$$a = qb + r$$

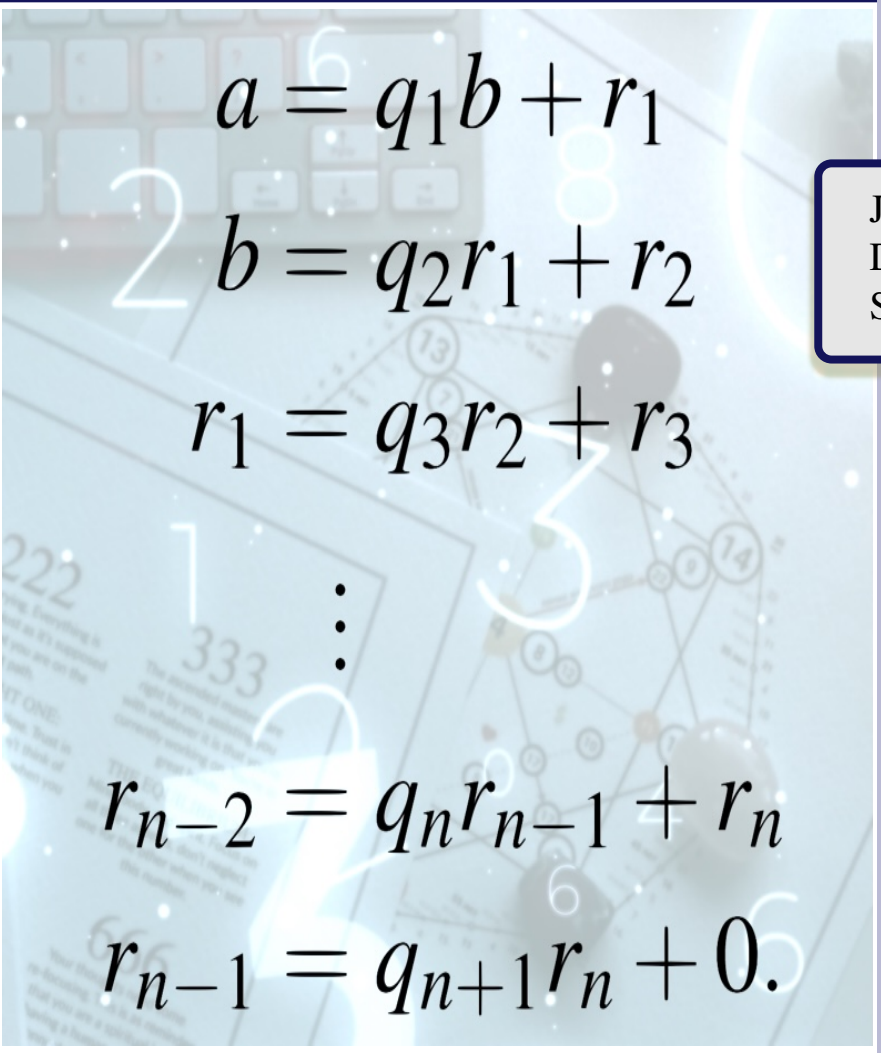
*Lecture notes on*

# NUMBER THEORY

PS01EMTH53

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

$$a^{p-1} \equiv 1 \pmod{p}$$





JAY MEHTA
Department of Mathematics,
Sardar Patel University.


$$\tau(n) \quad \sigma(n)$$

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

$$(p/q)(q/p)$$

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

SEMESTER - I
2025-26

# Contents

# Preface and Acknowledgments

This lecture note of the course "Number Theory" offered to the M.Sc. (Semester - I and Semester II) students at Department of Mathematics, Sardar Patel University, 2025-26 is aimed to provide a reading material to the students, in addition to the references mentioned in the university syllabus, so as to save time of the teacher and the students in writing on the board and copying in the notebooks, respectively. These notes are tailor-made for the "Number Theory" (PS01EMTH53/PS02EMTH53) syllabus of M.Sc. (Semester-I/II) of the University and do not cover all the topics of Number Theory.

This note is prepared from the recommended reference books, and it is not the original work of the author. We mostly followed the text book by "Elementary Number Theory" by David M. Burton.

This is the first version of the note on Number Theory. We have strictly followed the text in our syllabus and except a few examples, all the examples are taken from the book.

The language used is mostly of the book by Burton with some additional explanations provided wherever the requirement was felt. Students are encouraged to refer the book for reading in depth and for solving its exercises. This notes were prepared without having to taught the syllabus even once. So, there may be typos or corrections or some gaps which will probably be filled and improved in subsequent revisions any. Readers are welcome to point out errors, if any.

JAY MEHTA

**Date:** June 15, 2025

# Syllabus

## PS01EMTH53: Number Theory

**Unit I:** The division algorithm, the greatest common divisor, the Euclidean algorithm, the fundamental theorem of arithmetic, infinitude of prime numbers (Euclid's proof).

**Unit II:** Basic properties of congruence, linear congruences and the Chinese remainder theorem, Fermat's little theorem, Wilson's theorem.

**Unit III:** The sum and number of divisors, the Möbius inversion formula, the greatest integer function, Euler's phi-function, Euler's theorem, some properties of the phi-function.

**Unit IV:** Euler's criterion, Legendre's symbol: definition and its properties, evaluation of $(-1|p)$ and $(2|p)$, Gauss lemma, quadratic reciprocity.

## References


1. Burton David M., Elementary Number Theory, (Seventh Edition) McGraw Hill Education.
2. Hardy G. H. and Wright E. M., An Introduction to Theory of Numbers, (Sixth Edition) Oxford University Press.
3. Nivan Ivan, Zuckermann H. S. and Montgomery H. L., An Introduction to the Theory of Numbers, (Fifth Edition) John Wiley & Sons Inc.
4. Apostol Tom M., Introduction to Analytic Number Theory, Springer.

CHAPTER 1

# Divisibility and Primes

## 1.1 The Division Algorithm

**Theorem 1.1.1: Division Algorithm**

Given integers $a$ and $b$, with $b > 0$, there exists unique integers $q$ and $r$ satisfying

$$a = qb + r, \qquad 0 \leq r < b.$$

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

*Proof.* Consider the set

$$S = \{a - xb \mid x \text{ is an integer; } a - xb \geq 0\}.$$

We show that the set $S$ is nonempty. Since $b \geq 1$, we have $|a|b \geq |a|$. So,

$$a - (-|a|)b = a + |a|b \geq a + |a| \geq 0.$$

Thus, for $x = -|a|$, we have $a - xb \in S$ which implies that $S$ is nonempty subset (of $\mathbb{N} \cup \{0\}$). Hence, by well-ordering principle, $S$ contains a least element, say $r$. By the definition of $S$, we get that $r \geq 0$ and it is of the form

$$r = a - qb, \text{ for some integer } q.$$

Now, we show that $r < b$. If $r \geq b$, then

$$a - (q+1)b = (a - qb) - b = r - b \geq 0.$$

Thus, $a - (q+1)b \in S$ and $a - (q+1)b = r - b < r$ which is a contradiction as $r$ is the smallest element of $S$. Hence, $r < b$. This proves the existence of integers $q$ and $r$ such that $a = qb + r$ with $0 \leq r < b$. Now, we prove the uniqueness of $q$ and $r$.

Suppose $a$ has two representations of the form

$$a = q'b + r' = qb + r,$$

where $0 \leq r < b$ and $0 \leq r' \leq b$. We have to show that $q = q'$ and $r = r'$. Without the loss of generality, assume that $r \leq r'$. Then

$$(q - q')b = r' - r \geq 0,$$

where $0 \leq r' - r \leq r' < b$. The left hand side of the above equation is non-negative (since RHS is non-negative) and it is a multiple of $b$. This is a contradiction as right hand side is $< b$. Hence, $r = r'$ which implies $q = q'$. □

**Corollary 1.1.2**

If $a$ and $b$ are integers, with $b \neq 0$, then there exists unique integers $q$ and $r$ satisfying

$$a = qb + r, \qquad 0 \leq r < |b|.$$

*Proof.* It suffices to consider only the case when $b$ is negative. In this case $|b| > 0$ and by above theorem, there exists unique integers $q'$ and $r$ such that

$$a = q'|b| + r, \qquad 0 \leq r < |b|.$$

Since $b$ is negative, $|b| = -b$ and so taking $q = -q'$, we get

$$a = qb + r, \qquad 0 \leq r < |b|.$$

□

**Exercise 1.1**

Prove that if $a$ and $b$ are integers, with $b > 0$, then there exists unique integers $q$ and $r$ satisfying $a = qb + r$, where $2b \leq r < 3b$.

### 1.1.1 Applications of Division Algorithm

Taking $b = 2$, by division algorithm, the possible values of the remainder $r$ are 0 and 1. When $r = 1$, the integer $a$ is of the form $2q + 1$ which is *odd* and when $r = 0$, the integer $a$ is of the form $2q$, i.e. *even* integer. Thus, $a^2$ is either of the form $(2q)^2 = 4q^2 = 4k$ or $(2q+1)^2 = 4(q^2+q)+1 = 4k+1$. Hence, the remainder obtained by dividing square of any integer by 4 is either 0 or 1.

**Example 1.1.3.** We show that square of any odd integer is of the form $8k + 1$. By division algorithm, (taking $b = 4$) any integer can be represented in one of the following four forms:

$$4q, 4q+1, 4q+2, 4q+3.$$

Among the above four representations $4q + 1$ and $4q + 3$ are odd integers. Squaring them, we get

$$(4q+1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1 = 8k + 1$$

and

$$(4q+3)^2 = 16q^2+24q+9 = 8(2q^2+3q+1)+1 = 8k+1.$$

For example, the square of 7 is $7^2 = 49 = 8\times 6+1$, the square of 13 is $13^2 = 169 = 8\times 21+1$.

**Example 1.1.4.** For $a \geq 1$, we show that the expression $\frac{a(a^2+2)}{3}$ is an integer. By division algorithm, every integer $a$ is of the form $3q$, $3q+1$, or $3q+2$. We check the expression $\frac{a(a^2+2)}{3}$ in each of these three cases. For $a = 3q$, we get

$$\frac{a(a^2+2)}{3} = \frac{3q((3q)^2+2)}{3} = q(9q^2+2)$$

which is an integer. Similarly, for $a = 3q+1$, we get

$$\frac{a(a^2+2)}{3} = \frac{(3q+1)((3q+1)^2+2)}{3} = (3q+1)(3q^2+2q+1)$$

which is also an integer. Now, if $a = 3q+2$, then

$$\frac{a(a^2+2)}{3} = \frac{(3q+2)((3q+2)^2+2)}{3} = (3q+2)(3q^2+4q+2)$$

which is again an integer. Thus, $\frac{a(a^2+2)}{3}$ is always an integer for any integer $a$.

**Exercise 1.2**

For $n \geq 1$, prove that $\frac{n(n+1)(2n+1)}{6}$ is an integer.

**Exercise 1.3**

Using Division Algorithm show the following:

1. The square of any integer is either of the form $3k$ or $3k+1$.
2. The cube of any integer is of the form $9k$, $9k+1$, or $9k+8$.
3. The fourth power of any integer is either of the form $5k$ or $5k+1$.

**Exercise 1.4**

Prove that $3a^2-1$ is never a perfect square.

**Exercise 1.5**

Show that the cube of any integer is of the form $7k$ or $7k\pm 1$. Also verify that if an integer is simultaneously a square and a cube (as in the case with $64 = 8^2 = 4^3$), then it is either of the form $7k$ or $7k+1$.

**Exercise 1.6**

For $n \geq 1$, establish that the integer $n(7n^2+5)$ is of the form $6k$.

**Exercise 1.7**

If $n$ is an odd integer, then show that $n^4+4n^2+11$ is of the form $16k$.

## 1.2 The Greatest Common Divisor

Now, we consider a special case of division algorithm in which the remainder is zero.

**Definition 1.2.1**

An integer $b$ is said to be *divisible* by an integer $a \neq 0$, if there exists some integer $c$ such that $b = ac$. It is denoted by $a \mid b$ (read as "$a$ divides $b$"). We write $a \nmid b$ if $b$ is not divisible by $a$.

We also say that $a$ is a *divisor* of $b$, or $a$ is a *factor* of $b$, or $b$ is a *multiple* of $b$. Note that in the definition the divisor $a$ is assumed to be non-zero. Thus, whenever we say that $a \mid b$, it is assumed that $a$ is non-zero.

**Theorem 1.2.2**

For integers $a, b, c$, the following hold:

(a) $a \mid 0$, $1 \mid a$, $a \mid a$.
(b) $a \mid 1$ if and only if $a = \pm 1$.
(c) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
(d) If $a \mid b$ and $b \mid c$, then $a \mid c$.
(e) $a \mid b$ and $b \mid a$ if and only if $a = \pm b$.
(f) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.
(g) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for arbitrary integers $x$ and $y$.

*Proof.* (a) $0 = 0\,a \Rightarrow a \mid 0$.
$a = a\,1 \Rightarrow 1 \mid a$.
$a = 1\,a \Rightarrow a \mid a$.

(b) $a \mid 1 \Rightarrow 1 = b\,a$ for some integer $b$. This implies $a = b = \pm 1$.

(c) $a \mid b \Rightarrow b = k_1 a$ for some integer $k_1$ and $c \mid d \Rightarrow d = k_2 c$ for some integer $k_2$. Thus, $bd = k_1 k_2 ac \Rightarrow ac \mid bd$.

(d) $a \mid b \Rightarrow b = k_1 a$ for some integer $k_1$ and $b \mid c \Rightarrow c = k_2 b$ for some integer $k_2$. Now $c = k_2 b \Rightarrow c = k_2(k_1 a) = k_1 k_2 a$. Hence, $a \mid c$.

(e) $a \mid b \Rightarrow b = k_1 a$ for some integer $k_1$ and $b \mid a \Rightarrow a = k_2 b$ for some integer $k_2$. Now, $a = k_2 b = k_2(k_1 a) = k_1 k_2 a \Rightarrow k_1 k_2 = 1$. Thus, $k_1 = k_2 = \pm 1$. Substituting these values, we get $a = \pm b$.

(f) If $a \mid b$, then $b = k\,a$ for some integer $k$. Here, $b \neq 0 \Rightarrow k \neq 0$ and hence $|k| \geq 1$. Hence, $b = k\,a \Rightarrow |b| = |k||a| \geq |a|$ (since $|k| \geq 1$).

(g) $a \mid b \Rightarrow b = k_1 a$ for some integer $k_1$ and $a \mid c \Rightarrow c = k_2 a$ for some integer $k_2$. Then for any integers $x$ and $y$,

$$bx + cy = k_1, ax + k_2 ay = a(k_1 x + k_2 y).$$

Since, $k_1 x + k_2 y$ is an integer, it follows that $a \mid bx + cy$.

□

**Exercise 1.8**

If $a \mid b_k$ for $k = 1, 2, \ldots, n$, then

$$a \mid (b_1x_1 + b_2x_2 + \cdots + b_nx_n)$$

for all integers $x_1, x_2, \ldots, x_n$.

If $a$ and $b$ are arbitrary integers, then $d$ is a *common divisor* of $a$ and $b$ if both $d \mid a$ and $d \mid b$. Since 1 is a divisor of every integer, 1 is a common divisor of $a$ and $b$ and hence their set of positive common divisors is nonempty. Also, every integer divides zero, and hence if $a = b = 0$, then every integer is a common divisor of $a$ and $b$. Thus, in this case, the set of positive common divisors of $a$ and $b$ is $\mathbb{N}$ (i.e. infinite). If at least one of $a$ or $b$ is non-zero, then the set of positive divisors of $a$ and $b$ is finite and hence the there is a largest one among these common divisors, called the greatest common divisor of $a$ and $b$. It is defined as follows.

**Definition 1.2.3: Greatest Common Divisor**

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

(a) $d \mid a$ and $d \mid b$.
(b) If $c \mid a$ and $c \mid d$, then $c \leq d$.

**Remark 1.2.4.** Consider $a = 2$ and $b = 3$. Then there exists integers $x = 2$ and $y = -1$ such that $ax + by = 1$. That is, there is a linear combination of $a$ and $b$ which generates 1. Similarly, for $a = 24$ and $b = 35$, we get $x = -16$ and $y = 11$ such that

$$ax + by = (-16) \times 24 + 11 \times 35 = -384 + 385 = 1.$$

Now, consider $a = 12$ and $b = 15$. Try to find integers $x$ and $y$ such that $12x + 15y = 1$, i.e. find a linear combination of 12 and 15 that generates 1. Is it possible? No? Why does this happen?

We can ask a couple of questions here. First is given non-zero integers $a$ and $b$, does there exists integers $x$ and $y$ such that $ax + by = 1$. If yes, are they unique? Moreover, how to determine such a linear combination if it exists?

**Theorem 1.2.5: Bézout's identity**

Given integers $a$ and $b$, not both zero, there exists integers $x$ and $y$ such that

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

*Proof.* Let

$$S = \{au + bv \mid au + bv > 0,\ u, v \text{ integers}\}.$$

First we show that $S$ is nonempty. Since at least one of $a$ and $b$ is non-zero, without the loss of generality, assume that $a \neq 0$. If $a > 0$, then take $u = 1$ and $v = 0$ to get $au + bv = a \in S$. If $a < 0$, then take $u = -1$ and $v = 0$ to obtain $au + bv = -a > 0$. Hence, $S$ is nonempty. By Well-Ordering principle, $S$ has a least element, say $d$. Since $d \in S$, by the definition of $S$, there exists integers $x$ and $y$ such that $d = ax + by$.

Now, it remains to show that $d = \gcd(a,b)$. By Division Algorithm, there exists unique integers $q$ and $r$ such that $a = qd + r$, where $0 \leq r < d$. Then

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

If $0 < r < d$, then by the definition of $S$, it follows that $r \in S$. This is a contradiction as $d$ is the smallest element of $S$. Hence, $r = 0$ and so $a = qd$. This implies that $d \mid a$. Similarly, we can show that $d \mid b$. Thus, $d$ is a common divisor of $a$ and $b$. Now, we show that $d$ is the greatest common divisor.

Let $c$ be any positive common divisor of $a$ and $b$. Then $c \mid a$ and $c \mid b$. Hence, by Theorem 1.2.2 (g), $c \mid (ax+by)$, i.e. $c \mid d$. Again by Theorem 1.2.2 (f), $c = |c| \leq |d| = d$. Thus, $d = \gcd(a,b)$. □

**Corollary 1.2.6**

If $a$ and $b$ are given integers, not both zero, then the set

$$T = \{ax+by \mid x,y \text{ are integer}\}$$

is the set of all multipliers of $d = \gcd(a,b)$.

*Proof.* Since $d \mid a$ and $d \mid b$, we have $d \mid (ax+by)$ for all integers $x$ and $y$. Thus, every element of $T$ is a multiple of $d$.

Conversely, since $d = \gcd(a,b)$, by above theorem there exists integers $x_0$ and $y_0$ such that $d = ax_0 + by_0$. Then any multiple $nd$ of $d$ is of the form

$$nd = n(ax_0+by_0) = a(nx_0) + b(ny_0).$$

Thus, every multiple of $d$ is a linear combination of $a$ and $b$. Hence, by definition of $T$, every multiple of $d$ lies in $T$. □

**Definition 1.2.7**

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

**Theorem 1.2.8**

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

*Proof.* If $a$ and $b$ are relatively prime, i.e. $\gcd(a,b) = 1$, then by Theorem 1.2.5 there exists integers $x$ and $y$ such that $ax+by = 1$.

Conversely, suppose that there exists integers $x$ and $y$ such that $ax+by = 1$ and $\gcd(a,b) = 1$. We have to show that $d = 1$. Since $d = \gcd(a,b)$, $d \mid a$ and $d \mid b$. Hence, $d \mid (ax+by)$ and so $d \mid 1$. Hence, $d \leq 1$. Since $d$ is a positive integer, it follows that $d = 1$. □

Let $a$ and $b$ be two integers and $d = \gcd(a,b)$. Observe that since $d \mid a$ and $d \mid b$, $\frac{a}{d}$ and $\frac{b}{d}$ are integers. We have the following result.

**Corollary 1.2.9**

If $\gcd(a,b) = d$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

*Proof.* Since $d = \gcd(a,b)$, by Theorem 1.2.5, there exists integers $x$ and $y$ such that $ax+by = d$. Dividing by $d$, we get

$$\left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y = 1.$$

Since $\frac{a}{d}$ and $\frac{b}{d}$ are integers, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

For example, $\gcd(-15,20) = 5$ and $\gcd(-3,4) = 1$.

Note that, $6 \mid 24$ and $8 \mid 24$ but $6 \cdot 8 \nmid 24$. Thus, it is not true in general that if $a \mid c$ and $b \mid c$ then $ab \mid c$. It is true if $a$ and $b$ are relatively prime and we have the following corollary.

**Exercise 1.9**

Show that the converse of above corollary is also true. That is, if $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, then $\gcd(a,b) = 1$.

**Corollary 1.2.10**

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

*Proof.* Since $a \mid c$ and $b \mid c$, there exists integers $k_1$ and $k_2$ such that $c = k_1 a$ and $c = k_2 b$. Also since $\gcd(a,b) = 1$, there exists integers $x$ and $y$ such that $ax+by = 1$. Therefore,

$$c = c \cdot 1 = c(ax+by) = acx+bcy = a(k_2 b)x + b(k_1 a)y = ab(k_2 x + k_1 y).$$

Hence, $ab \mid c$. □

**Theorem 1.2.11: Euclid's lemma**

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

*Proof.* Since $\gcd(a,b) = 1$, there exists integers $x$ and $y$ such that $ax+by = 1$. Then

$$c = c \cdot 1 = c(ax+by) = acx+bcy.$$

Since, $a \mid ac$ and $a \mid bc$, we have $a \mid (acx+bcy)$, i.e. $a \mid c$. □

If $a$ and $b$ are not relatively prime, then Euclid's lemma does not hold. For example, $6 \mid 10 \cdot 15$ but $6 \nmid 10$ and $6 \nmid 15$.

The following result can be considered as the definition of $\gcd(a,b)$ even on set which do not have any order relation on it.

**Theorem 1.2.12**

Let $a$ and $b$ be integers, not both zero. A positive integer $d$ is $\gcd(a,b)$ if and only if

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

(b) If $c \mid a$ and $c \mid b$ for any integer $c$, then $c \mid d$

*Proof.* Suppose $d = \gcd(a,b)$. Then $d \mid a$ and $d \mid b$. This proves (a). By Theorem 1.2.5, there exists integers $x$ and $y$ such that $d = ax + by$. Thus, if $c$ is any integer such that $c \mid a$ and $c \mid b$, then $c \mid (ax + by)$. Thus, $c \mid d$. This proves part (b).

Conversely, let $d$ be a positive integer satisfying the above two conditions. If $c$ is any common divisor of $a$ and $b$, then by (b), $c \mid d$. Then by (f), $|c| \leq |d|$. Therefore, $c \leq |c| \leq |d|$ and since $d > 0$, we have $c \leq d$. Thus, by the definition of GCD, $d = \gcd(a,b)$. □

**Exercise 1.10**

Prove that if $d \mid n$, then $2^d - 1 \mid 2^n - 1$.

## 1.3 The Euclidean Algorithm

**Lemma 1.3.1**

If $a = qb + r$, then $\gcd(a,b) = \gcd(b,r)$.

*Proof.* Let $d = \gcd(a,b)$. Then $d \mid a$ and $d \mid b$ and hence $d \mid (a - qb)$, i.e. $d \mid r$. Thus, $d$ is a common divisor of $b$ and $r$.

Now, we show that $d$ is greatest common divisor or $b$ and $r$. Let $c$ be an arbitrary common divisor of $b$ and $r$, i.e. $c \mid b$ and $c \mid r$. Therefore, $c \mid (qb + r)$, i.e. $c \mid a$. Thus, $c$ is a common divisor of $a$ and $b$. Since $d = \gcd(a,b)$ and $c$ is arbitrary common divisor of $a$ and $b$, we have $c \leq d$. Hence, $d = \gcd(b,r)$. □

### 1.3.1 Euclidean Algorithm

The Euclidean Algorithm is an efficient process to obtain the gcd of two integers by a repeatedly applying division algorithm. Let $a$ and $b$ be two integers whose gcd is to be determined. We may assume that $a$ and $b$ are positive and $a > b$, since $\gcd(|a|,|b|) = \gcd(a,b)$. Apply division algorithm to $a$ and $b$ to get integers $q_1$ and $r_1$ such that

$$a = q_1 b + r_1, \qquad 0 \leq r_1 < b.$$

If $r_1 = 0$, then $b \mid a$ and hence $\gcd(a,b) = 1$. If $r_1 \neq 0$, then divide $b$ by $r_1$. By division algorithm, we get integers $q_2$ and $r_2$ such that

$$b = q_2 r_1 + r_2, \qquad 0 \leq r_2 < r_1.$$

Again, if $r_2 = 0$, we stop the process, else we divide $r_1$ by $r_2$ to get integers $q_3$ and $r_3$ such that

$$r_1 = q_3 r_2 + r_3, \qquad 0 \leq r_3 < r_2.$$

Since, the remainder is non-negative and decreasing at each stage, it eventually becomes zero at some stage. Thus, the process of applying division algorithm ends at the stage when remainder becomes zero. The non-zero remainder obtained at the last stage is the gcd of $a$ and $b$. Suppose this happens at $(n+1)$th stage. Then we have the following system of equations:

$$\begin{aligned} a &= q_1 b + r_1 && 0 < r_1 < b \\ b &= q_2 r_1 + r_2 && 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 && 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n && 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

By Lemma 1.3.1, we have

$$\gcd(a,b) = \gcd(b,r_1) = \cdots = \gcd(r_{n-1},r_n) = \gcd(r_n,0) = r_n.$$

**Remark 1.3.2.** By Theorem 1.2.5, there exists integers $x$ and $y$ such that $ax+by=d$. The question is how to determine these integers $x$ and $y$ and whether they are unique or not. The process with an example is given below.

From second last equation above, we have

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

Now, we solve the preceding equation for $r_{n-1}$ and substitute its values in the above equation to get

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

Thus, $r_n$ is represented as a linear combination of $r_{n-2}$ and $r_{n-3}$. Continuing this process backwards through the system of equations, we can express $r_n = \gcd(a,b)$ as a linear combination of $a$ and $b$. Let us see the Euclidean algorithm and this process by an example given below.

**Example 1.3.3.** First we find the gcd of 12378 and 3054 by Euclidean Algorithm. Let $a = 12378$ and $b = 3054$. Applying division algorithm repeatedly till we arrive at the stage when remainder is zero, we get

$$\begin{aligned} 12378 &= 4 \cdot 3054 + 162 \\ 3054 &= 18 \cdot 162 + 138 \\ 162 &= 1 \cdot 138 + 24 \\ 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0 \end{aligned}$$

Therefore,

$$\gcd(12378, 3054) = 6.$$

Now, we find integers $x$ and $y$ such that $12378x + 3054y = 6$. We start with the second last equation and successively eliminate the remainders 18, 24, 138 and 162 in each of the preceding steps.

$$\begin{aligned}
6 &= 24 - 18 \\
&= 24 - (138 - 5 \cdot 24) \\
&= 6 \cdot 24 - 138 \\
&= 6(162 - 138) - 138 \\
&= 6 \cdot 162 - 7 \cdot 138 \\
&= 6 \cdot 162 - 7(3054 - 18 \cdot 162) \\
&= 132 \cdot 162 - 7 \cdot 3054 \\
&= 132(12378 - 4 \cdot 3054) - 7 \cdot 3054 \\
&= 132 \cdot 12378 + (-535)3054
\end{aligned}$$

Thus,

$$\gcd(12378, 3054) = 6 = 12378x + 3054y,$$

where $x = 132$ and $y = -535$.

Note that this choice of $x$ and $y$ is not unique. We can add and subtract $3054 \cdot 12378$ to get

$$\begin{aligned}
6 &= (132 + 3054)12378 + (-535 - 12378)3054 \\
&= 3186 \cdot 12378 + (-12913)3054.
\end{aligned}$$

More generally, if $r_n = \gcd(a, b)$ and $r_n = ax + by$ for some integers $x$ and $y$, then we can also express it as

$$\begin{aligned}
r_n &= ax + by + ab - ab \\
&= a(x + b) + b(y - b) \\
&= ax' + by'
\end{aligned}$$

where $x' = x + b$ and $y' = y - b$. Hence, the representation of $\gcd(a, b)$ as a linear combination of $a$ and $b$ is not unique.

**Theorem 1.3.4**

If $k > 0$, then $\gcd(ka, kb) = k \gcd(a, b)$.

*Proof.* Note that, applying Euclidean Algorithm to $ka$ and $kb$ is same as multiplying by $k$ at each step (equations) in the Euclidean Algorithm for $a$ and $b$. To see this, consider

$$\begin{aligned}
ak &= q_1(bk) + r_1k && 0 < r_1k < bk \\
bk &= q_2(r_1k) + r_2k && 0 < r_2k < r_1k \\
&\vdots \\
r_{n-2}k &= q_n(r_{n-1}k) + r_nk && 0 < r_nk < r_{n-1}k \\
r_{n-1}k &= q_{n+1}(r_nk) + 0.
\end{aligned}$$

Hence,

$$\gcd(ka, kb) = kr_n = \gcd(a, b).$$

□

*Alternative argument.* By Theorem 1.2.5,

$$\begin{aligned}\gcd(ka,kb) &= \text{ the smallest positive integer of the form } (ak)x+(bk)y\\ &= k \text{ times the smallest positive integer of the form } ax+by\\ &= k\gcd(a,b)\end{aligned}$$

□

As an example, see that

$$\gcd(12,30) = 6\cdot\gcd(2,5) = 6\cdot 1 = 6.$$

**Theorem 1.3.5**

If $k>0$, then $\gcd(ka,kb) = k\gcd(a,b)$.

*Proof.* Multiplying each of the equation in the Euclidean Algorithm for $a$ and $b$ by $k$, we get

$$\begin{aligned} ak &= q_1(bk)+r_1k & 0<r_1k<bk\\ bk &= q_2(r_1k)+r_2k & 0<r_2k<r_1k\\ r_1k &= q_3(r_2k)+r_3 & 0<r_3k<r_2k\\ &\vdots\\ r_{n-2}k &= q_n(r_{n-1}k)+r_nk & 0<r_nk<r_{n-1}k\\ r_{n-1}k &= q_{n+1}(r_nk)+0.\end{aligned}$$

This is nothing but the Euclidean Algorithm applied to $ak$ and $bk$ and so their greatest common divisor is the last non-zero remainder, i.e., $r_nk$. Thus,

$$\gcd(ak,bk) = r_nk = k\gcd(a,b).$$

□

**Corollary 1.3.6**

For any integer $k\neq 0$, $\gcd(ka,kb) = |k|\gcd(a,b)$.

*Proof.* If $k>0$, then $|k|=k$ and the result follows from the above theorem. So it suffices to consider $k<0$. Then $-k=|k|>0$. Then by Theorem 1.3.5,

$$\begin{aligned}\gcd(ka,kb) &= \gcd(-ak,-bk)\\ &= \gcd(a|k|,b|k|)\\ &= |k|\gcd(a,b).\end{aligned}$$

□

As an example, see that $\gcd(12,30) = 6\cdot\gcd(2,5) = 6\cdot 1 = 6$.

## 1.4 Least Common Multiple

An integer $c$ is said to be a common multiple of $a$ and $b$ if $a \mid c$ and $b \mid c$. Clearly, zero is a common multiple of $a$ and $b$. Also, $ab$ and $-(ab)$ are non-trivial common multiples of $a$ and $b$. The set of positive common multiples of $a$ and $b$ is thus nonempty. Hence, by well-ordering principle, it has a least element, which we call the least common multiple of $a$ and $b$. More precisely, it is defined as follows:

**Definition 1.4.1: Least Common Multiple**

The *least common multiple* of $a$ and $b$ is denoted by $\operatorname{lcm}(a,b)$ and is defined as the positive integer $m$ satisfying the following properties:

(a) $a \mid m$ and $b \mid m$.
(b) If $c > 0$ such that $a \mid c$ and $b \mid c$, then $m \leq c$.

Let us observe the relationship between gcd and lcm of two integers by some examples.

**Example 1.4.2.** Let $a = 6$ and $b = 9$. Then $\gcd(6,9) = 3 = d$ and $\operatorname{lcm}(6,9) = 18 = l$. Observe that

$$6 = \underline{2} \times 3 \text{ and } 9 = \underline{3 \times 3} \text{ and } l = 2 \times (3 \times 3).$$

Also

$$6 = \underline{2 \times 3} \text{ and } 9 = \underline{3} \times 3 \text{ and } l = (2 \times 3) \times 3.$$

**Example 1.4.3.** Let $a = 30$ and $b = 40$. Then $\gcd(30,40) = 10 = d$ and $\operatorname{lcm}(30,40) = 120 = l$. Observe that

$$30 = \underline{3} \times 10 \text{ and } 40 = \underline{4 \times 10} \text{ and } l = 3 \times (4 \times 10).$$

Also

$$30 = \underline{3 \times 10} \text{ and } 40 = \underline{4} \times 10 \text{ and } l = (3 \times 10) \times 4.$$

From the above two examples we make the following observation: Let $\gcd(a,b) = d$. Then $d \mid a$ and $d \mid b$ and therefore $a = k_1 d$ and $b = k_2 d$ for some $k_1, k_2 \in \mathbb{Z}$. If $l = \operatorname{lcm}(a,b)$, then $l = k_1 k_2 d = k_1 b = k_2 a$. Hence, we have

$$\operatorname{lcm}(a,b)\gcd(a,b) = ld = (k_1 k_2 d)d = (k_1 d)(k_2 d) = ab.$$

We prove this result below.

The following result shows relationship between the gcd and lcm of two integers.

**Theorem 1.4.4**

For positive integers $a$ and $b$

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

*Proof.* Let $d = \gcd(a,b)$. Then $d \mid a$ and $d \mid b$. Hence, there exists integers $k_1$ and $k_2$ such that $a = k_1 d$ and $b = k_2 d$. Let $m = \frac{ab}{d}$. Then $m = k_1 b = a k_2$. Thus, $m$ is a (positive) multiple of $a$ and $b$ both and hence their common multiple. We show that $m$ is the least common multiple.

Let $c$ be any (positive) common multiple of $a$ and $b$. Then by definition of lcm, $c = au = bv$ for some integers $u$ and $v$. Since $d = \gcd(a,b)$, there exists integers $x$ and $y$ such that $d = ax+by$. Then

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y = vx+uy.$$

Therefore, $m \mid c$ and hence $m \leq c$. Thus, by definition, $m = \text{lcm}(a,b)$. Hence,

$$\text{lcm}(a,b) = \frac{ab}{d} = \frac{ab}{\gcd(a,b)}.$$

□

**Corollary 1.4.5**

For any choice of positive integers $a$ and $b$, $\text{lcm}(a,b) = ab$ if and only if $\gcd(a,b) = 1$.

## 1.5 The Diophantine Equation $ax+by=c$

**Theorem 1.5.1**

The linear Diophantine equation $ax+by=c$ has a solution if and only if $d \mid c$, where $d = \gcd(a,b)$. Further, if $(x_0,y_0)$ is any particular solution of this equation, then all other solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right)t, \qquad y = y_0 - \left(\frac{a}{d}\right)t,$$

where $t$ is an arbitrary integer.

*Proof.* Exercise. □

## 1.6 Fundamental Theorem of Arithmetic

**Definition 1.6.1**

An integer $p > 1$ is said to be a *prime number* or a *prime*, if its only positive divisors are 1 and $p$. An integer greater than 1 is called *composite* if it is not prime.

Note that, 2 is the only even prime and 1 is neither a prime nor a composite.

**Theorem 1.6.2**

If $p$ is a prime and $p \mid ab$, then $p \mid a$ and $p \mid b$.

*Proof.* If $p \mid a$, then we are done. Assume that $p \nmid a$. Since the only positive divisors of $p$ are 1 and $p$ itself, it follows that $\gcd(a,p) = 1$. Hence, by Euclid's lemma (Theorem 1.2.11), $p \mid b$. □

The result can be extended to more than two integers.

**Corollary 1.6.3**

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

*Proof.* We prove the result by induction on $n$, the number of factors. For $n = 1$, there is nothing to prove. For $n = 2$, the result holds by the above theorem. Suppose the result is true for $n-1$ factors, $n > 2$. That is, if $p \mid a_1 a_2 \cdots a_{n-1}$, then $p \mid a_k$ for some $k$, where $1 \leq k \leq n-1$.

Now suppose $p \mid a_1 a_2 \cdots a_n$. Then by the above theorem, $p \mid a_1 a_2 \cdots a_{n-1}$ or $p \mid a_n$. If $p \mid a_n$ then we are done. If $p \mid a_1 a_2 \cdots a_{n-1}$, then by induction hypothesis $p \mid a_k$ for some $k$, where $1 \leq k \leq n-1$. This proves the result. □

**Corollary 1.6.4**

If $p, q_1, q_2, \ldots, q_n$ are all primes such that $p \mid q_1 q_2 \cdots q_n$, then $p = q_k$ for some $k$, where $1 \leq k \leq n$.

*Proof.* By the above corollary, $p \mid q_k$ for some $k$, where $1 \leq k \leq n$. Since $q_k$ is a prime , the only positive divisors of $q_k$ are 1 and $q_k$ itself. Since $p$ is a prime $p > 1$ and hence $p = q_k$. □

**Theorem 1.6.5: Fundamental Theorem of Arithmetic**

Every positive integer $n > 1$ is either a prime or can be represented as a product of primes. Moreover, this representation is unique upto the order in which the factors occur.

*Proof.* If $n$ is itself a prime, then there is nothing to prove. If $n$ is composite, then there exists an integer $d$ such that $d \mid n$ and $1 < d < n$. The set of positive divisors of $n$ is thus nonempty and so by well-ordering principle it has a least element, say $p_1$. Then $p_1$ must be a prime number. For if, $p_1$ has a divisor $q$ such that $1 < q < p_1$, then $q \mid p$ and $p \mid n$ implies that $q \mid n$. This is a contradiction as $p_1$ is the smallest positive divisor of $n$ greater than 1.

Therefore, we write $n = p_1 n_1$ for some integer $n_1$, where $p_1$ is prime and $1 < n_1 < n$. If $n_1$ is prime, then we are done as we have the required representation. If $n_1$ is not a prime, then repeating the argument as above, we get prime $p_2$ and an integer $n_2$ such that $n_1 = p_2 n_2$, i.e.

$$n = p_1 p_2 n_2, \qquad 1 < n_2 < n_1.$$

Again if $n_2$ is a prime, then we are done. Otherwise, as before we get $n_2 = p_3 n_3$, where $p_3$ is a prime and $1 < n_3 < n_2$. Thus,

$$n = p_1 p_2 p_3 n_3, \qquad 1 < n_3 < n_2.$$

Since we have a decreasing sequence $n > n_1 > n_2 > \cdots > 1$, after some steps some integer $n_i$ is prime. Suppose $n_{k-1}$ is prime, call it $p_k$. Then we have the prime factorization of the form

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

Now, we prove the uniqueness of such a representation. Suppose that the integer $n$ can be represented as a product of primes in two ways as follows:

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

where $p_i$ and $q_j$ are primes such that

$$p_1 \leq p_2 \leq \cdots \leq p_r, \qquad q_1 \leq q_2 \leq \cdots \leq q_s.$$

Without the loss of generality, assume that $r \leq s$. Since $p_1 \mid q_1 q_2 \cdots q_s$ by Corollary 1.6.4, $p_1 = q_k$ for some $k$. Then $p_1 \geq q_1$. By similar argument, we get $q_1 \geq p_1$, and hence $p_1 = q_1$. Canceling this common factor, we get

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

Repeating the same process for $p_2$, we get $p_2 = q_2$ and hence

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s.$$

Continuing this way, if $r < s$, then we get

$$1 = q_{r+1} q_{r+2} \cdots q_s$$

which is not possible as $q_j > 1$ for all $j$. Hence, $r = s$ and $p_i = q_i$ for all $i = 1, 2, \ldots, r$. Hence, the factorization is unique. □

**Corollary 1.6.6**

Any positive integer $n > 1$ can be uniquely written as

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

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

For example,

$$4725 = 3^3 \cdot 5^2 \cdot 7 \quad \text{and} \quad 17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2.$$

**Remark 1.6.7.** Greatest common divisor can be determined easily from the prime factorization. Let $a$ and $b$ be two integers whose gcd we want to compute. Suppose $p_1, p_2, \ldots, p_n$ are distinct primes that divide either $a$ or $b$. Then we can write

$$a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}, \quad b = p_1^{j_1} p_2^{j_2} \cdots p_n^{j_n},$$

where $k_i \geq 0, j_i \geq 0$ for $i = 1, 2, \ldots, n$. Then

$$\gcd(a, b) = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n},$$

where $r_i = \min(k_i, j_i)$.

For example, let $a = 4725$ and $b = 17460$. We have

$$4725 = 2^0 \cdot 3^3 \cdot 5^2 \cdot 7, \quad 17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$$

and so

$$\gcd(4725, 17460) = 2^0 \cdot 3^2 \cdot 5 \cdot 7 = 315.$$

**Theorem 1.6.8: Euclid**

There is an infinite number of primes.

*Proof.* The proof given by Euclid is by contradiction. Let $p_1, p_2, \ldots, p_n$ be the only primes. Consider the integer

$$m = p_1 p_2 \cdots p_n + 1.$$

Since $m > 1$, by fundamental theorem of arithmetic, it is divisible by some prime $p$, i.e. $p \mid m$. Since $p_1, p_2, \ldots, p_n$ are the only primes, $p$ must be equal to one of the primes $p_1, p_2, \ldots, p_n$. Hence, $p \mid p_1 p_2 \cdots p_n$. But then $p \mid m$ implies that $p \mid m - p_1 p_2 \cdots p_n$. Thus, $p \mid 1$ which is a contradiction since $p$ is a prime (i.e. $p > 1$). Hence, our assumption that there are only finitely many primes is false and hence the result. □

**Theorem 1.6.9: Pythagoras**

The number $\sqrt{2}$ is irrational.

*Proof.* Suppose on the contrary that $\sqrt{2}$ is a rational number. Then $\sqrt{2} = \frac{a}{b}$ for some integers $a$ and $b$ and we may assume that $\gcd(a, b) = 1$. Squaring both the sides, we get $2 = \frac{a^2}{b^2}$ or $a^2 = 2b^2$. Then $b \mid a^2$. If $b > 1$, then by Fundamental Theorem of Arithmetic $p \mid b$ for some prime $p$. But then $p \mid a^2$ and hence $p \mid a$. This implies that $\gcd(a, b) \geq p$ which is a contradiction. So, there does not exists any prime $p$ such that $p \mid b$. Then $b = 1$. But then $a^2 = 2$ which is not possible. Hence, $\sqrt{2}$ is an irrational number. □

*Alternative argument.* Suppose on the contrary that $\sqrt{2}$ is a rational number. Then $\sqrt{2} = \frac{a}{b}$ for some integers $a$ and $b$ and we may assume that $\gcd(a, b) = 1$. Then there exists integers $x$ and $y$ such that $ax + by = 1$. Hence,

$$\sqrt{2} = \sqrt{2}(ax + by) = (\sqrt{2}a)x + (\sqrt{2}b)y = 2bx + ay$$

which implies that $\sqrt{2}$ is an integer. Hence, $\sqrt{2}$ cannot be rational. □

CHAPTER 2

# Congruences and Fermat's Theorem

## 2.1 Definition and Basic Properties

**Definition 2.1.1: Congruent Modulo $n$**

Let $n$ be a fixed positive integer. Two integers $a$ and $b$ are said to be *congruent modulo n* if $n$ divides $a-b$, i.e. $a-b=kn$ for some integer $k$. We denote it by $a \equiv b \pmod{n}$.

For $n=7$, we have

$$3 \equiv 24 \pmod{7}, \qquad -31 \equiv 11 \pmod{7}, \qquad -15 \equiv -64 \pmod{7}$$

as $3-24=(-3)7,\ -31-11=(-6)7,\ 15-(-64)=7\cdot 7$.

If $n \nmid (a-b)$, then we say that $n$ is *incongruent to b modulo n* and in this case we denote it by $a \not\equiv b \pmod{n}$. For example, $25 \not\equiv 12 \pmod{7}$ as $25-12=13$ is not divisible by 7.

Any two integers are congruent modulo 1. Two integers are congruent modulo 2 if both are either even or odd.

For $n>1$, let $a$ be an integer, and $q$ and $r$ be the quotient and the remainder obtained on dividing $a$ by $n$. Then we write

$$a = qn + r, \qquad 0 \le r < n.$$

Then by the definition of congruence, $a \equiv r \pmod{n}$. Since $0 \le r < n$, there are only $n$ choices for $r$ and hence every integer is congruent to exactly one of the values $0,1,2,\ldots,n-1$ modulo $n$. In particular, $a \equiv 0 \pmod{n}$ if and only if $n \mid a$. The set of $n$ integers $0,1,2,\ldots,n-1$ is called the set of *least non-negative residues modulo n*. In general, a collection of $n$ integers $a_1,a_2,\ldots,a_n$ is said to form a *complete set of residues* or a *complete system of residues modulo n* if every integer is congruent to one and only one of the $a_k$ modulo $n$. That is, $a_1,a_2,\ldots,a_n$ are congruent modulo $n$ to one of the values $0,1,2,\ldots,n-1$ in some order. For example,

$$-12,-4,11,13,22,82,91$$

form a complete residue system modulo 7 as

$$-12 \equiv 2 \pmod 7,\ -4 \equiv 3 \pmod 7,\ 11 \equiv 4 \pmod 7,\ 13 \equiv 6 \pmod 7,$$
$$22 \equiv 1 \pmod 7,\ 82 \equiv 5 \pmod 7,\ 91 \equiv 0 \pmod 7.$$

Observe that any $n$ integers form a complete residue system modulo $n$ if and only if no two of the integers are congruent modulo $n$.

**Theorem 2.1.2**

Let $a$ and $b$ be any integers. $a \equiv b \pmod n$ if and only if $a$ and $b$ leave the same non-negative remainder when divided by $n$.

*Proof.* First assume that $a \equiv b \pmod n$. This means that $n \mid (a-b)$ or $a = b+kn$ for some integer $k$. Suppose $b$ leaves the remainder $r$ on dividing by $n$, i.e. $b = qn+r$, where $0 \le r < n$. Therefore,

$$a = b+kn = (qn+r)+kn = (q+k)n+r.$$

Thus, $a$ also leaves the remainder $r$ on dividing by $n$.

Conversely, assume that $a$ and $b$ leave the same non-negative remainder, say $r$, on dividing by $n$. Then $a = q_1n+r$ and $b = q_2n+r$ for some integers $q_1$ and $q_2$, where $0 \le r < n$. Then

$$a-b = (q_1n+r)-(q_2n+r) = (q_1-q_2)n.$$

Thus, $n \mid (a-b)$ and hence by the definition of congruence, $a \equiv b \pmod n$. □

Some of the properties of congruences are shown in the next theorem.

**Theorem 2.1.3**

Let $n > 1$ be fixed and $a, b, c, d$ be arbitrary integers. Then the following properties hold:

(a) $a \equiv a \pmod n$.
(b) If $a \equiv b \pmod n$, then $b \equiv a \pmod n$.
(c) If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.
(d) If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $a+c \equiv b+d \pmod n$ and $ac \equiv bd \pmod n$.
(e) If $a \equiv b \pmod n$, then $a+c \equiv b+c \pmod n$ and $ac \equiv bc \pmod n$.
(f) If $a \equiv b \pmod n$, then $a^k \equiv b^k \pmod n$ for any positive integer $k$.

*Proof.* (a) For any integer $a$, $a-a = 0 \cdot n$ and hence $a \equiv a \pmod n$.

(b) If $a \equiv b \pmod n$, then $a-b = kn$ for some integer $k$. Therefore, $b-a = -k \cdot n = (-k)n$, i.e. $b \equiv a \pmod n$.

(c) $a \equiv b \pmod n$ implies $a-b = kn$ for some integer $k$ and $b \equiv c \pmod n$ implies $b-c = ln$ for some integer $l$. Now,

$$a-c = (a-b)+(b-c) = kn+ln = (k+l)n.$$

Thus, $n \mid (a-c)$ and hence $a \equiv c \pmod n$.

(d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then there exists integers $k_1$ and $k_2$ such that $a-b = k_1 n$ and $c-d = k_2 n$. Then, we have

$$(a-b)+(c-d) = (a+b)-(b+d) \equiv k_1 n + k_2 n = (k_1+k_2)n.$$

Thus, $a+c \equiv b+d \pmod{n}$. Also

$$ac = (b+k_1 n)(d+k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n.$$

Since $bk_2 + dk_1 + k_1 k_2 n$ is an integer, it follows that $n \mid (ac-bd)$ and hence $ac \equiv bd \pmod{n}$.

(e) Since $c \equiv c \pmod{n}$, taking $d = c$ in (d), we get the required result.

(f) We prove this by induction on $k$. Clearly, the result is true for $k = 1$. Assume that the result holds for some fixed $k$, i.e. $a^k \equiv b^k \pmod{n}$. Then, since $a \equiv b \pmod{n}$ and $a^k \equiv b^k \pmod{n}$, by (d), we have

$$aa^k \equiv bb^k \pmod{n} \Rightarrow a^{k+1} \equiv b^{k+1} \pmod{n}.$$

Hence, by induction $a^k \equiv b^k \pmod{n}$ for any positive integer $k$.

□

**Example 2.1.4.** We show that 41 divides $2^{20}-1$. Note that, $2^5 = 32 \equiv -9 \pmod{41}$. Hence, $(2^5)^4 \equiv (-9)^4 \pmod{41}$, i.e. $2^{20} \equiv 81 \cdot 81 \pmod{41}$. But $81 \equiv -1 \pmod{41}$ and hence $2^{20} \equiv (-1)(-1) \equiv 1 \pmod{41}$ or $2^{20}-1 \equiv 0 \pmod{41}$. Thus,

$$41 \mid 2^{20}-1.$$

**Example 2.1.5.** We determine the remainder obtained upon dividing the sum

$$1!+2!+3!+\cdots+99!+100!$$

by 12.

Observe that, $4! = 24 \equiv 0 \pmod{12}$. Hence for $k \geq 4$, we have $k! = k(k-1)\cdots 6\cdot 5\cdot 4! \equiv 0 \pmod{12}$. As a result,

$$1!+2!+3!+\cdots+99!+100! \equiv 1!+2!+3! \equiv 9 \pmod{12}.$$

Hence, the required remainder is 9.

**Exercise 2.1**

Find the remainder when $1!+2!+3!+\cdots+99!+100!$ is divided by 45.

**Exercise 2.2**

Find the remainder when $1!+2!+3!+\cdots+10000!$ is divided by 11.

**Exercise 2.3**

1. Find the remainders when $2^{50}$ and $41^{65}$ are divided by 7.

2. Find the remainder when the sum $1^5+2^5+3^5+\cdots+100^5$ is divided by 4.

We have seen that if $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$. However, its converse does not hold. For example, $2\cdot 4 \equiv 2\cdot 1 \pmod{6}$ but $4 \not\equiv 1 \pmod{6}$. The following result shows when the factor $c$ can be canceled.

**Theorem 2.1.6**

If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{\frac{n}{d}}$, where $d = \gcd(c,n)$.

*Proof.* If $ca \equiv cb \pmod{n}$, then we have $c(a-b) = ca - bc = kn$ for some integer $k$. Since $\gcd(c,n) = d$, $d \mid c$ and $d \mid n$. Therefore, there exists integers $r$ and $s$ such that $c = dr$ and $n = ds$. Then

$$c(a-b) = kn \Rightarrow r(a-b) = ks.$$

Hence, $s \mid r(a-b)$. Since $d = \gcd(c,n)$, it follows that $\gcd(r,s) = 1$ and hence by Euclid's lemma $s \mid a-b$. Hence, $a \equiv b \pmod{s}$, i.e. $a \equiv b \pmod{\frac{n}{d}}$. □

**Corollary 2.1.7**

If $ca \equiv cb \pmod{n}$ and $\gcd(c,n) = 1$, then $a \equiv b \pmod{n}$.

**Corollary 2.1.8**

If $ca \equiv cb \pmod{p}$ and $p \nmid c$, then $a \equiv b \pmod{p}$.

*Proof.* Since $p \nmid c$, $\gcd(p,c) = 1$. Hence, by above corollary $a \equiv b \pmod{p}$. □

Observe that, in general, $ab \equiv 0 \pmod{n}$ does not imply that $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$. For example, $4\cdot 3 \equiv 0 \pmod{12}$ but $4 \not\equiv 0 \pmod{12}$ and $3 \not\equiv 0 \pmod{12}$. However, if $ab \equiv 0 \pmod{n}$ and $\gcd(a,n) = 1$, then by Corollary 2.1.7 (alternatively by Euclid's lemma and definition of congruence) we have $b \equiv 0 \pmod{n}$. Similarly, if $p$ is a prime, then $ab \equiv 0 \pmod{p}$ implies that either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

## 2.2 Linear Congruences and the Chinese Remainder Theorem

A congruence which is an equation of the form $ax \equiv b \pmod{n}$ is called a *linear congruence*. By a solution of such a linear congruence, we mean an integer $x_0$ such that $ax_0 \equiv b \pmod{n}$. By definition, $ax_0 \equiv b \pmod{n}$ if and only if $n \mid ax_0 - b$. Therefore, $ax_0 - b = ny_0$ for some integer $y_0$. Thus, the problem of finding all integers that will satisfy the linear congruence $ax \equiv b \pmod{n}$ is identical with that of finding the solutions of the linear Diophantine equation $ax - ny = b$.

Note that $x = 3$ and $x = -9$ satisfy the linear congruence $3x \equiv 9 \pmod{12}$. However, we do not treat them as different solutions. Thus, by the number of solutions of $ax \equiv p \pmod{n}$ we mean the number of incongruent integers satisfying the congruence.

**Theorem 2.2.1**

The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$, where $d = \gcd(a,n)$. Further, if $d \mid b$, then it has $d$ mutually incongruent solutions modulo $n$.

*Proof.* Suppose the linear congruence $ax \equiv b \pmod{n}$ has a solution. Let $x_0$ be its solution. Then $ax_0 \equiv b \pmod{n}$. By definition, $n \mid ax_0 - b$. Then there is an integer $y_0$ such that $ax_0 - b = ny_0$ or $ax_0 - ny_0 = b$. Let $d = \gcd(a,n)$. Then $d \mid a$ and $d \mid n$. Then $d \mid ax_0 - ny_0$ (an integer linear combination of $a$ and $n$). Thus, $d \mid b$.

Conversely, assume that $d \mid b$, where $d = \gcd(a,n)$. Then $b = kd$ for some integer $k$. Since $d = \gcd(a,n)$, by Bézout's identity (Theorem 1.2.5), there exist integers $x_1$ and $y_1$ such that $ax_1 + ny_1 = d$. Multiplying both the sides by $k$, we get

$$a(kx_1) + n(ky_1) = kd = b.$$

Thus, $ax_0 \equiv b \pmod{n}$, where $x_0 = kx_1$. Hence, the linear congruence $ax \equiv b \pmod{n}$ has a solution.

If $x_0, y_0$ is one specific solution of the equation $ax - ny = b$, then by Theorem 1.5.1, any other solution has the form

$$x = x_0 + \frac{n}{d}t, \qquad y = y_0 + \frac{a}{d}t$$

for some choice of $t$.

Consider the first formula $x = x_0 + \frac{n}{d}t$. Among various integers satisfying this formula, consider those integers which satisfy it when $t$ takes successive values $t = 0, 1, 2, \ldots, d-1$, i.e.,

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}.$$

**Claim.**

1. These integers are incongruent modulo $n$.
2. All other such integers $x$ are congruent to one of them.

Suppose, if possible,

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n}$$

for some $0 \leq t_1 < t_2 \leq d-1$. Then we have

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}.$$

Since $\gcd(n/d, n) = n/d$, by Theorem 2.1.6, we have

$$t_1 \equiv t_2 \pmod{d}.$$

Then $d \mid t_2 - t_1$ which is not possible as $0 < t_2 - t_1 < d$. This proves the first part of our claim. Finally, it remains to show that any other solution $x = x_0 + \left(\frac{n}{d}\right)t$ is congruent modulo $n$ to one of the $d$ integers in the above list. By division algorithm, we have $t = qd + r$, where $0 \leq r \leq d-1$. Hence,

$$x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r)$$

$$\begin{aligned} &= x_0 + nq + \frac{n}{d}r \\ &= x_0 + \frac{n}{d}r \pmod{n}, \end{aligned}$$

where $x + 0 + \frac{n}{d}r$ with $0 \leq r \leq d-1$ is one of the $d$ solutions in the above list. This completes the proof. □

**Corollary 2.2.2**

If $\gcd(a,n) = 1$, then the linear congruence $ax \equiv b \pmod{n}$ has a unique solution modulo $n$.

In particular, if $a$ and $n$ are relatively prime integers, then the congruence $ax \equiv 1 \pmod{n}$ has a unique solution. In fact, the converse is also true. This solution is nothing but the multiplicative inverse of $a$ modulo $n$.

**Example 2.2.3.** Solve the linear congruence $18x \equiv 30 \pmod{42}$.

***Solution***. Since $\gcd(18,42) = 6$ and $6 \mid 30$, by Theorem 2.2.1, the given linear congruence has 6 solutions which are incongruent (to each other) modulo 42.

By trial method, we find that $x = 4$ is a solution of the given linear congruence. Then by the above theorem, the six solutions are as follows:

$$x \equiv 4 + \left(\frac{42}{6}\right)t \equiv 4 + 7t \pmod{42}, \quad t = 0, 1, \ldots, 5.$$

Thus,

$$x = 4, 11, 18, 25, 32, 39 \pmod{42}.$$

□

**Example 2.2.4.** Solve the linear congruence $9x \equiv 21 \pmod{30}$.

***Solution***. **Method 1.** Since $\gcd(9,30) = 3$ and $3 \mid 21$, by Theorem 2.2.1, the given linear congruence has 3 solutions which are incongruent modulo 30.

Dividing the given congruence by 3, we get $3x \equiv 7 \pmod{10}$. Since $\gcd(3,10) = 1$, the reduced congruence has a unique solution modulo 10. We can substitute $0, 1, \ldots, 9$ to find the solution. However, a better way is to multiply the congruence $3x \equiv 7 \pmod{10}$ by 7 since 7 is the multiplicative inverse of 3 modulo 10 as $7 \cdot 3 \equiv 21 \equiv 1 \pmod{10}$. Thus, multiplying the congruence $3x \equiv 7 \pmod{10}$ by 7, we get

$$21x \equiv 49 \pmod{10}$$

which reduces to $x \equiv 9 \pmod{10}$. But the original congruence was modulo 30 and so its solutions belong to the set $\{0, 1, \ldots, 29\}$. Taking $t - 0, 1, 2$ in the formula $x = 9 + 10t$, we get $x = 9, 19, 29$, and hence

$$x \equiv 9 \pmod{30},\ x \equiv 19 \pmod{30},\ x \equiv 29 \pmod{20}$$

are the required solutions of the congruence $9x \equiv 21 \pmod{30}$.

**Method 2.** Another method of obtaining the solution is to consider the congruence $9x \equiv 21 \pmod{30}$ equivalent to the linear Diophantine equation $9x - 30y = 21$ and obtain the solution of this linear Diophantine equation. Using the Euclidean algorithm, we express the GCD $3 = \gcd(9,30)$ as an integer linear combination of 9 and 30 to find that

$$3 = 9 \cdot (-3) + 30 \cdot 1$$

and so

$$21 = 9 \cdot (-21) - 30 \cdot (-7).$$

Thus, $x = -21$ and $y = -7$ is a solution of the linear Diophantine equatoin $9x - 30y = 21$ and hence all the solutions of the congruence $9x \equiv 21 \pmod{30}$ are given by

$$x = -21 + \left(\frac{30}{3}\right) t = -21 + 10t, \quad t = 0, 1, 2.$$

Thus, the incongruent solutions of the given linear congruence modulo 30 are

$$x \equiv -21 \equiv 9 \pmod{30},\ x \equiv -11 \equiv 19 \pmod{30},\ x \equiv -1 \equiv 29 \pmod{30}.$$

□

After considering a single linear congruence, naturally, one would turn to the question of solving a system of simultaneous linear congruences:

$$a_1 x \equiv b_1 \pmod{m_1},\ a_2 x \equiv b_2 \pmod{m_2}, \ldots, a_r x \equiv b_r \pmod{m_r}.$$

We shall assume that the moduli $m_k$ are pairwise relatively prime (or mutually coprime). The system will have no simultaneous solution unless each of these congruences are solvable, i.e., for each $k$, $d_k \mid b_k$, where $d_k = \gcd(a_k, m_k)$. When these conditions are satisfied, the common factor $d_k$ can be cancelled in the $k$-th congruence for each $k$ to obtain a new system of congruences with the same set of solutions as the above one as follows:

$$a_1' x \equiv b_1' \pmod{n_1},\ a_2' x \equiv b_2' \pmod{n_2}, \ldots, a_r' x \equiv b_r' \pmod{n_r},$$

where $n_k = \frac{m_k}{d_k}$ with $\gcd(n_i, n_j) = 1$ for $i \neq j$ and along with the condition that $\gcd(a_i', n_i) = 1$. The solutions of these individual congruences are of the form

$$x \equiv c_1 \pmod{n_1},\ x \equiv c_2 \pmod{n_2},\ \ldots,\ x \equiv c_r \pmod{n_r}.$$

Thus, the problem reduces to finding a solutions of the simultaneous system of linear congruences which is of simpler type as the above system.

This kind of problem has been found to have roots in the Chinese literature around the 1st century A.D. Sun-Tsu asked: Find a number that leaves a remainder of 2, 3, and 2 when divided by 3, 5, and 7 respectively. To honor their early contributions, the rule for obtaining such a solution is usually known as the Chinese Remainder Theorem.

**Theorem 2.2.5: Chinese Remainder Theorem**

Let $n_1, n_2, \ldots, n_r$ be positive integers pairwise relatively prime, i.e. $\gcd(n_j, n_k) = 1$ for all $j \neq k$. Then the system of linear congruences,

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$

$$\vdots$$
$$x \equiv a_r \pmod{n_r}$$

has a simultaneous solution, which is unique modulo the product $n_1 n_2 \cdots n_r$.

*Proof.* Let $n = n_1 n_2 \cdots n_r$ and for $k = 1, 2, \ldots, r$, let

$$N_k = \frac{n}{n_k} = n_1 n_2 \cdots n_{k-1} n_{k+1} \cdots n_r.$$

Note that $\gcd(N_k, n_k) = 1$ as the integers $n_i$ are pairwise relatively prime for all $i = 1, 2, \ldots, r$. Then (by Theorem 2.2.1) for every $k = 1, 2, \ldots, r$, the congruence $N_k x \equiv 1 \pmod{n_k}$ has a unique solution, say $x_k$, i.e.

$$N_k x_k \equiv 1 \pmod{n_k}, \qquad k = 1, 2, \ldots, r.$$

Since $n_k \mid N_j$ for all $k \neq j$, we have $N_j \equiv 0 \pmod{n_k}$ for all $k = 1, 2, \ldots, r$, $k \neq j$.

Let $y = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$. Then for any $k = 1, 2, \ldots, r$, observe that

$$\begin{aligned} y &\equiv a_k N_k x_k \pmod{n_k} \\ &\equiv a_k \cdot 1 \pmod{n_k} \\ &\equiv a_k \pmod{n_k}. \end{aligned}$$

Hence, $y$ is a simultaneous solution of the given system.

Now, we show the uniqueness of $y$ modulo $n = n_1 n_2 \cdots n_r$. Suppose $y$ and $z$ are simultaneous solutions of the given system of linear congruences. Then for all $k = 1, 2, \ldots, r$,

$$\begin{aligned} y &\equiv a_k \pmod{n_k} \\ z &\equiv a_k \pmod{n_k}. \end{aligned}$$

Therefore, $y \equiv z \pmod{n_k}$ or $n_k \mid y - z$ for all $k = 1, 2, \ldots, r$. Since $\gcd(n_j, n_k) = 1$ for all $j \neq k$, by Corollary 1.2.10, $n_1 \cdots n_r \mid y - z$, i.e.

$$y \equiv z \pmod{n}.$$

□

**Example 2.2.6.** The problem by Sun-Tsu corresponds to the following system of three congruences. Find the unique solution of the simultaneous system of congruences modulo 105.

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

***Solution***. In the notation of the Chinese remainder theorem, we have $n = 3 \cdot 5 \cdot 7 = 105$ and

$$N_1 = \frac{n}{3} = 35,\ N_2 = \frac{n}{5} = 21,\ N_3 = \frac{n}{7} = 15.$$

Now the linear congruences

$$35x \equiv 1 \pmod{3},\ 21x \equiv 1 \pmod{5},\ 15x \equiv 1 \pmod{7}$$

are satisfied by $x_1 = 2, x_2 = 1, x_3 = 1$ respectively. Thus, the solution of the given simultaneous system of congruences is given by

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv \pmod{105}.$$

Therefore,

$$x \equiv 23 \pmod{105}.$$

□

**Example 2.2.7.** Solve the linear congruence

$$17x \equiv 9 \pmod{276}.$$

***Solution***. Since $276 = 3 \cdot 4 \cdot 23$. Finding a solution of the given linear congruence is equivalent to solving the following simultaneous system of congruences.

$$\begin{aligned} 17x &\equiv 9 \pmod{3} \\ 17x &\equiv 9 \pmod{4} \\ 17x &\equiv 9 \pmod{23} \end{aligned}$$

or equivalently,

$$\begin{aligned} x &\equiv 0 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ 17x &\equiv 9 \pmod{23}. \end{aligned}$$

Note that if $x \equiv 0 \pmod{3}$, then $x = 3k$ for some integer $k$. Substituting this in the second congruence, we obtain

$$3k \equiv 1 \pmod{4}.$$

Since $3 \cdot 3 \equiv 9 \equiv 1 \pmod{4}$, multiplying the above congruence by 3, we get

$$k \equiv 9k \equiv 3 \pmod{4}.$$

Thus, $k = 3 + 4j$ for some integer $j$ and so

$$x = 3(3 + 4j) = 9 + 12j.$$

For $x$ to satisfy the third congruence of the system, we must have

$$17(9 + 12j) \equiv 9 \pmod{23}.$$

Therefore, $153 + 204j \equiv 9 \pmod{23}$ or $15 + 20j \equiv 9 \pmod{23}$. So, $20j \equiv -6 \pmod{23}$ which is same as $-3j \equiv -6 \pmod{23}$ or $j \equiv 2 \pmod{23}$. This gives $j = 2 + 23t$ for some integer $t$ and hence

$$x = 9 + 12j = 9 + 12(2 + 23t) = 33 + 276t.$$

Therefore, $x \equiv 33 \pmod{276}$ is a solution of the linear congruence $17x \equiv 9 \pmod{276}$. □

Consider a linear congruence in two variables of the form

$$ax + by \equiv c \pmod{n}.$$

Analogous to Theorem 2.2.1, such a linear congruence has a solution if and only if $\gcd(a,b,n) \mid c$. The condition for solvability holds if either $\gcd(a,n) = 1$ or $\gcd(b,n) = 1$. Suppose $\gcd(a,n) = 1$. When the congruence is expressed as

$$ax \equiv c - by \pmod{n},$$

Corollary 2.2.2 guarantees a unique solution for $x$ for each of the $n$ incongruent values of $y$.

For example, consider the congruence $7x + 4y \equiv 5 \pmod{12}$. Then $7x \equiv 5 - 4y \pmod{12}$. Substituting $y \equiv 5 \pmod{12}$ gives $7x \equiv -15 \pmod{12}$ and so

$$x \equiv 7 \cdot (-3) \equiv -21 \equiv 3 \pmod{12}.$$

Thus, $x \equiv 3 \pmod{12}$ and $y \equiv 5 \pmod{12}$ is one of the 12 incongruent solutions of the congruence $7x + 4y \equiv 5 \pmod{12}$.

**Theorem 2.2.8**

The system of linear congruences

$$\begin{aligned} ax + by &\equiv r \pmod{n} \\ cx + dy &\equiv s \pmod{n} \end{aligned}$$

has a unique solution modulo $n$ whenever $\gcd(ad - bc, n) = 1$.

*Proof.* Multiplying the first congruence by $d$ and the second congruence by $b$, and then subtracting the lower resultant congruence from the upper, we get

$$(ad - bc)x \equiv dr - bs \pmod{n}. \tag{2.1}$$

The assumption $\gcd(ad - bc, n) = 1$ guarantees that the congruence

$$(ad - bc)z \equiv 1 \pmod{n}$$

has a unique solution, say $t$. When the congruence (2.1) is multiplied by $t$, we get

$$x \equiv t(dr - bs) \pmod{n}.$$

By a similar process of elimination, a value of $y$ can also be found. That is, multiplying the first congruence of the system by $c$ and the second one by $a$, and then subtracting, we get

$$(ad - bc)y \equiv as - cr \pmod{n}. \tag{2.2}$$

Multiplying by $t$ gives

$$y \equiv t(as - cr) \pmod{n}.$$

Congruences (2.1) and (2.2) give a solution of the system. □

Let us consider an example of a system of linear congruences in two variables.

**Example 2.2.9.** Solve the following system of linear congruences.

$$7x+3y \equiv 10 \pmod{16},$$
$$2x+5y \equiv 9 \pmod{16}.$$

***Solution***. Since $\gcd(7\cdot 5-2\cdot 3,16)=\gcd(29,16)=1$, a solution to the given system exists. It is obtained by the method given in the above theorem. Multiplying the first congruence by 5 and the second one by 3, and subtracting, we get

$$29x \equiv 5\cdot 10-3\cdot 9 \equiv 23 \pmod{16}$$

or $13x \equiv 7 \pmod{16}$. Note that 5 is the inverse of 13 modulo 16 as $5\cdot 13 \equiv 65 \equiv 1 \pmod{16}$. So multiplying the above congruence by 5, we get $x \equiv 35 \equiv 3 \pmod{16}$.

Similarly, multiplying the first congruence of the system by 2 and the second by 7, and then subtracting, we get

$$29y \equiv 9\cdot 6-10\cdot 2 \equiv \pmod{16}.$$

So, $13y \equiv 11 \pmod{16}$. Multiplying the congruence by 5 (the inverse of 13), we get $y \equiv 55 \equiv 7 \pmod{16}$. Thus, the unique solution of the system is

$$x \equiv 3 \pmod{16}, \quad y \equiv 7 \pmod{16}.$$

□

## 2.3 Fermat's Theorem

**Theorem 2.3.1**

Let $p$ be a prime and suppose $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.

*Proof.* Consider the first $p-1$ positive multiples of $a$

$$a, 2a, 3a, \ldots, (p-1)a.$$

None of these numbers is congruent to any other number modulo $p$ because if

$$ra \equiv sa \pmod{p} \text{ for some } 1 \le r < s \le p-1,$$

then $a$ could be cancelled (since $\gcd(a,p)=1$ as $p \nmid a$) to give $r \equiv s \pmod{p}$, which is not possible. Also, since $p \nmid a$, and $p \nmid 1$, $p \nmid 2$, …, $p \nmid p-1$, none of the numbers in the above list is congruent to zero modulo $p$. Therefore, the set of integers in the above list must be congruent modulo $p$ to $1, 2, 3, \ldots, p-1$, taken in some order.

Multiplying all these congruences together, we get

$$a\cdot 2a\cdot 3a\cdots(p-1)a \equiv 1\cdot 2\cdot 3\cdots(p-1) \pmod{p}$$

and hence

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

Since $p \nmid (p-1)!$ (as $p \nmid n$ for all $n = 1, 2, \ldots, p-1$), it can be cancelled from both sides (i.e., multiplying its inverse on both sides), to get

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

This complete the proof. □

**Corollary 2.3.2**

If $p$ is a prime, then $a^p \equiv a \pmod{p}$ for any integer $a$.

*Proof.* If $p \mid a$, then $a \equiv 0 \pmod{p}$ and so $a^p \equiv 0 \pmod{p}$. Hence, $a^p \equiv 0 \equiv a \pmod{p}$ and the statement holds. If $p \nmid a$, then by Fermat's theorem $a^{p-1} \equiv 1 \pmod{p}$. Multiplying this congruence by $a$, we get $a^p \equiv a \pmod{p}$. □

There is another proof of the above corollary on our reference text by Burton using principle of mathematical induction which is left as an exercise.

**Exercise 2.4**

Using induction, prove that if $p$ is a prime, then $a^p \equiv a \pmod{p}$ for every integer $a$.

Fermat's theorem has many applications in number theory. Firstly, it can be applied to make calculations faster. For example, to verify that $5^{38} \equiv 4 \pmod{11}$, we apply Fermat's theorem to get $5^{10} \equiv 1 \pmod{11}$ since $11 \nmid 5$. Using this, we get

$$5^{38} = (5^{10})^3 \cdot 5^8 \equiv 1^3(5^2)^4 \equiv 1 \cdot 3^4 \equiv 81 \equiv 4 \pmod{11}.$$

As another application, Fermat's theorem can be applied in testing the primality of a given integer $n$. The contrapositive equivalent of the Fermat's theorem tells us that if

$$a^n \not\equiv a \pmod{n}$$

for some choice of $a$, then $n$ cannot be prime, i.e., it must be composite. For example, consider $n = 117$ and to minimize the computations let us take a small value of $a$, say $a = 2$. Then

$$2^{117} = (2^7)^{16} \cdot 2^5.$$

Now, $2^7 \equiv 128 \equiv 11 \pmod{117}$, and so

$$2^{117} \equiv 11^{16} \cdot 2^5 \equiv (121)^8 \cdot 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}.$$

But

$$2^{21} \equiv (2^7)^3 \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \pmod{117}.$$

Thus,

$$2^{117} \equiv 44 \not\equiv 2 \pmod{117}.$$

Therefore, by Fermat's theorem, 117 must be composite, and indeed it is as $117 = 9 \cdot 13$.

Note that Fermat's theorem says that if $p$ is prime, then $a^{p-1} \equiv 1 \pmod{p}$, where $p \nmid a$. However, the converse is not true. That is, if $a^{n-1} \equiv 1 \pmod{n}$, then $n$ need not be prime. The following lemma is a required to show this.

**Lemma 2.3.3**

If $p$ and $q$ are distinct primes with $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$, then $a^{pq} \equiv a \pmod{pq}$.

*Proof.* From Corollary 2.3.2, taking $a^q$ in place of $a$, we get

$$(a^q)^p \equiv a^q \pmod{p}.$$

But, by hypothesis, $a^q \equiv a \pmod{p}$. Then from the above congruence, we get

$$a^{pq} \equiv a \pmod{p}$$

or, in other words, $p \mid a^{pq} - a$. Similarly, $q \mid a^{pq} - a$. Since $p$ and $q$ are distinct prime, $\gcd(p,q) = 1$ and so by Corollary 1.2.10, $pq \mid a^{pq} - a$. Hence, $a^{pq} \equiv a \pmod{pq}$. □

Now, we show that the converse of Fermat's theorem is not true. The number $341 = 11 \cdot 31$ is not prime. But we shall show that $2^{340} \equiv 1 \pmod{341}$. Note that

$$2^{10} = 1024 \equiv 31 \cdot 33 + 1 = 93 \cdot 11 + 1$$

and so $2^{10} \equiv 1 \pmod{31}$ and $2^{10} \equiv 1 \pmod{11}$. Thus,

$$2^{11} \equiv 2^{10} \cdot 2 \equiv 1 \cdot 2 \equiv 2 \pmod{31}$$

and

$$2^{31} = (2^{10})^3 \cdot 2 \equiv 1^3 \cdot 2 \equiv 2 \pmod{11}.$$

Then by the above lemma,

$$2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$$

or $2^{341} \equiv 2 \pmod{341}$. Cancelling a factor of 2, we get

$$2^{340} \equiv 1 \pmod{341}.$$

Hence, the converse of Fermat's theorem is false.

Over 25 centuries ago Chinese mathematicians claimed that a number $n$ is prime if and only if $n \mid 2^n - 2$, i.e., $2^n \equiv 2 \pmod{n}$. However, this is only true for integers $n \leq 340$. From the above example, we have $341 \mid 2^{341} - 2$ but 341 is not prime. This was found in the year 1819. The situation $n \mid 2^n - 2$ occurs often enough that such composite numbers $n$ are called *pseudoprimes*. The four smallest pseudoprimes are 341, 561, 645, 1105. The following theorem helps us to construct an increasing sequence of pseudoprimes.

**Theorem 2.3.4**

If $n$ is an odd pseudoprime, then $M_n = 2^n - 1$ is a larger one.

*Proof.* Since $n$ is a composite, $n = rs$ for some integers $1 < r \leq s < n$. Then by Exercise 1.10 $2^r - 1 \mid 2^n - 1$, or equivalently $2^r - 1 \mid M_n$. Thus, $M_n$ is composite. To show that $M_n$ is a pseudoprime, it remains to show that $M_n \mid 2^{M_n} - 2$.

By hypothesis, $n \mid 2^n - 2$. Hence, $2^n - 2 = kn$ for some integer $k$. It follows that

$$2^{M_n - 1} = 2^{2^n - 2} = 2^{kn}.$$

Therefore,

$$\begin{aligned} 2^{M_n-1}-1 &= 2^{kn}-1 \\ &= (2^n-1)(2^{n(k-1)}+2^{n(k-2)}+\cdots+2^n+1) \\ &= M_n(2^{n(k-1)}+2^{n(k-2)}+\cdots+2^n+1) \\ &\equiv 0 \pmod{M_n}. \end{aligned}$$

Therefore, $2^{M_n}-2 \equiv 0 \pmod{M_n}$ and hence $M_n$ is a pseudoprime. □

## 2.4 Wilson's Theorem

**Theorem 2.4.1: Wilson's Theorem**

If $p$ is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

*Proof.* Since $1 \equiv -1 \pmod{2}$ and $2! = 2 \equiv -1 \pmod{3}$, the result holds for $p = 2$ and $p = 3$. So, assume that $p > 3$. Suppose $a$ is any one of the positive integers

$$1, 2, 3, \ldots, p-1$$

modulo $p$. Then $\gcd(a, p) = 1$ as $p$ does not divided $1, 2, \ldots, p-1$. Then the linear congruence $ax \equiv 1 \pmod{p}$ has a unique solution modulo $p$. That is, there is a unique integer $a'$ with $1 \leq a' \leq p-1$ such that $aa' \equiv 1 \pmod{p}$. Now,

$$\begin{aligned} a = a' &\Leftrightarrow a^2 \equiv 1 \pmod{p} \\ &\Leftrightarrow (a-1)(a+1) \equiv 0 \pmod{p} \\ &\Leftrightarrow a \equiv 1 \pmod{p} \quad \text{or} \quad a \equiv -1 \equiv p-1 \pmod{p}. \end{aligned}$$

Thus, excluding 1 and $p-1$ all the other integers $2, 3, \ldots, p-2$ are grouped in pairs $a, a'$, where $a \neq a'$ such that their product $aa' \equiv 1 \pmod{p}$. Note that there are a total $(p-3)/2$ such congruences $aa' \equiv 1 \pmod{p}$. Multiplying these congruences together and rearranging the factors, we get

$$(p-2)! = 2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}.$$

Therefore,

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

This completes the proof. □

Let us understand the process in the above proof by an example.

**Example 2.4.2.** Take $p = 13$. As in the proof of the above theorem, it is possible to divide the integers $2, 3, \ldots, 11$ into $(p-3)/2 = 5$ pairs, such that their product is congruent to 1 modulo 13. They are as follows:

$$\begin{aligned} 2 \cdot 7 &\equiv 1 \pmod{13} \\ 3 \cdot 9 &\equiv 1 \pmod{13} \end{aligned}$$

$$4 \cdot 10 \equiv 1 \pmod{13}$$
$$5 \cdot 8 \equiv 1 \pmod{13}$$
$$6 \cdot 11 \equiv 1 \pmod{13}.$$

Multiplying these congruences gives the result

$$11! = (2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11) \equiv 1 \pmod{13}$$

and hence

$$12! \equiv 12 \equiv -1 \pmod{13}.$$

Thus, we showed that $(p-1)! \equiv -1 \pmod{p}$ for $p = 13$.

The converse of Wilson's theorem is also true. That is, if $(n-1)! \equiv -1 pmod n$, then $n$ must be a prime. Let us prove this. Suppose, if possible, $n$ is not a prime. Then it has a proper divisor, i.e., there is an integer $d$ with $1 < d < n$ such that $d \mid n$. Further, since $d \leq n-1$, $d$ occurs as one of the factors (integers) in $(n-1)!$ and so $d \mid (n-1)!$. But by hypothesis $n \mid (n-1)!+1$ and since $d \mid n$, we have $d \mid (n-1)!+1$. Since $d \mid (n-1)!$, we conclude that $d \mid 1$. Then $d = 1$ which is a contradiction to our assumption $1 < d < n$. Hence, $n$ must be a prime.

Wilson's theorem and its converse provide a necessary and sufficient condition to determine primality of an integer $n > 1$, namely, $n$ is prime if and only if $(n-1)! \equiv -1 pmod n$. However, this remains merely a theoretic test as in practice $(n-1)!$ becomes so large to manage when $n$ is large.

We end this section and the unit with an application of Wilson's theorem in the study of quadratic congruences. A *quadratic congruence* is a congruence of the form $ax^2 + bx + c \equiv 0 \pmod{n}$, where $a \not\equiv 0 \pmod{n}$.

**Theorem 2.4.3**

The quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$, where $p$ is an odd prime, has a solutions if and only if $p \equiv 1 \pmod{4}$.

*Proof.* Let $a$ be any solution of the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$, i.e., $a^2 \equiv -1 \pmod{p}$. Since $a^2 \not\equiv 0 \pmod{p}$, $p \nmid a^2$ and so $p \nmid a$. Then by Fermat's theorem,

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

Suppose, if possible, $p = 4k+3$ for some integer $k$. Then

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1.$$

Then from the above congruence, we have $1 \equiv -1 \pmod{p}$ which means $p \mid 2$, a contradiction as $p$ is an odd prime. Hence, $p$ must be of the form $4k+1$.

Conversely, assume that $p$ is of the form $4k+1$ for some integer $k$. In the product,

$$(p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1),$$

we have the congruences

$$p - 1 \equiv -1 \pmod{p}$$

$$\begin{aligned} p-2 &\equiv -2 \pmod{p} \\ &\vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod{p}. \end{aligned}$$

Rearranging the factors gives

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

as there are $(p-1)/2$ minus signs. Now, by Wilson's theorem $(p-1)! \equiv -1 \pmod{p}$. Then from the above, we get

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

Since $p$ is of the form $4k+1$, $\frac{p-1}{2} = 2k$, an even number, and so $(-1)^{(p-1)/2} = 1$. Thus, we have

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

Hence, $x = \left(\frac{p-1}{2}\right)!$ satisfies the congruence $x^2+1 \equiv 0 \pmod{p}$. □

Let us see this by a concrete example.

**Example 2.4.4.** Take $p = 13$ which is of the form $4k+1$. Then $(p-1)/2 = 6$. It is easy to see that

$$6! = 720 \equiv 5 \pmod{13}$$

and

$$5^2 + 1 = 26 \equiv 0 \pmod{13}.$$

Thus, the assertion that $\left[\left(\frac{p-1}{2}\right)!\right]^2 + 1 \equiv 0 \pmod{p}$ is correct for $p = 13$.

Wilson's theorem says that there are infinitely many composite numbers of the form $n!+1$ (Why?). On the other hand, it is an open question whether $n!+1$ is a prime for infinitely many values of $n$. The only values of $n \leq 100$ for which $n!+1$ is known to be a primes are $n = 1, 2, 3, 11, 27, 37, 41, 73, 77$. Currently, the largest prime of the form $n!+1$ is $422429!+1$ which has 2193027 digits and it was discovered in 2022. A prime of the form $n!+1$ is called a *factorial prime*.

CHAPTER 3

# Number-Theoretic Functions and Euler's Theorem

## 3.1 The sum and the number of divisors

**Definition 3.1.1**

Given a positive integer $n$, let $\tau(n)$ denote the number of positive divisors of $n$ and $\sigma(n)$ denote the sum of these divisors.

For example, $n = 12$ has divisors $1,2,3,4,6,12$ and so

$$\tau(12) = 6 \quad \text{and} \quad \sigma(12) = 1+2+3+4+6+12 = 28.$$

For the first few integers,

$$r(l) = 1, \tau(2) = 2, \tau(3) = 2, \tau(4) = 3, \tau(S) = 2, \tau(6) = 4, \ldots$$

and

$$\sigma(l) = 1, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 7, \sigma(5) = 6, \sigma(6) = 12, \ldots.$$

It is easy to see that, $\tau(n) = 2$ if and only if $n$ is a prime number and $\sigma(n) = n+1$ if and only if $n$ is a prime.

In the summation notation,

$$\tau(n) = \sum_{d|n} 1 \text{ and } \sigma(n) = \sum_{d|n} d.$$

For example, 10 has divisors $1,2,5,10$ and hence

$$\tau(10) = \sum_{d|10} 1 = 4 \text{ and } \sigma(10) = \sum_{d|10} d = 1+2+5+10 = 18.$$

The following result gives an easy way to obtain the positive divisors of a positive integer $n$ from its prime factorization.

**Theorem 3.1.2**

If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of $n$ are precisely those integers $d$ of the form

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

where $0 \leq a_i \leq k_i$ $(i = 1, 2, \ldots, r)$.

*Proof.* Note that $d = 1$ is obtained when $a_1 = a_2 = \cdots = a_r = 0$, and $n$ itself is obtained when $a_1 = k_1, a_2 = k_2, \ldots a_r = k_r$. Suppose $d$ is a non-trivial divisor of $n$, say $n = dd'$, where $d > 1$, $d' > 1$. We express both $d$ and $d'$ as a product of primes, not necessarily distinct, as follows.

$$d = q_1 q_2 \cdots q_s \quad \text{and} \quad d' = t_1 t_2 \cdots t_u$$

with $q_i, t_j$ prime. Then

$$p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = q_1 q_2 \cdots q_s t_1 t_2 \cdots t_u$$

are two prime factorizations of the positive integer $n$. By the uniqueness of the prime factorization, each prime $q_i$ must be one of the $p_j$. Collecting the equal primes into a single integral power, we get

$$d = q_1 q_2 \cdots q_s = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

where the possibility of $a_i = 0$ is allowed.

Conversely, every number $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, $(0 \leq a_i \leq k_i)$ turns out to be a divisor of $n$ since we can write

$$\begin{aligned} n &= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \\ &= \left(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}\right) \left(p_1^{k_1 - a_1} p_2^{k_2 - a_2} \cdots p_r^{k_r - a_r}\right) \\ &= dd' \end{aligned}$$

with $d' = p_1^{k_1 - a_1} p_2^{k_2 - a_2} \cdots p_r^{k_r - a_r}$ and $k_i - a_i \geq 0$ for each $i$. Then $d' > 0$ and $d \mid n$. □

As a consequence of the above theorem, we have the following result.

**Theorem 3.1.3**

If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then

(a) $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$

(b) $\sigma(n) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}.$

*Proof.* By the above theorem, we know that the positive divisors of $n$ are precisely those integers

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

where $0 \leq a_i \leq k_i$. There are $k_1 + 1$ choices for the exponent $a_1$, $k_2 + 1$ choices for $a_2$, ..., and $k_r + 1$ choices for $a_r$. Hence, there are

$$(k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$$

possible divisors of $n$.

To evaluate $\sigma(n)$, consider the product

$$\left(1 + p_1 + p_1^2 + \cdots p_1^{k_1}\right)\left(1 + p_2 + p_2^2 + \cdots p_2^{k_2}\right) \cdots \left(1 + p_r + p_r^2 + \cdots p_r^{k_r}\right).$$

Each positive divisor of $n$ appears once and only once as a term in the expansion of this product. So,

$$\sigma(n) = \left(1 + p_1 + p_1^2 + \cdots p_1^{k_1}\right)\left(1 + p_2 + p_2^2 + \cdots p_2^{k_2}\right) \cdots \left(1 + p_r + p_r^2 + \cdots p_r^{k_r}\right).$$

Applying the formula for the sum of a finite geometric series to the $i$-th factor on the right-hand side, we get

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

Thus, it follows that

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}.$$

□

If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then in terms of the product notation, we have

$$\tau(n) = \prod_{1 \leq i \leq r} (k_i + 1) \quad \text{and} \quad \sigma(n) = \prod_{1 \leq i \leq r} \frac{p_i^{k_i+1} - 1}{p_i - 1}.$$

**Example 3.1.4.** The number $180 = 2^2 \cdot 3^2 \cdot 5$ has

$$\tau(n) = (2+1)(2+1)(1+1) = 18$$

positive divisors which are integers of the form $2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3}$, where $a_1 = 0, 1, 2$; $a_2 = 0, 1, 2$; and $a_3 = 0, 1$. Specifically, these divisors are

$$1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180.$$

The sum of these divisors is

$$\sigma(180) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = \frac{7}{1} \frac{26}{2} \frac{24}{4} = 7 \cdot 13 \cdot 6 = 546.$$

An interesting property of the divisor function $\tau$ is that the product of all the positive divisors of an integer $n > 1$ is equal to $n^{\tau(n)/2}$. To see this, let $d$ be an arbitrary positive divisor of $n$. Then $n = dd'$ for some integer $d'$. As $d$ runs over all the $\tau(n)$ positive divisors of $n$, there are $\tau(n)$ equations of the form $n = dd'$. Multiplying them, we get

$$n^{\tau(n)} = \prod_{d|n} d \cdot \prod_{d'|n} d'.$$

But as $d$ run through the divisors of $n$, so does $d'$. Hence, $\prod_{d|n} d = \prod_{d'|n} d'$. Therefore,

$$n^{\tau(n)} = \left(\prod_{d|n} d\right)^2$$

or equivalently

$$n^{\tau(n)/2} = \prod_{d|n} d.$$

Note that this formula makes sense because the left hand side is always an integer. If $\tau(n)$ is even, then clearly there is no problem. If $\tau(n)$ is odd, it is easy to see that $n$ is a perfect square, say $n = m^2$ for some integer $m$, then the left hand side becomes $n^{\tau(n)/2} = m^{\tau(n)}$.

As an example, the product of the divisors of 16 (namely 1, 2, 4, 8, 16) is

$$\prod_{d|16} d = 16^{\tau(16)/2} = 16^{5/2} = 4^5 = 1024.$$

**Definition 3.1.5: Multiplicative function**

A number theoretic function $f$ is said to be *multiplicative* if

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

whenever $\gcd(m,n) = 1$.

The function $f(n) = 1$ and $g(n) = n$ for all $n \geq 1$ are clearly multiplicative functions. By induction, if follows that if $f$ is multiplicative and $n_1, n_2, \ldots, n_r$ are positive integers that are pairwise relatively prime, then

$$f(n_1 n_2 \cdots n_r) = f(n_1)f(n_2)\cdots f(n_r).$$

An advantage of multiplicative function is that they are completely determined by their values at prime powers. If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then $\gcd(p_i^{k_i}, p_j^{k_j}) = 1$ for all $i \neq j$ and so the multiplicative property of $f$ gives

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

If $f$ is a multiplicative function which is not identically zero, then there is an integer $n$ such that $f(n) \neq 0$. But

$$f(n) = f(n \cdot 1) = f(n)f(1).$$

Since $f(n) \neq 0$, it can be cancelled out from both the sides, we get $f(1) = 1$. Thus, for any multiplicative function $f$ which is not identically zero, we always have $f(1) = 1$.

Now, we show that $\tau$ and $\sigma$ are multiplicative.

**Theorem 3.1.6**

The functions $\tau$ and $\sigma$ are both multiplicative functions.

*Proof.* Let $m$ and $n$ be relatively prime integers, i.e., $\gcd(m,n) = 1$. Since the result is trivially true if $m = 1$ or $n = 1$, we may assume that $m > 1$ and $n > 1$. If

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \quad \text{and} \quad n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

are the prime factorizations of $m$ and $n$, then since $\gcd(m,n) = 1$, no $p_i$ can occur among the $q_j$. It thus follows that the prime factorization of the product $mn$ is given by

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}.$$

Then by Theorem 3.1.3, we get

$$\begin{aligned} \tau(mn) &= [(k_1+1)(k_2+1)\cdots(k_r+1)][(j_1+1)(j_2+1)\cdots(j_s+1)] \\ &= \tau(m)\tau(n). \end{aligned}$$

Similarly, Theorem 3.1.3 gives

$$\begin{aligned} \sigma(m)\sigma(n) &= \left[\frac{p_1^{k_1+1}-1}{p_1-1}\frac{p_2^{k_2+1}-1}{p_2-1}\cdots\frac{p_r^{k_r+1}-1}{p_r-1}\right]\left[\frac{q_1^{j_1+1}-1}{q_1-1}\frac{q_2^{j_2+1}-1}{q_2-1}\cdots\frac{q_r^{j_s+1}-1}{q_s-1}\right] \\ &= \sigma(m)\sigma(n) \end{aligned}$$

Thus, $\tau$ and $\sigma$ are multiplicative functions. □

We prove a general result on multiplicative functions for which first we prove the following lemma.

**Lemma 3.1.7**

If $\gcd(m,n) = 1$, then the set of positive divisors of $mn$ consists of all the products $d_1 d_2$, where $d_1 \mid m$, $d_2 \mid n$, and $\gcd(d_1,d_2) = 1$. Furthermore, these products are all distinct.

*Proof.* The result is trivial if $m = 1$ or $n = 1$. So, we may assume that $m > 1$ and $n > 1$. Let $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and $n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$ be the prime factorizations of $m$ and $n$. Since $\gcd(m,n) = 1$, the primes $p_1,\ldots,p_r,q_1,\ldots,q_s$ are all distinct, and so the prime factorization of $mn$ is

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}.$$

Hence, any positive divisor $d$ of $mn$ can be uniquely represented as

$$d = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} \qquad 0 \le a_i \le k_i, 0 \le b_i \le j_i.$$

Then we can write $d$ as $d = d_1 d_2$, where $d_1 = p_1^{a_1} \cdots p_r^{a_r}$ is a divisor of $m$ and $d_2 = q_1^{b_1} \cdots q_s^{b_s}$ is a divisor of $n$. Since no $p_i$ is equal to any $q_j$, we must have $\gcd(d_1,d_2) = 1$. □

**Theorem 3.1.8**

If $f$ is a multiplicative function and $F$ is defined by

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

then $F$ is also multiplicative.

*Proof.* Let $m$ and $n$ be relatively prime integers, i.e., $\gcd(m,n) = 1$. Then

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) \end{aligned}$$

because by the above lemma, every divisor of $mn$ can be uniquely written as a product of a divisor $d_1$ of $m$ and a divisor $d_2$ of $n$, where $\gcd(d_1,d_2) = 1$. Since $f$ is multiplicative, we have

$$f(d_1 d_2) = f(d_1) f(d_2).$$

Therefore, it follows that

$$\begin{aligned} F(mn) &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) \\ &= \left( \sum_{d_1|n} f(d_1) \right) \left( \sum_{d_2|n} f(d_2) \right) \\ &= F(m)F(n). \end{aligned}$$

□

Let us consider an example to go through the proof of the above theorem in a concrete case. Let $m = 8$ and $n = 3$. Then we have

$$\begin{aligned} F(8.3) &= \sum_{d|24} f(d) \\ &= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(l2) + f(24) \\ &= f(1\cdot 1) + f(2\cdot 1) + f(1\cdot 3) + f(4\cdot 1) + f(2\cdot 3) + f(8\cdot 1) \\ &\quad + f(4\cdot 3) + f(8\cdot 3) \\ &= f(1)f(1) + f(2)f(1) + f(1)f(3) + f(4)f(1) + f(2)f(3) \\ &\quad + f(8)f(1) + f(4)f(3) + f(8)f(3) \\ &= [f(1) + f(2) + f(4) + f(8)][f(1) + f(3)] \\ &= \sum_{d|8} f(d) \cdot \sum_{d|3} f(d) = F(8)F(3). \end{aligned}$$

**Corollary 3.1.9**

The functions $\tau$ and $\sigma$ are multiplicative functions.

*Proof.* As mentioned earlier, we know that the constant function $f(n) = 1$ for all $n$ is multiplicative and the identity function $f(n) = n$ for all $n$ is multiplicative. Since $\tau$ and $\sigma$ are represented as

$$\tau(n) = \sum_{d|n} 1 \quad \text{and} \quad \sigma(n) = \sum_{d|n} d,$$

the result immediately follows from the above theorem. □

## 3.2 The Möbius Inversion Formula

**Definition 3.2.1**

For a positive integer $n$, define $\mu$ by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ where } p_i \text{ are distinct primes.} \end{cases}$$

Definition 3.2.1 states that $\mu(n) = 0$ if $n$ is not a square free integer, whereas $\mu(n) = (-1)^r$ if $n$ is a square-free integer with $r$ prime factors. For example, $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$. The first few values of $\mu$ are

$$\mu(1) = 1,\ \mu(2) = -1,\ \mu(3) = -1,\ \mu(4) = 0,\ \mu(5) = -1,\ \mu(6) = 1, \ldots.$$

If $p$ is a prime, then $\mu(p) = -1$. Also, $\mu(p^k) = 0$ if $k \geq 2$.

**Theorem 3.2.2**

The function $\mu$ is a multiplicative function.

*Proof.* We want to show that $\mu(mn) = \mu(m)\mu(n)$ for all $m$ and $n$ relatively prime. If either $p^2 \mid m$ or $p^2 \mid n$, where $p$ is a prime, then $p^2 \mid mn$. Then $\mu(mn) = 0 = \mu(m)\mu(n)$ and the formula holds trivially. So, assume that both $m$ and $n$ are square-free integers.

Let $m = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$, with all the primes $p_i$ and $q_j$ are distinct. Then

$$\mu(mn) = \mu(p_1 \cdots p_r q_1 \cdots q_s) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n).$$

This completes the proof. □

**Theorem 3.2.3**

For each positive integer $n \geq 1$,

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

where $d$ run through the positive divisors of $n$.

*Proof.* For $n = 1$, it is clear that $\sum_{d \mid 1} \mu(d) = \mu(1) = 1$.

Suppose that $n > 1$. Put

$$F(n) = \sum_{d \mid n} \mu(d).$$

First we calculate $F(n)$ for the prime powers, i.e., for $n = p^k$. The positive divisors of $p^k$ are just the $k+1$ integers $1, p, p^2, \ldots, p^k$. So,

$$\begin{aligned} F(p^k) = \sum_{d|p^k} \mu(d) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) \\ &= \mu(1) + \mu(p) + 0 + \cdots + 0 \\ &= 1 + (-1) = 0. \end{aligned} \tag{3.1}$$

By Theorem 3.2.2, we know $\mu$ is multiplicative. Then, by Theorem 3.1.8, $F(n) = \sum_{d|n} \mu(d)$ is multiplicative. Thus, if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n$, then by the multiplicativity of $F$ and by (3.1), we have

$$F(n) = F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r}) = 0.$$

This completes the proof. □

As an example, consider $n = 10$. The positive divisors of 10 are $1, 2, 5, 10$ and the sum in the above theorem is

$$\begin{aligned} \sum_{d|10} \mu(d) &= \mu(1) + \mu(2) + \mu(5) + \mu(10) \\ &= 1 + (-1) + (-1) + 1 = 0. \end{aligned}$$

The following result shows the significance of the Möbius function $\mu$.

**Theorem 3.2.4: Möbius inversion formula**

Let $F$ and $f$ be two number-theoretic functions related by the formula

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

Then

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$$

*Proof.* Note that the two sums in the conclusion of the theorem are essentially the same as one is obtained from the other on replacing the index $d$ by $d' = \frac{n}{d}$; as $d$ runs over all positive divisors of $n$, so does $d'$.

Carrying out the required computation, we get

$$\begin{aligned} \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \left( \mu(d) \sum_{c|(n/d)} f(c) \right) \\ &= \sum_{d|n} \left( \sum_{c|(n/d)} \mu(d) f(c) \right). \end{aligned} \tag{3.2}$$

It can be easily checked that $d \mid n$ and $c \mid (n/d)$ if and only if $c \mid n$ and $d \mid (n/c)$ (**Check!**). Consequently, the last expression in (3.2) becomes

$$\begin{aligned}\sum_{d|n}\left(\sum_{c|(n/d)}\mu(d)f(c)\right) &= \sum_{c|n}\left(\sum_{d|(n/c)}f(c)\mu(d)\right)\\ &= \sum_{c|n}\left(f(c)\sum_{d|(n/c)}\mu(d)\right). \qquad (3.3)\end{aligned}$$

By the above theorem, the sum $\displaystyle\sum_{d|(n/c)}\mu(d)$ must vanish except when $\frac{n}{c}=1$, i.e., when $n=c$, in which case it is equal to 1. As a result, the right-hand side of (3.3) simplifies to

$$\begin{aligned}\sum_{c|n}\left(f(c)\sum_{d|(n/c)}\mu(d)\right) &= \sum_{c=n}f(c)\cdot 1\\ &= f(n).\end{aligned}$$

This completes the proof. □

Let us take $n=10$ to see how the double sum in (3.3) is turned around. We find that

$$\begin{aligned}\sum_{d|10}\left(\sum_{c|(10/d)}\mu(d)f(c)\right) &= \mu(1)[f(1)+f(2)+f(5)+f(10)]+\mu(2)[f(1)+f(5)]\\ &\quad +\mu(5)[f(1)+f(2)]+\mu(10)f(1)\\ &= f(1)[\mu(1)+\mu(2)_{\mu}(5)+\mu(10)]+f(2)[\mu(1)+\mu(5)]\\ &\quad +f(5)[\mu(1)+\mu(2)]+f(10)\mu(1)\\ &= \sum_{c|10}\left(\sum_{d|(10/c)}f(c)\mu(d)\right).\end{aligned}$$

To see how the Möbius inversion formula works in a particular case, recall the summation formula of the functions $\tau$ and $\sigma$ given below.

$$\tau(n)=\sum_{d|n}1 \quad \text{and} \quad \sigma(n)=\sum_{d|n}d.$$

Theorem 3.2.4 tells us that these formulas may be inverted to give

$$1=\sum_{d|n}\mu\left(\frac{n}{d}\right)\tau(d) \quad \text{and} \quad n=\sum_{d|n}\mu\left(\frac{n}{d}\right)\sigma(d)$$

which are valid for all $n\geq 1$.

Recall that Theorem 3.1.8 tells us that if $f$ is multiplicative, then so is $F(n)=\displaystyle\sum_{d|n}f(d)$. Naturally, one might ask the converse, i.e., if $F$ is multiplicative, then will it force $f$ to be multiplicative. This is also true and can be proved with the help of the inversion formula.

**Theorem 3.2.5**

If $F$ is a multiplicative function and

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

then $f$ is also multiplicative.

*Proof.* Let $m$ and $n$ be relatively prime positive integers, i.e., $\gcd(m,n) = 1$. Recall Lemma 3.1.7 which states that any divisor $d$ of $mn$ can be uniquely written as $d = d_1 d_2$, where $d_1 \mid m$, $d_2 \mid n$, and $\gcd(d_1, d_2) = 1$. Thus, using the inversion formula,

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

This completes the proof. □

Note that, along with the inversion formula, the multiplicative character of $\mu$ and $F$ are crucial in the above proof.

## 3.3 The Greatest Integer Function

**Definition 3.3.1: The Greatest Integer Function**

For an arbitrary real number $x$, we denote by $[x]$, the largest integer less than or equal to $x$. That is, $[x]$ is the unique integer satisfying $x - 1 < [x] \leq x$.

For example, $[-3/2] = -2$, $[\sqrt{2}] = 1$, $[1/3] = 0$, $[\pi] = 3$, $[\pi] = -4$.

The important observation is that $[x] = x$ if and only if $x$ is an integer. Also, Definition 3.3.1 makes it clear that any real number $x$ can be written as

$$x = [x] + \theta$$

for a suitable choice of $\theta$, with $0 \leq \theta < 1$.

We now investigate how many times a particular prime $p$ appears in $n!$. For example, $p = 3$ appears 4 times in $n!$ for $n = 9$ as

$$9! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 = 2^7 \cdot 3^4 \cdot 5 \cdot 7.$$

It is desirable to have a formula for this number without actually having to write the product of $n!$. This is given in the following theorem.

**Theorem 3.3.2**

If $n$ is a positive integer and $p$ is a prime, then the exponent of the highest power of $p$ that divides $n!$ is

$$\sum_{k=1}^{\infty} \left[ \frac{n}{p^k} \right],$$

where the series is finite, because $\left[ \frac{n}{p^k} \right] = 0$ for $p^k > n$.

*Proof.* Among the first $n$ positive integers, those which are divisible by $p$ are $p, 2p, \ldots, tp$, where $t$ is the largest integer such that $tp \leq n$. In other words, $t$ is the largest integer less than or equal to $\frac{n}{p}$ (i.e., $t = \left[ \frac{n}{p} \right]$). Thus, there are exactly $\left[ \frac{n}{p} \right]$ multiples of $p$ occurring in the product of $n!$, namely,

$$p, 2p, \ldots, \left[ \frac{n}{p} \right] p. \tag{3.4}$$

The exponent of $p$ in the prime factorization of $n!$ is obtained by adding the number of integers in (3.6), the number of integers among $1, 2, \ldots, n$ which are divisible by $p^2$, and the number of integers upto $n$ which are divisible by $p^3$, and so on. Arguing as above, the integers between 1 and $n$ that are divisible by $p^2$ are

$$p^2, 2p^2, \ldots, \left[ \frac{n}{p^2} \right] p^2. \tag{3.5}$$

which are $\left[ \frac{n}{p^2} \right]$ in number. Again, among these, the $\left[ \frac{n}{p^3} \right]$ integers which are divisible by $p^3$ are

$$p^3, 2p^3, \ldots, \left[ \frac{n}{p^3} \right] p^3. \tag{3.6}$$

Continuing this process, after a finite number of repetitions, we can conclude that the total number of times $p$ divides $n!$ is

$$\sum_{k=1}^{\infty} \left[ \frac{n}{p^k} \right].$$

This completes the proof. □

The above result can be stated as the following equation which is often called the *Legendre formula*.

$$n! = \prod_{p \leq n} p^{\sum_{k=1}^{\infty} \left[ n/p^k \right]}.$$

**Example 3.3.3.** Let us find the number of zeros with which the decimal representation of 50! terminates, i.e., the number of zeros at the end of 50!. Thus, we have to determine the number of times 10 appears in the product 50! which is equivalent to find the exponents of 2 and 5 in the prime factorization of 50!, and then choose the smallest exponent among the two.

By a direct calculation, we see that

$$\begin{aligned}[50/2]+\left[50/2^2\right]+\left[50/2^3\right]+\left[50/2^4\right]+\left[50/2^5\right] &\\ &= 25+12+6+3+1\\ &= 47.\end{aligned}$$

Thus, Theorem 3.3.2 says that $2^{47} \mid 50!$, but $2^{48} \nmid 50!$, i.e., the highest power of 2 dividing 50! is 47. Similarly,

$$[50/5]+\left[50/5^2\right] = 10+2 = 12.$$

Thus, the highest power of 5 dividing 50! is 12. The minimum of 47 and 12 is 12. Thus, the number of zeros in 50! (i.e., the powers of 10 in 50!) is 12.

Theorem 3.3.2 can be used to prove that the binomial coefficient is an integer.

**Theorem 3.3.4**

If $n$ and $r$ are positive integers with $1 \leq r < n$, then the binomial coefficient

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

is also an integer.

*Proof.* The argument of this result depends on the observation that if $a$ and $b$ are arbitrary real numbers, then $[a+b] \geq [a]+[b]$. In particular, for each prime factor $p$ of $r!(n-r)!$, we have

$$\left[\frac{n}{p^k}\right] \geq \left[\frac{r}{p^k}\right] + \left[\frac{(n-r)}{p^k}\right], \quad k = 1,2,\ldots.$$

Adding these inequalities, we get

$$\sum_{k\geq 1}\left[\frac{n}{p^k}\right] \geq \sum_{k\geq 1}\left[\frac{r}{p^k}\right] + \sum_{k\geq 1}\left[\frac{(n-r)}{p^k}\right]. \tag{3.7}$$

Note that, the left-hand side of (3.7) gives the highest power of the prime $p$ that divides $n!$, whereas the right-hand side gives the highest power of this prime contained in the product $r!(n-r)!$. Hence, a prime $p$ appears in the numerator of $\frac{n!}{r!(n-r)!}$ at least as many times as it occurs in its denominator. Sine this is true for every prime divisor of the denominator, $r!(n-r)!$ must divide $n!$, thereby making $\frac{n!}{r!(n-r)!}$ an integer. This completes the proof. □

**Corollary 3.3.5**

For a positive integer $r$, the product of any $r$ consecutive positive integers is divisible by $r!$.

*Proof.* The product of $r$ consecutive positive integers, the largest of which is $n$, is

$$n(n-1)(n-2)\cdots(n-r+1).$$

Note that

$$n(n-1)\cdots(n-r+1) = \left(\frac{n!}{r!(n-r)!}\right) r!.$$

Since $\frac{n!}{r!(n-r)!}$ is an integer by the above theorem, it follows that $r!$ must divide the product on the left-hand side, i.e., $r! \mid n(n-1)\cdots(n-r+1)$. This completes the proof. □

The following result related the greatest integer function in the study of number-theoretic functions.

**Theorem 3.3.6**

Let $f$ and $F$ be number-theoretic functions such that

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

Then, for any positive integer $N$,

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right].$$

*Proof.* Note that

$$\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N} \sum_{d|n} f(d). \tag{3.8}$$

We collect the terms with equal values of $f(d)$ in the double sum in (3.8). For a fixed positive integer $k \leq N$, the term $f(k)$ appears in $\sum_{d|n} f(d)$ if and only if $k$ is a divisor of $n$. (Since the previous sum runs over $n$ and each integer is a divisor of itself, the right-hand side of (3.8) includes $f(k)$ at least once.)

Now, to calculate the number of sums $\sum_{d|n} f(d)$ in which $f(k)$ occurs as a term, it suffices to find the number of integers among $1, 2, \ldots, N$, which are divisible by $k$. There are exactly $\left[\frac{N}{k}\right]$ such integers which are:

$$k, 2k, 3k, \ldots, \left[\frac{N}{k}\right] k.$$

Thus, for each $k$ with $1 \leq k \leq N$, the number $f(k)$ appears as a term in the sum $\sum_{d|n} f(d)$ for $\left[\frac{N}{k}\right]$ different positive integers less than or equal to $N$. Consequently, the double sum in (3.8) can be rewritten as

$$\sum_{n=1}^{N} \sum_{d|n} f(d) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right].$$

This completes our proof. □

As an immediate consequence, we have the following result.

**Corollary 3.3.7**

If $N$ is a positive integer, then

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right].$$

*Proof.* Note that $\tau(n) = \sum_{d|n} 1$. In the above theorem, taking $\tau$ for $F$ and taking $f$ to be the constant function $f(n) = 1$ for all $n$ (and writing the index $n$ instead of $k$ in the summation on the right-hand side), the result follows. □

Similarly, the relation $\sigma(n) = \sum_{d|n} d$ gives the following Corollary.

**Corollary 3.3.8**

If $N$ is a positive integer, then

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n\left[\frac{N}{n}\right].$$

**Example 3.3.9.** Consider the case $N = 6$. The definition $\tau$ gives us that

$$\sum_{n=1}^{6} \tau(n) = 14.$$

From Corollary 3.3.7, we have

$$\begin{aligned}\sum_{n=1}^{6} \left[\frac{6}{n}\right] &= [6] + [3] + [2] + [3/2] + [6/5] + [1] \\ &= 6+3+2+1+1+1 \\ &=14\end{aligned}$$

as computed above.

In this case, we also have

$$\sum_{n=1}^{6} \sigma(n) = 33.$$

A simple calculation leads to

$$\begin{aligned}\sum_{n=1}^{6} n\left[\frac{6}{n}\right] &= 1[6] + 2[3] + 3[2] + 4[3/2] + 5[6/5] + 6[1] \\ &= 1\cdot 6 + 2\cdot 3 + 3\cdot 2 + 4\cdot 1 + 5\cdot 1 + 6\cdot 1 \\ &=33.\end{aligned}$$

## 3.4 Euler's Phi-function

**Definition 3.4.1: Euler's $\phi$-function**

For $n \geq 1$, $\phi(n)$ denotes the number of positive integers not exceeding $n$ that are relatively prime to $n$.

For example, $\phi(10) = 4$, since $1, 3, 7, 9$ are the four positive integers that are relatively prime to 10. Similarly,

$$\phi(1) = 1,\ \phi(2) = 1,\ \phi(3) = 2,\ \phi(4) = 2,\ \phi(5) = 4,\ \phi(6) = 2,\ \phi(7) = 6,\ \phi(8) = 4, \ldots.$$

Note that, $\phi(1) = 1$ as $\gcd(1,1) = 1$. Hence for $n > 1$, $\phi(n)$ can be defined as the number of positive integers less than $n$ that are relatively prime to $n$. The function $\phi$ is called the *Euler's phi-function* or the *Euler's totient function*.

Observe that if $n$ is prime, then every positive integer less than $n$ is relatively prime to $n$. Hence $\phi(n) = n - 1$. On the other hand, if $n$ is composite, then it has a divisor $d$ such that $1 < d < n$. Thus, if $n$ is composite, then at least two integers among $1, 2, \ldots, n$ are not relatively prime to $n$. Hence, in this case $\phi(n) \leq n - 2$. Thus for $n > 1$, we have

$$\phi(n) = n - 1 \quad \text{if and only if } n \text{ is prime.}$$

In the next few results, we derive a formula to compute $\phi(n)$.

**Theorem 3.4.2**

If $p$ is prime and $k > 0$, then

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

*Proof.* By definition $\phi(p^k)$ is the number of integers among $1, 2, \ldots, p^k$ that are relatively prime to $p^k$. The idea is to remove those integers, from total $p^k$ integers, that are not relatively prime to $p^k$.

Observe that $\gcd(n, p^k) = 1$ if and only if $p \nmid n$. This means that if $n$ is relatively prime to $p^k$, then $n$ is not a multiple of $p$. The multiples of $p$ upto $p^k$ are

$$p, 2p, 3p, \ldots, p \cdot p, (p+1) \cdot p, \ldots, p^{k-1} \cdot p.$$

Thus, the number of integers in the set $\{1, 2, \ldots, p^k\}$ which are divisible by $p$ is $p^{k-1}$. Hence, the number of integers in that set which are relatively prime to $p^k$ is exactly $p^k - p^{k-1}$. Therefore, by the definition of the $\phi$-function, $\phi(p^k) = p^k - p^{k-1}$. □

For example, $\phi(9) = \phi(3^2) = 3^2 - 3 = 6$. Similarly, $\phi(16) = \phi(2^4) = 2^4 - 2^3 = 8$.

Having the formula to compute the phi-function at prime powers, we can compute $\phi(n)$ for all integers $n$ based on prime factorization of $n$ if we can show that $\phi$ is a multiplicative function.

**Theorem 3.4.3**

The function $\phi$ is multiplicative.

*Proof.* We have to show that if $m$ and $n$ are relatively prime integers, then $\phi(mn) = \phi(m)\phi(n)$. This is an easy consequence of the Chinese Remainder Theorem. Consider

$$C_t := \{k \in \mathbb{N} \mid k \leq t,\ \gcd(k,t) = 1\}.$$

Thus, $C_t$ contains $\phi(t)$ elements. We prove the result by showing that $C_{mn}$ and $C_m \times C_n$ have the same number of elements. For this, we show a one-one correspondence between the two sets. Define

$$f : C_{mn} \to C_m \times C_n \quad \text{by} \quad f(a) := (a \bmod m,\ a \bmod n).$$

First we show that $f$ is one-one. Let $a, b \in C_{mn}$ with $a > b$ such that $f(a) = f(b)$, i.e.

$$(a \bmod m,\ a \bmod n) = (b \bmod m,\ b \bmod n).$$

Hence, $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$. This implies, $m \mid (a-b)$ and $n \mid (a-b)$. Since $\gcd(m,n) = 1$, by Corollary 1.2.10, $mn \mid (a-b)$ and so $mn \leq (a-b)$ which is a contradiction as $0 < a-b < mn$. Hence, $a = b$.

Now, we show that $f$ is onto. Let $(a,b) \in C_m \times C_n$. We have to find an element $c \in C_{mn}$ such that $f(c) = (a,b)$, i.e. $(c \bmod m, c \bmod n) = (a,b)$. Thus, we have to find an integer $c \in C_{mn}$ such that $c \equiv a \pmod{m}$ and $c \equiv b \pmod{n}$. Since $\gcd(m,n) = 1$, by Chinese Remainder Theorem there exists such $c \in \mathbb{Z}_{mn}$. Since $\gcd(c,m) = 1$ and $\gcd(c,n) = 1$ (by the following lemma), $\gcd(c,mn) = 1$. Hence, $c \in C_{mn}$ and $f$ is onto. □

Now, it remains to show that if $\gcd(c,m) = 1$ and $\gcd(c,n) = 1$, then $\gcd(c,mn) = 1$. The following lemma proves this part as well as its converse.

**Lemma 3.4.4**

For integers $c, m, n$, $\gcd(c,mn) = 1$ if and only if $\gcd(c,m) = 1$ and $\gcd(c,n) = 1$.

*Proof.* First assume that $\gcd(c,mn) = 1$ and $\gcd(c,m) = d$. Then $d \mid c$ and $d \mid m$ and hence $d \mid c$ and $d \mid mn$. This implies $\gcd(c,mn) \geq d$ and hence we must have $d = 1$, i.e. $\gcd(c,m) = 1$. Similarly, $\gcd(c,n) = 1$.

Conversely, assume that $\gcd(c,m) = 1$ and $\gcd(c,n) = 1$. Suppose $\gcd(c,mn) = d' > 1$ and $p$ be a prime divisor of $d'$. Since $d' \mid mn$, we have $p \mid mn$ and $p$ being prime $p \mid m$ or $p \mid n$. If $p \mid m$, then since $p \mid c$, $\gcd(c,m) \geq p$ which is not possible. Similarly, if $p \mid n$ then $\gcd(c,n) \geq p$ which is again not possible. Hence, $d'$ has no such prime divisor $p$. Therefore, $d' = 1$ or $\gcd(c,mn) = 1$. □

As an immediate consequence of the above theorem, we have the following result.

**Theorem 3.4.5**

If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then

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

*Proof.* We prove the result by using induction on $r$, the number of distinct prime factors of $n$. By Theorem 3.4.2, the result is true for $r = 1$.

Suppose that the result holds for $r = i$.

Since $\gcd\left(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}, p_{i+1}^{k_{i+1}}\right) = 1$, the definition of multiplicative function gives

$$\begin{aligned}\phi\left(\left(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}\right) p_{i+1}^{k_{i+1}}\right) &= \phi\left(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}\right)\phi\left(p_{i+1}^{k_{i+1}}\right)\\ &= \phi\left(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}\right)\left(p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1}\right).\end{aligned}$$

Using the induction hypothesis to expand the first factor on the right-hand side of the above expression, we get

$$\phi\left(\left(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}\right) p_{i+1}^{k_{i+1}}\right) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\cdots\left(p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1}\right).$$

This completes the proof.

Now, for $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, where $p_i$'s $(i = 1, 2, \ldots, r)$ are distinct primes, we have

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

where the above product is over the distinct prime factors of $n$. □

**Example 3.4.6.** We compute $\phi(100)$. Writing prime factorization of $100 = 2^2 \cdot 5^2$, we get

$$\phi(100) = 100 \cdot \left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40.$$

As computed above, $\phi(100) = 40$ is an even number. Observe that, except for $\phi(1) = 1$ and $\phi(2) = 1$, for all $n \geq 3$, $\phi(n)$ is an even integer. We have the following result.

**Theorem 3.4.7**

For $n > 2$, $\phi(n)$ is an even integer.

*Proof.* If $n$ is a power of 2, i.e. $n = 2^k$ with $k \geq 2$ (as $n > 2$), then by the above corollary,

$$\phi(n) = \phi(2^k) = 2^k\left(1 - \frac{1}{2}\right) = 2^{k-1}$$

is an even integer. If $n$ is not a power of 2, then $n$ is divisible by some odd prime $p$. Then $n$ can be written as $n = p^k m$ for some integer $k \geq 1$ and for some integer $m$ such that $\gcd(p^k, m) = 1$. Since $\phi$ is multiplicative, we have

$$\phi(n) = \phi(p^k m) = \phi(p^k)\phi(m) = p^{k-1}(p-1)\phi(m).$$

Since $p$ is an odd prime, $2 \mid p-1$ and hence $\phi(n)$ is even. □

An alternative proof of the above result can be given as follows:

*Alternative proof.* . Its an easy exercise to show that If $1 \leq k \leq n$ such that $\gcd(k,n) = 1$, then $\gcd(n-k,n) = 1$. Thus, for every integer $k$ relatively prime to $n$ there is another integer $n-k$ which is also relatively prime to $n$, i.e. they occur in pairs $\{k, n-k\}$. The pairing is not possible only when $k = n-k$ in which case $n = 2k$. But then $n \mid n \Rightarrow n \mid 2k$ and since $\gcd(n,k) = 1$, we have $n \mid 2$ which is not possible as $n > 2$. Hence, $\phi(n)$ is always an even integer for $n > 2$. □

**Exercise 3.1**

Let $n$ be a positive integer $n$. If $\gcd(k,n) = 1$ for $1 \leq k \leq n$, then $\gcd(n-k,n) = 1$.

**Remark 3.4.8.** Note that the above such pairs $k$ and $n-k$ add up to give $n$. Also, there are $\frac{\phi(n)}{2}$ such pairs. Hence for $n > 1$, the sum of positive integers less than $n$ and relatively prime to $n$ is $\frac{1}{2}n\phi(n)$.

## 3.5 Euler's Theorem

The first published proof of Fermat's theorem ($a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$) was given by Euler in 1736. Late in 1760, he generalized this result to an arbitrary positive integer $n$ in place of a prime $p$. This result is stated as: if $\gcd(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

For example, $n = 30$ and $a = 11$ gives

$$11^{\phi(30)} \equiv 11^8 \equiv (121)^4 \equiv 1^4 \pmod{30}.$$

Before we prove Euler's theorem, we require the following lemma.

**Lemma 3.5.1**

Let $n > 1$ and $\gcd(a,n) = 1$. If $a_1, a_2, \ldots, a_{\phi(n)}$ are the positive integers less than $n$ and relatively prime to $n$, then

$$aa_1, aa_2, \ldots, aa_{\phi(n)}$$

are congruent modulo $n$ to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

*Proof.* Note that no two of the integers $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent modulo $n$. For if $aa_i \equiv aa_j \pmod{n}$ for some $1 \leq i < j \leq \phi(n)$, then the cancellation law gives $a_i \equiv a_j \pmod{n}$, and thus $a_i = a_j$, which is a contradiction. Further, since $\gcd(a_i, n) = 1$ for all $i$ and $\gcd(a, n) = 1$, by Lemma 3.4.4, $\gcd(aa_i, n) = 1$ for all $i$.

Fix on some particular $aa_i$. By Theorem 2.2.1, the congruence $x \equiv aa_i \pmod{n}$ has a unique solution modulo $n$, say $b$. That is, there is a unique integer $b$, $0 \leq b < n$ such that $aa_i \equiv b \pmod{n}$. Sine

$$\gcd(b, n) = \gcd(aa_i, n) = 1,$$

$b$ must be one of the integers $a_1, a_2, \ldots, a_{\phi(n)}$. This proves that the numbers $aa_1, aa_2, \ldots, aa_{\phi(n)}$ and the numbers $a_1, a_2, \ldots, a_{\phi(n)}$ are the same modulo $n$ in some order. This completes the proof. □

**Theorem 3.5.2: Euler**

If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

*Proof.* The result is trivially true for $n = 1$. So, assume that $n > 1$. Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than $n$ that are relatively prime to $n$. Since $\gcd(a, n) = 1$, by the above lemma, it follows that $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order (i.e., not necessarily in the order of appearance). Then

$$\begin{aligned} aa_1 &\equiv a_1' \pmod{n} \\ aa_2 &\equiv a_2' \pmod{n} \\ &\vdots \qquad\qquad \vdots \\ aa_{\phi(n)} &\equiv a_{\phi(n)}' \pmod{n}, \end{aligned}$$

where $a_1', a_2', \ldots, a_{\phi(n)}'$ are the integers $a_1, a_2, \ldots, a_{\phi(n)}$ in some order. On taking the product of the above $\phi(n)$ congruences, we get

$$\begin{aligned} (aa_1)(aa_2)\cdots(aa_{\phi(n)}) &\equiv a_1' a_2' \cdots a_{\phi(n)}' \pmod{n} \\ &\equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n} \end{aligned}$$

and so

$$a^{\phi(n)}(a_1 a_2 \cdots a_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n}.$$

Since $\gcd(a_i, n) = 1$ for each $i$, by Lemma 3.4.4, we have $\gcd(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$. Therefore, dividing both sides of the above congruence by the common factor $a_1 a_2 \cdots a_{\phi(n)}$, we get

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

□

For better understanding of the proof, let us take $n = 9$. The positive integers less than and relatively prime to 9 are

$$1, 2, 4, 5, 7, 8.$$

These integers play the role of $a_1, a_2, \ldots, a_{\phi(n)}$ in the proof of Theorem 3.5.2. If $a = -4$, then the integers $aa_i$ are

$$-4, -8, -16, -20, -28, -32,$$

where, modulo 9, we have

$$-4 \equiv 5,\ -8 \equiv 1,\ -16 \equiv 2,\ -20 \equiv 7,\ -28 \equiv 8,\ -32 \equiv 4.$$

When the above congruences are multiplied together, we get

$$(-4)(-8)(-16)(-20)(-28)(-32) = 5 \cdot 1 \cdot 2 \cdot 7 \cdot 8 \cdot 4 \pmod 9$$

which becomes

$$(1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8)(-4)^6 = (1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8) \pmod 9.$$

Since the six integers $1, 2, 4, 5, 7, 8$ are relatively prime to 9, so is their product, and hence it can be cancelled to obtain

$$(-4)^6 \equiv 1 \pmod 9.$$

The following calculation confirms the validity of the above congruence.

$$(-4)^6 \equiv 4^6 \equiv 64^2 \equiv 1^2 \equiv 1 \pmod 9.$$

Euler's theorem is a generalization of the Fermat's theorem which was proved earlier. If $p$ is a prime, then $\phi(p) = p - 1$, and hence when $\gcd(a, p) = 1$ (equivalently, $p \nmid a$), we get

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

Consequently, we have the following corollary.

**Corollary 3.5.3: Fermat**

If $p$ is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$.

Let us see an example to see the significance of Euler's theorem in reducing large powers modulo $n$.

**Example 3.5.4.** Let us find the last two digits in the decimal expansion of $3^{256}$. This is equivalent to obtaining the smallest non-negative integer to which $3^{256}$ is congruent to modulo 100, i.e., the remainder obtained on dividing $3^{256}$ by 100.

By Example 3.4.6, $\phi(100) = 40$. Since $\gcd(3, 100) = 1$, by Euler's theorem

$$3^{\phi(100)} = 3^{40} \equiv 1 \pmod{100}.$$

By the Division algorithm, $256 = 6 \cdot 40 + 16$, and hence

$$3^{256} \equiv 3^{6 \cdot 40 + 16} \equiv (3^{40})^6 \cdot 3^{16} \equiv 3^{16} \pmod{100}.$$

Thus, our problem reduces to the one of evaluating $3^{16} \pmod{100}$. By successive squaring, we have

$$\begin{aligned} 3^2 &\equiv 9 \pmod{100} \\ 3^4 &\equiv 81 \pmod{100} \\ 3^8 &\equiv 61 \pmod{100} \\ 3^{16} &\equiv 21 \pmod{100}. \end{aligned}$$

There is another way to prove Euler's theorem, which is using the Fermat's theorem we proved earlier. We leave this proof as a seminar exercise and students are advised to refer the reference book.

**Exercise 3.2 [Second Proof of Euler's Theorem]**

Prove Euler's theorem using the Fermat's theorem.

Euler's theorem can be applied to give a different proof of the Chinese Remainder Theorem which is also left as a seminar exercise.

**Exercise 3.3**

Using Euler's theorem prove the Chinese remainder theorem.

As another application of Euler's theorem, we show that if $n$ is an odd integer which is not a multiple of 5, then $n$ divides an integer all of whose digits are equal to 1.

By our assumption ($n$ being an odd integer, not divisible by 5), we have $\gcd(n,10) = 1$. Also, since $\gcd(9,10) = 1$, by Lemma 3.4.4, $\gcd(9n,10) = 1$. Then by Euler's theorem (Theorem 3.5.2), we have

$$10^{\phi(9n)} \equiv 1 \pmod{9n}.$$

Therefore, $10^{\phi(9n)} - 1 = 9nk$ for some integer $k$ or equivalently

$$kn = \frac{10^{\phi(9n)} - 1}{9}.$$

The right-hand side of the above expression is an integer whose digits are all equal to 1 since each digit of the numerator is clearly equal to 9. This proves that $n$ divides an integer having all its digits equal to 1.

## 3.6 Some Properties of the Phi-Function

**Theorem 3.6.1: Gauss**

For each positive integer $n \geq 1$,

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

the sum being extended over all positive divisors of $n$.

*Proof.* The set of integers between 1 and $n$ can be separated into classes (i.e., sets) as follows: For a positive divisor $d$ of $n$, the class $S_d$ contains all the integers $m$ such that $\gcd(m,n) = d$. In mathematical notation, we have

$$S_d = \{m \mid \gcd(m,n) = d;\ 1 \leq m \leq n\}.$$

Now (by Corollary 1.2.9 and Exercise 1.9), $\gcd(m,n) = d$ if and only if $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$. Thus, the number of integers in the class $S_d$ is equal to the number of positive integers not exceeding $\frac{n}{d}$ that are relatively prime with $\frac{n}{d}$. In other words, the number of integers in the class $S_d$ is equal

to $\phi\left(\frac{n}{d}\right)$. By uniqueness of GCD, each of the $n$ integers in the set $\{1,2,\ldots,n\}$ lies in exactly one class $S_d$. Therefore, we have

$$n = \sum_{d|n} \phi\left(\frac{n}{d}\right).$$

But as $d$ run through all the positive divisors of $n$, so does $\frac{n}{d}$. Hence,

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d).$$

This proves the theorem. □

**Example 3.6.2.** Let $n = 10$. Here, the classes $S_d$ are

$$\begin{aligned} S_1 &= \{1,3,7,9\} \\ S_2 &= \{2,4,6,8\} \\ S_5 &= \{5\} \\ S_{10} &= \{10\}. \end{aligned}$$

These classes contain $\phi(10) = 4$, $\phi(5) = 4$, $\phi(2) = 1$, and $\phi(1) = 1$ integers respectively. Therefore,

$$\begin{aligned} \sum_{d|10} \phi(d) &= \phi(10) + \phi(5) + \phi(2) + \phi(1) \\ &= 4 + 4 + 1 + 1 = 10. \end{aligned}$$

Another proof of Theorem 3.6.1 can be given using the fact that $\phi$ is multiplicative. This proof is left as an exercise.

**Exercise 3.4**

Prove Gauss's theorem (Theorem 3.6.1) using the fact that $\phi$ is multiplicative.

There is another interesting identity involving the phi-function which is given below which we have already remarked earlier in Remark 3.4.8.

**Theorem 3.6.3**

For $n > 1$, the sum of the positive integers less than $n$ and relatively prime to $n$ is $\frac{1}{2}n\phi(n)$.

*Proof.* Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than $n$ and relatively prime to $n$. It is easy to see that $\gcd(a,n) = 1$ if and only if $\gcd(n-a,n) = 1$ (see Exercise 3.1). Consequently, the numbers $n-a_1, n-a_2, \ldots, n-a_{\phi(n)}$ are equal to the integers $a_1, a_2, \ldots, a_{\phi(n)}$ in some order. Thus,

$$\begin{aligned} a_1 + a_2 + \ldots + a_{\phi(n)} &= (n-a_1) + (n-a_2) + \cdots + (n-a_{\phi(n)}) \\ &= \phi(n)n - \left(a_1 + a_2 + \cdots + a_{\phi(n)}\right). \end{aligned}$$

Hence,

$$2\left(a_1 + a_2 + \cdots + a_{\phi(n)}\right) = \phi(n)n$$

and therefore, $a_1 + a_2 + \cdots + a_{\phi(n)} = \frac{1}{2}n\phi(n)$. □

**Example 3.6.4.** Consider $n = 30$. Then $\phi(30) = 8$. The 8 integers that are less than 30 and relatively prime to 30 are

$$1, 7, 11, 13, 17, 19, 23, 29$$

and their sum is $1+7+11+13+17+19+23+29 = 120$ which is the desired sum as $\frac{1}{2}n\phi(n) = \frac{1}{2}\cdot 30\cdot 8 = 120$.

Also, note the pairings

$$1+29 = 30, \quad 7+23 = 30, \quad 11+19 = 30, \quad 13+17 = 30.$$

As an application of the Möbius inversion formula, we have the following result, the proof of which is surprisingly simple.

**Theorem 3.6.5**

For any positive integer $n$,

$$\phi(n) = n\sum_{d|n}\frac{\mu(d)}{d}.$$

*Proof.* Applying the inversion formula to

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

we get

$$\begin{aligned}\phi(n) &= \sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)\\ &= \sum_{d|n}\mu(d)\frac{n}{d} = n\sum_{d|n}\frac{\mu(d)}{d}.\end{aligned}$$

□

Let us consider the situation when $n = 10$. It can be easily seen that

$$\begin{aligned}10\sum_{d|10}\frac{\mu(d)}{d} &= 10\left[\mu(1)+\frac{\mu(2)}{2}+\frac{\mu(5)}{5}+\frac{\mu(10)}{10}\right]\\ &= 10\left[1+\frac{(-1)}{2}+\frac{(-1)}{5}+\frac{(-1)^2}{10}\right]\\ &= 10\left[1-\frac{1}{2}-\frac{1}{5}+\frac{1}{10}\right]\\ &= 10\cdot\frac{2}{5} = 4 = \phi(10).\end{aligned}$$

CHAPTER 4

# Quadratic Reciprocity

The goal of this chapter is to prove the Quadratic Reciprocity Law for which in the first section, we study some of the prerequisites.

## 4.1 Primitive Roots and Indices

**Definition 4.1.1**

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

Considering powers of 2 modulo 7, we have the congruences

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, 2^5 \equiv 4, 2^6 \equiv 1, \ldots.$$

It is clear that the order of 2 modulo 7 is 3.

**Theorem 4.1.2**

Let the integer $a$ have order $k$ modulo $n$. Then $a^h \equiv 1 \pmod{n}$ if and only if $k \mid h$. In particular, $k \mid \phi(n)$.

*Proof.* Exercise. □

Let us find order of 2 modulo 13. Since $\phi(13) = 12$, the order of 2 must be a divisor of 12. Thus, the possibilities of order of 2 are $1, 2, 3, 4, 6, 12$. Note that

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^6 \equiv 12,\ 2^{12} \equiv 1 \pmod{13}.$$

Thus, the order of 2 modulo 13 is 12.

By Euler's theorem, we know that if $\gcd(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$. Thus, the highest possible order of $a$ modulo $n$ is $\phi(n)$. If an integer $a$ has the largest possible order (i.e., order of $a$ is $\phi(n)$ modulo $n$), then it is called a primitive root of $n$.

**Definition 4.1.3**

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

**Theorem 4.1.4: Lagrange**

If $p$ is a prime and

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \not\equiv 0 \pmod{p}$$

is a polynomial of degree $n \geq 1$ with integral coefficients, then the congruence

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

has at most $n$ incongruent solutions modulo $p$.

*Proof.* Without proof (not in our syllabus). □

## 4.2 Euler's Criterion

The main goal of this unit is the Quadratic Reciprocity Law which is one of the major contribution of Gauss. Since the time of Gauss, over a hundred proofs of it has been published. Among the eminent mathematician of the 19th century who gave their proofs are Cauchy, Jacobi, Dirichlet, Eisenstein, Kronecker, and Dedekind.

Vaguely speaking, the Quadratic Reciprocity Law deals with the solvability of the quadratic congruence of the form

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{4.1}$$

where $p$ is an odd prime and $a \not\equiv 0 \pmod{p}$, i.e., $\gcd(a,p) = 1$ or equivalently $p \nmid a$. The condition that $p$ is an odd prime implies that $\gcd(4a,p) = 1$. Thus, the quadratic congruence in (4.1) is equivalent to

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}.$$

By using the identity

$$4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$$

the above quadratic congruence may be expressed as

$$(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}.$$

Now, putting $y = 2ax + b$ and $d = b^2 - 4ac$, we get

$$y^2 \equiv d \pmod{p}. \tag{4.2}$$

If $x \equiv x_0 \pmod{p}$ is a solution of the quadratic congruence in (4.1), then the integer $y \equiv 2ax_0 + b \pmod{p}$ is a solution of the quadratic congruence in (4.2). Conversely, if $y \equiv y_0 \pmod{p}$ is a solution of the quadratic congruence in (4.2), then the linear congruence $2ax \equiv y_0 - b \pmod{p}$ can be solved to obtain a solution of the quadratic congruence in (4.1).

Thus, the problem of finding a solution to the quadratic congruence in (4.1) is equivalent to that of finding a solution to a linear congruence and a quadratic congruence of the form

$$x^2 \equiv a \pmod{p}. \tag{4.3}$$

If $p \mid a$, then the quadratic congruence in (4.3) has $x \equiv 0 \pmod{p}$ as its only solution. To avoid this trivial case, we assume that $p \nmid a$. Under this assumption, whenever the congruence $x^2 \equiv a \pmod{p}$ has a (non-trivial) solution $x = x_0$, it also has a second solution $x = p - x_0$. This second solution cannot be congruent to the first solution $x_0$, for if $x_0 \equiv p - x_0 \pmod{p}$, then $2x_0 \equiv p \equiv 0 \pmod{p}$ which is not possible. Thus, the two solutions are distinct modulo $p$. By Lagrange's theorem, these two solutions are the only two solutions of $x^2 \equiv a \pmod{p}$. Thus, the congruence $x^2 \equiv a \pmod{p}$ has exactly two solutions or no solution.

Let us consider a simple numerical example of what we discussed above. Consider the quadratic congruence

$$5x^2 - 6x + 2 \equiv 0 \pmod{13}.$$

To obtain the solution, we replace this congruence by the simpler one given by

$$y^2 \equiv 9 \pmod{13}.$$

This is the congruence $y^2 \equiv (b^2 - 4ac) \pmod{p}$ as given in (4.2), where

$$d = b^2 - 4ac = (-6)^2 - 4 \cdot 5 \cdot 2 = 36 - 40 = -4 \equiv 9 \pmod{13}.$$

The congruence $y^2 \equiv 9 \pmod{13}$ has solutions $y \equiv 3, 10 \pmod{13}$. Then as discussed above, for these two values of $y = y_0$, we have to solve the linear congruences $2ax \equiv y_0 - b \pmod{p}$. Here, in our case, we solve the congruences

$$(2 \cdot 5)x \equiv 3 - (-6) \pmod{13} \quad \text{and} \quad (2 \cdot 5)x \equiv 10 - (-6) \pmod{13}.$$

Thus, the congruences, we solve are

$$10x \equiv 9 \pmod{13} \quad \text{and} \quad 10x \equiv 16 \equiv 3 \pmod{13}.$$

Multiplying both the congruences on both the sides by 4 (as $10 \cdot 4 \equiv 40 \equiv 1 \pmod{p} mod 13$), we get

$$x \equiv 36 \equiv 10 \pmod{13} \quad \text{and} \quad x \equiv 12 \pmod{13}$$

are the two solutions. It can also be seen that these two solutions satisfy our original quadratic congruence, as we discussed above.

Thus, the major focus of the discussion is towards providing a test for the existence of solutions of the quadratic congruence

$$x^2 \equiv a \pmod{p}, \quad \gcd(a, p) = 1. \tag{4.4}$$

Thus, we wish to identify those integers $a$ that are perfect squares modulo the prime $p$. We have the following definition in this regard.

**Definition 4.2.1: Quadratic residue**

Let $p$ be an odd prime and $\gcd(a,p)=1$. If the quadratic congruence $x^2 \equiv a \pmod{p}$ has a solution, then $a$ is said to be a *quadratic residue of* $p$. Otherwise, $a$ is called a *quadratic nonresidue of* $p$.

Note that if $a \equiv b \pmod{p}$, then $a$ is a quadratic residue of $p$ if and only if $b$ is a quadratic residue of $p$. Thus, to determine whether a positive integer is a quadratic residue or not (i.e., to determine the quadratic character of a positive integer), we need to consider only integers modulo $p$.

**Example 4.2.2.** Consider the case for the prime $p=13$. To find out how many of the integers $1,2,3,\ldots,12$ are quadratic residues of 13, we must find out which of the congruences

$$x^2 \equiv a \pmod{13}$$

are solvable when $a$ runs through the set $\{1,2,\ldots,12\}$. Modulo 13, the squares of these integers are

$$\begin{aligned}
1^2 &\equiv (-1)^2 \equiv 12^2 \equiv 1\\
2^2 &\equiv (-2)^2 \equiv 11^2 \equiv 4\\
3^2 &\equiv (-3)^2 \equiv 10^2 \equiv 9\\
4^2 &\equiv (-4)^2 \equiv 9^2 \equiv 3\\
5^2 &\equiv (-5)^2 \equiv 8^2 \equiv 12\\
6^2 &\equiv (-6)^2 \equiv 7^2 \equiv 10.
\end{aligned}$$

Thus, it follows that the quadratic residues of 13 are the integers $1,3,4,9,10,12$ while the nonresidues of 13 are $2,5,6,7,8,11$.

Observe that the integers from 1 to 12 are equally divided among the quadratic residues and the nonresidues.

Euler gave a simple criterion for deciding whether an integer $a$ is a quadratic residue of a given prime $p$.

**Theorem 4.2.3: Euler's criterion**

Let $p$ be an odd prime and $\gcd(a,p)=1$. Then $a$ is a quadratic residue of $p$ if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

*Proof.* Suppose that $a$ is a quadratic residue of $p$. Then $x^2 \equiv a \pmod{p}$ has a solution, say $x_1$. Since $\gcd(a,p)=1$, it follows that $\gcd(x_1,p)=1$ (**Why?**). Then by Fermat's theorem, we have

$$a^{(p-1)/2} \equiv (x_1^2)^{(p-1)/2} \equiv x_1^{p-1} \equiv 1 \pmod{p}.$$

Conversely, assume that the congruence $a^{(p-1)/2} \equiv 1 \pmod{p}$ holds. Let $r$ be a primitive root of $p$. Then $a \equiv r^k \pmod{p}$ for some integer $k$ with $1 \le k \le p-1$. It follows that

$$r^{k(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}.$$

By Theorem 4.1.2, the order of $r$ (which is $p-1$, being a primitive root) must divide the exponent $\frac{k(p-1)}{2}$. This implies that $k$ is an even integer, say $k = 2j$ for some integer $j$. Then

$$(r^j)^2 = r^{2j} = r^k \equiv a \pmod{p}.$$

Thus, $r^j$ is a solution of the congruence $x^2 \equiv a \pmod{p}$. This proves that $a$ is a quadratic residue of the prime $p$. □

Now, if $p$ is an odd prime and $\gcd(a,p) = 1$, then

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 \equiv 0 \pmod{p}$$

as by Fermat's theorem $a^{p-1} \equiv 1 \pmod{p}$. Hence, either

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \text{or} \quad a^{(p-1)/2} \equiv -1 \pmod{p}$$

but not both. For if, both the congruences hold simultaneously, then $1 \equiv -1 \pmod{p}$ which means that $p \mid 2$, a contradiction to the hypothesis that $p$ is an odd prime. Since a quadratic nonresidue of $p$ does not satisfy $a^{(p-1)/2} \equiv 1 \pmod{p}$, it must therefore satisfy $a^{(p-1)/2} \equiv -1 \pmod{p}$. This observation provides an alternate formulation of the Euler's criterion which can be stated as "the integer $a$ is a quadratic nonresidue of the prime $p$ if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$. We have the following corollary.

**Corollary 4.2.4**

Let $p$ be an odd prime and $\gcd(a,p) = 1$. Then $a$ is a quadratic rsidue or nonresidue of $p$ according to whether

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \text{or} \quad a^{(p-1)/2} \equiv -1 \pmod{p}.$$

**Example 4.2.5.** Consider the case where $p = 13$. We find that

$$2^{(13-1)/2} = 2^6 \equiv 64 \equiv -1 \pmod{13}.$$

Thus, by the above corollary, the integer 2 is a quadratic nonresidue of 13. However,

$$3^{(13-1)/2} = 3^6 = (27)^2 \equiv 1^2 \equiv 1 \pmod{13}.$$

So, 3 is a quadratic residue of 13 and so the congruence $x^2 \equiv 3 \pmod{13}$ is solvable and the its two incongruent solutions are $x \equiv 4$ and $x \equiv 9 \pmod{13}$.

There is an alternative proof the Euler's criterion due to Dirichlet. The proof is as follows.

*Dirichlet's proof of Euler's criterion.* Let $a$ be a quadratic nonresidue of $p$ and let $c$ be any one of the integers $1, 2, \ldots, p-1$. By the theory of linear congruences, there exists a solution $c'$ of the congruence $cx \equiv a \pmod{p}$, with $c'$ also in the set $\{1, 2, \ldots, p-1\}$. Note that $c' \neq c$. Otherwise, $c^2 \equiv a \pmod{p}$ which contradicts our assumption that $a$ is a quadratic nonresidue of $p$. Thus, the integers between 1 and $p-1$ can be divided into $(p-1)/2$ pairs $c, c'$, where $cc' \equiv a \pmod{p}$. This gives us $(p-1)/2$ congruences,

$$c_1 c_1' \equiv a \pmod{p}$$

$$c_2 c_2' \equiv a \pmod{p}$$
$$\vdots$$
$$c_{(p-1)/2} c_{(p-1)/2}' \equiv a \pmod{p}.$$

Multiplying these congruences and observing that the product

$$c_1 c_1' c_2 c_2' \cdots c_{(p-1)/2} c_{(p-1)/2}'$$

is simply a rearrangement of $1 \cdot 2 \cdot 3 \cdots (p-1)$, we get

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

By Wilson's theorem (Theorem 2.4.1), we know that $(p-1)! \equiv -1 \pmod{p}$. Therefore, we have

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

which is Euler's criterion when $a$ is a quadratic nonresidue of $p$.

Next, we examine the case when $a$ is a quadratic residue of $p$. In this case, the congruence $x^2 \equiv a \pmod{p}$ has two solutions $x = x_1$ and $x = p - x_1$ for some integer $x_1$ with $1 \leq x_1 \leq p-1$. If $x_1$ and $p - x_1$ are removed from the set $\{1, 2, \ldots, p-1\}$, then the remaining $p-3$ integers can be grouped into pairs $c, c'$, where $c \neq c'$ such that $cc' \equiv a \pmod{p}$. There are $\frac{p-3}{2}$ such congruences. In addition to these congruences, there is a congruence

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

So, total there are $\frac{p-3}{2} + 1 = \frac{p-1}{2}$ congruences. Taking the product of all these $\frac{p-1}{2}$ congruences, we get

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

Again by Wilson's theorem, we get

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

Summing up, we have shown that $a^{(p-1)/2} \equiv 1 \pmod{p}$ or $a^{(p-1)/2} \equiv -1 \pmod{p}$ according to whether $a$ is a quadratic residue or a nonresidue of $p$.

This completes the proof. □

Euler's criterion is not preferred for practical implementation because for determining whether a given integer is a quadratic residue or is not a quadratic residue of $p$, the calculations involved become too cumbersome if the modulus is large. A more effective method of computation is given in the Quadratic Reciprocity Law, which we prove at the end of this unit.

## 4.3 The Legendre Symbol and its Properties

**Definition 4.3.1: Legendre symbol**

Let $p$ be an odd prime and let $\gcd(a, p) = 1$. The *Legendre symbol* $(a/p)$ is defined by

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

For better terminology, $a$ is called the *numerator* and $p$ is called the *denominator* of the symbol $(a/p)$. Another standard notation of the Legendre symbol is $\left(\frac{a}{p}\right)$ or $(a\,|\,p)$.

**Example 4.3.2.** Consider the prime $p = 13$. By Example 4.2.5, we know that $1, 3, 4, 9, 10, 12$ are quadratic residues of 13 and $2, 5, 6, 7, 8, 11$ are quadratic nonresidues of 13. Therefore, the Legendre symbols may be expressed as

$$(1/13) = (3/13) = (4/13) = (9/13) = (10/13) = (12/13) = 1$$

and

$$(2/13) = (5/13) = (6/13) = (7/13) = (8/13) = (11/13) = -1.$$

**Remark 4.3.3.** For $p \mid a$, the symbol $(a/p)$ is purposely left undefined. Some authors find it convenient to extend Legendre's definition to this case by setting $(a/p) = 0$. An advantage of this is that the number of solutions of $x^2 \equiv a \pmod{p}$ can then be given by the formula $1 + (a/p)$.

The next result gives some elementary properties of the Legendre's symbol.

**Theorem 4.3.4**

Let $p$ be an odd prime and $a$ and $b$ be integers that are relatively prime to $p$. Then the Legendre symbol has the following properties:

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

(b) $(a^2/p) = 1$.

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

(d) $(ab/p) = (a/p)(b/p)$.

(e) $(1/p) = 1$ and $(-1/p) = (-1)^{(p-1)/2}$.

*Proof.* If $a \equiv b \pmod{p}$, then the two congruence $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ have exactly the same solutions, if any at all. Thus, $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ are both solvable, or neither one has a solution. Hence, $(a/p) = (b/p)$.

Regarding property (b), observe that the integer $a$ trivially satisfies the congruence $x^2 \equiv a^2 \pmod{p}$. Hence, $(a^2/p) = 1$.

Property (c) is just Corollary 4.2.4 but in terms of the Legendre symbol.

We shall use (c) to prove (d).

$$(ab/p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv (a/p)(b/p) \pmod{p}.$$

Now, the Legendre symbol assumes only the values 1 or $-1$. If $(ab/p) \neq (a/p)(b/p)$, then we would have $1 \equiv -1 \pmod{p}$ or $2 \equiv 0 \pmod{p}$. This cannot happen since $p > 2$ is an odd prime. Thus, it follows that

$$(ab/p) = (a/p)(b/p).$$

Finally, observe that the first equality in the property (e) is a special case of the property (b) for $a = 1$, while the second equality in the property (e) is a special case of the property (c) for $a = -1$. Since the quantities $(-1/p)$ and $(-1)^{(p-1)/2}$ are either 1 or $-1$, the resulting congruence

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

implies that $(-1/p) = (-1)^{(p-1)/2}$. □

From parts (b) and (d), we have

(f) $(ab^2/p) = (a/p)(b^2/p) = (a/p) \cdot 1 = (a/p)$.

In other words, a square factor that is relatively prime to $p$ can be deleted from the numerator of the Legendre symbol without affecting its value.

Since $\frac{p-1}{2}$ is even for a prime $p$ of the form $4k+1$ and odd for a prime $p$ of the form $4k+3$, the equation $(-1/p) = (-1)^{(p-1)/2}$ yields the following corollary to Theorem 4.3.4.

**Corollary 4.3.5**

If $p$ is an odd prime, then

$$(-1/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

This corollary can be viewed by stating that the quadratic congruence $x^2 \equiv -1 \pmod{p}$ has a solution for an odd prime $p$ if and only if $p$ is of the form $4k+1$.

**Example 4.3.6.** Let us check whether the congruence $x^2 \equiv -46 \pmod{17}$ is solvable. This can be done by evaluating the Legendre symbol $(-46/17)$. By properties (d) and (e) of Theorem 4.3.4,

$$(-46/17) = (-1/17)(46/17).$$

Since $46 \equiv 12 \pmod{17}$, it follows that

$$(46/17) = (12/17).$$

Now, by property (f),

$$(12/17) = (3 \cdot 2^2/17) = (3/17).$$

But then using property (c) of Theorem 4.3.4, we have

$$(3/17) \equiv 3^{(17-1)/2} \equiv 3^8 \equiv (81)^2 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}.$$

Hence, $(3/17) = -1$ and so $(-46/17) = -1$, i.e., the quadratic congruence $x^2 \equiv -46 \pmod{17}$ admits no solution.

An application of Corollary 4.3.5 helps to prove the infinitude of primes of the form $4k+1$.

**Theorem 4.3.7**

There are infinitely many primes of the form $4k+1$.

*Proof.* Suppose that there are finitely many primes of the form $4k+1$, say $p_1, p_2, \ldots, p_n$. Consider the integer

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

Clearly, $N$ is odd. So, there exists some odd prime $p$ such that $p \mid N$. Then

$$(2p_1p_2\cdots p_n)^2 \equiv -1 \pmod{p}.$$

In terms of the Legendre symbol, this means that the symbol $(-1/p) = 1$. But the relation $(-1/p) = 1$ holds if and only if $p$ is of the form $4k+1$. Hence, $p$ is one of the primes $p_i$. But then $p_i \mid N - (2p_1p_2\cdots p_n)^2$ and so $p_i \mid 1$, which is a contradiction. Hence, there must be infinitely many primes of the form $4k+1$. □

**Theorem 4.3.8**

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 $r$ be a primitive root of $p$. We know that the powers of $r$ generate all the integers $1, 2, \ldots, p-1$. In other word, modulo $p$, the powers $r, r^2, \ldots r^{p-1}$ are just a permutation of the integers $1, 2, \ldots, p-1$. Thus, for any $a$ between 1 and $p-1$, inclusive, there exists a unique positive integer $k$ $(1 \leq k \leq p-1)$, such that $a \equiv r^k \pmod{p}$. By Euler's criterion, we have

$$(a/p) \equiv (r^k/p) \equiv (r^k)^{(p-1)/2} \equiv \left(r^{(p-1)/2}\right)^k \equiv (-1)^k \pmod{p}, \tag{4.5}$$

where $r^{(p-1)/2} \equiv -1 \pmod{p}$ since $r$ is a primitive rood of $p$. But $(a/p)$ and $(-1)^k$ are equal to either 1 or $-1$ and so the equality holds in equation (4.5). Now, adding the required Legendre symbols, we get

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

which is the desired conclusion. □

As a consequence of the above theorem, we have the following corollary.

**Corollary 4.3.9**

The quadratic residues of an odd prime $p$ are congruent modulo $p$ to the even powers of a primitive root $r$ of $p$; the quadratic nonresidues are congruent to the odd powers of $r$.

Lets us again consider the prime $p = 13$. Since 2 is a primitive root of 13, the quadratic residues of 13 are given by the even powers of 2, namely

$$\begin{aligned} 2^2 &\equiv 4 \\ 2^4 &\equiv 3 \\ 2^6 &\equiv 12 \\ 2^8 &\equiv 9 \\ 2^{10} &\equiv 10 \\ 2^{12} &\equiv 1, \end{aligned}$$

where all the congruences are modulo 13. Similarly, the nonresidues occur as the odd powers of 2, namely

$$\begin{aligned} 2^1 &\equiv 2 \\ 2^3 &\equiv 8 \\ 2^5 &\equiv 6 \\ 2^8 &\equiv 11 \\ 2^9 &\equiv 5 \\ 2^{11} &\equiv 7. \end{aligned}$$

Most of the proofs of the Quadratic Reciprocity Law including the one which we will discuss in this course, rest ultimately on the following result which is known as Gauss's lemma. Although this lemma gives the quadratic character of an integer, it is more useful from a theoretical point of view rather than for computation purpose.

**Theorem 4.3.10: Gauss's lemma**

Let $p$ be an odd prime and let $\gcd(a, p) = 1$. If $n$ denotes the number of integers in the set

$$S = \left\{ a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a \right\}$$

whose remainders upon division by $p$ exceed $p/2$, then

$$(a/p) = (-1)^n.$$

*Proof.* Since $\gcd(a, p) = 1$, it easily follows that none of the $(p-1)/2$ integers in the set $S$ is congruent to zero modulo $p$ and no two of them are congruent to each other modulo $p$ (**Why?**). Let $r_1, \ldots, r_m$ be those remainders upon division by $p$ such that $0 < r_i < p/2$, and let $s_1, \ldots, s_n$ be those remainders such that $p > s_i > p/2$. Then $m + n = (p-1)/2$, and the integers

$$r_1, \ldots, r_m \qquad p - s_1, \ldots, p - s_n$$

are all positive and less than $p/2$.

To prove that these integers are all distinct, it suffices to show that no $p - s_i$ is equal to any $r_j$. Assume on the contrary that

$$p - s_i = r_j$$

for some $i$ and $j$. Then there exist integers $u$ and $v$, with $1 \leq u, v \leq (p-1)/2$, satisfying $s_i \equiv ua \pmod{p}$ and $r_j \equiv va \pmod{p}$. Hence,

$$(u+v)a \equiv s_i + r_j = p \equiv 0 \pmod{p}$$

which says that $u+v \equiv 0 \pmod{p}$. But this is not possible since $1 < u+v \leq p-1$.

Thus, the $(p-1)/2$ numbers

$$r_1, \ldots, r_m \qquad p-s_1, \ldots, p-s_n$$

being distinct, are simply the integers $1, 2, \ldots, (p-1)/2$, not necessarily in the order of appearance. Thus, their product is $[(p-1)/2]!$:

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= r_1 \cdots r_m (p-s_1) \cdots (p-s_n) \\ &\equiv r_1 \cdots r_m (-s_1) \cdots (-s_n) \pmod{p} \\ &\equiv (-1)^n r_1 \cdots r_m s_1 \cdots s_n \pmod{p}.\end{aligned}$$

But we know that $r_1, \ldots, r_m, s_1, \ldots, s_n$ are congruent modulo $p$ to $a, 2a, \ldots, [(p-1)/2]a$ in some order. Therefore,

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

Since $[(p-1)/2]!$ is relatively prime to $p$, it can be cancelled from both the sides of the above congruence to give

$$1 \equiv (-1)^n a^{(p-1)/2} \pmod{p}$$

or on multiplying by $(-1)^n$, we have

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

By Euler's criterion,

$$(a/p) \equiv a^{(p-1)/2} \equiv (-1)^n \pmod{p}$$

which implies that

$$(a/p) = (-1)^n.$$

□

As an illustration, let $p = 13$ and $a = 5$. Then $(p-1)/2 = 6$, so that

$$S = \{5, 10, 15, 20, 25, 30\}$$

modulo 13, the members of $S$ are the same as the integers

$$5, 10, 2, 7, 12, 4.$$

Three of these are greater than $\frac{13}{2}$, hence $n = 3$, and Theorem 3.6.1 says that

$$(5/13) = (-1)^3 = -1.$$

**Theorem 4.3.11**

If $p$ is an odd prime, then

$$(2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8. \end{cases}$$

*Proof.* By Gauss's lemma, $(2/p) = (-1)^n$, where $n$ is the number of integers in the set

$$S = \left\{1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \ldots, \left(\frac{p-1}{2}\right) \cdot 2\right\}$$

which on dividing by $p$ have remainders greater than $p/2$. Since, all the members of $S$ are less than $p$, it suffices to count the number that exceeds $p/2$. For $1 \leq k \leq (p-1)/2$, we have $2k < p/2$ if and only if $k < p/4$. If $[\,]$ denotes the greatest integer function, then there are $\left[\frac{p}{4}\right]$ integers in $S$ less than $p/2$. Hence,

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

is the number of integers that are greater than $p/2$.

Given any odd prime, there are four possibilities. It is either of the form $8k+1$, $8k+3$, $8k+5$, or $8k+7$.

$$\begin{aligned}
\text{if } p = 8k+1, \text{ then } n &= 4k - \left[2k + \frac{1}{4}\right] = 4k - 2k = 2k \\
\text{if } p = 8k+3, \text{ then } n &= 4k+1 - \left[2k + \frac{3}{4}\right] = 4k+1-2k = 2k+1 \\
\text{if } p = 8k+5, \text{ then } n &= 4k+2 - \left[2k+1+\frac{1}{4}\right] \\
&= 4k+2-(2k+1) = 2k+1 \\
\text{if } p = 8k+7, \text{ then } n &= 4k+3 - \left[2k+1+\frac{3}{4}\right] \\
&= 4k+3-(2k+1) = 2k+2.
\end{aligned}$$

Thus, when $p$ is of the form $8k+1$ or $8k+7$, $n$ is even and $(2/p) = 1$. On the other hand, when $p$ is of the form $8k+3$ or $8k_5$, then $n$ is odd and $(2/p) = -1$. □

**Corollary 4.3.12**

If $p$ is an odd prime, then

$$(2/p) = (-1)^{(p^2-1)/8}.$$

*Proof.* If $p$ is of the form $8k \pm 1$, i.e., $p \equiv 1 \pmod 8$ or $p \equiv 7 \pmod 8$, then

$$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k,$$

which is an even integer. In this case, $(-1)^{(p^2-1)/8} = 1 = (2/p)$. On the other hand, if $p$ is of the form $8k \pm 3$, i.e., $p \equiv 3 \pmod 8$ or $p \equiv 5 \pmod 8$, then

$$\frac{p^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1,$$

which is odd. Hence, in this case, $(-1)^{(p^2-1)/8} = -1 = (2/p)$. □

**Theorem 4.3.13**

If $p$ and $2p+1$ are both odd primes, then the integer $(-1)^{(p-1)/2}2$ is a primitive root of $2p+1$.

*Proof.* Let $q = 2p+1$. We consider two cases: $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$.

If $p \equiv 1 \pmod 4$, then $(-1)^{(p-1)/2}2 = 2$. Since $\phi(q) = q - 1 = 2p$, the order of 2 modulo $q$ is one of the numbers 1, 2, $p$, or $2p$. Then by the property (c) of Theorem 4.3.4, we have

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

Now, $p \equiv 1 \pmod 4$ implies $p = 4k+1$ for some integer $k$, and so $q = 2p+1 = 8k+3$. Thus, $q \equiv 3 \pmod 8$. Then by Theorem 4.3.11, $(2/q) = -1$. It follows that $2^p \equiv -1 \pmod q$, and so the order of 2 modulo $q$ cannot be $p$. Also, $2^2 \equiv 1 \pmod q$ implies that $q \mid 3$ which is not possible as $8 \mid q-3$. Thus, order of 2 modulo $q$ cannot be 2 also. The order of 2 being neither 1, 2, nor $p$, we can conclude that the order of 2 modulo $q$ must be $2p = q-1$. Then, by definition, 2 a primitive root modulo $q$.

Now, we consider the case $p \equiv 3 \pmod 4$. In this case, $(-1)^{(p-1)/2}2 = -2$ and

$$(-2)^p \equiv (-2/q) = (-1/q)(2/q) \pmod q.$$

Since $p$ is of the form $4k+3$, $q = 2p+1$ is of the form $8k+7$, i.e., $q \equiv 7 \pmod 8$. Then by Corollary 4.3.5, we have $(-1/q) = -1$, whereas once again $(2/q) = 1$. This leads to the congruence

$$(-2)^p \equiv -1 \pmod q.$$

Then as argued above, we can conclude that $-2$ is a primitive root of $q$.

This completes the proof. □

**Remark 4.3.14.**

1. A similar result as above: If $p$ and $4p+1$ are primes, then 2 is a primitive root of $4p+1$.

2. An odd prime $p$ such that $2p+1$ is also a prime is called a *Germain prime* named after the French number theorist Sophie Germain. It is an open problem to determine whether there are infinitely many Germain primes.

   The largest Germain prime known till date is $2618163402417 \times 2^{1290000} - 1$ which has 388342 digits and was discovered by Dr. James Scott Brown in February 2016 (source: wikipedia).

**Theorem 4.3.15**

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

*Proof.* Suppose, if possible, there are only finitely many primes of the form $8k-1$, say $p_1, p_2, \ldots, p_n$. Consider the integer

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

Then there exists an odd prime $p$ such that $p \mid N$. Therefore,

$$(4p_1p_2\cdots p_n)^2 \equiv 2 \pmod{p}$$

or in terms of Legendre symbol $(2/p) = 1$. By Theorem 4.3.11, $p \equiv \pm 1 \pmod 8$. It can be easily checked that product of two integers of the form $8k+1$ is again of the same form. Thus, if all the odd prime divisors of $N$ were of the form $8k+1$, then $N$ would also be of the form $8a+1$. This is not possible since $N$ is of the form $16a-2$. Thus, $N$ must have a prime divisor $q$ of the form $8k-1$. That is $q$ is one of the primes $p_1, p_2, \ldots, p_n$. But then $q \mid N$ and $q \mid (4p_1p_2\cdots p_n)^2$ would imply that $q \mid 2$ which is a contradiction to $q$ being an odd prime. Therefore, our supposition that there are only finitely many primes of the form $8k-1$ is wrong, which completes the proof. □

The following is an important result which serves a bridge from Gauss's lemma to the Quadratic Reciprocity Law.

**Lemma 4.3.16**

If $p$ is an odd prime and $a$ is an odd integer, with $\gcd(a,p) = 1$, then

$$(a/p) = (-1)^{\sum_{k=1}^{(p-1)/2}[ka/p]}.$$

*Proof.* We use the same notation as used in the proof of Gauss's lemma. Consider the set of integers

$$S = \left\{a, 2a, \ldots, \left(\frac{p-1}{2}\right)a\right\}.$$

Divide each of these multiples of $a$ by $p$ to obtain

$$ka = q_kp + t_k, \qquad 1 \le t_k \le p-1.$$

Then $\frac{ka}{p} = q_k + \frac{t_k}{p}$, and so $\left[\frac{ka}{p}\right] = q_k$. Thus, for $1 \le k \le (p-1)/2$, we can write $ka$ in the form

$$ka = \left[\frac{ka}{p}\right]p + t_k. \tag{4.6}$$

If the remainder $t_k < p/2$, then it is one of the integers $r_1, \ldots, r_m$. On the other hand, if $t_k > p/2$, then it is one of the integers $s_1, \ldots, s_n$. Taking the sum of the $(p-1)/2$ equations in equation 4.6, we get the following relation.

$$\sum_{k=1}^{(p-1)/2} ka = \sum_{k=1}^{(p-1)/2}\left[\frac{ka}{p}\right]p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k. \tag{4.7}$$

Then as argued in the proof of Gauss's lemma, the $(p-1)/2$ numbers

$$r_1, \ldots, r_m \qquad p - s_1, \ldots, p - s_n$$

are just a rearrangement of the integers $1, 2, \ldots, (p-1)/2$. Hence,

$$\sum_{k=1}^{(p-1)/2} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p - s_k) = pn + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k \tag{4.8}$$

Subtracting equation 4.8 from equation 4.7, we get

$$(a-1) \sum_{k=1}^{(p-1)/2} k = p \left( \sum_{k=1}^{(p-1)/2} \left[ \frac{ka}{p} \right] - n \right) + 2 \sum_{k=1}^{n} s_k. \tag{4.9}$$

Using the fact that $p \equiv a \equiv 1 \pmod 2$ and reducing the last equation modulo 2, we get

$$0 \cdot \sum_{k=1}^{(p-1)/2} k \equiv 1 \cdot \left( \sum_{k=1}^{(p-1)/2} \left[ \frac{ka}{p} \right] - n \right) \pmod 2$$

or

$$n \equiv \sum_{k=1}^{(p-1)/2} \left[ \frac{ka}{p} \right] \pmod 2.$$

The rest follows from Gauss's lemma as

$$(a/p) = (-1)^n = (-1)^{\sum_{k=1}^{(p-1)/2} [ka/p]}.$$

This completes the proof. □

As an example of this last result, consider $p = 13$ and $a = 5$. Since $(p-1)/2 = 6$, we have to calculate $[ka/p]$ for $k = 1, \ldots, 6$:

$$\begin{aligned} [5/13] &= [10/13] = 0 \\ [15/13] &= [20/13] = [25/13] = 1 \\ [30/13] &= 2. \end{aligned}$$

By the above lemma, we have

$$(5/13) = (-1)^{1+1+1+2} = (-1)^5 = -1$$

which confirms what we saw earlier.

## 4.4 Quadratic Reciprocity

For an interesting story of the historical events in the development of the proof of our main result, the quadratic reciprocity law, read the introduction of this section from the Burton's book. The result is given below.

**Theorem 4.4.1: Quadratic Reciprocity Law**

If $p$ and $q$ are odd primes, then

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

*Proof.* Consider the rectangle in the $xy$-plane whose vertices are $(0,0)$, $(\frac{p}{2},0)$, $(0,\frac{q}{2})$, and $(\frac{p}{2},\frac{q}{2})$. Let $R$ denote the region within this rectangle, excluding the boundary lines. The general idea of the proof is to count the number of lattice points (i.e., the points whose coordinates are integers) inside $R$ in two different ways. One way to count the number of lattice points in $R$ is the following.

Since $p$ and $q$ are odd, the lattice points in $R$ consists of all the points $(n,m)$, where $1 \le n \le \frac{p-1}{2}$ and $1 \le m \le \frac{q-1}{2}$. Clearly, the number of such points is

$$\frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Another way to count these lattice points is as follows.

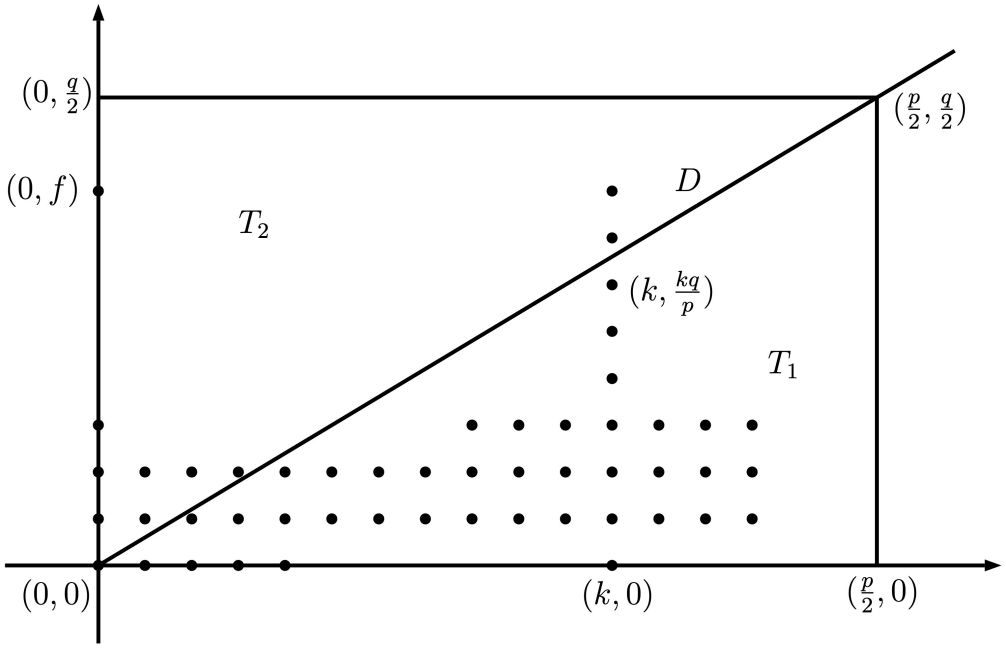



Figure 4.1: Counting lattice points in the rectangle $R$

Let $D$ be the diagonal of the rectangle joining points $(0,0)$ to $(\frac{p}{2},\frac{q}{2})$. The equation of this line is $y = (\frac{q}{p})x$ (because it has slope $q/p$ and it is passing through origin $(0,0)$. Equivalently, the equation of $D$ can be given by $py = qx$. Let $T_1$ denote the portion of $R$ below the diagonal $D$ and $T_2$ denote the portion of $R$ above the diagonal $D$ as shown in Figure 4.1. Another way to count the number of lattice points in $R$ is by first showing that there is no lattice point on $D$ and then counting the number of lattice points inside the triangles $T_1$ and $T_2$.

First we show that there is no lattice point on $D$. Suppose, if $(x_0, y_0) \in D$ is a lattice point (i.e., $x_0, y_0$ are integers), then by the equation of $D$, we have $py_0 = qx_0$. Since $p \mid py_0$, we must

have $p \mid qx_0$. Since $\gcd(p,q) = 1$, by Euclid' lemma (Theorem 1.2.11), $p \mid x_0$. This is not possible since $1 \leq x_0 \leq \frac{p-1}{2}$ (i.e., $x_0$ is a positive integer less than $p$). Similarly, $q \mid y_0$ is also no possible. Thus, there are no integers $x_0$ and $y_0$ satisfying the equation $py = qx$ of $D$. In other words, there are no lattice points on $D$.

Now, we count the number of points inside the triangle $T_1$. Fix a point $(k,0)$ on the $x$-axis. The points above $(k,0)$ in $R$ (i.e., on the vertical segment of $x = k$) are $(k,1), (k,2), \ldots, (k, \frac{q-1}{2})$. Among all these points, the points inside $T_1$ (i.e., below the line $D : y = \frac{q}{p}x$) are the points whose $y$ coordinate is less than $\frac{q}{p}k$. The number of integers in the interval $0 < y < \frac{kq}{p}$ is $\left[\frac{kq}{p}\right]$, the integer part of $\frac{kq}{p}$. This is true for all $1 \leq k \leq \frac{p-1}{2}$. Thus, the total number of points inside $T_1$ is

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

Interchanging the roles of $p$ and $q$, a similar calculation would give the number of points inside $T_2$ as

$$\sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right].$$

Thus, the sum of lattice points inside $R$ counted this way is the total of the above two sums. Comparing our count in both the ways, we have

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right].$$

Then by the above lemma, we have

$$\begin{aligned}(p/q)(q/p) &= (-1)^{\sum_{j=1}^{(q-1)/2}\left[\frac{jp}{q}\right]} \cdot (-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]} \\ &= (-1)^{\sum_{j=1}^{(q-1)/2}\left[\frac{jp}{q}\right] + \sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.\end{aligned}$$

This completes the proof. □

The following is an immediate consequence of the Quadratic Reciprocity Law.

**Corollary 4.4.2**

If $p$ and $q$ are distinct odd primes, then

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

*Proof.* By the above theorem, it is clear that $(p/q)(q/p)$ is 1 is $\frac{p-1}{2} \cdot \frac{q-1}{2}$ is even, and $-1$ otherwise. Clearly, the number $\frac{p-1}{2} \cdot \frac{q-1}{2}$ is even if and only if at at least one of the primes $p$ and $q$ is of the form $4k+1$, and the number if odd if both $p$ and $q$ are of the form $4k+3$. Hence, the result follows. □

**Corollary 4.4.3**

If $p$ and $q$ are distinct odd primes, then

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

*Proof.* Multiplying both the sides of Corollary 4.4.2 by $(q/p)$ and using the fact that $(q/p)^2 = 1$, the result follows. □

Let us understand the significance of the Quadratic Reciprocity Law. Let $p$ be an odd prime and $a \neq \pm 1$ be an integer not divisible by $p$. Let

$$a = \pm 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

be the prime factorization of $a$, where $p_i$ are distinct odd primes. Since the Legendre symbol is multiplicative, we have

$$(a/p) = (\pm 1/p)(2/p)^{k_0}(p_1/p)^{k_1} \cdots (p_r/p)^{k_r}.$$

Thus, to evaluate $(a/p)$ we only need to compute each of these symbols $(-1/p)$, $(2/p)$, and $(p_i/p)$. The values of $(-1/p)$ and $(2/p)$ are already discussed earlier in Corollary 4.3.5 and Theorem 4.3.11 respectively. So we only need to find $(p_i/p)$, where $p_i$ and $p$ are distinct odd primes. This is where Quadratic Reciprocity Law comes into picture. By Corollary 4.4.3, we can replace the symbol $(p_i/p)$ with a new Legendre symbol with a smaller denominator. Through continued inversions and divisions, the computations can be reduced to the known quantities

$$(-1/q), \quad (1/q), \quad (2/q).$$

This process will be more clear with a concrete example given below.

**Example 4.4.4.** Consider the Legendre symbol $(29/53)$. Since both $20 \equiv 1 \pmod 4$ and $54 \equiv 1 \pmod 4$, by the above Corollary and applying the properties of the Legendre symbol proved in Theorem 4.3.4, we have

$$(29/53) = (53/29) = (24/29) = (2/29)(3/29)(4/29) = (2/29)(3/29).$$

By Theorem 4.3.11, $(2/29) = -1$, while inverting the other symbol again, we get

$$(3/29) = (29/3) = (2/3) = -1$$

since $29 \equiv 2 \pmod 3$. Hence, we have

$$(29/53) = (2/29)(3/29) = (-1)(-1) = 1.$$

The Quadratic Reciprocity Law provides a very satisfactory answer to the problem of finding primes $p \neq 3$ for which $e$ is a quadratic residue.

**Theorem 4.4.5**

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

*Proof.* Since $3 \equiv 4 \pmod{4}$, by Corollary 4.4.3, we have

$$(3/p) = \begin{cases} (p/3) & \text{if } p \equiv 1 \pmod{4} \\ -(p/3) & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Now, $p \equiv 1 \pmod{3}$ or $p \equiv 2 \pmod{3}$. Then by Theorems 4.3.4 and 4.3.11, we have

$$(p/3) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{3} \\ -1 & \text{if } p \equiv 2 \pmod{3}. \end{cases}$$

This implies that $(3/p) = 1$ if and only if

$$p \equiv 1 \pmod{4} \text{ and } p \equiv 1 \pmod{3} \tag{4.10}$$

or

$$p \equiv 3 \pmod{4} \text{ and } p \equiv 2 \pmod{3}. \tag{4.11}$$

The restrictions of the conrguences in equation 4.10 are equivalent to $p \equiv 1 \pmod{12}$ (hint: use the Chinese Remainder Theorem), whereas the congruences in equation 4.11 are equivalent to the congruence $p \equiv 11 \equiv -1 \pmod{12}$ (using CRT).

This proves the first part of the result. Similarly, we can prove the second part $(3/p) = -1$ which is left as an **Exercise**. □

**Example 4.4.6.** Consider the following quadratic congruence of composite modulus.

$$x^2 \equiv 196 \pmod{1357}.$$

Since $1357 = 23 \cdot 59$, the given quadratic congruence is solvable if and only if both the following congruences are solvable.

$$x^2 \equiv 196 \pmod{29} \text{ and } x^2 \equiv 196 \pmod{59}.$$

We find the values of the Legendre symbols $(196/23)$ and $(196/59)$. By Theorem 4.4.5, we have

$$(196/23) = (12/23) = (3/23) = 1.$$

Thus, the congruence $x^2 \equiv 196 \pmod{29}$ has a solution. Again by the Quadratic Reciprocity Law and the properties of Legendre symbol, we have

$$(196/59) = (19/59) = -(59/19) = -(2/19) = -(-1) = 1.$$

Therefore, the congruence $x^2 \equiv 196 \pmod{59}$ is also solvable. Consequently, the congruence $x^2 \equiv 196 \pmod{1357}$ is solvable.

To actually find a solution of the given quadratic congruence $x^2 \equiv 186 \equiv 12 \pmod{23}$ is satisfied by $x = 9, 14 \pmod{23}$, while the congruence $x^2 \equiv 196 \equiv 19 \pmod{59}$ has solutions

$x = 14, 45 \pmod{59}$. We now use the Chinese Remainder Theorem to obtain simultaneous solutions of the following four systems of congruences.

$$\begin{aligned} x &\equiv 14 \pmod{23} \text{ and } x \equiv 14 \pmod{59} \\ x &\equiv 14 \pmod{23} \text{ and } x \equiv 45 \pmod{59} \\ x &\equiv 9 \pmod{23} \text{ and } x \equiv 14 \pmod{59} \\ x &\equiv 9 \pmod{23} \text{ and } x \equiv 45 \pmod{59}. \end{aligned}$$

The resulting values $x = 14, 635, 722, 1343 \pmod{1357}$ are the required solutions (**Check using CRT!**) of the given quadratic congruence.

# Index

## Q



## R



## S



## W