22 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

1.1 Divisibility

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

$$\text{“}a \textit{ divides } b\text{”} \quad \text{or} \quad \text{“}b \textit{ is divisible by } a\text{”}$$

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 $a \mid (m_1 b_1 + \cdots + m_r b_r)$. ■

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 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

$$n = p_1 p_2 \cdots p_k + 1.$$

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

$$n = 4p_1 p_2 \cdots p_k - 1.$$

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 $n = 0,1,2,\ldots$

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 $0 \le m < n$. 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 $n \ge 2$ 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 $k \ge 2$. 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 $n \ge 2$ as a product of primes?* This question is answered by the *Fundamental Theorem of Arithmetic*, also known as the *Unique Factorization Theorem*.

Theorem 1.8 (Fundamental Theorem of Arithmetic). Every integer $n \ge 2$ 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

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

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 $m \le n$.

Therefore,

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

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 1.9 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 1.9. ■

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 Paul Erdős (*Mathematica, Zutphen. B.* **7** (1938), 1–2).

Theorem 1.10 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

$$
\begin{aligned}
r_{-1} &= q_1 r_0 + r_1, && 0 < r_1 < r_0; && \text{(2.1a)}\\
r_0 &= q_2 r_1 + r_2, && 0 < r_2 < r_1; && \text{(2.1b)}\\
r_1 &= q_3 r_2 + r_3, && 0 < r_3 < r_2; && \text{(2.1c)}\\
&\cdots\\
r_{k-2} &= q_k r_{k-1} + r_k, && 0 < r_k < r_{k-1}; && \text{(2.1d)}\\
r_{k-1} &= q_{k+1} r_k + 0. && && \text{(2.1e)}
\end{aligned}
$$

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 in Theorem 1.8.

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 $p_1 \mid q_1 q_2 \cdots q_\ell$, 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 2.8 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 2.9 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

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

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

Theorem 2.10 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 2.10, 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

$$a_1m' \equiv a_2m' \pmod{m} \quad \Rightarrow \quad a_1 \equiv a_2 \pmod{m}$$

and

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

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 $k\in\mathbb{Z}$,

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

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 $\overline{a}$ is a *modular inverse of a modulo m* if

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

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 2.10. ■

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), and was further developed by 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. The *Euler totient function* $\phi(n)$ denotes the number of integers among $\{1, 2, \ldots, n\}$ that are coprime to n.

■ **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 $\{1,2,\ldots,n\}$ 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 $\{1,\ldots,p^k\}$ that are coprime to p^k, or in other words, that are not divisible by p. Since there are p^{k-1} integers among $\{1,\ldots,p^k\}$ 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

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

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 an arithmetic function $f:\mathbb{Z}\to\mathbb{C}$, we say that it is *multiplicative* if 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 Let n be a positive integer. Then

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

where the sum runs over all divisors of n.

Proof. We write $n = \prod_{p|n} p^{\alpha}$. Then the divisors of n are of the form $\prod_{p|n} p^{\beta}$ with $0 \le \beta \le \alpha$ for each p. Thus,

$$\begin{aligned}\sum_{d|n} \phi(n) &= \sum \phi\left(\prod_{\substack{p|n \\ 0\le\beta\le\alpha}} p^{\beta}\right) = \sum \prod_{\substack{p|n \\ 0\le\beta\le\alpha}} \phi(p^{\beta}) \\ &= \prod_{p|n} \sum_{0\le\beta\le\alpha} \phi(p^{\beta}) = \prod_{p|n} \left(1 + (p-1) + (p^2-p) + \cdots + (p^{\alpha} - p^{\alpha-1})\right) \\ &= \prod_{p|n} p^{\alpha} = n,\end{aligned}$$

giving the desired result. ∎

R This relation gives an instance of the *Dirichlet convolution* that will be discussed in later lectures.

4.3 Fermat–Euler Theorem

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

$$a^{\phi(m)} \equiv 1 \pmod{m}. \tag{4.4}$$

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

$$a^{p-1} \equiv 1 \pmod{p}. \tag{4.5}$$

4.4 Binomial coefficients

Definition 4.3 For integers $m \ge n \ge 0$, 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 $m \geq n > 0$,

$$\binom{m+1}{n} = \binom{m}{n} + \binom{m}{n-1}. \tag{4.6}$$

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 $n \geq 1$,

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}. \tag{4.7}$$

Proof. We prove by induction on n. First, when $n = 1$, both sides of (4.7) are $x+y$. Assume that (4.7) is true for some $n \geq 1$, we want to show that it is also true for $n+1$. Note that

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

which is exactly the $n+1$ case of (4.7). ∎

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 $1 \le r \le p^\alpha$,

$$\nu_p\left(\binom{p^\alpha}{r}\right) = \alpha - \nu_p(r). \tag{4.8}$$

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,

$$(x_1 + x_2 + \cdots + x_k)^p \equiv x_1^p + x_2^p + \cdots x_k^p \pmod{p}. \tag{4.9}$$

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:

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

by our inductive assumption. ■

4.5 Euler's proof of the Fermat–Euler Theorem

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

$$a^{\phi(p^\alpha)} \equiv 1 \pmod{p^\alpha}. \tag{4.10}$$

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 (4.10).

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 (4.10),

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

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 $\overline{a}$ 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,

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

as desired. ■

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 $a^{x+y}\equiv a^xa^y \pmod m$;
(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 $a^xa^{-x}\equiv a^{x+(-x)}=a^0=1 \pmod m$, 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. ■

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, $a^{dd_b} = a^{dd_b} \cdot 1^d \equiv a^{dd_b} \cdot (b^{d_b})^d = (ab)^{dd_b} = \big((ab)^d\big)^{d_b} \equiv 1^{d_b} = 1 \pmod{m}$, 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 $d_i = \mathrm{ord}_m a_i$ 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 an y such that $d = \mathrm{ord}_m y \nmid D$. 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 $\mathrm{lcm}(d, D) > D$ as $\mathrm{lcm}(d, D) = \prod_i p_i^{\max(\alpha_i, \beta_i)}$. 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 $d'D' = \mathrm{lcm}(d, D)$. By Theorem 5.5, there exists an a of order d' and a b of order D'. Thus, by Theorem 5.6, $\mathrm{ord}_m(ab) = d'D' = \mathrm{lcm}(d, D) > D$. 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 $\mathrm{ord}_m g = \phi(m)$.

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.

R 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 $\mathrm{ord}_m g = \phi(m)$. 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 $\mathrm{ord}_m g = \phi(m)$. Then 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 $\mathrm{ord}_m g^i = \phi(m)$. On the other hand, we know from Theorem 5.5 that $\mathrm{ord}_m g^i = \frac{\phi(m)}{(i, \phi(m))}$. 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 Lagrange, which will be a key to confirm 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 $1,\dots,n$ 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 $d_k=\operatorname{ord}_p k$ 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 $\operatorname{ord}_p g=\phi(p)=p-1$ and g is such that

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

with $p\nmid x$. Let $\operatorname{ord}_{p^\alpha} g=d$. 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 $0 \le s \le \alpha - 1$. 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, $s+2 \ge \alpha+1$. 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 $s, t \ge 3$ and $(s,t) = 1$. Note that since $\phi(n)$ is multiplicative, $\phi(m) = \phi(s)\phi(t)$. 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 $\alpha \ge 3$. 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 $(\alpha \ge 3)$ has no primitive roots. ■

6. Quadratic residues

6.1 Quadratic residues

Assume that $p \geq 3$ is prime and that x is such that $1 \leq x \leq p-1$. 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

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

We usually write $a \,\mathrm{R}\, p$ is this case. If such x does not exist, we say that a is a *quadratic non-residue modulo p*, and write $a \,\mathrm{N}\, p$.

Note that when $p=2$, for any a such that $(a,2)=1$, we always have $a \equiv 1 = 1^2 \pmod{2}$. Thus, all such a's 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 $\geq \frac{p+1}{2}$ quadratic residues, then there are $\geq 2 \cdot \frac{p+1}{2} = p+1$ 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*.

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* 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 be such that $(a, p) = 1$. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{6.5}$$

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

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right). \tag{6.6}$$

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 6.6,

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

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, $\left|\left(\frac{mn}{p}\right) - \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\right| \leq 2$, implying that $\left(\frac{mn}{p}\right) - \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = 0$, as desired. ■

R Given an arithmetic function $f : \mathbb{Z} \to \mathbb{C}$, we say that it is *completely multiplicative* if 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 6.8 Let $p \geq 3$ be a prime. Then

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{6.7}$$

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 6.6 that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$, and thus (6.7) 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 6.9 Let $p \geq 3$ 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 6.8 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 6.10 Let $p \ge 3$ 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 $0 \le x \le \frac{p-1}{2}$ and $-(y^2+1)$ for $0 \le y \le \frac{p-1}{2}$. 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's are incongruent modulo p, and so are the $-(y^2+1)$'s. Thus, the two integers falling into the same residue class must be one x^2 and one $-(y^2+1)$. That is, there exists x and y with $0 \le x, y \le \frac{p-1}{2}$ 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

Lemma 7.1 (Gauss's Lemma). Let $p \geq 3$ be a prime and a be such that $(a,p)=1$. For each k with $1 \leq k \leq \frac{p-1}{2}$, 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

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

Proof. Since $(a,p)=1$, we have $1 \leq r_k \leq p-1$ for each k. Assume that $x_1,\ldots,x_\mu$ are those $r_k > \frac{p}{2}$ and $y_1,\ldots,y_\nu$ are those $r_k < \frac{p}{2}$. Note that $\mu+\nu = \frac{p-1}{2}$. Also, the x's are pairwise distinct and so are the y's. We further claim that there are no x_i and y_j with $p-x_i = y_j$; otherwise, we have k_i and k_j such that $ak_i + ak_j \equiv 0 \pmod{p}$, or $k_i + k_j \equiv 0 \pmod{p}$, which is impossible since $1 \leq k_i, k_j \leq \frac{p-1}{2}$. Noting that $1 \leq (p-x), y < \frac{p}{2}$, we conclude that the $\frac{p-1}{2}$ integers $(p-x_1),\ldots,(p-x_\mu)$ and $y_1,\ldots,y_\nu$ form a rearrangement of $1,\ldots,\frac{p-1}{2}$. Thus,

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

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 6.6. ∎

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,

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

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

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

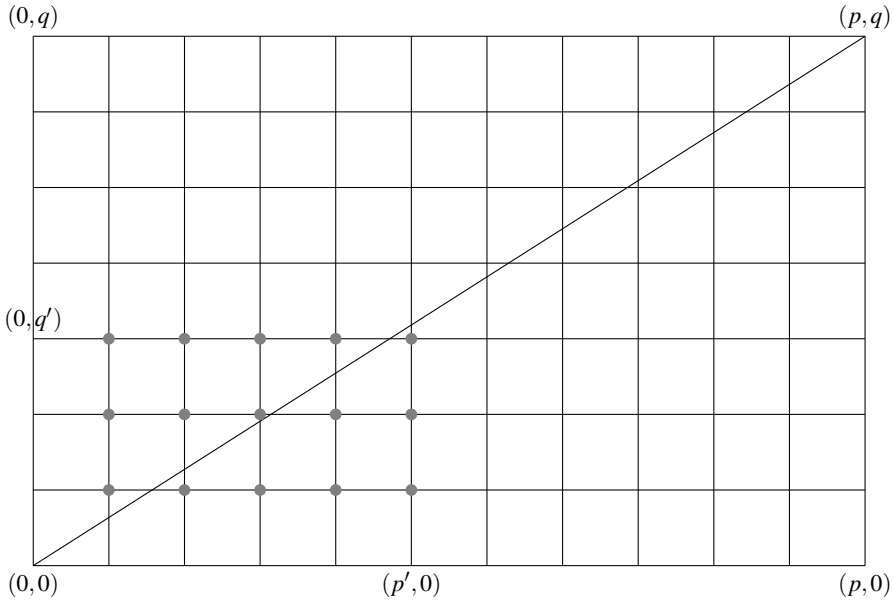

Figure 7.1: Integer lattices and $y = \frac{q}{p}x$

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 $1 \le x \le p'$ **and** $1 \le y \le q'$ 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 $1 \le x \le p'$ 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 $\frac{y}{x} \ge \frac{q'+1}{p'} = \frac{q+1}{p-1} > \frac{q}{p}$, and thus the lattice is above ℓ, so not in $\mathscr{B}$.

(iii). For any lattice with $x > p'$ and $1 \le y \le q'$ (so it is not in $\mathscr{B}$), we compute the slope of the line connecting this lattice and the origin, which is $\frac{y}{x} \le \frac{q'}{p'+1} = \frac{q-1}{p+1} < \frac{q}{p}$, 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 $p,q \ge 3$ be primes with $p \ne q$. 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 $p \ge 5$ 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 $p \ge 3$ 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 7.1** 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 $n_p \le \frac{p-1}{2}+1 = \frac{p+1}{2}$. But the upper bound for n_p could be sharper.

Theorem 7.7 Let $p \ge 3$ 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 6.7 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 $n_p \le m$. So,

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

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 and sums of two squares

Recall that the following notation has been used before 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 6.8, 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 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*, 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 6.9 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 $|n_0| \leq \frac{m}{2}$ 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 $|x_0| \leq \frac{m}{2}$ and $y \equiv y_0 \pmod m$ with $|y_0| \leq \frac{m}{2}$. 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, $x_0^2 + y_0^2 \leq 2 \cdot (\frac{m}{2})^2 < m^2$. 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 even exponents 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

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

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 6.10 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. ■

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] B. C. Berndt, *Number Theory in the Spirit of Ramanujan*, American Mathematical Society, Providence, RI, 2006.

[5] L. E. Dickson, *History of the Theory of Numbers. Vols. I–III*, Chelsea Publishing Co., New York, 1966.

[6] K. Dilcher, *Elementary Number Theory: Class Notes for MATH 3070*, unpublished notes.

[7] C. F. Gauss, *Disquisitiones Arithmeticae*, Translated by A. A. Clarke, Springer-Verlag, New York, 1986.

[8] R. K. Guy, *Unsolved Problems in Number Theory. Third Edition*, Springer-Verlag, New York, 2004.

[9] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers. Sixth Edition*, Oxford University Press, Oxford, 2008.

[10] M. D. Hirschhorn, *The Power of q. A Personal Journey*, Springer, Cham, 2017.

[11] H. S. Wilf, *Generatingfunctionology. Third Edition*, A K Peters, Ltd., Wellesley, MA, 2006.