30 Lectures on The Theory of Numbers

Shane Chern

Dalhousie University

E-mail: chenxiaohang92@gmail.com
xh375529@dal.ca
Website: https://shanechern.github.io/

Lecture notes for *MATH 3070 – Theory of Numbers* at Dalhousie University.

Contents

1 Primes . . . 7

1.1 Divisibility . . . 7

1.2 Primes . . . 8

1.3 Infinitude of primes . . . 8

1.4 Fermat numbers and the second proof of the infinitude of primes . . . 9

1.5 Fundamental theorem of arithmetic . . . 10

1.6 Divergence of $\sum_p \frac{1}{p}$ and the third proof of the infinitude of primes . . . 10

1.7 Erdős's proof of the divergence of $\sum_p \frac{1}{p}$ . . . 12

2 Fundamental theorem of arithmetic . . . 13

2.1 Greatest common divisor and Euclidean algorithm . . . 13

2.2 Modular systems . . . 14

2.3 Proof of the fundamental theorem of arithmetic . . . 15

2.4 Least common multiple . . . 16

3 Linear congruences . . . 19

3.1 Congruences . . . 19

3.2 Residue classes . . . 20

3.3 Linear congruences . . . 21

3.4 Chinese remainder theorem . . . 22

4 Fermat–Euler Theorem . . . 25

4.1 Reduced residue systems . . . 25

4.2 Euler's totient function . . . 25

4.3 Fermat–Euler Theorem . . . 27

4.4 Binomial coefficients 28
4.5 Euler’s proof of the Fermat–Euler Theorem 30

5 Primitive roots 31
5.1 Powers of integers 31
5.2 Orders 33
5.3 Primitive roots 34
5.4 Lagrange’s polynomial congruence theorem 34
5.5 Existence of primitive roots 35

6 Quadratic residues 37
6.1 Quadratic residues 37
6.2 Wilson’s Theorem 39
6.3 Legendre symbol 39
6.4 When is -1 a quadratic residue modulo p? 41
6.5 Starters for sums of squares 41

7 Quadratic reciprocity 43
7.1 Gauss’s Lemma 43
7.2 When is 2 a quadratic residue modulo p? 44
7.3 Guass’s law of quadratic reciprocity 44
7.4 When is 3 a quadratic residue modulo p? 46
7.5 An upper bound for the least quadratic non-residue 47

8 Sums of squares 49
8.1 Primes as a sum of two squares 49
8.2 The method of infinite descent 50
8.3 Zagier’s magical involution 50
8.4 Fermat’s two-square theorem 52
8.5 Lagrange’s four-square theorem 52

9 Generating functions 55
9.1 Generating functions 55
9.2 Formal power series 55
9.3 Fibonacci numbers 57
9.4 Compositions 58

10 Integer partitions 61
10.1 Integer partitions 61

10.2 Generating function for partitions 61
10.3 “Odd partitions” vs “Distinct partitions” 63
10.4 Ferrers diagrams 63
10.5 Euler’s summations 64
10.6 Durfee squares 65

11 Basic q-series 67
11.1 q-Binomial series 67
11.2 Heine’s transformations 68
11.3 Jacobi’s triple product identity 70
11.4 Ramanujan’s theta function 71

12 Sums of squares (II) 73
12.1 Jacobi’s identity 73
12.2 Lambert series 74
12.3 Jacobi’s two-square formula 75
12.4 Jacobi’s four-square formula 76

13 Arithmetic functions 79
13.1 Arithmetic functions 79
13.2 Divisor functions 80
13.3 Möbius function 80
13.4 Euler’s totient function revisited 81
13.5 Mangoldt function 82

14 Möbius inversion formula 85
14.1 Möbius inversion formula 85
14.2 Multiplicative Möbius inversion formula 86
14.3 Dirichlet convolutions 87
14.4 Ramanujan’s sums 90

15 Averages of arithmetic functions 93
15.1 Asymptotic relations 93
15.2 Abel’s summation formula 94
15.3 Average order of $\sigma(n)$ 96
15.4 Average order of $\phi(n)$ 97
15.5 Dirichlet hyperbola method 97
15.6 Average order of $d(n)$ 98

16 Dirichlet series . . . 99
16.1 Dirichlet series . . . 99
16.2 Multiplication of Dirichlet series . . . 101
16.3 Dirichlet series for some arithmetic functions . . . 102
16.4 Euler products . . . 104

17 Dirichlet characters . . . 107
17.1 Dirichlet characters . . . 107
17.2 Construction of Dirichlet characters modulo prime powers . . . 108
17.3 Construction of Dirichlet characters modulo general integers . . . 110
17.4 Orthogonality relations for Dirichlet characters . . . 113

18 Dirichlet's Theorem . . . 115
18.1 Riemann zeta function . . . 115
18.2 Dirichlet L-functions . . . 116
18.3 Dirichlet's Theorem . . . 120

Bibliography . . . 123

1. Primes

1.1 Divisibility

Definition 1.1 Let a and b be integers. We say that

"*a divides b*" or "*b is divisible by a*"

if there exists an integer x such that

$$b = ax.$$

We usually write $a \mid b$ if a divides b. Otherwise, if a does not divide b, we write $a \nmid b$.

Example 1.1 Since $18 = 2 \times 9$, we have $2 \mid 18$; since $35 = 7 \times 5$, we have $7 \mid 35$. ■

Definition 1.2 If $a \mid b$, then a is called a *divisor* of b. In particular, a positive divisor of b which is different from b is called a *proper divisor*.

Theorem 1.1 Assume that all variables in this theorem are integers.

(i) $1 \mid a$, $a \mid a$ and $a \mid 0$;
(ii) If $a \mid b$, then $a \mid bc$;
(iii) If $a \mid b$ and $b \mid c$, then $a \mid c$;
(iv) If $a \mid b$, then $ac \mid bc$;
(v) If $a \mid b_i$ for $i = 1 \ldots, r$, then $a \mid (m_1 b_1 + \cdots + m_r b_r)$.

Proof. (i). Since $a = 1 \cdot a = a \cdot 1$, we have $1 \mid a$ and $a \mid a$; since $0 = a \cdot 0$, we have $a \mid 0$.

(ii). Note that $a \mid b$ implies that $b = ax$ for some integer x. Thus, $bc = (ax) \cdot c = a \cdot (cx)$, implying that $a \mid bc$.

(iii). Note that $a \mid b$ implies that $b = ax$ and that $b \mid c$ implies that $c = by$. Thus, $c = by = (ax) \cdot y = a \cdot (xy)$, implying that $a \mid c$.

(iv). Note that $a \mid b$ implies that $b = ax$. Thus, $bc = (ax) \cdot c = (ac) \cdot x$, implying that $ac \mid bc$.

(v). Note that $a \mid b_i$ implies that $b_i = ax_i$. Thus,

$$m_1 b_1 + \cdots + m_r b_r = \sum_{i=1}^{r} m_i \cdot (ax_i) = a \sum_{i=1}^{r} m_i x_i,$$

implying that $a \mid (m_1b_1 + \cdots + m_rb_r)$. ■

1.2 Primes

Definition 1.3 A positive integer p is a *prime* if

(i) $p \geq 2$;

(ii) p has no positive divisors other than 1 and p.

A positive integer *greater than* 1 that is not prime is a *composite*.

R 1 is neither prime nor composite.

Example 1.2 The sequence of primes starts with

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$$

The sequence of composites starts with

$$4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, \ldots$$

1.3 Infinitude of primes

Now, there is a natural question:

Question 1.1 Will the sequence of primes terminate at some place? Or is it infinite?

The first answer to this question was given over 2,000 years ago by the ancient Greek mathematician Euclid (c. 300 BCE).

Theorem 1.2 (Euclid). The number of primes is infinite.

Proof (of Euclid). Let $\{p_1, \ldots p_k\}$ be a finite set of primes. Consider

$$n = p_1p_2 \cdots p_k + 1.$$

Then $p \geq 3$. Note that n has a prime factor p. But p is not one of p_i's; otherwise, we have $p \mid p_1 \cdots p_k$ and since $p \mid n$, it follows that $p \mid (n - p_1 \cdots p_k)$. Thus, $p \mid 1$, leading to a contradiction.

Therefore, for any finite set of primes, we are always able to generate a new prime. In other words, a finite set of primes cannot cover all primes. ■

The idea of the above proof is very natural. In fact, one may modify it to establish other interesting results.

Theorem 1.3 The number of primes of the form $4s + 3$ is infinite.

Proof. Let $\{p_1, \ldots p_k\}$ be a finite set of primes. Consider

$$n = 4p_1p_2 \cdots p_k - 1.$$

Note that n is of the form $4s + 3$. We claim that n has at least one prime factor p of the form $4s + 3$. Otherwise, if all prime factors of n are of the form $4s + 1$, then so is their product, namely, n, leading to a contradiction. Further, the above p is not one of 2, p_1, ..., p_k by a similar argument to that for Theorem 1.2. Thus, we arrive at a new prime of the form $4s + 3$ from the set $\{p_1, \ldots p_k\}$, thereby implying the infinitude of primes of the form $4s + 3$. ■

Theorem 1.4 The number of primes of the form $6s+5$ is infinite.

Proof. Exercise. ■

R In general, let a and m be positive integers such that $1 \leq a \leq m$ and $(a,m) = 1$. Then number of primes of the form $ms+a$ is infinite. Furthermore, let $\pi_{a,m}(x)$ count the number of primes $\leq x$ that are of the form $ms+a$. For fixed m, let a_1 and a_2 be such that $1 \leq a_1, a_2 \leq m$ and $(a_1,m) = (a_2,m) = 1$. Then

$$\lim_{x\to\infty} \frac{\pi_{a_1,m}(x)}{\pi_{a_2,m}(x)} = 1.$$

This is known as *Dirichlet's theorem on primes in arithmetic progressions.*

1.4 Fermat numbers and the second proof of the infinitude of primes

Definition 1.4 *Fermat numbers* are those of the form $F_n = 2^{2^n}+1$ with $n = 0,1,2,\ldots$

The French mathematician Pierre de Fermat wrote to Marin Mersenne on December 25, 1640 that:

> If I can determine the basic reason why
>
> $$3,5,17,257,65537,\ldots,$$
>
> are prime numbers, I feel that I would find very interesting results, for I have already found marvelous things [along these lines] which I will tell you about later.

However, Fermat's conjecture that all F_n are primes is unfortunately proved incorrect as Euler discovered in 1732 that

$$F_5 = 4294967297 = 641 \times 6700417.$$

Furthermore, the known prime Fermat numbers, also known as *Fermat primes* are still the five numbers $F_0,\ldots,F_4$ examined by Fermat. As of 2014, it is known that F_n is composite for $5 \leq n \leq 32$. The largest Fermat number known to be composite is $F_{18233954}$, and its prime factor $7\times 2^{18233956}+1$ was discovered in October 2020. It is now conjectured that just the first 5 Fermat numbers are primes.

Theorem 1.5 For $n \geq 1$,

$$F_n - 2 = \prod_{i=0}^{n-1} F_i.$$

Proof. We prove this result by induction on n. First, it is true for $n=1$ since $F_1 - 2 = 3 = F_0$. Next, we assume that it is true for $n = k$ for some $k \geq 1$. Thus,

$$F_k - 2 = \prod_{i=0}^{k-1} F_i.$$

Now, we have

$$F_{k+1} - 2 = (2^{2^{k+1}}+1) - 2 = 2^{2^{k+1}} - 1 = (2^{2^k}+1)(2^{2^k}-1)$$

$$= F_k(F_k - 2) = F_k \cdot \prod_{i=0}^{k-1} F_i$$
$$= \prod_{i=0}^{k} F_i,$$

implying that the statement is also valid for $n = k+1$. ■

Corollary 1.6 Any two distinct Fermat numbers have no common divisor greater than 1.

Proof. Assume that a prime p divides both F_m and F_n with $0 \leq m < n$. Since $p \mid F_m$, we have $p \mid \prod_{i=0}^{n-1} F_i$. Now, $p \mid F_n$ implies that $p \mid \left(F_n - \prod_{i=0}^{n-1} F_i\right)$, and thus $p \mid 2$ by Theorem 1.5. Thus, $p = 2$. But this is impossible since all Fermat numbers are odd. ■

Now we are in a position to present the second proof of the infinitude of primes.

Second Proof of Theorem 1.2. Note that the sequence of Fermat numbers is infinite. We collect prime factors of these Fermat numbers, and by Corollary 1.6, they are pairwise distinct. Therefore, there are infinite primes. ■

1.5 Fundamental theorem of arithmetic

Theorem 1.7 Every integer $n \geq 2$ is a product of primes.

Proof. We prove by induction on n. First, 2 is a prime itself, and thus the statement is true for $n = 2$. Assume that the statement is true for $n = 2\ldots,k$ for some $k \geq 2$. Then if $n = k+1$ is prime, there is nothing to prove. If $n = k+1$ is composite, then we may write $k+1 = x \cdot y$ such that $1 < x, y < k+1$. By our assumption, both x and y are products of products, so is their product $xy = k+1$. Hence, the statement is also true for $n = k+1$. ■

Now, a natural question is *how many representations are there to factorize $n \geq 2$ as a product of primes?* This question is answered by the *Fundamental Theorem of Arithmetic*, also known as the *Unique Factorization Theorem*.

Fundamental Theorem of Arithmetic Every integer $n \geq 2$ has a unique (up to order of factors) representation as a product of primes.

This theorem, although intuitionistic, is far more than trivial. We will give its proof in the next lecture.

1.6 Divergence of $\sum_p \frac{1}{p}$ and the third proof of the infinitude of primes

Now, we have a straightforward consequence of the Fundamental Theorem of Arithmetic. Consider

$$\prod_{\substack{p \text{ prime} \\ p \leq n}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right).$$

If we expand the product, then for each i with all its prime factors at most n, we have that $\frac{1}{i}$ appears as exactly one of the terms. In particular, such i's include all integers $m \leq n$.

Therefore,

$$\prod_{\substack{p \text{ prime} \\ p \le n}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \geq \sum_{m=1}^{n} \frac{1}{m}.$$

Then,

$$\prod_{p \le n} \frac{1}{1 - \frac{1}{p}} = \prod_{p \le n} \sum_{k=0}^{\infty} \frac{1}{p^k} > \sum_{m=1}^{n} \frac{1}{m} > \int_1^n \frac{dt}{t} = \log n.$$

On the other hand,

$$\begin{aligned}
\log \prod_{p \le n} \frac{1}{1 - \frac{1}{p}} &= \sum_{p \le n} \log \frac{1}{1 - \frac{1}{p}} = \sum_{p \le n} \sum_{k=1}^{\infty} \frac{1}{k \cdot p^k} = \sum_{p \le n} \frac{1}{p} + \sum_{p \le n} \sum_{k=2}^{\infty} \frac{1}{k \cdot p^k} \\
&< \sum_{p \le n} \frac{1}{p} + \sum_{p \le n} \sum_{k=2}^{\infty} \frac{1}{2p^2 \cdot p^{k-2}} = \sum_{p \le n} \frac{1}{p} + \sum_{p \le n} \frac{1}{2p^2} \sum_{k=0}^{\infty} \frac{1}{\cdot p^k} \\
&= \sum_{p \le n} \frac{1}{p} + \sum_{p \le n} \frac{1}{2p^2} \frac{p}{p-1} \le \sum_{p \le n} \frac{1}{p} + \frac{1}{2} \sum_{m=2}^{n} \frac{1}{m(m-1)} \\
&< \sum_{p \le n} \frac{1}{p} + \frac{1}{2}.
\end{aligned}$$

Thus,

$$\sum_{p \le n} \frac{1}{p} + \frac{1}{2} > \log \prod_{p \le n} \frac{1}{1 - \frac{1}{p}} > \log \log n.$$

Theorem 1.8 We have

$$\sum_{\substack{p \text{ prime} \\ p \le n}} \frac{1}{p} > \log \log n - \frac{1}{2}. \tag{1.1}$$

In particular, $\sum_{p \text{ prime}} \frac{1}{p}$ diverges.

This result gives the third proof of the infinitude of primes.

Third Proof of Theorem 1.2. If there are finitely many primes, then $\sum_p \frac{1}{p}$ is also finite, which contradicts to the divergence of $\sum_p \frac{1}{p}$ established in Theorem 1.8. ■

R In fact, as $x \to \infty$,

$$\sum_{p \le x} \frac{1}{p} \sim \log \log x,$$

or more precisely,

$$\sum_{p \le x} \frac{1}{p} = \log \log x + B + o(1),$$

where B is a constant.

1.7 Erdős's proof of the divergence of $\sum_p \frac{1}{p}$

The previous proof of the divergence of $\sum_p \frac{1}{p}$ has, more or less, an analytic flavor. What will be provided here is an elegant elementrary attack due to the Hungarian mathematician Paul Erdős (*Mathematica, Zutphen. B.* **7** (1938), 1–2).

Theorem 1.9 The series $\sum_{p \text{ prime}} \frac{1}{p}$ diverges.

Proof. We prove by contradiction. That is, we assume that $\sum_p \frac{1}{p}$ converges. Let $\{p_1, p_2, \ldots\}$ be the sequence of primes in increasing order.

First, given an arbitrary positive integer n and an index K, we denote by $N_K(n)$ the number of positive integers $m \le n$ such that the prime factors of m are exclusively from $p_1, \ldots, p_K$. Note that by the Fundamental Theorem of Arithmetic, each integer a can be uniquely written as $a = s^2 \cdot t$ where t has no square factor greater than 1. Meanwhile, the squares no greater than n are 1^2, 2^2, ..., $\lfloor\sqrt{n}\rfloor^2$ where $\lfloor x \rfloor$ denotes the largest integer not exceeding a real x. Also, there are 2^K integers of the form $\prod_{i=1}^K p_i^{\varepsilon_i}$ with $\varepsilon_i \in \{0,1\}$. Now, if we write integers m counted by $N_K(n)$ as $m = s^2 \cdot t$, then s^2 comes from the above squares and t comes from the above $\prod_{i=1}^K p_i^{\varepsilon_i}$. Hence, $N_K(n) \le 2^K \sqrt{n}$.

On the other hand, the assumption of the convergence of $\sum_p \frac{1}{p}$ means that the index K may be choosen so that $\frac{1}{p_{K+1}} + \frac{1}{p_{K+2}} + \cdots < \frac{1}{2}$. Now, we observe that the number $N'_K(n)$ of integers $m' \le n$ with at least one prime factor among $p_{K+1}, p_{K+2}, \ldots$ is bounded by

$$N'_K(n) \le \frac{n}{p_{K+1}} + \frac{n}{p_{K+2}} + \cdots < \frac{n}{2}.$$

Noting that $N_K(n) + N'_K(n) = n$, we obtain that the following holds true for any positive integer n:

$$n < 2^K \sqrt{n} + \frac{n}{2}.$$

However, it fails when $n = 2^{2K+2}$, thereby giving a contradiction. Hence, $\sum_p \frac{1}{p}$ diverges. ■

2. Fundamental theorem of arithmetic

2.1 Greatest common divisor and Euclidean algorithm

Theorem 2.1 Given integers a and b, not both 0. There exists a unique positive integer d such that

(i) $d \mid a$ and $d \mid b$;

(ii) If $\delta \mid a$ and $\delta \mid b$, then $\delta \mid d$.

Definition 2.1 The number d in Theorem 2.1 is called the *greatest common divisor* of a and b, written as $d = \gcd(a,b) = (a,b)$.

R The gcd of a and b is the largest positive integer that is a divisor of both a and b.

Definition 2.2 If $(a,b) = 1$, we say that a and b are *relatively prime*, or *coprime*.

The proof of Theorem 2.1 is based on the so-called *Euclidean Algorithm*.

Proof (Euclidean Algorithm). Without loss of generality, we assume that $a \geq b > 0$. We also put $r_{-1} = a$ and $r_0 = b$. Now, we iteratively write

$$r_{-1} = q_1 r_0 + r_1, \qquad 0 < r_1 < r_0; \tag{2.1a}$$

$$r_0 = q_2 r_1 + r_2, \qquad 0 < r_2 < r_1; \tag{2.1b}$$

$$r_1 = q_3 r_2 + r_3, \qquad 0 < r_3 < r_2; \tag{2.1c}$$

$$\cdots$$

$$r_{k-2} = q_k r_{k-1} + r_k, \qquad 0 < r_k < r_{k-1}; \tag{2.1d}$$

$$r_{k-1} = q_{k+1} r_k + 0. \tag{2.1e}$$

We claim that $d = r_k > 0$.

(i). By (2.1e), we have $r_k \mid r_{k-1}$. Then by (2.1d), $r_k \mid r_{k-2}$. Continuing this process, we have $r_k \mid r_0 = b$ and $r_k \mid r_{-1} = a$.

(ii). If $\delta \mid a = r_{-1}$ and $\delta \mid b = r_0$, we know from (2.1a) that $\delta \mid r_1$, and then by (2.1b), $\delta \mid r_2$. Continuing this process, we have $\delta \mid r_k = d$. ■

We may use the Euclidean algorithm to calculate the gcd.

■ **Example 2.1** *Find* $(1071,462)$:

$$\begin{aligned} 1071 &= 2\times 462+147;\\ 462 &= 3\times 147+\mathbf{21};\\ 147 &= 7\times 21+0. \end{aligned}$$

Thus, $(1071,462)=21$. ■

Definition 2.3 The greatest common divisor of $n_1,\ldots,n_k$ is the largest positive integer that divides all of $n_1,\ldots,n_k$.

2.2 Modular systems

Definition 2.4 A *modular system* S is a subset of integers such that

(i) If $n\in S$, then $-n\in S$;
(ii) If $m,n\in S$, then $m+n\in S$.

R Modular systems are instances of additive groups under the "+" operation.

■ **Example 2.2** The set of integers $\{\ldots,-2,-1,0,1,2,\ldots\}$ is a modular system. The set of multiples of 3, namely, $\{\ldots,-6,-3,0,3,6,\ldots\}$, is also a modular system. Further, the set $\{0\}$ is also a modular system. ■

Theorem 2.2 Let S be a modular system such that $S\neq\emptyset$. Then

(i) $0\in S$;
(ii) If $n\in S$ and x is an integer, then $xn\in S$.

Proof. (i). Let $m\in S$ since S is non-empty. Then by definition, $-m\in S$. Finally, $0=m+(-m)\in S$.

(ii). Without loss of generality, we assume that x is a nonnegative integer. Otherwise, we write $xn=(-x)(-n)$. Note that the statement is true for $x=0$ by Part (i). Assume that it is true for $x=0,\ldots,k$ for some $k\geq 0$, i.e., $xn\in S$ for $x=0,\ldots,k$. Then for $x=k+1$, we have $(k+1)n=n+kn\in S$ since both n and kn are in S. The statement then follows by induction. ■

Theorem 2.3 Let a and b be integers. Then $S=\{ax+by : x,y\in\mathbb{Z}\}$ is a modular system.

Proof. (i). Given any $n\in S$, it is of the form $n=ax+by$ for some integers x and y. Now, $-n=-(ax+by)=a\cdot(-x)+b\cdot(-y)\in S$.

(ii). Given any $m,n\in S$, then they are of the form $m=ax_1+by_1$ and $n=ax_2+by_2$. Now, $m+n=a(x_1+x_2)+b(y_1+y_2)\in S$. ■

Theorem 2.4 Let S be a modular system such that S is neither $\emptyset$ nor $\{0\}$. Let δ be the smallest positive integer in S. Then $S=\{k\delta : k\in\mathbb{Z}\}$.

Proof. We first note that $k\delta\in S$ for all integers k by Theorem 2.2(ii). Now assume that there exists an integer $n\in S$ such that n is not a multiple of δ. Then we may write

$$n=q\cdot\delta+r,\qquad 0<r<\delta.$$

This implies that $r=n-q\delta\in S$. But it contradicts to the assumption that δ is the smallest positive integer in S. ■

Theorem 2.5 Let a and b be integers, not both 0. Let $d = (a,b)$. Then

$$\{ax+by : x,y \in \mathbb{Z}\} = \{kd : k \in \mathbb{Z}\}.$$

In other words, an integer n can be written as

$$n = ax+by, \qquad x,y \in \mathbb{Z}$$

if and only if n is a multiple of (a,b).

Proof. We write

$$S_1 = \{ax+by : x,y \in \mathbb{Z}\},$$
$$S_2 = \{kd : k \in \mathbb{Z}\}.$$

(i). Show $S_1 \subset S_2$. That is, if $n = ax+by$, then $n \in S_2$. This is obvious since both a and b are multiples of $d = (a,b)$, so is $ax+by$.

(ii). Show $S_2 \subset S_1$. That is, there exist integers x and y such that $kd = ax+by$ for any $k \in \mathbb{Z}$. Note that it suffices to prove the case $k = 1$, i.e., $d = ax+by$ or $d \in S_1$. We will require the process in the Euclidean algorithm. Note that S_1 is a modular system by Theorem 2.3 and $a,b \in S_1$. By (2.1a), $r_1 \in S_1$, and then by (2.1b), $r_2 \in S_1$. Continuing this process, we find that $d = r_k \in S_1$, as desired.

We conclude that $S_1 = S_2$ since they are subsets of one another. ■

2.3 Proof of the fundamental theorem of arithmetic

Theorem 2.6 If $a \mid bc$ and $(a,b) = 1$, then $a \mid c$.

Proof. By Theorem 2.5, we may find integers x and y such that $1 = ax+by$. Now,

$$c = c \cdot 1 = c \cdot (ax+by) = a \cdot (cx) + (bc) \cdot y.$$

Since bc is a multiple of a, we have $a \mid c$. ■

Corollary 2.7 If a prime $p \mid p_1 p_2 \cdots p_k$ with $p_1, \ldots, p_k$ primes, then $p = p_j$ for at least one j.

Proof. Since $p \mid p_1(p_2 \cdots p_k)$, we have either $p \mid p_1$, which implies $p = p_1$, or $p \mid p_2 \cdots p_k$ by Theorem 2.6 since $(p, p_1) = 1$ for $p \neq p_1$. Now, we repeat the process for the latter case. ■

Now, we are in a position to prove the Fundamental Theorem of Arithmetic.

Theorem 2.8 (Fundamental Theorem of Arithmetic). Every integer $n \geq 2$ has a unique (up to order of factors) representation as a product of primes.

Proof. In Theorem 1.7, we have shown that every integer $n \geq 2$ is a product of primes. It suffices to establish the uniqueness. Assume that n has prime factorizations

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell.$$

Then $p_1 \mid q_1q_2\cdots q_\ell$, and thus by renumbering the q's, we have $p_1 = q_1$ by Corollary 2.7. Dividing by p_1 on both sides, we have

$$p_2\cdots p_k = q_2\cdots q_\ell.$$

Repeating this process gives the desired result. ■

R We often write a (positive) integer n in its *canonical form*

$$n = \prod_{j=1}^{k} p_j^{\alpha_j}$$

with p_j its distinct prime factors and $\alpha_j > 0$.

Theorem 2.9 If

$$a = \prod_{j=1}^{r} p_j^{\alpha_j} \qquad \text{and} \qquad b = \prod_{j=1}^{r} p_j^{\beta_j},$$

where p_j's are distinct prime factors of either a or b and $\alpha_j, \beta_j \geq 0$, then

$$(a,b) = \prod_{j=1}^{r} p_j^{\min(\alpha_j,\beta_j)}.$$

Proof. We write

$$(a,b) = \prod_{j=1}^{r} p_j^{\delta_j}.$$

Then $\delta_j \leq \alpha_j$ and $\delta_j \leq \beta_j$ but δ_j is not smaller than both of α_j and β_j. ■

2.4 Least common multiple

Definition 2.5 Let a and b be integers with $a, b \neq 0$. Then the *least common multiple* of a and b is the positive integer m such that

(i) $a \mid m$ and $b \mid m$;

(ii) If $a \mid \mu$ and $b \mid \mu$, then $m \mid \mu$.

We write $m = \operatorname{lcm}(a,b) = [a,b]$.

R The lcm of a and b is the smallest positive integer that is a multiple of both a and b.

Definition 2.6 The least common multiple of $n_1, \ldots, n_k$ is the smallest positive integer that is divisible by all of $n_1, \ldots, n_k$.

Theorem 2.10 If

$$a = \prod_{j=1}^{r} p_j^{\alpha_j} \qquad \text{and} \qquad b = \prod_{j=1}^{r} p_j^{\beta_j},$$

where p_j's are distinct prime factors of either a or b and $\alpha_j,]beta_j \geq 0$, then

$$[a,b] = \prod_{j=1}^{r} p_j^{\max(\alpha_j,\beta_j)}.$$

Proof. This is a direct consequence of the definition of lcm. ■

Theorem 2.11 Let a and b be positive integers. Then

$$[a,b] = \frac{ab}{(a,b)}.$$

Proof. Note that if we write $a = \prod_{j=1}^{r} p_j^{\alpha_j}$ and $b = \prod_{j=1}^{r} p_j^{\beta_j}$, then

$$\begin{aligned}
[a,b]\cdot(a,b) &= \prod_{j=1}^{r} p_j^{\max(\alpha_j,\beta_j)} \cdot \prod_{j=1}^{r} p_j^{\min(\alpha_j,\beta_j)} \\
&= \prod_{j=1}^{r} p_j^{\max(\alpha_j,\beta_j)+\min(\alpha_j,\beta_j)} \\
&= \prod_{j=1}^{r} p_j^{\alpha_j+\beta_j} \\
&= \prod_{j=1}^{r} p_j^{\alpha_j} \cdot \prod_{j=1}^{r} p_j^{\beta_j} \\
&= ab,
\end{aligned}$$

where we make use of the fact that $\max(\alpha,\beta)+\min(\alpha,\beta) = \alpha+\beta$. ■

3. Linear congruences

3.1 Congruences

Definition 3.1 Let m be a positive integer. Let a and b be integers. We say that a *is congruent to b modulo m* if

$$m \mid (a-b).$$

We write

$$a \equiv b \pmod{m}.$$

If $m \nmid (a-b)$, we write

$$a \not\equiv b \pmod{m}.$$

Theorem 3.1 Let m be a positive integer.

(i) $a \equiv a \pmod{m}$;
(ii) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$;
(iii) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Proof. (i). We have $a-a=0$ and $m \mid 0$.

(ii). Since $a \equiv b \pmod{m}$, we have $m \mid (a-b)$, and thus $m \mid -(a-b)=(b-a)$, thereby implying that $b \equiv a \pmod{m}$.

(iii). Since $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, we have $m \mid (a-b)$ and $m \mid (b-c)$, and thus $m \mid \big((a-b)+(b-c)\big)=(a-c)$, thereby implying that $a \equiv c \pmod{m}$. ■

R A relation "$\sim$" between the elements of a set M is an *equivalence* if

(i) $a \sim a$ (*reflexivity*);
(ii) If $a \sim b$, then $b \sim a$ (*symmetry*);
(iii) If $a \sim b$ and $b \sim c$, then $a \sim c$ (*transitivity*).

Congruence modulo a fixed m is an equivalence relation.

Theorem 3.2 We have

(i) $a \equiv b \pmod{m}$ if and only if $a-b \equiv 0 \pmod{m}$;

(ii) If $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, then

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m},$$
$$a_1 a_2 \equiv b_1 b_2 \pmod{m};$$

(iii) If $a \equiv b \pmod{m}$, then for any positive integer k,

$$a^k \equiv b^k \pmod{m};$$

(iv) If $f(x_1, x_2, \ldots)$ is a multivariate polynomial with integer coefficients, and $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, ..., then

$$f(a_1, a_2, \ldots) \equiv f(b_1, b_2, \ldots) \pmod{m}.$$

Proof. Exercise. ■

Theorem 3.3 If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, then

$$a \equiv b \pmod{[m,n]}.$$

R If $(m,n) = 1$, then by Theorem 2.11, we have $[m,n] = \frac{mn}{(m,n)} = mn$. Thus in this case $a \equiv b \pmod{mn}$.

Proof. Since $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, we have $m \mid (a-b)$ and $n \mid (a-b)$. Thus, $a - b$ is a common multiple of m and n, and thus a multiple of $[m,n]$. ■

Note that if $ka \equiv ka' \pmod{m}$, it is *not* always true that $a \equiv a' \pmod{m}$.

Example 3.1 We have $10 \times 1 \equiv 10 \times 4 \pmod{15}$, but $1 \not\equiv 4 \pmod{15}$. However, it is true that $1 \equiv 4 \pmod{3}$ where $3 = \frac{15}{(10,15)} = \frac{15}{5}$.

Theorem 3.4 If $(k,m) = d$, then $ka \equiv ka' \pmod{m}$ if and only if $a \equiv a' \pmod{\frac{m}{d}}$.

Proof. We write $k = k_1 d$ and $m = m_1 d$ so that $(k_1, m_1) = 1$. Thus,

$$\frac{ka - ka'}{m} = \frac{k(a-a')}{m} = \frac{k_1(a-a')}{m_1}.$$

Since $(k_1, m_1) = 1$, the left-hand side is an integer if and only if $m_1 \mid (a - a')$, namely, $a \equiv a' \pmod{m_1}$ while we also note that $m_1 = \frac{m}{d}$. ■

Now, we can determine in which case one may apply “division” to congruences.

Corollary 3.5 If $(k,m) = 1$, then $ka \equiv ka' \pmod{m}$ if and only if $a \equiv a' \pmod{m}$.

3.2 Residue classes

Definition 3.2 A set $\{a_1, a_2, \ldots, a_m\}$ is called a *complete residue system modulo* m, or a *complete system modulo* m, if

(i) $a_i \not\equiv a_j \pmod{m}$ for any $i \neq j$;
(ii) For any integer a, there exists an index i such that $a \equiv a_i \pmod{m}$.

Example 3.2 (i). $\{0,7,2,-3,-8,5\}$ is a complete system modulo 6; (ii). $\{0,1,2,\ldots,n-1\}$ is a complete system modulo n.

R Given a set of m integers, to verify whether it forms a complete system modulo m, it suffices to check if the m integers are pairwise distinct modulo m.

Theorem 3.6 Let $\{a_1,\ldots,a_m\}$ be a complete system modulo m and let k be an integer with $(k,m)=1$. Then $\{ka_1,\ldots,ka_m\}$ is also a complete system modulo m.

Proof. (i). Show $ka_i \not\equiv ka_j \pmod m$ for $i\neq j$. Otherwise, if $ka_i\equiv ka_j \pmod m$, then since $(k,m)=1$, we have $a_i\equiv a_j \pmod m$ by Corollary 3.5, yielding to a contradiction to the assumption that $\{a_1,\ldots,a_m\}$ is a complete system modulo m.

(ii). Show $a\equiv ka_i \pmod m$ for some i. Since $(k,m)=1$, we may find integers k' and m' such that $kk'+mm'=1$ by Theorem 2.5, and thus $kk'\equiv 1 \pmod m$. Choose i such that $a_i\equiv ak' \pmod m$. Then $ka_i\equiv k(ak')=a(kk')\equiv a \pmod m$. ∎

Theorem 3.7 Let m and m' be such that $(m,m')=1$. Suppose that a runs through a complete system modulo m and a' runs through a complete system modulo m'. Then $a'm+am'$ runs through a complete system modulo mm'.

Proof. There are mm' numbers $a'm+am'$. Thus, it suffices to verify that they are pairwise distinct modulo mm'. Note that if

$$a_1'm+a_1m'\equiv a_2'm+a_2m' \pmod{mm'},$$

then since $(m,m')=1$, it follows from Corollary 3.5 that

$$a_1m'\equiv a_2m' \pmod m \qquad\Rightarrow\qquad a_1\equiv a_2 \pmod m$$

and

$$a_1'm\equiv a_2'm \pmod{m'} \qquad\Rightarrow\qquad a_1'\equiv a_2' \pmod{m'}.$$

leading to the same choice of $a'm+am'$ as a runs through a complete system modulo m and a' runs through a complete system modulo m'. ∎

3.3 Linear congruences

Theorem 3.8 The linear congruence

$$ax\equiv b \pmod m \tag{3.1}$$

is solvable if and only if $(a,m)\mid b$. In this case, there is a unique solution modulo $\frac{m}{(a,m)}$.

Proof. The congruence $ax\equiv b \pmod m$ is equivalent to $b-ax=my$ for some y. That is

$$ax+my=b. \tag{3.2}$$

By Theorem 2.5, it has integer solutions (x,y) if and only if b is a multiple of (a,m).

For the second part, assume that (x_0,y_0) is a solution to (3.2). Then we parametrize its solutions as follows. First, note that

$$ax+my=b=ax_0+my_0.$$

Thus, $a(x-x_0) = m(y_0-y)$, or if we put $d=(a,m)$,

$$\frac{a}{d}(x-x_0) = \frac{m}{d}(y_0-y).$$

Since $(\frac{a}{d}, \frac{m}{d}) = 1$, we have that for $k \in \mathbb{Z}$,

$$\begin{cases} x - x_0 = k \cdot \frac{m}{d}, \\ y_0 - y = k \cdot \frac{a}{d}, \end{cases} \qquad \Rightarrow \qquad \begin{cases} x = x_0 + k \cdot \frac{m}{d}, \\ y = y_0 - k \cdot \frac{a}{d}. \end{cases}$$

Thus, modulo $\frac{m}{d}$, x has only one possibility. ■

Now, our question is how to construct an explicit expression of the solution to $ax \equiv b \pmod{m}$.

Definition 3.3 Let a and m be such that $(a,m)=1$. We say that $\bar{a}$ is a *modular inverse of a modulo m* if

$$a\bar{a} \equiv 1 \pmod{m}.$$

Theorem 3.9 Let a, b and m be such that $d \mid b$ where $d=(a,m)$. Then the solution to $ax \equiv b \pmod{m}$ is given by

$$x \equiv a' \cdot \frac{b}{d} \pmod{\frac{m}{d}},$$

where a' is the modular inverse of $\frac{a}{d}$ modulo $\frac{m}{d}$.

Proof. Note that we may rewrite $ax \equiv b \pmod{m}$ as

$$d \cdot \frac{a}{d} x \equiv d \cdot \frac{b}{d} \pmod{m},$$

which is equivalent to

$$\frac{a}{d} x \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

by Theorem 3.4 as $(d,m)=d$. Note also that $a' \cdot \frac{a}{d} \equiv 1 \pmod{\frac{m}{d}}$. Thus,

$$x \equiv a' \cdot \frac{b}{d} \pmod{\frac{m}{d}},$$

which is our desired result. ■

■ **Example 3.3** *Solve* $10x \equiv 15 \pmod{35}$: We have $d=(10,35)=5$. Also, $\frac{10}{5} \times 4 \equiv 1 \pmod{\frac{35}{5}}$. Thus, $x \equiv 4 \times \frac{15}{5} = 12 \pmod{\frac{35}{5}}$, that is $x \equiv 5 \pmod{7}$. ■

3.4 Chinese remainder theorem

We have seen that linear congruences are essentially equivalent to $x \equiv c \pmod{m}$.

Theorem 3.10 The system

$$x \equiv c_1 \pmod{m_1}, \tag{3.3a}$$
$$x \equiv c_2 \pmod{m_2}, \tag{3.3b}$$

has a solution if and only if $(m_1,m_2) \mid (c_2-c_1)$. The solution, if it exists, is unique modulo $[m_1,m_2]$.

Proof. From (3.3a), we may write $x = m_1 y + c_1$ for some indeterminate y. Substituting it into (3.3b), we have

$$m_1 y + c_1 \equiv c_2 \pmod{m_2},$$

or

$$m_1 y \equiv c_2 - c_1 \pmod{m_2}.$$

By Theorem 3.8, it is solvable if and only if $(m_1, m_2) \mid (c_2 - c_1)$. Further, the solution y is unique modulo $\frac{m_2}{(m_1,m_2)}$, and thus the solution x is unique modulo $m_1 \cdot \frac{m_2}{(m_1,m_2)} = [m_1, m_2]$ by Theorem 2.11. ■

Corollary 3.11 Let m_1 and m_2 be such that $(m_1, m_2) = 1$. Then the system in Theorem 3.10 is solvable, and its solution is unique modulo $m_1 m_2$.

In general, we may consider an analogous system with multiple linear congruences. Along this line, we have the *Chinese Remainder Theorem*, which first appears in the writings of Sun Tzu (孙武: 孙子兵法), an ancient Chinese philosopher who lived during the Eastern Zhou period, and was further developed by the Chinese mathematician Qin Jiushao (秦九韶).

Theorem 3.12 (Chinese Remainder Theorem). Let $m_1, \ldots, m_r$ be such that $(m_i, m_j) = 1$ for $i \neq j$. Then the system $x \equiv c_i \pmod{m_i}$ for $1 \leq i \leq r$ has a unique solution modulo $m_1 \cdots m_r$.

Proof. This result follows by an iterative application of Corollary 3.11. ■

4. Fermat–Euler Theorem

4.1 Reduced residue systems

Definition 4.1 A set $\{a_1, a_2, \ldots, a_h\}$ is called a *reduced residue system modulo m*, or a *reduced system modulo m*, if

(i) $a_i \not\equiv a_j \pmod{m}$ for any $i \neq j$;
(ii) $(a_i, m) = 1$ for $1 \leq i \leq h$;
(iii) For any integer a with $(a, m) = 1$, there exists an index i such that $a \equiv a_i \pmod{m}$.

Example 4.1 (i). $\{1, 5\}$ is a reduced system modulo 6; (ii). $\{1, 2, \ldots, p-1\}$ is a reduced system modulo p for p a prime. ▪

Theorem 4.1 Let $\{a_1, \ldots, a_h\}$ be a reduced system modulo m and let k be an integer with $(k, m) = 1$. Then $\{ka_1, \ldots, ka_h\}$ is also a reduced system modulo m.

Proof. This proof is similar to that for Theorem 3.6.

(i). The same as Part (i) in the proof of Theorem 3.6.

(ii). Show $(ka_i, m) = 1$ for $1 \leq i \leq h$. Since k and a_i have no common divisors > 1 with m, so does their product ka_i.

(iii). Show $a \equiv ka_i \pmod{m}$ for some i for any a with $(a, m) = 1$. Since $(k, m) = 1$, we may find an integer k' with $kk' \equiv 1 \pmod{m}$. Note that $(k', m) = 1$ for if d is a common divisor of k' and m, then $d \mid (kk' - mx) = 1$ where x is such that $kk' - 1 = mx$. Thus, $(ak', m) = 1$. Choose i such that $a_i \equiv ak' \pmod{m}$. Then $ka_i \equiv k(ak') = a(kk') \equiv a \pmod{m}$. ■

4.2 Euler's totient function

Note that a reduced system modulo m is a subset of a complete system modulo m. In particular, the size h of any reduced system modulo m equals the number of integers among $\{1, 2, \ldots, m\}$ that are coprime to m.

Definition 4.2 Let n be a positive integer. *Euler's totient function* $\phi(n)$ denotes the number of integers among $\{1, 2, \ldots, n\}$ that are coprime to n.

R The totient function was introduced by the Swiss mathematician Leonhard Euler (*Novi commentarii academiae scientiarum imperialis Petropolitanae* **8** (1763), 74–

104).

■ **Example 4.2** (i). $\phi(1)=1$ for 1 is the only integer in $\{1\}$ that is coprime to 1; (ii). $\phi(3)=2$ for 1 and 2 are the integers in $\{1,2,3\}$ that are coprime to 3; (iii). $\phi(6)=2$ for 1 and 5 are the integers in $\{1,2,3,4,5,6\}$ that are coprime to 6. ■

R We may replace $\{1,2,\dots,n\}$ in the definition of Euler's totient function by any complete system modulo n.

Theorem 4.2 Let p be a prime and k be a positive integer. Then

$$\phi(p^k)=p^k-p^{k-1}. \tag{4.1}$$

Proof. Recall that $\phi(p^k)$ equals the number of integers in $\{1,\dots,p^k\}$ that are coprime to p^k, or in other words, that are not divisible by p. Since there are p^{k-1} integers among $\{1,\dots,p^k\}$ that are multiples of p, namely, $p\cdot 1$, $p\cdot 2$, …, $p\cdot p^{k-1}$, we have $\phi(p^k)=p^k-p^{k-1}$. ■

How to determine $\phi(n)$ if n is not a prime power?

Theorem 4.3 Let m and n be such that $(m,n)=1$. Then

$$\phi(mn)=\phi(m)\phi(n). \tag{4.2}$$

Proof. We have shown in Theorem 3.7 that $\{bm+an : 1\le a\le m, 1\le b\le n\}$ is a complete system modulo mn. Thus, to compute $\phi(mn)$, it suffices to count the number of such $bm+an$ with $(bm+an,mn)=1$. Note that

$$\begin{aligned}(bm+an,mn)=1 \quad &\Leftrightarrow \quad (bm+an,m)=1 \ \ \&\ \ (bm+an,n)=1\\ &\Leftrightarrow \quad (an,m)=1 \qquad\quad \&\ \ (bm,n)=1\\ &\Leftrightarrow \quad (a,m)=1 \qquad\quad\ \ \&\ \ (b,n)=1.\end{aligned}$$

Thus, there are $\phi(m)$ possibilities of a and $\phi(n)$ possibilities of b, and therefore $\phi(m)\phi(n)$ possibilities of admissible $bm+an$. It follows that $\phi(mn)=\phi(m)\phi(n)$. ■

R Given a function $f:\mathbb{Z}\to\mathbb{C}$, we say that it is *multiplicative* if $f(1)=1$ and for any m and n with $(m,n)=1$,
$$f(mn)=f(m)f(n).$$

Corollary 4.4 For any integer $n\ge 2$,

$$\phi(n)=n\cdot\prod_{p\mid n}\left(1-\frac{1}{p}\right), \tag{4.3}$$

where the product runs over all prime divisors of n.

Proof. We write n in its canonical form $n=\prod_{i=1}^{r}p_i^{\alpha_i}$. Then by Theorem 4.3,

$$\phi(n)=\prod_{i=1}^{r}\phi(p_i^{\alpha_i}).$$

Further, making use of Theorem 4.2 gives

$$\prod_{i=1}^{r}\phi(p_i^{\alpha_i})=\prod_{i=1}^{r}(p_i^{\alpha_i}-p_i^{\alpha_i-1})=\prod_{i=1}^{r}p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right)=\prod_{i=1}^{r}p_i^{\alpha_i}\cdot\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)=n\cdot\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right),$$

implying the desired result. ■

Theorem 4.5 For $n\geq 1$,

$$\sum_{d|n}\phi(d)=n, \tag{4.4}$$

where the sum runs over all positive divisors of n.

Proof. The formula is trivial when $n=1$. For $n>1$, we write n in the canonical form $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$. Then all divisors of n are of the form $p_1^{\beta_1}\cdots p_r^{\beta_r}$ with $0\leq\beta_k\leq\alpha_k$ for all k. Thus,

$$\begin{aligned}\sum_{d|n}\phi(d)&=\sum_{\beta_1=0}^{\alpha_1}\cdots\sum_{\beta_r=0}^{\alpha_r}\phi(p_1^{\beta_1}\cdots p_r^{\beta_r})=\sum_{\beta_1=0}^{\alpha_1}\cdots\sum_{\beta_r=0}^{\alpha_r}\phi(p_1^{\beta_1})\cdots\phi(p_r^{\beta_r})\\&=\prod_{k=1}^{r}\left(\phi(1)+\phi(p_k)+\cdots+\phi(p_k^{\alpha_k})\right)\\&=\prod_{k=1}^{r}\left(1+(p_k-1)+(p_k^2-p_k)+\cdots+(p_k^{\alpha_k}-p_k^{\alpha_k-1})\right)\\&=\prod_{k=1}^{r}p_k^{\alpha_k}=n,\end{aligned}$$

as required. ■

R This relation can also be understood as follows. Consider the n fractions $\frac{1}{n}$, $\frac{2}{n}$, …, $\frac{n}{n}$. For each $\frac{k}{n}$, we can uniquely write it in the irreducible form $\frac{k}{n}=\frac{a}{d}$ with $(a,d)=1$. Note that $d\mid n$. Also, since $1\leq k\leq n$, we have $1\leq a\leq d$. Since there are exactly $\phi(d)$ such $\frac{a}{d}$, and they correspond to exactly $\phi(d)$ fractions among $\{\frac{k}{n}:1\leq k\leq n\}$, we have $n=\sum_{d|n}\phi(d)$.

4.3 Fermat–Euler Theorem

Theorem 4.6 (Fermat–Euler Theorem). If $(a,m)=1$, then

$$a^{\phi(m)}\equiv 1 \pmod{m}. \tag{4.5}$$

Proof. Let $\{x_1,\ldots,x_{\phi(m)}\}$ be a reduced system modulo m. Thus, $(x_i,m)=1$ for each i. Since $(a,m)=1$, we know from Theorem 4.1 that $\{ax_1,\ldots ax_{\phi(m)}\}$ is also a reduced system modulo m. Thus,

$$\prod_{i=1}^{\phi(m)}x_i\equiv\prod_{i=1}^{\phi(m)}(ax_i)=a^{\phi(m)}\prod_{i=1}^{\phi(m)}x_i \pmod{m}.$$

Since $(x_i,m)=1$ for each i, we have $(\prod_i x_i,m)=1$. Thus, by Corollary 3.5, $a^{\phi(m)}\equiv 1 \pmod{m}$. ■

The m equal to a prime p case is also known as *Fermat's Theorem.*

Corollary 4.7 (Fermat's Theorem). If p is a prime and $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}. \tag{4.6}$$

4.4 Binomial coefficients

Definition 4.3 For integers $m \geq n \geq 0$, the *binomial coefficients* are defined by

$$\binom{m}{n} = \frac{m!}{n!(m-n)!} = \frac{m(m-1)\cdots(m-n+1)}{n(n-1)\cdots 1}.$$

In particular, $\binom{m}{0} = 1$.

Theorem 4.8 (Pascal's identity). For integers $m \geq n > 0$,

$$\binom{m+1}{n} = \binom{m}{n} + \binom{m}{n-1}. \tag{4.7}$$

Proof. We have

$$\begin{aligned}\binom{m}{n} + \binom{m}{n-1} &= \frac{m!}{n!(m-n)!} + \frac{m!}{(n-1)!(m-n+1)!} \\ &= \frac{m!}{(n-1)!(m-n)!} \cdot \frac{1}{n} + \frac{m!}{(n-1)!(m-n)!} \cdot \frac{1}{m-n+1} \\ &= \frac{m!}{(n-1)!(m-n)!} \cdot \frac{m+1}{n(m-n+1)} \\ &= \frac{(m+1)!}{(n)!(m-n+1)!},\end{aligned}$$

which is exactly $\binom{m+1}{n}$. ■

Theorem 4.9 (Binomial Theorem). For $n \geq 1$,

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}. \tag{4.8}$$

Proof. We prove by induction on n. First, when $n = 1$, both sides of (4.8) are $x+y$. Assuming that (4.8) is true for some $n \geq 1$, we want to show that it is also true for $n+1$. Note that

$$\begin{aligned}(x+y)^{n+1} &= (x+y)(x+y)^n \\ &= (x+y)\left(\sum_{r=0}^{n}\binom{n}{r}x^r y^{n-r}\right) \\ &= \sum_{r=0}^{n}\binom{n}{r}x^{r+1}y^{n-r} + \sum_{r=0}^{n}\binom{n}{r}x^r y^{n-r+1} \\ &= \left(x^{n+1} + \sum_{r=0}^{n-1}\binom{n}{r}x^{r+1}y^{n-r}\right) + \left(y^{n+1} + \sum_{r=1}^{n}\binom{n}{r}x^r y^{n-r+1}\right) \\ &= \left(x^{n+1} + \sum_{r=1}^{n}\binom{n}{r-1}x^r y^{n-r+1}\right) + \left(y^{n+1} + \sum_{r=1}^{n}\binom{n}{r}x^r y^{n-r+1}\right)\end{aligned}$$

$$
\begin{aligned}
&= x^{n+1} + y^{n+1} + \sum_{r=1}^{n} \left(\binom{n}{r-1} + \binom{n}{r} \right) x^r y^{n-r+1} \\
&= x^{n+1} + y^{n+1} + \sum_{r=1}^{n} \binom{n+1}{r} x^r y^{n-r+1} \\
&= \sum_{r=0}^{n+1} \binom{n+1}{r} x^r y^{n-r+1},
\end{aligned}
$$

which is exactly the $n+1$ case of (4.8). ■

Corollary 4.10 The binomial coefficients $\binom{m}{n}$ are integers.

Theorem 4.11 Let p be a prime. Given any nonzero integer n, we denote by $\nu_p(n)$ the unique nonnegative integer k such that $p^k \mid n$ and $p^{k+1} \nmid n$, namely, $\nu_p(n)$ is the power of p in the canonical form of n. Let α be a positive integer. For $1 \le r \le p^\alpha$,

$$\nu_p\left(\binom{p^\alpha}{r}\right) = \alpha - \nu_p(r). \tag{4.9}$$

In particular, for any r with $1 \le r \le p-1$, we have $p \mid \binom{p}{r}$.

Proof. Recall that $\binom{p^\alpha}{r} = \frac{p^\alpha(p^\alpha-1)\cdots(p^\alpha-r+1)}{r(r-1)\cdots 1}$. For each s with $1 \le s \le r-1 < p^\alpha$, we observe the simple fact that $\nu_p(s) = \nu_p(p^\alpha - s)$. Hence, $\nu_p(\binom{p^\alpha}{r}) = \nu_p(p^\alpha) - \nu_p(r) = \alpha - \nu_p(r)$. ■

Theorem 4.11 has two important consequences.

Theorem 4.12 For $\alpha \ge 1$ and p prime, if

$$m \equiv 1 \pmod{p^\alpha},$$

then

$$m^p \equiv 1 \pmod{p^{\alpha+1}}.$$

Proof. We write $m = kp^\alpha + 1$ for a certain integer k. Then

$$m^p = (kp^\alpha + 1)^p = \sum_{r=0}^{p} \binom{p}{r} (kp^\alpha)^r = 1 + \sum_{r=1}^{p} \binom{p}{r} (kp^\alpha)^r.$$

Now, for $1 \le r \le p$, $\binom{p}{r} \cdot (p^\alpha)^r$ is always divisible by $p^{\alpha+1}$. ■

Theorem 4.13 For $k \ge 1$ and p prime,

$$(x_1 + x_2 + \cdots + x_k)^p \equiv x_1^p + x_2^p + \cdots x_k^p \pmod{p}. \tag{4.10}$$

Proof. We apply induction on k. The $k = 1$ case is trivial. Assume that the statement is true for some $k \ge 1$. Then we prove the $k+1$ case:

$$
\begin{aligned}
(x_1 + x_2 + \cdots + x_{k+1})^p &= \big(x_1 + (x_2 + \cdots + x_{k+1})\big)^p \\
&= \sum_{r=0}^{p} \binom{p}{r} x_1^r (x_2 + \cdots + x_{k+1})^{p-r} \\
&\equiv x_1^p + (x_2 + \cdots + x_{k+1})^p
\end{aligned}
$$

$$\equiv x_1^p + x_2^p + \cdots x_{k+1}^p \pmod{p},$$

by our inductive assumption. ■

4.5 Euler's proof of the Fermat–Euler Theorem

We first prove that for $\alpha \geq 1$ and p prime, if a is such that $(a,p) = 1$,

$$a^{\phi(p^\alpha)} \equiv 1 \pmod{p^\alpha}. \tag{4.11}$$

For its proof, we first choose $k = a$ in Theorem 4.13 and then put $x_1 = \cdots = x_a = 1$. Thus, $a^p \equiv a \pmod{p}$. Since $(a,p) = 1$, we have $a^{p-1} \equiv 1 \pmod{p}$. Now, by an iterative application of Theorem 4.12, we have $a^{(p-1)p} \equiv 1 \pmod{p^2}$, ..., and $a^{(p-1)p^{\alpha-1}} \equiv 1 \pmod{p^\alpha}$, which is exactly (4.11).

Now, for integers m, we write $m = \prod_i p_i^{\alpha_i}$. Assume that a is such that $(a,m) = 1$, and thus $(a,p_i) = 1$ for each i. We also write for convenience $m = p_i^{\alpha_i} m_i$. Since ϕ is multiplicative, $\phi(m) = \phi(p_i^{\alpha_i})\phi(m_i)$. Thus, by (4.11),

$$a^{\phi(m)} = \left(a^{\phi(p_i^{\alpha_i})}\right)^{\phi(m_i)} \equiv 1^{\phi(m_i)} = 1 \pmod{p_i^{\alpha_i}}.$$

That is, $a^{\phi(m)} - 1$ is a multiple of each $p_i^{\alpha_i}$, and thus a multiple of $m = \prod_i p_i^{\alpha_i}$. In other words,

$$a^{\phi(m)} \equiv 1 \pmod{m},$$

as desired.

5. Primitive roots

5.1 Powers of integers

Let m be a positive integer and a be an integer with $(a,m)=1$. Let $k \geq 0$ be a nonnegative integer.

(i) For nonnegative powers of a, we know that a^k is an integer, and hence we may directly determine the residue class of a^k modulo m.

(ii) For negative powers of a, we recall from Definition 3.3 that there exists an integer $\overline{a}$ such that $a\overline{a} \equiv 1 \pmod{m}$. Thus, we may use a^{-1} to represent the residue class of $\overline{a}$ modulo m. In particular, we have $aa^{-1} \equiv 1 \pmod{m}$, which is a natural analogy to the usual inverse of integers; this explains why we call a^{-1} the modular inverse of a in Definition 3.3. Now, we may naturally define negative powers of a modulo m by $a^{-k} \equiv (a^{-1})^k \pmod{m}$.

R Note that if a is such that $(a,m) > 1$, then there is no integer $\overline{a}$ such that $a\overline{a} \equiv 1 \pmod{m}$, since by Theorem 2.5, $ax - 1 = my$ has no integer solutions (x,y). Thus, we cannot define negative powers of a modulo m in this case. However, nonnegative powers of a can be defined as the normal powers.

From the above definition, we have the following trivial fact.

Theorem 5.1 Let m be a positive integer and a,b be integers with $(a,m)=(b,m)=1$ and $a \equiv b \pmod{m}$. Then for any integer x,

$$a^x \equiv b^x \pmod{m}. \tag{5.1}$$

The next two results show that integer powers in the modular sense have similar properties to normal powers of integers.

Theorem 5.2 Let m be a positive integer and a,b be integers with $(a,m)=(b,m)=1$. Then for any integer x,

$$(ab)^x \equiv a^x b^x \pmod{m}. \tag{5.2}$$

Proof. If $x \geq 0$, then $(ab)^x = a^x b^x$ as normal integer powers, and hence they are congruent modulo m. If $x<0$, we first note that $(ab)^{-1} \equiv a^{-1}b^{-1} \pmod{m}$ for

$$(ab)\cdot(a^{-1}b^{-1}) = (aa^{-1})\cdot(bb^{-1}) \equiv 1\cdot 1 = 1 \pmod{m}.$$

Thus,

$$(ab)^x \equiv \left((ab)^{-1}\right)^{-x} \equiv (a^{-1}b^{-1})^{-x} = (a^{-1})^{-x}(b^{-1})^{-x} \equiv a^x b^x \pmod{m},$$

as desired. $\blacksquare$

Theorem 5.3 Let m be a positive integer and a be an integer with $(a,m)=1$. Then
- (i) $1^{-1} \equiv 1 \pmod{m}$;
- (ii) $(a^{-1})^{-1} \equiv a \pmod{m}$;
- (iii) For any integers x and y, we have $a^{x+y} \equiv a^x a^y \pmod{m}$;
- (iv) For any integers x and y, we have $a^{xy} \equiv (a^x)^y \pmod{m}$.

Proof. (i). Note that $1\cdot 1 \equiv 1 \pmod{m}$, and hence $1^{-1} \equiv 1 \pmod{m}$.

(ii). Note that a^{-1} is the modular inverse of a modulo m and vice versa by definition. This means that $(a^{-1})^{-1} \equiv a \pmod{m}$.

(iii). This relation is trivial if x and y are simultaneously nonnegative, or simultaneously nonpositive. Without loss of generality, we assume that $x>0>y$. In particular, we may further assume that $x+y \geq 0$, for if $x+y<0$, we only need to rewrite the congruence as $(a^{-1})^{-(x+y)} \equiv (a^{-1})^{-x}(a^{-1})^{-y} \pmod{m}$. Now, we note that $a^x = a^{x+y-y} = a^{x+y}a^{-y}$ for both $x+y$ and $-y$ are nonnegative integers. Hence,

$$a^x \cdot a^y = (a^{x+y}a^{-y})\cdot a^y \equiv (a^{x+y}a^{-y})\cdot(a^{-1})^{-y} = a^{x+y}\cdot(a\cdot a^{-1})^{-y} \equiv a^{x+y}\cdot 1^{-y} = a^{x+y} \pmod{m}.$$

(iv). We require three basic facts. Firstly, for x and y nonnegative integers,

$$(a^x)^y = a^{xy}; \tag{5.3}$$

this is a property of normal integer powers. Secondly, for x a nonnegative integer,

$$(a^{-1})^x \equiv a^{-x} \pmod{m}; \tag{5.4}$$

this follows from the definition of negative powers in the modular sense. Thirdly, for x an integer,

$$(a^x)^{-1} = a^{-x}; \tag{5.5}$$

this follows from Part (iii) as $a^x a^{-x} \equiv a^{x+(-x)} = a^0 = 1 \pmod{m}$, namely, a^{-x} is the modular inverse of a^x. Now, we prove Part (iv) according to the following four cases. **(a).** If $x,y \geq 0$, then by (5.3) $a^{xy} = (a^x)^y$ and thus they are congruent modulo m. **(b).** If $x \geq 0 > y$, then

$$(a^x)^y \overset{(5.4)}{\equiv} \left((a^x)^{-1}\right)^{-y} \overset{(5.5)}{\equiv} (a^{-x})^{-y} \overset{(5.4)}{\equiv} \left((a^{-1})^x\right)^{-y} \overset{(5.3)}{=} (a^{-1})^{-xy} \overset{(5.4)}{\equiv} a^{xy} \pmod{m}.$$

(c). If $y \geq 0 > x$, then

$$(a^x)^y \overset{(5.4)}{\equiv} \left((a^{-1})^{-x}\right)^y \overset{(5.3)}{=} (a^{-1})^{-xy} \overset{(5.4)}{\equiv} a^{xy} \pmod{m}.$$

(d). If $x,y<0$, then

$$(a^x)^y \overset{(5.4)}{\equiv} \left((a^x)^{-1}\right)^{-y} \overset{(5.5)}{\equiv} (a^{-x})^{-y} \overset{(5.3)}{=} a^{xy} \pmod{m}.$$

The desired result hence holds true. $\blacksquare$

5.2 Orders

By the Fermat–Euler Theorem (Theorem 4.6), we have $a^{\phi(m)} \equiv 1 \pmod{m}$, indicating that there exists at least one positive integer x such that $a^x \equiv 1 \pmod{m}$.

Definition 5.1 Let m be a positive integer and a be an integer with $(a,m) = 1$. The smallest positive integer d such that

$$a^d \equiv 1 \pmod{m} \tag{5.6}$$

is called the *order of a modulo m*, denoted by $\operatorname{ord}_m a$.

■ **Example 5.1** (i). We have $\operatorname{ord}_5 2 = 4$ for $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$ and $2^4 \equiv 1 \pmod{5}$. (ii). We have $\operatorname{ord}_7 2 = 3$ for $2^1 \equiv 2$, $2^2 \equiv 4$ and $2^3 \equiv 1 \pmod{7}$. ■

Theorem 5.4 Let m be a positive integer and a be an integer with $(a,m) = 1$. Then an integer x satisfies $a^x \equiv 1 \pmod{m}$ if and only if $\operatorname{ord}_m a \mid x$. In particular, $\operatorname{ord}_m a \mid \phi(m)$.

Proof. Let $d = \operatorname{ord}_m a$. Then $a^d \equiv 1 \pmod{m}$ by definition. If $d \mid x$, then we may write $x = q \cdot d$ and thus,

$$a^x = a^{qd} \equiv (a^d)^q \equiv 1^q = 1 \pmod{m}.$$

Assume that there exists an x with $d \nmid x$ such that $a^x \equiv 1 \pmod{m}$. Thus, we may write $x = q \cdot d + r$ for q and r integers with $0 < r < d$. It follows that

$$1 \equiv a^x = a^{qd+r} \equiv a^{qd} \cdot a^r \equiv (a^d)^q \cdot a^r \equiv 1 \cdot a^r = a^r \pmod{m}.$$

But this violates the assumption that d is the smallest positive integer such that $a^d \equiv 1 \pmod{m}$. Finally, $\operatorname{ord}_m a \mid \phi(m)$ since $a^{\phi(m)} \equiv 1 \pmod{m}$ by the Fermat–Euler Theorem. ■

Theorem 5.5 Let m be a positive integer and a be an integer with $(a,m) = 1$. If we write $d = \operatorname{ord}_m a$, then for any integer k,

$$\operatorname{ord}_m a^k = \frac{d}{(d,k)}. \tag{5.7}$$

In particular, for any positive d^* with $d^* \mid d$, we have $\operatorname{ord}_m a^{\frac{d}{d^*}} = d^*$.

Proof. We write $d' = \operatorname{ord}_m a^k$ and $\delta = (d,k)$. First, noting that $(a^k)^{\frac{d}{\delta}} = (a^d)^{\frac{k}{\delta}} \equiv 1^{\frac{k}{\delta}} = 1 \pmod{m}$, we have $d' \mid \frac{d}{\delta}$ by Theorem 5.4. Also, $a^{kd'} = (a^k)^{d'} \equiv 1 \pmod{m}$, and therefore $d \mid kd'$ by Theorem 5.4, implying that $\frac{d}{\delta} \mid \frac{k}{\delta} d'$. Further, we have $(\frac{d}{\delta}, \frac{k}{\delta}) = 1$ since $\delta = (d,k)$. Hence, $\frac{d}{\delta} \mid d'$. It follows that $d' = \frac{d}{\delta}$. Finally, we choose $k = \frac{d}{d^*}$ and note that $(d, \frac{d}{d^*}) = \frac{d}{d^*}$, thereby getting the last part. ■

Theorem 5.6 Let m be a positive integer and a,b be integers with $(a,m) = (b,m) = 1$. Let $d_a = \operatorname{ord}_m a$ and $d_b = \operatorname{ord}_m b$. If $(d_a, d_b) = 1$, then $\operatorname{ord}_m(ab) = d_a d_b$.

Proof. Let $d = \operatorname{ord}_m(ab)$. First, noting that $(ab)^{d_a d_b} = (a^{d_a})^{d_b} \cdot (b^{d_b})^{d_a} \equiv 1^{d_b} \cdot 1^{d_a} = 1 \pmod{m}$, we have $d \mid d_a d_b$. Also, $a^{dd_b} = a^{dd_b} \cdot 1^d \equiv a^{dd_b} \cdot (b^{d_b})^d = (ab)^{dd_b} = \left((ab)^d\right)^{d_b} \equiv 1^{d_b} = 1 \pmod{m}$, and thus $d_a \mid dd_b$. Noting further that $(d_a, d_b) = 1$, we have $d_a \mid d$. Similarly, $d_b \mid d$ and thus $d_a d_b \mid d$ since $(d_a, d_b) = 1$. It follows that $d = d_a d_b$. ■

Theorem 5.7 Let m be a positive integer and $\{a_1, a_2, \ldots, a_{\phi(m)}\}$ be a reduced residue system modulo m. Let $d_i = \operatorname{ord}_m a_i$ for $1 \le i \le \phi(m)$ and define $D = \max_{1 \le i \le \phi(m)}\{d_i\}$. Then $D \mid \phi(m)$, and $d_i \mid D$ for each $1 \le i \le \phi(m)$.

Proof. First, $D \mid \phi(m)$ follows from Theorem 5.4 and the fact that D is the order of a certain a_i, say x. For the second part, we prove by contradiction. Assume that there exists a y such that $d = \operatorname{ord}_m y \nmid D$. If we write in the canonical form $d = \prod_i p_i^{\alpha_i}$ and $D = \prod_i p_i^{\beta_i}$, then there exists at least one index i such that $\alpha_i > \beta_i$ since $d \nmid D$. Then $\operatorname{lcm}(d,D) > D$ as $\operatorname{lcm}(d,D) = \prod_i p_i^{\max(\alpha_i,\beta_i)}$. Now, we define $d' = \prod_{k:\alpha_k > \beta_k} p_k^{\alpha_k}$ and $D' = \prod_{\ell:\beta_\ell \ge \alpha_\ell} p_\ell^{\beta_\ell}$. Then $d' \mid d$, $D' \mid D$, $(d', D') = 1$ and $d'D' = \operatorname{lcm}(d,D)$. By Theorem 5.5, there exists an a of order d' and a b of order D'. Thus, by Theorem 5.6, $\operatorname{ord}_m(ab) = d'D' = \operatorname{lcm}(d,D) > D$. But this violates the fact that D is the maximum among the orders. ■

5.3 Primitive roots

Recall that the orders modulo m are always divisors of $\phi(m)$. We now focus on the case where the order equals $\phi(m)$.

Definition 5.2 An integer g is called a *primitive root* of m if $\operatorname{ord}_m g = \phi(m)$.

Theorem 5.8 If m has a primitive root g, then $\{g, g^2, \ldots, g^{\phi(m)}\}$ gives a reduced residue system modulo m.

If m has a primitive root, then the multiplicative group $\mathbb{Z}_m^\times$ is cyclic.

Proof. Note that the $\phi(m)$ integers g, ..., $g^{\phi(m)}$ are coprime to m since $(g,m) = 1$. Hence, it suffices to show that they are pairwise distinct modulo m. Assume not; then there are integers i and j with $1 \le i < j \le \phi(m)$ such that $g^i \equiv g^j \pmod{m}$, or $g^{j-i} \equiv 1 \pmod{m}$. But g is a primitive root of m, and thus $\operatorname{ord}_m g = \phi(m)$. By Theorem 5.4, $\phi(m) \mid (j-i)$, which is impossible. ■

Theorem 5.9 If m has a primitive root, then there are $\phi(\phi(m))$ primitive roots among $1, 2, \ldots, m$.

Proof. Let g be a primitive root of m and hence $\operatorname{ord}_m g = \phi(m)$. Then Theorem 5.8 tells us that the reduced system modulo m can be represented by $\{g, \ldots, g^{\phi(m)}\}$. Thus, it suffices to determine the number of i's with $1 \le i \le \phi(m)$ such that $\operatorname{ord}_m g^i = \phi(m)$. On the other hand, we know from Theorem 5.5 that $\operatorname{ord}_m g^i = \frac{\phi(m)}{(i,\phi(m))}$. So we only need to count the number of i's such that $(i, \phi(m)) = 1$ and there are $\phi(\phi(m))$ such i's among $1, \ldots, \phi(m)$. ■

5.4 Lagrange's polynomial congruence theorem

Here, we present a theorem of the Italian mathematician Joseph-Louis Lagrange, which will be a key for confirming the existence of primitive roots of an odd prime.

Theorem 5.10 (Lagrange's Polynomial Congruence Theorem). Let p be a prime. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients such that $p \nmid a_n$. Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n solutions modulo p.

Proof. We prove by induction on the degree n of $f(x)$. When $n=1$, $f(x)$ is linear and the statement is trivial. Now we assume that the statement is true for $1,\ldots,n$ with $n\geq 1$. Let $f(x)$ be of degree $n+1$. If $f(x)\equiv 0 \pmod{p}$ has no solutions, then there is nothing to prove. If there is one solution, say $x\equiv x_0 \pmod{p}$, then $f(x_0)\equiv 0 \pmod{p}$. Now, we consider $g(x)=f(x)-f(x_0)=(x-x_0)q(x)$ where $q(x)$ is a polynomial with integer coefficients whose degree is n. Note that $f(x)\equiv 0 \pmod{p}$ is equivalent to $g(x)\equiv 0 \pmod{p}$. Since p is a prime, we either have $x-x_0\equiv 0 \pmod{p}$ which has one solution modulo p, or $q(x)\equiv 0 \pmod{p}$ which has at most n solutions modulo p by our inductive assumption. It follows that there are at most $n+1$ solutions to $f(x)\equiv 0 \pmod{p}$, as desired. ■

5.5 Existence of primitive roots

Now, we are in a position to characterize which integers have primitive roots.

Theorem 5.11 Every odd prime p has a primitive root.

Proof. As in Theorem 5.7, we write $d_k=\mathrm{ord}_p\, k$ for $1\leq k\leq p-1$, and define $D=\max_k\{d_k\}$ so that $D\mid \phi(p)=p-1$. Since $d_k\mid D$, we have $k^D\equiv 1 \pmod{p}$ for each k. It turns out that the congruence $x^D-1\equiv 0 \pmod{p}$ has $p-1$ solutions modulo p. By Lagrange's Polynomial Congruence Theorem (Theorem 5.10), we have $D\geq p-1$. Combining with the fact that $D\mid p-1$, we have $D=p-1$, and hence, there exists an integer g of order $D=p-1=\phi(p)$, thereby giving our desired primitive root. ■

Lemma 5.12 For any odd prime p, there exists a primitive root g such that $p\mid (g^{p-1}-1)$ and $p^2\nmid (g^{p-1}-1)$.

Proof. Let g be an arbitrary primitive root of p. Then $g^{p-1}\equiv 1 \pmod{p}$, namely, $p\mid (g^{p-1}-1)$. If we also have $p^2\nmid (g^{p-1}-1)$, there is nothing to prove. If $p^2\mid (g^{p-1}-1)$, namely, $g^{p-1}-1\equiv 0 \pmod{p^2}$, then we note that $g_*=p+g$ is also a primitive root of p. Meanwhile,

$$\begin{aligned} g_*^{p-1}-1=(p+g)^{p-1}-1&=\sum_{r=0}^{p-1}\binom{p-1}{r}p^r g^{p-1-r}-1\\ &\equiv g^{p-1}+p(p-1)g^{p-2}-1\equiv -pg^{p-2}\not\equiv 0 \pmod{p^2}. \end{aligned}$$

Hence, in this case g_* is the desired primitive root. ■

Theorem 5.13 For any odd prime p, let g be a primitive root as in Lemma 5.12. Then for any positive integer α, g is also a primitive root of p^α. In particular, p^α always has an odd primitive root.

Proof. Since g is a primitive root of p as in Lemma 5.12, we have $\mathrm{ord}_p\, g=\phi(p)=p-1$ and g is such that

$$g^{p-1}=px+1$$

with $p\nmid x$. Let $\mathrm{ord}_{p^\alpha}\, g=d$. Then $g^d\equiv 1 \pmod{p^\alpha}$, and thus $g^d\equiv 1 \pmod{p}$. Hence, $(p-1)\mid d$. On the other hand, $d\mid \phi(p^\alpha)=(p-1)p^{\alpha-1}$. Hence, d is of the form $d=(p-1)p^s$

for some $0 \leq s \leq \alpha - 1$. Now, recalling that $p \nmid x$, we have, with an application of Theorem 4.11,

$$g^d = g^{(p-1)p^s} = (px+1)^{p^s} = \sum_{r=0}^{p^s} \binom{p^s}{r} (px)^r \equiv 1 + p^{s+1}x \not\equiv 1 \pmod{p^{s+2}}.$$

However, $g^d \equiv 1 \pmod{p^\alpha}$. Hence, $s+2 \geq \alpha+1$. It follows that the only possibility is $s = \alpha - 1$, implying that $\mathrm{ord}_{p^\alpha} g = d = (p-1)p^{\alpha-1} = \phi(p^\alpha)$, or g is a primitive root of p^α. Finally, we observe that both g and $g + p^\alpha$ are primitive roots of p^α, and they are of different parities, thereby concluding the last part. ■

Theorem 5.14 For any odd prime p and positive integer α, let g be an odd primitive root of p^α. Then g is also a primitive root of $2p^\alpha$.

Proof. Note that g being an odd primitive root of p^α implies that $(g, 2p^\alpha) = 1$. Let $d = \mathrm{ord}_{2p^\alpha} g$ and we have $d \mid \phi(2p^\alpha)$. Then $g^d \equiv 1 \pmod{2p^\alpha}$, and hence, $g^d \equiv 1 \pmod{p^\alpha}$. Since g is a primitive root of p^α, we have $\phi(p^\alpha) = \mathrm{ord}_{p^\alpha} g \mid d$. However, $\phi(2p^\alpha) = \phi(p^\alpha) = (p-1)p^{\alpha-1}$. It follows that $d = \phi(2p^\alpha)$, namely, g is a primitive root of $2p^\alpha$. ■

Theorem 5.15 The positive integer m has a primitive root if and only if m is of the form 1, 2, 4, p^α or $2p^\alpha$ where p is an odd prime and α is a positive integer.

Proof. Note that 1 has a primitive root 1, that 2 has a primitive root 1, and that 4 has a primitive root 3. It remains to show that no other positive integers have primitive roots.

We first exclude ingeters m that can be written as $m = st$ with $s, t \geq 3$ and $(s,t) = 1$. Note that Euler's totient function ϕ is multiplicative, namely, $\phi(m) = \phi(s)\phi(t)$. Also, $\phi(s)$ and $\phi(t)$ are even by recalling Theorem 4.2. Thus, $\frac{\phi(m)}{2}$ is a integer. We prove that for any a with $(a,m) = 1$, $a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{m}$. To see this, we have

$$a^{\frac{\phi(m)}{2}} = \left(a^{\phi(s)}\right)^{\frac{\phi(t)}{2}} \equiv 1^{\frac{\phi(t)}{2}} = 1 \pmod{s},$$

and similarly,

$$a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{t}.$$

Note that $(s,t) = 1$ and $st = m$. By Chinese Remainder Theorem, we have $a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{m}$. Hence, m has no primitive roots.

Finally, we exclude integers of the form 2^α with $\alpha \geq 3$. Note that if a is such that $(a, 2^\alpha) = 1$, then a is odd and we write $a = 2b+1$. We prove that $a^{\frac{\phi(2^\alpha)}{2}} = a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$ always holds true. To see this, we have, with Theorem 4.11 applied,

$$\begin{aligned} a^{\frac{\phi(2^\alpha)}{2}} &= (2b+1)^{2^{\alpha-2}} = \sum_{r=0}^{2^{\alpha-2}} \binom{2^{\alpha-2}}{r} (2b)^r \\ &\equiv 1 + 2^{\alpha-2}(2b) + (2^{\alpha-2}-1)2^{\alpha-3}(2b)^2 \\ &\equiv 1 + 2^{\alpha-1}(b - b^2) \equiv 1 \pmod{2^\alpha}. \end{aligned}$$

Hence 2^α $(\alpha \geq 3)$ has no primitive roots. ■

6. Quadratic residues

6.1 Quadratic residues

Assume that $p \geq 3$ is prime and that x is such that $1 \leq x \leq p-1$. Recall from Theorem 4.1 that $\{xy : 1 \leq y \leq p-1\}$ covers a reduced system modulo p. Hence, for any integer a with $(a,p) = 1$, there exists a unique x' with $1 \leq x' \leq p-1$ such that $xx' \equiv a \pmod{p}$.

Definition 6.1 We call x' the *associate of x with respect to a modulo p* if

$$xx' \equiv a \pmod{p}$$

with $1 \leq x' \leq p-1$.

We are in particular interested in the case where the associate of x is itself.

Definition 6.2 Let p be a prime and a be such that $(a,p) = 1$. We say that a is a *quadratic residue modulo p* if there exists an x such that

$$x^2 \equiv a \pmod{p}.$$

If such x does not exist, we say that a is a *quadratic non-residue modulo p*.

R By definition, it is straightforward to see that for p a prime, if a and b are such that $(a,p) = (b,p) = 1$ and $a \equiv b \pmod{p}$, then a and b are simultaneously quadratic residues modulo p, or simultaneously quadratic non-residues modulo p.

Note that when $p = 2$, for any a with $(a,2) = 1$ so that a is an odd integer, we always have $a \equiv 1 = 1^2 \pmod{2}$. Thus, all odd integers are quadratic residues modulo 2. Below, we only focus on the case where $p \geq 3$.

Lemma 6.1 Let $p \geq 3$ be a prime and x_0 be such that $(x_0, p) = 1$. Then

$$x^2 \equiv x_0^2 \pmod{p} \tag{6.1}$$

has exactly two solutions

$$x_+ \equiv x_0 \pmod{p} \qquad \text{and} \qquad x_- \equiv -x_0 \pmod{p},$$

and in particular $x_+ \not\equiv x_- \pmod{p}$.

Proof. We rewite (6.1) as

$$(x-x_0)(x+x_0) \equiv 0 \pmod{p}.$$

Since p is prime, it follows that $p \mid (x-x_0)$ or $p \mid (x+x_0)$, thereby leading to the two solutions $x_\pm$. Also, $x_+ \not\equiv x_- \pmod{p}$; otherwise, we have $x_0 \equiv -x_0 \pmod{p}$, or $p \mid 2x_0$, or $p \mid x_0$ since $p \geq 3$ is prime, which violates the assumption that $(x_0, p) = 1$. ■

Theorem 6.2 Let $p \geq 3$ be a prime.

(i) If a is a quadratic residue modulo p, then there are exactly two distinct residue classes $x \equiv x_1, x_2$ modulo p with $x_2 \equiv -x_1 \pmod{p}$ such that $x^2 \equiv a \pmod{p}$.

(ii) There are exactly $\frac{p-1}{2}$ quadratic residues modulo p, and $\frac{p-1}{2}$ quadratic non-residues modulo p. In particular, the quadratic residues can be represented by the residue classes $\{1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}$ modulo p.

Proof. (i). Since a is a quadratic residue, we may always find an x_1 such that $x_1^2 \equiv a \pmod{p}$. Thus, by Lemma 6.1, the only two solutions to $x^2 \equiv a \equiv x_1^2 \pmod{p}$ are $x \equiv \pm x_1 \pmod{p}$ and they are distinct.

(ii). First, Part (i) implies that there are at most $\frac{p-1}{2}$ quadratic residues modulo p. Otherwise, if there are at least $\frac{p+1}{2}$ quadratic residues, then there are at least $2 \cdot \frac{p+1}{2} = p+1$ residue classes modulo p, which is impossible. Next, we show that $\{1^2, \ldots, (\frac{p-1}{2})^2\}$ are pairwise distinct residue classes modulo p. To see this, we choose $1 \leq i, j \leq \frac{p-1}{2}$ with $i \neq j$. We claim that $i^2 \not\equiv j^2 \pmod{p}$. Otherwise, if $i^2 \equiv j^2 \pmod{p}$, then $p \mid (i-j)(i+j)$. But since $1 \leq i, j \leq \frac{p-1}{2}$ and $i \neq j$, both $i-j$ and $i+j$ are not multiples of p, thereby leading to a contradiction. Thus, there are exactly $\frac{p-1}{2}$ quadratic residues modulo p, characterized by $\{1^2, \ldots, (\frac{p-1}{2})^2\}$ modulo p, and as a consequence, there are exactly $(p-1) - \frac{p-1}{2} = \frac{p-1}{2}$ quadratic non-residues modulo p. ■

Theorem 6.3 Let $p \geq 3$ be a prime.

(i) If a is a quadratic residue modulo p, then

$$(p-1)! \equiv -a^{\frac{p-1}{2}} \pmod{p}. \tag{6.2}$$

(ii) If a is a quadratic non-residue modulo p, then

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{6.3}$$

Proof. Recall that for each a with $(a, p) = 1$, every integer x with $1 \leq x \leq p-1$ has a unique associate x' (with respect to a modulo p) of one another with $1 \leq x' \leq p-1$.

For quadratic residues a, we know from Theorem 6.2(i) that there are exactly two x's, say $x = x_1$ and $x = p - x_1$, whose associate is itself. Therefore, we may group $\{1, \ldots, p-1\}$ into (x_1), $(p-x_1)$ and $\frac{p-3}{2}$ distinct unordered pairs (x, x') with

$$x_1^2 \equiv (p-x_1)^2 \equiv a \pmod{p}$$

and

$$xx' \equiv a \pmod{p}.$$

Thus,

$$(p-1)! = x_1 \cdot (p - x_1) \cdot \prod (xx') \equiv -x_1^2 \cdot \prod (xx') \equiv -a \cdot a^{\frac{p-3}{2}} = -a^{\frac{p-1}{2}} \pmod{p}.$$

For quadratic non-residues a, we cannot find any x such that $x^2 \equiv a \pmod{p}$. Therefore, we group $\{1, \ldots, p-1\}$ into $\frac{p-1}{2}$ distinct unordered pairs (x, x') with

$$xx' \equiv a \pmod{p}.$$

Thus,

$$(p-1)! = \prod (xx') \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

The proof is therefore complete. ■

6.2 Wilson's Theorem

Let us take a look at the special case $a = 1$ of Theorem 6.3, which is known as *Wilson's Theorem*, named after the English mathematician John Wilson.

Theorem 6.4 (Wilson's Theorem). Let p be a prime. Then

$$(p-1)! \equiv -1 \pmod{p}. \tag{6.4}$$

Proof. If $p = 2$, we simply have $1 \equiv -1 \pmod{2}$, which is trivial. If p is an odd prime, then we note that 1 is a quadratic residue modulo p, for $1 \equiv 1^2 \pmod{p}$. Therefore, taking $a = 1$ in (6.2) yields (6.4). ■

Note that (6.4) is always false if the prime p is replaced by a composite.

Theorem 6.5 For $m \geq 2$, we have $(m-1)! \equiv -1 \pmod{m}$ if and only if m is prime.

Proof. The "if" part is exactly Wilson's Theorem. For the "only if" part, we assume that m is composite. Then m has a divisor d with $1 < d < m$. Thus, this d is among $2, \ldots, m-1$, and thus $d \mid (m-1)!$. This then implies that $d \nmid \big((m-1)! + 1\big)$. But if $(m-1)! \equiv -1 \pmod{m}$, or equivalently, $m \mid \big((m-1)! + 1\big)$, then all the divisors of m also divide $(m-1)! + 1$, thereby leading to a contradiction. ■

6.3 Legendre symbol

We usually use the *Legendre symbol*, which was introduced by the French mathematician Adrien-Marie Legendre in 1798, to characterize whether an integer a is a quadratic residue modulo an odd prime p.

Definition 6.3 Let $p \geq 3$ be a prime and a be an integer. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a, \\ 1, & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1, & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Theorem 6.6 Let $p \geq 3$ be a prime, and a and b be integers such that $a \equiv b \pmod{p}$. Then

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right). \tag{6.5}$$

Proof. If $a \equiv b \equiv 0 \pmod{p}$, we have $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 0$ by definition. If $a \equiv b \not\equiv 0 \pmod{p}$ and hence $(a,p) = (b,p) = 1$, the equality $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ follows by noting that in this case, a and b are simultaneously quadratic residues modulo p, or simultaneously quadratic non-residues modulo p. ■

Theorem 6.7 Let $p \geq 3$ be a prime. Then

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0. \tag{6.6}$$

Further, if $\{a_1, \ldots, a_{p-1}\}$ is a reduced system modulo p, then

$$\sum_{k=1}^{p-1} \left(\frac{a_k}{p}\right) = 0. \tag{6.7}$$

Proof. For (6.6), we make use of the fact from Theorem 6.2(ii) that there are exactly $\frac{p-1}{2}$ quadratic residues modulo p, and $\frac{p-1}{2}$ quadratic non-residues modulo p. For (6.7), we further apply Theorem 6.6. ■

Theorem 6.8 Let $p \geq 3$ be a prime and a be such that $(a,p) = 1$. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{6.8}$$

Proof. Note that Theorem 6.3 can be understood as

$$(p-1)! \equiv -\left(\frac{a}{p}\right) \cdot a^{\frac{p-1}{2}} \pmod{p}.$$

On the other hand, Wilson's Theorem asserts that

$$(p-1)! \equiv -1 \pmod{p}.$$

The desired result therefore follows. ■

Theorem 6.9 Let $p \geq 3$ be a prime and m, n be integers. Then

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right). \tag{6.9}$$

Proof. If one of m and n is a multiple of p, so is mn. Thus, in this case,

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = 0.$$

Now, we assume that $(m,p)=(n,p)=1$ and thus $(mn,p)=1$. Then by Theorem 6.8,

$$\left(\frac{mn}{p}\right) \equiv (mn)^{\frac{p-1}{2}} = m^{\frac{p-1}{2}} n^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \pmod{p},$$

that is, $p \mid \left|\left(\frac{mn}{p}\right) - \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\right|$. However, the values of $\left(\frac{m}{p}\right)$, $\left(\frac{n}{p}\right)$ and $\left(\frac{mn}{p}\right)$ are taken from $\{-1,1\}$. Thus, $\left|\left(\frac{mn}{p}\right) - \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\right| \le 2$, implying that $\left(\frac{mn}{p}\right) - \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = 0$, as desired. ■

R Given a function $f : \mathbb{Z} \to \mathbb{C}$, we say that it is *completely multiplicative* if $f(1)=1$ and for any m and n,

$$f(mn) = f(m)f(n).$$

"Multiplicative" vs "Completely multiplicative": For completely multiplicative functions, the above relation holds true even if $(m,n)>1$.

6.4 When is -1 a quadratic residue modulo p?

Theorem 6.10 Let $p \ge 3$ be a prime. Then

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{6.10}$$

In particulae, -1 is a quadratic residue modulo p if $p \equiv 1 \pmod 4$, and a quadratic non-residue modulo p if $p \equiv 3 \pmod 4$.

Proof. We know from Theorem 6.8 that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$, and thus (6.10) follows since $\left(\frac{-1}{p}\right)$ takes value from $\{-1,1\}$ for odd primes p. Finally, $\frac{p-1}{2}$ is even if $p \equiv 1 \pmod 4$, and odd if $p \equiv 3 \pmod 4$. ■

6.5 Starters for sums of squares

We prove two additional results based on the knowledge of quadratic residues; they will be used in our later study of the "sum of squares" problems.

Theorem 6.11 Let $p \ge 3$ be a prime such that $p \equiv 1 \pmod 4$. Then there exists an integer x such that

$$x^2 + 1 = mp$$

with $0 < m < p$.

Proof. For primes $p \equiv 1 \pmod 4$, Theorem 6.10 tells us that -1 is a quadratic residue modulo p. Thus, there exists an x among $1, \ldots, p-1$ such that

$$x^2 \equiv -1 \pmod p.$$

In particular, we may choose x with $1 \le x \le \frac{p-1}{2}$, for if x satisfies the above congruence, so does $p-x$. Finally, we have $0 < x^2+1 < \left(\frac{p}{2}\right)^2 + 1 < p^2$. Thus, $x^2+1 = mp$ with $0 < m < p$. ■

Theorem 6.12 Let $p \geq 3$ be a prime. Then there exist integers x and y such that

$$x^2 + y^2 + 1 = mp$$

with $0 < m < p$.

Proof. Consider the following $p+1$ integers: x^2 for $0 \leq x \leq \frac{p-1}{2}$ and $-(y^2+1)$ for $0 \leq y \leq \frac{p-1}{2}$. Since there are p residue classes modulo p, by the pigeonhole principle, at least two of the $p+1$ integers fall into the same residue class. Note that all the x^2 are incongruent modulo p, and so are the $-(y^2+1)$. Thus, the two integers falling into the same residue class must be one x^2 and one $-(y^2+1)$. That is, there exist x and y with $0 \leq x, y \leq \frac{p-1}{2}$ such that $x^2 \equiv -(y^2+1) \pmod{p}$, or $x^2+y^2+1 = mp$ for an integer m. Finally, we have $0 < 1+x^2+y^2 < 1+2\left(\frac{p}{2}\right)^2 < p^2$. Thus, $0 < m < p$. ■

7. Quadratic reciprocity

7.1 Gauss's Lemma

To further evaluate the Legendre symbol $\left(\frac{a}{p}\right)$, we require a lemma due to the German mathematician Carl Friedrich Gauss. This lemma plays as a key in the derivation of the famous quadratic reciprocity law that was conjectured by Euler and Legendre and first proved by Gauss himself.

Lemma 7.1 (Gauss's Lemma). Let $p \ge 3$ be a prime and a be such that $(a,p)=1$. For each k with $1 \le k \le \frac{p-1}{2}$, let r_k be the smallest nonnegative residue of ak modulo p. If $\mu = \mu_a$ counts the number of r_k greater than $\frac{p}{2}$, then

$$\left(\frac{a}{p}\right) = (-1)^{\mu}. \tag{7.1}$$

Example 7.1 We provide an illustration of Gauss's Lemma with $p=11$. Noting that the quadratic residues modulo 11 are given by the residue classes $\{1,3,4,5,9\}$ and that the non-residues are given by the residue classes $\{2,6,7,8,10\}$, we have, for instance, $\left(\frac{2}{11}\right)=-1$ and $\left(\frac{5}{11}\right)=1$. **(i).** $a=2$: We have $\{2k \bmod 11 : 1 \le k \le 5\} = \{2,4,\mathbf{6},\mathbf{8},\mathbf{10}\}$, and hence $\mu_2 = 3$ and $\left(\frac{2}{11}\right)=(-1)^3=-1$; **(ii).** $a=5$: We have $\{5k \bmod 11 : 1 \le k \le 5\} = \{5,\mathbf{10},4,\mathbf{9},3\}$, and hence $\mu_5=2$ and $\left(\frac{5}{11}\right)=(-1)^2=1$. ■

Proof. Since $(a,p)=1$, we have $1 \le r_k \le p-1$ for each k. Now, we separate these $k \in \{1,2,\ldots,\frac{p-1}{2}\}$ into two disjoint groups $\{x_1,\ldots,x_\mu\}$ and $\{y_1,\ldots,y_\nu\}$ such that $r_x > \frac{p}{2}$ for all x and $r_y < \frac{p}{2}$ for all y. Note that $\mu+\nu = \frac{p-1}{2}$. Also, the r_x are pairwise distinct and so are the r_y. We further claim that there are no x and y with $p - r_x = r_y$; otherwise, we have $0 \equiv p = r_x + r_y \equiv ax + ay \pmod p$, or $x + y \equiv 0 \pmod p$, which is impossible since $1 \le x, y \le \frac{p-1}{2}$. Noting that $1 \le p - r_x < \frac{p}{2}$ and $1 \le r_y < \frac{p}{2}$, we conclude that the $\frac{p-1}{2}$ pairwise distinct integers $(p-r_{x_1}),\ldots,(p-r_{x_\mu})$ and $r_{y_1},\ldots,r_{y_\nu}$ form a rearrangement of $1,\ldots,\frac{p-1}{2}$. Thus,

$$a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! = \prod_{k=1}^{(p-1)/2}(ak) \equiv \prod_{k=1}^{(p-1)/2} r_k = \prod_{i=1}^{\mu} r_{x_i} \cdot \prod_{j=1}^{\nu} r_{y_j}$$

$$\equiv (-1)^{\mu}\prod_{i=1}^{\mu}(p-r_{x_i})\cdot\prod_{j=1}^{\nu}r_{y_j} = (-1)^{\mu}\left(\frac{p-1}{2}\right)! \pmod p.$$

Since $(\frac{p-1}{2})!$ is coprime to p, we have $a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod p$. Finally, (7.1) follows since $\left(\frac{a}{p}\right)$ takes value from $\{\pm 1\}$ by definition and $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ by Theorem 6.8. ■

For any real number x, let $\lfloor x \rfloor$ denote the largest integer not exceeding x.

Lemma 7.2 With the notation in Lemma 7.1, we have

$$\mu_a \equiv (a-1)\cdot\frac{p^2-1}{8} + \sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ak}{p}\right\rfloor \pmod 2. \tag{7.2}$$

Proof. Note that each r_k is the remainder of ak divided by p. Thus, $ak = p\cdot\lfloor\frac{ak}{p}\rfloor + r_k$. Now, recalling that p is an odd prime,

$$\begin{aligned} a\cdot\frac{p^2-1}{8} &= \sum_{k=1}^{(p-1)/2}(ak) = \sum_{k=1}^{(p-1)/2}\left(p\cdot\left\lfloor\frac{ak}{p}\right\rfloor + r_k\right) = p\sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ak}{p}\right\rfloor + \sum_{i=1}^{\mu}r_{x_i} + \sum_{j=1}^{\nu}r_{y_j} \\ &\equiv \sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ak}{p}\right\rfloor + \left(\mu + \sum_{i=1}^{\mu}(p-r_{x_i})\right) + \sum_{j=1}^{\nu}r_{y_j} = \sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ak}{p}\right\rfloor + \mu + \sum_{k=1}^{(p-1)/2}k \\ &= \sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ak}{p}\right\rfloor + \mu + \frac{p^2-1}{8} \pmod 2, \end{aligned}$$

thereby yielding the desired result. ■

7.2 When is 2 a quadratic residue modulo p?

Theorem 7.3 Let $p \geq 3$ be a prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{7.3}$$

In particulae, 2 is a quadratic residue modulo p if $p \equiv \pm 1 \pmod 8$, and a quadratic non-residue modulo p if $p \equiv \pm 3 \pmod 8$.

Proof. Note that for k with $1 \leq k \leq \frac{p-1}{2}$, we have $0 < \frac{2k}{p} < 1$ and thus $\lfloor\frac{2k}{p}\rfloor = 0$. Now, taking $a = 2$ in (7.3) gives $\mu_2 \equiv \frac{p^2-1}{8} \pmod 2$, and it follows from Gauss's Lemma that $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod p$. Hence, (7.3) follows since $\left(\frac{2}{p}\right)$ takes value from $\{-1, 1\}$ for odd primes p. Finally, $\frac{p^2-1}{8}$ is even if $p \equiv \pm 1 \pmod 8$, and odd if $p \equiv \pm 3 \pmod 8$. ■

7.3 Guass's law of quadratic reciprocity

We have witnessed from Gauss's Lemma (Lemma 7.1) and Lemma 7.2 that for $p \geq 3$ a prime and a an integer with $(a, p) = 1$,

$$\left(\frac{a}{p}\right) = (-1)^{(a-1)\cdot\frac{p^2-1}{8} + \sum_{k=1}^{(p-1)/2}\lfloor\frac{ak}{p}\rfloor}.$$

Now, we further assume that $q \geq 3$ is a prime such that $q \neq p$. Then $(q-1) \cdot \frac{p^2-1}{8}$ is even for $q-1$ is even and $\frac{p^2-1}{8} = \sum_{k=1}^{(p-1)/2} k$ is an integer. It follows that

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor}.$$

Similarly,

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{(q-1)/2} \lfloor \frac{kp}{q} \rfloor}.$$

It turns out that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor + \sum_{k=1}^{(q-1)/2} \lfloor \frac{kp}{q} \rfloor}. \tag{7.4}$$

Theorem 7.4 Let $p, q \geq 3$ be primes with $p \neq q$. Then

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor = \frac{(p-1)(q-1)}{4}. \tag{7.5}$$

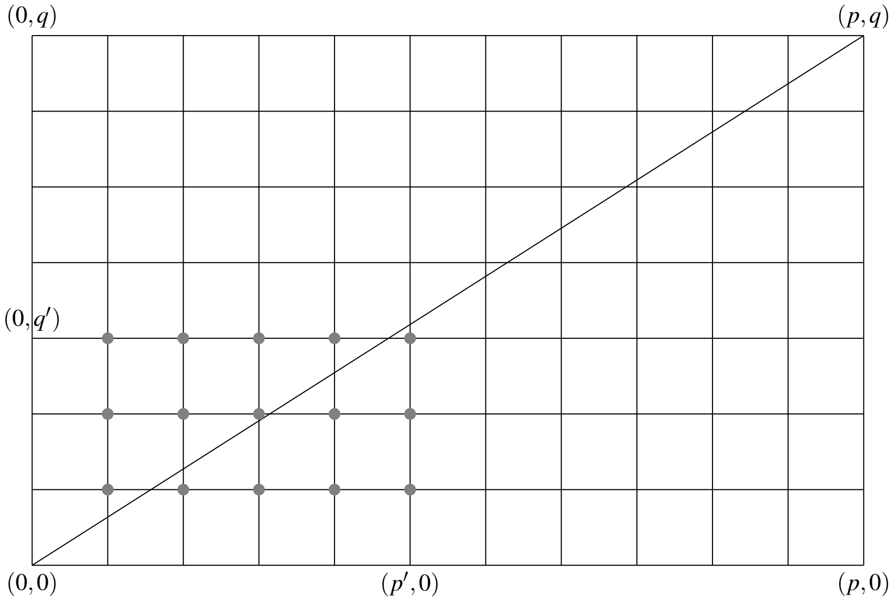


Figure 7.1: Integer lattices and $y = \frac{q}{p}x$

Proof. For convenience, we write $p' = \frac{p-1}{2}$ and $q' = \frac{q-1}{2}$. Consider the line

$$\ell : y = \frac{q}{p}x$$

on the xy-plane. We begin with some observations.

Observation 1. *For any integer $k \geq 1$, $\lfloor \frac{kq}{p} \rfloor$ equals the number of points with integer coordinates, or lattices for short, (k,y) which are below ℓ (with lattices on ℓ included).* For its proof, we note that ℓ touches the vertical line $x = k$ at $(k, \frac{kq}{p})$. Thus, such lattices are those with $1 \leq y \leq \frac{kq}{p}$, and the number of them equals the integer part of $\frac{kq}{p}$, that is $\lfloor \frac{kq}{p} \rfloor$.

Observation 2. *For any integer $k \geq 1$, $\lfloor \frac{kp}{q} \rfloor$ equals the number of lattices (x,k) which are above ℓ (with lattices on ℓ included).* The proof is similar to that for the first observation — we only need to note that ℓ touches the horizontal line $y = k$ at $(\frac{kp}{q}, k)$.

Observation 3. *There is no lattice (x,y) with $1 \leq x \leq p'$ or $1 \leq y \leq q'$ that is on ℓ.* Otherwise, assume that there exists an x_0 with $1 \leq x_0 \leq p'$ such that $(x_0, \frac{q}{p}x_0)$ is a lattice. Then $\frac{q}{p}x_0$ is an integer, which is impossible since $p \nmid q$ for p,q are distinct odd primes and $p \nmid x_0$ for $1 \leq x \leq p' = \frac{p-1}{2}$. Similarly, if we assume that there exists a y_0 with $1 \leq y_0 \leq q'$ such that $(\frac{p}{q}y_0, y_0)$ is a lattice, then $\frac{p}{q}y_0$ is an integer, and it is also impossible. The claim follows by contradiction.

Now, we focus on the set of lattices (x,y) with $1 \leq x \leq p'$ and $y \geq 1$ that are **strictly** below ℓ, denoted by $\mathscr{B}$, and the set of lattices (x,y) with $x \geq 1$ and $1 \leq y \leq q'$ that are **strictly** above ℓ, denoted by $\mathscr{A}$.

By the three observations (especially Observation 3, which allows us to add the strengthening of "**strictly**"), we have

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor = \operatorname{card} \mathscr{A} + \operatorname{card} \mathscr{B}.$$

First, it is apparent that all lattices (x,y) with $1 \leq x \leq p'$ **and** $1 \leq y \leq q'$ are in $\mathscr{A} \cup \mathscr{B}$. Now, we show that they are the only lattices in $\mathscr{A} \cup \mathscr{B}$.

(i). For lattices with $x > p'$ and $y > q'$, they are not in $\mathscr{A} \cup \mathscr{B}$ by definition.

(ii). For any lattice with $1 \leq x \leq p'$ and $y > q'$ (so it is not in $\mathscr{A}$), we compute the slope of the line connecting this lattice and the origin, which is $\frac{y}{x} \geq \frac{q'+1}{p'} = \frac{q+1}{p-1} > \frac{q}{p}$, and thus the lattice is above ℓ, so not in $\mathscr{B}$.

(iii). For any lattice with $x > p'$ and $1 \leq y \leq q'$ (so it is not in $\mathscr{B}$), we compute the slope of the line connecting this lattice and the origin, which is $\frac{y}{x} \leq \frac{q'}{p'+1} = \frac{q-1}{p+1} < \frac{q}{p}$, and thus the lattice is below ℓ, so not in $\mathscr{A}$.

Noting that $\mathscr{A}$ and $\mathscr{B}$ are disjoint, we have $\operatorname{card} \mathscr{A} + \operatorname{card} \mathscr{B} = \operatorname{card} \mathscr{A} \cup \mathscr{B} = p'q'$. Thus,

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor = \operatorname{card} \mathscr{A} + \operatorname{card} \mathscr{B} = p'q' = \frac{(p-1)(q-1)}{4},$$

proving the desired result. ■

Now, we can state *Guass's law of quadratic reciprocity.*

Theorem 7.5 (Guass's Law of Quadratic Reciprocity). Let $p,q \geq 3$ be primes with $p \neq q$. Then

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}. \tag{7.6}$$

Proof. This is a direct application of (7.4) and (7.5). ■

7.4 When is 3 a quadratic residue modulo p?

Theorem 7.6 Let $p \geq 5$ be a prime. Then 3 is a quadratic residue modulo p if $p \equiv \pm 1 \pmod{12}$, and a quadratic non-residue modulo p if $p \equiv \pm 5 \pmod{12}$.

Proof. By Guass's law of quadratic reciprocity, we have

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}.$$

Further, $\left(\frac{p}{3}\right)$ equals 1 if $p \equiv 1 \pmod 3$ and equals -1 if $p \equiv -1 \pmod 3$. Also, $(-1)^{\frac{p-1}{2}}$ equals 1 if $p \equiv 1 \pmod 4$ and equals -1 if $p \equiv -1 \pmod 4$. The desired result follows by a simple calculation. ■

7.5 An upper bound for the least quadratic non-residue

Definition 7.1 Let $p \geq 3$ be a prime. The *least quadratic non-residue modulo* p, usually denoted by n_p, is the smallest positive integer that is a quadratic non-residue modulo p.

■ **Example 7.2** We have $n_3 = 2$, $n_5 = 2$, $n_7 = 3$, ... ■

R The least quadratic residue is less interesting because 1 is always a quadratic residue modulo any odd prime p.

Recall from Theorem 6.2 that there are $\frac{p-1}{2}$ residues and $\frac{p-1}{2}$ non-residues modulo p among $1, \ldots, p-1$. Therefore, we trivially have $n_p \leq \frac{p-1}{2} + 1 = \frac{p+1}{2}$. But the upper bound for n_p could be sharper.

Theorem 7.7 Let $p \geq 3$ be a prime. Then

$$n_p < \sqrt{p} + 1. \tag{7.7}$$

Proof. Note that $1 < n_p < p$. Let $m = \lfloor \frac{p}{n_p} \rfloor + 1$. Since $\frac{p}{n_p}$ is not an integer, we have $(m-1)n_p < p < mn_p$. Thus, $0 < mn_p - p < n_p$. Since n_p is the least non-residue, we have that all $1, \ldots, n_p - 1$ are residues, and so is $mn_p - p$. It follows that

$$1 = \left(\frac{mn_p - p}{p}\right) = \left(\frac{mn_p}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n_p}{p}\right),$$

where Theorem 6.9 is used. Since n_p is a non-residue, we have $\left(\frac{n_p}{p}\right) = -1$, and thus $\left(\frac{m}{p}\right) = -1$ from the above. Thus, m is also a non-residue. It follows that $n_p \leq m$. So,

$$p > (m-1)n_p \geq (n_p - 1)n_p > (n_p - 1)^2,$$

yielding the desired result. ■

R The upper bound for n_p is far sharper than (7.7). The best bound known today is

$$n_p = O_\varepsilon\left(p^{\frac{1}{4\sqrt{e}}+\varepsilon}\right),$$

for all $\varepsilon > 0$. It was proved with recourse to Burgess's estimate of certain character sums and Vinogradov's sieving trick. An excellent exposition of the idea can be found in Terry Tao's blog post:

https://terrytao.wordpress.com/2009/08/18/the-least-quadratic-nonresidue-and-the-square-root-barrier/

8. Sums of squares

8.1 Primes as a sum of two squares

Recall that the following notation has been used earlier in the study of binomial coefficients.

Definition 8.1 Let p be a prime. Given any nonzero integer n, we denote by $\nu_p(n)$ the unique nonnegative integer k such that $p^k \mid n$ and $p^{k+1} \nmid n$, namely, $\nu_p(n)$ is the power of p in the canonical form of n.

Theorem 8.1 Let x and y be integers, not both zero. For any prime p with $p \equiv 3 \pmod 4$, we have that $\nu_p(x^2+y^2)$ is even.

Proof. Let $n = x^2+y^2$. Note that $n>0$. Let $d = (x,y)$ and write $x = x_0 d$ and $y = y_0 d$ so $(x_0,y_0) = 1$. Hence, $n = d^2(x_0^2+y_0^2)$.

We first show that $p \nmid (x_0^2+y_0^2)$. If not, then $x_0^2+y_0^2 \equiv 0 \pmod p$, or $x_0^2 \equiv -y_0^2 \pmod p$. Since $(x_0,y_0)=1$, at least one of x_0 and y_0 is coprime to p. Without loss of generality, we assume that $(y_0,p)=1$, meaning that y_0 has a modular inverse y_0^{-1} modulo p. Hence, $(x_0 y_0^{-1})^2 \equiv -1 \pmod p$, indicating that -1 is a quadratic residue modulo p. However, this violates Theorem 6.10, saying that -1 is a quadratic non-residue as $p \equiv 3 \pmod 4$.

Thus, $\nu_p(n) = \nu_p(d^2) = 2\nu_p(d)$, which is even. ■

Theorem 8.2 Any prime p with $p \equiv 1 \pmod 4$ can be written as a sum of two squares.

We will present two proofs of this result: one is based on an important method called "infinite descent" developed by Fermat, and the other relies on a magical involution due to the American-German mathematician Don Zagier.

Before moving forward, we record a simple but useful formula.

Theorem 8.3 Let $x_1, y_1, x_2, y_2 \in \mathbb{R}$. Then

$$(x_1^2+y_1^2)(x_2^2+y_2^2) = (x_1x_2+y_1y_2)^2 + (x_1y_2-x_2y_1)^2. \tag{8.1}$$

Proof. This formula can be examined by a direct calculation. ■

R We may also understand (8.1) with recourse to complex numbers. Recall that a *complex number* z is of the form $z = x + yi$ with $x, y \in \mathbb{R}$ where $i = \sqrt{-1}$ is the *imaginary unit*. The *modulus* of z is define by $|z| = \sqrt{x^2 + y^2}$. Let $z_1 = x_1 + y_1 i$ and $z_2 = x_2 + y_2 i$. Note that the left hand side of (8.1) is $|z_1|^2|z_2|^2$ and the right hand side is $|z_1 z_2|^2$. So, $|z_1|^2|z_2|^2 = |z_1 z_2|^2$.

8.2 The method of infinite descent

Among different variants of the method of *infinite descent*, which is also known as *Fermat's method of descent*, we will make use of the following version.

The Method of Infinite Descent Let P be a property that at least one positive integer possesses. Assume that whenever $m > 1$ possesses P, we may find another positive integer m_0 with $m_0 < m$ such that m_0 also possesses P. Then 1 possesses P.

First Proof of Theorem 8.2. Recall from Theorem 6.11 that for primes p with $p \equiv 1 \pmod 4$, there exists an integer x such that $x^2 + 1 = mp$ with $0 < m < p$. In other words, there exists an integer m with $0 < m < p$ such that the equation

$$x^2 + y^2 = mp$$

has an integer solution (x, y).

Assume that $m > 1$. Note that for any integer n, we may always find an integer n_0 with $|n_0| \le \frac{m}{2}$ such that $n \equiv n_0 \pmod m$. This is because there are at least m consecutive integers in the interval $[-\frac{m}{2}, \frac{m}{2}]$, thereby covering a complete system modulo m.

Now, we find $x \equiv x_0 \pmod m$ with $|x_0| \le \frac{m}{2}$ and $y \equiv y_0 \pmod m$ with $|y_0| \le \frac{m}{2}$. Note that we cannot simultaneously have $m \mid x$ and $m \mid y$ for if this is the case, then $m^2 \mid (x^2 + y^2)$ but $m^2 \nmid mp$ since $0 < m < p$ (and hence $(m, p) = 1$), thereby leading to a contradiction. Hence, x_0 and y_0 are not simutaneously 0, and we then have $x_0^2 + y_0^2 > 0$. On the other hand, $x_0^2 + y_0^2 \le 2 \cdot (\frac{m}{2})^2 < m^2$. Noting that $x_0^2 + y_0^2 \equiv x^2 + y^2 = mp \equiv 0 \pmod m$, we may write $x_0^2 + y_0^2 = m_0 m$ with $0 < m_0 < m$. By Theorem 8.3, we have

$$(xx_0 + yy_0)^2 + (xy_0 - x_0 y)^2 = (x^2 + y^2)(x_0^2 + y_0^2) = (mp) \cdot (m_0 m) = m^2 m_0 p.$$

Meanwhile, we have $xx_0 + yy_0 \equiv x^2 + y^2 \equiv 0 \pmod m$ and $xy_0 - x_0 y \equiv xy - xy = 0 \pmod m$. Hence, $\frac{xx_0 + yy_0}{m}$ and $\frac{xy_0 - x_0 y}{m}$ are integers. It follows that

$$m_0 p = \left(\frac{xx_0 + yy_0}{m}\right)^2 + \left(\frac{xy_0 - x_0 y}{m}\right)^2,$$

a sum of two squares.

Finally, noting that m_0 is a positive integer with $m_0 < m$, we deduce that $x^2 + y^2 = p$ has an integer solution (x, y) with recourse to the method of infinite descent. ■

8.3 Zagier's magical involution

Definition 8.2 Let S be a set. We say that $f : S \to S$ is an *involution* on S if for any $x \in S$, there holds true that $f(f(x)) = x$.

R In fact, every involution f is a bijective map on S. The surjectivity follows by the fact every $x \in S$ in the image of $f(x)$ under f, and the injectivity follows by the fact that if $f(x) = f(y)$, then $x = f(f(x)) = f(f(y)) = y$.

Definition 8.3 Let S be a set and $f : S \to S$ be a map on S. We say that $x \in S$ is a *fixed point* under f if $f(x) = x$.

Theorem 8.4 Let S be a finite set and assume that there is an involution f on S.

(i) If f has no fixed points, then the size $|S|$ of S is even.

(ii) If f has exactly one fixed point, then $|S|$ is odd.

Proof. Since f is an involution on S, we may pair elements of S according to $(x, f(x))$ and treat $(f(x), x)$ as the same pair. Assume that there are s such pairs.

(i). Since f has no fixed points, we have $x \neq f(x)$ in each pair. Thus, every $x \in S$ belongs to exactly one of the pairs. It follows that $|S| = 2s$, which is even.

(ii). Assume that the only fixed point of f is x_0. Every $x \in S$ is either x_0, or belongs to exactly one of the pairs, excluding $(x_0, f(x_0)) = (x_0, x_0)$. Thus, $|S| = 1 + 2(s-1) = 2s-1$, which is odd. ■

Theorem 8.5 Let p be a prime with $p \equiv 1 \pmod 4$. Consider the finite set $S = \{(x,y,z) \in \mathbb{Z}^3_{>0} : x^2 + 4yz = p\}$. Then the following map f on S,

$$f(x,y,z) = \begin{cases} (x+2z, z, y-x-z), & \text{if } x < y-z, \\ (2y-x, y, x-y+z), & \text{if } y-z < x < 2y, \\ (x-2y, x-y+z, y), & \text{if } x > 2y, \end{cases}$$

is an involution, and it has exactly one fixed point. In particular, $|S|$ is odd.

Proof. We first show that $x \neq y-z$ and $x \neq 2y$. If $x = y-z$, then $p = (y-z)^2 + 4yz = (y+z)^2$ which is impossible since p is prime. If $x = 2y$, then $p = (2y)^2 + 4yz = 4y(y+z)$ which is also impossible. Thus, we may separate S into three disjoint subsets S_1, S_2 and S_3 according to **(1).** $x < y-z$, **(2).** $y-z < x < 2y$, **(3).** $x > 2y$.

A direct calculation reveals that for any $(x,y,z) \in S$, $f(f(x,y,z)) = (x,y,z)$, and hence, f is an involution. Also, if $(x,y,z) \in S_1$, then $f(x,y,z) \in S_3$; if $(x,y,z) \in S_2$, then $f(x,y,z) \in S_2$; and if $(x,y,z) \in S_3$, then $f(x,y,z) \in S_1$. Hence, fixed points (x,y,z) are only in S_2, with

$$x = 2y - x, \qquad y = y, \qquad z = x - y + z,$$

or $x = y$. But in this case, $p = x^2 + 4xz = x(x+4z)$ implies that the only possible x is $x = 1$, and so $y = x = 1$. Finally, since $p \equiv 1 \pmod 4$, that is, $p = 4k+1$ with $k > 0$, we have the unique fixed point $(x,y,z) = (1,1,k)$. We conclude from Theorem 8.4 that $|S|$ is odd. ■

Second Proof of Theorem 8.2. The set S in Theorem 8.5 also has a trivial involution g given by $g(x,y,z) = (x,z,y)$. But g must have a fixed point; otherwise, $|S|$ is even by Theorem 8.4, thereby contradicting to Theorem 8.5. But the fixed point of g means that $z = y$. Hence, we may find positive integers x and y such that $p = x^2 + 4y^2 = x^2 + (2y)^2$. ■

R Don Zagier's proof was published in (*Amer. Math. Monthly* **97** (1990), no. 2, 144). In fact, his involution is a refinement of an equally beautiful argument attributed to Roger Heath-Brown (*Invariant* (1984), 2–5). Heath-Brown's proof, dating back to 1971, was motivated by his study of J. V. Uspensky and M. A. Heaslet's book "*Elementary Number Theory*" (McGraw-Hill Book Co., Inc., New York, 1939), which accounts Liouville's papers on identities for parity functions.

8.4 Fermat's two-square theorem

Now, we are in a position to characterize which integers can be written as a sum of two squares.

Theorem 8.6 (Fermat's Two-Square Theorem). A positive integer n can be written as a sum of two squares if and only if all prime factors p of n with $p \equiv 3 \pmod 4$ have an even power in the canonical form of n.

Proof. The "only if" part has been shown by Theorem 8.1. For the "if" part, we write in the canonical form

$$n = 2^\alpha \prod_{p\equiv 1 \bmod 4} p^\beta \prod_{q\equiv 3 \bmod 4} q^{2\gamma}.$$

Here, p runs over all distinct prime factors of n that are congruent to 1 modulo 4, and q runs over all distinct prime factors of n that are congruent to 3 modulo 4. In particular, the exponent of each q is even as assumed. Now, note that $2 = 1^2 + 1^2$, that for each q, we have $q^2 = 0^2 + q^2$, and that for each p, we have $p = x^2 + y^2$ for certain integers x and y by Theorem 8.2. A repeated application of Theorem 8.3 gives the desired result. ■

8.5 Lagrange's four-square theorem

Concerning sums of four squares, we first require an analog of Theorem 8.3.

Theorem 8.7 Let $x_1, y_1, z_1, w_1, x_2, y_2, z_2, w_2 \in \mathbb{R}$. Then

$$\begin{aligned}(x_1^2+y_1^2+z_1^2+w_1^2)(x_2^2+y_2^2+z_2^2+w_2^2)\\ &= (x_1x_2+y_1y_2+z_1z_2+w_1w_2)^2 + (x_1y_2-y_1x_2+z_1w_2-w_1z_2)^2\\ &\quad + (x_1z_2-y_1w_2-z_1x_2+w_1y_2)^2 + (x_1w_2+y_1z_2-z_1y_2-w_1x_2)^2. \end{aligned} \tag{8.2}$$

Proof. This formula can also be examined by a direct calculation. ■

Theorem 8.8 (Lagrange's Four-Square Theorem). Every positive integer can be written as a sum of four squares.

Proof. Note that $1 = 0^2 + 0^2 + 0^2 + 1^2$ and $2 = 0^2 + 0^2 + 1^2 + 1^2$. In view of Theorem 8.7, it suffices to show that every odd prime can be written as a sum of four squares.

Recall from Theorem 6.12 that for odd primes p, there exists integer x and y such that $x^2 + y^2 + 1 = mp$ with $0 < m < p$. In other words, there exists an integer m with $0 < m < p$ such that the equation

$$x^2 + y^2 + z^2 + w^2 = mp$$

has an integer solution (x, y, z, w).

Assume that $m > 1$. We have two cases.

(i). If m is even, then two of the integers x, y, z and w have the same parity, and the remaining two also have the same parity. Without loss of generality, we assume that x and y have the same parity, and z and w have the same parity. Thus, the four integers $x+y$, $x-y$, $z+w$, $z-w$ are even. Note that if $m_0 = \frac{m}{2}$, then $0 < m_0 < m$. Also,

$$\begin{aligned} m_0 p &= \frac{1}{2}(x^2+y^2+z^2+w^2)\\ &= \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2, \end{aligned}$$

a sum of four squares.

(ii). If m is odd, then similar to the first proof of Theorem 8.2, we find $x \equiv x_0 \pmod{m}$ with $|x_0| < \frac{m}{2}$, $y \equiv y_0 \pmod{m}$ with $|y_0| < \frac{m}{2}$, $z \equiv z_0 \pmod{m}$ with $|z_0| < \frac{m}{2}$ and $w \equiv w_0 \pmod{m}$ with $|w_0| < \frac{m}{2}$. Here, we use strict "$<$" since m is odd. Therefore, $x_0^2+y_0^2+z_0^2+w_0^2 < 4 \cdot (\frac{m}{2})^2 = m^2$. Also, we cannot simultaneously have $m \mid x$, $m \mid y$, $m \mid z$ and $m \mid w$, and hence, $x_0^2+y_0^2+z_0^2+w_0^2 > 0$. Noting that $x_0^2+y_0^2+z_0^2+w_0^2 \equiv x^2+y^2+z^2+w^2 = mp \equiv 0 \pmod{m}$, we may write $x_0^2+y_0^2+z_0^2+w_0^2 = m_0 m$ with $0 < m_0 < m$. By Theorem 8.7, we have

$$\begin{aligned} m^2 m_0 p &= (mp) \cdot (m_0 m) = (x^2+y^2+z^2+w^2)(x_0^2+y_0^2+z_0^2+w_0^2) \\ &= (xx_0+yy_0+zz_0+ww_0)^2 + (xy_0-yx_0+zw_0-wz_0)^2 = \\ &\quad + (xz_0-yw_0-zx_0+wy_0)^2 + (xw_0+yz_0-zy_0-wx_0)^2 \\ &=: \tilde{x}^2+\tilde{y}^2+\tilde{z}^2+\tilde{w}^2. \end{aligned}$$

Since $x \equiv x_0 \pmod{m}$, $y \equiv y_0 \pmod{m}$, $z \equiv z_0 \pmod{m}$, $w \equiv w_0 \pmod{m}$ and $x^2+y^2+z^2+w^2 \equiv 0 \pmod{m}$, we find that $\tilde{x}$, $\tilde{y}$, $\tilde{z}$ and $\tilde{w}$ are all multiples of m. Hence,

$$m_0 p = \left(\frac{\tilde{x}}{m}\right)^2 + \left(\frac{\tilde{y}}{m}\right)^2 + \left(\frac{\tilde{z}}{m}\right)^2 + \left(\frac{\tilde{w}}{m}\right)^2,$$

a sum of two squares.

Finally, noting that in both cases of the above, m_0 is a positive integer with $m_0 < m$, we deduce that $x^2+y^2+z^2+w^2 = p$ has an integer solution (x,y,z,w) with recourse to the method of infinite descent. ■

9. Generating functions

9.1 Generating functions

In the previous lecture, we have shown the existence of a representation as the sum of four squares for each nonnegative integer n. Now a natural question is how many such representations do we have? Is there a formula, or at least a nice way, to characterize the number of such representations for each n?

In general, for $\{a_n\}_{n\geq 0}$ a sequence of numbers, not necessarily integers, we want to find a clothesline on which we hang up $\{a_n\}$ for display.

Definition 9.1 Let $\{a_n\}_{n\geq 0}$ be a sequence of numbers. The the power series

$$\sum_{n\geq 0} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots$$

is called the *generating function* of $\{a_n\}$.

R Since we are considering power series, a natural question is their radii of convergence. However, this question is uaually not very interesting for generating functions, and in many cases we only treat these power series as *formal* power series. However, there are still occassions that the radii of convergence should be taken into account, especially when analytic techniques are applied. For instance, when we want to make use of Cauchy's integral formula to recover the coefficients a_n from its generating function $A(x) = \sum_{n\geq 0} a_n x^n$:

$$a_n = \frac{1}{2\pi i} \oint \frac{A(x)}{x^{n+1}} dx,$$

we must be careful about the convergence conditions when choosing the contour.

9.2 Formal power series

Definition 9.2 A *formal power series* is an expression of the form

$$a_0 + a_1 x + a_2 x^2 + \cdots,$$

where the sequence $\{a_n\}_{n\geq 0}$ is called the *sequence of coefficients*.

We say two series $A(x) = \sum_{n\geq 0} a_n x^n$ and $B(x) = \sum_{n\geq 0} b_n x^n$ are *equal* if $a_n = b_n$ for all $n \geq 0$. We can also define the usual operations for formal power series:

▷ *Addition/Subtraction*:

$$\sum_{n\geq 0} a_n x^n \pm \sum_{n\geq 0} b_n x^n = \sum_{n\geq 0} (a_n \pm b_n) x^n;$$

▷ *Multiplication* by the Cauchy product rule:

$$\left(\sum_{n\geq 0} a_n x^n\right)\left(\sum_{n\geq 0} b_n x^n\right) = \sum_{n\geq 0} c_n x^n, \quad \text{where } c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

To determine if division works, we need to check if a series has a *reciprocal*. In other words, given $\sum_{n\geq 0} a_n x^n$, we want to know if there exists a series $\sum_{n\geq 0} b_n x^n$ such that their product is 1.

Theorem 9.1 A formal power series $A(x) = \sum_{n\geq 0} a_n x^n$ has a reciprocal if and only if $a_0 \neq 0$. In that case, the reciprocal is unique.

Proof. (i). If $A(x)$ has a reciprocal, say $B(x) = \sum_{n\geq 0} b_n x^n$. Then $A(x)B(x) = 1$. Hence, $a_0 b_0 = 1$, which implies that $a_0 \neq 0$. Further, b_0 is uniquely given by $1/a_0$. Also, for $n \geq 1$, we have $0 = \sum_{k=0}^{n} a_k b_{n-k}$. Therefore,

$$b_n = -\frac{1}{a_0} \sum_{k=1}^{n} a_k b_{n-k}.$$

By induction, the b_n's are uniquely determined.

(ii). If $a_n \neq 0$, we choose $b_0 = 1/a_0$, and iteratively define $b_n = -\frac{1}{a_0} \sum_{k=1}^{n} a_k b_{n-k}$. Then we get a series $B(x) = \sum_{n\geq 0} b_n x^n$. It is straightforward to verify that $A(x)B(x) = 1$, and hence $B(x)$ is a reciprocal of $A(x)$. ■

■ **Example 9.1** We have

$$(1-x)(1+x+x^2+\cdots) = 1.$$

Hence, the reciprocal of $1-x$ is given by $1+x+x^2+\cdots$, written as

$$\frac{1}{1-x} = 1+x+x^2+\cdots.$$

This is exactly identical to what is obtained by applying the Taylor expansion to $\frac{1}{1-x}$. ■

Definition 9.3 Let $A(x) = \sum_{n\geq 0} a_n x^n$ be a formal power series. Its *derivative* is the series

$$A'(x) = \sum_{n\geq 1} n a_n x^{n-1}.$$

■ **Example 9.2** We know that

$$e^x = \sum_{n\geq 0} \frac{x^n}{n!}.$$

Now,

$$\left(\sum_{n\geq 0} \frac{x^n}{n!}\right)' = \sum_{n\geq 1} \frac{n x^{n-1}}{n!} = \sum_{n\geq 1} \frac{x^{n-1}}{(n-1)!} = e^x.$$

This is exactly identical to $(e^x)' = e^x$. ■

9.3 Fibonacci numbers

The *Fibonacci numbers* are named after the Italian mathematician Leonardo of Pisa, later known as Fibonacci, for his famous "*Rabbit Puzzle*" in his 1202 book *Liber Abaci*:

> *Assume that we have a pair of fictional rabbits, and they*
>
> (i) *produce a new pair of rabbits every month, starting from the second month that they are alive;*
>
> (ii) *and the new generations always repeat the trajectory of their parents' life.*
>
> *If rabbits never die and continue breeding forever, how many pairs will there be in one year?*

Assume that there are F_n pairs of rabbits after n months, starting with $F_0 = 0$ and $F_1 = 1$. Now, for F_n with $n \geq 2$, the rabbits are from the alive ones of the previous month, F_{n-1} pairs in total, and the newly born rabbits produced by those of at least two-month-old, F_{n-2} pairs in total. Therefore, for $n \geq 2$,

$$F_n = F_{n-1} + F_{n-2}. \tag{9.1}$$

Theorem 9.2 We have

$$\sum_{n\geq 0} F_n x^n = \frac{x}{1-x-x^2}. \tag{9.2}$$

Proof. We multiply (9.1) by x^n, and then sum over $n \geq 2$. Then

$$\sum_{n\geq 2} F_n x^n = \sum_{n\geq 2}(F_{n-1}+F_{n-2})x^n = x\sum_{n\geq 2} F_{n-1}x^{n-1} + x^2\sum_{n\geq 2} F_{n-2}x^{n-2} = x\sum_{n\geq 1} F_n x^n + x^2 \sum_{n\geq 0} F_n x^n.$$

Let $f = \sum_{n\geq 2} F_n x^n$. We have

$$f - (0+x) = x(f-0) + x^2 f,$$

or

$$(1-x-x^2)f = x.$$

This gives the desired result. ■

Can we find an explicit formula for F_n?

Theorem 9.3 For $n \geq 0$,

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) \tag{9.3}$$

Proof. Let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Then $(1-x-x^2) = (1-\alpha x)(1-\beta x)$. Therefore,

$$\begin{aligned}\frac{x}{1-x-x^2} &= \frac{x}{(1-\alpha x)(1-\beta x)} = \frac{1}{\alpha-\beta}\left(\frac{1}{1-\alpha x} - \frac{1}{1-\beta x}\right)\\ &= \frac{1}{\alpha-\beta}\left(\sum_{n\geq 0}\alpha^n x^n - \sum_{n\geq 0}\beta^n x^n\right).\end{aligned}$$

By equating the coefficient of x^n, we have

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

which is exactly as desired. ■

In general, we may consider the sequence $\{G_n\}_{n\ge 0}$ with $G_0 = a$, $G_1 = b$, and for $n \ge 2$, $G_n = sG_{n-1} + tG_{n-2}$ where a, b, s and t are fixed.

Theorem 9.4 We have

$$\sum_{n\ge 0} G_n x^n = \frac{a + bx - asx}{1 - sx - tx^2}. \tag{9.4}$$

Proof. Note that

$$\sum_{n\ge 2} G_n x^n = sx \sum_{n\ge 1} G_n x^n + tx^2 \sum_{n\ge 0} G_n x^n.$$

Thus,

$$\sum_{n\ge 0} G_n x^n - (a + bx) = sx \left(\sum_{n\ge 0} G_n x^n - a \right) + tx^2 \sum_{n\ge 0} G_n x^n,$$

yielding the desired result. ■

For example, the *Lucas numbers* L_n, which were introduced by the Frence mathematician François Lucas, are given by $L_0 = 2$, $L_1 = 1$, and for $n \ge 2$, $F_n = F_{n-1} + F_{n-2}$.

Theorem 9.5 We have

$$\sum_{n\ge 0} L_n x^n = \frac{2 - x}{1 - x - x^2}. \tag{9.5}$$

In particular, for $n \ge 0$,

$$L_n = \left(\frac{1+\sqrt{5}}{2} \right)^n + \left(\frac{1-\sqrt{5}}{2} \right)^n. \tag{9.6}$$

Proof. The first part is the $(a,b,s,t) = (2,1,1,1)$ case of Theorem 9.4. For the second part, we still write $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Then

$$\frac{2-x}{1-x-x^2} = \frac{1}{1-\alpha x} + \frac{1}{1-\beta x} = \sum_{n\ge 0} \alpha^n x^n + \sum_{n\ge 0} \beta^n x^n.$$

Equating the coefficient of x^n implies the desired result. ■

9.4 Compositions

Generating functions are of significant use in combinatorics. Here, we will take compositions as an example.

Definition 9.4 A *composition* of an integer n is a way of writing n as the sum of a sequence of positive integers, and the order of these summands matters.

■ **Example 9.3** There are four compositions of 3, namely, 3, $2+1$, $1+2$ and $1+1+1+1$. ■

Theorem 9.6 There are 2^{n-1} compositions of n.

Proof. We represent the integer n by n nodes in a row. Then there are $n-1$ gaps between consecutive nodes. Now, let us choose to place a stick at each gap or not, and there are 2^{n-1} choices. Each choice will induce a unique composition of n by counting the number of nodes between each consecutive pair of sticks while we assume that there are two invisible sticks at the two ends. Hence, there are 2^{n-1} compositions of n.

• • | • • • | • • | • | •

For instance, the above diagram gives $2+3+2+1+1$, which is a composition of 9. ■

Is it possible to avoid such a combinatorial argument?

Theorem 9.7 Let $c(k,n)$ count the number of compositions of n into k parts. Then

$$\sum_{n\geq 1} c(k,n)x^n = \left(\frac{x}{1-x}\right)^k. \tag{9.7}$$

Proof. Let us consider the product

$$(x+x^2+\cdots)^k = (x+x^2+\cdots)(x+x^2+\cdots)\cdots(x+x^2+\cdots),$$

where there are k multiplicands. If we expand this product, then the terms are of the form $x^{n_1+n_2+\cdots+n_k} =: x^n$ where each x^{n_i} comes from the i-th multiplicand. Also, this term corresponds to a unique composition of n, given by $n_1+n_2+\cdots+n_k$, and there are exactly k parts in this composition. Hence,

$$\sum_{n\geq 1} c(k,n)x^n = (x+x^2+\cdots)^k = \left(\frac{x}{1-x}\right)^k,$$

as required. ■

Theorem 9.8 Let $c(n)$ count the number of compositions of n. Then

$$\sum_{n\geq 1} c(n)x^n = \frac{x}{1-2x}. \tag{9.8}$$

In particular, $c(n) = 2^{n-1}$.

Proof. For the first part, we deduce from Theorem 9.7 that

$$\sum_{n\geq 1} c(n)x^n = \sum_{k\geq 1}\sum_{n\geq 1} c(k,n)x^n = \sum_{k\geq 1}\left(\frac{x}{1-x}\right)^k = \frac{\frac{x}{1-x}}{1-\frac{x}{1-x}} = \frac{x}{1-2x}.$$

Further, $\frac{x}{1-2x} = \sum_{n\geq 1} 2^{n-1}x^n$. By equating the coefficient of x^n, we arrive at the second part. ■

10. Integer partitions

10.1 Integer partitions

Integer partitions can be seen as a twin sibling of compositions.

Definition 10.1 An *integer partition* or a *partition* of an integer n is a way of writing n as the sum of a sequence of positive integers, and the order of these summands does *not* matter. We usually denote by $p(n)$ the number of partitions of n, and call $p(n)$ the *partition function*.

R Since for a partition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_\ell)$ of n, the order of these positive integers does not matter, we usually assume that they are in **weakly decreasing** order $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell$, as a representative. We also often write a partition as $\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_\ell$.

■ **Example 10.1** There are five partitions of 4, namely, 4, $3+1$, $2+2$, $2+1+1$ and $1+1+1+1$. Therefore, $p(5) = 4$. ■

Definition 10.2 Given a partition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_\ell)$ of n, usually written as $\lambda \vdash n$, we call each λ_i a *part* of λ; call $n = \lambda_1 + \lambda_2 + \cdots + \lambda_\ell$ the *size* of λ, denoted by $|\lambda|$; and call the number ℓ of parts the *length* of λ, denoted by $\ell(\lambda)$.

R We assume that 0 has an empty partition, written as $\varnothing$, and thus $p(0) = 1$. For the empty partition $\varnothing$, we have $|\varnothing| = 0$ and $\ell(\varnothing) = 0$.

10.2 Generating function for partitions

Another convenient way to represent partitions is through the *frequency notation*. Given a partition λ, for each positive integer i, we may count the number f_i of occurrences of i among the parts in λ, and we call f_i the frequency of i. Hence, we may represent λ in the frequency notation $1^{f_1}2^{f_2}3^{f_3}\cdots$, and we often omit the integers whose frequency is zero.

■ **Example 10.2** The partition $6+6+5+3+3+3+2+1+1+1+1+1$ has the frequency notation $6^2 5^1 3^3 2^1 1^5$. ■

R When using the frequency notation, it is necessary to avoid confusion with products of powers.

Taking advantage the frequency notation, it is easy to determine the generating function of $p(n)$.

Theorem 10.1 Let $p_{\leq N}(n)$ count the number of partitions of n with largest part at most N. We have

$$\sum_{n\geq 0} p_{\leq N}(n)q^n = \prod_{k=1}^{N} \frac{1}{1-q^k}. \tag{10.1}$$

Proof. We expand the multiplicand

$$\frac{1}{1-q^k} = 1+q^k+q^{2k}+q^{3k}+\cdots = q^{0\cdot k}+q^{1\cdot k}+q^{2\cdot k}+q^{3\cdot k}+\cdots.$$

Hence, each term $q^{f_k\cdot k}$ enumerates the case where the frequency of k is f_k for f_k a nonnegative integer. Further, if we expand the infinite product $\prod_{k=1}^{N}\frac{1}{1-q^k}$, its terms are of the form $q^{f_1\cdot 1+f_2\cdot 2+\cdots+f_N\cdot N}$, corresponding to a unique partition with frequency notation $1^{f_1}2^{f_2}\cdots N^{f_N}$, which also restricts the largest part to be at most N. ■

Letting $N\to\infty$, we immediately see that the generating function of $p(n)$ is given by an infinite product.

Theorem 10.2 We have

$$\sum_{n\geq 0} p(n)q^n = \prod_{k\geq 1} \frac{1}{1-q^k}. \tag{10.2}$$

We may also apply some additional restrictions to the parts.

Theorem 10.3 For any positive integers $0<a\leq m$, let $p_{a,m}(n)$ count the number of partitions of n with parts congruent to a modulo m. We have

$$\sum_{n\geq 0} p_{a,m}(n)q^n = \prod_{k\geq 0} \frac{1}{1-q^{km+a}}. \tag{10.3}$$

Proof. Note that

$$\sum_{n\geq 0} p_{a,m}(n)q^n = \prod_{k\geq 0}\left(q^{0\cdot(km+a)}+q^{1\cdot(km+a)}+q^{2\cdot(km+a)}+\cdots\right) = \prod_{k\geq 0}\frac{1}{1-q^{km+a}},$$

as required. ■

Theorem 10.4 For any positive integer s, let $p_{[s]}(n)$ count the number of partitions of n in which each distinct part appears at most s times, i.e., the frequency $f_k\leq s$ for each k. We have

$$\sum_{n\geq 0} p_{[s]}(n)q^n = \prod_{k\geq 1} \frac{1-q^{(s+1)k}}{1-q^k}. \tag{10.4}$$

Proof. Note that

$$\sum_{n\geq 0} p_{[s]}(n)q^n = \prod_{k\geq 1}\left(q^{0\cdot k}+q^{1\cdot k}+\cdots+q^{s\cdot k}\right) = \prod_{k\geq 1}\frac{(1-q^k)\left(1+q+\cdots+q^{sk}\right)}{1-q^k} = \prod_{k\geq 1}\frac{1-q^{(s+1)k}}{1-q^k},$$

as required. ■

10.3 “Odd partitions” vs “Distinct partitions”

Definition 10.3 A partition is called an *odd partition* if all its parts are odd integers, and a partition is called an *even partition* if all its parts are even integers. We denote by $p_o(n)$ the number of odd partitions of n, and by $p_e(n)$ the number of even partitions of n.

Taking $m = 2$, and $a = 1$ and 2, respectively, in Theorem 10.3, we have the following generating function identities.

Theorem 10.5 We have

$$\sum_{n\geq 0} p_o(n)q^n = \prod_{k\geq 1} \frac{1}{1-q^{2k-1}}, \tag{10.5}$$

$$\sum_{n\geq 0} p_e(n)q^n = \prod_{k\geq 1} \frac{1}{1-q^{2k}}. \tag{10.6}$$

Definition 10.4 A partition is called a *distinct partition* if all its parts are pairwise distinct. We denote by $p_D(n)$ the number of distinct partitions of n.

From the proof of Theorem 10.4 with $s = 1$, the following generating function identity holds true.

Theorem 10.6 We have

$$\sum_{n\geq 0} p_D(n)q^n = \prod_{k\geq 1} (1+q^k). \tag{10.7}$$

Euler established a well-known result on odd partitions and distinct partitions.

Theorem 10.7 (Euler). For $n \geq 0$, we have $p_o(n) = p_D(n)$.

Proof. It suffices to show that $p_o(n)$ and $p_D(n)$ have the same generating function:

$$\sum_{n\geq 0} p_o(n)q^n = \prod_{k\geq 1} \frac{1}{1-q^{2k-1}} = \prod_{k\geq 1} \frac{1}{1-q^{2k-1}} \frac{1-q^{2k}}{1-q^{2k}} = \prod_{k\geq 1} \frac{1-q^{2k}}{1-q^k} = \prod_{k\geq 1} (1+q^k) = \sum_{n\geq 0} p_D(n)q^n,$$

as required. ■

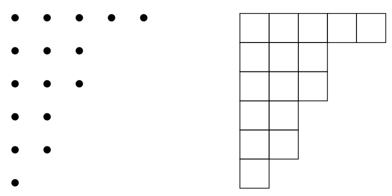
10.4 Ferrers diagrams

We may also represent partitions in a graphical way.

Definition 10.5 A *Ferrers diagram* represents partitions as patterns of dots, with the n-th row having the same number of dots as the n-th part of the partition. If we replace these dots by squares, the graph is often called a *Young diagram*.

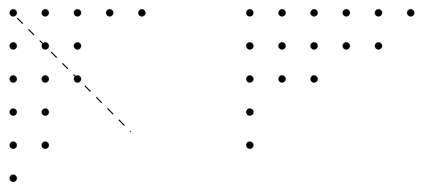
R Ferrers diagrams are named after the British mathematician Norman Macleod Ferrers, and Young diagrams are named after the British mathematician Alfred Young.

■ **Example 10.3** The graphical representations of the partition $5+3+3+2+2+1$ are given as follows — Ferrers diagram (left) and Young diagram (right): ■



Definition 10.6 Given a partition λ, its *conjugate partition*, denoted by λ^{T}, is the partition whose Ferrers diagram is obtained by fliping the diagram of λ along its main diagonal.

■ **Example 10.4** For the partition $\lambda = 5+3+3+2+2+1$, its conjugate is $\lambda^{\mathsf{T}} = 6+5+3+1+1$. ■



Theorem 10.8 Let $p(N,n)$ count the number of partitions of n with at most N parts. We have

$$\sum_{n\geq 0} p(N,n)q^n = \prod_{k=1}^{N} \frac{1}{1-q^k}. \tag{10.8}$$

Proof. Note that for any partition with at most N parts, its conjugate is a partition with largest part at most N. Hence, $p(N,n) = p_{\leq N}(n)$. Recalling Theorem 10.1 gives the desired result. ■

10.5 Euler's summations

Note that the above generating functions are represented in the product form. Now, we introduce the *q-Pochhammer symbols* for notational brevity.

Definition 10.7 Let $q \in \mathbb{C}$ be such that $|q| < 1$. Let $n \in \mathbb{N}$. The *q-Pochhammer symbols* are given by

$$(A;q)_n := \prod_{k=0}^{n-1}(1-Aq^k),$$
$$(A;q)_\infty := \prod_{k\geq 0}(1-Aq^k).$$

We first present refinements of Theorems 10.2 and 10.6.

Theorem 10.9 Let $\mathscr{P}$ be the set of partitions and $\mathscr{D}$ be the set of distinct partitions. We have

$$\sum_{\lambda\in\mathscr{P}} z^{\ell(\lambda)}q^{|\lambda|} = \frac{1}{(zq;q)_\infty}, \tag{10.9}$$
$$\sum_{\lambda\in\mathscr{D}} z^{\ell(\lambda)}q^{|\lambda|} = (-zq;q)_\infty. \tag{10.10}$$

Proof. We have

$$\sum_{\lambda\in\mathscr{P}} z^{\ell(\lambda)}q^{|\lambda|} = \prod_{k\geq 1}\left(1+zq^k+z^2q^{2k}+\cdots\right) = \prod_{k\geq 1}\frac{1}{1-zq^k} = \frac{1}{(zq;q)_\infty}.$$

Similarly,

$$\sum_{\lambda\in\mathscr{D}} z^{\ell(\lambda)}q^{|\lambda|} = \prod_{k\geq 1}\left(1+zq^k\right) = (-zq;q)_\infty,$$

as required. ■

Now, our objective is two important summation formulas due to Euler.

Theorem 10.10 (Euler's Summations). We have

$$\sum_{k\geq 0}\frac{z^kq^k}{(q;q)_k}=\frac{1}{(zq;q)_\infty}, \tag{10.11}$$

$$\sum_{k\geq 0}\frac{z^kq^{\frac{k(k+1)}{2}}}{(q;q)_k}=(-zq;q)_\infty. \tag{10.12}$$

Proof. For Euler's first summation, we consider partitions $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_k)\in\mathscr{P}$ with exactly k parts. Then $\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_k\geq 1$. Now, we construct a new partition $\lambda'=(\lambda'_1,\lambda'_2,\ldots,\lambda'_k)$ with $\lambda'_i=\lambda_i-1$. Noting that $\lambda'_1\geq\lambda'_2\geq\cdots\geq\lambda'_k\geq 0$, we find that λ' is a partition with at most k parts. Since $|\lambda|=|\lambda'|+k$, we have

$$\sum_{\lambda\in\mathscr{P}}z^{\ell(\lambda)}q^{|\lambda|}=\sum_{k\geq 0}z^kq^k\sum_{n\geq 0}p(k,n)q^n=\sum_{k\geq 0}\frac{z^kq^k}{(q;q)_k},$$

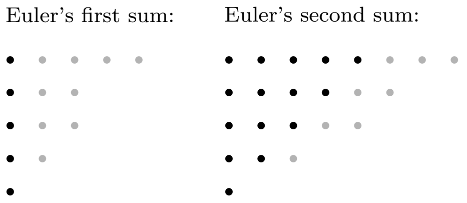
where we make use of Theorem 10.8. Recalling (10.9) gives what we want.

For Euler's second summation, we consider partitions $\pi=(\pi_1,\pi_2,\ldots,\pi_k)\in\mathscr{D}$ with exactly k parts. Then $\pi_1>\pi_2>\cdots>\pi_k\geq 1$. Now, we construct a new partition $\pi'=(\pi'_1,\pi'_2,\ldots,\pi'_k)$ with $\pi'_i=\pi_i-(k+1-i)$. Noting that $\pi'_1\geq\pi'_2\geq\cdots\geq\pi'_k\geq 0$, we find that π' is a partition with at most k parts. Since $|\pi|=|\pi'|+(1+2+\cdots+k)=|\pi'|+\frac{k(k+1)}{2}$, we have

$$\sum_{\pi\in\mathscr{D}}z^{\ell(\pi)}q^{|\pi|}=\sum_{k\geq 0}z^kq^{\frac{k(k+1)}{2}}\sum_{n\geq 0}p(k,n)q^n=\sum_{k\geq 0}\frac{z^kq^{\frac{k(k+1)}{2}}}{(q;q)_k},$$

where we also use Theorem 10.8. Recalling (10.10) implies the desired result. ■

The above proof can also be understood graphically.



Euler's first sum:

Euler's second sum:

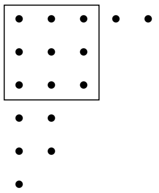
10.6 Durfee squares

From the Ferrers diagram of a partition, another important concept can be introduced.

Definition 10.8 Given a partition, its *Durfee square* is the largest square contained in its Ferrers diagram.

Durfee squares are named after the American mathematician William Pitt Durfee, a student of James Joseph Sylvester.

Example 10.5 The partition $5+3+3+2+2+1$ has a Durfee square of size 3, as shown in the Ferrers diagram.



Theorem 10.11 We have

$$\sum_{k\geq 0}\frac{q^{k^2}}{(q;q)_k^2}=\frac{1}{(q;q)_\infty}. \tag{10.13}$$

Proof. We consider partitions λ whose Durfee square is of size k. Note that below the Durfee square, we have a partition μ with largest part at most k; and that to the right of the Durfee square, we have a partition ν with at most k parts. Since $|\lambda|=|\mu|+|\nu|+k^2$ where k^2 is contributed by the Durfee square, we have

$$\sum_{\lambda\in\mathscr{P}}q^{|\lambda|}=\sum_{k\geq 0}q^{k^2}\sum_{n\geq 0}p_{\leq k}(n)q^n\sum_{n\geq 0}p(k,n)q^n=\sum_{k\geq 0}\frac{q^{k^2}}{(q;q)_k^2},$$

where we use Theorems 10.1 and 10.8. The desired identity follows from Theorem 10.2. ∎

11. Basic q-series

11.1 q-Binomial series

We start with an identity due to the French mathematician Augustin-Louis Cauchy, which is also known as the *q-binomial series*.

Theorem 11.1 (q-Binomial Series). For $|q| < 1$ and $|t| < 1$,

$$\sum_{n\geq 0} \frac{(a;q)_n t^n}{(q;q)_n} = \frac{(at;q)_\infty}{(t;q)_\infty}. \tag{11.1}$$

R Taking $a = q^\alpha$ in (11.1) with α a positive integer gives $\sum_{n\geq 0} \frac{(q^\alpha;q)_n t^n}{(q;q)_n} = \frac{1}{(t;q)_\alpha}$. Further letting $q \to 1^-$ implies that

$$\sum_{n\geq 0} \binom{\alpha+n-1}{n} t^n = (1-t)^{-\alpha}.$$

This provides an instance of the binomial theorem for negative powers.

Proof. Let us define

$$F(t) := \frac{(at;q)_\infty}{(t;q)_\infty}.$$

Note that as a function of t, $F(t)$ is analytic inside $|t| < 1$. Hence, we may expand $F(t)$ as a power series in t, i.e.,

$$F(t) = \sum_{n\geq 0} f_n t^n.$$

Clearly, $f_0 = F(0) = 1$. Further, we have

$$F(tq) = \frac{(atq;q)_\infty}{(tq;q)_\infty} = \frac{1-t}{1-at} \cdot \frac{(at;q)_\infty}{(t;q)_\infty} = \frac{1-t}{1-at} \cdot F(t).$$

Since $F(tq) = \sum_{n\geq 0} f_n (tq)^n = \sum_{n\geq 0} \big(f_n q^n\big) t^n$, it follows that

$$(1-at) \sum_{n\geq 0} \big(f_n q^n\big) t^n = (1-t) \sum_{n\geq 0} f_n t^n.$$

Hence, for $n \geq 1$, we equate the coefficients of q^n on both sides of the above and obtain

$$f_n q^n - a f_{n-1} q^{n-1} = f_n - f_{n-1},$$

or

$$f_n = \frac{1 - aq^{n-1}}{1 - q^n} \cdot f_{n-1}.$$

Iterating the above gives

$$f_n = \frac{(a;q)_n}{(q;q)_n}$$

for $n \geq 1$. Substituting the above together with $f_0 = 1$ back to $F(t) = \sum_{n \geq 0} f_n t^n$ confirms the required result. ■

R Euler's summations (10.11) and (10.12) are indeed special cases of the q-binomial series (11.1). For (10.11), we simply take $a = 0$ and $t = zq$ in (11.1), and note that for $n \in \mathbb{N} \cup \{\infty\}$, $(0;q)_n = (1-0)(1-0\cdot q)\cdots(1-0\cdot q^{n-1}) = 1$. For (10.12), we need the following trickier observation: for any nonnegative integer n,

$$\lim_{\tau \to 0} (a/\tau;q)_n \tau^n = \lim_{\tau \to 0} \tau^n \prod_{k=0}^{n-1} \left(1 - aq^k/\tau\right) = \lim_{\tau \to 0} \prod_{k=0}^{n-1} \left(\tau - aq^k\right) = \prod_{k=0}^{n-1} \left(-aq^k\right) = (-a)^n q^{\frac{n(n-1)}{2}}.$$

Now, in (11.1), we take $a \mapsto -zq/t$ and then let $t \to 0$. Therefore, (10.12) follows.

11.2 Heine's transformations

The q-binomial series serves as a key to many basic hypergeometric identities. Among these, *Heine's fundamental transformations* are of substantial significance.

Theorem 11.2 (Heine's Transformations). Let $|q| < 1$ and $|t| < 1$. For $|b| < 1$,

$$\sum_{n \geq 0} \frac{(a;q)_n (b;q)_n t^n}{(q;q)_n (c;q)_n} = \frac{(b;q)_\infty (at;q)_\infty}{(c;q)_\infty (t;q)_\infty} \sum_{n \geq 0} \frac{(c/b;q)_n (t;q)_n b^n}{(q;q)_n (at;q)_n}; \tag{11.2}$$

For $|c| < |b|$,

$$\sum_{n \geq 0} \frac{(a;q)_n (b;q)_n t^n}{(q;q)_n (c;q)_n} = \frac{(c/b;q)_\infty (bt;q)_\infty}{(c;q)_\infty (t;q)_\infty} \sum_{n \geq 0} \frac{(abt/c;q)_n (b;q)_n (c/b)^n}{(q;q)_n (bt;q)_n}; \tag{11.3}$$

For $|abt| < |c|$,

$$\sum_{n \geq 0} \frac{(a;q)_n (b;q)_n t^n}{(q;q)_n (c;q)_n} = \frac{(abt/c;q)_\infty}{(t;q)_\infty} \sum_{n \geq 0} \frac{(c/a;q)_n (c/b;q)_n (abt/c)^n}{(q;q)_n (c;q)_n}. \tag{11.4}$$

R These transformation formulas were first studied by the German mathematician Eduard Heine (*J. Reine Angew. Math.* **32** (1846), 210–212).

Proof. We begin with a trivial observation that for any nonnegative integer n,

$$\frac{(\alpha;q)_n}{(\beta;q)_n} = \frac{(\alpha;q)_\infty}{(\beta;q)_\infty} \frac{(\beta q^n;q)_\infty}{(\alpha q^n;q)_\infty}.$$

Now, for (11.2), we have

$$\begin{aligned}
\sum_{n\geq 0}\frac{(a;q)_n(b;q)_nt^n}{(q;q)_n(c;q)_n} &= \frac{(b;q)_\infty}{(c;q)_\infty}\sum_{n\geq 0}\frac{(a;q)_nt^n}{(q;q)_n}\cdot\frac{(cq^n;q)_\infty}{(bq^n;q)_\infty}\\
\text{(by (11.1))} &= \frac{(b;q)_\infty}{(c;q)_\infty}\sum_{n\geq 0}\frac{(a;q)_nt^n}{(q;q)_n}\sum_{m\geq 0}\frac{(c/b;q)_m(bq^n)^m}{(q;q)_m}\\
&= \frac{(b;q)_\infty}{(c;q)_\infty}\sum_{m\geq 0}\frac{(c/b;q)_mb^m}{(q;q)_m}\sum_{n\geq 0}\frac{(a;q)_n(tq^m)^n}{(q;q)_n}\\
\text{(by (11.1))} &= \frac{(b;q)_\infty}{(c;q)_\infty}\sum_{m\geq 0}\frac{(c/b;q)_mb^m}{(q;q)_m}\cdot\frac{(atq^m;q)_\infty}{(tq^m;q)_\infty}\\
&= \frac{(b;q)_\infty}{(c;q)_\infty}\frac{(at;q)_\infty}{(t;q)_\infty}\sum_{m\geq 0}\frac{(c/b;q)_mb^m}{(q;q)_m}\cdot\frac{(t;q)_m}{(at;q)_m},
\end{aligned}$$

as required. For (11.3), we first take $(a,b,c,t)\mapsto(t,c/b,at,b)$ in (11.2). Then

$$\sum_{n\geq 0}\frac{(t;q)_n(c/b;q)_nb^n}{(q;q)_n(at;q)_n} = \frac{(c/b;q)_\infty(bt;q)_\infty}{(at;q)_\infty(b;q)_\infty}\sum_{n\geq 0}\frac{(abt/c;q)_n(b;q)_n(c/b)^n}{(q;q)_n(bt;q)_n}.$$

Substituting the above into the right-hand side of (11.2) gives

$$\sum_{n\geq 0}\frac{(a;q)_n(b;q)_nt^n}{(q;q)_n(c;q)_n} = \frac{(b;q)_\infty(at;q)_\infty}{(c;q)_\infty(t;q)_\infty}\cdot\frac{(c/b;q)_\infty(bt;q)_\infty}{(at;q)_\infty(b;q)_\infty}\sum_{n\geq 0}\frac{(abt/c;q)_n(b;q)_n(c/b)^n}{(q;q)_n(bt;q)_n},$$

which is exactly (11.3). Finally, for (11.4), we take $(a,b,c,t)\mapsto(b,abt/c,bt,c/b)$ in (11.2). Then

$$\sum_{n\geq 0}\frac{(b;q)_n(abt/c;q)_n(c/b)^n}{(q;q)_n(bt;q)_n} = \frac{(abt/c;q)_\infty(c;q)_\infty}{(bt;q)_\infty(c/b;q)_\infty}\sum_{n\geq 0}\frac{(c/a;q)_n(c/b;q)_n(abt/c)^n}{(q;q)_n(c;q)_n}.$$

Substituting the above into the right-hand side of (11.3) gives

$$\sum_{n\geq 0}\frac{(a;q)_n(b;q)_nt^n}{(q;q)_n(c;q)_n} = \frac{(c/b;q)_\infty(bt;q)_\infty}{(c;q)_\infty(t;q)_\infty}\cdot\frac{(abt/c;q)_\infty(c;q)_\infty}{(bt;q)_\infty(c/b;q)_\infty}\sum_{n\geq 0}\frac{(c/a;q)_n(c/b;q)_n(abt/c)^n}{(q;q)_n(c;q)_n},$$

thereby confirming (11.4). ■

As an important consequence of Heine's transformations, we have the q-Gauss summation.

Corollary 11.3 (q-Gauss Summation). For $|q|<1$ and $|c|<|ab|$,

$$\sum_{n\geq 0}\frac{(a;q)_n(b;q)_n}{(q;q)_n(c;q)_n}\left(\frac{c}{ab}\right)^n = \frac{(c/a;q)_\infty(c/b;q)_\infty}{(c;q)_\infty(c/(ab);q)_\infty}. \tag{11.5}$$

Proof. In Heine's first transformation (11.2), we take $t\mapsto c/(ab)$. Then

$$\begin{aligned}
\sum_{n\geq 0}\frac{(a;q)_n(b;q)_n}{(q;q)_n(c;q)_n}\left(\frac{c}{ab}\right)^n &= \frac{(b;q)_\infty(c/b;q)_\infty}{(c;q)_\infty(c/(ab);q)_\infty}\sum_{n\geq 0}\frac{(c/b;q)_n(c/(ab);q)_nb^n}{(q;q)_n(c/b;q)_n}\\
&= \frac{(b;q)_\infty(c/b;q)_\infty}{(c;q)_\infty(c/(ab);q)_\infty}\sum_{n\geq 0}\frac{(c/(ab);q)_nb^n}{(q;q)_n}\\
\text{(by (11.1))} &= \frac{(b;q)_\infty(c/b;q)_\infty}{(c;q)_\infty(c/(ab);q)_\infty}\cdot\frac{(c/a;q)_\infty}{(b;q)_\infty},
\end{aligned}$$

which leads to the required identity. ■

R It is worth pointing out that (10.13) is a special case of the q-Gauss summation by first taking $(a,b,c)\mapsto(1/\tau,1/\tau,q)$ in (11.5) and then letting $\tau\to 0$.

11.3 Jacobi's triple product identity

Let us recall Euler's two summation formulas (10.11) and (10.11) with $z\mapsto z/q$:

$$\sum_{k\geq 0}\frac{z^k}{(q;q)_k}=\frac{1}{(z;q)_\infty},\tag{11.6}$$

$$\sum_{k\geq 0}\frac{z^k q^{\frac{k(k-1)}{2}}}{(q;q)_k}=(-z;q)_\infty.\tag{11.7}$$

From the discussion in the final remark in §11.1, we see that under the assumption of $|q|<1$, (11.6) is true for $|z|<1$ and (11.7) is true for general z.

Now, we shall use them to prove one of the most important q-series identities — *Jacobi's triple product identity*, named after the German mathematician Carl Gustav Jacob Jacobi.

Theorem 11.4 (Jacobi's Triple Product Identity). For $|q|<1$ and $z\neq 0$,

$$\sum_{n=-\infty}^{\infty}(-z)^n q^{\frac{n(n-1)}{2}}=(z;q)_\infty(q/z;q)_\infty(q;q)_\infty.\tag{11.8}$$

Proof. We start with (11.7) and deduce that

$$(-z;q)_\infty=\sum_{k\geq 0}\frac{z^k q^{\frac{k(k-1)}{2}}}{(q;q)_k}=\frac{1}{(q;q)_\infty}\sum_{k\geq 0}z^k q^{\frac{k(k-1)}{2}}(q^{k+1};q)_\infty.$$

Note that for j a nonpositive integer, in $(q^j;q)_\infty=(1-q^j)(1-q^{j+1})\cdots$, one of the factors is $(1-q^0)=(1-1)=0$. Hence, $(q^j;q)_\infty=0$ for any nonpositive integer j. It follows that

$$\begin{aligned}
(-z;q)_\infty&=\frac{1}{(q;q)_\infty}\sum_{k=-\infty}^{\infty}z^k q^{\frac{k(k-1)}{2}}(q^{k+1};q)_\infty\\
(\text{by (11.7)})&=\frac{1}{(q;q)_\infty}\sum_{k=-\infty}^{\infty}z^k q^{\frac{k(k-1)}{2}}\sum_{\ell\geq 0}\frac{(-q^{k+1})^\ell q^{\frac{\ell(\ell-1)}{2}}}{(q;q)_\ell}\\
&=\frac{1}{(q;q)_\infty}\sum_{k=-\infty}^{\infty}\sum_{\ell\geq 0}\frac{(-1)^\ell\cdot z^k\cdot q^{\frac{\ell(\ell-1)}{2}+\frac{k(k-1)}{2}+(k+1)\ell}}{(q;q)_\ell}\\
&=\frac{1}{(q;q)_\infty}\sum_{k=-\infty}^{\infty}\sum_{\ell\geq 0}\frac{(-1)^\ell\cdot z^k\cdot q^{\frac{(\ell+k)(\ell+k-1)}{2}+\ell}}{(q;q)_\ell}\\
&=\frac{1}{(q;q)_\infty}\sum_{\ell\geq 0}\frac{(-1)^\ell z^{-\ell}q^\ell}{(q;q)_\ell}\sum_{k=-\infty}^{\infty}z^{\ell+k}q^{\frac{(\ell+k)(\ell+k-1)}{2}}\\
(\text{with } n=\ell+k)&=\frac{1}{(q;q)_\infty}\sum_{\ell\geq 0}\frac{(-1)^\ell z^{-\ell}q^\ell}{(q;q)_\ell}\sum_{n=-\infty}^{\infty}z^n q^{\frac{n(n-1)}{2}}\\
(\text{by (11.6)})&=\frac{1}{(q;q)_\infty}\frac{1}{(-q/z;q)_\infty}\sum_{n=-\infty}^{\infty}z^n q^{\frac{n(n-1)}{2}}.
\end{aligned}$$

Note that in the last equality, we should require $|q/z|<1$, or $|z|>|q|$ to pertain absolute convergence. However, the entire argument can be carried out again with z replaced by

q/z. Namely, for $0<|z|<1$,

$$(-q/z;q)_\infty = \frac{1}{(q;q)_\infty(-z;q)_\infty}\sum_{n=-\infty}^{\infty} z^{-n}q^{\frac{n(n+1)}{2}} = \frac{1}{(q;q)_\infty(-z;q)_\infty}\sum_{n=-\infty}^{\infty} z^{n}q^{\frac{n(n-1)}{2}}.$$

Further, $\{z:|z|>|q|\}\cup\{z:0<|z|<1\}=\mathbb{C}\backslash\{0\}$ since $|q|<1$. We remark that a simpler way to get rid of the requirement that $|z|>|q|$ is by invoking analytic continuation. Finally, we derive from the above that for $z\neq 0$,

$$\sum_{n=-\infty}^{\infty} z^n q^{\frac{n(n-1)}{2}} = (-z;q)_\infty(-q/z;q)_\infty(q;q)_\infty,$$

thereby yielding the desired result by setting $z\mapsto -z$. ■

A direct consequence of Jacobi's triple product identity is *Euler's pentagonal number theorem*.

Corollary 11.5 (Euler's Pentagonal Number Theorem). For $|q|<1$,

$$\sum_{n=-\infty}^{\infty}(-1)^n q^{\frac{n(3n-1)}{2}} = (q;q)_\infty. \tag{11.9}$$

Proof. In (11.8), we take $(z,q)\mapsto(q,q^3)$. Noting that $(q;q^3)_\infty(q^2;q^3)_\infty(q^3;q^3)_\infty=(q;q)_\infty$, we arrive at the desired result. ■

11.4 Ramanujan's theta function

An important object in the theory of q-series is the theta function introduced by the Indian mathematician Srinivasa Ramanujan.

Definition 11.1 *Ramanujan's general theta function* is defined as

$$f(a,b) := \sum_{n=-\infty}^{\infty} a^{\frac{n(n+1)}{2}} b^{\frac{n(n-1)}{2}} \qquad (|ab|<1). \tag{11.10}$$

Theorem 11.6 For $|ab|<1$,

$$f(a,b) = (-a;ab)_\infty(-b;ab)_\infty(ab;ab)_\infty. \tag{11.11}$$

Proof. This is (11.8) with $(z,q)\mapsto(-a,ab)$. ■

Two special cases of the general theta function are of particular interest.

Definition 11.2 *Ramanujan's classical theta functions* are defined as

$$\phi(q) := \sum_{n=-\infty}^{\infty} q^{n^2}, \tag{11.12}$$

$$\psi(q) := \sum_{n\geq 0} q^{\frac{n(n+1)}{2}}. \tag{11.13}$$

Theorem 11.7 We have

$$\phi(q) = \frac{(q^2;q^2)_\infty^5}{(q;q)_\infty^2(q^4;q^4)_\infty^2}, \tag{11.14}$$

$$\psi(q) = \frac{(q^2;q^2)_\infty^2}{(q;q)_\infty}, \tag{11.15}$$

$$\phi(-q) = \frac{(q;q)_\infty^2}{(q^2;q^2)_\infty}, \tag{11.16}$$

$$\psi(-q) = \frac{(q;q)_\infty(q^4;q^4)_\infty}{(q^2;q^2)_\infty}. \tag{11.17}$$

Proof. For (11.14), we take $(z,q) \mapsto (-q,q^2)$ in (11.8), and derive that

$$\begin{aligned}\phi(q) = \sum_{n=-\infty}^{\infty} q^{n^2} &= (-q;q^2)_\infty^2 (q^2;q^2)_\infty = \frac{(q^2;q^4)_\infty^2}{(q;q^2)_\infty^2}(q^2;q^2)_\infty \\ &= \frac{(q^2;q^2)_\infty^2}{(q^4;q^4)_\infty^2}\frac{(q^2;q^2)_\infty^2}{(q;q)_\infty^2}(q^2;q^2)_\infty,\end{aligned}$$

as required. For (11.15), we first show that

$$\sum_{n\ge 0} q^{\frac{n(n+1)}{2}} = \sum_{n=-\infty}^{\infty} q^{2n^2+n}.$$

To see this, for the left-hand side, we distinguish the parity of n and write n as $2k$ and $2k+1$ with $k \ge 0$. On the other hand, for the right-hand side, we separate n into k and $-k-1$, also with $k \ge 0$. Then

$$\sum_{n\ge 0} q^{\frac{n(n+1)}{2}} = \sum_{k\ge 0} q^{\frac{(2k)(2k+1)}{2}} + \sum_{k\ge 0} q^{\frac{(2k+1)(2k+2)}{2}} = \sum_{k\ge 0} q^{k(2k+1)} + \sum_{k\ge 0} q^{(k+1)(2k+1)}$$

and

$$\sum_{n=-\infty}^{\infty} q^{2n^2+n} = \sum_{k\ge 0} q^{2k^2+k} + \sum_{k\ge 0} q^{2(-k-1)^2+(-k-1)} = \sum_{k\ge 0} q^{k(2k+1)} + \sum_{k\ge 0} q^{(k+1)(2k+1)},$$

and thus they are equal. Now, we take $(z,q) \mapsto (-q^3,q^4)$ in (11.8), and derive that

$$\begin{aligned}\psi(q) = \sum_{n\ge 0} q^{\frac{n(n+1)}{2}} = \sum_{n=-\infty}^{\infty} q^{2n^2+n} &= (-q;q^4)_\infty(-q^3;q^4)_\infty(q^4;q^4)_\infty \\ &= (-q;q^2)_\infty(q^4;q^4)_\infty = \frac{(q^2;q^4)_\infty}{(q;q^2)_\infty}(q^4;q^4)_\infty \\ &= \frac{(q^2;q^2)_\infty}{(q^4;q^4)_\infty}\frac{(q^2;q^2)_\infty}{(q;q)_\infty}(q^4;q^4)_\infty,\end{aligned}$$

as required. Finally, for (11.16) and (11.17), we note that

$$\begin{aligned}(-q;-q)_\infty &= (1+q)(1-q^2)(1+q^3)(1-q^4)\cdots \\ &= (-q;q^2)_\infty(q^2;q^2)_\infty = \frac{(q^2;q^2)_\infty^3}{(q;q)_\infty(q^4;q^4)_\infty}.\end{aligned}$$

Taking $q \mapsto -q$ in (11.14) and (11.15), and making use of the above relation, the desired results follow. ■

12. Sums of squares (II)

12.1 Jacobi's identity

Here, we record another important implication of Jacobi's triple product identity.

Theorem 12.1 (Jacobi's identity). For $|q| < 1$,

$$\sum_{n\geq 0}(-1)^n(2n+1)q^{\frac{n(n+1)}{2}} = (q;q)_\infty^3. \tag{12.1}$$

Proof. Recall (11.8):

$$(z;q)_\infty(z^{-1}q;q)_\infty(q;q)_\infty = \sum_{n=-\infty}^{\infty}(-z)^n q^{\frac{n(n-1)}{2}}.$$

Note that the product side can be rewritten as

$$(z;q)_\infty(z^{-1}q;q)_\infty(q;q)_\infty = -(z-1)(zq;q)_\infty(z^{-1}q;q)_\infty(q;q)_\infty.$$

For the sum side, we first change n to $-n$, and then distinguish n as k and $-k-1$ with $k \geq 0$:

$$\begin{aligned}\sum_{n=-\infty}^{\infty}(-z)^n q^{\frac{n(n-1)}{2}} &= \sum_{n=-\infty}^{\infty}(-1)^n z^{-n} q^{\frac{n(n+1)}{2}}\\ &= \sum_{k\geq 0}(-1)^k z^{-k} q^{\frac{k(k+1)}{2}} - \sum_{k\geq 0}(-1)^k z^{k+1} q^{\frac{k(k+1)}{2}}\\ &= -\sum_{k\geq 0}(-1)^k\left(z^{k+1}-z^{-k}\right)q^{\frac{k(k+1)}{2}}.\end{aligned}$$

Hence,

$$(z-1)(zq;q)_\infty(z^{-1}q;q)_\infty(q;q)_\infty = \sum_{k\geq 0}(-1)^k\left(z^{k+1}-z^{-k}\right)q^{\frac{k(k+1)}{2}}.$$

Now, note that $z^{k+1}-z^{-k} = (z-1)(z^k+z^{k-1}+\cdots+z^{-k})$. We then divide by $z-1$ on both sides of the above and obtain

$$(zq;q)_\infty(z^{-1}q;q)_\infty(q;q)_\infty = \sum_{k\geq 0}(-1)^k\left(z^k+z^{k-1}+\cdots+z^{-k}\right)q^{\frac{k(k+1)}{2}}.$$

Finally, taking $z=1$ gives the desired result. ■

12.2 Lambert series

Definition 12.1 Let k be a fixed positive integer. For n a natural number, we denote by $r_k(n)$ the number of representations of n as $m_1^2+m_2^2+\cdots+m_k^2$ with m_i an integer for each i, where representations differing only in the sign or order of the m are reckoned as distinct.

Example 12.1 We can represent 5 as

$$\begin{array}{cccc} 1^2+2^2, & (-1)^2+2^2, & 1^2+(-2)^2, & (-1)^2+(-2)^2, \\ 2^2+1^2, & 2^2+(-1)^2, & (-2)^2+1^2, & (-2)^2+(-1)^2. \end{array}$$

Hence, $r_2(5)=8$. ■

Theorem 12.2 Let $\phi(q)$ be Ramanujan's theta function as in (11.12). We have

$$1+\sum_{n\geq 1} r_k(n)q^n = \phi(q)^k. \tag{12.2}$$

Proof. This is a direct consequence of $\phi(q)=\sum_{n=-\infty}^{\infty} q^{n^2}$. ■

Now, our objective is to derive explicit formulas for $r_2(n)$ and $r_4(n)$. For this purpose, we require the knowledge of Lambert series, named for Johann Heinrich Lambert.

Definition 12.2 A *Lambert series* is of the form

$$\sum_{k\geq 1} \frac{a_k q^k}{1-q^k},$$

where $\{a_k\}_{k\geq 1}$ is a sequence of complex numbers.

Theorem 12.3 Let

$$\sum_{n\geq 1} u_n q^n = \sum_{\substack{k\geq 1 \\ k\equiv r \text{ mod } m}} \frac{a_k q^k}{1-q^k}.$$

Then

$$u_n = \sum_{\substack{d|n \\ d\equiv r \text{ mod } m}} a_d. \tag{12.3}$$

Proof. We expand the summand

$$\frac{a_k q^k}{1-q^k} = a_k\left(q^k+q^{2k}+q^{3k}+\cdots\right).$$

Note that q^n appears in this series if and only if $k \mid n$. Since we are summing over all positive integers k with $k\equiv r \pmod m$ in the Lambert series, then to compute the coefficient u_n, we need to take into account all positive divisors d of n with $d\equiv r \pmod m$. ■

Lemma 12.4 We have

$$\frac{d}{dx}\prod_k f_k(x) = \left(\prod_k f_k(x)\right)\cdot\sum_k\left(\frac{1}{f_k(x)}\cdot\frac{d}{dx}f_k(x)\right). \tag{12.4}$$

Proof. Let $F(x) = \prod_k f_k(x)$. Note that $\frac{d}{dx}\log F(x) = \frac{F'(x)}{F(x)}$, where $F'(x)$ denotes the derivative of $F(x)$. Hence,

$$F'(x) = F(x)\cdot\frac{d}{dx}\log F(x) = F(x)\cdot\frac{d}{dx}\sum_k \log f_k(x) = F(x)\cdot\sum_k\frac{d}{dx}\log f_k(x) = F(x)\cdot\sum_k\frac{f_k'(x)}{f_k(x)},$$

as required. ■

R This lemma allows us to connect q-Pochhammer symbols with Lambert series through differentiation. For instance,

$$q\cdot\frac{d}{dq}(q;q)_\infty = q\cdot\frac{d}{dq}\prod_{k\geq1}(1-q^k) = q(q;q)_\infty\sum_{k\geq1}\frac{-kq^{k-1}}{1-q^k} = -(q;q)_\infty\sum_{k\geq1}\frac{kq^k}{1-q^k}.$$

12.3 Jacobi's two-square formula

Theorem 12.5 (Jacobi's Two-Square Formula). For $n\geq1$,

$$r_2(n) = 4\left(\sum_{\substack{d\mid n\\ d\equiv1 \bmod 4}}1 - \sum_{\substack{d\mid n\\ d\equiv3 \bmod 4}}1\right). \tag{12.5}$$

Proof. We begin with Jacobi's identity (12.1):

$$\begin{aligned}(q;q)_\infty^3 &= \sum_{n\geq0}(-1)^n(2n+1)q^{\frac{n(n+1)}{2}} = \sum_{k\geq0}(4k+1)q^{\frac{(2k)(2k+1)}{2}} - \sum_{k\geq0}(4k+3)q^{\frac{(2k+1)(2k+2)}{2}}\\ &= \sum_{k\geq0}(4k+1)q^{2k^2+k} + \sum_{k\geq0}\left(4(-k-1)+1\right)q^{2(-k-1)^2+(-k-1)}\\ &= \sum_{n=-\infty}^{\infty}(4n+1)q^{2n^2+n}.\end{aligned}$$

Hence,

$$\begin{aligned}(q;q)_\infty^3 &= \left[\frac{d}{dz}\left(\sum_{n=-\infty}^{\infty}z^{4n+1}q^{2n^2+n}\right)\right]_{z=1}\\ \text{(by (11.8))} &= \left[\frac{d}{dz}\left(z(-z^{-4}q;q^4)_\infty(-z^4q^3;q^4)_\infty(q^4;q^4)_\infty\right)\right]_{z=1}\\ \text{(by (12.4))} &= (-q;q^4)_\infty(-q^3;q^4)_\infty(q^4;q^4)_\infty\left(1-\sum_{\substack{k\geq1\\ k\equiv1 \bmod 4}}\frac{4q^k}{1-q^k}+\sum_{\substack{k\geq1\\ k\equiv3 \bmod 4}}\frac{4q^k}{1-q^k}\right).\end{aligned}$$

In the proof of Theorem 11.7, we have shown that $\psi(q) = (-q;q^4)_\infty(-q^3;q^4)_\infty(q^4;q^4)_\infty$. Recalling (11.15) and (11.16), we have

$$\phi(-q)^2 = 1-\sum_{\substack{k\geq1\\ k\equiv1 \bmod 4}}\frac{4q^k}{1-q^k}+\sum_{\substack{k\geq1\\ k\equiv3 \bmod 4}}\frac{4q^k}{1-q^k}.$$

Now, we take $q \mapsto -q$ and derive that

$$\phi(q)^2 = 1 + \sum_{\substack{k\ge 1\\ k\equiv 1 \bmod 4}} \frac{4q^k}{1-q^k} - \sum_{\substack{k\ge 1\\ k\equiv 3 \bmod 4}} \frac{4q^k}{1-q^k}.$$

Finally, the required result follows by using (12.2) and (12.3). ■

R This proof comes from an unpublished work of the Australian mathematician Michael Hirschhorn. See also Hirschhorn's monograph *The power of q*, Sect. 2.3.

12.4 Jacobi's four-square formula

Theorem 12.6 (Jacobi's Four-Square Formula). For $n \ge 1$,

$$r_4(n) = 8 \sum_{\substack{d\mid n\\ d\not\equiv 0 \bmod 4}} d. \tag{12.6}$$

For its proof, we need a reformulation of $(q;q)_\infty^6$.

Lemma 12.7 We have

$$(q;q)_\infty^6 = \frac{1}{2}\sum_{s=-\infty}^{\infty} q^{s^2} \sum_{r=-\infty}^{\infty} (2r+1)^2 q^{r^2+r} - \frac{1}{2}\sum_{r=-\infty}^{\infty} q^{r^2+r} \sum_{s=-\infty}^{\infty} (2s)^2 q^{s^2}. \tag{12.7}$$

Proof. We note from Jacobi's identity (12.1) that

$$\begin{aligned}
&\sum_{n=-\infty}^{\infty} (-1)^n(2n+1)q^{\frac{n(n+1)}{2}}\\
&\quad= \sum_{n\ge 0}(-1)^n(2n+1)q^{\frac{n(n+1)}{2}} + \sum_{n<0}(-1)^n(2n+1)q^{\frac{n(n+1)}{2}}\\
&\quad= \sum_{n\ge 0}(-1)^n(2n+1)q^{\frac{n(n+1)}{2}} + \sum_{n\ge 0}(-1)^{-n-1}\big(2(-n-1)+1\big)q^{\frac{(-n-1)((-n-1)+1)}{2}}\\
&\quad= 2\sum_{n\ge 0}(-1)^n(2n+1)q^{\frac{n(n+1)}{2}}\\
&\quad= 2(q;q)_\infty^3.
\end{aligned}$$

Hence,

$$(q;q)_\infty^6 = \frac{1}{4}\sum_{m,n=-\infty}^{\infty} (-1)^{m+n}(2m+1)(2n+1)q^{\frac{m(m+1)}{2}+\frac{n(n+1)}{2}}.$$

We may further split the sum in two parts, according to whether m and n have the same parity or not, and obtain

$$\begin{aligned}
(q;q)_\infty^6 = \frac{1}{4}&\sum_{\substack{m,n=-\infty\\ m\equiv n \bmod 2}}^{\infty} (2m+1)(2n+1)q^{\frac{m(m+1)}{2}+\frac{n(n+1)}{2}}\\
&- \frac{1}{4}\sum_{\substack{m,n=-\infty\\ m\not\equiv n \bmod 2}}^{\infty} (2m+1)(2n+1)q^{\frac{m(m+1)}{2}+\frac{n(n+1)}{2}}.
\end{aligned}$$

For the first sum,

$$\sum_{\substack{m,n=-\infty\\ m\equiv n \bmod 2}}^{\infty} (2m+1)(2n+1)q^{\frac{m(m+1)}{2}+\frac{n(n+1)}{2}},$$

we make the following change of variables (so that r and s run over all integers):

$$\begin{cases} r=\frac{m+n}{2}\\ s=\frac{m-n}{2}\end{cases} \iff \begin{cases} m=r+s\\ n=r-s\end{cases}.$$

Similarly, for the second sum,

$$\sum_{\substack{m,n=-\infty\\ m\not\equiv n \bmod 2}}^{\infty} (2m+1)(2n+1)q^{\frac{m(m+1)}{2}+\frac{n(n+1)}{2}},$$

we make another change of variables:

$$\begin{cases} r=\frac{m-n-1}{2}\\ s=\frac{m+n+1}{2}\end{cases} \iff \begin{cases} m=r+s\\ n=s-r-1\end{cases}.$$

Thus,

$$\begin{aligned}(q;q)_\infty^6 &= \frac{1}{4}\sum_{r,s=-\infty}^{\infty}\big((2r+1)^2-(2s)^2\big)q^{r^2+r+s^2} - \frac{1}{4}\sum_{r,s=-\infty}^{\infty}\big((2s)^2-(2r+1)^2\big)q^{r^2+r+s^2}\\ &= \frac{1}{2}\sum_{r,s=-\infty}^{\infty}\big((2r+1)^2-(2s)^2\big)q^{r^2+r+s^2},\end{aligned}$$

as required. ■

Now, we are in a position to prove Theorem 12.6.

Proof of Theorem 12.6. We deduce from (12.7) that

$$\begin{aligned}(q;q)_\infty^6 &= \frac{1}{2}\sum_{s=-\infty}^{\infty} q^{s^2}\sum_{r=-\infty}^{\infty}(2r+1)^2q^{r^2+r} - \frac{1}{2}\sum_{r=-\infty}^{\infty} q^{r^2+r}\sum_{s=-\infty}^{\infty}(2s)^2q^{s^2}\\ &= \frac{1}{2}\sum_{s=-\infty}^{\infty} q^{s^2}\sum_{r=-\infty}^{\infty} q^{r^2+r} + 2\sum_{s=-\infty}^{\infty} q^{s^2}\sum_{r=-\infty}^{\infty}(r^2+r)q^{r^2+r} - 2\sum_{r=-\infty}^{\infty} q^{r^2+r}\sum_{s=-\infty}^{\infty} s^2q^{s^2}\\ &= \frac{1}{2}\sum_{s=-\infty}^{\infty} q^{s^2}\sum_{r=-\infty}^{\infty} q^{r^2+r} + 2\sum_{s=-\infty}^{\infty} q^{s^2}\cdot q\frac{d}{dq}\sum_{r=-\infty}^{\infty} q^{r^2+r} - 2\sum_{r=-\infty}^{\infty} q^{r^2+r}\cdot q\frac{d}{dq}\sum_{s=-\infty}^{\infty} q^{s^2}.\end{aligned}$$

Note that

$$\sum_{n=-\infty}^{\infty} q^{n^2} = \phi(q)$$

and

$$\sum_{n=-\infty}^{\infty} q^{n^2+n} = 2\sum_{n\ge 0} q^{n^2+n} = 2\psi(q^2).$$

Hence,

$$(q;q)_\infty^6 = \phi(q)\psi(q^2) + 4\phi(q)\cdot q\frac{d}{dq}\psi(q^2) - 4\psi(q^2)\cdot q\frac{d}{dq}\phi(q).$$

Now, by Jacobi's triple product identity (11.8),

$$\phi(q) = (-q;q^2)_\infty^2(q^2;q^2)_\infty.$$

Also, by (11.15),

$$\psi(q^2)=\frac{(q^4;q^4)_\infty^2}{(q^2;q^2)_\infty}=\frac{(q^4;q^4)_\infty^2}{(q^2;q^2)_\infty}\frac{(q^2;q^4)_\infty^2}{(q^2;q^4)_\infty^2}=\frac{(q^2;q^2)_\infty}{(q^2;q^4)_\infty^2}.$$

It is a routine exercise by applying (12.4) to the above two relations that

$$q\frac{d}{dq}\phi(q)=\phi(q)\sum_{k\geq 1}\left(\frac{2(2k-1)q^{2k-1}}{1+q^{2k-1}}-\frac{2kq^{2k}}{1-q^{2k}}\right)$$

and

$$q\frac{d}{dq}\psi(q^2)=\psi(q^2)\sum_{k\geq 1}\left(\frac{2(4k-2)q^{4k-2}}{1-q^{4k-2}}-\frac{2kq^{2k}}{1-q^{2k}}\right).$$

Therefore,

$$(q;q)_\infty^6=\phi(q)\psi(q^2)\left(1+8\sum_{k\geq 1}\left(\frac{(4k-2)q^{4k-2}}{1-q^{4k-2}}-\frac{(2k-1)q^{2k-1}}{1+q^{2k-1}}\right)\right).$$

Recalling (11.14), (11.15) and (11.16), we have

$$\phi(-q)^4=1+8\sum_{k\geq 1}\left(\frac{(4k-2)q^{4k-2}}{1-q^{4k-2}}-\frac{(2k-1)q^{2k-1}}{1+q^{2k-1}}\right).$$

Finally, we take $q\mapsto -q$ and derive that

$$\begin{aligned}\phi(q)^4&=1+8\sum_{k\geq 1}\left(\frac{(4k-2)q^{4k-2}}{1-q^{4k-2}}+\frac{(2k-1)q^{2k-1}}{1-q^{2k-1}}\right)\\&=1+8\sum_{\substack{k\geq 1\\ k\not\equiv 0 \bmod 4}}\frac{kq^k}{1-q^k}.\end{aligned}$$

The desired result follows by applying (12.2) and (12.3). ■

R This proof is also attributed to Hirschhorn (*Proc. Amer. Math. Soc.* **101** (1987), no. 3, 436–438).

13. Arithmetic functions

13.1 Arithmetic functions

In the previous lectures, we have witnessed functions like the "sum-of-squares" functions $r_k(n)$ that are defined on the positive integers. Such functions are of particular interest in the study of number theory.

Definition 13.1 An *arithmetic function* is a complex-valued function that is defined on the positive integers.

R In G. H. Hardy and E. M. Wright's *Introduction*, they also include in their definition the requirement that an arithmetical function "expresses some arithmetical property of n."

Recall that we have also encountered multiplicative functions such as Euler's totient function $\phi(n)$.

Definition 13.2 An arithmetic function f is

(i) *multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all positive integers m and n with $(m,n) = 1$;
(ii) *completely multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all positive integers m and n.

Analogously, we may replace the above multiplicative condtion with an additive condition.

Definition 13.3 An arithmetic function f is

(i) *additive* if $f(mn) = f(m) + f(n)$ for all positive integers m and n with $(m,n) = 1$;
(ii) *completely additive* if $f(mn) = f(m) + f(n)$ for all positive integers m and n.

We list here several simple but important arithmetic functions:

- the *constant function* $\mathbf{1}(n)$, defined by $\mathbf{1}(n) = 1$ for all n — *completely multiplicative*;
- the *identity function* $\mathrm{id}(n)$, defined by $\mathrm{id}(n) = n$ for all n — *completely multiplicative*;
- the *unit function* $\varepsilon(n)$, defined by $\varepsilon(n) = 1$ if $n = 1$, and 0 otherwise — *completely multiplicative*;
- the function $\Omega(n)$, defined by the total number of prime factors of n (e.g. $\Omega(1) = 0$, $\Omega(2) = 1$, $\Omega(4) = 2$, $\Omega(6) = 2$, $\Omega(12) = 3$, etc.) — *completely additive*;

- ▷ the function $\omega(n)$, defined by the number of distinct prime factors of n (e.g. $\omega(1)=0$, $\omega(2)=1$, $\omega(4)=1$, $\omega(6)=2$, $\omega(12)=2$, etc.) — *additive*.

13.2 Divisor functions

Definition 13.4 For real or complex s, the *divisor functions* are defined $\sigma_s(n)$ by

$$\sigma_s(n) := \sum_{d|n} d^s,$$

where the summation runs over all positive divisors of n. In particular, we define

$$d(n)=\sigma_0(n)=\sum_{d|n} 1 \qquad \text{and} \qquad \sigma(n)=\sigma_1(n)=\sum_{d|n} d.$$

Theorem 13.1 Let $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ be in the canonical form. Then

$$d(n)=\prod_{k=1}^{r}(a_k+1) \tag{13.1}$$

and for $s\neq 0$,

$$\sigma_s(n)=\prod_{k=1}^{r}\frac{p_k^{(a_k+1)s}-1}{p_k^s-1}. \tag{13.2}$$

Proof. Noting that all divisors of n are of the form $p_1^{\beta_1}\cdots p_r^{\beta_r}$ with $0\le\beta_k\le\alpha_k$ for all k, we have

$$\sigma_s(n)=\sum_{d|n}d^s=\sum_{\beta_1=0}^{\alpha_1}\cdots\sum_{\beta_r=0}^{\alpha_r}\left(p_1^{\beta_1}\cdots p_r^{\beta_r}\right)^s=\prod_{k=1}^{r}\left(1+p_k^s+p_k^{2s}+\cdots+p_k^{\alpha_k s}\right).$$

We further get (13.1) and (13.2) by using the fact that $1+p^s+\cdots+p^{\alpha s}$ equals $\alpha+1$ if $s=0$, and $\frac{p^{(\alpha+1)s}-1}{p-1}$ if $s\neq 0$. ■

Corollary 13.2 For any s, the divisor function $\sigma_s(n)$ is multiplicative.

Proof. This is a direct implication of Theorem 13.1. ■

13.3 Möbius function

Recall that $\omega(n)$ counts by the number of distinct prime factors of n.

Definition 13.5 An positive integer n is *squarefree* if no squares other than 1 divide n; otherwise, we say n is *squareful*.

▪ **Example 13.1** The first several squarefree integers are $1,2,3,5,6,7,10,11,\dots$ and the first several squareful integers are $4,8,9,12,16,18,20,24\dots$ ▪

Definition 13.6 The *Möbius function* $\mu(n)$ is defined by

$$\mu(n)=\begin{cases}(-1)^{\omega(n)} & \text{if } n \text{ is squarefree,}\\ 0 & \text{otherwise.}\end{cases}$$

R The Möbius function was introduced by the German mathematician August Ferdinand Möbius (*J. Reine Angew. Math.* **9** (1832), 105–123).

Example 13.2 We have $\mu(1)=1$, $\mu(2)=-1$, $\mu(3)=-1$, $\mu(4)=0$, $\mu(5)=-1$, $\mu(6)=1$, etc. ■

Theorem 13.3 The Möbius function $\mu(n)$ is multiplicative.

Proof. First, we have $\mu(1)=1$. Let us assume that m and n are such that $(m,n)=1$. If one of m and n is squareful, so is mn, and hence $\mu(mn)=0=\mu(m)\mu(n)$. Further, $\mu(mn)=(-1)^{\omega(mn)}=(-1)^{\omega(m)+\omega(n)}=\mu(m)\mu(n)$ since $\omega(n)$ is additive. ■

Theorem 13.4 For $n\geq 1$,

$$\sum_{d|n}\mu(d)=\begin{cases}1 & \text{if } n=1,\\ 0 & \text{if } n>1.\end{cases} \tag{13.3}$$

Proof. The formula is trivial when $n=1$. For $n>1$, we write n in the canonical form $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$. Note that if suffices to consider squarefree divisors d of n in the sum $\sum_{d|n}\mu(d)$. We have

$$\begin{aligned}\sum_{d|n}\mu(d)&=\mu(1)+\mu(p_1)+\cdots+\mu(p_r)+\mu(p_1p_2)+\cdots+\mu(p_{r-1}p_r)+\cdots+\mu(p_1\cdots p_r)\\ &=\binom{r}{0}-\binom{r}{1}+\binom{r}{2}+\cdots+(-1)^r\binom{r}{r}=(1-1)^r=0,\end{aligned}$$

as required. ■

R Recalling the definition of the unit function ε, i.e., $\varepsilon(n)=1$ if $n=1$, and 0 otherwise, we have

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

13.4 Euler's totient function revisited

Recall that Euler's totient function $\phi(n)$ was well studied in Sect. 4.2 and later lectures. In particular, we know that $\phi(n)$ is multiplicative. Also, we have shown in Theorem 4.5 that

$$\sum_{d|n}\phi(d)=n. \tag{13.4}$$

Now, we establish a formula connecting Euler's totient function and the Möbius function.

Theorem 13.5 For $n\geq 1$,

$$\phi(n)=\sum_{d|n}\mu(d)\frac{n}{d}. \tag{13.5}$$

Proof. By the definition of $\phi(n)$, we have, with (13.3) applied, that

$$\phi(n)=\sum_{k=1}^{n}\varepsilon\big((k,n)\big)=\sum_{k=1}^{n}\sum_{d|(k,n)}\mu(d)=\sum_{k=1}^{n}\sum_{\substack{d|k\\ d|n}}\mu(d)=\sum_{d|n}\sum_{\substack{k=1\\ d|k}}^{n}\mu(d)=\sum_{d|n}\mu(d)\frac{n}{d},$$

as required. ■

13.5 Mangoldt function

In this part, we introduct the Mangoldt function $\Lambda(n)$ which plays a crucial role in the distribution of primes.

Definition 13.7 The *Mangoldt function* $\Lambda(n)$ is defined by

$$\Lambda(n)=\begin{cases}\log p & \text{if } n=p^{\alpha} \text{ with } p \text{ a prime and } \alpha \text{ a positive integer,}\\ 0 & \text{otherwise.}\end{cases}$$

R The Mangoldt function is named after the German mathematician Hans von Mangoldt.

Example 13.3 We have $\Lambda(1)=0,\ \Lambda(2)=\log 2,\ \Lambda(3)=\log 3,\ \Lambda(4)=\log 2,\ \Lambda(5)=\log 5,$ $\Lambda(6)=0$, etc.

R The Mangoldt function $\Lambda(n)$ is neither multiplicative nor additive, for $\Lambda(6)\neq\Lambda(2)\Lambda(3)$ and $\Lambda(6)\neq\Lambda(2)+\Lambda(3)$.

Theorem 13.6 For $n\geq 1$,

$$\log n=\sum_{d|n}\Lambda(d). \tag{13.6}$$

Proof. The formula is trivial when $n=1$. For $n>1$, we write n in the canonical form $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$. Then

$$\sum_{d|n}\Lambda(d)=\sum_{k=1}^{r}\big(\Lambda(p_k)+\Lambda(p_k^2)+\cdots+\Lambda(p_k^{\alpha_k})\big)=\sum_{k=1}^{r}\alpha_k\log p_k=\sum_{k=1}^{r}\log p_k^{\alpha_k}=\log n,$$

as deseried. ■

Theorem 13.7 For $n\geq 1$,

$$\Lambda(n)=-\sum_{d|n}\mu(d)\log d. \tag{13.7}$$

Proof. The formula is trivial when $n=1$. Also, if $n=p^{\alpha}$ with p a prime and α a positive integer, we have

$$-\sum_{d|p^{\alpha}}\mu(d)\log d=-\mu(1)\log 1-\mu(p)\log p=\log p=\Lambda(p^{\alpha}).$$

Now, we assume that n is written in the canonical form $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ with $r\geq 2$. Then

$$-\sum_{d|n}\mu(d)\log d=\sum_{1\leq i\leq r}\log p_i-\sum_{1\leq i<j\leq r}\log p_ip_j$$

$$+\sum_{1\le i<j<k\le r}\log p_ip_jp_k-\cdots+(-1)^{r-1}\log p_1p_2\cdots p_r.$$

Note that $\log xy=\log x+\log y$. We find that in the summation $\sum_{1\le i\le r}\log p_i$, each $\log p_\ell$ appears $1=\binom{r-1}{0}$ time; in the summation $\sum_{1\le i<j\le r}\log p_ip_j$, each $\log p_\ell$ appears $r-1=\binom{r-1}{1}$ times; in the summation $\sum_{1\le i<j\le r}\log p_ip_j$, each $\log p_\ell$ appears $\binom{r-1}{2}$ times, etc. Hence,

$$\begin{aligned}-\sum_{d|n}\mu(d)\log d&=\sum_{\ell=1}^{r}\left(\binom{r-1}{0}-\binom{r-1}{1}+\binom{r-1}{2}-\cdots+(-1)^{r-1}\binom{r-1}{r-1}\right)\log p_\ell\\&=\sum_{\ell=1}^{r}(1-1)^{r-1}\log p_\ell=0.\end{aligned}$$

However, for $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ with $r\ge 2$, we also have $\Lambda(n)=0$ by definition. The desired identity holds true. ■

Corollary 13.8 For $n\ge 1$,

$$\Lambda(n)=\sum_{d|n}\mu(d)\log\frac{n}{d}. \tag{13.8}$$

Proof. Note that

$$\sum_{d|n}\mu(d)\log\frac{n}{d}=\sum_{d|n}\mu(d)\big(\log n-\log d\big)=(\log n)\sum_{d|n}\mu(d)-\sum_{d|n}\mu(d)\log d.$$

Since $(\log n)\sum_{d|n}\mu(d)=0$ for $n\ge 1$ by (13.3), we arrive at the required result by recalling (13.7). ■

14. Möbius inversion formula

14.1 Möbius inversion formula

The pair of relations (13.4) and (13.5), and the pair of relations (13.6) and (13.8) are indeed special cases of a general phenomenon, known as the *Möbius inversion formula*.

Theorem 14.1 (Möbius Inversion Formula). Let $f(n)$ and $g(n)$ be arithmetic functions. If

$$g(n) = \sum_{d|n} f(d) \tag{14.1}$$

then

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right), \tag{14.2}$$

and vice versa.

R In (13.4) and (13.5), we have $f = \phi$ and $g = \mathrm{id}$; in (13.6) and (13.8), we have $f = \Lambda$ and $g = \log$.

Proof. We first prove (14.2) by (14.1). Note that

$$\begin{aligned}\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{\substack{d,d' \\ dd'|n}} \mu(d) f(d') \\ &= \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) = \sum_{d'|n} f(d') \varepsilon\left(\frac{n}{d'}\right) = f(n),\end{aligned}$$

where we make use of (13.3). Conversely, to show (14.1) from (14.2), we first require the trivial fact that for any arithmetic function $a(n)$,

$$\sum_{d|n} a(d) = \sum_{d|n} a\left(\frac{n}{d}\right).$$

Rewriting (14.2) as

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

it follows that

$$\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right) = \sum_{d|n}\sum_{d'|\frac{n}{d}} \mu\left(\frac{n/d}{d'}\right) g(d') = \sum_{\substack{d,d' \\ dd'|n}} \mu\left(\frac{n}{dd'}\right) g(d')$$

$$= \sum_{d'|n} g(d') \sum_{d|\frac{n}{d'}} \mu\left(\frac{n/d'}{d}\right) = \sum_{d'|n} g(d') \sum_{d|\frac{n}{d'}} \mu(d) = \sum_{d'|n} g(d')\varepsilon\left(\frac{n}{d'}\right) = g(n),$$

where (13.3) is also applied. ■

There is a slightly different type of Möbius inversion formula working for functions defined on real $x > 0$. Below, in the summation $\sum_{n\le x}$, the index n runs over all positive integers no larger than x.

Theorem 14.2 Let $F(x)$ and $G(x)$ be functions defined on real $x > 0$. If

$$G(x) = \sum_{n\le x} F\left(\frac{x}{n}\right) \tag{14.3}$$

then

$$F(x) = \sum_{n\le x} \mu(n) G\left(\frac{x}{n}\right), \tag{14.4}$$

and vice versa.

Proof. We first prove (14.4) by (14.3). Note that

$$\sum_{n\le x} \mu(n) G\left(\frac{x}{n}\right) = \sum_{n\le x} \mu(n) \sum_{m\le \frac{x}{n}} F\left(\frac{x/n}{m}\right) = \sum_{\substack{m,n \\ mn\le x}} \mu(n) F\left(\frac{x}{mn}\right)$$

$$(\text{with } N = mn) = \sum_{N\le x} F\left(\frac{x}{N}\right) \sum_{n|N} \mu(n) = \sum_{N\le x} F\left(\frac{x}{N}\right) \varepsilon(N) = F(x).$$

Conversely, to show (14.3) from (14.4), we have

$$\sum_{n\le x} F\left(\frac{x}{n}\right) = \sum_{n\le x}\sum_{m\le \frac{x}{n}} \mu(m) G\left(\frac{x/n}{m}\right) = \sum_{\substack{m,n \\ mn\le x}} \mu(m) G\left(\frac{x}{mn}\right)$$

$$(\text{with } N = mn) = \sum_{N\le x} G\left(\frac{x}{N}\right) \sum_{m|N} \mu(m) = \sum_{N\le x} G\left(\frac{x}{N}\right) \varepsilon(N) = G(x),$$

as required. ■

14.2 Multiplicative Möbius inversion formula

Another important variant of Möbius inversion formula is in the multiplicative notation.

Theorem 14.3 Let $f(n)$ and $g(n)$ be arithmetic functions such that $f(n) \neq 0$ and $g(n) \neq 0$ for all n. If

$$g(n) = \prod_{d|n} f(d) \tag{14.5}$$

then

$$f(n)=\prod_{d\mid n} g\left(\frac{n}{d}\right)^{\mu(d)}, \tag{14.6}$$

and vice versa.

Proof. We first prove (14.6) by (14.5). Note that

$$\begin{aligned}\prod_{d\mid n} g\left(\frac{n}{d}\right)^{\mu(d)} &= \prod_{d\mid n}\Bigg(\prod_{d'\mid \frac{n}{d}} f(d')\Bigg)^{\mu(d)} = \prod_{d\mid n}\prod_{d'\mid \frac{n}{d}} f(d')^{\mu(d)} = \prod_{d'\mid n}\prod_{d\mid \frac{n}{d'}} f(d')^{\mu(d)}\\ &= \prod_{d'\mid n} f(d')^{\sum_{d\mid \frac{n}{d'}}\mu(d)} = \prod_{d'\mid n} f(d')^{\varepsilon(n/d')} = f(n).\end{aligned}$$

Conversely, to show (14.5) from (14.6), we have

$$\begin{aligned}\prod_{d\mid n} f(d) = \prod_{d\mid n} f\left(\frac{n}{d}\right) &= \prod_{d\mid n}\prod_{d'\mid \frac{n}{d}} g(d')^{\mu\left(\frac{n/d}{d'}\right)} = \prod_{d'\mid n}\prod_{d\mid \frac{n}{d'}} g(d')^{\mu\left(\frac{n}{dd'}\right)}\\ &= \prod_{d'\mid n} g(d')^{\sum_{d\mid \frac{n}{d'}}\mu\left(\frac{n/d'}{d}\right)} = \prod_{d'\mid n} g(d')^{\sum_{d\mid \frac{n}{d'}}\mu(d)} = \prod_{d'\mid n} g(d')^{\varepsilon(n/d')} = g(n),\end{aligned}$$

as required. ■

Intuitively, for positive-valued f and g, we may define $\tilde{f}(n)=\log f(n)$ and $\tilde{g}(n)=\log g(n)$. By taking logarithm in (14.5) and (14.6), their equivalence becomes

$$\tilde{g}(n)=\sum_{d\mid n}\tilde{f}(d) \qquad \Longleftrightarrow \qquad \tilde{f}(n)=\sum_{d\mid n}\mu(d)\tilde{g}\left(\frac{n}{d}\right),$$

which is exactly the usual Möbius inversion formula.

14.3 Dirichlet convolutions

The Möbius inversion formula can be further understood in a more abstract way, through *Dirichlet convolutions*, named after the German mathematician Peter Gustav Lejeune Dirichlet.

Definition 14.1 For arithmetic functions f and g, their *Dirichlet convolution* is defined to be an arithmetic function h with

$$h(n)=\sum_{d\mid n} f(d)g\left(\frac{n}{d}\right),$$

where the summation runs over all positive divisors of n. We write

$$h=f*g.$$

Dirichlet convolutions satisfy the following algebraic properties.

Theorem 14.4 For any arithmetic functions u, v and w, we have

(i) $u*v=v*u$ (commutative law);

(ii) $(u*v)*w=u*(v*w)$ (associative law).

Proof. It is straightforward to verify that

$$(u*v)(n) = (v*u)(n) = \sum_{\substack{a,b\\ ab=n}} u(a)v(b)$$

and

$$\big((u*v)*w\big)(n) = \big(u*(v*w)\big)(n) = \sum_{\substack{a,b,c\\ abc=n}} u(a)v(b)w(c),$$

where a, b and c run over positive integers. ■

Theorem 14.5 Let ε be the unit function. For any arithmetic function f, we have $f*\varepsilon = \varepsilon * f = f$.

Proof. We have

$$(f*\varepsilon)(n) = \sum_{d|n} f(d)\varepsilon\left(\frac{n}{d}\right) = f(n),$$

as required. ■

Theorem 14.6 Let f be an arithmetic function with $f(1)\neq 0$. Then there exists a unique arithmetic function g such that $f*g = g*f = \varepsilon$. Moreover, g is given by

$$g(1) = \frac{1}{f(1)} \tag{14.7}$$

and for $n>1$,

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n\\ d<n}} f\left(\frac{n}{d}\right) g(d). \tag{14.8}$$

Proof. First, we note that $(f*g)(1) = f(1)g(1) = \varepsilon(1) = 1$ gives $g(1) = 1/f(1)$. For $n>1$, we have $\varepsilon(n) = 0$, and hence,

$$0 = (f*g)(n) = (g*f)(n) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d) = f(1)g(n) + \sum_{\substack{d|n\\ d<n}} f\left(\frac{n}{d}\right) g(d).$$

Hence, we may iteratively determine the unique $g(n)$ by (14.8). ■

Definition 14.2 Given an arithmetic function f with $f(1)\neq 0$, we call the unique arithmetic function g such that $f*g = g*f = \varepsilon$ the *Dirichlet inverse* of f, denoted by $g = f^{-1}$.

Theorem 14.7 For any arithmetic functions with $f(1)\neq 0$ and $g(1)\neq 0$, we have $(f*g)^{-1} = f^{-1}*g^{-1}$.

Proof. We have $(f*g)*(f^{-1}*g^{-1}) = (f*f^{-1})*(g*g^{-1}) = \varepsilon*\varepsilon = \varepsilon$, as required. ■

R In the language of group theory, the set of arithmetic functions f with $f(1)\neq 0$ forms an Abelien group with respect to the operation "$*$" (Dirichlet convolution), and the identity element of this group is the unit function ε.

Corollary 14.8 The Möbius function μ and the constant function $\mathbf{1}$ are Dirichlet inverses of one another.

Proof. We simply rewrite the relation (13.3), $\sum_{d|n}\mu(d)=\varepsilon(n)$, in terms of Dirichlet convolution, and find that $\mu*\mathbf{1}=\varepsilon$, yielding the desired result. ■

R We may also interpret the Möbius inversion formula in this setting by noting that it is exactly the equivalence

$$g=f*\mathbf{1} \qquad \Longleftrightarrow \qquad f=g*\mu.$$

This is trivial since if $g=f*\mathbf{1}$, then $g*\mu=(f*\mathbf{1})*\mu=f*(\mu*\mathbf{1})=f*\varepsilon=f$; and if $f=g*\mu$, then $f*\mathbf{1}=(g*\mu)*\mathbf{1}=g*(\mu*\mathbf{1})=g*\varepsilon=g$.

Now, we consider Dirichlet convolutions on multiplicative functions.

Theorem 14.9 If f and g are multiplicative functions, so is their Dirichlet convolution $f*g$.

Proof. We write $h=f*g$. Let m and n be positive integers with $(m,n)=1$. We use the fact that if $d\mid mn$, then we may uniquely write $d=ab$ with $a\mid m$ and $b\mid n$. In particular, $(a,b)=1$ and $(\frac{m}{a},\frac{n}{b})=1$. Now,

$$\begin{aligned}h(mn)&=\sum_{d|mn}f(d)g\left(\frac{mn}{d}\right)=\sum_{a|m,b|n}f(ab)g\left(\frac{mn}{ab}\right)=\sum_{a|m,b|n}f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)\\&=\sum_{a|m}f(a)g\left(\frac{m}{a}\right)\sum_{b|n}f(b)g\left(\frac{n}{b}\right)=h(m)h(n).\end{aligned}$$

Hence, $h=f*g$ is multiplicative. ■

Theorem 14.10 If f is a multiplicative function, so is its Dirichlet inverse f^{-1}.

Proof. Noting that f is multiplicative, we have $f(1)=1$, and hence $f^{-1}(1)=\frac{1}{f(1)}=1$. Now we shall show that for every positive integer N, $f^{-1}(N)=f^{-1}(m)f^{-1}(n)$ holds true for any positive integers m and n with $(m,n)=1$ and $mn=N$. We prove by induction on N. The base case $N=1$ is confirmed by the fact that $f^{-1}(1)=1$. Assume that the claim is true for $1,\dots,N-1$ for some $N\geq 2$, and we shall prove the case of N. Note that

$$\begin{aligned}\varepsilon(N)=(f^{-1}*f)(mn)&=\sum_{a|m,b|n}f^{-1}(ab)f\left(\frac{mn}{ab}\right)\\&=f^{-1}(mn)f(1)+\sum_{\substack{a|m,b|n\\ab<N}}f^{-1}(ab)f\left(\frac{mn}{ab}\right)\\\text{(induc. assump.)}&=f^{-1}(mn)f(1)+\sum_{\substack{a|m,b|n\\ab<N}}f^{-1}(a)f^{-1}(b)f\left(\frac{m}{a}\right)f\left(\frac{n}{b}\right)\\&=f^{-1}(mn)f(1)-f^{-1}(m)f^{-1}(n)f(1)f(1)+\sum_{a|m,b|n}f^{-1}(a)f^{-1}(b)f\left(\frac{m}{a}\right)f\left(\frac{n}{b}\right)\\&=f^{-1}(N)-f^{-1}(m)f^{-1}(n)+(f^{-1}*f)(m)(f^{-1}*f)(n)\\&=f^{-1}(N)-f^{-1}(m)f^{-1}(n)+\varepsilon(N),\end{aligned}$$

thereby implying that $f^{-1}(N)=f^{-1}(m)f^{-1}(n)$, as required. ■

R The set of multiplicative functions is a subgroup of the group of all arithmetic functions f with $f(1) \neq 0$.

14.4 Ramanujan's sums

We first adopt a conventional nonation in analytic number theory.

Definition 14.3 For any complex τ, we define

$$e(\tau) := e^{2\pi i\tau}.$$

Now, we introduce Ramanujan's sums, which is crucial in, for instance, the proof of I. M. Vinogradov's theorem (*Recueil Math.* **2** (1937), 179–195) that *every sufficiently large odd number is the sum of three primes.*

Definition 14.4 For q and n positive integers, *Ramanujan's sums* are defined by

$$c_q(n) := \sum_{\substack{1\le a\le q\\(a,q)=1}} e\left(\frac{an}{q}\right).$$

R Ramanujan's sums were introduced by Srinivasa Ramanujan (*Trans. Cambridge Philos. Soc.* **22** (1918), no. 13, 259–276).

We introduce another sum for q and n positive integers:

$$\eta_q(n) := \sum_{1\le a\le q} e\left(\frac{an}{q}\right).$$

Lemma 14.11 For positive integers q and n,

$$\eta_q(n) = \begin{cases} q & \text{if } q \mid n,\\ 0 & \text{if } q \nmid n. \end{cases} \tag{14.9}$$

In particular, for positive integers s and t with $(s,t)=1$, we have $\eta_s(n)\eta_t(n) = \eta_{st}(n)$.

Proof. Let $d = (q,n)$, and write $q = q'd$ and $n = n'd$. Noting that $(q',n') = 1$, we have $\{an' : 1 \le a \le q'\}$ covers a complete system modulo q'. Now,

$$\eta_q(n) = \sum_{1\le a\le q} e\left(\frac{an}{q}\right) = \eta_q(n) := \sum_{1\le a\le q'd} e\left(\frac{an'}{q'}\right) = d\sum_{1\le a\le q'} e\left(\frac{an'}{q'}\right) = d\sum_{1\le a\le q'} e\left(\frac{a}{q'}\right)$$

Note that

$$\sum_{1\le a\le q'} e\left(\frac{a}{q'}\right) = \begin{cases} 1 & \text{if } q' = 1,\\ 0 & \text{if } q' > 1. \end{cases}$$

Finally, we use the fact that $q' = 1$ if and only if $q = d = (q,n)$, or $q \mid n$, as desired. The second part is a direct consequence of (14.9). ■

Now, we establish a relation between $c_q(n)$ and $\eta_q(n)$.

Theorem 14.12 For positive integers q and n,

$$\eta_q(n) = \sum_{d|q} c_d(n). \tag{14.10}$$

Proof. We use the fact that $\{\frac{a}{q} : 1 \le a \le q\} = \cup_{d|q}\{\frac{b}{d} : 1 \le b \le d \text{ and } (b,d) = 1\}$, by simplifying each $\frac{a}{q}$ to its irreducible form. Hence,

$$\sum_{1\le a\le q} e\left(\frac{an}{q}\right) = \sum_{d|q} \sum_{\substack{1\le b\le d\\(b,d)=1}} e\left(\frac{bn}{d}\right),$$

as required. ∎

Let us treat $\eta_q(n)$ and $c_q(n)$ as functions in q with n fixed, and define $H(q) := \eta_q(n)$ and $C(q) := c_q(n)$ for clarity. Then we may paraphrase (14.10) as

$$H = C * \mathbf{1}. \tag{14.11}$$

Corollary 14.13 Let n be a positive integer. For positive integers s and t with $(s,t) = 1$,

$$c_s(n)c_t(n) = c_{st}(n). \tag{14.12}$$

Proof. We use Theorems 14.9 and 14.10 by noting that both H and $\mathbf{1}$ are multiplicative. ∎

Corollary 14.14 For positive integers q and n,

$$c_q(n) = \sum_{d|q,d|n} \mu\left(\frac{q}{d}\right) d. \tag{14.13}$$

Proof. We apply Möbius inversion formula to (14.11), and find that

$$c_q(n) = \sum_{d|q} \mu\left(\frac{q}{d}\right) \eta_d(n).$$

The desired relation follows with recourse to (14.9). ∎

Theorem 14.15 For positive integers q and n,

$$c_q(n) = \mu\left(\frac{q}{(q,n)}\right) \frac{\phi(q)}{\phi\left(\frac{q}{(q,n)}\right)}. \tag{14.14}$$

Proof. For convenience, we write

$$R_q(n) := \mu\left(\frac{q}{(q,n)}\right) \frac{\phi(q)}{\phi\left(\frac{q}{(q,n)}\right)}. \tag{14.15}$$

Let n be an arbitrary positive integer. Note that $c_1(n) = R_1(n)$. Also, let s and t be such that $(s,t) = 1$. Then $(st,n) = (s,n)(t,n)$ and $\left(\frac{s}{(s,n)}, \frac{t}{(t,n)}\right) = 1$. Thus,

$$R_{st}(n) = \mu\left(\frac{st}{(st,n)}\right) \frac{\phi(st)}{\phi\left(\frac{st}{(st,n)}\right)} = \mu\left(\frac{s}{(s,n)}\right) \mu\left(\frac{t}{(t,n)}\right) \frac{\phi(s)\phi(t)}{\phi\left(\frac{s}{(s,n)}\right)\phi\left(\frac{t}{(t,n)}\right)} = R_s(n)R_t(n).$$

Recalling (14.12), it suffices to prove for prime powers p^α that $c_{p^\alpha}(n) = R_{p^\alpha}(n)$. Finally, it is straightforward to calculate from (14.13) and (14.15) that

$$c_{p^\alpha}(n) = R_{p^\alpha}(n) = \begin{cases} p^{\alpha-1}(p-1) & \text{if } (p^\alpha, n) = p^\alpha, \\ -p^{\alpha-1} & \text{if } (p^\alpha, n) = p^{\alpha-1}, \\ 0 & \text{otherwise.} \end{cases}$$

The desired relation holds true. ■

15. Averages of arithmetic functions

15.1 Asymptotic relations

Given an arithmetic function f, one of the basic problems in analytic number theory concerns the asymptotic analysis of the partial sum

$$\sum_{n \le x} f(n)$$

where the summation runs over all **positive integers** no larger than x. Meanwhile, we are also often interested in the behavior of

$$\sum_{p \le x} f(p)$$

in which the index p means that we are summing over **primes** no larger than x.

To begin with, we introduce some useful notations for asymptotic analysis.

Definition 15.1 (Bachmann–Landau Notations).

- ▷ The *big O notation* $f(x) = O(g(x))$ means that there exists a constant C such that $|f(x)| \le C|g(x)|$;
- ▷ The *small o notation* $f(x) = o(g(x))$ means that $\lim f(x)/g(x) = 0$.

R Big O and small o belong to a family of notations invented by the German mathematicians Paul Bachmann and Edmund Landau.

Definition 15.2 (Vinogradov Notations).

- ▷ The notation $f(x) \ll g(x)$ means that $f(x) = O(g(x))$;
- ▷ The notation $f(x) \gg g(x)$ means that $g(x) \ll f(x)$.

R These notations were introduced by the Russian mathematician Ivan Matveevich Vinogradov.

Definition 15.3

- ▷ The *asymptotic equivalence* symbol $f(x) \sim g(x)$ means that $\lim f(x)/g(x) = 1$;
- ▷ The *order of magnitude estimate* symbol $f(x) \asymp g(x)$ means that both $f(x) \ll g(x)$ and $g(x) \ll f(x)$ hold. Equivalently, there exist constants C_1 and C_2 such that

$$C_1|g(x)| \leq |f(x)| \leq C_2|g(x)|.$$

15.2 Abel's summation formula

In many occassions, a partial sum can be nicely estimated by comparing it with an integral. To do so, a summation formula due to the Norwegian mathematician Niels Henrik Abel, and especially its special case that was obtained earlier by Euler, plays a crucial role.

Definition 15.4 We denote by $\lfloor x \rfloor$ the largest integer not exceeding x, and by $\{x\} := x - \lfloor x \rfloor$.

Theorem 15.1 (Abel's Summation Formula). Let $a : \mathbb{Z}_{>0} \to \mathbb{C}$ be an arithmetic function, let $0 < y < x$ be real numbers, and $f : [y,x] \to \mathbb{C}$ be a function with continuous derivative f' on the interval $[y,x]$. Then

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt, \tag{15.1}$$

where $A(t) = \sum_{n\leq t} a(n)$.

Proof. We start by observing that $A(t) = A(\lfloor t \rfloor)$ and $A(t+1) - A(t) = a(\lfloor t \rfloor + 1)$. It is also straightforward to see that if there is no integer in the interval $(y,x]$, both sides of (15.1) are zero. Now, we assume that there is at least one integer in $(y,x]$, and evaluate the integral one the right-hand side of (15.1):

$$\begin{aligned}
\int_y^x A(t)f'(t)dt &= \left(\int_y^{\lfloor y \rfloor+1} + \int_{\lfloor y \rfloor+1}^{\lfloor y \rfloor+2} + \cdots + \int_{\lfloor x \rfloor-1}^{\lfloor x \rfloor} + \int_{\lfloor x \rfloor}^{x}\right) A(t)f'(t)dt \\
&= A(y)\big(f(\lfloor y \rfloor+1) - f(y)\big) + A(y+1)\big(f(\lfloor y \rfloor+2) - f(\lfloor y \rfloor+1)\big) + \cdots \\
&\quad + A(x-1)\big(f(\lfloor x \rfloor) - f(\lfloor x \rfloor-1)\big) + A(x)\big(f(x) - f(\lfloor x \rfloor)\big) \\
&= A(x)f(x) - A(y)f(y) - \big(A(y+1) - A(y)\big)f(\lfloor y \rfloor+1) - \cdots \\
&\quad - \big(A(x) - A(x-1)\big)f(\lfloor x \rfloor) \\
&= A(x)f(x) - A(y)f(y) - a(\lfloor y \rfloor+1)f(\lfloor y \rfloor+1) - \cdots - a(\lfloor x \rfloor)f(\lfloor x \rfloor) \\
&= A(x)f(x) - A(y)f(y) - \sum_{y<n\leq x} a(n)f(n),
\end{aligned}$$

as required. ■

R A more advanced way to think of Abel's summation formula is by means of the Riemann–Stieltjes integral:

$$\begin{aligned}
\sum_{y<n\leq x} a(n)f(n) &= \int_y^x f(t)dA(t) \\
&= f(x)A(x) - f(y)A(y) - \int_y^x A(t)df(t),
\end{aligned}$$

where we use integration by parts in the second equality.

Corollary 15.2 (Euler's Summation Formula). Let $0 < y < x$ be real numbers, and $f : [y,x] \to$

$\mathbb{C}$ be a function with continuous derivative f' on the interval $[y,x]$. Then

$$\sum_{y<n\le x} f(n) = \int_y^x f(t)dt + \int_y^x \{t\}f'(t)dt + \{y\}f(y) - \{x\}f(x). \tag{15.2}$$

Proof. In Abel's summation formula, we choose $a(n)=1$ for all n, and observe that $A(t)=\lfloor t\rfloor$. Hence, it follows from (15.1) that

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

Also, by integration by parts,

$$\int_y^x f(t)dt = f(x) - f(y) - \int_y^x tf'(t)dt.$$

Combining the above two relations gives (15.2) by recalling that $\{x\} = x - \lfloor x\rfloor$. ■

In the sequel, we present some applications of Euler's summation formula. Here,

$$\gamma := \lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n} - \log x\right) = 1 - \int_1^\infty \frac{\{t\}}{t^2}dt = 0.577215\cdots$$

is the *Euler–Mascheroni constant*, named after Euler and the Italian mathematician Lorenzo Mascheroni;

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

with s a complex number such that $\Re(s)>1$ is the *Riemann zeta function* which is absolutely convergent in this half-plane.

Theorem 15.3 As $x\to\infty$,

(i) $\displaystyle\sum_{n\le x}\frac{1}{n} = \log x + \gamma + O(x^{-1})$;

(ii) $\displaystyle\sum_{n\le x}\frac{1}{n^s} = \zeta(s) + O(x^{1-s})$ if $\Re(s)>1$;

(iii) $\displaystyle\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + O(1)$ if $0<\Re(s)\le 1$ and $s\ne 1$;

(iv) $\displaystyle\sum_{n\le x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha)$ if $\Re(\alpha)\ge 0$.

R Parts (ii) and (iii) can be improved uniformly. It is known that the Riemann zeta function has an analytic continuation to $\mathbb{C}\backslash\{1\}$. In particular, we will show in Theorem 18.3 that, for $s\ne 1$ with $0<\Re(s)\le 1$, $\zeta(s)$ is continued analytically as

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

Mimicking the proof of Part (iii) with Euler's summation formula applied with $f(t) = t^{-s}$ for all complex $s\ne 1$ with $\Re(s)>0$, we have

$$\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s}).$$

This is left as an exercise.

Proof. (i). We take $f(t)=t^{-1}$ in Euler's summation formula and find that

$$\sum_{n\le x}\frac{1}{n}=\int_{1^-}^{x}\frac{dt}{t}-\int_{1^-}^{x}\frac{\{t\}}{t^2}dt+1-\frac{\{x\}}{x}=\log x-\int_{1}^{x}\frac{\{t\}}{t^2}dt+1+O(x^{-1})$$
$$=\log x+1-\int_{1}^{\infty}\frac{\{t\}}{t^2}dt+\int_{x}^{\infty}\frac{\{t\}}{t^2}dt+O(x^{-1})=\log x+\gamma+O(x^{-1}),$$

since $\int_x^\infty \frac{\{t\}}{t^2}dt \ll \int_x^\infty \frac{1}{t^2}dt=x^{-1}$.

(ii). We directly have that, for $\Re(s)>1$,

$$\sum_{n\le x}\frac{1}{n^s}=\zeta(s)-\sum_{n>x}\frac{1}{n^s}=\zeta(s)+O\left(\int_x^\infty\frac{dt}{t^s}\right)=\zeta(s)+O(x^{1-s}).$$

(iii). With $f(t)=t^{-s}$ where $0<\Re(s)\le 1$ and $s\neq 1$, we know from Euler's summation formula that

$$\sum_{n\le x}\frac{1}{n^s}=\int_{1^-}^{x}\frac{dt}{t^s}-s\int_{1^-}^{x}\frac{\{t\}}{t^{s+1}}dt+1-\frac{\{x\}}{x^s}=\int_1^x\frac{dt}{t^s}+O(1)=\frac{x^{1-s}}{1-s}+O(1).$$

(iv). With $f(t)=t^\alpha$ where $\Re(\alpha)\ge 0$, Euler's summation formula gives us that

$$\sum_{n\le x}n^\alpha=\int_{1^-}^{x}t^\alpha dt+\alpha\int_{1^-}^{x}\{t\}t^{\alpha-1}dt+1-\{x\}x^\alpha=\int_1^x t^\alpha dt+O(x^\alpha)=\frac{x^{\alpha+1}}{\alpha+1}+O(x^\alpha),$$

as required. ■

15.3 Average order of $\sigma(n)$

Theorem 15.4 As $x\to\infty$,

$$\sum_{n\le x}\sigma(n)=\frac{\zeta(2)}{2}x^2+O(x\log x). \qquad (15.3)$$

Proof. We have

$$\sum_{n\le x}\sigma(n)=\sum_{n\le x}\sum_{m|n}m=\sum_{\substack{m,d\\ md\le x}}m=\sum_{d\le x}\sum_{m\le\frac{x}{d}}m=\sum_{d\le x}\frac{1}{2}\left\lfloor\frac{x}{d}\right\rfloor\left(\left\lfloor\frac{x}{d}\right\rfloor+1\right)$$
$$=\frac{1}{2}\sum_{d\le x}\left(\frac{x}{d}\right)^2+O\left(\sum_{d\le x}\frac{x}{d}\right)=\frac{\zeta(2)}{2}x^2+O(x\log x),$$

where we make use of Theorem 15.3, Parts (i) and (ii). ■

Theorem 15.5 Let $\alpha\neq 1$ be a complex number with $\Re(\alpha)>0$. As $x\to\infty$,

$$\sum_{n\le x}\sigma_\alpha(n)=\frac{\zeta(\alpha+1)}{\alpha+1}x^{\alpha+1}+O(x^{\max\{1,\Re(\alpha)\}}). \qquad (15.4)$$

Proof. We have

$$\sum_{n\le x}\sigma_\alpha(n)=\sum_{n\le x}\sum_{m|n}m^\alpha=\sum_{\substack{m,d\\ md\le x}}m^\alpha=\sum_{d\le x}\sum_{m\le\frac{x}{d}}m^\alpha=\sum_{d\le x}\left(\frac{(\frac{x}{d})^{\alpha+1}}{\alpha+1}+O\left(\left(\frac{x}{d}\right)^\alpha\right)\right)$$

$$= \frac{x^{\alpha+1}}{\alpha+1}\sum_{d\le x}\frac{1}{d^{\alpha+1}} + O\left(x^{\alpha}\sum_{d\le x}\frac{1}{d^{\alpha}}\right) = \left(\frac{\zeta(\alpha+1)}{\alpha+1}x^{\alpha+1} + O(x)\right) + O(x^{\max\{1,\Re(\alpha)\}}),$$

where we make use of Theorem 15.3, Parts (ii), (iii) and (iv). ■

15.4 Average order of $\phi(n)$

Theorem 15.6 As $x\to\infty$,

$$\sum_{n\le x}\phi(n) = \frac{1}{2\zeta(2)}x^2 + O(x\log x). \tag{15.5}$$

Proof. We recall (13.5) and obtain

$$\sum_{n\le x}\phi(n) = \sum_{n\le x}\sum_{d|n}\mu(d)\frac{n}{d} = \sum_{\substack{m,d\\ md\le x}}\mu(d)m = \sum_{d\le x}\mu(d)\sum_{m\le \frac{x}{d}} m = \sum_{d\le x}\frac{\mu(d)}{2}\left(\left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)\right)$$
$$= \frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{d^2} + O\left(\sum_{d\le x}\frac{x}{d}\right) = \frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{d^2} + O(x\log x).$$

Finally, we will show later in Example 16.4 that

$$\sum_{d\ge 1}\frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)}.$$

Hence,

$$\frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{d^2} = \frac{x^2}{2}\left(\sum_{d\ge 1}\frac{\mu(d)}{d^2} - \sum_{d>x}\frac{\mu(d)}{d^2}\right) = \frac{x^2}{2}\sum_{d\ge 1}\frac{\mu(d)}{d^2} + O\left(x^2\int_x^{\infty}\frac{dt}{t^2}\right) = \frac{x^2}{2\zeta(2)} + O(x),$$

thereby confirming the desired relation. ■

15.5 Dirichlet hyperbola method

For the purpose of getting a better estimate of the partial sum of the Dirichlet convolution of certain arithmetic functions, we sometimes require a trick due to Dirichlet, known as the *Dirichlet hyperbola method.*

Theorem 15.7 (Dirichlet Hyperbola Method). Let f and g be arithmetic functions and define

$$F(x) = \sum_{n\le x} f(n) \qquad \text{and} \qquad G(x) = \sum_{n\le x} g(n).$$

Then for any $1\le M\le x$,

$$\sum_{n\le x}(f*g)(n) = \sum_{u\le M} f(u)G\left(\frac{x}{u}\right) + \sum_{v\le x/M} g(v)F\left(\frac{x}{v}\right) - F(M)G\left(\frac{x}{M}\right). \tag{15.6}$$

Proof. We have

$$\sum_{n\le x}(f*g)(n) = \sum_{\substack{u,v\\ uv\le x}} f(u)g(v).$$

Now, we consider the set of integer lattices $S = \{(u,v) \in \mathbb{Z}^2_{>0} : uv \le x\}$. By the inclusion-exclusion principle, we may rewrite S as $S = S_{\mathsf{L}} \cup S_{\mathsf{B}} \backslash S_{\mathsf{O}}$, where

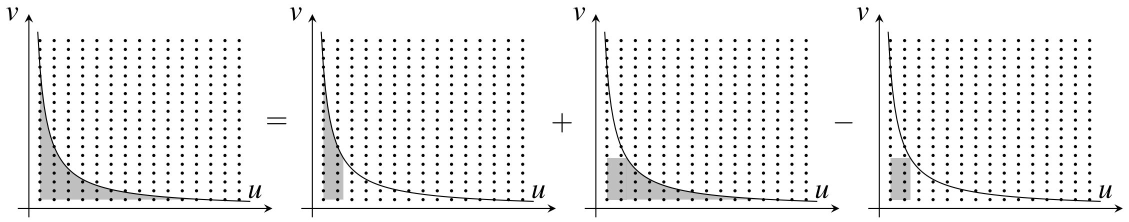
$$\begin{aligned} S_{\mathsf{Left}} &:= \{(u,v) \in \mathbb{Z}^2_{>0} : uv \le x \text{ and } u \le M\}, \\ S_{\mathsf{Below}} &:= \{(u,v) \in \mathbb{Z}^2_{>0} : uv \le x \text{ and } v \le x/M\}, \\ S_{\mathsf{Overlapping}} &:= \{(u,v) \in \mathbb{Z}^2_{>0} : u \le M \text{ and } v \le x/M\}. \end{aligned}$$

Hence,

$$\sum_{n \le x} (f*g)(n) = \sum_{\substack{u \le M \\ uv \le x}} f(u)g(v) + \sum_{\substack{v \le x/M \\ uv \le x}} f(u)g(v) - \sum_{\substack{u \le M \\ v \le x/M}} f(u)g(v),$$

yielding the required result. ■

Visually, the above argument can be understood as follows.



15.6 Average order of $d(n)$

Here we give an instance of how the Dirichlet hyperbola method provides better estimates. We start by mimicking the proof of Theorem 15.4 to estimate the partial sum of $d(n)$, the divisor function:

$$\sum_{n \le x} d(n) = \sum_{n \le x} \sum_{m \mid n} 1 = \sum_{\substack{m,d \\ md \le x}} 1 = \sum_{d \le x} \left\lfloor \frac{x}{d} \right\rfloor = \sum_{d \le x} \left(\frac{x}{d} + O(1) \right) = x \log x + O(x).$$

Then in the next theorem, we will see that with the Dirichlet hyperbola method, the above $O(x)$ term can be explicitly expressed, and the error can be reduced to $O(\sqrt{x})$.

Theorem 15.8 As $x \to \infty$,

$$\sum_{n \le x} d(n) = x \log x + (2\gamma - 1)x + O(\sqrt{x}). \tag{15.7}$$

Proof. Recalling from the definition of $d(n)$, we have $d = \mathbf{1} * \mathbf{1}$. Now, in Theorem 15.7, we take $f = g = \mathbf{1}$, and note that $F(x) = G(x) = \lfloor x \rfloor$. Choosing $M = \sqrt{x}$ gives

$$\begin{aligned} \sum_{n \le x} d(n) &= 2 \sum_{d \le \sqrt{x}} \left\lfloor \frac{x}{d} \right\rfloor - \lfloor \sqrt{x} \rfloor^2 = 2x \sum_{d \le \sqrt{x}} \frac{1}{d} - x + O(\sqrt{x}) \\ &= 2x \left(\log \sqrt{x} + \gamma + O(x^{-1/2}) \right) - x + O(\sqrt{x}) = x \log x + (2\gamma - 1)x + O(\sqrt{x}), \end{aligned}$$

as required. ■

16. Dirichlet series

16.1 Dirichlet series

In 1837, Lejeune Dirichlet (*Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin* **48** (1837), 45–71) proved the following important result, which fully extends Theorems 1.2, 1.3 and 1.4.

Dirichlet's Theorem There are infinitely many primes that are congruent to a modulo N provided that $(a,N)=1$.

To establish this result, many influential techniques in analytic number theory were introduced, one of which is the *Dirichlet series*, an infinite series associated to an arithmetic function.

Definition 16.1 Let f be an arithmetic function. The *Dirichlet series* for f is defined by

$$\sum_{n\ge 1}\frac{f(n)}{n^s},$$

where s is a complex variable.

R Following the German mathematician Bernhard Riemann, we always write complex variables s as

$$s=\sigma+it,$$

where σ and t are real. We usually call the set of complex numbers $\{s:\sigma>\sigma_0\}$ with σ_0 a certain real number a *half-plane.*

As we are looking at infinite series, an exigent issue is the analysis of convergence. One basic fact that will be frequently used is $|n^s|=n^\sigma$ for all positive integers n since $n^s=e^{s\log n}=n^\sigma e^{it\log n}$.

Rule 16.1 (Abscissa of Absolute Convergence). Suppose the series $\sum_{n\ge1}|f(n)n^{-s}|$ does not converge for all s or diverge for all s. Then there exists a real number σ_a, called the *abscissa of absolute convergence*, such that the series $\sum_{n\ge1}f(n)n^{-s}$ converges absolutely if $\sigma>\sigma_a$, but does not converge absolutely if $\sigma<\sigma_a$.

Proof. This is a direct consequence of the comparison test. ■

Lemma 16.2 Suppose that the series $\sum_{n\ge 1} f(n)n^{-s}$ converges for $s_0=\sigma_0+it_0$. Then this series converges for all s with $\sigma>\sigma_0$. Moreover, the convergence is uniform in every compact region contained in the half-plane $\sigma>\sigma_0$.

Proof. For convenience, we define for $1\le a<b$,

$$S(a,b):=\sum_{a<n\le b}\frac{f(n)}{n^s}.$$

Since $\sum_{n\ge 1} f(n)n^{-s_0}$ converges, there exists a constant M such that the partial sum $S(x):=\sum_{n\le x} f(n)n^{-s_0}$ satisfies $|S(x)|\le M$ for all $x\ge 1$. By Abel's summation formula (15.1),

$$S(a,b)=\sum_{a<n\le b}\frac{f(n)}{n^{s_0}}\frac{1}{n^{s-s_0}}=\frac{S(b)}{b^{s-s_0}}-\frac{S(a)}{a^{s-s_0}}+(s-s_0)\int_a^b\frac{S(x)}{x^{s-s_0+1}}dx.$$

Hence,

$$\begin{aligned}|S(a,b)|&\le\frac{M}{b^{\sigma-\sigma_0}}+\frac{M}{a^{\sigma-\sigma_0}}+|s-s_0|M\int_a^b\frac{dx}{x^{\sigma-\sigma_0+1}}\\&=\frac{M}{b^{\sigma-\sigma_0}}+\frac{M}{a^{\sigma-\sigma_0}}+\frac{M|s-s_0|}{\sigma-\sigma_0}\left(\frac{1}{a^{\sigma-\sigma_0}}-\frac{1}{b^{\sigma-\sigma_0}}\right)\\&\le 2Ma^{\sigma_0-\sigma}\left(1+\frac{|s-s_0|}{\sigma-\sigma_0}\right)=C\cdot a^{\sigma_0-\sigma}.\end{aligned}$$

Here, the factor $C=C(s,s_0):=2M\left(1+\frac{|s-s_0|}{\sigma-\sigma_0}\right)$ is independent of a. Noting that $\sigma>\sigma_0$ and hence that $a^{\sigma_0-\sigma}\to 0$ as $a\to+\infty$, it follows by Cauchy's criterion that $\sum_{n\ge 1} f(n)n^{-s}$ converges for all s with $\sigma>\sigma_0$.

Further, in any compact region K contained in the half-plane $\sigma>\sigma_0$, we find that both $\sigma-\sigma_0>0$ and $|s-s_0|$ are bounded from below and above. Hence C only depends on K, thereby implying the uniform convergence in K. ■

Rule 16.3 (Abscissa of Convergence). Suppose the series $\sum_{n\ge 1} f(n)n^{-s}$ does not converge for all s or diverge for all s. Then there exists a real number σ_c, called the *abscissa of convergence*, such that this series converges if $\sigma>\sigma_c$, and diverges if $\sigma<\sigma_c$.

Proof. This is a direct consequence of the first part in Lemma 16.2. ■

Corollary 16.4 For any Dirichlet series $\sum_{n\ge 1} f(n)n^{-s}$ with σ_c finite, we have $0\le\sigma_a-\sigma_c\le 1$.

Proof. It is sufficient to show that if $\sum_{n\ge 1} f(n)n^{-s}$ converges at some s_0, then it is absolutely convergent for all s with $\sigma>\sigma_0+1$. Noting that from the above assumption, $|f(n)n^{-s_0}|$ is bounded. Further, $|f(n)n^{-s}|=|f(n)n^{-s_0}|\cdot n^{\sigma_0-\sigma}$. Therefore, we obtain the absolute convergence by comparison with the series $\sum_{n\ge 1} n^{\sigma_0-\sigma}$. ■

R The equality in $0\le\sigma_a-\sigma_c\le 1$ can occur in both cases: **(i).** For the Riemann zeta function $\sum_{n\ge 1}\frac{1}{n^s}$, we have $\sigma_a=\sigma_c=1$; **(ii).** For the alternating series $\sum_{n\ge 1}\frac{(-1)^n}{n^s}$, we have $\sigma_a=1$ and $\sigma_c=0$.

Rule 16.5 (Analyticity Theorem). Any Dirichlet series $F(s) = \sum_{n\geq 1} f(n)n^{-s}$ is analytic in its half-plane of convergence $\sigma > \sigma_c$, and its derivative $F'(s)$ is represented in this half-plane by the Dirichlet series

$$F'(s) = -\sum_{n\geq 1} \frac{f(n)\log n}{n^s}. \tag{16.1}$$

In particular, $F(s)$ and $F'(s)$ have the same abscissa of convergence and the same abscissa of absolute convergence.

Proof. Let us write $F_N(s) = \sum_{n\leq N} f(n)n^{-s}$ for N positive integers. Note that $F_N(s)$ is entire since each $f(n)n^{-s}$ is entire. Also, we know from the second part in Lemma 16.2 that as $N \to \infty$, $F_N(s)$ converges to $F(s)$, uniformly in every compact region contained in the half-plane $\sigma > \sigma_0$ for any $\sigma_0 > \sigma_c$. Since σ_0 can be taken arbitrarily close to σ_c, we may also replace σ_0 by σ_c in the above conclusion. Further, such a compact convergence implies the locally uniform convergence of $F_N(s) \to F(s)$ in the open half-plane $\sigma > \sigma_c$. Karl Weierstrass's theorem on uniformly convergent sequences of analytic functions (see, for instance, E. Freitagand R. Busam,*Complex Analysis*, 2nd Edition, Theorem III.1.3, p. 106) then asserts that $F(s)$ is analytic in the half-plane $\sigma > \sigma_c$. Further, its derivative is obtained by differentiating term by term. ■

Rule 16.6 (Uniqueness Theorem). Given two Dirichlet series

$$F(s) = \sum_{n\geq 1} \frac{f(n)}{n^s} \qquad \text{and} \qquad G(s) = \sum_{n\geq 1} \frac{g(n)}{n^s},$$

both convergent for $\sigma > \sigma_0$. If $F(s) = G(s)$ for each s in an infinite sequence $\{s_k\}$ such that $\sigma_k \to +\infty$ as $k \to \infty$, then $f(n) = g(n)$ for every n.

Proof. Note that the Dirichlet series for $h(n) = f(n) - g(n)$, denoted by $H(s)$, is also convergent for $\sigma > \sigma_0$. Meanwhile, $H(s) = F(s) - G(s)$. By Corollary 16.4, all the three series are absolute convergent for $\sigma > \sigma_0 + 1$. Without loss of generality, we assume that the sequence $\{s_k\}$ is such that $\sigma_0 + 1 < \sigma_1 < \sigma_2 < \cdots$. Supposing that $h(n)$ is not identical to zero for all n, there exists a smallest N with $h(N) \neq 0$ and $h(n) = 0$ for $n = 1, \ldots, N$. Noting that $H(s_k) = 0$, we have $h(N)N^{-s_k} = -\sum_{n\geq N+1} h(n)n^{-s_k}$. Hence,

$$|h(N)| \leq \sum_{n\geq N+1} |h(n)|\frac{N^{\sigma_k}}{n^{\sigma_k}} = \sum_{n\geq N+1} |h(n)|\frac{N^{\sigma_1}}{n^{\sigma_1}}\left(\frac{N}{n}\right)^{\sigma_k-\sigma_1} \leq \left(\sum_{n\geq N+1} |h(n)|\frac{N^{\sigma_1}}{n^{\sigma_1}}\right)\left(\frac{N}{N+1}\right)^{\sigma_k-\sigma_1}.$$

Note that $\sum_{n\geq N+1} |h(n)|\frac{N^{\sigma_1}}{n^{\sigma_1}}$ is a finite constant, independent of k. Letting $k \to \infty$ so that $(\sigma_k - \sigma_1) \to \infty$, we have $\left(\frac{N}{N+1}\right)^{\sigma_k-\sigma_1} \to 0$ and hence $h(N) = 0$. This leads to a contradiction, thereby implying that $h(n) = 0$, i.e. $f(n) = g(n)$, for all n. ■

16.2 Multiplication of Dirichlet series

Definition 16.2 For any arithmetic function f, we denote by $D(f;s)$ the Dirichlet series for f, namely,

$$D(f;s) := \sum_{n\geq 1} \frac{f(n)}{n^s}.$$

Theorem 16.7 Let f and g be arithmetic functions such that $D(f;s)$ and $D(g;s)$ have finite abscissas of absolute convergence. In the half-plane where both $D(f;s)$ and $D(g;s)$ converge absolutely, we have that $D(f*g;s)$ also converges absolutely in this half-plane, and that

$$D(f;s)D(g;s) = D(f*g;s), \tag{16.2}$$

where $f*g$ is the Dirichlet convolution of f and g.

Proof. Since the series $D(f;s)$ and $D(g;s)$ are absolutely convergent in the half-plane, so is their Cauchy product, which has the same value as $D(f;s)D(g;s)$. Note that the Cauchy product of $D(f;s) = \sum_{m\geq 1} \frac{f(m)}{m^s}$ and $D(g;s) = \sum_{n\geq 1} \frac{g(n)}{n^s}$ equals

$$\sum_{k\geq 2} \sum_{\substack{m,n\geq 1 \\ m+n=k}} \frac{f(m)g(n)}{(mn)^s} = \sum_{\ell\geq 1} \sum_{\substack{m,n\geq 1 \\ mn=\ell}} \frac{f(m)g(n)}{(mn)^s} = \sum_{\ell\geq 1} \frac{(f*g)(\ell)}{\ell^s} = D(f*g;s),$$

in which the first equality is valid as absolute convergence allows us to rearrange the terms without altering the sum. The desired result therefore follows. ■

Corollary 16.8 Let f be an arithmetic function with $f(1)\neq 0$, and let f^{-1} be the Dirichlet inverse of f. Then in any half-plane where $D(f;s)$ and $D(f^{-1};s)$ converge absolutely, we have $D(f;s)\neq 0$ and $D(f^{-1};s)\neq 0$. Also,

$$D(f^{-1};s) = \frac{1}{D(f;s)}. \tag{16.3}$$

Proof. We use the fact that $f*f^{-1} = \varepsilon$. Hence, by Theorem 16.7, $D(f;s)D(f^{-1};s) = D(\varepsilon;s) = 1$. ■

16.3 Dirichlet series for some arithmetic functions

Now, we present some examples of Dirichlet series.

■ **Example 16.1** The Dirichlet series for the constant function $\mathbf{1}$ is the *Riemann zeta function*

$$D(\mathbf{1};s) = \sum_{n\geq 1} \frac{1}{n^s} = \zeta(s). \tag{16.4}$$

Also, $D(\mathbf{1};s)$ has abscissa of absolute convergence $\sigma_a = 1$ and abscissa of convergence $\sigma(c) = 1$. ■

■ **Example 16.2** The Dirichlet series for the unit function ε is

$$D(\varepsilon;s) = 1. \tag{16.5}$$

Also, $D(\varepsilon;s)$ is absolutely convergent in $\mathbb{C}$. ■

■ **Example 16.3** The Dirichlet series for the identity function $\mathbf{id}$ is

$$D(\mathrm{id};s) = \sum_{n\geq 1} \frac{1}{n^{s-1}} = \zeta(s-1). \tag{16.6}$$

Also, $D(\mathrm{id};s)$ has abscissa of absolute convergence $\sigma_a = 2$ and abscissa of convergence $\sigma(c) = 2$. Further, if we define $\mathrm{id}^{\alpha}(n) = n^{\alpha}$ for all n with $\alpha \in \mathbb{C}$, then the Dirichlet series for id^{α} is

$$D(\mathrm{id}^{\alpha};s) = \sum_{n\geq 1} \frac{1}{n^{s-\alpha}} = \zeta(s-\alpha). \tag{16.7}$$

Also, $D(\mathrm{id}^{\alpha};s)$ has abscissa of absolute convergence $\sigma_a = 1+\Re(\alpha)$ and abscissa of convergence $\sigma(c) = 1+\Re(\alpha)$. ■

■ **Example 16.4** The Dirichlet series for the Möbius function μ is

$$D(\mu;s) = \sum_{n\geq 1} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}, \tag{16.8}$$

for $\sigma > 1$. This is because μ is the Dirichlet inverse of $\mathbf{1}$, i.e. $\mu * \mathbf{1} = \varepsilon$. ■

■ **Example 16.5** The Dirichlet series for the divisor function σ_{α} is

$$D(\sigma_{\alpha};s) = \sum_{n\geq 1} \frac{\sigma_{\alpha}(n)}{n^s} = \zeta(s)\zeta(s-\alpha), \tag{16.9}$$

for $\sigma > \max\{1, 1+\Re(\alpha)\}$. This is because $\sigma_{\alpha} = \mathbf{1} * \mathrm{id}^{\alpha}$, and hence $D(\sigma_{\alpha};s) = D(\mathbf{1};s)D(\mathrm{id}^{\alpha};s)$. In particular, the Dirichlet series for the number-of-divisors function d is

$$D(d;s) = \sum_{n\geq 1} \frac{d(n)}{n^s} = \zeta(s)^2, \tag{16.10}$$

for $\sigma > 1$, and the Dirichlet series for the sum-of-divisors function σ is

$$D(\sigma;s) = \sum_{n\geq 1} \frac{\sigma(n)}{n^s} = \zeta(s)\zeta(s-1), \tag{16.11}$$

for $\sigma > 2$. ■

■ **Example 16.6** The Dirichlet series for Euler's totient function ϕ is

$$D(\phi;s) = \sum_{n\geq 1} \frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}, \tag{16.12}$$

for $\sigma > 2$. This is because $\phi = \mu * \mathrm{id}$ by (13.5), and hence $D(\phi;s) = D(\mu;s)D(\mathrm{id};s)$. ■

■ **Example 16.7** The Dirichlet series for the logarithm function log is

$$D(\log;s) = \sum_{n\geq 1} \frac{\log(n)}{n^s} = -\zeta'(s), \tag{16.13}$$

where we make use of (16.1). Also, $D(\log;s)$ has abscissa of absolute convergence $\sigma_a = 1$ and abscissa of convergence $\sigma(c) = 1$. ■

■ **Example 16.8** The Dirichlet series for the Mangoldt function Λ is

$$D(\Lambda;s) = \sum_{n\geq 1} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}, \tag{16.14}$$

for $\sigma > 1$. This is because $\Lambda = \mu * \log$ by (13.8), and hence $D(\Lambda;s) = D(\mu;s)D(\log;s)$. ■

16.4 Euler products

Recall that in our proof of the divergence of $\sum_p \frac{1}{p}$ in Sect. 1.6, we make use of the following relation

$$\prod_{p\le N}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)=\sum_{\substack{n\ge 1\\ n \text{ has no factor } >N}}\frac{1}{n}. \tag{16.15}$$

This idea was first discovered by Euler, and in 1737 he proved the following theorem, also known as the analytic version of the fundamental theorem of arithmetic.

Theorem 16.9 (Euler). Let a be a multiplicative function such that the series $\sum_{n\ge 1} a(n)$ is absolutely convergent. Then this series can be expressed as an absolutely convergent infinite product indexed by prime numbers,

$$\sum_{n\ge 1} a(n)=\prod_p\big(1+a(p)+a(p^2)+\cdots\big). \tag{16.16}$$

In particular, if a is completely multiplicative, we have

$$\sum_{n\ge 1} a(n)=\prod_p\frac{1}{1-a(p)}. \tag{16.17}$$

R The infinite product in (16.16) is called the *Euler product* of the series $\sum_{n\ge 1} a(n)$.

Proof. We elaborate our argument for (16.15) in Sect. 1.6. Recall always that $a(1)=1$ since a is multiplicative. Let us define the partial product

$$P(N):=\prod_{p\le N}\big(1+a(p)+a(p^2)+\cdots\big).$$

Note that for each p, the series $\sum_{k\ge 0} a(p^k)$ is absolutely convergent as $\sum_{n\ge 1} a(n)$ converges absolutely. As a consequence, we may expand the product and rearrange the terms. On the other hand, for any n with the canonical form $n=\prod_j p_j^{\alpha_j}$ such that no prime factor is greater than N, i.e. $p_j\le N$ for all j, we have $a(n)=\prod_j a(p_j^{\alpha_j})$ since a is multiplicative, and it corresponds to exactly one term in the expansion of $P(N)$. Thus,

$$P(N)=\sum_{\substack{n\ge 1\\ n \text{ has no factor } >N}} a(n),$$

or equivalently,

$$\sum_{n\ge 1} a(n)-P(N)=\sum_{\substack{n\ge 1\\ n \text{ has at least one factor } >N}} a(n).$$

Hence, recalling that $\sum_{n\ge 1}|a(n)|$ converges, we have

$$\left|\sum_{n\ge 1} a(n)-P(N)\right|\le\sum_{n>N}|a(n)|\to 0 \qquad (\text{as } N\to\infty),$$

thereby implying that $P(N)\to\sum_{n\ge 1} a(n)$ as $N\to\infty$.

Now let us show that the infinite product in (16.16) is absolutely convergent. To see this, it is sufficient to prove that $\sum_p |u_p|$ converges where $u_p = a(p) + a(p^2) + \cdots$. This is obvious since

$$\sum_p |u_p| \leq \sum_p (|a(p)| + |a(p^2)| + \cdots) \leq \sum_{n\geq 2} |a(n)|,$$

while $\sum_{n\geq 2} |a(n)|$ is finite by the absolute convergence of $\sum_{n\geq 1} a(n)$.

Finally, when a is completely multiplicative, we have $a(p^k) = a(p)^k$ for all prime powers p^k. Therefore, the absolutely convergent subseries $\sum_{k\geq 0} a(p^k) = \sum_{k\geq 0} a(p)^k$ can be evaluated as a geometric series and hence equals $\frac{1}{1-a(p)}$. ■

Corollary 16.10 Let $\sum_{n\geq 1} f(n)n^{-s}$ be a Dirichlet series that converges absolutely in the half-plane $\sigma > \sigma_a$. If f is multiplicative, then for $\sigma > \sigma_a$,

$$\sum_{n\geq 1} \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\right). \tag{16.18}$$

In particular, if f is completely multiplicative, then for $\sigma > \sigma_a$,

$$\sum_{n\geq 1} \frac{f(n)}{n^s} = \prod_p \frac{1}{1 - f(p)p^{-s}}. \tag{16.19}$$

Proof. We simply use the fact that if $f(n)$ is multiplicative or completely multiplicative, so is $f(n)n^{-s}$. ■

■ **Example 16.9** We have the following Euler product expressions:

(i) $\displaystyle\sum_{n\geq 1} \frac{1}{n^s} = \zeta(s) = \prod_p \frac{1}{1-p^{-s}}$ for $\sigma > 1$;

(ii) $\displaystyle\sum_{n\geq 1} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)} = \prod_p (1-p^{-s})$ for $\sigma > 1$;

(iii) $\displaystyle\sum_{n\geq 1} \frac{\sigma_\alpha(n)}{n^s} = \zeta(s)\zeta(s-\alpha) = \prod_p \frac{1}{(1-p^{-s})(1-p^{\alpha-s})}$ for $\sigma > \max\{1, 1+\Re(\alpha)\}$;

(iv) $\displaystyle\sum_{n\geq 1} \frac{d(n)}{n^s} = \zeta(s)^2 = \prod_p \frac{1}{(1-p^{-s})^2}$ for $\sigma > 1$;

(v) $\displaystyle\sum_{n\geq 1} \frac{\sigma(n)}{n^s} = \zeta(s)\zeta(s-1) = \prod_p \frac{1}{(1-p^{-s})(1-p^{1-s})}$ for $\sigma > 2$;

(vi) $\displaystyle\sum_{n\geq 1} \frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} = \prod_p \frac{1-p^{-s}}{1-p^{1-s}}$ for $\sigma > 2$.

■

17. Dirichlet characters

17.1 Dirichlet characters

For the purpose of proving Dirichlet's theorem, another crucial tool is the *Dirichlet character*.

Definition 17.1 Let N be a positive integer. A *Dirichlet character* or a *character modulo N* is a complex-valued arithmetic function $\chi : \mathbb{Z}_{>0} \to \mathbb{C}$ with the following properties:

(i) $\chi(ab) = \chi(a)\chi(b)$, i.e., χ is completely multiplicative;

(ii) $\chi(a) \begin{cases} = 0 & \text{if } (a,N) > 1, \\ \neq 0 & \text{if } (a,N) = 1; \end{cases}$

(iii) $\chi(a+N) = \chi(a)$, i.e., χ is periodic with period N.

R We sometimes define Dirichlet characters on $\mathbb{Z}$ instead of $\mathbb{Z}_{>0}$ by the same conditions.

Example 17.1 For each positive integer N,

$$\chi_0(a) = \chi_{N,0}(a) = \begin{cases} 0 & \text{if } (a,N) > 1 \\ 1 & \text{if } (a,N) = 1 \end{cases}$$

is a Dirichlet character modulo N. We call this character the *principal character*. We will label Dirichlet characters modulo N by $\chi_{N,0}$, $\chi_{N,1}$, ..., or by χ_0, χ_1, ... if there is no ambiguity concerning the modulus. ■

Theorem 17.1 Let N be a positive integer and a be such that $(a,N) = 1$. Then for any character χ modulo N, $\chi(a)$ is a $\phi(N)$-th root of unity.

Proof. By the Fermat–Euler theorem, $a^{\phi(N)} \equiv 1 \pmod{N}$. Hence, $\chi(a)^{\phi(N)} = \chi(a^{\phi(N)}) = \chi(1) = 1$, where we use the fact that χ is completely multiplicative. ■

From Theorem 17.1, we see that if $\chi(a)$ is a real number, then it takes value only from $\{-1, 0, 1\}$.

Definition 17.2 Let χ be a Dirichlet character modulo a positive integer N. If all of its values are real, we say χ is a *real character*. Otherwise, it is called a *complex character*.

Example 17.2 The principal character modulo any N is real. Another example of real character is the Legendre symbol $\left(\frac{a}{p}\right)$ where the modulus $N = p$ is an odd prime. We will give some complex characters in later sections.

Theorem 17.2 Let N be a positive integer.

(i) If χ and χ' are two characters modulo N, so is their product $\chi\chi'$, defined by $\chi\chi'(a) := \chi(a)\chi'(a)$.

(ii) If χ is a character modulo N, so is its complex conjugate $\overline{\chi}$, defined by $\overline{\chi}(a) := \overline{\chi(a)}$, the complex conjugate of $\chi(a)$. In particular, $\chi\overline{\chi} = \chi_0$, the principal character.

Proof. The results follow by a direct verification of the three conditions in Definition 17.1. For the second part in (ii), we also use the fact that $z\overline{z} = |z|^2$ for any complex z, and any root of unity has absolute value 1. ■

Corollary 17.3 Let N be a positive integer. If χ is a real character modulo N, then $\chi^2 = \chi_0$, the principal character.

Proof. This is because for real χ, we have $\chi(a) \in \{-1, 1\}$ for all $(a,N) = 1$. Hence, $\chi^2(a) = \chi(a)^2 = (\pm 1)^2 = 1 = \chi_0(a)$. ■

Theorem 17.4 Let N be a positive integer and a be such that $(a,N) = 1$. Let $\overline{a}$ be the inverse of a modulo N, i.e., $a\overline{a} \equiv 1 \pmod{N}$. Then for any character χ modulo N, $\chi(\overline{a}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Proof. Noting that $a\overline{a} \equiv 1 \pmod{N}$, we have $\chi(a)\chi(\overline{a}) = \chi(a\overline{a}) = \chi(1) = 1$. Hence, $\chi(\overline{a}) = \chi(a)^{-1}$. Also, for any complex z with $|z| = 1$, we have $z^{-1} = \overline{z}$, giving the second equality. ■

17.2 Construction of Dirichlet characters modulo prime powers

Definition 17.3 For positive integers n, we define $\zeta_n := e^{\frac{2\pi i}{n}}$.

Construction 17.1 Let $N = 2$, or 4, or p^α with p an odd prime and α a positive integer. Let g be a primitive root of N. We know that $\{g^0, g^1, \dots, g^{\phi(N)-1}\}$ gives a reduced system modulo N. For each a with $(a,N) = 1$, we may find a unique integer d with $0 \le d < \phi(N)$ such that $a \equiv g^d \pmod{N}$. We call this d the *index of a modulo N with respect to g*, denoted by $\operatorname{ind} a = \operatorname{ind}_{N:g} a = d$. For any character χ modulo N, we know from Theorem 17.1 that $\chi(g)$ is a $\phi(N)$-th root of unity. We claim that this character χ is uniquely determined by $\chi(g)$. This is because for any a with $(a,N) = 1$, we have $\chi(a) = \chi(g^{\operatorname{ind} a}) = \chi(g)^{\operatorname{ind} a}$.

Example 17.3 For $N = 2$, we choose the primitive root $g = 1$; for $N = 3$, we choose the primitive root $g = 2$; for $N = 5$, we choose the primitive root $g = 2$.

a	1
$\operatorname{ind}_{2:1} a$	0

a χ	1
$\chi_{2,0}$	1

a	1	2
$\operatorname{ind}_{3:2} a$	0	1

a χ	1	2
$\chi_{3,0}$	1	1
$\chi_{3,1}$	1	-1

a	1	2	3	4
$\operatorname{ind}_{5:2} a$	0	1	3	2

a χ	1	2	3	4
$\chi_{5,0}$	1	1	1	1
$\chi_{5,1}$	1	i	$-i$	-1
$\chi_{5,2}$	1	-1	-1	1
$\chi_{5,3}$	1	$-i$	i	-1

For $N = 2^\alpha$ with $\alpha \ge 3$, however, we know from Theorem 5.15 that N has no primitive roots. Hence, a different construction is necessary.

Lemma 17.5 For $\alpha \geq 3$, we have $\operatorname{ord}_{2^\alpha} 5 = 2^{\alpha-2}$.

Proof. We have seen from the proof of Theorem 5.15 that $5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$. Now, it suffices to show that $5^{2^{\alpha-3}} = 1 + 2^{\alpha-1}x$ with $2 \nmid x$, so that $5^{2^{\alpha-3}} \not\equiv 1 \pmod{2^\alpha}$. We prove this claim by induction on α. For $\alpha = 3$, we have $5^{2^0} = 5 = 1 + 2^2 \cdot 1$. Now, we assume that the claim is true for some $\alpha \geq 3$, and we prove the $\alpha + 1$ case. Note that

$$5^{2^{(\alpha+1)-3}} = \left(5^{2^{\alpha-3}}\right)^2 = \left(1 + 2^{\alpha-1}x\right)^2 = 1 + 2^\alpha\left(x + 2^{\alpha-2}x^2\right).$$

Here, $x + 2^{\alpha-2}x^2$ is odd since x is odd and $\alpha \geq 3$. We remark that above argument also gives another confirmation of $5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$. ■

Lemma 17.6 Let $N = 2^\alpha$ with $\alpha \geq 3$. For every odd integer a, there exists unique integers $\nu_{N:-1}(a)$ and $\nu_{N:5}(a)$ with $0 \leq \nu_{N:-1}(a) < 2$ and $0 \leq \nu_{N:5}(a) < 2^{\alpha-2}$ such that $a \equiv (-1)^{\nu_{N:-1}(a)} 5^{\nu_{N:5}(a)} \pmod{N}$.

Proof. It suffices to show that $\{(-1)^u 5^v : 0 \leq u < 2 \text{ and } 0 \leq v < 2^{\alpha-2}\}$ is a reduced system modulo $N = 2^\alpha$. First, the $2^{\alpha-2}$ numbers 5^v (with $0 \leq v < 2^{\alpha-2}$) are pairwise incongruent modulo N since $\operatorname{ord}_{2^\alpha} 5 = 2^{\alpha-2}$ by Lemma 17.5. The same property also holds true for the $2^{\alpha-2}$ numbers -5^v (with $0 \leq v < 2^{\alpha-2}$). Finally, we see that $5^{u_1} \not\equiv -5^{u_2} \pmod{N}$ since $5^{u_1} \equiv 1 \pmod{4}$, while $-5^{u_1} \equiv 3 \pmod{4}$, where we recall that $4 \mid N$. ■

■ **Construction 17.2** Let $N = 2^\alpha$ with $\alpha \geq 3$. For any character χ modulo N, we find that $\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1$, implying that $\chi(-1)$ is a quadratic root of unity. Also, since $\operatorname{ord}_N 5 = 2^{\alpha-2} = \frac{\phi(N)}{2}$ by Lemma 17.5, we have that $\chi(5)$ is a $\frac{\phi(N)}{2}$-th root of unity. We claim that this character χ is uniquely determined by $\chi(-1)$ and $\chi(5)$. This is because for any a with $(a,N) = 1$, we know from Lemma 17.6 that $\chi(a) = \chi((-1)^{\nu_{N:-1}(a)} 5^{\nu_{N:5}(a)}) = \chi(-1)^{\nu_{N:-1}(a)} \chi(5)^{\nu_{N:5}(a)}$. ■

■ **Example 17.4** For $N = 2^3 = 8$, we have $\chi(-1) \in \{1, -1\}$ and $\chi(5) \in \{1, -1\}$. We write the characters modulo N as $\chi_{(\chi(-1);\chi(5))}$ for clarity. ■

a	1	3	5	7
$\nu_{8:-1}(a)$	0	1	0	1
$\nu_{8:5}(a)$	0	1	1	0

a χ	1	3	5	7
$\chi_{(1;1)}$	1	1	1	1
$\chi_{(1;-1)}$	1	-1	-1	1
$\chi_{(-1;1)}$	1	-1	1	-1
$\chi_{(-1;-1)}$	1	1	-1	-1

Corollary 17.7 Let N be a prime power. Then there are exactly $\phi(N)$ characters modulo N. In particular, for any a with $(a,N) = 1$ and $a \not\equiv 1 \pmod{N}$, there always exists a character χ such that $\chi(a) \neq 1$.

Proof. For $N = 2$, or 4, or p^α with p an odd prime and α a positive integer, the first part comes from the fact that the number of $\phi(N)$-th roots of unity is $\phi(N)$, namely, $\zeta_{\phi(N)}^0 = 1$, $\zeta_{\phi(N)}^1$, $\ldots$, $\zeta_{\phi(N)}^{\phi(N)-1}$. Hence, there are exactly $\phi(N)$ choices of $\chi(g)$ as in Construction 17.1, and thus exactly $\phi(N)$ characters modulo N. Finally, for any a with $(a,N) = 1$ and $a \not\equiv 1 \pmod{N}$, we know that $0 < \operatorname{ind} a < \phi(N)$. Hence, we choose a character χ such that $\chi(g) = \zeta_{\phi(N)}$, and thus $\chi(a) = \zeta_{\phi(N)}^{\operatorname{ind} a} \neq 1$.

For $N = 2^\alpha$ with $\alpha \geq 3$, the first part comes from the fact that the number of quadratic roots of unity is 2, namely 1 and -1; and the number of $\frac{\phi(N)}{2}$-th roots of unity is $\frac{\phi(N)}{2}$, namely, $\zeta^0_{\phi(N)/2} = 1$, $\zeta^1_{\phi(N)/2}$, $\dots$, $\zeta^{\phi(N)/2-1}_{\phi(N)/2}$. Hence, there are exactly 2 choices of $\chi(-1)$ and exactly $\frac{\phi(N)}{2}$ choices of $\chi(5)$ as in Construction 17.2, and thus exactly $2 \cdot \frac{\phi(N)}{2} = \phi(N)$ characters modulo N. Finally, for any a with $(a,N) = 1$ and $a \not\equiv 1 \pmod N$, we see from Lemma 17.6 that at least one of $\nu_{N:-1}(a)$ and $\nu_{N:5}(a)$ is not zero. If $\nu_{N:-1}(a) \neq 0$ (and hence $\nu_{N:-1}(a) = 1$), we choose a character χ such that $\chi(-1) = -1$ and $\chi(5) = 1$, and thus $\chi(a) = (-1)^1 \cdot 1 = -1 \neq 1$; if $\nu_{N:5}(a) \neq 0$ (and hence $0 < \nu_{N:5}(a) < \frac{\phi(N)}{2}$), we choose a character χ such that $\chi(-1) = 1$ and $\chi(5) = \zeta_{\phi(N)/2}$, and thus $\chi(a) = 1 \cdot \zeta^{\nu_{N:5}(a)}_{\phi(N)/2} \neq 1$. ■

17.3 Construction of Dirichlet characters modulo general integers

Now, we construct characters modulo general integers.

Lemma 17.8 Let m and n be positive integers such that $(m,n) = 1$, and write $N = mn$. There exist a unique reduced system $R_n(m) := \{r_{m,1}, \dots, r_{m,\phi(m)}\}$ modulo m such that $1 \le r_{m,i} \le N$ and $r_{m,i} \equiv 1 \pmod n$ for all i, and a unique reduced system $R_m(n) := \{r_{n,1}, \dots, r_{n,\phi(n)}\}$ modulo n such that $1 \le r_{n,j} \le N$ and $r_{n,j} \equiv 1 \pmod m$ for all j. In particular,

(i) $(r_{m,i}, N) = 1$ for all i and $(r_{n,j}, N) = 1$ for all j;

(ii) $R_n(m) \cap R_m(n) = \{1\}$.

Proof. By Chinese remainder theorem, the system

$$\begin{cases} x_a \equiv a & \pmod m \\ x_a \equiv 1 & \pmod n \end{cases}$$

has a unique solution modulo N. Running a over a reduced system modulo m and choosing the solutions x_a so that $1 \le x_a \le N$, we arrive the unique reduced system $R_n(m)$ modulo m. Similarly, we have the unique reduced system $R_m(n)$ modulo n. Further, $(r_{m,i}, m) = 1$ by definition. Also, $r_{m,i} \equiv 1 \pmod n$ implies that $(r_{m,i}, n) = 1$. Hence, $(r_{m,i}, N) = 1$. By symmetry, we also have $(r_{n,j}, N) = 1$. Finally, if $r \in R_n(m) \cap R_m(n)$, then $r \equiv 1 \pmod m$ and $r \equiv 1 \pmod n$, and hence the only possibility is $r = 1$. ■

Lemma 17.9 Let m and n be positive integers such that $(m,n) = 1$, and write $N = mn$. Let $R_n(m) = \{r_{m,1}, \dots, r_{m,\phi(m)}\}$ and $R_m(n) = \{r_{n,1}, \dots, r_{n,\phi(n)}\}$ be as in Lemma 17.8. Then for any a such that $(a,N) = 1$, there are unique integers $r_{m,i} \in R_n(m)$ and $r_{n,j} \in R_m(n)$ such that $a \equiv r_{m,i} r_{n,j} \pmod N$.

Proof. Note that there are $\phi(m)\phi(n) = \phi(N)$ such $r_{m,i} r_{n,j}$. Further, by Lemma 17.8, $(r_{m,i} r_{n,j}, N) = 1$. Now, it suffices to show that they are pairwise incongruent modulo N. If we have $r_{m,i} r_{n,j} \equiv r_{m,i'} r_{n,j'} \pmod N$, then it implies that $r_{m,i} r_{n,j} \equiv r_{m,i'} r_{n,j'} \pmod m$ and hence $r_{m,i} \equiv r_{m,i'} \pmod m$ since $r_{n,j} \equiv r_{n,j'} \equiv 1 \pmod m$. Similarly, we have $r_{n,j} \equiv r_{n,j'} \pmod n$. The desired result thus follows. ■

■ **Construction 17.3** Let m and n be positive integers such that $(m,n) = 1$, and write $N = mn$. Let $R_n(m) = \{r_{m,1}, \dots, r_{m,\phi(m)}\}$ and $R_m(n) = \{r_{n,1}, \dots, r_{n,\phi(n)}\}$ be as in Lemma 17.8. For each character χ' modulo m and character χ'' modulo n, we define $[\chi', \chi''] =: \chi$ by

$$\chi(a) = \begin{cases} 0 & \text{if } (a,N) > 1, \\ \chi'(r_{m,i})\chi''(r_{n,j}) & \text{if } (a,N) = 1, \end{cases}$$

where we use Lemma 17.9 to write $a \equiv r_{m,i} r_{n,j} \pmod N$ for the second case. ■

Theorem 17.10 The function χ as in Construction 17.3 is a character modulo N.

Proof. It is sufficient to show that χ is completely multiplicative. In particular, given a and b with $(a,N) = (b,N) = 1$, we want to show that $\chi(ab) = \chi(a)\chi(b)$. By Lemma 17.9, we write $a \equiv r_{m,i_1}r_{n,j_1} \pmod N$, $b \equiv r_{m,i_2}r_{n,j_2} \pmod N$ and $ab \equiv r_{m,I}r_{n,J} \pmod N$. Hence, $r_{m,I}r_{n,J} \equiv r_{m,i_1}r_{m,i_2}r_{n,j_1}r_{n,j_2} \pmod N$, and further $r_{m,I}r_{n,J} \equiv r_{m,i_1}r_{m,i_2}r_{n,j_1}r_{n,j_2} \pmod m$. Since $r_{n,J} \equiv r_{n,j_1} \equiv r_{n,j_2} \equiv 1 \pmod m$, we have $r_{m,I} \equiv r_{m,i_1}r_{m,i_2} \pmod m$, and therefore, $\chi'(r_{m,I}) = \chi'(r_{m,i_1}r_{m,i_2}) = \chi'(r_{m,i_1})\chi'(r_{m,i_2})$. Similarly, $\chi''(r_{n,J}) = \chi''(r_{n,j_1})\chi''(r_{n,j_2})$. It follows that

$$\chi(ab) = \chi'(r_{m,I})\chi''(r_{n,J}) = \chi'(r_{m,i_1})\chi'(r_{m,i_2})\chi''(r_{n,j_1})\chi''(r_{n,j_2}) = \chi(a)\chi(b),$$

as required. ■

■ **Example 17.5** For $N = 3 \cdot 5 = 15$, we first find that $R_5(3) = \{1, 11\}$ and $R_3(5) = \{1, 7, 13, 4\}$, and then compute $r_{3,i}r_{5,j}$ mod 15 for each i and j. The characters modulo 3 and 5 are given in Example 17.3. ■

$r_{5,j}$ $r_{3,i}$	1	7	13	4
1	1	7	13	4
11	11	2	8	14

a χ	1	2	4	7	8	11	13	14
$[\chi_{3,0}, \chi_{5,0}]$	1	1	1	1	1	1	1	1
$[\chi_{3,0}, \chi_{5,1}]$	1	i	-1	i	$-i$	1	$-i$	-1
$[\chi_{3,0}, \chi_{5,2}]$	1	-1	1	-1	-1	1	-1	1
$[\chi_{3,0}, \chi_{5,3}]$	1	$-i$	-1	$-i$	i	1	i	-1
$[\chi_{3,1}, \chi_{5,0}]$	1	-1	1	1	-1	-1	1	-1
$[\chi_{3,1}, \chi_{5,1}]$	1	$-i$	-1	i	i	-1	$-i$	1
$[\chi_{3,1}, \chi_{5,2}]$	1	1	1	-1	1	-1	-1	-1
$[\chi_{3,1}, \chi_{5,3}]$	1	i	-1	$-i$	$-i$	-1	i	1

The following are implications of Construction 17.3.

Theorem 17.11 Let m and n be positive integers such that $(m,n) = 1$, and write $N = mn$. If $[\chi', \chi''] = [\hat{\chi}', \hat{\chi}'']$ with χ' and $\hat{\chi}'$ characters modulo m, and χ'' and $\hat{\chi}''$ characters modulo m, then $\chi' = \hat{\chi}'$ and $\chi'' = \hat{\chi}''$.

Proof. For each $r_{m,i} \in R_n(m)$, we note that $r_{m,i} \equiv r_{m,i} \cdot 1 \pmod N$ while $1 \in R_m(n)$. Hence, $[\chi', \chi''] = [\hat{\chi}', \hat{\chi}'']$ implies that $[\chi', \chi''](r_{m,i}) = [\hat{\chi}', \hat{\chi}''](r_{m,i})$, or $\chi'(r_{m,i})\chi''(1) = \hat{\chi}'(r_{m,i})\hat{\chi}''(1)$, or $\chi'(r_{m,i}) = \hat{\chi}'(r_{m,i})$. Since $R_n(m)$ is a reduced system modulo m, we have $\chi' = \hat{\chi}'$. By symmetry, we also have $\chi'' = \hat{\chi}''$. ■

Theorem 17.12 Let m and n be positive integers such that $(m,n) = 1$, and write $N = mn$. Let $\chi = [\chi', \chi'']$. If $\chi' = \chi_{m,0}$, the principal character modulo m, then for any a with $(a,N) = 1$, we have $\chi(a) = \chi''(a)$. Also, if $\chi'' = \chi_{n,0}$, the principal character modulo n, then for any a with $(a,N) = 1$, we have $\chi(a) = \chi'(a)$.

Proof. For any a with $(a,N) = 1$. We write $a \equiv r_{m,i}r_{n,j} \pmod N$ as in Construction 17.3, and hence $a \equiv r_{m,i}r_{n,j} \pmod n$. Noting that $r_{m,i} \equiv 1 \pmod n$ by definition, we have $a \equiv r_{n,j} \pmod n$. If $\chi' = \chi_{m,0}$, then $\chi(a) = \chi_{m,0}(r_{m,i})\chi''(r_{n,j}) = \chi''(r_{n,j}) = \chi''(a)$, as required. We further derive the second part by symmetry. ■

Theorem 17.13 Let m and n be positive integers such that $(m,n) = 1$, and write $N = mn$. There are no characters modulo N other than those as constructed in Construction 17.3.

Proof. To show that there are no other characters modulo N, if suffices to prove that for each character χ modulo N, we can find a character χ' modulo m and a character χ''

modulo n such that $\chi = [\chi', \chi'']$. Let $R_n(m) = \{r_{m,1}, \dots, r_{m,\phi(m)}\}$ and $R_m(n) = \{r_{n,1}, \dots, r_{n,\phi(n)}\}$ be as in Construction 17.3. We first define

$$\chi|_m(a) = \begin{cases} 0 & \text{if } (a,m) > 1, \\ \chi(r_{m,i}) & \text{if } (a,m) = 1 \text{ and } a \equiv r_{m,i} \pmod{m}. \end{cases}$$

We claim that $\chi|_m$ is a character modulo m. In fact, it suffices to show that $\chi|_m$ is completely multiplicative. For any a and b with $(a,m) = (b,m) = 1$, we assume that $a \equiv r_{m,i'} \pmod{m}$, $b \equiv r_{m,i''} \pmod{m}$ and $ab \equiv r_{m,I} \pmod{m}$. Then $r_{m,I} \equiv r_{m,i'} r_{m,i''} \pmod{m}$. Also, $r_{m,I} \equiv 1 \equiv r_{m,i'} r_{m,i''} \pmod{n}$ by definition. Hence, by Chinese remainder theorem, $r_{m,I} \equiv r_{m,i'} r_{m,i''} \pmod{N}$. We then have

$$\chi|_m(ab) = \chi(r_{m,I}) = \chi(r_{m,i'} r_{m,i''}) = \chi(r_{m,i'})\chi(r_{m,i''}) = \chi|_m(a)\chi|_m(b),$$

as required. Similarly, we define

$$\chi|_n(a) = \begin{cases} 0 & \text{if } (a,n) > 1, \\ \chi(r_{n,j}) & \text{if } (a,n) = 1 \text{ and } a \equiv r_{n,j} \pmod{n}, \end{cases}$$

and find that $\chi|_n$ is a character modulo n. Finally, we claim that $\chi = [\chi|_m, \chi|_n]$. In fact, if we write $[\chi|_m, \chi|_n] = \tilde{\chi}$, then for any a with $(a,N) = 1$, we write $a \equiv r_{m,i} r_{n,j} \pmod{N}$, and thus,

$$\tilde{\chi}(a) = \chi|_m(r_{m,i})\chi|_n(r_{n,j}) = \chi(r_{m,i})\chi(r_{n,j}) = \chi(r_{m,i} r_{n,j}) = \chi(a),$$

as desired. ■

Corollary 17.14 Let m and n be positive integers such that $(m,n) = 1$, and write $N = mn$.

(i) If there are A characters modulo m and B characters modulo n, provided that A and B are finite, then there are AB characters modulo N;

(ii) If for each u with $(u,m) = 1$ and $u \not\equiv 1 \pmod{m}$ there exists a character χ' modulo m such that $\chi'(u) \neq 1$, and for each v with $(v,n) = 1$ and $v \not\equiv 1 \pmod{n}$ there exists a character χ'' modulo n such that $\chi''(v) \neq 1$, then for each w with $(w,N) = 1$ and $w \not\equiv 1 \pmod{N}$ there exists a character χ modulo N such that $\chi(w) \neq 1$.

Proof. Part (i) is a direct consequence of Construction 17.3 and Theorems 17.10, 17.11 and 17.13. For Part (ii), we note that $(w,N) = 1$ implies that $(w,m) = 1$ and $(w,n) = 1$. Also, since $w \not\equiv 1 \pmod{N}$, we have either $w \not\equiv 1 \pmod{m}$ or $w \not\equiv 1 \pmod{n}$. Otherwise, if $w \equiv 1 \pmod{m}$ and $w \equiv 1 \pmod{n}$, then Chinese remainder theorem tells us that $w \equiv 1 \pmod{N}$. Now, if $w \not\equiv 1 \pmod{m}$, we choose $\chi = [\chi', \chi_{n,0}]$ with $\chi'(w) \neq 1$ and use 17.12 to obtain that $\chi(w) = \chi'(w) \neq 1$. Similarly, if $w \not\equiv 1 \pmod{n}$, we choose $\chi = [\chi_{m,0}, \chi'']$ with $\chi''(w) \neq 1$. ■

Theorem 17.15 For any positive integer N, there are exactly $\phi(N)$ characters modulo N. In particular, for any a with $(a,N) = 1$ and $a \not\equiv 1 \pmod{N}$, there always exists a character χ such that $\chi(a) \neq 1$.

Proof. First, there is a unique character modulo 1, namely, $\chi_{1,0}(a) = 1$ for all a. Also, there exists no a such that $a \not\equiv 1 \pmod{1}$. Now, we assume that $N \geq 2$. We write N in the canonical form $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$. Using Corollary 17.7 as base cases, we iteratively apply Corollary 17.14 and derive that there are $\phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})$ characters modulo $p_1^{\alpha_1} p_2^{\alpha_2}$, …, and $\phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_\ell^{\alpha_\ell}) = \phi(N)$ characters modulo N. The second part also holds true by this argument. ■

Theorem 17.16 Let N be a positive integer and $\{\chi_0,\dots,\chi_{\phi(N)-1}\}$ be the set of characters modulo N. Then for any $\chi\in\{\chi_1,\dots,\chi_{\phi(N)}\}$, the set $\{\chi\chi_1,\dots,\chi\chi_{\phi(N)-1}\}$ also covers all characters modulo N.

Proof. This follows from the trivial fact that if $\chi\chi_i=\chi\chi_j$, then $\chi_i=\chi_j$. ■

R In general, we may define characters on a group G as group homomorphisms from G to the multiplicative group of a field, usually the field of complex numbers. If G is a finite Abelian group, then the number of characters equals the size of G. The Dirichlet characters modulo N coorspond to the case of the finite Abelian group $(\mathbb{Z}/N\mathbb{Z})^\times$, which is of size $\phi(N)$.

17.4 Orthogonality relations for Dirichlet characters

As we are comfortable with the construction of all Dirichlet characters for a given modulus, we shall establish one of their most important properties, the *orthogonality*.

Theorem 17.17 Let N be a positive integer.

(i) For any Dirichlet character χ modulo N,

$$\sum_{a=1}^{N}\chi(a)=\begin{cases}\phi(N) & \text{if } \chi=\chi_0,\\ 0 & \text{otherwise,}\end{cases}\tag{17.1}$$

where χ_0 is the principal character modulo N;

(ii) For any integer $a\in\mathbb{Z}_{>0}$,

$$\sum_{\chi \bmod N}\chi(a)=\begin{cases}\phi(N) & \text{if } a\equiv 1 \pmod N,\\ 0 & \text{otherwise,}\end{cases}\tag{17.2}$$

where the summation runs over all Dirichlet characters modulo N.

Proof. Part (i) is trivial when $\chi=\chi_0$. If $\chi\neq\chi_0$, we choose k with $(k,N)=1$ and $\chi(k)\neq 1$. By Theorem 3.6, $\{k,2\cdot k,\dots,N\cdot k\}$ gives a complete system modulo N. Hence,

$$\chi(k)\sum_{a=1}^{N}\chi(a)=\sum_{a=1}^{N}\chi(ak)=\sum_{a=1}^{N}\chi(a),$$

implying the desired result since $\chi(k)\neq 1$.

For Part (ii), it is trivial when $a\equiv 1 \pmod N$ or $(a,N)>1$. If a is such that $(a,N)=1$ and $a\not\equiv 1 \pmod N$, by Theorem 17.15, we have a character $\tilde{\chi}$ modulo N such that $\tilde{\chi}(a)\neq 1$. Also, Theorem 17.16 tells us that if χ run over all characters modulo N, so do $\tilde{\chi}\chi$. Hence,

$$\tilde{\chi}(a)\sum_{\chi \bmod N}\chi(a)=\sum_{\chi \bmod N}\tilde{\chi}\chi(a)=\sum_{\chi \bmod N}\chi(a),$$

yielding the required result since $\tilde{\chi}(a)\neq 1$. ■

Corollary 17.18 Let χ be a non-principal character modulo a positive integer N. For

$n \geq 1$,

$$\left|\sum_{a=1}^{n} \chi(a)\right| \leq \phi(N). \tag{17.3}$$

Proof. We write $n = qN + r$ where $0 \leq r < N$. Then with recourse to (17.1),

$$\left|\sum_{a=1}^{n} \chi(a)\right| = \left|\left(\sum_{k=0}^{q-1}\sum_{a=1}^{N} \chi(kN+a)\right) + \sum_{a=1}^{r} \chi(qN+a)\right| = \left|\sum_{a=1}^{r} \chi(a)\right| \leq \sum_{a=1}^{r} |\chi(a)| \leq \phi(N),$$

since among $|\chi(1)|, \ldots, |\chi(N-1)|$, there are exactly $\phi(N)$ of them equal to 1, and all others are 0. ■

Theorem 17.19 (Orthogonality Relations). Let N be a positive integer.

(i) For any Dirichlet characters χ_1, χ_2 modulo N,

$$\sum_{a=1}^{N} \chi_1(a)\overline{\chi_2(a)} = \begin{cases} \phi(N) & \text{if } \chi_1 = \chi_2, \\ 0 & \text{otherwise;} \end{cases} \tag{17.4}$$

(ii) For any integers $a_1, a_2 \in \mathbb{Z}_{>0}$,

$$\sum_{\chi \bmod N} \chi(a_1)\overline{\chi(a_2)} = \begin{cases} \phi(N) & \text{if } a_1 \equiv a_2 \pmod{N} \text{ and } (a_1,N) = (a_2,N) = 1, \\ 0 & \text{otherwise,} \end{cases} \tag{17.5}$$

where the summation runs over all Dirichlet characters modulo N.

Proof. For Part (i), we use (17.1) by noting from Theorem 17.2 that $\chi_1(a)\overline{\chi_2(a)} = \chi_1\overline{\chi_2}(a)$ and $\chi_1\overline{\chi_2} = \chi_0$ when $\chi_1 = \chi_2$. For Part (ii), we use (17.2) by noting from Theorem 17.4 that $\chi(a_1)\overline{\chi(a_2)} = \chi(a_1)\chi(\overline{a_2}) = \chi(a_1\overline{a_2})$ whenever a_2 is invertible modulo N. ■

The orthogonality relation (17.5) is by far the most crucial, as it allows one to extract terms satisfying a given congruence from a sum.

Definition 17.4 Let N be a positive integer and a be an integer. We define

$$\mathbf{1}_a(x) = \mathbf{1}_{N,a}(x) := \begin{cases} 1 & \text{if } x \equiv a \pmod{N}, \\ 0 & \text{otherwise.} \end{cases}$$

Corollary 17.20 Let N be a positive integer and a be an integer such that $(a,N) = 1$. We have

$$\mathbf{1}_a(x) = \frac{1}{\phi(N)} \sum_{\chi \bmod N} \overline{\chi(a)}\chi(x), \tag{17.6}$$

where the summation runs over all Dirichlet characters modulo N.

Proof. This is simply (17.5) with $a_1 = x$ and $a_2 = a$. ■

18. Dirichlet's Theorem

18.1 Riemann zeta function

Now we shall take a formal look at the *Riemann zeta function*.

Definition 18.1 For s a complex variable with $\Re(s) > 1$, the *Riemann zeta function* is defined by

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

We have seen from the theory of Dirichlet series that the series $\sum_{n\geq 1} \frac{1}{n^s}$ is absolutely convergent in the half-plane $\sigma > 1$, and the Riemann zeta function is analytic in its domain. Further, we have the Euler product for $\zeta(s)$ by taking $f = \mathbf{1}$ in (16.19).

Theorem 18.1 For $\sigma > 1$,

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}. \tag{18.1}$$

As for many other functions of a complex variable, we also hope to extend the domain of definition of the Riemann zeta function through analytic continuation.

Lemma 18.2 Suppose that $s \neq 1$ is in the half-plane $\sigma > 0$. For $x > 0$,

$$\zeta(s) = \sum_{n\leq x} \frac{1}{n^s} + \frac{x^{1-s}}{s-1} + \frac{\{x\}}{x^s} - s\int_x^\infty \frac{\{u\}}{u^{s+1}} du. \tag{18.2}$$

Proof. We start with the case $\sigma > 1$. Note that $\zeta(s) = \sum_{n\leq x} n^{-s} + \sum_{n>x} n^{-s}$. For the second sum, we make use of Euler's summation formula (15.2),

$$\begin{aligned}\sum_{x<n\leq y} \frac{1}{n^s} &= \int_x^y \frac{du}{u^s} - s\int_x^y \frac{\{u\}}{u^{s+1}} du + \frac{\{x\}}{x^s} - \frac{\{y\}}{y^s} \\ &= \frac{x^{1-s}}{s-1} - \frac{y^{1-s}}{s-1} + \frac{\{x\}}{x^s} - \frac{\{y\}}{y^s} - s\int_x^y \frac{\{u\}}{u^{s+1}} du.\end{aligned}$$

Noting that $\sigma > 1$, we let $y \to \infty$ and derive that

$$\sum_{n>x} \frac{1}{n^s} = \frac{x^{1-s}}{s-1} + \frac{\{x\}}{x^s} - s\int_x^\infty \frac{\{u\}}{u^{s+1}} du,$$

which proves (18.2) for $\sigma > 1$. This is doable since the integral $\int_x^\infty \{u\} u^{-s-1} du$ is convergent in the half-plane $\sigma > 0$ by comparison with $\int_x^\infty u^{-\sigma-1} du$. The convergence is also uniform in every compact region contained in the half-plane $\sigma > 0$, and hence locally uniform in this open half-plane. By Weierstrass's theorem on uniformly convergent sequences of analytic functions, we see that the integral $\int_x^\infty \{u\} u^{-s-1} du$ is an analytic function for $\sigma > 0$. By the uniqueness of analytic continuation the formula (18.2) is valid in this larger half-plane. ■

Theorem 18.3 For $s \neq 1$ with $\sigma > 0$,

$$\zeta(s) = \frac{s}{s-1} - s\int_1^\infty \frac{\{u\}}{u^{s+1}} du. \tag{18.3}$$

In particular, $\zeta(s)$ is analytic in the half-plane $\sigma > 0$ but with a simple pole at $s = 1$, with residue 1.

Proof. We take $x = 1$ in (18.2) to get (18.3). The simple pole at $s = 1$ comes from $\frac{s}{s-1}$, as we have shown earlier that the integral in (18.3) is analytic in the half-plane $\sigma > 0$. ■

R In general, the Riemann zeta function can be analytically continued to $\mathbb{C}\backslash\{1\}$. This can be achieved by applying the Euler–Maclaurin formula, which extends Euler's summation formula (15.2) via repeated integration by parts. A more immediate way is by invoking the functional equation for the Riemann zeta function

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos(\tfrac{\pi s}{2})\zeta(s),$$

where $\Gamma(s)$ is the Gamma function; see T. M. Apostol, Ch. 12.

18.2 Dirichlet L-functions

Noting that the Dirichlet characters are arithmetic functions, we may further consider their associated Dirichlet series.

Definition 18.2 Let χ be a Dirichlet character modulo N. Its Dirichlet series

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

is called the *Dirichlet L-function*, or the *Dirichlet L-series*, associated with χ.

Recall that we have $\chi(n) = 0$ if $(n,N) > 1$ by definition, and $|\chi(n)| = 1$ if $(n,N) = 1$ by Theorem 17.1. Therefore, the series $\sum_{n\geq 1} \frac{\chi(n)}{n^s}$ is absolutely convergent in the half-plane $\sigma > 1$. Noting that χ is completely multiplicative, we then derive the Euler product for $L(s,\chi)$ by taking $f = \chi(n)$ in (16.19).

Theorem 18.4 Let χ be a Dirichlet character modulo N. For $\sigma > 1$,

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}}. \tag{18.4}$$

Now, we work on the analytic properties of Dirichlet L-functions.

Theorem 18.5 Let χ_0 be the principal Dirichlet character modulo N. For $s \neq 1$ with $\sigma > 0$,

$$L(s,\chi_0) = \zeta(s) \prod_{p|N} \left(1 - \frac{1}{p^s}\right). \tag{18.5}$$

In particular, $L(s,\chi_0)$ is analytic in the half-plane $\sigma > 0$ but with a simple pole at $s = 1$, with residue $\phi(N)/N$.

Proof. It is sufficient to prove (18.5) for $\sigma > 1$; we may then analytically extend the domain to the larger half-plane $\sigma > 0$ as $\prod_{p|N}\left(1 - \frac{1}{p^s}\right)$ is entire. Since χ_0 is principal, we have $\chi(p) = 1$ if $p \nmid N$, and 0 if $p \mid N$. For $\sigma > 1$, we derive from the Euler products for $\zeta(s)$ and $L(s,\chi_0)$ that

$$L(s,\chi_0) = \prod_{p \nmid N} \frac{1}{1-p^{-s}} = \prod_{p} \frac{1}{1-p^{-s}} \prod_{p|N} (1-p^{-s}) = \zeta(s) \prod_{p|N} (1-p^{-s}),$$

as required. The simple pole of $L(s,\chi)$ at $s = 1$ comes from the simple pole of $\zeta(s)$. Also, the residue at $s = 1$ equals $\prod_{p|N}\left(1 - p^{-1}\right) = \frac{\phi(N)}{N}$. ■

Theorem 18.6 Let $\chi \neq \chi_0$ be a non-principal Dirichlet character modulo N. The series $\sum_{n \geq 1} \chi(n) n^{-s}$ converges in the half-plane $\sigma > 0$. Also, $L(s,\chi)$ is analytic in this half-plane, and

$$L(s,\chi) = s \int_1^\infty \frac{X(u)}{u^{s+1}} du, \tag{18.6}$$

where $X(u) := \sum_{n \leq u} \chi(n)$.

Proof. We apply Abel's summation formula (15.1) and derive that

$$\sum_{n \leq x} \frac{\chi(n)}{n^s} = \frac{X(x)}{x^s} + s \int_1^x \frac{X(u)}{u^{s+1}} du.$$

Recall from Corollary 17.18 that $|X(u)| \leq \phi(N)$ for all $u > 0$. Hence, for $\sigma > 0$, $X(x)x^{-s} \to 0$ as $x \to \infty$. Also, the integral $\int_1^\infty X(u) u^{-s-1} du$ is convergent in the half-plane $\sigma > 0$ by comparison with $\int_x^\infty \phi(N) u^{-\sigma-1} du$. The above argument implies the convergence of $\sum_{n \geq 1} \chi(n) n^{-s}$ for $\sigma > 0$, and also the formula (18.6). Finally, $L(s,\chi)$ is analytic in the half-plane $\sigma > 0$ due to the Analyticity Theorem in Rule 16.5. ■

One crucial property of the Dirichlet L-function is the non-vanishing of $L(1,\chi)$ for all non-principal character χ.

Theorem 18.7 Let $\chi \neq \chi_0$ be a non-principal Dirichlet character modulo N. Then $L(1,\chi) \neq 0$.

We shall separate this theorem into two parts, according to whether χ is non-real or real; see Theorem 18.9 and 18.10, respectively.

Here one necessary step is to consider the logarithm of the L-functions. Since the L-functions are complex-valued, we should choose a suitable branch for the complex logarithm. Throughout, what we mean by $\log$ is the principal branch, which is analytically continued by the normal real logarithm to $\mathbb{C} \backslash \mathbb{R}_{\leq 0}$. For this choice of $\log$, we know that

$\log z$ is real if and only if z is a positive real number. Also, it has the power series expansion for $|z| < 1$,

$$\log \frac{1}{1-z} = \sum_{m\geq 0} \frac{z^m}{m}.$$

Now, let us constrain our focus from the whole half-plane $\sigma > 0$ to the positive real axis.

Lemma 18.8 Let N be a positive integer, and define

$$Z(s) := \prod_{\chi \bmod N} L(s,\chi).$$

Then for $\sigma > 1$, $Z(\sigma)$ is real-valued with $Z(\sigma) > 1$.

Proof. We make use of the Euler product (18.4) for L-functions, and obtain that

$$\begin{aligned}\log Z(\sigma) = \log \prod_{\chi \bmod N} \prod_{p} \frac{1}{1-\chi(p)p^{-s}} &= \sum_{\chi \bmod N} \sum_{p} \log \frac{1}{1-\chi(p)p^{-\sigma}} \\ &= \sum_{\chi \bmod N} \sum_{p} \sum_{m\geq 1} \frac{\chi(p)^m}{mp^{m\sigma}} = \sum_{p} \sum_{m\geq 1} \frac{1}{mp^{m\sigma}} \sum_{\chi \bmod N} \chi(p)^m \\ &= \sum_{p} \sum_{m\geq 1} \frac{1}{mp^{m\sigma}} \sum_{\chi \bmod N} \chi(p^m).\end{aligned}$$

By (17.2),

$$\sum_{\chi \bmod N} \chi(p^m) = \begin{cases} \phi(N) & \text{if } p^m \equiv 1 \pmod{N}, \\ 0 & \text{otherwise.} \end{cases}$$

For every $p \nmid N$, we may always find such m with $p^m \equiv 1 \pmod{N}$, viz., m are multiples of $\operatorname{ord}_N p$. It follows that $\log Z(\sigma)$ is a positive real number, and hence $Z(\sigma)$ is real-valued with $Z(\sigma) > 1$. ■

Theorem 18.9 Let $\chi \neq \chi_0$ be a non-principal non-real Dirichlet character modulo N. Then $L(1,\chi) \neq 0$.

Proof. We prove by contradiction. If $\chi_\dagger$ is a non-principal non-real character such that $L(1,\chi_\dagger) = 0$, so is $\overline{\chi_\dagger}$ since

$$L(1,\overline{\chi_\dagger}) = \sum_{n\geq 0} \frac{\overline{\chi_\dagger(n)}}{n} = \sum_{n\geq 0} \overline{\frac{\chi_\dagger(n)}{n}} = \overline{L(1,\chi_\dagger)} = 0.$$

Note that the three characters χ_0, $\chi_\dagger$ and $\overline{\chi_\dagger}$ are pairwise distinct. Hence, we may rewrite $Z(\sigma)$ in Lemma 18.8 as

$$Z(\sigma) = L(\sigma,\chi_0)L(\sigma,\chi_\dagger)L(\sigma,\overline{\chi_\dagger}) \prod_{\chi \neq \chi_0,\chi_\dagger,\overline{\chi_\dagger}} L(\sigma,\chi).$$

If we look at a small neighborhood $|\sigma - 1| < \varepsilon \to 0$ near $\sigma = 1$, we have that $L(1+\varepsilon,\chi_0) = O(\varepsilon^{-1})$ by the simple pole of $L(s,\chi_0)$ at $s = 1$, and that $L(1+\varepsilon,\chi_\dagger) = O(\varepsilon)$, $L(1+\varepsilon,\overline{\chi_\dagger}) = O(\varepsilon)$ and $L(1+\varepsilon,\chi) = O(1)$ otherwise by the analyticity of L-functions in the half-plane $\sigma > 0$ for every non-principal characters together with the assumption that $L(1,\chi_\dagger) = L(1,\overline{\chi_\dagger}) = 0$. Hence, as $\varepsilon \to 0$, $Z(1+\varepsilon) = O(\varepsilon) \to 0$. But this violates Lemma 18.8, claiming that $Z(1+\varepsilon) > 1$ whenever $\varepsilon > 0$. ■

However, for non-principal real characters, we *cannot* proceed with the above argument as the complex conjugate of a real character is still itself. So we cannot automatically get another copy of $L(1+\varepsilon,\chi'_\dagger)=O(\varepsilon)$ as above to reduce $P(1+\varepsilon)$ to $O(\varepsilon)$. Now, we shall adopt an elegant device due to Paul Monsky (*Amer. Math. Monthly* **100** (1993), no. 9, 861–862).

Theorem 18.10 Let $\chi\neq\chi_0$ be a non-principal real Dirichlet character modulo N. Then $L(1,\chi)\neq 0$.

Proof. We start with the Lambert series with $0<x<1$,

$$F(x)=\sum_{k\geq 1}\frac{\chi(k)x^k}{1-x^k}.$$

Note that this series is absolutely convergent by comparison with $\sum_{k\geq 1}\frac{x^k}{1-x^k}$ whose convergence follows by the ratio test. We may also expand $F(x)$ as a power series in x, say, $F(x)=\sum_{n\geq 1}a(n)x^n$. With recourse to (12.3), we have

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

By Theorem 14.9, the arithmetic function a is multiplicative since $a=\chi*\mathbf{1}$ while both χ and $\mathbf{1}$ are multiplicative. We then claim that $a(n)\geq 0$ for all n. Here it is sufficient to verify that $a(p^\alpha)\geq 0$ for all prime powers. Recalling that χ is real, and hence that $\chi(p)\in\{-1,0,1\}$, we have

$$a(p^\alpha)=1+\chi(p)+\cdots+\chi(p^\alpha)=1+\chi(p)+\cdots+\chi(p)^\alpha\geq 0,$$

by grouping terms $\chi(p)^{2j}+\chi(p)^{2j+1}\geq 0$. In particular, we deduce by the same argument that $a(p^{2\beta})\geq 1$ for all even powers of primes $p^{2\beta}$. Since a is multiplicative, we have $a(n^2)\geq 1$ for all n. It follows from the above that the series $\sum_{n\geq 0}a(n)$ diverges. For each $M\geq 1$, we have $\limsup_{x\to 1^-}F(x)\geq\lim_{x\to 1^-}\sum_{n\leq M}a(n)x^n=\sum_{n\leq M}a(n)$. Hence, as $x\to 1^-$, $F(x)\to\infty$.

Let us assume that the real character $\chi\neq\chi_0$ is such that $L(1,\chi)=0$. Then

$$-F(x)=\frac{L(1,\chi)}{1-x}-F(x)=\sum_{n\geq 1}\chi(n)\left(\frac{1}{(1-x)n}-\frac{x^n}{1-x^n}\right)=:\sum_{n\geq 1}f_n(x)\chi(n).$$

Then for $0<x<1$, $\lim_{n\to\infty}f_n(x)=0$. Also,

$$\begin{aligned}f_n(x)-f_{n+1}(x)&=\left(\frac{1}{(1-x)n}-\frac{x^n}{1-x^n}\right)-\left(\frac{1}{(1-x)(n+1)}-\frac{x^{n+1}}{1-x^{n+1}}\right)\\&=\frac{1}{1-x}\left(\frac{1}{n(n+1)}-\frac{x^n(1-x)^2}{(1-x^n)(1-x^{n+1})}\right).\end{aligned}$$

Further, we apply the arithmetic-geometric mean inequality to find that for every positive integer k,

$$\frac{1-x^k}{1-x}=1+x+\cdots+x^{k-1}=\frac{1+x^{k-1}}{2}+\frac{x+x^{k-2}}{2}+\cdots+\frac{x^{k-1}+1}{2}\geq kx^{\frac{k-1}{2}}.$$

Hence,

$$f_n(x)-f_{n+1}(x)\geq\frac{1}{1-x}\left(\frac{1}{n(n+1)}-\frac{x^{\frac{1}{2}}}{n(n+1)}\right)>0.$$

That is, $f_n(x)$ is a decreasing sequence whenever $0 < x < 1$.

Now, if we as usual write $X(u) = \sum_{n\le u}\chi(n)$, then for every integer $M \ge 1$, by replacing $\chi(n)$ with $X(n) - X(n-1)$ and then rearranging terms, we have

$$\sum_{n\le M} f_n(x)\chi(n) = X(M)f_{M+1}(x) + \sum_{n\le M} X(n)\big(f_n(x) - f_{n+1}(x)\big).$$

Since $f_n(x) \searrow 0$ as $n \to \infty$, we have the following bound by also recalling from Corollary 17.18 that $|X(u)| \le \phi(N)$,

$$\left|\sum_{n\le M} f_n(x)\chi(n)\right| \le \phi(N)f_{M+1}(x) + \phi(N)\sum_{n\le M}\big(f_n(x) - f_{n+1}(x)\big) = \phi(N)f_1(x),$$

for all $0 < x < 1$. However, $f_1(x) = \frac{1}{1-x} - \frac{x}{1-x} = 1$. Hence, we have that $|F(x)| \le \phi(N)$ whenever $0 < x < 1$. But this contradicts what we have shown earlier that $F(x) \to \infty$ as $x \to 1^-$. Thus, we cannot have any real character $\chi \ne \chi_0$ with $L(1,\chi) = 0$. ■

R The above evaluation of $\sum_{n\le M} f_n(x)\chi(n)$ is indeed an instance of the *Abel transformation*, also know as *summation by parts*.

Theorem 18.11 (Abel Transformation). For sequences $\{a_n\}_{n\ge 1}$ and $\{b_n\}_{n\ge 1}$, if we put $A_n := \sum_{N<m\le n} a_m$, then for integers $0 \le N < M$,

$$\sum_{N<n\le M} a_n b_n = A_M b_{M+1} + \sum_{N<n\le M} A_n(b_n - b_{n+1}).$$

This can be regarded as a *discrete* version of Abel's summation formula (15.1). For its proof, we simply replace a_n with $A_n - A_{n-1}$ and rearrange terms.

18.3 Dirichlet's Theorem

Now we are in a position to put the finishing touches to the proof of Dirichlet's theorem.

Theorem 18.12 (Dirichlet's Theorem). There are infinitely many primes that are congruent to a modulo N provided that $(a,N) = 1$.

We first summarize what was obtained earlier.

Lemma 18.13 In the half-plane $\sigma > 1$, we have, as $s \to 1$,

$$\log L(s,\chi_0) \sim -\log(s-1) \tag{18.7}$$

where χ_0 is the principal Dirichlet character modulo a positive integer N, and

$$\log L(s,\chi) = O(1), \tag{18.8}$$

where $\chi \ne \chi_0$ is a non-principal Dirichlet character modulo N.

Proof. For (18.7), we use (18.3) and (18.5). For (18.8), we know from Theorems 18.6 and 18.7 that in the half-plane $\sigma > 0$ there exists a neighborhood near $s = 1$ such that within this neighborhood $L(s,\chi)$ is bounded and $L(s,\chi) \ne 0$, thereby implying that $\log L(s,\chi)$ is also bounded. ■

Proof of Theorem 18.12. We make use of the Euler product (18.4) for L-functions, and obtain that for $\sigma > 1$,

$$\begin{aligned}\sum_{\chi \bmod N} \overline{\chi(a)} \log L(s,\chi) &= \sum_{\chi \bmod N} \overline{\chi(a)} \sum_p \log \frac{1}{1-\chi(p)p^{-s}} \\ &= \sum_{\chi \bmod N} \overline{\chi(a)} \sum_p \sum_{m\geq 1} \frac{\chi(p)^m}{mp^{ms}} \\ &= \sum_p \sum_{\chi \bmod N} \overline{\chi(a)} \frac{\chi(p)}{p^s} + \sum_p \sum_{m\geq 2} \sum_{\chi \bmod N} \overline{\chi(a)} \frac{\chi(p)^m}{mp^{ms}}.\end{aligned}$$

For the first term, we deduce from Corollary 17.20 that

$$\sum_p \sum_{\chi \bmod N} \overline{\chi(a)} \frac{\chi(p)}{p^s} = \phi(N) \sum_{p\equiv a \bmod N} \frac{1}{p^s}.$$

For the second term, we have the bound for $\sigma > 1$,

$$\begin{aligned}\left| \sum_p \sum_{m\geq 2} \sum_{\chi \bmod N} \overline{\chi(a)} \frac{\chi(p)^m}{mp^{ms}} \right| &\leq \sum_p \sum_{m\geq 2} \sum_{\chi \bmod N} \frac{1}{mp^{m\sigma}} \\ &< \frac{\phi(N)}{2} \sum_p \sum_{m\geq 2} \frac{1}{p^m} = \frac{\phi(N)}{2} \sum_p \frac{1}{p(p-1)} \\ &< \frac{\phi(N)}{2} \sum_{n\geq 2} \frac{1}{n(n-1)} = \frac{\phi(N)}{2}.\end{aligned}$$

Finally, since $(a,N) = 1$, we have $\overline{\chi_0(a)} = 1$. It follows from (18.7) and (18.8) that, as $s \to 1$ in the half-plane $\sigma > 1$,

$$\sum_{\chi \bmod N} \overline{\chi(a)} \log L(s,\chi) \sim -\log(s-1) \to \infty.$$

This in turn implies the divergence of $\sum_{p\equiv a \bmod N} \frac{1}{p}$, and therefore the infinitude of primes congruent to a modulo N. ■

Bibliography

[1] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK. Sixth Edition*, Springer, Berlin, 2018.

[2] G. E. Andrews, *The Theory of Partitions*, Reprint of the 1976 original, Cambridge University Press, Cambridge, 1998.

[3] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York-Heidelberg, 1976.

[4] A. Baker, *Transcendental Number Theory*, Reprint of the 1975 original, Cambridge University Press, Cambridge, 2022.

[5] B. C. Berndt, *Number Theory in the Spirit of Ramanujan*, American Mathematical Society, Providence, RI, 2006.

[6] H. Davenport, *The Higher Arithmetic. An Introduction to the Theory of Numbers. Eighth Edition*, Cambridge University Press, Cambridge, 2008.

[7] L. E. Dickson, *History of the Theory of Numbers. Vols. I–III*, Chelsea Publishing Co., New York, 1966.

[8] G. Gasper and M. Rahman, *Basic Hypergeometric Series. Second Edition*, Cambridge University Press, Cambridge, 2004.

[9] C. F. Gauss, *Disquisitiones Arithmeticae*, Translated by A. A. Clarke, Springer-Verlag, New York, 1986.

[10] R. K. Guy, *Unsolved Problems in Number Theory. Third Edition*, Springer-Verlag, New York, 2004.

[11] H. Halberstam and H.-E. Richert, *Sieve Methods*, No. 4. Academic Press [Harcourt Brace Jovanovich, Publishers], London-New York, 1974.

[12] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers. Sixth Edition*, Oxford University Press, Oxford, 2008.

[13] M. D. Hirschhorn, *The Power of q. A Personal Journey*, Springer, Cham, 2017.

[14] E. Landau, *Elementary number theory*, Translated by J. E. Goodman, Chelsea Publishing Co., New York, 1958.

[15] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory. I. Classical Theory*, Cambridge University Press, Cambridge, 2007.

[16] S. Lang, *Algebraic Number Theory. Second Edition*, Springer-Verlag, New York, 1994.

[17] L. J. Mordell, *Diophantine Equations*, Academic Press, London-New York, 1969.

[18] R. C. Vaughan, *The Hardy-Littlewood Method. Second Edition*, Cambridge University Press, Cambridge, 1997.

[19] A. Weil, *Number Theory. An Approach Through History from Hammurapi to Legendre*, Reprint of the 1984 edition, Birkhäuser Boston, Inc., Boston, MA, 2007.

[20] H. S. Wilf, *Generatingfunctionology. Third Edition*, A K Peters, Ltd., Wellesley, MA, 2006.