Theory of Numbers

Divisibility Theory in the Integers,
The Theory of Congruences,
Number-Theoretic Functions,
Primitive Roots, Quadratic Residues

YOTSANAN MEEMARK

Informal style based on the course
2301331 Theory of Numbers, offered at
Department of Mathematics and Computer Science,
Faculty of Science, Chulalongkorn University

Second version August 2016

Any comment or suggestion, please write to
`yzm101@yahoo.com`

Contents

Chapter 1

Divisibility Theory in the Integers

Let $\mathbb{N}$ denote the set of positive integers and let $\mathbb{Z}$ be the set of integers.

1.1 The Division Algorithm and GCD

Theorem 1.1.1. [Well-Ordering Principle] *Every nonempty set S of nonnegative integers contains a least element; that is, there is some integer a in S such that $a \le b$ for all $b \in S$.*

Theorem 1.1.2. [Division Algorithm] *Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying*

$$a = qb + r, \qquad \textit{where} \quad 0 \le r < b.$$

The integers q and r are called, respectively, the **quotient** *and* **remainder** *in the division of a by b.*

Proof. Existence: Let $S = \{a - xb : x \in \mathbb{Z} \text{ and } a - xb \ge 0\} \subseteq \mathbb{N} \cup \{0\}$. We shall show that $S \ne \emptyset$. Since $b \ge 1$, we have $|a|b \ge |a|$, so

$$a - (-|a|)b = a + |a|b \ge a + |a| \ge 0,$$

Then $a - (-|a|)b \in S$, so $S \ne \emptyset$. By the well-ordering principle, S contains a least element, call it r. Then $a - qb = r$ for some $q \in \mathbb{Z}$. Since $r \in S$, $r \ge 0$ and $a = qb + r$. It remains to show that $r < b$. Suppose that $r \ge b$. Thus,

$$0 \le r - b = a - qb - b = a - (q+1)b,$$

so $r - b \le r$ and $r - b \in S$. This contradicts the minimality of r. Hence, $r < b$.

Uniqueness: Let $q, q', r, r' \in \mathbb{Z}$ be such that

$$a = qb + r \quad \text{and} \quad a = q'b + r',$$

where $0 \le r, r' < b$. Then

$$(q - q')b = r' - r.$$

Since $0 \le r, r' < b$, we have $|r' - r| < b$, so $b|q - q'| = |r' - r| < b$. This implies that $0 \le |q - q'| < 1$, hence $q = q'$ which also forces $r = r'$. □

Corollary 1.1.3. *If a and b are integers, with $b \ne 0$, then there exist unique integers q and r such that*

$$a = qb + r, \qquad \textit{where} \quad 0 \le r < |b|.$$

Proof. It suffices to consider the case in which $b < 0$. Then $|b| > 0$ and Theorem 1.1.2 gives $q', r \in \mathbb{Z}$ such that

$$a = q'|b| + r, \quad \text{where} \quad 0 \le r < |b|.$$

Since $|b| = -b$, we may take $q = -q'$ to arrive at

$$a = qb + r, \quad \text{where} \quad 0 \le r < |b|$$

as desired. □

Example 1.1.1. Show that $\dfrac{a(a^2+2)}{3}$ is an integer for all $a \ge 1$.

Solution. By the division algorithm, every $a \in \mathbb{Z}$ is of the form

$$3q \text{ or } 3q+1 \text{ or } 3q+2, \qquad \text{where } q \in \mathbb{Z}.$$

We distinguish three cases.

(1) $a = 3q$. Then $\dfrac{a(a^2+2)}{2} = \dfrac{3q((3q)^2+2)}{3} = q((3q)^2+2) \in \mathbb{Z}$.

(2) $a = 3q+1$. Then $\dfrac{a(a^2+2)}{2} = \dfrac{(3q+1)((3q+1)^2+2)}{3} = (3q+1)(3q^2+2q+1) \in \mathbb{Z}$.

(3) $a = 3q+2$. Then $\dfrac{a(a^2+2)}{2} = \dfrac{(3q+2)((3q+2)^2+2)}{3} = (3q+2)(3q^2+2q+2) \in \mathbb{Z}$.

Hence, $\dfrac{a(a^2+2)}{3}$ is an integer. □

Definition. An integer b is said to be **divisible** by an integer $a \neq 0$, in symbols $a \mid b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

There is other language for expressing the divisibility relation $a \mid b$. One could say that a is a **divisor** of b, that a is a **factor** of b or that b is a **multiple** of a. Notice that there is a restriction on the divisor a: whenever the notation $a \mid b$ is employed, it is understood that $a \neq 0$.

An **even number** is an integer divisible by 2 and an **odd number** is an integer not divisible by 2.

It will be helpful to list some immediate consequences.

Theorem 1.1.4. *For integers a, b and c, the following statements hold:*

(1) $a \mid 0$, $1 \mid a$, $a \mid a$.

(2) $a \mid 1$ *if and only if* $a = \pm 1$.

(3) *If* $a \mid b$, *then* $a \mid (-b)$, $(-a) \mid b$ *and* $(-a) \mid (-b)$.

(4) *If* $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.

(5) *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.

(6) ($a \mid b$ *and* $b \mid a$) *if and only if* $a = \pm b$.

(7) *If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.*

(8) *If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for arbitrary integers x and y.*

Proof. Exercises. □

Theorem 1.1.5. *A positive integer n always divides the product of n consecutive integers.*

Proof. Let a be an integer. By the division algorithm, there exist $q, r \in \mathbb{Z}$ such that

$$a = nq + r, \quad \text{where } 0 \leq r < n.$$

Thus, $n \mid (a - r)$ and $0 \leq r < n$, so n divides $a(a-1)(a-2)\dots(a-n+1)$. □

Definition. Let a and b be given integers, with at least one of them different from zero. The **greatest common divisor (gcd)** of a and b, denoted by $\gcd(a, b)$, is the positive integer d satisfying

(1) $d \mid a$ and $d \mid b$,

(2) for all $c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$, then $c \leq d$.

Example 1.1.2. $\gcd(-12, 30) = 6$ and $\gcd(8, 15) = 1$.

Remarks. (1) If $a \neq 0$, then $\gcd(a, 0) = |a|$.

(2) $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$.

(3) If $a \mid b$, then $\gcd(a, b) = |a|$.

Theorem 1.1.6. *Given integers a and b, not both of which are zero, there exist integers x and y such that*

$$\gcd(a, b) = ax + by.$$

Proof. Assume that $a \neq 0$. Consider the set

$$S = \{au + bv : au + bv > 0 \text{ and } u, v \in \mathbb{Z}\}.$$

Since $|a| = au + b \cdot 0$, where we choose $u = 1$ or -1 according as a is positive or negative, we have $S \neq \emptyset$. By the well-ordering principle, S contains the least element d. Since $d \in S$, there exist integers x and y for which $d = ax + by > 0$. We shall claim that $d = \gcd(a, b)$.

The division algorithm gives $q, r \in \mathbb{Z}$ such that $a = qd + r$, where $0 \leq r < d$. Assume that $r \neq 0$. Then

$$0 < r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy).$$

This implies that $r \in S$ which contradicts the minimality of d. Thus, $d \mid a$. Similarly, we can show that $d \mid b$.

Now, let $c \in \mathbb{Z}$ be such that $c \mid a$ and $c \mid b$. Then $c \mid (ax + by)$, so $c \mid d$. Thus, $c \leq |c| \leq |d| = d$. Hence, $d = \gcd(a, b)$. □

Corollary 1.1.7. *Let a and b be integers not both zero and let $d = \gcd(a, b)$. Then the set*

$$T = \{au + bv : u, v \in \mathbb{Z}\}$$

is precisely the set of all multiples of d. That is, $T = d\mathbb{Z}$.

Proof. Let $u, v \in \mathbb{Z}$. Since $d \mid a$ and $d \mid b$, $d \mid (au+bv)$, so $T \subseteq d\mathbb{Z}$. Conversely, let $q \in \mathbb{Z}$. By Theorem 1.1.6, there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$. Then

$$dq = (ax + by)q = a(xq) + b(yq) \in T.$$

Hence, $d\mathbb{Z} \subseteq T$. □

Corollary 1.1.8. *Let a and b be integers, not both zero. For a positive integer d, $d = \gcd(a, b)$ if and only if (1) $d \mid a$ and $d \mid b$, and (2) if $c \mid a$ and $c \mid b$, then $c \mid d$.*

Proof. It suffices to show that if $d = \gcd(a, b)$, $c \mid a$ and $c \mid b$, then $c \mid d$. By Theorem 1.1.6, there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$. Since $c \mid a$ and $c \mid b$, we have $c \mid d$. □

Definition. Two integers a and b, not both of which are zero, are said to be **relatively prime** whenever $\gcd(a, b) = 1$.

Theorem 1.1.9. *Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax + by$.*

Proof. It follows directly from Theorem 1.1.6 and the definition of gcd. □

Corollary 1.1.10. *If $\gcd(a, b) = d$, then $\gcd(a/d, b/d) = 1$.*

Proof. By Theorem 1.1.6, there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$, so

$$1 = (a/d)x + (b/d)y.$$

Since a/d and b/d are integers, by Theorem 1.1.9, $\gcd(a/d, b/d) = 1$. □

Corollary 1.1.11. *If $a \mid c$ and $b \mid c$, with $\gcd(a, b) = 1$, then $ab \mid c$.*

Proof. Write $c = aq$ and $c = bq'$ for some integers q and q'. Since $\gcd(a, b) = 1$, there exist $x, y \in \mathbb{Z}$ such that $1 = ax + by$. Then $c = acx + bcy = a(bq')x + b(aq)y = ab(q'x + qy)$, so $ab \mid c$ □

Corollary 1.1.12. *If $a \mid bc$, with $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. Since $\gcd(a, b) = 1$, we have $1 = ax + by$ for some $x, y \in \mathbb{Z}$. Then $c = acx + bcy$. Since $a \mid bc$, $a \mid c$. □

Remark. If $\gcd(a, b) > 1$, the above corollaries are false. For example,
(1) $6 \mid 18$ and $9 \mid 18$ but $54 \nmid 18$, (2) $6 \mid 4 \cdot 3$ but $6 \nmid 4$.

Remark. Observe that $\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$. The greatest common divisor of three integers a, b and c is denoted by $\gcd(a, b, c)$ is defined by the relation

$$\gcd(a, b, c) = \gcd(\gcd(a, b), c).$$

Similarly, the gcd of n integers $a_1, a_2, \ldots, a_n$ is defined inductively by the relation

$$\gcd(a_1, a_2, \ldots, a_n) = \gcd(\gcd(a_1, a_2, \ldots, a_{n-1}), a_n).$$

Again, this number is independent on the order in which the a_i appear. Moreover, there exist integers $x_1, x_2, \ldots, x_n$ such that

$$\gcd(a_1, a_2, \ldots, a_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

Definition. If $\gcd(a_i, a_j) = 1$ whenever $i \neq j$, the number $a_1, a_2, \ldots, a_n$ are said to be **pairwise relatively prime** or **relatively prime in pairs**.

Exercise 1.1.

1. Use the division algorithm to show that the fourth power of any integer is of the form either $5k$ or $5k + 1$.
2. If a is an odd integer, show that $8 \mid (a^2 - 1)$.
3. If a and b are both odd integers, then $16 \mid (a^4 + b^4 - 2)$.
4. Prove the following statements.
(i) If $c \mid ab$ and $d = \gcd(c, a)$, then $c \mid db$.
(ii) If $a \mid bc$, then $a \mid \gcd(a, b)\gcd(a, c)$.
(iii) If $\gcd(a, c) = 1$ and $\gcd(b, c) = d$, then $\gcd(ab, c) = d$.
(iv) If $\gcd(a, b) = 1$, then $\gcd(a^2, b^2) = 1$.
5. Given an odd integer a, show that $a^2 + (a + 2)^2 + (a + 4)^2 + 1$ is divisible by 12.
6. Let a, m and n be positive integers. If r is the remainder when m divides n, prove that $a^r - 1$ is the remainder when $a^m - 1$ divides $a^n - 1$. Deduce that if $m \mid n$, then $(a^m - 1) \mid (a^n - 1)$.
7. Given integers a and b, prove that
(i) there exist integers x and y for which $c = ax + by$ if and only if $\gcd(a, b) \mid c$, and
(ii) if there exist integers x and y for which $ax + by = \gcd(a, b)$, then $\gcd(x, y) = 1$.

1.2 The Fundamental Theorem of Arithmetic

Definition. An integer $p > 1$ is called a **prime number**, or simply a **prime**, if its only positive divisors are 1 and p. An integer greater than 1 which is not a prime is termed **composite**.

Example 1.2.1. $2, 3, 5, 11, 2011$ are primes. $6, 8, 12, 2554$ are composite numbers.

Remark. Let p be a prime. Then p does not divide a if and only if $\gcd(p, a) = 1$.

Theorem 1.2.1. *If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. Assume that $p \mid ab$ and $p \nmid a$. Then $\gcd(p, a) = 1$, so $p \mid b$ by Corollary 1.1.12. □

Corollary 1.2.2. *If p is a prime and $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_k$ for some k, where $1 \leq k \leq n$.*

Corollary 1.2.3. *If $p, q_1, q_2, \ldots, q_n$ are all primes and $p \mid q_1 q_2 \ldots q_n$, then $p = q_k$ for some k, where $1 \leq k \leq n$.*

Theorem 1.2.4. [Fundamental Theorem of Arithmetic] *Every positive integer $n > 1$ can be expressed as a product of primes; this representation is unique, apart from the order in which the factors occur.*

Proof. Expressible: Assume on the contrary that there exists an integer $n > 1$ which is *not* a product of primes. By the well-ordering principle, there is a smallest n_0 such that n_0 is not a product of primes. Then n_0 is composite, so there exist integers $1 < d_1, d_2 < n_0$ such that $n_0 = d_1 d_2$. Since $d_1, d_2 < n_0$, d_1 and d_2 are products of primes, and so is n_0. This gives a contradiction. Hence, every positive integer $n > 1$ can be expressed as a product of primes.

Uniqueness: Assume that

$$n = p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_t,$$

where $1 \leq s \leq t$ and p_i and q_j are prime such that

$$p_1 \leq p_2 \leq \cdots \leq p_s \quad \text{and} \quad q_1 \leq q_2 \leq \cdots \leq q_t.$$

Corollary 1.2.3 tells us that $p_1 = q_k$ for some $k \in \{1, \ldots, t\}$. It makes $p_1 \geq q_1$. Similarly, $q_1 = p_l$ for some $l \in \{1, \ldots, s\}$. Then $q_1 \geq p_1$, so $p_1 = q_1$. Thus,

$$p_2 \ldots p_s = q_2 \ldots q_t.$$

Now, repeat the process to get $p_2 = q_2$, and we obtain

$$p_3 \ldots p_s = q_3 \ldots q_t.$$

Continue in this manner. If $s < t$, we would get

$$1 = q_{s+1} q_{s+2} \ldots q_t,$$

which is impossible. Hence, $s = t$ and

$$p_1 = q_1, p_2 = q_2, \ldots, p_s = q_s$$

as desired. □

Corollary 1.2.5. *Any positive integer $n > 1$ can be written uniquely in a canonical form*

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r},$$

where, for $i = 1, 2, \ldots, r$, each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \cdots < p_r$.

Corollary 1.2.6. *Any positive integer $n > 1$ has a prime divisor.*

Theorem 1.2.7. [Euclid] *There are an infinite number of primes.*

Proof. Assume that there are only finite numbers of primes, say $p_1, p_2, \ldots, p_s$. Consider

$$n = p_1 p_2 \ldots p_s + 1 > 1.$$

By Corollary 1.2.6, there exists a prime p such that $p \mid n$. Thus, $p = p_i$ for some $i \in \{1, 2, \ldots, s\}$. Since $p \mid n$ and $p \mid p_1 p_2 \ldots p_s$, we have $p \mid 1$, which is a contradiction. □

Corollary 1.2.8. *A composite number $a > 1$ always possesses a prime divisor p satisfying $p \leq \sqrt{a}$.*

In particular, in testing the primality of a specify integer $a > 1$, it therefore suffices to divide a by those primes not exceeding $\sqrt{a}$, e.g., 149 is a prime because $\sqrt{149} < 13$ and $2, 3, 5, 7, 11$ are not divisors of 149.

Proof of Corollary 1.2.8. Let a be a composite number. Then there exist $1 < d_1, d_2 < a$ such that $a = d_1 d_2$. If $d_1 > \sqrt{a}$ and $d_2 > \sqrt{a}$, then $d_1 d_2 > a$, a contradiction. Thus, $d_1 \leq \sqrt{a}$ or $d_2 \leq \sqrt{a}$. Assume that $d_1 \leq \sqrt{a}$. By Corollary 1.2.6, there is a prime p such that $p \mid d_1$. Hence, $p \leq \sqrt{a}$ and $p \mid a$. □

Remark. The so-called **sieve of Eratosthenes** is an algorithm for single out the primes from among the set of integers k with $|k| \le n$, for arbitrary $n > 0$. It depends on Corollary 1.2.8. First, the smallest integer larger than 1, namely 2, must be a prime, and now we know all the primes with $p \le 2$. Suppose we know all the primes p with $1 < p < n$. Then the primes in the set of m with $n < m \le n^2$ are the integers left in this set after eliminating all the multiples of those known primes.

Example 1.2.2. Find all primes less than 100.

Solution. Write

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100.

Eliminate all even numbers except 2. Since $\sqrt{100} = 10$, delete all multiples of 3, 5 and 7. All numbers left are primes less than 100. □

A **Mersenne number** is a number $M_p = 2^p - 1$, where p is a *prime*. If M_p itself is a prime, then it is called a **Mersenne prime**. Note that numbers of the form $2^n - 1$, where n is composite, can never be prime because, for $n = kl$ with $1 < k, l < n$, we have

$$2^n - 1 = (2^k - 1)(2^{k(l-1)} + 2^{k(l-2)} + \cdots + 1).$$

However, not all primes p yield Mersenne primes, the first exception being $p = 11$, because $2^{11} - 1 = 2047 = 23 \cdot 89$. Mersenne primes are useful in discovering large primes, e.g., $2^{43,112,609} - 1$ is a prime with $12,978,189$ digits.

Exercise 1.2.

1. (i) Prove that $\gcd(a, a+k) \mid k$ for all integers a and k not both zero.
   (ii) Prove that $\gcd(a, a+p) = 1$ or p for every integer a and prime p.
2. If p is a prime, $p \mid (ra - b)$ and $p \mid (rc - d)$ for some $r \in \mathbb{Z}$, then $p \mid (ad - bc)$.
3. If p is a prime, prove that $\sqrt{p}$ is irrational.
4. If $p \ge 5$ is a prime, show that $p^2 + 2$ is composite.
5. Let p be the least prime factor of n where n is composite. Prove that if $p > n^{1/3}$, then n/p is prime.
6. **Twin primes** are pairs of primes which differ by two (such as 3 and 5, 11 and 13, etc). Prove that the sum of twin primes greater than 3 is divisible by 12.
7. Prove that every $n \ge 12$ is the sum of two composite numbers.
8. Prove that if $2^m + 1$ is an odd prime, then there exists $n \in \mathbb{N} \cup \{0\}$ such that $m = 2^n$.
9. For each $n \in \mathbb{N}$, let $F_n = 2^{2^n} + 1$. Let $m, n \in \mathbb{N}$. Prove that if $m \ne n$, then $\gcd(F_m, F_n) = 1$.

1.3 The Euclidean Algorithm and Linear Diophantine Equations

Lemma 1.3.1. *If* $a = qb + r$, *then* $\gcd(a, b) = \gcd(b, r) = \gcd(b, a - bq)$.

Proof. Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$. We shall show that $d = \gcd(b, r)$. Since $d \mid a$ and $d \mid b$, $d \mid (a - bq)$, so $d \mid r$. Next, let $c \in \mathbb{Z}$ be such that $c \mid b$ and $c \mid r$. Then $c \mid a$, so c is a common divisor of a and b. Thus, $c \leq d$. Hence, $d = \gcd(b, r) = \gcd(b, a - bq)$. □

Theorem 1.3.2. [Euclidean Algorithm] *Let a and b be positive integers, with* $b \leq a$. *Repeatedly applications of the division algorithm to a and b give*

$$\begin{aligned}
a &= bq_1 + r_1, && \textit{where} \quad 0 < r_1 < b \\
b &= r_1 q_2 + r_2, && \textit{where} \quad 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, && \textit{where} \quad 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, && \textit{where} \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}$$

Then $r_n = \gcd(a, b)$.

Proof. Since $r_n \mid r_{n-1}$, we repeatedly have

$$r_n = \gcd(r_n, r_{n-1}) = \gcd(r_{n-2}, r_{n-1}) = \cdots = \gcd(r_1, r_2) = \gcd(b, r_1) = \gcd(a, b)$$

as desired. □

Remark. For expressing $\gcd(a, b)$ in the form $ax + by$, we fall back the Euclidean algorithm. Starting with the next-to-last equation arising from the algorithm, we write

$$r_n = r_{n-2} - q_n r_{n-1}.$$

Now solve the preceding equation in the algorithm for r_{n-1} and substitute to obtain

$$\begin{aligned}
r_n &= r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) \\
&= (1 + q_n q_{n-1}) r_{n-2} + (-q_n) r_{n-3}.
\end{aligned}$$

This represents r_n as a linear combination of r_{n-2} and r_{n-3}. Continuing backwards through the system of equations, we successively eliminate the remainders $r_{n-1}, r_{n-2}, \ldots, r_2, r_1$ until a stage is reached where $r_n = \gcd(a, b)$ is expressed as a linear combination of a and b.

Example 1.3.1. Find the $\gcd(a, b)$ and express it as a linear combination of a and b.
(1) $a = 70$ and $b = 15$ (2) $a = 1770$ and $b = 234$

Let $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$. Consider the linear Diophantine equation

$$ax + by = c. \tag{1.3.1}$$

Theorem 1.3.3. (1) *The equation* (1.3.1) *has a solution in integers if and only if* $d \mid c$.

(2) *If* (x_0, y_0) *is any particular integer solution of* (1.3.1), *then all other solutions are given by*

$$x = x_0 + (b/d)t \qquad \text{and} \qquad y = y_0 - (a/d)t$$

for varying integers t.

Proof. (1) Assume that Eq. (1.3.1) has a solution, say (x_1, y_1). Then $ax_1 + by_1 = c$. Since $d \mid a$ and $d \mid b$, we have $d \mid c$. Conversely, suppose that $d \mid c$. Since $\gcd(a, b) = d$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$. In addition, since $d \mid c$, $c = dq$ for some $q \in \mathbb{Z}$. Then

$$a(xq) + b(yq) = dq = c.$$

Hence, (xq, yq) is a desired solution.

(2) Assume that $d \mid c$ and $ax_0 + by_0 = c$, and let (x, y) be any other solution of (1.3.1). Then $ax + by = c$. This gives

$$a(x - x_0) + b(y - y_0) = 0, \tag{1.3.2}$$

so

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0),$$

which implies $\frac{a}{d} \mid \frac{b}{d}(y_0 - y)$. Since $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, we have $\frac{a}{d} \mid (y_0 - y)$. Thus, there exists $t \in \mathbb{Z}$ such that $y_0 - y = \frac{a}{d}t$, that is,

$$y = y_0 - \frac{a}{d}t.$$

Put this y into (1.3.2), we get

$$a(x - x_0) + b(-\frac{a}{d}t) = 0,$$

so

$$x = x_0 + \frac{b}{d}t.$$

Note that if (x_0, y_0) is a solution of $ax + by = c$, then

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + by_0 = c$$

for all integers t, and hence

$$x = x_0 + (b/d)t \qquad \text{and} \qquad y = y_0 - (a/d)t$$

are solution of (1.3.1) for all $t \in \mathbb{Z}$. □

Corollary 1.3.4. *If* $\gcd(a, b) = 1$ *and if* (x_0, y_0) *is a particular integer solution of the linear Diophantine equation* $ax + by = c$, *then all solutions are given by*

$$x = x_0 + bt \qquad \text{and} \qquad y = y_0 - at$$

for integer values of t.

Example 1.3.2. Determine all solutions in integers (if any) of the following Diophantine equations:
(1) $70x + 15y = 5$ (2) $1770x + 234y = 18$ (3) $33x + 121y = 919$

Example 1.3.3. Determine all solutions in positive integers of the Diophantine equation $21x + 49y = 903$.

Example 1.3.4. Solve: Divide 100 into two summands such that one is divisible by 7 and the other by 11.

Definition. The **least common multiple (lcm)** of two nonzero integers a and b, denoted by $\operatorname{lcm}(a, b)$ or $[a, b]$, is the positive integer m satisfying

(1) $a \mid m$ and $b \mid m$,

(2) if $a \mid c$ and $b \mid c$, with $c > 0$, then $m \leq c$.

Remarks. (1) If c is a common multiple of a and b, then $\operatorname{lcm}(a, b) \mid c$.

(2) If $a \mid b$, then $\operatorname{lcm}(a, b) = |b|$.

Theorem 1.3.5. *For positive integers a and b,*

$$\gcd(a, b) \operatorname{lcm}(a, b) = ab.$$

Proof. Let $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$. Since $d \mid a$, $d \mid ab$, so we have $m = \frac{ab}{d} \in \mathbb{Z}$. We shall show that $m = \operatorname{lcm}(a, b)$. Since $d \mid a$ and $d \mid b$, there exist $r, s \in \mathbb{Z}$ such that $a = dr$ and $b = ds$. Then

$$m = \frac{ab}{d} = \frac{(dr)(ds)}{d} = drs = as = rb,$$

so $a \mid m$ and $b \mid m$.

Next, let $c > 0$ be such that $a \mid c$ and $b \mid c$. Then there exist $u, v \in \mathbb{Z}$ such that $c = au$ and $c = bv$. Since $d = \gcd(a, b)$, $d = ax + by$ for some integers x and y. Thus,

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax + by)}{ab} = \frac{cax + cby}{ab} = \frac{bvax}{ab} + \frac{auby}{ab} = av + bu \in \mathbb{Z},$$

which gives $m \mid c$. But $m, c > 0$, so $m \leq c$. Hence, $m = [a, b]$. □

Corollary 1.3.6. *Given positive integers a and b,* $\operatorname{lcm}(a, b) = ab$ *if and only if* $\gcd(a, b) = 1$.

Proof. It follows from Theorem 1.3.5. □

Lemma 1.3.7. *Let $n > 1$ be factored as $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ for some primes p_i and $r, k_i \in \mathbb{N}$ for all $i \in \{1, 2, \dots, r\}$. Then for $d \in \mathbb{N}$,*

$$d \mid n \Leftrightarrow d = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}, \text{ where } 0 \leq a_i \leq k_i \text{ for all } i \in \{1, 2, \dots, r\}.$$

Hence, $\{d \in \mathbb{N} : d \mid n\} = \{p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} : 0 \leq a_i \leq k_i \text{ for all } i \in \{1, 2, \dots, r\}\}$.

Proof. Assume that $d \mid n$. If $d = 1$, then $d = p_1^0 p_2^0 \dots p_r^0$. Suppose that $d > 1$. If a prime p divides d, then $p \mid n$, so $p = p_i$ for some $i \in \{1, 2, \dots, n\}$. This implies that $d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$ for some $d_i \in \mathbb{N} \cup \{0\}$ for all $i \in \{1, 2, \dots, r\}$. Since $d \mid n$, we have $n = cd$ for some $c \in \mathbb{N}$ which also means that $c \mid n$. Thus, $c = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$ for some $c_i \in \mathbb{N} \cup \{0\}$ for all $i \in \{1, 2, \dots, r\}$. Hence,

$$p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = n = p_1^{c_1 + d_1} p_2^{c_2 + d_2} \dots p_r^{c_r + d_r},$$

so $k_i = c_i + d_i$ for all i. This forces that $k_i \geq d_i$ for all i. The converse of the statement is clear. □

Theorem 1.3.8. *Let a and b be two integers greater than 1 factored as*

$$a = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} \quad \textit{and} \quad b = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r},$$

where for $i = 1, 2, \dots, r$, each p_i is a prime with $p_1 < p_2 < \dots < p_r$, each a_i and b_i are nonnegative integers, and each a_i or b_i are positive. Then we have

$$\gcd(a, b) = p_1^{d_1} p_2^{d_2} \dots p_r^{d_r}, \ \textit{where } d_i = \min\{a_i, b_i\} \ \textit{ for all } i = 1, 2, \dots, r$$

and

$$\operatorname{lcm}(a, b) = p_1^{c_1} p_2^{c_2} \dots p_r^{c_r}, \ \textit{where } c_i = \max\{a_i, b_i\} \ \textit{ for all } i = 1, 2, \dots, r.$$

Proof. Let $d = p_1^{d_1} p_2^{d_2} \dots p_r^{d_r}$, where $d_i = \min\{a_i, b_i\}$ for all $i = 1, 2, \dots, r$. We shall show that $d = \gcd(a, b)$. Since $d_i \le a_i$ and $d_i \le b_i$ for all i, $d \mid a$ and $d \mid b$. Next, let $c \mid a$ and $c \mid b$. Write

$$c = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$$

for some $n_i \le a_i$ and $n_i \le b_i$ for all $i \in \{1, \dots, r\}$. Thus, $n_i \le \min\{a_i, b_i\} = d_i$ for all $i \in \{1, \dots, r\}$. Hence, $c \le d$.

Now, let $m = p_1^{c_1} p_2^{c_2} \dots p_r^{c_r}$, where $c_i = \max\{a_i, b_i\}$ for all i. We proceed to show that $m = \operatorname{lcm}(a, b)$. Since $c_i = \max\{a_i, b_i\}$, we have $a_i \le c_i$ and $b_i \le c_i$ for all i, so $a \mid m$ and $b \mid m$. Finally, let $c > 0$ and $a \mid c$ and $b \mid c$. Write

$$c = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r} t$$

for some $m_i \ge a_i$ and $m_i \ge b_i$ for all $i \in \{1, \dots, r\}$ and $\gcd(t, p_1 p_2 \dots p_r) = 1$. Thus, $m_i \ge \max\{a_i, b_i\} = c_i$ for all i, so $m \le c$. $\square$

Example 1.3.5. Let $a, b, c \in \mathbb{N}$. Prove that $\gcd(\operatorname{lcm}(a, b), c) = \operatorname{lcm}(\gcd(a, c), \gcd(b, c))$.

Solution. Let

$$a = p_1^{a_1} \dots p_r^{a_r}, \ b = p_1^{b_1} \dots p_r^{b_r}, \text{ and, } c = p_1^{c_1} \dots p_r^{c_r},$$

where for $i = 1, \dots, r$, each p_i is a prime with $p_1 < p_2 < \dots < p_r$, each $a_i, b_i, c_i \in \mathbb{N} \cup \{0\}$, and each a_i, b_i or c_i is positive. By Theorem 1.3.8, we have

$$d = \gcd(\operatorname{lcm}(a, b), c) = p_1^{d_1} \dots p_r^{d_r} \text{ and, } e = \operatorname{lcm}(\gcd(a, c), \gcd(b, c)) = p_1^{e_1} \dots p_r^{e_r},$$

where $d_i = \min\{\max\{a_i, b_i\}, c_i\}$ and $e_i = \max\{\min\{a_i, c_i\}, \min\{b_i, c_i\}\}$. Thus, to prove the result, it suffices to show that

$$D = \min\{\max\{\alpha, \beta\}, \gamma\} = \max\{\min\{\alpha, \gamma\}, \min\{\beta, \gamma\}\} = E$$

for all $\alpha, \beta, \gamma \in \mathbb{N} \cup \{0\}$. We distinguish six cases as follows.

	D	E		D	E
$\alpha \le \beta \le \gamma$	β	β	$\alpha \le \gamma \le \beta$	γ	γ
$\beta \le \alpha \le \gamma$	α	α	$\beta \le \gamma \le \alpha$	γ	γ
$\gamma \le \alpha \le \beta$	α	α	$\gamma \le \beta \le \alpha$	β	β

Hence, $D = E$. $\square$

Remark. It is similar to the gcd, we have $\operatorname{lcm}(a, \operatorname{lcm}(b, c)) = \operatorname{lcm}(\operatorname{lcm}(a, b), c)$. The least common multiple of three nonzero integers a, b and c is denoted by $\operatorname{lcm}(a, b, c)$ is defined by

$$\operatorname{lcm}(a, b, c) = \operatorname{lcm}(\operatorname{lcm}(a, b), c).$$

Consequently, the lcm of n nonzero integers $a_1, a_2, \ldots, a_n$ is defined inductively by the relation

$$\operatorname{lcm}(a_1, a_2, \ldots, a_n) = \operatorname{lcm}(\operatorname{lcm}(a_1, a_2, \ldots, a_{n-1}), a_n).$$

Exercise 1.3.

1. Find the $\gcd(a, b)$, express it as a linear combination of a and b and compute $\operatorname{lcm}(a, b)$.
   (i) $a = 741$ and $b = 715$ (ii) $a = 12075$ and $b = 4655$
2. Determine all solutions in integers (if any) of the following Diophantine equations:
   (i) $741x + 715y = 130$ (ii) $2072x + 1813y = 2849$ (iii) $117x + 143y = 919$
3. Determine all solutions in integers of $39x + 42y + 54z = 6$.
4. Determine all solutions in positive integers of the Diophantine equation $20x + 21y = 2010$.
5. If a and b are relatively prime positive integers, prove that there are no positive integers x and y such that $ab = ax + by$.
6. Find the prime factorization of the integers 1224, 3600 and 10140 and use them to compute $\gcd(1224, 3600, 10140)$ and $\operatorname{lcm}(1224, 3600, 10140)$.
7. Let a, b, c and d be integers with ab and cd not both 0. Write $(\cdot, \cdot)$ for $\gcd(\cdot, \cdot)$. Show that

$$(ab, cd) = (a, c)(b, d)\left(\frac{a}{(a, c)}, \frac{d}{(b, d)}\right)\left(\frac{c}{(a, c)}, \frac{b}{(b, d)}\right).$$

Chapter 2

The Theory of Congruences

2.1 Basic Properties of Congruence

Definition. Let m be a fixed positive integer. Two integers a and b are said to be **congruent modulo** m, symbolized by

$$a \equiv b \pmod{m} \quad \text{or} \quad a \equiv b \mod m$$

if m divides the difference $a - b$; that is, provided that $a - b = km$ for some integer k. The number m is called the **modulus of the congruence**. When $m \nmid (a - b)$, then we say that a is **incongruent to** b **modulo** m and in this case we write $a \not\equiv b \pmod{m}$.

Remark. If $m \mid a$, we may write $a \equiv 0 \pmod{m}$.

Theorem 2.1.1. *The congruence is an equivalence relation. That is, we have:*

(1) $a \equiv a \pmod{m}$ *(reflexivity),*

(2) $a \equiv b \pmod{m}$ *implies* $b \equiv a \pmod{m}$ *(symmetry),*

(3) $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$ *imply* $b \equiv c \pmod{m}$ *(transitivity).*

Theorem 2.1.2. *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then we have:*

(1) $ax + cy \equiv bx + dy \pmod{m}$ *for all integers* x *and* y*,*

(2) $ac \equiv bd \pmod{m}$*,*

(3) $a^n \equiv b^n \pmod{m}$ *for every positive integer* n*, and*

(4) $f(a) \equiv f(b) \pmod{m}$ *for every polynomial* f *with integer coefficients.*

Example 2.1.1. Let $N = a_0 + a_1 10 + \cdots + a_{n-1}10^{n-1} + a_n 10^n$ be the decimal expansion of the positive integer N, $0 \le a_k < 10$, and let

$$S = a_0 + a_1 + \cdots + a_n \quad \text{and} \quad T = a_0 - a_1 + a_2 - \cdots + (-1)^n a_n.$$

Then we have:

(1) $3 \mid N$ if and only if $3 \mid S$ and $9 \mid N$ if and only if $9 \mid S$,

(2) $11 \mid N$ if and only if $11 \mid T$.

Proof. Since $10 \equiv 1 \pmod 3$, we have

$$3 \mid N \Leftrightarrow N \equiv 0 \pmod 3 \Leftrightarrow a_0 + a_1 + \cdots + a_n \equiv 0 \pmod 3 \Leftrightarrow 3 \mid S.$$

The others statements are exercises. □

Theorem 2.1.3. *If $c > 0$, then $a \equiv b \pmod m$ if and only if $ac \equiv bc \pmod{mc}$.*

Proof. It follows from $m \mid (a-b) \Leftrightarrow mc \mid (a-b)c \Leftrightarrow mc \mid (ac-bc)$. □

Theorem 2.1.4. *If $ac \equiv bc \pmod m$, then $a \equiv b \pmod{\dfrac{m}{\gcd(m,c)}}$.*

Proof. Since $m \mid (a-b)c$, $\dfrac{m}{\gcd(m,c)} \,\Big|\, (a-b)\dfrac{c}{\gcd(m,c)}$. By Theorem 1.1.12, we have $\dfrac{m}{\gcd(m,c)} \,\Big|\, (a-b)$ because $\gcd\left(\frac{m}{\gcd(m,c)}, \frac{c}{\gcd(m,c)}\right) = 1$. □

Corollary 2.1.5. *If $ac \equiv bc \pmod m$ and $\gcd(m,c) = 1$, then $a \equiv b \pmod m$.*

Corollary 2.1.6. *Let p be a prime. If $ac \equiv bc \pmod p$ and $p \nmid c$, then $a \equiv b \pmod p$.*

Theorem 2.1.7. *If $a \equiv b \pmod m$, then $\gcd(a,m) = \gcd(b,m)$. In other words, numbers which are congruent modulo m have the same gcd with m.*

Proof. Assume that $a \equiv b \pmod m$. Then $a - b = mk$ for some $k \in \mathbb{Z}$. Thus, $\gcd(a,m) = \gcd(b+mk, m) = \gcd(b,m)$ by Lemma 1.3.1. □

Theorem 2.1.8. *For each integer a, there exists a unique integer r, with $0 \le r < m$, such that $a \equiv r \pmod m$.*

Proof. Let $a \in \mathbb{Z}$. By the division algorithm, there exist unique $q, r \in \mathbb{Z}$ such that $a = mq + r$, where $0 \le r < m$. Then $a \equiv r \pmod m$. □

Theorem 2.1.9. *If $a \equiv b \pmod m$ and $0 \le |a-b| < m$, then $a = b$.*

Proof. Since $m \mid (a-b)$, $m \le |a-b|$ unless $a - b = 0$. □

Corollary 2.1.10. *We have $a \equiv b \pmod m$ if and only if a and b give the same remainder when divided by m.*

Proof. It follows from Theorems 2.1.8 and 2.1.9. □

Theorem 2.1.11. *If $a \equiv b \pmod m$ and $a \equiv b \pmod n$, where $\gcd(m,n) = 1$, then $a \equiv b \pmod{mn}$.*

Proof. Since $\gcd(m,n) = 1$, we have $m \mid (a-b)$ and $n \mid (a-b)$ implies $mn \mid (a-b)$ by Corollary 1.1.11. □

Definition. Consider a fixed modulus $m > 0$. We denote by $[a]_m$ the set of all integers x such that $x \equiv a \pmod m$ and we call $[a]_m$ the **residue class of a modulo** m. That is,

$$[a]_m = \{x \in \mathbb{Z} : x \equiv a \pmod m\} = \{a + mq : q \in \mathbb{Z}\} = a + m\mathbb{Z}.$$

Since $\cdot \equiv \cdot \pmod{m}$ is an equivalence relation on $\mathbb{Z}$, for $a \in \mathbb{Z}$, the residue class of a modulo m is just the equivalence class of a with respect to this relation.

Properties of equivalence classes give the following theorem.

Theorem 2.1.12. *For a given modulus $m > 0$ and $a, b \in \mathbb{Z}$ we have:*

(1) $[a]_m = [b]_m$ *if and only if* $a \equiv b \pmod{m}$*,*

(2) $[a]_m \cap [b]_m = \emptyset$ *or* $[a]_m = [b]_m$*,*

(3) $\displaystyle\bigcup_{x \in \mathbb{Z}} [x]_m = \mathbb{Z}$*,*

(4) *two integers x and y are in the same residue class if and only if* $x \equiv y \pmod{m}$*, and*

(5) *the m residue classes $[0]_m, [1]_m, \ldots, [m-1]_m$ are disjoint and their union is the set of all integers.*

Definition. A set of m representatives, one from each of the residue classes $[0]_m, [1]_m, \ldots, [m-1]_m$ is called a **complete residue system modulo** m. That is, the set of integers $\{a_1, a_2, \ldots, a_m\}$ is a complete residue system modulo m if

(1) $a_i \not\equiv a_j \pmod{m}$ whenever $i \neq j$;

(2) for each integer x, there is an $i \in \{1, 2, \ldots, m\}$ such that $x \equiv a_i \pmod{m}$.

Example 2.1.2. $\{0, 1, \ldots, m-1\}$ is a complete residue system modulo m.
$\{-12, -4, 11, 13, 22, 82, 91\}$ is a complete residue system modulo 7.

Remarks. Let m be a positive integer.

(1) Let $S = \{a_1, a_2, \ldots, a_m\} \subseteq \mathbb{Z}$. Then S is a complete residue system if and only if $a_i \not\equiv a_j \pmod{m}$ whenever $i \neq j$.

(2) If m is odd, then $\left\{0, \pm 1, \pm 2, \ldots, \pm \frac{m-1}{2}\right\}$ is a complete residue system modulo m.

(3) If m is even, then $\left\{0, \pm 1, \pm 2, \ldots, \pm \frac{m-2}{2}, \frac{m}{2}\right\}$ is a complete residue system modulo m.

Theorem 2.1.13. *Assume that* $\gcd(k, m) = 1$*. If $\{a_1, a_2, \ldots, a_m\}$ is a complete residue system modulo m, so is $\{ka_1, ka_2, \ldots, ka_m\}$.*

Proof. Assume that $ka_i \equiv ka_j \pmod{m}$ for some $i \neq j$. Since $\gcd(k, m) = 1$, $a_i \equiv a_j \pmod{m}$, so $\{a_1, \ldots, a_m\}$ is not a complete residue system modulo m. □

Exercise 2.1. 1. Prove that $7 \mid (3^{2n+1} + 2^{n+2})$ for all $n \in \mathbb{N}$ without using mathematical induction.

2. Let $N = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N. Prove that $2^k \mid N$ if and only if $2^k \mid (a_k 10^k + \cdots + a_1 10 + a_0)$ for all $k \in \mathbb{N}$.

3. (i) Find the remainders when 2^{50} and 41^{65} are divided by 7.
(ii) What is the remainder when the sum $1^5 + 2^5 + \cdots + 99^5 + 100^5$ is divided by 4.

4. (i) For any integer a, prove that the units digit of a^2 is $0, 1, 4, 5, 6$ or 9.
(ii) Find all positive integers n for which $1! + 2! + 3! + \cdots + n!$ is a perfect square.

5. If $\{a_1, a_2, \ldots, a_p\}$ is a complete residue system modulo an odd prime p, prove that p divides $a_1 + a_2 + \cdots + a_p$.

2.2 Linear Congruences

Consider a linear congruence

$$ax \equiv b \pmod{m}. \tag{2.2.1}$$

Note that $ax + my = b$ has a solution $\Leftrightarrow$ $ax \equiv b \mod m$ has a solution.

Theorem 2.2.1. *Let $d = \gcd(a, m)$.*

(1) *$ax \equiv b \pmod{m}$ has a solution if and only if $d \mid b$.*

(2) *If $d \mid b$ and x_0 is its solution, then it has d mutually incongruent solutions modulo m given by $x = x_0 + (m/d)t$, where $t = 0, 1, \ldots, d-1$.*

Proof. (1) follows from Theorem 1.3.3 (1). To prove (2), assume that $d \mid b$ and $ax \equiv b \pmod{m}$. By Theorem 1.3.3 (2), $x = x_0 + \frac{m}{d}t$, $t \in \mathbb{Z}$, are solutions of (2.2.1). Let $x = x_0 + \frac{m}{d}t$ and $x' = x_0 + \frac{m}{d}t'$ for some $t, t' \in \mathbb{Z}$. Then

$$x \equiv x' \pmod{m} \Leftrightarrow \tfrac{m}{d}t \equiv \tfrac{m}{d}t' \pmod{m} \Leftrightarrow t \equiv t' \pmod{\tfrac{m}{\gcd(\frac{m}{d}, m)} = d}.$$

Since $\{0, 1, \ldots, d-1\}$ is a complete residue system modulo d, $x = x_0 + (m/d)t$, where $t \in \{0, 1, \ldots, d-1\}$ are incongruent solutions modulo m. □

Corollary 2.2.2. *If $\gcd(a, m) = 1$, then the linear congruence $ax \equiv b \pmod{m}$ has a unique solution modulo m. The solution of $ax \equiv 1 \pmod{m}$ is called the* **inverse of** a **modulo** m.

Example 2.2.1. Find a complete set of mutually incongruent solutions (if any) of
(1) $21x \equiv 11 \pmod{7}$ (2) $15x \equiv 9 \pmod{12}$

Example 2.2.2. Find the inverse of 201 modulo 251.

Theorem 2.2.3. [Chinese Remainder Theorem] *Assume that $m_1, m_2, \ldots, m_r$ are pairwise relatively prime positive integers: $\gcd(m_i, m_k) = 1$ if $i \neq k$. Let $b_1, b_2, \ldots, b_r$ be arbitrary integers. Then the system of congruences*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_r \pmod{m_r} \end{aligned}$$

has exactly one solution modulo the product $m_1 m_2 \cdots m_r$.

Proof. For each i, let $m_i' = m/m_i$, where $m = m_1 m_2 \ldots m_r$. Since $m_1, m_2, \ldots, m_r$ are pairwise relatively prime, $\gcd(m_i', m_i) = 1$ for all i. Then for each $i \in \{1, 2, \ldots, r\}$, $m_i' y_i \equiv 1 \pmod{m_i}$ for some $y_i \in \mathbb{Z}$. Choose

$$x = b_1 m_1' y_1 + b_2 m_2' y_2 + \cdots + b_r m_r' y_r \in \mathbb{Z}.$$

Thus, $x \equiv b_i m_i' y_i \equiv b_i \pmod{m_i}$ for all $i \in \{1, 2, \ldots, r\}$.

To prove the uniqueness, let x_1 and x_2 be solutions of the system. Then

$$x_1 \equiv b_i \pmod{m_i} \quad \text{and} \quad x_2 \equiv b_i \pmod{m_i}$$

for all i. Thus, $x_1 \equiv x_2 \pmod{m_i}$ for all $i \in \{1, \dots, r\}$. Since $m_1, m_2, \dots, m_r$ are pairwise relatively prime, $x_1 \equiv x_2 \pmod{m_1 m_2 \dots m_r}$ by Theorem 2.1.11. □

Example 2.2.3. Solve the following system of linear congruences.

(1) $$\begin{aligned} x &\equiv 2 \pmod{3} \\ 2x &\equiv 3 \pmod{5} \\ 3x &\equiv 4 \pmod{7} \end{aligned}$$

(2) $$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

Theorem 2.2.4. *Let m_1 and m_2 be positive integers and $d = \gcd(m_1, m_2)$. For integers b_1 and b_2, the congruences*

$$x \equiv b_1 \pmod{m_1} \quad \textit{and} \quad x \equiv b_2 \pmod{m_2}$$

admit a simultaneous solution if and only if $d \mid (b_1 - b_2)$. Moreover, if a solution exists, then it is unique modulo $\operatorname{lcm}(m_1, m_2)$.

Proof. Assume that x_0 is a solution. Then

$$x_0 \equiv b_1 \pmod{m_1} \quad \text{and} \quad x_0 \equiv b_2 \pmod{m_2},$$

so

$$x_0 \equiv b_1 \pmod{d} \quad \text{and} \quad x_0 \equiv b_2 \pmod{d}$$

since $d \mid m_1$ and $d \mid m_2$. Hence, $b_1 \equiv b_2 \pmod{d}$. Conversely, suppose that $d \mid (b_1 - b_2)$. That is, $b_1 - b_2 = dk$ for some $k \in \mathbb{Z}$. Since $d = \gcd(m_1, m_2)$, there are integers s and t such that $d = m_1 s + m_2 t$. Thus,

$$b_1 - b_2 = dk = m_1 ks + m_2 kt,$$

so

$$m_2 kt \equiv (b_1 - b_2) \pmod{m_1}.$$

This gives $m_2 kt + b_2 \equiv b_1 \pmod{m_1}$. Choose $x_0 = m_2 kt + b_2$. Then

$$x_0 \equiv b_1 \pmod{m_1} \quad \text{and} \quad x_0 \equiv b_2 \pmod{m_2}.$$

Finally, the uniqueness follows from the fact that $m_1 \mid c$ and $m_2 \mid c$ implies $\operatorname{lcm}(m_1, m_2) \mid c$. □

Example 2.2.4. Solve the following system of linear congruences.

(1) $$\begin{aligned} x &\equiv 7 \pmod{10} \\ x &\equiv 4 \pmod{12} \end{aligned}$$

(2) $$\begin{aligned} x &\equiv 6 \pmod{8} \\ x &\equiv 2 \pmod{12} \end{aligned}$$

Remark. Assume that $\gcd(m, n) = 1$. Let $\{a_1, \dots, a_m\}$ be a complete residue system modulo m, $\{b_1, \dots, b_n\}$ be a complete residue system modulo n and $\{c_1, \dots, c_{mn}\}$ be a complete residue system modulo mn. By the Chinese remainder theorem, the pair

$$x \equiv a_i \pmod{m} \quad \text{and} \quad x \equiv b_j \pmod{n}$$

has a unique solution c_k modulo mn. Conversely, let $k \in \{1, 2, \dots, mn\}$. Then c_k is a solution of

$$x = c_k \equiv a_i \pmod{m} \quad \text{and} \quad x = c_k \equiv b_j \pmod{n}$$

for some $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, n\}$. Thus, there is a 1-1 correspondence between

$$\left\{ \begin{array}{ll} x \equiv a_i & \pmod{m} \\ x \equiv b_j & \pmod{n} \end{array} : i \in \{1, \dots, m\} \text{ and } j \in \{1, \dots, n\} \right\} \quad \text{and} \quad \{c_1, \dots, c_{mn}\}.$$

Exercise 2.2. 1. Solve the following linear congruences (if possible).
(i) $25x \equiv 15 \pmod{29}$ (ii) $36x \equiv 42 \pmod{102}$ (iii) $140x \equiv 132 \pmod{301}$

2. Solve the following system of linear congruences (if possible).
(i) $\begin{array}{ll} x \equiv 1 & \pmod{10} \\ x \equiv 3 & \pmod{15} \end{array}$ (ii) $\begin{array}{ll} x \equiv 2 & \pmod{6} \\ x \equiv 11 & \pmod{15} \end{array}$

3. (i) Solve the system $x \equiv 5 \pmod{6}$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$.
(ii) Find the smallest integer $a > 2$ such that $2 \mid a$, $3 \mid (a+1)$, $4 \mid (a+2)$ and $5 \mid (a+3)$.

4. If $x \equiv a \pmod{n}$, prove that either $x \equiv a \pmod{2n}$ or $x \equiv a + n \pmod{2n}$.

2.3 Reduced Residue Systems

Definition. Let m be a positive integer. A subset S of a complete residue system modulo m is called a **reduced residue system modulo** m if for $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$, there exists an $r \in S$ such that $a \equiv r \pmod{m}$.

Remark. If $\{a_1, a_2, \dots, a_m\}$ is a complete residue system modulo m, then

$$S = \{a_i : i \in \{1, \dots, m\} \text{ and } \gcd(a_i, m) = 1\}$$

is a reduced residue system modulo m.

Example 2.3.1. (1) $\{1, 5, 7, 11\}$ is a reduced residue system modulo 12.

(2) $\{1, 2, \dots, p-1\}$ is a reduced residue system modulo a prime p.

(3) $\{r \in \mathbb{Z} : 0 \le r < m \text{ and } \gcd(r, m) = 1\}$ is a reduced residue system modulo m.

Definition. Let m be a positive integer. Define the **Euler's totient** $\phi(m)$ by

$$\phi(m) = |\{r \in \mathbb{Z} : 0 \le r < m \text{ and } \gcd(r, m) = 1\}|.$$

E.g., $\phi(12) = 4$. Note that $\phi(1) = 1$ and $\phi(m) \le m - 1$ for all $m \ge 2$. Clearly, if p is a prime, then $\phi(p) = p - 1$. Moreover, $\phi(m) = m - 1$ if and only if m is a prime.

Theorem 2.3.1. *If p is a prime, then $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(1 - 1/p)$ for every $k \in \mathbb{N}$.*

Proof. Consider the p^{k-1}-row-list of integers from 1 to p^k:

$$\begin{array}{ccccc} 1 & 2 & 3 & \dots & p \\ p+1 & p+2 & p+3 & \dots & 2p \\ \vdots & \vdots & \vdots & & \vdots \\ (p^{k-1}-1)p+1 & (p^{k-1}-1)p+2 & (p^{k-1}-1)p+3 & \dots & p^k. \end{array}$$

Note that for $1 \le a \le p^k$, $\gcd(a, p^k) = 1 \Leftrightarrow p \nmid a$. Thus, we eliminate only the last column, so $\phi(p^k) = p^k - p^{k-1}$. □

Remarks. (1) By Theorem 2.1.7, a reduced residue system modulo m consists of $\phi(m)$ integers. Moreover, from Theorem 2.1.8, any $\phi(m)$ incongruent integers relatively prime to m form a reduced residue system modulo m.

(2) $\gcd(a, c) = 1 = \gcd(b, c) \Leftrightarrow \gcd(ab, c) = 1$.

Theorem 2.3.2. *If* $\gcd(a, m) = 1$ *and* $\{r_1, r_2, \dots, r_{\phi(m)}\}$ *is a reduced residue system modulo m, then* $\{ar_1, ar_2, \dots, ar_{\phi(m)}\}$ *is also a reduced residue system.*

Proof. Since $\gcd(r_i, m) = 1$ for all i and $\gcd(a, m) = 1$, $\gcd(ar_i, m) = 1$ for all $i \in \{1, \dots, \phi(m)\}$. Assume that $ar_i \equiv ar_j \pmod{m}$ for some $i, j \in \{1, \dots, m\}$. Since $(a, m) = 1$, we have $r_i \equiv r_j \pmod{m}$ by Corollary 2.1.5, so $i = j$. Hence, $ar_1, ar_2, \dots, ar_{\phi(m)}$ are $\phi(m)$ incongruent integers relatively prime to m, and so they form a reduced residue system modulo m. □

Theorem 2.3.3. [Euler] *Assume that* $\gcd(a, m) = 1$. *Then we have* $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof. Let $\{r_1, r_2, \dots, r_{\phi(m)}\}$ be a reduced residue system modulo m. By Theorem 2.3.2, we have $\{ar_1, ar_2, \dots, ar_{\phi(m)}\}$ is a reduced residue system. Then from Theorem 2.1.8,

$$(ar_1)(ar_2)\dots(ar_{\phi(m)}) \equiv r_1 r_2 \dots r_{\phi(m)} \pmod{m},$$

so

$$a^{\phi(m)} r_1 r_2 \dots r_{\phi(m)} \equiv r_1 r_2 \dots r_{\phi(m)} \pmod{m}.$$

Since $\gcd(r_i, m) = 1$ for all i, $\gcd(r_1 r_2 \dots r_{\phi(m)}, m) = 1$. Hence, $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Corollary 2.3.4. [Fermat] *If p is a prime, then* $a^p \equiv a \pmod{p}$ *for all* $a \in \mathbb{Z}$.

Proof. If $p \mid a$, then $p \mid (a^p - a)$. Assume that $p \nmid a$. Then $\gcd(a, p) = 1$, so by Euler's theorem, we have $a^{\phi(p)} \equiv 1 \pmod{p}$. Since $\phi(p) = p - 1$, we have $a^{p-1} \equiv 1 \pmod{p}$. Hence, $a^p \equiv a \pmod{p}$. □

Remark. If $\gcd(a, m) = 1$, then $a^{\phi(m)-1} a \equiv 1 \pmod{m}$, so $a^{\phi(m)-1}$ is the inverse of a modulo m.

Corollary 2.3.5. *If* $\gcd(a, m) = 1$, *then the solution (unique modulo m) of the linear congruence*

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

is given by $x \equiv ba^{\phi(m)-1} \pmod{m}$.

Example 2.3.2. Solve the linear congruences:
(1) $5x \equiv 3 \pmod{24}$ and (2) $25x \equiv 15 \pmod{120}$

Theorem 2.3.6. *If m and n are relatively prime positive integers, then* $\phi(mn) = \phi(m)\phi(n)$.

Proof. Consider the list of integers from 1 to mn:

$$\begin{array}{cccccc} 1 & 2 & \dots & r & \dots & m \\ m+1 & m+2 & \dots & m+r & \dots & 2m \\ 2m+1 & 2m+2 & \dots & 2m+r & \dots & 3m \\ \vdots & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & \dots & (n-1)m+r & \dots & nm. \end{array}$$

Clearly, each row forms a complete residue system modulo m. Each column forms a complete residue system by Theorem 2.1.13 because $\gcd(m,n) = 1$. Moreover, elements in each column are congruent modulo m, so they have the same gcd with m.

Since $\gcd(m,n) = 1$, we have

$$\gcd(k, mn) = 1 \quad \Leftrightarrow \quad \gcd(k,m) = 1 = \gcd(k,n)$$

for all $k \in \mathbb{Z}$. Thus,

$$\{k : 1 \le k \le mn, \gcd(k, mn) = 1\} = \{k : 1 \le k \le mn, \gcd(k,m) = 1 = \gcd(k,n)\}.$$

We now count the numbers relatively prime to m and to n. First, eliminate all columns which are not relatively prime to m. Then we have $\phi(m)$ columns left. Next, in each column, there are $\phi(n)$ members relatively prime to n. Hence, there are $\phi(m)\phi(n)$ numbers in $\{1, 2, \dots, mn\}$, which are relatively prime to m and to n. Therefore, $\phi(mn) = \phi(m)\phi(n)$. □

Corollary 2.3.7. *If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime-power factorization of $n > 1$, then*

$$\begin{aligned} \phi(n) &= \phi(p_1^{k_1})\phi(p_2^{k_2}) \dots \phi(p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \dots (p_r^{k_r} - p_r^{k_r-1}) \\ &= p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right). \end{aligned}$$

E.g., $\phi(1000) = \phi(2^3 \cdot 5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$.

Exercise 2.3.

1. For any integer a, prove that (i) $42 \mid a^7 - a$ (ii) $23 \nmid (a^2 + 1)$.
2. (i) Find the remainder when $2222^{5555} + 5555^{2222}$ is divided by 7.
   (ii) What is the last digit of 3^{100}?
   (iii) Use Euler's theorem to confirm that $51 \mid (10^{32n+9} - 7)$ for all $n \in \mathbb{N} \cup \{0\}$.
3. Find all positive integers n for which $n^{13} \equiv n \pmod{1365}$.
4. (i) Prove that $\phi(n) \equiv 2 \pmod 4$ when $n = 4$ and when $n = p^a$, a prime $p \equiv 3 \pmod 4$.
   (ii) Find all n for which $\phi(n) \equiv 2 \pmod 4$.
5. If $m > 1$ is an odd number, find the remainder when $2^{\phi(m)-1}$ is divided by m.
6. If p is a prime and $n \in \mathbb{N} \cup \{0\}$, prove that $a^{n(p-1)+1} \equiv a \pmod p$ for all $a \in \mathbb{Z}$.
7. (i) If the integer n has r distinct odd prime factors, prove that $2^r \mid \phi(n)$.
   (ii) If every prime that divides n also divides m, prove that $\phi(mn) = n\phi(m)$.
8. If a and b are relatively prime with 91, prove that $91 \mid (a^{12} - b^{12})$.
9. If p and q are distinct primes, prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

10. Assume that $\gcd(m, n) = 1$. Let $\{r_1, \dots, r_{\phi(m)}\}$ be a reduced residue system modulo m, $\{s_1, \dots, s_{\phi(n)}\}$ be a reduced residue system modulo n and $\{t_1, \dots, t_{\phi(mn)}\}$ be a reduced residue system modulo mn. Prove that there is a 1-1 correspondence between

$$\left\{ \begin{cases} x \equiv r_i \pmod{m} \\ x \equiv s_j \pmod{n} \end{cases} : i \in \{1, \dots, \phi(m)\} \text{ and } j \in \{1, \dots, \phi(n)\} \right\} \quad \text{and} \quad \{t_1, \dots, t_{\phi(mn)}\}.$$

Hence, we may deduce that $\phi(mn) = \phi(m)\phi(n)$ if $\gcd(m, n) = 1$.

2.4 Polynomial Congruences

Theorem 2.4.1. [Lagrange] *Given a prime p, let*

$$f(x) = c_0 + c_1 x + \cdots + c_n x^n$$

be a polynomial of degree n with integer coefficients such that $p \nmid c_n$. Then the polynomial congruence

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

has at most n incongruent solutions modulo p.

Proof. We use induction on $n \in \mathbb{N}$. For $n = 1$, we consider $f(x) = c_0 + c_1 x \equiv 0 \pmod{p}$ and $p \nmid c_1$. Then $c_1 x \equiv -c_0 \pmod{p}$. Since $p \nmid c_1$, $\gcd(c_1, p) = 1$, so by Corollary 2.2.2, there exists a unique x_0 modulo p such that $c_1 x_0 + c_0 \equiv 0 \pmod{p}$.

Assume that $n > 1$ and every polynomial $g(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$, where $p \nmid b_n$, $g(x) \equiv 0 \pmod{p}$ has at most n incongruent solutions modulo p. Let $f(x) = c_0 + c_1 x + \cdots + c_n x^n$ and $p \nmid c_n$. If $f(x) \equiv 0 \pmod{p}$ has no solutions modulo p, then the number of solution is zero and $\leq n$. Let x_0 be a solution of $f(x) \equiv 0 \pmod{p}$. Then

$$c_0 + c_1 x_0 + \cdots + c_n x_0^n \equiv 0 \pmod{p},$$

so

$$f(x) \equiv c_1(x - x_0) + c_2(x^2 - x_0^2) + \cdots + c_n(x^n - x_0^n) = (x - x_0)g(x) \pmod{p},$$

where $g(x) = b_0 + b_1 x + \cdots + c_n x^{n-1}$. Since $p \mid c_n$, by induction hypothesis we have $g(x) \equiv 0 \pmod{p}$ has at most $n - 1$ solutions modulo p. Together with x_0, $f(x) \equiv 0 \pmod{p}$ has at most $(n - 1) + 1 = n$ incongruent solutions modulo p. $\square$

The above theorem immediately implies:

Theorem 2.4.2. *If $f(x) = c_0 + c_1 x + \cdots + c_n x^n$ is a polynomial of degree n with integer coefficients, and if the congruence $f(x) \equiv 0 \pmod{p}$ has more than n solutions, where p is a prime, then every coefficient of f is divisible by p.*

Theorem 2.4.3. *For any prime p, all the coefficients of the polynomial*

$$f(x) = (x - 1)(x - 2) \dots (x - (p - 1)) - x^{p-1} + 1$$

are divisible by p.

Proof. Note that $\deg f(x) < p-1$ and $f(1), f(2), \ldots, f(p-1)$ are congruent to 0 modulo p by Fermat. Hence, all coefficients of f is divisible by p. $\square$

Theorem 2.4.4. [Wilson] *For any prime p, we have*

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

Proof. The constant term of $f(x) = (x-1)(x-2)\ldots(x-(p-1)) - x^{p-1} + 1$ is

$$(-1)^{p-1}(p-1)! + 1.$$

By Theorem 2.4.3, it is divisible by p. Since $p = 2$ or p is odd, $(-1)^{p-1} \equiv 1 \pmod{p}$. Hence, $(p-1)! \equiv -1 \pmod{p}$ as desired. $\square$

Remark. The converse of Wilson's theorem also holds. That is, if $n > 1$ and $(n-1)! \equiv -1 \pmod{n}$, then n is a prime.

Proof. Let $n > 1$. Assume that n is composite. Then there is a prime $p < n$ such that $p \mid n$, so $p \mid (n-1)!$. Since $n \mid (n-1)! + 1$, $p \mid 1$, a contradiction. Hence, n is a prime. $\square$

Theorem 2.4.5. [Wolstenholme] *For any prime $p \geq 5$, we have*

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}.$$

Proof. Since $p \geq 5$,

$$g(x) = (x-1)(x-2)\ldots(x-(p-1)) = x^{p-1} + c_{p-2}x^{p-2} + \cdots + c_2x^2 + c_1x + (p-1)!.$$

Observe that $c_1, c_2, \ldots, c_{p-2}$ are the coefficients of $x, x^2, \ldots, x^{p-2}$ of $f(x)$ in Theorem 2.4.3, so $p \mid c_i$ for all $i \in \{1, 2, \ldots, p-2\}$. In particular,

$$-c_1 = \sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p}.$$

Moreover,

$$(p-1)! = g(p) = p^{p-1} + c_{p-2}p^{p-2} + \cdots + c_2p^2 + c_1p + (p-1)!.$$

Hence, $0 \equiv c_1p \pmod{p^3}$, so $c_1 \equiv 0 \pmod{p^2}$. $\square$

Remark. If p is a prime and $a^2 \equiv b^2 \pmod{p}$, then $a \equiv \pm b \pmod{p}$.

Theorem 2.4.6. *Let p be an odd prime. Then $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.*

Proof. Let a be a solution of $x^2 \equiv -1 \pmod{p}$. Then $p \nmid a$, so $a^{p-1} \equiv 1 \pmod{p}$. This implies

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

Since p is odd, $\frac{p-1}{2}$ must be even, so $4 \mid (p-1)$. Conversely, assume that $p \equiv 1 \pmod 4$. Observe that

$$\begin{aligned}(p-1)! &= \left[1\cdot 2\cdots \frac{p-1}{2}\right]\left[\left(p-\frac{p-1}{2}\right)\cdots(p-2)(p-1)\right]\\ &\equiv \left[1\cdot 2\cdots \frac{p-1}{2}\right]\left[\left(-\frac{p-1}{2}\right)\cdots(-2)(-1)\right] = (-1)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p.\end{aligned}$$

By Wilson's theorem, we have $(p-1)! \equiv -1 \pmod p$ and $p \equiv 1 \pmod 4$ implies $\frac{p-1}{2}$ is even. Hence,

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

Therefore, $\pm\left(\frac{p-1}{2}\right)!$ are solutions of $x^2 \equiv -1 \pmod p$. □

Example 2.4.1. Solutions of $x^2 \equiv -1 \pmod{37}$ are $\pm\left(\frac{37-1}{2}\right)! = \pm 18!$.

Exercise 2.4.

1. Show that $18! \equiv -1 \pmod{437}$.
2. Prove that for $1 < k < p-1$, $(p-k)!(k-1)! \equiv (-1)^k \pmod p$.
3. Let $n > 3$. If p and q are primes such that $p \mid n!$ and $q \mid ((n-1)! - 1)$, prove that $p < q$.
4. Given a prime number p, prove that $(p-1)! \equiv p-1 \pmod{1+2+\cdots+(p-1)}$.
5. Let p be a prime, $p \geq 5$, and write $1 + \dfrac{1}{2} + \dfrac{1}{3} + \cdots + \dfrac{1}{p} = \dfrac{r}{ps}$. Prove that $p^3 \mid (r-s)$.
6. Show that if a prime $p \equiv 3 \pmod 4$, then $\left(\dfrac{p-1}{2}\right)! \equiv \pm 1 \pmod p$.
7. Let p be an odd prime. Prove that
$$1^2\cdot 3^2\cdots(p-2)^2 \equiv (-1)^{(p+1)/2} \pmod p \text{ and } 2^2\cdot 4^2\cdots(p-1)^2 \equiv (-1)^{(p+1)/2} \pmod p.$$
8. Find all $n \in \mathbb{N}$ for which $(n-1)! + 1$ is a power of n. (*Hint*: Try to show that $n \leq 5$.)

Chapter 3

Number-Theoretic Functions

3.1 Multiplicative Functions

Definition. A real- or complex-valued function defined on the positive integers is called an **arithmetic function** or a **number-theoretic function**.

Throughout this chapter, variables occurring as arguments of number-theoretic functions are understood to be positive. The same applies to their divisors.

Examples 3.1.1. The following functions are arithmetic functions.

(1) $\phi(n) = |\{r \in \mathbb{Z} : 0 \le r < n \text{ and } \gcd(r,n) = 1\}|$.

(2) $\tau(n) =$ the number of positive divisors of $n = \displaystyle\sum_{d|n} 1$.

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

Here, $\displaystyle\sum_{d|n} f(d)$ means the sum of the values $f(d)$ as d runs over all *positive divisors* of the positive integer n. E.g., $\displaystyle\sum_{d|12} f(d) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$.

Theorem 3.1.1. *Let p be a prime and $k \in \mathbb{N} \cup \{0\}$. Then*

$$\tau(p^k) = |\{1, p, p^2, \dots, p^k\}| = k + 1$$

and

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

Definition. A number-theoretic function f which is *not* identically zero is said to be **multiplicative** if $\forall m, n \in \mathbb{N}, \gcd(m,n) = 1 \Rightarrow f(mn) = f(m)f(n)$.

Example 3.1.2. The following functions are multiplicative.

(1) ϕ (Theorem 2.3.6) (2) $U(n) = 1$ for all $n \in \mathbb{N}$ (3) $N(n) = n$ for all $n \in \mathbb{N}$.

Remark. Let f be a multiplicative function. Then $f(1) = f(1 \cdot 1) = f(1)f(1)$, so $f(1) = 0$ or 1. If $f(1) = 0$, then $f(n) = f(1 \cdot n) = f(1)f(n) = 0$, so f is the zero function. Hence, if f is multiplicative, then $f(1) = 1$.

Lemma 3.1.2. *f is multiplicative $\Leftrightarrow$ $f(1) = 1$ and $f(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = f(p_1^{k_1}) f(p_2^{k_2}) \dots f(p_r^{k_r})$ for all distinct primes p_i and $r, k_i \in \mathbb{N}$.*

Remarks. (1) From the above lemma, to compute the values of a multiplicative function f, it suffices to know only the values of $f(p^k)$ for all primes p and $k \in \mathbb{N}$.

(2) If f and g are multiplicative functions and $f(p^k) = g(p^k)$ for all primes p and $k \in \mathbb{N}$, then $f = g$.

Definition. A number-theoretic function f which is *not* identically zero is said to be **completely multiplicative** if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$.

E.g., (1) $U(n) = 1$, for all $n \in \mathbb{N}$, and (2) $N(n) = n$, for all $n \in \mathbb{N}$, are completely multiplicative.

Remark. If f is completely multiplicative, then

$$f(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = f(p_1)^{k_1} f(p_2)^{k_2} \dots f(p_r)^{k_r}.$$

Thus, to determine the values of a completely multiplicative function f, it suffices to know only the values of $f(p)$ for all primes p.

By Lemma 1.3.7, we have the next result.

Theorem 3.1.3. *If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of $n > 1$, then*

$$\tau(n) = (k_1 + 1)(k_2 + 2) \dots (k_r + 1) = \tau(p_1^{k_1}) \tau(p_2^{k_2}) \dots \tau(p_r^{k_r}).$$

Moreover, τ is multiplicative.

Definition. A positive integer n is a perfect square number if $\exists a \in \mathbb{Z}, n = a^2$.

Remarks. (1) If n is a perfect square number, then $n \equiv 0$ or $1 \pmod 4$.

(2) n is a perfect square if and only if $\tau(n)$ is odd.

Let $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of $n > 1$. Consider the product

$$\begin{aligned}(1 + p_1 + p_1^2 + \dots + p_1^{k_1})(1 + p_2 + p_2^2 + \dots + p_2^{k_2}) \dots (1 + p_k + p_k^2 \dots + p_r^{k_r}) \\ = \sum \{p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} : \ 0 \le a_i \le k_i \text{ for all } i \in \{1, 2, \dots, r\}\} \\ = \sum \{d \in \mathbb{N} : d \mid n\} = \sigma(n).\end{aligned}$$

Theorem 3.1.4. *If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of $n > 1$, then*

$$\begin{aligned}\sigma(n) &= (1 + p_1 + p_1^2 + \dots + p_1^{k_1})(1 + p_2 + p_2^2 + \dots + p_2^{k_2}) \dots (1 + p_k + p_k^2 \dots + p_r^{k_r}) \\ &= \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1} \\ &= \sigma(p_1^{k_1}) \sigma(p_2^{k_2}) \dots \sigma(p_r^{k_r}).\end{aligned}$$

Moreover, σ is multiplicative.

Lemma 3.1.5. *Assume that* $\gcd(m,n) = 1$. *Then*

$$\{d \in \mathbb{N} : d \mid mn\} = \{d_1d_2 : d_1, d_2 \in \mathbb{N}, d_1 \mid m,\ d_2 \mid n \text{ and } \gcd(d_1,d_2) = 1\}.$$

Proof. The result is clear when m or n is 1. Assume that $m,n > 1$ and $\gcd(m,n) = 1$. Let $m = p_1^{m_1} \dots p_r^{m_r}$ and $n = q_1^{n_1} \dots q_s^{n_s}$, where p_i and q_j are all distinct primes and $m_i, n_j \in \mathbb{N}$ for all $i \in \{1,\dots,r\}$ and $j \in \{1,\dots,s\}$.

Suppose that $d \mid mn$. By Lemma 1.3.7, $d = p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$ for some $0 \le a_i \le m_i$ and $0 \le b_j \le n_j$ for all i, j. Thus $d = d_1d_2$ where $d_1 = p_1^{a_1} \dots p_r^{a_r}$, $d_2 = q_1^{b_1} \dots q_s^{b_s}$, so $d_1 \mid m$, $d_2 \mid n$ and $\gcd(d_1,d_2) = 1$. The converse is clear. □

Remark. If $\gcd(m,n) = 1$, then the above lemma gives

$$\sum_{d \mid mn} f(d) = \sum_{\substack{d_1 \mid m, d_2 \mid n,\\ \gcd(d_1,d_2)=1}} f(d_1d_2).$$

Theorem 3.1.6. *If f is multiplicative function and F is defined by*

$$F(n) = \sum_{d \mid n} f(d),$$

then F is also multiplicative.

Proof. Let $m,n \in \mathbb{N}$ be such that $\gcd(m,n) = 1$. Then

$$\begin{aligned} F(mn) &= \sum_{d \mid mn} f(d) = \sum_{\substack{d_1 \mid m, d_2 \mid n,\\ \gcd(d_1,d_2)=1}} f(d_1d_2) = \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1)f(d_2) \quad (\text{since } \gcd(d_1,d_2) = 1) \\ &= \sum_{d_1 \mid m} f(d_1) \sum_{d_2 \mid n} f(d_2) = F(m)F(n). \end{aligned}$$

Hence, F is multiplicative. □

Recall that $U(n) = 1$ for all $n \in \mathbb{N}$ and $N(n) = n$ for all $n \in \mathbb{N}$ are multiplicative. The above theorem gives another proof of the following result.

Corollary 3.1.7. $\tau(n) = \sum_{d \mid n} 1$ *and* $\sigma(n) = \sum_{d \mid n} d$ *are multiplicative.*

Theorem 3.1.8. $\sum_{d \mid n} \phi(d) = n$

Proof. We first observe that

$$\left\{\frac{1}{n}, \frac{2}{n}, \dots, \frac{n-1}{n}, \frac{n}{n}\right\} = \bigcup_{d \mid n} \left\{\frac{a}{d} : 1 \le a \le d \text{ and } \gcd(a,d) = 1\right\}.$$

Moreover, for $d \mid n$, each set in the union is of cardinality $\phi(d)$. Assume that $d_1 \mid n$, $d_2 \mid n$ and $\frac{a}{d_1} = \frac{b}{d_2}$ for some $1 \le a \le d_1, \gcd(a,d_1) = 1$ and $1 \le b \le d_2, \gcd(b,d_2) = 1$. Then $ad_2 = bd_1$ which implies $d_1 \mid ad_2$ and $d_2 \mid bd_1$. Since $\gcd(a, d_1) = 1 = \gcd(b, d_2)$, $d_1 \mid d_2$ and $d_2 \mid d_1$ by Corollary 1.1.12, so $d_1 = d_2$ and $a = b$. This shows that the union on the right hand side is a disjoint union. Hence,

$$n = \left|\left\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}\right\}\right| = \left|\bigcup_{d|n}\left\{\frac{a}{d} : 1 \le a \le d \text{ and } \gcd(a,d) = 1\right\}\right|$$
$$= \sum_{d|n}\left|\left\{\frac{a}{d} : 1 \le a \le d \text{ and } \gcd(a,d) = 1\right\}\right| = \sum_{d|n}\phi(d)$$

as desired. □

Exercise 3.1. 1. Find the smallest $n \in \mathbb{N}$ such that $\tau(n) = 10$.

2. Prove that $\sum_{d|n} \tau^3(d) = \left(\sum_{d|n} \tau(d)\right)^2$.
3. Prove that $\sigma(n)$ is odd if and only if n is a perfect square or twice a perfect square.
4. Prove that $\phi(m)\phi(n) = \phi(\gcd(m, n))\phi(\operatorname{lcm}(m, n))$ for all $m, n \in \mathbb{N}$.
5. Show that the number of ordered pairs of positive integers whose lcm is n is $\tau(n^2)$.
6. (i) For a fixed integer k, show that the function $f_k(n) = n^k$ for all $n \in \mathbb{N}$ is multiplicative.
   (ii) For each $k \in \mathbb{N}$, show that the function $\sigma_k(n) = \sum_{d|n} d^k$ for all $n \in \mathbb{N}$ is multiplicative and find a formula for it.
7. For $k \ge 2$, show each of the following:
   (i) $n = 2^{k-1}$ satisfies the equation $\sigma(n) = 2n - 1$;
   (ii) if $2^k - 1$ is prime, then $n = 2^{k-1}(2^k - 1)$ satisfies the equation $\sigma(n) = 2n$;
   (iii) if $2^k - 3$ is prime, then $n = 2^{k-1}(2^k - 3)$ satisfies the equation $\sigma(n) = 2n + 2$.
8. For any positive integer n, show that
   (i) $\sum_{d|n} \sigma(d) = \sum_{d|n} \frac{n}{d}\tau(d)$; (ii) $\sum_{d|n} \frac{n}{d}\sigma(d) = \sum_{d|n} d\tau(d)$; (iii) $\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$.

3.2 The Möbius Inversion Formula

Definition. An integer n is said to be **square-free** if it is *not* divisible by the square of any prime.

Remark. Every positive integer n can be written uniquely in the form $n = ab^2$, where $a, b \in \mathbb{N}$ and a is square-free.

Definition. [Möbius, 1832] For a positive integer n, we define the **Möbius function**, μ, by the rules

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } \exists \text{ a prime } p, p^2 \mid n, \text{ i.e., } n \text{ is } \textit{not} \text{ square-free}, \\ (-1)^r, & \text{if } n = p_1 p_2 \ldots p_r \text{ where } p_1, p_2, \ldots, p_r \text{ are distinct primes.} \end{cases}$$

Theorem 3.2.1. *The Möbius function μ is multiplicative.*

Proof. Note that $\mu(1) = 1$. Suppose $n > 1$ and write $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, where p_i are distinct primes and $k_i \ge 1$ for all i. If $k_j > 1$ for some $j \in \{1, 2, \ldots, r\}$, we have $\mu(n) = 0$ and $\mu(p_j^{k_j}) = 0$, so $\mu(n) = \mu(p_1^{k_1})\mu(p_2^{k_2}) \ldots \mu(p_r^{k_r})$. Assume that $k_i = 1$ for all i. Then $n = p_1 p_2 \ldots p_r$, so $\mu(n) = (-1)^r$. Since $\mu(p_i) = -1$ for all i, we have $\mu(p_1)\mu(p_2) \cdots \mu(p_r) = (-1)^r = \mu(n)$. Hence, μ is multiplicative by Lemma 3.1.2. □

Theorem 3.2.2. $E(n) = \sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1, \end{cases}$ *for all $n \in \mathbb{N}$ is a multiplicative function.*

Proof. By Theorem 3.1.6, E is multiplicative, and since

$$E(p^k) = \begin{cases} 1, & \text{if } k = 0, \\ 1 - 1 + 0 + \cdots + 0, & \text{if } k \geq 1, \end{cases}$$

we see that $E(n) = 0$ if n is divisible by a prime p, that is, if $n > 1$. □

Remark. For $n \in \mathbb{N}$, $\{d \in \mathbb{N} : d \mid n\} = \{n/d : d \in \mathbb{N} \text{ and } d \mid n\}$.

Lemma 3.2.3. *Let f and g be multiplicative functions. Then*

1. *fg and f/g are multiplicative (whenever the latter function is defined), and*
2. *$F(n) = \sum_{d|n} f(d)g(n/d) = \sum_{d|n} f(n/d)g(d)$ is a multiplicative function.*

Proof. Exercises. □

Definition. For arithmetic functions f and g, we define the **Dirichlet convolution** by

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d)$$

for all $n \in \mathbb{N}$.

Remarks. (1) Clearly, $f * g = g * f$ and we can verify that $f * (g * h) = (f * g) * h$.

(2) By Lemma 3.2.3, if f and g are multiplicative, then $f * g$ is also multiplicative.

(3) The set of multiplicative functions is an abelian group under the Dirichlet convolution with identity element $E(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1. \end{cases}$

Theorem 3.2.4. [Möbius Inversion Formula] *Let F and f be two arithmetic functions (not necessarily multiplicative) related by the formula*

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

Then $f(n) = \sum_{d|n} F(d)\mu(n/d) = \sum_{d|n} F(n/d)\mu(d) = \sum_{d_1 d_2 = n} F(d_1)\mu(d_2)$, i.e., $f = F * \mu$.

Proof. We have

$$\begin{aligned} \sum_{d|n} F(n/d)\mu(d) &= \sum_{d_1 d_2 = n} F(d_1)\mu(d_2) = \sum_{d_1 d_2 = n} \left(\sum_{d|d_1} f(d) \right) \mu(d_2) \\ &= \sum_{d_2 d | n} f(d)\mu(d_2) = \sum_{d|n} f(d) \sum_{d_2|(n/d)} \mu(d_2). \end{aligned}$$

But $\sum_{d_2|(n/d)} \mu(d_2) = 0$ unless $n/d = 1$ (that is, unless $d = n$) when it is 1, so that this last sum is equal to $f(n)$. □

Example 3.2.1. We know by Theorem 3.1.8 that $\sum_{d|n} \phi(d) = n$, i.e., $\phi * U = N$. The Möbius inversion formula gives $\phi = N * \mu$, i.e., we have

$$\phi(n) = \sum_{d|n} \frac{n}{d}\mu(d) = n \sum_{d|n} \frac{\mu(d)}{d} \quad \text{for all } n \in \mathbb{N}.$$

Corollary 3.2.5. *Let F and f be two arithmetic functions related by the formula*

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

If F is multiplicative, then f is also multiplicative.

Proof. It follows from Theorem 3.2.4 and Theorems 3.2.3, 3.2.1. □

Corollary 3.2.6. *Let F and f be two arithmetic functions related by the formula*

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

Then $f(n) = \prod_{d|n} F(n/d)^{\mu(d)}$.

Proof. Its proof is similar to the Möbius inversion formula and is left as an exercise. □

Exercise 3.2.

1. Prove Lemma 3.2.3 and Corollary 3.2.6.
2. Prove that $\sum_{d|n} \sigma(d)\mu(n/d) = n$ for all $n \in \mathbb{N}$.
3. Let f, g and h be arithmetic functions. Prove that
   (i) $f * (g * h) = (f * g) * h$, (ii) $f * (g + h) = f * g + f * h$,
   (iii) ($\exists$ an arithmetic function F such that $f * F = E$) if and only if $f(1) \neq 0$.
4. Determine the arithmetic function f such that $\mu = f * U$. Is f multiplicative? If so, find its values on the prime powers.
5. Show that if f is multiplicative, then $\sum_{d|n} \mu(d)f(d) = \prod_{\substack{p|n \\ p \text{ prime}}} (1 - f(p))$.
6. Show that $\prod_{d|n} d = n^{\tau(n)/2}$ for all $n \in \mathbb{N}$.

3.3 The Greatest Integer Function

Let $x \in \mathbb{R}$. By Archimedean property and well-ordering principle, we can prove that there exists an $n_x \in \mathbb{Z}$ such that

$$n_x \leq x < n_x + 1.$$

This leads to the following definition.

Definition. For each real number x, $[x]$ is the unique integer such that

$$x - 1 < [x] \leq x < [x] + 1.$$

That is, $[x]$ is the largest integer $\leq x$. Sometimes, $[x]$ is called the **floor of** x. Note that $[x] = \max((-\infty, x] \cap \mathbb{Z})$. The **greastest integer function** is the map $x \mapsto [x]$ for all $x \in \mathbb{R}$.

Some properties of $[x]$ are listed in the following theorem.

Theorem 3.3.1. *Let x, x_1 and x_2 be real numbers.*

(1) $x = [x] + \{x\}$, *where* $0 \le \{x\} < 1$. $\{x\}$ *is called the* **fractional part of** x.

(2) $[x] = x$ *if and only if x is an integer.*

(3) $[x + a] = [x] + a$, *if* $a \in \mathbb{Z}$.

(4) $[x] + [-x] = \begin{cases} 0, & \text{if } x \in \mathbb{Z}, \\ -1, & \text{otherwise.} \end{cases}$

(5) $[x_1] + [x_2] \le [x_1 + x_2] \le [x_1] + [x_2] + 1$.

(6) $[x/n] = [[x]/n]$ *if* $n \in \mathbb{N}$.

(7) $-[-x]$ *is the least integer* $\ge x$ *and* $[x + \frac{1}{2}]$ *is the nearest integer to* x.

(8) $0 \le [x] - 2[x/2] \le 1$.

(9) *If* $x_1 < x_2$, *then* $|(x_1, x_2] \cap \mathbb{Z}| = [x_2] - [x_1]$.

(10) *For* $d \in \mathbb{N}$ *and* $x > 0$, $|\{n \in \mathbb{N} : d \mid n \text{ and } n \le x\}| = [x/d]$, *so* $\displaystyle\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} [x/k]$.

Theorem 3.3.2. *If $a \in \mathbb{Z}$ and $m \in \mathbb{N}$, then*

$$a = m[a/m] + m\{a/m\} \quad \text{and} \quad 0 \le m\{a/m\} < m.$$

That is, $[a/m]$ and $m\{a/m\}$ are the quotient and the remainder in the division of a by m.

We write $p^e \| n$ if $p^e \mid n$ and $p^{e+1} \nmid n$, i.e., e is the highest exponent of p that divides n.

Theorem 3.3.3. [de Polignac's Formula] *If n is a positive integer and p is a prime, then the highest exponent of p that divides $n!$ is*

$$e = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots = \sum_{j=1}^{\infty} [n/p^j].$$

That is, $p^e \| n!$.

Proof. The sum has only finitely many nonzero terms, since $[n/p^k] = 0$ for $p^k > n$. Note that if $p > n$, then $p \nmid n!$ and $\sum_{j=1}^{\infty} [n/p^j] = 0$. If $p \le n$, then $[n/p]$ integers in $\{1, 2, \dots, n\}$ are divisible by p, namely,

$$p, 2p, 3p, \dots, [n/p]p.$$

Of these integers, $[n/p^2]$ are again divisible by p^2:

$$p^2, 2p^2, \dots, [n/p^2]p^2.$$

By the same idea, $[n/p^3]$ of these are divisible by p^3:

$$p^3, 2p^3, \dots, [n/p^3]p^3.$$

After finitely many repetitions of this argument, the total number of times p divides number in $\{1, 2, \ldots, n\}$ is precisely

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots.$$

Hence, this sum is the exponent of p appearing in the prime factorization of $n!$. □

Remark. Recall that $[x/k] = [[x]/k]$ if $k \in \mathbb{N}$, this shortens the computation for e as follows:

$$e = \left[\frac{n}{p}\right] + \left[\frac{[n/p]}{p}\right] + \left[\frac{[[n/p]/p]}{p}\right] + \cdots.$$

Example 3.3.1. Find the highest power of 7 that divides 1000!.

Proof. We compute $[1000/7] = 142$, $[142/7] = 20$, $[20/7] = 2$ and $[2/7] = 0$. Thus $e = 142+20+2+0 = 164$ is the highest power of 7 divides 1000!. □

Theorem 3.3.4. *If $0 \leq k \leq n$, then the binomial coefficient $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ is an integer.*

Proof. This follows from the fact that

$$[n/p^j] = [(n-k+k)/p^j] \geq [(n-k)/p^j] + [k/p^j]$$

for all $j \in \mathbb{N}$. □

Corollary 3.3.5. *For $k \in \mathbb{N}$, $k!$ divides the product of k consecutive integers.*

Exercise 3.3. 1. Prove Theorem 3.3.1 (6)–(10).

2. Prove that if $n \in \mathbb{N}$ and α is a non-negative real number, then $\displaystyle\sum_{k=0}^{n-1}\left[\alpha + \frac{k}{n}\right] = [n\alpha]$.

3. (i) Let F and f be two arithmetic functions related by the formula $F(n) = \sum_{d|n} f(d)$.
   Prove that $\displaystyle\sum_{k=1}^{n} F(k) = \sum_{k=1}^{n} f(k)[n/k]$ for all $n \in \mathbb{N}$.
   (ii) Conclude that $\displaystyle\sum_{k=1}^{n}\tau(k) = \sum_{k=1}^{n}[n/k]$ and $\displaystyle\sum_{k=1}^{n}\sigma(k) = \sum_{k=1}^{n}k[n/k]$.
   (iii) Evaluate the sum $\displaystyle\sum_{k=1}^{n}[n/k]\phi(n)$.

4. Find the highest power of 17 that divides 2010!.

5. (i) Verify that 1000! terminates in 249 zeros.
   (ii) For what values of n does $n!$ terminate in 37 zeros.

6. Find the greatest common divisor of the binomial coefficients $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$.

Chapter 4

Primitive Roots

4.1 The Order of an Integer Modulo n

Example 4.1.1. We know that $\phi(10) = 4$, and we observe that $\{1, 3, 7, 9\}$ is a reduced residue system modulo 10. Since

$$\begin{aligned} 3^1 &= 3 \equiv 3 \pmod{10}, & 7^1 &= 7 \equiv 7 \pmod{10}, \\ 3^2 &= 9 \equiv 9 \pmod{10}, & 7^2 &= 49 \equiv 9 \pmod{10}, \\ 3^3 &= 27 \equiv 7 \pmod{10}, & 7^3 &= 343 \equiv 3 \pmod{10}, \\ 3^4 &= 81 \equiv 1 \pmod{10}, & 7^4 &= 2401 \equiv 1 \pmod{10}, \end{aligned}$$

we see that each of $\{3, 3^2, 3^3, 3^4\}$ and $\{7, 7^2, 7^3, 7^4\}$ is also a reduced residue system modulo 10.

From Euler's theorem, we know that $a^{\phi(m)} \equiv 1 \pmod{m}$ whenever $\gcd(a, m) = 1$. This leads to the following definition.

Definition. Let $m > 1$ and $\gcd(a, m) = 1$. The **order of** a **modulo** m, $\mathrm{ord}_m\, a$, is the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$. That is,

$$\mathrm{ord}_m\, a = \min\{k \in \mathbb{N} : a^k \equiv 1 \pmod{m}\}.$$

Remarks. (1) $\mathrm{ord}_m\, a \le \phi(m)$.

(2) If $a \equiv b \pmod{m}$, then $\mathrm{ord}_m\, a = \mathrm{ord}_m\, b$.

(3) If $\gcd(a, m) > 1$, then $a^k \equiv 1 \pmod{m}$ cannot hold for any $k \in \mathbb{N}$.

Theorem 4.1.1. *Let* $m > 1$ *and* $\gcd(a, m) = 1$. *If* $\mathrm{ord}_m(a) = h$, *then*

$$\forall k \in \mathbb{N}(a^k \equiv 1 \pmod{m} \Leftrightarrow h \mid k).$$

In particular, $\mathrm{ord}_m(a) \mid \phi(m)$.

Proof. Suppose that $\mathrm{ord}_a(m) = h$. Then h is the smallest positive integer such that $a^h \equiv 1 \pmod{m}$. Let $k \in \mathbb{N}$. If $h \mid k$, then $k = hq$ for some $q \in \mathbb{N}$, so

$$a^k \equiv a^{hq} \equiv (a^h)^q \equiv 1 \pmod{m}.$$

On the other hand, assume that $a^k \equiv 1 \pmod{m}$. By the Division Algorithm, $\exists q, r \in \mathbb{Z}, k = hq + r$, where $0 \le r < h$. If $r > 0$, then

$$a^r = a^{k-hq} = a^k a^{-hq} \equiv a^k (a^h)^{-q} \equiv 1 \pmod{m}$$

which contradicts the minimality of h. Thus $h \mid k$. □

Example 4.1.2. Find the order of 3 and of 5 modulo 31.

Theorem 4.1.2. *If* $\mathrm{ord}_m(a) = h$*, then* $a^i \equiv a^j \pmod{m}$ *if and only if* $i \equiv j \pmod{h}$*.*

Proof. Let $\mathrm{ord}_m(a) = h$. Assume that $a^i \equiv a^j \pmod{m}$, where $i \ge j$. Then $a^{i-j} \equiv 1 \pmod{m}$. By Theorem 4.1.1, $h \mid (i - j)$.

Conversely, suppose that $i \equiv j \mod h$. Then $\exists q \in \mathbb{Z}, i = j + qh$. Since $a^h \equiv 1 \pmod{m}$,

$$a^i = a^{j+qh} = a^j (a^h)^q \equiv a^j \pmod{m}$$

as desired. □

Corollary 4.1.3. *If* $\mathrm{ord}_m(a) = h$*, then the integers* $a, a^2, \dots, a^h$ *are incongruent modulo* m*.*

Theorem 4.1.4. *If* $\mathrm{ord}_m(a) = h$*, then* $\mathrm{ord}_m(a^k) = \dfrac{h}{\gcd(h,k)}$.

Proof. Let $\mathrm{ord}_m(a) = h$ and $d = \gcd(h, k)$. Since $d \mid k$, $(a^k)^{h/d} = (a^h)^{k/d} \equiv 1 \pmod{m}$. Let $t \in \mathbb{N}$ be such that $(a^k)^t \equiv 1 \pmod{m}$. By Theorem 4.1.1, $h \mid kt$. Then $(h/d) \mid (k/d)t$. Recall that $\gcd(h/d, k/d) = 1$, so Corollary 1.1.12 gives $(h/d) \mid t$. Hence $h/d \le t$. □

Theorem 4.1.5. *Let* $\mathrm{ord}_m(a) = h_1$ *and* $\mathrm{ord}_m(b) = h_2$*. If* $\gcd(h_1, h_2) = 1$*, then*

$$\mathrm{ord}_m(ab) = h_1 h_2.$$

Proof. Assume that $\gcd(h_1, h_2) = 1$. Since $a^{h_1} \equiv 1 \pmod{m}$ and $b^{h_2} \equiv 1 \pmod{m}$,

$$(ab)^{h_1 h_2} = (a^{h_1})^{h_2} (b^{h_2})^{h_1} \equiv 1 \pmod{m}.$$

Let $t \in \mathbb{N}$ be such that $(ab)^t \equiv 1 \pmod{m}$. Then $b^{h_1 t} = a^{h_1 t} b^{h_1 t} = (ab)^{h_1 t} = ((ab)^t)^{h_1} = 1$, so $h_2 \mid h_1 t$ by Theorem 4.1.1. Since $\gcd(h_1, h_2) = 1$, we conclude by Corollary 1.1.12 that $h_2 \mid t$. Similarly, we can show that $h_1 \mid t$. We have thus by Corollary 1.1.11 that $h_1 h_2 \mid t$, so $h_1 h_2 \le t$. □

Definition. If $\gcd(a, m) = 1$ and a is of order $\phi(m)$ modulo m, then a is a **primitive root** of the integer m.

Example 4.1.3. (1) Since $\phi(31) = 30$, $\mathrm{ord}_{31} 3 = 30$ and $\mathrm{ord}_{31} 5 = 3$, 3 is a primitive root of 31 while 5 is not.

(2) 3 and 7 are all primitive roots of 10.

(3) 8 and 12 have no primitive root.

Remarks. (1) By Corollary 4.1.3, if a is a primitive root of m, then $\{a, a^2, \dots, a^{\phi(m)}\}$ is reduced residue system modulo m.

(2) Let a be a primitive root of m. For $k \in \mathbb{N}$,

$$a^k \text{ is a primitive root of } m \iff \operatorname{ord}_m(a^k) = \phi(m) \iff \gcd(\phi(m), k) = 1.$$

Hence, if m has a primitive root, then there are $\phi(\phi(m))$ incongruent primitive roots of m.

Example 4.1.4. Find all incongruent primitive roots modulo 31.

Proof. Since 3 is a primitive root of 31 and $\phi(31) = 30$, we have $3, 3^7, 3^{11}, 3^{13}, 3^{17}, 3^{19}$, 3^{23} and 3^{29} are all incongruent primitive roots of 31. □

Exercise 4.1.

1. Find the order of the integers 2, 3 and 5: (i) modulo 17 (ii) modulo 19 (iii) modulo 23.
2. (i) If a has order hk, then a^h has order k modulo n
   (ii) If a has order $m-1$, then m is a prime.
3. If g and g' are primitive roots of an odd prime p, then gg' is not a primitive root of p.
4. Given a has order 3 modulo p, where p is an odd prime. Show that $\operatorname{ord}_p(a+1) = 6$.

4.2 Integers Having Primitive Roots

Lemma 4.2.1. *If $d \mid p-1$, then the polynomial $x^d - 1$ is a factor of the polynomial $x^{p-1} - 1$.*

Proof. Since $d \mid p-1$, we have $p - 1 = dq$ for some $q \in \mathbb{N}$. Then

$$x^{p-1} - 1 = (x^d)^q - 1 = (x^d - 1)(x^{d(q-1)} + x^{d(q-2)} + \cdots + x^d + 1)$$

as desired. □

Recall that all the coefficients of the polynomial

$$f(x) = (x-1)(x-2)\ldots(x-(p-1)) - (x^{p-1} - 1)$$

is divisible by p (Theorem 2.4.3). That is, as polynomials,

$$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-(p-1)) \pmod{p}.$$

Corollary 4.2.2. *If $d \mid p-1$, then the congruence $x^d \equiv 1 \pmod{p}$ has d solutions.*

Proof. Since $d \mid p-1$, we have $x^d - 1$ is a factor of $x^{p-1} - 1$, so

$$x^d - 1 \equiv (x - a_1)(x - a_2)\ldots(x - a_d) \pmod{p}$$

for some distinct $a_1, a_2 \ldots, a_d$ in $\{1, 2, \ldots, p-1\}$. Thus $x^d \equiv 1 \pmod{p}$ has d solutions. □

Corollary 4.2.3. *If $d \mid p-1$, then the number of integers a, $1 \le a \le p-1$, having order d modulo p is either 0 or $\phi(d)$.*

Proof. Assume that $1 \le a \le p-1$ and $\operatorname{ord}_p a = d$. Then $a^d \equiv 1 \pmod{p}$ and by Corollary 4.1.3, $a, a^2, \ldots, a^d$ are incongruent modulo p and so are all solutions of $x^d \equiv 1 \pmod{p}$. Thus, every element of order d is congruent to a^k with $1 \le k \le d$ and $\gcd(k, d) = 1$. Hence, there are $\phi(d)$ such k. □

Theorem 4.2.4. *If p is a prime and $d \mid p-1$, then there are exactly $\phi(d)$ incongruent integers having order d modulo p.*

Proof. For each $d \mid p-1$, let $\psi(d)$ be the number of integers a, $1 \leq a \leq p-1$, having order d modulo p. Since each integer between 1 and $p-1$ has order d for some $d \mid p-1$,

$$p-1 = \sum_{d \mid p-1} \psi(d).$$

On the other hand, by Theorem 3.1.8, $p-1 = \sum_{d \mid p-1} \phi(d)$ and by Corollary 4.2.3, we have $0 \leq \psi(d) \leq \phi(d)$ for all $d \mid p-1$. Hence $\sum_{d \mid p-1} \psi(d) = \sum_{d \mid p-1} \phi(d)$ forces $\psi(d) = \phi(d)$ for all $d \mid p-1$. □

Corollary 4.2.5. *If p is a prime, then there are exactly $\phi(p-1)$ incongruent primitive roots of p.*

Example 4.2.1. Find all incongruent elements of order 5 modulo 31.

Lemma 4.2.6. *If p is a prime, then all coefficients of $f(x) = (x+1)^p - x^p - 1$ is divisible by p. Hence, p divides $\binom{p}{i}$ for all $1 \leq i \leq p-1$.*

Proof. It follows from Lagrange since $\deg f(x) = p-1$ and $f(a) \equiv 0 \pmod{p}$ for all $a \in \{0, 1, \dots, p-1\}$ by Fermat. □

Lemma 4.2.7. *Let $k \in \mathbb{N}$ and p be a prime. If $p > 2$ or $k > 1$, $p^k \| (a-b)$ and $p \nmid b$, then $p^{k+1} \| (a^p - b^p)$.*

Proof. Assume that $a \equiv b \pmod{p^k}$. Then $a = b + cp^k$ for some $c \in \mathbb{Z}$ and $p \nmid c$. Thus,

$$a^p = (b + cp^k)^p = b^p + \binom{p}{1} b^{p-1} cp^k + \binom{p}{2} b^{p-2} (cp^k)^2 + \cdots + \binom{p}{p-1} b (cp^k)^{p-1} + (cp^k)^p$$

By the previous lemma, the interior binomial coefficients are divisible by p. Hence, the p-components of the successive terms after the first, on the right side at at least $p^{k+1}, p^{2k+1}, \dots, p^{(p-1)k+1}, p^{kp}$. Note that $kp > k+1$ is equivalent to $k(p-1) > 1$ which follows from the hypothesis that $p > 2$ or $k > 1$. Since $p \nmid b$, we can conclude that $p^{k+1} \| (a^p - b^p)$. □

Theorem 4.2.8. *Let p be a prime and suppose that $p \nmid a$. Assume that $\operatorname{ord}_p a = h$ and let k be such that $p^k \| (a^h - 1)$. Then if $p > 2$ or $k > 1$, we have*

$$h_n = \operatorname{ord}_{p^n} a = \begin{cases} h, & \text{if } n \leq k; \\ hp^{n-k}, & \text{if } n \geq k. \end{cases}$$

Proof. a) Suppose that $n \leq k$. Since $p^k \mid (a^h - 1)$, $a^h \equiv 1 \pmod{p^n}$, so $h_n \mid h$. But $a^{h_n} \equiv 1 \pmod{p^n}$ implies $a^{h_n} \equiv 1 \pmod{p}$, and thus $h \mid h_n$. Hence $h_n = h$.
b) Suppose that $n \geq k$. Since $a^h \equiv 1 \pmod{p^k}$, by applying Lemma 4.2.7 repeatedly, we have $p^n \| (a^{hp^{n-k}} - 1)$. This implies that $h_n \mid hp^{n-k}$. Let $h_n = h' p^{n-l}$, where $h' \mid h$ and $l \geq k$. Now $a^{h_n} \equiv 1 \pmod{p^n}$ gives $a^{h_n} \equiv 1 \pmod{p}$, so $h \mid h_n$. Since $\gcd(h, p) = 1$, we get $h \mid h'$, so $h = h'$. Thus, $a^{hp^{n-l}} \equiv 1 \pmod{p^n}$. But $p^k \| (a^h - 1)$, so $p^{n-l+k} \| (a^{hp^{(n-l+k)-k}} - 1)$ by Lemma 4.2.7, i.e, $p^{n-(l-k)} \| (a^{hp^{n-l}} - 1)$. Hence, $l = k$ and $h_n = hp^{n-k}$. □

We can use Theorem 4.2.8 to construct a primitive root of p^n when p is an odd prime. Let g be a primitive root of p and suppose first, in the notation of Theorem 4.2.8, that $k = 1$, so that $p^2 \nmid (g^{p-1} - 1)$. Then for $n \geq 1$,

$$\operatorname{ord}_{p^n} g = (p-1)p^{n-1} = \phi(p^n),$$

so g is also a primitive root of p^n. On the other hand, if $k > 1$, consider the number $g_1 = g + p$, which is again a primitive root of p. Let $p^{k_1} \| (g_1^{p-1} - 1)$. We have

$$g_1^{p-1} - 1 = (g+p)^{p-1} - 1 \equiv g^{p-1} + (p-1)g^{p-2}p - 1 \pmod{p^2},$$

so $g_1^{p-1} - 1 \equiv (p-1)g^{p-2}p \pmod{p^2}$. Since $p^2 \nmid (p-1)g^{p-2}p$, we have $p^2 \nmid (g_1^{p-1} - 1)$, so $k_1 = 1$, and the preceding argument shows that g_1 is a primitive root of p^n for all $n \geq 1$.

Theorem 4.2.9. (1) *There exists a primitive root g_1 such that $g_1^{p-1} \not\equiv 1 \pmod{p^2}$.*

(2) *g_1 is a primitive root of p^n for all $n \geq 1$.*

Corollary 4.2.10. *Each positive power of an odd prime has a primitive root g_1. In group-theoretic language, if p is an odd prime, then $\mathbb{Z}_{p^n}^\times = \langle g_1 \rangle$ for all $n \geq 1$.*

Observe that if we take $a = 5$ and $k = 2$, then $\operatorname{ord}_2 5 = 1$, and Theorem 4.2.8 gives

$$\operatorname{ord}_{2^n} 5 = 2^{n-2} = \frac{\phi(2^n)}{2}, \quad \text{for all } n \geq 2.$$

Theorem 4.2.11. (1) *Both 2 and 2^2 have the primitive root -1.*

(2) *For $n \geq 3$, 2^n does not have primitive roots. On the other hand, the powers $5, 5^2, 5^3 \ldots, 5^{2^{n-2}}$ constitute half of a reduced residue system modulo 2^n, namely all the integers $\equiv 1 \pmod 4$. The missing residue classes are represented by $-5, -5^2, -5^3, \ldots, -5^{n-2}$.*

(3) *In group-theoretic language, $\mathbb{Z}_2^\times = \langle -1 \rangle$, $\mathbb{Z}_{2^2}^\times = \langle -1 \rangle$ and $\mathbb{Z}_{2^n}^\times = \langle -1 \rangle \times \langle 5 \rangle$ for all $n \geq 3$.*

Proof. Let $n \geq 3$. Let a be an odd integer. Since $a^2 \equiv 1 \pmod 8$, we have

$$(a^2)^{2^{n-3}} = a^{2^{n-2}} \equiv 1 \pmod{2^n}.$$

Then $(\operatorname{ord}_{2^n} a) \mid 2^{n-2}$, $\operatorname{ord}_{2^n} a < 2^{n-1} = \phi(2^n)$. Hence, 2^n has no primitive root.

Recall that $\operatorname{ord}_{2^n} 5 = 2^{n-2}$ and all powers of 5 are $\equiv 1 \pmod 4$, together with the fact that there are exactly 2^{n-2} positive integers less than 2^n and $\equiv 1 \pmod 4$. This proves the powers $5, 5^2, 5^3 \ldots, 5^{2^{n-2}}$ constitute half of a reduced residue system modulo 2^n. Similarly, the numbers $-5, -5^2, -5^3, \ldots, -5^{n-2}$ are distinct modulo 2^n, and they are all $\equiv -1 \pmod 4$, so they must be congruent in some order to $3, 7, 11, \ldots, 2^n - 1$. □

Theorem 4.2.12. *Let g be a primitive root of p^n, where p is an odd prime.*

(1) *If g is odd, then g is a primitive root of $2p^n$.*

(2) *If g is even, then $g + p^n$ is a primitive root of $2p^n$.*

Proof. Since $g \equiv g + p^n \pmod{p^n}$, $g + p^n$ is a primitive root of p^n. Observe that one of g and $g + p^n$ is odd, say g_2. Since g_2 is a primitive root of p^n, if $d \mid \phi(p^n)$, then $g_2^d \equiv 1 \pmod{p^n} \Leftrightarrow d = \phi(p^n)$. But $\phi(2p^n) = \phi(p^n)$, and since g_2 is odd, $2 \mid (g_2^d - 1)$ for all d, so if $d \mid \phi(p^n)$, then $g_2^d \equiv 1 \pmod{2p^n} \Leftrightarrow d = \phi(2p^n)$. Thus g_2 is a primitive root of $2p^n$. □

Remark. In group-theoretic language, if p is an odd prime, then $\mathbb{Z}_{2p^n}^\times = \langle g_2 \rangle$ for all $n \geq 1$.

Theorem 4.2.13. *The numbers having primitive roots are $2, 4, p^n$ and $2p^n$, where $n \in \mathbb{N}$ and p runs over the odd primes.*

Proof. What is left is to show that m does not have a primitive root if at least two of the prime-power factors in $m = \prod p_i^{e_i}$ are such that $\phi(p_i^{e_i}) > 1$. Put $M = \operatorname{lcm}(\phi(p_1^{e^1}), \phi(p_2^{e^2}), \ldots)$. Since

$$a^{\phi(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}, \quad i = 1, 2, \ldots,$$

we have

$$a^M \equiv 1 \pmod{p_i^{e_i}}, \quad i = 1, 2, \ldots$$

and hence

$$a^M \equiv 1 \pmod{m}.$$

But if $\phi(r) > 1$, then $\phi(r)$ is even, so the lcm in the exponent is strictly smaller than the product of the entries, and the product is $\phi(m)$ as ϕ is multiplicative. □

By the Chinese remainder theorem, we can prove

Theorem 4.2.14. *If $m = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, where the p_i are arbitrary distinct primes and the e_i are positive, then the group*

$$\mathbb{Z}_m^\times \cong \mathbb{Z}_{p_1^{e_1}}^\times \times \mathbb{Z}_{p_2^{e_2}}^\times \times \cdots \times \mathbb{Z}_{p_r^{e_r}}^\times.$$

We can go a step further, using what we know about the individual factors $\mathbb{Z}_{p^e}^\times$. But now 2 is exceptional so we change notation slightly. We continue to use $\langle a \rangle$ for the cyclic group generated by a.

Theorem 4.2.15. *Suppose $m \geq 2$ has the prime-power decomposition $m = 2^e p_1^{e_1} \ldots p_r^{e_r}$, where $e \geq 0$, $r \geq 0$, and if $r \geq 0$, then $p_1, \ldots, p_r$ are distinct odd primes and $e_1, \ldots, e_r$ are positive. Let $g_1, \ldots, g_r$ be primitive roots of $p_1^{e_1}, \ldots, p_r^{e_r}$, respectively, if $r > 0$. Then*

$$\mathbb{Z}_m^\times \cong \langle [-1]_{2^2} \rangle \times \langle [5]_{2^3} \rangle \times \langle [g_1]_{p_1^{e_1}} \rangle \times \cdots \times \langle [g_r]_{p_r^{e_r}} \rangle,$$

where the first two factors are to be omitted if $e = 0$ or 1 and the second factor is to be omitted if $e = 2$.

Corollary 4.2.16. *$\mathbb{Z}_m^\times$ is cyclic $\Leftrightarrow m = 2, 4, p^n$ and $2p^n$, where p is an odd prime and $n \in \mathbb{N}$.*

Exercise 4.2.

1. Find a primitive root of 11, 11^n for all $n \geq 1$.
2. How many primitive roots does 22 have? Find them all.
3. Find a primitive root of $2 \cdot 5^n$ for all $n \geq 1$.
4. The prime $p = 71$ has 7 as a primitive root. Find *all* primitive roots of 71 and also find *a* primitive root of p^2 and of $2p^2$.

5. If $p > 3$ is a prime, prove that the product of all incongruent primitive roots of p is congruent to 1 modulo p.

6. Let m be a number having primitive roots and let g be a primitive root of m. Prove that
(i) $g^{\phi(m)/2} \equiv -1 \pmod{m}$,
(ii) the inverse of g modulo m is also a primitive root of m, and
(iii) $x^2 \equiv 1 \pmod{m}$ if and only if $x \equiv 1$ or $-1 \pmod{m}$.

7. If p is a prime, show that the product of the $\phi(p-1)$ primitive roots of p is congruent to $(-1)^{\phi(p-1)}$ modulo p.

8. Let p be an odd prime. Prove that

$$1^n + 2^n + \cdots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} & \text{if } (p-1) \nmid n, \\ -1 \pmod{p} & \text{if } (p-1) \mid n. \end{cases}$$

4.3 nth power residues

Let m be a number having primitive roots and let g be one of them. Then the numbers $g, g^2, \ldots, g^{\phi(m)}$ form a reduced residue system of m. The relation between a number a and the exponent of a power of g which is congruent to a modulo m is very similar to the relation between an ordinary positive real number x and its logarithm.

Definition. Let m be a number having primitive roots and let g be one of them. Let $a \in \mathbb{Z}$ be such that $\gcd(a, m) = 1$. Then $\exists!\, t \in \{1, 2, \ldots, \phi(m)\}, a \equiv g^t \pmod{m}$. This exponent is called an **index of a to the base g**, and written $\operatorname{ind}_g a$. That is,

$$\operatorname{ind}_g a \equiv t \pmod{\phi(m)} \quad \Leftrightarrow \quad a \equiv g^t \pmod{m}.$$

Theorem 4.3.1. *Let g be a primitive root of m and let a and b be relatively prime to m.*

(1) *If $a \equiv b \pmod{m}$, then $\operatorname{ind}_g a \equiv \operatorname{ind}_g b \pmod{\phi(m)}$,*

(2) $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\phi(m)}$,

(3) $\operatorname{ind}_g a^n \equiv n \operatorname{ind}_g a \pmod{\phi(m)}$,

(4) $\operatorname{ind}_g 1 \equiv 0 \pmod{\phi(m)}$ *and* $\operatorname{ind}_g g \equiv 1 \pmod{\phi(m)}$.

Example 4.3.1. (1) If $m = 17$ and $g = 3$, we have the table

a :	3	9	10	13	5	15	11	16
$\operatorname{ind}_g a$:	1	2	3	4	5	6	7	8

a :	14	8	7	4	12	2	6	1
$\operatorname{ind}_g a$:	9	10	11	12	13	14	15	16

(2) If $m = 18$ and $g = 5$, we have

a :	5	7	17	13	11	1
$\operatorname{ind}_g a$:	1	2	3	4	5	6

Remark. Let g be a primitive root of m and $\gcd(a, m) = 1$. Recall that $\operatorname{ord}_m(g^k) = \dfrac{\phi(m)}{\gcd(k, \phi(m))}$. Then a is a primitive root of m if and only if $\gcd(\operatorname{ind}_g a, \phi(m)) = 1$.

Example 4.3.2. Solve (1) $4x^6 \equiv 9 \pmod{17}$ (2) $x^9 \equiv 7 \pmod{18}$.

Definition. Let $m \geq 2$, $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$ be such that $\gcd(a, m) = 1$. We say that a is an n**th power residue** [resp. **non-residue**] **of** m if the congruence $x^n \equiv a \pmod{m}$ is [resp. is not] solvable. If $n = 2$, we call a a **quadratic residue** [resp. **non-residue**] **of** m.

Remark. Clearly, 1 is an nth power residue for all $n \in \mathbb{N}$.

Theorem 4.3.2. *If a and b are both nth power residue of m, then the congruences $x^n \equiv a \pmod{m}$ and $x^n \equiv b \pmod{m}$ have the same number of solutions.*

Proof. Let a be an nth power residue. We shall show that $x^n \equiv a \pmod{m}$ has the same number of solutions as $x^n \equiv 1 \pmod{m}$. Let $x_1, x_2, \ldots, x_k$ be all incongruent such that $x_i^n \equiv a \pmod{m}$ for all i. Then $x_k^{-1}x_i$ are incongruent and $(x_k^{-1}x_i)^n = a^{-1}a \equiv 1 \pmod{m}$ for all i. By symmetry, we can show that the solutions of $x^n \equiv 1 \pmod{m}$ will yield as many as solutions to $x^n \equiv a \pmod{m}$. Hence the numbers of solutions of both congruences are the same. □

Remark. The set of all nth power residues of m forms a subgroup of $\mathbb{Z}_m^\times$.

Theorem 4.3.3. *Suppose m is a number having primitive roots and let g be a primitive root of m. Let $a \in \mathbb{Z}$ be such that $\gcd(a, m) = 1$ and $n \in \mathbb{N}$. Then*

(1) *a is an n-th power residue of m if and only if*

$$a^{\phi(m)/d} \equiv 1 \pmod{m}, \quad \text{where } d = \gcd(n, \phi(m)). \tag{4.3.1}$$

(2) *The number of nth power residues of m is $\phi(m)/d$, and each of them is the nth power of exactly d incongruent integers modulo m.*

Proof. (1) It follows from

$$\begin{aligned} x^n \equiv a \pmod{m} \text{ has a solution} &\Leftrightarrow n \operatorname{ind}_g x \equiv \operatorname{ind}_g a \pmod{\phi(m)} \text{ has a solution} \\ &\Leftrightarrow d \mid (\operatorname{ind}_g a), \text{ where } d = \gcd(n, \phi(m)) \\ &\Leftrightarrow \operatorname{ind}_g a \equiv 0 \pmod{d}, \text{ where } d = \gcd(n, \phi(m)) \\ &\Leftrightarrow \tfrac{\phi(m)}{d} \operatorname{ind}_g a \equiv 0 \pmod{\phi(m)} \\ &\Leftrightarrow \operatorname{ind}_g a^{\phi(m)/d} \equiv 0 \pmod{\phi(m)} \\ &\Leftrightarrow a^{\phi(m)/d} \equiv 1 \pmod{m}. \end{aligned}$$

(2) The second assertion follows from the second line above and Theorem 2.2.1. Finally, the $\phi(m)/d$ numbers $g^d, g^{2d}, \ldots, g^{(\phi(m)/d)d}$ are distinct modulo m and satisfy (4.3.1). □

Corollary 4.3.4. [Euler's criterion] *If p is a prime and $\gcd(a, p) = 1$. Then a is an n-th power residue of p if and only if $a^{(p-1)/d} \equiv 1 \pmod{p}$, where $d = \gcd(n, p-1)$. In particular, if p is an odd prime, then a is a quadratic residue of $p \Leftrightarrow a^{(p-1)/2} \equiv 1 \pmod{p}$.*

Exercise 4.3. 1. Is 5 a cubic residue of 18? What are all cubic residues of 18?

2. (i) Calculate a table for indices of 50 and solve $3x^4 \equiv 7 \pmod{50}$
   (ii) Is 43 is the fifth power residue of 50? If so, find all fifth power residues of 50.

3. If g and g' are both primitive roots of the odd prime p, show that for $\gcd(a, p) = 1$,

$$\operatorname{ind}_{g'} a \equiv (\operatorname{ind}_g a)(\operatorname{ind}_{g'} g) \pmod{p-1}.$$

4. If p is an odd prime, prove that $x^4 \equiv -1 \pmod{p} \Leftrightarrow p \equiv 1 \pmod{8}$.

5. Given that 2 is a primitive root of 29. Find the solutions of
(i) $x^7 \equiv 1 \pmod{29}$, (ii) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{29}$.

4.4 Hensel's Lemma

Theorem 4.4.1. *Let f be a polynomial with integer coefficients, let $m_1, m_2, \ldots, m_r$ be pairwise relatively prime positive integers, and let $m = m_1 m_2 \ldots m_r$. Then the congruence*

$$f(x) \equiv 0 \pmod{m} \tag{4.4.1}$$

has a solution if and only if each of the congruences

$$f(x) \equiv 0 \pmod{m_i} \tag{4.4.2}$$

has a solution for all $i = 1, 2, \ldots, r$. Moreover, if $\nu(m)$ and $\nu(m_i)$ denote the number of solutions of (4.4.1) *and* (4.4.2)*, respectively, then*

$$\nu(m) = \nu(m_1)\nu(m_2)\ldots\nu(m_r).$$

Proof. Clearly, if $f(x) \equiv 0 \pmod{m}$, then $f(a) \equiv 0 \pmod{m_i}$ for all $i \in \{1, \ldots, r\}$. Thus, (4.4.1) implies (4.4.2).

Conversely, let a_i be a solution of (4.4.2) for each $i \in \{1, \ldots, r\}$. Then by Chinese remainder theorem, $\exists a \in \mathbb{Z}$, $a_i \equiv a \pmod{m_i}$ for all i, so

$$0 \equiv f(a_i) \equiv f(a) \pmod{m_i}$$

for all i. Since $m_1, \ldots, m_r$ are positive relatively prime,

$$f(a) \equiv 0 \pmod{m_1 \ldots m_r = m}.$$

Hence, (4.4.2) implies (4.4.1).

Finally, by Chinese remainder theorem, each r-tuple of solution $(a_1, \ldots, a_r)$ of (4.4.2) gives rises to a unique integer a modulo m satisfying (4.4.1). As each a_i runs through the $\nu(m_i)$ solutions of (4.4.2), the number of integers a modulo m which satisfy (4.4.1) is $\nu(m_1)\ldots\nu(m_r)$. □

Remark. If $m > 1$ has the prime-power factorization $m = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, we can take $m_i = p_i^{k_i}$ for all $i = 1, 2, \ldots, r$ in the previous theorem and we see that the problem of solving a polynomial congruence for a composite modulus is reduced to that for prime-power moduli.

Lemma 4.4.2. *Let $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$ be a polynomial with integer coefficients. Then every coefficient of $f^{(k)}(x)$ is divisible by $k!$ for all $k \in \mathbb{N}$.*

Proof. Recall that $\binom{m}{k} = \frac{m(m-1)\dots(m-(k-1))}{k!} \in \mathbb{Z}$ for all $0 \le k \le m$. This implies that $k!$ divides the product of k consecutive integers. Moreover, for $\ell \in \mathbb{N}$,

$$\frac{d}{dx^k}x^\ell = \begin{cases} \ell(\ell-1)\dots(\ell-(k-1))x^{\ell-k} & \text{if } \ell \ge k, \\ 0 & \text{if } \ell < k. \end{cases}$$

Hence, $k!$ divides every coefficient of $f^{(k)}(x)$. □

Lemma 4.4.3. [Hensel] *Assume that $k \ge 2$ and let r be a solution of the congruence*

$$f(x) \equiv 0 \pmod{p^{k-1}}$$

lying in the interval $0 \le r < p^{k-1}$.

(1) *Assume $p \nmid f'(r)$. Then r can be lifted in a unique way from p^{k-1} to p^k. That is, there is a unique a in the interval $0 \le a < p^k$ such that $a \equiv r \pmod{p^{k-1}}$ and a satisfies the congruence $f(x) \equiv 0 \pmod{p^k}$.*

(2) *Assume $p \mid f'(r)$. Then we have two possibilities:*

   (a) *If $p^k \mid f(r)$, r can be lifted from p^{k-1} to p^k in p distinct ways.*

   (b) *If $p^k \nmid f(r)$, r cannot be lifted from p^{k-1} to p^k.*

Proof. From Calculus, the Taylor's expansion of $f(x)$ is

$$f(x+h) = f(x) + f'(x)h + \frac{f''(x)}{2!}h^2 + \dots + \frac{f^{(n)}(x)}{n!}h^n$$

for all $x, h \in \mathbb{Z}$ and $\deg f(x) = n$. Take $x = r$ and $h = qp^{k-1}$, where $q \in \mathbb{Z}$, we have

$$f(r + qp^{k-1}) \equiv f(r) + f'(r)qp^{k-1} \pmod{p^k}. \tag{4.4.3}$$

Since $f(r) \equiv 0 \pmod{p^{k-1}}$, we have $f(r) = mp^{k-1}$ for some $m \in \mathbb{Z}$ and so (4.4.3) becomes

$$f(r + qp^{k-1}) \equiv mp^{k-1} + f'(r)qp^{k-1} = (m + f'(r)q)p^{k-1} \pmod{p^k}.$$

Suppose $p \nmid f'(r)$. We can choose a unique $q \in \{0, 1, \dots, p-1\}$ such that $m + f'(r)q \equiv 0 \pmod{p}$. Thus,

$$f(r + qp^{k-1}) \equiv 0 \pmod{p^k},$$

where $0 \le r + qp^{k-1} < p^k$. Let $a = r + qp^{k-1}$. Then a is unique and $a \equiv r \pmod{p^{k-1}}$.

Next, we suppose that $p \mid f'(r)$. Then

$$m + f'(r)x \equiv 0 \pmod{p} \text{ has a solution} \Leftrightarrow p \mid m \Leftrightarrow f(r) \equiv 0 \pmod{p^k}.$$

Moreover, $m + f'(r)x \equiv 0 \pmod{p}$ has p incongruent solutions modulo p if $p \mid m$. We now distinguish two cases.
(a) If $p^k \mid f(r)$, then for each $q \in \{0, 1, \dots, p-1\}$, $r_q = r + qp^{k-1}$ is a solution of $f(x) \equiv 0 \pmod{p^k}$. These gives p incongruent solutions.
(b) If $p^k \nmid f(r)$, then $m + f'(r)x \equiv 0 \pmod{p}$ has no solution, so r cannot be lifted from p^{k-1} to p^k. □

Corollary 4.4.4. *Let p be an odd prime and $n \in \mathbb{N}$. For $a \in \mathbb{Z}$ and $p \nmid a$, if $x^2 \equiv a \pmod{p}$ has a solution, so does $x^2 \equiv a \pmod{p^n}$.*

Proof. Consider $f(x) = x^2 - a$. Then $f'(x) = 2x$, so $p \nmid f'(r)$ for all $r \in \mathbb{Z}$ such that $p \nmid r$ and the statement follows from Hensel's lemma (1). □

Example 4.4.1. Determine the number of solutions of $x^7 + x + 1 \equiv 0 \pmod{343}$.

Example 4.4.2. Find all solutions of $x^4 + x + 1 \equiv 0 \pmod{27}$.

Example 4.4.3. Find all solutions of $x^3 + x^2 + 23 \equiv 0 \pmod{125}$.

Exercise 4.4.
1. Find all solutions of the following congruences
   (i) $x^3 - 3x^2 + 27 \equiv 0 \pmod{1125}$ (ii) $x^7 + x + 1 \equiv 0 \pmod{343}$
   (iii) $x^4 + 2x + 2 \equiv 0 \pmod{125}$.
2. Find all solutions of $x^3 + 2x^2 - 3 \equiv 0 \pmod{7^3}$
3. Prove that $3^n \nmid (a^2 + 1)$ for all $a \in \mathbb{Z}$ and $n \in \mathbb{N}$.

Chapter 5

Quadratic Residues

5.1 The Legendre Symbol

Definition. Let $m \geq 2$ and let $a \in \mathbb{Z}$ be such that $\gcd(a, m) = 1$. We call a a **quadratic residue** [resp. **non-residue**] **of** m if the congruence $x^2 \equiv a \pmod{m}$ is [resp. is not] solvable.

Theorem 5.1.1. *(1) 1 is the only quadratic residue of 2 and of 4.*

(2) a is a quadratic residue of 2^e for all $e \geq 3 \Leftrightarrow a \equiv 1 \pmod{8}$.

(3) If p is an odd prime and $n \in \mathbb{N}$, then
a is a quadratic residue of $p^n \Leftrightarrow a$ is a quadratic residue of p.

Proof. (1) It is obtained by basic calculation.
(2) Since a is a quadratic residue for all $e \geq 3$, $a \equiv t^2 \pmod{2^e}$ for some $t \in \mathbb{Z}$. Recall that for any odd integer t, $t^2 \equiv 1 \pmod{8}$. Hence, $a \equiv 1 \pmod{8}$.

Conversely, assume that $a \equiv 1 \pmod{8}$. Clearly, a is a quadratic residue modulo $2^3 = 8$. Let $e > 3$ and assume that a is a quadratic residue modulo 2^{e-1}. Then $a = t^2 + k2^{e-1}$ for some $k, t \in \mathbb{Z}$. Since a is odd, t is odd. Thus, there is a $k' \in \mathbb{Z}$ such that $tk' \equiv k \pmod{2}$. Note that

$$(t + k'2^{e-2})^2 = t^2 + 2tk'2^{e-2} + (k'2^{e-2})^2 = t^2 + tk'2^{e-1} + k'^2 2^{2e-4}.$$

Substitute $a = t^2 + k2^{e-1}$, we have

$$(t + k'2^{e-2})^2 = a - k2^{e-1} + tk'2^{e-1} + k'^2 2^{2e-4} = a - (tk' - k)2^{e-1} + k'^2 2^{2e-4},$$

so $a \equiv (t + k'2^{e-2})^2 \pmod{2^e}$ because $e > 3$.
(3) It follows from Corollary 4.4.4. □

Hence, to determine a quadratic residue of $m \geq 2$, by Theorem 4.4.1, it suffices to study a quadratic residue of an odd prime p.

Definition. For an *odd prime* p, we define the **Legendre symbol** $(\cdot/p)$ by

$$(a/p) = \begin{cases} 0, & \text{if } p \mid a; \\ 1, & \text{if } a \text{ is a quadratic residue of } p; \\ -1, & \text{if } a \text{ is a quadratic nonresidue of } p. \end{cases}$$

Using the symbol, the Euler's criterion can be rephrased more simply.

Theorem 5.1.2. *If p is an odd prime, then for arbitrary $a \in \mathbb{Z}$, $a^{(p-1)/2} \equiv (a/p) \pmod{p}$.*

Proof. Observe that $1 \equiv a^{p-1} = a^{(p-1)/2} \pmod{p}$, so $a^{(p-1)/2} \equiv 1$ or $-1 \pmod{p}$. The Euler's criterion gives $a^{(p-1)/2} \equiv 1 \Leftrightarrow (a/p) = 1$, which is equivalent to $a^{(p-1)/2} \equiv -1 \Leftrightarrow (a/p) = -1$. Hence $a^{(p-1)/2} \equiv (a/p) \pmod{p}$. □

Corollary 5.1.3. *For an odd prime p, $(-1/p) = (-1)^{(p-1)/2}$.*
Thus -1 is a quadratic residue of $p \Leftrightarrow p \equiv 1 \pmod{4}$.

The Legendre symbol $(\cdot/p)$ has the following properties.

Theorem 5.1.4. *Let p be an odd prime.*

(1) $(ab/p) = (a/p)(b/p)$. Thus, $(QR)(QR) = QR$, $(QR)(QNR) = QNR$ and $(QNR)(QNR) = QR$.

(2) If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$.

(3) $(a^2/p) = 1$ if $p \nmid a$.

Proof. Note that $(ab/p) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} \equiv (a/p)(b/p) \pmod{p}$. Since the values of $(\cdot/p)$ is 0 or ± 1 and p is odd, we have $(ab/p) = (a/p)(b/p)$. The later two statements follow from (1). □

Example 5.1.1. Determine whether the congruence $x^2 \equiv -46 \pmod{17}$ is solvable.

Theorem 5.1.5. *If p is an odd prime, then*

$$\sum_{a=1}^{p-1} (a/p) = 0.$$

Hence, there are precisely $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues of p.

Proof. Let g be a primitive root of p. Then $g, g^2, \dots, g^{p-1}$ forms a reduced residue modulo p. Recall that $g^{(p-1)/2)} \equiv -1 \pmod{p}$, so we have

$$(g^k/p) = (g/p)^k \equiv (g^{(p-1/2)})^k \equiv (-1)^k \pmod{p}$$

for all $k \in \{1, 2, \dots, p-1\}$. Since the values of $(\cdot/p)$ is 0 or ± 1 and p is odd, $(g^k/p) = (-1)^k$, and hence

$$\sum_{a=1}^{p-1} (a/p) = \sum_{k=1}^{p-1} (g^k/p) = \sum_{k=1}^{p-1} (-1)^k = 0$$

as desired. □

Theorem 5.1.6. *There are infinitely many primes of the form $4k + 1$, $k \in \mathbb{N}$.*

Proof. Suppose that there are finitely many such primes; let us call them $p_1, p_2, \dots, p_n$ and consider the integer

$$N = (2p_1p_2 \dots p_n)^2 + 1.$$

Clearly, N is odd, so that there exists some odd prime p with $p \mid N$. That is,

$$(2p_1p_2 \dots p_n)^2 \equiv -1 \pmod{p},$$

so $(-1/p) = 1$. Hence $p = 4k + 1$ for some $k \in \mathbb{N}$, so $p = p_i$ for some i. This implies that $p \mid 1$ which is a contradiction. □

From Theorem 5.1.4, in investigating the Legendre symbol $(\cdot/p)$, there will be be no loss in generality in assuming that a is a positive prime. In general, (a/p) can be written as the product of Legendre symbols, in which the first entries are the distinct prime divisors of a which divide a to an odd power.

Example 5.1.2. Show that $(-48/31) = -(3/31) = (2/31)(7/31)$.

Theorem 5.1.7. [Gauss' lemma] *If μ is the number of elements of the set*

$$\{a, 2a, \dots, \tfrac{1}{2}(p-1)a\}$$

whose numerically smallest remainders modulo p, lied in the interval $(-p/2, p/2)$, are negative, then we have

$$(a/p) = (-1)^{\mu}.$$

Example 5.1.3. If $a = 3, p = 31$, the numerically smallest remainders modulo 31 of $3{\cdot}1, 3{\cdot}2, \dots, 3{\cdot}15$ are $3, 6, 9, 12, 15, -13, -10, -7, -4, -1, 2, 5, 8, 11, 14$; thus we have $\mu = 5, (3/31) = -1$, and hence $(-48/31) = 1$.

Proof of Gauss' lemma. Replace the number of the set $\{a, 2a, \dots, \frac{1}{2}(p-1)a\}$ by their numerically smallest remainder modulo p lied in the interval $(-p/2, p/2)$; denote the positive ones by $r_1, r_2, \dots$ and the negative ones by $-r'_1, -r'_2, \dots$. Clearly, no two r_i's are equal, and no two r'_j's are equal. Note that $r_i \not\equiv r'_j \pmod p$ for all i, j. Hence the $(p-1)/2$ numbers r_i, r'_j are distinct integers between 1 and $(p-1)/2$ inclusive, and are therefore exactly the numbers $1, 2, \dots, (p-1)/2$ in some order. Thus

$$a \cdot 2a \cdot \dots \cdot \tfrac{p-1}{2}a \equiv (-1)^{\mu} \tfrac{p-1}{2}! \pmod p$$
$$(a/p) = a^{(p-1)/2} \equiv (-1)^{\mu} \pmod p.$$

Since p is odd and (a/p) assumes only the values ± 1, $(a/p) = (-1)^{\mu}$ as desired. □

If $a = 2$, then μ is the number of elements of the set $\{2m : 1 \le m \le \frac{p-1}{2}\} = \{2, 4, \dots, p-1\}$ which are greater than $p/2$; clearly; this is true $\Leftrightarrow m > p/4$. Thus

$$\mu = \frac{p-1}{2} - \left[\frac{p}{4}\right].$$

If now,

$$\begin{aligned}
&p = 8k+1, \text{ then } \mu = 4k - [2k + \tfrac{1}{4}] = 4k - 2k = 2k \text{ is even,}\\
&p = 8k+3, \text{ then } \mu = 4k + 1 - [2k + \tfrac{3}{4}] = 4k + 1 - 2k = 2k+1 \text{ is odd,}\\
&p = 8k-3, \text{ then } \mu = 4k - 2 - [2k - 1 + \tfrac{1}{4}] = 2k - 1 \text{ is odd, and}\\
&p = 8k-1, \text{ then } \mu = 4k - 1 - [2k - 1 + \tfrac{3}{4}] = 2k \text{ is even.}
\end{aligned}$$

Observe that the quality $(p^2-1)/8$ satisfies exactly the same parities as μ above. This result can be concluded in the following form.

Theorem 5.1.8. *For an odd prime p, 2 is a quadratic residue of $p \Leftrightarrow p \equiv \pm 1 \pmod 8$.*
Briefly, $(2/p) = (-1)^{(p^2-1)/8}$.

Theorem 5.1.9. *(1) 2 is a primitive root of the prime $q = 4p + 1$ if p is an odd prime.*

(2) 2 is a primitive root of $q = 2p + 1$ if p is a prime of the form $4k + 1$.

(3) -2 is a primitive root of $q = 2p + 1$ if p is a prime of the form $4k - 1$.

Proof. (1) If $\operatorname{ord}_q 2 = t$, then $t \mid (q-1)$, that is $t \mid 4p$. Aside from 4, every proper divisor of $4p$ is also a divisor of $2p$, and if $2^4 \equiv 1 \pmod q$, then $q = 5$ and $p = 1$ is not a prime. Hence it suffices to show that $2^{2p} \not\equiv 1 \pmod q$. But $2^{2p} = 2^{(q-1)/2} \equiv (2/q) \pmod q$ and $(2/q) = -1$ since $q \equiv 5 \pmod 8$. The other statements are exercises. □

Theorem 5.1.10. *There are infinitely many primes of the form $8k - 1$.*

Proof. As usual, suppose that there are finitely many such primes; let us call them $p_1, p_2, \dots, p_n$ and consider the integer

$$N = (4p_1p_2\dots p_n)^2 - 2.$$

Then there exists an odd prime divisor of N, so that

$$(4p_1p_2\dots p_n)^2 \equiv 2 \pmod p$$

or $(2/p) = 1$. In view of Theorem 5.1.8, $p \equiv \pm 1 \pmod 8$. If all the odd prime divisors of N were of the form $8k + 1$, then N would be of the form $16a + 2$ which is impossible, since N is of the form $16a - 2$. Thus N must have a prime divisor q of the form $8k - 1$. But $q \mid N$ and $q \mid (4p_1p_2\dots p_n)^2$ leads to the contradiction that $q \mid 2$. □

Exercise 5.1.

1. Suppose $p \nmid a$. Show that if $p \equiv 1 \pmod 4$, then both or neither of a and $-a$ are quadratic residues of p, while if $p \equiv -1 \pmod 4$, exactly one is a quadratic residue.
2. Complete the proof of Theorem 5.1.9.
3. If $p \nmid a$, prove that the number of solutions to $ax^2 + bx + c \equiv 0 \pmod p$ is $1 + ((b^2 - 4ac)/p)$.
4. Show that if $p = 2q + 1$ and q are both odd primes, then -4 is a primitive root of p.
5. Let p be an odd prime. Find the sum $\displaystyle\sum_{1\le a<b<p}\left(\left(\frac{a}{p}\right)+\left(\frac{b}{p}\right)\right)^2$.

5.2 Quadratic Reciprocity

Remark. For $m, n \in \mathbb{Z}$, $(-1)^m = (-1)^n \Leftrightarrow m \equiv n \pmod 2$.

Lemma 5.2.1. *Let p be an odd prime. If $p \nmid a$, then*

$$(a/p) = (-1)^{\nu}, \quad \textit{where} \quad \nu = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right].$$

Proof. We start from Gauss' lemma, μ is the number of x with $0 < x < p/2$ and $p/2 < ax - p[ax/p] < p$, i.e.,

$$1 \le \frac{2ax}{p} - 2\left[\frac{ax}{p}\right] < 2.$$

Hence

$$\mu = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p} - 2\left[\frac{ax}{p}\right]\right] = \sum_{x=1}^{\frac{p-1}{2}} \left(\left[\frac{2ax}{p}\right] - 2\left[\frac{ax}{p}\right]\right) \equiv \nu \pmod 2$$

as desired. □

Lemma 5.2.2. *If p and q are distinct odd primes, then*

$$(p/q)(q/p) = (-1)^{\lambda}, \quad \textit{where} \quad \lambda = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right] + \sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right].$$

Proof. From Lemma 5.2.1, for an odd number a we have

$$\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\kappa},$$

where

$$\kappa = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{(a+p)x}{p}\right] + \frac{p^2-1}{8} = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right] + \sum_{x=1}^{\frac{p-1}{2}} x + \frac{p^2-1}{8} = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right] + \frac{p^2-1}{4}.$$

Now, take $a = q$ and also switch p and q, we have finally proved the lemma. □

Theorem 5.2.3. [Quadratic reciprocity law] *If p and q are distinct positive odd primes, then*

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

That is,

$$(p/q) = \begin{cases} (q/p), & \textit{if } p \equiv 1 \pmod 4 \ \textit{ or } \ q \equiv 1 \pmod 4; \\ -(q/p), & \textit{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Proof. Consider the lattice points (i.e., integer coordinates) inside the rectangle

$$R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : 0 < x < p/2 \text{ and } 0 < y < q/2\}$$

Then $|R| = \frac{p-1}{2}\frac{q-1}{2}$. Note that $R = R_1 \cup R_2$, where

$$R_1 = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : 0 < x < p/2 \text{ and } 0 < y < qx/p\}$$

and

$$\begin{aligned} R_2 &= \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : 0 < x < p/2 \text{ and } qx/p < y < q/2\} \\ &= \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : 0 < x < py/q \text{ and } 0 < y < q/2\}. \end{aligned}$$

Moreover, $R_1 \cap R_2 = \emptyset$. Thus

$$\frac{p-1}{2}\frac{q-1}{2} = |R| = |R_1| + |R_2| = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right] + \sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right].$$

Hence Lemma 5.2.2 establishes the theorem. □

Example 5.2.1. Compute (2011/2551).

Solution. Since $2011 \equiv 3 \equiv 2551 \pmod 4$,

$$(2011/2551) = -(2551/2011) = -(540/2011) = -((4 \cdot 9 \cdot 3 \cdot 5)/2011) = -(3/2011)(5/2011).$$

Next, since $5 \equiv 1 \pmod 4$, $(5/2011) = (2011/5) = (1/5) = 1$. Also, $(3/2011) = -(2011/3) = -(1/3) = -1$. Hence, $(2011/2551) = -(-1)(1) = 1$. □

Moreover, the quadratic reciprocity law can be used to determine the primes p of which a given prime q is a quadratic residue. This result, which is contained in the next theorem, has sometimes been taken as the quadratic reciprocity law, rather than Theorem 5.2.3. (Each can be deduced from the other.)

Theorem 5.2.4. *Let q be a fixed positive odd prime, and let p range over the odd positive primes $\neq q$. Every such p has a unique representation in exactly one of the two forms*

$$p = 4qk \pm a, \quad \text{with } k \in \mathbb{Z}, \quad 0 < a < 4q, \quad \text{and } a \equiv 1 \pmod 4. \tag{5.2.1}$$

When (5.2.1) *holds,*

$$(q/p) = (a/q). \tag{5.2.2}$$

Thus the p for which $(q/p) = 1$ are exactly those $p \equiv \pm a \pmod{4q}$, for all a such that

$$0 < a < 4q, \quad a \equiv 1 \pmod 4, \quad \text{and}(a/q) = 1. \tag{5.2.3}$$

The a's satisfying (5.2.3) *are given by the smallest positive remainders modulo $4q$ of the odd squares*

$$1^2, 3^2, \dots, (q-2)^2.$$

Example 5.2.2. (1) Take $q = 3$. Then the only integer satisfying the condition (5.2.3) is 1, so the 3 is a quadratic residue of primes $12k \pm 1$. Every other odd number is one of the forms $12k \pm 3$ or $12k \pm 5$, and no prime except 3 occurs in the progressions $12k \pm 3$. Hence $(3/p)$ is completely determined by the equations

$$(3/p) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{12}; \\ -1, & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

(2) Take $q = 17$. We consider the squares

$$1^2, 3^2, 5^2, 7^2, 9^2, 11^2, 13^2, 15^2,$$

which reduce modulo $4 \cdot 17 = 68$ to

$$1, 9, 25, 49, 13, 53, 33, 21.$$

We have that 17 is a quadratic residue of primes of the forms

$$68k \pm 1, 9, 13, 21, 25, 33, 49, 53,$$

and a nonresidue of primes of the forms

$$68k \pm 5, 29, 37, 41, 45, 57, 61, 65;$$

17 itself is the only primes of the forms 68 ± 17.

(3) Determine all odd primes p such that $(6/p) = 1$.

Proof of Theorem 5.2.4. By the division algorithm, there are unique k' and a' such that

$$p = 4qk' + a', \quad 1 \leq a' < 4q,$$

and clearly a' is odd. If $a' \equiv 1 \pmod 4$, (5.2.1) holds with the plus sign and with $k = k'$, $a = a'$. If $a' \equiv -1 \pmod 4$, (5.2.1) holds with the minus sign and $k = k' + 1$, $a = 4q - a'$. Any other value of k than k' and $k' + 1$ would yield $|a| > 4q$.

To verify (5.2.2), first suppose that the plus sign is correct in (5.2.1). Then $p \equiv 1 \pmod 4$, and $p \equiv a \pmod q$, so $(q/p) = (p/q) = (a/q)$. If the minus sign is correct, then $p \equiv -1 \pmod 4$ and $p \equiv -a \pmod q$, so either

$$q \equiv -1 \pmod 4, \quad \text{and then } (q/p) = -(p/q) = -(-a/q) = (a/q),$$

or

$$q \equiv 1 \pmod 4, \quad \text{and then } (q/p) = (p/q) = (-a/q) = (a/q).$$

Finally, if $(a/q) = 1$, there is a b such that

$$a \equiv b^2 \pmod q \quad \text{and} \quad 1 \leq b \leq q - 1,$$

whence also

$$a \equiv (q - b)^2 \pmod q \quad \text{and} \quad 1 \leq q - b \leq q - 1.$$

Since either b or $q - b$ is odd, say b', we have

$$a \equiv b'^2 \pmod q, \quad 1 \leq b' \leq q - 2, \quad b' \equiv 1 \pmod 2.$$

But then also

$$a \equiv 1 \equiv b'^2 \pmod 4,$$

so that

$$a \equiv b'^2 \pmod{4q},$$

as asserted. □

Example 5.2.3. Determine whether the congruence $x^2 \equiv 248 \pmod{1357}$ is solvable.

Definition. Let m be an odd positive integer and $a \in \mathbb{Z}$. Write $m = p_1^{k_1} \dots p_r^{k_r}$, where p_i are distinct odd primes. Define the **Jacobi symbol** by

$$(a/m)_J = (a/p_1)^{k_1} \dots (a/p_r)^{k_r}.$$

Theorem 5.2.5. *Let m be an odd positive integer and $a \in \mathbb{Z}$. If $x^2 \equiv a \pmod m$ is solvable, then $(a/m)_J = 1$.*

Proof. Let $m = p_1^{k_1} \dots p_r^{k_r}$. Since $x^2 \equiv a \pmod m$ is solvable, $x^2 \equiv a \pmod{p_i^{k_i}}$ is solvable for all i. By Theorem 5.1.1, $(a/p_i) = 1$ for all i. Hence $(a/m)_J = 1$. □

Remark. The converse of Theorem 5.2.5 is not true in general, e.g., $(2/9)_J = (2/3)^2 = 1$ but $x^2 \equiv 2 \pmod 9$ has no solution.

Exercise 5.2.

1. Evaluate the Legendre symbols $(503/773)$ and $(501/773)$.
2. Characterize the primes of which 5 is quadratic residue; those of which 10 is a quadratic residue; and those of which -5 is a quadratic residue.
3. Decide which of the following congruences are solvable:
   (i) $x^2 \equiv 2455 \pmod{4993}$, (ii) $x^2 \equiv 245 \pmod{27496}$,
   (iii) $x^2 \equiv 11 \pmod{35}$, (iv) $x^2 \equiv 19 \pmod{30}$,
   (v) $x^2 \equiv 12 \pmod{2989}$, (vi) $x^2 + 5x \equiv 12 \pmod{31}$.
4. Assume Theorem 5.2.4. Prove Theorem 5.2.3.
5. Show that for $p > 3$, the congruence $x^2 \equiv -3 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{6}$. Deduce that there are infinitely many primes of the form $6k + 1$.
6. Prove that 7 is a primitive root of any prime of the form $p = 2^{4n} + 1$. [*Hint*: Show that $(7/p) = (p/7) = -1$.]
7. Characterize the primes p of which the congruence $2x^2 + 1 \equiv 0 \pmod{p}$ is solvable.
8. Compute $(5/21)_J$ and $(39/539)_J$.

Bibliography

[1] G. E. Andrews, *Number Theory*, Dover Publications, Inc., New York, 1994.

[2] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, 1976.

[3] D. M. Burton, *Elementary Number Theory*, 7th edn, Mcgraw Hill Higher Education, Dubuque, 2010.

[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edn, Springer, New York, 1990.

[5] W. J. LeVeque, *Fundamentals of Number Theory*, Dover Publications, Inc., New York, 1996.

[6] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th edn, John Wiley & Sons, Inc., Hoboken, 1991.

[7] M. R. Schroeder, *Number Theory in Science and Communication with Applications in Cryptography, Physics, Digital Information, Computing, and Self-Similarity*, 4th edn, Springer, Berlin, 2006.

Index