ANALYTIC AND COMBINATORIAL NUMBER THEORY I

(Lecture Notes)

MARTIN KLAZAR

These are lecture notes for the summer semester 2008 of the course *Analytic and combinatorial number theory* (NDMI045, *Analytická a kombinatorická teorie čísel*) which I have been teaching on the Faculty of Mathematics and Physics of the Charles University in Prague. The first booklet (the second one, [25], is for summer semester 2010) covers four major theorems, three on the distribution of prime numbers and one from additive combinatorics: Dirichlet's theorem on prime numbers in arithmetic progression, the Prime Number Theorem, Shnirel'man's theorem on sums of primes, and Roth's theorem on 3-term arithmetic progressions. Actually, I did not have time to lecture on the Prime Number Theorem. I thank Petr Glivický for valuable remarks on the proof of Roth's theorem.

July 2010 Martin Klazar

Contents

Notation

$\lvert X\rvert$, $\#X$	cardinality of a set or sequence X
$\langle C\rangle$	the characteristic function of a condition C, p. 59
(a,b)	the greatest common divisor of a and b, or ordered pair a,b
$[a,b]$	the smallest common multiple of a and b
$a\mid b$	a divides b
$\mathbb{C}$	complex numbers
χ	characters of finite abelian groups, p. 6
$C(m)$	cyclic groups of order m, p. 6
$d(m)$	the number of divisors of m, p. 55
$\exp(z)$	$\sum_{n\ge 0} z^n/n!$
$\varphi(m)$	Euler's function, p. 8
$f(x) \ll g(x)$	same as $f(x) = O(g(x))$
$f(x) = o(g(x))$	$f(x)/g(x) \to 0$
$f(x) \approx g(x)$	$f(x)/g(x) \to 1$
$G(m) = \mathbb{Z}_m^*$	the group of residues coprime to m, p. 8
$L(s,\chi)$	Dirichlet's L-functions, p. 8
$M(m)$	the smallest prime factor of m, p. 51
$\mu(m)$	the Möbius function, p. 58
$\mathbb{N}$	$\{1,2,3,\ldots\}$
$\mathbb{N}_0$	$\{0,1,2,\ldots\}$
$[n]$	$\{1,2,\ldots,n\}$
$\omega(m)$	the number of distinct prime factors of m
p,q	in chapters 1–3 denote prime numbers
$\pi(x)$	the function counting primes, p. 29
$\mathbb{Q}$	rational numbers
$\mathbb{R}$	real numbers
$\vartheta(x)$	Chebyshev's function, p. 33
$\zeta(s)$	the zeta function, p. 36
$\mathbb{Z}$	the integers, $\{\ldots,-2,-1,0,1,2,\ldots\}$

Chapter 1

Dirichlet's theorem on primes in arithmetic progression

Die aufmerksame Betrachtung der natürlichen Reihe der Primzahlen lässt an derselben eine Menge von Eigenschaften wahrnehmen, deren Allgemeinheit durch fortgesetzte Induction zu jedem beliebigen Grade von Wahrscheinlichkeit erhoben werden kann, während die Auffindung eines Beweises, der allen Anforderungen der Strenge genügen soll, mit den grössten Schwierigkeiten verbunden ist. (...) *Erst nachdem ich den von* Legendre *eingeschlagenen Weg ganz verlassen hatte, bin ich auf einen völlig strengen Beweis des Theorems über die arithmetische Progression gekommen. Der von mir gefundene Beweis, welchen ich der Akademie in dieser Abhandlung vorzulegen die Ehre habe, ist nicht rein arithmetisch, sondern beruht zum Theil auf der Betrachtung stetig veränderlicher Grössen.* [1]

G. Lejeune Dirichlet [12]

In 1837, P. Dirichlet (1805–1859) extended earlier partial results of L. Euler (and of A.-M. Legendre, as he himself writes) and proved the following theorem.

[1] For translation see Section 1.5 or [13].

Theorem 1.0.1 (Dirichlet, 1837) *Every arithmetic progression*

$$a, a + m, a + 2m, a + 3m, \dots$$

with coprime $a \in \mathbb{Z}$ *and* $m \in \mathbb{N}$ *contains infinitely many prime numbers.*

In other words, if the greatest common divisor of the numbers $a \in \mathbb{Z}$ and $m \in \mathbb{N}$ is 1, then infinitely many prime numbers have form $p = mn + a$ for some $n \in \mathbb{N}$. Dirichlet's theorem was a starting point of analytic number theory and we devote Chapter 1 to this fundamental and fascinating result.

We start in Section 1.1 with two proofs of the infinitude of primes of the form $p = 4n + 1$ and $p = 4n - 1$, by Euclid's argument and by Euler's analytic method. We present a simple proof of the infinitude of primes of the form $p = qn + 1$ for any prime q. Section 1.2 contains a proof of Theorem 1.0.1. The most difficult step, establishing that $L(1, \chi) \neq 0$ for nonprincipal characters χ, is relegated to Section 1.3. In Section 1.4 we derive decomposition of the multiplicative group $\mathbb{Z}_m^*$ of residues modulo m coprime with m into cyclic factors; $\mathbb{Z}_m^*$ plays an important role in the proof of Dirichlet's theorem but this decomposition is not needed for the proof.

We present a classical version of the proof based on Dirichlet's L-functions $L(s, \chi)$ but we avoid functions of complex variable and work only with real s and real-variable (but generally complex-valued) functions, with the exception of complex logarithm. We derive the required properties of complex logarithm in a self-contained manner in Proposition 1.2.7 and use them also in Chapter 2. Another two proofs of Dirichlet's theorem, one of them partial, are presented in my second booklet [25].

1.1 Cases $p = 4n \pm 1$ and $p = qn + 1$

We begin with Euclid's proof of the infinitude of primes. Suppose that there are only finitely many primes, $p_1, p_2, \dots, p_m$. Consider their product $r = p_1 p_2 \dots p_m$. The number $r + 1$ is bigger than 1 and is divisible by a prime p. But then $p = p_i$ for some i and thus p_i divides also $1 = (r + 1) - r$, which is impossible.

One can modify Euclid's argument so that it proves the infinitude of primes of both forms $4n - 1$ and $4n + 1$. Suppose that there are only finitely many primes of the form $4n - 1$, $p_1, p_2, \dots, p_m$, and consider their product $r = p_1 p_2 \dots p_m$. The number $4r - 1$ is bigger than 1 and odd. The primes in its decomposition have form $4n - 1$ or $4n + 1$ but not all may be of the latter form because then their product $4r-1$ would also have form $4n+1$. Thus $4r-1$ is divisible by at least one prime $p = p_i$ of the form $4n-1$ and we obtain the same contradiction that p divides $1 = 4r - (4r-1)$.

For primes of the form $4n+1$ this argument ceases to work. Instead, we use quadratic residues: $-1 \equiv x^2$ has a solution $x \in \mathbb{Z}$ modulo p if and only if $p = 2$ or $p = 4n+1$. Suppose again that all primes of the form $4n+1$ are $p_1, p_2, \ldots, p_m$ and for $r = p_1 p_2 \ldots p_m$ consider the number $(2r)^2 + 1$. It is divisible by an odd prime p and hence -1 is a quadratic residue modulo p. Thus $p = 4n+1$ and $p = p_i$ divides $1 = (2r)^2 + 1 - 4r^2$, a contradiction.

An ingenious algebraic argument proves Dirichlet's theorem for primes of the form $qn+1$, q prime. It is based on prime divisors of values of polynomials.

Proposition 1.1.1 *The nonzero values $f(m)$, $m \in \mathbb{Z}$, of a nonconstant integral polynomial $f(x)$ are divisible by infinitely many primes.*

Proof. Let

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,\ n \geq 1,\ a_i \in \mathbb{Z},\ a_n \neq 0.$$

The claim holds if $a_0 = 0$. Suppose that $a_0 \neq 0$ and that S is a finite set of primes. We find an m in $\mathbb{Z}$ such that $f(m)$ is nonzero and is divisible by a prime not in S. Let r be the product of the primes in S. For k in $\mathbb{Z}$ we have

$$f(kra_0) = a_0[a_n(kr)^n a_0^{n-1} + a_{n-1}(kr)^{n-1} a_0^{n-2} + \cdots + a_1 kr + 1] = a_0 b.$$

The number b is 1 modulo r, hence is nonzero and not divisible by any prime in S, and equals ± 1 for at most $2n$ values of k. For any k distinct from these values, the number $f(kra_0) = a_0 b \neq 0, -1, 1$ and is divisible by a prime not in S. $\square$

Proposition 1.1.2 *For every prime q there are infinitely many primes p of the form $p = qn+1$.*

Proof. Fix a prime q. By Proposition 1.1.1 we know that the nonzero values $f(m)$, $m \in \mathbb{Z}$, of the polynomial

$$f(x) = 1 + x + x^2 + \cdots + x^{q-1} = \frac{x^q - 1}{x - 1}$$

are divisible by infinitely many primes p. We show that with a single exception all these p are 1 modulo q. Consider $m \in \mathbb{Z}$ and a prime p dividing the value $f(m) \neq 0$. If $m \equiv 1$ modulo p, then $f(m) \equiv q$ modulo p and $q \equiv 0$ modulo p. We get the exception $p = q$. If $p \neq q$, then $m \not\equiv 1$ modulo p. The order of m modulo p then equals q (it is a divisor of q because $m^q \equiv 1$ modulo p but it is not 1) and is a divisor of $p - 1$ (the order of an element divides the order of the whole group, in this case $(\mathbb{Z}_p^*, \cdot)$ with order $p - 1$). Thus $p \equiv 1$ modulo q. $\square$

We recall Euler's analytic proof of the infinitude of primes and present its extension, due also to Euler, to primes of the form $4n - 1$ and $4n + 1$. For every $s > 1$ one has the Euler identity

$$\prod_p \frac{1}{1 - 1/p^s} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

For $s \to 1^+$ the sum of the series on the right goes to $+\infty$ as its partial sums approximate with arbitrary precision partial sums of the divergent series $1 + \frac{1}{2} + \frac{1}{3} + \cdots$. If $p_1, p_2, \ldots, p_m$ were the only primes, the product on the left would go to the finite value $1/(1 - 1/p_1)(1 - 1/p_2) \ldots (1 - 1/p_m)$, which contradicts the equality. Thus there are infinitely many primes. (This argument can be simplified so that the variable s and the infinite product are avoided—see Proposition 2.1.1.)

Back to primes of the form $4n + 1$ and $4n - 1$. We define mappings χ_0 and χ from $\mathbb{Z}$ to $\{-1, 0, 1\}$ by $\chi_0(2n) = \chi(2n) = 0$ and

$$\chi_0(2n + 1) = 1 \quad \text{and} \quad \chi(2n + 1) = (-1)^n$$

and consider, for real s, functions defined by the series

$$L(s, \chi_0) = \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s} = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \cdots$$

and

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \cdots .$$

For $s > 1$ both series converge absolutely and for $s \to 1^+$ the sum of the first series goes to $+\infty$. For $0 < s \leq 1$ the second series converges conditionally (by Leibniz test) and for $s = 1$ has clearly a positive sum

$$L(1, \chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots$$

(equal, in fact, to $\frac{\pi}{4}$). Mappings χ_0 and χ are completely multiplicative, for every $a, b \in \mathbb{Z}$ one has

$$\chi_0(ab) = \chi_0(a)\chi_0(b) \quad \text{and} \quad \chi(ab) = \chi(a)\chi(b).$$

It follows that $L(s, \chi_0)$ and $L(s, \chi)$ have for $s > 1$ product representations

$$L(s, \chi_0) = \prod_p \frac{1}{1 - \chi_0(p)/p^s} \quad \text{and} \quad L(s, \chi) = \prod_p \frac{1}{1 - \chi(p)/p^s}.$$

Multiplying them we get (for $s > 1$)

$$L(s, \chi_0)L(s, \chi) = \prod_{p \equiv 1\ (4)} \frac{1}{(1 - 1/p^s)^2} \prod_{p \equiv -1\ (4)} \frac{1}{1 - 1/p^{2s}}.$$

By Euler's identity, the second product is finite for $s > \frac{1}{2}$ as it is majorized by $\prod_p (1-p^{-2s})^{-1}$. Now let $s \to 1^+$. If there were only finitely many primes of the form $4n+1$, the first product would go to a finite value too and the right side would have a finite limit. But the left side has limit $+\infty$ because $L(s, \chi_0) \to +\infty$ and $L(s, \chi)$ goes to a nonzero limit value $L(1, \chi)$. (We use that $L(s, \chi)$ is continuous for $s > 0$. We establish this and other properties of L-functions in the next section.) We get a contradiction and conclude that there are infinitely many primes of the form $4n+1$. The ratio of both products is

$$\frac{L(s, \chi_0)}{L(s, \chi)} = \prod_{p \equiv -1\ (4)} \frac{1 + 1/p^s}{1 - 1/p^s}.$$

For $s \to 1^+$ the left side goes to $+\infty$. However, the right side would have finite limit if there were finitely many primes of the form $4n - 1$. Hence there are infinitely many of them.

In the next section we describe Dirichlet's generalization of Euler's arguments from $m = 4$ to arbitrary modulus m.

1.2 Proof of Dirichlet's theorem

Suppose that $G = (G, \cdot)$ is a finite abelian group, written multiplicatively, and $\chi:\ G \to \mathbb{C}$ is a mapping such that $\chi(ab) = \chi(a)\chi(b)$ for every a, b and

$\chi(a) \neq 0$ for some a. It follows that $\chi(1_G) = 1$ and that each value $\chi(a)$ lies on the unit circle $|z| = 1$ and is an n-th root of unity, $n = |G|$ being the order of G. Such mappings are called *characters of* G and we write G^* for their set. The *principal character* χ_0, $\chi_0 \equiv 1$, sends everything to 1. The set G^* is endowed with a multiplication: if χ and ψ are characters of G,

$$(\chi\psi)(a) = \chi(a)\psi(a),\ a \in G,$$

defines the character $\chi\psi$ of G. With this multiplication, G^* is an abelian group, the *dual group of* G. The principal character serves as a neutral element and the inverse character is obtained by the complex conjugation, $\chi^{-1}(a) = 1/\chi(a) = \overline{\chi(a)}$. The groups G and G^* are actually isomorphic but we will not need this (see the beginning of Section 1.4).

We denote by $C(n)$ the class of *cyclic groups* of order n; these are the groups of order n generated by a single element, isomorphic to the additive group $\mathbb{Z}_n = (\mathbb{Z}_n, +)$ of residues modulo n.

Proposition 1.2.1 *Let $n \in \mathbb{N}$ and H, G be finite abelian groups.*

1. *If H is a subgroup of G and the factorgroup G/H is $C(n)$, then every character of H has exactly n extensions to a character of G. It follows that*
$$|G^*| = |G/H| \cdot |H^*| = n|H^*|.$$
2. *The dual group of the cyclic group $C(n)$ is $C(n)$.*

Proof. 1. Suppose that $\chi \in H^*$ extends to $\psi \in G^*$ and that the generator of G/H is aH, $a \in G$. So $a^n = b \in H$ and $a^m \notin H$ for $0 < m < n$. Every element $g \in G$ has a unique expression as $g = a^k h$ with $0 \leq k < n$ and $h \in H$. Since $\psi(g) = \psi(a^k h) = \psi(a)^k \chi(h)$, the extension ψ is determined by χ and by the value $\psi(a)$. From $\psi(a)^n = \psi(a^n) = \chi(b)$ it follows that $\psi(a)$ is an n-th root of the number $\chi(b)$. It is easy to check that setting $\psi(a)$ equal to any of these n roots, we get a character ψ of G extending χ and that these n characters are distinct. Also, every $\psi \in G^*$ is an extension of some $\chi \in H^*$, namely of its restriction to H. Thus $|G^*| = n|H^*|$.

2. Let $G = C(n)$, with the generator a. By part 1 (for $H = \{1_H\}$ and $G = C(n)$), $|G^*| = n$ and G^* has n elements χ_r, $0 \leq r < n$, where $\chi_r(a) = \exp(2\pi i r/n)$. Since $\chi_r \chi_s = \chi_{r+s \bmod n}$, $G^* = C(n)^*$ is isomorphic to $\mathbb{Z}_n$ and is $C(n)$. □

Proposition 1.2.2 *Let G be a finite abelian group.*

1. *The dual group G^* has the same number of elements, $|G^*| = |G|$.*
2. *If the element $a \in G$ has order r, then the list*

$$(\chi(a) \mid \chi \in G^*)$$

of all character values on a consists of the r-th roots of unity, each of them repeated $|G|/r$ times.

Proof. We prove parts 1 and 2 together. For $r = 1$ and $a = 1_G$ part 2 holds trivially and therefore we assume that $r > 1$ and $a \neq 1_G$. We set $a_1 = a$ and $G_1 = \langle a_1 \rangle$, the cyclic subgroup generated by $a_1 = a$. If $G_1 \neq G$, we take an element $a_2 \in G \backslash G_1$ and set $G_2 = \langle G_1 \cup \{a_2\} \rangle$. Thus G_2/G_1 is cyclic and $|G_2| > |G_1|$. Continuing this way, after finitely many steps (as $|G| < +\infty$) we obtain a chain of subgroups

$$\{1_G\} = G_0 \subset G_1 \subset \cdots \subset G_k = G$$

such that each factorgroup G_{i+1}/G_i is cyclic. Denoting $r_i = |G_i/G_{i-1}|$, we have $|G| = |G_k| = r_k|G_{k-1}| = r_k r_{k-1}|G_{k-2}| = \cdots = r_k r_{k-1} \dots r_1$. Hence, by part 1 of Proposition 1.2.1,

$$|G^*| = |G_k^*| = r_k|G_{k-1}^*| = r_k r_{k-1}|G_{k-2}^*| = \cdots = r_k r_{k-1} \dots r_1 = |G|,$$

which proves part 1. $G_1 = C(r)$ has r characters and, since a generates G_1, their values on a give all r-th roots of unity, each of them once. Using again the above chain of subgroups with cyclic factors and part 1 of Proposition 1.2.1, we see that each character of G_1 is a restriction of exactly $r_2 r_3 \dots r_k = |G|/r$ characters of G, which proves part 2. □

Part 2 implies that for every $a \in G$, $a \neq 1_G$, there is a $\psi \in G^*$ such that $\psi(a) \neq 1$.

Proposition 1.2.3 *Let G be a finite abelian group of order n, $a \in G$ and $\psi \in G^*$. Then*

$$\sum_{\chi \in G^*} \chi(a) = \begin{cases} n & \dots\ a = 1_G \\ 0 & \dots\ a \neq 1_G \end{cases} \quad \textit{and} \quad \sum_{x \in G} \psi(x) = \begin{cases} n & \dots\ \psi = \chi_0 \\ 0 & \dots\ \psi \neq \chi_0. \end{cases}$$

Also, if $a, b \in G$ then

$$\sum_{\chi \in G^*} \chi(a)\chi(b)^{-1} = \begin{cases} n & \dots\ a = b \\ 0 & \dots\ a \neq b. \end{cases}$$

Proof. If $a = 1_G$, resp. $\psi = \chi_0$, then the first, resp. the second, formula holds trivially. If $a \neq 1_G$, there is a $\psi \in G^*$ such that $\psi(a) \neq 1$ (part 2 of Proposition 1.2.2). Denoting by S the sum in the first formula and changing the summation variable χ to $\psi\chi$, we get the equation

$$S = \sum_{\chi \in G^*} \chi(a) = \sum_{\chi \in G^*} \psi\chi(a) = \sum_{\chi \in G^*} \psi(a)\chi(a) = \psi(a)S.$$

Thus $S = 0$, because $\psi(a) \neq 1$. If $\chi \neq \chi_0$, in the second formula we argue in a similar way, changing the summation variable x to ax where $a \in G$ satisfies $\chi(a) \neq 1$. Finally, the third formula follows from the first upon noting that $\chi(a)\chi(b)^{-1} = \chi(ab^{-1})$. $\square$

For $m \in \mathbb{N}$, we consider the multiplicative group

$$G(m) = \mathbb{Z}_m^* = (\mathbb{Z}_m^*, \cdot)$$

of the residues modulo m coprime to m. Recall that its order equals

$$\varphi(m) = m \textstyle\prod_{p|m}(1 - p^{-1})$$

(Euler function). We pull every character $\chi \in G(m)^*$ back to the function $\chi:\ \mathbb{Z} \to \mathbb{C}$ (denoted by the same symbol),

$$\chi(a) = \begin{cases} 0 & \ldots\ (a, m) > 1 \\ \chi(a \bmod m) & \ldots\ (a, m) = 1. \end{cases}$$

The complete multiplicativity $\chi(ab) = \chi(a)\chi(b)$ remains preserved. These multiplicative mappings $\chi:\ \mathbb{Z} \to \mathbb{C}$, associated with the characters of $G(m)$, are called *modular characters*. If χ is non-principal, by the second formula in Proposition 1.2.3 we have that $\chi(k) + \chi(k+1) + \cdots + \chi(k+m-1) = 0$ for every $k \in \mathbb{N}$ and hence

$$|\chi(k) + \chi(k+1) + \cdots + \chi(k+l)| \leq m - 1$$

for every $k, l \in \mathbb{N}$. (In fact, this holds even with $\varphi(m)$ in place of $m - 1$.)

For real s and a modular character χ, we consider the series

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

In the domain of convergence it defines (in general complex-valued) function $L(s, \chi)$, *Dirichlet's L-function.* We shall work with $L(s, \chi)$ only as functions of real variable s.

Lemma 1.2.4 *Let $a_1, a_2, \ldots, a_n$ be complex numbers and $b_1 \geq b_2 \geq \cdots \geq b_n \geq 0$ be real numbers. Then*

$$|a_1 b_1 + a_2 b_2 + \cdots + a_n b_n| \leq b_1 \max_{m=1,2,\ldots,n} |a_1 + a_2 + \cdots + a_m|.$$

Proof. We set $A_m = a_1 + a_2 + \cdots + a_m$, $A_0 = b_{n+1} = 0$, and transform the sum as

$$\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} (A_i - A_{i-1}) b_i = \sum_{i=1}^{n} A_i (b_i - b_{i+1}).$$

Then

$$\left| \sum_{i=1}^{n} a_i b_i \right| \leq \sum_{i=1}^{n} |A_i| (b_i - b_{i+1}) \leq \max_m |A_m| \cdot \sum_{i=1}^{n} (b_i - b_{i+1}) = b_1 \max_m |A_m|.$$

□

Proposition 1.2.5 *Let χ be a modular character of $G(m)$.*

1. *The series $L(s, \chi)$ converges absolutely for $s > 1$.*
2. *If χ is non-principal, then $L(s, \chi)$ converges conditionally for $s > 0$ and $L(s, \chi)$ is a continuous function for $s > 0$.*
3. *For the principal character, $L(s, \chi_0) \to +\infty$ as $s \to 1^+$.*
4. *For $s > 1$ one has the Euler product representation*

$$L(s, \chi) = \prod_p \frac{1}{1 - \chi(p)/p^s}.$$

5. *$L(s, \chi) \neq 0$ for $s > 1$.*

Proof. 1. This is immediate from $|\chi(n) n^{-s}| = n^{-s}$ and from the fact that the series $\sum n^{-s}$ converges for $s > 1$.

2. We know that non-principal χ satisfies $|\chi(k) + \chi(k+1) + \cdots + \chi(k+l)| \leq m - 1$ for every $k, l \in \mathbb{N}$. Using Lemma 1.2.4 with $a_n = \chi(n)$ and $b_n = n^{-s}$, we get that for every $k, l \in \mathbb{N}$,

$$\left| \sum_{n=k}^{k+l} \frac{\chi(n)}{n^s} \right| \leq \frac{m-1}{k^s}.$$

It follows that $L(s,\chi)$ converges for $s > 0$ and that it converges uniformly for $s > \delta > 0$. It is a sum of continuous functions $\chi(n)n^{-s}$ and therefore it is continuous for $s > 0$.

3. If $s > 1$ and $\chi = \chi_0$, we have

$$L(s,\chi_0) = \sum_{n,\ (n,m)=1} \frac{1}{n^s}.$$

For $s \to 1^+$, $L(s,\chi_0) \to +\infty$ because the partial sums approximate with arbitrary precision partial sums of the series $\sum_{n,\ (n,m)=1} 1/n$. This series is divergent because it includes as a subseries the divergent series $1 + \frac{1}{m+1} + \frac{1}{2m+1} + \frac{1}{3m+1} + \cdots$.

4. For $s > 1$ and $P \in \mathbb{N}$, we consider the finite product

$$S(P) = \prod_{p \le P} \frac{1}{1 - \chi(p)/p^s} = \prod_{p \le P} \sum_{k=0}^{\infty} \frac{\chi(p)^k}{p^{ks}}.$$

Multiplying the finitely many geometric series, we see that

$$S(P) = \sum^{*} \frac{\chi(n)}{n^s}$$

where * signifies summation over $n \in \mathbb{N}$ not divisible by any prime larger than P. Denoting by ** the summation over $n \in \mathbb{N}$ divisible by at least one prime larger than P, we therefore have

$$|L(s,\chi) - S(P)| = \left| \sum^{**} \frac{\chi(n)}{n^s} \right| \le \sum_{n > P} \frac{1}{n^s} < \int_P^{+\infty} \frac{dt}{t^s} = \frac{1}{(s-1)P^{s-1}}.$$

Thus $S(P) \to L(s,\chi)$ as $P \to \infty$.

5. For principal χ this is clear as $L(s,\chi_0)$ is a sum of positive numbers. In general this follows from the Euler product in part 4. Let $s > 1$. To prove that $L(s,\chi) \neq 0$, it suffices to show that there is a $c \in \mathbb{R}$ such that

$$\log \left| \prod_{p \le x} \frac{1}{1 - \chi(p)p^{-s}} \right| = -\sum_{p \le x} \log |1 - \chi(p)p^{-s}| > c$$

holds for every $x > 0$. But $\log |1 - \chi(p)p^{-s}| < \log(1 + |\chi(p)p^{-s}|) < |\chi(p)p^{-s}| = p^{-s}$. Hence the inequality holds for every $x > 0$ with $c = -\sum n^{-s}$. □

Thus $L(s,\chi)$ is defined on $(1,+\infty)$ and for non-principal χ on $(0,+\infty)$. However, for Dirichlet's theorem we will need $L(s,\chi)$ only for $s\in[1,1+\delta)$ for some $\delta>0$ and never for $s<1$. This contrasts with the proof of the PNT in the next chapter where the values of $\zeta(s)$ $(=L(s,\chi_0)$ for $m=1)$ in certain $s\in\mathbb{C}$ with $\mathrm{Re}(s)<1$ are crucial, which agrees with the stronger conclusion of the PNT compared to that of Dirichlet's theorem. Part 5 also follows from the fact that the product $\prod_{\chi\in G(m)^*}L(s,\chi)$ is a positive real number (Proposition 1.3.2).

For Dirichlet's theorem we need to extend the nonvanishing of $L(s,\chi)$ to $s=1$. We postpone the proof of this crucial result to Section 1.3.

Theorem 1.2.6 $L(1,\chi)\neq 0$ *for every non-principal modular character* χ*.*

Using complex logarithm, we extract from the infinite product $L(s,\chi)^{-1}=\prod_p(1-\chi(p)/p^s)$ the series $\sum_p\chi(p)/p^s$. We recall complex logarithm and in the next proposition establish required properties.

For a number $z\in\mathbb{C}\backslash\{0\}$, where $z=|z|\exp(i\arg z)$ has the normalized argument $\arg z$ in $[-\pi,\pi)$, we define

$$\log z=\log|z|+i\arg z,$$

$\log|z|$ being the real logarithm. This complex logarithm $\log:\ \mathbb{C}\backslash\{0\}\to\mathbb{C}$ extends the standard real logarithm $\log:\ \mathbb{R}^+\to\mathbb{R}$ and behaves more or less like it. However, continuity and the identity $\log(z_1z_2)=\log z_1+\log z_2$ in general hold only with the correction term $2\pi i$.

Proposition 1.2.7 *Let* $\log z:\ \mathbb{C}\backslash\{0\}\to\mathbb{C}$ *be the specified complex logarithm.*

1. *Function* $\log z$ *is continuous on* $\mathbb{C}\backslash(-\infty,0]$*.*
2. *For every* n*-tuple of nonzero numbers* $z_1,z_2,\dots,z_n\in\mathbb{C}$ *there is a* $k\in\mathbb{Z}$ *such that*
$$\log(z_1z_2\dots z_n)=\log z_1+\log z_2+\cdots+\log z_n+2k\pi i.$$
3. *If* a_n *are in* $\mathbb{C}$ *and* $a=\prod_{n=1}^{\infty}a_n\neq 0$*, then*
$$\log a=\sum_{n=1}^{\infty}\log a_n+2k\pi i$$
for some $k\in\mathbb{Z}$*.*

4. *For z near 0,* $\log(1+z) = z + O(z^2)$.

5. *Function* $\log z$ *is holomorphic on* $\mathbb{C}\backslash(-\infty, 0]$ *because* $(\log z)' = z^{-1}$ *for every* $z \in \mathbb{C}\backslash(-\infty, 0]$.

6. *For every* $z \in \mathbb{C}$ *with* $|z| < 1$,

$$\log(1+z) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} z^n}{n} \quad \textit{and} \quad \log(1-z)^{-1} = \sum_{n=1}^{\infty} \frac{z^n}{n}.$$

7. *Consequently,* $|\log(1+z) - z| \leq |z|^2$ *for* $|z| \leq \frac{1}{2}$.

Proof. 1. Clear from the definition.

2. It suffices to prove the identity for $n = 2$. If $z_j = |z_j| \exp(i\varphi_j)$ with $\varphi_j \in [-\pi, \pi)$, $j = 1, 2$, then

$$z_1 z_2 = (|z_1| \cdot |z_2|) \exp(i(\varphi_1 + \varphi_2)), \ \varphi_1 + \varphi_2 \in [-2\pi, 2\pi)$$

(by the properties of the complex exponential). Thus also

$$z_1 z_2 = (|z_1| \cdot |z_2|) \exp(i\varphi), \ \varphi \in [-\pi, \pi),$$

where $\varphi = \varphi_1 + \varphi_2 + 2k\pi$ with $k = -1, 0$ or 1. The identity then follows by the definition of log and the identity $\log(|z_1| \cdot |z_2|) = \log |z_1| + \log |z_2|$ for the real logarithm.

3. We assume first that $a \notin (-\infty, 0]$. For every large n, $a_1 a_2 \dots a_n$ is near a and, since $a \neq 0$, a_n is near 1. We fix an ε, $0 < \varepsilon < 1$. By part 1, there is an $N \in \mathbb{N}$ such that for every $n \geq N$ we have $|\log a - \log(a_1 a_2 \dots a_n)| < \varepsilon$ and $|\log a_n| < \varepsilon$. Thus, by part 2, for $n \geq N$ we have

$$\log a = \log(a_1 a_2 \dots a_n) + c_n = \sum_{j=1}^{n} \log a_j + 2k_n \pi i + c_n$$

where $k_n \in \mathbb{Z}$ and $|c_n| < \varepsilon < 1$. These equalities give

$$|k_{n+1} - k_n| \leq \frac{|\log a_{n+1}| + |c_n| + |c_{n+1}|}{2\pi} < \frac{3\varepsilon}{2\pi} < 1$$

and we conclude that $k_N = k_{N+1} = k_{N+2} = \cdots = k$. This conclusion holds for any $0 < \varepsilon < 1$ and the same argument shows that the stabilized value k

is independent of ε (but N of course depends on it). Taking $\varepsilon \to 0$, we get the equality.

If $a \in (-\infty, 0)$, we apply the previous case to $-a$ and get

$$\pi i + \log a = \log(-a) = \log(-1) + \sum_{n=1}^{\infty} \log a_n + 2k\pi i$$

for some $k \in \mathbb{Z}$. Since $\log(-1) = -\pi i$, by rearrangement we have $\log a = \sum_{n=1}^{\infty} \log a_n + 2(k-1)\pi i$.

4. Let $z = a + bi$ with $a, b \in \mathbb{R}$ close to 0. Then

$$\begin{aligned} |\log(1+z) - z| &\leq |\log|1+z| - a| + |\arg(1+z) - b| \\ &= |\log(1+x) - a| + |\arctan y - b| \\ &\text{where } x = \sqrt{(1+a)^2 + b^2} - 1,\ y = b/(1+a). \end{aligned}$$

For $a, b \to 0$, we have $x = a + O(a^2 + b^2)$, $y = b + O(ab)$, $\log(1+x) = x + O(x^2)$, and $\arctan y = y + O(y^3)$. Thus $\log(1+z) - z = O(a^2 + b^2 + ab) = O(|z|^2)$.

5. We fix a $z \in \mathbb{C}\backslash(-\infty, 0]$. For every $u \in \mathbb{C}$ sufficiently close to 0, we have $z + u \in \mathbb{C}\backslash(-\infty, 0]$. Applying on the product $z + u = z(1 + uz^{-1})$ the identity in part 2 and using the estimate in part 4, for $u \to 0$ we get the equality

$$\log(z+u) - \log z = \log(1 + uz^{-1}) + 2k(u) \cdot \pi i = uz^{-1} + 2k(u) \cdot \pi i + O(|u|^2)$$

with some $k(u) \in \mathbb{Z}$. The continuity of log at z shows that $k(u) \equiv 0$. Thus

$$(\log z)' = \lim_{u \to 0} (\log(z+u) - \log z) u^{-1} = z^{-1}.$$

6. This follows from the theory of holomorphic functions. Functions $\log(1+z)$ and $\log(1-z)^{-1}$ are holomorphic for $|z| < 1$ and have there derivatives $(\log(1+z))^{(k)} = (-1)^{k-1}(k-1)!(1+z)^{-k}$ and $(\log(1-z)^{-1})^{(k)} = (k-1)!(1-z)^{-k}$. The two expansions are their Taylor series centered at $z = 0$.

7. For $|z| \leq \frac{1}{2}$ the first expansion gives

$$|\log(1+z) - z| \leq (1/2) \sum_{n=2}^{\infty} |z|^n = \frac{|z|^2}{2(1-|z|)} \leq |z|^2.$$

□

The nuisance with discontinuity of $\log z$ in negative real points can be usually circumvented by multiplying z in advance by -1 as, for example, in the proof of part 3 or in the next proof. Part 5 and the expansions in part 6 will be needed only in the next chapter. In the next proof we use the estimate from part 7, which was derived by the theory of holomorphic functions, but we could get an elementary and fully sufficient estimate $|\log(1+z)-z| < c|z|^2$ for some $c > 0$ simply by obtaining via the mean value theorem explicit constants in the big O's in the proof of part 4. The Taylor expansion of $\log(1+z)$ and Lemma 1.2.4 give the more general inequality $|\log(1+z)-z| \le |z|^2/|1+z|$ that holds for every $|z| < 1$.

The following result is the cornerstone in the proof of Dirichlet's theorem.

Proposition 1.2.8 *If χ is a non-principal modular character, then*

$$\sum_p \frac{\chi(p)}{p^s} = O(1) \quad \text{as} \quad s \to 1^+.$$

For the principal character χ_0, the sum goes to $+\infty$.

Proof. We define $\Delta(z)$ by $\log(1+z) = z + \Delta(z)$. For every $s > 1$ and character χ,

$$\sum_p \log(1-\chi(p)/p^s) = -\sum_p \frac{\chi(p)}{p^s} + \sum_p \Delta(-\chi(p)/p^s).$$

By part 7 of Proposition 1.2.7, $|\Delta(-\chi(p)/p^s)| \le p^{-2s}$. The sum of logarithms is a sum of continuous functions (part 1 of Proposition 1.2.7) and converges uniformly for $s > 1+\delta > 1$, as shown by the last two sums. Therefore it defines on $s > 1$ a continuous function. The last sum is bounded for $s > 1$ because it converges absolutely for $s > \frac{1}{2}$. Hence it suffices to show that for $s \to 1^+$ the sum $\sum_p \log(1-\chi(p)/p^s)$ is bounded if $\chi \ne \chi_0$ and goes to $-\infty$ if $\chi = \chi_0$.

Let $s > 1$. We take logarithm of the reciprocal of the infinite product in part 4 of Proposition 1.2.5, which we can do by part 5. By part 3 of Proposition 1.2.7,

$$\log(L(s,\chi)^{-1}) = \sum_p \log(1-\chi(p)/p^s) + 2k(s)\cdot\pi i, \quad k(s) \in \mathbb{Z}.$$

If $\chi = \chi_0$ then $L(s,\chi_0) > 0$ for every $s > 1$, the equality holds with the real logarithm and $k(s) = 0$. For $s \to 1^+$, $\log(L(s,\chi_0)^{-1}) \to -\infty$ by part 3 of Proposition 1.2.5 and the sum of logarithms goes to $-\infty$ as well.

If $\chi \neq \chi_0$ and $L(1,\chi) \notin (-\infty, 0]$, by the continuity of $L(s,\chi)$ we have $L(s,\chi) \notin (-\infty, 0]$ for every $s \in [1, 1+\delta)$ for some $\delta > 0$. Thus $\log(L(s,\chi)^{-1})$ is continuous on $[1, 1+\delta)$ and hence bounded for $s \to 1^+$. The sum of logarithms is continuous on $(1, 1+\delta)$ and so $k(s) = k$ is a constant independent of s. Hence $\sum_p \log(1 - \chi(p)/p^s)$ is bounded for $s \to 1^+$.

It remains to deal with the case $\chi \neq \chi_0$ and $L(1,\chi) \in (-\infty, 0)$, the case $L(1,\chi) = 0$ being excluded by Theorem 1.2.6. We take logarithm of the infinite product for $(-1)L(s,\chi)^{-1}$ and get

$$\log(-L(s,\chi)^{-1}) = \sum_p \log(1 - \chi(p)/p^s) + 2(k(s) - 1/2) \cdot \pi i, \quad k(s) \in \mathbb{Z}.$$

As $-L(1,\chi)^{-1} > 0$, the function $\log(-L(s,\chi)^{-1})$ is continuous on $[1, 1+\delta)$ and as before $k(s)$ is constant and $\sum_p \log(1-\chi(p)/p^s)$ bounded for $s \to 1^+$.
$\Box$

Proof of Dirichlet's theorem. Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$ satisfy $(a,m) = 1$ and let $s > 1$. By the third formula in Proposition 1.2.3, summation over all characters χ of $G(m)$ gives the identity

$$\sum_\chi \chi(a)^{-1} \sum_p \frac{\chi(p)}{p^s} = \sum_p \sum_\chi \frac{\chi(p)\chi(a)^{-1}}{p^s} = \varphi(m) \sum_{p \equiv a \pmod{m}} \frac{1}{p^s}.$$

If there were finitely many primes of the form $mn + a$, the last sum would be finite and thus bounded for $s \to 1^+$. However, by Proposition 1.2.8 the initial expression is unbounded as $s \to 1^+$, because $\sum_p \frac{\chi(p)}{p^s} \to +\infty$ if $\chi = \chi_0$ and all other sums with $\chi \neq \chi_0$ are bounded. This contradiction shows that there are infinitely many primes of the form $mn + a$. $\Box$

1.3 Nonvanishing of $L(1,\chi)$

To complete the proof of Dirichlet's theorem, we prove that $L(1,\chi) \neq 0$ for non-principal χ (Theorem 1.2.6). We sketch another proof in Section 1.5. For yet another proof see [25]. We begin with refining our findings about the behaviour of L-functions near 1.

Proposition 1.3.1 *Let χ be a modular character of $G(m)$ and $s \to 1^+$.*

1. *If $\chi = \chi_0$, $L(s,\chi_0) = (c+o(1))(s-1)^{-1}$ where $c = \prod_{p|m}(1-1/p) > 0$.*

2. If $\chi \neq \chi_0$, $L(s,\chi) = c + O(s-1)$ where $c = L(1,\chi)$.

Proof. 1. Let $s > 1$. Since

$$\frac{1}{s-1} = \int_1^{+\infty} \frac{dt}{t^s} < \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} < 1 + \int_1^{+\infty} \frac{dt}{t^s} = 1 + \frac{1}{s-1}$$

and

$$L(s,\chi_0) = \prod_{(p,m)=1} \frac{1}{1-1/p^s} = \prod_{p|m}(1-1/p^s) \prod_{p} \frac{1}{1-1/p^s} = \prod_{p|m}(1-1/p^s) \cdot \zeta(s)$$

(by part 4 of Proposition 1.2.5), the asymptotic relation follows.

2. Let $\chi \neq \chi_0$. For $x \geq 1$ and $s \in (\frac{1}{2}, \frac{3}{2})$, we consider the function $f(x,s)$ defined by

$$x^{-s} - x^{-1} = (s-1)f(x,s) \quad \text{for} \quad s \neq 1, \; f(x,1) = -x^{-1}\log x.$$

For each fixed s, $f(x,s) \to 0$ as $x \to +\infty$. Taking the Taylor expansion of $x^{-s} - x^{-1}$ at $s = 1$ with remainder in the Lagrange form, we get that $f(x,s) = -x^{-1}\log x + \frac{1}{2}(s-1)x^{-t}(\log x)^2$ where t lies between 1 and s. Thus, for every $x \geq 1$ and $s \in (\frac{1}{2}, \frac{3}{2})$,

$$|f(x,s)| \leq \frac{\log x}{x} + \frac{(\log x)^2}{4\sqrt{x}} < K$$

with an absolute constant $K > 0$. For $s \neq 1$, the partial derivative by x is

$$f_x(x,s) = \frac{1 - s/x^{s-1}}{(s-1)x^2}.$$

We see that for fixed $s \in (\frac{1}{2}, \frac{3}{2})$, $s \neq 1$, the function $f_x(x,s)$ changes sign only once at $x_s = s^{1/(s-1)}$ and $f(x,s)$ is increasing in x on $[x_s, +\infty)$; the same holds for $f(x,1) = -x^{-1}\log x$, with $x_1 = e$. We estimate x_s. From

$$\log x_s = \frac{\log(1+(s-1))}{s-1} = \sum_{k=1}^{\infty} \frac{(1-s)^{k-1}}{k} < 1 + \frac{1}{2}\sum_{k\geq 1}(1/2)^k = \frac{3}{2}$$

we get that $0 < x_s < \exp(3/2) < 5$. We have

$$L(s,\chi) - L(1,\chi) = \sum_{n=1}^{\infty} \chi(n)(n^{-s} - n^{-1}) = (s-1)\sum_{n=1}^{\infty} \chi(n) f(n,s).$$

Using the properties of $f(x,s)$ and, for $n \geq 5$, Lemma 1.2.4 with $a_n = -\chi(n)$ and $b_n = -f(n,s)$, we see that for $s \in (\frac{1}{2}, \frac{3}{2})$ the last series converges and its sum is uniformly bounded:

$$\left|\sum_{n=1}^{\infty} \chi(n) f(n,s)\right| \leq 4K + \left|\sum_{n=5}^{\infty} \chi(n) f(n,s)\right| \leq 4K + K(m-1).$$

So $L(s,\chi) = L(1,\chi) + O(s-1)$ as $s \to 1^+$. □

Proposition 1.3.2 *Let $m \in \mathbb{N}$. For $s > 1$ we have*

$$\prod_{\chi \in G(m)^*} L(s,\chi) = \prod_{p,\ (p,m)=1} \left(\frac{1}{1-p^{-f(p)s}}\right)^{g(p)} \geq \sum_{n,\ (n,m)=1} \frac{1}{n^{\varphi(m)s}} \geq 1$$

where $f(p)$ is the order of p modulo m and $g(p) = |G(m)|/f(p) = \varphi(m)/f(p)$. In particular, the product $\prod_{\chi \in G(m)^*} L(s,\chi)$ is a positive real number.

Proof. If A is the set of all k-th roots of unity, then $\prod_{\alpha \in A}(1-\alpha x) = 1-x^k$, by the factorization $x^k - 1 = \prod_{\alpha \in A}(x-\alpha)$. Using part 4 of Proposition 1.2.5, part 2 of Proposition 1.2.2 and this identity with $\alpha = \chi(p)$ and $x = 1/p^s$, we express $\prod_\chi L(s,\chi)$ as

$$\prod_\chi \prod_p \frac{1}{1-\chi(p)/p^s} = \prod_p \prod_\chi \frac{1}{1-\chi(p)/p^s} = \prod_p \left(\frac{1}{1-(1/p^s)^{f(p)}}\right)^{g(p)},$$

which proves the equality. The inequality follows upon expanding the factors $1/(1-1/p^{f(p)s})$ into geometric series and multiplying them. □

For our purposes it suffices to know that $\prod_\chi L(s,\chi) \geq 1$ for $s > 1$, which is clear already from the equality.

$G(m)^*$ partitions into the pairs of characters $\{\chi, \chi^{-1}\}$ with $\chi \neq \chi^{-1}$ and the singletons $\{\chi\}$ with $\chi = \chi^{-1}$. Since $\chi^{-1} = \overline{\chi}$, the former *complex characters* attain at least one nonreal value, while the latter *real characters* have only real values $-1, 1$ (and 0 in the modular version).

Corollary 1.3.3 *If χ is a complex character of $G(m)$, then $L(1,\chi) \neq 0$.*

Proof. Suppose that $L(1, \chi) = 0$ for a complex character χ modulo m. Since $\chi^{-1}(n) = \overline{\chi(n)}$, we have also $L(1, \chi^{-1}) = \overline{L(1, \chi)} = 0$. Thus

$$\prod_{\chi \in G(m)^*} L(s, \chi) = O(s-1) \quad \text{for} \quad s \to 1^+$$

because the unbounded factor $L(s, \chi_0) = (c + o(1))/(s-1)$ is overturn by the two factors $L(s, \chi) = O(s-1)$, $L(s, \chi^{-1}) = O(s-1)$ and the other factors are bounded (Proposition 1.3.1). This contradicts the inequality

$$\prod_{\chi \in G(m)^*} L(s, \chi) \geq 1 \quad \text{for} \quad s > 1$$

following from Proposition 1.3.2. □

It remains to prove that $L(1, \chi)$ is nonzero if χ is a (non-principal) real character. We establish this by a clever application of Lemma 1.2.4. For it we need monotonicity of certain coefficients.

Lemma 1.3.4 *For $n \in \mathbb{N}$ and $t \in [0, 1)$, let*

$$b_n = b_n(t) = \frac{1}{n(1-t)} - \frac{t^n}{1-t^n}.$$

Then $b_1 = 1$ and $b_1 \geq b_2 \geq b_3 \geq \cdots \geq 0$.

Proof. Clearly, $b_1 = 1$ and $b_n \to 0$ for $n \to \infty$. Monotonicity and non-negativity of b_n then follow from the inequality $b_n - b_{n+1} \geq 0$, which is a corollary of the inequality $(a_1 + a_2 + \cdots + a_k)/k \geq (a_1 a_2 \ldots a_k)^{1/k}$ (for every $a_i \geq 0$) between the arithmetic and geometric mean:

$$\begin{aligned}
(1-t)(b_n - b_{n+1}) &= \frac{1}{n} - \frac{1}{n+1} - \frac{t^n}{1+t+\cdots+t^{n-1}} + \frac{t^{n+1}}{1+t+\cdots+t^n} \\
&= \frac{1}{n(n+1)} - \frac{t^n}{(1+t+\cdots+t^{n-1})(1+t+\cdots+t^n)} \\
&\geq 0
\end{aligned}$$

because $1 + t + t^2 + \cdots + t^{n-1} \geq n(t^{1+2+\cdots+(n-1)})^{1/n} = nt^{(n-1)/2} \geq nt^{n/2}$ and, similarly, $1 + t + t^2 + \cdots + t^n \geq (n+1)t^{n/2}$, by the mentioned inequality between means. □

Proposition 1.3.5 $L(1,\chi) \neq 0$ *for every real non-principal character of* $G(m)$.

Proof. Let $\chi \in G(m)^*$, $m > 1$ and $\chi \neq \chi_0$, be a real character with $L(1,\chi) = 0$. We derive a contradiction. For $t \in [0,1)$, we start with the identity

$$\sum_{n=1}^{\infty} \frac{\chi(n)t^n}{1-t^n} = \sum_{n=1}^{\infty} \chi(n) \sum_{k=1}^{\infty} t^{kn} = \sum_{n=1}^{\infty} t^n \sum_{d|n} \chi(d)$$

(we can exchange the order of summation because the first series absolutely converges). Thus, setting $c_n = \sum_{d|n} \chi(d)$, we have for the generating function $f(t)$ of the numbers c_n for every $t \in [0,1)$ two expressions:

$$f(t) = \sum_{n=1}^{\infty} c_n t^n = \sum_{n=1}^{\infty} \frac{\chi(n)t^n}{1-t^n}.$$

We let $t \to 1^-$ and derive two contradictory estimates: $f(t) \to +\infty$ by the first expression but, assuming $L(1,\chi) = 0$, $f(t) = O(1)$ by the second expression.

If $n \in \mathbb{N}$ and $n = p_1^{a_1} \dots p_r^{a_r}$ is the prime factorization, then

$$c_n = \sum_{d|n} \chi(d) = \prod_{i=1}^{r} \sum_{d|p_i^{a_i}} \chi(d) = \prod_{i=1}^{r} (1 + \chi(p_i) + \chi(p_i)^2 + \dots + \chi(p_i)^{a_i}).$$

Since the sequence

$$\chi(p_i), \chi(p_i)^2, \chi(p_i)^3, \chi(p_i)^4, \dots$$

is $0,0,0,0,\dots$ (if p_i divides m) or $1,1,1,1,\dots$ or $-1,1,-1,1,\dots$, we see that $c_n \geq 0$ for every n because every factor is nonnegative and that $c_{k^2} \geq 1$ for every $k \in \mathbb{N}$. Thus $f(t) = \sum_{n=1}^{\infty} c_n t^n \to +\infty$ as $t \to 1^-$, because all c_n are nonnegative and infinitely many of them are at least 1.

Using that $0 = L(1,\chi) = \sum_{n \geq 1} \chi(n)/n$ and $f(t) = \sum_{n \geq 1} \chi(n)t^n/(1-t^n)$ we write, for $t \in [0,1)$,

$$-f(t) = \frac{0}{1-t} - f(t) = \sum_{n=1}^{\infty} \chi(n) \left(\frac{1}{n(1-t)} - \frac{t^n}{1-t^n} \right).$$

By Lemma 1.3.4, Lemma 1.2.4 with the choice $a_n = \chi(n)$ and $b_n = 1/n(t-1) - t^n/(1-t^n)$ gives estimate

$$|f(t)| = \left|\sum_{n=1}^{\infty} \chi(n) b_n\right| \leq b_1(m-1) = m-1 \quad \text{for} \quad t \in [0,1).$$

This is a contradiction. □

The proof of Dirichlet's theorem is now complete.

1.4 Decomposition of $\mathbb{Z}_m^*$ into cyclic groups

This section is a remnant from the previous drafts and is not needed for the proof of Dirichlet's theorem but we hope that it is of some interest. We derive a decomposition of the group $G(m) = \mathbb{Z}_m^*$ into cyclic subgroups, described in Theorem 1.4.1 below.

Recall that the dual of any cyclic group G is isomorphic to G. It is easy to see that for two finite abelian groups G and H, $(G \oplus H)^*$ is isomorphic to $G^* \oplus H^*$. As $G(m)$ is, by the theorem below, a direct product of cyclic groups, not only $|G(m)^*| = |G(m)|$ but $G(m)^*$ is isomorphic to $G(m)$. More generally, G^* is isomorphic to G for any finite abelian group G because any such group is a direct product of cyclic groups (see, e.g., Lang [26, Theorem 8.2 in Chapter 1]).

Theorem 1.4.1 *Let $m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ be the prime decomposition of $m \in \mathbb{N}$.*

1. *The group $G(m)$ is isomorphic to the direct product*

$$G(p_1^{e_1}) \oplus G(p_2^{e_2}) \oplus \cdots \oplus G(p_r^{e_r}).$$

2. *If $p > 2$ or if $e \leq 2$, then $G(p^e)$ is cyclic, $G(p^e) = C((p-1)p^{e-1})$.*

3. *For $e \geq 3$, $G(2^e)$ is not cyclic but is a direct product of two cyclic groups, $G(2^e) = C(2) \oplus C(2^{e-2})$.*

The decomposition in part 1 follows from the Chinese remainder theorem, which we now recall.

Theorem 1.4.2 *Let $m_1, m_2, \ldots, m_r \in \mathbb{N}$ be pairwise coprime numbers and $R_i = (\mathbb{Z}_{m_i}, +, \cdot)$ and $R = (\mathbb{Z}_m, +, \cdot)$ be the rings of residue classes modulo m_i, $i = 1, 2, \ldots, r$, and $m = m_1 m_2 \ldots m_r$. The mapping*

$$R \to R_1 \oplus R_2 \oplus \cdots \oplus R_r, \ a \mapsto (a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_r)$$

is a ring isomorphism.

Proof. It is easy to check that this mapping sends 1 to 1, 0 to 0, and preserves addition and multiplication. It is injective, because $a \mapsto (0, \ldots, 0)$ means that a is 0 modulo every m_i, which implies, by the coprimality of m_i, that a is 0 modulo $m_1 m_2 \ldots m_r$. It is also surjective, the domain and the range are finite sets with equal cardinalities: $m = |R| = |R_1 \oplus \cdots \oplus R_r| = m_1 m_2 \ldots m_r$. $\square$

Consequently, this mapping gives an isomorphism of the group of units $G(m)$ of R and the group of units $G(m_1) \oplus \cdots \oplus G(m_r)$ of $R_1 \oplus \cdots \oplus R_r$.

We proceed to part 2 of Theorem 1.4.1 and start with the case $e = 1$. We need an elementary identity for the function $\varphi(m)$ counting numbers $1, 2, \ldots, m$ coprime with m.

Proposition 1.4.3 *For every $n \in \mathbb{N}$,*

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

Proof. If we partition $[n]$ by the equivalence relation $i \sim j \iff (n, i) = (n, j) = d$, then the blocks are in a 1-1 correspondence with divisors d of n and the block corresponding to d has $\varphi(n/d)$ elements. $\square$

Proposition 1.4.4 *For every prime p, the group $G(p)$ is cyclic and $G(p) = C(p-1)$.*

Proof. We consider the field $\mathbb{F}_p = (\mathbb{Z}_p, +, \cdot)$ of residues modulo p. For x in $\mathbb{F}_p^* = \mathbb{F}_p \backslash \{0\}$ we denote $\mathrm{ord}(x)$ the order of x in the group $G(p) = (\mathbb{F}_p^*, \cdot)$. This is a divisor of $|G(p)| = p - 1$. For d dividing $p - 1$, we let H_d denote the set of x in $\mathbb{F}_p^*$ with $\mathrm{ord}(x) = d$. We prove that $|H_d| = 0$ or $|H_d| = \varphi(d)$. Then the equality

$$\sum_{d|(p-1)} |H_d| = |G(p)| = p - 1$$

and the previous identity show that in fact always $|H_d| = \varphi(d)$. In particular, $|H_{p-1}| = \varphi(p-1) > 0$ and there is at least one element with the maximum order $p-1$, generating $G(p)$.

The bound on $|H_d|$ follows from an interplay with the set T_d of x in $\mathbb{F}_p^*$ such that $x^d = 1$. We have $H_d \subset T_d$, and $|T_d| \leq d$ because T_d consists of the roots of the polynomial $x^d - 1$. Suppose that $|H_d| > 0$ and fix an $\alpha \in H_d$. Since $\operatorname{ord}(\alpha) = d$, all d powers $\alpha, \alpha^2, \ldots, \alpha^d$ are distinct. All are elements of T_d and hence $|T_d| = d$ and $T_d = \{\alpha, \alpha^2, \ldots, \alpha^d\}$. From $H_d \subset T_d$ it follows that every element $\beta \in H_d$ is of the form $\beta = \alpha^i$ for some i, $1 \leq i \leq d$. Also, $\alpha^i \in H_d$ if and only if $(i, d) = 1$. Thus $H_d \neq \emptyset$ implies $|H_d| = \varphi(d)$. □

This proof works without change for any finite field $\mathbb{F}_{p^e}$ and shows that the multiplicative group $\mathbb{F}_{p^e}^*$ is cyclic.

For the proof that $G(p^e)$ is cyclic for $e \geq 2$, we need some simple results on congruences.

Proposition 1.4.5 *In the following, p is a prime, $e, k \in \mathbb{N}$, and $a, b \in \mathbb{Z}$.*

1. *Every binomial coefficient $\binom{p}{k}$ with $0 < k < p$ is a multiple of p.*
2. *If $a \equiv b$ modulo p^e, then $a^p \equiv b^p$ modulo p^{e+1}.*
3. *If $p > 2$ and $e \geq 2$ then $(1 + ap)^{p^{e-2}} \equiv 1 + ap^{e-1}$ modulo p^e.*
4. *If $p > 2$ and p does not divide a, then the order of $1 + ap$ in $G(p^e)$ is p^{e-1}.*

Proof. 1. This is immediate from $\binom{p}{k} = \frac{p!}{k!(p-k)!}$.

2. We have $a = b + p^e c$ for some $c \in \mathbb{Z}$. By the binomial theorem,

$$a^p = (b + p^e c)^p = b^p + \binom{p}{1} b^{p-1} (cp^e)^1 + A \equiv b^p \pmod{p^{e+1}}$$

because every term in the sum A is divisible by p^{2e} and thus by p^{e+1}.

3. For $e = 2$ this holds as equality. Suppose this congruence holds for e. Raising it to the power p, part 2 gives

$$(1 + ap)^{p^{e-1}} \equiv (1 + ap^{e-1})^p = 1 + \binom{p}{1} ap^{e-1} + A \pmod{p^{e+1}},$$

where every term in the sum A but the last is divisible by $p^{1+2(e-1)}$ (1 comes from the binomial coefficient by part 1) and thus by p^{e+1} (because $e \geq 2$).

The last term in A is divisible by $p^{p(e-1)}$ and thus also by p^{e+1} (because $p \geq 3$, here $p = 2$ fails). Hence $(1+ap)^{p^{e-1}} \equiv 1+\binom{p}{1}ap^{e-1} = 1+ap^e$ modulo p^{e+1}.

4. It suffices to prove that the p^{e-1}-th power of $1 + ap$ is 1 modulo p^e but the p^{e-2}-th power is not. But this is clearly so by the congruence in part 3, applied with $e + 1$ and e, respectively. $\square$

Proposition 1.4.6 *For every prime $p > 2$ and $e \in \mathbb{N}$, the group $G(p^e)$ is cyclic.*

Proof. Let g be the generator of $G(p)$, which exists by Proposition 1.4.4. This means that $g^{p-1} \equiv 1$ modulo p but $g^i \not\equiv 1$ modulo p for every $0 < i < p - 1$. We may assume that $g^{p-1} \not\equiv 1$ modulo p^2. (Otherwise we replace g with $g + p$, which is still a generator of $G(p)$, and then $(g + p)^{p-1} \equiv g^{p-1}+(p-1)g^{p-2}p \pmod{p^2}$ by the binomial theorem and $1+(p-1)g^{p-2}p \not\equiv 1 \pmod{p^2}$.) We show that this g is a generator of $G(p^e)$.

Let $g^n \equiv 1 \pmod{p^e}$, we need to show that then $\varphi(p^e) = (p-1)p^{e-1}$ divides n. We write $g^{p-1} = 1 + ap$ where $a \in \mathbb{Z}$ is not divisible by p. Since

$$1 \equiv (g^n)^{p-1} = (g^{p-1})^n = (1 + ap)^n \pmod{p^e},$$

part 4 of Proposition 1.4.5 tells us that p^{e-1} divides n. We write $n = p^{e-1}m$. Since $g^p \equiv g$ modulo p (the little theorem of Fermat or from $g^{p-1} \equiv 1$ modulo p),

$$1 \equiv g^n = (g^{p^{e-1}})^m \equiv g^m \pmod{p}.$$

Thus $p - 1$ divides m, since g generates $G(p)$, and $p^{e-1}(p - 1)$ divides n. $\square$

It remains to prove part 3 of Theorem 1.4.1. (The case $p = 2$ and $e = 2$ is trivial, $G(2^2) = C(2)$.)

Proposition 1.4.7 *Let $e \in \mathbb{N}$, $e \geq 3$.*

1. *The number 5 has in $G(2^e)$ order 2^{e-2}.*

2. *The 2^{e-1} odd numbers*

$$M = \{(-1)^a 5^b \mid a = 0, 1 \textit{ and } 0 \leq b < 2^{e-2}\}$$

are pairwise noncongruent modulo 2^e. Hence $G(2^e) = C(2) \oplus C(2^{e-2})$.

Proof. 1. We show that $5^{2^{e-3}} \equiv 1 + 2^{e-1}$ modulo 2^e. This congruence, applied with $e+1$ and e, proves the claim on order of 5. For $e = 3$ it holds as equality. Suppose it holds for some $e \geq 3$. Squaring it, we get $5^{2^{e-2}} \equiv (1 + 2^{e-1})^2$ modulo 2^{e+1} (by part 2 of Proposition 1.4.5). But this is $1 + 2^e + 2^{2e-2} \equiv 1 + 2^e$ modulo 2^{e+1} (since $e \geq 3$).

2. Suppose that $(-1)^a 5^b \equiv (-1)^{a'} 5^{b'}$ modulo 2^e, with a, a', b, b' in the stated ranges. Modulo 4 this gives that $(-1)^a \equiv (-1)^{a'}$ and a and a' have the same parity, so $a = a'$. Thus $5^b \equiv 5^{b'}$ modulo 2^e. By part 1, $b - b'$ is divisible by 2^{e-2} and $b = b'$. The elements of M are therefore mutually noncongruent modulo 2^e. They are all coprime with 2^e and $|M| = \varphi(2^e) = 2^{e-1}$. So under multiplication modulo 2^e, M is isomorphic to $G(2^e)$. On the other hand, the form of elements in M shows that the group M is also isomorphic to $C(2) \oplus C(2^{e-2})$. □

This completes the proof of Theorem 1.4.1.

We conclude this section by a characterization of m with cyclic group $G(m)$. The generators of $G(m)$, if they exist, are called *primitive roots modulo m.*

Corollary 1.4.8 *The modulus $m \in \mathbb{N}$ has a primitive root if and only if m is one of the numbers $2, 4, p^e, 2p^e$, for a prime $p > 2$ and $e \in \mathbb{N}$.*

Proof. In the stated cases m has a primitive root because $G(2) = C(1)$ and $G(4) = C(2)$, and, by Theorem 1.4.1, $G(p^e) = C((p-1)p^{e-1})$ and $G(2p^e)$ is isomorphic to $G(2) \oplus G(p^e) = G(p^e)$. If m is not in the stated form, Theorem 1.4.1 shows that $G(m)$ is a direct product of several cyclic groups, of which at least two have even order. Thus $G(m)$ has at least two elements of order 2 and therefore cannot be cyclic (any cyclic group has at most one element of order 2). □

1.5 Remarks

The proof of Dirichlet's theorem in the case $p = qn + 1$ in Section 1.1 is taken from Iwaniec and Kowalski [22, Chapter 2.3]. Bateman and Low [6] extend the argument for $p = 4n + 1$ based on quadratic residues to the cases $p = 24n + 1, 5, 7, 11, 13, 17, 19, 23$. Section 1.2 was inspired by Serre [43, Chapter VI]; later I found on the Internet presentation by Chapman [9] along similar lines. The proof of $L(1, \chi) \neq 0$ for real χ in Section 1.3 is due to Monsky [28], who simplified an argument given by Gelfond and Linnik [16, Chapter 3.2]. Section 1.4 follows the textbook of Ireland and Rosen [21, Chapters 3 and 4].

I included Proposition 1.2.7 on complex logarithm in order to keep the proof of Dirichlet's theorem self-contained and explicit. Study of several renderings of Dirichlet's theorem in the literature has shown me that the (lack of) justification of the step

$$L(s,\chi)=\prod_p \frac{1}{1-\chi(p)p^{-s}} \rightsquigarrow \log L(s,\chi)=\sum_p \log(1-\chi(p)p^{-s})^{-1}=\cdots$$

is often problematic (e.g., see [43, p. 74]). We stress that as far as this step is employed and $\log z$ with complex argument is invoked, the proof cannot be regarded as only real variable proof (cf. [9]).

My translation of the opening quotation from Dirichlet's memoir:

> Careful inspection of the sequence of prime numbers reveals multitude of its properties, whose general validity can be established by repeated checks to any degree of certainty, while quest for a proof that should fulfil all requirements of exactness meets with highest difficulties. (...) Only after having completely abandoned search in the direction started by Legendre, did I arrive at a fully rigorous proof of the theorem about arithmetic progression. The proof which I have found and which I have the honor to submit to the Academy in this tract, is not purely arithmetical but is based in part on considering continuously varying quantities.

See [13] for the translation of Dirichlet's memoir. For the life and work of Dirichlet see Elstrodt [14].

In [12], Dirichlet proves his theorem for the case of prime modulus and the case of composite modulus only sketches. At the end he writes that originally he had a complicated argument showing $L(1,\chi)\neq 0$ for χ of composite modulus but later discovered an interesting connection between $L(s,\chi)$ and the theory of quadratic forms, which gives nonvanishing of $L(1,\chi)$ in complete generality as a corollary, and so he decided to deal with this matter in detail elsewhere. The connection that Dirichlet discovered includes his remarkable *class number formula* (Varadarajan [48])

$$h(d) = \begin{cases} \frac{w\sqrt{|d|}}{2\pi} L(1,\chi_d) & \text{if } d < 0 \\ \\ \frac{\sqrt{d}}{\log \alpha} L(1,\chi_d) & \text{if } d > 0. \end{cases}$$

Here $d \in \mathbb{Z}$ is a *fundamental discriminant*, meaning that $d = 4n + 1$ and d is square-free or $d = 16n + 8, 12$ and $d/4$ is square-free; $h(d)$ is the number of equivalence classes of the quadratic forms $ax^2 + bxy + cy^2$ with discriminant $d = b^2 - 4ac$ and coprime coefficients $a, b, c \in \mathbb{Z}$, under the action of the matrix group $\mathrm{SL}_2(\mathbb{Z})$; in other words, $h(d)$ is the class number of the quadratic number field $\mathbb{Q}[\sqrt{d}]$; $\chi_d(n) = (\frac{d}{n})$, so called Kronecker's symbol, is an extension of Legendre's symbol from the theory of quadratic residues; $w = 2, 4$ or 6 as $d < -4$, $d = -4$ or $d = -3$, respectively; and, finally, $\alpha = \frac{1}{2}(x_0 + y_0\sqrt{d})$ where $x_0, y_0 \in \mathbb{N}$ is the smallest solution to the Pell equation $x^2 - dy^2 = 4$, so α is the primitive unit in the ring of integers of $\mathbb{Q}[\sqrt{d}]$. Because $h(d) \neq 0$, in fact $h(d) \in \mathbb{N}$, and every real character χ has the form $\chi = \chi_d$ for some fundamental discriminant d, a corollary of this formula is that $L(1, \chi) \neq 0$.

An alternative proof of nonvanishing of $L(1, \chi)$ based on properties of holomorphic functions, especially those defined by Dirichlet series, goes as follows (e.g., [43, Chapter VI]). The proof of continuity of $L(s, \chi)$ for $s > 0$ and $\chi \neq \chi_0$ gives in the complex domain $s \in \mathbb{C}$ that $L(s, \chi)$ is holomorphic for $\mathrm{Re}(s) > 0$. Also, $L(s, \chi_0) - c(s - 1)^{-1}$, $c = \prod_{p|m}(1 - p^{-1})$, is holomorphic for $\mathrm{Re}(s) > 0$ (see part 1 of Proposition 1.3.1 and part 5 of Proposition 2.3.1). Now assume for the contrary that $L(1, \psi) = 0$ for a non-principal character ψ modulo m. Then, on the one hand, the product

$$P(s) = \prod_{\chi \in G(m)^*} L(s, \chi)$$

defines a function holomorphic for $\mathrm{Re}(s) > 0$ as the pole of $L(s, \chi_0)$ at $s = 1$ is cancelled by the zero of $L(s, \psi)$ at the same point. On the other hand, by Proposition 1.3.2, for $\mathrm{Re}(s) > 1$ this function is also given by Dirichlet series

$$S(s) = \sum_{n \geq 1} \frac{a_n}{n^s} = \prod_{p,\ (p,m)=1} \Big(\sum_{k \geq 0} \frac{1}{p^{kf(p)s}} \Big)^{g(p)}$$

where $a_n \in \mathbb{N}_0$. The lower bound in Proposition 1.3.2 shows that there is a real number $\kappa \in [1/\varphi(m), 1]$ such that the series $S(s)$ converges for $s > \kappa$

but diverges for $s = \kappa$. By a theorem on Dirichlet series with nonnegative real coefficients, due to E. Landau, $S(s)$ defines a function holomorphic for $\mathrm{Re}(s) > \kappa$ but with a singularity at $s = \kappa$. This contradicts uniqueness of holomorphic extensions: $S(s) = P(s)$ for $\mathrm{Re}(s) > 1$ and $P(s)$ is holomorphic for $\mathrm{Re}(s) > 0$.

Proofs of Dirichlet's theorem can be found in Chandrasekharan [8, Chapter 10], Chapman [9], Hermoso [19], Ireland and Rosen [21, Chapter 16], Iwaniec and Kowalski [22, Chapter 2.3], Montgomery and Vaughan [29, Chapter 4.3], Nathanson [32, Chapter 10], Pollack [36, Chapter 2], Pollack [37, Chapter 4], Selberg [42], Serre [43, Chapter VI], Shapiro [44], Varadarajan [48, Chapter 6.1] and many other sources. For a view of Dirichlet's theorem from the point of logic see Avigad [3].

Chapter 2

The Prime Number Theorem

Le plus court chemin entre deux vérités dans le domaine réel passe par le domaine complexe.

The shortest path between two truths in the real domain passes through the complex domain.

J. Hadamard, apocryphal quote

The very first question one can ask about the infinite sequence of prime numbers,

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,\ p_6 = 13,\ p_7 = 17,\ p_8 = 19,\ \ldots,$$

is how fast it grows. Around 1800, young C. F. Gauss conjectured that for large x the number of primes not exceeding x is nearly

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

$\mathrm{Li}(x) \approx x/\log x$ in the first approximation but on finer scale $\mathrm{Li}(x)$ deviates markedly from $x/\log x$. Gauss' conjecture was proved one century later independently by J. Hadamard (1865–1963) and Ch. de la Valée Poussin (1866–1962).

Theorem 2.0.1 (Hadamard, de la Valée Poussin, 1896) *The number of prime numbers that are smaller or equal to x is asymptotic to $x/\log x$.*

This is usually called *the Prime Number Theorem (PNT).* We state it in the traditional 'explicit' form with $x/\log x$ but it should be noted that Hadamard and de la Valée Poussin proved the more precise version with the main term $\mathrm{Li}(x)$ and certain error term. Using the standard notation for the number of primes not exceeding x,

$$\pi(x) = |\{p \mid p \le x\}|,$$

we can write the PNT as

$$\pi(x) = (1 + o(1))\frac{x}{\log x} \quad \text{where} \quad x \to +\infty.$$

For the sequence of primes $(p_n)_{n\ge 1}$ this gives for $n \to \infty$ the asymptotic relation $p_n \approx n \log n$.

In Proposition 2.1.1 we present in a simple form the analytic approach to primes and derive by means of it that $\pi(x) \to +\infty$ and, on the other hand, an upper bound on $\pi(x)$ showing that primes form a sparse subset of $\mathbb{N}$; this argument (in part 4) goes back to Legendre. In Proposition 2.1.4 and Corollary 2.1.5 we prove the classical bounds $x/\log x \ll \pi(x) \ll x/\log x$ obtained first by Chebyshev around 1850. Section 2.2 contains a proof of the PNT. It is short but we achieve this by the usual trick of moving the hardest steps to separate places, Sections 2.3 and 2.4. The proof uses basic complex analysis — properties of holomorphic functions, especially $\zeta(s)$ — and goes back to N. Wiener, with further simplifications due to D. J. Newman.

2.1 Chebyshev's bounds on $\pi(x)$

Recall that if x is real, $\pi(x)$ denotes the number of primes $\le x$.

Proposition 2.1.1 *For every real $x > 1$ we have the estimate*

$$\prod_{p\le x} \frac{1}{1 - 1/p} > \log x.$$

It has the following corollaries.

1. *For $x \to +\infty$, $\pi(x) \to +\infty$ — the set of prime numbers is infinite.*

2. For every $x > 1$,

$$\sum_{p \le x} \frac{1}{p} > \log\log x - 1.$$

3. For every $x > 1$,

$$0 < \prod_{p \le x} (1 - 1/p) < \frac{1}{\log x}.$$

4. For $x \to +\infty$, $\pi(x) = o(x)$ — the set of prime numbers is sparse.

Proof. The estimate follows from

$$\prod_{p \le x} \frac{1}{1 - 1/p} = \prod_{p \le x} (1 + p^{-1} + p^{-2} + \cdots) \ge \sum_{n \le x} \frac{1}{n} > \int_1^{\lfloor x \rfloor + 1} \frac{dt}{t} > \log x.$$

The first and key inequality is implied by the fact that every number $n \le x$ is a product of powers of distinct primes not exceeding x. Note that the uniqueness of this expression is not needed.

1. By the estimate, for $x \to +\infty$ the product goes to $+\infty$ and cannot be finite.

2. Comparing the Taylor expansions of $\log(1+x)$ and $\log(1-x)^{-1}$, we get that

$$\begin{aligned}
\log(1 + p^{-1}) &= \log(1 - p^{-1})^{-1} - \sum_{k \ge 1} \frac{2}{2kp^{2k}} \\
&> \log(1 - p^{-1})^{-1} - \sum_{k \ge 1} \frac{1}{p^{2k}} \\
&= \log(1 - p^{-1})^{-1} - \frac{1}{p^2 - 1}.
\end{aligned}$$

Thus, for $x > 1$,

$$\begin{aligned}
\sum_{p \le x} \log(1 + p^{-1}) &> \sum_{p \le x} \log(1 - p^{-1})^{-1} - \sum_{n=2}^{\infty} \frac{1}{n^2 - 1} \\
&> \sum_{p \le x} \log(1 - p^{-1})^{-1} - \sum_{n=2}^{\infty} \frac{1}{n(n-1)} \\
&= \sum_{p \le x} \log(1 - p^{-1})^{-1} - 1
\end{aligned}$$

and, using the initial estimate,

$$\begin{aligned}
\sum_{p\le x}\frac{1}{p} &> \sum_{p\le x}\sum_{k\ge 1}\frac{(-1)^{k-1}}{kp^k} = \sum_{p\le x}\log(1+p^{-1})\\
&> \sum_{p\le x}\log(1-p^{-1})^{-1} - 1 = \log\prod_{p\le x}\frac{1}{1-p^{-1}} - 1\\
&> \log\log x - 1.
\end{aligned}$$

3. This is the reciprocal form of the estimate.

4. Let $\varepsilon > 0$ be given. We show that $\pi(n) < \varepsilon n$ for every $n > N$. Recall that in every interval $k+1, k+2, \ldots, k+m$ of m consecutive integers,

$$\varphi(m) = m\prod_{p|m}(1-1/p)$$

are coprime with m. Using part 3, we fix m so that $\prod_{p|m}(1-1/p) < \varepsilon/2$ and then take $N \in \mathbb{N}$ so that $n > N$ implies $m < (\varepsilon/2)n$. Then, for $n > N$,

$$\pi(n) \le m + \varphi(m)\tfrac{n}{m} = m + n\prod_{p|m}(1-1/p) < (\varepsilon/2)n + n(\varepsilon/2) = \varepsilon n,$$

where the first inequality follows from the fact that if $p \le n$ then $p \le m$ or $m < p \le n$ but $(p, m) = 1$. □

Proposition 2.1.2 *For every $n \in \mathbb{N}$, we have the following estimates.*

1. $\binom{2n}{n} \ge \frac{4^n}{2n+1}$.
2. $\binom{2n+1}{n} \le 4^n$.
3. $\binom{2n}{n} \le (2n)^{\pi(2n)}$.
4. $\prod_{p\le n} p \le 4^n$.

Proof. 1. This estimate follows from the binomial expansion $4^n = (1+1)^{2n} = \sum_{k=0}^{2n}\binom{2n}{k}$ and the inequalities $\binom{2n}{k} \le \binom{2n}{n}$, $0 \le k \le 2n$.

2. Since $2\cdot 4^n = (1+1)^{2n+1} = \sum_{k=0}^{2n+1}\binom{2n+1}{k} \ge \binom{2n+1}{n} + \binom{2n+1}{n+1} = 2\binom{2n+1}{n}$.

3. This follows from the fact that no prime factor p of $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$ exceeds $2n$ and from the inequality $p^a \le 2n$ for the highest power of p dividing $\binom{2n}{n}$. Indeed,

$$a = \sum_{k=1}^{\infty} \left(\lfloor 2n/p^k \rfloor - 2\lfloor n/p^k \rfloor \right) \le \sum_{k,\ p^k \le 2n} 1, \quad \text{thus} \quad p^a \le 2n,$$

because $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$, the highest exponent b with which p^b divides $m!$ is $b = \lfloor m/p \rfloor + \lfloor m/p^2 \rfloor + \cdots$, $\lfloor 2\alpha \rfloor - 2\lfloor \alpha \rfloor \le 1$ for every $\alpha \in \mathbb{R}$ and $\lfloor 2\alpha \rfloor - 2\lfloor \alpha \rfloor = 0$ if $0 \le 2\alpha < 1$.

4. We proceed by induction on n. For $n = 1$ and 2 the estimate holds. For even $n > 2$ it holds because $\prod_{p \le n} p = \prod_{p \le n-1} p \le 4^{n-1} < 4^n$. For odd $n = 2m + 1 > 1$ we split the product as

$$\prod_{p \le n} p = \Bigg(\prod_{p \le m+1} p \Bigg) \Bigg(\prod_{m+1 < p \le 2m+1} p \Bigg).$$

The first product is $\le 4^{m+1}$ by induction. The second product divides $\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$ and thus is at most 4^m by part 2. Hence

$$\prod_{p \le n} p \le 4^{m+1} \cdot 4^m = 4^n.$$

$\square$

Setting $n = \lfloor x \rfloor$ in part 4 and taking logarithm, we get the next bound.

Corollary 2.1.3 *For every real $x > 1$,*

$$\sum_{p \le x} \log p \le (2 \log 2) x.$$

Proposition 2.1.4 *For every real $\delta > 1$ and $x \ge 2$,*

$$\frac{(\log 2)x}{\log x} - 4 < \pi(x) < \frac{(2\delta \log 2)x}{\log x} + x^{1/\delta}.$$

Proof. To obtain the lower bound, we take logarithm of the inequality in part 3 of Proposition 2.1.2 and estimate $\log \binom{2n}{n}$ from below by part 1:

$$\pi(2n) \ge \frac{(\log 4)n - \log(2n+1)}{\log(2n)} > \frac{(\log 2)2n}{\log(2n)} - 2.$$

For $x \geq 2$, we take the unique $n \in \mathbb{N}$ such that $2n \leq x < 2n + 2$ and get

$$\pi(x) \geq \pi(2n) > \frac{(\log 2)2n}{\log(2n)} - 2 > \frac{(\log 2)(x-2)}{\log x} - 2 \geq \frac{(\log 2)x}{\log x} - 4.$$

The upper bound follows from Corollary 2.1.3: for fixed $\delta > 1$,

$$2(\log 2)x > \sum_{x^{1/\delta} < p \leq x} \log p \geq (\pi(x) - \pi(x^{1/\delta})) \log(x^{1/\delta}) \geq \frac{(\pi(x) - x^{1/\delta}) \log x}{\delta}$$

or

$$\frac{(2\delta \log 2)x}{\log x} + x^{1/\delta} > \pi(x).$$

□

For large x we obtain the following estimate.

Corollary 2.1.5 *For every $\varepsilon > 0$ there is an $x_0 = x_0(\varepsilon)$ such that if $x > x_0$ then*

$$\frac{(\log 2 - \varepsilon)x}{\log x} < \pi(x) < \frac{(2\log 2 + \varepsilon)x}{\log x}.$$

2.2 Proof of the Prime Number Theorem

We prove the PNT (Theorem 2.0.1). We know the *Chebyshev function*

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

from Corollary 2.1.3: $\vartheta(x) \leq (2\log 2)x$ for $x \geq 1$. First we show that the stronger relation $\vartheta(x) = x + o(x)$, $x \to +\infty$, is equivalent with the PNT.

Proposition 2.2.1 *For $x \to +\infty$, we have the equivalence*

$$\pi(x) = \frac{x + o(x)}{\log x} \iff \vartheta(x) = x + o(x).$$

Proof. This follows from the estimates

$$\begin{aligned} \frac{\vartheta(x)}{\log x} \leq \pi(x) &\leq \frac{\vartheta(x)}{\log x}(1 + O(\log\log x/\log x)) + \frac{x}{(\log x)^2} \\ &= \frac{\vartheta(x)}{\log x} + O(x(\log\log x)/(\log x)^2). \end{aligned}$$

The lower bound is immediate from $\sum_{p\le x}\log p \le \pi(x)\log x$. As for the upper bound, from $\vartheta(x) \ge \sum_{y<p\le x}\log p \ge (\pi(x)-\pi(y))\log y$ we get

$$\pi(x) \le \frac{\vartheta(x)}{\log y} + \pi(y) \le \frac{\vartheta(x)}{\log y} + y.$$

Setting $y = x/(\log x)^2$, we get the upper bound. $\square$

Proposition 2.2.2 *If the integral*

$$\int_1^{+\infty} \frac{\vartheta(x)-x}{x^2}\,dx = \int_0^{+\infty} (\vartheta(\mathrm{e}^t)\mathrm{e}^{-t}-1)\,dt$$

converges then $\vartheta(x) = x + o(x)$ for $x \to +\infty$ and hence the PNT holds.

Proof. The second integral is obtained from the first by the substitution $x = \mathrm{e}^t$. Suppose that $\vartheta(x) \ne x + o(x)$ as $x \to +\infty$. This means that $\limsup \vartheta(x)/x > 1$ or $\liminf \vartheta(x)/x < 1$. Suppose the first case occurs, the second is similar. There exists a $\lambda > 1$ such that for every $y > 0$ there is an x, $x > y$, with $\vartheta(x) > \lambda x$. The integral of $(\vartheta(t)-t)t^{-2}$ over the interval $[x, \lambda x]$ is (since $\vartheta(t)$ is nondecreasing)

$$\int_x^{\lambda x} \frac{\vartheta(t)-t}{t^2}\,dt > \int_x^{\lambda x} \frac{\lambda x - t}{t^2}\,dt = \int_1^{\lambda} \frac{\lambda - u}{u^2}\,du = c > 0$$

where the constant c depends only on λ. So

$$\lim_{r\to+\infty} \int_1^r \frac{\vartheta(t)-t}{t^2}\,dt$$

does not exist or is $+\infty$ because the Cauchy condition is violated. $\square$

We need to prove the convergence of the above integral. To this end we calculate the Laplace transform of the integrand $\vartheta(\mathrm{e}^t)\mathrm{e}^{-t}-1$. For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, let

$$F(s) = \sum_p \frac{\log p}{p^s}.$$

Proposition 2.2.3 *For $z \in \mathbb{C}$ with $\mathrm{Re}(z) > 0$,*

$$\int_0^{+\infty} \left(\frac{\vartheta(\mathrm{e}^t)}{\mathrm{e}^t} - 1\right)\mathrm{e}^{-zt}\,dt = \frac{F(z+1)}{z+1} - \frac{1}{z}.$$

Proof. It suffices to show that for $\mathrm{Re}(s) > 1$,

$$s\int_0^{+\infty} \vartheta(\mathrm{e}^t)\mathrm{e}^{-st}\, dt = F(s)$$

—then we set $s = z+1$ and subtract $\int_0^{+\infty} \mathrm{e}^{-zt}\, dt = 1/z$. Indeed,

$$\begin{aligned} s\int_0^{+\infty} \vartheta(\mathrm{e}^t)\mathrm{e}^{-st}\, dt &= s\int_1^{+\infty} \vartheta(x)x^{-s-1}\, dx = \sum_{n=1}^{\infty} \vartheta(n)\cdot s\int_n^{n+1} x^{-s-1}\, dx \\ &= \sum_{n=1}^{\infty} \vartheta(n)(n^{-s} - (n+1)^{-s}) = \sum_{n=1}^{\infty} n^{-s}(\vartheta(n) - \vartheta(n-1)) \\ &= \sum_p \frac{\log p}{p^s} = F(s). \end{aligned}$$

□

The proof of the PNT rests on the following two results whose proof we postpone in the next two sections.

Proposition 2.2.4 *The function*

$$\frac{F(z+1)}{z+1} - \frac{1}{z} = \frac{1}{z+1}\sum_p \frac{\log p}{p^{z+1}} - \frac{1}{z}$$

has a holomorphic extension from $\mathrm{Re}(z) > 0$ *to* $\mathrm{Re}(z) \geq 0$*.*

By its definition, $F(s)$ is holomorphic on $\mathrm{Re}(s) > 1$ because it is a sum of entire functions and the sum converges uniformly for $\mathrm{Re}(s) > 1 + \delta$, $\delta > 0$. Thus $(z+1)^{-1}F(z+1) - z^{-1}$ is holomorphic on $\mathrm{Re}(z) > 0$. The proposition says that there is an open set $D \subset \mathbb{C}$ and a holomorphic function $f : D \to \mathbb{C}$ such that D contains the right halfplane $\mathrm{Re}(z) \geq 0$ and $f(z) = (z+1)^{-1}F(z+1) - z^{-1}$ for $\mathrm{Re}(z) > 0$.

Theorem 2.2.5 (Wiener and Ikehara, 1932) *Let* $f : [0, +\infty) \to \mathbb{R}$ *be a function such that (i)* f *is bounded, (ii)* f *has integral on every bounded interval* $[a, b] \subset [0, +\infty)$ *and (iii) the Laplace transform of* f*,*

$$g(z) = \int_0^{+\infty} f(t)\mathrm{e}^{-zt}\, dt,$$

has a holomorphic extension from $\mathrm{Re}(z) > 0$ *to* $\mathrm{Re}(z) \geq 0$. *Then the integral*

$$\int_0^{+\infty} f(t)\, dt$$

converges and equals $g(0)$. *That is to say, we may set* $z = 0$ *in the Laplace transform of* $f(t)$.

For $\mathrm{Re}(z) > \delta > 0$ we have in the integral defining $g(z)$ the integrable majorant $f(t)\mathrm{e}^{-\delta t}$. Thus, calculating $g'(z)$, we can exchange limits and see that $g(z)$ is indeed holomorphic on $\mathrm{Re}(z) > 0$. The theorem says that the existence of holomorphic extension to $\mathrm{Re}(z) \geq 0$ forces $f(t)$ behave regularly for $t \to +\infty$.

Proof of Theorem 2.0.1. We set

$$f(t) = \vartheta(\mathrm{e}^t)\mathrm{e}^{-t} - 1 \ \text{ and } \ g(z) = F(z+1)(z+1)^{-1} - z^{-1}.$$

Function $f(t)$ is locally integrable and is bounded because $0 \leq \vartheta(\mathrm{e}^t) \leq (\log 4)\mathrm{e}^t$ by Corollary 2.1.3. Function $g(z)$ is the Laplace transform of $f(t)$ by Proposition 2.2.3 and has the required holomorphic extension by Proposition 2.2.4. Therefore, by Theorem 2.2.5, the integral

$$\int_0^{+\infty} f(t)\, dt = \int_0^{+\infty} \left(\frac{\vartheta(\mathrm{e}^t)}{\mathrm{e}^t} - 1\right) dt = \int_1^{+\infty} \frac{\vartheta(x) - x}{x^2}\, dx$$

converges. By Propositions 2.2.1 and 2.2.2, the PNT holds. $\square$

2.3 The extension of $(z+1)^{-1}F(z+1) - z^{-1}$

We prove Proposition 2.2.4. The function $F(s)$ is roughly the logarithmic derivative of the *zeta function* ($s \in \mathbb{C}$)

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

Here the power n^s for $s \in \mathbb{C}$ and $n \in \mathbb{N}$ or more generally α^s for real $\alpha > 0$ is to be understood as $\exp(s \log \alpha)$ with the real logarithm (in Chapter 3 of [25] you may enjoy α^s with both $\alpha, s \in \mathbb{C}$).

Proposition 2.3.1 *The function $\zeta(s)$ has the following properties.*

1. *$\zeta(s)$ is holomorphic on* $\mathrm{Re}(s) > 1$.
2. *For* $\mathrm{Re}(s) > 1$ *we have the Euler product*
$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$
3. *For* $\mathrm{Re}(s) > 1$ *one has* $\zeta(s) \neq 0$.
4. *For any $s \in \mathbb{C}$ with* $\mathrm{Re}(s) > 1$ *there are points $u \in \mathbb{C}$ arbitrarily close to s such that $\zeta(u) \notin (-\infty, 0]$.*
5. *The function $\zeta(s) - (s-1)^{-1}$ has a holomorphic extension from* $\mathrm{Re}(s) > 1$ *to* $\mathrm{Re}(s) > 0$.
6. *For* $\mathrm{Re}(s) = 1$, *$s \neq 1$, one has $\zeta(s) \neq 0$.*

Proof. 1. By the definition, $\zeta(s)$ is a sum of series of entire functions and the series converges uniformly for $\mathrm{Re}(s) > 1 + \delta > 1$.

2 and 3. As $\zeta(s) = L(s, \chi_0)$ for the modulus $m = 1$, we proved parts 2 and 3 already in parts 4 and 5 of Proposition 1.2.5. The small distinction is that there $s \in (1, +\infty)$ but here $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$. Just replace in the proof of part 4 the summand $1/n^s$ by $|1/n^s| = n^{-\mathrm{Re}(s)}$ and in the proof of part 5 the identity $|\chi(p)p^{-s}| = p^{-s}$ by $|\chi(p)p^{-s}| = p^{-\mathrm{Re}(s)}$ and set $c = -\zeta(\mathrm{Re}(s))$.

4. This follows from the local expansion around s: for u near fixed s, $\zeta(u) = \zeta(s) + (a + o(1))(u - s)^k$ where $k \in \mathbb{N}$ and $a \in \mathbb{C}$, $a \neq 0$ ($\zeta(u)$ is not locally constant anywhere because it decreases for $u > 1$).

5. For $\mathrm{Re}(s) > 1$,
$$\zeta(s) - (s-1)^{-1} = \sum_{n=1}^{\infty} n^{-s} - \int_1^{+\infty} x^{-s} dx = \sum_{n=1}^{\infty} F_n(s)$$
where
$$F_n(s) = \int_n^{n+1} (n^{-s} - x^{-s})\, dx.$$
It is easy to show directly from this formula that for every fixed $s \in \mathbb{C}$, the limit $\lim_{u \to s}(F_n(u) - F_n(s))(u - s)^{-1}$ exists. Thus each $F_n(s)$ is an entire function. Further,
$$|F_n(s)| = \left| s \int_n^{n+1} \int_n^x u^{-s-1}\, du\, dx \right| \leq |s| \max_{n \leq u \leq n+1} |u^{-s-1}| = \frac{|s|}{n^{\mathrm{Re}(s)+1}}.$$

So $\sum_n F_n(s)$ converges uniformly for $\mathrm{Re}(s) > \delta > 0$ and defines on $\mathrm{Re}(s) > 0$ a holomorphic extension of $\zeta(s) - (s-1)^{-1}$.

6. To approach the values of $\zeta(s)$ on the line $\mathrm{Re}(s) = 1$, we derive for $\mathrm{Re}(s) > 1$ an expansion of $\log|\zeta(s)|$ into a real series.

Since $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$ by part 3, for such s we can take complex logarithm of the product in part 2 (see part 3 of Proposition 1.2.7), and comparison of the real parts gives (the correction term $2k(s)\cdot\pi i$ is irrelevant)

$$\log|\zeta(s)| = \mathrm{Re}\Big(\sum_p \log(1-p^{-s})^{-1}\Big),\ \mathrm{Re}(s) > 1.$$

Writing $s = \sigma + it$, $\sigma > 1$, and expanding $\log(1-p^{-s})^{-1}$ by part 6 of Proposition 1.2.7, we get the series

$$\log|\zeta(s)| = \mathrm{Re}\Big(\sum_p (p^{-s} + p^{-2s}/2 + p^{-3s}/3 + \cdots)\Big) = \sum_{n=1}^{\infty} a_n n^{-\sigma}\cos(t\log n)$$

where $a_n = r^{-1}$ if $n = p^r$, $r \in \mathbb{N}$, and $a_n = 0$ else.

We have $a_n \geq 0$ and $n^{-\sigma} \geq 0$ for every $n \in \mathbb{N}$ and $\sigma > 1$ but $\cos(t\log n)$ may be negative. Using the identity

$$3 + 4\cos x + \cos 2x = 2(1+\cos x)^2 \geq 0,\ x \in \mathbb{R},$$

we achieve nonnegativity of the cosinus factors by taking a linear combination of three of these series: for every $\sigma, t \in \mathbb{R}$, $\sigma > 1$, we have

$$\log|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)| = \sum_{n=1}^{\infty} 2a_n n^{-\sigma}(1+\cos(t\log n))^2 \geq 0.$$

This inequality implies that no number $1+it$ can be a zero of $\zeta(s)$. Indeed, if $\zeta(1+it_0) = 0$ for some $t_0 \neq 0$, then $\zeta(\sigma)^3\zeta(\sigma+it_0)^4\zeta(\sigma+2it_0) = O(\sigma-1) \to 0$ as $\sigma \to 1^+$ because $\zeta(\sigma)^3 \sim (\sigma-1)^{-3}$ (by part 5 or part 1 of Proposition 1.3.1), $\zeta(\sigma+it_0)^4 = O((\sigma-1)^4)$ (local expansion of $\zeta(s)$ around $1+it_0$) and $\zeta(\sigma+2it_0) = O(1)$. Thus for $t = t_0$ and $\sigma \to 1^+$ the left side of the inequality goes to $-\infty$, which is impossible. □

Proof of Proposition 2.2.4. We extend $F(s)-(s-1)^{-1} = \sum_p p^{-s}\log p - (s-1)^{-1}$ holomorphicaly to $\mathrm{Re}(s) \geq 1$. This provides a holomorphic extension of

$$\frac{F(z+1)}{z+1} - \frac{1}{z} = \frac{1}{z+1}\left(F(z+1) - \frac{1}{z} - 1\right)$$

to $\mathrm{Re}(z) \geq 0$. If $\mathrm{Re}(s) > 1$ and $\zeta(s) \notin (-\infty, 0]$, logarithmic derivative of the Euler product for $\zeta(s)$ gives (by part 3 of Proposition 1.2.7)

$$
\begin{aligned}
\frac{\zeta(s)'}{\zeta(s)} &= (\log \zeta(s))' = \left(2k(s) \cdot \pi i + \sum_p \log(1 - p^{-s})^{-1}\right)' \\
&= -\sum_p \frac{\log p}{p^s - 1} = -F(s) - \sum_p \frac{\log p}{p^s(p^s - 1)}
\end{aligned}
$$

as $k(s) \in \mathbb{Z}$ is locally constant. By part 4 of Proposition 2.3.1 and the continuity of involved functions, for every s with $\mathrm{Re}(s) > 1$ we get

$$
F(s) - \frac{1}{s-1} = -\left(\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1}\right) - \sum_p \frac{\log p}{p^s(p^s - 1)}.
$$

The expression on the right side is holomorphic on $\mathrm{Re}(s) \geq 1$. The sum defines a function holomorphic for $\mathrm{Re}(s) > \frac{1}{2}$. By parts 1, 3, 5 and 6 of Proposition 2.3.1, $\zeta'(s)/\zeta(s) + (s-1)^{-1}$ is holomorphic in a neighborhood of every point s with $\mathrm{Re}(s) \geq 1$ and $s \neq 1$. In a deleted neighborhood of $s = 1$ we have $\zeta(s) = (s-1)^{-1} + z(s)$ with $z(s)$ holomorphic on $\mathrm{Re}(s) > 0$ (by part 5). So

$$
\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1} = \frac{-(s-1)^{-2} + z'(s)}{(s-1)^{-1} + z(s)} + \frac{1}{s-1} = \frac{z(s) + (s-1)z'(s)}{1 + (s-1)z(s)}
$$

is holomorphic in a neighborhood of $s = 1$ as well. $\square$

2.4 The theorem of Wiener and Ikehara

We proceed to the proof of Theorem 2.2.5; it is due to D. J. Newman. For a bounded function

$$
f : [0, +\infty) \to \mathbb{R}
$$

that is integrable on bounded intervals, we set

$$
g(z) = \int_0^{+\infty} f(t) \mathrm{e}^{-tz} \, dt \quad \text{for} \quad \mathrm{Re}(z) > 0
$$

and assume that $g(z)$ has a holomorphic extension to $\mathrm{Re}(z) \geq 0$. We prove that

$$\int_0^{+\infty} f(t)\, dt = g(0).$$

For real $T > 0$ we set

$$g_T(z) = \int_0^T f(t)\mathrm{e}^{-zt}\, dt.$$

Like for the functions $F_n(s)$ in the extension of $\zeta(s)$, it is easy to show directly that $g_T(z)$ is an entire function of z. We prove that

$$\lim_{T\to+\infty} g_T(0) = g(0).$$

Let $R > 0$ be real and C be the domain

$$C = C(R) = \{z \in \mathbb{C} :\ |z| < R \ \&\ \mathrm{Re}(z) > -\delta\}$$

where $\delta = \delta(R) > 0$ is so small that $g(z)$ has a holomorphic extension to $\overline{C}$ — such δ exists because the segment $[-iR, iR]$ is compact. By the Cauchy theorem,

$$g(0) - g_T(0) = \frac{1}{2\pi i}\int_{\partial C} \frac{g(z) - g_T(z)}{z}\, dz$$

where ∂C is the D-shaped boundary curve of C, oriented counterclockwise.

We estimate the last integral by introducing an appropriate integration kernel $G(z)$. By the Cauchy theorem, also

$$g(0) - g_T(0) = \frac{1}{2\pi i}\int_{\partial C} \frac{g(z) - g_T(z)}{z} G(z)\, dz$$

provided that $G(z)$ is holomorphic on $\overline{C}$ and $G(0) = 1$. We set

$$G(z) = G(z, R, T) = \left(1 + \frac{z^2}{R^2}\right)\mathrm{e}^{zT}$$

where $R, T > 0$ have the previous meaning. The function $G(z)$ is entire and $G(0) = 1$. Its task is to tame the integrand on the circle $|z| = R$: on $|z| = R$ we have

$$\left|\frac{G(z)}{z}\right| = \left|\frac{\mathrm{e}^{zT}(z + \overline{z})}{R^2}\right| = 2\mathrm{e}^{\mathrm{Re}(z)T} \cdot \frac{|\mathrm{Re}(z)|}{R^2}.$$

It suffices to show that

$$I = \int_{\partial C} \frac{g(z) - g_T(z)}{z} G(z)\, dz \to 0 \quad \text{as} \quad T \to +\infty.$$

We split the integral I in three summands:

$$\begin{aligned} I &= \int_{\partial C^-} \frac{g(z)}{z} G(z)\, dz - \int_{\partial C^-} \frac{g_T(z)}{z} G(z)\, dz + \int_{\partial C^+} \frac{g(z) - g_T(z)}{z} G(z)\, dz \\ &= \int_{\partial C^-} \frac{g(z)}{z} G(z)\, dz - \int_{K^-} g_T(z) \frac{G(z)}{z}\, dz + \int_{\partial C^+} (g(z) - g_T(z)) \frac{G(z)}{z}\, dz \\ &= I_1 - I_2 + I_3 \end{aligned}$$

where ∂C^- and ∂C^+ are the arcs of the curve ∂C lying in $\mathrm{Re}(z) \leq 0$ and $\mathrm{Re}(z) \geq 0$, respectively, and K^- is the halfcircle of $|z| = R$ in $\mathrm{Re}(z) \leq 0$. In I_2 we could replace ∂C^- with K^- without changing the integral because the integrand is holomorphic in $\mathbb{C} \backslash \{0\}$.

To bound the integral I_1, we split the integrand as $J(z) \cdot \mathrm{e}^{zT}$ where $J(z) = g(z) z^{-1}(1 + z^2 R^{-2})$ is independent of T. Let $M_1 = M_1(R)$ be the maximum modulus of $J(z)$ on ∂C^-. We have

$$|I_1| \leq M_1 \int_{\partial C^-} \left| \mathrm{e}^{zT} \right|\, dz.$$

Due to the location of ∂C^-, for every $\varepsilon > 0$ there is a $\kappa > 0$ such that $\left| \mathrm{e}^{zT} \right| \leq \mathrm{e}^{-\kappa T}$ on ∂C^-, except for a part of ∂C^- close to the imaginary axis, whose length is an ε-fraction of the total length $|\partial C^-| < 3R$. On this small part of ∂C^- we use the trivial estimate $\left| \mathrm{e}^{zT} \right| \leq 1$. Thus

$$|I_1| \leq M_1(\mathrm{e}^{-\kappa T} + \varepsilon)|\partial C^-| < 3 M_1 R \cdot (\mathrm{e}^{-\kappa T} + \varepsilon).$$

It follows that for every fixed $R > 0$,

$$\lim_{T \to +\infty} |I_1| = 0.$$

Integrals I_2 and I_3 are estimated with the help of the kernel $G(z)$. We set $B = \sup_{t \geq 0} |f(t)|$. For $\mathrm{Re}(z) < 0$ we have

$$|g_T(z)| = \left| \int_0^T f(t) \mathrm{e}^{-tz}\, dt \right| \leq B \int_{-\infty}^T \left| \mathrm{e}^{-tz} \right|\, dt = \frac{B \mathrm{e}^{-\mathrm{Re}(z) T}}{|\mathrm{Re}(z)|}$$

and for $\mathrm{Re}(z) > 0$ similarly

$$|g(z) - g_T(z)| \leq B \int_T^{+\infty} |\mathrm{e}^{-tz}|\, dt = \frac{B\mathrm{e}^{-\mathrm{Re}(z)T}}{\mathrm{Re}(z)}.$$

Using the above expression for $|G(z)/z|$ on the circle $|z| = R$ and the fact that the curves K^- and ∂C^+ have length πR, we obtain the neat estimates

$$|I_2| \leq \frac{2\pi B}{R} \quad \text{and} \quad |I_3| \leq \frac{2\pi B}{R}$$

which are independent of T.

For given $\varepsilon > 0$, we fix $R > 8\pi B/\varepsilon$ and the corresponding domain $C = C(R)$; then $|I_2| + |I_3| < \varepsilon/2$ regardless of T. We know that for this fixed R the contribution from I_1 is for large T smaller than $\varepsilon/2$. Thus $|I| \leq |I_1| + |I_2| + |I_3| < \varepsilon$ for every large T. We conclude that $I \to 0$ as $T \to +\infty$.

This finishes the proof of Theorem 2.2.5 and also of the PNT.

2.5 Remarks

For more information on the origin of the quotation attributed to Hadamard see [23]. Section 2.1 is based on Pollack [36, Sections 1.2 and 1.4] and Aigner and Ziegler [1, Chapter 2 on Bertrand postulate]. The cute arguments using binomial coefficients are due to P. Erdős. The exact asymptotic relation for the sum of reciprocals of primes is (Tenenbaum [47, Theorem 9 in Section 1.6])

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + 0.261497\cdots + O(1/\log x),\ x \to +\infty,$$

where

$$0.261497\cdots = \gamma - c_0 = \lim_{n\to\infty}\left(\sum_{m\leq n} 1/m - \log n\right) - \sum_p \big(\log(1-1/p)^{-1} - 1/p\big).$$

The proof of the PNT in Sections 2.2–2.4, in which the crucial simplification in Section 2.4 is due to D. J. Newman, is based on Bak and Newman [5, Section 19.5], Hlawka, Schoißengaier and Taschner [20, Chapter 5], Newman [33], [34, Chapter 7] and Zagier [50].

More information on the prime number theory and the PNT is in Narkiewicz [30]. The formal proof of the PNT (not the one using complex analysis but the elementary proof due to Selberg and Erdős) was computationally verified, see Avigad et al. [2].

Chapter 3

Shnirel'man's theorem on sums of prime numbers

И заранее никогда не скажешь — как кому обернется в итоге та или иная жизненная история: травимый в 1936 году академик Николай Николаевич Лузин сравнительно благополучно закончил жизнь в 1950 году в своей московской квартире на Сретенском бульваре, а творившие над ним суд Непременный секретарь Академии Н. П. Горбунов и член-корреспондент Академии блистательный Л. Г. Шнирельман уйдут из жизни в 1938 году — первый будет расстрелян как враг народа, второй, возвратившись с "беседы" в НКВД, пустит газ в своей квартире.[1]

С. С. Демидов, Б. В. Левшин [10]

In 1930, L. G. Shnirel'man (1905–1938) made a sensational progress in one of the oldest unsolved problems in number theory, the *Goldbach conjecture.* This problem, posed in 1742 in a letter by L. Euler to Ch. Goldbach, states that every even number bigger than 2 is a sum of two prime numbers. As of 2010, it is still wide open. Shnirel'man proved a weaker but significant result.

[1]For translation see Section 3.5.

Theorem 3.0.1 (Shnirel'man, 1930) *There is a constant h such that every natural number bigger than 1 is a sum of at most h (not necessarily distinct) prime numbers.*

His proof provided value $h = 800\ 000$. The Goldbach conjecture, if true, implies that $h = 3$ suffices: 2 and 3 are primes, even numbers $n \geq 4$ have form $n = p + q$, 5 is a prime, and odd numbers $n \geq 7$ have form $n = 3 + (n - 3) = 3 + p + q$. It is easy to see that $h = 2$ is not enough and that there exist infinitely many n not expressible as a sum of at most two prime numbers. We obtain the value $h = 800\ 000$ as well (Corollary 3.2.3).

We prove Shnirel'man's theorem in Section 3.2. In Section 3.1 we introduce the notion of Shnirel'man's density and derive its key property, which we apply in the proof of Theorem 3.0.1. This property (Theorem 3.1.2), found by Shnirel'man, asserts that in order to prove that every $n \in \mathbb{N}$ is a sum of at most h numbers from a subset $A \subset \mathbb{N}$, it suffices to show this for any positive fraction (in the sense of Shnirel'man's density) of numbers in $\mathbb{N}$. The main step in the proof of Theorem 3.0.1 is the bound

$$r(n) < \frac{cn}{(\log n)^2} \prod_{p|n} (1 + 1/p)$$

where $c > 0$ is a constant and $r(n)$ is the number of solutions of the equation $n = p + q$, that is, the number of ways to write n as a sum of two prime numbers. This upper bound on $r(n)$ is established in Section 3.3 by means of Selberg sieve. In Section 3.4 we complete a technical step in the derivation of Selberg sieve.

3.1 Shnirel'man's density

For h sets $A_1, A_2, \ldots, A_h \subset \mathbb{N}_0$ we define their sumset as

$$A_1 + A_2 + \cdots + A_h = \{a_1 + a_2 + \cdots + a_h \mid a_i \in A_i, 1 \leq i \leq h\}.$$

If $A_1 = A_2 = \cdots = A_h = A$, we abbreviate $A + A + \cdots + A$ (h terms) by hA. Let $A \subset \mathbb{N}_0$. For $n \in \mathbb{N}$ we set

$$A(n) = |A \cap [n]| = |A \cap \{1, 2, \ldots, n\}|.$$

Shnirel'man's density $\sigma(A)$ of A is

$$\sigma(A) = \inf_{n \in \mathbb{N}} \frac{A(n)}{n}.$$

Note that $\sigma(A) = 0$ if $1 \notin A$. Also, $0 \le \sigma(A) \le 1$, $A(n) \ge \sigma(A)n$ for every $n \in \mathbb{N}$, and for $A \subset \mathbb{N}$ we have $\sigma(A) = 1 \iff A = \mathbb{N}$. *The lower density* $\underline{d}(A)$ of A is

$$\underline{d}(A) = \liminf_{n\to\infty} \frac{A(n)}{n}.$$

Again, $0 \le \underline{d}(A) \le 1$.

Proposition 3.1.1 *Let $A, B \subset \mathbb{N}_0$ be two sets of nonnegative integers.*

1. *One has*

$$\underline{d}(A) > 0 \iff A(n)/n > c > 0 \ \text{ for every } n > N$$

where $c > 0$ and $N \in \mathbb{N}$ are constants.

2. *One has*

$$\sigma(A) > 0 \iff 1 \in A \ \&\ \underline{d}(A) > 0.$$

3. *If $0 \in A \cap B$ and $\sigma(A) + \sigma(B) \ge 1$ then $A + B = \mathbb{N}_0$.*

4. *If $0 \in A \cap B$ then*

$$\sigma(A + B) \ge \sigma(A) + \sigma(B) - \sigma(A)\sigma(B).$$

Proof. 1 and 2. This follows from definition of both densities.

3. Let $n \in \mathbb{N}_0$ be arbitrary. The sum of cardinalities of the sets

$$\{a \in A \mid 0 \le a \le n\} \ \text{ and } \ \{n - b \mid b \in B, 0 \le b \le n\}$$

is at least $\sigma(A)n + 1 + \sigma(B)n + 1 \ge n + 2$. But these sets are subsets of the $(n+1)$-element set $\{0, 1, \ldots, n\}$ and therefore intersect: $a = n - b$ for some $a \in A$ and $b \in B$. Thus $n = a + b$ with $a \in A$, $b \in B$.

4. Let $n \in \mathbb{N}$ be arbitrary and $0 = a_0 < a_1 < \cdots < a_k \le n$ be the elements of A not exceeding n. Consider the $k + 2$ sets

$$\{a_i + 0 \mid 1 \le i \le k\},\ \{a_i + b \mid b \in B, 1 \le b \le a_{i+1} - a_i - 1\} \ \text{ for } \ 0 \le i \le k-1,$$

and

$$\{a_k + b \mid b \in B, 1 \le b \le n - a_k\}.$$

They lie in $(A+B)\cap[n]$ and are pairwise disjoint. The sum of their cardinalities is a lower bound on $(A+B)(n)$. We have

$$\begin{aligned}
(A+B)(n) &\geq k+\sum_{i=0}^{k-1} B(a_{i+1}-a_i-1)+B(n-a_k) \\
&\geq k+\sigma(B)\sum_{i=0}^{k-1}(a_{i+1}-a_i-1)+\sigma(B)(n-a_k) \\
&= k+\sigma(B)(n-k)=A(n)(1-\sigma(B))+\sigma(B)n \\
&\geq \sigma(A)n(1-\sigma(B))+\sigma(B)n \\
&= (\sigma(A)+\sigma(B)-\sigma(A)\sigma(B))n.
\end{aligned}$$

Hence $\sigma(A+B)\geq\sigma(A)+\sigma(B)-\sigma(A)\sigma(B)$. □

Theorem 3.1.2 *If $A\subset\mathbb{N}$ has $\sigma(A)>0$, then there is an h such that every $n\in\mathbb{N}$ is a sum of at most h (not necessarily distinct) elements of A.*

Proof. We add 0 to A so that $0\in A$. Rewriting the inequality in part 4 of Proposition 3.1.1 as

$$1-\sigma(A+B)\leq(1-\sigma(A))(1-\sigma(B))$$

and iterating this, we obtain

$$1-\sigma(kA)\leq(1-\sigma(A))^k \quad\text{and}\quad \sigma(kA)\geq 1-(1-\sigma(A))^k$$

for every $k\in\mathbb{N}$. From $\sigma(A)>0$ we have $\sigma(kA)\geq\frac{1}{2}$ for sufficiently big k. By part 3 of Proposition 3.1.1, $kA+kA=(2k)A=\mathbb{N}_0$. Thus every $n\in\mathbb{N}$ is a sum of at most $h=2k$ positive elements of A. □

Corollary 3.1.3 *Suppose that $A\subset\mathbb{N}$ has $\underline{d}(A)>0$ and $2,3\in A$. Then there is an h such that every $n\in\mathbb{N}$, $n\geq 2$, is a sum of at most h (not necessarily distinct) elements of A.*

Proof. By part 2 of Proposition 3.1.1, we can apply Theorem 3.1.2 to $A\cup\{1\}$ and write every $n\in\mathbb{N}$ as a sum of at most h summands which are either 1 or lie in A. Let $n\geq 2$. If $n=2$, we are done, $n\in A$. If $n\geq 3$, we write

$$n=2+(n-2)=2+m_1+m_2+\cdots+m_k$$

where $k \le h$ and $m_i \in A \cup \{1\}$. If no m_i is 1, we use this expression without change. If exactly one m_i is 1, say $m_1 = 1$, we have

$$n = 3 + m_2 + \cdots + m_k.$$

If at least two m_i are 1, say $m_1 = m_2 = \cdots = m_l = 1$, $2 \le l \le k$, and $m_i \in A$ for $i > l$, we replace the sum $m_1 + m_2 + \cdots + m_l = l$ by an equal sum of less than l 2's and 3's ($1+1 = 2$, $1+1+1 = 3$, $1+1+1+1 = 2+2$, $1+1+1+1+1 = 2+3$, and so on) and have

$$n = 2 + (2 + \cdots + 3) + m_{l+1} + \cdots + m_k,$$

with at most l initial 2's and 3's. In all three cases, n is expressed as a sum of at most $k+1 \le h+1$ elements from A. □

3.2 Proof of Shnirel'man's theorem

Corollary 3.1.3 does not apply directly to the set of prime numbers

$$P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots\}$$

because $\underline{d}(P) = 0$ (as we know from the previous chapter). But Shnirel'man could prove that $\underline{d}(2P) > 0$. Applying Corollary 3.1.3 to

$$A = \{2, 3\} \cup 2P,$$

we see that every $n \in \mathbb{N}$, $n \ge 2$, is a sum of at most h summands which are $2, 3$ or of the form $p + q$. Thus every $n \ge 2$ is a sum of at most $2h$ primes and Theorem 3.0.1 is proved.

But it is hard to prove that $\underline{d}(2P) > 0$. We begin by showing how it follows, perhaps surprisingly, from an upper bound on $r(n)$.

Theorem 3.2.1 *Let $r(n)$ be the number of representations $n = p + q$ of $n \in \mathbb{N}$ as a sum of two primes. Then for every $n \ge 2$,*

$$r(n) < \frac{cn}{(\log n)^2} \prod_{p|n} (1 + 1/p)$$

where $c = 827$. For $n > 2.85 \cdot 10^6$ we may take $c = 580$.

Corollary 3.2.2 *The set of primes P has the property that $\underline{d}(2P) > 0$.*

Proof. We prove that $(2P)(n) \gg n$ for $n \geq 4$. Let $n \geq 4$ be arbitrary. By the Cauchy–Schwarz inequality,

$$\begin{aligned}(r(4)+r(5)+\cdots+r(n))^2 &\leq \left(\textstyle\sum_{m=4,\ r(m)>0}^{n} 1^2\right)\left(r(4)^2+r(5)^2+\cdots+r(n)^2\right)\\ &= (2P)(n)\cdot(r(4)^2+r(5)^2+\cdots+r(n)^2)\end{aligned}$$

and we have

$$(2P)(n) \geq \frac{\big(r(4)+r(5)+\cdots+r(n)\big)^2}{r(4)^2+r(5)^2+\cdots+r(n)^2}.$$

The sum in the numerator counts all pairs of primes p, q such that $p+q \leq n$. Thus, by Proposition 2.1.4,

$$\big(r(4)+r(5)+\cdots+r(n)\big)^2 \geq \big(\pi(n/2)^2\big)^2 \gg n^4/(\log n)^4.$$

By Theorem 3.2.1, the sum in the denominator satisfies

$$\sum_{m=4}^{n} r(m)^2 \ll \sum_{m=4}^{n} \frac{m^2}{(\log m)^4} \prod_{p|m}(1+1/p)^2 \leq \frac{n^2}{(\log n)^4} \sum_{m=4}^{n} \prod_{p|m}(1+1/p)^2.$$

As for the last sum,

$$\begin{aligned}\sum_{m=4}^{n}\prod_{p|m}(1+1/p)^2 &\leq \sum_{m=4}^{n}\Big(\sum_{d|m}\frac{1}{d}\Big)^2 = \sum_{m=4}^{n}\Big(\sum_{d|m}\frac{1}{d}\Big)\Big(\sum_{e|m}\frac{1}{e}\Big)\\ &= \sum_{d,e}\frac{1}{de}\sum_{m=4,d|m,e|m}^{n} 1 \leq n\sum_{d,e}\frac{1}{de[d,e]}\\ &\qquad \text{(as } d|m, e|m \iff [d,e]|m)\\ &\leq n\sum_{d,e}\frac{1}{(de)^{3/2}} \quad \text{(since } [d,e] \geq \max(d,e) \geq \sqrt{de})\\ &= n\Big(\sum_{d=1}^{\infty}\frac{1}{d^{3/2}}\Big)^2\\ &\ll n.\end{aligned}$$

Thus the denominator is $\ll n^3/(\log n)^4$. Together, for $n \geq 4$, we get the desired estimate

$$(2P)(n) \gg \frac{n^4/(\log n)^4}{n^3/(\log n)^4} = n.$$

$\square$

To complete the proof of Shnirel'man's Theorem 3.0.1, it remains to establish Theorem 3.2.1. The main bulk of the proof still lies ahead of us.

We extract from the calculations specific value of Shnirel'man's constant.

Corollary 3.2.3 *Every number $n \in \mathbb{N}$, $n \geq 2$, is a sum of at most* 800 000 *prime numbers.*

Proof. First we need an explicit constant in the last asymptotic inequality $\gg$ in the previous proof. We show that

$$\frac{\pi(n/2)}{n/\log n} > \frac{\log 2}{2} > 0.345 \quad \text{for} \quad n > 730.$$

Setting in the lower bound of Proposition 2.1.4 $x = n/2$, we get

$$\frac{\pi(n/2)}{n/\log n} > \frac{\log 2}{2} + \frac{(\log 2)^2/2}{\log n - \log 2} - \frac{4\log n}{n} \quad \text{for} \quad n \geq 4.$$

The stated inequality holds if $n(\log n)^{-2} > 8(\log 2)^{-2} = 16.65\ldots$, which is true if $n > 730$; note that $n/\log n$ increases for $n > 3$ and $n/(\log n)^2$ for $n > 8$. We obtain an explicit lower bound on the numerator: for every $n > 730$,

$$(r(4) + r(5) + \cdots + r(n))^2 > ((1/2)\log 2)^4 (n/\log n)^4 > 0.014(n/\log n)^4.$$

As for the denominator, $\zeta(3/2)^2 < 6.9$ because

$$\zeta(3/2) < \sum_{n=1}^{N} n^{-3/2} + \int_N^{+\infty} x^{-3/2}\, dx = \sum_{n=1}^{N} n^{-3/2} + 2N^{-1/2} < 2.625$$

for $N = 12$. By Theorem 3.2.1, for $n > 2.85 \cdot 10^6$ we have

$$r(4)^2 + r(5)^2 + \cdots + r(n)^2 < (580 \cdot 6.9)n^3/(\log n)^4$$

and

$$2P(n) > \frac{0.014}{580 \cdot 6.9} n > (3.49 \cdot 10^{-6})n, \ \ n > 2.85 \cdot 10^6.$$

For small n, $1 \leq n \leq 2.85 \cdot 10^6$, the set $A = \{1, 2, 3\} \cup 2P$ satisfies that $A(n) > (10/2.85 \cdot 10^6)n > (3.5 \cdot 10^{-6})n$ because $\{1, 2, \ldots, 10\} \subset A$. Shnirel'man's density of A therefore satisfies

$$\sigma(A) = \sigma(\{1, 2, 3\} \cup 2P) > \min(3.49 \cdot 10^{-6}, 3.5 \cdot 10^{-6}) = 3.49 \cdot 10^{-6}.$$

By the proofs of Theorem 3.1.2 and Corollary 3.1.3, if $(1-3.49\cdot 10^{-6})^k \le \frac{1}{2}$ then every $n \ge 2$ is a sum of at most $4k+1$ primes. Since

$$k = \left\lceil \frac{\log(1/2)}{\log(1-3.49\cdot 10^{-6})} \right\rceil < 1.99\cdot 10^5$$

works, every $n \ge 2$ is a sum of $4k+1 < 800\,000$ primes. $\square$

3.3 Bounding $r(n)$ by Selberg sieve

We prove Theorem 3.2.1. For $m \in \mathbb{N}$, we denote by $M(m)$ the smallest prime factor of m. For any real $z > 1$ we have the inequality

$$r(n) \le 2z + \#\big(m(n-m) \mid m \in \mathbb{N}, 1 \le m \le n-1, M(m(n-m)) \ge z\big).$$

Indeed, every expression $n = p + q$ contributing to $r(n)$ is accounted for in an expression $n = m + (n-m)$ with $m < z$ or $n - m < z$ or in an expression $n = m + (n-m)$ with $m(n-m)$ having no prime factor $< z$. If we set, as we will do, $z = n^\alpha$ for some $0 < \alpha < 1$, then the first term $2z = 2n^\alpha$ is small and it suffices to bound the second term counting the numbers among $n-1, 2(n-2), 3(n-3), \ldots, (n-2)2, n-1$ with no prime factor $< n^\alpha$.

Thus it is of great interest to bound, for real $z > 1$ and general finite sequence $A \subset \mathbb{N}$ (both z and A will depend on a parameter $n \in \mathbb{N}$), the quantity

$$S(A, z) = \#(a \in A \mid M(a) \ge z)$$

counting terms in A with no prime factor $< z$. We derive a general upper bound on $S(A, z)$ and apply it to the particular sequence $A = (m(n-m) \mid m \in \mathbb{N}, 1 \le m \le n-1)$ relevant for bounding $r(n)$.

We expand $S(A, z)$ by the inclusion-exclusion principle. For this, we need to estimate the quantities $|A_d|$, $d \in \mathbb{N}$, where

$$A_d = (a \in A \mid a \equiv 0 \ (\mathrm{mod}\ d))$$

is the subsequence of multiples of d in A. The inclusion-exclusion gives the formula

$$\begin{aligned} S(A, z) &= |A| - \#(a \in A \mid a \in A_p \text{ for some } p < z) \\ &= \sum_{d \in D} (-1)^{\omega(d)} |A_d| \end{aligned}$$

where $\omega(d)$ is the number of prime factors of d and

$$D = D(z) = \{n \in \mathbb{N} \mid n < z \text{ and } n \text{ is square-free}\}.$$

We write

$$|A_d| = g(d)|A|,\ g:\ \mathbb{N} \to [0,1].$$

Suppose that $g(d)$ is a simple function, namely that it is completely multiplicative: $g(ab) = g(a)g(b)$ for every $a, b \in \mathbb{N}$ and $g(1) = 1$. The formula for $S(A, z)$ then can be written in the multiplicative form

$$S(A,z) = |A| \prod_{p<z}(1-g(p)) = \frac{|A|}{\prod_{p<z}(1-g(p))^{-1}} = \frac{|A|}{\sum_{k,\ p|k \Rightarrow p<z} g(k)}$$

and we get the neat inequality

$$S(A,z) \le \frac{|A|}{\sum_{k<z} g(k)}.$$

Unfortunately, it is not widely applicable because the only sequence A with completely multiplicative $g(d)$ is $(1, 1, \ldots, 1)$. But perhaps one can obtain a useful inequality for more sequences A, by relaxing equalities $|A_d| = g(d)|A|$ to approximations and estimating errors? This is what A. Selberg (1917–2006) achieved. If the approximation errors are in average small, we obtain a nontrivial upper bound on $S(A, z)$, called *Selberg sieve*.

Theorem 3.3.1 (Selberg, 1947) *Let A, $z > 1$ and $D = D(z)$ be as above. Suppose that $g:\ \mathbb{N} \to \mathbb{R}$ is a completely multiplicative function satisfying $g(1) = 1$ and $0 < g(n) < 1$ for every $n \ge 2$, and the numbers $r_d \in \mathbb{R}$, $d \in D$, are defined by*

$$|A_d| = g(d)|A| + r_d.$$

Then, with the above notation,

$$S(A,z) < \frac{|A|}{\sum_{k<z} g(k)} + \sum_{f \in D(z^2)} 3^{\omega(f)}|r_f|.$$

To derive this inequality we need a technical lemma whose proof we postpone to Section 3.4. For fixed $z > 1$ and $D = D(z)$ we consider the quadratic form

$$G(x_d \mid d \in D) = \sum_{e,d \in D} g([e,d]) \cdot x_e x_d.$$

Lemma 3.3.2 *There exist real numbers* λ_d^**,* $d \in \mathbb{N}$*, such that* $\lambda_1^* = 1$*,* $|\lambda_d^*| \le 1$ *for all* $d \in D$*, and*

$$G(\lambda_d^* \mid d \in D) \le \frac{1}{\sum_{k<z} g(k)}.$$

Proof of Theorem 3.3.1. If λ_d, $d \in D$, are any real numbers satisfying just the condition $\lambda_1 = 1$, we have the bound

$$S(A, z) \le \sum_{a \in A} \Big(\sum_{d \in D, d|a} \lambda_d \Big)^2 = \sum_{a \in A} \Big(\sum_{d \in D, d|a} \lambda_d \Big)\Big(\sum_{e \in D, e|a} \lambda_e \Big).$$

Indeed, for $a \in A$ with $M(a) \ge z$ the summand is $\lambda_1^2 = 1$ and all summands are nonnegative. Changing the summation order, we get

$$\begin{aligned} S(A, z) &\le \sum_{e,d \in D} \lambda_e \lambda_d \sum_{a \in A,\ [e,d]|a} 1 \\ &= \sum_{e,d \in D} \lambda_e \lambda_d \cdot (g([e, d])|A| + r_{[e,d]}) \\ &= G(\lambda_d \mid d \in D) \cdot |A| + \sum_{e,d \in D} r_{[e,d]} \lambda_e \lambda_d. \end{aligned}$$

By Lemma 3.3.2, for $\lambda_d = \lambda_d^*$ we have

$$S(A, z) < \frac{|A|}{\sum_{k<z} g(k)} + \sum_{e,d \in D} |r_{[e,d]}|.$$

To bound the last sum, we consider the equality

$$f = [e, d],\ e, d \in D.$$

Since $e, d < z$ are squarefree, so is f and $f < z^2$. For fixed $f = p_1 p_2 \dots p_k$, the number of pairs $e, d \in \mathbb{N}$ for which $f = [e, d]$ (we may drop the condition $e, d \in D$ since we are proving an upper bound) is the number of pairs of sets A, B such that

$$\{1, 2, \dots, k\} = A \cup B.$$

These pairs correspond bijectively to 3-colorings of $\{1, 2, \dots, k\}$—one color for the elements in $A \backslash B$, the second for the elements in $B \backslash A$, and the third for the elements in $A \cap B$. Thus there are $3^k = 3^{\omega(f)}$ pairs. Summing over square-free numbers $f < z^2$, we get

$$\sum_{e,d \in D} |r_{[e,d]}| \leq \sum_{f \in D(z^2)} 3^{\omega(f)} |r_f|.$$

□

For bounding $r(n)$ by Selberg sieve we assume that n is even; for odd n we have $r(n) = 0$ or 2—the latter occurs when $n-2, n$ are prime twins. We need to count the multiples of a square-free number d among the numbers $m(n-m)$, $1 \leq m \leq n-1$. We start, for a prime p, with the congruence

$$m(n-m) \equiv 0,\ m \in \mathbb{Z}_p.$$

Its solutions m are the residues 0 and n modulo p. Thus for p dividing n it has one solution and else it has two solutions. For given even $n \in \mathbb{N}$, we define the function $g:\ P \to (0,1)$ by

$$g(p) = \begin{cases} 1/p & \dots\ p \text{ divides } n \\ 2/p & \dots\ p \text{ does not divide } n. \end{cases}$$

The above congruence has then $g(p)p$ solutions. We extend g multiplicatively to $g:\ \mathbb{N} \to (0,1]$ (and set $g(1) = 1$); g is completely multiplicative and $0 < g(d) < 1$ for every $d \geq 2$, as 2 divides n. We see that more generally for every square-free $d \in \mathbb{N}$ the congruence

$$m(n-m) \equiv 0,\ m \in \mathbb{Z}_d,$$

has exactly $g(d)d$ solutions: for $d = p_1 p_2 \dots p_a q_1 q_2 \dots q_b$, where the primes p_i divide n and the primes q_i do not divide n, only one m makes $m(n-m)$ zero in $\mathbb{Z}_{p_i}$ and exactly two m's in $\mathbb{Z}_{q_i}$, thus by the Chinese remainder theorem exactly $2^b = g(d)d$ residues m make $m(n-m)$ zero in $\mathbb{Z}_d$. Finally, we consider the number of solutions $|A_d|$ of the congruence

$$m(n-m) \equiv 0 \pmod{d},\ 1 \leq m \leq n-1.$$

The interval $1, 2, \dots, n-1$ contains $\lfloor (n-1)/d \rfloor$ disjoint complete systems of residues modulo d and is contained in $\lceil (n-1)/d \rceil$ such systems. In each system we have $g(d)d$ solutions. Thus

$$g(d)d\lfloor (n-1)/d \rfloor \leq |A_d| \leq g(d)d\lceil (n-1)/d \rceil.$$

The upper and the lower bound differ by at most $g(d)d = 2^b \le 2^{\omega(d)}$ and the number $g(d)(n-1)$ lies between them like $|A_d|$. We have the following result.

Lemma 3.3.3 *Let $n \in \mathbb{N}$ be even and $g:\ \mathbb{N} \to (0,1]$ be the corresponding above defined completely multiplicative function. Then for every square-free number $d \in \mathbb{N}$, the number $|A_d|$ of multiples of d in the sequence*

$$A = (m(n-m) \mid 1 \le m \le n-1)$$

satisfies $|A_d| = g(d)(n-1) + r_d$ where $|r_d| \le 2^{\omega(d)}$. Hence, for $z > 1$ we have

$$\sum_{k \in D(z^2)} 3^{\omega(k)} |r_k| \le \sum_{k \in D(z^2)} 6^{\omega(k)} \le z^{2+2\log_2 6} < z^{7.17}.$$

Proof. We have proven the first part already. As for the sum, the bound follows from that it has less than z^2 summands and $6^{\omega(k)} = 2^{\omega(k)\log_2 6} < z^{2\log_2 6}$ (because $2^{\omega(k)} \le k < z^2$ for $k \in D(z^2)$). □

The second ingredient in Selberg sieve is a good lower bound on $\sum_{k<z} g(k)$. For it we need some estimates, one of them involving the function $d(n)$ counting divisors of $n \in \mathbb{N}$,

$$d(n) = \sum_{d|n} 1 = |\{(k,l) \in \mathbb{N}^2 \mid kl = n\}|.$$

Proposition 3.3.4 *For every real $x > 1$ and $m \in \mathbb{N}$ the following holds.*

1. $\sum_{n<x} 1/n > \log x$.
2. $\sum_{n<x} (\log n)/n < (3/4)(\log x)^2$.
3. $\sum_{n<x} d(n)/n > (1/4)(\log x)^2$.
4. $\prod_{p|m}(1-p^{-1}) > (1/2)\prod_{p|m}(1+p^{-1})^{-1}$.

Proof. 1. This is the integral estimate

$$\sum_{n<x} \frac{1}{n} > \int_1^x \frac{dt}{t} = \log x.$$

2. For $x \leq 3$ the inequality holds, as $(\log 2)/2 < 0.73(\log 2)^2$. For $x > 3$ we have the integral estimate

$$\begin{aligned}
\sum_{n<x} \frac{\log n}{n} &< \frac{\log 2}{2} + \frac{\log 3}{3} + \int_3^x \frac{\log t}{t} dt \\
&= \frac{(\log x)^2}{2} + \frac{\log 2}{2} + \frac{\log 3}{3} - \frac{(\log 3)^2}{2} \\
&< \frac{(\log x)^2}{2} + 0.2 \\
&< 0.7(\log x)^2 \quad (\text{as } \log x > 1)
\end{aligned}$$

and the inequality also holds.

3. By the bounds in parts 1 and 2,

$$\begin{aligned}
\sum_{n<x} \frac{d(n)}{n} &= \sum_{kl<x} \frac{1}{kl} = \sum_{k<x} \frac{1}{k} \sum_{l<x/k} \frac{1}{l} > \sum_{k<x} \frac{\log(x/k)}{k} \\
&= (\log x) \sum_{k<x} \frac{1}{k} - \sum_{k<x} \frac{\log k}{k} \\
&> \frac{(\log x)^2}{4}.
\end{aligned}$$

4. This follows from the equality

$$\prod_{n=2}^{\infty} (1 - n^{-2}) = \prod_{n=2}^{\infty} \frac{(n-1)(n+1)}{n^2} = \frac{1}{2}.$$

□

Lemma 3.3.5 *Let $n \in \mathbb{N}$ be even, $g: \mathbb{N} \to (0,1]$ be the corresponding above defined completely multiplicative function and $z > 1$ be a real number. Then*

$$\sum_{k<z} g(k) > \frac{(\log z)^2}{8 \prod_{p|n} (1 + p^{-1})}.$$

Proof. For $k \in \mathbb{N}$, let $s_1, s_2, \ldots, s_j$ be the exponents of the primes in the decomposition of k that do not divide n. Then

$$g(k) = \frac{2^{s_1+s_2+\cdots+s_j}}{k} \geq \frac{(s_1+1)(s_2+1)\ldots(s_j+1)}{k} = \frac{d_n(k)}{k}$$

where $d_n(k)$ is the number of divisors of k coprime with n. Also,

$$\prod_{p|n}(1-1/p)^{-1} = \sum_{k\in P_n} k^{-1}$$

where P_n is the set of numbers composed only of primes dividing n. Hence

$$\begin{aligned}
\frac{\sum_{k<z} g(k)}{\prod_{p|n}(1-1/p)} &\geq \sum_{k<z} d_n(k)k^{-1} \sum_{l\in P_n} l^{-1} = \sum_{k<z} d_n(k) \sum_{k|t,\ t/k\in P_n} t^{-1} \\
&= \sum_{t=1}^{\infty} t^{-1} \sum_{k<z,\ k|t,\ t/k\in P_n} d_n(k) \\
&\geq \sum_{t<z} t^{-1} \sum_{k|t,\ t/k\in P_n} d_n(k).
\end{aligned}$$

The last inner sum equals $d(t)$. To see it, we split t as $t = t_1t_2$ with $t_1 \in P_n$ and $(t_2, n) = 1$. Then k runs through the numbers it_2 with $i|t_1$ and the sum contains $d(t_1)$ summands, each of which equals $d(t_2)$. The inner sum equals $d(t_1)d(t_2) = d(t)$ because $(t_1, t_2) = 1$ and $d(\cdot)$ is multiplicative. Thus, by bounds in parts 3 and 4 of Proposition 3.3.4,

$$\sum_{k<z} g(k) \geq \prod_{p|n}(1-1/p) \sum_{t<z} d(t)/t > (1/8) \prod_{p|n}(1+1/p)^{-1}(\log z)^2.$$

□

Proof of Theorem 3.2.1. Let $n \in \mathbb{N}$ be even and

$$A = (m(n-m) \mid 1 \leq m \leq n-1).$$

Let $z > 1$, $S(A, z)$, $g(k)$ and r_k be as above. By Theorem 3.3.1,

$$r(n) \leq 2z + S(A, z) < 2z + \frac{n}{\sum_{k<z} g(k)} + \sum_{k\in D(z^2)} 3^{\omega(k)}|r_k|.$$

We set $z = n^{1/10}$, then $(\log z)^2 = (\log n)^2/100$ and $z^{7.17} < n^{3/4}$. By Lemmas 3.3.3 and 3.3.5,

$$r(n) < 2n^{1/10} + \frac{800n}{(\log n)^2} \prod_{p|n}(1+1/p) + n^{3/4} < \frac{827n}{(\log n)^2} \prod_{p|n}(1+1/p) \quad \text{for } n \geq 2,$$

because $n^{1/10} < n^{3/4} < 9n/(\log n)^2$ for every $n \geq 2$.

To get a smaller c for (not too) large n, we set $z = n^\alpha$ for an appropriate positive $\alpha < 7.17^{-1} < 0.139$ and find positive constants c_1 and n_0 such that $2n^\alpha + n^{7.17\alpha} < c_1 n(\log n)^{-2}$ for every $n > n_0$. We omit $2n^\alpha$ as it is negligible in the considered ranges of n and look for the maximum c_1 of $f(n) = (\log n)^2/n^\beta$ on $[2, +\infty)$ where $\beta = 1 - 7.17\alpha \in (0, 1)$. It is attained at $n_0 = \exp(2/\beta)$ and $c_1 = f(n_0) = (2/\mathrm{e}\beta)^2$. Selecting $\beta = 0.134581$ corresponding to $\alpha = 0.1207\ldots$ we get $n_0 = 2.844\ldots \cdot 10^6$ and $c_1 = 29.888\ldots$. The neglected term contributes factor $2n^\alpha/n^{7.17\alpha} = 2/n^{6.17\alpha} < 2/n^{0.6} < 0.001$ for $n > n_0$. Thus for $n > n_0 > 2.85 \cdot 10^6$ we may take $c = 8\alpha^{-2} + c_1 < 580$.
$\square$

3.4 Numbers λ_d^*

It remains to prove Lemma 3.3.2. We begin by recalling properties of the *Möbius function* $\mu : \mathbb{N} \to \{-1, 0, 1\}$, defined by $\mu(n) = \mu(p_1 p_2 \ldots p_k) = (-1)^k$ for square-free numbers $n = p_1 p_2 \ldots p_k$ and by $\mu(n) = 0$ else.

Proposition 3.4.1 *Möbius function μ has the following properties.*

1. *It is multiplicative: $\mu(1) = 1$ and $\mu(ab) = \mu(a)\mu(b)$ for every pair of coprime numbers $a, b \in \mathbb{N}$.*

2. *For every $n \in \mathbb{N}$,*

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

3. *The Möbius inversion formula: for any pair of functions $f, g : \mathbb{N} \to \mathbb{R}$,*

$$\forall n \in \mathbb{N} :\ f(n) = \sum_{d|n} \mu(n/d) g(d) \iff \forall n \in \mathbb{N} :\ g(n) = \sum_{d|n} f(n).$$

Proof. 1. This follows from the definition of μ and from the uniqueness of the prime factorization.

2. For $n = 1$ the sum equals 1. For $n > 1$ the sum does not change if we replace n by the product $p_1 p_2 \ldots p_k$ of its prime factors. By the binomial

formula, the sum equals

$$\sum_{d|p_1\dots p_k} \mu(d) = \sum_{j=0}^{k} \binom{k}{j}(-1)^j = (1-1)^k = 0.$$

3. This follows from part 2. We show only the implication $\Rightarrow$, the proof of the converse is similar. Suppose that $f(n)$ is for every n expressed by the stated formula. Then

$$\sum_{d|n} f(d) = \sum_{d|n}\sum_{e|d} \mu(d/e)g(e) = \sum_{e|n} g(e) \sum_{f|(n/e)} \mu(f) = g(n).$$

□

We define numbers λ_n^*. Recall that $z > 1$ is a real number, $D = D(z)$ is the set of square-free numbers smaler than z, $g : \mathbb{N} \to (0, 1]$ is a completely multiplicative function satisfying $g(1) = 1$ and $0 < g(n) < 1$ for $n > 1$, and

$$G(x_d \mid d \in D) = \sum_{d,e\in D} g([d, e]) \cdot x_d x_e.$$

For $l \in \mathbb{N}$, we define

$$f(l) = \sum_{d|l} \frac{\mu(d)}{g(l/d)}.$$

By the complete multiplicativity of g and the definition of μ,

$$f(l) = \frac{1}{g(l)} \sum_{d|l} \mu(d)g(d) = \frac{1}{g(l)} \prod_{p|l}(1 - g(p)) > 0$$

and we see that f is multiplicative. By Möbius inversion formula,

$$\frac{1}{g(k)} = \sum_{d|k} f(d).$$

For $d \in D$ we define

$$\alpha_d = \sum_{dl\in D} \frac{1}{f(l)} \quad \text{and} \quad \lambda_d^* = \frac{\mu(d)\alpha_d}{f(d)g(d)\alpha_1}.$$

We prove four properties of the numbers α_d and λ_d^*, of which 1, 3 and 4 give Lemma 3.3.2. To simplify notation, we use symbol $\langle C\rangle$ for the characteristic function of a condition C: $\langle C\rangle = 1$ if C holds and as $\langle C\rangle = 0$ if it does not.

Proposition 3.4.2 *With the above notation, the following holds.*

1. *$\lambda_1^* = 1$ and $|\lambda_d^*| \leq 1$ for every $d \in D$.*
2. *For every $k \in D$ we have $\sum_{d \in D} \langle k|d \rangle \cdot g(d)\lambda_d^* = \mu(k)/(\alpha_1 f(k))$.*
3. *$G(\lambda_d^* \mid d \in D) = (\alpha_1)^{-1}$.*
4. *$\alpha_1 = \sum_{k \in D} f(k)^{-1} \geq \sum_{k<z} g(k)$.*

Proof. 1. Since $\mu(1) = g(1) = f(1) = 1$, $\lambda_1^* = 1$. Note that for any multiplicative function h we have $h(ab) = h(a)h(b)$ whenever $ab \in D$, as then $(a, b) = 1$. Let $d \in D$, then

$$\begin{aligned}
\alpha_1 &= \sum_{k \in D} \frac{1}{f(k)} = \sum_l \langle l|d \rangle \sum_{k \in D} \frac{\langle (k,d) = l \rangle}{f(k)} \\
&= \sum_l \frac{\langle l|d \rangle}{f(l)} \sum_m \frac{\langle ml \in D \;\&\; (m, d/l) = 1 \rangle}{f(m)} \\
&\geq \sum_l \frac{\langle l|d \rangle}{f(l)} \sum_m \frac{\langle md \in D \rangle}{f(m)} = \sum_m \frac{\langle md \in D \rangle}{f(m)} \sum_l \frac{\langle l|d \rangle}{f(l)} \\
&= \frac{\alpha_d}{f(d)} \sum_l \langle l|d \rangle f(d/l) \\
&= \frac{\alpha_d}{f(d)g(d)}.
\end{aligned}$$

Thus

$$|\lambda_d^*| = \frac{\alpha_d}{f(d)g(d)\alpha_1} \leq 1.$$

2. Let $k \in D$. Then

$$\begin{aligned}
\sum_{d \in D} \langle k|d \rangle g(d) \lambda_d^* &= \sum_{d \in D} \langle k|d \rangle g(d) \frac{\mu(d)\alpha_d}{f(d)g(d)\alpha_1} \\
&= \frac{1}{\alpha_1} \sum_l \langle kl \in D \rangle \frac{\mu(kl)\alpha_{kl}}{f(kl)} \\
&= \frac{\mu(k)}{\alpha_1 f(k)} \sum_l \langle kl \in D \rangle \frac{\mu(l)}{f(l)} \sum_m \frac{\langle klm \in D \rangle}{f(m)} \\
&= \frac{\mu(k)}{\alpha_1 f(k)} \sum_l \langle kl \in D \rangle \mu(l) \sum_m \frac{\langle klm \in D \rangle}{f(lm)} \\
&= \frac{\mu(k)}{\alpha_1 f(k)} \sum_n \frac{\langle kn \in D \rangle}{f(n)} \sum_l \langle l|n \rangle \mu(l) \\
&= \frac{\mu(k)}{\alpha_1 f(k)}.
\end{aligned}$$

3. Using the identity $[d, e] = de/(d, e)$ and complete multiplicativity of g, we transform $G(x_d \mid d \in D)$ and get

$$\begin{aligned}
G(x_d \mid d \in D) &= \sum_{d_i \in D} \frac{g(d_1)x_{d_1} g(d_2)x_{d_2}}{g((d_1, d_2))} \\
&= \sum_{d_i \in D} \sum_{k|d_i} f(k) g(d_1)x_{d_1} g(d_2)x_{d_2} \\
&= \sum_{k \in D} f(k) \sum_{d_i \in D} \langle k|d_1 \ \& \ k|d_2 \rangle g(d_1)x_{d_1} g(d_2)x_{d_2} \\
&= \sum_{k \in D} f(k) \Big(\sum_{d \in D} \langle k|d \rangle g(d) x_d \Big)^2.
\end{aligned}$$

Setting $x_d = \lambda_d^*$ we get, by part 2,

$$G(\lambda_d^* \mid d \in D) = \sum_{k \in D} f(k) \left(\frac{\mu(k)}{\alpha_1 f(k)} \right)^2 = \frac{1}{\alpha_1^2} \sum_{k \in D} \frac{1}{f(k)} = \frac{1}{\alpha_1}.$$

4. Finally,

$$\alpha_1 = \sum_{k \in D} \frac{1}{f(k)} = \sum_{k \in D} g(k) \prod_{p|k} (1 - g(p))^{-1}$$

which equals

$$\begin{aligned}
&= \sum_{k\in D} g(k) \prod_{p|k} (1 + g(p) + g(p^2) + \cdots) \\
&= \sum_{k\in D} g(k) \sum_{l} \langle p|l \Rightarrow p|k\rangle g(l) \\
&= \sum_{k,l} \langle k \in D \;\&\; (p|l \Rightarrow p|k)\rangle g(kl) \\
&= \sum_{m} g(m) \sum_{k} \langle k \in D \;\&\; k|m \;\&\; (p|(m/k) \Rightarrow p|k)\rangle \\
&\geq \sum_{m<z} g(m)
\end{aligned}$$

because for $m < z$ the last inner sum is ≥ 1 (set k to be the product of the prime factors of m). □

3.5 Remarks

This chapter is based on Nathanson [31, Chapter 7] and Gelfond and Linnik [16, Chapter 1 and 6]. Here is a translation of the opening quotation.

> Beforehand you can never say what will be the final turn in this or that life story: academician Nikolaj Nikolajevič Luzin, persecuted in 1936, ended his life peacefully in his Moscow appartment at Stretenskij boulevard in 1950, but those who were plotting a tribunal for him, the regular secretary of the Academy N. P. Gorbunov and the corresponding member of the Academy, briliant L. G. Shnirel'man, would die in 1938 — the first will be shot dead as an enemy of the people and the second, coming home from a "conversation" at NKVD, will open gas faucet in his flat.
>
> S. S. Demidov, B. V. Levšin [10]

Shnirel'man proved his theorem in [45] and in [46] published an expanded version of his memoir. The inequality $\sigma(A+B) \geq \sigma(A)+\sigma(B)-\sigma(A)\sigma(B)$

(part 4 of Theorem 3.1.1) was later improved by Mann [27] to $\sigma(A+B) \geq \min(1, \sigma(A)+\sigma(B))$. To bound $r(n)$, Shnirel'man used the sieve of V. Brunn that had been developed around 1920. The technically simpler Selberg sieve was published in [41]. The current record value of Shnirel'man's constant $h = 7$ is due to Ramaré [38] who proved that every even number is a sum of at most six primes. In 1937, I.M. Vinogradov [49] proved that every sufficiently large odd number is a sum of three primes; for the proof see, for example, Nathanson [31, Chapter 7], Gowers [18] or Karacuba [24, Chapter 10]. Thus every sufficiently large $n \in \mathbb{N}$ is a sum of at most four primes.

Bratus and Pak [7] give an application of Goldbach's conjecture in algorithmic group theory. Pintz [35] presents interesting information on the origin of Goldbach's conjecture. For the life and mathematics of A. Selberg see Baas and Skau [4].

Chapter 4

Roth's theorem on 3-term arithmetic progressions

Denote by $1 = u_1 < u_2 < \cdots < u_k \leq x$ *a sequence of integers no three of which form an arithmetic progression. Denote by* $A(x)$ *the maximum value of* k*. The author proves that* $\lim_{x\to\infty} A(x)/x = 0$*. This has been conjectured for about 20 years. Outline of the proof: Put* $(\dots)$

P. Erdős's review [15] of K. Roth's article [39]

We present two proofs of a fundamental result obtained by K. Roth in 1952.

Theorem 4.0.1 (Roth, 1952) *For every* $\delta > 0$ *there is an* $N \in \mathbb{N}$ *such that if* $n > N$ *and the set* $A \subset \{1, 2, \dots, n\}$ *has more than* δn *elements, then* A *contains an arithmetic progression* $a, a + d, a + 2d$, $d > 0$, *of length* 3.

By arithmetic progression we shall mean one with positive difference; progressions $a, a, \dots, a$ with zero difference will be called degenerate. Denoting by $r_3(n)$ the maximum size of a subset in $\{1, 2, \dots, n\}$ containing no arithmetic progression of length 3, we rephrase Roth's theorem as $r_3(n) = o(n)$ for $n \to \infty$.

Sections 4.1 and 4.2 contain an analytic proof of Roth's theorem using the *circle method.* In Sections 4.3, 4.4 and 4.5 we give a different combinatorial proof using tools of the *extremal graph theory.*

4.1 Analytic proof

For real t we consider the function ($i = \sqrt{-1}$ is the imaginary unit)

$$e(t) = \exp(2\pi i t) : \mathbb{R} \to \{z \in \mathbb{C} \mid |z| = 1\}$$

mapping $\mathbb{R}$ onto the unit circle in $\mathbb{C}$. Recall that for every $z \in \mathbb{C}$,

$$\exp(z) = \sum_{n \geq 0} \frac{z^n}{n!}.$$

We summarize some useful properties of $e(t)$.

Proposition 4.1.1 *Let $e(t) = \exp(2\pi i t)$ and $f(z), g(z)$ be two complex Laurent polynomials, which means that*

$$f(z) = \sum_{k \in X} a_k z^k \quad \text{and} \quad g(z) = \sum_{k \in Y} b_k z^k$$

where $a_k, b_k \in \mathbb{C}$ and $X, Y \subset \mathbb{Z}$ are finite sets of integers; we set $a_k = 0$ if $k \notin X$ and similarly for b_k. The following hold.

1. *For every $t, u \in \mathbb{R}$ and $m \in \mathbb{Z}$ we have $e(t)e(u) = e(t+u)$, $e(t)^m = e(mt)$ and $\overline{e(t)} = e(-t) = 1/e(t)$.*
2. *If $m \in \mathbb{Z}$ then*
$$\int_0^1 e(mt)\, dt = \langle m = 0 \rangle = \begin{cases} 1 & \text{if } m = 0 \\ 0 & \text{if } m \neq 0. \end{cases}$$
3. *The identity*
$$\int_0^1 f(e(t)) \cdot g(e(t))\, dt = \sum_{k+l=0} a_k b_l.$$
Analogous identities hold for products of several Laurent polynomials.
4. *The* Parseval identity
$$\int_0^1 |f(e(t))|^2\, dt = \sum_{k \in X} |a_k|^2.$$

5. *The* Cauchy–Schwarz inequality

$$\int_0^1 |f(e(t))\cdot g(e(t))|\,dt \le \left(\int_0^1 |f(e(t))|^2\,dt\right)^{1/2} \left(\int_0^1 |g(e(t))|^2\,dt\right)^{1/2}.$$

Proof. 1. We have $\exp(0) = 1$ and, by the binomial theorem,

$$\begin{aligned}\exp(z_1)\exp(z_2) &= \sum_{k\ge 0}\frac{z_1^k}{k!}\sum_{l\ge 0}\frac{z_2^l}{l!} = \sum_{k+l\ge 0}\frac{1}{(k+l)!}\sum_{k=0}^{k+l}\binom{k+l}{k}z_1^k z_2^l \\ &= \sum_{m\ge 0}\frac{(z_1+z_2)^m}{m!} \\ &= \exp(z_1+z_2).\end{aligned}$$

This gives the identities for $e(t)$.

2. Indeed, $m = 0$ gives $\int_0^1 e(0)\,dt = \int_0^1 1\,dt = 1$, while for $m \neq 0$ one has

$$\int_0^1 e(mt)\,dt = \left[\frac{1}{2\pi i m}\exp(2\pi i m t)\right]_0^1 = \frac{1-1}{2\pi i m} = 0$$

as $\exp(2\pi i m) = 1$ for every $m \in \mathbb{Z}$.

3. Multiplying both polynomials, using linearity of integration and parts 1 and 2, we see that the integral equals

$$\sum_{k,l\ (\in X\cup Y)} a_k b_l \int_0^1 e((k+l)t)\,dt = \sum_{k+l=0} a_k b_l.$$

4. This follows from the previous identity by setting $g(z) = \overline{f(z)}$, because $\overline{f(z)} = \sum_{k\in -X}\overline{a_{-k}}z^k$ where $-X = \{-x \mid x \in X\}$.

5. We review the proof of the Cauchy–Schwarz inequality for real vector spaces with inner product. Suppose V is a vector space with the field of scalars $\mathbb{R}$ and the inner product

$$\langle\cdot,\cdot\rangle:\ V\times V \to \mathbb{R},$$

which is a bilinear and symmetric mapping ($\langle \alpha u+\beta v, w\rangle = \alpha\langle u,w\rangle + \beta\langle v,w\rangle$ and $\langle v,u\rangle = \langle u,v\rangle$ for any $\alpha,\beta\in\mathbb{R}$ and $u,v,w\in V$) satisfying $\langle u,u\rangle \ge 0$ for any $u \in V$, with equality only for $u = 0$. Thus, for any $u, v \in V$, $v \neq 0$, and $\lambda \in \mathbb{R}$,

$$\langle u-\lambda v, u-\lambda v\rangle \ge 0,$$

equivalently

$$\langle u, u\rangle - 2\lambda\langle u, v\rangle + \lambda^2\langle v, v\rangle \geq 0.$$

Setting $\lambda = \langle u, v\rangle/\langle v, v\rangle$ we get

$$\langle u, u\rangle - 2\frac{\langle u, v\rangle^2}{\langle v, v\rangle} + \frac{\langle u, v\rangle^2}{\langle v, v\rangle} \geq 0.$$

This after rearrangement gives the general Cauchy–Schwarz inequality

$$|\langle u, v\rangle| \leq \sqrt{\langle u, u\rangle\langle v, v\rangle}.$$

Now we take the vector space of real continuous functions $F: [0, 1] \to \mathbb{R}$, with the inner product

$$\langle F, G\rangle = \int_0^1 F(t) \cdot G(t)\, dt.$$

The stated inequality follows by applying the Cauchy–Schwarz inequality to the functions $|f(e(t))|$ and $|g(e(t))|$. $\square$

Let $A \subset \mathbb{Z}$ be a finite set. We consider the generating Laurent polynomial of A,

$$f_A(z) = \sum_{a\in A} z^a = \sum_{k\in\mathbb{Z}} \langle k \in A\rangle z^k.$$

For $m \in \mathbb{Z}$, $m \neq 0$, note the identity

$$f_A(z^m) = f_{mA}(z)$$

where $mA = \{ma \mid a \in A\}$. We define the function

$$p_3(A) = \#\{(a, a + d, a + 2d) \in A^3 \mid d \in \mathbb{Z}\}.$$

It counts twice every arithmetic progressions of length 3 in A (as $(a, a + d, a + 2d)$ and $(a + 2d, a + 2d - d, a + 2d - 2d)$) plus the degenerate ones (a, a, a), $a \in A$. Note that A contains no arithmetic progressions of length 3 if and only if $p_3(A) = |A|$.

Proposition 4.1.2 *For any finite set $A \subset \mathbb{Z}$,*

$$p_3(A) = \int_0^1 f_A(e(t))^2 \cdot f_A(e(-2t))\, dt.$$

Proof. The integrand is the product of $f_A(e(t))$, $f_A(e(t))$, and $f_A(e(-2t)) = f_A(e(t)^{-2}) = f_{-2A}(e(t))$. By part 3 of Proposition 4.1.1, the integral equals

$$\#\{(x, y, z) \in A^3 \mid x + y - 2z = 0\}.$$

By the parametrization $x = a, y = a + 2d, z = a + d$, this equals $p_3(A)$. $\square$

The next result is often called *Fekete's lemma.*

Lemma 4.1.3 *If a sequence of nonnegative real numbers $a_1, a_2, \ldots$ is subadditive, which is to say that, for all $m, n \geq 1$,*

$$a_{m+n} \leq a_m + a_n,$$

then the limit

$$L = \lim_{n\to\infty} \frac{a_n}{n}$$

exists, is finite and $a_n/n \geq L$ for every $n \geq 1$.

Proof. For $m, n \in \mathbb{N}$ we write $n = km + l$ where $k, l \in \mathbb{N}_0$ and $0 \leq l < m$. The subadditivity implies $a_n \leq ka_m + a_l$, which we rewrite as the inequality

$$\frac{a_n}{n} \leq \frac{a_m}{m} \cdot \frac{1}{1 + l/km} + \frac{a_l}{km + l}.$$

For $m = 1$ this is just $a_n/n \leq a_1$, so $0 \leq a_n/n \leq a_1$ and a_n/n is bounded. Let

$$L = \liminf_{r\to\infty} a_r/r < +\infty.$$

We fix m so that a_m/m is near to L and let $n \to \infty$. Then, as the factor at a_m/m goes to 1 and the last term in the inequality goes to 0, for every large n the fraction a_n/n is also near to L. Thus

$$L = \lim_{r\to\infty} a_r/r.$$

By the inequality, if $a_m/m < L$ for some m, then $a_n/n < L - \delta$ for some $\delta > 0$ and every large n, which is not possible. Thus $a_m/m \geq L$ for every m. $\square$

Recall that for $n \in \mathbb{N}$,

$$r_3(n) = \max\{|A| \mid A \subset [n],\ p_3(A) = |A|\}$$

equals to the maximum size of a subset in $[n]$ free of arithmetic progressions of length 3.

Proposition 4.1.4 *Let $A \subset \mathbb{Z}$ be any (not necessarily finite) set and $m, n \in \mathbb{N}$.*

1. *If A is free of arithmetic progressions of length 3, then so is any subset $B \subset A$ and any affine image $B = \{\alpha a + \beta \mid a \in A\}$, $\alpha, \beta \in \mathbb{Z}$.*
2. *We have the inequalities*
$$r_3(n) \leq r_3(n+1) \quad \textit{and} \quad r_3(m+n) \leq r_3(m) + r_3(n).$$
3. *There exists a limit*
$$d_3 = \lim_{n\to\infty} \frac{r_3(n)}{n} \in [0, 1]$$
and $r_3(n) \geq d_3 n$ for all $n \geq 1$.

Proof. 1. This is clear from the definitions and from the fact that arithmetic progressions of length 3 are preserved by affine mappings.

2. Suppose that $A \subset [n]$, $|A| = r_3(n)$, contains no arithmetic progressions of length 3. But A is a subset of $[n + 1]$ as well and thus $r_3(n) = |A| \leq r_3(n + 1)$. Suppose that $A \subset [m + n]$, $|A| = r_3(m + n)$, contains no arithmetic progressions of length 3. Thus $r_3(m + n) = |A| = |A \cap [m]| + |A \cap [m + 1, m + n]| \leq r_3(m) + r_3(n)$, by part 1.

3. This follows by the second inequality in part 2 and Lemma 4.1.3. □

Hence Roth's theorem amounts to proving that $d_3 = 0$.

For every $n \in \mathbb{N}$, we fix a subset $A(n)$ of $[n]$ with the size $r_3(n)$ and no arithmetic progression of length 3. Further, we let
$$g_n(z) = d_3 z + d_3 z^2 + \cdots + d_3 z^n.$$
Then
$$f_{A(n)}(1) - g_n(1) = |A(n)| - d_3 n = r_3(n) - d_3 n = o(n), \; n \to \infty.$$
The main step is to extend this estimate from $z = 1$ to any z on the unit circle $|z| = 1$.

Proposition 4.1.5 *In the above notation,*
$$f_{A(n)}(z) - g_n(z) = o(n), \; n \to \infty,$$

uniformly on the unit circle $|z| = 1$. Said explicitly, for every $\varepsilon > 0$ there is an $n_0 = n_0(\varepsilon)$ such that if $n > n_0$ then

$$\max_{|z|=1} |f_{A(n)}(z) - g_n(z)| < \varepsilon n.$$

We defer the proof to the next section. Note that, trivially,

$$\max_{|z|=1} |f_{A(n)}(z) - g_n(z)| \leq \max(d_3, 1 - d_3)n.$$

Now we can prove Roth's theorem.

Proof of Theorem 4.0.1. Let $n \in \mathbb{N}$ and the set $A(n) \subset [n]$ be as before (i.e., witnessing the value $r_3(n)$). We define

$$f(z) = f_{A(n)}(z) = \sum_{a \in A(n)} z^a,\ g(z) = g_n(z) = d_3 \sum_{k=1}^{n} z^k \ \text{ and } \ h(z) = f(z) - g(z).$$

Thus

$$f(z) = g(z) + h(z).$$

By Proposition 4.1.2,

$$\begin{aligned}
|A(n)| = p_3(A(n)) &= \int_0^1 f(e(t))^2 \cdot f(e(-2t))\, dt \\
&= \int_0^1 \big(g(e(t)) + h(e(t))\big)^2 \cdot \big(g(e(-2t)) + h(e(-2t))\big)\, dt \\
&= \int_0^1 g(e(t))^2 \cdot g(e(-2t))\, dt \ + \ \text{seven integrals} \\
&= d_3^3 \int_0^1 g_0(e(t))^2 \cdot g_0(e(-2t))\, dt \ + \ \text{seven integrals}
\end{aligned}$$

where $g_0(z) = z + z^2 + \cdots + z^n$ and each of the seven integrals has the form

$$\int_0^1 a(e(t)) \cdot b(e(t)) \cdot c(e(-2t))\, dt$$

with $a(z), b(z), c(z) \in \{g(z), h(z)\}$ and at least one of $a(z), b(z), c(z)$ equal to $h(z)$. Since $g_0(z) = z + z^2 + \cdots + z^n = f_{[n]}(z)$, Proposition 4.1.2 gives us the value of the first integral without $h(z)$ in the integrand: it equals

$$\begin{aligned} p_3([n]) &= 2((n-2)+(n-4)+\cdots+(n-2\lfloor n/2\rfloor))+n \\ &= 2\lfloor n/2\rfloor(\lceil n/2\rceil-1)+n \\ &= n^2/2+O(n). \end{aligned}$$

We show that each of the remaining seven integrals is $o(n^2)$. We demonstrate this in the case when $b(z)=h(z)$, other cases are very similar. By Proposition 4.1.5, $h(z)=o(n)$ uniformly in $z\in\mathbb{C}$, $|z|=1$. Thus

$$\begin{aligned} \left|\int_0^1 a(e(t))\cdot h(e(t))\cdot c(e(-2t))\,dt\right| &\le \int_0^1 |h(e(t))|\cdot|a(e(t))\cdot c(e(-2t))|\,dt \\ &= o(n)\int_0^1 |a(e(t))\cdot c(e(-2t))|\,dt. \end{aligned}$$

By part 5 of Proposition 4.1.1 this is at most

$$o(n)\left(\int_0^1 |a(e(t))|^2\,dt\right)^{1/2}\left(\int_0^1 |c(e(-2t))|^2\,dt\right)^{1/2}.$$

As the Laurent polynomials $a(z)$ and $c(z^{-2})$ have at most n nonzero coefficients, all in $[0,1]$, by part 4 of Proposition 4.1.1 each of the two integrals is $\le n$. Thus

$$\left|\int_0^1 a(e(t))\cdot h(e(t))\cdot c(e(-2t))\,dt\right| \le o(n)\sqrt{n}\sqrt{n}=o(n^2).$$

We see that, for $n\to\infty$,

$$n\ge|A(n)|=p_3(A(n))=\frac{d_3^3n^2}{2}+o(n^2).$$

This forces $d_3=\lim_{n\to\infty} r_3(n)/n=0$ and Roth's theorem is proved. $\square$

4.2 Uniform bound on the unit circle

We need four lemmas. For a polynomial $p(z)=a_0+a_1z+\cdots+a_nz^n$ and $0\le m\le n$, we define $p_m(z)=a_0+a_1z+\cdots+a_mz^m$; thus $p_n(z)=p(z)$.

Lemma 4.2.1 *Let $p(z) = a_0 + a_1 z + \cdots + a_n z^n \in \mathbb{C}[z]$ be a polynomial, numbers $u, \zeta \in \mathbb{C}$ satisfy $|u| = |\zeta| = 1$, and $|p_m(\zeta)| \le M$ for all $0 \le m \le n$ for a constant $M > 0$. Then*

$$|p(u)| \le M(n|u-\zeta| + 1).$$

Proof. If z is a variable and $\zeta \in \mathbb{C}$ is nonzero, we have the identity

$$p(z)/(1 - z/\zeta) = \sum_{m=0}^{n-1} p_m(\zeta)(z/\zeta)^m + p(\zeta)(z/\zeta)^n/(1 - z/\zeta),$$

which follows by expanding the left side in geometric series:

$$p(z) \sum_{n \ge 0} (z/\zeta)^n = a_0 + (a_0 + a_1\zeta)(z/\zeta) + (a_0 + a_1\zeta + a_2\zeta^2)(z/\zeta)^2 + \cdots .$$

Hence, because $|u| = |\zeta| = 1$,

$$\begin{aligned} |p(u)| &\le |1 - u/\zeta| \sum_{m=0}^{n-1} |p_m(\zeta)| \cdot |(u/\zeta)^m| + |p(\zeta)| \cdot |(u/\zeta)^n| \\ &= |\zeta - u| \sum_{m=0}^{n-1} |p_m(\zeta)| + |p(\zeta)| \le |\zeta - u| nM + M. \end{aligned}$$

□

Another Dirichlet's theorem says that for every $\alpha \in \mathbb{R}$ and $Q \in \mathbb{N}$ there is a fraction p/q such that $|\alpha - p/q| < 1/qQ$ and $q \le Q$. The next result is a multiplicative version.

Lemma 4.2.2 *For every $u \in \mathbb{C}$, $|u| = 1$, and every $N \in \mathbb{N}$ there is an $\omega \in \mathbb{C}$, $|\omega| = 1$, and an $a \in \mathbb{N}$ such that $a \le N$, $\omega^a = 1$, and*

$$|u - \omega| < \frac{2\pi}{a(N+1)}.$$

Proof. Two of the $N+1$ numbers $1, u, u^2, \ldots, u^N$ on the unit circle are within arc distance at most $2\pi/(N+1)$. Thus $|u^j - u^i| < 2\pi/(N+1)$ for some $0 \le i < j \le N$ and $|u^a - 1| < 2\pi/(N+1)$ where $0 < a = j - i \le N$. Consider the a-th roots of the number u^a. Since $|u^a - 1| < 2\pi/(N+1)$, one of them, v, is closer to 1 than $2\pi/a(N+1)$. Another is u. All these roots form vertices of a regular a-gon R inscribed in the unit circle. We rotate R around the origin so that v is moved to 1 and obtain a regular a-gon R' whose vertices are a-th roots of unity. Vertex u is rotated to a number ω which is an a-th root of unity and satisfies $|u-\omega| < 2\pi/a(N+1)$. $\square$

We extend the function $r_3(n)$ to positive real numbers by setting

$$r_3(x) = r_3(\lceil x \rceil).$$

We know that $r_3(x) - d_3x = o(x)$ but it is not clear whether $r_3(x) - d_3x$ is monotonous. It is convenient to have a monotonous quantity and therefore we define

$$R(x) = \max_{1 \le t \le x}(r_3(t) - d_3t).$$

Lemma 4.2.3 *$R(x) \ge 0$ for every $x > 0$, function $R(x)$ is nondecreasing and $R(x) = o(x)$ as $x \to +\infty$*

Proof. The first two properties are clear from the definition. We show that $R(x) = o(x)$. Given $\varepsilon > 0$, we take x_0 such that $t > x_0$ implies $r_3(t) - d_3t < \varepsilon t$, and then we take an $x_1 > x_0$ such that $(x_0+1)/x_1 < \varepsilon$. Let $x > x_1$. Thus $R(x) = r_3(t_0) - d_3t_0$ for some $t_0 \in [1, x]$. If $t_0 > x_0$, $R(x) = r_3(t_0) - d_3t_0 < \varepsilon t_0 \le \varepsilon x$. If $t_0 \le x_0$, $R(x) = r_3(t_0) - d_3t_0 \le r_3(t_0) < t_0 + 1 \le x_0 + 1 < \varepsilon x_1 < \varepsilon x$. $\square$

Recall that $A(n) \subset [n]$ is a set of size $r_3(n)$ not containing any arithmetic progression of length 3 and

$$h(z) = f_{A(n)}(z) - g_n(z) = \sum_{k=1}^{n}(\langle k \in A(n)\rangle - d_3)z^k.$$

Recall that for $0 \le m \le n$, $h_m(z)$ is the initial sum of $h(z)$ obtained by replacing the upper summation index n by m.

Lemma 4.2.4 *If $a, n \in \mathbb{N}$ and $\omega \in \mathbb{C}$ satisfies $\omega^a = 1$, then for $0 \le m \le n$,*

$$|h_m(\omega)| < 2aR(n/a) + R(n).$$

Proof. For $a, b, m \in \mathbb{N}$ we denote $\alpha(b, a, m)$, resp. $\beta(b, a, m)$, the number of elements in $A(n) \cap [m]$, resp. in $[m]$, congruent to b modulo a. Note that

$$\sum_{b=1}^{a}\alpha(b, a, m) = |A(n) \cap [m]| \quad \text{and} \quad \sum_{b=1}^{a}\beta(b, a, m) = m.$$

By parts 1 and 3 of Proposition 4.1.4,

$$|A(n)\cap[m]| = r_3(n)-|A(n)\cap[m+1,n]| \geq r_3(n)-r_3(n-m) \geq d_3n-r_3(n-m)$$

and

$$r_3(m/a) \geq \alpha(b,a,m)$$

because the set $\{c \in A(n) \mid c \leq m \ \& \ c \equiv b \pmod{a}\}$, counted by $\alpha(b,a,m)$, can be affinely mapped to $[\lfloor m/a \rfloor]$. Also,

$$r_3(m/a) = r_3(\lceil m/a \rceil) \geq d_3\lceil m/a \rceil \geq d_3\beta(b,a,m).$$

Thus, using that $\omega^c = \omega^b$ if $c \equiv b$ modulo a, the above inequalities and the monotonicity of $R(x)$, we have

$$\begin{aligned}
|h_m(\omega)| &= \left|\sum_{b=1}^{a} \omega^b(\alpha(b,a,m) - d_3\beta(b,a,m))\right| \\
&\leq \sum_{b=1}^{a} |\alpha(b,a,m) - r_3(m/a) + r_3(m/a) - d_3\beta(b,a,m)| \\
&\leq \sum_{b=1}^{a}(r_3(m/a) - \alpha(b,a,m)) + \sum_{b=1}^{a}(r_3(m/a) - d_3\beta(b,a,m)) \\
&= 2ar_3(m/a) - |A(n)\cap[m]| - d_3m \\
&\leq 2ar_3(m/a) - d_3n + r_3(n-m) - d_3m \\
&= 2a(r_3(m/a) - d_3m/a) + (r_3(n-m) - d_3(n-m)) \\
&\leq 2aR(n/a) + R(n).
\end{aligned}$$

□

Proof of Proposition 4.1.5. Let $\varepsilon > 0$ be given. We want to estimate

$$|h(z)| = \left|\sum_{k=1}^{n}(\langle k \in A(n)\rangle - d_3)z^k\right|$$

when n is big and $z \in \mathbb{C}$ satisfies $|z| = 1$. We take an $n_0 \in \mathbb{N}$ such that $x \geq n_0$ implies $R(x) < \varepsilon x$ and then an $n_1 \in \mathbb{N}$ such that $x \geq n_1$ implies $R(x) < (\varepsilon/n_0)x$ (Lemma 4.2.3). Let $n > n_1$ and $z \in \mathbb{C}$ be arbitrary with $|z| = 1$. We set $N = \lfloor n/n_0 \rfloor$ and use Lemma 4.2.2:

$$|z-\omega| < \frac{2\pi}{a(N+1)}$$

for some a-th root of unity ω, where $1 \le a \le N$. By Lemma 4.2.1, applied with $M = 2aR(n/a) + R(n)$ (Lemma 4.2.4),

$$\begin{aligned}
|h(z)| &\le (2aR(n/a) + R(n)) \cdot (1 + n|z - \omega|) \\
&< (2aR(n/a) + R(n)) \cdot (1 + 2\pi n_0/a).
\end{aligned}$$

We distinguish two cases according to the size of a. If $a \le n_0$, then $R(n/a) \le R(n) < (\varepsilon/n_0)n$ gives

$$\begin{aligned}
|h(z)| &\le R(n) \cdot (2a + 1)(1 + 2\pi n_0/a) \\
&\le R(n) \cdot (3a + 6\pi n_0) \\
&< (\varepsilon/n_0)n \cdot 22n_0 \\
&= 22\varepsilon n.
\end{aligned}$$

If $n_0 \le a \le N$, we have $n/a \ge n/N \ge n_0$ and $R(n/a) < \varepsilon n/a$. Thus

$$\begin{aligned}
|h(z)| &\le (2aR(n/a) + R(n)) \cdot (1 + 2\pi) \\
&\le (2a\varepsilon n/a + \varepsilon n) \cdot (1 + 2\pi) \\
&\le 3\varepsilon n(1 + 2\pi) \\
&< 22\varepsilon n.
\end{aligned}$$

□

This completes the analytic proof of Roth's theorem. We turn to combinatorics.

4.3 Graph-theoretical proof

A *graph* is a pair

$$G = (V, E)$$

where V is a finite set of *vertices* and $E \subset \binom{V}{2}$ is a set of two-element subsets of V, called *edges*. A *triangle* in G is a triple of distinct vertices $\{a, b, c\}$ such that the pairs $\{a, b\}$, $\{a, c\}$, and $\{b, c\}$ are edges of G. A set of triangles in G is *edge-disjoint* if no two of them share an edge, i.e., every two intersect in at most one vertex.

Proposition 4.3.1 *For every $\delta > 0$ there exists an n_0 such that if $n > n_0$ and G is a graph on n vertices containing $m > \delta n^2$ edge-disjoint triangles $T_1, T_2, \ldots, T_m$, then G contains a triangle distinct from every T_i.*

Note that $m \leq \binom{n}{2}/3 < n^2/6$ because the edge sets of $T_1, \ldots, T_m$ are disjoint. Proposition 4.3.1 says that if G has, in the order of magnitude, the maximum possible number of edge-disjoint triangles, then some three of them pairwise intersect so that the three intersections are distinct and form a new triangle. In the next section we establish Proposition 4.3.1 in a stronger form and show that G contains $\gg n^3$ triangles. Let us see now how Proposition 4.3.1 implies Roth's theorem.

Corollary 4.3.2 *For every $\delta > 0$ there is an n_0 such that if $n > n_0$ and $X \subset [n] \times [n]$ satisfies $|X| > \delta n^2$, then X contains three elements (a, b), $(a + d, b)$, and $(a, b + d)$ with $d \neq 0$, that is, X contains an equilateral right-angle triangle.*

Proof. Horizontal lines in $[n] \times [n]$ are the n subsets

$$\{(k, l) \mid k \in [n]\},\ l \in [n],$$

and, similarly, the n vertical lines have fixed k. Skew lines are the $2n - 1$ sets $\{(k, l) \mid k, l \in [n], k + l = p\}$ with fixed sum of coordinates $p \in [2, 2n]$. We denote the set of horizontal, vertical and skew lines in $[n] \times [n]$ by L. So $|L| = 4n - 1$. To $X \subset [n] \times [n]$ we assign the graph

$$G = G_{n,X} = (L, E) \ \text{ where } \ E = \{\{e, f\} \mid e, f \in L, e \cap f \in X\}.$$

Edges of G are the pairs of lines with intersection in X. A triangle in G is formed by three lines, one horizontal, vertical and skew, which pairwise intersect in points lying in X. If the three intersections coincide in one point $v \in X$ (so the three lines go through the common point v), we denote the coresponding triangle by T_v. Triangles T_v are edge-disjoint, because two lines intersect in at most one point, and we have exactly $|X|$ of them.

For given $\delta > 0$, we assume that $|X| > \delta n^2$ and $n > n_0$ where n_0 is the bound of Proposition 4.3.1 corresponding to $\delta/16$. Since $|X| > \delta n^2 > (\delta/16)|L|^2$, by Proposition 4.3.1 the graph G contains a triangle T distinct from all T_v, $v \in X$. The lines in T must intersect in three distinct points, which form an equilateral right-angle triangle in X. $\square$

From this we get Roth's theorem.

Proof of Theorem 4.0.1. For $A \subset [n]$ we consider the set $X \subset [n] \times [n]$ defined by

$$(a, b) \in X \iff a + 2b \in A.$$

Hence (the worst case is when $A = [|A|]$)

$$|X| \geq \sum_{k=1}^{|A|} (\lceil k/2 \rceil - 1) \geq \frac{|A|(|A|+1)}{4} - |A| \geq \frac{|A|^2}{5} \ \text{ if } \ |A| \geq 15.$$

For given $\delta > 0$, we assume that $|A| > \delta n$ and $n > n_0$ where n_0 is larger than $15/\delta$ and the bound of Corollary 4.3.2 corresponding to $\delta^2/5$. Since the set of pairs X satisfies $|X| \geq |A|^2/5 > (\delta^2/5)n^2$, by Corollary 4.3.2 it contains pairs (a, b), $(a + d, b)$, and $(a, b + d)$ with $d \neq 0$. Hence A contains the arithmetic progression $a + 2b$, $a + 2b + d$, $a + 2b + 2d$. $\square$

4.4 The triangle removal lemma

We prove Proposition 4.3.1 in the following stronger form.

Proposition 4.4.1 *For every $\delta > 0$ there exist a $\kappa > 0$ and an $n_0 \in \mathbb{N}$ such that if $n > n_0$ and G is a graph on n vertices containing more than δn^2 edge-disjoint triangles, then G contains more than κn^3 triangles.*

Thus $\gg n^2$ edge-disjoint triangles in G force many more, $\gg n^3$, new triangles. An equivalent formulation is the *triangle removal lemma*: For $n \to \infty$, if a graph $G = G_n$ on n vertices has only $o(n^3)$ triangles, then all of them can be removed by deleting only $o(n^2)$ edges from G. Indeed, if S is the largest set of edge-disjoint triangles in G, then every triangle in G shares an edge with a triangle in S and $|S| = o(n^2)$ (by Proposition 4.4.1). By deleting the $3|S| = o(n^2)$ edges of the triangles in S, we destroy all triangles in G. Yet more briefly: If a graph contains few triangles, then it can be well approximated by a triangle-free graph.

In order to prove Proposition 4.4.1, we introduce a special kind of homogeneous graphs, ε-regular pairs, and prove that every tripartite graph such that each two parts form an ε-regular pair contains many triangles (*counting lemma*). Then we state the *regularity lemma* and prove by means of it and by means of the counting lemma Proposition 4.4.1. The proof of the regularity lemma follows in the next section.

Let $G = (V, E)$ be a graph. For two disjoint and nonempty sets $X, Y \subset V$ we denote by $e(X, Y)$ the number of edges in G joining X and Y, and by $d(X, Y)$ the density of these edges:

$$d(X, Y) = \frac{e(X, Y)}{|X| \cdot |Y|}.$$

For $\varepsilon \in (0,1)$ we call (X,Y) an *ε-regular pair* if for every two subsets $X_1 \subset X$ and $Y_1 \subset Y$ satisfying $|X_1| \geq \varepsilon|X|$ and $|Y_1| \geq \varepsilon|Y|$,

$$|d(X_1,Y_1) - d(X,Y)| < \varepsilon.$$

Note that every pair (X,Y) with $|X| = |Y| = 1$ is ε-regular for any $\varepsilon > 0$. Also, if $\varepsilon' \geq \varepsilon > 0$ then ε-regularity implies ε'-regularity. For $x \in X$ we denote

$$\Gamma_Y(x) = \{y \in Y \mid \{x,y\} \in E\},$$

the set of neighbors of x in Y. Clearly, $|\Gamma_Y(x)| = e(\{x\},Y)$.

Lemma 4.4.2 *Let (X,Y) be an ε-regular pair in a graph $G = (V,E)$ with edge density $d = d(X,Y)$ and let $X_1 \subset X$ and $Y_1 \subset Y$ be subsets satisfying $|X_1| \geq \varepsilon|X|$ and $|Y_1| \geq \varepsilon|Y|$. Then there exists a vertex $x \in X_1$ such that*

$$|\Gamma_{Y_1}(x)| > (d-\varepsilon)|Y_1|.$$

The same holds for the inequality $< (d+\varepsilon)|Y_1|$.

Proof. If this were not true, then $|\Gamma_{Y_1}(x)| \leq (d-\varepsilon)|Y_1|$ for every $x \in X_1$. It would follow that

$$e(X_1,Y_1) = \sum_{x \in X_1} |\Gamma_{Y_1}(x)| \leq (d-\varepsilon)|X_1| \cdot |Y_1|$$

and $d(X_1,Y_1) \leq d-\varepsilon$, contradicting the regularity of the pair (X,Y). The proof for the other inequality is similar. □

Lemma 4.4.3 *If $\varepsilon > 0$ and $G = (U \cup V \cup W, E)$ is a tripartite graph (edges go only between the disjoint sets U and V, U and W, and V and W) in which all three pairs (U,V), (U,W) and (V,W) ε-regular, then, denoting the edge densities by $\kappa = d(U,V)$, $\lambda = d(U,W)$ and $\mu = d(V,W)$,*

$$\#\textit{triangles in } G > (\kappa\lambda\mu - 5\varepsilon - 7\varepsilon^3)|U| \cdot |V| \cdot |W|.$$

Proof. The inequality holds trivially if one of the densities is smaller than 2ε (then $\kappa\lambda\mu - 5\varepsilon - \varepsilon^3 < 2\varepsilon - 5\varepsilon - 7\varepsilon^3 < 0$). We therefore assume that $\kappa, \lambda, \mu \geq 2\varepsilon$. Let

$U_1 = \{u \in U \mid |\Gamma_V(u)| \leq (\kappa-\varepsilon)|V|\}$, $U_2 = \{u \in U \mid |\Gamma_W(u)| \leq (\kappa-\varepsilon)|W|\}$.

By Lemma 4.4.2, $|U_1|, |U_2| < \varepsilon|U|$. Thus the set $U_0 = U \backslash (U_1 \cup U_2)$ satisfies $|U_0| \geq (1 - 2\varepsilon)|U|$ and if $u \in U_0$ then

$$|\Gamma_V(u)| > (\kappa - \varepsilon)|V| \quad \text{and} \quad |\Gamma_W(u)| > (\lambda - \varepsilon)|W|.$$

Because $\kappa - \varepsilon, \lambda - \varepsilon \geq \varepsilon$ and the pair (V, W) is ε-regular, for every $u \in U_0$ we have

$$e(\Gamma_V(u), \Gamma_W(u)) > (\mu - \varepsilon)|\Gamma_V(u)| \cdot |\Gamma_W(u)|.$$

This is a lower bound on the number of triangles with one vertex being u because every edge joining $\Gamma_V(u)$ and $\Gamma_W(u)$ forms together with u a triangle. Summing over U_0 we get the lower bound

$$\begin{aligned}
\#\text{triangles in } G \quad &> \quad \sum_{u \in U_0} e(\Gamma_V(u), \Gamma_W(u)) > (\mu - \varepsilon) \sum_{u \in U_0} |\Gamma_V(u)| \cdot |\Gamma_W(u)| \\
&> \quad (\mu - \varepsilon)|U_0| \cdot (\kappa - \varepsilon)|V| \cdot (\lambda - \varepsilon)|W| \\
&> \quad (1 - 2\varepsilon)(\kappa - \varepsilon)(\lambda - \varepsilon)(\mu - \varepsilon)|U| \cdot |V| \cdot |W| \\
&> \quad (\kappa\lambda\mu - 5\varepsilon - 7\varepsilon^3)|U| \cdot |V| \cdot |W|.
\end{aligned}$$

$\square$

The following decomposition of large graphs into ε-regular pairs, the regularity lemma of E. Szemerédi (1941), is one of the most important results in graph theory.

Theorem 4.4.4 (Szemerédi, 1975) *For every $\varepsilon \in (0, 1)$ and every $m \in \mathbb{N}$, there exists an $M \in \mathbb{N}$, $M \geq m$, such that the vertex set of every graph $G = (V, E)$ with $|V| = n \geq m$ vertices can be partitioned into r nonempty sets*

$$V = V_1 \,\dot{\cup}\, V_2 \,\dot{\cup}\, \ldots \,\dot{\cup}\, V_r$$

so that (i) $m \leq r \leq M$, (ii) the cardinalities $|V_i|$ differ among themselves at most by 1 (hence $\lfloor n/r \rfloor \leq |V_i| \leq \lceil n/r \rceil$), and (iii) all but at most $\varepsilon\binom{r}{2}$ pairs (V_i, V_j), $1 \leq i < j \leq r$, are ε-regular.

If $m \leq |V| \leq M$ the partition of V into singletons has the required properties. The theorem is interesting only for large graphs with $|V| > M$. We prove the theorem in the next section. For an equivalent formulation see Proposition 4.5.2.

Given a parameter $h > 0$ and a partition of V described in the regularity lemma, we say that an edge e in G is *h-good* (with respect to the partition), if e joins two parts V_i and V_j such that the pair (V_i, V_j) is ε-regular and $d(V_i, V_j) \geq h$. Remaining edges of G are called *h-bad*.

Lemma 4.4.5 *The number of h-bad edges does not exceed*

$$2(1/m + \varepsilon + h)n^2.$$

Proof. An edge e is h-bad if and only if it lies inside one part V_i or joins two distinct parts V_i and V_j such that the pair (V_i, V_j) is not ε-regular or has $d(V_i, V_j) < h$. Thus the number of h-bad edges is at most

$$r\binom{\lceil n/r\rceil}{2} + \varepsilon\binom{r}{2}\lceil n/r\rceil^2 + h\binom{r}{2}\lceil n/r\rceil^2.$$

From $n/r > M/M = 1$ we have $\lceil n/r\rceil \le 2n/r$. This and $r \ge m$ implies the stated bound. $\square$

Proof of Proposition 4.3.1. We prove that if $G = (V, E)$ is a graph on n vertices containing $> \delta n^2$ edge-disjoint triangles and n is big (depending on $\delta > 0$), then

$$\#\text{triangles in } G > \kappa n^3$$

for some constant $\kappa > 0$ depending only on δ.

Let $\delta > 0$ be given. We fix sufficiently small $\varepsilon > 0$ and sufficiently large $m \in \mathbb{N}$ such that

$$2(1/m + \varepsilon + (6\varepsilon + 7\varepsilon^3)^{1/3}) < \delta.$$

Let $M \in \mathbb{N}$ be the constant corresponding to these ε and m in Theorem 4.4.4 and let $G = (V, E)$ be any graph that has $n > 2M$ vertices and contains more than δn^2 edge-disjoint triangles. We consider the partition $V = V_1 \cup V_2 \cup \cdots \cup V_r$, $m \le r \le M$, ensured by the regularity lemma and delete from G all h-bad edges, where

$$h = (6\varepsilon + 7\varepsilon^3)^{1/3}.$$

By Lemma 4.4.5 and by the selection of ε and m, the resulting graph G' still contains at least one of the edge-disjoint triangles (their edge sets are disjoint and to get rid of all of them, we have to delete more than δn^2 edges). Since G' consists only of h-good edges, this implies that in the partition of G there are three parts V_i, V_j, and V_k, $1 \le i < j < k \le r$, such that all three pairs (V_i, V_j), (V_i, V_k), and (V_j, V_k) are ε-regular and their edge densities are $\ge h$. By Lemma 4.4.3 and by $\lfloor n/r\rfloor > n/2M$, in the tripartite graph H induced by G on $V_i \cup V_j \cup V_k$,

$$\begin{aligned}\#\text{triangles in } H &> (h^3 - 5\varepsilon - 7\varepsilon^3)|V_i| \cdot |V_j| \cdot |V_k| \\ &> \varepsilon\lfloor n/r\rfloor^3 \\ &> (\varepsilon/8M^3)n^3.\end{aligned}$$

Thus the proposition holds with $\kappa = \varepsilon/8M^3$. □

4.5 Proof of Szemerédi's regularity lemma

We prove Theorem 4.4.4. We start with estimates on change in regularity caused by perturbing parts in a pair; we prove only a restricted result sufficient for our purposes.

Proposition 4.5.1 *Let $G = (V, E)$ be a graph, (X_1, X_2) be an ε-regular pair in G and X_1', X_2' be two nonempty and disjoint subsets of V.*

1. *Let $b = \min(|X_1|, |X_2|) \geq 1$. If $X_i' = X_i$ or X_i' is obtained from X_i by deleting one vertex then (X_1', X_2') is an ε'-regular pair with*
$$\varepsilon' = 2\varepsilon + 4b^{-1}.$$
2. *Let $\delta \in (0, 1)$. If X_i' is obtained from X_i by adding at most $\delta|X_i|$ vertices then (X_1', X_2') is an ε'-regular pair with*
$$\varepsilon' = \varepsilon + 12\delta\varepsilon^{-1}.$$

Proof. 1. It is easy to see that

$$\big|\,|X_1'|\cdot|X_2'| - |X_1|\cdot|X_2|\,\big|,\ |e(X_1', X_2') - e(X_1, X_2)| < |X_1| + |X_2|.$$

From this and $e(X_1', X_2') \leq |X_1'| \cdot |X_2'|$ we deduce that

$$\begin{aligned}
&|d(X_1', X_2') - d(X_1, X_2)| = \left|\frac{e(X_1', X_2')}{|X_1'|\cdot|X_2'|} - \frac{e(X_1, X_2)}{|X_1|\cdot|X_2|}\right| \\
<\ & e(X_1', X_2')\left|\frac{1}{|X_1'|\cdot|X_2'|} - \frac{1}{|X_1|\cdot|X_2|}\right| + \frac{|X_1| + |X_2|}{|X_1|\cdot|X_2|} \\
\leq\ & \frac{\big|\,|X_1'|\cdot|X_2'| - |X_1|\cdot|X_2|\,\big|}{|X_1|\cdot|X_2|} + \frac{|X_1| + |X_2|}{|X_1|\cdot|X_2|} \\
<\ & 2\left(|X_1|^{-1} + |X_2|^{-1}\right) \leq 4b^{-1}.
\end{aligned}$$

For $i = 1, 2$ consider arbitrary sets $Y_i' \subset X_i'$ satisfying $|Y_i'| \geq 2\varepsilon|X_i'|$. We have $Y_i' \subset X_i$ and

$$\frac{|Y_i'|}{|X_i|} \geq \frac{|Y_i'|}{|X_i'| + 1} = \frac{|Y_i'|\cdot|X_i'|^{-1}}{1 + |X_i'|^{-1}} \geq \varepsilon.$$

Using the estimate on change in edge density and the ε-regularity of (X_1, X_2) we get

$$\begin{aligned}\left|d(X_1', X_2') - d(Y_1', Y_2')\right| &\leq \left|d(X_1', X_2') - d(X_1, X_2)\right| + \left|d(X_1, X_2) - d(Y_1', Y_2')\right| \\ &< 4b^{-1} + \varepsilon.\end{aligned}$$

Since ε' is larger than this and 2ε, (X_1', X_2') is an ε'-regular pair.

2. Now

$$\left|\,|X_1'| \cdot |X_2'| - |X_1| \cdot |X_2|\,\right|,\ |e(X_1', X_2') - e(X_1, X_2)| \leq (2\delta + \delta^2)|X_1| \cdot |X_2|$$

and as in part 1 we get

$$|d(X_1', X_2') - d(X_1, X_2)| \leq 2(2\delta + \delta^2) \leq 6\delta.$$

This is independent of the ε-regularity of (X_1, X_2). For $i = 1, 2$ consider arbitrary sets $Y_i' \subset X_i'$ satisfying $|Y_i'| \geq (\varepsilon + \delta)|X_i'|$ and set $Y_i = Y_i' \cap X_i$. Then $Y_i \subset X_i$,

$$\frac{|Y_i|}{|X_i|} \geq \frac{|Y_i'| - \delta|X_i|}{|X_i|} \geq \frac{|Y_i'|}{|X_i'|} - \delta \geq \varepsilon$$

and $Y_i \subset Y_i'$, $|Y_i'|/|Y_i| \leq 1 + \delta|X_i|/|Y_i| \leq 1 + \delta\varepsilon^{-1}$. Using twice the estimate on change in edge density and the ε-regularity of (X_1, X_2) we see that $|d(X_1', X_2') - d(Y_1', Y_2')|$ is at most

$$\begin{aligned}&|d(X_1', X_2') - d(X_1, X_2)| + |d(X_1, X_2) - d(Y_1, Y_2)| + |d(Y_1, Y_2) - d(Y_1', Y_2')| \\ &\qquad < 6\delta + \varepsilon + 6\delta\varepsilon^{-1} < \varepsilon + 12\delta\varepsilon^{-1}.\end{aligned}$$

Since ε' is at least this and $\varepsilon + \delta$, (X_1', X_2') is an ε'-regular pair. □

We will consider families of nonempty and disjoint subsets $X_1, X_2, \dots, X_r$ of a vertex set in a graph. For $\varepsilon \in (0, 1)$ and a graf $G = (V, E)$, we call such family of subsets of V *ε-regular* if all but at most $\varepsilon\binom{r}{2}$ pairs (X_i, X_j), $1 \leq i < j \leq r$, are ε-regular. We prove equivalence of two common formulations of the regularity lemma. The first only restates Theorem 4.4.4 but the proof uses the second formulation.

Proposition 4.5.2 *The following two assertions are equivalent.*

1. *For every $\varepsilon \in (0, 1)$ and every $m \in \mathbb{N}$, there exists an $M \in \mathbb{N}$, $M \geq m$, with the property that the vertex set of any graph $G = (V, E)$ with*

$|V| \geq m$ contains an ε-regular *family of subsets $X_1, X_2, \ldots, X_r$ such that*

$$m \leq r \leq M, \ \bigcup_{i=1}^{r} X_i = V \quad \text{and} \quad |X_1| \geq |X_2| \geq \cdots \geq |X_r| \geq |X_1| - 1.$$

2. *For every $\varepsilon \in (0,1)$ and every $m \in \mathbb{N}$, there exists an $M \in \mathbb{N}$, $M \geq m$, with the property that the vertex set of any graph $G = (V, E)$ with $|V| \geq m$ contains an* ε-regular *family of subsets $X_1, X_2, \ldots, X_r$ such that*

$$m \leq r \leq M, \ \left| V \backslash \bigcup_{i=1}^{r} X_i \right| < \varepsilon |V| \quad \text{and} \quad |X_1| = |X_2| = \cdots = |X_r|.$$

Proof. We know that 1 and 2 are trivially true if $|V| \leq M$; there is something to prove only for $|V| > M$ which we will assume.

We suppose that 1 holds and derive 2. Let $\varepsilon_2 \in (0,1)$ and $m_2 \in \mathbb{N}$ be given. Let M_1 be the value of M ensured by 1 for $\varepsilon_1 = \varepsilon_2/2$ and $m_1 = m_2$. We fix $M_2 \in \mathbb{N}$ so large that $M_2 \geq M_1$, $\varepsilon_1 + 4(\lfloor M_2/M_1 \rfloor)^{-1} < \varepsilon_2$ and $M_1/M_2 < \varepsilon_2$. Let $G = (V, E)$ be any graph with $|V| > M_2$. We take the ε_1-regular family $X_1, X_2, \ldots, X_r$ with properties stated in 1. Note that $\min |X_i| \geq \lfloor |V|/r \rfloor \geq \lfloor M_2/M_1 \rfloor$. We obtain the family $Y_1, Y_2, \ldots, Y_r$ by deleting one vertex from the X_i with $|X_i| > |X_r|$. Clearly, $m_2 = m_1 \leq r \leq M_1 \leq M_2$ and all Y_i have equal cardinality. By 1 of Proposition 4.5.1, $Y_1, Y_2, \ldots, Y_r$ is an ε'-regular family where $\varepsilon' = \varepsilon_1 + 4(\lfloor M_2/M_1 \rfloor)^{-1} < \varepsilon_2$. The number of vertices in V not covered by the Y_is is smaller than $r \leq M_1 < \varepsilon_2 |V|$. Therefore M_2 and $Y_1, Y_2, \ldots, Y_r$ have the properties required by 2 for ε_2 and m_2.

Conversely, we suppose that 2 holds and derive 1. Let $\varepsilon_1 \in (0,1)$ and $m_1 \in \mathbb{N}$ be given. Let M_2 be the value of M ensured by 2 for $\varepsilon_2 = \min(\frac{1}{2}, \varepsilon_1/7)$ and $m_2 = \max(m_1, 12\varepsilon_2^{-2})$. We fix $M_1 \in \mathbb{N}$ so that $M_1 \geq 2M_2$. Let $G = (V, E)$ be any graph with $|V| > M_1$. We take the ε_2-regular family $X_1, X_2, \ldots, X_r$ with properties stated in 2. Hence $|X_1| = \cdots = |X_r| = t$. To obtain the family $Y_1, Y_2, \ldots, Y_s$, we start with the X_is, partition $V \backslash X_1 \cup \cdots \cup X_r$ arbitrarily into $u \leq r$ sets Z_i with size t and a set R with less than t elements, and distribute the elements of R one by one to the sets $X_1, X_2, \ldots, X_r, Z_1, Z_2, \ldots, Z_u$ in this cyclic order. The resulting $s = r + u \leq 2r$ sets $Y_1, Y_2, \ldots, Y_s$ are disjoint, cover the whole V and $|Y_1| \geq |Y_2| \geq \cdots \geq |Y_s| \geq |Y_1| - 1$. For $1 \leq i \leq r$

is Y_i obtained from X_i by adding at most $t/s \leq t/r \leq t/m_2$ vertices. Also, $m_1 \leq m_2 \leq r \leq s = r + u \leq 2M_2 \leq M_1$. We consider the pairs (Y_i, Y_j), $1 \leq i < j \leq s$. If $j \leq r$ and (X_i, X_j) was an ε_2-regular pair, 2 of Proposition 4.5.1 for $\delta = 1/m_2$ tells us that (Y_i, Y_j) is ε'-regular with $\varepsilon' = \varepsilon_2 + 12/m_2\varepsilon_2 \leq 2\varepsilon_2$. The number of other pairs (Y_i, Y_j) is bounded by $\varepsilon_2\binom{r}{2} + ru + \binom{u}{2} \leq \binom{s}{2}(\varepsilon_2 + 5\varepsilon_2 + 2\varepsilon_2^2) \leq 7\varepsilon_2\binom{s}{2}$ because $r \leq s$ and $u < \varepsilon_2|V|/t \leq 2\varepsilon_2(1-\varepsilon_2)|V|/t < 2\varepsilon_2 r$. Thus $Y_1, Y_2, \ldots, Y_s$ is ε_1-regular as ε_1 is at least $7\varepsilon_2$ and $2\varepsilon_2$. Therefore M_1 and $Y_1, Y_2, \ldots, Y_s$ have the properties required by 1 for ε_1 and m_1. □

After these preparations we finally begin with the proof of Theorem 4.4.4 in the formulation of part 2 of the previous Proposition. For a family $P = \{X_1, X_2, \ldots, X_r\}$ of disjoint subsets of a vertex set V of a graph $G = (V, E)$ we define its *energy* $q(P)$ as

$$q(P) = \sum_{1 \leq i < j \leq r} \frac{e(X_i, X_j)^2}{|X_i| \cdot |X_j|} = \sum_{1 \leq i < j \leq r} d(X_i, X_j) e(X_i, X_j).$$

Clearly, $0 \leq q(P) \leq \binom{|V|}{2} < |V|^2$. By P^* we denote the completion of P to a partition of V obtained by adding vertices not covered by the X_is to P as singleton parts. Theorem 4.4.4 follows from the next Proposition.

Proposition 4.5.3 *Suppose that $G = (V, E)$ is a graph, $\varepsilon \in (0, \frac{1}{4})$ and $P = \{X_1, X_2, \ldots, X_r\}$ is a family of disjoint subsets of V with equal sizes that does not cover less than $\varepsilon|V|$ vertices of V and is not ε-regular. Then there is another family $Q = \{Y_1, Y_2, \ldots, Y_s\}$ of disjoint subsets of V with equal sizes such that*

$$r \leq s \leq r8^r, \quad \left|V \setminus \bigcup_{i=1}^{s} Y_i\right| < \left|V \setminus \bigcup_{i=1}^{r} X_i\right| + \frac{|V|}{2^r} \quad \textit{and} \quad q(Q^*) \geq q(P^*) + \frac{|V|^2\varepsilon^5}{8}.$$

Proof Theorem 4.4.4. We prove the claim in part 2 of Proposition 4.5.2. Let $\varepsilon \in (0, \frac{1}{4})$ and $m \in \mathbb{N}$ be given. We set $t = \lfloor 8/\varepsilon^5 \rfloor$, enlarge m so that $1/(m+1) < \varepsilon/2$ and $t/2^m < \varepsilon/2$, and fix $M \in \mathbb{N}$ so large that $M \geq (m+1)^2$ and $M \geq a_t$ where the numbers a_i are given by $a_1 = m$ and $a_{i+1} = a_i 8^{a_i}$. Now let $G = (V, E)$ be any graph with $|V| > M$ (for $m \leq |V| \leq M$ the claim holds trivially due to the partition of V into $|V|$ singletons). We partition V arbitrarily into m disjoint sets $X_1, X_2, \ldots, X_m$ of the same size $t = \lceil |V|/(m+1) \rceil$ and a residual set R with size $|V|/(m+1) - m \leq |V| - mt =$

$|R| \leq |V|/(m+1)$. Due to the selection of M this is possible and the X_i do not cover $< (\varepsilon/2)|V|$ of the vertices.

We start with the family $X_1, X_2, \ldots, X_m$ and apply repeatedly Proposition 4.5.3 — until ε-regularity is achieved, we keep replacing the old non-ε-regular family $X_1, X_2, \ldots, X_r$ with $r \geq m$ disjoint and equal sized subsets of V that do not cover $< \varepsilon|V|$ of the vertices by a new family $Y_1, Y_2, \ldots, Y_s$ of the same type but with $r \leq s \leq r8^r$ sets, energy larger by at least $|V|^2\varepsilon^5/8$ and proportion of uncovered vertices larger by at most $1/2^m$. By the selection of m, if the number of applications does not exceed t then proportion of uncovered vertices remains under ε and Proposition 4.5.3 may be used. Since energy cannot increase above $|V|^2$, it may increase by at least $|V|^2\varepsilon^5/8$ at most t times. Thus at the last after the t-th application of Proposition 4.5.3 we arrive at the desired ε-regular family of at least m and at most M equal sized disjoint subsets of V that do not cover less than $\varepsilon|V|$ of the vertices. In view of Proposition 4.5.2 this proves Theorem 4.4.4. $\square$

It remains to prove Proposition 4.5.3. For the proof we need a more general notion of energy of a family $P = \{X_1, X_2, \ldots, X_r\}$ of disjoint subsets of a vertex set V of a graph $G = (V, E)$. Suppose that in addition R is a partition of P given by the equivalence relation $\sim$. We define

$$q(P, R) = \sum_{X_i \not\sim X_j} \frac{e(X_i, X_j)^2}{|X_i| \cdot |X_j|}$$

—we omit from the sum of $q(P)$ the pairs of equivalent set. Clearly, $q(P) \geq q(P, R)$ for any R.

Now we prove that refining a family does not decrease its energy. More precisely, suppose that $P = \{X_1, X_2, \ldots, X_r\}$ and $Q = \{Y_1, Y_2, \ldots, Y_s\}$ are two families of disjoint subsets of a vertex set V of a graph $G = (V, E)$ such that Q refines P, which means that every X_j is a union of several sets Y_i, and R is a partition of P into two blocks. R induces naturally a partition S of Q into two blocks. We show that

$$q(Q, S) \geq q(P, R).$$

In fact, it suffices to prove this only in the case when $r = 2$, $s = 3$, $X_1 = Y_1$, $X_2 = Y_2 \cup Y_3$ and R has blocks $\{X_1\}$ and $\{X_2\}$ (so S has blocks $\{Y_1\}$ and $\{Y_2, Y_3\}$). Indeed, P can be transformed into Q by a series of splits that divide one set into two and after each split the contribution to q from the affected pairs is a sum of elementary contributions of the described type. Thus it suffices to show that

$$\frac{e(Y_1,Y_2)^2}{|Y_1|\cdot|Y_2|}+\frac{e(Y_1,Y_3)^2}{|Y_1|\cdot|Y_3|}\geq\frac{e(X_1,X_2)^2}{|X_1|\cdot|X_2|}.$$

This is easy to verify remembering that $|X_1|=|Y_1|$, $|X_2|=|Y_2|+|Y_3|$ and $e(X_1,X_2)=e(Y_1,Y_2)+e(Y_1,Y_3)$; it is more or less the inequality $\alpha+\alpha^{-1}\geq 2$ for $\alpha>0$ in disguise.

Next we consider a non-ε-regular pair $P=(X,Y)$ in a graph $G=(V,E)$ and show that it can be refined into disjoint sets $Q=\{X_1,X_2,Y_1,Y_2\}$, $X=X_1\cup X_2$ and $Y=Y_1\cup Y_2$, so that, denoting S the partition of Q with blocks $\{X_1,X_2\}$ and $\{Y_1,Y_2\}$,

$$q(Q,S)\geq q(P)+\varepsilon^4|X|\cdot|Y|.$$

We expectedly select $X_1\subset X$ and $Y_1\subset Y$ so that $|X_1|\geq\varepsilon|X|$, $|Y_1|\geq\varepsilon|Y|$ and

$$\eta=d(X_1,Y_1)-d(X,Y)$$

satisfies $|\eta|\geq\varepsilon$, and set $X_2=X\backslash X_1$, $Y_2=Y\backslash Y_1$. We denote $x=|X|$, $y=|Y|$, $e=e(X,Y)$, $x_i=|X_i|$, $y_i=|Y_i|$ and $e_{ij}=e(X_i,Y_j)$. The Cauchy–Schwarz inequality with n-tuples $a_i\geq 0$ and $b_i>0$,

$$\left(\sum_{i=1}^n a_i\right)^2=\left(\sum_{i=1}^n(a_i/b_i^{1/2})\cdot b_i^{1/2}\right)^2\leq\sum_{i=1}^n a_i^2/b_i\cdot\sum_{i=1}^n b_i,$$

provides the inequality

$$\sum_{i=1}^n a_i^2/b_i\geq\frac{\left(\sum_{i=1}^n a_i\right)^2}{\sum_{i=1}^n b_i}.$$

With its help and using $\eta = e_{11}/x_1y_1 - e/xy$ we see that $q(Q,S)$ equals

$$\begin{aligned} & \frac{e_{11}^2}{x_1y_1} + \sum_{i+j>2} \frac{e_{ij}^2}{x_iy_j} \geq \frac{e_{11}^2}{x_1y_1} + \frac{(e-e_{11})^2}{xy - x_1y_1} \\ = \ & \frac{1}{x_1y_1}\left(\frac{x_1y_1e}{xy} + \eta x_1y_1\right)^2 + \frac{1}{xy-x_1y_1}\left(\frac{xy-x_1y_1}{xy}e - \eta x_1y_1\right)^2 \\ = \ & \frac{x_1y_1e^2}{x^2y^2} + \frac{2e\eta x_1y_1}{xy} + \eta^2 x_1y_1 + \frac{xy-x_1y_1}{x^2y^2}e^2 - \frac{2e\eta x_1y_1}{xy} + \frac{\eta^2 x_1^2y_1^2}{xy-x_1y_1} \\ \geq \ & \frac{e^2}{xy} + \eta^2 x_1y_1 \geq q(P) + \varepsilon^4 xy. \end{aligned}$$

Let $\varepsilon \in (0, \frac{1}{4})$ and $P = \{X_1, X_2, \ldots, X_r\}$ be a non-ε-regular family of disjoint sets with equal sizes in a graph $G = (V, E)$ with $|V \backslash (X_1 \cup \cdots \cup X_r)| < \varepsilon|V|$; hence $r \geq 2$. Let N be the set of at least $\varepsilon\binom{r}{2}$ non-ε-regular pairs in P. As we have just shown, for every $p = (X_i, X_j) \in N$, $1 \leq i < j \leq r$, there are partitions $A_{i,p}$ and $A_{j,p}$ of X_i and X_j, respectively, into two sets such that if we refine by them the parts of p, energy increases by $\geq \varepsilon^4|X_i| \cdot |X_j| \geq \varepsilon^4(3|V|/4r)^2 > \varepsilon^4|V|^2/2r^2$. Generally, for every two partitions A and B of the same set X there is a partition C of X that refines both of them and has at most $|A| \cdot |B|$ parts. Thus there exists a refinement $P_0 = \{X_1', X_2', \ldots, X_{r_0}'\}$ of P with the property that every X_i is in P_0 partitioned in at most 2^{r-1} sets X_j' so that this partition refines every partition $A_{i,p}$ for p running through N. This refinement defines a partition R of P_0 putting the X_j's partitioning the same X_i in one block, which naturally extends to a partition of P_0^*. It follows that $r \leq r_0 \leq r2^{r-1}$ and, using the monotonicity of energy to refinements, that

$$q(P_0^*) \geq q(P_0^*, R) \geq q(P^*) + \varepsilon\binom{r}{2}\varepsilon^4|V|^2/2r^2 \geq q(P^*) + \varepsilon^5|V|^2/8$$

because $\binom{r}{2} \geq r^2/4$ for $r \geq 2$. The family P_0 only lacks equal sizes of sets. If c is the common size of sets in P, we set

$$d = \lceil c/4^r \rceil \geq 1$$

and define the desired family $Q = \{Y_1, Y_2, \ldots, Y_s\}$ as the maximum family of disjoint subsets of V such that each Y_i has size d and is contained in some set X_j' of P_0. It follows that Q^* refines P_0^* and therefore

$$q(Q^*) \geq q(P_0^*) \geq q(P^*) + \varepsilon^5|V|^2/8.$$

Obviously, Q has all sets with equal size d. By the maximality of Q, from every X'_j only at most $d-1$ vertices are not used in any Y_i and therefore Y_i do not cover less than

$$\left|V \setminus \bigcup_{i=1}^{r} X_i\right| + (d-1)r_0 < \left|V \setminus \bigcup_{i=1}^{r} X_i\right| + (c/4^r)r2^{r-1} < \left|V \setminus \bigcup_{i=1}^{r} X_i\right| + |V|/2^r$$

vertices. As for the number of sets in Q, we have

$$r \leq s \leq r2^{r-1} \cdot 4^r < r8^r.$$

The lower bound follows from the fact that every X_j contains some Y_i because some $X'_t \subset X_j$ has size $\geq \lceil c/2^{r-1} \rceil \geq d$. The upper bound follows from the fact that at most $\lfloor c/d \rfloor \leq c/(c/4^r) = 4^r$ sets Y_i are contained in one X'_j. Thus Q has all required properties. This finishes the proof of Proposition 4.5.3 and of Szemerédi's regularity lemma.

4.6 Remarks

Roth's theorem on arithmetic progressions was proved in [39] (see also [40]). The analytic proof of Roth's theorem follows the expositions in Newman [34, Chapter 4] and Pollack [36, Chapter 6]. The combinatorial proof is taken from Gowers' exposition in [17]. The proof of Szemerédi's regularity lemma in formulation 2 of Proposition 4.5.2 is taken from Diestel [11, Chapter 7.4]

Bibliography

[1] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, Springer 2001.

[2] J. Avigad, K. Donnelly, D. Gray and P. Raff, A formally verified proof of the prime number theorem, *ACM Trans. Comput. Log.* **9** (2008) 23 pp.

[3] J. Avigad, Number theory and elementary arithmetic, *Philos. Math.* **11** (2003) 257–284.

[4] N. A. Baas and Ch. F. Skau, The lord of the numbers, Atle Selberg. On his life and mathematics, *Bull. Amer. Math. Soc.* **45** (2008) 617–649.

[5] J. Bak and D. J. Newman, *Complex Analysis*, Springer 1997.

[6] P. Bateman and M. E. Low, Prime numbers in arithmetic progressions with difference 24, *Amer. Math. Monthly* **72** (1965) 139–143.

[7] S. Bratus and I. Pak, Fast constructive recognition of a black box group isomorphic to S_n or A_n using Goldbach conjecture, *J. Symbol. Comput.* **29** (2000) 33–57.

[8] K. Chandrasekharan, *Einführung in die Analytische Zahlentheorie*, Lecture Notes in Mathematics 29, Springer, 1966.

[9] R. Chapman, Dirichlet's theorem, a real variable approach, manuscript, 2008, 20 pp., available at `http://secamlocal.ex.ac.uk/people/staff/rjchapma/rjc.html`.

[10] S. S. Demidov and B. V. Levshin (eds.), *The Affair of Academician N. N. Luzin*, RChGI, Sankt-Petersburg, 1999 (Russian).

[11] R. Diestel, *Graph Theory*, Springer, 2005 (3rd edition).

[12] G. Lejeune Dirichlet, Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält, *Abh. der Königlich Preuss. Akad. der Wiss.* (1837), 45–81.

[13] P. G. L. Dirichlet, There are infinitely many prime numbers in all arithmetic progressions with first term and difference coprime, ArXiv:0808.1408 (translated by R. Stephan). `http://arxiv.org/abs/0808.1408`

[14] J. Elstrodt, The life and work of Gustav Lejeune Dirichlet (1805–1859). Analytic number theory, 1–37, Clay Math. Proc., 7, Amer. Math. Soc., 2007.

[15] P. Erdős, review MR0046374 for Mathematical Reviews, 1952.

[16] A. O. Gelfond and Yu. V. Linnik, *Elementary Methods in Analytic Number Theory*, Fizmatgiz, Moscow, 1962 (Russian).

[17] T. Gowers, Quasirandomness, counting and regularity for 3-uniform hypergraphs, *Combin. Probab. Comput.* **15** (2006) 143–184.

[18] T. Gowers, Vinogradov's three-primes theorem, available at `http://www.dpmms.cam.ac.uk/~wtg10/`

[19] J. G. Hermoso, An elementary proof of Dirichlet's theorem on primes in arithmetic progression, manuscript, 2002, 30 pp., available at `http://math.arizona.edu/~savitt/teaching/nt/projects/`

[20] E. Hlawka, J. Schoißengaier and R. Taschner, *Geometric and Analytic Number Theory*, Springer, 1991.

[21] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer 1990.

[22] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, AMS 2004.

[23] P. Jorgensen, quotes, available at `http://www.cs.uiowa.edu/~jorgen/quotes.html`

[24] A. A. Karacuba, *Basic Analytic Number Theory*, Springer, 1988.

[25] M. Klazar, *Analytic and Combinatorial Number Theory II. Lecture Notes*, KAM-DIMATIA Series 2010-969, 2010.

[26] S. Lang, *Algebra*, Springer, 2002 (3rd edition).

[27] H. B. Mann, A proof of the fundamental theorem on the density of sums of sets of positive integers, *Ann. Math.* **43** (1942) 523–527.

[28] P. Monsky, Simplifying the proof of Dirichlet's theorem, *Amer. Math. Monthly* **100** (1993) 861–862.

[29] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge University Press, Cambridge, 2007.

[30] W. Narkiewicz, *The development of prime number theory. From Euclid to Hardy and Littlewood*, Springer, 2000.

[31] M. B. Nathanson, *Additive Number Theory: The Classical Bases*, Springer, 1996.

[32] M. B. Nathanson, *Elementary Methods in Number Theory*, Springer, 2000.

[33] D. J. Newman, Simple analytic proof of the prime number theorem, *Amer. Math. Monthly* **87** (1980) 693–696.

[34] D. J. Newman, *Analytic Number Theory*, Springer, Berlin, 1998.

[35] J. Pintz, Landau's problems on primes, 43 pp., available at `http://www.renyi.hu/~pintz/`

[36] P. Pollack, *Not Always Burried Deep. Selections from Analytic and Combinatorial Number Theory*, manuscript, 2004, 306 pp., available at `http://www.math.dartmouth.edu/~ppollack/notes.pdf`

[37] P. Pollack, *Not Always Burried Deep: A Second Course in Elementary Number Theory*, AMS, 2009.

[38] O. Ramaré, On Šnirel'man's constant, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* **22** (1995) 645–706.

[39] K. Roth, Sur quelques ensembles d'entiers, *C. R. Acad. Sci. Paris* **234** (1952) 388–390.

[40] K. F. Roth, On certain sets of integers, *J. London Math. Soc.* **28** (1953) 104–109.

[41] A. Selberg, On an elementary method in the theory of primes, *Norske Vid. Selsk., Trondhejm* **19** (1947) 64–67.

[42] A. Selberg, An elementary proof of Dirichlet's theorem about primes in arithmetic progression, *Ann. of Math.* **50** (1949) 287–304.

[43] J.-P. Serre, *A Course in Arithmetic*, Springer 1973.

[44] H. N. Shapiro, On primes in arithmetic progression (II), *Ann. of Math.* **52** (1950) 231–243.

[45] L. G. Shnirel'man, On additive properties of numbers, *Izv. Donskogo Politekh. Inst. v Novocherkasske* **14** (1930) 3–28. [in Russian]

[46] L. G. Schnirelmann, Über additive Eigenschaften von Zahlen, *Math. Ann.* **107** (1933) 649–690.

[47] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, Cambridge, U.K., 1997.

[48] V. S. Varadarajan, *Euler Through Time: A New Look at Old Themes*, AMS, 2006.

[49] I. M. Vinogradov, Representation of an odd number as the sum of three primes, *Doklady Akad. Nauk SSSR* **15** (1937) 291–294.

[50] D. Zagier, Newman's short proof of the prime number theorem, *Amer. Math. Monthly* **104** (1997) 705–708.