NUMBER

THEORY

DR. T. S. GOVINDALAKSHMI

B. Sc. MATHEMATICS- V YEAR

NUMBER THEORY SYLLABUS

UNIT I: Preliminaries: Mathematical induction The Binomial Theorem Early Number Theory.
(Chapter 1: Sections 1.1, 1.2 and Chapter 2: Section 2.1)

UNIT II: Division Algorithm GCD Euclidean Algorithm The Diophantine Equation $ax + by = c$.
(Chapter 2: Sections 2.3 to 2.5)

UNIT III: The Fundamental Theorem of Arithmetic The Sieve of Eratosthenes The Goldbach Conjecture.
(Chapter 3: Sections 3.1 to 3.3)

UNIT IV: Basic properties of congruences Binary and Decimal representation of integer Linear congruence and The Chinese Remainder Theorem.
(Chapter 4: Sections 4.2 to 4.4)

UNIT V: Fermat's Theorem Wilson's Theorem The Fermat-Kraitchik Factorization Method.
(Chapter 5: Sections 5.1 to 5.4)

Recommended Text

1. David M. Burton, *Elementary Number Theory*, McGraw Hill Education (India) Pvt. Ltd., New Delhi, 2014.

Reference Books

1. Neville Robinns, *Beginning Number Theory*, 2nd Ed., Narosa Publishing House Pvt. Limited, Delhi, 2006.

2. Richard E. Klima, Neil Sigmon, Ernest Stitzinger, *Applications of Abstract Algebra with Maple*, CRC Press, Boca Raton, 2000.

3. S. Kumaravelu and Susheela Kumaravelu, *Elements of Number Theory*, Raja Sankar Offset Printers, 2002.

NUMBER THEORY
CONTENTS

Unit I

Unit II

Unit III

Unit IV

Unit V:

UNIT I

1.1 Preliminaries-Mathematical Induction

Well-Ordering Principle: Every nonempty set S of nonnegative integers contains a least element; (i.e) there is some integer a in S such that $a \in S$ for all b's belonging to S.

Theorem 1. Archimedean property
If a and b are any positive integers, then there exists a positive integer n such that $na \geq b$.

Proof. Suppose the statement of the theorem is not true. Then there exist a and b such that $na < b$ for every positive integer n.
Then the set S = b-na: n is a positive integer consists entirely of positive integers.
By the Well-Ordering Principle, S will possess a least element, say, $b - ma$. Note that $b - (m + l)a$ also lies in S, because S contains all integers of this form.
Further, we have $b - (m + l)a = (b - ma) - a < b - ma$ which is a contradiction to $b - ma$ is the smallest integer in S.
Thus our assumption is wrong. Hence, this property is true.

Theorem 2. First Principle of Finite Induction.
Let S be a set of positive integers with the following properties:
(a) The integer 1 belongs to S.
(b) Whenever the integer k is in S, the next integer $k + 1$ must also be in S.
Then S is the set of all positive integers.

Proof. Let T be the set of all positive integers not in S, and assume that T is nonempty. By Well-Ordering Principle, T contains a least element, say a.
Since $1 \in S$, $a > 1$, and so $0 < a - 1 < a$. By the choice of a, $a - 1 \notin T$, or equivalently $a - 1 \in S$. By hypothesis, S must also contain $(a - 1) + 1 = a$,which contradicts to $a \in T$. Hence T is empty and so S contains all the positive integers. □

Problem 3. Prove that $1^2+2^2+3^2+\cdots+n^2 = \frac{n(2n+1)(n+1)}{6}$ ....(1)

Solution. Let S denote the set of all positive integers n for which Eq. (1) is true

For n=1,

$$1^2 = \frac{1(2+1)(1+1)}{6} = 1$$

Hence $1 \in S$. Assume that $k \in S$. Then

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(2k+1)(k+1)}{6} \qquad ....(2)$$

To obtain the sum of the first $k + 1$ squares, we add the next one, $(k + 1)^2$, to both sides of Eq. (2). This gives

$$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{k(2k+1)(k+1)}{6} + (k+1)^2$$

After some algebraic manipulation, the right-hand side becomes

$$(k+1)\left[\frac{k(2k+1)+6(k+1)}{6}\right] = (k+1)\left[\frac{2k^2+7k+6}{6}\right] = \frac{(k+1)(2k+3)(k+2)}{6}$$

Thus

$$1^2+2^2+\cdots+k^2+(k+1)^2 = \frac{(k+1)(2k+3)(k+2)}{6}$$

Hence Eq. (1) is true when $n = k+1$.
The set S contains the integer $k+1$ whenever it contains the integer k. By Theorem 2, S must be all the positive integers; that is, the given formula is true for $n = 1, 2, 3, \ldots$.

Theorem 4. Second Principle of Finite Induction.
Let S be a set of positive integers with the following properties:
(a) The integer 1 belongs to S.
(b) If $1, 2, 3, \ldots, k \in S$ for some integer $k \geq 1$ then $k+1 \in S$.
Then S is the set of all positive integers.

Proof. Let S be consists of all positive integers same as that of Theorem 2. Again, let T be the set of positive integers not in S. Assume that T is nonempty
Choose n to be the smallest integer in T. Then $n > 1$ by assumption (a).
By minimality of n, none of the integers $1, 2, \ldots, n-1$ lies in T or $1, 2, \ldots, n-1 \in S$.
By Property (b′), $n = (n-1)+1$ in S, which is a contradiction. Hence T is empty and so S contains all the positive integers. □

Note 5. Mathematical induction is often used as a method of definition as well as a method of proof.
1. A common way of introducing the symbol $n!$ (pronounced "n factorial") is by means of the inductive definition

(a) $1! = 1$,
(b) $n! = n \cdot (n-1)!$ for $n > 1$.

This pair of conditions provides a rule whereby the meaning of $n!$ is specified for each positive integer n. Thus, by (a), $1! = 1$; (a) and (b) yield

$$2! = 2 \cdot 1! = 2 \cdot 1$$

while by (b), again,

$$3! = 3 \cdot 2! = 3 \cdot 2 \cdot 1$$

Continuing in this manner, using condition (b) repeatedly, the numbers $1!, 2!, 3!, \ldots\ n!$ are defined in succession up to any chosen n. In fact,

$$n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$$

2. Induction enters in showing that $n!$, as a function on the positive integers, exists and is unique.
3. $0! = 1$.

The following example illustrate a proof that requires the Second Principle of Finite Induction.

Lucas sequence:

$$1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots$$

Except for the first two terms, each term of this sequence is the sum of the preceding two, so that the sequence may be defined inductively by

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 3 \\ a_n &= a_{n-1} + a_{n-2} \quad \text{for all } n > 3. \end{aligned}$$

Example 6.
Prove that the inequality

$$a_n < (7/4)^n$$

where $n \geq 1$ using Lucas sequence.

Proof. Proof is by induction on n.
First of all, for $n = 1$ and 2, we have

$$a_1 = 1 < (7/4)^1 = 7/4 \quad \text{and} \quad a_2 = 3 < (7/4)^2 = 49/16$$

whence the inequality in question holds in these two cases.
For the induction step, choose an integer $k \geq 3$ and assume that the inequality is valid for $n = 1, 2, \ldots, k-1$. Then, in particular,

$$a_{k-1} < (7/4)^{k-1} \quad \text{and} \quad a_{k-2} < (7/4)^{k-2}.$$

By the way in which the Lucas sequence is formed, it follows that

$$\begin{aligned} a_k &= a_{k-1} + a_{k-2} \\ &< (7/4)^{k-1} + (7/4)^{k-2} \\ &= (7/4)^{k-2}(7/4 + 1) \\ &= (7/4)^{k-2}(11/4) \\ &< (7/4)^{k-2}(7/4)^2 = (7/4)^k. \end{aligned}$$

Because the inequality is true for $n = k$ whenever it is true for the integers $1, 2, \ldots, k-1$, we conclude by the second induction principle that $a_n < (7/4)^n$ for all $n \geq 1$. □

Exercise 1.1

1. Establish the formulas below by mathematical induction:

(a) $1+2+3+\cdots+n=\frac{n(n+1)}{2}$ for all $n\geq 1$.

(b) $1+3+5+\cdots+(2n-1)=n^2$ for all $n\geq 1$.

(c) $1\cdot 2+2\cdot 3+3\cdot 4+\cdots+n(n+1)=\frac{n(n+1)(n+2)}{3}$ for all $n\geq 1$.

(d) $1^2+3^2+5^2+\cdots+(2n-1)^2=\frac{n(2n-1)(2n+1)}{3}$ for all $n\geq 1$.

(e) $1^3+2^3+3^3+\cdots+n^3=\left[\frac{n(n+1)}{2}\right]^2$ for all $n\geq 1$.

2. If $r\neq 1$, show that for any positive integer n,

$$a+ar+ar^2+\cdots+ar^n=\frac{a(r^{n+1}-1)}{r-1}.$$

3. Use the Second Principle of Finite Induction to establish that for all $n\geq 1$,

$$a^n-1=(a-1)(a^{n-1}+a^{n-2}+a^{n-3}+\cdots+a+1).$$

[Hint: $a^{n+1}-1=(a+1)(a^n-1)-a(a^{n-1}-1)$.]

4. Prove that the cube of any integer can be written as the difference of two squares. [Hint: Notice that

$$n^3=(1^3+2^3+\cdots+n^3)-(1^3+2^3+\cdots+(n-1)^3)].$$

1.2 THE BINOMIAL THEOREM

Definition 7. For any positive integer n and any integer k satisfying $0\leq k\leq n$, **binomial coefficients** $\binom{n}{k}$ are defined by

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

By canceling out either $k!$ or $(n-k)!$, $\binom{n}{k}$ can be written as

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

Example 8.

1. For $n=8$ and $k=3$, we have

$$\binom{8}{3}=\frac{8!}{3!5!}=\frac{8\cdot 7\cdot 6\cdot 5\cdot 4}{5!}=\frac{8\cdot 7\cdot 6}{3!}=56.$$

2.

$$\binom{n}{0}=\binom{n}{n}=1.$$

Example 9. Pascal's rule:

$$\binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k}\qquad 1\leq k\leq n.$$

Proof. Its proof consists of multiplying the identity

$$\frac{1}{k}+\frac{1}{n-k+1}=\frac{n+1}{k(n-k+1)}$$

by $n!/(k-1)!(n-k)!$ to obtain

$$\frac{n!}{k(k-1)!(n-k)!}+\frac{n!}{(k-1)!(n-k+1)(n-k)!}=\frac{(n+1)n!}{k(k-1)!(n-k+1)(n-k)!}.$$

Falling back on the definition of the factorial function,

$$\frac{n!}{k!(n-k)!}+\frac{n!}{(k-1)!(n-k+1)!}=\frac{(n+1)!}{k!(n+1-k)!}$$

from which Pascal's rule follows. □

Pascal's triangle

This relation gives rise to a configuration, known as *Pascal's triangle*, in which the binomial coefficient $\binom{n}{k}$ appears as the $(k+1)$th number in the nth row:

$$\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & 1 & 2 & 1 & & \\
 & 1 & 3 & 3 & 1 & & \\
1 & 4 & 6 & 4 & 1 & & \\
1 & 5 & 10 & 10 & 5 & 1 & \\
1 & 6 & 15 & 20 & 15 & 6 & 1
\end{array}$$

The rule of formation should be clear. The borders of the triangle are composed of 1's; a number not on the border is the sum of the two numbers nearest it in the row immediately above.
Consider the expansion of $(a+b)^n$, $n\geq 1$, into a sum of powers of a and b.
By direct multiplication,

$$\begin{aligned}
(a+b)^1 &= a+b\\
(a+b)^2 &= a^2+2ab+b^2\\
(a+b)^3 &= a^3+3a^2b+3ab^2+b^3\\
(a+b)^4 &= a^4+4a^3b+6a^2b^2+4ab^3+b^4\,.
\end{aligned}$$

The question is how to predict the coefficients. A clue lies in the observation that the coefficients of these first few expansions form the successive rows of Pascal's triangle. This leads us to suspect that the general binomial expansion takes the form

$$(a+b)^n=\binom{n}{0}a^n+\binom{n}{1}a^{n-1}b+\binom{n}{2}a^{n-2}b^2+\cdots+\binom{n}{n-1}ab^{n-1}+\binom{n}{n}b^n$$

or, written as,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \, .$$

Problem 10. (Binomial Theorem)
Prove that $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$, $n \geq 1$

Proof. Let P(n): $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$
When $n = 1$, the formula reduces to

$$(a+b)^1 = \sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k = \binom{1}{0} a^1 b^0 + \binom{1}{1} a$$

=a+b.
P(1) is true.
Assume that the formula holds for some fixed integer m.
To prove P(n) is true for $n = m+1$.
Consider

$$(a+b)^{m+1} = a(a+b)^m + b(a+b)^m$$

Under the induction hypothesis,

$$\begin{aligned} a(a+b)^m &= \sum_{k=0}^{m} \binom{m}{k} a^{m-k+1} b^k \\ &= a^{m+1} + \sum_{k=1}^{m} \binom{m}{k} a^{m+1-k} b^k \end{aligned}$$

and

$$\begin{aligned} b(a+b)^m &= \sum_{j=0}^{m} \binom{m}{j} a^{m-j} b^{j+1} \\ &= \sum_{k=1}^{m} \binom{m}{k-1} a^{m+1-k} b^k + b^{m+1}. \end{aligned}$$

Upon adding these expressions, we obtain

$$\begin{aligned} (a+b)^{m+1} &= a^{m+1} + \sum_{k=1}^{m} \left[\binom{m}{k} + \binom{m}{k-1} \right] a^{m+1-k} b^k + b^{m+1} \\ &= \sum_{k=0}^{m+1} \binom{m+1}{k} a^{m+1-k} b^k \end{aligned}$$

which is the formula in the case $n = m+1$. Hence binomial theorem is true for every n by induction.

□

Exercise 1.2

1. (a) Derive Newton's identity

$$\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r}, \quad n \geq k \geq r \geq 0.$$

   (b) Use part (a) to express $\binom{n}{k}$ in terms of its predecessor:

$$\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}, \quad n \geq k \geq 1.$$

2. If $2 \leq k \leq n-2$, show that

$$\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}, \quad n \geq 4.$$

3. For $n \geq 1$, derive each of the identities below:

   (a) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$.

   (b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n\binom{n}{n} = 0$.

   (c) $\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n} = n2^{n-1}$.

2.1 Early Number Theory

The theory of numbers is one of the oldest branches of mathematics; an enthusiast, by stretching a point here and there, could extend its roots back to a surprisingly remote date. Although it seems probable that the Greeks were largely indebted to the Babylonians and ancient Egyptians for a core of information about the properties of the natural numbers, the first rudiments of an actual theory are generally credited to Pythagoras and his disciples.

The Pythagoreans believed that the key to an explanation of the universe lay in number and form, their general thesis being that ”Everything is Number.” (By number, they meant, of course, a positive integer.) For a rational understanding of nature, they considered it sufficient to analyze the properties of certain numbers. Pythagoras himself, we are told ”seems to have attached supreme importance to the study of arithmetic, which he advanced and took out of the realm of commercial utility.”

Triangular Numbers

Triangular numbers are numbers that can be represented as the sum of consecutive integers beginning with 1. They represent the number of dots that can be arranged evenly in an equilateral triangle.

Example 11.

$$\begin{aligned}1 &= 1\\ 3 &= 1+2\\ 6 &= 1+2+3\\ 10 &= 1+2+3+4\end{aligned}$$

Problem 12. Prove the following facts concerning triangular numbers:

(a) A number is triangular if and only if it is of the form $\frac{n(n+1)}{2}$ for some $n \geq 1$.

(b) The integer n is a triangular number if and only if $8n+1$ is a perfect square.

(c) The sum of any two consecutive triangular numbers is a perfect square.

(d) If n is a triangular number, then so are $9n+1$, $25n+3$, and $49n+6$.

Proof. Triangular number is the sum of consecutive integers beginning with 1.

(a) To prove a number is triangular iff it is of the form $\frac{n(n+1)}{2}$, $n > 1$.

A number t is triangular iff $t = 1+2+...+n = \frac{n(n+1)}{2}$.

(b) To prove the integer n is a triangular number iff $8n+1$ is a perfect square.
Take n is a triangular number.
Then $n = 1+2+...+t = \frac{t(t+1)}{2}$.
To prove $8n+1$ is a perfect square.
i.e. $\sqrt{8n+1} \in \mathbb{Z}_+$.

$$\begin{aligned}8n &= \frac{8t(t+1)}{2} = 4t(t+1)\\ 8n+1 &= 4t^2+4t+1 = (2t+1)^2\end{aligned}$$

$\sqrt{8n+1} = 2t+1 \in \mathbb{Z}_+$.
$\therefore$ $8n+1$ is a perfect square.

(c) To prove the sum of any two consecutive triangular numbers is a perfect square.
Let t_i denote the nth triangular number.

$$\begin{aligned}t_k + t_{k+1} &= t_k + (t_k + k + 1)\\ &= 2t_k + k + 1\\ &= 2\left(1+2+\cdots+k\right) + (k+1)\\ &= 2\left(\frac{k(k+1)}{2}\right) + (k+1)\\ &= k(k+1) + (k+1)\\ &= (k+1)(k+1)\\ &= (k+1)^2.\end{aligned}$$

$\therefore$ $t_k + t_{k+1}$ is a perfect square.

(d) To prove if n is a triangular number, then so are $9n+1$, $25n+3$, $49n+6$.
n is triangular number $\Rightarrow n = \frac{k(k+1)}{2}$.

$$\begin{aligned}
9n+1 &= 9\frac{t(t+1)}{2} \\
&= \frac{9t^2+9t+2}{2} \\
&= \frac{(3t+1)(3t+2)}{2} \\
&= \frac{m(m+1)}{2}; \quad m = 3t+1 \\
&= 1+2+\ldots+m \\
&= t_m \\
&= t_{3t+1}.
\end{aligned}$$

$\therefore 9n+1$ is triangular.

$$\begin{aligned}
25n+3 &= \frac{25t(t+1)}{2}+3 \\
&= \frac{25t^2+25t+6}{2} \\
&= \frac{(5t+2)(5t+3)}{2} \\
&= \frac{(5t+2)((5t+2)+1)}{2} \\
&= \frac{m(m+1)}{2}; \quad m = 5t+2 \\
&= t_m \\
&= t_{5t+2}.
\end{aligned}$$

$\therefore 25n+3$ is triangular.

$$\begin{aligned}
49n+6 &= \frac{49t(t+1)}{2}+6 = \frac{49t^2+49t+12}{2} \\
&= \frac{(7t+3)(7t+4)}{2} \\
&= t_{7t+3}
\end{aligned}$$

$\therefore 49n+6$ is triangular.

□

Problem 13. If t_n denotes the nth triangular number then prove that in terms of the binomial coefficients, $t_n = \binom{n+1}{2}$, $n \geq 1$.

Proof. Let $t_n = n$th triangular number

$$\begin{aligned}
t_n &= 1 + 2 + \cdots + n \\
&= \frac{n(n+1)}{2} \\
&= \frac{n(n+1)}{2} \times \left[\frac{1 \times 2 \times 3 \times \cdots \times (n-1)}{1 \times 2 \times 3 \times \cdots \times (n-1)}\right] \\
&= \frac{(n+1)!}{2!\,(n-1)!} \\
&= \frac{(n+1)!}{2!\,(n+1-2)!} \\
&= \binom{n+1}{2}
\end{aligned}$$

□

Problem 14. Derive the formula for the sum of triangular numbers

$$t_1 + t_2 + \cdots + t_n = \frac{n(n+1)(n+2)}{6}, \quad n \geq 1.$$

Proof.

$$\begin{aligned}
t_{k-1} + t_k &= \binom{k}{2} + \binom{k+1}{2} \\
&= \frac{k!}{2!(k-2)!} + \frac{(k+1)!}{2!(k-1)!} \\
&= \frac{2k^2}{2} = k^2
\end{aligned}$$

Now $t_1 + t_2 + t_3 + \ldots + t_n = (t_1 + t_2) + (t_3 + t_4) + \ldots + (t_{n-1} + t_n)$

$$= 2^2 + 4^2 + \ldots + n^2$$

$$= \frac{n(n+1)(n+2)}{6}.$$

Exercise 2.1

1. Prove that the square of any odd multiple of 3 is the difference of two triangular numbers; specifically, that
$$9(2n+1)^2 = t_{9n+4} - t_{3n+1}$$

2. In the sequence of triangular numbers, find the following:

   (a) Two triangular numbers whose sum and difference are also triangular numbers.

   (b) Three successive triangular numbers whose product is a perfect square.

   (c) Three successive triangular numbers whose sum is a perfect square.

3. (a) If the triangular number t_n is a perfect square, prove that $t_{4n(n+1)}$ is also a square.

   (b) Use part (a) to find three examples of squares that are also triangular numbers.

4. Show that the difference between the squares of two consecutive triangular numbers is always a cube.

5. Prove that the sum of the reciprocals of the first n triangular numbers is less than 2; that is,

$$\frac{1}{1} + \frac{1}{3} + \frac{1}{6} + \frac{1}{10} + \cdots + \frac{1}{t_n} < 2$$

   [Hint: Observe that $\frac{2}{n(n+1)} = 2(\frac{1}{n} - \frac{1}{n+1})$].

UNIT II

2.2 THE DIVISION ALGORITHM

Theorem 1. [Division Algorithm] Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying

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

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

Proof. We prove that the set

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

is nonempty.
It suffices to show the value of x making $a - xb$ nonnegative.
Since $b \geq 1$, $|a|b \geq |a|$, and so

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

For the choice $x = -|a|$, then $a - xb \in S$. By Well-Ordering Principle, S contains a smallest integer say r.
By the definition of S, there exists an integer q satisfying

$$r = a - qb \qquad 0 \leq r.$$

We conclude that $r < b$. If not, then $r \geq b$ and

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

This implies $a - (q+1)b \in S$. But $a - (q+1)b = r - b < r$, a contradiction to the choice of r. Hence r¡b.

To prove the uniqueness of q and r.
Suppose that a has two representations, say,

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

where $0 \leq r < b$, $0 \leq r' < b$. Then $r' - r = b(q - q')$ and, the absolute value of a product is equal to the product of the absolute values,

$$|r' - r| = b|q - q'|\,.$$

Upon adding the two inequalities $-b < -r \leq 0$ and $0 \leq r' < b$, we obtain $-b < r' - r < b$ or, in equivalent terms, $|r' - r| < b$. Thus, $b|q - q'| < b$, which yields

$$0 \leq |q - q'| < 1\,.$$

Since $|q - q'|$ is a nonnegative integer, the only possibility is that $|q - q'| = 0$, whence $q = q'$ and so $r = r'$. This completes the proof. □

Corollary 2. If a and b are integers, with $b \neq 0$, then there exist unique integers q and r such that

$$a = qb + r \quad 0 \leq r < |b|$$

Proof. It is enough to consider the case in which b is negative. Then $|b| > 0$, and by Division algorithm produces unique integers q' and r for which

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

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

$$a = qb + r, \quad \text{with } 0 \leq r < |b|.$$

□

Example 3. Illustration of the Division Algorithm when $b < 0$. Let us take $b = -7$. Then, for the choices of $a = 1, -2, 61$, and -59, we obtain the expressions

$$\begin{aligned} 1 &= 0(-7) + 1 \\ -2 &= 1(-7) + 5 \\ 61 &= (-8)(-7) + 5 \\ -59 &= 9(-7) + 4. \end{aligned}$$

Example 4. Show that the expression $a(a^2 + 2)/3$ is an integer for all $a \geq 1$.

Proof. By Division Algorithm, every a is of the form $3q$, $3q + 1$, or $3q + 2$. Assume the first of these cases. Then $\frac{a(a^2+2)}{3} = q(9q^2 + 2)$ which is an integer.
Similarly, if $a = 3q+1$, then $\frac{(3q+1)((3q+1)^2+2)}{3} = (3q+1)(3q^2+2q+1)$ and $a(a^2+2)/3$ is an integer in this case also. Finally, for $a = 3q + 2$, we obtain $\frac{(3q+2)((3q+2)^2+2)}{3} = (3q + 2)(3q^2 + 4q + 2)$ an integer once more. □

Exercise 2.2

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

2. Show that any integer of the form 6k + 5 is also of the form 3 j + 2, but not conversely.

3. Use the Division Algorithm to establish the following:
   (a) The square of any integer is either of the form 3k or 3k + 1.
   (b) The cube of any integer has one of the forms: 9k, 9k + 1, or 9k + 8.
   (c) The fourth power of any integer is either of the form 5k or 5k + 1.

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

2.3 THE GREATEST COMMON DIVISOR

Definition 5. An integer b is said to be *divisible* by an integer $a \neq 0$, in symbols $a \mid b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

Example 6. $1.$ -12 is divisible by 4, because $-12 = 4(-3)$.
2. 10 is not divisible by 3; for there is no integer c that makes the statement $10 = 3c$ true.

Note 7. The divisibility relation $a \mid b$ is also say that a is a *divisor* of b, that a is a *factor* of b, or that b is a *multiple* of a.

Theorem 8. 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. Clearly (a) is obvious.
(b)

$$\begin{aligned} a \mid 1 &\iff \exists\, t \in \mathbb{Z} \text{ s.t. } 1 = t \cdot a. \\ &\iff t = 1 = a \text{ or } t = -1 = a. \\ &\implies a = \pm 1. \end{aligned}$$

c)

$$\begin{aligned} a \mid b &\implies \exists\, t_1 \in \mathbb{Z} \text{ s.t. } b = t_1 \cdot a. \\ c \mid d &\implies \exists\, t_2 \in \mathbb{Z} \text{ s.t. } d = t_2 \cdot c. \\ &\implies bd = (t_1 t_2)\, ac. \\ &\implies ac \mid bd. \end{aligned}$$

d)

$$\begin{aligned} a \mid b &\implies \exists\, t_1 \in \mathbb{Z} \text{ s.t. } b = t_1 \cdot a. \\ b \mid c &\implies \exists\, t_2 \in \mathbb{Z} \text{ s.t. } c = t_2 \cdot b. \\ &\implies c = t_2(t_1 a) = (t_2 t_1) a. \\ &\implies a \mid c. \end{aligned}$$

e)

$$a \mid b \implies \exists t_1 \in \mathbb{Z} \text{ s.t. } b = t_1 \cdot a.$$

$$b \mid a \implies \exists t_2 \in \mathbb{Z} \text{ s.t. } a = t_2 \cdot b.$$

$$a \mid b \text{ and } b \mid a \iff a = t_2 b = (t_1 t_2) a$$

$$\implies t_1 t_2 = 1.$$

$$\implies t_1 = 1, t_2 = 1 \text{ or } t_1 = -1, t_2 = -1.$$

$$\iff a = \pm b.$$

(f) $a \mid b \implies \exists\, t_1 \in \mathbb{Z}$ s.t. $b = t_1 \cdot a$.
Since $b \neq 0$, $t_1 \neq 0$.

$$|b| = |t_1 a| = |t_1| \cdot |a|.$$

$$|b| > |a| \quad (\because |t_1| > 1).$$

(g) $a \mid b \implies \exists\, t_1 \in \mathbb{Z}$ s.t. $b = t_1 \cdot a$.
$a \mid c \implies \exists\, t_2 \in \mathbb{Z}$ s.t. $c = t_2 \cdot a$.

Now

$$bx + cy = t_1 \cdot ax + t_2 \cdot ay = (t_1 x + t_2 y) a$$

$$\implies a \mid (b + c). \quad (\because t_1 x + t_2 y \in \mathbb{Z}).$$

□

Note 9. The property (g) of previous Theorem extends by induction to sums of more than two terms. That is, if $a \mid b_k$ for $k = 1, 2, \ldots, n$, then

$$a \mid (b_1 x_1 + b_2 x_2 + \cdots + b_n x_n)$$

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

Definition 10. Let a and b be given integers with $a \neq 0$ (or) $b \neq 0$. The greatest common divisor of a, b, $\gcd(a, b)$ is the positive integer d satisfying the following:

1. $d \mid a$ and $d \mid b$.
2. If $c \mid a$, $c \mid b$, then $c \mid d$.

Example 11. 1. The positive divisors of -12 are $1, 2, 3, 4, 6, 12$.
2. The positive divisors of 30 are $1, 2, 3, 5, 6, 10, 15, 30$.

The positive common divisors of $(-12, 30)$ are $1, 2, 3, 6$.
Here the largest is 6.

$$\gcd(-12, 30) = 6.$$

Theorem 12. Given integers a and b, not both of which are zero, there exist integers x and y s.t. $\gcd(a, b) = ax + by$.

Proof. Consider the set S of all positive linear combinations of a and b.

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

If $a \neq 0$, then $|a| = au + b.0$, where $u = \pm 1$.

$$\Rightarrow |a| \in S$$

Hence $S \neq \emptyset$.

By well ordering principle, S must contain a smallest element 'd'.

By definition of S, $\exists x, y \in \mathbb{Z}$ s.t

$$d = ax + by.$$

claim: $d = \gcd(a, b)$.

consider a, d.

By Division Algorithm, $\exists\ q, r \in \mathbb{Z}$ s.t

$$a = qd + r, \quad 0 \leq r < d$$

$$\Rightarrow r = a - qd.$$

$$= a - q(ax + by)$$

$$r = a(1 - qx) + b(-qy)$$

Since r is positive, $r \in S$.

But $r = a - qd < d \Rightarrow\Leftarrow$.

Thus $r = 0$.

Hence $a = qd$.

$$\therefore d \mid a.$$

Similarly $d \mid b$.

Suppose c is common divisor of a and b. Then $c \mid a$, $c \mid b$.

By Theorem 8,

$$c \mid ax + by$$

$$c \mid d.$$

By Theorem 8, $|c| \leq |d|$.

$$c \leq d.$$

Hence $d = \gcd(a, b)$. □

Corollary 13. If a and b are given integers not both zero, then the set

$$T = \{ax + by : x, y \in \mathbb{Z}\}$$

is precisely the set of multiples of $d = \gcd(a, b)$.

Proof. Let $d = \gcd(a, b)$. Since $d \mid a$, $d \mid b$, $d \mid ax + by, \forall x, y \in \mathbb{Z}$.

$$\Rightarrow ax + by \text{ is a multiple of } d.$$

Hence every member of T is a multiple of d. Conversely, suppose $d = ax_0 + by_0$, for some $x_0, y_0 \in \mathbb{Z}$. Any multiple of d, $nd = n(ax_0 + by_0) = a(nx_0) + b(ny_0) \Rightarrow nd$ is a linear combination of a and b and so $nd \in T$.
$\therefore T =$ set of all multiples of d. □

Definition 14. Two integers a and b, not both of which are zero, are said to be relatively prime if $\gcd(a, b) = 1$.

Theorem 15. Let a and b be integers, not both zero. Then a and b are relatively prime iff $\exists$ integers x and y s.t. $1 = ax + by$.

Proof. Suppose a and b are relatively prime. Then $\gcd(a, b) = 1$. By Theorem 12, there exist integers x, y s.t. $k = \gcd(a, b) = ax + by$.

$$\Rightarrow 1 = ax + by.$$

Conversely, suppose there exist integers x and y s.t. $1 = ax + by$ & $d = \gcd(a, b)$

$$\begin{aligned}
&\Rightarrow d \mid a,\ d \mid b \\
&\Rightarrow d \mid ax + by,\ \forall x', y' \text{ (by theorem 8)} \\
&\Rightarrow d \mid ax + by \text{ (particularly)} \\
&\Rightarrow d \mid 1 \\
&\Rightarrow d = \pm 1.
\end{aligned}$$

But d is positive, $d = 1$.

$$\therefore \gcd(a, b) = 1.$$

i.e. a, b are relatively prime. □

Corollary 16. If $\gcd(a, b) = d$, then

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

Proof. Suppose $\gcd(a, b) = d$. Then $\exists\, x, y \in \mathbb{Z}$ s.t.

$$d = ax + by.$$

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

By theorem 15,

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

□

Corollary 17. If $a \mid c$, $b \mid c$, with $\gcd(a,b) = 1$ then $ab \mid c$.

Proof. Given $a \mid c$, $b \mid c$.

$$a \mid c \Rightarrow \exists\, t_1 \in \mathbb{Z} \text{ s.t. } c = t_1 \cdot a.$$

$$b \mid c \Rightarrow \exists\, t_2 \in \mathbb{Z} \text{ s.t. } c = t_2 \cdot b.$$

Since $\gcd(a,b) = 1$, $\exists\, x, y \in \mathbb{Z}$ s.t.

$$1 = ax + by.$$

Now

$$\begin{aligned} c &= c \cdot 1 \\ &= c(ax + by) \\ &= acx + bcy \\ &= a(t_2 b)x + b(t_2 a)y \\ &= ab[t_2 x + t_1 y]. \end{aligned}$$

Thus $ab \mid c$.

□

Lemma 18. Euclid Lemma

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

Proof. Suppose $\gcd(a,b) = 1$. Then by Theorem 12, $\exists\, x, y \in \mathbb{Z}$ such that $1 = ax + by$.

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

Given $a \mid bc$. Also $a \mid ac \implies a \mid ac + bc \implies a \mid c$. □

Note 19. $\gcd(a,b) \neq 1$ and $a \mid bc \not\Rightarrow a \mid c$.
Take $a = 12$, $b = 9$, $c = 8$.
$\gcd(a,b) = \gcd(12,9) \neq 1$.
$12 \mid 9 \times 8$ ($a \mid bc$)
But $12 \nmid 9$ and $12 \nmid 8$.

Theorem 20. Let a, b be integers, not both zero. For a positive integer d, $d = \gcd(a,b)$ iff
(1) $d \mid a$, $d \mid b$
(2) Whenever $c \mid a$ and $c \mid b$, then $c \mid d$.

Proof. Suppose $d = \gcd(a,b)$. Then $d \mid a$, $d \mid b$. $\therefore$ (1) is true. Suppose $c \mid a$, $c \mid b$. Then $c \mid ax + by$, $\forall x, y$.

$$\Rightarrow c \mid d.$$

(2) is true. Conversely, let d satisfy (1), (2). From (2), $c \mid d \Rightarrow c = d$. Hence $d = \gcd(a,b)$. □

Exercise 2.3

1. If $a \mid b$, show that $(-a) \mid b$, $a \mid (-b)$, and $(-a) \mid (-b)$.
2. Given integers a, b, c, d, verify the following:
   (a) If $a \mid b$, then $a \mid bc$.
   (b) If $a \mid b$ and $a \mid c$, then $a^2 \mid bc$.
   (c) $a \mid b$ if and only if $ac \mid bc$, where $c \neq 0$.
   (d) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
3. Prove or disprove: If $a \mid (b+c)$, then either $a \mid b$ or $a \mid c$.
4. For $n \geq 1$, use mathematical induction to establish each of the following divisibility statements:
   (a) $8 \mid 5^{2n} + 7$. [Hint: $5^{2(k+1)} + 7 = 5^2(5^{2k} + 7) + (7 - 5^2 \cdot 7)$.]
   (b) $15 \mid 2^{4n} - 1$.
   (c) $5 \mid 3^{3n+1} + 2^{n+1}$.
   (d) $21 \mid 4^{n+1} + 5^{2n-1}$.
   (e) $24 \mid 2 \cdot 7^n + 3 \cdot 5^n - 5$.
5. Prove that for any integer a, one of the integers $a, a+2, a+4$ is divisible by 3.

2.4 EUCLIDEAN ALGORITHM

Lemma 21. If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$. By the Division Algorithm, $\exists\, q, r$ s.t.

$$a = bq + r; \quad 0 \leq r < b.$$

$$a - bq = r.$$

$$\Rightarrow d \mid a - bq \Rightarrow d \mid r$$

Hence $d|b$ and $d|r$ so d is the common multiple of b and r.
Let c be any arbitrary common divisor of b and r. If $c \mid b$, $c \mid r$

$$\Rightarrow c \mid qb, \quad c \mid r \Rightarrow c \mid qb + r.$$

$$\Rightarrow c \mid a \quad (\text{since } a = bq + r).$$

$$\therefore c \mid a \text{ and } c \mid b \text{ (both imply } c \mid d \text{ since } d = \gcd(a, b)).$$

$$\therefore c \leq d.$$

$$d = \gcd(b, r).$$

Thus $\gcd(b, r) = \gcd(a, b)$. □

Note 22. Consider the system of equations

$$a = q_1 b + r_1, 0 \le r_1 < b, b = q_2 r_1 + r_2, 0 \le r_2 < r_1.$$

$$\begin{aligned} r_1 &= q_2 r_2 + r_3 \quad ; 0 \le r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n; \quad 0 \le r_n < r_{n-1} \\ r_{n-1} &= q_n r_n + 0 \end{aligned}$$

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

$$(d \mid b \text{ and } d \mid r_1) \iff \gcd(r_n, 0) = r_n.$$

Example 23. Find $\gcd(12378, 3054)$.

Solution.

$$\begin{aligned} 12378 &= 4 \times 3054 + 162 \\ 3054 &= 18 \times 162 + 138. \end{aligned}$$

$$\begin{aligned} 162 &= 1 \times 138 + 24 \\ 138 &= 5 \times 24 + 18 \\ 24 &= 1 \times 18 + 6 \\ 18 &= 3 \times 6 + 0 \end{aligned}$$

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

Theorem 24. If $k > 0$, then $\gcd(ka, kb) = k \gcd(a, b)$.

Proof. Let $d = \gcd(a, b)$. Then Euclidean Algorithm for a and b is multiplied by k, i.e.,

$$\begin{aligned} ak &= q_1(bk) + r_1 k \\ bk &= q_2(r_1 k) + r_2 k \text{ with} 0 \le r_2 k < b_1 k. \end{aligned}$$

$$bk = q_2(r_1 k) + r_2 k; \quad 0 \le r_2 k < r_1 k$$

$$r_{n-2} k = q_n(r_{n-1} k) + r_n k; \quad 0 \le r_n k < r_{n-1} k$$

$$r_{n-1} k = q_{n+1}(r_n k) + 0.$$

$$\gcd(ka, kb) = r_n k = k \cdot \gcd(a, b)$$

□

Corollary 25. For any integer $k \ne 0, \gcd(ka, kb) = |k| \cdot \gcd(a, b)$.

Proof. It suffices to consider the case in which $k < 0$.
Then $-k = |k| > 0$. By Theorem 24,

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

$$\gcd(ak, bk) = |k| \cdot \gcd(a, b)$$

□

Example 26. Find $gcd(12, 30)$.

$$\begin{aligned}\gcd(12, 30) &= \gcd(3 \times 4, 3 \times 10)\\ &= 3 \cdot \gcd(4, 10)\\ &= 3 \times 2 \cdot \gcd(2, 5)\\ &= 3 \times 2 \times 1 = 6.\end{aligned}$$

Definition 27. The *least common multiple* of two nonzero integers a, b, lcm(a, b), is the positive integer m satisfying

(i) $a \mid m, b \mid m$.

(ii) If $a \mid c$, $b \mid c$, with $c > 0$, then $m \mid c$.

Example 28. $\operatorname{lcm}(-12, 30) = 60$.

Theorem 29. For positive integers a, b,

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

Proof. Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$. $\Rightarrow a = dr, \quad b = ds$, for some $r, s \in \mathbb{Z}$. If $m = \frac{ab}{d}$, then $m = as = rb$.

Let c be a common multiple of a, b. Then $c = au = bv$. Since $d = \gcd(a, b)$, $\exists\, x, y \in \mathbb{Z}$ s.t.

$$d = ax + by.$$

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

This implies $m \mid c$ and so $m \leq c$. By definition m=lcm(a,b).
(i.e) $lcm(a, b) = \frac{ab}{d} = \frac{ab}{gcd(a,b)}$. □

Corollary 30. For any choice of positive integers a and b, $lcm(a, b) = ab$ if and only if $gcd(a, b) = 1$.

Example 31. Find lcm(3054,12378)

$$\begin{aligned}\mathrm{lcm}(3054, 12378) &= \frac{3054 \times 12378}{\gcd(3054, 12378)}\\ &= \frac{3054 \times 12378}{6}\\ &= 6300402.\end{aligned}$$

Exercise 2.4

1. Find $\gcd(143, 227)$, $\gcd(306, 657)$, and $\gcd(272, 1479)$.

2. Use the Euclidean Algorithm to obtain integers x and y satisfying the following:

   (a) $\gcd(56, 72) = 56x + 72y$.

   (b) $\gcd(24, 138) = 24x + 138y$.

   (c) $\gcd(119, 272) = 119x + 272y$.

   (d) $\gcd(1769, 2378) = 1769x + 2378y$.

3. Prove that if d is a common divisor of a and b, then $d = \gcd(a, b)$ if and only if $\gcd(a/d, b/d) = 1$. [Hint: Use Theorem 2.7.]

4. Assuming that $\gcd(a, b) = 1$, prove the following:

   (a) $\gcd(a + b, a - b) = 1$ or 2. [Hint: Let $d = \gcd(a + b, a - b)$ and show that $d \mid 2a$, $d \mid 2b$, and thus that $d \leq \gcd(2a, 2b) = 2\gcd(a, b)$.]

   (b) $\gcd(2a + b, a + 2b) = 1$ or 3.

   (c) $\gcd(a + b, a^2 + b^2) = 1$ or 2. [Hint: $a^2 + b^2 = (a + b)(a - b) + 2b^2$.]

   (d) $\gcd(a + b, a^2 - ab + b^2) = 1$ or 3. [Hint: $a^2 - ab + b^2 = (a + b)^2 - 3ab$.]

5. For $n \geq 1$, and positive integers a, b, show the following:

   (a) If $\gcd(a, b) = 1$, then $\gcd(a^n, b^n) = 1$. [Hint: See Problem 20(a), Section 2.2.]

   (b) The relation $a^n \mid b^n$ implies that $a \mid b$. [Hint: Put $d = \gcd(a, b)$ and write $a = rd$, $b = sd$, where $\gcd(r, s) = 1$. By part (a), $\gcd(r^n, s^n) = 1$. Show that $r = 1$, whence $a = d$.]

6. Prove that if $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$.

7. For nonzero integers a and b, verify that the following conditions are equivalent:

   (a) $a \mid b$.

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

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

   (d) $\mathrm{lcm}(a, b) = |b|$.

8. Find $\mathrm{lcm}(143, 227)$, $\mathrm{lcm}(306, 657)$, and $\mathrm{lcm}(272, 1479)$.

9. Prove that the greatest common divisor of two positive integers divides their least common multiple.

2.5 THE DIOPHANTINE EQUATION $ax + by = c$

Theorem 32. The linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$, where $d = \gcd(a, b)$. If x_0, y_0 is any particular solution of this equation, then all other solutions are given by $x = x_0 + \left(\frac{b}{d}\right) t \quad y = y_0 - \left(\frac{a}{d}\right) t$, where t is an arbitrary integer.

Proof. Suppose the linear Diophantine equation

$$ax + by = c$$

has a solution (x_0, y_0). Then

$$c = ax_0 + by_0. \tag{i}$$

Given $d = \gcd(a, b)$.

$$\Rightarrow d \mid a \text{ and } d \mid b.$$

$$\implies a = dr, \quad b = ds.$$

$$\therefore c = drx_0 + dsy_0 = d(rx_0 + sy_0).$$

$$\Rightarrow d \mid c.$$

Conversely, $d \mid c$ and $d = \gcd(a, b)$. Then

$$a(x' - x_0) = b(y_0 - y') \qquad (1)$$

Let $d = \gcd(a, b)$. Then $\exists\, r, s \in \mathbb{Z}$ s.t. $a = dr$, $b = ds$.

$$\begin{aligned} (1) &\Rightarrow dr(x' - x_0) = ds(y_0 - y') \\ &\Rightarrow r(x' - x_0) = s(y_0 - y') \\ &\Rightarrow r \mid s(y_0 - y') \\ &\Rightarrow r \mid (y_0 - y') \quad (\because \gcd(r, s) = 1) \end{aligned}$$

$$\begin{aligned} y_0 - y' &= rt \\ x' - x_0 &= st. \end{aligned}$$

$$\begin{aligned} x' &= x_0 + \left(\frac{b}{d}\right) t \\ y' &= y_0 - \left(\frac{a}{d}\right) t. \end{aligned}$$

Easy to see verify it satisfy Diophantine equation:

$$
\begin{aligned}
ax' + by' &= a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) \\
&= ax_0 + by_0 + \left(\frac{ab}{d} - \frac{ab}{d}\right)t.
\end{aligned}
$$

Now $ax' + by' = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right)$

$$
\begin{aligned}
&= ax_0 + by_0 + \left(\frac{ab}{d} - \frac{ab}{d}\right)t \\
&= ax_0 + by_0 + 0 \cdot t \\
&= c.
\end{aligned}
$$

For each value of t there are infinite number of solutions of the given equation. □

Example 33. Consider the linear Diophantine equation

$$172x + 20y = 1000. \quad (1)$$

Proof. First find $\gcd(172, 20)$.

$$
\begin{aligned}
172 &= 8 \times 20 + 12 \\
20 &= 1 \times 20 + 8 \\
12 &= 1 \times 4 + 4.
\end{aligned}
$$

Thus $\gcd(172, 20) = 4$. Here $d = 4$, $c = 1000$.
$d \mid c$ (4 | 1000).
By previous theorem, solution of equation (1) exists.

Find x_0, y_0

$$
\begin{aligned}
4 &= 12 - 8 \\
&= 12 - (20 - 12) = 2 \times 12 - 20 \\
&= 2\,(172 - 8 \times 20) - 20 \\
&= 2 \times 172 + (-17)\,20.
\end{aligned}
$$

Now

$$
\begin{aligned}
1000 &= 250 \times 4 \\
&= 250\,[\,2 \times 172 + (-17)\,20\,] \\
&= 500 \times 172 + (-4250)\,20.
\end{aligned}
$$

Thus $x_0 = 500$, $y_0 = -4250$ is one solution of Diophantine equation. All other solutions are expressed by

$$x = 500 + 5t \quad y = -4250 - 43t$$

□

Corollary 34. If $\gcd(a, b) = 1$ and if x_0, y_0 is a particular solution of the linear Diophantine equation

$ax + by = c$, then all solutions are given by

$$x = x_0 + bt, \quad y = y_0 - at$$

for integral values of t.

Example 35. The equation $5x + 22y = 18$ has $x_0 = 8$, $y_0 = -1$ as one solution; from the corollary, a complete solution is given by $x = 8 + 22t$, $y = -1 - 5t$ for arbitrary t.

Example 36. A customer bought a dozen pieces of fruit apples and oranges for 132. If an apple costs 3 cents more than an orange and more apples than oranges were purchased, how many pieces of each kind were bought?

Solution. Let x be the number of apples and y be the number of oranges purchased.
Let z be the cost of an orange (in cents).

Then

$$(x + y)z + 3x = 132$$

$$\implies xz + yz + 3x = 132.$$

Also,

$$x + y = 12.$$

So

$$\begin{aligned} 3x + (x + y)z &= 132 \\ 3x + 12z &= 132 \\ x + 4z &= 44. \end{aligned}$$

We have to find x, z satisfying the Diophantine equation

$$x + 4z = 44.$$

Since $\gcd(1, 4) = 1$ is a divisor of 44, there are integer solutions.

We have to find x, z satisfying Diophantine equation 1.

Since $\gcd(1, 4) = 1$ is a divisor of 44, there is a solution to the equation 2.

$$\gcd(1, 4) = 1 = 1(-3) + 4(1)$$

$$\Rightarrow 44 = 1(-132) + 4(44)$$

$\therefore x_0 = -132$; $z_0 = 44$ is one solution of 1. All other solutions are

$$x = -132 + 4t.$$

Given

$$6 \leq x \leq 12 \implies 6 \leq 4t - 132 \leq 12.$$

Solving the inequalities:

$$4t - 132 > 6 \implies t > 34.5$$
$$4t - 132 \leq 12 \implies t \leq 36.$$

Thus

$$t = 35, 36.$$

Thus there are two possible purchases:

1. A dozen apples costing 11 cents each (the case for $t = 36$).

2. 8 apples at 12 cents and 4 oranges at 9 cents each (the case for $t = 35$).

Example 37. Given a cock is worth 5 coins, a hen 3 coins, and three chicks 1 coin, how many cocks, hens and chicks totaling 100 can be bought for 100 coins?

Solution. Let x be the number of cocks, y be the number of hens, and z be the number of chicks. The equations are:

1. $x + y + z = 100$ (total number of birds)

2. $5x + 3y + \frac{1}{3}z = 100$ (total cost in coins)

Solving these equations:

$$\begin{cases} x + y + z = 100 \\ 15x + 9y + z = 300 \end{cases}$$
$$\Rightarrow 14x + 8y = 200$$
$$\Rightarrow 7x + 4y = 100.$$

Solving for integers $x, y, z \geq 0$,

$$x = 4, \quad y = 18, \quad z = 78.$$

The general solution is

$$\begin{cases} x = 4t \\ y = 25 - 7t \\ z = 75 + 3t \end{cases} \qquad t \in \mathbb{Z}.$$

For $t = 1 \Rightarrow x = 4$, $y = 18$, $z = 78$.
For $t = 2 \Rightarrow x = 8$, $y = 11$, $z = 81$.
For $t = 3 \Rightarrow x = 12$, $y = 4$, $z = 84$.

For $x > 0$, $y > 0$, $z > 0$,

$$y > 0 \Rightarrow 25 - 7t > 0 \Rightarrow t < \frac{25}{7},$$
$$z > 0 \Rightarrow 75 + 3t > 0 \Rightarrow t > -25.$$

Thus

$$-25 < t < \frac{25}{7}.$$

Therefore t=1,2,3 and $t > 0$

Exercise 2.5

1. Which of the following Diophantine equations cannot be solved?

   (a) $6x + 51y = 22$.

   (b) $33x + 14y = 115$.

   (c) $14x + 35y = 93$.

2. Determine all solutions in the integers of the following Diophantine equations:

   (a) $56x + 72y = 40$.

   (b) $24x + 138y = 18$.

   (c) $221x + 35y = 11$.

3. Determine all solutions in the positive integers of the following Diophantine equations:

   (a) $18x + 5y = 48$.

   (b) $54x + 21y = 906$.

   (c) $123x + 360y = 99$.

   (d) $158x - 57y = 7$.

4. If a and b are relatively prime positive integers, prove that the Diophantine equation $ax - by = c$ has infinitely many solutions in the positive integers.

   [Hint: There exist integers x_0 and y_0 such that $ax_0 + by_0 = c$. For any integer t, which is larger than both $|x_0|/b$ and $|y_0|/a$, a positive solution of the given equation is $x = x_0 + bt$, $y = -(y_0 - at)$.]

UNIT III

Primes and their Distribution

3.1. The Fundamental Theorem of Arithmetic

Definition 1. An integer $p > 1$ is called a prime number (prime) if its only positive divisors are 1 and p. An integer greater than 1 that is not a prime is called composite.

Example 2. 1. $2, 3, 5, 7$ are primes.

2. $4, 6, 8, 9, 10$ are composite.

Theorem 3. If p is a prime, and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof. If $p \mid a$, then the proof is over. So assume that $p \nmid a$. Clearly the only positive divisors of p are 1 and p itself.

$$\gcd(p, a) = 1$$

(In general, $\gcd(p, a) = p$ if $p \mid a$ and $\gcd(p, a) = 1$ if $p \nmid a$) By Euclid's lemma, $p \mid ab$ and $\gcd(p, a) = 1$

$$\Rightarrow \quad p \mid b.$$

□

Corollary 4. If p is a prime and

$$p \mid a_1 a_2 \dots a_n,$$

then $p \mid a_k$ for some $k, 1 \leq k \leq n$.

Proof. Proof is by induction on n, where n is the number of factors.

Then $P(n) : p \mid a_1 a_2 \cdots a_n \Rightarrow p \mid a_k$ for some k.
Take $n = 1$. Then $p \mid a_1$. It is obvious.
Take $n = 2$. Then $p \mid a_1 a_2$. By Theorem 3, $p \mid a_1$ or $p \mid a_2$.
Now $p \mid a_1 a_2 \dots a_n$. By Theorem 3, $p \mid (a_n)$ or $p \mid a_1 a_2 \dots a_{n-1}$.
For $p \mid a_1, a_2, \dots a_{n-1}$, use induction for $n - 1$, p $\mid a_i$, $1 \leq i \leq n - 1$. Already, we have $p \mid a_n$.
$\therefore P \mid a_i$, $1 \leq i \leq n$.
Hence $P(n)$ is true $\forall n \in \mathbb{N}$.
Thus $P \mid a_1 \dots a_n$, then $P \mid a_i$ for some i, $1 \leq i \leq n$. □

Corollary 5. *If $p, q_1, q_2, \dots q_n$ are all primes and $p \mid q_1 q_2 \dots q q_n$, then $p = q_k$ for some k, $1 \leq k \leq n$.*

Proof. Given $p \mid q_1 q_2 \dots q_n$.

Then by corollary, $p \mid a_k$ for some k, $1 \leq k \leq n$.
Since q_k is prime, $p = 1$ or $q_k = p$.
Since p is prime, $p > 1$.
$\therefore p = q_k$. □

Theorem 6. (Fundamental Theorem of Arithmetic)
Every positive integer $n > 1$ is either a prime or a product of primes. This representation is unique, apart from the order in which the factors occur.

Proof. Let n be a positive integer and $n > 1$. Then either n is prime or n is composite.

- If n is prime, then the statement is obvious.

- If n is composite, then there exists an integer d satisfying $d \mid n$ and $1 < d < n$.

Among all such integers d, choose p_1 to be the smallest. (By well-ordering principle) Suppose p_1 is composite.Then $\exists\ q \in \mathbb{Z}$ s.t. $q|p_1$ and $1 < q < p_1$.
$p_1|n$ and $q|p_1 \Rightarrow q|n$, $1 < q < p_1 < n$ which is a contradiction to p_1 is smallest $\leq p_1$.
$\therefore p_1$ must be prime.
Hence $n = p_1.n_1$, where p_1 is prime and $1 < n_1 < n$.

If n_1 is prime, then we have required representation.

If n_1 is not prime composite, then the above argument repeated and we get a second prime number p_2 s.t $n_1 = p_2.n_2$
(i.e) $n = p_1p_2n_2, 1 < n_2 < n$.

If n_2 is prime, then it is not necessary to go further.

If n_2 is composite, then $n_2 = p_3n_3$, with p_3 prime,

$n = p_1p_2p_3n_3$, $1 < n_3 < n_2$.

The decreasing sequence $n > n_1 > n_2 > n_3 > \ldots > 1$ cannot continue indefinitely.

After a finite number of steps, we get n_k is a prime and take it as p_k. The prime factorization

$$n = p_1p_2 \cdots p_r$$

Uniqueness: Suppose that the integer n can be represented as a product of primes in two ways.

$$n = p_1 \cdot p_2 \cdots p_r \quad \text{and} \quad n = q_1 \cdot q_2 \cdots q_s, \quad r \leq s$$

when p_i and q_j are all primes st

$$p_1 \leq p_2 \leq \cdots \leq p_r \quad \& \quad q_1 \leq q_2 \leq \cdots \leq q_s.$$

we have $p_1p_2 \cdots p_r = q_1q_2 \cdots q_s$.......(*)

$$\implies p_1|q_1q_2 \cdots q_s.$$

By corollary 4, $p_1 = q_k$ for some k.

$$\implies p_1 = q_1$$

Cancel the common factor in (*) and obtain

$$\implies p_2p_3 \cdots p_r = q_2q_3 \cdots q_s......(1)$$

Repeat the process, we get $p_2 = q_2$ & cancel in ①

$$\implies p_3 \cdots p_r = q_3 \cdots q_s.$$

Continue this process. $1 = q_1 \cdot q_2 \cdots q_r$, which is separable because each $q_j > 1$.
$\Rightarrow$ Hence $r = s$ and $p_i = q_i \forall i$
Hence every positive integer can be uniquely expressed as product of primes. □

Example 7. The illustration of the canonical form of the integer
$360 = 2^3 \cdot 3^2 \cdot 5$.
$4725 = 3^3 \cdot 5^2 \cdot 7$ and
$17460 = 2^2 \cdot 3^2 \cdot 5 \cdot 7^2$.

Theorem 8. (Pythagoras)
The number $\sqrt{2}$ is irrational

Proof. Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$.

$$\sqrt{2} = \frac{a}{b} \Rightarrow 2 = \frac{a^2}{b^2}$$

$$\Rightarrow 2b^2 = a^2$$

$$\Rightarrow b \mid a^2$$

If $b > 1$, then by Fundamental theorem of arithmetic $p \mid b$

$$\text{since } b \mid a^2, p \mid a^2.$$

By Theorem 3., $p \mid a$.
Hence $p|a$ & $p|a$.
$\therefore \gcd(a, b) \geq p$ which is a contradiction to $gcd(a, b) = 1$.
$\gcd(a, b) = 1 \Rightarrow b = 1$.
$(1) \Rightarrow a^2 = 2$, which is also impossible.
Hence our supposition $\sqrt{2}$ is rational is wrong. Hence $\sqrt{2}$ must be irrational. □

Exercise 3.1

1. It has been conjectured that there are infinitely many primes of the form $n^2 - 2$. Exhibit five such primes.

2. Give an example to show that the following conjecture is not true: Every positive integer can be written in the form $p + a^2$, where p is either a prime or 1, and $a \geq 0$.

3. Prove each of the assertions below:

    (a) Any prime of the form $3n + 1$ is also of the form $6m + 1$.

(b) Each integer of the form $3n + 2$ has a prime factor of this form.

(c) The only prime of the form $n^3 - 1$ is 7. [Hint: Write $n^3 - 1$ as $(n - 1)(n^2 + n + 1)$.]

(d) The only prime p for which $3p + 1$ is a perfect square is $p = 5$.

(e) The only prime of the form $n^2 - 4$ is 5.

4. If $p \geq 5$ is a prime number, show that $p^2 + 2$ is composite. [Hint: p takes one of the forms $6k + 1$ or $6k + 5$.]

5. (a) Given that p is a prime and $p \mid a^n$, prove that $p^n \mid a^n$.

   (b) If $\gcd(a, b) = p$, a prime, what are the possible values of $\gcd(a^2, b^2)$, $\gcd(a^2, b)$ and $\gcd(a^3, b^2)$?

3.2 THE SIEVE OF ERATOSTHENES

Lemma 9. Every composite number a will possess a prime divisor p satisfying $p \leq \sqrt{a}$.

Proof. Given a composite number a, assume that $a = bc, 1 < b \leq c \leq a.$
Without loss of generality assume that $b \leq c$. Then $b^2 \leq bc = a \Rightarrow b \leq \sqrt{a}$
. Since b ¿ 1, b has a prime divisor p. By the Fundamental Theorem of Arithmetic $p \mid b, b \mid a$. Hence $p \mid a$. Since $p \mid b$, we have $p \leq b$. From $b \leq \sqrt{a}, p \leq \sqrt{a}$. □

Note 10. Now this technique is used for finding all primes below a given integer n .
1. Write down the integer 2 up n in natural number order
2. Eliminate all composite numbers by striking out multiples of 2p, 3p, 5p, ... of the prime $p \leq \sqrt{n}$.
3. The integers that do not fall through the Sieve Eratosthenes are the integers that are left on the list of primes.

Problem 11. Find all the prime numbers below 100.

Solution:
The prime numbers below 100 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89,97.

Theorem 12. Euclid. There is an infinite number of primes.

Proof. The Euclid's proof is by contradiction. Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$. Arrange the primes in ascending order, and suppose that there is a last prime,say p_n. Now consider the positive integer

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

Since $P > 1$ and by Theorem 6,P is divisible by some prime p. But $p_1, p_2, \ldots, p_n$ are the only prime numbers, so $p = P$ for some prime P from $p_1, p_2, \ldots, p_n$.
Now $p \mid P$ and $p \mid p_1 p_2 \cdots p_n$
$\Rightarrow p \mid (P - p_1 p_2 \cdots p_n)$

$\Rightarrow p \mid 1.$

Thus the only positive divisor of the integer 1 is 1 itself, a contradiction because $p > 1$.

Thus, no finite list of primes is complete. Hence the number of primes is infinite. □

Note 13. Euclidean Numbers's

For a prime p, define $p^{\#}$ to be the product of all primes that are less than or equal to p. Numbers of the form $p^{\#} + 1$ is known as *Euclidean numbers*, because they appear in Euclid's scheme for proving the infinitude of primes. It is interesting that in forming these integers, the first five, namely,

$$\begin{aligned}
2^{\#} + 1 &= 2 + 1 = 3\\
3^{\#} + 1 &= 2 \cdot 3 + 1 = 7\\
5^{\#} + 1 &= 2 \cdot 3 \cdot 5 + 1 = 31\\
7^{\#} + 1 &= 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211\\
11^{\#} + 1 &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311
\end{aligned}$$

However the numbers

$$\begin{aligned}
13^{\#} + 1 &= 59 \cdot 509\\
17^{\#} + 1 &= 19 \cdot 97 \cdot 277\\
19^{\#} + 1 &= 347 \cdot 27953
\end{aligned}$$

are not prime.

Theorem 14. If p_n is the nth prime number, then $p_n \leq 2^{2^{n-1}}$........$(*)$

Proof. Proof is by induction on n.

Take $n = 1$,

$$2^{2^{1-1}} = 2^{2^0} = 2 = 2$$

$p_1 = 2$ is the first prime number.

$\therefore$ The statement is true for $n = 1$.

Assume that the statement hold for all integers upto n. To prove the result is true for $n + 1$.

To prove, $P_{n+1} \leq 2^{2^n}$.

Now

$$\begin{aligned}
P_{n+1} &\leq P_1 \cdot P_2 \cdots P_n + 1\\
&\leq 2 \cdot 2^2 \cdot 2^{2^2} \cdots 2^{2^{n-1}} + 1\\
&= 2^{(1+2+2^2+\cdots+2^{n-1})} + 1.
\end{aligned}$$

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

$$\Longrightarrow \; P_{n+1} \leq 2^{2^n - 1} + 1.$$

Always $1 \leq 2^{2^n - 1}, \forall n.$

$$\begin{aligned}P_{n+1} &\leq 2^{2^n} + 2^{2^{n-1}}\\ &= 2^{2^{n-1}} \times (2^{2^{n-1}-2^{n-1}} + 1)\\ &= 2^{2^{n-1}} \times 2\\ &= 2^{2^{n-1}+1}\\ \therefore P_{n+1} &\leq 2^{2^n}\end{aligned}$$

Hence the result $*$ is true for $n+1$.
Thus $P_n \leq 2^{2^n}, \forall n \in \mathbb{N}$. □

Corollary 15. For $n > 1$, there are at least n primes less than 2^{2^n}.

Proof. From previous theorem,

$$p_{n+1} \leq 2^{2^n}.$$

Always $P_1 < P_2 < P_3 < \ldots < P_{n+1} \leq 2^{n+1}$
Hence $P_1, P_2, \ldots, P_{n+1}$ are all primes less than 2^{n+1} □

Exercise 3.2

1. Determine whether the integer 701 is prime by testing all primes $p \leq \sqrt{701}$ as possible divisors. Do the same for the integer 1009.

2. Employing the Sieve of Eratosthenes, obtain all the primes between 100 and 200.

3. Given that $p \nmid n$ for all primes $p \leq \sqrt[3]{n}$, show that $n > 1$ is either a prime or the product of two primes.

   [Hint: Assume to the contrary that n contains at least three prime factors.]

4. Establish the following facts:

   (a) $\sqrt{p}$ is irrational for any prime p.

   (b) If $a > 0$ and $\sqrt[n]{a}$ is rational, then $\sqrt[n]{a}$ must be an integer.

   (c) For $n \geq 2$, $\sqrt[n]{n}$ is irrational.

   [Hint: Use the fact that $2^n > n$.]

5. Show that any composite three-digit number must have a prime factor less than or equal to 31.

6. Fill in any missing details in this sketch of a proof of the infinitude of primes: Assume that there are only finitely many primes, say $p_1, p_2, \ldots, p_n$. Let A be the product of any r of these primes and put $B = p_1 p_2 \cdots p_n / A$. Then each p_k divides either A or B, but not both. Because $A + B > 1$, $A + B$ has a prime divisor different from any of the p_k, which is a contradiction.

7. Modify Euclid's proof that there are infinitely many primes by assuming the existence of a largest prime p and using the integer $N = p! + 1$ to arrive at a contradiction.

3.3 THE GOLDBACH CONJECTURE

Lemma 16. The product of two or more integers of the form $4n + 1$ is of the same form.

Proof. It is sufficient to consider the product of just two integers.
Let $k = 4n + 1$ and $k' = 4m + 1$. Then

$$\begin{aligned} kk' &= (4n + 1)(4m + 1) \\ &= 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1 \end{aligned}$$

which is of the desired form. □

Theorem 17. There are an infinite number of primes of the form $4n + 3$.

Proof. Assume that there exist only finitely many primes of the form $4n + 3$ say $q_1, q_2, \ldots, q_s$.
Consider the positive integer

$$N = 4q_1q_2 \cdots q_s - 1 = 4(q_1q_2 \cdots q_s - 1) + 3$$

and let $N = r_1r_2 \cdots r_t$ be its prime factorization.
Since N is an odd integer, we have $r_k \neq 2$ for all k, so that each r_i is either of the form $4n + 1$ or $4n + 3$. By the lemma 16, the product of any number of primes of the form $4n + 1$ is again an integer of this type. For N to take the form $4n + 3$, as it clearly does, N must contain at least one prime factor r_i of the form $4n + 3$. But r_i cannot be found among the listing $q_1, q_2, \ldots, q_s$, which is a contradiction that $r_i \mid 1$. The only possible conclusion is that there are infinitely many primes of the form $4n + 3$. □

Theorem 18. If all the $n > 2$ terms of the arithmetic progression

$$p, p + d, p + 2d, \ldots, p + (n - 1)d$$

are prime numbers, then the common difference d is divisible by every prime $q < n$.

Proof. Consider a prime number $q < n$ and assume that $q \nmid d$.
claim: The first q terms of the progression

$$p, p + d, p + 2d, \ldots, p + (q - 1)d \tag{1}$$

will leave different remainders when divided by q.
If not, there exist integers j and k, with $0 \leq j < k \leq q - 1$, such that the numbers $p + jd$ and $p + kd$ yield the same remainder upon division by q.
Then q divides their difference $(k - j)d$.
But $\gcd(q, d) = 1$, and so Euclid's lemma leads to $q \mid k - j$, which is a contradiction to $k - j \leq q - 1$.
Since q different remainders produced from Eq. (1) are drawn from the q integers $0, 1, \ldots, q - 1$, one of these remainders must be zero. Hence $q \mid p + td$ for some t satisfying $0 \leq t \leq q - 1$. Since $q < n \leq p \leq p + td$, $p + td$ is composite. If p were less than n, one of the terms of the progression would be $p + pd = p(1 + d)$ which is a contradiction. Hence $q \mid d$. □

Exercise 3.3

1. Verify that the integers 1949 and 1951 are twin primes.

2. (a) If 1 is added to a product of twin primes, prove that a perfect square is always obtained.

   (b) Show that the sum of twin primes p and $p+2$ is divisible by 12, provided that $p > 3$.

3. Find all pairs of primes p and q satisfying $p - q = 3$.

4. Sylvester (1896) rephrased the Goldbach conjecture: Every even integer $2n$ greater than 4 is the sum of two primes, one larger than $n/2$ and the other less than $3n/2$. Verify this version of the conjecture for all even integers between 6 and 76.

5. In 1752, Goldbach submitted the following conjecture to Euler: Every odd integer can be written in the form $p + 2a^2$, where p is either a prime or 1 and $a \geq 0$. Show that the integer 5777 refutes this conjecture.

6. Prove that the Goldbach conjecture that every even integer greater than 2 is the sum of two primes is equivalent to the statement that every integer greater than 5 is the sum of three primes.[Hint: If $2n - 2 = p_1 + p_2$, then $2n = p_1 + p_2 + 2$ and $2n + 1 = p_1 + p_2 + 3$.]

7. A conjecture of Lagrange (1775) asserts that every odd integer greater than 5 can be written as a sum $p_1 + 2p_2$, where p_1, p_2 are both primes. Confirm this for all odd integers through 75.

UNIT IV

4.2 BASIC PROPERTIES OF CONGRUENCE

Definition 1. Let n be a fixed positive integer. Two integers a and b are said to be *congruent modulo* n $a \equiv b \pmod{n}$ if n divides $a - b$.

Example 2. 1. $24 \equiv 3 \pmod{7}$.

2. $-31 \equiv 11 \pmod{7}$.

3. $-15 \equiv -64 \pmod{7}$.

Note 3. If $n \nmid (a - b)$, then $a \not\equiv b \pmod{n}$.
a is incongruent to b modulo n.

Example 4. $25 \not\equiv 12 \pmod{7}$ since

$$25 - 12 = 13 \not\equiv 0 \pmod{7}.$$

Note 5. $a \equiv 0 \pmod{n} \iff n \mid a$.

Remark 6. 1. By Division Algorithm, for a & n, $\exists\, q, r \in \mathbb{Z}$ s.t.

$$a = qn + r, \quad 0 \leq r < n.$$

By definition of congruence,

$$a \equiv r \pmod{n}.$$

2. Since there are n choices for r, every integer is congruent modulo n to one of $0, 1, 2, \ldots, n - 1$.
Every integer is congruent modulo n to exactly one of the values $0, 1, 2, \ldots, n - 1$.
Also $a \equiv 0 \pmod{n}$ iff $n \mid a$.
The set of integers $0, 1, 2, \ldots, n - 1$ is called the set of least nonnegative residues modulo n.

3.In general, a collection of n integers $a_1, a_2, \ldots, a_n$ is said to form a *complete set of residues* modulo n if every integer is congruent modulo n to one and only one of the a_k.

Example 7. $-12, -4, 11, 13, 22, 82, 91$ constitute a complete set of residues modulo 7.

$$-12 \equiv 2, \quad -4 \equiv 3, \quad 11 \equiv 4, \qquad 13 \equiv 6,$$
$$22 \equiv 1, \quad 82 \equiv 5, \quad 91 \equiv 0 \quad \text{all modulo 7.}$$

Theorem 8. For arbitrary integers a and b $a \equiv b \pmod{n}$ if and only if a and b leave the same non-negative remainder when divided by n.

Proof. Suppose $a \equiv b \pmod{n}$. Then $n \mid (a - b)$.

$$\Rightarrow a - b = kn, \quad k \in \mathbb{Z}. \qquad (1)$$

By Division Algorithm, $\exists$ q and r

$$b = qn + r; \quad 0 \leq r < n. \qquad (2)$$

$$\begin{aligned}
(1) \Rightarrow \quad a &= b + kn \\
&qn + r + kn \\
a &= (q+k)n + r. \\
\therefore a &\equiv r \pmod{n}.
\end{aligned}$$

$$\begin{aligned}
(2.) \Rightarrow \quad b &= qn + r \\
b &\equiv r \pmod{n}.
\end{aligned}$$

Hence a and b leave the same remainder (non-negative) when divided by n.

Conversely, suppose a and b leave the same remainder when divided by n. Then

$$\begin{aligned}
a &= q_1 n + r, \\
b &= q_2 n + r, \quad 0 \leq r < n.
\end{aligned}$$

$$\begin{aligned}
\Rightarrow \quad a - b &= q_1 n - q_2 n \\
a - b &= (q_1 - q_2)n \\
\therefore \quad a - b &\equiv 0 \pmod{n} \text{ and } n \mid (a-b). \\
\therefore \quad a &\equiv b \pmod{n}.
\end{aligned}$$

□

Example 9. Consider the integers -56 and -11.

$$-56 = (-7)9 + 7.$$

$$-11 = (-2)9 + 7.$$

$$\Longrightarrow -56 \equiv -11 \pmod{9}.$$

Other way,

$$-31 \equiv 11 \pmod{7}.$$

$$-31 = (-5)7 + 4; \quad 11 = 1 \cdot 7 + 4.$$

Remainders are same.

Theorem 10. Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

1. $a \equiv a \pmod{n}$.

2. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

4. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

5. If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$.

6. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for all $k \in \mathbb{Z}^+$.

Proof. (1) To prove $a \equiv a \pmod{n}$.
For any integer a, $a - a = 0 = 0 \cdot n$.
$\therefore a \equiv a \pmod{n}$.
(2) To prove **Symmetry**: $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$.

$$\begin{aligned} \text{Given } a &\equiv b \pmod{n} \\ \text{Then } n &\mid a - b \\ \Rightarrow& a - b = k_1 n, \quad k_1 \in \mathbb{Z} \\ \Rightarrow& b - a = (-k_1)n, \quad -k_1 \in \mathbb{Z}. \end{aligned}$$

$$\therefore n \mid b - a.$$

$$\text{Hence } b \equiv a \pmod{n}.$$

(3) To prove **Transitivity**: If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

$$\begin{aligned} a \equiv b \pmod{n} &\Rightarrow a - b = k_1 n \\ b \equiv c \pmod{n} &\Rightarrow b - c = k_2 n. \end{aligned}$$

$$\begin{aligned} a - c &= (a - b) + (b - c) \\ &= k_1 n + k_2 n \\ &= (k_1 + k_2)n. \end{aligned}$$

$$\begin{aligned} n &\mid a - c \\ \therefore a &\equiv c \pmod{n}. \end{aligned}$$

Given $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

Then

$$a - b = k_3 n, \quad c - d = k_4 n.$$

To prove (i) $a + c \equiv b + d \pmod{n}$,

$$(a + c) - (b + d) = (a - b) + (c - d) = k_3 n + k_4 n = (k_3 + k_4)n.$$

$$\therefore a + c \equiv b + d \pmod{n}.$$

To prove (ii) $ac \equiv bd \pmod{n}$,

$$\begin{aligned} ac &= (b + k_3 n)(d + k_4 n) \\ &= bd + (bk_3 + dk_4 + k_3 k_4 n)n. \end{aligned}$$

$$\therefore ac - bd = [bk_3 + dk_4 + k_3 k_4 n]n.$$

$$ac \equiv bd \pmod{n}.$$

Suppose $bk_3 + dk_4 \equiv k_3 k_4 n \in \mathbb{Z}$,

$$ac \equiv bd \pmod{n}.$$

(5) Given $a \equiv b \pmod{n}$. Then $a - b = kn$, $k \in \mathbb{Z}$.

To prove $a + c \equiv b + c \pmod{n}$.

$$(a + c) - (b + c) = a - b = kn.$$

$\therefore a + c \equiv b + c \pmod{n}$.

(6) Given $a \equiv b \pmod{n}$ — (1)

Then $a - b = kn$, $k \in \mathbb{Z}$.

Let

$$P(k) : a^k \equiv b^k \pmod{n}, \quad \forall k \in \mathbb{Z}^+.$$

We prove $\circledast$ by induction on k.

For $k = 1$, the statement $\circledast$ holds from (1). Assume that $a \equiv b \pmod{n}$.

(i) $P(k)$ is true.

(ii) $P(k + 1)$ is true.

From (1), (2),

$$a \equiv b \pmod{n} \text{ and } a^k \equiv b^k \pmod{n}.$$

By

$$a \cdot a^k \equiv b \cdot b^k \pmod{n}$$

$$\therefore a^{k+1} \equiv b^{k+1} \pmod{n}.$$

$\therefore P(k + 1)$ is true.

$$a^k \equiv b^k \pmod{n}, \forall k \in \mathbb{Z}^+.$$

□

Example 11. Show that $41 \mid 2^{20} - 1$.

Solution.

$$\begin{aligned}2^3 &= 8\\ 2^4 &= 16\\ 2^5 &= 32\\ 2^6 &= 64\\ 2^6 &\equiv 23 \pmod{41}\\ 2^5 &\equiv 32 \pmod{41}\\ 2^5 &\equiv -9 \pmod{41}\\ (2^5)^4 &\equiv (-9)^4 \pmod{41}\end{aligned}$$

$$\begin{aligned}2^{20} &\equiv 81 \times 81 \pmod{41}\\ 81 &\equiv -1 \pmod{41}\\ 2^{20} &\equiv (-1)^2 \pmod{41}\\ 2^{20} &\equiv 1 \pmod{41}. Thus 41 \mid 2^{20} - 1.\end{aligned}$$

Example 12. Consider the congruence

$$33 \equiv 15 \pmod{9}.$$

$$\Rightarrow 3 \times 11 \equiv 3 \times 5 \pmod{9}.$$

Since $\gcd(3, 9) = 3$.

Here $a = 11$; $b = 5$; $c = 3$, $n = 9$; $d = 3$.

By Previous Theorem,

$$11 \equiv 5 \pmod{\frac{9}{3}}$$

i.e.

$$11 \equiv 5 \pmod{3}.$$

(2)

$$-35 \equiv 45 \pmod{8}$$

$$5 \cdot (-7) \equiv 5 \cdot 9 \pmod{8}.$$

$$\gcd(5, 8) = 1.$$

Here $a = -7$; $b = 9$; $c = 5$; $d = 1$, $n = 8$.

Example 13. Find the remainder obtained upon dividing the sum $1! + 2! + 3! + \cdots + 99! + 100!$ by 12.

Solution.

$$\begin{aligned}1! &\equiv 1 \pmod{12}\\ 2! &\equiv 2 \pmod{12}\\ 3! &\equiv 6 \pmod{12}\\ 4! &\equiv 24 \equiv 0 \pmod{12}.\end{aligned}$$

For $k \geq 4$,

$$k! \equiv 0 \pmod{12}.$$

Thus,

$$\begin{aligned} 1! + 2! + 3! + 4! + \cdots + 100! &\equiv 1 + 2 + 6 + 0 + \cdots + 0 \pmod{12} \\ &\equiv 1 + 2 + 6 \pmod{12} \\ &\equiv 9 \pmod{12}. \end{aligned}$$

Hence the sum leaves remainder 9 when divided by 12.

Theorem 14. If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof. Given $ca \equiv cb \pmod{n}$. Then

$$c(a - b) = ca - cb = kn$$

for some integer k. We have $\gcd(c, n) = d$, there exist relatively prime integers r and s satisfying $c = dr$, $n = ds$.

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

Hence, $s \mid r(a - b)$ and $\gcd(r, s) = 1$. By Euclid's lemma $s \mid a - b$.
So$a \equiv b \pmod{s}$;
(ie) $a \equiv b \pmod{n/d}$. □

Corollary 15. If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

Corollary 16. If $ca \equiv cb \pmod{n}$ and $p \nmid c$, where p is a prime then $a \equiv b \pmod{p}$.

Exercise 4.2

1. Prove each of the following assertions:

   (a) If $a \equiv b \pmod{n}$ and $m \mid n$, then $a \equiv b \pmod{m}$.

   (b) If $a \equiv b \pmod{n}$ and $c > 0$, then $ca \equiv cb \pmod{cn}$.

   (c) If $a \equiv b \pmod{n}$ and the integers a, b, n are all divisible by $d > 0$, then $a/d \equiv b/d \pmod{n/d}$.

2. Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.

3. If $a \equiv b \pmod{n}$, prove that $\gcd(a, n) = \gcd(b, n)$.

4. (a) Find the remainders when 2^{50} and 41^{65} are divided by 7. (b) What is the remainder when the following sum is divided by 4?

$$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$$

5. Prove that the integer $52^{103}+103^{52}$ is divisible by 39, and that $111^{333}+333^{111}$ is divisible by 7.

4.3 BINARY AND DECIMAL REPRESENTATIONS

Theorem 17. Let $P(x)=\sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients c_k. If $a \equiv b \pmod{n}$, then $P(a) \equiv P(b) \pmod{n}$.

Proof. Because $a \equiv b \pmod{n}$, part (f) of Theorem 4.2 can be applied to give

$$a^k \equiv b^k \pmod{n}$$

for $k=0,1,\ldots,m$. Therefore,

$$c_k a^k \equiv c_k b^k \pmod{n}$$

for all such k. Adding these $m+1$ congruences, we conclude that

$$\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \pmod{n}$$

or, in different notation, $P(a) \equiv P(b) \pmod{n}$. □

Corollary 18. If a is a solution of $P(x) \equiv 0 \pmod{n}$ and $a \equiv b \pmod{n}$, then b also is a solution.

Proof. From the last theorem, $P(a) \equiv P(b) \pmod{n}$. Hence, if a is a solution of $P(x) \equiv 0 \pmod{n}$, then $P(b) \equiv P(a) \equiv 0 \pmod{n}$, making b a solution.

□

Theorem 19. Let $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \le a_k < 10$, and let $S = a_0 + a_1 + \cdots + a_m$. Then

$$9 \mid N \text{ if and only if } 9 \mid S.$$

Proof. Consider $P(x)=\sum_{k=0}^{m} a_k x^k$, a polynomial with integral coefficients. observe that $10 \equiv 1 \pmod{9}$, by Theorem 10, $P(10) \equiv P(1) \pmod{9}$. But $P(10)=N$ and $P(1)=a_0+a_1+\cdots+a_m=S$, so that $N \equiv S \pmod{9}$. It follows that $N \equiv 0 \pmod{9}$ if and only if $S \equiv 0 \pmod{9}$.

□

Theorem 20. Let $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \le a_k < 10$, and let $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. Then $11 \mid N$ if and only if $11 \mid T$.

Proof. As in the proof of Theorem 4.5, put $P(x)=\sum_{k=0}^{m} a_k x^k$. Because $10 \equiv -1 \pmod{11}$ we get $P(10) \equiv P(-1) \pmod{11}$. But $P(10)=N$, whereas $P(-1)=a_0-a_1+a_2-\cdots+(-1)^m a_m = T$, so that $N \equiv T \pmod{11}$. The implication is that either both N and T are divisible by 11 or neither is divisible by 11. □

Example 21. To see an illustration of the last two results, consider the integer $N = 1\,571\,724$. Because the sum

$$1 + 5 + 7 + 1 + 7 + 2 + 4 = 27$$

is divisible by 9, Theorem 19 guarantees that 9 divides N. It also can be divided by 11; for, the alternating sum

$$4 - 2 + 7 - 1 + 7 - 5 + 1 = 11$$

is divisible by 11.

Exercise 4.3

1. Use the binary exponentiation algorithm to compute both $19^{53} \pmod{503}$ and $141^{47} \pmod{1537}$.

2. Prove the following statements:

   (a) For any integer a, the units digit of a^2 is $0, 1, 4, 5, 6$, or 9.

   (b) Any one of the integers $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ can occur as the units digit of a^3.

   (c) For any integer a, the units digit of a^4 is $0, 1, 5$, or 6.

   (d) The units digit of a triangular number is $0, 1, 3, 5, 6$, or 8.

3. Find the last two digits of the number 9^{99}. [Hint: $9^9 \equiv 9 \pmod{10}$; hence, $9^{99} \equiv 9^{9+10k}$; now use the fact that $9^9 \equiv 89 \pmod{100}$.]

4. Without performing the divisions, determine whether the integers $176, 521, 221$ and $149, 235, 678$ are divisible by 9 or 11.

5. Obtain the following generalization of Theorem 4.6: If the integer N is represented in the base b by

$$N = a_m b^m + \cdots + a_2 b^2 + a_1 b + a_0 \quad 0 \leq a_k \leq b - 1$$

   then $b - 1 \mid N$ if and only if $b - 1 \mid (a_m + \cdots + a_2 + a_1 + a_0)$.

4.4 LINEAR CONGRUENCES AND THE CHINESE REMAINDER THEOREM

Definition 22. An equation of the form $ax \equiv b \pmod{n}$ is called a **linear congruence**.

Remark 23. An integer x_0 is a solution of the linear congruence if $ax_0 \equiv b \pmod{n}$ iff $ax_0 - b = ny_0$ or $ax_0 + ny_0 = b$ iff (x_0, y_0) is a solution of the linear Diophantine equation $ax + ny = b$.

Theorem 24. The linear congruence $ax \equiv b \pmod{n}$ has a solution if $d \mid b$, where $d = \gcd(a, n)$. If $d \mid b$, it has d mutually incongruent solutions modulo n.

Proof. By Remark, we have the linear congruence is equivalent to the linear Diophantine equation

$$ax - ny = b.$$

By Theorem 32, the linear Diophantine equation $ax - ny = b$ has a solution iff $d \mid b$, $d = \gcd(a, n)$.
$\therefore ax \equiv b \pmod{n}$ has a solution iff $d \mid b$.
Suppose $d \mid b$. Also by Theorem 32, if x_0 and y_0 are a specific solution, then any other solution has the form

$$\begin{aligned} x &= x_0 + \frac{n}{d}t, \\ y &= y_0 + \frac{a}{d}t, \quad t \in \mathbb{Z}. \end{aligned}$$

Take $t = 0, 1, 2, \ldots, d-1$. Consider the terms

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

Claim: These integers are incongruent modulo n.
If

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

then

$$\begin{aligned} \frac{n}{d}t_1 &\equiv \frac{n}{d}t_2 \pmod{n}. \\ \gcd(d, \frac{n}{n/d}) &= 1 \\ \Rightarrow \quad t_1 &\equiv t_2 \pmod{\frac{n}{n/d}} \\ \Rightarrow \quad t_1 &\equiv t_2 \pmod{d}. \\ &\Rightarrow d \mid (t_2 - t_1). \end{aligned}$$

But $0 < t_1, t_2 < d$, $\Rightarrow$ a contradiction.

Hence the integers mentioned above are pairwise incongruent to each other.

Claim: Any other solution of the linear congruence $x_0 + \left(\frac{n}{d}\right) t$ is congruent modulo n to one of the "d" integers in 1.

By Division Algorithm, $t = qd + r$, $0 \le r \le d - 1$.

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

$$= x_0 + nq + \frac{n}{d}r$$

$$\therefore x_0 + \left(\frac{n}{d}\right) t \equiv x_0 + \frac{n}{d}r \pmod{n},$$

$$0 \le r \le d - 1.$$

$$\therefore x_0 + \left(\frac{n}{d}\right) r \text{ is one of our } d \text{ selected solutions in } 1.$$

Hence the linear congruence has d mutually incongruent solution modulo n. □

Corollary 25. If $\gcd(a, n) = 1$, then the first linear congruence $ax \equiv b \pmod{n}$ has a unique solution modulo n.

Remark: Given $\gcd(a, n) = 1$, then the congruence $ax \equiv 1 \pmod{n}$ has a unique solution, say $x_0.ax_0 \equiv 1 \pmod{n} \Rightarrow x_0$ is the inverse of a (multiplicative).

Example 26. Solve the linear congruence

$$18x \equiv 30 \pmod{42}.$$

Solution:

$$\gcd(18, 42) = 6.$$

$$6 \mid 30 \quad (\because d \mid b).$$

By Theorem 8, $18x \equiv 30 \pmod{42}$ has 6 solutions, which are incongruent modulo $\frac{42}{6} = 7$. When $x = 4$,

$$\begin{aligned} 18 \times x = 18 \times 4 &= 72 \\ 18 \times 4 \equiv 72 &\pmod{42} \\ \equiv 30 &\pmod{42}. \end{aligned}$$

So $x = 4$ is one solution.

Remaining solutions can be got by

$$x \equiv 4 + \left(\frac{42}{6}\right) t \pmod{42}.$$

$$x \equiv 4 + 7t \pmod{42}, \quad 0 \leq t \leq 5.$$

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

Theorem 27. Chinese Remainder Theorem
Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

has a simultaneous solution which is unique modulo the integer $n = n_1 n_2 \cdots n_r$.

Proof. Consider the product

$$n = n_1 n_2 \cdots n_r.$$

For each $k = 1, 2, \ldots, r$, let

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

N_k is the product of all integers n_i with the factor n_k omitted. By hypothesis,

$$\gcd(N_k, n_k) = 1.$$

According to the theory of a single linear congruence, $N_k x \equiv 1 \pmod{n_k}$ has a unique solution x_k.

Claim: $\overline{x} = a_1N_1x_1 + a_2N_2x_2 + \cdots + a_rN_rx_r$ is a simultaneous solution of the given system.

$$N_i = \frac{n}{n_i} = n_1n_2\cdots n_{i-1}n_{i+1}\cdots n_r.$$

For $i \neq k$,

$$\begin{aligned} N_i &\equiv 0 \pmod{n_k} \\ \Rightarrow \quad n_k &\mid N_i. \end{aligned}$$

$$\begin{aligned} \overline{x} &= a_1N_1x_1 + \cdots + a_rN_rx_r \\ \overline{x} &= a_kN_kx_k \pmod{n_k}. \end{aligned}$$

But

$$\begin{aligned} N_k x &\equiv 1 \pmod{n_k} \\ \Rightarrow \quad \overline{x} &\equiv a_kN_kx_k \pmod{n_k} \\ &= a_k \cdot 1 \pmod{n_k}. \\ \overline{x} &\equiv a_k \pmod{n_k}. \end{aligned}$$

For uniqueness, if $\bar{x}$ and x' are two solutions,

$$\bar{x} \equiv x' \pmod{n_k} \quad \forall k$$

$$\Rightarrow n_k \mid \bar{x} - x', \forall k.$$

$$\gcd(n_i, n_j) = 1 \quad \Rightarrow \quad n_1n_2\cdots n_k \mid \bar{x} - x'$$

$$\Rightarrow \bar{x} \equiv x' \pmod{n}.$$

$\therefore$ The solution of ⊛ is unique.

[n$_k|\bar{x} - x', \forall k$.

$$\gcd(n_i, n_j) = 1 \implies n_1n_2\cdots n_k|\bar{x} - x'$$

$$\Rightarrow \bar{x} = x' \pmod{n}.$$

$\therefore$ The solution of $\otimes$ is unique. □

Example 28. Solve the system

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

Solution.

$$n = 3 \cdot 5 \cdot 7 = 105.$$

$$N_1 = \frac{n}{n_1} = 35; \quad N_2 = 21; \quad N_3 = 15.$$

Now the linear congruences

$$35x \equiv 1 \pmod 3 \quad (1),$$
$$21x \equiv 1 \pmod 5 \quad (2),$$
$$15x \equiv 1 \pmod 7 \quad (3).$$

Solutions are $x_1 = 2; x_2 = 1; x_3 = 1$ respectively.

$$\begin{aligned} x &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \\ &= 233. \end{aligned}$$

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

Example 29. Solve the linear congruence

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

Solution.

$$276 = 3 \times 4 \times 23.$$

$$17x \equiv 9 \pmod 3 \implies x \equiv 0 \pmod 3 \quad (1)$$

$$17x \equiv 9 \pmod 4 \implies x \equiv 1 \pmod 4 \quad (2)$$

$$17x \equiv 9 \pmod{23} \implies 17x \equiv 9 \pmod{23}. \quad (3)$$

(1) $\implies x = 3k.$

(2) $\implies 3k \equiv 1 \pmod 4$

$$\implies 9k \equiv 3 \pmod 4$$

$$\implies k \equiv 3 \pmod 4$$

$$\implies k = 3 + 4j.$$

$$x = 3k$$

$$= 3(3 + 4j)$$

$$x = 9 + 12j.$$

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

$$153 + 204j \equiv 9 \pmod{23}.$$

Theorem 30. The system of linear congruences

$$ax + by \equiv r \pmod n \quad (1)$$

$$cx + dy \equiv s \pmod n \quad (2)$$

has a unique solution modulo n whenever

$$\gcd(ad - bc, n) = 1.$$

Proof.

$$(1) \times d \Rightarrow \quad adx + bdy \equiv rd \pmod{n}.$$

$$(2) \times b \Rightarrow \quad bcx + bdy \equiv bs \pmod{n}.$$

Multiply the first congruence by d:

$$adx + bdy \equiv rd \pmod{n}.$$

multiply the second congruence by b:

$$bcx + bdy \equiv sb \pmod{n}.$$

Subtracting these,

$$\begin{aligned} adx + bdy - (bcx + bdy)& \\ \equiv rd - sb \pmod{n},& \\ adx - bcx \equiv rd - sb \pmod{n},& \\ (ad - bc)x \equiv rd - sb \pmod{n}.& \end{aligned}$$

Since $\gcd(ad - bc, n) = 1$, the congruence

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

has a unique solution, say t. Then

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

$$\Rightarrow x \equiv t(dx - by) \pmod{n}.$$

Similarly,

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

□

Example 31. Solve the system

$$\begin{cases} 7x + 3y \equiv 10 \pmod{16} & (1) \\ 2x + 5y \equiv 9 \pmod{16} & (2) \end{cases}$$

Solution. Here $a = 7$, $b = 3$, $c = 2$, $d = 5$, $n = 16$.

$$\begin{aligned} ad - bc &= 7 \cdot 5 - 3 \cdot 2 = 35 - 6 = 29 \\ \gcd(ad - bc, n) &= \gcd(29, 16) = 1. \end{aligned}$$

$\therefore$ the solution exists.

$$\begin{aligned} (1) \times 5 \quad 35x + 15y &\equiv 50 \pmod{16} \\ (2) \times 3 \quad 6x + 15y &\equiv 27 \pmod{16}. \end{aligned}$$

$$\begin{aligned} 35x - 6x &\equiv 50 - 27 \pmod{16} \\ 29x &\equiv 23 \pmod{16} \\ 13x &\equiv 7 \pmod{16}. \quad (4) \end{aligned}$$

Clearly $5 \cdot 13 \equiv 1 \pmod{16}$.

$$\begin{aligned} 5 \times (4) \quad 13 \cdot 5x &\equiv 7 \times 5 \pmod{16} \\ x &\equiv 3 \pmod{16}. \end{aligned}$$

Similarly

$$y \equiv 7 \pmod{16}.$$

5.2 Fermat's Theorem

Theorem 1. (Fermat's Theorem)
Let p be a prime and suppose that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Consider the first $p-1$ positive multiples of a, say $a, 2a, 3a, \ldots, (p-1)a$.

Claim: None of these integers is congruent modulo p to any other, nor is any congruent to zero.

Suppose $ra \equiv sa \pmod{p}$, $1 \leq r < s \leq p-1$.
Then $p \mid ra - sa$
$\Rightarrow p \mid (r-s)a$. Since $p \nmid a$, $p \mid (a-s)$.

$$\Rightarrow r \equiv s \pmod{p}, \text{ which is impossible.}$$

Hence the positive set of integers must be congruent modulo p to $1, 2, 3, \ldots, p-1$ taken in some order.

Multiplying all these congruence together, we get

$$\begin{aligned} & a \cdot (2a) \cdot (3a) \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \\ \Rightarrow \quad & a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) \equiv (p-1)! \pmod{p} \\ \Rightarrow \quad & a^{p-1}(p-1)! \equiv (p-1)! \pmod{p} \\ \text{since } p \nmid (p-1!), \quad & a^{p-1} \equiv 1 \pmod{p} \end{aligned}$$

□

Corollary 2. If p is a prime, then $a^p \equiv a \pmod{p}$ for any integer a.

Proof. If $p \mid a$, then $a \equiv 0 \pmod{p}$

$$\therefore a^p \equiv 0 \pmod{p}$$

$$\Rightarrow a^p \equiv a \pmod{p}.$$

If $p \nmid a$, then by Fermat's Theorem,

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

$$\times a \implies a^p \equiv a \pmod{p}.$$

Alternate Proof

Proof is by induction on a.

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

Take $a = 1$, then $a^p = 1$;

$$\therefore a^p \equiv a \pmod{p}.$$

$$P(1) \text{ is true.}$$

Assume that $P(a)$ is true.

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

$\Rightarrow P(a+1)$ is true.

$$\begin{aligned}
(a+1)^p &\equiv (a+1) \pmod{p} \\
(a+1)^p &= a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a + 1
\end{aligned}$$

Now

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{1\cdot 2\cdot 3\cdots k}$$

Claim: $\binom{p}{k} \equiv 0 \pmod{p}; \; 1 \le k \le p-1.$

$$\begin{aligned}
\Rightarrow k! \cdot \binom{p}{k} &= p(p-1)\cdots(p-k+1) \\
k! \cdot \binom{p}{k} &\equiv 0 \pmod{p}.
\end{aligned}$$

$$k!\binom{p}{k} \equiv 0 \pmod{p}$$

$$\Rightarrow p \mid k!\binom{p}{k}$$

$$\Rightarrow p \mid k! \quad \text{(or)} \quad p \mid \binom{p}{k}$$

$$p \mid k! \Rightarrow p \mid j \text{ for some } j, 1 \le j \le k \le p-1$$

which is impossible.

$$\therefore p \mid \binom{p}{k}$$

$$\therefore \binom{p}{k} \equiv 0 \pmod{p}.$$

$$\therefore (a+1)^p \equiv a^p + 1 \pmod{p}$$

$$\equiv a+1 \pmod{p} \quad \text{(by 1)}$$

□

Example 3. Verify $5^{38} \equiv 4 \pmod{11}$

Solution.

$$38 = 30 + 8 = (3 \times 10) + (2 \times 4)$$

$$\therefore 5^{38} = (5^{10})^3(5^2)^4 \quad (1)$$

clearly $5 \nmid 11$.

By Fermat's Theorem,

$$\begin{aligned} 5^{p-1} &\equiv 1 \pmod{p} \\ \Rightarrow \quad 5^{10} &\equiv 1 \pmod{11} \\ \therefore (5^{10})^3 &\equiv 1 \pmod{11} \\ 5^{30} &\equiv 1 \pmod{11} \end{aligned}$$

clearly

$$\begin{aligned} 5^2 = 25 &\equiv 3 \pmod{11} \\ (5^2)^4 &\equiv 3^4 \pmod{11} \\ 5^8 &\equiv 81 \pmod{11} \\ 5^8 &\equiv 4 \pmod{11} \end{aligned}$$

Lemma 4. If p and q are distinct primes with

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

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

then

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

Proof. Given $a^q \equiv a \pmod{p}$

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

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

By Fermat's Theorem, $a^p \equiv a \pmod{p}$

$$\begin{aligned} a^{pq} &\equiv a \pmod{p} \\ &\implies p \mid a^{pq} - a \\ \text{Similarly } & q \mid a^{pq} - a \\ & \text{Since } \gcd(p,q) = 1, \quad pq \mid a^{pq} - a \\ & \therefore a^{pq} \equiv a \pmod{pq}. \end{aligned}$$

□

Note: The converse of Fermat's theorem is false.

Pseudoprimes

Definition: A composite integer n is called *pseudoprime* if $n \mid 2^n - 2$.

Example 5. 1. There are infinitely many pseudoprimes.

2. The smallest four numbers are $341, 561, 645, 1105$.

Theorem 6. If n is an odd pseudoprime then $M_n = 2^n - 1$ is a larger one.

Proof. Since n is composite number, $n = rs$, $1 \leq r \leq s < n$. Then $r \mid n$
$\Rightarrow 2^r - 1 \mid 2^n - 1$

$$r \mid n \implies 2^r - 1 \mid 2^n - 1.$$

$$\therefore 2^r - 1 \mid M_n.$$

By hypothesis [n is pseudoprime],

$$\begin{aligned} & n \mid 2^n - 2 \\ & \implies 2^n \equiv 2 \pmod{n} \\ & \implies 2^n - 2 = kn, \text{ for some } k \in \mathbb{Z}. \end{aligned}$$

Now

$$\begin{aligned} 2^{Mn-1} &= 2^{\frac{2^n-2}{2}} = 2^{kn}. \\ \therefore 2^{Mn-1} &= 2^{kn} - 1 \\ &= (2^n - 1)(2^{n(k-1)} + \cdots + 2^2 + 1) \\ &= M_n(2^{n(k-1)} + \cdots + 2^2 + 1) \end{aligned}$$

$$\begin{aligned} & 2^{Mn-1} \equiv 0 \pmod{M_n} \\ & \therefore 2^{Mn-1} \equiv 1 \pmod{M_n} \\ & 2^{Mn} \equiv 2 \pmod{M_n}. \end{aligned}$$

Definition 7. A composite integer n for which $a^n \equiv a \pmod{n}$ is called a pseudoprime to the base 'a'.

Example 8.
1. 91 is the smallest pseudoprime to base 2.
2. 217 is the smallest pseudoprime to base 5.

Note: There exist composite numbers n that are pseudoprime to every base ‘’.

Example 9.
1. 91 is the smallest pseudoprime to base 2.
2. 217 is the smallest pseudoprime to base 5.

Note 10. There exist composite numbers n that are pseudoprime to every base 'a' i.e. $a^n \equiv a \pmod{n}, \forall a \in \mathbb{Z}$.
The least such number is 561.
These exceptional numbers are called absolute pseudoprimes (or) Carmichael numbers.

Problem 11. 561 is absolute pseudoprime.

Proof. $561 = 3 \times 11 \times 17$.

$$\begin{aligned}&\gcd(a,561)=1 \implies\\&\gcd(a,3)=1\\&\gcd(a,11)=1\\&\gcd(a,17)=1\end{aligned}$$

By Fermat's theorem,

$$\begin{aligned}a^2 &\equiv 1 \pmod 3 \quad (1)\\a^{10} &\equiv 1 \pmod{11} \quad (2)\\a^{16} &\equiv 1 \pmod{17} \quad (3)\end{aligned}$$

$$\begin{aligned}(1) &\implies a^{560} \equiv 1 \pmod 3\\(2) &\implies a^{560} \equiv 1 \pmod{11}\\(3) &\implies a^{560} \equiv 1 \pmod{17}\end{aligned}$$

$$\therefore \quad 3 \mid a^{560}-1; \quad 11 \mid a^{560}-1; \quad 17 \mid a^{560}-1$$

$$\therefore \quad 3 \times 11 \times 17 \mid a^{560}-1$$

$$561 \mid a^{560}-1$$

$$a^{560} \equiv 1 \pmod{561}.$$

$$\therefore a^{561} \equiv a \pmod{561}, \forall a \in \mathbb{Z}.$$

Hence 561 is absolute pseudoprime. □

Problem 12. Any absolute pseudoprime is square-free.

Proof.

$$a^n \equiv a \pmod n, \forall a.$$

Suppose n is pseudoprime. Then $a^n \equiv a \pmod n, \forall a \in \mathbb{Z}$.
Suppose n is perfect square.
Then $n = k^2$ for some $k > 1$.
$k^2 \mid n$.

If $a = k$, then

$$\begin{aligned}(1) &\Rightarrow k^n \equiv k \pmod n\\&\Rightarrow k^n \equiv 0 \pmod{k^2}\\&\Rightarrow k \equiv 0 \pmod{k^2}.\end{aligned}$$

$\therefore k^2 \mid k \implies k$
Hence n is square-free. □

Theorem 13. Let n be a composite square free integer, say $n = p_1 p_2 \cdots p_r$, where p_i are distinct primes. If $p_i - 1 | n - 1$ for $i = 1, 2, \ldots, r$, then n is an absolute pseudoprime.

Proof. Suppose 'a' is an integer satisfying $\gcd(a,n)=1$.
Suppose $a\in\mathbb{Z}$ s.t. $\gcd(a,n)=1$. Then $a^n\equiv a \pmod{n}$
$\implies a^{p_i}\equiv a \pmod{p_i}$
$\implies \gcd(a,p_i)=1,\forall i$ By Fermat's theorem,

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

$$\Rightarrow p_i \mid a^{p_i-1}-1.$$

Given $p_i-1\mid n-1$.

$$\therefore a^{p_i-1}\mid a^{n-1}.$$

$$\Rightarrow p_i\mid a^{n-1}$$

$$p_i\mid a^n-a,\forall a.$$

$$p_1\cdot p_2\cdots p_r\mid a^n-a.$$

$\therefore n$ is an absolute pseudoprime. □

Exercise 5.2

1. Use Fermat's theorem to verify that 17 divides $11^{104}+1$.
2. (a) If $\gcd(a,35)=1$, show that $a^{12}\equiv 1 \pmod{35}$. [Hint: From Fermat's theorem $a^6\equiv 1 \pmod{7}$ and $a^4\equiv 1 \pmod{5}$.]

   (b) If $\gcd(a,42)=1$, show that $168=3\cdot 7\cdot 8$ divides a^6-1.

   (c) If $\gcd(a,133)=\gcd(b,133)=1$, show that $133\mid a^{18}-b^{18}$.
3. From Fermat's theorem deduce that, for any integer $n\geq 0$, $13\mid 11^{12n+6}+1$.
4. Derive each of the following congruences:

   (a) $a^{21}\equiv a \pmod{15}$ for all a. [Hint: By Fermat's theorem, $a^5\equiv a \pmod{5}$.]

   (b) $a^7\equiv a \pmod{42}$ for all a.

   (c) $a^{13}\equiv a \pmod{3\cdot 7\cdot 13}$ for all a.

   (d) $a^9\equiv a \pmod{30}$ for all a.
5. If $\gcd(a,30)=1$, show that 60 divides a^4+59.

5.3 WILSON'S THEOREM

Theorem 14. (Wilson's Theorem)
If p is a prime, then $(p-1)!\equiv -1 \pmod{p}$.

Proof. It is clear for $p = 2, 3$.

Suppose that 'a' is anyone of the $p - 1$ positive integers, $1, 2, 3, \ldots p - 1$ and consider the linear congruence $ax \equiv 1 \pmod{p}$.

Then $\gcd(a, p) = 1$.

By theorem. (1) has a unique solution modulo p.

Hence there is a unique integer a' with $1 \leq a' \leq p - 1$ satisfying $aa' \equiv 1 \pmod{p}$.

Since p is prime, $a^p \equiv a$ if and only if $a \equiv 1$ or $a \equiv p - 1$.

The congruence $a^2 \equiv 1 \pmod{p}$ is equivalent to

$$a^2 - 1 \equiv 0 \pmod{p}$$

$$\implies (a-1)(a+1) \equiv 0 \pmod{p}$$

$$\begin{cases} a - 1 \equiv 0 \pmod{p} & \text{if } a \equiv 1 \\ a + 1 \equiv 0 \pmod{p} & \text{if } a \equiv p - 1 \end{cases}$$

If we omit the numbers 1 and $p - 1$, then group the remaining integers $2, 3, \ldots, p - 2$ into pairs a, a' with $a \neq a'$ s.t. $aa' \equiv 1 \pmod{p}$. When these $\frac{p-3}{2}$ congruence are multiplied together,

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

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

$$\Rightarrow (p-2)! \equiv 1 \pmod{p}.$$

Since $\gcd(p, p-1) = 1$,

$$\begin{aligned} (p-1)(p-2)! &\equiv p - 1 \pmod{p} \\ (p-2)! &\equiv 1 \pmod{p} \\ \therefore \quad (p-1)! &\equiv -1 \pmod{p}. \end{aligned}$$

□

Example 15. $12! \equiv -1 \pmod{13}$.

Solution Take $p = 13$.

It is possible to divide the integers $2, 3, 4, \ldots, 11$ into $\frac{p-3}{2} = 5$ pairs, each product of which is congruent to 1 modulo 13.

$$\begin{aligned} 2 \cdot 7 = 14 &\equiv 1 \pmod{13}, \\ 3 \cdot 9 = 27 &\equiv 1 \pmod{13}, \\ 4 \cdot 10 = 40 &\equiv 1 \pmod{13}, \\ 5 \cdot 8 = 40 &\equiv 1 \pmod{13}, \\ 6 \cdot 11 = 66 &\equiv 1 \pmod{13}. \end{aligned}$$

Multiplying these congruences,

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

$$\therefore 12 \times 11! \equiv 12 \pmod{13}.$$

Hence $12! \equiv -1 \pmod{13}$.
i.e. $(p-1)! \equiv -1 \pmod{p}$ with $p = 13$.

Note 16. The converse of Wilson's theorem is also true.
For
If $(n-1)! \equiv -1 \pmod{n}$, then n must be prime. Suppose n is not a prime.
then n has a divisor d with $1 < d < n$
since $d \leq n-1$, d occurs as one of the factors
in $(n-1)!$.
$\therefore d|(n-1)!$
since $(n-1)! \equiv -1 \pmod{n}$,
$n|((n-1)!+1)$
$\therefore n|(n-1)!+1-(n-1)!$
$n|1, \Rightarrow$
$\therefore n$ is prime.

Note 17. An integer $n > 1$ is prime if $(n-1)! \equiv -1 \pmod{n}$.

Definition 18. A congruence of the form $ax^2 + bx + c \equiv 0 \pmod{n}$ with $a \not\equiv 0 \pmod{n}$ is called a quadratic congruence.

Theorem 19. The quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$ where p is an odd prime, has a solution if and only if $p \equiv 1 \pmod{4}$.

Proof. Let a be any solution of $x^2 + 1 \equiv 0 \pmod{p}$.
Then $a^2 + 1 \equiv 0 \pmod{p}$
$\implies p \mid a^2 + 1, a^2 \equiv -1 \pmod{p}$.
Since $(a, p) = 1$ and a, by Fermat's theorem,

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

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

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \rightarrow 4$$

If $p = 4k+3$, then $\frac{p-1}{2} = 2k+1$.

$$(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1, \text{ which is impossible.}$$

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

$$2 \equiv 0 \pmod{p}$$

$$\therefore p \mid 2. \Rightarrow\Leftarrow .$$

$$\therefore p \text{ must be of the form } 4k+1.$$

Conversely, suppose $p \equiv 1 \pmod 4$
Then $p = 4k+1$. Now $(p-1)! = 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1)$.
We have the congruences

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

Rearranging the factors produces

$$\begin{aligned} (p-1)! &\equiv 1(-1) \cdot 2(-2) \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \pmod{p} \\ &\equiv (-1)^{\frac{p-1}{2}} \left[1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right]^2 \pmod{p}. \end{aligned}$$

By Wilson's theorem,

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

Since $p = 4k+1$, $(-1)^{\frac{p-1}{2}} = 1$

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

Since $p = 4k+1$,

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

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

$$\therefore \left(\frac{p-1}{2}\right)! \text{ satisfies the quadratic congruence } x^2+1 \equiv 0 \pmod{p}.$$

□

Example 20. Take $p = 13$.

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 + 1 \equiv (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)^2 + 1 \pmod{13}.$$

$$1 \cdot 2 \cdot 3 \cdot 4 = 24$$

$$24 \equiv 11 \pmod{13}.$$

$$1 \cdot 2 \cdot 3 \cdot 4 \equiv -2 \pmod{13}.$$

$$4! \equiv -2 \pmod{13}.$$

$$5! \equiv -10 \pmod{13}.$$

$$5! \equiv 3 \pmod{13}.$$

$$6! \equiv 18 \pmod{13}.$$

$$6! \equiv 5 \pmod{13}.$$

$$(6!)^2 \equiv 5^2 \pmod{13}.$$

$(6!)^2 \equiv 12 \pmod{13}$
$(6!)^2 \equiv -1 \pmod{13}$
$(6!)^2 + 1 \equiv 0 \pmod{13}$
$\therefore \left[\left(\frac{p-1}{2}\right)!\right]^2 + 1 \equiv 0 \pmod{p}$ is true for p=13.

Exercise 5.3

1. (a) Find the remainder when 15! is divided by 17.
   (b) Find the remainder when 2(26!) is divided by 29.
2. Determine whether 17 is a prime by deciding whether $16! \equiv -1 \pmod{17}$.
3. Arrange the integers $2, 3, 4, \ldots, 21$ in pairs a and b that satisfy $ab \equiv 1 \pmod{23}$.
4. Show that $18! \equiv -1 \pmod{437}$.
5. (a) Prove that an integer $n > 1$ is prime if and only if $(n-2)! \equiv 1 \pmod{n}$.
   (b) If n is a composite integer, show that $(n-1)! \equiv 0 \pmod{n}$, except when $n = 4$.
6. Given a prime number p, establish the congruence

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

5.4 THE FERMAT-KRAITCHIK FACTORIZATION METHOD

Example 21. Suppose we wish to factor the positive integer $n = 2189$ and happen to notice that $579^2 \equiv 18^2 \pmod{2189}$. Then we compute

$$\gcd(579 - 18, 2189) = \gcd(561, 2189) = 11$$

using the Euclidean Algorithm:

$$\begin{aligned} 2189 &= 3 \cdot 561 + 506 \\ 561 &= 1 \cdot 506 + 55 \\ 506 &= 9 \cdot 55 + 11 \\ 55 &= 5 \cdot 11 \end{aligned}$$

This leads to the prime divisor 11 of 2189. The other factor,199, can be obtained by

$$\gcd(579 + 18, 2189) = \gcd(597, 2189) = 199.$$

observe that

$$81^2 - 3 \cdot 2189 = -6 \quad \text{and} \quad 155^2 - 11 \cdot 2189 = -54$$

$$81^2 \equiv -2 \cdot 3 \pmod{2189} \quad \text{and} \quad 155^2 \equiv -2 \cdot 3^3 \pmod{2189}.$$

When these congruences are multiplied, they produce

$$(81 \cdot 155)^2 \equiv (2 \cdot 3^2)^2 \pmod{2189}.$$

Since $81 \cdot 155 = 12555 \equiv -579 \pmod{2189}$, $579^2 \equiv 18^2 \pmod{2189}$.

Example 22. Let $n = 12499$ be the integer to be factored. The first square just larger than n is $112^2 = 12544$. So we begin by considering the sequence of numbers $x^2 - n$ for $x = 112, 113, \ldots$. As before, our interest is in obtaining a set of values $x_1, x_2, \ldots, x_k$ for which the product $(x_i - n) \cdots (x_k - n)$ is a square, say y^2. Then

$$(x_1 \cdots x_k)^2 \equiv y^2 \pmod{n},$$

which might lead to a nontrivial factor of n.

A short search reveals that

$$\begin{aligned} 112^2 - 12499 &= 45 \\ 117^2 - 12499 &= 1190 \\ 121^2 - 12499 &= 2142 \end{aligned}$$

or, written as congruences,

$$\begin{aligned} 112^2 &\equiv 3^2 \cdot 5 \pmod{12499} \\ 117^2 &\equiv 2 \cdot 5 \cdot 7 \cdot 17 \pmod{12499} \\ 121^2 &\equiv 2 \cdot 3^2 \cdot 7 \cdot 17 \pmod{12499}. \end{aligned}$$

Multiplying these together results in the congruence

$$(112 \cdot 117 \cdot 121)^2 \equiv (2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17)^2 \pmod{12499}$$

that is,

$$1585584^2 \equiv 10710^2 \pmod{12499}.$$

But we are unlucky with this square combination. Because

$$1585584 \equiv 10710 \pmod{12499}$$

only a trivial divisor of 12499 will be found. To be specific,

$$\begin{aligned}\gcd(1585584 + 10710, 12499) &= 1\\ \gcd(1585584 - 10710, 12499) &= 12499.\end{aligned}$$

Exercise 5.4

1. Use Fermat's method to factor each of the following numbers:

   (a) 2279.

   (b) 10541.

   (c) 340663. [Hint: The smallest square just exceeding 340663 is 584^2.]

2. Prove that a perfect square must end in one of the following pairs of digits: 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96. [Hint: Because $x^2 \equiv (50 + x)^2 \pmod{100}$ and $x^2 \equiv (50 - x)^2 \pmod{100}$, examine the final digits of x^2 for the 26 values $x = 0, 1, 2, \ldots, 24, 25$.]

3. Factor the number $2^{11} - 1$ by Fermat's factorization method.

4. In 1647, Mersenne noted that when a number can be written as a sum of two relatively prime squares in two distinct ways, it is composite and can be factored as follows: If

   $$n = a^2 + b^2 = c^2 + d^2,$$

   then

   $$n = \frac{(ac + bd)(ac - bd)}{(a + d)(a - d)}.$$

   Use this result to factor the numbers

   $$493 = 18^2 + 13^2 = 22^2 + 3^2$$

   and

   $$38025 = 168^2 + 99^2 = 156^2 + 117^2.$$

5. Employ the generalized Fermat method to factor each of the following numbers:

   (a) 2911 [Hint: $138^2 \equiv 67^2 \pmod{2911}$].

   (b) 4573 [Hint: $177^2 \equiv 92^2 \pmod{4573}$].

   (c) 6923 [Hint: $208^2 \equiv 93^2 \pmod{6923}$].

6. Factor 13561 with the help of the congruences

$$233^2 \equiv 3^2 \cdot 5 \pmod{13561}$$

and

$$1281^2 \equiv 2^4 \cdot 5 \pmod{13561}.$$

7. (a) Factor the number 4537 by searching for x such that

$$x^2 - k \cdot 4537$$

is the product of small prime powers.

   (b) Use the procedure indicated in part (a) to factor 14429. [Hint: $120^2 - 14429 = -29$ and $3003^2 - 625 \cdot 14429 = -116$.]

8. Use Kraitchik's method to factor the number 20437.

Study Learning Material Prepared by

Dr. T.S. GOVINDALAKSHMI M.Sc. , M.Phil., Ph.D
ASSISTANT PROFESSOR
DEPARTMENT OF MATHEMATICS
MANONMANIAM SUNDARANAR UNIVERSITY COLLEGE
PULIANGUDI-627855
TAMILNADU, INDIA