective in this section is to prove Theorem 7.9.

4.1. Schnirelmann density. Write $\mathbf{N}_0$ for the set of nonnegative integers. In what follows we use script letters to denote subsets of $\mathbf{N}_0$ and use the corresponding Roman letters for their counting functions. Even though such sets may contain zero, it is convenient to define our counting functions so that only positive elements are tallied; thus, e.g.,

$$A(n) = \#\{a \in \mathscr{A} : 1 \le a \le n\}.$$

If $\mathscr{A}, \mathscr{B} \subset \mathbf{N}$, we define the *sumset* $\mathscr{A} \oplus \mathscr{B}$ by

$$\mathscr{A} \oplus \mathscr{B} := \{a + b : a \in \mathscr{A}, b \in \mathscr{B}\}.$$

For $h \in \mathbf{N}$, we put

$$h\mathscr{A} := \overbrace{\mathscr{A} \oplus \cdots \oplus \mathscr{A}}^{h \text{ summands}}.$$

We say that $\mathscr{A}$ is a *basis of finite order* if $h\mathscr{A} = \mathbf{N}_0$ for some $h \in \mathbf{N}$. In this case the smallest such h is called the *order* of the basis. For example, if $\mathscr{A} = \{n^2 : n \in \mathbf{Z}\}$, then $\mathscr{A}$ is a basis of order 4. In fact, if k is any integer with $k \ge 2$, then $\{n^k : n \in \mathbf{N}_0\}$ is a basis of finite order by the Hilbert–Waring Theorem considered in Chapter 5.

For each subset $A \subset \mathbf{N}_0$, we define the *Schnirelmann density* $\delta(\mathscr{A})$ of $\mathscr{A}$ by

$$\delta(\mathscr{A}) := \inf_{n=1,2,3,\ldots} \frac{A(n)}{n}.$$

This definition is a bit odd; unlike (e.g.) the notion of asymptotic density, the presence (or absence) of small numbers in $\mathscr{A}$ has a disproportionate impact. The most extreme instance of this is that $\mathscr{A}$ automatically has Schnirelmann density zero whenever $1 \notin \mathscr{A}$. Moreover, the only way that a set $\mathscr{A}$ can have Schnirelmann density 1 is if $\mathscr{A}$ contains every natural number. Despite these peculiarities, the Schnirelmann density is a very convenient measure of size for questions in additive number theory. Indeed, Schnirelmann succeeded in proving the following very useful criterion for a set to be a basis of finite order:

Theorem 7.10 (Schnirelmann's basis theorem)**.** *Let $\mathscr{A}$ be a subset of $\mathbf{N}_0$ with $0 \in \mathscr{A}$ and $\delta(\mathscr{A}) > 0$. Then $\mathscr{A}$ is a basis of finite order.*

The proof requires two simple lemmas.

Lemma 7.11. *If $\mathscr{A}$ and $\mathscr{B}$ are sets of nonnegative integers, each containing 0, and $\delta(\mathscr{A}) + \delta(\mathscr{B}) \geq 1$, then $\mathscr{A} \oplus \mathscr{B} = \mathbf{N}_0$. In particular, if $0 \in \mathscr{A}$ and $\delta(\mathscr{A}) \geq 1/2$, then $2\mathscr{A} = \mathbf{N}_0$.*

Proof. We will show that each $n \in \mathbf{N}_0$ belongs to the sumset $\mathscr{A} \oplus \mathscr{B}$. Suppose that $a_0 = 0 < a_1 < a_2 < \cdots$ is an enumeration of $\mathscr{A}$ and that $0 = b_0 < b_1 < b_2 < \cdots$ is an enumeration of $\mathscr{B}$. Let $n \in \mathbf{N}_0$, and consider the following list of nonnegative integers from $[0, n]$:

$$0 = a_0, a_1, \ldots, a_{A(n)}, n = n - b_0, n - b_1, \ldots, n - b_{B(n)}.$$

This list has length

$$(A(n) + 1) + (B(n) + 1) \geq \delta(\mathscr{A})n + \delta(\mathscr{B})n + 2 \geq n + 2 > n + 1.$$

Since there are only $n + 1$ integers in the interval $[0, n]$, it must be that for some pair of i and j with $0 \leq i \leq A(n)$ and $0 \leq j \leq B(n)$, we have $a_i = n - b_j$. But then $n = a_i + b_j \in \mathscr{A} \oplus \mathscr{B}$. $\square$

Lemma 7.12. *If $\mathscr{A}$ and $\mathscr{B}$ are sets of nonnegative integers, each containing 0, then $\delta(\mathscr{A} \oplus \mathscr{B}) \geq \delta(\mathscr{A}) + \delta(\mathscr{B}) - \delta(\mathscr{A})\delta(\mathscr{B})$.*

Proof. Let $n \in \mathbf{N}$, and let $0 < a_1 < a_2 < \cdots < a_{A(n)} \leq n$ be a list of the elements of $\mathscr{A} \cap [1, n]$. Define intervals I_j for $0 \leq j \leq A(n)$ by putting $I_0 = (0, a_1)$, $I_1 = (a_1, a_2)$, $I_2 = (a_2, a_3)$, $\ldots$, $I_{A(n)-1} = (a_{A(n)-1}, a_{A(n)})$, and $I_{A(n)} = (a_{A(n)}, n]$. We now estimate $\#(\mathscr{A} \oplus \mathscr{B}) \cap I_j$ for each j.

For $j = 0$, we have $\#(\mathscr{A} \oplus \mathscr{B}) \cap I_0 \geq B(a_1 - 1)$, since if $b \in \mathscr{B} \cap [1, a_1 - 1]$, then $0 + b \in (\mathscr{A} \oplus \mathscr{B}) \cap I_0$. Similarly, for $1 \leq j < A(n)$, we have $\#(\mathscr{A} \oplus \mathscr{B}) \cap I_j \geq B(a_{j+1} - a_j - 1)$, since if $b \in \mathscr{B} \cap [1, a_{j+1} - a_j - 1]$, then $a_j + b \in (\mathscr{A} \oplus \mathscr{B}) \cap I_j$. Finally, $\#(\mathscr{A} \oplus \mathscr{B}) \cap I_{A(n)} \geq B(n - a_{A(n)})$, since if $b \in \mathscr{B} \cap [1, n - a_{A(n)}]$, then $a_{A(n)} + b \in (\mathscr{A} \oplus \mathscr{B}) \cap I_{A(n)}$. Moreover, since

$0 \in \mathscr{B}$, we know also that $\mathscr{A} \oplus \mathscr{B} \supset \mathscr{A}$. Hence,

$$\begin{aligned}(A \oplus B)(n) &\geq A(n) + \sum\nolimits_{i=0}^{A(n)} \#(\mathscr{A} \oplus \mathscr{B}) \cap I_j \\ &\geq A(n) + B(a_1 - 1) + \sum_{i=1}^{A(n)-1} B(a_{i+1} - a_i - 1) + B(n - a_n).\end{aligned}$$

Since $B(m) \geq \delta(\mathscr{B})m$ for each $m \in \mathbf{N}_0$, this is at least

$$\begin{aligned}&A(n) + \delta(\mathscr{B}) \left((a_1 - 1) + \sum_{i=1}^{A(n)-1} (a_{i+1} - a_i - 1) + n - a_{A(n)} \right) \\ &\qquad = A(n) + \delta(\mathscr{B})(n - A(n)) = A(n)(1 - \delta(\mathscr{B})) + \delta(\mathscr{B}).\end{aligned}$$

But $A(n) \geq \delta(\mathscr{A})n$, so that

$$\begin{aligned}(A \oplus B)(n) &\geq \delta(\mathscr{A})n(1 - \delta(\mathscr{B})) + \delta(\mathscr{B})n \\ &= n(\delta(\mathscr{A}) + \delta(\mathscr{B}) - \delta(\mathscr{A})\delta(\mathscr{B})).\end{aligned}$$

Since n was arbitrary, the assertion of the lemma follows from the definition of Schnirelmann density. □

Proof of Theorem 7.10. Taking $\mathscr{A} = \mathscr{B}$ in Lemma 7.12, we find $\delta(2\mathscr{A}) \geq 2\delta(\mathscr{A}) - \delta(\mathscr{A})^2$. Said differently, $1 - \delta(2\mathscr{A}) \leq (1 - \delta(\mathscr{A}))^2$. Starting from this inequality, an easy induction shows that for every $k \geq 1$,

$$1 - \delta(2^k\mathscr{A}) \leq (1 - \delta(\mathscr{A}))^{2^k}.$$

Since $\delta(\mathscr{A}) > 0$, we can choose a natural number k for which the right-hand side of this inequality is at most $1/2$. Then $\delta(2^k\mathscr{A}) \geq 1/2$, and so $2^{k+1}\mathscr{A} = \mathbf{N}_0$ by Lemma 7.11. So $\mathscr{A}$ is a basis of order at most 2^{k+1}. □

Remark. A theorem of Mann [**Man42**], strengthening Lemma 7.12, asserts that if $\mathscr{A}$ and $\mathscr{B}$ are subsets of $\mathbf{N}_0$ with $0 \in \mathscr{A} \cap \mathscr{B}$, then $\delta(\mathscr{A} \oplus \mathscr{B}) \geq \min\{1, \delta(\mathscr{A}) + \delta(\mathscr{B})\}$. This had been conjectured by Landau & Schnirelmann. An immediate consequence of Mann's theorem is that under the hypotheses of Theorem 7.10, $\mathscr{A}$ is a basis of order at most $\lceil 1/\delta(\mathscr{A}) \rceil$. For a discussion of Mann's theorem and subsequent related developments (including the important work of Kneser), see the volumes of Ostmann mentioned in the notes at the end of this chapter. There is also some discussion of these results in the appealing survey [**PS95**].

4.2. Proof of Theorem 7.9. Observe that if $\mathscr{A} \subset \mathbf{N}_0$ has positive lower density, in the sense that

$$\liminf_{x \to \infty} \frac{A(x)}{x} > 0, \tag{7.30}$$

then $\mathscr{B} := \{0,1\} \cup \mathscr{A}$ has positive Schnirelmann density. Indeed, (7.30) implies that for some $\delta_0 > 0$ and $N_0 \in \mathbf{N}$, we have $A(N) \geq \delta_0 N$ for all $N \geq N_0$. But then $\delta(\mathscr{B}) \geq \min\{\delta_0, 1/N_0\} > 0$. Since also $0 \in \mathscr{B}$, we may apply Theorem 7.10 to deduce that $\mathscr{B}$ is a basis of finite order. We will shortly make use of these observations for an appropriately chosen set $\mathscr{A}$.

Recall that for a natural number N, the number of ordered representations of N as a sum of two primes is denoted by $R(N)$. For each $N \geq 2$, we have

$$R(N) \ll \left(\prod_{\substack{p\mid N\\ p>2}} \frac{p-1}{p-2}\right)\frac{N}{(\log N)^2}. \tag{7.31}$$

In this chapter, we have seen two proofs of §3.2 for even N – one using the fundamental lemma and one using the Brun–Hooley sieve. If N is odd, then $R(N) \leq 2$ and so (7.31) is trivial.

For our later work, it is convenient to write the bound (7.31) in an equivalent but slightly simpler form:

Lemma 7.13. *For all integers $N \geq 2$, we have*

$$R(N) \ll \frac{N}{(\log N)^2}\prod_{p\mid N}\left(1+\frac{1}{p}\right). \tag{7.32}$$

Proof. In view of (7.31), it is sufficient to check that

$$\prod_{\substack{p\mid N\\ p>2}} \frac{(p-1)/(p-2)}{1+1/p} \ll 1,$$

uniformly in N. This is easy; since

$$\frac{(p-1)/(p-2)}{1+1/p} = \frac{p(p-1)}{(p+1)(p-2)} = 1 + \frac{2}{p^2-p-2} < \exp\left(\frac{2}{p^2-p-2}\right),$$

the product in question is $< \exp(2\sum_{p>2}(p^2-p-2)^{-1}) \ll 1$. ∎

We now let

$$\mathscr{A} := \{N \in \mathbf{N} : R(N) > 0\}.$$

We will prove the following:

Theorem 7.14. *The set $\mathscr{A}$ has positive lower density.*

Once this is proved, Theorem 7.10 follows easily. Indeed, let $\mathscr{B} = \mathscr{A} \cup \{0,1\}$, so that from the above discussion $\mathscr{B}$ is a basis of finite order $h \geq 1$, say. Then for every integer $n \geq 2$, we can write

$$n-2 = p_1 + p_2 + \cdots + p_{2k} + \overbrace{1+1+\cdots+1}^{l\text{ summands}},$$

say, where the p_i are primes, k and l are nonnegative integers, and $k+l \leq h$. Then

$$n = p_1 + \cdots + p_{2k} + (l+2).$$

Since $l+2 \geq 2$, it can be written as a sum of 2s and 3s, where the number of summands is at most $(l+2)/2 \leq h/2+1$. This means that n has a representation as a sum of at most $2k+h/2+1 \leq 5h/2+1$ primes. Theorem 7.10 follows with $S = 5h/2+1$.

The main tool needed in the proof of Theorem 7.14 is the upper bound (7.32). It is initially surprising that an upper bound for $R(N)$ would be of use in establishing a lower density result. But this seeming paradox is easily explained: As we will see shortly, it is a simple matter to obtain a lower bound for $\sum_{N \leq x} R(N)$. If, as (7.32) asserts, $R(N)$ is never too big, then the only way to account for the size of this lower bound is for there to be many terms for which $R(N)$ is nonzero. In other words, $\mathscr{A}$ must be fairly dense.

Lemma 7.15. *As $x \to \infty$, we have $\sum_{N \leq x} R(N) \gg x^2/(\log x)^2$.*

Proof. By Chebyshev's results from Chapter 3, we have $\pi(x/2) \gg x/\log x$ as $x \to \infty$. Thus

$$\sum_{N \leq x} R(N) = \sum_{N \leq x} \sum_{p+q=N} 1 = \sum_{p+q \leq x} 1 \geq \left(\sum_{p \leq x/2} 1\right)^2 \gg \frac{x^2}{(\log x)^2}. \qquad \square$$

Lemma 7.16. *As $x \to \infty$, we have $\sum_{N \leq x} R(N)^2 \ll x^3/(\log x)^4$.*

Proof. From (7.32),

$$\begin{aligned}
\sum_{N \leq x} R(N)^2 &\ll \sum_{2 \leq N \leq x} \left(\frac{N}{(\log N)^2} \prod_{p \mid N}\left(1+\frac{1}{p}\right)\right)^2 \\
&\ll \frac{x^2}{(\log x)^4} \sum_{2 \leq N \leq x} \left(\prod_{p \mid N}\left(1+\frac{1}{p}\right)\right)^2 \\
&\ll \frac{x^2}{(\log x)^4} \sum_{2 \leq N \leq x} \left(\sum_{d \mid N} \frac{1}{d}\right)^2.
\end{aligned}$$

It remains to show that the outer sum is $O(x)$. For this, observe that for any natural numbers d_1 and d_2,

$$[d_1, d_2] \geq \max\{d_1, d_2\} \geq (d_1 d_2)^{1/2},$$

so that

$$\sum_{N\le x}\left(\sum_{d\mid N}\frac{1}{d}\right)^2=\sum_{N\le x}\sum_{d_1\mid N}\sum_{d_2\mid N}\frac{1}{d_1d_2}=\sum_{d_1,d_2\le x}\frac{1}{d_1d_2}\sum_{\substack{N\le x\\ d_1\mid N,d_2\mid N}}1$$

$$\le\sum_{d_1,d_2\le x}\frac{1}{d_1d_2}\frac{x}{[d_1,d_2]}\le x\sum_{d_1,d_2\le x}\frac{1}{(d_1d_2)^{\frac{3}{2}}}\le x\left(\sum_{d=1}^{\infty}d^{-\frac{3}{2}}\right)^2\ll x.\quad\square$$

Proof of Theorem 7.14. Writing $R(N)=R(N)\cdot 1$, the Schwarz inequality and Lemmas 7.15 and 7.16 yield that

$$\frac{x^4}{(\log x)^4}\ll\left(\sum_{N\le x}R(N)\right)^2=\left(\sum_{\substack{N\le x\\ R(N)>0}}R(N)\cdot 1\right)^2$$

$$\le\sum_{\substack{N\le x\\ R(N)>0}}R(N)^2\sum_{\substack{N\le x\\ R(N)>0}}1\ll\frac{x^3}{(\log x)^4}A(x),$$

so that $A(x)\gg x$ as $x\to\infty$. In other words, $\mathscr{A}$ has positive lower density. $\square$

5. Appendix: Justifying the Brun–Hooley sieve

5.1. The sifting function perspective. It is worthwhile for us to revisit some of the results of Chapter 6 from a a slightly different perspective. Keeping the notation of Chapter 6, §2, we introduce the *sifting function*

$$s(n):=\begin{cases}1 & \text{if } \gcd(n,P)=1,\\ 0 & \text{otherwise.}\end{cases}$$

Then

$$S(\mathscr{A},\mathscr{P})=\sum_{a\in A}s(a).\tag{7.33}$$

Since $\sum_{d\mid m}\mu(d)$ vanishes for each natural number $m>1$, the sifting function $s(n)$ has the following important representation:

$$s(n)=\sum_{d\mid n,\ d\mid P}\mu(d).$$

Substituting this into (7.33) and interchanging the order of summation, we easily arrive at Theorem 6.2 (the sieve of Eratosthenes–Legendre). In the same way, Brun's pure sieve is a consequence of the following lemma:

Lemma 7.17. *Let n be a natural number. The expression*

$$\sum_{\substack{d|n, d|P \\ \omega(d) \leq m}} \mu(d) - \sum_{d|n, d|P} \mu(d)$$

is nonnegative or nonpositive according to whether the integer $m \geq 0$ is even or odd.

The proof of Lemma 7.17 is essentially the one already given for the Bonferroni inequalities. Namely, if we suppose that n is divisible by exactly l primes $p \in \mathscr{P}$, then by Lemma 6.10,

$$\sum_{\substack{d|n, d|P \\ \omega(d) \leq m}} \mu(d) = \sum_{k=0}^{m} (-1)^k \binom{l}{k} \begin{cases} = 1 & \text{if } l = 0 \text{ (i.e., if } \gcd(n, P) = 1), \\ \geq 0 & \text{if } l \geq 1, m \text{ even}, \\ \leq 0 & \text{if } l \geq 1, m \text{ odd}. \end{cases}$$

For later use we note the following consequence of Lemma 7.17:

Lemma 7.18. *If n is a natural number and $m \geq 0$ is even, then*

$$0 \leq \sum_{\substack{d|n, d|P \\ \omega(d) \leq m}} \mu(d) - \sum_{d|n, d|P} \mu(d) \leq \sum_{\substack{d|n, d|P \\ \omega(d) = m+1}} 1.$$

5.2. The upper bound. The Brun–Hooley method takes two forms, depending on whether we are after upper or lower bounds. Here we describe the simpler upper bound method. We suppose the sifting set $\mathscr{P}$ to be partitioned into r disjoint sets, say $\mathscr{P} = \dot{\bigcup}_{j=1}^{r} \mathscr{P}_j$. Then n is divisible by no prime $p \in \mathscr{P}$ precisely when n is divisible by no prime $p \in \mathscr{P}_j$ for every $1 \leq j \leq r$. Consequently, setting $P_j := \prod_{p \in \mathscr{P}_j} p$, and invoking Lemma 7.17 (with $\mathscr{P}_j, P_j$ in place of $\mathscr{P}, P$) we see that

$$\begin{aligned} s(n) = \sum_{d|n, d|P} \mu(d) &= \prod_{j=1}^{r} \sum_{d_j|n, d_j|P_j} \mu(d_j) \\ &\leq \prod_{j=1}^{r} \sum_{\substack{d_j|n, d_j|P_j \\ \omega(d_j) \leq m_j}} \mu(d_j), \end{aligned}$$

for any choice of nonnegative even integers $m_1, \ldots, m_r$. Referring to (7.33), we obtain the upper bound

$$\begin{aligned} S(\mathscr{A}, \mathscr{P}) &\leq \sum_{\substack{d_1,\ldots,d_r \\ d_j \mid P_j,\ \omega(d_j)\leq m_j}} \mu(d_1)\cdots\mu(d_r) A_{d_1\cdots d_r} \\ &= X \sum_{\substack{d_1,\ldots,d_r \\ d_j \mid P_j,\ \omega(d_j)\leq m_j}} \mu(d_1)\cdots\mu(d_r)\alpha(d_1)\cdots\alpha(d_r) \\ &\qquad + \sum_{\substack{d_1,\ldots,d_r \\ d_j \mid P_j, \omega(d_j)\leq m_j}} \mu(d_1)\cdots\mu(d_r) r(d_1\cdots d_r). \end{aligned}$$

Hence $S(\mathscr{A}, \mathscr{P})$ is bounded above by

$$X \prod_{j=1}^{r} \sum_{\substack{d_j \mid P_j \\ \omega(d_j)\leq m_j}} \mu(d_j)\alpha(d_j) + \sum_{\substack{d_1,\ldots,d_r \\ d_j \mid P_j,\ \omega(d_j)\leq m_j}} \mu(d_1)\cdots\mu(d_r) r(d_1\cdots d_r). \tag{7.34}$$

This is the basic inequality behind the upper bound of the Brun–Hooley method. To facilitate applications, we replace the first term of (7.34), which we think of as the main term, with something more easily compared with $X\prod_{p\in\mathscr{P}}(1-\alpha(p))$. This can be accomplished by replacing the jth term of the product in (7.34) with something more easily compared with $\prod_{p\in\mathscr{P}_j}(1-\alpha(p))$. For this, we utilize Lemma 6.10, which implies that for each $1 \leq j \leq r$,

$$0 \leq \sum_{\substack{d_j \mid P_j \\ \omega(d_j)\leq m_j}} \mu(d_j)\alpha(d_j) - \prod_{p\in\mathscr{P}_j}(1-\alpha(p)) \leq \sum_{\substack{d_j \mid P_j \\ \omega(d_j)=m_j+1}} \alpha(d_j).$$

Thus, if we set

$$\prod\nolimits^{(j)} := \prod_{p\in\mathscr{P}_j}(1-\alpha(p)), \qquad \sum\nolimits^{(j)} := \sum_{\substack{d_j \mid P_j \\ \omega(d_j)=m_j+1}} \alpha(d_j), \tag{7.35}$$

then

$$\begin{aligned} X \prod_{j=1}^{r} \sum_{\substack{d_j \mid P_j \\ \omega(d_j)\leq m_j}} \mu(d_j)\alpha(d_j) &\leq X \prod_{j=1}^{r} \left(\prod\nolimits^{(j)} + \sum\nolimits^{(j)} \right) \\ &= X \prod_{p\in\mathscr{P}}(1-\alpha(p)) \prod_{j=1}^{r} \left(1 + \sum\nolimits^{(j)} \Big/ \prod\nolimits^{(j)} \right), \end{aligned}$$

provided the division makes sense, i.e., provided $\alpha(p) < 1$ for each $p \in \mathscr{P}$. Henceforth, we assume this condition on α.

Recalling that $1 + t \leq \exp(t)$, after estimating the remainder term of (7.34) trivially, we arrive at the following theorem:

Theorem 7.19 (Brun–Hooley sieve, upper bound)**.** *Let $\mathscr{P} = \dot{\bigcup}_{j=1}^{r} \mathscr{P}_j$ be a partition of $\mathscr{P}$. Suppose that $\alpha(p) < 1$ for each $p \in \mathscr{P}$. For any choice of nonnegative even integers $m_1, \ldots, m_r$, we have*

$$S(\mathscr{A}, \mathscr{P}) \leq X \prod_{p \in \mathscr{P}} (1 - \alpha(p)) \exp\left(\sum_{j=1}^{r} \left(\sum\nolimits^{(j)} \Big/ \prod\nolimits^{(j)} \right) \right) + O\Bigg(\sum_{\substack{d_1, \ldots, d_r \\ d_j \mid P_j,\ \omega(d_j) \leq m_j}} |r(d_1 \cdots d_r)| \Bigg),$$

where $\prod^{(j)}$ and $\sum^{(j)}$ are defined, for $1 \leq j \leq r$, by (7.35)*, and the implied constant is absolute.*

5.3. The lower bound. We turn now to the problem of bounding $S(\mathscr{A}, \mathscr{P})$ from below. A natural temptation here is to simply parallel what we did in the upper bound case: If we suppose $m_1, \ldots, m_r$ to be r odd natural numbers, then for each j,

$$\sum_{\substack{d_j \mid n, d_j \mid P_j \\ \omega(d_j) \leq m_j}} \mu(d_j) \leq \sum_{d_j \mid n, d_j \mid P_j} \mu(d_j).$$

But since it is (generally) not the case that for every $1 \leq j \leq r$, both sides of this inequality are nonnegative, we cannot simply take the product of both sides over j and expect the inequality to be preserved.

So we require a different approach. By Lemma 7.18 (with $\mathscr{P}, P$ replaced by $\mathscr{P}_j, P_j$), for any choice of nonnegative even integers $m_1, \ldots, m_r$, we have

$$0 \leq \sum_{\substack{d_j \mid n, d_j \mid P_j \\ \omega(d_j) \leq m_j}} \mu(d_j) - \sum_{d_j \mid n, d_j \mid P} \mu(d_j) \leq \sum_{\substack{d_j \mid n, d_j \mid P \\ \omega(d_j) = m_j + 1}} 1 \quad (1 \leq j \leq r). \tag{7.36}$$

These bounds allow us to a coax a lower bound for the sifting function

$$s(n) = \prod_{j=1}^{r} \sum_{d_j \mid n, d_j \mid P_j} \mu(d_j) \tag{7.37}$$

out of the following general inequality:

Lemma 7.20 ([**FH00**, Lemma 1])**.** *Suppose that $0 \leq x_j \leq y_j$ for $1 \leq j \leq r$. Then*

$$x_1 \cdots x_r \geq y_1 \cdots y_r - \sum_{l=1}^{r} (y_l - x_l) \prod_{\substack{j=1 \\ j \neq l}}^{r} y_j.$$

Proof. The result holds with equality when $r=1$. If the lemma holds for $r-1$ for a certain $r\geq 2$, then

$$\begin{aligned} y_1\cdots y_r - x_1\cdots x_r &= (y_1\cdots y_{r-1}-x_1\cdots x_{r-1})y_r + (x_1\cdots x_{r-1})(y_r-x_r)\\ &\leq (y_1\cdots y_{r-1}-x_1\cdots x_{r-1})y_r + (y_1\cdots y_{r-1})(y_r-x_r)\\ &\leq \sum_{l=1}^{r-1}(y_l-x_l)\prod_{\substack{j=1\\ j\neq l}}^{r} y_j + (y_r-x_r)\prod_{\substack{j=1\\ j\neq r}}^{r} y_j, \end{aligned}$$

which is just $\sum_{l=1}^{r}(y_l-x_l)\prod_{\substack{j=1\\ j\neq l}}^{r} y_j$. So the result follows by induction. $\square$

Assuming $m_1,\dots,m_r$ are nonnegative even integers, we apply Lemma 7.20 with

$$x_j := \sum_{d_j\mid n, d_j\mid P_j}\mu(d_j),\quad y_j := \sum_{\substack{d_j\mid n, d_j\mid P_j\\ \omega(d_j)\leq m_j}}\mu(d_j).$$

Equation (7.36) implies that the hypotheses of Lemma 7.20 are satisfied and gives us an upper bound on the terms y_l-x_l. Using this bound in Lemma 7.20 and recalling (7.37), we obtain

$$s(n)\geq \prod_{j=1}^{r}\sum_{\substack{d_j\mid n,\ d_j\mid P_j\\ \omega(d_j)\leq m_j}}\mu(d_j) - \sum_{l=1}^{r}\Bigg(\sum_{\substack{d_l\mid n,\ d_l\mid P_l\\ \omega(d_l)=m_l+1}} 1\Bigg)\prod_{\substack{j=1\\ j\neq l}}^{r}\Bigg(\sum_{\substack{d_j\mid n,\ d_j\mid P_j\\ \omega(d_j)\leq m_j}}\mu(d_j)\Bigg).$$

Summing over $n\in\mathscr{A}$ shows that

$$\begin{aligned} (7.38)\quad S(\mathscr{A},\mathscr{P}) \geq &\sum_{\substack{d_1,\dots,d_r\\ d_j\mid P_j,\ \omega(d_j)\leq m_j}}\mu(d_1)\cdots\mu(d_r)A_{d_1\cdots d_r}\\ &-\sum_{l=1}^{r}\sum_{\substack{d_1,\dots,d_r\\ d_j\mid P_j,\ \omega(d_j)\leq m_j\,(j\neq l)\\ d_l\mid P_l,\ \omega(d_l)=m_l+1}}\frac{\mu(d_1)\cdots\mu(d_r)}{\mu(d_l)}A_{d_1\cdots d_r}. \end{aligned}$$

Writing $A_d = X\alpha(d)+r(d)$, the right-hand side of (7.38) becomes

$$(7.39)\quad X\prod_{j=1}^{r}\sum_{\substack{d_j\mid P_j\\ \omega(d_j)\leq m_j}}\mu(d_j)\alpha(d_j) - X\sum_{l=1}^{r}\sum_{\substack{d_l\mid P_l\\ \omega(d_l)=m_l+1}}\alpha(d_l)\prod_{j\neq l}\sum_{\substack{d_j\mid P_j\\ \omega(d_j)\leq m_j}}\mu(d_j)\alpha(d_j),$$

up to an error term that is (with an absolute implied constant)

$$\ll \sum_{\substack{d_j\mid P_j\ (1\leq j\leq r)\\ \theta_{d_1,\dots,d_r}}}|r(d_1\cdots d_r)|.$$

Here $\theta_{d_1,\ldots,d_r}$ denotes the condition that there exist $r-1$ indices j, $1 \le j \le r$, for which $\omega(d_j) \le m_j$, while the remaining index satisfies $\omega(d_j) \le m_j + 1$.

Assume, as we did for the upper bound, that $\alpha(p) < 1$ for each $p \in \mathscr{P}$. Lemma 6.10 implies that for each $1 \le j \le r$,

$$\sum_{\substack{d_j \mid P_j \\ \omega(d_j) \le m_j}} \mu(d_j)\alpha(d_j) \ge \prod_{p \in \mathscr{P}_j} (1 - \alpha(p)) > 0,$$

so that the main term in (7.39) is

$$X\left(1 - \sum_{1 \le l \le r} \frac{\sum_{d_l \mid P_l,\ \omega(d_l) = m_l + 1} \alpha(d_l)}{\sum_{d_l \mid P_l,\ \omega(d_l) \le m_l} \mu(d_l)\alpha(d_l)}\right) \prod_{j=1}^{r} \sum_{\substack{d_j \mid P_j \\ \omega(d_j) \le m_j}} \mu(d_j)\alpha(d_j)$$

$$\ge X \prod_{p \in \mathscr{P}} (1 - \alpha(p)) \left(1 - \sum_{1 \le l \le r} \left(\sum_{\substack{d_l \mid P_l \\ \omega(d_l) = m_l + 1}} \alpha(d_l) \Big/ \prod_{p \in \mathscr{P}_l} (1 - \alpha(p))\right)\right).$$

Summarizing, we have proved the following theorem:

Theorem 7.21 (Brun–Hooley sieve, lower bound)**.** *Let $\mathscr{P} = \dot{\bigcup}_{j=1}^{r} \mathscr{P}_j$ be a partition of $\mathscr{P}$. Suppose that $\alpha(p) < 1$ for each $p \in \mathscr{P}$. For any choice of nonnegative even integers $m_1, \ldots, m_r$, we have*

$$S(\mathscr{A}, \mathscr{P}) \ge X \prod_{p \in \mathscr{P}} (1 - \alpha(p)) \left(1 - \sum_{j=1}^{r} \left(\sum\nolimits^{(j)} \Big/ \prod\nolimits^{(j)} \right)\right) + O\Bigg(\sum_{\substack{d_j \mid P_j (1 \le j \le r) \\ \theta_{d_1,\ldots,d_r}}} |r(d_1 \cdots d_r)| \Bigg),$$

where $\prod^{(j)}$ and $\sum^{(j)}$ are defined, for $1 \le j \le r$, by (7.35)*, and the implied constant is absolute.*

Notes

Brun's paper [**Bru20**], and much else besides, can be found translated into English in Wang's anthology [**Wan02**] of papers on the Goldbach problem.

Chapters 6 and 7 are intended as a first introduction to sieves. Thus, we barely scratch the surface of the modern theory; e.g., we have not touched at all on Selberg's Λ^2-method, even though its upper bound form is not so difficult to understand and in many problems gives stronger upper bounds than the Brun–Hooley method. We have also said nothing about the "large sieve". For the reader looking to approach these subjects for the first time, we recommend the texts of Schwarz [**Sch74**], Cojocaru & Murty [**CM06**], and (for the Selberg sieve) Montgomery and Vaughan [**MV07**, Chapter 3]. More encyclopedic accounts of sieve methods include the monographs of Halberstam & Richert [**HR74**], Greaves [**Gre01**], and Friedlander & Iwaniec [**FI10**]. See See also [**DH08**] and [**IK04**, Chapter 6]. Another treatment of the Brun–Hooley sieve can be found in the the introduction to analytic number theory written by wwBateman & Diamond [**BD04**].

For the study of classical problems in additive number theory, excellent references are Ostmann's two-volume work [**Ost56**] and Nathanson's book [**Nat96**]. Nathanson's text includes a proof of the following important theorem of Vinogradov which should be compared with Theorem 7.9:

★ **Theorem 7.22** (Three primes theorem)**.** *Let $R_3(N)$ denote the number of ways of writing N as an ordered sum of three primes. As $N \to \infty$ through odd integers, we have*

$$R_3(N) \sim \prod_{p} \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p \mid N} \left(1 - \frac{1}{p^2 - 3p + 3}\right) \frac{N^2}{2(\log N)^3}.$$

In particular, every sufficiently large odd integer is a sum of three primes.

It follows from Vinogradov's result that every large enough natural number is the sum of at most 4 primes. (This can be compared with the result of Ramaré [**Ram95**] that *every* integer > 1 is a sum of at most 7 primes.) While Vinogradov's theorem has a similar flavor to Schnirelmann's result (Theorem 7.9), the proof, which depends on the Hardy–Littlewood circle method, requires substantially deeper input from prime number theory. Kumchev & Tolev have written an up-to-date survey of additive prime number theory [**KT05**].

Exercises

1. Let $\pi(x, z)$ denote the number of $n \leq x$ with no prime divisor $\leq z$. Suppose $z = z(x) \to \infty$ but that $z = x^{o(1)}$, as $x \to \infty$. Using the fundamental lemma, prove that $\pi(x, z) \sim x \prod_{p \leq z}(1 - 1/p)$. Prove a similar result for the function $\pi_2(x, z)$ introduced in (6.4).
2. (Titchmarsh [**Tit30**]) Use the Brun–Titchmarsh inequality so show that $\sum_{p \leq x} \tau(p-1) \ll x$, where the sum is over all primes $p \leq x$ and τ is the usual divisor function. *Hint:* For each $n \leq x$, one has $\tau(n) \leq 2 \sum_{d \mid n,\ d \leq \sqrt{x}} 1$.

   Remark. Linnik [**Lin61**] showed that $\sum_{p \leq x} \tau(p-1) \sim \frac{\zeta(2)\zeta(3)}{\zeta(6)} x$, as $x \to \infty$. A modern proof is suggested in the book of Iwaniec and Kowalski [**IK04**, p. 420].

3. Check the details of the remark following Theorem 7.3. In other words, show how to deduce from that theorem our previous upper bounds on $\pi_2(x)$, $R(N)$, and $\pi(x; q, a)$.
4. (Hardy & Littlewood [**HL23**]) Using Theorem 7.3 (or otherwise), show that $\pi(y + x) - \pi(y) \ll \frac{x}{\log x}$ for $x, y \geq 2$, where the implied constant is absolute.

   Remark. Hardy & Littlewood conjectured that in fact $\pi(x + y) \leq \pi(x) + \pi(y)$ for all $x, y \geq 2$. This conjecture is now in disrepute, as Hensley & Richards have shown that it contradicts Schinzel's Hypothesis H (see [**HR73**]).

5. Suppose that y is a function of x which tends to infinity, but which satisfies $y = x^{\epsilon}$, where $\epsilon(x) \to 0$ as $x \to \infty$. Show that all but $o(x)$ of the natural numbers $n \leq x$ have a prime factor $> y$. In other words, with Ψ defined by (1.7), we have $\Psi(x, y) = o(x)$, as $x \to \infty$.
6. (Heilbronn [**Hei31**]) Suppose that $F(T) \in \mathbf{Z}[T]$ is irreducible over $\mathbf{Q}$, and let $\nu(d)$ denote the number of roots of f modulo d. Landau showed ([**Lan02**]; see also [**DH09**]) that $\sum_{p \leq x} \nu(p) p^{-1} = \log\log x + C_F + O_F(1/\log x)$. (One should think of this as a number field analogue of Mertens's first theorem.)

   Assuming Landau's result, show that the number of $n \leq x$ for which $F(n)$ is prime is $\ll_F x/\log x$, for all $x \geq 2$.
7. Erdős & Mirsky [**EM52**] conjectured in 1952 that there are infinitely many pairs of integers N and $N+1$ with $\tau(N) = \tau(N+1)$. In this exercise, we outline a proof that the related equation $\tau(N) = \tau(N+360)$

has infinitely many solutions. Let

$$p_1 = 11, \quad p_2 = 17, \quad p_3 = 23, \quad p_4 = 29, \quad p_5 = 41, \quad p_6 = 47.$$

Let L be the least common multiple of the differences $p_j - p_i$, for $1 \leq i < j \leq 6$; one checks directly that $L = 360$. Set $M := \operatorname{lcm}[L, \prod_{i=1}^{6} p_i]$.

(a) Referring to Table 1, show that there are infinitely many n for which each of the numbers $Mp_i n + 1$ is squarefree and for which

$$\sum_{i=1}^{6} \omega(Mp_i n + 1) \leq 20.$$

(b) For each n as in (a), show that there is a pair of indices i and j, with $1 \leq i < j \leq 6$, for which $\omega(Mp_i n + 1) = \omega(Mp_j n + 1)$.

(c) With n, i, and j as above, show that the numbers

$$N := \frac{L}{p_j - p_i} p_i (Mp_j n + 1), \quad N' := \frac{L}{p_j - p_i} p_j (Mp_i n + 1)$$

have the same number of divisors.

(d) Check that $N' - N = L$. Conclude.

Remark. The method of proof here is due to Spiro [**Spi81**] (cf. the exposition of Hildebrand [**Hil02**]). Building on her ideas, Heath-Brown [**HB84**] later settled the original Erdős–Mirsky conjecture. By different methods, Graham et al. [**GGPY11**] have proved the stronger assertion that infinitely often both n and $n+1$ have factorization pattern $\{2, 1, 1, 1\}$. Here the *factorization pattern* of a number is the multiset of exponents appearing in its canonical prime factorization.

8. (Estermann [**Est32**]) One form of the *Riemann Hypothesis for Dirichlet L-functions*, also called the *Extended Riemann Hypothesis*, is that if a and $m \geq 2$ are coprime integers, and $x \geq 2$, then

$$\left| \pi(x; m, a) - \frac{1}{\varphi(m)} \operatorname{Li}(x) \right| < x^{1/2} (\log x + 2 \log m).$$

Let $\mathscr{A}$ be the set of shifted primes $\{p + 2 : p \leq x\}$, and let $\mathscr{P}$ be the set of odd primes. Assuming the Extended Riemann Hypothesis (ERH), show that for some fixed $u > 0$, we have $S(\mathscr{A}, \mathscr{P}, x^{1/u}) \gg x/(\log x)^2$ for large x. Deduce that there are infinitely many primes p for which $p + 2$ has at most u prime factors. *Hint:* Use the fundamental lemma!

Remark. Under ERH, Estermann showed that $p + 2$ is infinitely often a 6-almost prime. Renyi [**Ren48**] later proved (unconditionally) that $p + 2$ is infinitely often an r-almost prime for a fixed, unspecified r. In the text, we have already alluded to Chen's result [**Che73**], still state-of-the-art, that $p + 2$ is infinitely often a 2-almost prime. For a proof that $p+2$ is infinitely often an 8-almost prime using the Brun–Hooley sieve, see [**FH00**, §4]

9. (Erdős [**Erd35d**]) In this exercise, we study smooth values of shifted primes $p-1$. (Recall that a number is said to be y-smooth if $P(n) \le y$, where $P(n)$ denotes the largest prime factor of n.) Our goal is the following result: There is an $\epsilon > 0$ with the property that for large x, at least $\frac{1}{2}\frac{x}{\log x}$ of the primes $p \le x$ have $P(p-1) < x^{1-\epsilon}$.
   (a) Given a prime $2 < p \le x$, put $M_p := (p-1)/P(p-1)$. Using Theorem 7.3, prove that for a fixed $M \le x^{1/2}$, the number of $p \le x$ with $M_p = M$ is $\ll \frac{1}{\varphi(M)} x/(\log x)^2$.
   (b) Show that for each $\epsilon > 0$ and all $x > \exp(1/\epsilon)$, we have
   $$\sum_{M \le x^{\epsilon}} \frac{1}{\varphi(M)} \ll \epsilon \log x,$$
   with an absolute implied constant. *Hint:* Compare the left-hand sum to the product $\prod_{p \le x^{\epsilon}} \left(\sum_{j=0}^{\infty} 1/\varphi(p^j)\right)$.
   (c) Using (a) and (b), show for each $\epsilon \in (0, 1/2)$ and all $x > \exp(1/\epsilon)$, the number of $p \le x$ with $P(p-1) \ge x^{1-\epsilon}$ is $\ll \epsilon x/\log x$. Here the implied constant is absolute.
   (d) Conclude by taking $\epsilon > 0$ sufficiently small.

10. (Continuation) In Exercise 6.10, we showed that almost all natural numbers do not belong to the range of the Euler function. Since φ maps each natural number to one that is no larger, it follows from the Pigeonhole principle that the function
   $$M(x) := \max_{n \le x} \#\varphi^{-1}(n)$$
   tends to infinity as $x \to \infty$. In other words, there are values of the Euler function assumed arbitrarily often. Here we show that if ϵ is chosen as in the preceding exercise and $x > x_0(\epsilon)$, then
   $$M(x) > x^{\epsilon/2}.$$
   Thus, there are values of n for which the number of preimages of n under the Euler function is as large as a fixed power of n.
   (a) Let $\mathscr{Q}$ be the set of primes $p \le (\log x)^{\frac{1}{1-\epsilon}}$ with $P(p-1) \le \log x$. Show that $\#\mathscr{Q} \gg (\log x)^{\frac{1}{1-\epsilon}}/\log\log x$ for large x.
   (b) Let $l = \lfloor (1-\epsilon)\frac{\log x}{\log\log x} \rfloor$, and let $\mathscr{A}$ be the set of natural numbers which can be formed as a product of l distinct elements of $\mathscr{Q}$. Show that $\mathscr{A} \subset [1, x]$. Prove that for large x,
   $$\#\mathscr{A} = \binom{\#\mathscr{Q}}{l} \ge \left(\frac{\#\mathscr{Q}}{l}\right)^l > x^{2\epsilon/3}.$$

(c) Show that if $a \in \mathscr{A}$, then $\varphi(a)$ is $(\log x)$-smooth.

(d) Let $\mathscr{B}$ be the set of $(\log x)$-smooth integers in $[1, x]$, so that φ maps $\mathscr{A}$ into $\mathscr{B}$. Show that the number of elements of $\mathscr{B}$ is at most $x^{\epsilon/6}$, once x is large.

Hint: Let $r = \lceil 12/\epsilon \rceil$. Given $b \in \mathscr{B}$, write $b = b_1 b_2$, where b_1 is not divisible by the rth power of a prime and b_2 is r-full, in the sense of Exercise 11. Show that the number of possibilities for b_1 is $x^{o(1)}$ and the number of possibilities for b_2 is $\ll x^{1/r} \ll x^{\epsilon/12}$.

(e) Conclude that there is some $n \le x$ for which $\#\varphi^{-1}(n) \ge \frac{\#\mathscr{A}}{\#\mathscr{B}} > x^{\epsilon/2}$.

Remark. It seems likely that for each fixed $\epsilon \in (0,1)$ and all $x > x_0(\epsilon)$, there are $\gg_\epsilon x/\log x$ primes $p \le x$ for which $p-1$ is x^ϵ-smooth. (If one considers all natural numbers n and not just shifted primes, the analogous lower bound is known and simple to prove; see, e.g., [**IK04**, p. 182].) If this conjecture is true, then an easy modification of the above argument shows that $M(x) > x^{1-o(1)}$, as $x \to \infty$. For further discussion, as well as a more precise conjecture on the true behavior of $M(x)$, see Pomerance's survey [**Pom89**].

† 11. (Erdős [**Erd35d**]) In Exercise 3.24, we proved that a typical natural number $n \le x$ has about $\log\log x$ prime factors. One may wonder whether such a result continues to hold if one restricts n to certain special classes of numbers. Here we treat numbers of the form $p-1$, where p is prime. (Such numbers are important, for example, in the study of the Euler φ-function.) We show that we do indeed have such a result, and that in fact for each $\epsilon > 0$,

$$\#\{p \le x : |\omega(p-1) - \log\log x| > \epsilon \log\log x\} \ll_\epsilon x/(\log x)^{1+\delta},$$

where $\delta > 0$ depends on ϵ.

(a) Assume $x \ge 3$. Show that all but $O(x/(\log x)^2)$ natural numbers $n \le x$ possess both of the following properties:

(i) the largest prime factor $P(n)$ (say) of n satisfies $P(n) > x^{1/(6\log\log x)}$,

(ii) n is not divisible by $P(n)^2$,

Hint: Use the result of Exercise 3.34 to handle condition (i).

(b) For each nonnegative integer k, let N_k be the number of primes $p \le x$ for which $p-1$ has both properties (i) and (ii) and satisfies $\omega(p-1) = k$. Show that

$$N_k \le \sum_{\substack{a \le x^{1-1/(6\log\log x)} \\ \omega(a) = k-1}} \sum_{\substack{p \le x \\ a \mid p-1 \text{ and } \frac{p-1}{a} \text{ is prime}}} 1.$$

(c) Show that for each natural number $a < x$,

$$\sum_{\substack{p \le x \\ a \mid p-1 \text{ and } \frac{p-1}{a} \text{ is prime}}} 1 \ll \frac{x}{\varphi(a)(\log \frac{x}{a})^2},$$

with an absolute implied constant.

(d) Convince yourself that

$$\sum_{\substack{a \le x \\ \omega(a) = k-1}} \frac{1}{\varphi(a)} \le \frac{1}{(k-1)!} \left(\sum_{p^l \le x} \frac{1}{\varphi(p^l)} \right)^{k-1},$$

where the right-hand sum is over primes and prime powers $p^l \le x$.

(e) Show that for a certain absolute constant C,

$$N_k \ll \frac{x(\log\log x)^2}{(\log x)^2} \frac{(\log\log x + C)^{k-1}}{(k-1)!},$$

uniformly in k. Complete the proof by summing this estimate over $k < (1-\epsilon)\log\log x$ and $k > (1+\epsilon)\log\log x$.

12. For each prime p, let p' be the prime immediately following p.
    (a) Show (without using the sieve!) that given $\epsilon > 0$, one can choose U so large that the following holds: The number of primes $p \le x$ for which $p' - p > U \log x$ is $< \epsilon x/\log x$, once x is large.
    (b) Show (now using the sieve) that given $\epsilon > 0$, one can choose u small enough that the following holds: The number of primes $p \le x$ with $p' - p < u \log x$ is $< \epsilon x/\log x$, once x is large.

Remark. It is conjectured (see, e.g., [**Sou07**, Conjecture 1]) that for each fixed $u > 0$,

$$\lim_{x \to \infty} \frac{\#\{p \le x : p' - p \le u \log x\}}{\#\{p \le x\}} \to 1 - e^{-u}.$$

In recent work, Goldston, Pintz, and Yıldırım [**GPY11**] have shown that with lim replaced by lim inf, the left-hand side is positive for every choice of $u > 0$.

13. (Erdős & Nathanson [**EN96**]) Let p_n be the nth prime number (in the usual, increasing order). Use Theorem 7.8 to show that for each $\lambda > 2$, the series

$$\sum_{n=1}^{\infty} \frac{1}{n(\log\log 3n)^{\lambda}(p_{n+1} - p_n)}$$

converges. It is conjectured that this result is the best possible, in the sense that the series diverges when $\lambda = 2$.

† 14. (Luca [**Luc07**]) Show that the number of natural numbers not exceeding x which can be written in the form $p^2 - q^2$, where p and q are primes, is $\ll x/\log x$.

15. Call the natural number n *twinnish* if $d + n/d + 1$ is prime for every d dividing n. If p is the smaller member of a twin prime pair, then p is twinnish, but there are many other such n, for example $n = 21$ and (less obviously) $n = 190757 = 7^2 \cdot 17 \cdot 229$. Prove or disprove: $\sum \frac{1}{n} < \infty$, where the sum is extended over all twinnish numbers n.

16. By modifying the argument of §3.3, show that the number of representations of an even natural number N as a sum of two 7-almost primes is $\gg \frac{N}{(\log N)^2} \prod_{p|N,\ p>2} \frac{p-1}{p-2}$, as $N \to \infty$.

† 17. (Brun [**Bru19b**], [**Bru20**]) Use the Brun–Hooley sieve to prove the following theorems of Brun:
   (a) Every infinite arithmetic progression $a \bmod m$ with $\gcd(a, m) = 1$ contains infinitely many 5-almost primes. (Naturally, Dirichlet's theorem is off-limits here.)
   (b) If x is sufficiently large, there is always an 11-almost prime in the interval $(x, x + \sqrt{x}]$.

   Suggestion: Imitate the lower bound applications of the text, including the selection of the first several m_j by the greedy algorithm, but begin instead with the values $K = 2.49, K_1 = 2.50$.

18. (Landau [**Lan30**]) Show that under the hypotheses of Theorem 7.10, the set $\mathscr{A}$ is a basis of order at most $2\lfloor 1/\delta(\mathscr{A})\rfloor$.

† 19. Say that a set $\mathscr{A} \subset \mathbf{N}_0$ is an *asymptotic basis of finite order* if $\mathbf{N} \setminus h\mathscr{A}$ is finite for some $h \in \mathbf{N}$.
   (a) Show that if $a_1, \dots, a_k \in \mathbf{N}$ and $\gcd(a_1, \dots, a_k) = 1$, then every sufficiently large natural number can be written in the form $\sum_{i=1}^k a_i x_i$, where each $x_i \in \mathbf{N}_0$.
   (b) Let $\mathscr{A}$ be a subset of $\mathbf{N}_0$. Suppose that $0 \in \mathscr{A}$, that $\mathscr{A}$ has positive lower density (i.e., (7.30) holds), and that there is no integer $d > 1$ dividing each $a \in \mathscr{A}$. Show that $\mathscr{A}$ is an asymptotic basis of finite order.

20. (Landau, ibid.; see also Nathanson [**Nat87a**]) Suppose $\mathscr{P}$ is a set of primes with the property that

$$\liminf_{x\to\infty} \frac{\#\{p \in \mathscr{P} : p \le x\}}{x/\log x} > 0.$$

Show that there is a constant $S_{\mathscr{P}}$ with the property that every sufficiently large natural number is the sum of at most $S_{\mathscr{P}}$ primes all of which belong to $\mathscr{P}$.

† 21. (Prachar [**Pra52**]) Show that for large x, there are $\gg x$ natural numbers $n \le x$ that can be written in the form $q - p$, where $p, q \le x$ are primes. *Hint:* Adapt the second-moment method appearing in the proof of Schnirelmann's theorem.

† 22. (Continuation) For each prime p, write p' for the prime immediately following p. Show that for some $U > 0$, the following holds: For all large x, there are $\gg \log x$ natural numbers $n \le U \log x$ which can be written in the form $p' - p$ for some prime $p \le x$. *Hint:* Use Exercise 12.

23. (Romanov [**Rom34**]) Let $r(n)$ be the number of representations of n in the form $2^k + p$, where p is prime and $k \ge 1$. In this exercise and the next, we sketch a proof that $r(n) > 0$ on a set of positive lower density. In Exercise 25, we prove the complementary result that $r(n) = 0$ on a set of odd numbers of positive density.
   (a) Show that for all natural numbers n, we have $\sum_{d \mid n} \frac{1}{d} \ll \log\log 3n$.
   (b) For each odd integer d, let $l(d)$ denote the order of 2 modulo d. Show that if $l(d) \le x$, then d divides $D := \prod_{1 \le k \le x}(2^k - 1)$. Deduce from (a) that $\sum_{l(d) \le x} d^{-1} \ll \log(2x)$ for $x \ge 1$.
   (c) Using partial summation, prove that $\sum_{\substack{d \text{ odd} \\ d \ge 1}} \frac{1}{d \cdot l(d)} < \infty$.

24. (Continuation)
   (a) Show that $\sum_{n \le x} r(n) \gg x$ as $x \to \infty$.
   (b) Show that $\sum_{n \le x} r(n)^2$ does not exceed the number of solutions (p_1, p_2, k_1, k_2) to
   $$p_2 - p_1 = 2^{k_1} - 2^{k_2},$$
   where p_1, p_2 are primes $\le x$ and $1 \le k_1, k_2 \le \log x / \log 2$.
   (c) Show that the number of solutions as in (b) is $\ll x$. *Hint:* To estimate the number of solutions with $k_1 \ne k_2$, use Theorem 7.8 and the result of Exercise 23(c).
   (d) Deduce from (a)–(c), and the Cauchy–Schwarz inequality that there are $\gg x$ natural numbers $n \le x$ for which $r(n) > 0$.

25. (Continuation; Erdős [**Erd50b**], following Sierpiński [**Sie88**, Chapter XII])
   (a) Check that every integer k belongs to at least one of the congruence classes 0 mod 2, 0 mod 3, 1 mod 4, 3 mod 8, 7 mod 12, 23 mod 24.
   (b) Suppose $n \equiv 1 \pmod 3$, $n \equiv 1 \pmod 7$, $n \equiv 2 \pmod 5$, $n \equiv 2^3 \pmod{17}$, $n \equiv 2^7 \pmod{13}$, and $n \equiv 2^{23} \pmod{241}$. Show that for every integer $k \ge 0$, the number $n - 2^k$ is divisible by some prime from the set $\{3, 5, 7, 13, 17, 241\}$.
   (c) Suppose that in addition to the congruences in (b), we require also that $n \equiv 1 \pmod 2$ and $n \equiv 3 \pmod{31}$. Show that the positive n

satisfying all of these congruences comprise an infinite arithmetic progression of odd integers n with $r(n) = 0$.

Chapter 8

An Elementary Proof of the Prime Number Theorem

No elementary proof of the prime number theorem is known, and one may ask whether it is reasonable to expect one. Now we know that the theorem is roughly equivalent to a theorem about an analytic function, the theorem that Riemann's zeta function has no roots on a certain line. A proof of such a theorem, not fundamentally dependent on the theory of functions, seems to me extraordinarily unlikely. It is rash to assert that a mathematical theorem cannot be proved in a particular way; but one thing seems quite clear. We have certain views about the logic of the theory; we think that some theorems, as we say, "lie deep" and others nearer to the surface. If anyone produces an elementary proof of the prime number theorem, he will show that these views are wrong, that the subject does not hang together in the way we have supposed, and that it is time for the books to be cast aside and for the theory to be rewritten. – G. H. Hardy [**Boh52**]

1. Introduction

Recall that the *prime number theorem* asserts that as $x \to \infty$,

$$\pi(x) = (1 + o(1))\frac{x}{\log x}.$$

In Chapter 3, we described the early history of this result, including its origin as a conjecture by a young Gauss and its eventual proof by Hadamard and de la Vallée-Poussin (independently) in 1896, following a plan laid out by Riemann. Their proofs relied heavily on results from the then-budding field of complex analysis.

In 1931, Wiener and Ikehara proved the following theorem, which leads quickly to a proof of the prime number theorem requiring only scant knowledge of the analytic properties of the Riemann zeta-function $\zeta(s)$:

★ **Theorem 8.1.** *Let $\sum_{n=1}^{\infty} f(n)n^{-s}$ be a Dirichlet series with nonnegative coefficients, convergent for $\Re(s) > 1$. Let F be the (analytic) function defined by the series in this region, and suppose that F can be extended to a function analytic on an open set containing $\Re(s) \geq 1$, except possibly for a simple pole at $s = 1$. If R is the residue of F at $s = 1$, then*

$$\sum_{n \leq x} f(n) = (R + o(1))x \quad (x \to \infty).$$

Let us briefly sketch the derivation of the prime number theorem from Theorem 8.1. An easy calculation (Exercise 1) shows that

$$\zeta(s) = 1 + \frac{1}{s-1} - s\int_1^{\infty} \frac{\{x\}}{x^{s+1}}\,dx \tag{8.1}$$

in the region $\Re(s) > 1$. The integral in (8.1) is analytic for $\Re(s) > 0$, and so $\zeta(s)$ can be continued to a function which is analytic for $\Re(s) > 0$, except for a simple pole at $s = 1$ with residue 1. Since $\zeta(s)$ has no zeros for $\Re(s) > 1$ (since it can be written as an absolutely convergent Euler product there), *if* one can show that $\zeta(s)$ also has no zeros on $\Re(s) = 1$, then $-\zeta'(s)/\zeta(s)$ analytically continues to an open set containing $\Re(s) \geq 1$, apart from a simple pole at $s = 1$ with residue 1. Since

(8.2) $\quad \zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$, we obtain by logarithmic differentiation

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{\log p/p^s}{1 - 1/p^s} = \sum_p \left(\frac{\log p}{p^s} + \frac{\log p}{p^{2s}} + \cdots\right) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

and so the Wiener–Ikehara result shows that

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = (1 + o(1))x,$$

an assertion we have seen to be equivalent to the prime number theorem (Corollary 3.8). Conversely, if $\zeta(s)$ has any zeros on the line $\Re(s) = 1$, then it is relatively easy to prove directly that the prime number theorem cannot hold (see Exercise 4).

Thus the prime number theorem is, more or less, equivalent to an analytic assertion, namely the nonvanishing of $\zeta(s)$ on the line $\Re(s) = 1$. How could an elementary, real-variables proof establish an inherently complex-analytic fact such as this? It was this line of reasoning that led many prominent mathematicians, including Hardy, to the mistaken conclusion that such an elementary proof probably did not exist. When such a proof surfaced in 1948, it sent shockwaves throughout the world of mathematics.

1.1. Selberg's fundamental formula and its consequences. The key ingredient in the early elementary proofs of the prime number theorem is the *fundamental formula* (also called the *symmetry formula*) discovered by Selberg in March of 1948,

$$\theta(x)\log x + \sum_{p\le x}\theta\left(\frac{x}{p}\right)\log p = 2x\log x + O(x). \tag{8.3}$$

The proof, which appears below in §3, can be understood by a talented high-school student. But the implications of this formula are unexpectedly far-reaching. One striking consequence was noticed by Selberg early on (already by April of 1948). Chebyshev had shown (see Theorem 3.5) that

$$0 < a := \liminf \frac{\theta(x)}{x} \le \limsup \frac{\theta(x)}{x} =: A < \infty.$$

Using the symmetry formula, one can effect a simple proof that

$$A + a = 2,$$

a result not easily accessible to other elementary methods. Indeed, let $x \to \infty$ along a sequence of values on which $\theta(x) = (A + o(1))x$. Then for the left-hand side of (8.3) we have the estimate

$$\begin{aligned}\theta(x)\log x + \sum_{p\le x}\theta\left(\frac{x}{p}\right)\log p &\ge (A + o(1))x\log x \\ &\quad + \sum_{p\le x/\log x}\left((a+o(1))\frac{x}{p}\right)\log p = (A + a + o(1))x\log x,\end{aligned}$$

so that (8.3) implies $A+a \le 2$. If we begin instead with a sequence on which $\theta(x) = (a + o(1))x$, then a similar argument yields the reverse inequality $A + a \ge 2$. So $A + a = 2$.

In July, 1948, Turán gave a seminar at the Institute for Advanced Study on Selberg's elementary proof of Dirichlet's theorem on primes in progressions. In passing, he mentioned Selberg's fundamental formula. Erdős, who was in the audience, quickly realized that (8.3) could be used to give an elementary proof that the ratio p_{n+1}/p_n of consecutive primes tends to 1. Actually Erdős was able to deduce from Selberg's formula the stronger result that for any $\delta > 0$, there are $> c(\delta)x/\log x$ primes in the interval $(x, (1+\delta)x]$ (for sufficiently large x).

Erdős excitedly described his result and proof to Selberg. Two days later, on July 18, 1948, Selberg used Erdős's result to fashion the first elementary proof of the prime number theorem. Selberg's original argument and certain simplifications, due to Selberg and Erdős, are described in [**Erd49**].

1.2. Proving the prime number theorem from the symmetry formula. The proof of the prime number theorem given in this chapter is similar to the one ultimately published by Selberg in the *Annals of Mathematics* [**Sel49b**]. Define the remainder term $R(x)$ by the formula $\theta(x) = x + R(x)$, so that the prime number theorem is equivalent to the estimate $R(x) = o(x)$. From the fundamental formula (8.3) one easily deduces (cf. (8.25)) that

$$|R(x)| \log x \leq \sum_{p \leq x} |R(x/p)| \log p + O(x). \tag{8.4}$$

The prime number theorem says that $\sum_{p \leq x} \log p \sim x$, so that (8.4) should translate under partial summation to an estimate of the shape

$$|R(x)| \log x \lessapprox \sum_{n \leq x} |R(x/n)|.$$

It turns out that an estimate of this kind can be deduced starting from the fundamental formula without appeal to the prime number theorem, namely

$$|R(x)| \log x \leq \sum_{n \leq x} |R(x/n)| + O(x \log\log 3x). \tag{8.5}$$

(See (8.31).) This is more convenient to work with than (8.4), because in (8.5) the primes do not explicitly appear on the right-hand side.

Let us suppose that $\alpha := \limsup_{x\to\infty} |R(x)|/x$. Then $\alpha < \infty$, since $\theta(x) \ll x$, and the prime number theorem is the assertion that $\alpha = 0$. From (8.5), we find that

$$\frac{|R(x)|}{x} \lessapprox \frac{1}{x \log x} \sum_{n \leq x} |R(x/n)| \lessapprox \frac{1}{x \log x} \sum_{n \leq x} \alpha \frac{x}{n} \approx \alpha.$$

In fact, if one is a little careful here, one gets from this argument that

$$\limsup |R(x)|/x \leq \alpha. \tag{8.6}$$

Given how we defined α, the reader will be forgiven if she is not impressed by (8.6)! But there is reason to take heart: Granted, (8.6) doesn't tell us anything that we don't already know; in the terminology of H. N. Shapiro [**Sha83**], (8.5) is a *balanced* inequality, meaning that it returns whatever upper bound on $\limsup |R(x)|/x$ that it is fed. But if the right-hand side of (8.6) had been any smaller, we would have a contradiction to the choice of α. The plan of the proof is to show that unless $\alpha = 0$, one can indeed get an upper bound for $\limsup |R(x)|/x$ improving upon α. This contradiction forces us to have $\alpha = 0$, so that the prime number theorem follows.

Actually the means of producing such an improvement are a bit clearer if we part ways from Selberg and work with integrals instead of sums. (This seems to have been first noticed by Wright [**Wri52**]. The similar approach we take here is due to Nevanlinna [**Nev62**].) Rescale the remainder term $R(x)$ by introducing the function $r(x) := e^{-x}R(e^x)$. Then the prime number theorem amounts to the assertion that $r(x) = o(1)$. Instead of working with (8.5), we work with the corresponding integral inequality

$$|r(x)| \leq \int_0^x |r(t)|\,dt + o(1). \tag{8.7}$$

(See Theorem 8.10.) In parallel with the above, if we suppose $\limsup |r(x)| = \lambda$, then (8.7) returns to us to the same estimate. In order to forcibly unbalance the inequality (8.7), Nevanlinna examines what happens between the sign changes of $r(x)$, showing that if $\lambda > 0$, then over each interval between sign changes, $|r(x)|$ is quite often appreciably smaller than λ. This implies that (8.7) returns an improved estimate unless $\lambda = 0$. Thus $r(x) = o(1)$.

Notation. If A is a bounded subset of $\mathbf{R}$, the expression $\int_A f(t)\,dt$ should be read as a synonym for the (improper) Riemann integral $\int_{-\infty}^{\infty} \chi_A(t)f(t)\,dt$, where χ_A is the indicator function of A. The (Jordan) *measure* $\mu(A)$ of A is defined by $\mu(A) := \int_A 1\,dt$. When these expressions exist, their values agree with those from the Lebesgue theory of integration, but this chapter can be read without any knowledge of that subject.

When any of p, q, and r appear in the conditions of summation in this chapter, they always denote primes.

2. Chebyshev's theorems revisited

Recall the following three results from Chapter 3: First, $\pi(x) \ll x/\log x$. Second, $\pi(x) \gg x/\log x$. Third, *if* there is a constant C for which $\pi(x) = (C + o(1))x/\log x$, then necessarily $C = 1$. Our approach to the Selberg symmetry formula will be clearer if we first revisit these results of Chebyshev from a somewhat different perspective.

In Chapter 3, the identity $\sum_{d|n} \Lambda(d) = \log n$ played the key role. If we Möbius-invert this identity, we find that

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = \sum_{ab=n} \mu(a) \log b. \tag{8.8}$$

Thus

$$\begin{aligned} \psi(x) = \sum_{n \le x} \Lambda(n) &= \sum_{ab \le x} \mu(a) \log b \\ &= \sum_{a \le x} \mu(a) \left(\frac{x}{a} \log \frac{x}{a} - \frac{x}{a} + O\left(\log \frac{ex}{a} \right) \right), \end{aligned} \tag{8.9}$$

using Lemma 3.10 to estimate $\sum_{b \le x/a} \log b$. (Here e is the usual base of the natural logarithm. The factor of e is included in the error term so that the estimate is valid even when x/a is very close to 1.) This does not look like a promising approach to estimating $\psi(x)$, because at this point we have no way to estimate the sums of the Möbius function that appear. But as we will see shortly, this barrier is not at all insurmountable.

2.1. Another Möbius inversion formula.

Lemma 8.2. *Let f and g be any two complex-valued functions on $[1, \infty)$ satisfying the functional equation*

$$f(x) = \sum_{n \le x} g(x/n).$$

Then

$$g(x) = \sum_{n \le x} \mu(n) f(x/n).$$

Proof. If f and g obey the given relation, then

$$\begin{aligned} \sum_{n \le x} \mu(n) f(x/n) &= \sum_{n \le x} \mu(n) \sum_{m \le x/n} g\left(\frac{x}{mn}\right) \\ &= \sum_{mn \le x} \mu(n) g\left(\frac{x}{mn}\right) = \sum_{N \le x} g\left(\frac{x}{N}\right) \sum_{m|N} \mu(m) = g(x), \end{aligned}$$

since $\sum_{m|N} \mu(m)$ vanishes unless $N = 1$. □

Remark. If f and g are arithmetic functions, we may extend their domain to $[1, \infty)$ by declaring that they vanish at nonintegral arguments. Then Lemma 8.2 reduces to one direction of the usual Möbius inversion formula.

Corollary 8.3. *For $x \ge 1$,*

(i) $\displaystyle\sum_{n \le x} \frac{\mu(n)}{n} = O(1)$,

(ii) $\displaystyle\sum_{n\le x} \frac{\mu(n)}{n} \log \frac{x}{n} = O(1)$,

(iii) $\displaystyle\sum_{n\le x} \frac{\mu(n)}{n} \left(\log \frac{x}{n}\right)^2 = 2\log x + O(1)$.

Proof. We apply the inversion formula of Lemma 8.2 for three different choices of f and g. First, take g to be identically 1. Then $\sum_{n\le x} g(x/n) = \lfloor x \rfloor$, and so taking $f(x) := \lfloor x \rfloor$, Lemma 8.2 gives us that

$$1 = \sum_{n\le x} \mu(n) \lfloor x/n \rfloor = \sum_{n\le x} \mu(n) \left(\frac{x}{n} + O(1)\right),$$

from which (i) easily follows. Next, apply Lemma 8.2 with $g(x) := x$ and $f(x) := \sum_{n\le x} x/n$. Since $f(x) = x\log x + \gamma x + O(1)$, we find that

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

Rearranging this estimate and using (i) yields (ii). Lastly, take $g(x) := x\log x$ and $f(x) := \sum_{n\le x} g(x/n)$. Then

$$\begin{aligned} f(x) &= \sum_{n\le x} \frac{x}{n} \log \frac{x}{n} \\ &= x\log x \sum_{n\le x} \frac{1}{n} - x \sum_{n\le x} \frac{\log n}{n}. \end{aligned}$$

It is easy to show (by imitating the proof of Theorem 3.16) that

$$\sum_{n\le x} \frac{\log n}{n} = \frac{1}{2}(\log x)^2 + c + O\left(\frac{\log ex}{x}\right)$$

for some positive constant c. Thus

$$\begin{aligned} f(x) &= x\log x \left(\log x + \gamma + O\left(\frac{1}{x}\right)\right) - x\left(\frac{1}{2}(\log x)^2 + c + O\left(\frac{\log ex}{x}\right)\right) \\ &= \frac{1}{2}x(\log x)^2 + \gamma x\log x - cx + O(\log ex). \end{aligned}$$

So from Lemma 8.2 and (i) and (ii), we find that

$$\begin{aligned}
x\log x &= \sum_{n\le x}\mu(n)f(x/n)\\
&= \sum_{n\le x}\mu(n)\left(\frac{1}{2}\frac{x}{n}\left(\log\frac{x}{n}\right)^2+\gamma\frac{x}{n}\log\frac{x}{n}-c\frac{x}{n}+O\left(\log\frac{ex}{n}\right)\right)\\
&= \frac{1}{2}x\sum_{n\le x}\frac{\mu(n)}{n}\left(\log\frac{x}{n}\right)^2+O(x)+O\left(\sum_{n\le x}\log\frac{ex}{n}\right).
\end{aligned}$$

The final error term here is also $O(x)$ (cf. (4.19)), so that dividing by $\frac{1}{2}x$ gives us (iii). □

2.2. Another proof of Chebyshev's results. With Corollary 8.3 in hand, we can again pick up our new approach to Chebyshev's results. In (8.9), we found that

$$\psi(x) = x\sum_{a\le x}\frac{\mu(a)}{a}\log\frac{x}{a} - x\sum_{a\le x}\frac{\mu(a)}{a}+O\left(\sum_{a\le x}\log\frac{ex}{a}\right),$$

and Corollary 8.3 (parts (i) and (ii)) says that both of the sums here are $O(1)$. Since the O-term is $O(x)$, this yields another proof that $\psi(x)\ll x$, which is equivalent to the upper estimate $\pi(x)\ll x/\log x$.

What about the latter two results of Chebyshev? Suppose we multiply the identity (8.8) by $1/n$ before summing; then we obtain

$$\begin{aligned}
\sum_{n\le x}\frac{\Lambda(n)}{n} &= \sum_{ab\le x}\frac{\mu(a)}{ab}\log b = \sum_{a\le x}\frac{\mu(a)}{a}\sum_{b\le x/a}\frac{\log b}{b}\\
&= \sum_{a\le x}\frac{\mu(a)}{a}\left(\frac{1}{2}\left(\log\frac{x}{a}\right)^2+c+O\left(\frac{\log e(x/a)}{x/a}\right)\right)\\
&= \frac{1}{2}\sum_{a\le x}\frac{\mu(a)}{a}\left(\log\frac{x}{a}\right)^2+c\sum_{a\le x}\frac{\mu(a)}{a}+O(1).
\end{aligned}$$

Applying (i) and (iii) of Corollary 8.3, we arrive at the estimate

$$\sum_{n\le x}\frac{\Lambda(n)}{n}=\log x+O(1). \tag{8.10}$$

The estimate (8.10) by itself can be used to rederive all three of Chebyshev's results. For example, if $\psi(x)=(C+o(1))x$ for a constant C, then partial summation implies that $\sum_{n\le x}\Lambda(n)/n=(C+o(1))\log x$, so that we must have $C=1$. Also, from (8.10) we find that one can choose a constant B for which

$$\sum_{x<n\le Bx} \frac{\Lambda(n)}{n} > 1 \tag{8.11}$$

for all $x \ge 1$. But the left-hand side of (8.11) is bounded above by $\psi(Bx)/x$. Hence $\psi(Bx) > x$ and so $\psi(x) > x/B$ whenever $x \ge B$. This implies the lower estimate $\pi(x) \gg x/\log x$ as $x \to \infty$. A similar argument, omitted here, would show that (8.10) by itself also implies the upper estimate $\pi(x) \ll x/\log x$.

The upshot of our work in this section is that the Möbius sum estimates of Corollary 8.3 contain all the information about primes embodied in these three results of Chebyshev. As we shall establish in the remainder of this chapter, the estimates of Corollary 8.3 in fact already contain the prime number theorem.

3. Proof of Selberg's fundamental formula

3.1. An identity of arithmetic functions. Our jumping-off point for the proof of Selberg's fundamental formula is the following identity, whose (formal) verification requires only the familiar quotient rule from differential calculus:

$$\frac{\zeta''(s)}{\zeta(s)} = \left(\frac{\zeta'(s)}{\zeta(s)}\right)' + \left(\frac{\zeta'(s)}{\zeta(s)}\right)^2. \tag{8.12}$$

To get at the arithmetic content implicit in this identity, we expand both sides of (8.12) as Dirichlet series (in the region $\Re(s) > 1$) and then equate corresponding coefficients.

This is straightforward once we know how to multiply Dirichlet series. If f is an arithmetic function, let us agree that the *Dirichlet series associated to* f refers to the function F defined by

$$F(s) := \sum_{n=1}^{\infty} \frac{f(n)}{n^s},$$

with domain consisting of those complex numbers s for which the series converges. Suppose that F and G are the Dirichlet series associated with f and g, respectively, and that the series defining F and G converge absolutely at s. Then

$$\begin{aligned} F(s)G(s) &= \left(\sum_{n=1}^{\infty} \frac{f(n)}{n^s}\right)\left(\sum_{m=1}^{\infty} \frac{g(m)}{m^s}\right) \\ &= \sum_{n,m\in\mathbf{N}} \frac{f(n)g(m)}{(nm)^s} = \sum_{N=1}^{\infty} \frac{h(N)}{N^s}, \end{aligned} \tag{8.13}$$

where

$$h(N) := \sum_{nm=N} f(n)g(m). \tag{8.14}$$

The function h is referred to as the *Dirichlet convolution* of f and g.

We can now obtain Dirichlet series expansions of both sides of (8.12). Differentiating $\zeta(s)$ twice, term-by-term, shows that (for $\Re(s) > 1$)

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

The Euler product representation of $\zeta(s)$ implies that (for $\Re(s) > 1$)

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

So from (8.13) and (8.14), the left-hand side of (8.12) is represented by the Dirichlet series associated to the convolution of μ and $\log^2$. To handle the right-hand side, we recall from the introduction that for $\Re(s) > 1$,

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

From this we easily read off a Dirichlet series expansion of the right-hand side of (8.12); equating this expansion coefficient-by-coefficient with what we obtained for the left-hand side, we find that for each natural number n,

$$\sum_{ab=n} \mu(a)(\log b)^2 = \Lambda(n)\log n + \sum_{ab=n} \Lambda(a)\Lambda(b). \tag{8.15}$$

This identity of arithmetic functions will be used below, in combination with the results of Corollary 8.3, to prove Selberg's fundamental formula.

But is our derivation of (8.15) legal? By equating coefficients as above, we are implicitly assuming that (under reasonable hypotheses) the same function cannot have two Dirichlet series expansions. We could prove such a result; this is not hard (see, e.g., [**Apo76**, Theorem 11.3]), but it would take us somewhat afield. Alternatively, it is possible to develop a theory of formal Dirichlet series which allows one to justify all of the above manipulations without any recourse to analysis (see, e.g., [**Sha83**, Chapter 4]). Again, this would take us somewhat off point. Perhaps the simplest procedure is to view the above argument simply as a heuristic suggesting (8.15). We can then try to prove (8.15) directly.

This last plan is relatively painless to execute. The left-hand side of (8.15) can be rewritten as

$$\begin{aligned}\sum_{ab=n}\mu(a)\left(\sum_{d|b}\Lambda(d)\right)^2 &= \sum_{d_1|n,\ d_2|n}\Lambda(d_1)\Lambda(d_2)\sum_{\substack{ab=n\\ [d_1,d_2]|b}}\mu(a)\\ &= \sum_{\substack{d_1,d_2\\ [d_1,d_2]|n}}\Lambda(d_1)\Lambda(d_2)\sum_{a|\frac{n}{[d_1,d_2]}}\mu(a)\\ &= \sum_{\substack{d_1,d_2\\ [d_1,d_2]=n}}\Lambda(d_1)\Lambda(d_2), \qquad (8.16)\end{aligned}$$

where $[d_1, d_2]$ denotes the least common multiple of d_1 and d_2. But the von Mangoldt function Λ is supported on prime powers. So to prove (8.15), it is enough to check that (8.16) and the right-hand side of (8.15) agree when $\omega(n) = 1$ or 2, since in all other cases both expressions vanish. But if $n = p^e$, then both expressions equal $(2e-1)(\log p)^2$, while if $n = p_1^{e_1}p_2^{e_2}$ (with $p_1 \neq p_2$), then both come out to $2\log p_1 \log p_2$.

3.2. Estimating. Starting with the identity (8.15), we sum over $n \le x$ to find that

$$\sum_{ab\le x}\mu(a)(\log b)^2 = \sum_{n\le x}\Lambda(n)\log n + \sum_{ab\le x}\Lambda(a)\Lambda(b).$$

We would like an estimate for the left-hand side with an error term of at most $O(x)$. Write

(8.17)

$$\begin{aligned}\sum_{a\le x}\mu(a)\sum_{b\le x/a}(\log b)^2 &= \sum_{a\le x}\mu(a)\left(\int_1^{x/a}(\log t)^2\,dt + O\left(\left(\log\frac{x}{a}\right)^2\right)\right)\\ &= \sum_{a\le x}\mu(a)\left(\frac{x}{a}\left(\log\frac{x}{a}\right)^2 - 2\frac{x}{a}\log\frac{x}{a} + 2\frac{x}{a} - 2\right) + O\left(\sum_{a\le x}\left(\log\frac{x}{a}\right)^2\right).\end{aligned}$$

The error term here is

$$\ll \int_1^x\left(\log\frac{x}{t}\right)^2\,dt + O((\log x)^2) \ll x,$$

by a straightforward calculation. The main terms of (8.17) are estimated for us by Corollary 8.3, and collecting these estimates shows that

$$\sum_{n\le x}\Lambda(n)\log n + \sum_{ab\le x}\Lambda(a)\Lambda(b) = 2x\log x + O(x). \qquad (8.18)$$

Now

$$\begin{aligned}(8.19)\qquad \sum_{n\le x}\Lambda(n)\log n &= \int_1^x \log t\, d\psi(t)\\ &= \psi(x)\log x - \int_1^x \frac{\psi(t)}{t}\,dt = \psi(x)\log x + O(x).\end{aligned}$$

Inserting this estimate into (8.18), we have proved our first version of Selberg's fundamental formula: For $x \ge 1$,

$$(8.20)\qquad \psi(x)\log x + \sum_{ab\le x}\Lambda(a)\Lambda(b) = 2x\log x + O(x).$$

It is convenient later to have a result expressed just in terms of primes and not prime powers. If we replace ψ by θ on the left-hand side of (8.20), then we introduce an error of $\ll (\psi(x)-\theta(x))\log x \ll x^{1/2}(\log x)^2$ (by (3.4)), which is certainly $O(x)$. Moreover, replacing

$$\sum_{ab\le x}\Lambda(a)\Lambda(b) \quad\text{by}\quad \sum_{pq\le x}\log p\log q$$

results in an error which is

$$\begin{aligned}&\ll \sum_{\substack{p^a q^b\le x\\ a\ge 2\text{ or }b\ge 2}}\log p\log q \ll \sum_{\substack{p^a q^b\le x\\ a\ge 2}}\log p\log q \ll \sum_{\substack{p^a\le x\\ a\ge 2}}\log p\sum_{q^b\le x/p^a}\log q\\ &\qquad \ll \sum_{\substack{p^a\le x\\ a\ge 2}}(\log p)\psi(x/p^a) \ll x\sum_{\substack{p^a\le x\\ a\ge 2}}\frac{\log p}{p^a} \le x\sum_p \frac{\log p}{p^2-p} \ll x,\end{aligned}$$

and this again fits within our existing error term. Thus

$$(8.21)\qquad \theta(x)\log x + \sum_{pq\le x}\log p\log q = 2x\log x + O(x).$$

This is Selberg's formula in the shape (8.3) of the introduction, except that the second term in (8.3) appears as a sum over two variables here.

If we replace ψ by θ in the calculation which gave (8.19), we find that $\sum_{p\le x}(\log p)^2 = \theta(x)\log x + O(x)$; this gives yet another form of the symmetry formula, which will also be helpful in the sequel:

$$(8.22)\qquad \sum_{p\le x}(\log p)^2 + \sum_{pq\le x}\log p\log q = 2x\log x + O(x).$$

4. Removing the explicit appearance of primes

The goal of this section is to transition from the fundamental formula to the following inequality, where primes do not appear explicitly. Recall from the introduction that the remainder-term function $R(x)$ is defined by the relation $\theta(x) = x + R(x)$.

Theorem 8.4. *For $x \ge 1$, we have*

$$|R(x)| \log x \le \int_1^x |R(x/t)|\, dt + O(x \log\log 3x).$$

The proof of Theorem 8.4 is not difficult, but it is somewhat long. We begin with a few routine but technical estimates.

Lemma 8.5. *For $x \ge 1$, we have*

$$\sum_{pq \le x} \frac{\log p \log q}{pq} = \frac{1}{2}(\log x)^2 + O(\log x).$$

Proof. We have

$$\begin{aligned}
\sum_{pq \le x} \frac{\log p \log q}{pq} &= \sum_{p \le x} \frac{\log p}{p} \sum_{q \le x/p} \frac{\log q}{q} = \sum_{p \le x} \frac{\log p}{p} (\log x - \log p + O(1)) \\
&= \log x \sum_{p \le x} \frac{\log p}{p} - \sum_{p \le x} \frac{(\log p)^2}{p} + O\left(\sum_{p \le x} \frac{\log p}{p} \right) \\
&= \log x (\log x + O(1)) - \sum_{p \le x} \frac{(\log p)^2}{p} + O(\log x) \\
&= (\log x)^2 - \sum_{p \le x} \frac{(\log p)^2}{p} + O(\log x). \qquad (8.23)
\end{aligned}$$

To handle the remaining sum we use partial summation. With $A(x) = \sum_{p \le x} p^{-1} \log p$, we have

$$\begin{aligned}
\sum_{p \le x} \frac{(\log p)^2}{p} &= A(x) \log x - \int_1^x \frac{A(t)}{t}\, dt \\
&= (\log x + O(1)) \log x - \int_1^x \frac{\log t + O(1)}{t}\, dt \\
&= (\log x)^2 - \int_1^x \frac{\log t}{t}\, dt + O(\log x) = \frac{1}{2}(\log x)^2 + O(\log x);
\end{aligned}$$

inserting this estimate into (8.23) finishes the proof. □

Lemma 8.6. *For $x \ge 1$, we have*

$$\sum_{pq \le x} \frac{\log p \log q}{pq \log(pq)} = \log x + O(\log\log 3x).$$

Proof. Let $a_n := \sum_{pq=n} \frac{\log p \log q}{pq}$, and let $A(x) := \sum_{n \le x} a_n$. Then $A(x) = \frac{1}{2}(\log x)^2 + O(\log x)$ for $x \ge 1$, by Lemma 8.5. So for $x \ge 3$, we have

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

Replacing $\log\log x$ by $\log\log 3x$ ensures that the estimate is also valid for $1 \le x \le 3$. □

Lemma 8.7. *For $x \ge 1$, we have*

$$\sum_{p \le x} \log p + \sum_{pq \le x} \frac{\log p \log q}{\log(pq)} = 2x + O\left(\frac{x}{\log ex}\right).$$

Proof. With $A(x) := \sum_{p \le x} (\log p)^2 + \sum_{pq \le x} \log p \log q$, the fundamental formula in the shape (8.22) supplies us with the estimate $A(x) = 2x \log x + O(x)$. For $x \ge 2$, partial summation shows that

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

and this implies the stated result. □

Lemma 8.8. *For $x \ge 1$, we have*

$$\sum_{pq \le x} \log p \log q = 2x \log x - \sum_{pq \le x} \frac{\log p \log q}{\log(pq)} \theta(x/pq) + O(x \log\log 3x).$$

Proof. By Lemma 8.7 with x replaced by x/p, we have

$$\begin{aligned}\sum_{pq \le x} \log p \log q &= \sum_{p \le x} \log p \sum_{q \le x/p} \log q \\ &= \sum_{p \le x} \log p \left(2\frac{x}{p} - \sum_{qr \le x/p} \frac{\log q \log r}{\log(qr)} + O\left(\frac{x/p}{\log ex/p}\right)\right).\end{aligned}$$

This simplifies to

$$
\begin{aligned}
&2x\sum_{p\le x}\frac{\log p}{p}-\sum_{p\le x}\log p\sum_{qr\le x/p}\frac{\log q\log r}{\log(qr)}+O\left(x\sum_{p\le x}\frac{\log p}{p\left(1+\log\frac{x}{p}\right)}\right)\\
&=2x\log x+O(x)-\sum_{qr\le x}\frac{\log q\log r}{\log(qr)}\theta(x/qr)+O\left(x\sum_{p\le x}\frac{\log p}{p\left(1+\log\frac{x}{p}\right)}\right).
\end{aligned}
$$

To estimate the O-term, we partition those $p\le x$ according to the integer $j\ge 0$ for which $e^j\le x/p<e^{j+1}$; in this way we find

$$
\begin{aligned}
\sum_{p\le x}\frac{\log p}{p\left(1+\log\frac{x}{p}\right)}&\le\sum_{0\le j\le\log x}\frac{1}{1+j}\sum_{x/e^{j+1}\le p\le x/e^j}\frac{\log p}{p}\\
&\ll\sum_{0\le j\le\log x}\frac{1}{1+j}\ll\log\log 3x.
\end{aligned}
$$

Collecting these estimates and relabeling gives the statement of the lemma. $\square$

Lemma 8.9. *For $x\ge 1$, we have*

$$
\theta(x)\log x=\sum_{pq\le x}\frac{\log p\log q}{\log(pq)}\theta\left(\frac{x}{pq}\right)+O(x\log\log 3x).
$$

Proof. According to Selberg's fundamental formula in the form (8.21), we have

$$
\theta(x)\log x=-\sum_{pq\le x}\log p\log q+2x\log x+O(x).
$$

The result is obtained by replacing the right-hand sum with the estimate supplied for it by Lemma 8.8. $\square$

Proof of Theorem 8.4. We first re-express the fundamental formula as a relation involving $R(x)$. (Such a computation was alluded to in the introduction.) We have

$$
\begin{aligned}
R(x)\log x&=\theta(x)\log x-x\log x\\
&=\left(2x\log x-\sum_{pq\le x}\log p\log q\right)-x\log x+O(x)\\
&=x\log x-\sum_{p\le x}\theta(x/p)\log p+O(x).
\end{aligned}
$$

Replacing $\theta(x/p)$ with $x/p + R(x/p)$, we find that

$$\begin{aligned} R(x)\log x &= x\log x - \sum_{p\le x}\left(\frac{x}{p} + R\left(\frac{x}{p}\right)\right)\log p + O(x) \\ &= x\log x - x\sum_{p\le x}\frac{\log p}{p} - \sum_{p\le x} R\left(\frac{x}{p}\right)\log p + O(x) \\ &= -\sum_{p\le x} R\left(\frac{x}{p}\right)\log p + O(x), \end{aligned} \tag{8.24}$$

and so, in particular,

$$|R(x)|\log x \le \sum_{p\le x}|R(x/p)|\log p + O(x). \tag{8.25}$$

In order to deduce something like Theorem 8.4 from (8.25), we would like to have precise information about the partial sums of $\log p$. Of course such information is not available to us at this point! In order to work around this difficulty, we supplement (8.25) with another upper estimate on $|R(x)|\log x$: By Lemma 8.9,

$$\begin{aligned} R(x)\log x &= \theta(x)\log x - x\log x \\ &= x\sum_{pq\le x}\frac{\log p\log q}{pq\log(pq)} + \sum_{pq\le x}\frac{\log p\log q}{\log(pq)}R(x/pq) \\ &\qquad - x\log x + O(x\log\log 3x). \end{aligned}$$

Using Lemma 8.6 to estimate the first term here, we find that

$$R(x)\log x = \sum_{pq\le x}\frac{\log p\log q}{\log(pq)}R(x/pq) + O(x\log\log 3x), \tag{8.26}$$

and so in particular,

$$|R(x)|\log x \le \sum_{pq\le x}\frac{\log p\log q}{\log(pq)}|R(x/pq)| + O(x\log\log 3x). \tag{8.27}$$

Adding (8.25) to (8.27) shows that

$$\begin{aligned} &2|R(x)|\log x \\ &\quad\le \sum_{p\le x}\log p|R(x/p)| + \sum_{pq\le x}\frac{\log p\log q}{\log(pq)}|R(x/pq)| + O(x\log\log 3x). \end{aligned} \tag{8.28}$$

The contribution from the two sums on the right-hand side of (8.28) can be written in the form

$$\sum_{n\le x} a_n|R(x/n)|, \quad \text{where} \quad a_n := \sum_{p=n}\log p + \sum_{pq=n}\frac{\log p\log q}{\log(pq)}.$$

We are now in good shape, because we have an asymptotic formula for $A(x) := \sum_{n\le x} a_n$; indeed, $A(x) = 2x + O(x/\log ex)$ by Lemma 8.7.

By Abel summation,

$$\begin{aligned}\sum_{n\le x} a_n|R(x/n)| &= \sum_{n\le x} A(n)\left|R\left(\frac{x}{n}\right)\right| - \sum_{n\le x-1} A(n)\left|R\left(\frac{x}{n+1}\right)\right| \\ &= \sum_{n\le x} A(n)\left(\left|R\left(\frac{x}{n}\right)\right| - \left|R\left(\frac{x}{n+1}\right)\right|\right) + O(x). \end{aligned} \tag{8.29}$$

Substituting in our estimate for $A(x)$ and applying the triangle inequality, we deduce that the sum in (8.29) is

$$\begin{aligned} &2\sum_{n\le x} n\left(\left|R\left(\frac{x}{n}\right)\right| - \left|R\left(\frac{x}{n+1}\right)\right|\right) \\ &\qquad + O\left(\sum_{n\le x}\frac{n}{1+\log n}\left|R\left(\frac{x}{n}\right) - R\left(\frac{x}{n+1}\right)\right|\right). \end{aligned} \tag{8.30}$$

The main term of (8.30) telescopes to

$$2\sum_{n\le x}|R(x/n)| - 2\lfloor x\rfloor R\left(\frac{x}{\lfloor x\rfloor+1}\right) = 2\sum_{n\le x}|R(x/n)| + O(x).$$

To estimate the O-term in (8.30), we observe that

$$\left|R\left(\frac{x}{n}\right) - R\left(\frac{x}{n+1}\right)\right| < \theta\left(\frac{x}{n}\right) - \theta\left(\frac{x}{n+1}\right) + \frac{x}{n^2},$$

so that

$$\begin{aligned}&\sum_{n\le x}\frac{n}{1+\log n}\left|R\left(\frac{x}{n}\right) - R\left(\frac{x}{n+1}\right)\right| \\ &\qquad \ll \sum_{n\le x}\frac{n}{1+\log n}\left(\theta\left(\frac{x}{n}\right) - \theta\left(\frac{x}{n+1}\right)\right) + \sum_{n\le x}\frac{x}{n(1+\log n)}.\end{aligned}$$

The latter sum on the right-hand side is $\ll x\log\log 3x$, as we see by comparing with the corresponding integral. We rewrite the former sum, observing that

$$\begin{aligned}&\sum_{n\le x}\frac{n}{1+\log n}\left(\theta\left(\frac{x}{n}\right) - \theta\left(\frac{x}{n+1}\right)\right) \\ &\qquad = \theta(x) + \sum_{n\le x-1}\theta\left(\frac{x}{n+1}\right)\left(\frac{n+1}{1+\log(n+1)} - \frac{n}{1+\log n}\right).\end{aligned}$$

Now $\theta(x) \ll x$. Moreover, since $\theta(x/(n+1)) \ll x/n$ and

$$0 \leq \frac{n+1}{1+\log(n+1)} - \frac{n}{1+\log n} \leq \frac{1}{1+\log n},$$

it follows that

$$\sum_{n \leq x-1} \theta\left(\frac{x}{n+1}\right)\left(\frac{n+1}{1+\log(n+1)} - \frac{n}{1+\log n}\right) \\ \ll x \sum_{n \leq x-1} \frac{1}{n(1+\log n)} \ll x \log\log 3x.$$

Collecting all of our estimates shows that

$$|R(x)| \log x \leq \sum_{n \leq x} |R(x/n)| + O(x \log\log 3x). \tag{8.31}$$

In order to prove Theorem 8.4, we need to convert (8.31) into an inequality of integrals. To this end, observe that

$$\begin{aligned} \sum_{n \leq x} |R(x/n)| - \int_1^x |R(x/t)|\, dt &= \sum_{n \leq x} \int_n^{n+1} (|R(x/n)| - |R(x/t)|)\, dt + O(1) \\ &\leq \sum_{n \leq x} \int_n^{n+1} |R(x/n) - R(x/t)|\, dt + O(1). \end{aligned}$$

Now for $n \leq t \leq n+1$,

$$\begin{aligned} |R(x/n) - R(x/t)| &\leq \theta\left(\frac{x}{n}\right) - \theta\left(\frac{x}{t}\right) + \frac{x}{n} - \frac{x}{t} \\ &< \theta\left(\frac{x}{n}\right) - \theta\left(\frac{x}{n+1}\right) + \frac{x}{n^2}; \end{aligned}$$

thus

$$\begin{aligned} \sum_{n \leq x} |R(x/n)| - \int_1^x |R(x/t)|\, dt &\leq \sum_{n \leq x} \left(\theta\left(\frac{x}{n}\right) - \theta\left(\frac{x}{n+1}\right) + \frac{x}{n^2}\right) + O(1) \\ &= \theta(x) + x \sum_{n \leq x} \frac{1}{n^2} + O(1) \ll x. \end{aligned}$$

So by (8.31),

$$|R(x)| \log x \leq \int_1^x |R(x/t)|\, dt + O(x \log\log 3x),$$

which is Theorem 8.4. $\square$

5. Nevanlinna's finishing strategy

5.1. Rescaling the remainder term. Put

$$r(x) := e^{-x}R(e^x) = e^{-x}\theta(e^x) - 1.$$

Our first goal is to prove the following analogue of Theorem 8.4 for $r(x)$, which appeared already in the introduction:

Theorem 8.10. *As $x \to \infty$, we have*

$$|r(x)| \le \frac{1}{x}\int_0^x |r(t)|\,dt + o(1).$$

Proof. We change variables in Theorem 8.4, replacing t by x/t. This gives

$$|R(x)|\log x \le x\int_1^x \frac{|R(t)|}{t^2}\,dt + O(x\log\log 3x).$$

We now put $x = e^y$ and $t = e^u$ to find that

$$\begin{aligned}|R(e^y)| &\le \frac{1}{y}e^y\int_1^{e^y}\frac{|R(t)|}{t^2}\,dt + O\left(e^y\frac{\log ey}{y}\right)\\ &= e^y\frac{1}{y}\int_0^y |R(e^u)|e^{-u}\,du + O\left(e^y\frac{\log ey}{y}\right).\end{aligned}$$

Theorem 8.10 follows upon multiplying both sides by e^{-y}. □

The familiar estimate

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

also has a simple reformulation in terms of the function $r(x)$:

Lemma 8.11. *We have $\int_0^x r(t)\,dt = O(1)$ for all $x \ge 0$. As a consequence, there is a constant C with*

$$\left|\int_x^y r(t)\,dt\right| \le C$$

for every pair of nonnegative real numbers x and y.

Proof. We have

$$\begin{aligned}\int_0^x r(t)\,dt &= \int_0^x e^{-t}R(e^t)\,dt = \int_1^{e^x}\frac{R(u)}{u^2}\,du = \int_1^{e^x}\frac{\theta(u)-u}{u^2}\,du\\ &= \int_1^{e^x}\frac{\theta(u)}{u^2}\,du - \int_1^{e^x}\frac{du}{u} = \left(\sum_{p\le e^x}\frac{\log p}{p} - x\right) + O(1) = O(1).\end{aligned}$$ □

5.2. Unbalancing the inequality. We say that r *changes sign at the point* x if there is a deleted neighborhood of x on which r has opposite signs to the left and right of x. Since r is continuous except at the points of the set $\{\log p\}$ and is strictly decreasing between discontinuities, it is clear that r has only countably many sign changes on $(0, \infty)$. Enumerate them as

$$x_1 < x_2 < x_3 < \cdots .$$

(The ellipsis is not meant to imply that the sequence of x_i is infinite; in fact it is — this follows from the work Littlewood alluded to in the notes to Chapter 3 — but this is immaterial for our purposes.) Whenever x_i and x_{i+1} are defined, let I_i denote the half-open interval $[x_i, x_{i+1})$.

Lemma 8.12. *Suppose that x and x' are consecutive sign changes of r, and let $I = [x, x')$.*

(i) *If x is a sign change from negative to positive, then r is positive on all of I. In this case r is discontinuous at x.*

(ii) *If x is a sign change from positive to negative, then r is nonpositive on all of I. In this case r is continuous at x.*

Proof. Let x be a change of sign from negative to positive. Since r is strictly decreasing on each interval between discontinuities, it must be that $x = \log p_0$ for some prime p_0 and that $r(x) > 0$. Suppose first that there are no primes p with $x < \log p < x'$. Then the restriction of r to I is continuous and strictly decreasing. This implies that any zero of r on I would be a change of sign in r. Since x and x' are consecutive sign changes, r is nonvanishing on I. So by continuity, r is positive on all of I, as desired. If there are primes p with $x < \log p < x'$, then list the consecutive primes $p_1 < \cdots < p_k$ for which

$$x < \log p_1 < \log p_2 < \cdots < \log p_k < x'. \tag{8.32}$$

The argument just given shows that there are no zeros of r in $[x, \log p_1)$. So by continuity, r is positive on $[x, \log p_1)$. Since r has a positive jump at $\log p_1$, we have $r(\log p_1) > 0$, and repeating the argument shows that r is positive on $[\log p_1, \log p_2)$. Continuing in this way we eventually find that r is positive on all of I.

Now suppose that x is a sign change from positive to negative. Since r has positive jumps at its discontinuities, x must be a point of continuity of r, and so $r(x) = 0$. If there are no primes p with $x < \log p < x'$, then r is decreasing on I and so the conclusion of (ii) is obvious. Otherwise, let $p_1 < p_2 < \cdots < p_k$ be the primes satisfying (8.32). We have that r is negative on $(x, \log p_1)$, since $r(x) = 0$ and r is strictly decreasing on $[x, \log p_1)$. As a consequence, $r(\log p_1) \leq 0$, since otherwise $\log p_1$ would be a sign change between x and x'. Repeating this argument shows that

r is nonpositive on each of the intervals $[\log p_1, \log p_2)$, $[\log p_2, \log p_3)$, $\dots$, $[\log p_k, x')$; in fact, we find that r is negative at each point of I except possibly at x and the $\log p_i$. $\square$

Put $\lambda := \limsup |r(x)|$. The prime number theorem is the assertion that $\lambda = 0$. Suppose for the sake of contradiction that $\lambda > 0$, and fix a positive λ' with $\lambda' < \min\{1, \lambda\}$. For each i for which I_i is defined, put

$$I_i' := \{x \in I_i : |r(x)| \le \lambda'\}.$$

The rest of this section is devoted to proving the following lemma:

Lemma 8.13. *There is a constant $\kappa \in (0,1]$, depending only on λ', with $\mu(I_i') \ge \kappa\mu(I_i)$ whenever I_i is defined.*

Proof. Since r does not change sign on $I_i = [x_i, x_{i+1})$, Lemma 8.11 implies that

$$\lambda'(\mu(I_i) - \mu(I_i')) = \lambda'\mu(I_i \setminus I_i') \le \int_{I_i \setminus I_i'} |r(t)|\, dt \le \left| \int_{x_i}^{x_{i+1}} r(t)\, dt \right| \le C,$$

so that

$$\mu(I_i') \ge \mu(I_i) - C/\lambda' = \left(1 - \frac{C}{\lambda'\mu(I_i)}\right)\mu(I_i). \tag{8.33}$$

This is enough to give the conclusion of Lemma 8.13 in the case when $\mu(I_i)$ is large (e.g., if $\mu(I_i) \ge 2C/\lambda'$). We now derive another estimate which will allow us to draw the same conclusion when $\mu(I_i)$ is small.

Lemma 8.12 implies that whenever I_i is defined, precisely one of its endpoints is a point of continuity of r. Suppose it is the right endpoint x_{i+1}. Then $r(x_{i+1}) = 0$, so that $\theta(e^{x_{i+1}}) = e^{x_{i+1}}$. Since x_{i+1} represents a change from positive to negative, for each $x \in I_i$, we have

$$0 \le r(x) = e^{-x}\theta(e^x) - 1 \le e^{-x}\theta(e^{x_{i+1}}) - 1 = e^{x_{i+1}-x} - 1.$$

In particular, $|r(x)| \le \lambda'$ for all $x \in I_i$ close enough to x_{i+1}, e.g., all $x \in I_i$ which satisfy

$$x \ge x_{i+1} - \log(1 + \lambda').$$

(This situation is illustrated in Figure 1.) Similarly, if the left endpoint x_i of I_i is a point of continuity of r, then for each $x \in I_i$,

$$0 \ge r(x) = e^{-x}\theta(e^x) - 1 \ge e^{-x}\theta(e^{x_i}) - 1 = e^{x_i - x} - 1.$$

Thus $|r(x)| = -r(x) \le \lambda'$ for all $x \in I_i$ close enough to x_i, say $x \le x_i - \log(1 - \lambda')$. So certainly $|r(x)| \le \lambda'$ for those x in the even smaller range $x \le x_i + \log(1 + \lambda')$.

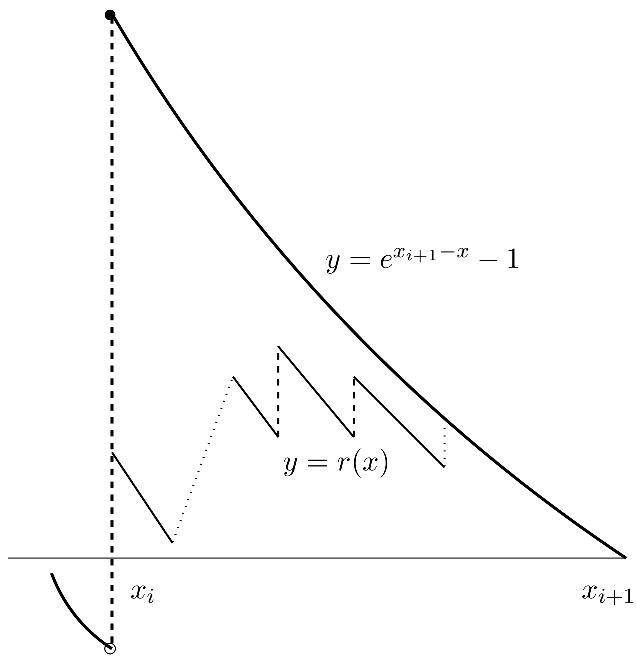

Figure 1. Rough sketch of $r(x)$ vs. $e^{x_{i+1}-x}-1$ between the sign changes x_i and x_{i+1}, in the case when x_{i+1} is a point of continuity. Based on [**Nev62**].

So regardless of which endpoint of I_i represents a point of continuity of r, we have

$$\begin{aligned} \mu(I_i') &\geq \min\{\log(1+\lambda'), \mu(I_i)\} \\ &= \min\{1, \log(1+\lambda')/\mu(I_i)\}\mu(I_i). \end{aligned} \tag{8.34}$$

Now (8.34) is the sought-after dual to (8.33); together these estimates imply Lemma 8.13. Indeed, set $C' := 2C/\lambda'$. If $\mu(I_i) \geq C'$, then we have $\mu(I_i') \geq \frac{1}{2}\mu(I_i)$ by (8.33). Otherwise

$$\mu(I_i') \geq \min\{1, \log(1+\lambda')/C'\}\mu(I_i)$$

by (8.34). So Lemma 8.13 follows with $\kappa = \min\{1/2, \log(1+\lambda')/C'\}$. $\square$

5.3. Endgame. We can now complete the proof of the prime number theorem in the form $r(x) = o(1)$. Let $\epsilon > 0$ be arbitrary but fixed. By the choice of λ, we can select a positive number x_ϵ with the property that for every $x > x_\epsilon$, we have

$$|r(x)| \leq \lambda + \epsilon.$$

Now let x be large, and let $x_\epsilon < x_m < x_{m+1} < \cdots < x_n \le x$ be a list of the sign changes of r in $(x_\epsilon, x]$. If there are no sign changes in this interval, then

$$\int_0^x |r(t)|\,dt \le \int_0^{x_\epsilon} |r(t)|\,dt + \left|\int_{x_\epsilon}^x r(t)\,dt\right| = O(1),$$

by Lemma 8.11. Otherwise, by Lemmas 8.11 and 8.13, we have

$$\begin{aligned}
\int_0^x |r(t)|\,dt &\le \int_0^{x_m} |r(t)|\,dt + \sum_{j=m}^{n-1} \int_{x_j}^{x_{j+1}} |r(t)|\,dt + \int_{x_n}^x |r(t)|\,dt \\
&\le \sum_{j=m}^{n-1} \big((\lambda+\epsilon)(\mu(I_j) - \mu(I_j')) + \lambda'\mu(I_j')\big) + O(1) \\
&= \sum_{j=m}^{n-1} \big((\lambda+\epsilon)\mu(I_j) + (\lambda' - \lambda - \epsilon)\mu(I_j')\big) + O(1) \\
&\le \sum_{j=m}^{n-1} \big((\lambda+\epsilon)\mu(I_j) + \kappa(\lambda' - \lambda - \epsilon)\mu(I_j)\big) + O(1) \\
&\le \big((\lambda+\epsilon) + \kappa(\lambda' - \lambda - \epsilon)\big)\, x + O(1).
\end{aligned}$$

Therefore, by Theorem 8.10,

$$\limsup_{x\to\infty} |r(x)| \le \limsup_{x\to\infty} \frac{1}{x}\int_0^x |r(t)|\,dt \le (\lambda+\epsilon) + \kappa(\lambda' - \lambda - \epsilon).$$

Since this holds for each $\epsilon > 0$, letting $\epsilon \downarrow 0$, it follows that

$$\limsup_{x\to\infty} |r(x)| \le \lambda + \kappa(\lambda' - \lambda) < \lambda,$$

contradicting that $\lambda = \limsup |r(x)|$. We have proved the prime number theorem!

Notes

In addition to the original papers of Nevanlinna and Selberg, our organization of the proof of the prime number theorem has been influenced heavily by Shapiro's treatment [**Sha83**, Chapter 10]. Our account of the early history of the elementary proof of the prime number theorem is based on the recollections of Selberg (as recorded in [**Gol04**], [**BS08**]) and Straus (see [**SG09**]).

The Wiener–Ikehara theorem and its application to the prime number theorem are described, for example, in [**Mur01**, Chapter 3]. The approach to the PNT via theorems of this type (so-called "Tauberian theorems") is discussed extensively in [**Kor02**, §§1-8]; see also [**Nar04**, §6.4]. Using little more than Cauchy's integral theorem, one can prove a weak version of the Wiener–Ikehara result that suffices for the proof of the prime number theorem. In this way one obtains the simplest known analytic proof. The groundwork for these developments was laid by Newman ([**New80**], see also [**New98**, Chapter VII]). Polished versions of this argument appear in papers of Korevaar [**Kor82**] and Zagier [**Zag97**], and a very readable account of the method is given in the text of Hlawka et al. [**HST91**].

The Erdős–Selberg method applies also to certain generalizations of the prime number theorem. In particular, their method leads to an elementary proof of the prime number theorem for arithmetic progressions (see [**Sel50**]) as well as a proof of the "prime ideal theorem" of algebraic number theory (see [**Sha49a**]). One version of the argument for arithmetic progressions is sketched in the exercises (cf. [**Nev64**, Kapitel III]).

Until 1980 all extant elementary proofs of the prime number theorem were variants on the Erdős–Selberg argument, at their core relying on some version of Selberg's fundamental formula. Since then Daboussi [**Dab84**] and Hildebrand [**Hil86**] have given proofs independent of the Erdős–Selberg work. Daboussi's argument is described at length in the engaging monograph of Tenenbaum & Mendès France [**TMF00**].

So far the elementary proofs of the prime number theorem have not had the dramatic effect on the number-theoretic landscape predicted by Hardy. Rather than overthrow the use of complex-variable methods, the existing elementary proofs have shown themselves to be comparatively inflexible, and if anything have underscored the utility of analytic techniques. For example, no elementary proof of the prime number theorem is known which gives an estimate for the error term of the same quality as what was obtained by de la Vallée-Poussin already in 1899 (cf. the notes to Chapter 3).

Exercises

Analytic exercises. This series of exercises requires familiarity with complex analysis. Unless otherwise specified, s denotes a complex variable and we write $s = \sigma + i\tau$, where $\sigma, \tau \in \mathbf{R}$.

1. Prove (8.1) by computing $\int t^{-s}\, dA(t)$ for $A(x) := \sum_{n \le x} 1$.
2. (Dirichlet–Dedekind [**Dir99**, §118]) Suppose that f is a complex-valued arithmetic function whose partial sums satisfy
$$\sum_{n \le x} f(n) = (R + o(1))x$$
for some complex number R (as $x \to \infty$). Prove that the Dirichlet series $F(s) := \sum_{n=1}^{\infty} f(n)/n^s$ converges to a continuous function on $(1, \infty)$ and that
$$\lim_{s \downarrow 1} (s-1)F(s) = R.$$
(Theorem 8.1 may be viewed as a sort of converse of this result.)

† 3. (Chebyshev [**Che51**]; cf. [**Nar04**, pp. 100–102]) In Chapter 3 we proved the theorem of Chebyshev (Theorem 3.4) that if $\frac{\pi(x)}{x/\log x}$ tends to a limit as $x \to \infty$, then that limit is necessarily 1. Actually Chebyshev proved a stronger result: If we put $E(x) := \pi(x) - \mathrm{Li}(x)$, then for each natural number k,
$$\limsup_{x\to\infty} \frac{E(x)}{x/(\log x)^k} \ge 0 \quad \text{and} \quad \liminf_{x\to\infty} \frac{E(x)}{x/(\log x)^k} \le 0. \tag{8.35}$$
In this exercise we sketch a proof of this result.

Let k be a natural number. For real $s > 1$, put $P(s) := \sum_p p^{-s}$.

(a) Show that $P(s) - \log \frac{1}{s-1}$ has an analytic continuation to an open subset of the complex plane containing all real $s \ge 1$. Deduce that if we put
$$F(s) := (-1)^k (P^{(k)}(s) + \zeta^{(k-1)}(s)),$$
then $F(s)$ remains bounded as s tends to 1 from above.

(b) Show that for $s > 1$, we have $F(s) = \sum_p \frac{(\log p)^k}{p^s} - \sum_{n=2}^{\infty} \frac{(\log n)^{k-1}}{n^s}$.

(c) Show that for $s > 1$,
$$F(s) = -\int_2^{\infty} E(t)\, \frac{d}{dt}\left(\frac{(\log t)^k}{t^s}\right) dt + O_k(1).$$

(d) Deduce (8.35) from (a) and (c). Check that when $k = 1$, these inequalities imply Theorem 3.4.

Remark. It follows from Exercise 3.8 (which assumes the prime number theorem with a reasonable error term) that both limits in (8.35) vanish for each k.

4. Define $Z(s) := -\frac{\zeta'(s)}{\zeta(s)}$. From (8.2) we know that

$$Z(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \quad (\sigma > 1).$$

(a) Prove that for $\sigma > 1$,

$$Z(s) = \frac{s}{s-1} + s \int_1^{\infty} (\psi(t) - t) \frac{dt}{t^{s+1}}.$$

(b) Assuming the prime number theorem in the form $\psi(x) \sim x$, show that the integral in (a) is $o(1/(\sigma - 1))$, as $\sigma \downarrow 1$, uniformly in τ. Conclude that for fixed $\tau \neq 0$, one has

$$\lim_{\sigma \downarrow 1} (\sigma - 1)|Z(\sigma + i\tau)| = 0.$$

(c) On the other hand, show that if $\zeta(s)$ has a zero of order $m \geq 0$ at $1 + i\tau$ (so that necessarily $\tau \neq 0$), then

$$\lim_{\sigma \downarrow 1} (\sigma - 1) Z(\sigma + i\tau) = -m.$$

Combining the results of (b) and (c), deduce that if the prime number theorem is true, then $\zeta(s)$ has no zeros on the line $\sigma = 1$.

5. Let $M(x) := \sum_{n \leq x} \mu(n)$, where μ is the Möbius function.

(a) Prove that if $M(x)/x$ tends to a limit, then that limit must be zero. *Hint:* Use Corollary 8.3(i) or the result of Exercise 2.

(b) Assuming that $\zeta(s)$ has no zeros on the line $\sigma = 1$, deduce from the Wiener–Ikehara Theorem (Theorem 8.1) that $M(x)/x$ does, in fact, tend to zero.

(c) Suppose, conversely, that $M(x)/x$ tends to zero. Prove that $\zeta(s)$ has no zeros on the line $\Re(s) = 1$. (Cf. Exercise 4.)

The estimate $M(x) = o(x)$ can be interpreted probabilistically: If a squarefree number n is chosen at random, it is equally likely to have an even number of prime factors as an odd number of prime factors.

Remark. From (b) and (c), we see that the estimate $M(x) = o(x)$ is in some sense equivalent to the prime number theorem, since both amount to the nonexistence of zeros of $\zeta(s)$ on the line $\sigma = 1$. For an elementary proof of this equivalence, see [**Apo76**, §4.9].

† 6. We outline a proof, taken from [**Tit86**, §3.2], that $\zeta(s)$ is nonvanishing on the line $\sigma = 1$. We assume the result of Exercise 1, so that $\zeta(s)$ is

known to be analytic for $\sigma > 0$ except for a simple pole at $s = 1$ with residue 1. As before we let $Z(s) = -\frac{\zeta'(s)}{\zeta(s)}$.

(a) Suppose that $\zeta(s)$ has a zero at $s_0 = 1 + i\tau_0$, where necessarily $\tau_0 \neq 0$. Prove that s_0 is necessarily simple. *Hint:* If $\zeta(s)$ has a zero of order k at s_0, then $Z(s)$ has a simple pole at s_0 with residue $-k$; however,

$$\left|\frac{\zeta'(\sigma + i\tau_0)}{\zeta(\sigma + i\tau_0)}\right| \leq \left|\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^{\sigma + i\tau_0}}\right| \leq \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^{\sigma}} \sim \frac{1}{\sigma - 1} \quad \text{as } \sigma \downarrow 1.$$

(b) Show that

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)\cos(\tau_0 \log n)}{n^{\sigma}} \sim -\frac{1}{\sigma - 1} \quad \text{as } \sigma \downarrow 1.$$

(c) By the Cauchy–Schwarz inequality, we now have

$$\begin{aligned} \frac{1}{(\sigma - 1)^2} &\sim \left(\sum_{n=1}^{\infty} \frac{\Lambda(n)\cos(\tau_0 \log n)}{n^{\sigma}}\right)^2 \\ &\leq \left(\sum_{n=1}^{\infty} \frac{\Lambda(n)\cos^2(\tau_0 \log n)}{n^{\sigma}}\right)\left(\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^{\sigma}}\right). \end{aligned}$$

Rewriting $\cos^2(\tau_0 \log n) = \frac{1}{2}(1 + \cos(2\tau_0 \log n))$ and using that $Z(s)$ has a simple pole at $s = 1$ with residue 1, prove that

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)\cos(2\tau_0 \log n)}{n^{\sigma}} \geq (1 + o(1))\frac{1}{\sigma - 1} \quad \text{as } \sigma \downarrow 1.$$

(d) Show that the estimate of (c) contradicts the regularity of $\zeta(s)$ at the point $1 + 2i\tau_0$.

In Exercises 7–10, we look a bit deeper at how an elementary proof of the prime number theorem is possible given its equivalence to the nonvanishing of $\zeta(s)$ on the line $\sigma = 1$. This paradox was addressed by Ingham in his expert review [**Ing48**] of the Erdős–Selberg papers. Following Ingham, suppose that F is any function of a complex variable with the following three properties:

(i) F is represented by the Dirichlet series $\sum_{n=1}^{\infty} a_n/n^s$ in the region $\sigma > 1$, where each a_n is real.

(ii) F is analytic on the closed half-plane $\sigma \geq 1$, except possibly for simple poles on the line $\sigma = 1$.

(iii) For $\sigma > 1$, we have $-F'(s) + F(s)^2 = \sum_{n=1}^{\infty} b_n/n^s$, where $B(x) := \sum_{n \leq x} b_n$ satisfies $B(x) \sim 2x \log x$ as $x \to \infty$.

The reader should have in the back of her mind the special case $F(s) = -\frac{\zeta'(s)}{\zeta(s)}$. Then (i) holds with $a_n = \Lambda(n)$, and (iii) is a consequence of Selberg's fundamental formula in the shape (8.18).

7. Let $G(s) := -F'(s) + F(s)^2 + 2\zeta'(s)$. Show that G is represented by a Dirichlet series $\sum c_n/n^s$ where $\sum_{n\le x} c_n = o(x\log x)$. Deduce that G has no poles of order ≥ 2 on $\sigma = 1$, and hence that $-F'(s) + F(s)^2$ has no poles of order ≥ 2 on $\sigma = 1$ except possibly at $s = 1$.
8. Deduce from Exercise 7 that if F has a pole at $1 + i\tau_0$ with $\tau_0 \neq 0$, then its residue R there satisfies $R + R^2 = 0$. Conclude that $R = -1$.
9. We now describe how to construct a function F possessing properties (i)–(iii) which nevertheless has a pole on the line $\sigma = 1$ other than $s = 1$.

   (a) For each fixed real number $\alpha \neq 0$, show that
   $$\sum_{n\le x} n^{i\alpha} = \frac{1}{1+i\alpha}x^{1+i\alpha} + o(x) \quad \text{while} \quad \sum_{n\le x} \frac{1}{n} n^{i\alpha} = o(\log x).$$
   (b) Show that $F(s) := \zeta(s) - \zeta(s - i\alpha) - \zeta(s + i\alpha)$ possesses each of Ingham's properties (i)–(iii). Of course (i) and (ii) are immediate; establishing (iii) is the difficult component and where the estimates of (a) come into play.
   (c) Show that F has a pole at $s = 1 + i\alpha$.

Exercise 9 shows that (i)–(iii) are not enough to rule out poles of F of the form $1 + i\tau_0$, with $\tau_0 \neq 0$. Quoting Ingham (ibid.),

> this may be taken as a reason why it is possible to give an elementary proof of [Selberg's fundamental formula] without becoming involved in the question of the existence of zeros of ζ on $\sigma = 1$.

10. Now suppose that in addition to (i)–(iii) we require that each $a_n \ge 0$, i.e., that F is represented by a Dirichlet series with nonnegative coefficients. (This is *not* satisfied for the F of Exercise 9.) If F has a pole at $1 + i\tau_0$ with $\tau_0 \neq 0$, then by assumption (ii) and Exercise 8, this pole is simple with residue -1. By imitating the argument of Exercise 6, show that this forces F to have a pole of residue ≥ 1 at $1 + 2i\tau_0$, contradicting Exercise 8.

Taking $F(s) = -\frac{\zeta'(s)}{\zeta(s)}$ in Exercise 10, we see that the nonvanishing of $\zeta(s)$ on $\sigma = 1$ is a consequence of Selberg's fundamental formula paired with the nonnegativity of $\Lambda(n)$.

Primes in progressions. Recall that $\pi(x; m, a)$ denotes the number of primes $p \le x$ with $p \equiv a \pmod{m}$. The next series of exercises leads the reader through a proof of the following fundamental equidistribution result, already alluded to in Chapter 1.

★ **Theorem 8.14** (The prime number theorem for arithmetic progressions). *Suppose that a and m are relatively prime integers with $m > 0$. Then*

$$\pi(x; m, a) \sim \frac{1}{\varphi(m)} \frac{x}{\log x} \quad (x \to \infty).$$

The steps in the proof of Theorem 8.14 correspond closely to those in the proof of the prime number theorem (which is the case $m = 1$ of Theorem 8.14). However, in place of Mertens' estimate for the partial sums of $\log p/p$, we make frequent use of the deeper result that for $(a, m) = 1$,

$$\sum_{\substack{p \le x \\ p \equiv a \bmod m}} \frac{\log p}{p} = \frac{1}{\varphi(m)} \log x + O(1), \tag{8.36}$$

which we established elementarily in the course of proving Dirichlet's theorem. In (8.36) and the exercises below, all the implied constants are allowed to depend on m.

Define

$$\theta(x; m, a) := \sum_{\substack{p \le x \\ p \equiv a \pmod{m}}} \log p.$$

11. Let a and m be coprime integers with $m > 0$. Prove that as $x \to \infty$,

$$\pi(x; m, a) \sim \frac{1}{\varphi(m)} \frac{x}{\log x} \Longleftrightarrow \theta(x; m, a) \sim \frac{x}{\varphi(m)}.$$

It is in this latter form that Theorem 8.14 will be established.

We begin the demonstration of Theorem 8.14 by proving an analogue of Selberg's fundamental formula:

★ **Theorem 8.15** (Selberg's formula for arithmetic progressions). *Let a and m be coprime integers with $m > 0$. Then for $x \ge 1$,*

$$\sum_{\substack{p \le x \\ p \equiv a \pmod{m}}} (\log p)^2 + \sum_{\substack{pq \le x \\ pq \equiv a \pmod{m}}} \log p \log q = \frac{2}{\varphi(m)} x \log x + O(x).$$

† 12. (a) Fix a coprime residue class $a \bmod m$. By summing both sides of the identity (8.15) over the progression $a \bmod m$, show that

$$\sum_{\substack{n\le x\\ n\equiv a \ (\mathrm{mod}\ m)}} \Lambda(n)\log n + \sum_{\substack{df\le x\\ df\equiv a \ (\mathrm{mod}\ m)}} \Lambda(d)\Lambda(f) \tag{8.37}$$
$$= \sum_{\substack{d\le x\\ (d,m)=1}} \mu(d) \sum_{\substack{f\le x/d\\ f\equiv a\bar{d} \ (\mathrm{mod}\ m)}} (\log f)^2$$
$$= \frac{1}{m} \sum_{\substack{df\le x\\ (df,m)=1}} \mu(d)(\log f)^2 + O(x),$$

where $\bar{d}$ denotes a solution of $d\bar{d} \equiv 1 \pmod{m}$.

(b) Summing over all invertible residue classes $a \bmod m$, deduce that

$$\sum_{n\le x}\Lambda(n)\log n + \sum_{df\le x}\Lambda(d)\Lambda(f) = \frac{\varphi(m)}{m} \sum_{\substack{df\le x\\ (df,m)=1}} \mu(d)(\log f)^2 + O(x).$$

The left-hand side here coincides with that of Selberg's original fundamental formula (in the form (8.18)). Deduce from that formula and (8.37) that

$$\sum_{\substack{n\le x\\ n\equiv a \ (\mathrm{mod}\ m)}} \Lambda(n)\log n + \sum_{\substack{df\le x\\ df\equiv a \ (\mathrm{mod}\ m)}} \Lambda(d)\Lambda(f) = \frac{2}{\varphi(m)} x\log x + O(x). \tag{8.38}$$

(c) Deduce Theorem 8.15 from (8.38) by showing that the contribution in (8.38) from proper prime powers is $O(x)$.

Define the remainder term $R(x; m, a)$ by

$$R(x; m, a) := \theta(x; m, a) - \frac{x}{\varphi(m)}.$$

Theorem 8.14 amounts to the assertion that $R(x; m, a) = o(x)$ whenever a and m are coprime integers with $m > 0$.

To proceed we need the following analogue of Theorem 8.4: If a and m are coprime integers with $m > 0$, then for $x \ge 1$,

$$|R(x; m, a)|\log x \le \frac{1}{\varphi(m)} \sum_{\substack{b \bmod m\\ (b,m)=1}} \int_1^x |R(x/t; m, b)|\, dt + O(x\log\log 3x). \tag{8.39}$$

† 13. Here is an outline of the proof of (8.39). Let a and m be coprime integers with $m > 0$. Prove that each of the following estimates holds for all $x \ge 1$:

(a) (Cf. Lemma 8.5)

$$\sum_{\substack{pq\le x\\ pq\equiv a \pmod m}} \frac{\log p\log q}{pq} = \frac{1}{2\varphi(m)}(\log x)^2 + O(\log x).$$

(b) (Cf. Lemma 8.6)

$$\sum_{\substack{pq\le x\\ pq\equiv a \pmod m}} \frac{\log p\log q}{pq\log(pq)} = \frac{1}{\varphi(m)}\log x + O(\log\log 3x).$$

(c) (Cf. Lemma 8.7)

$$\sum_{\substack{p\le x\\ p\equiv a \pmod m}} \log p + \sum_{\substack{pq\le x\\ pq\equiv a \pmod m}} \frac{\log p\log q}{\log(pq)} = \frac{2}{\varphi(m)}x + O\left(\frac{x}{\log ex}\right).$$

(d) (Cf. Lemma 8.8)

$$\sum_{\substack{pq\le x\\ pq\equiv a \pmod m}} \log p\log q = \frac{2}{\varphi(m)}x\log x - \sum_{\substack{pq\le x\\ (pq,m)=1}} \frac{\log p\log q}{\log(pq)}\theta(x/pq; m, a\overline{pq}) + O(x\log\log 3x),$$

where $\overline{pq}$ is an inverse of pq modulo m.

(e) (Cf. Lemma 8.9)

$$\theta(x;m,a)\log x = \sum_{\substack{pq\le x\\ pq\equiv a \pmod m}} \frac{\log p\log q}{\log(pq)}\theta(x/pq; m, a\overline{pq}) + O(x\log\log 3x).$$

(f) (Cf. (8.24))

$$R(x;m,a)\log x = -\sum_{\substack{p\le x\\ p\nmid m}} R(x/p; m, a\overline{p})\log p + O(x).$$

(g) (Cf. (8.26))

$$R(x;m,a)\log x = \sum_{\substack{pq\le x\\ (pq,m)=1}} \frac{\log p\log q}{\log(pq)} R(x/pq; m, a\overline{pq}) + O(x\log\log 3x).$$

(h) Suppose that b is coprime to m. With $\bar{b}$ denoting an inverse of b modulo p, show that

$$\sum_{\substack{p\le x\\ p\equiv a\bar{b} \pmod{m}}} |R(x/p;m,b)|\log p + \sum_{\substack{pq\le x\\ pq\equiv a\bar{b} \pmod{m}}} \frac{\log p\log q}{\log(pq)}|R(x/pq;m,b)|$$
$$= \frac{2}{\varphi(m)}\sum_{n\le x}|R(x/n;m,b)| + O(x\log\log 3x).$$

(i) Combining the results of (f)–(h), prove that

$$|R(x;m,a)|\log x \le \frac{1}{\varphi(m)}\sum_{\substack{b \bmod m\\ (b,m)=1}}\sum_{n\le x}|R(x/n;m,b)|+O(x\log\log 3x). \tag{8.40}$$

(j) By replacing the inner sum in (8.40) by the corresponding integral, prove the original claim (8.39).

† 14. We can now complete the proof of the prime number theorem for arithmetic progressions (Theorem 8.14). Define a rescaled remainder term function $r(x;m,a)$ by

$$\begin{aligned} r(x;m,a) &:= e^{-x}R(e^x;m,a)\\ &= e^{-x}\theta(e^x;m,a) - \frac{1}{\varphi(m)}. \end{aligned}$$

Fix a positive integer m. The prime number theorem for primes in residue classes modulo m is the assertion that $r(x;m,a)=o(1)$ whenever $\gcd(a,m)=1$. Put

$$\lambda := \max_{(a,m)=1}\limsup |r(x;m,a)|.$$

Assume for the sake of contradiction that $\lambda>0$.

(a) (Cf. Theorem 8.10) Show that if a is coprime to m, then as $x\to\infty$,

$$|r(x;m,a)| \le \frac{1}{\varphi(m)}\sum_{\substack{b \bmod m\\ (b,m)=1}}\frac{1}{x}\int_0^x |r(t;m,b)|\,dt + o(1).$$

(b) (Cf. Lemma 8.11) Prove that if a is coprime to m, then

$$\left|\int_x^y r(t;m,a)\,dt\right| \le C$$

for all nonnegative real numbers x and y, where C is a constant depending only on m.

(c) By mimicking the arguments of §§5.2–5.3, show that whenever b is coprime to m,

$$\limsup_{x\to\infty}\frac{1}{x}\int_0^x |r(t;m,b)|\,dt < \lambda.$$

Deduce from part (a) that whenever a is coprime to m,

$$\limsup |r(x; m, a)| < \lambda.$$

Since this holds for each a coprime to m, this contradicts the definition of λ. Hence, $\lambda = 0$.

This completes the proof of Theorem 8.14.

Miscellany.

† 15. Let $\beta(n) = \sum_{p \mid n} p$ be the sum of the distinct prime divisors of n and let $p(n)$ and $P(n)$ denote the smallest and largest prime factors of n. Show that as $x \to \infty$,

$$\sum_{n \le x} \beta(n) \sim \sum_{2 \le n \le x} P(n) \sim \frac{\zeta(2)}{2} \frac{x^2}{\log x}, \text{ and}$$

$$\sum_{p \le x} p \sim \sum_{2 \le n \le x} p(n) \sim \frac{1}{2} \frac{x^2}{\log x}.$$

The results for $\beta(n)$ and $p(n)$ here are due to Kalecki [**Kal64**]; a sharper form of the $P(n)$ estimate is due to Brouwer [**Bro74**].

16. (Moser [**Mos63**]; see also [**Guy04**, C2]) Let $r(n)$ be the number of ways of writing the natural number n as a sum of consecutive primes. For example, $r(83) = 3$, since 83 has the three representations

$$11 + 13 + 17 + 19 + 23, \quad 23 + 29 + 31, \quad 83.$$

Show that $r(n)$ has mean value $\log 2$; in other words, prove that as $x \to \infty$,

$$\frac{1}{x} \sum_{n \le x} r(n) \to \log 2.$$

Hint: For each natural number k, let $r(n, k)$ be the number of ways of writing n as a sum of k consecutive primes (so $r(n, k)$ is 0 or 1 for each n). Begin by showing that $\pi(x/k) - (k-1) \le \sum_{n \le x} r(n, k) \le \pi(x/k)$.

17. (Cf. Mirsky [**Mir49**]) Let $\pi^*(x)$ denote the number of primes $p \le x$ for which $p - 1$ is squarefree. In this exercise we outline a proof, based on the prime number theorem for arithmetic progressions (Theorem 8.14) and the Brun–Titchmarsh inequality (Theorem 7.2), that as $x \to \infty$,

$$\pi^*(x) \sim A \frac{x}{\log x} \quad \text{where} \quad A = \prod_q \left(1 - \frac{1}{q(q-1)}\right).$$

(Here, as usual, q denotes a prime variable.) In particular, $p - 1$ is squarefree for a positive proportion of primes p. The constant of proportionality A is known as *Artin's constant* and $A \approx 0.3739558$.

(a) Let $z > 0$ be arbitrary but fixed. Using Theorem 8.14 and the principle of inclusion-exclusion, show that as $x \to \infty$,

$$\sum_{\substack{p \le x \\ q^2 | p-1 \Rightarrow q > z}} 1 \sim A_z \frac{x}{\log x}, \quad \text{where} \quad A_z = \prod_{q \le z} \left(1 - \frac{1}{q(q-1)}\right).$$

(b) The sum in (a) majorizes $\pi^*(x)$, since it includes every prime p for which $p - 1$ is squarefree. On the other hand, if p is counted by that sum but $p - 1$ is not squarefree, then $p - 1$ is divisible by q^2 for some prime $q > z$. It follows that

$$\sum_{\substack{p \le x \\ q^2 | p-1 \Rightarrow q > z}} 1 \le \pi^*(x) + \sum_{q > z} \pi(x; q^2, 1).$$

Using the Brun–Titchmarsh inequality (Theorem 7.2), show that the terms of the right-hand sum corresponding to $q \in (z, (\log x)^2]$ contribute $\ll x/(z \log x)$. Using the trivial bound $\pi(x; q^2, 1) \le x/q^2$, show that those $q > (\log x)^2$ contribute $\ll x/(\log x)^2$.

(c) Deduce from (a) and (b) that for each fixed z,

$$\limsup_{x \to \infty} \frac{\pi^*(x)}{x/\log x} \le A_z \quad \text{while} \quad \liminf_{x \to \infty} \frac{\pi^*(x)}{x/\log x} \ge A_z - O(1/z).$$

Complete the proof by letting $z \to \infty$.

Chapter 9

Perfect Numbers and their Friends

Among all the problems which we are used to dealing with in Mathematics, none for certain, are judged by the majority of modern mathematicians, to be more sterile or more detached from all possible use, than those which concern speculation about the nature of numbers and research into their divisors. In this judgement the mathematicians of today differ greatly from the Ancients, who were accustomed to accord a great value to these speculations... For as well as it seeming to them that investigation of the truth was in itself laudable and worthy of human consciousness, they judged also, rightly, that by these researches the art of investigation could be extended, and that the faculties of the mind would become better able to deal with important questions. And in this opinion they were not deceived, for we have manifest proof of this in the considerable developments that have enriched Analysis since that epoch; in fact it appears entirely to be the case that science would never have achieved such a degree of perfection had the Ancients not put so much zeal into developing questions of this type, which the greater part of modern mathematicians despise so much on account of their sterility. – L. Euler (see [**CS97**])

1. Introduction and overview

For each natural number n, let $\sigma(n)$ be the sum of all the (positive) divisors of n, and let $s(n)$ be the sum of all the proper divisors. Here a *proper divisor* of n is a divisor of n other than n itself, so that $s(n) = \sigma(n) - n$. The ancient Greeks partitioned the natural numbers according to whether $s(n) < n$, $s(n) = n$, or $s(n) > n$ (equivalently, $\sigma(n) < 2n$, $\sigma(n) = 2n$, or $\sigma(n) > 2n$). Numbers n of the first kind were termed *deficient*, numbers of the third kind *abundant*, and numbers of the second kind *perfect*.

Fast-forwarding to modern times, it is routine to verify by computer that among the first million natural numbers, 247,545 are abundant, 752,451 are deficient, and only 4 are perfect. This simple computation raises a number of questions: It seems that both the abundant and deficient numbers are relatively common. Do both of these sets constitute a well-defined proportion of the natural numbers? More precisely, is it true that the set of abundant numbers (or deficient numbers) possesses an asymptotic density? Given that we found just four perfect numbers up to 10^6, should we expect infinitely many as we head out to infinity? The first four perfect numbers are

$$6 = 2 \cdot 3, \quad 28 = 2^2 \cdot 7, \quad 496 = 2^4 \cdot 31, \quad \text{and} \quad 8128 = 2^6 \cdot 127.$$

Are all perfect numbers even? Do they all only have two prime factors? The astute reader may have noticed that in our examples, all four factorizations have the form $2^k(2^{k+1} - 1)$; does this continue?

1.1. Even perfect numbers. Let us turn to what is known about these questions. Suppose first that $2^{k+1} - 1$ is a prime number. It was known already to Euclid that in this case the number $n := 2^k(2^{k+1} - 1)$ is perfect, and this can be verified very quickly using the multiplicativity of the σ-function:

$$\begin{aligned}\sigma(n) &= \sigma(2^k)\sigma(2^{k+1} - 1)\\ &= (1 + 2 + 4 + \cdots + 2^k)(1 + (2^{k+1} - 1)) = (2^{k+1} - 1)2^{k+1} = 2n,\end{aligned}$$

so that $s(n) = \sigma(n) - n = n$, i.e., n is perfect.

Two thousand years later, Euler established a partial converse by proving that Euclid's rule accounts for every *even* perfect number. Here is a simple argument for this: Suppose that n is an even perfect mumber and write $n = 2^k q$, where q is odd and $k \geq 1$. Then

$$2^{k+1}q = 2n = \sigma(n) = \sigma(2^k)\sigma(q) = (2^{k+1} - 1)\sigma(q). \tag{9.1}$$

Because $2^{k+1} - 1$ and 2^{k+1} are coprime, it must be that $(2^{k+1} - 1) \mid q$, so that we can write $q = (2^{k+1} - 1)r$. Substituting this expression for q into

(9.1), we obtain (upon canceling $2^{k+1}-1$ from both sides) that

$$2^{k+1}r = \sigma(q). \tag{9.2}$$

This forces us to have $r = 1$, since otherwise 1, r, and $(2^{k+1}-1)r$ are distinct divisors of q which sum to more than

$$(2^{k+1}-1)r + r = 2^{k+1}r = \sigma(q).$$

Hence $q = 2^{k+1}-1$. Moreover, putting $r = 1$ in (9.2), we obtain

$$\sigma(q) = 2^{k+1}.$$

So $\sigma(q) = q+1$. But this implies that q is prime. So $n = 2^k(2^{k+1}-1)$, where the second factor is prime, and this is exactly what we set out to show.

Summarizing, we have proved the following classical result:

Theorem 9.1 (Euclid–Euler)**.** *If $2^{k+1}-1$ is prime, then $2^k(2^{k+1}-1)$ is a perfect number. Conversely, if n is an* even *perfect number, then $n = 2^k(2^{k+1}-1)$ for some $k \geq 1$ for which $2^{k+1}-1$ is prime.*

The Euclid–Euler classification more or less closes the book on even perfect numbers. Of course it does not single-handedly answer all of the many questions one might have about these numbers, but it shows that such questions may be thought of as questions about primes of the form $2^{k+1}-1$ (so-called Mersenne primes). These new questions may in turn prove intractable, but the blame now rests with the analytic number theorists and not the investigator of perfect numbers. As an example of this process of translation, consider the question of how many even perfect numbers there are up to x. In Chapter 3, we suggested (Conjecture 3.20) that 2^m-1 is prime for $(1+o(1))e^{\gamma}\log x/\log 2$ values of $m \leq x$. So from the Euclid–Euler result, we find that the number of even perfect numbers up to x should be

$$\sim \frac{e^{\gamma}}{\log 2}\log\log x.$$

1.2. Odd perfect numbers. So what about odd perfect numbers? Here much less is known; in particular, not a single example has ever been discovered. One of the earliest results of substance is due to Euler, who showed that the factorization of a hypothetical odd perfect number must take a certain peculiar form: Suppose that n is an odd perfect number, and write the prime factorization of n in the form $n = \prod_{i=0}^{k} p_i^{f_i}$. Since n is odd,

$$2 \parallel 2n = \sigma(n) = \prod_{i=0}^{k}\sigma(p_i^{f_i}).$$

As a consequence, each term $\sigma(p_i^{f_i})$ in the product is odd except for a single exceptional value of i, where $2 \parallel \sigma(p_i^{f_i})$. By relabeling if necessary, we can assume $i = 0$ corresponds to the special term. Since each of the primes p_i is odd, we have

$$\sigma(p_i^{f_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{f_i} \equiv f_i + 1 \pmod{2},$$

and so f_i must be even for every $1 \le i \le k$. For $i = 0$, the condition $2 \parallel \sigma(p_i^{f_i})$ says that $\sigma(p_0^{f_0}) \equiv 2 \pmod{4}$. But it is easy to check that this happens only when $p_0 \equiv f_0 \equiv 1 \pmod{4}$. We have thus proved (writing $e = f_0$ and $e_i = \frac{1}{2} f_i$ for $1 \le i \le k$):

Theorem 9.2 (Euler)**.** *Every odd perfect number has the form* $p^e \prod_{i=1}^k p_i^{2e_i}$*, where* p *and the* p_i *are distinct primes, and* $p \equiv e \equiv 1 \pmod{4}$*.*

Since the time of Euler, several mathematicians have obtained other results on what an odd perfect number must look like if one exists. Here are four results representative of the current state-of-the-art: If n is an odd perfect number, then:

- n has more than 300 decimal digits (Brent, Cohen & te Riele [**BCtR91**]),
- n has a prime factor larger than 10^8 (Goto & Ohno [**GO08**]),
- n has at least 9 distinct prime factors (Nielsen [**Nie07**]),
- n has at least 75 prime factors, counted with multiplicity (Hare [**Har07**]).

While at their core the arguments of these four papers are elementary, in each case the proofs require extensive computer work. We will not prove these results here. Instead we focus our discussion of odd perfect numbers on two theorems not about the structure of individual odd perfect numbers, but about the set of odd perfect numbers as a whole. The first is the following "finiteness theorem" due to Dickson [**Dic13a**]:

Theorem 9.3. *For each fixed* $k \in \mathbf{N}$*, there are only finitely many odd perfect numbers with precisely* k *distinct prime factors.*

Theorem 9.3 shows that odd perfect numbers behave quite differently from even perfect numbers, where each (of the probably infinitely many examples) has exactly two distinct prime factors.

Upon reading the statement of Theorem 9.3, it is natural to think that the result of Nielsen quoted above has been reduced to a finite check. But this is not the case: The proof we will give of Theorem 9.3 in §9.3 is *ineffective*, in that while it shows that there are at most finitely many examples for each fixed value of k, it does not yield any finite procedure for finding all of them. Doing a bit more work, one can prove an effective version of

Theorem 9.3. Indeed, Pomerance [**Pom77a**] has shown that an odd perfect number with k distinct prime factors is necessarily less than

$$(4k)^{(4k)^{2^{k^2}}},$$

so that (in principle) one can simply test all candidates up to this bound! Heath-Brown [**HB94**] has shown that this gargantuan bound can be replaced with the (still astronomical) 4^{4^k}. Nielsen [**Nie03**] has reduced this further to 2^{4^k}. (Of course, since $2^{4^8} > 2 \cdot 10^{19728}$, this is not how Nielsen shows that an odd perfect number has at least 9 prime factors; more cunning is required!) Pollack [**Pol11c**] has shown that at most 4^{k^2} of the odd numbers $< 2^{4^k}$ are perfect.

Our second theorem addresses the distribution of odd perfect numbers. It is relatively easy to show that the odd perfect numbers are at least as sparse as the perfect squares: From Theorem 9.2, every odd perfect number n has the form $p^e m^2$, where $\gcd(p, m) = 1$. If $n \leq x$, then clearly $m \leq \sqrt{x}$. So let us fix a natural number $m \leq \sqrt{x}$ and ask for a prime power p^e with $\gcd(p, m) = 1$ for which $p^e m^2$ is perfect. In that case,

$$\sigma(p^e m^2) = 2p^e m^2, \quad \text{so that} \quad \frac{\sigma(p^e)}{p^e} = \frac{2m^2}{\sigma(m^2)}.$$

But as p^e ranges over prime powers, the numbers $\sigma(p^e)/p^e$ are all distinct; the simplest way to see this is to observe that $\sigma(p^e)/p^e$ is already a fraction in lowest terms. So there can be at most one prime power p^e (with $p \nmid m$) making $p^e m^2$ perfect, and we obtain immediately that there are at most $x^{1/2}$ odd perfect numbers $n \leq x$. This simple argument is due to Hornfeck [**Hor55**]. Later, in joint work with Wirsing, Hornfeck established [**HW57**] that the number of odd perfect numbers up to x is $O_\epsilon(x^\epsilon)$ for each $\epsilon > 0$. The strongest known result in this direction is due to Wirsing [**Wir59**]:

Theorem 9.4. *There is an absolute constant $W > 0$ with the property that the number of perfect numbers $n \leq x$ is smaller than $x^{W/\log\log x}$ for every $x \geq 3$.*

We will give Wirsing's proof in §3. In that section we also include a heuristic argument, due to Pomerance, suggesting that probably there aren't any odd perfect numbers at all.

1.3. The density of the abundant numbers. So far we have yet to answer the very first question we posed: Does the set of abundant numbers have an asymptotic density? The answer to this question is "yes", and in fact much more is true. The following beautiful result is due to Davenport [**Dav33**]; we give an elementary proof (essentially due to Erdős) in §4.

Theorem 9.5. *For each real number u, the set of natural numbers n for which $\sigma(n)/n \leq u$ possesses an asymptotic density. Calling this density $D(u)$, the function D is continuous on all of* $\mathbf{R}$ *and satisfies $D(1) = 0$ and* $\lim_{u\to\infty} D(u) = 1$.

The function $D(u)$ is known as the *distribution function for $\sigma(n)/n$.*

Since (as discussed above) the set of perfect numbers has density zero,[1] it is immediate from Theorem 9.5 that the deficient numbers have density $D(2)$ and the abundant numbers have density $1 - D(2)$. M. Kobayashi, improving earlier results of Behrend [**Beh33**], Salié [**Sal55**], Wall et al. [**Wal72, WCJ72**], and Deléglise [**Del98**], shows in his Ph.D. thesis [**Kob10**] that

$$0.24761 < 1 - D(2) < 0.24765.$$

So just under 1 in 4 natural numbers are abundant. Precise numerical values of $D(2)$ and $1 - D(2)$ are not important for the rest of this chapter, but it will be useful to keep in mind that the abundant numbers have positive density. (This is obvious once one knows that the density exists, since, e.g., it is easily shown that every multiple of 12 is abundant.)

1.4. Aliquot sequences and sociable numbers. In the remainder of this chapter we broaden our study to include certain relatives of the perfect numbers. Say that two (distinct) natural numbers m and n form an *amicable pair* if each is the sum of the proper divisors of the other, i.e., if $s(m) = n$ and $s(n) = m$. In this case both m and n are called *amicable.* For example, 220 and 284 form an amicable pair, since

$$s(284) = 1 + 2 + 4 + 71 + 142 = 220, \quad \text{while}$$
$$s(220) = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284.$$

The study of amicable numbers goes back to the Pythagoreans, but still many of the simplest questions remain unanswered. For example, while there are over 12 million examples of amicable pairs known ([**Ped**]; see also [**GPtR04**]), we have no proof that there are infinitely many.

To understand the relation between amicable numbers and perfect numbers, it is illuminating to bring into play the concept of an *aliquot sequence.* Let s_k be the kth iterate of s, defined as follows: $s_0(n) = n$, and if $k \geq 0$ and $s_k(n) > 0$, then $s_{k+1}(n) := s(s_k(n))$. The sequence of iterates $n, s(n), s_2(n), \ldots$ is called the *aliquot sequence at n.* For example, if $n = 24$, we obtain $24, 36, 55, 17, 1, 0,$ and so the sequence terminates. However, if $n = 25$, the sequence is $25, 6, 6, 6, \ldots$, so is eventually periodic. A conjecture of Catalan [**Cat88**] (as corrected by Dickson [**Dic13b**]) asserts that if

[1] One can recover that the perfect numbers make up a set of density zero from the continuity of $D(u)$, since it is plain that the upper density of the perfect numbers is bounded by $D(2+\epsilon) - D(2-\epsilon)$ for each $\epsilon > 0$.

n is any natural number, then the aliquot sequence at n is always either terminating or eventually periodic.

The Catalan–Dickson conjecture has been verified by computer to hold for all $n < 276$. But when $n = 276$, the corresponding aliquot sequence has been computed to well over a thousand terms without any repetition. Guy & Selfridge [**GS75**] have suggested that the early initial evidence for the Catalan–Dickson conjecture is deceptive, and that infinitely many aliquot sequences, perhaps most of those that start at an even value of n, tend to infinity. We will not enter into this controversy here.

We say that the natural number n is *sociable* if the aliquot sequence at n is purely periodic. In this case we call the length k of the period the *order* of n, and the set $\{n, s(n), s_2(n), \dots, s_{k-1}(n)\}$ is called a *sociable cycle* of *length* (or *order*) k. For example, 7169104 starts a sociable cycle of length 4, since under repeated application of s,

$$7169104 \mapsto 7538660 \mapsto 8292568 \mapsto 7520432 \mapsto 7169104 \mapsto \cdots .$$

At present, there are 204 known examples of sociable cycles of length > 2 [**Moe**]; of these, all but 11 have length 4.

It is reasonable to wonder what can be said, in general, about the distribution of sociable numbers. The following theorem, proved in §5, is due to Erdős:

Theorem 9.6. *For each fixed $k \in \mathbf{N}$, the set of sociable numbers of order k has asymptotic density zero.*

Probably much more than Theorem 9.6 is true; the authors of [**KPP09**] conjecture that the set of all sociable numbers (with no restriction on order) has density zero and prove that this holds if we discard the odd abundant members of this set.

When $k = 2$, Pomerance [**Pom81**] has proved a much stronger upper bound than that furnished by Theorem 9.6:

★ **Theorem 9.7.** *The number of amicable numbers $n \le x$ is smaller than $x/\exp((\log x)^{1/3})$ for all sufficiently large x.*

No result of comparable strength is known when $k > 2$. We conclude the chapter by demonstrating a slightly weaker form of Theorem 9.7 in §6.

2. Proof of Dickson's finiteness theorem

Lemma 9.8. *Let $k \in \mathbf{N}$. Suppose that A is an infinite, strictly increasing sequence of natural numbers each of which has precisely k distinct prime* *divisors. Then we may extract from A an infinite subsequence $\{n_j\}_{j=1}^{\infty}$, where each n_j has the form*

$$n_j := p_1^{e_1} \cdots p_r^{e_r} p_{r+1}^{e_{r+1,j}} \cdots p_t^{e_{t,j}} p_{t+1,j}^{e_{t+1,j}} \cdots p_{k,j}^{e_{k,j}}, \tag{9.3}$$

and where

(i) *$p_i^{e_i}$ is fixed independently of j for $1 \le i \le r$,*

(ii) *p_i is fixed independently of j and $e_{i,j} \to \infty$ as $j \to \infty$, for each $r < i \le t$, and*

(iii) *$p_{i,j} \to \infty$ as $j \to \infty$, for $t < i \le k$.*

Proof. If there is an infinite subsequence of A all of whose terms are exactly divisible by a fixed prime power $p_1^{e_1}$, pass to this subsequence. If there is an infinite subsequence of remaining terms exactly divisible by some other prime power $p_2^{e_2}$, then pass to this subsequence. Continuing, we eventually arrive at an infinite sequence all of whose terms are exactly divisible by $p_1^{e_1}, \dots, p_r^{e_r}$ (say), and which does not have any infinite subsequence of integers whose canonical factorizations contain a fixed prime power other than $p_1^{e_1}, \dots, p_r^{e_r}$. (This process necessarily terminates in $r \le k$ steps. Of course it is also possible that it never starts, i.e., that $r = 0$.)

If at this point our sequence has an infinite subsequence all of whose terms are divisible by a fixed prime p_{r+1} different from $p_1, \dots, p_r$, then pass to this subsequence. Note that the exponent of p_{r+1} along the terms of this subsequence must tend to infinity to avoid contradicting the conclusion of the last paragraph. If our sequence has an infinite subsequence all of whose terms are divisible by the fixed prime $p_{r+2} \notin \{p_1, \dots, p_{r+1}\}$, pass to this subsequence. Continue this process as long as possible, ending with (say) p_t. Then our final sequence has all of the properties specified in Lemma 9.8. $\square$

Lemma 9.9. *For every natural number n, we have $\sigma(n)/n = \sigma_{-1}(n)$, where*

$$\sigma_{-1}(n) := \sum_{d \mid n} \frac{1}{d}.$$

Consequently, if m and n are two natural numbers for which $m \mid n$, then $\sigma(m)/m \le \sigma(n)/n$ with equality only if $m = n$.

Proof. We have $\sigma(n)/n = (1/n)\sum_{d \mid n} d = \sum_{d \mid n} (n/d)^{-1} = \sigma_{-1}(n)$, since n/d runs over all the divisors of n as d does. The rest of the lemma is now obvious. $\square$

Lemma 9.9 implies, in particular, that it is impossible for one perfect number to properly divide another.

We now prove Theorem 9.3, following the approach of Artjuhov [**Art73**]; cf. Gradstein [**Gra25**], Shapiro [**Sha49b**].

Proof of Theorem 9.3. Suppose that there are infinitely many odd perfect numbers with exactly k distinct prime factors, and consider the sequence of all such numbers in increasing order. Use Lemma 9.8 to extract an infinite subsequence $n_1 < n_2 < n_3 < \cdots$ whose factorizations have the form (9.3). Applying σ_{-1} to both sides of (9.3), we find that for each $j = 1, 2, 3, \dots,$

$$\begin{aligned} 2 = \sigma_{-1}(n_j) &= \prod_{i=1}^{r} \sigma_{-1}(p_i^{e_i}) \prod_{i=r+1}^{t} \sigma_{-1}(p_i^{e_{i,j}}) \prod_{i=t+1}^{k} \sigma_{-1}(p_{i,j}^{e_{i,j}}) \\ &= \prod_{i=1}^{r} \frac{p_i^{e_i+1}-1}{p_i^{e_i}(p_i-1)} \prod_{i=r+1}^{t} \left(1 + \frac{1}{p_i} + \cdots + \frac{1}{p_i^{e_{i,j}}}\right) \prod_{i=t+1}^{k} \sigma_{-1}(p_{i,j}^{e_{i,j}}). \end{aligned} \tag{9.4}$$

Letting $j \to \infty$, we find (referring back to the statement of Lemma 9.8) that

$$2 = \prod_{i=1}^{r} \frac{p_i^{e_i+1}-1}{p_i^{e_i}(p_i-1)} \prod_{i=r+1}^{t} \frac{p_i}{p_i - 1}. \tag{9.5}$$

Comparing (9.5) with (9.4) shows that (for each j)

$$\prod_{i=r+1}^{t} \left(1 + \frac{1}{p_i} + \cdots + \frac{1}{p_i^{e_{i,j}}}\right) \prod_{i=t+1}^{k} \sigma_{-1}(p_{i,j}^{e_{i,j}}) = \prod_{i=r+1}^{t} \frac{p_i}{p_i - 1}.$$

For any j, the left-hand side has odd denominator in lowest terms. This forces $r = t$, since otherwise the right-hand product represents a rational number with even denominator. Now (9.5) shows that

$$2 \prod_{i=1}^{r} p_i^{e_i} = \prod_{i=1}^{r} \frac{p_i^{e_i+1}-1}{p_i - 1},$$

which says that $n := \prod_{i=1}^{r} p_i^{e_i}$ is perfect. But this is impossible, since n divides every n_j and no perfect number can properly divide another. □

3. How rare are odd perfect numbers?

3.1. Proof of Wirsing's theorem. We need two combinatorial lemmas before we can prove Theorem 9.4:

Lemma 9.10. *Let M be a nonnegative integer. Then there are exactly 2^M solutions to the inequality*

$$e_1 + e_2 + \cdots + e_k \le M,$$

where $k \ge 0$ and the e_i are positive integers. Here the empty sum is counted as a solution corresponding to $k = 0$.

Proof. Define the formal power series $P(T)$ by putting $P(T) := T + T^2 + T^3 + \cdots$. Then $P(T) = T/(1-T)$. Moreover, the number of solutions in positive integers $e_1, \dots, e_k$ to $e_1 + \cdots + e_k = m$ is given by the coefficient of T^m in

$$1 + P(T) + P(T)^2 + P(T)^3 + \cdots = \frac{1}{1-P(T)} = \frac{1-T}{1-2T}.$$

Consequently, the quantity described in the lemma statement is given by the coefficient of T^M in

$$(1 + T + T^2 + \dots)\frac{1-T}{1-2T} = \frac{1}{1-T}\frac{1-T}{1-2T} = \frac{1}{1-2T},$$

which is just 2^M, as claimed. □

Lemma 9.11. *Let M and k be nonnegative integers. Then the inequality*

$$e_1 + e_2 + \cdots + e_k \leq M$$

has exactly $\binom{M+k}{M} \leq 2^{M+k}$ solutions in nonnegative integers $e_1, e_2, \dots, e_k$.

Proof. The number of solutions to the inequality of the lemma is the same as the number of solutions in nonnegative e_i to the equation $e_0+e_1+\cdots+e_k = M$. This is given by the coefficient of T^M in the power series

$$(1 + T + T^2 + T^3 + \cdots)^{k+1} = (1-T)^{-(k+1)},$$

which by the binomial theorem is precisely

$$(-1)^M\binom{-k-1}{M} = \binom{M+k}{M},$$

as claimed. The upper bound $\binom{M+k}{M} \leq 2^{M+k}$ is obvious, since $\binom{M+k}{M}$ is a summand in the binomial expansion of $(1+1)^{M+k}$. □

Proof of Theorem 9.4. For each perfect number $n \leq x$, we write $n = AQ$, where

$$A := \prod_{\substack{p^{e_p} \| n \\ p > \log x}} p^{e_p} \quad \text{and} \quad Q := \prod_{\substack{p^{e_p} \| n \\ p \leq \log x}} p^{e_p}.$$

Thus Q represents the $(\log x)$-smooth part of n.[2] Loosely speaking, we will show that Q essentially determines A, and so also essentially determines n. Theorem 9.4 will then follow from an upper bound on the number of $(\log x)$-smooth integers $Q \leq x$.

[2] Recall from Chapter 1 that a number is said to be *y-smooth* if all of its prime factors are $\leq y$.

Fix a $(\log x)$-smooth integer $Q \le x$. Let us suppose $n \le x$ is perfect, where $n = AQ$ and every prime factor of A exceeds $\log x$. Then A can have at most $\log x/\log\log x$ distinct prime factors, and so

$$\begin{aligned}\frac{A}{\sigma(A)} &\ge \prod_{\substack{\log x < p \le x \\ p \mid A}} \left(1 - \frac{1}{p}\right) \ge 1 - \sum_{\substack{\log x < p \le x \\ p \mid A}} \frac{1}{p} \\ &\ge 1 - \frac{1}{\log x}\frac{\log x}{\log\log x} = 1 - \frac{1}{\log\log x} > 1/2\end{aligned}$$

if x is large (which we assume). Since

$$\sigma(A)\sigma(Q) = \sigma(n) = 2n = 2AQ, \tag{9.6}$$

we have

$$Q < \frac{2A}{\sigma(A)} Q = \sigma(Q) \le 2Q, \tag{9.7}$$

with equality on the right only if $A = 1$. Thus if $A \ne 1$, then $\sigma(Q) \nmid 2Q$, so that there is a prime dividing $\sigma(Q)$ to a higher power than it divides $2Q$. Let p_1 be the least such prime. It follows from (9.6) that $p_1^{e_1} \parallel A$ for a certain exponent $e_1 \ge 1$. Now write

$$n = A'Q', \qquad \text{where} \qquad A' := \frac{A}{p_1^{e_1}}, \quad Q' := Qp_1^{e_1}.$$

Then $A'/\sigma(A') \ge A/\sigma(A) > 1/2$ and both (9.6) and (9.7) hold with A and Q replaced by A' and Q' (respectively). Repeating the above argument, we find that if $A' \ne 1$, then there exists a prime dividing $\sigma(Q')$ to a higher power than it divides $2Q'$. Letting p_2 be the smallest such prime, we have that $p_2^{e_2} \parallel A'$ for a certain exponent $e_2 \ge 1$. We then set $A'' := A'/p_2^{e_2}, Q'' := Q'p_2^{e_2}$, and continue. This process eventually terminates and we obtain a factorization of the form

$$A = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}.$$

Notice that the prime p_1 is completely determined by Q, while for $i > 1$, the prime p_i is completely determined by Q and $e_1, e_2, \ldots, e_{i-1}$. So, for fixed Q, the number A is completely determined by the sequence of exponents $e_1, \ldots, e_t$. Since each prime divisor of A exceeds $\log x$, we have

$$e_1 + \cdots + e_t \le \frac{\log x}{\log\log x}.$$

It now follows from Lemma 9.10 that for each Q, there are at most

$$2^{\log x/\log\log x} = x^{\log 2/\log\log x} \tag{9.8}$$

choices for A.

It remains to estimate the number of $(\log x)$-smooth natural numbers $Q \leq x$. For each such Q, put $Q = Q_1 Q_2$, where

$$Q_1 := \prod_{\substack{p^{e_p} \| Q \\ \sqrt{\log x} < p \leq \log x}} p^{e_p} \quad \text{and} \quad Q_2 := \prod_{\substack{p^{e_p} \| Q \\ p \leq \sqrt{\log x}}} p^{e_p}.$$

Because $Q_1 \leq Q \leq x$, the exponents e_p appearing in the factorization of Q_1 must satisfy

$$\sum_{\sqrt{\log x} < p \leq \log x} e_p \leq \frac{\log x}{\log \sqrt{\log x}} = 2\frac{\log x}{\log\log x}.$$

The number of summands here is bounded by $\pi(\log x)$, which by the results of Chebyshev is at most $K \log x/\log\log x$ for a certain constant $K > 0$. So by Lemma 9.11, the number of possibilities for Q_1 is at most

$$2^{(K+2)\log x/\log\log x} = x^{(K+2)\log 2/\log\log x}. \tag{9.9}$$

Since also $Q_2 \leq x$, the exponent e_p of each prime appearing in the definition of Q_2 is trivially $\leq \log x/\log 2$. Thus the number of possibilities for Q_2 is bounded by

$$\prod_{p \leq \sqrt{\log x}} \left(1 + \frac{\log x}{\log 2}\right) \leq \left(1 + \frac{\log x}{\log 2}\right)^{\sqrt{\log x}}$$
$$\leq \exp(2\sqrt{\log x}\log\log x) = \exp(o(\log x/\log\log x)). \tag{9.10}$$

From (9.9) and (9.10), the total number of $(\log x)$-smooth $Q \leq x$ is at most $x^{((K+2)\log 2 + o(1))/\log\log x}$. So from (9.8), if $W > (K+3)\log 2$, then the number of perfect numbers $\leq x$ is at most $x^{W/\log\log x}$ for all sufficiently large values of x. Adjusting the value of W if necessary, this can be made to hold for all $x \geq 3$. $\square$

3.2. A heuristic. Theorem 9.2 tells us that every odd perfect number can be written in the form $p^e m^2$, where $p \equiv e \equiv 1 \pmod 4$ and $\gcd(p, m) = 1$. Call a number n of this form a *candidate*, and say that n is *successful* if n is actually an odd perfect number, i.e., if

$$2p^e m^2 = 2n = \sigma(n) = \sigma(p^e)\sigma(m^2).$$

Let us attempt to estimate the odds that a given m corresponds to a successful candidate $n = p^e m^2$. (Strictly speaking this is nonsense, since such an m either does or doesn't correspond to such an n; there are no "odds" about it. But it is a useful bit of nonsense!) Since $\gcd(p^e, \sigma(p^e)) = 1$, if n is successful, then $p^e \parallel \sigma(m^2)$. The number of exact prime power divisors of $\sigma(m^2)$ is trivially at most $\log \sigma(m^2)/\log 2$. Since

$$\sigma(m^2) \leq \sum_{d \leq m^2} d \leq m^2 \cdot m^2 = m^4,$$

there are at most $4 \log m/ \log 2$ possibilities for p^e. Supposing now that p^e does exactly divide $\sigma(m^2)$, for $n = p^e m^2$ to be successful, we also need that

$$m^2 \mid \sigma(p^e)\frac{\sigma(m^2)}{p^e},$$

which we might expect to hold with "probability" $1/m^2$.

The upshot is that for a given value of m, the "probability" that there is a successful candidate of the form $p^e m^2$ is at most $(4 \log 2) \log m/m^2$. Since the sum $\sum_{m \geq 1}(4\log 2)\log m/m^2$ converges, we expect that there are only finitely many successful candidates (odd perfect numbers).

We can take this a bit further. Suppose n is an odd perfect number, and write $n = p^e m^2$ as above. Since m^2 is a proper divisor of n, we have $\sigma(m^2)/m^2 < \sigma(n)/n = 2$. Since also p^e divides $\sigma(m^2)$, it follows that

$$2m^4 > \sigma(m^2)m^2 \geq p^e m^2 = n > 10^{300},$$

using the result of Brent, Cohen, and te Riele mentioned on p. 276. Thus $m > 2^{-1/4} \cdot 10^{75}$. If we compute $\sum (4\log 2)\log m/m^2$ over these values of m, we obtain an upper bound of less than 10^{-70} for the expected total count of odd perfect numbers. So it seems highly unlikely that any example exists.

This is (a slight variant of) an unpublished argument of Pomerance.

4. The distribution function of $\sigma(n)/n$

Theorem 9.5 asserts that for each real u, the density of the set of n with $\sigma(n)/n \leq u$ exists; moreover, calling this density $D(u)$, we have that $D(u)$ is a continuous function of u, $D(1) = 0$, and $\lim_{u\to\infty} D(u) = 1$. Owing to Lemma 9.9, we may replace "$\sigma(n)/n$" in this statement with "$\sigma_{-1}(n)$", which will prove convenient both notationally and psychologically.

For each $B > 0$, we define the arithmetic function σ_{-1}^B by putting

$$\sigma_{-1}^B(n) := \sum_{\substack{d\mid n \\ p\mid d \Rightarrow p \leq B}} \frac{1}{d}.$$

In other words, σ_{-1}^B is obtained by restricting the sum defining σ_{-1} to B-smooth divisors of n. We also set $F^B(n)$ equal to the B-smooth part of n, i.e., $F^B(n) := \prod_{p^e \| n, p\leq B} p^e$. Note that with these definitions, we have $\sigma_{-1}^B(n) = \sigma_{-1}(F^B(n))$. Define

$$\mathscr{N}(x,u) := \{n \leq x : \sigma_{-1}(n) \leq u\} \quad \text{and} \quad \mathscr{N}^B(x,u) := \{n \leq x : \sigma_{-1}^B(n) \leq u\},$$

and set $N(x,u) := \#\mathscr{N}(x,u)$ and $N^B(x,u) := \#\mathscr{N}^B(x,u)$.

We begin the proof of Theorem 9.5 by demonstrating a partial analogue of that result for the functions σ_{-1}^B:

Lemma 9.12. *Let $B > 0$. For each real u, the quantity $N^B(x,u)/x$ tends to a limit, say $D^B(u)$, as $x \to \infty$.*

Proof. Let S be the collection of B-smooth numbers m with $\sigma_{-1}(m) \le u$. For a natural number n, we have $\sigma_{-1}^B(n) \le u$ precisely when $F^B(n) = m$ for some $m \in S$. For each $m \in S$, the set of natural numbers n with $F^B(n) = m$ possesses an asymptotic density, since this set is just the union of certain residue classes modulo $m \prod_{p \le B} p$. Denote this density by d_m. We claim that $N^B(x,u)/x \to \sum_{m \in S} d_m$ as $x \to \infty$.

For the proof, let z be a positive real parameter. Since $\sigma_{-1}^B(n) \le u$ whenever $F^B(n) \in S \cap [1,z]$, it is clear that

$$\liminf_{x\to\infty} \frac{N^B(x,u)}{x} \ge \sum_{\substack{m \in S\\ m \le z}} d_m. \tag{9.11}$$

On the other hand, if $\sigma_{-1}^B(n) \le u$, then either $F^B(n) \in S \cap [1,z]$, or n is divisible by some $m \in S$ with $m > z$. So

$$\limsup_{x\to\infty} \frac{N^B(x,u)}{x} \le \sum_{\substack{m \in S\\ m \le z}} d_m + \sum_{\substack{m \in S\\ m > z}} \frac{1}{m}. \tag{9.12}$$

Since $\sum_{m \in S} m^{-1} \le \sum_{m\ B\text{-smooth}} m^{-1} = \prod_{p \le B}(1 - 1/p)^{-1} < \infty$, the final sum in (9.12) is the tail of a convergent series. So the desired equality $D^B(u) = \sum_{m \in S} d_m$ follows by letting $z \to \infty$ in (9.11) and (9.12). □

Lemma 9.13. *Let $\mathscr{P}$ be a set of primes for which $\sum_{p \in \mathscr{P}} p^{-1}$ diverges. For each $\epsilon > 0$, there is a $z > 0$ for which the following holds: For all n outside of a set of density $< \epsilon$, there is a prime $p \in \mathscr{P} \cap [2,z]$ for which $p \parallel n$.*

Proof. The relation $p \parallel n$ holds precisely when n falls into one of the $p-1$ residue classes $p, 2p, \dots, (p-1)p \bmod p^2$. So by the Chinese remainder theorem and the principle of inclusion-exclusion, the set of n exactly divisible by none of the primes $p \in \mathscr{P} \cap [2,z]$ has density

$$\prod_{\substack{p \in \mathscr{P}\\ p \le z}} \left(1 - \frac{p-1}{p^2}\right) < 3\exp\Bigg(-\sum_{\substack{p \in \mathscr{P}\\ p \le z}} \frac{1}{p}\Bigg),$$

which for large values of z is less than ϵ. □

Lemma 9.14. *Let u be any real number. As $\delta \downarrow 0$, the upper density of the set of n with $u - \delta < \sigma_{-1}(n) < u + \delta$ tends to zero.*

Proof. Since the image of σ_{-1} is contained in $[1,\infty)$, we may assume that $u \ge 1$. Let $\epsilon > 0$, and fix a real number $B > 0$ with $1/B < \epsilon$. By Lemma

9.13, we can fix z so that if $p_1 < p_2 < \cdots < p_k$ is the list of primes in the interval $(B, z]$, then all n outside of an exceptional set of density $< \epsilon$ are exactly divisible by at least one of $p_1, \ldots, p_k$.

Let

$$\mathscr{N}(x) := \{n \le x : u - \delta < \sigma_{-1}(n) < u + \delta\}.$$

For each $n \in \mathscr{N}(x)$ not in the exceptional set described above, fix a prime p_i (with $1 \le i \le k$) exactly dividing n and form the quotient n/p_i. We claim that if $\delta > 0$ is chosen sufficiently small depending on ϵ, then all of the quotients n/p_i are distinct. Since each such quotient is at most x/B, for large x this implies

$$\#\mathscr{N}(x) < \epsilon x + x/B < 2\epsilon x,$$

which proves the lemma.

To establish the claim, suppose that n and n' are distinct elements of $\mathscr{N}(x)$, that $p_i \parallel n$ and $p_j \parallel n'$ (where $1 \le i, j \le k$), and that $n/p_i = n'/p_j$. Clearly $i \ne j$. Moreover,

$$\frac{\sigma_{-1}(n)}{\sigma_{-1}(p_i)} = \sigma_{-1}(n/p_i) = \sigma_{-1}(n'/p_j) = \frac{\sigma_{-1}(n')}{\sigma_{-1}(p_j)},$$

which implies that

$$\frac{u-\delta}{u+\delta} \le \frac{\sigma_{-1}(n)}{\sigma_{-1}(n')} = \frac{\sigma_{-1}(p_i)}{\sigma_{-1}(p_j)} \le \frac{u+\delta}{u-\delta}.$$

Thus, assuming $\delta < 1/2$,

$$\left|\frac{\sigma_{-1}(p_i)}{\sigma_{-1}(p_j)} - 1\right| \le \frac{2\delta}{u-\delta} < 4\delta.$$

(Recall that $u \ge 1$.) But this is impossible for sufficiently small values of δ, since the numbers $\sigma_{-1}(p_1), \ldots, \sigma_{-1}(p_k)$ are all distinct. (In fact, $\sigma_{-1}(p_1) > \sigma_{-1}(p_2) > \cdots > \sigma_{-1}(p_k)$.) □

We can now prove the first half of Theorem 9.5, that the set of $n \in \mathbf{N}$ with $\sigma_{-1}(n) \le u$ always possesses an asymptotic density:

Proposition 9.15. *For each real u, the quantity $N(x,u)/x$ tends to a limit, say $D(u)$, as $x \to \infty$.*

Proof. If $B_1 < B_2$, then $\sigma_{-1}^{B_1}(n) \le \sigma_{-1}^{B_2}(n)$ for each n, and so $D^{B_1}(u) \ge D^{B_2}(u)$. Hence (for each fixed u) $D^B(u)$ converges as $B \to \infty$ to $D^*(u) := \inf_{B>0} D^B(u)$. We will prove that $N(x,u)/x \to D^*(u)$ as $x \to \infty$.

If $B > 0$, then $\sigma_{-1}^B(n) \le \sigma_{-1}(n)$ for every natural number n. Consequently, $\mathscr{N}(x,u) \subset \mathscr{N}^B(x,u)$ for all x. Thus

$$\limsup_{x\to\infty} \frac{N(x,u)}{x} \le \inf_{B>0}\left(\limsup_{x\to\infty}\frac{N^B(x,u)}{x}\right) = \inf_{B>0} D^B(u) = D^*(u).$$

We would like to establish the corresponding lower bound for the lim inf of $N(x,u)/x$.

Let $\epsilon > 0$. For a parameter $\delta > 0$ to be specified shortly, put

$$\mathscr{M}_1^B(x,u) := \{n \le x : \sigma_{-1}^B(n) \le u \text{ and } u < \sigma_{-1}(n) < u + \delta\}$$

and

$$\mathscr{M}_2^B(x,u) := \{n \le x : \sigma_{-1}^B(n) \le u \text{ and } \sigma_{-1}(n) \ge u + \delta\},$$

and set $M_i^B(x,u) := \#\mathscr{M}_i^B(x,u)$. Then

$$\frac{N(x,u)}{x} = \frac{N^B(x,u)}{x} - \frac{M_1^B(x,u)}{x} - \frac{M_2^B(x,u)}{x}. \tag{9.13}$$

If $\delta > 0$ is small enough in terms of ϵ, then $\limsup M_1^B(x,u)/x < \epsilon$ by Lemma 9.14. Having fixed such a δ, notice that

$$\begin{aligned} M_2^B(x,u) &= \sum_{n \in \mathscr{M}_2^B(x,u)} 1 \le \delta^{-1} \sum_{n \le x} \left(\sigma_{-1}(n) - \sigma_{-1}^B(n)\right) \\ &= \delta^{-1} \sum_{\substack{d \le x \\ p \mid d \text{ for some } p > B}} \frac{1}{d} \sum_{\substack{n \le x \\ d \mid n}} 1 \le \delta^{-1} x \sum_{d > B} d^{-2} \ll \delta^{-1} x/B. \end{aligned}$$

In particular, $\limsup M_2^B(x,u)/x$ tends to zero as $B \to \infty$. Letting first x tend to infinity in (9.13) and then also B, we find

$$\liminf \frac{N(x,u)}{x} \ge \lim_{B \to \infty} D^B(u) - \epsilon = D^*(u) - \epsilon.$$

Since $\epsilon > 0$ is arbitrary, Proposition 9.15 follows. □

The next proposition completes the proof of Theorem 9.3.

Proposition 9.16. *If $D(u)$ is defined as in the statement of Proposition 9.15, then $D(u)$ defines a continuous function of u on all of $\mathbf{R}$. Moreover, $D(1) = 0$ and $D(u) \to 1$ as $u \to \infty$.*

Proof. Clearly $D(u)$ is nondecreasing as a function of u. So if u is an arbitrary real number, then for every real δ we have

$$|D(u + \delta/2) - D(u)| \le |D(u + |\delta|/2) - D(u - |\delta|/2)|.$$

The right-hand side of this inequality represents the density of the set of n for which $u - |\delta|/2 < \sigma_{-1}(n) \le u + |\delta|/2$, and this tends to zero with δ by Lemma 9.14. Hence D is continuous at u.

It is clear that $D(1) = 0$, since $\sigma_{-1}(n) > 1$ except when $n = 1$. Moreover, for all $x > 0$,

$$\sum_{n \le x} \sigma_{-1}(n) = \sum_{d \le x} \frac{1}{d} \sum_{\substack{n \le x \\ d \mid n}} 1 \le x \sum_{d} d^{-2} < 2x.$$

Thus, for each $u > 0$, the number of $n \leq x$ with $\sigma_{-1}(n) > u$ is $< 2x/u$. Hence $1 - D(u) \leq 2/u$, so that $D(u) \geq 1 - 2/u$. Since $D(u) \leq 1$ for all u, it follows that $D(u) \to 1$ as $u \to \infty$, as desired. □

In Exercises 38 and 38 we outline a proof that $D(u)$ is strictly increasing for $u \geq 1$. In fact, that argument shows that $D(u)$ has an infinite right-sided derivative at every rational number u of the form $\sigma_{-1}(n)$ (where $n \in \mathbf{N}$) while the set of such u is dense in $[1, \infty)$. Erdős has proved [**Erd39**] the curious result that $D'(u) = 0$ for all u outside of a set of measure zero.

5. Sociable numbers

5.1. A theorem on the local behavior of aliquot sequences. One way to disprove the Catalan–Dickson conjecture mentioned in this chapter's introduction would be to produce a natural number n for which the sequence $\{s_j(n)\}_{j=0}^{\infty}$ is strictly increasing. It seems unlikely that such an n exists. However, in 1975 Lenstra [**Len75**] showed that for each fixed K, there are infinitely many natural numbers n with

$$n < s(n) < s_2(n) < \cdots < s_{K+1}(n). \tag{9.14}$$

Actually (9.14) is more common than one might expect: In 1976, Erdős showed [**Erd76**] that for each fixed K, (9.14) holds for almost all abundant numbers n. In other words, if n increases once when s is applied, then almost surely n increases $K + 1$ times. Erdős deduced this result from the following theorem, which is of independent interest:

Theorem 9.17. *Let K be a natural number, and let $\epsilon > 0$. For almost all natural numbers n,*

$$\frac{s_{k+1}(n)}{s_k(n)} > \frac{s(n)}{n} - \epsilon$$

for all $1 \leq k \leq K$.

Before proceeding to the proof of Theorem 9.17, let us see how to derive the stated consequence:

Corollary 9.18. *For each fixed k, the set of abundant numbers n for which* (9.14) *fails has asymptotic density zero.*

Proof. Let $\epsilon > 0$. Using the continuity of the distribution function $D(u)$ of Theorem 9.5, choose a small $\delta > 0$ with $D(2 + \delta) < D(2) + \epsilon$. Suppose n is abundant but that (9.14) fails. If $\sigma(n)/n \leq 2 + \delta$, then n belongs to a set of density $D(2 + \delta) - D(2) < \epsilon$. Now suppose that $\sigma(n)/n > 2 + \delta$. By Theorem 9.17, unless n belongs to a certain set of density zero,

$$s_{k+1}(n)/s_k(n) > s(n)/n - \delta/2 > (1 + \delta) - \delta/2 > 1$$

for all $1 \leq k \leq K$, and so (9.14) holds.

So the set of abundant counterexamples to (9.14) has upper density less than ϵ. Since $\epsilon > 0$ was arbitrary, the corollary follows. $\square$

The proof of Theorem 9.17 requires a preliminary technical lemma.

Lemma 9.19. *Let K and M be integers with $K \geq 0$ and $M \geq 1$. Then the following is true for almost all natural numbers n: There are primes $p_0, p_1, \ldots, p_K$ for which*

$$p_i \parallel n \quad \textit{for each } i = 0, 1, 2, \ldots, K, \tag{9.15}$$

and

$$p_0 \equiv -1 \pmod{M}, \quad \textit{and} \quad p_{i+1} \equiv -1 \pmod{p_i^2} \quad \textit{for all} \quad 0 \leq i < K. \tag{9.16}$$

Proof. The lemma is a consequence of the following assertion, which we prove by induction on K: For each nonnegative integer K, each $M \in \mathbf{N}$, and each $\epsilon > 0$, there is a number B with the property that for all n outside of a set of upper density $< \epsilon$, one can find primes $p_0, \ldots, p_K \leq B$ satisfying both (9.15) and (9.16). When $K = 0$, this statement follows immediately from Lemma 9.13, applied with

$$\mathscr{P} := \{p \equiv -1 \pmod{M}\}.$$

(Note that $\sum_{p \in \mathscr{P}} p^{-1}$ diverges by the results of Chapter 4.)

Now suppose the statement is known to hold for a certain integer $K \geq 0$. If $M \in \mathbf{N}$ and $\epsilon > 0$ are given, the induction hypothesis permits us to choose a number B_0 with the property that for all n outside of a set E_0 (say) of upper density $< \epsilon/2$, there are primes $p_0, \ldots, p_K \leq B_0$ satisfying (9.15) and (9.16). Let $R := (\prod_{p \leq B_0} p)^2$ and apply Lemma 9.13 with $\mathscr{P} := \{p \equiv -1 \pmod{R}\}$. We find that for a suitable choice of z, all n outside of a set E_1 (say) of upper density $< \epsilon/2$ have an exact prime divisor $p_{K+1} \equiv -1 \pmod{R}$ with $p_{K+1} \leq z$. But then if n lies outside $E_0 \cup E_1$, the primes $p_1, \ldots, p_{K+1}$ satisfy (9.15) and (9.16) with K replaced by $K + 1$. Since $E_0 \cup E_1$ has upper density $< \epsilon$, we obtain the $(K + 1)$-case of the assertion with $B = \max\{B_0, z\}$. $\square$

Proof of Theorem 9.17. Let B be an arbitrary natural number, and put $M := (\prod_{p \leq B} p)^B$. We claim that for almost all n, the number M divides $\sigma(s_i(n))$ for each $0 \leq i \leq K$.

The proof of the claim starts with the observation that by Lemma 9.19, for almost all n there are primes $p_0, \ldots, p_K$ satisfying (9.15) and (9.16). Then for each $0 \leq i < K$, we have

$$p_i^2 \mid \sigma(p_{i+1}) \mid \sigma(n), \quad \text{so that since } p_i \parallel n, \text{ we have} \quad p_i \parallel \sigma(n) - n = s(n).$$

Thus $p_0, \ldots, p_{K-1}$ exactly divide $s(n)$. We can repeat the argument with n replaced by $s(n)$ to see that $s_2(n)$ is exactly divisible by $p_0, \ldots, p_{K-2}$. Continuing in the same manner, we find that $s_i(n)$ is exactly divisible by $p_0, \ldots, p_{K-i}$, for each $0 \le i \le K$. In particular, p_0 exactly divides each of n, $s(n)$, $\ldots$, $s_K(n)$. Thus

$$M \mid \sigma(p_0) \mid \sigma(s_i(n)) \quad \text{for all } 0 \le i \le K,$$

as we originally claimed.

So at the cost of throwing away a set of density zero, we may assume that the claim holds for n. As a consequence, for each $0 < k \le K+1$, we have

$$s_k(n) = \sigma(s_{k-1}(n)) - s_{k-1}(n) \equiv -s_{k-1}(n) \pmod{M}. \tag{9.17}$$

For each $0 \le i \le K$, write $s_i(n) = m_i n_i$, where $\gcd(m_i, n_i) = 1$ and every prime divisor of n_i is at most B. (So n_i is the B-smooth part of $s_i(n)$.) We claim that for all n outside of a set of upper density $o(1)$, we have

$$n_0 = n_1 = \cdots = n_K; \tag{9.18}$$

here and below, $o(1)$ denotes a quantity that tends to zero as $B \to \infty$. For the proof, suppose (9.18) fails, so that $n_i \ne n_{i+1}$ for some $0 \le i < K$. Writing

$$s_{i+1}(n) = \sigma(s_i(n)) - s_i(n),$$

we see that $n_i \ne n_{i+1}$ implies that there is a prime $p \le B$ which divides $s_i(n)$ to at least as high a power as it divides $\sigma(s_i(n))$. Since $\sigma(s_i(n))$ is divisible by M, and hence by p^B, it must be that p^B divides $s_i(n)$. But then by repeated application of (9.17) (starting with $k = i$), we find that p^B divides $s_0(n) = n$. But the upper density of the set of n divisible by p^B for some $p \le B$ is bounded by $\sum_{p \le B} p^{-B}$, which is $o(1)$.

So, excepting a set of upper density $o(1)$, we may suppose that (9.18) holds. Then for each $1 \le k \le K$,

$$\begin{aligned}
\frac{s(n)}{n} - \frac{s_{k+1}(n)}{s_k(n)} &= \frac{\sigma(n)}{n} - \frac{\sigma(s_k(n))}{s_k(n)} \\
&= \frac{\sigma(n_0)}{n_0}\left(\frac{\sigma(m_0)}{m_0} - \frac{\sigma(m_k)}{m_k}\right) \\
&\le \frac{\sigma(n_0)}{n_0}\left(\frac{\sigma(m_0)}{m_0} - 1\right).
\end{aligned}$$

Now $\sigma(n_0)/n_0 = \sigma_{-1}(n_0) \le \sigma_{-1}(n)$; moreover, $\sigma_{-1}(n) \le B^{1/2}$ for all n outside of a set of density $o(1)$, by the latter half of Lemma 9.16. We claim that we also have

$$\frac{\sigma(m_0)}{m_0} - 1 \le \frac{1}{B^{3/4}}$$

for all n outside of a set of upper density $o(1)$. Once this claim is established, we will have shown that for all n outside of a set of upper density $o(1)$,

$$\frac{s(n)}{n} - \frac{s_{k+1}(n)}{s_k(n)} \leq \frac{B^{1/2}}{B^{3/4}} = \frac{1}{B^{1/4}} = o(1) \qquad \text{for all } 1 \leq k \leq K,$$

and Theorem 9.17 follows upon letting $B \to \infty$.

To prove this last claim, notice that

$$\frac{\sigma(m_0)}{m_0} - 1 = \sum_{\substack{d \mid n \\ p \mid d \Rightarrow p > B \\ d > 1}} \frac{1}{d},$$

so that the number of $n \leq x$ with $\sigma(m_0)/m_0 - 1 > B^{-3/4}$ is at most

$$B^{3/4} \sum_{n \leq x} \sum_{\substack{1 < d \mid n \\ p \mid d \Rightarrow p > B}} \frac{1}{d} = B^{3/4} \sum_{\substack{1 < d \leq x \\ p \mid d \Rightarrow p > B}} \frac{1}{d} \sum_{\substack{n \leq x \\ d \mid n}} 1$$
$$\leq B^{3/4} \sum_{d > B} \frac{x}{d^2} \leq B^{-1/4} x.$$

Thus the set of such n has upper density $\leq B^{-1/4} = o(1)$, as desired. □

5.2. An application to sociable numbers. Theorem 9.6, which asserts that the set of sociable numbers of order k has density zero for each fixed k, is almost immediate from Corollary 9.18. Indeed, fix a natural number $k > 1$. (When $k = 1$, we have already seen that the sociable numbers of order k — i.e., the perfect numbers — comprise a set of density zero.) Let $A(x)$ be the number of sociable $n \leq x$ of order k, and let $A'(x)$ be the number of $n \leq x$ which are the smallest member of some sociable k-cycle. Then $A(x) \leq kA'(x)$. So to show that $A(x) = o(x)$, it is enough to show that $A'(x) = o(x)$. But this is clear from Corollary 9.18, since if n is the smallest member of a sociable k-cycle, then $n < s(n)$ (i.e., n is abundant), but we do not have

$$n < s(n) < s_2(n) < \ldots < s_k(n),$$

since $n = s_k(n)$.

Remark. By making the error terms in the above argument explicit when $k = 2$, Erdős & Rieger ([**Rie73**], [**ER75**]) showed that the number of amicable $n \leq x$ is $\ll x/\log\log\log x$. Let $\log_1 x := \max\{1, \log x\}$ and for $k > 1$, define $\log_k x := \max\{1, \log(\log_{k-1} x)\}$. For general k, the Erdős–Rieger method shows that there are $\ll_k x/\log_r x$ sociable numbers of order k not exceeding x, where r grows linearly with k (e.g., $r = 3k$ is permissible). In

[**KPP09**], it is proved that the number of sociable $n \le x$ of order k is at most

$$k(2\log_4 x)^k \frac{x}{\exp((1+o(1))\sqrt{\log_3 x \log_4 x})}$$

where the $o(1)$ term tends to zero as $x \to \infty$, and the estimate is uniform in $k \ge 1$. Moreover, for fixed odd k, one can do a bit better; as shown in [**Pol10**], the count in this case is at most

$$x/(\log x)^{1+o(1)}, \tag{9.19}$$

as $x \to \infty$ (where the rate of decay of the $o(1)$ term may depend on k).

6. The distribution of amicable numbers

Recall that n is said to be *amicable* if there is a number $m \ne n$ with $m = s(n)$ and $n = s(m)$. In this section, we present a proof of the following slight weakening of Theorem 9.7. We largely follow the original argument of Pomerance [**Pom81**], but at various points employ cruder, more easily established estimates.

Theorem 9.20. *As $x \to \infty$, the number of amicable numbers $n \le x$ is $o(Z)$, where*

$$Z := x/\exp\left(\frac{1}{250}(\log x)^{1/3}\right). \tag{9.20}$$

It is natural to wonder how close (9.20) is to the truth. The estimate of Theorem 9.20 saves an arbitrary power of $\log x$ over the trivial upper bound of x, confirming a conjecture of Erdős from [**Erd55a**]. (In particular, Theorem 9.20 implies that the sum of the reciprocals of the amicable numbers converges.) But it does not save a power of x, and perhaps it is impossible to do so: Erdős conjectured that the number of amicable numbers in $[1, x]$ is eventually larger than $x^{1-\epsilon}$, for any fixed $\epsilon > 0$. See [**GPtR04**, §6] for the empirical data up to 10^{13}.

Let $P(n)$ denote the largest prime factor of n, where we set $P(1) = 1$. Recall that n is said to be *y-smooth* if $P(n) \le y$, and that $\Psi(x, y)$ denotes the number of y-smooth $n \le x$. Set

$$\Psi'(x, y) := \#\{n \le x : P(\sigma(n)) \le y\}.$$

The proof of Theorem 9.20 depends crucially on upper estimates for Ψ and Ψ'. In Exercise 3.34, we showed that for all $x \ge y \ge 2$,

$$\Psi(x, y) \ll xe^{-u/2}\log y, \quad \text{where} \quad u := \frac{\log x}{\log y}. \tag{9.21}$$

We now establish a similar upper bound for $\Psi'(x, y)$ (cf. [**Pom81**, pp. 185–186], [**BFPS04**, §3]).

Lemma 9.21. *For all $x \geq y \geq 3$, we have*

$$\Psi'(x,y) \ll xy^5 e^{-u/2}.$$

Here the implied constants are absolute, and u is defined as in (9.21)*.*

Proof. As in Exercise 3.34, we employ "Rankin's trick." If $\sigma(n)$ is y-smooth, then $p+1$ is y-smooth for every prime p for which $p \parallel n$. Hence, for each $\sigma > 0$,

$$\Psi'(x,y) = \sum_{\substack{n \leq x \\ P(\sigma(n)) \leq y}} 1 \leq x^\sigma \sum_{\substack{n \leq x \\ p \parallel n \Rightarrow P(p+1) \leq y}} \frac{1}{n^\sigma}.$$

Assume now that $\sigma \geq \frac{1}{2} + \frac{1}{100}$ (say). Viewing n as the product of a squarefull component and a squarefree part, we see that

$$\sum_{\substack{n \leq x \\ p \parallel n \Rightarrow P(p+1) \leq y}} \frac{1}{n^\sigma} \leq \prod_p \left(1 + \frac{1}{p^{2\sigma}} + \frac{1}{p^{3\sigma}} + \dots\right) \prod_{p\colon P(p+1) \leq y} \left(1 + \frac{1}{p^\sigma}\right).$$

Our condition on σ shows that the first factor here is absolutely bounded:

$$\log \prod_p \left(1 + \frac{1}{p^{2\sigma}} + \frac{1}{p^{3\sigma}} + \dots\right) \leq \sum_p \sum_{k \geq 2} \frac{1}{p^{k\sigma}} \ll \sum_p \frac{1}{p^{2\sigma}} \ll 1.$$

Moreover,

$$\log \prod_{p\colon P(p+1) \leq y} \left(1 + \frac{1}{p^\sigma}\right) \leq \sum_{p\colon P(p+1) \leq y} \frac{1}{p^\sigma}.$$

Collecting what we have shown so far gives

$$\Psi'(x,y) \ll x^\sigma \exp\left(\sum_{p\colon P(p+1) \leq y} \frac{1}{p^\sigma}\right). \tag{9.22}$$

As in Exercise 3.34, we choose $\sigma = 1 - \frac{1}{2\log y}$; since $y \geq 3$, our lower bound condition on σ holds. We have $p^{-\sigma} - (p+1)^{-\sigma} \ll p^{-1-\sigma} \ll p^{-3/2}$, and so

$$\sum_{p\colon P(p+1) \leq y} \frac{1}{p^\sigma} \leq \sum_{p\colon P(p+1) \leq y} \frac{1}{(p+1)^\sigma} + O(1). \tag{9.23}$$

Also,

$$\sum_{p\colon P(p+1) \leq y} \frac{1}{(p+1)^\sigma} \leq \sum_{m\colon P(m) \leq y} \frac{1}{m^\sigma} = \prod_{p \leq y} \left(1 + \frac{1}{p^\sigma} + \frac{1}{p^{2\sigma}} + \dots\right). \tag{9.24}$$

This last product was shown to be $\ll \log y$ in the course of Exercise 3.34. We now prove a sharper upper bound of $e^{\frac{5}{6}+\gamma}(\log y) + O(1)$. Since $e^{\frac{5}{6}+\gamma} < 5$, the lemma then follows from (9.22), (9.23), and (9.24), after observing that $x^\sigma = xe^{-u/2}$.

To prove the estimate for the product, write

$$\frac{\prod_{p\le y}\left(1+\frac{1}{p^\sigma}+\frac{1}{p^{2\sigma}}+\dots\right)}{\prod_{p\le y}\left(1+\frac{1}{p}+\frac{1}{p^2}+\dots\right)} = \prod_{p\le y}\left(1+\frac{1-p^{\sigma-1}}{p^\sigma-1}\right) \le \exp\left(\sum_{p\le y}\frac{1-p^{\sigma-1}}{p^\sigma-1}\right).$$

Since $p^{\sigma-1} = \exp\left(-\frac{\log p}{2\log y}\right) \ge 1-\frac{\log p}{2\log y}$, we have

$$\sum_{p\le y}\frac{1-p^{\sigma-1}}{p^\sigma-1} \le \frac{1}{2\log y}\sum_{p\le y}\frac{\log p}{p^\sigma-1}.$$

For $p\le y$ we have $p^\sigma \ge p\cdot\exp(-1/2) > 0.606p$. Since $0.606p-1 > 3p/5$ for large p, we find that

$$\frac{1}{2\log y}\sum_{p\le y}\frac{\log p}{p^\sigma-1} \le \frac{1}{2\log y}\left(\sum_{p\le y}\frac{\log p}{3p/5}+O(1)\right) = \frac{5}{6}+O(1/\log y),$$

using (3.17). Collecting our estimates and applying Mertens's second theorem (see Theorems 3.15 and 3.17), we obtain that

$$\begin{aligned}\prod_{p\le y}\left(1+\frac{1}{p^\sigma}+\frac{1}{p^{2\sigma}}+\dots\right) &\le e^{5/6}\left(\prod_{p\le y}\left(1-\frac{1}{p}\right)^{-1}\right)(1+O(1/\log y))\\ &= e^{\frac{5}{6}+\gamma}\log y+O(1),\end{aligned}$$

as asserted. □

We will also use the following result of Gronwall, whose proof is left as Exercise 11.

Lemma 9.22. *The maximal order of $\sigma(n)$ is $e^\gamma n\log\log n$. More precisely,*

$$\limsup_{n\to\infty}\frac{\sigma(n)}{n\log\log n} = e^\gamma.$$

In what follows, we use n to denote an amicable number and m to denote $s(n)$, so that $\{n,m\}$ is an amicable pair. For large x, we set

$$y := \exp((\log x)^{1/3}), \quad \text{and} \quad Y := \exp(50(\log x)^{2/3}).$$

Lemma 9.23. *Let Z be defined by (9.20). As $x\to\infty$, all but $o(Z)$ amicable numbers $n\le x$ satisfy all of the following:*

(i) *$P(n) > Y^2$ and $P(m) > Y^2$,*

(ii) *the largest squarefull divisor of n or m is at most y,*

(iii) *we have $P(\gcd(n,\sigma(n))) \le 2y$ and $P(\gcd(m,\sigma(m))) \le 2y$,*

(iv) *$n/P(n) > Y$ and $m/P(m) > Y$,*

(v) *with $n' := n/P(n)$ and $m' := m/P(m)$, we have $P(\sigma(n')) > y^2$ and $P(\sigma(m')) > y^2$.*

Proof. We start by observing that n and m play nearly symmetric roles, each determining the other through the equations $s(n) = m$ and $s(m) = n$. However, while we know that $n \le x$, we are not assuming an upper bound on m. This is remedied by an appeal to Lemma 9.22, which shows (assuming, as we may, that x is large) that $m = s(n) \le 2x \log\log x$.

From the above remarks, we see that the number of exceptional n for which (i) fails is at most twice the smooth number count $\Psi(2x\log\log x, Y^2)$. Now

$$\frac{\log(2x\log\log x)}{\log(Y^2)} \ge \frac{\log x}{2\log Y} = \frac{1}{100}(\log x)^{1/3},$$

and so (9.21) gives that

$$\Psi(2x\log\log x, Y^2) \ll \frac{(x\log\log x)(\log x)^{2/3}}{\exp(\frac{1}{200}(\log x)^{1/3})} = o(Z).$$

Turning to (ii), the number of exceptional n is at most twice the count of integers $\le 2x\log\log x$ with a squarefull divisor $> y$. The number of squarefull integers d up to t is $\ll \sqrt{t}$, for all $t \ge 1$ (cf. Exercise 1.10). So by partial summation, the count of exceptional n is

$$\ll 2x\log\log x \sum_{\substack{d>y \\ d \text{ squarefull}}} \frac{1}{d} \ll 2x(\log\log x)y^{-1/2} = \frac{2x\log\log x}{\exp(\frac{1}{2}(\log x)^{1/3})} = o(Z).$$

Suppose now that (i) and (ii) hold but that (iii) fails. Then with either $N = n$ or $N = m$, we have that $N \le 2x\log\log x$ and that there is some prime $p > 2y$ dividing both N and $\sigma(N)$. Since $p \mid \sigma(N)$, either $p \mid \sigma(\ell)$ for some prime $\ell \parallel N$, or $p \mid \sigma(\ell^e)$ for some proper prime power $\ell^e \parallel N$. In the second case,

$$2\ell^e > \ell^e + \ell^{e-1} + \cdots + 1 = \sigma(\ell^e) \ge p > 2y,$$

so $\ell^e > y$, contradicting (ii). So assume we are in the first case. Then $p \mid \ell+1$ and $p\ell \mid N$. Hence, the number of possibilities for N is bounded above by

$$2x\log\log x \sum_{\substack{p\ell \le 2x\log\log x \\ p>2y \\ \ell \equiv -1 \pmod{p}}} \frac{1}{p\ell} \le 2x\log\log x \sum_{2y<p\le 2x\log\log x} \frac{1}{p} \sum_{\substack{\ell \le 2x\log\log x \\ \ell \equiv -1 \pmod{p}}} \frac{1}{\ell}.$$

Writing $\ell+1=pk$ in the inner sum, we have that $k=\frac{\ell+1}{p}<2x\log\log x$, and so the inner sum is

$$\leq \sum_{\substack{\ell\leq 2x\log\log x\\ \ell\equiv -1 \pmod{p}}} \frac{2}{\ell+1} \leq \frac{2}{p}\sum_{k<2x\log\log x}\frac{1}{k} \ll \frac{\log x}{p},$$

which with the above shows that the number of possible N is

$$\ll x(\log x)(\log\log x)\sum_{p>2y}\frac{1}{p^2} \ll \frac{x(\log x)(\log\log x)}{y} = o(Z).$$

But the number of possibilities for n is at most twice that for N.

Suppose that all of (i)–(iii) hold. Write $p=P(n)$ and $q=P(m)$, and let $n=pn'$ and $m=qm'$. Our task is to show that both $n',m'\geq Y$, apart from a negligible set of exceptional n. Observe that from (i), we have

$$n'\leq x/Y^2, \quad \text{and} \quad m'\leq 2x(\log\log x)/Y^2. \tag{9.25}$$

We claim that the numbers n' and m' completely determine the pair n and m. If the claim is proved, the result follows: If $n'\leq Y$, the claim and (9.25) show that the number of remaining possibilities for the pair $\{n,m\}$ is at most

$$Y\cdot(2x\log\log x)/Y^2 = 2x(\log\log x)/Y = o(Z),$$

and similarly, if $m'\leq Y$, then the number of possibilities for the pair $\{n,m\}$ is at most

$$Y\cdot(x/Y^2) = x/Y = o(Z).$$

To prove the claim, notice that from (i) and (ii), we have that $p\nmid n'$ and $q\nmid m'$. Hence,

$$\begin{aligned} pn' = n = s(m) = \sigma(m) - m &= \sigma(qm') - qm' \\ &= (q+1)\sigma(m') - qm' = qs(m') + \sigma(m'). \end{aligned}$$

Similarly,

$$qm' = ps(n') + \sigma(n').$$

This gives us a system of two equations in the variables p' and q' with coefficients determined by n' and m', namely

$$\begin{aligned} pn' - qs(m') &= \sigma(m'), \\ ps(n') - qm' &= -\sigma(n'). \end{aligned}$$

Multiply the first equation by m', the second by $s(m')$, and subtract the second from the first to find that

$$p(n'm' - s(n')s(m')) = m'\sigma(m') + s(m')\sigma(n').$$

The right-hand side is positive, which means both factors on the left are nonzero. Thus,

$$p = \frac{m'\sigma(m') + s(m')\sigma(n')}{n'm' - s(n')s(m')}$$

is determined by m' and n'. Hence, $n = pn'$ is also determined, as is $m = s(n)$. This completes the treatment of (iv).

Finally, suppose that (i)–(iv) hold and (v) fails. Then either $P(\sigma(n')) \le y^2$ or $P(\sigma(m')) \le y^2$. Suppose it is the former. Write $n = pn'$ with $p = P(n)$, as in the treatment of condition (iv). We know from (iv) that $n' \ge Y$, and so $p = n/n' \le x/Y$. For each fixed p, the number of corresponding n is at most $\Psi'(x/p, y^2)$. When $p \le x/Y$,

$$\frac{\log(x/p)}{\log(y^2)} \ge \frac{\log Y}{\log(y^2)} = 25(\log x)^{1/3},$$

and so by Lemma 9.21,

$$\begin{aligned}\Psi'(x/p, y^2) &\ll (x/p)(y^2)^5 \exp(-12.5(\log x)^{1/3}) \\ &= x \exp(-2.5(\log x)^{1/3})/p.\end{aligned}$$

Summing over p shows that the number of these n is $o(Z)$. The case when $P(\sigma(m')) \ge y^2$ is similar, but we sum the quantity $\Psi'(2x(\log\log x)/q, y^2)$ over primes $q \le 2x(\log\log x)/Y$. Just as before, we obtain a contribution that is $o(Z)$. This completes the proof of the lemma. $\square$

Proof of Theorem 9.20. It remains to estimate the number of amicable numbers $n \le x$ obeying conditions (i)–(v) of Lemma 9.23. By doubling the count and extending the range up to $2x \log\log x$, we can assume that

$$P(n) \ge P(m). \tag{9.26}$$

Write $n = pn'$, where $p = P(n)$. By (v), there is a prime $r > y^2$ dividing $\sigma(n')$. Consequently, $r \mid \sigma(\ell^e)$ for some prime power $\ell^e \parallel n'$. If $e > 1$, then ℓ^e is a squarefull divisor of n with $\ell^e > \frac{1}{2}\sigma(\ell^e) \ge \frac{r}{2} > \frac{1}{2}y^2$, contradicting (ii). Hence $e = 1$, $\ell \parallel n'$, and $\ell \equiv -1 \pmod{r}$.

From (i) and (ii), we have that $p \nmid n'$; hence,

$$r \mid \sigma(n') \mid \sigma(n')\sigma(p) = \sigma(n) = n + m = \sigma(m).$$

Arguing as above, we obtain the existence of a prime $\ell' \parallel m$ with $\ell' \equiv -1 \pmod{r}$. Moreover, since ℓ' divides $m = s(pn')$, we have

$$s(n')p + \sigma(n') \equiv 0 \pmod{\ell'}. \tag{9.27}$$

If ℓ' divides $s(n')$, then (9.27) forces

$$\ell' \mid \sigma(n') \mid \sigma(n) = \sigma(m),$$

so that $\ell' \mid \gcd(m, \sigma(m))$, contradicting (iii). (Note that $\ell' > r > y^2$.) So $\ell' \nmid s(n')$, and (9.27) uniquely determines the residue class of p modulo ℓ', say $p \equiv a(n', \ell') \pmod{\ell'}$.

Putting all of this together, we find that the number of n under consideration is

$$\ll \sum_{r > y^2} \sum_{\substack{\ell \equiv -1 \pmod r \\ \ell \le x}} \sum_{\substack{n' \equiv 0 \pmod \ell \\ n' \le x}} \sum_{\substack{\ell' \equiv -1 \pmod r \\ \ell' \le 2x \log\log x}} \sum_{\substack{p \equiv a(n', \ell') \pmod{\ell'} \\ p \le 2x(\log\log x)/n' \\ p \ge \ell'}} 1.$$

(Note that the final condition in the last sum uses our assumption (9.26).) Crude estimates (ignoring the primality conditions) show that

$$\begin{aligned}\sum_r \sum_\ell \sum_{n'} \sum_{\ell'} \sum_p 1 &\ll \sum_r \sum_\ell \sum_{n'} \sum_{\ell'} \frac{x \log\log x}{\ell' n'} \\ &\ll \sum_r \sum_\ell \sum_{n'} \frac{x(\log\log x)(\log x)}{r n'} \ll \sum_r \sum_\ell \frac{x(\log\log x)(\log x)^2}{r\ell} \\ &\ll \sum_r \frac{x(\log\log x)(\log x)^3}{r^2} \ll \frac{x(\log\log x)(\log x)^3}{y^2} = o(Z).\end{aligned}$$

This completes the proof of Theorem 9.20. □

Notes

The first chapter of Dickson's *History of the Theory of Numbers* [**Dic66**] is a thorough compendium of results on perfect numbers and related matters, covering antiquity to the early twentieth century. Many of the more recent results (up to about 2003) are catalogued in the two-volume *Handbook of Number Theory*; see, in particular, [**SC04**, Chapter 3] and [**SMC06**, Chapter 1].

Our Theorem 9.4 is a special case of Wirsing's original theorem. What Wirsing actually shows in [**Wir59**] is that for any α, the number of $n \le x$ with

$$\sigma(n)/n = \alpha \tag{9.28}$$

is at most $x^{W/\log\log x}$, for an absolute constant $W > 0$ (and all $x \ge 3$). The complete uniformity in α is frequently useful in applications. To give one example, it is simple to deduce from Wirsing's result that the number of multiply perfect $n \le x$ is at most $x^{W'/\log\log x}$ for some absolute constant $W' > 0$ and all $x > 3$; here the number n is said to be *multiply perfect* if n divides $\sigma(n)$. Some relatives of Wirsing's theorem are considered in [**Pol11a**], [**PP11**]; the former paper studies how often $\gcd(n, \sigma(n))$ is large, and the latter examines how often n and $\sigma(n)$ share the same set of distinct prime factors.

The following elegant generalization of Dickson's finiteness theorem was proved by Kanold [**Kan56**]: *Call a solution n to* (9.28) primitive *if n does not have a unitary divisor which is an even perfect number.*[3] *For each $\alpha \in \mathbf{Q}$ and $k \in \mathbf{N}$, there are only finitely many primitive solutions n to* (9.28) *with exactly k distinct prime factors.* In [**Pom77a**], Pomerance shows how Baker's estimates for linear forms in logarithms can be used to obtain an effective version of Kanold's result. Borho [**Bor74a, Bor74b**] and Artjuhov [**Art75**] have obtained results for amicable pairs which are cognate to Dickson's theorem.

In the theory of probability, a function $F\colon \mathbf{R} \to \mathbf{R}$ is called a *distribution function* if F is nondecreasing, right-continuous,

$$\lim_{u\to-\infty} F(u) = 0 \quad \text{and} \quad \lim_{u\to\infty} F(u) = 1.$$

We say that an arithmetic function f *has a distribution function* if there is a distribution function D_f (say) with the property that

$$\lim_{x\to\infty} \frac{\#\{n \le x : f(n) \le u\}}{x} = D_f(u)$$

whenever u is a point of continuity of D_f. The result of Davenport recorded in Theorem 9.5 is an early precursor of the following theorem of Erdős ([**Erd35b, Erd37, Erd38**]) & Wintner [**EW39**]:

★ **Theorem 9.24.** *A real-valued additive arithmetic function $f(n)$ has a distribution function if and only if all of the three series*

$$\sum_{|f(p)|>1} \frac{1}{p}, \qquad \sum_{|f(p)|\le 1} \frac{f(p)}{p}, \qquad \sum_{|f(p)|\le 1} \frac{f(p)^2}{p}$$

converge. If all three series converge, then the distribution function of f is continuous if and only $\sum_{f(p)\neq 0} p^{-1}$ diverges.

Of course $\sigma(n)/n$ is multiplicative, not additive, but one can recover Theorem 9.5 by applying Theorem 9.24 to $\log(\sigma(n)/n)$. The Erdős–Wintner result can be considered the first general theorem in the subject that has come to be known as "probabilistic number theory".

Theorem 9.17 says that for most natural numbers n, the aliquot sequence $n, s(n), s(s(n)), \dots$ initially grows almost as fast as a geometric progression with common ratio $s(n)/n$. While technical, our proof from §5 can be summarized neatly in one sentence: For most n, the first few terms of the aliquot sequence at n have all of the same small prime factors, while for most m,

[3] Recall that a divisor m of n is said to be *unitary* if $\gcd(m, n/m) = 1$.

the ratio $\sigma(m)/m$ is "nearly determined" by the small prime factors of m. This summary might lead one to expect that one should also have the statement analogous to Theorem 9.17 where the inequality points in the opposite direction. This was conjectured by Erdős [**Erd76**]:

Conjecture 9.25. *Let K be a natural number, and let $\epsilon > 0$. For almost all natural numbers n,*

$$\frac{s_{k+1}(n)}{s_k(n)} < \frac{s(n)}{n} + \epsilon$$

for all $1 \leq k \leq K$.

This conjecture has proved surprisingly difficult and remains open in general. For a proof when $K = 1$, see the paper [**EGPS90**] of Erdős et al.

Exercises

1. (Lucas) The *digital root* of a natural number n is defined by summing the (decimal) digits of n, then the digits of the result, then the digits of the new result, etc., until reaching a single digit. Prove that every even perfect number $n > 6$ has digital root 1.

2. Identify the flaw in the following "proof" that all perfect numbers n are even: Starting with $2n = \sum_{d|n} d$, we can apply Möbius inversion to find that
$$n = \sum_{d|n} \mu(n/d)(2d) = 2\left(\sum_{d|n} \mu(n/d)d\right),$$
which is visibly even.

3. (Thābit ibn Qurra) Suppose that for the integer $k > 1$, all three of $p := 3 \cdot 2^{k-1} - 1$, $q := 3 \cdot 2^k - 1$, and $r := 9 \cdot 2^{2k-1} - 1$ are prime numbers. Show that $n := 2^k pq$ and $m := 2^k r$ form an amicable pair. Explain why one expects this rule to yield only finitely many amicable pairs.

† 4. (Ewell [**Ewe80**]) Suppose that n is an odd perfect number. Write $n = p^e \prod_{i=1}^r p_i^{2e_i} \prod_{j=1}^s q_j^{2f_j}$, where $p, p_1, \dots, p_r, q_1, \dots, q_s$ are distinct primes, $p \equiv e \equiv 1 \pmod 4$, each $p_i \equiv 1 \pmod 4$, and each $q_j \equiv 3 \pmod 4$. Show that $p \equiv e \pmod 8$ precisely when there are an even number of odd e_i.

† 5. (Starni [**Sta91**]) Suppose that n is an odd perfect number. Write $n = p^e \prod_{i=1}^k p_i^{2e_i}$, as in Euler's theorem (Theorem 9.2).
   (a) Show that if $p_i \equiv 3 \pmod 4$ for all $1 \le i \le k$, then $\frac{1}{2}\sigma(p^e)$ is composite.
   (b) Show that if $p_i \equiv 1 \pmod 4$ for all $1 \le i \le k$, then $p \equiv e \pmod 8$.

† 6. (Starni [**Sta93**]) Let n be an odd perfect number, say $n = p^e m^2$, where $\gcd(p, m) = 1$ and $p \equiv e \equiv 1 \pmod 4$. Show that if $e + 2$ is a prime which does not divide $p - 1$, then $e + 2$ divides m^2. For example, if $13^{17} m^2$ is perfect (with $13 \nmid m$), then 19 divides m.

† 7. (Slowak [**Slo99**]) Let n be an odd perfect number, say $n = p^e m^2$, where $\gcd(p, m) = 1$ and $p \equiv e \equiv 1 \pmod 4$. Show that p^e is a proper divisor of $\sigma(m^2)$.

8. (Touchard [**Tou53**]) Show that if n is an odd perfect number, then either $n \equiv 1 \pmod{12}$ or $n \equiv 9 \pmod{36}$.

9. (Luca [**Luc99**]) Prove that two consecutive natural numbers cannot both be perfect.

† 10. (Continuation) Show that if m and n form an amicable pair of opposite parity, then the odd member is a square and the even member is a square or twice a square. Then show that there is no amicable pair of the form $\{2n, 2n+1\}$.

Remark. It is an open problem to show that there are no amicable pairs of the form $\{2n-1, 2n\}$.

11. (Gronwall [**Gro13**]) Show that $\limsup_{n\to\infty} \frac{\sigma(n)}{n\log\log n} = e^{\gamma}$, where γ is the Euler–Mascheroni constant.

Remark. A handsome theorem of Robin [**Rob84**] asserts that the Riemann Hypothesis (see p. 109) holds if and only if $\sigma(n) < e^{\gamma} n \log\log n$ for all $n > 5040$.

12. Suppose that $\mathscr{C}$ is a sociable cycle (as defined on p. 279). Put $g := \gcd(\mathscr{C})$ and $G := \gcd(\sigma(\mathscr{C}))$, where $\sigma(\mathscr{C})$ is the set of numbers of the form $\sigma(m)$ with $m \in \mathscr{C}$. Prove that g always divides G, and that whenever $\mathscr{C}$ has odd length, G divides $2g$. (This is the key observation behind the proof of the bound (9.19).)

13. (Salié [**Sal53**]) Let n be an abundant or perfect number with k distinct prime factors, and let q be its least prime divisor. Let q' be the kth prime exceeding q. Observing that

$$2 \le \frac{\sigma(n)}{n} < \prod_{p\mid n} \frac{p}{p-1} \le \prod_{q\le p<q'} \left(1-\frac{1}{p}\right)^{-1},$$

deduce from Mertens' theorem that $q \ll \sqrt{k\log k}$, where the implied constant is absolute. Some related results can be found in the paper [**Nor61**] of Norton.

14. (Yamada [**Yam07**]; see also Fletcher et al. [**FNO**]) Let E be a finite, nonempty set of natural numbers. Let n be an odd perfect number, and suppose that every even exponent appearing in the canonical prime factorization of n belongs to the set $\{2e : e \in E\}$. Put $\mathscr{Q} := \{q \text{ prime} : q \equiv 1 \pmod{\prod_{e\in E}(2e+1)}, q \nmid 2n\}$.
   (a) Suppose $e \in E$ and that $p^{2e} \parallel n$ for the prime p. Show that for each $q \in \mathscr{Q}$,
   $$1 + p + p^2 + \cdots + p^{2e} \not\equiv 0 \pmod{q}.$$
   (b) Show that the polynomial $1 + T + T^2 + \cdots + T^{2e}$ has exactly $2e$ distinct roots modulo q, for each $q \in \mathscr{Q}$.
   (c) Let $x \ge 3$. Show that for each $e \in E$, the number of primes $p \le x$ for which $p^{2e} \parallel n$ is $\ll x/(\log x)^{1+c}$, where $c > 0$, and where both c and the implied constant depend only on E (and not on n). *Hint:* Use sieve methods and the results of (a) and (b).

(d) Let n' be the product of the prime powers with even exponent which exactly divide n. Show that $\sigma(n')/n' \geq 8/5$. Deduce that for some choice of $e \in E$,

$$(8/5)^{1/\#E} \leq \prod_{p:p^{2e}\|n} \left(1+\frac{1}{p-1}\right).$$

(e) Combining the results of (c) and (d), show that if p is the smallest prime appearing to an even exponent in n, then p is bounded above by a constant depending only on E.

15. (Anderson [**And74**]) Show that if $\sigma(n)/n = 5/3$, then n is coprime to 10. Deduce that in this case $5n$ is an odd perfect number.

16. (Anderson, ibid.)
    (a) Suppose $1 \leq b \leq a < \sigma(b)$ and $\gcd(a,b) = 1$. Prove that the rational number a/b is not of the form $\sigma(n)/n$ for any $n \in \mathbf{N}$.
    (b) Show that the rational numbers not of the form $\sigma(n)/n$ are dense in $[1,\infty)$.

    Further results related to those of Exercises 15 and 16 may be found in [**Wei00**], [**Hol06**], and [**SH07**].

† 17. Call the natural number n *superperfect* if $\sigma(\sigma(n)) = 2n$.
    (a) (Suryanarayana [**Sur69**]) Show that if n is an even superperfect number, then $n = 2^k$ for some $k \in \mathbf{N}$ for which $2^{k+1}-1$ is prime. Conversely, show that any n of this form is superperfect.
    (b) (Kanold [**Kan69b**]) Show that if n is an odd superperfect number, then n is a perfect square. (No examples of odd superperfect numbers are known.)

18. (Mąkowski [**Mąk62**]) Show that 28 is the only even perfect number of the form n^3+1 and the only even perfect number of the form n^n+1.

† 19. (Continuation; Montgomery & Selfridge [**MS92**]) Prove that 28 is the only perfect number of the form n^n+1. *Hint:* Use Touchard's result (Exercise 8) to prove that if n^n+1 is odd and perfect, then $6 \mid n$.

    Remark. Probably 28 is also the only perfect number of the form n^3+1. That there are only finitely many perfect numbers of this shape would follow from the *abc*-conjecture and the main result of [**LP10**].

† 20. (Wall [**Wal81**])
    (a) Prove that for every $k \in \mathbf{N}$, there are infinitely many blocks of k consecutive natural numbers all of which are abundant.
    (b) Show that there are infinitely many blocks of 5 consecutive numbers all of which are deficient and that 5 cannot be replaced with any larger number.

† 21. Show that every sufficiently large natural number can be written as a sum of two abundant numbers and as a sum of two deficient numbers.

22. (Pomerance [unpublished], te Riele [**tR76**, Chapter 7]) The *Dedekind ψ-function* is defined by setting $\psi(n) := n\prod_{p|n}(1+1/p)$ for every natural number n. (Thus $\psi(n) \le \sigma(n)$ for all n, with equality precisely when n is squarefree.) Show that the analogue of the Catalan–Dickson conjecture fails for $s^*(n) := \psi(n) - n$. That is, there are natural numbers n for which the sequence $n, s^*(n), s^*(s^*(n)), \ldots$ is unbounded. *Hint:* Try $n = 318$.

23. (Alaoglu & Erdős [**AE44**]) Prove that for each fixed $\epsilon > 0$, the inequality $\varphi(\sigma(n)) < \epsilon n$ holds on a set of n of density 1.

24. (Kanold [**Kan69a**], see also Borho [**Bor70**]) It is not known whether an amicable number can possess only a single prime factor (and so be a prime or prime power). Show that the number of amicable numbers of this type not exceeding x is $O_\epsilon((\log x)^{1+\epsilon})$ as $x \to \infty$, for each $\epsilon > 0$.

25. (a) (Dirichlet) Show that $\frac{\sigma(n)}{n}$ has mean value $\frac{\pi^2}{6}$. In other words, prove that $\frac{1}{x}\sum_{n\le x}\frac{\sigma(n)}{n} \to \frac{\pi^2}{6}$ as $x \to \infty$.
    (b) (Erdős [**Erd51**]) Prove that $\frac{\sigma(2^n-1)}{2^n-1}$ possesses a (finite) mean value. *Hint:* Use the result of Exercise 6.23(c).

26. (Bojanić [**Boj54**]) Show that $\frac{\sigma(2^p-1)}{2^p-1} \to 1$ as $p \to \infty$ through prime values.

27. (Luca [**Luc00a**]) Let $F_m = 2^{2^m} + 1$ be the mth Fermat number. Show that $s(F_m) \ll mF_m/2^m$ for $m \ge 1$. Combining this with the result of Exercise 11, prove that only finitely many Fermat numbers F_m are members of an amicable pair. (With a bit of extra work, one can show that there are no such numbers.)

† 28. (Luca [**Luc06**, Problem 171]) Call the natural number n *multiply perfect* if n divides $\sigma(n)$. Show that for each fixed B, there are only finitely many multiply perfect numbers all of whose prime factors are bounded by B.

† 29. (Pomerance [**Pom93**]) Prove that $n!$ is multiply perfect for only finitely many n. (It can be shown that $n = 1, 3$, and 5 are the only such n.) *Hint:* One argument starts by showing that $v \ll n/\log n$ as $n \to \infty$, where $v = v(n)$ is defined by the relation $2^v \parallel \sigma(n!)$.

    Remark. A plausible strengthening of the result of this exercise was suggested by Erdős: It is not hard to check that as $n \to \infty$, we have $\sigma(n!)/n! \sim e^\gamma \log\log n!$ (cf. Exercise 11). Erdős's conjecture is that for each $\epsilon > 0$, there are only finitely many multiply perfect m with $\sigma(m)/m > \epsilon \log\log m$.

30. A natural number m is called *untouchable* if it is not of the form $s(n)$ for any $n \in \mathbf{N}$. The sequence of untouchable numbers begins $2, 5, 52, 88, 96, 120, 124, 146, \dots$.
    (a) Prove that $s(n) > \sqrt{n}$ for every composite number n. Using this inequality (or not) check that 2 and 5 are both untouchable.
    (b) Show that if every even number $m \geq 8$ is the sum of two distinct primes (a conjecture strengthening Goldbach's), then 5 is the only odd untouchable number.

31. (Continuation; Erdős [**Erd73**], see also [**BL05**]) We now show that a positive proportion of natural numbers are untouchable.

    Let M be a fixed even natural number. We consider the inequality

$$(9.29) \qquad s(n) \leq x, \quad \text{with the constraint} \quad s(n) \equiv 0 \pmod{M}.$$

    (a) Show that the number of odd n for which (9.29) holds is $\ll x/\log x$ as $x \to \infty$. *Hint*: $\sigma(n)$ is odd only if n is a perfect square.
    (b) Show that the number of solutions to (9.29) in even numbers n not divisible by M is $o(x)$.
    (c) Show that the number of solutions to (9.29) in numbers n which are divisible by M is at most αx, where $\alpha := (\sigma(M) - M)^{-1}$.
    (d) Combining the results of (a)–(c), deduce that the number of solutions to (9.29) is $\leq (\alpha + o(1))x$.
    (e) Taking $M = 12$, show that at least $(\frac{1}{48} + o(1))x$ natural numbers $n \leq x$ are untouchable.

    Let δ denote the lower density of the untouchable numbers. The inequality $\delta \geq 1/48$ of part (e) was improved to $\delta > 0.0324$ by te Riele [**tR76**, Corollary 9.2] and more recently to $\delta > 0.0602$ by Chen & Zhao [**CZ11**].

† 32. Show that for each fixed natural number k and rational number α, the set of natural numbers n with $s_k(n) = \alpha n$ has density zero.

† 33. (Banks et al. [**BFPS04**]) Show that there are infinitely many natural numbers n for which $\sigma(n)$ is a perfect square. This had been conjectured by Sierpiński [**Sie88**, p. 179]. *Hint:* View the group $\mathbf{Q}^\times/(\mathbf{Q}^\times)^2$ as an $\mathbf{F}_2$-vector space, with a basis given by the images of -1 and the rational primes. Show that there are many linear dependencies in $\mathbf{Q}^\times/(\mathbf{Q}^\times)^2$ among the shifted primes $p+1$.

† 34. (Pomerance [**Pom77b**]) Show that $\tau(n)$ divides $\sigma(n)$ for almost all natural numbers n. That is, the arithmetic mean of the divisors of n is almost always an integer.

    Remark. In [**BEPS81**], it is shown that the number of exceptional $n \leq x$ is $x \exp(-(2 + o(1))\sqrt{\log 2}\sqrt{\log\log x})$ as $x \to \infty$.

35. (Adapted from [**Luc06**, Problem 148]) Fill in the details in the following proof that the arithmetic mean of the distinct prime divisors of n is almost never an integer (i.e., is an integer only on a set of density zero):

    Let $n \leq x$. We can assume that the largest prime divisor $P(n)$ of n satisfies $P(n) > y$, where $y := x^{1/\log\log\log x}$, since the $n \leq x$ for which this fails make up a set of size $o(x)$ by Exercise 6.5. Write $n = Pm$, where $P = P(n)$. We can further assume $P \nmid m$, since otherwise n has a large square divisor, and such n are also rare. Finally, Exercise 3.24 allows us to assume that $\omega(n) \in [\log\log x - (\log\log x)^{2/3}, \log\log x + (\log\log x)^{2/3}]$. If the average of the prime divisors of n is an integer, this forces P to lie in a residue class, modulo $\omega(m)+1$, determined entirely by m. We now consider the number of possibilities for P corresponding to a given $m \leq x/y$. With $k := \omega(m) + 1$, the number of suitable $P \leq x/m$ is, by the Brun–Titchmarsh inequality (Theorem 7.2),

    $$\ll \frac{x/m}{\varphi(k)\log(x/(mk))} \ll \frac{x\log\log\log x}{m\varphi(k)\log x}$$
    $$\ll \frac{x(\log\log\log x)(\log\log\log\log x)}{m(\log\log x)(\log x)},$$

    where we use that $x/m \geq y$, that $k \approx \log\log x$, and that $\varphi(r) \gg r/\log\log r$ for all $r \geq 3$ (cf. Exercise 11). The result follows upon summing over the possibilities for m.

    Remark. For strengthenings of this result, see the papers of Banks et al. [**BGLS05**] and Kátai [**Kát07**].

36. (Erdős [**Erd46**]) In this exercise we investigate the rate at which $D(u) \to 1$ as $u \to \infty$, where $D(u)$ is the function of Theorem 9.5. We show that the density $1 - D(u)$ of those n for which $\sigma(n)/n > u$ is

$$1/\exp(\exp((e^{-\gamma} + o(1))u)). \tag{9.30}$$

The bulk of the proof (parts (a)–(d)) concerns the upper bound. Actually we prove a somewhat stronger result, namely that (9.30) is an upper bound for the upper density of the set of n with

$$\prod_{p|n}(1 - 1/p)^{-1} > u. \tag{9.31}$$

(Notice that the left-hand side of (9.31) majorizes $\sigma(n)/n$.)

(a) With p_i denoting the ith prime, let $k = k(u)$ be the smallest natural number with $\prod_{i=1}^{k}(1 - 1/p_i)^{-1} > u$. Prove that $\log p_k \sim e^{-\gamma}u$ as $u \to \infty$.

(b) Divide the solutions n of (9.31) into two classes:

(i) n has at least $r := \lfloor k/2 \rfloor$ prime factors not exceeding $4p_k$,

(ii) all other solutions to (9.31).

Show that class (i) has upper density at most $2^{\pi(4p_k)}/\prod_{p\le p_r} p$. Use (a) and the prime number theorem to verify that this bound has the form (9.30). Thus we may focus attention on class (ii).

(c) Use the minimality of k to show that if n is a solution to (9.31) belonging to class (ii), then (for large u)

$$\prod_{\substack{p\mid n\\ p>4p_k}} (1-1/p) \le \prod_{j=r+1}^{k-1} (1-1/p_j) < 1 - \frac{1}{4\log k}.$$

Deduce that for some natural number j,

$$\sum_{\substack{p\mid n\\ 4^j p_k < p \le 4^{j+1} p_k}} \frac{1}{p} > \frac{1}{2^j}\cdot\frac{1}{4\log k},$$

so that n is divisible by at least $N_j := \lceil 2^j \frac{p_k}{4\log k}\rceil$ distinct primes from the interval $I_j := (4^j p_k, 4^{j+1} p_k]$.

(d) Conclude that the upper density of class (ii) is, for large u, bounded above by $\sum_{j=1}^{\infty} \frac{1}{N_j!}\left(\sum_{p\in I_j} 1/p\right)^{N_j}$. Check that this is, in turn, bounded above by an expression of the shape (9.30).

(e) It remains only to prove that (9.30) is a lower bound for the density of the set of n with $\sigma(n)/n > u$. To accomplish this, construct a number

$$n_0 \le \exp(\exp((e^{-\gamma} + o(1))u))$$

with $\sigma(n_0)/n_0 > u$, and observe that $\sigma(n)/n > u$ whenever n_0 divides n. (Cf. Exercise 11.)

37. (Erdős, ibid.) Now we consider the decay of $D(u)$ to 0 as u tends down to 1. We show that the set of n with $\sigma(n)/n \le 1+\epsilon$ has density $\sim e^{-\gamma}/\log(\epsilon^{-1})$ as $\epsilon \downarrow 0$.

(a) Let A_ϵ be the set of natural numbers with no prime factor $< \epsilon^{-1}$. Show that if $\sigma(n)/n \le 1+\epsilon$, then $n \in A_\epsilon$.

(b) Show that A_ϵ has density $(1+o(1))e^{-\gamma}/\log(\epsilon^{-1})$ as $\epsilon \downarrow 0$.

(c) Prove that if ϵ is sufficiently small, then the following holds: If $n \in A_\epsilon$ but $\sigma(n)/n > 1+\epsilon$, then for some natural number j, n has at least j distinct prime factors from the interval $I_j := [4^{j-1}\epsilon^{-1}, 4^j\epsilon^{-1})$.

(d) For each natural number j, let E_j be the set of $n \in A_\epsilon$ with at least j distinct prime factors from I_j. Show that E_j has upper density at most

$$(1+o(1))\frac{1}{j!}\frac{e^{-\gamma}}{\log(1/\epsilon)}\left(\sum_{p\in I_j}\frac{1}{p}\right)^j.$$

(e) Show that $\bigcup_{j\geq 1} E_j$ has upper density at most

$$(1+o(1))\frac{e^{-\gamma}}{\log(1/\epsilon)}\sum_{j=1}^{\infty}\frac{1}{j!}\left(\sum_{p\in I_j}\frac{1}{p}\right)^j.$$

(f) Complete the proof by showing that the sum in (e) tends to zero as $\epsilon \downarrow 0$.

38. Suppose that f is a nonnegative-valued additive function for which
   (i) $f(p) \to 0$ as $p \to \infty$,
   (ii) $\sum_p f(p)$ diverges.

   Show that the image of f is dense in $[0, \infty)$. Taking $f(n) := \log \frac{\sigma(n)}{n}$, conclude that the set of rational numbers of the form $\sigma(n)/n$ is dense in $[1, \infty)$.
   (a) Use the result of Exercise 37 to show that the function $D(u)$ of Theorem 9.5 has an infinite right-sided derivative at $u = 1$.
   (b) Generalizing the result of (a), show that if $u = \sigma(n)/n$ for some n, then $D(u)$ has an infinite right-sided derivative at u. *Hint:* Consider numbers of the form nm, where $\sigma(m)/m$ is very close to 1.
   (c) Combining part (b) with Exercise 38, prove that $D(u)$ is strictly increasing on $[1, \infty)$.

† 39. (Suggested by C. Pomerance) Using the result of Exercise 37 (or otherwise), prove that the numbers from the set $\{\frac{s(n)}{n}\}_{n\geq 2}$ have vanishing geometric mean, i.e., that $(\prod_{j=2}^{N}\frac{s(n)}{n})^{\frac{1}{N-1}} \to 0$ as $N \to \infty$.

   Remark. Bosma & Kane [**BK10**] have considered the geometric mean of the same sequence extended only over *even* numbers n. (Note that when n is even, $s(n)/n \geq 1/2$.) They show that this mean exists and is strictly less than 1 (in fact, it is ≈ 0.969). This result, as well as the result of the exercise, is of use in heuristic arguments surrounding the Catalan–Dickson conjecture.

40. (Erdős & Turán [**Erd45**]; see also [**Dre72b**], [**Bat72**]) Let $S(x) := \#\{m \in \mathbf{N} : \sigma(m) \leq x\}$.
   (a) Show that $S(x)/x \to \int_1^\infty D(u)/u^2\, du$ as $x \to \infty$.
   (b) Show that the limit in (a) can also be written in the form

$$\prod_p\left(1-\frac{1}{p}\right)\left(1+\frac{1}{p+1}+\frac{1}{p^2+p+1}+\frac{1}{p^3+p^2+p+1}+\dots\right).$$

Hint: Let $r(n)$ denote the number of solutions m to $\sigma(m) = n$. Observe that $\sum_{n=1}^{\infty} \frac{r(n)}{n^s} = \sum_{m=1}^{\infty} \frac{1}{\sigma(m)^s} = \prod_p \left(\sum_{j=0}^{\infty} \frac{1}{\sigma(p^j)^s}\right)$ for real $s > 1$. Apply the Dirichlet–Dedekind theorem of Exercise 8.2.

41. Given a set of natural numbers S, let $M(S)$ be the set of natural numbers possessing a divisor from S, i.e.,

$$M(S) := \{m \in \mathbf{N} : n \mid m \text{ for some } n \in S\}.$$

For obvious reasons, $M(S)$ is referred to as the *set of multiples* of S. If $M(S)$ has an asymptotic density, we call S a *Besicovitch set*. This (somewhat confusing) terminology honors A. S. Besicovitch, who was the first to produce [**Bes34**] an example of a set S for which the asymptotic density of $M(S)$ does *not* exist.

(a) Show that if S is finite, then S is a Besicovitch set.

(b) For each $x > 0$, put $S_x := S \cap [1, x]$ and $S^x := S \setminus S_x$. Show that if the upper density of $M(S^x)$ tends to zero as $x \to \infty$, then S is Besicovitch, and in fact the density of $M(S)$ is the limit of the numbers d_x as $x \to \infty$, where d_x denotes the density of $M(S_x)$.

(c) Using the result of (b), show that if the sum of the reciprocals of the elements of S converges, then S is Besicovitch.

42. (Continuation; cf. Erdős [**Erd70**], Benkoski & Erdős [**BE74**]) A natural number n is said to be *pseudoperfect* if some subset of the proper divisors of n sums to n. For example, 104 is pseudoperfect, since

$$104 = 52 + 26 + 13 + 8 + 4 + 1.$$

(a) Say that the natural number n is *primitive pseudoperfect* if n is pseudoperfect and no proper divisor of n is pseudoperfect, and let S be the set of primitive pseudoperfect numbers. Show that the set of all pseudoperfect numbers is the set $M(S)$.

(b) Write $S = S_1 \cup S_2$, where $S_1 := \{n \in S : \Omega(n) > \frac{101}{100} \log\log n\}$ and $S_2 := S \setminus S_1$. Using the result of Exercise 3.26, show that the upper density of $M(S_1^x)$ tends to zero as $x \to \infty$.

(c) We now turn our attention to S_2. In this part and the next, we show that the sum of the reciprocals of the elements of S_2 converges, so that the upper density of $M(S_2^x)$ tends to zero as $x \to \infty$.

For a natural number $n > 1$, write $P(n)$ for the largest prime divisor of n. Using the result of Exercise 3.34, show that as $x \to \infty$, the number of $n \le x$ with $P(n) \le x^{1/(\log\log x)^2}$ is at most $x \exp\left(-(\frac{1}{2} + o(1))(\log\log x)^2\right)$.

(d) Suppose $n \in S_2 \cap [1, x]$ and $P(n) > x^{1/(\log\log x)^2}$. Put $p = P(n)$ and write $n = pn'$. Since n is pseudoperfect, we can write $n = d_1 + d_2 + \cdots + d_t$ (say), where $d_1, \ldots, d_t$ are proper divisors of n. By considering this decomposition modulo p and using that n is *primitive* pseudoperfect, show that p divides the sum of a nonempty collection of divisors of n'.

Deduce that for each fixed $n' \leq x^{1-1/(\log\log x)^2}$, the number of possibilities for p is $\ll 2^{\tau(n')} \log x$. Using the bound $\tau(n') \leq 2^{\Omega(n')}$, deduce that the number of elements of $S_2 \cap [1, x]$ with $P(n) > x^{1/(\log\log x)^2}$ is at most

$$x \exp(-(1 + o(1)) \log x/(\log\log x)^2).$$

Combining this with the result of (c), show that the sum of the reciprocals of the elements of S_2 converges.

(e) Combining (a)–(d), prove that S is Besicovitch, i.e., that the set of pseudoperfect numbers possesses an asymptotic density.

43. (Benkoski & Erdős, ibid.) It is clear that every pseudoperfect number n (as defined in Exercise 42) is nondeficient, i.e., perfect or abundant. A natural number n which is nondeficient but not pseudoperfect is called *weird*. The sequence of weird numbers begins $70, 836, 4030, 5830, \ldots$.

Suppose that n is a weird number.

(a) Show that there is no solution to

$$1 = \frac{1}{d_1} + \frac{1}{d_2} + \frac{1}{d_3} + \cdots + \frac{1}{d_t},$$

where $d_1, \ldots, d_t > 1$ are distinct divisors of n.

(b) Let ϵ be the smallest positive number of the form $1 - (\frac{1}{d_1} + \cdots + \frac{1}{d_t})$, with the d_i as in (a). Show that if $m \in \mathbf{N}$ and mn is not weird, then $\sigma_{-1}(mn) \geq \sigma_{-1}(n) + \epsilon$. *Hint:* Begin by writing $1 = \sum 1/d_i$, where the d_i are distinct divisors of mn and each $d_i > 1$.

(c) Deduce from (b) and Theorem 9.5 that the set of weird multiples of n has positive lower density.

Here are two open questions about weird numbers: Are all weird numbers even? Can $\sigma(n)/n$ be arbitrarily large for weird n?

References

[AB03] J. M. Aldaz and A. Bravo, *Euclid's argument on the infinitude of primes*, Amer. Math. Monthly **110** (2003), no. 2, 141–142.

[ABGU01] J. M. Aldaz, A. Bravo, S. Gutiérrez, and A. Ubis, *A theorem of D. J. Newman on Euler's ϕ function and arithmetic progressions*, Amer. Math. Monthly **108** (2001), no. 4, 364–367.

[AE44] L. Alaoglu and P. Erdős, *A conjecture in elementary number theory*, Bull. Amer. Math. Soc. **50** (1944), 881–882.

[And74] C. W. Anderson, *The solutions of* $\Sigma(n) = \frac{\sigma(n)}{n} = \frac{a}{b}$, $\Phi(n) = \frac{\varphi(n)}{n} = \frac{a}{b}$, *and related considerations*, unpublished manuscript, 1974.

[Ank60] N. C. Ankeny, *Criterion for rth power residuacity*, Pacific J. Math. **10** (1960), 1115–1124.

[Apo76] T. M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976, Undergraduate Texts in Mathematics.

[Art73] M. M. Artjuhov, *On the problem of odd h-fold perfect numbers*, Acta Arith. **23** (1973), 249–255.

[Art75] ———, *On problems of the theory of amicable numbers*, Acta Arith. **27** (1975), 281–291 (Russian).

[AZ04] M. Aigner and G. M. Ziegler, *Proofs from The Book*, third ed., Springer-Verlag, Berlin, 2004, Including illustrations by Karl H. Hofmann.

[Ban86] A. S. Bang, *Taltheoretiske Undersølgelser*, Tidsskrift f. Math. **5** (1886), 70–80, 130–137.

[Ban91] ———, *Om Primtal af bestemte Former*, Nyt Tidsskrift for Matematik, B (advanced) **2** (1891), 73–82.

[Ban37] ———, *Elementære Beviser for specielle Tilfælde af Dirichlets Sætning om Differensrækker*, H. Chr. Bakkes Boghandel, København, 1937.

[Bat72] P. T. Bateman, *The distribution of values of the Euler function*, Acta Arith. **21** (1972), 329–345.

[Bau06] M. Bauer, *Über die arithmetische Reihe*, J. Reine Angew. Math. **131** (1906), 265–267.

[BCtR91] R. P. Brent, G. L. Cohen, and H. J. J. te Riele, *Improved techniques for lower bounds for odd perfect numbers*, Math. Comp. **57** (1991), no. 196, 857–868.

[BD04] P. T. Bateman and H. G. Diamond, *Analytic number theory: An introductory course*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2004.

[BDD86a] R. Balasubramanian, J.-M. Deshouillers, and F. Dress, *Problème de Waring pour les bicarrés. I. Schéma de la solution*, C. R. Acad. Sci. Paris Sér. I Math. **303** (1986), no. 4, 85–88.

[BDD86b] ______, *Problème de Waring pour les bicarrés. II. Résultats auxiliaires pour le théorème asymptotique*, C. R. Acad. Sci. Paris Sér. I Math. **303** (1986), no. 5, 161–163.

[BE74] S. J. Benkoski and P. Erdős, *On weird and pseudoperfect numbers*, Math. Comp. **28** (1974), 617–623.

[Beh33] F. Behrend, *Über numeri abundantes. I, II*, Sitzungsberichte Akad. Berlin (1932), 322-328; (1933), 280–293.

[Bel43] R. Bellman, *A note on the divergence of a series*, Amer. Math. Monthly **50** (1943), 318–319.

[BEPS81] P. T. Bateman, P. Erdős, C. Pomerance, and E. G. Straus, *The arithmetic mean of the divisors of an integer*, Analytic number theory (Philadelphia, PA, 1980), Lecture Notes in Math., vol. 899, Springer, Berlin, 1981, pp. 197–220.

[Bes34] A. S. Besicovitch, *On the density of certain sequences of integers*, Math. Ann. **110** (1934), 336–341.

[BES99] R. Blecksmith, P. Erdős, and J. L. Selfridge, *Cluster primes*, Amer. Math. Monthly **106** (1999), no. 1, 43–48.

[BEW98] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998, A Wiley-Interscience Publication.

[BFPS04] W. D. Banks, J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, *Multiplicative structure of values of the Euler function*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 29–47.

[BGLS05] W. D. Banks, M. Z. Garaev, F. Luca, and I. E. Shparlinski, *Uniform distribution of the fractional part of the average prime divisor*, Forum Math. **17** (2005), no. 6, 885–901.

[BH62] P. T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. **16** (1962), 363–367.

[BHS04] W. D. Banks, D. N. Hart, and M. Sakata, *Almost all palindromes are composite*, Math. Res. Lett. **11** (2004), no. 5-6, 853–868.

[BK10] W. Bosma and B. Kane, *The aliquot constant*, Quart. J. Math. Oxford (2010), published online December 23, 2010.

[BL65] P. T. Bateman and M. E. Low, *Prime numbers in arithmetic progressions with difference* 24, Amer. Math. Monthly **72** (1965), 139–143.

[BL05] W. D. Banks and F. Luca, *Nonaliquots and Robbins numbers*, Colloq. Math. **103** (2005), no. 1, 27–32.

[BL07] C. Ballot and F. Luca, *On the equation $x^2+dy^2 = F_n$*, Acta Arith. **127** (2007), no. 2, 145–155.

[Boh52] H. Bohr, *Address of Professor Harald Bohr*, Proceedings of the International Congress of Mathematicians, Cambridge, Mass., 1950, vol. 1 (Providence, RI), Amer. Math. Soc., 1952, pp. 127–134.

[Boj54] R. Bojanić, *Asymptotic evaluations of the sum of divisors of certain numbers*, Bull. Soc. Math.-Phys., R.P. Macédoine **5** (1954), 5–15.

[Bor70] W. Borho, *Bemerkung zu einer Arbeit von H.-J. Kanold*, J. Reine Angew. Math. **243** (1970), 219–220.

[Bor74a] ———, *Befreundete Zahlen mit gegebener Primteileranzahl*, Math. Ann. **209** (1974), 183–193.

[Bor74b] ———, *Eine Schranke für befreundete Zahlen mit gegebener Teileranzahl*, Math. Nachr. **63** (1974), 297–301.

[BR51] A. Brauer and R. L. Reynolds, *On a theorem of Aubry-Thue*, Canadian J. Math. **3** (1951), 367–374.

[Bro74] A. E. Brouwer, *Two number theoretic sums*, Mathematisch Centrum, Amsterdam, 1974, Mathematisch Centrum, Afdeling Zuivere Wiskunde, ZW 19/74.

[Bru17] V. Brun, *Sur les nombres premiers de la forme $ap + b$*, Archiv for Mathem. og Naturw. **34** (1917), no. 8, 1–19.

[Bru19a] ———, *La série $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ où les dénominateurs sont "nombres premiers jumeaux" est convergente ou finie*, Bull. Sci. Math **43** (1919), 100–104, 124–128.

[Bru19b] ———, *Le crible d'Eratosthène et le théorème de Goldbach*, C. R. Math. Acad. Sci. Paris **168** (1919), 544–546.

[Bru20] ———, *Le crible d'Eratosthène et le théorème de Goldbach*, Christiania Vidensk. Selsk. Skr (1920), no. 3, 36 pp.

[BS92] V. Bergelson and D. B. Shapiro, *Multiplicative subgroups of finite index in a ring*, Proc. Amer. Math. Soc. **116** (1992), no. 4, 885–896.

[BS96] E. Bach and J. Sorenson, *Explicit bounds for primes in residue classes*, Math. Comp. **65** (1996), no. 216, 1717–1735.

[BS08] N. A. Baas and C. F. Skau, *The lord of the numbers, Atle Selberg, on his life and mathematics*, Bull. Amer. Math. Soc. (N.S.) **45** (2008), no. 4, 617–649 (electronic).

[Bun57] V. Bunyakovsky, *Sur les diviseurs numeriques invariables des fonctions rationnelles entieres*, Mem. Acad. Sci. St. Petersburg **6** (1857), 305–329.

[Bur62] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) **12** (1962), 179–192.

[Cat88] E. Catalan, *Propositions et questions diverses*, Bull. Soc. Math. France **16** (1888), 128–129.

[Cau15] A. L. Cauchy, *Démonstration du théorème général de Fermat sur les nombres polygones*, Mém. Sci. Math. Phys. Inst. France **14** (1813–1815), 177–220.

[CCC80] S. Chowla, M. Cowles, and J. Cowles, *On the difference of cubes* $(\bmod p)$, Acta Arith. **37** (1980), 61–65.

[CE46] A. H. Copeland and P. Erdős, *Note on normal numbers*, Bull. Amer. Math. Soc. **52** (1946), 857–860.

[CG20] A. Cunningham and T. Gosset, *4-tic & 3-bic residuacity-tables*, Messenger Math. **50** (1920), 1–30.

[Cha03] R. J. Chapman, *Evaluating* $\zeta(2)$, available from the author's website at `http://empslocal.ex.ac.uk/people/staff/rjchapma/etc/zeta2.pdf`, 2003.

[Che51] P. L. Chebyshev, *Sur la fonction qui detérmine la totalité des nombres premiers inférieurs à une limite donnée*, Mémoires présentés à l'Académie Impériale des Sciences de St. Pétersbourg par divers Savants **6** (1851), 141–157.

[Che52] ______, *Mémoire sur les nombres premiers*, Journal de Mathématique pures et appliquées **17** (1852), 366–390.

[Che65] P. R. Chernoff, *A "Lattice Point" Proof of the Infinitude of Primes*, Math. Mag. **38** (1965), no. 4, 208.

[Che73] 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.

[Cho89] M. R. Chowdhury, *Über die Zahlenfolge* $n! + k$, $2 \leq k \leq n$, Elem. Math. **44** (1989), 129–130.

[Cil08] J. Cilleruelo, *Squares in* $(1^2 + 1) \cdots (n^2 + 1)$, J. Number Theory **128** (2008), no. 8, 2488–2491.

[CL77] G. J. Chang and K. W. Lih, *Polynomial representation of primes*, Tamkang J. Math. **8** (1977), no. 2, 197–198.

[Cle49] P. A. Clement, *Congruences for sets of primes*, Amer. Math. Monthly **56** (1949), 23–25.

[CM06] A. C. Cojocaru and M. R. Murty, *An introduction to sieve methods and their applications*, London Mathematical Society Student Texts, vol. 66, Cambridge University Press, Cambridge, 2006.

[CO09] W. K. Chan and B.-K. Oh, *Almost universal ternary sums of triangular numbers*, Proc. Amer. Math. Soc. **137** (2009), no. 11, 3553–3562.

[Col09] S. Col, *Palindromes dans les progressions arithmétiques*, Acta Arith. **137** (2009), no. 1, 1–41.

[Con87] J.H Conway, *FRACTRAN: A simple universal programming language for arithmetic*, Open problems in communication and computation (Thomas M. Cover and B. Gopinath, eds.), Springer-Verlag, New York, 1987, pp. 4–26.

[Cox89] D. A. Cox, *Primes of the form* x^2+ny^2*: Fermat, class field theory and complex multiplication*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.

[CP05] R. Crandall and C. Pomerance, *Prime numbers: a computational perspective*, second ed., Springer, New York, 2005.

[CR41] R. Courant and H. Robbins, *What Is Mathematics?*, Oxford University Press, New York, 1941.

[CS97] M. Crubellier and J. Sip, *Looking for perfect numbers*, History of mathematics. Histories of problems, Ellipses Édition Marketing, Paris, 1997, pp. 389–410.

[Cuc68] I. Cucurezeanu, *A generalization of the theorem of Clement*, Stud. Cerc. Mat. **20** (1968), 841–843.

[CZ11] Y.-G. Chen and Q.-Q. Zhao, *Nonaliquot numbers*, Publ. Math. Debrecen **78** (2011), no. 2, 439–442.

[Dab84] H. Daboussi, *Sur le théorème des nombres premiers*, C. R. Acad. Sci. Paris Sér. I Math. **298** (1984), no. 8, 161–164.

[Dąb96] A. Dąbrowski, *On the Diophantine equation* $x! + A = y^2$, Nieuw Arch. Wisk. (4) **14** (1996), no. 3, 321–324.

[Dav33] H. Davenport, *Über numeri abundantes*, Sitzungsberichte Akad. Berlin (1933), 830–837.

[Dav39] ______, *On Waring's problem for fourth powers*, Ann. of Math. (2) **40** (1939), 731–747.

[Del98] M. Deléglise, *Bounds for the density of abundant integers*, Experiment. Math. **7** (1998), no. 2, 137–143.

[DGNP93] J.-M. Deshouillers, A. Granville, W. Narkiewicz, and C. Pomerance, *An upper bound in Goldbach's problem*, Math. Comp. **61** (1993), no. 203, 209–213.

[DH08] H. G. Diamond and H. Halberstam, *A higher-dimensional sieve method*, Cambridge Tracts in Mathematics, vol. 177, Cambridge University Press, Cambridge, 2008.

[DH09] ______, *Congruences and ideals*, Analytic number theory, Cambridge Univ. Press, Cambridge, 2009, pp. 164–169.

[DI82] J.-M. Deshouillers and H. Iwaniec, *On the greatest prime factor of $n^2 + 1$*, Ann. Inst. Fourier (Grenoble) **32** (1982), no. 4, 1–11 (1983).

[Dic04] L. E. Dickson, *A new extension of Dirichlet's theorem on prime numbers*, Messenger Math. **33** (1904), 155–161.

[Dic13a] ______, *Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors*, Amer. J. Math. **35** (1913), no. 4, 413–422.

[Dic13b] ______, *Theorems and tables on the sum of the divisors of a number*, Quart. J. Math. **44** (1913), 264–296.

[Dic66] ______, *History of the theory of numbers. Vol. I: Divisibility and primality.*, Chelsea Publishing Co., New York, 1966.

[Dir37] P. G. L. Dirichlet, *Beweis des Satzes, dass jede unbegrenzte arithmetische progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*, Abhandl. Kgl. Preuß Akad. Wiss. (1837), 45–81.

[Dir39] ______, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres: première partie*, J. Reine Angew. Math. **19** (1839), 324–369.

[Dir41] ______, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres: seconde partie*, J. Reine Angew. Math. **21** (1841), 1–12, 134–155.

[Dir99] ______, *Lectures on number theory*, History of Mathematics, vol. 16, American Mathematical Society, Providence, RI, 1999, Supplements by R. Dedekind, Translated from the 1863 German original and with an introduction by John Stillwell.

[Dix62] J. D. Dixon, *Mathematical Notes: π is not Algebraic of Degree One or Two*, Amer. Math. Monthly **69** (1962), no. 7, 636.

[DN05] A. Dubickas and A. Novikas, *Integer parts of powers of rational numbers*, Math. Z. **251** (2005), no. 3, 635–648.

[Dre71] F. Dress, *Méthodes élémentaires dans le problème de Waring pour les entiers*, Université de Provence, Marseille, 1971, Journées Arithmétiques Françaises, Mai 1971.

[Dre72a] ______, *Théorie additive des nombres, problème de Waring et théorème de Hilbert*, Enseignement Math. (2) **18** (1972), 175–190; errata, ibid. (2) 18 (1972), 301–302 (1973).

[Dre72b] R. E. Dressler, *An elementary proof of a theorem of Erdős on the sum of divisors function*, J. Number Theory **4** (1972), 532–536.

[Dre75] ———, *A lower bound for $\pi(n)$*, Amer. Math. Monthly **82** (1975), 151–152.

[Duk97] W. Duke, *Some old problems and new results about quadratic forms*, Notices Amer. Math. Soc. **44** (1997), no. 2, 190–196.

[Dun04] G. W. Dunnington, *Carl Friedrich Gauss: Titan of science. A study of his life and work*, Mathematical Association of America, New York, 2004.

[Eff08] G. W. Effinger, *Toward a complete twin primes theorem for polynomials over finite fields*, Finite Fields and Applications: Proceedings of the Eighth International Conference, Melbourne, July 2007, Amer. Math. Soc., 2008, pp. 103–110.

[EGPS90] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions*, Analytic number theory (Allerton Park, IL, 1989), Progr. Math., vol. 85, Birkhäuser Boston, Boston, MA, 1990, pp. 165–204.

[EHM02] G. W. Effinger, K. Hicks, and G. L. Mullen, *Twin irreducible polynomials over finite fields*, Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), Springer, Berlin, 2002, pp. 94–111.

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

[Ell71] W. J. Ellison, *Waring's problem*, Amer. Math. Monthly **78** (1971), no. 1, 10–36.

[EM52] P. Erdős and L. Mirsky, *The distribution of values of the divisor function $d(n)$*, Proc. London Math. Soc. (3) **2** (1952), 257–271.

[EN96] P. Erdös and M. B. Nathanson, *On the sum of the reciprocals of the differences between consecutive primes*, Number theory (New York, 1991–1995), Springer, New York, 1996, pp. 97–101.

[EO37] P. Erdős and R. Obláth, *Über diophantische Gleichungen der Form $n! = x^p \pm y^p$ und $n! \pm m! = x^p$*, Acta Litt. Sci. Univ., Szeged **8** (1937), 241–255.

[EP78] P. Erdős and C. Pomerance, *On the largest prime factors of n and $n+1$*, Aequationes Math. **17** (1978), no. 2-3, 311–321.

[EP90] ———, *On a theorem of Besicovitch: values of arithmetic functions that divide their arguments*, Indian J. Math. **32** (1990), no. 3, 279–287.

[ER75] P. Erdős and G. J. Rieger, *Ein Nachtrag über befreundete Zahlen*, J. Reine Angew. Math. **273** (1975), 220.

[Erd32] P. Erdős, *Beweis eines Satzes von Tschebyschef*, Acta Litt. Sci. Szeged **5** (1932), 194–198.

[Erd35a] ———, *Note on sequences of integers no one of which is divisible by any other*, J. London Math. Soc. **10** (1935), 126–128.

[Erd35b] ———, *On the density of some sequences of numbers*, J. London Math. Soc. **10** (1935), 120–125.

[Erd35c] ———, *On the difference of consecutive primes*, Quart J. Math. Oxford **6** (1935), 124–128.

[Erd35d] ———, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ-function*, Quart J. Math. Oxford **6** (1935), 205–213.

[Erd35e] ______, *Über die Primzahlen gewisser arithmetischer Reihen*, Math Z. **39** (1935), 473–491.

[Erd36] ______, *On a problem of Chowla and some related problems*, Proc. Cambridge Philos. Soc. **32** (1936), 530–540.

[Erd37] ______, *On the density of some sequences of numbers, II*, J. London Math. Soc. **12** (1937), 7–11.

[Erd38] ______, *On the density of some sequences of numbers, III*, J. London Math. Soc. **13** (1938), 119–127.

[Erd39] ______, *On the smoothness of the asymptotic distribution of additive arithmetical functions*, Amer. J. Math. **61** (1939), 722–725.

[Erd45] ______, *Some remarks on Euler's ϕ function and some related problems*, Bull. Amer. Math. Soc. **51** (1945), 540–544.

[Erd46] ______, *Some remarks about additive and multiplicative functions*, Bull. Amer. Math. Soc. **52** (1946), 527–537.

[Erd49] ______, *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.

[Erd50a] ______, *On a Diophantine equation*, Mat. Lapok **1** (1950), 192–210.

[Erd50b] ______, *On integers of the form $2^k + p$ and some related problems*, Summa Brasil. Math. **2** (1950), 113–123.

[Erd51] ______, *On some problems of Bellman and a theorem of Romanoff*, J. Chinese Math. Soc. (N.S.) **1** (1951), 409–421.

[Erd55a] ______, *On amicable numbers*, Publ. Math. Debrecen **4** (1955), 108–111.

[Erd55b] ______, *Some remarks on number theory*, Riveon Lematematika **9** (1955), 45–48 (Hebrew).

[Erd60] ______, *An asymptotic inequality in the theory of numbers*, Vestnik Leningrad. Univ. **15** (1960), no. 13, 41–49.

[Erd65] ______, *Some recent advances and current problems in number theory*, Lectures on Modern Mathematics, Vol. III, Wiley, New York, 1965, pp. 196–244.

[Erd70] ______, *Some extremal problems in combinatorial number theory*, Mathematical Essays Dedicated to A. J. Macintyre, Ohio Univ. Press, Athens, Ohio, 1970, pp. 123–133.

[Erd73] ______, *Über die Zahlen der Form $\sigma(n) - n$ und $n - \phi(n)$*, Elem. Math. **28** (1973), 83–86.

[Erd76] ______, *On asymptotic properties of aliquot sequences*, Math. Comp. **30** (1976), no. 135, 641–645.

[Erd79] ______, *Some unconventional problems in number theory*, Journées Arithmétiques de Luminy (Colloq. Internat. CNRS, Centre Univ. Luminy, Luminy, 1978), Astérisque, vol. 61, Soc. Math. France, Paris, 1979, pp. 73–82.

[Erd89] ______, *Ramanujan and I*, Number theory, Madras 1987, Lecture Notes in Math., vol. 1395, Springer, Berlin, 1989, pp. 1–20.

[Est32] T. Estermann, *Eine neue Darstellung und neue Anwendungen der Viggo Brunschen Methode*, J. Reine Angew. Math. **168** (1932), 106–116.

[ET34] P. Erdős and P. Turán, *On a problem in the elementary theory of numbers*, Amer. Math. Monthly **41** (1934), no. 10, 608–611.

[ET48] ______, *On some new questions on the distribution of prime numbers*, Bull. Amer. Math. Soc. **54** (1948), 371–378.

[Eul37] L. Euler, *Variae observationes circa series infinites*, Comm. Acad. Petropolitanae **9** (1737), 160–188.

[EW39] P. Erdös and A. Wintner, *Additive arithmetical functions and statistical independence*, Amer. J. Math. **61** (1939), 713–721.

[Ewe80] J. A. Ewell, *On the multiplicative structure of odd perfect numbers*, J. Number Theory **12** (1980), no. 3, 339–342.

[FH00] K. Ford and H. Halberstam, *The Brun-Hooley sieve*, J. Number Theory **81** (2000), no. 2, 335–350.

[FI10] J. Friedlander and H. Iwaniec, *Opera de cribro*, American Mathematical Society Colloquium Publications, vol. 57, American Mathematical Society, Providence, RI, 2010.

[FK96] M. Filaseta and S. Konyagin, *Squarefree values of polynomials all of whose coefficients are* 0 *and* 1, Acta Arith. **74** (1996), no. 3, 191–205.

[FNO] S. A. Fletcher, P. P. Nilesen, and P. Ochem, *Sieve methods for odd perfect numbers*, Math. Comp., to appear.

[For98a] K. Ford, *The distribution of totients*, Electron. Res. Announc. Amer. Math. Soc. **4** (1998), 27–34 (electronic).

[For98b] ———, *The distribution of totients*, Ramanujan J. **2** (1998), no. 1-2, 67–151, corrected e-print version available as `arXiv:1104.3264 [math.NT]`.

[For08a] ———, *The distribution of integers with a divisor in a given interval*, Ann. of Math. (2) **168** (2008), no. 2, 367–433.

[For08b] ———, *Integers with a divisor in* $(y, 2y]$, Anatomy of Integers, CRM Proceedings and Lecture Notes, 2008, pp. 65–80.

[FR07] B. Fine and G. Rosenberger, *Number theory: An introduction via the distribution of primes*, Birkhäuser Boston, Boston, MA, 2007.

[Fre07] G. Frei, *The unpublished section eight: on the way to function fields over a finite field*, The shaping of arithmetic after C. F. Gauss's *Disquisitiones arithmeticae*, Springer, Berlin, 2007, pp. 159–198.

[FS67] W. Forman and H. N. Shapiro, *An arithmetic property of certain rational powers*, Comm. Pure Appl. Math. **20** (1967), 561–573.

[Fue46] R. Fueter, *Über primitive Wurzeln von Primzahlen*, Comment. Math. Helv. **18** (1946), 217–223.

[Fur55] H. Furstenberg, *On the infinitude of primes*, Amer. Math. Monthly **62** (1955), 353.

[Gan71] J. M. Gandhi, *Formulae for the nth prime*, Proceedings of the Washington State University Conference on Number Theory (Washington State Univ., Pullman, Wash., 1971), Dept. Math., Washington State Univ., Pullman, Wash., 1971, pp. 96–106.

[Gau65] C. F. Gauss, *Die Lehre von den Resten. II. Allgemeine Untersuchungen über die Congruenzen*, Untersuchungen über höhere Arithmetik, Deutsch herausgegeben von H. Maser, Chelsea Publishing Co., New York, 1965, pp. 602–629.

[Gau73a] ———, *Notizen über cubische und biquadratische Reste*, Werke. Band VII, Georg Olms Verlag, Hildesheim, 1973, Reprint of the 1906 original, pp. 5–14.

[Gau73b] ———, *Werke. Band II*, Georg Olms Verlag, Hildesheim, 1973, Reprint of the 1863 original.

[Gau73c] ———, *Werke. Band X. Abt. I, II*, Georg Olms Verlag, Hildesheim, 1973, Reprint of the 1917 and the 1922–1933 originals.

[Gau86] ———, *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986, Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[Gel46] A. O. Gel′fond, *Commentary on the papers "On the estimation of the number of primes not exceeding a given value" and "On prime numbers"*, Collected works of P. L. Chebyshev, vol. 1, Akad. Nauk SSSR, Moscow-Leningrad, 1946, pp. 285–288.

[Gel56] ———, *On the arithmetic equivalent of analyticity of the Dirichlet L-series on the line* $\operatorname{Re} s = 1$, Izv. Akad. Nauk SSSR. Ser. Mat. **20** (1956), 145–166.

[GGPY11] D. A. Goldston, S. W. Graham, J. Pintz, and C. Y. Yıldırım, *Small gaps between almost primes, the parity problem, and some conjectures of Erdős on consecutive integers*, Int. Math. Res. Not. IMRN (2011), no. 7, 1439–1450.

[GL66] A. O. Gel′fond and Yu. V. Linnik, *Elementary methods in the analytic theory of numbers*, Translated from the Russian by D. E. Brown. Translation edited by I. N. Sneddon. International Series of Monographs in Pure and Applied Mathematics, Vol. 92, Pergamon Press, Oxford, 1966.

[GLMU56] V. Gardiner, R. Lazarus, N. Metropolis, and S. Ulam, *On certain sequences of integers defined by sieves*, Math. Mag. **29** (1956), 117–122.

[GMPY06] D. A. Goldston, Y. Motohashi, J. Pintz, and C. Y. Yıldırım, *Small gaps between primes exist*, Proc. Japan Acad. Ser. A Math. Sci. **82** (2006), no. 4, 61–65.

[GO08] T. Goto and Y. Ohno, *Odd perfect numbers have a prime factor exceeding* 10^8, Math. Comp. **77** (2008), no. 263, 1859–1868.

[Gol55] S. W. Golomb, *Sets of primes with intermediate density*, Math. Scand. **3** (1955), 264–274 (1956).

[Gol58] V. A. Golubev, *Nombres de Mersenne et caractères du nombre* 2, Mathesis **67** (1958), 257–262.

[Gol60] S. W. Golomb, *The twin prime constant*, Amer. Math. Monthly **67** (1960), no. 8, 767–769.

[Gol62] ———, *On the ratio of* n *to* $\pi(n)$, Amer. Math. Monthly **69** (1962), no. 1, 36–37.

[Gol74] ———, *A direct interpretation of Gandhi's formula*, Amer. Math. Monthly **81** (1974), 752–754.

[Gol76] ———, *Properties of the sequences* $3 \cdot 2^n + 1$, Math. Comp. **30** (1976), no. 135, 657–663.

[Gol98] R. Goldblatt, *Lectures on the hyperreals: An introduction to nonstandard analysis*, Graduate Texts in Mathematics, vol. 188, Springer-Verlag, New York, 1998.

[Gol04] D. Goldfeld, *The elementary proof of the prime number theorem: an historical perspective*, Number theory (New York, 2003), Springer, New York, 2004, pp. 179–192.

[GPS07] S. Guo, H. Pan, and Z.-W. Sun, *Mixed sums of squares and triangular numbers. II*, Integers **7** (2007), A56, 5.

[GPtR04] M. García, J. M. Pedersen, and H. J. J. te Riele, *Amicable pairs, a survey*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 179–196.

[GPY09] D. A. Goldston, J. Pintz, and C. Y. Yıldırım, *Primes in tuples. I*, Annals of Mathematics **170** (2009), 819–862.

[GPY10] ———, *Primes in tuples. II*, Acta Math. **204** (2010), 1–47.

[GPY11] ———, *Primes in tuples. IV*, e-print available as `arXiv:1103.5886 [math.NT]`, 2011.

[GR90] S. W. Graham and C. J. Ringrose, *Lower bounds for least quadratic non-residues*, Analytic number theory (Allerton Park, IL, 1989), Progr. Math., vol. 85, Birkhäuser Boston, Boston, MA, 1990, pp. 269–309.

[Gra23] K. Grandjot, *Über die Irreduzibilität der Kreisteilungsgleichung*, Math. Zeitschrift **19** (1923), 128–129.

[Gra25] I. S. Gradstein, *On odd perfect numbers*, Mat. Sbornik **32** (1925), 476–510 (Russian).

[Gra84] J. J. Gray, *A commentary on Gauss's mathematical diary, 1796–1814, with an English translation*, Exposition. Math. **2** (1984), no. 2, 97–130.

[Gra95] A. Granville, *Harald Cramér and the distribution of prime numbers*, Scand. Actuar. J. (1995), no. 1, 12–28, Harald Cramér Symposium (Stockholm, 1993).

[Gra08a] ———, *Prime number patterns*, Amer. Math. Monthly **115** (2008), no. 4, 279–296.

[Gra08b] ———, *Smooth numbers: computational number theory and beyond*, Algorithmic Number Theory (J. P. Buhler and P. Stevenhagen, eds.), Cambridge University Press, Cambridge, 2008, pp. 267–323.

[Gre01] G. Greaves, *Sieves in number theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 43, Springer-Verlag, Berlin, 2001.

[Gro13] T. H. Gronwall, *Some asymptotic expressions in the theory of numbers*, Trans. Amer. Math. Soc. **14** (1913), 113–122.

[Grö06] D. Gröger, *On Gauss's entry from January 6, 1809*, Amer. Math. Monthly **113** (2006), no. 5, 455–458.

[Gru80] T. Grundhöfer, *Über die Zahlen der Form* $n! + k$, Arch. Math. (Basel) **33** (1979/80), no. 4, 361–363.

[GS75] R. K. Guy and J. L. Selfridge, *What drives an aliquot sequence?*, Math. Comput. **29** (1975), 101–107, Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday.

[GT08] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) **167** (2008), no. 2, 481–547.

[GT10] ———, *Linear equations in primes*, Ann. of Math. (2) **171** (2010), no. 3, 1753–1850.

[GTZ11] B. Green, T. Tao, and T. Ziegler, *An inverse theorem for the Gowers* $U^{s+1}[N]$*-norm*, e-print available as `arXiv:1009.3998 [math.NT]`, 2011.

[Guy83] R. K. Guy, *Conway's prime producing machine*, Math. Mag. **56** (1983), no. 1, 26–33.

[Guy04] ———, *Unsolved problems in number theory*, third ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004.

[Gya83] E. Gyarmati, *A note on my paper: "Unique prime factorization in imaginary quadratic number fields"*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **26** (1983), 195–196.

[Hal03] C. J. Hall, *L-functions of twisted Legendre curves*, Ph.D. thesis, Princeton University, 2003.

[Hal06] ———, *L-functions of twisted Legendre curves*, J. Number Theory **119** (2006), no. 1, 128–147.

[Har20] G. H. Hardy, *Some famous problems of the theory of numbers and in particular Waring's problem*, Clarendon Press, Oxford, 1920, An inaugural lecture delivered before the University of Oxford.

[Har56] V. C. Harris, *Another proof of the infinitude of primes*, Amer. Math. Monthly **63** (1956), 711.

[Har97] G. Harman, *Metrical theorems on prime values of the integer parts of real sequences*, Proc. London Math. Soc. (3) **75** (1997), no. 3, 481–496.

[Har07] K. G. Hare, *New techniques for bounds on the total number of prime factors of an odd perfect number*, Math. Comp. **76** (2007), no. 260, 2241–2248 (electronic).

[Hau09] F. Hausdorff, *Zur Hilbertschen Lösung des Waringschen Problems*, Math. Ann. **67** (1909), 301–305.

[Haw58] D. Hawkins, *The random sieve*, Math. Mag. **31** (1957/1958), 1–3.

[Haw74] ———, *Random sieves. II*, J. Number Theory **6** (1974), 192–200.

[Hay65] D. R. Hayes, *A Goldbach theorem for polynomials with integral coefficients*, Amer. Math. Monthly **72** (1965), 45–46.

[HB58] D. Hawkins and W. E. Briggs, *The lucky number theorem*, Math. Mag. **31** (1957/1958), 81–84.

[HB84] D. R. Heath-Brown, *The divisor function at consecutive integers*, Mathematika **31** (1984), no. 1, 141–149.

[HB87] ———, *Consecutive almost-primes*, J. Indian Math. Soc. (N.S.) **52** (1987), 39–49 (1988).

[HB92] ———, *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.

[HB94] ———, *Odd perfect numbers*, Math. Proc. Cambridge Philos. Soc. **115** (1994), no. 2, 191–196.

[Heg93] N. Hegyvári, *On some irrational decimal fractions*, Amer. Math. Monthly **100** (1993), no. 8, 779–780.

[Hei31] H. Heilbronn, *Über die Verteilung der Primzahlen in Polynomen*, Math. Ann. **104** (1931), 794–799.

[Hem66] R. L. Hemminger, *Classroom Notes: More on the Infinite Primes Theorem*, Amer. Math. Monthly **73** (1966), no. 9, 1001–1002.

[Hil09] D. Hilbert, *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem). Dem Andenken an Hermann Minkowski gewidmet*, Math. Ann. **67** (1909), 281–300.

[Hil86] A. J. Hildebrand, *The prime number theorem via the large sieve*, Mathematika **33** (1986), no. 1, 23–30.

[Hil97] ———, *Multiplicative properties of consecutive integers*, Analytic number theory (Kyoto, 1996), London Math. Soc. Lecture Note Ser., vol. 247, Cambridge Univ. Press, Cambridge, 1997, pp. 103–117.

[Hil02] ———, *Erdős' problems on consecutive integers*, Paul Erdős and his mathematics, I (Budapest, 1999), Bolyai Soc. Math. Stud., vol. 11, János Bolyai Math. Soc., Budapest, 2002, pp. 305–317.

[Hir02] M. D. Hirschhorn, *There are infinitely many prime numbers*, Austral. Math. Soc. Gaz. **29** (2002), no. 2, 103.

[HL23] G. H. Hardy and J. E. Littlewood, *Some problems of Partitio Numerorum III: on the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.

[HL34] H. Heilbronn and E. Linfoot, *On the imaginary quadratic corpora of class-number one*, Quarterly J. Math **5** (1934), 293–301.

[Hol06] J. A. Holdener, *Conditions equivalent to the existence of an odd perfect number*, Math. Mag. **79** (2006), 389–391.

[Hoo76] C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge University Press, Cambridge, 1976, Cambridge Tracts in Mathematics, No. 70.

[Hoo94] ———, *On an almost pure sieve*, Acta Arith. **66** (1994), no. 4, 359–368.

[Hor55] B. Hornfeck, *Zur Dichte der Menge der vollkommenen Zahlen*, Arch. Math. (Basel) **6** (1955), 442–443.

[HR17] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Math. **48** (1917), 76–92.

[HR73] D. Hensley and I. Richards, *On the incompatibility of two conjectures concerning primes*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R.I., 1973, pp. 123–127.

[HR74] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974, London Mathematical Society Monographs, No. 4.

[HS85] G. Hofmeister and P. Stoll, *Note on Egyptian fractions*, J. Reine Angew. Math. **362** (1985), 141–145.

[HST91] E. Hlawka, J. Schoissengeier, and R. Taschner, *Geometric and analytic number theory*, Universitext, Springer-Verlag, Berlin, 1991, Translated from the 1986 German edition by Charles Thomas.

[HT06] K.-H. Ho and K.-M. Tsang, *On almost prime k-tuples*, J. Number Theory **120** (2006), no. 1, 33–46.

[Hua82] L. K. Hua, *Introduction to number theory*, Springer-Verlag, Berlin, 1982, Translated from the Chinese by Peter Shiu.

[HW57] B. Hornfeck and E. Wirsing, *Über die Häufigkeit vollkommener Zahlen*, Math. Ann. **133** (1957), 431–438.

[HW08] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008, Revised by D. R. Heath-Brown and J. H. Silverman.

[IK04] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.

[Ing48] A. E. Ingham, *Review of two papers:* An elementary proof of the prime-number theorem*, by A. Selberg and* On a new method in elementary number theory which leads to an elementary proof of the prime number theorem*, by P. Erdős*, Reviews in Number Theory as printed in Mathematical Reviews 1940-1872, vol. 4, Amer. Math. Soc., Providence, RI, 1948, pp. 191–193.

[IR90] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[Isr83] R. B. Israel, *Solution to problem 6384*, Amer. Math. Monthly **90** (1983), no. 9, 650.

[Iwa78] H. Iwaniec, *Almost-primes represented by quadratic polynomials*, Invent. Math. **47** (1978), no. 2, 171–188.

[Jac27] C. G. J. Jacobi, *De residuis cubicis commentatio numerosa*, J. Reine Angew. Math. **2** (1827), 66–69.

[Jac69] ______, *Letter to Gauss (February 8, 1827)*, Gesammelte Werke, Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften. Zweite Ausgabe, vol. VII, Chelsea Publishing Co., New York, 1969, pp. 393–400.

[JSWW76] J. P. Jones, D. Sato, H. Wada, and D. Wiens, *Diophantine representation of the set of prime numbers*, Amer. Math. Monthly **83** (1976), no. 6, 449–464.

[Kal64] M. Kalecki, *On certain sums extended over primes or prime factors*, Prace Mat. **8** (1963/1964), 121–129.

[Kan56] H.-J. Kanold, *Über einen Satz von L. E. Dickson. II*, Math. Ann. **132** (1956), 246–255.

[Kan69a] ______, *Über befreundete Zahlen. III*, J. Reine Angew. Math. **234** (1969), 207–215.

[Kan69b] ______, *Über "super perfect numbers"*, Elem. Math. **24** (1969), 61–62.

[Kát07] I. Kátai, *On the average prime divisors*, Ann. Univ. Sci. Budapest. Sect. Comput. **27** (2007), 137–144.

[Kem12] A. Kempner, *Bemerkungen zum Waringschen Problem*, Math. Ann. **72** (1912), 387–399.

[KLS02] M. Křížek, F. Luca, and L. Somer, *On the convergence of series of reciprocals of primes related to the Fermat numbers*, J. Number Theory **97** (2002), no. 1, 95–112.

[Kly07] D. Klyve, *Explicit bounds on twin primes and Brun's constant*, Ph.D. thesis, Dartmouth College, 2007.

[Kob84] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984.

[Kob10] M. Kobayashi, *On the density of abundant numbers*, Ph.D. thesis, Dartmouth College, 2010, (expected).

[Koc01] H. von Koch, *Sur la distribution des nombres premiers*, Acta Math. **24** (1901), 159–182.

[Kor82] J. Korevaar, *On Newman's quick way to the prime number theorem*, Math. Intelligencer **4** (1982), no. 3, 108–115.

[Kor02] ______, *A century of complex Tauberian theory*, Bull. Amer. Math. Soc. (N.S.) **39** (2002), no. 4, 475–531 (electronic).

[KPP09] M. Kobayashi, P. Pollack, and C. Pomerance, *On the distribution of sociable numbers*, J. Number Theory **129** (2009), 1990–2009.

[Kro88] L. Kronecker, *Über die arithmetischen Sätze, welche Lejeune Dirichlet in seiner Breslauer Habilitationsschrift entwickelt hat*, Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin **16** (1888), 417–423.

[KS10] B. Kane and Z.-W. Sun, *On almost universal mixed sums of squares and triangular numbers*, Trans. Amer. Math. Soc. **362** (2010), no. 12, 6425–6455.

[KT05] A. V. Kumchev and D. I. Tolev, *An invitation to additive prime number theory*, Serdica Math. J. **31** (2005), no. 1-2, 1–74.

[Kum46] E. E. Kummer, *Über die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung entstehen*, J. Reine Angew. Math. **30** (1846), 107–116.

[KW90] J. M. Kubina and M. C. Wunderlich, *Extending Waring's conjecture to* $471,600,000$, Math. Comp. **55** (1990), no. 192, 815–820.

[Lan00] E. Landau, *Ueber die zahlentheoretische Function* $\varphi(n)$ *und ihre Beziehung zum Goldbachschen Satz*, Göttinger Nachrichten (1900), 177–186.

[Lan01] ———, *Solutions de questions proposées, 1075*, Nouv. Ann. Math. **1** (1901), 138–142.

[Lan02] ———, *Ueber die zu einem algebraischen Zahlkörper gehörige Zetafunction und die Ausdehnung der Tschebyschefschen Primzahlentheorie auf das Problem der Verteilung der Primideale*, J. Reine Angew. Math. **128** (1902), 64–188.

[Lan08] ———, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der mindest Anzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. der Math. und Phys. **13** (1908), 305–312.

[Lan28] ———, *Über die Irreduzibilität der Kreisteilungsgleichung*, Math. Zeitschrift **29** (1928), 462.

[Lan30] ———, *Die Goldbachsche Vermutung und der Schnirelmannsche Satz*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. (1930), 255–276.

[Lán65] E. Lánczi, *Unique prime factorization in imaginary quadratic number fields*, Acta Math. Acad. Sci. Hungar. **16** (1965), 453–466.

[Lan02] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[Lay82] S. R. Lay, *Convex sets and their applications*, John Wiley & Sons, Inc., New York, 1982, Pure and Applied Mathematics, A Wiley-Interscience Publication.

[Leb60] V. A. Lebesgue, *Note sur les congruences*, C.R. Acad. Sci. Paris **51** (1860), 9–13.

[Leg00] A.-M. Legendre, *Théorie des nombres*, 3rd (reprinted) ed., Librairie Scientifique A. Hermann, Paris, 1900, 2 volumes.

[Leh33] D. H. Lehmer, *On imaginary quadratic fields whose class number is unity*, Bull. Amer. Math. Soc. **39** (1933), 360.

[Leh58] E. Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika **5** (1958), 20–29.

[Lem00] F. Lemmermeyer, *Reciprocity laws: From Euler to Eisenstein*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[Len75] H. W. Lenstra, Jr., *Problem 6061*, Amer. Math. Monthly **82** (1975), 1016, solution by the proposer in **84** (1977), 580.

[LeV96] W. J. LeVeque, *Fundamentals of number theory*, Dover Publications Inc., Mineola, NY, 1996, Reprint of the 1977 original.

[Lin61] Yu. V. Linnik, *New versions and new uses of the dispersion methods in binary additive problems*, Dokl. Akad. Nauk SSSR **137** (1961), 1299–1302 (Russian).

[Lit14] J. E. Littlewood, *Sur la distribution des nombres premiers*, Comptes Rendus Acad. Sci. Paris **158** (1914), 1869–1872.

[LO11] R. Lemke Oliver, *Almost-primes represented by quadratic polynomials*, Acta Arith. (2011), to appear.

[Lor96] D. Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics, vol. 9, American Mathematical Society, Providence, RI, 1996.

[LP97] P. Lindqvist and J. Peetre, *On the remainder in a series of Mertens*, Exposition. Math. **15** (1997), no. 5, 467–478.

[LP10] F. Luca and C. Pomerance, *On the radical of a perfect number*, New York J. Math. **16** (2010), 23–30.

[LPZ11] Y. Lamzouri, M. Phaovibul, and A. Zaharescu, *On the distribution of the partial sum of Euler's totient function in residue classes*, Colloq. Math. **123** (2011), 115–127.

[LS89] D. B. Leep and D. B. Shapiro, *Multiplicative subgroups of index three in a field*, Proc. Amer. Math. Soc. **105** (1989), no. 4, 802–807.

[Luc99] F. Luca, *Problem 10711*, Amer. Math. Monthly **106** (1999), 166, solution by F. B. Coghlan in **108** (2001), 80.

[Luc00a] ———, *The anti-social Fermat number*, Amer. Math. Monthly **107** (2000), no. 2, 171–173.

[Luc00b] ———, *Pascal's triangle and constructible polygons*, Util. Math. **58** (2000), 209–214.

[Luc06] ———, *Williams College MATH 303 course notes*, unpublished manuscript, 2006.

[Luc07] ———, *On the densities of some subsets of integers*, Missouri J. Math. Sciences **19** (2007), (electronic), available on the web at `http://www.math-cs.ucmo.edu/∼mjms/mjms.html`.

[LZ07] A. Languasco and A. Zaccagnini, *A note on Mertens' formula for arithmetic progressions*, J. Number Theory **127** (2007), no. 1, 37–46.

[Mah57] K. Mahler, *On the fractional parts of the powers of a rational number. II*, Mathematika **4** (1957), 122–124.

[Mąk62] A. Mąkowski, *Remark on perfect numbers*, Elem. Math. **17** (1962), no. 5, 109.

[Man42] H. B. Mann, *A proof of the fundamental theorem on the density of sums of sets of positive integers*, Ann. of Math. (2) **43** (1942), 523–527.

[Mar99] G. Martin, *The smallest solution of* $\phi(30n+1) < \phi(30n)$ *is* …, Amer. Math. Monthly **106** (1999), no. 5, 449–451.

[Mat93] Yu. V. Matijasevich, *Hilbert's tenth problem*, Foundations of Computing Series, MIT Press, Cambridge, MA, 1993, Translated from the 1993 Russian original by the author, With a foreword by Martin Davis.

[Mat99] ———, *Formulas for prime numbers [Kvant* **1975***, no. 5, 5–13]*, Kvant selecta: algebra and analysis, II, Math. World, vol. 15, Amer. Math. Soc., Providence, RI, 1999, pp. 13–24.

[Mer74] F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. Reine Angew. Math. **78** (1874), 46–62.

[Mer97] ———, *Über Dirichlet's Beweis des Satzes, daß jede unbegrenzte ganzzahlige arithmetische Progression, deren Differenz zu ihren Gliedern teilerfremd ist, unendlich viele Primzahlen enthält.*, Sber. Kais. Akad. Wissensch. Wien **106** (1897), 254–286.

[Mil47] W. H. Mills, *A prime-representing function*, Bull. Amer. Math. Soc. **53** (1947), 604.

[Mir49] L. Mirsky, *The number of representations of an integer as the sum of a prime and a k-free integer*, Amer. Math. Monthly **56** (1949), 17–19.

[Moe] D. Moews, *A list of aliquot cycles of length greater than* 2, available from the author's website: `http://djm.cc/sociable.txt`.

[Moh79] S. P. Mohanty, *The number of primes is infinite*, Bull. Math. Assoc. India **11** (1979), no. 1-2, 62–68.

[Mol97] R. A. Mollin, *Prime-producing quadratics*, Amer. Math. Monthly **104** (1997), no. 6, 529–544.

[Mon94] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, vol. 84, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1994.

[Mor93] P. Moree, *Bertrand's postulate for primes in arithmetical progressions*, Comput. Math. Appl. **26** (1993), no. 5, 35–43.

[Mos58] L. Moser, *On the series,* $\sum 1/p$, Amer. Math. Monthly **65** (1958), 104–105.

[Mos63] ———, *Notes on number theory. III. On the sum of consecutive primes*, Canad. Math. Bull. **6** (1963), 159–161.

[Mot05] Y. Motohashi, *Prime numbers – your gems*, e-print available as `arXiv:math/0512143 [math.HO]`, 2005.

[MP88] H. Maier and C. Pomerance, *On the number of distinct values of Euler's ϕ-function*, Acta Arith. **49** (1988), no. 3, 263–275.

[MS72] H. B. Mann and D. Shanks, *A necessary and sufficient condition for primality, and its source*, J. Combinatorial Theory Ser. A **13** (1972), 131–134.

[MS92] P. L. Montgomery and J. L. Selfridge, *Problem 10230*, Amer. Math. Monthly **99** (1992), 570, solution by D. Ianucci and G. L. Cohen in **102** (1995), 75.

[MS00] P. Moree and P. Stevenhagen, *A two-variable Artin conjecture*, J. Number Theory **85** (2000), no. 2, 291–304.

[MT06] M. R. Murty and N. Thain, *Prime numbers in certain arithmetic progressions*, Funct. Approx. Comment. Math. **35** (2006), 249–259.

[Mur88] M. R. Murty, *Primes in certain arithmetic progressions*, Journal of the Madras University (1988), 161–169.

[Mur01] ———, *Problems in analytic number theory*, Graduate Texts in Mathematics, vol. 206, Springer-Verlag, New York, 2001, Readings in Mathematics.

[MV73] H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika **20** (1973), 119–134.

[MV07] ———, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.

[MW06] H. L. Montgomery and S. Wagon, *A heuristic for the prime number theorem*, Math. Intelligencer **28** (2006), no. 3, 6–9.

[Nag22] T. Nagell, *Zur Arithmetik der Polynome*, Abh. Math. Sem. Hamburg **1** (1922), 178–193.

[Nar00] W. Narkiewicz, *The development of prime number theory: From Euclid to Hardy and Littlewood*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[Nar04] ———, *Elementary and analytic theory of algebraic numbers*, third ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004.

[Nat87a] M. B. Nathanson, *A generalization of the Goldbach-Shnirelman theorem*, Amer. Math. Monthly **94** (1987), no. 8, 768–771.

[Nat87b] ______, *Sums of polygonal numbers*, Analytic number theory and Diophantine problems (Stillwater, OK, 1984), Progr. Math., vol. 70, Birkhäuser Boston, Boston, MA, 1987, pp. 305–316.

[Nat96] ______, *Additive number theory: the classical bases*, Graduate Texts in Mathematics, vol. 164, Springer-Verlag, New York, 1996.

[Nev62] V. Nevanlinna, *Über den elementaren Beweis des Primzahlsatzes*, Soc. Sci. Fenn. Comment. Phys.-Math. **27** (1962), no. 3, 8.

[Nev64] ______, *Über die elementaren Beweise der Primzahlsätze und deren äquivalente Fassungen*, Ann. Acad. Sci. Fenn. Ser. A I No. **343** (1964), 52pp.

[New80] D. J. Newman, *Simple analytic proof of the prime number theorem*, Amer. Math. Monthly **87** (1980), no. 9, 693–696.

[New97] ______, *Euler's ϕ function on arithmetic progressions*, Amer. Math. Monthly **104** (1997), no. 3, 256–257.

[New98] ______, *Analytic number theory*, Graduate Texts in Mathematics, vol. 177, Springer-Verlag, New York, 1998.

[Nie03] P. Nielsen, *An upper bound for odd perfect numbers*, Integers **3** (2003), A14, 9 pp. (electronic).

[Nie07] ______, *Odd perfect numbers have at least nine distinct prime factors*, Math. Comp. **76** (2007), no. 260, 2109–2126 (electronic).

[Niv47] I. Niven, *A simple proof that π is irrational*, Bull. Amer. Math. Soc. **53** (1947), 509.

[Nor61] K. K. Norton, *Remarks on the number of factors of an odd perfect number*, Acta Arith. **6** (1960/1961), 365–374.

[OS09] B.-K. Oh and Z.-W. Sun, *Mixed sums of squares and triangular numbers. III*, J. Number Theory **129** (2009), 964–969.

[Ost56] H.-H. Ostmann, *Additive Zahlentheorie. Erster Teil: Allgemeine Untersuchungen. Zweiter Teil: Spezielle Zahlenmengen*, Ergebnisse der Mathematik und ihrer Grenzgebiete (N.F.), Hefte 7, vol. 11, Springer-Verlag, Berlin, 1956.

[Ped] J. M. Pedersen, *Tables of aliquot cycles*, electronic resource available from the author's website: `http://amicable.homepage.dk/`.

[Pil29] S. S. Pillai, *On some functions connected with $\phi(n)$*, Bull. Amer. Math. Soc. **35** (1929), no. 6, 832–836.

[Pin97] J. Pintz, *Very large gaps between consecutive primes*, J. Number Theory **63** (1997), no. 2, 286–301.

[Pin09] J. P. Pinasco, *New proofs of Euclid's and Euler's theorems*, Amer. Math. Monthly **116** (2009), no. 2, 172–173.

[Pól21] G. Pólya, *Arithmetische Eigenschaften der Reihenentwicklungen rationaler funktionen*, J. Reine Angew. Math. **151** (1921), 1–31.

[Pol08a] P. Pollack, *An explicit approach to Hypothesis H for polynomials over a finite field*, Anatomy of Integers, CRM Proceedings and Lecture Notes, 2008, pp. 259–273.

[Pol08b] ______, *A polynomial analogue of the twin prime conjecture*, Proc. Amer. Math. Soc. **136** (2008), 3775–3784.

[Pol10] ______, *A remark on sociable numbers of odd order*, J. Number Theory **130** (2010), no. 8, 1732–1736.

[Pol11a] ———, *The greatest common divisor of a number and its sum of divisors*, Michigan Math. J. **60** (2011), 199–214.

[Pol11b] ———, *The Möbius transform and the infinitude of primes*, Elem. Math. **66** (2011), 118–120.

[Pol11c] ———, *On Dickson's theorem concerning odd perfect numbers*, Amer. Math. Monthly **118** (2011), 71–77.

[Pol11d] ———, *On Hilbert's solution of Waring's problem*, Cent. Eur. J. Math. **9** (2011), 294–301.

[Pol11e] ———, *On polynomial rings with a Goldbach property*, Amer. Math. Monthly **118** (2011), 71–77.

[Pom77a] C. Pomerance, *Multiply perfect numbers, Mersenne primes, and effective computability*, Math. Ann. **226** (1977), no. 3, 195–206.

[Pom77b] ———, *Problem 6144*, Amer. Math. Monthly **84** (1977), 299–300.

[Pom79] ———, *The prime number graph*, Math. Comp. **33** (1979), no. 145, 399–408.

[Pom81] ———, *On the distribution of amicable numbers. II*, J. Reine Angew. Math. **325** (1981), 183–188.

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

[Pom93] ———, *Problem 10331*, Amer. Math. Monthly **100** (1993), 796, solution by U. Everling in **103** (1996), 701–702.

[Pom98] ———, *Paul Erdős, number theorist extraordinaire*, Notices Amer. Math. Soc. **45** (1998), 19–23.

[Por01] Š. Porubský, *Arithmetically related ideal topologies and the infinitude of primes*, Quaest. Math. **24** (2001), no. 3, 373–391, Dedicated to the memory of John Knopfmacher.

[PP11] P. Pollack and C. Pomerance, *Prime-perfect numbers*, Integers (2011), to appear.

[Pra52] K. Prachar, *Über Primzahldifferenzen*, Monatsh. Math. **56** (1952), 304–306.

[Pri01] W. Pribitkin, *Notes: A Simpler Proof of sin* $\pi z = \pi z \prod_{k=1}^{\infty}(1 - z^2/k^2)$, Amer. Math. Monthly **108** (2001), no. 8, 767–768.

[PS73] R. M. Pollack and H. N. Shapiro, *The next to last case of a factorial diophantine equation*, Comm. Pure Appl. Math. **26** (1973), 313–325.

[PS95] C. Pomerance and A. Sárközy, *Combinatorial number theory*, Handbook of combinatorics, Vol. 1, 2, Elsevier, Amsterdam, 1995, pp. 967–1018.

[PSG02] LSU Problem Solving Group, *Problem 10947*, Amer. Math. Monthly **109** (2002), 476, solution by M. A. Chamberland in **111** (2002), 362.

[Rab13] G. Rabinowitsch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, Proc. Fifth Intern. Math. Congr. **1** (1913), 418–421.

[Rad64] H. Rademacher, *Lectures on elementary number theory*, A Blaisdell Book in the Pure and Applied Sciences, Blaisdell Publishing Co. Ginn and Co. New York-Toronto-London, 1964.

[Ram19] S. Ramanujan, *A proof of Bertrand's postulate*, J. Indian Math. Soc. **11** (1919), 181–182.

[Ram95] O. Ramaré, *On Šnirel′man's constant*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **22** (1995), no. 4, 645–706.

[Ran38] R. A. Rankin, *The difference between consecutive primes*, J. London Math. Soc. **13** (1938), 242–247.

[Rei43] I. Reiner, *Discussions and notes: Functions not formulas for primes*, Amer. Math. Monthly **50** (1943), no. 10, 619–621.

[Ren48] A. Renyi, *On the representation of an even number as the sum of a single prime and single almost-prime number*, Izvestiya Akad. Nauk SSSR. Ser. Mat. **12** (1948), 57–78 (Russian).

[Rén55] A. Rényi, *On the density of certain sequences of integers*, Acad. Serbe Sci. Publ. Inst. Math. **8** (1955), 157–162.

[Rév80] Sz. Gy. Révész, *On the least prime in an arithmetic progression*, Studia Sci. Math. Hungar. **15** (1980), no. 1-3, 83–87.

[Rib96] P. Ribenboim, *The new book of prime number records*, Springer-Verlag, New York, 1996.

[Ric93] H.W. Richmond, *A construction for a polygon of seventeen sides*, Quart. J. Math. **XXVI** (1893), 206–207.

[Ric09] ———, *To construct a regular polygon of* 17 *sides*, Math. Ann. **67** (1909), 459–461.

[Ric33] G. Ricci, *Sul teorema di Dirichlet relativo alla progressione aritmetica*, Boll. Un. Mat. Ital. **12** (1933), 304–309.

[Ric34] ———, *Sui teoremi di Dirichlet e di Bertrand-Tchebychef relativi alla progressione aritmetica*, Boll. Un. Mat. Ital. **13** (1934), 7–17.

[Ric49] H.-E. Richert, *Über Zerfällungen in ungleiche Primzahlen*, Math. Z. **52** (1949), 342–343.

[Ric69] ———, *Selberg's sieve with weights*, Mathematika **16** (1969), 1–22.

[Rie59] B. Riemann, *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse*, Monatsberichte der Berliner Akademie (1859), 671–680.

[Rie53a] G. J. Rieger, *Zur Hilbertschen Lösung des Waringschen Problems: Abschätzung von $g(n)$*, Mitt. Math. Sem. Giessen. **44** (1953), 35 pp.

[Rie53b] ———, *Zur Hilbertschen Lösung des Waringschen Problems: Abschätzung von $g(n)$*, Arch. Math. **4** (1953), 275–281.

[Rie56] ———, *Zum Waringschen Problem fur algebraische Zahlen and Polynome*, J. Reine Angew. Math. **195** (1956), 108–120 (1955).

[Rie73] ———, *Bemerkung zu einem Ergebnis von Erdős über befreundete Zahlen*, J. Reine Angew. Math. **261** (1973), 157–163.

[Rie77] ———, *Sur les nombres de Cullen*, Séminaire de Théorie des Nombres (1976–1977), CNRS, Talence, 1977, pp. Exp. No. 16, 9.

[Rob84] G. Robin, *Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann*, J. Math. Pures Appl. (9) **63** (1984), no. 2, 187–213.

[Roi97] M. Roitman, *On Zsigmondy primes*, Proc. Amer. Math. Soc. **125** (1997), no. 7, 1913–1919.

[Rom34] N. P. Romanov, *Über einige Sätze der additiven Zahlentheorie*, Math. Ann. **109** (1934), 668–678.

[Rub93] M. Rubinstein, *A formula and a proof of the infinitude of the primes*, Amer. Math. Monthly **100** (1993), 388–392.

[RV83] H. Riesel and R. C. Vaughan, *On sums of primes*, Ark. Mat. **21** (1983), no. 1, 46–74.

[Sai06] F. Saidak, *A new proof of Euclid's theorem*, Amer. Math. Monthly **113** (2006), no. 10, 937–938.

[Sal53] H. Salié, *Über abundante Zahlen*, Math. Nachr. **9** (1953), 217–220.

[Sal55] H. Salié, *Über die Dichte abundanter Zahlen*, Math. Nachr. **14** (1955), 39–46.

[SC04] J. Sándor and B. Crstici, *Handbook of number theory. II*, Kluwer Academic Publishers, Dordrecht, 2004.

[Sch12] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, Sitzungsber. Berl. Math. Ges. **11** (1912), 40–50.

[Sch13] E. Schmidt, *Zum Hilbertschen Beweise des Waringschen Theorems*, Math. Ann. **74** (1913), 271–274.

[Sch33] L. G. Schnirelmann, *Über additive Eigenschaften von Zahlen*, Math. Ann. **107** (1933), 649–690.

[Sch40] ———, *Prime numbers*, State Publishing House of Technico-Theoretical Literature, Moscow, 1940.

[Sch59] A. Schinzel, *Démonstration d'une conséquence de l'hypothèse de Goldbach*, Compositio Math. **14** (1959), 74–76.

[Sch60] ———, *On the congruence* $a^x \equiv b \pmod{p}$, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. **8** (1960), 307–309.

[Sch62a] ———, *Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers"*, Acta Arith. **7** (1961/1962), 1–8.

[Sch62b] ———, *On the composite integers of the form* $c(ak+b)! \pm 1$, Nordisk Mat. Tidskr. **10** (1962), 8–10.

[Sch63] ———, *Remarque au travail de W. Sieĭński su les nombres* $a^{2^n}+1$, Colloq. Math. **10** (1963), 137–138.

[Sch74] W. Schwarz, *Einführung in Siebmethoden der analytischen Zahlentheorie*, Bibliographisches Institut, Mannheim, 1974.

[Sel42] E. S. Selmer, *En enkel summasjonsmetode i primtallsteorien, og dens anvendelse på "Bruns sum"*, Norsk mat. tiddskr. **24** (1942), 74–81.

[Sel49a] A. Selberg, *An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*, Ann. of Math. (2) **50** (1949), 297–304.

[Sel49b] ———, *An elementary proof of the prime-number theorem*, Ann. of Math. (2) **50** (1949), 305–313.

[Sel50] ———, *An elementary proof of the prime-number theorem for arithmetic progressions*, Canadian J. Math. **2** (1950), 66–78.

[Sel91] ———, *Collected papers. Vol. II*, Springer-Verlag, Berlin, 1991, With a foreword by K. Chandrasekharan.

[Ser73] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.

[SG] P. Sebah and X. Gourdon, *Introduction to twin primes and Brun's constant computation*, available from the authors' website at the URL `http://numbers.computation.free.fr/Constants/constants.html`.

[SG09] J. Spencer and R. Graham, *The elementary proof of the prime number theorem: With a note on the controversy by E. G. Straus and a postscript by Carl Pomerance*, Math. Intelligencer **31** (2009), no. 3, 18–23.

[SH07] W. G. Stanton and J. A. Holdener, *Abundancy "outlaws" of the form* $\frac{\sigma(N)+t}{N}$, J. Integer Seq. **10** (2007), no. 9, Article 07.9.6, 19 pp. (electronic).

[Sha49a] H. N. Shapiro, *An elementary proof of the prime ideal theorem*, Comm. Pure Appl. Math. **2** (1949), 309–323.

[Sha49b] ———, *Note on a theorem of Dickson*, Bull. Amer. Math. Soc. **55** (1949), 450–452.

[Sha50] ———, *On primes in arithmetic progression. II*, Ann. of Math. (2) **52** (1950), 231–243.

[Sha64] D. Shanks, *An analytic criterion for the existence of infinitely many primes of the form* $\frac{1}{2}(n^2+1)$, Illinois J. Math. **8** (1964), 377–379.

[Sha83] H. N. Shapiro, *Introduction to the theory of numbers*, Pure and Applied Mathematics, John Wiley & Sons, Inc., New York, 1983, A Wiley-Interscience Publication.

[Shi00] D. K. L. Shiu, *Strings of congruent primes*, J. London Math. Soc. (2) **61** (2000), no. 2, 359–373.

[Sho92] V. Shoup, *Searching for primitive roots in finite fields*, Math. Comp. **58** (1992), no. 197, 369–380.

[Sie48] W. Sierpiński, *Remarque sur la répartition des nombres premiers*, Colloquium Math. **1** (1948), 193–194.

[Sie52] ———, *Sur une formule donnant tous les nombres premiers*, C. R. Acad. Sci. Paris **235** (1952), 1078–1079.

[Sie59] ———, *Sur les nombres premiers ayant des chiffres initiaux et finals donnés*, Acta Arith. **5** (1959), 265–266 (1959).

[Sie62] ———, *Sur une conséquence d'une hypothèse sur les polynômes*, Rend. Circ. Mat. Palermo (2) **11** (1962), 283–284.

[Sie64] ———, *Les binômes* x^2+n *et les nombres premiers*, Bull. Soc. Roy. Sci. Liège **33** (1964), 259–260.

[Sie88] ———, *Elementary theory of numbers*, second ed., North-Holland Mathematical Library, vol. 31, North-Holland Publishing Co., Amsterdam, 1988, Edited and with a preface by Andrzej Schinzel.

[SL96] P. Stevenhagen and H. W. Lenstra, Jr., *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37.

[Slo99] J. Slowak, *Odd perfect numbers*, Math. Slovaca **49** (1999), no. 3, 253–254.

[SMC06] J. Sándor, D. S. Mitrinović, and B. Crstici, *Handbook of number theory. I*, Springer, Dordrecht, 2006, Second printing of the 1996 original.

[SO85] W. Scharlau and H. Opolka, *From Fermat to Minkowski: Lectures on the theory of numbers and its historical development*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1985, Translated from the German by Walter K. Bühler and Gary Cornell.

[Sou07] K. Soundararajan, *Small gaps between prime numbers: the work of Goldston-Pintz-Yıldırım*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), no. 1, 1–18 (electronic).

[Spi81] C. Spiro, *The frequency with which an integral-valued, prime-independent, multiplicative or additive function of* n *divides a polynomial function of* n, Ph.D. thesis, University of Illinois, 1981.

[SS58] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208; erratum **5** (1958), 259.

[SS72] H. N. Shapiro and G. H. Sparer, *Composite values of exponential and related sequences*, Comm. Pure Appl. Math. **25** (1972), 569–615.

[Sta91] P. Starni, *On the Euler's factor of an odd perfect number*, J. Number Theory **37** (1991), no. 3, 366–369.

[Sta93] ———, *Odd perfect numbers: a divisor related to the Euler's factor*, J. Number Theory **44** (1993), no. 1, 58–59.

[Sto55] E. Storchi, *Alcuni criteri di divisibilità per i numeri di Mersenne e il carattere* 6^{co}, 12^{mo}, 24^{mo}, 48^{mo}, *dell'interno* 2, Boll. Un. Mat. Ital. (3) **10** (1955), 363–375.

[Sun] Z.-W. Sun, *On universal sums of polygonal numbers*, e-print available as `arXiv:0905.0635 [math.NT]`.

[Sun98] Z.-H. Sun, *On the theory of cubic residues and nonresidues*, Acta Arith. **84** (1998), no. 4, 291–335.

[Sun07] Z.-W. Sun, *Mixed sums of squares and triangular numbers*, Acta Arith. **127** (2007), no. 2, 103–113.

[Sur69] D. Suryanarayana, *Super perfect numbers*, Elem. Math. **24** (1969), 16–17.

[Syl88] J. J. Sylvester, *On certain inequalities relating to prime numbers*, Nature **XXXVIII** (1888), 259–262.

[Ten95] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995, Translated from the second French edition (1995) by C. B. Thomas.

[Tit30] E. C. Titchmarsh, *A divisor problem*, Rend. Circ. Mat. Palermo **54** (1930), 414–429.

[Tit86] ———, *The theory of the Riemann zeta-function*, second ed., The Clarendon Press Oxford University Press, New York, 1986, Edited and with a preface by D. R. Heath-Brown.

[TMF00] G. Tenenbaum and M. Mendès France, *The prime numbers and their distribution*, Student Mathematical Library, vol. 6, American Mathematical Society, Providence, RI, 2000, Translated from the 1997 French original by Philip G. Spain.

[Tou53] J. Touchard, *On prime numbers and perfect numbers*, Scripta Math. **19** (1953), 35–39.

[tR76] H. J. J. te Riele, *A theoretical and computational study of generalized aliquot sequences*, Mathematisch Centrum, Amsterdam, 1976, Mathematical Centre Tracts, No. 74.

[Tul83] M. I. Tulyaganova, *Matrix analogue of Dirichlet's theorem on prime numbers*, Izv. Akad. Nauk UzSSR Ser. Fiz.-Mat. Nauk (1983), no. 3, 34–35 (Russian).

[Tur33] S. Turski, *Décomposition de nombres entiers en sommes de carrés de nombres impairs*, Bull. Soc. Roy. Sci. Liége **2** (1933), 70–71.

[Tur34] P. Turán, *On a theorem of Hardy and Ramanujan*, J. London Math. Soc. **9** (1934), 274–276.

[TV11] R. Thangadurai and A. Vatwani, *The least prime congruent to one modulo n*, Amer. Math. Monthly **118** (2011), 737–742.

[UH39] J. V. Uspensky and M. A. Heaslet, *Elementary Number Theory*, McGraw-Hill Book Company, Inc., New York, 1939.

[Vau70] R. C. Vaughan, *On a problem of Erdős, Straus and Schinzel*, Mathematika **17** (1970), 193–198.

[Vau97] ———, *The Hardy-Littlewood method*, second ed., Cambridge Tracts in Mathematics, vol. 125, Cambridge University Press, Cambridge, 1997.

[VE80] C. Vanden Eynden, *Proofs that $\sum 1/p$ diverges*, Amer. Math. Monthly **87** (1980), no. 5, 394–397.

[Ven70] B. A. Venkov, *Elementary number theory*, Translated from the Russian and edited by Helen Alderson, Wolters-Noordhoff Publishing, Groningen, 1970.

[vL79] H. von Lienen, *Reelle kubische und biquadratische Legendre-Symbole*, J. Reine Angew. Math. **305** (1979), 140–154.

[VP99] C. J. de la Vallée-Poussin, *Sur la fonction $\zeta(s)$ de Riemann et le nombre es nombres premiers inférieurs à une limite donnée*, Mem. Couronnés de l'Acad. Roy. Sci. Bruxelles **59** (1899), 74 pp.

[VW02] R. C. Vaughan and T. D. Wooley, *Waring's problem: a survey*, Number theory for the millennium, III (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 301–340.

[Wag83] S. S. Wagstaff, Jr., *Divisors of Mersenne numbers*, Math. Comp. **40** (1983), no. 161, 385–397.

[Wal72] C. R. Wall, *Density bounds for the sum of divisors function*, The theory of arithmetic functions (Proc. Conf., Western Michigan Univ., Kalamazoo, Mich., 1971), Springer, Berlin, 1972, pp. 283–287. Lecture Notes in Math., Vol. 251.

[Wal81] ———, *Problem 6356*, Amer. Math. Monthly **88** (1981), 623, solution by L. L. Foster in **90** (1983), 215–216.

[Wan37] P. L. Wantzel, *Recherches sur les moyens de reconnaître si un problème de Géometrie se résoudre avec la règle et le compas*, J. Pures Appl. **2** (1837), 366–372.

[Wan02] Y. Wang (ed.), *Goldbach conjecture*, 2nd ed., Series in Pure Mathematics, vol. 4, World Scientific Publishing Co., Singapore, 2002.

[War30] M. Ward, *A generalization of a familiar theorem concerning prime numbers*, J. London Math. Soc. **5** (1930), 106–107.

[War91] E. Waring, *Meditationes algebraicæ*, American Mathematical Society, Providence, RI, 1991, Translated from the Latin, edited and with a foreword by Dennis Weeks, With an appendix by Franz X. Mayer, translated from the German by Weeks.

[WCJ72] C. R. Wall, P. L. Crews, and D. B. Johnson, *Density bounds for the sum of divisors function*, Math. Comp. **26** (1972), 773–777.

[Web70] W. A. Webb, *On $4/n = 1/x + 1/y + 1/z$*, Proc. Amer. Math. Soc. **25** (1970), 578–584.

[Wei00] P. A. Weiner, *The abundancy ratio, a measure of perfection*, Math. Mag. **73** (2000), 307–310.

[Wen95] E. Wendt, *Elementarer Beweis des Satzes, dass in jeder unbegrenzten arithmetischen Progression $my+1$ unendlich viele Primzahlen vorkommen*, J. Reine Angew. Math. **115** (1895), 85–88.

[Wes31] E. Westzynthius, *Über die Verteilung der Zahlen, die zu der n ersten Primzahlen teilerfremd sind*, Comm. Phys. Math. Helsingfors **25** (1931), 1–37.

[Wie09] A. Wieferich, *Beweis des Satzes, daß sich eine jede ganze Zahl als Summe von höchstens neun positiven Kuben darstellen läßt*, Math. Ann. **66** (1909), 95–101.

[Wig07] S. Wigert, *Sur l'ordre de grandeur du nombre des diviseurs d'un entier*, Ark. Mat. **3** (1907), 1–9.

[Win43] A. Wintner, *Eratosthenian Averages*, Waverly Press, Baltimore, 1943.

[Wir59] E. Wirsing, *Bemerkung zu der Arbeit über vollkommene Zahlen*, Math. Ann. **137** (1959), 316–318.

[Wój72] J. Wójcik, *On sums of three squares*, Colloq. Math. **24** (1971/72), 117–119.

[Woo95] T. D. Wooley, *New estimates for smooth Weyl sums*, J. London Math. Soc. (2) **51** (1995), no. 1, 1–13.

[Wri52] E. M. Wright, *The elementary proof of the prime number theorem*, Proc. Roy. Soc. Edinburgh. Sect. A. **63** (1952), 257–267.

[Wun65] M. Wunderlich, *Another proof of the infinite primes theorem*, Amer. Math. Monthly **72** (1965), 305.

[Wun75] ______, *A probabilistic setting for prime number theory*, Acta Arith. **26** (1974/75), 59–81.

[Yam07] T. Yamada, *On the divisibility of odd perfect numbers by a high power of a prime*, e-print available as `arXiv:math/0511410v2 [math.NT]`, 2007.

[Yan82] X. Q. Yang, *A note on* $4/n = 1/x + 1/y + 1/z$, Proc. Amer. Math. Soc. **85** (1982), no. 4, 496–498.

[Yan98] N. Yanagisawa, *A simple proof that* $L(1,\chi) > 0$, Sūgaku **50** (1998), no. 3, 314–315.

[Zag97] D. Zagier, *Newman's short proof of the prime number theorem*, Amer. Math. Monthly **104** (1997), no. 8, 705–708.

[Zau83] T. Zaupper, *A note on unique factorization in imaginary quadratic fields*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **26** (1983), 197–203.

Index