Study Material
(Semester - 1)

Department of Mathematics, P. R. Thakur Govt. College

Part of University Syllabus

MTMACOR02T-Unit-2: Equivalence relations and partitions, Functions, Composition of functions, Invertible functions, One to one correspondence and cardinality of a set. Well-ordering property of positive integers, Division algorithm, Divisibility and Euclidean algorithm. Congruence relation between integers. Principles of Mathematical Induction, statement of Fundamental Theorem of Arithmetic.

1 Equivalence Relation and Partitions

1.1 Definitions and elementary properties

Definition. 1.1 The Cartesian product of two non-empty sets A, B is the set of all ordered pairs (a, b), where $a \in A, b \in B$ and is denoted by $A \times B$. Thus

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

For a finite number of non-empty sets $A_1, A_2, \ldots, A_n$ their Cartesian product is

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i, i \leq i \leq n\}.$$

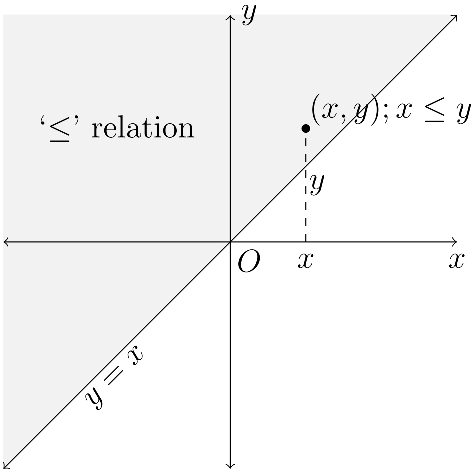
An element of the form $(a_1, a_2, \ldots, a_n)$ is called an ordered n-tuple. The i-th entry a_i of this ordered n-tuple is called the i-th component of the n-tuple. Thus the Cartesian product of n non-empty sets is the set of all the n-tuples, whose i-th component belongs to the i-th set where $1 \leq i \leq n$.

If $A = A_1 = A_2 = \cdots = A_n$ then $A_1 \times A_2 \times \cdots \times A_n$ is denoted by A^n. Hence $A^n = \{(a_1, a_2, \ldots, a_n) : a_i \in A, 1 \leq i \leq n\}$.

Definition. 1.2 For two non-empty sets A, B a set $S \subset A \times B$ is called a *relation* from A to B. The set A is called the domain and B is called the codomain of the relation S. If for $(x,y) \in A \times B$, $(x,y) \in S$ it is usually written as xSy. If $(x,y) \notin S$ it is also written as $x \not S y$.

when $A = B$ a set $S \subset A \times A = A^2$ is called a *binary relation on* A or simply a *relation on* A. For any positive integer n a subset $S \subset A^n$ is called an n-ary relation on A.

Example. 1.3 Consider the set $\mathbb{R}$ and the set $S = \{(x,y) : x \leq y\} \subset \mathbb{R}^2$. The set S is called the *less than or equal to* relation on $\mathbb{R}$.
In Cartesian plane the set S is the upper portion of the diagonal line $y = x$, including that line. As usual if $(x,y) \in S$ we write it as xSy or $x \leq y$. The upper portion of the diagonal line $y = y$, excluding that line, is the ‘ $<$’ relation. The lower portion of the diagonal is ‘$\geq$’ relation when the diagonal line is included and is the $>$ relation when the diagonal line is excluded.



Example. 1.4 1. Let X be any non-empty set. Then the set $\Delta_X = \{(x,x) : x \in X\}$ is a relation on X, called the diagonal relation on X. hence $(x,y) \in \Delta_x$ if and only id $x = y$.

2. For any non-empty set X, $X \times X$ is itself a relation on X.

3. Let $S = \{(x,y) \in \mathbb{R}^2 : |x| > |y|\}$. Then S is a relation on R.

4. Let $A = \{a,b,c,d,\}$. Then $S = \{((a,b),(a,c),(a,d),(b,c),(b,d),(c,d)\}$ is a relation on A.

Definition. 1.5 A relation R on a set X is called a *reflexive relation* if xRx for all $x \in X$, or in other words if $\Delta_X \subset R$.

Example. 1.6 1. In any non-empty set X the relation Δ_X is a reflexive relation.

2. The relations ‘$\leq$’ and ‘$\geq$’ are reflexive relations on $\mathbb{R}$, whereas ‘$<$’ and ‘$>$’ are not reflexive relations.

3. Let $A = \{a,b,c,d,e\}$. Then the relation

$$R = \{(a,a),(a,b),(b,b),(b,c),(b,d),(c,c),(c,d),(d,c),(d,d),(e,a),(e,b),(e,e)\}$$

is reflexive, since $\Delta_A = \{(a,a),(b,b),(c,c),(d,d),(e,e)\} \subset R$. But the relation

$$S = \{(a,a),(a,b),(b,b),(b,c),(b,d),(c,c),(c,e),(d,c),(d,e),(e,a),(e,b),(e,e)\}.$$

is not reflexive, since $(d,d) \notin S$.

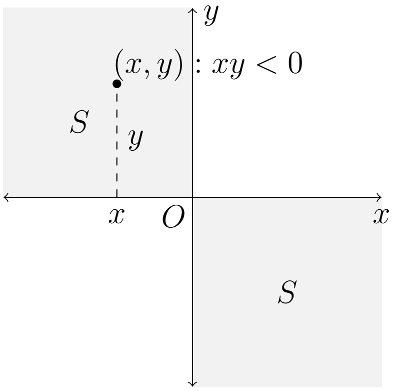
4. let p be a positive integer. On the set $\mathbb{Z}$ of all integers the relation ρ_p, defined by $\rho_p = \{(m,n) : m-n \text{ is divisible by } p\}$, is a reflexive relation, since for every $m \in \mathbb{Z}$, $m-m=0$ is divisible by p and hence $m\rho_p m$ for every $m \in \mathbb{Z}$.

Definition. 1.7 A relation R on a set X is called a *transitive relation* if for $a,b,c \in X$, aRb and bRc implies that aRc.

Example. 1.8 1. On $\mathbb{R}$ all of the relations $<, \leq, >, \geq$ are transitive relations.

2. for $p \in \mathbb{N}$, the relation ρ_p on $\mathbb{Z}$, as defined earlier, is a transitive relation. Let $i,j,k \in \mathbb{N}$ such that $i\rho_p j$ and $j\rho_p k$. Then $j-i$ is divisible by p and $k-j$ is also divisible by p. Hence $k-i = (k-j)+(j-i)$ is divisible by p, i.e., $i\rho_p k$. So ρ_p is transitive.

3. On the set $\mathbb{R}$ define a relation S by $S = \{(x,y) : xy < 0\}$. Then S is not transitive. For $x,y,z \in \mathbb{R}$, assume that xSy and ySz. Then xSy gives that x and y are of opposite signs and ySz gives that y and z have opposite signs. Hence x and z must have the same signs, i.e., $xz > 0$. This shows that $(x,z) \notin S$, i.e., $x \not S z$. Hence the relation S is not transitive.



4. On the set $A = \{a,b,c,d,e\}$ the relation

$$R = \{(a,a),(a,b),(b,b),(b,c),(b,d),(c,c),(c,d),(d,c),(d,d),(e,a),(e,b),(e,e)\}$$

is not transitive, since $(a,b) \in R, (b,c) \in R$, but $(a,c) \notin R$.

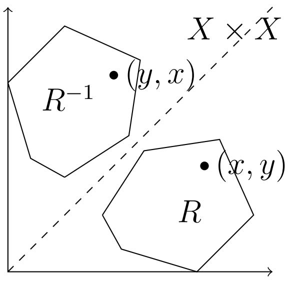
Definition. 1.9 A relation R on a set X is called *symmetric* if for all $x,y \in X$, $(x,y) \in R$ implies that $(y,x) \in R$, i.e., if for all $x,y \in X$, $xRy \Rightarrow yRx$.

A relation R on a set X is called *anti-symmetric* if for all $x,y \in X$, $(x,y) \in R$ and $(y,x) \in R$, implies that $x = y$ i.e., if for all $x,y \in X$, xRy and $yRx \Rightarrow x = y$.

Example. 1.10

1. The relations $\leq$ and $\geq$ are both anti-symmetric but not symmetric.
2. The relation ρ_p on $\mathbb{Z}$, where $p \in \mathbb{N}$, is symmetric but not anti-symmetric.
3. On any non-empty set X the relation Δ_X is both symmetric and anti-symmetric.
4. On the set $A = \{a, b, c, d, e\}$ where the elements are distinct, the relation
$$R = \{(a,a),(a,b),(b,b),(b,c),(b,d),(c,c),(c,d),(d,c),(d,d),(e,a),(e,b),(e,e)\}$$
is neither symmetric, nor anti-symmetric. Here $(a,b) \in R$ but $(b,a) \notin R$ – hence R is not symmetric. Also $(c,d) \in R$, $(d,c) \in R$, but $c \neq d$ – thus R is not anti-symmetric.

Definition. 1.11 Let R be a relation on a set X. Then the *inverse* of R, denoted by R^{-1}, is the relation $R^{-1} = \{(y,x) \in X \times X : (x,y) \in R\}$.



If one draws the figure, it can be observed that the inverse of a relation R is nothing but the mirror image of R about the diagonal.

From the definition it immediately follows that:

1. A relation R is symmetric if and only if $R = R^{-1}$.
2. A relation R is anti-symmetric if and only if $R \cap R^{-1} = \Delta_X$.

Definition. 1.12 A relation R on a set S is called a *preorder relation* if it is (i) reflexive and (ii) transitive. R is called a *partial order relation* if it is (i) reflexive, (ii) transitive and (iii) anti-symmetric.

Usually a partial order is written as '$\leq$'. If P is a set and $\leq$ is a partial order on the set P then the pair $(P, \leq)$ is called a *partially ordered set* or a POset.

Example. 1.13

1. The usual '$<$' or '$>$' are preorder relations on $\mathbb{R}$. The relations '$\leq$' and ' $\geq$' are partial orders on $\mathbb{R}$.
2. On $\mathbb{N}$ define a relation $\preccurlyeq$ is defined by $m \preccurlyeq n$ if and only if m divides n, i.e., there exists an integer q such that $n = mq$. Then $\preccurlyeq$ is a partial order on $\mathbb{N}$.
3. If X is a non-empty set then the relation $\subseteq$ on the power set $P(X)$ is a partial order.

Definition. 1.14 A relation R on a set X is called an *equivalence relation* on X if it is (i) reflexive, (ii) symmetric and (iii) transitive.

Example. 1.15

1. For any non-empty set X the diagonal relation Δ_X is the simplest example of equivalence relation.
2. For any set X, $X \times X$ is an equivalence relation.
3. For a positive integer p, the relation ρ_p on $\mathbb{Z}$ is an example of equivalence relation.
4. On $\mathbb{C}$, the set of all the complex numbers, define a relation '$\sim$' as follows: for all $z_1, z_2 \in \mathbb{C}$, $z_1 \sim z_2$ if and only if $|z_1| = |z_2|$. Then '$\sim$' is an equivalence relation.

Theorem. 1.16 *Intersection of two equivalence relations is an equivalence relation.*

Proof. Let R and S be two equivalence relations on a set X.

Since R and S are reflexive, $\Delta_X \subset R$ and $\Delta_X \subset S$ and hence $\Delta_X \subset R \cap S$. Thus $R \cap S$ is reflexive.

Also by symmetry of R and S, for $x, y \in X$, $(x, y) \in R \cap S \Rightarrow (x, y) \in R$ and $(x, y) \in S \Rightarrow (y, x) \in R$ and $(y, x) \in S \Rightarrow (y, x) \in R \cap S$. Hence $R \cap S$ is symmetric.

Finally, assume that $(x, y) \in R \cap S$ and $(y, z) \in R \cap S$ where $x, y, z \in X$. Then $(x, y) \in R$ and $(y, z) \in R$, also $(x, y) \in S$ and $(y, z) \in S$. By transitivity of R and S we have $(x, z) \in R$ and $(x, z) \in S$. Thus $(x, z) \in R \cap S$, i.e., $R \cap S$ is transitive.

Hence $R \cap S$ is an equivalence relation on X. ■

Union of two equivalence relations need not be an equivalence relation. We can see it by citing the following example.

Example. 1.17 Consider the equivalence relations ρ_5 and ρ_7 on $\mathbb{Z}$. Here $(1, 6) \in \rho_5$ since $|6 - 1| = 5$ is divisible by 5. Also $(6, 13) \in \rho_7$ since $|13 - 6| = 7$ is divisible by 7. Since $\rho_5 \subset \rho_5 \cup \rho_7$ and $\rho_7 \subset \rho_5 \cup \rho_7$ it follows that $(1, 6)$ and $(6, 13)$ both belong to $\rho_5 \cup \rho_7$. But $(1, 13)$ does not belong to either of ρ_5 and ρ_7 and hence $(1, 13) \notin \rho_5 \cup \rho_7$. Thus $\rho_5 \cup \rho_7$ is not transitive and hence it is not an equivalence relation.

1.2 Partition of a Set

Definition. 1.18 Let I be a non-empty set, if for each $i \in I$ there is a set A_i then the collection $\{A_i : i \in I\}$ is called an *indexed family of sets*, the set I is called the *index set*.

EXAMPLE. 1.19 1. Let $I = \{1, 2, 3, 4\}$. Then the set of sets $\{A_1, A_2, A_3, A_4\}$ is an indexed family of sets can be written as $\{A_i : i \in \{1, 2, 3, 4\}\}$.

2. If for each $n \in \mathbb{N}$ there is a set A_n, then $\{A_n : n \in \mathbb{N}\}$ is an indexed family of sets, $\mathbb{N}$ being the index set.

3. Let $I = \{x : 1 \leq x \leq 1\}$, the closed interval $[0, 1]$. If for each $x \in I$, $J_x = [x-1, x+1]$, the closed interval with end points $x - 1$ and $x + 1$, then $\{J_x : x \in I\}$ is an indexed family of sets.

DEFINITION. 1.20 Let $\{A_i : i \in I\}$ be an indexed family of sets. The union of this family is the set

$$\bigcup_{i \in I} A_i = \cup\{A_i : i \in I\} = \{x : x \in A_i \text{ for some } i \in I\}.$$

The intersection of this family is

$$\bigcap_{i \in I} A_i = \cap\{A_i : i \in I\} = \{x : x \in A_i \text{ for all } i \in I\}.$$

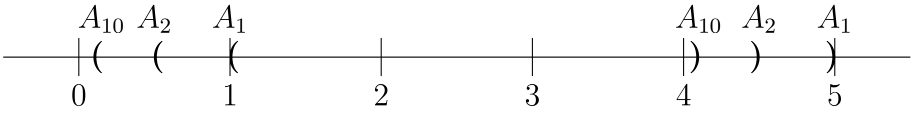
EXAMPLE. 1.21 1. If $I = \{1, 2, 3, 4, 5\}$ and $A_i = (i, i + 1)$ for all $i \in I$, find $\cup_{i=1}^{5} A_i$ and $\cap_{i=1}^{5} A_i$.

$$\begin{aligned} \cup_{i=1}^{5} A_i &= \cup\{A_i : i \in I\} = \{x : x \in A_i \text{ for some } i \in I\} \\ &= \{x : i < x < i + 1 \text{ for some } i \in I\} \\ &= \{x : i < x < i + 1, \text{ for some } i, 1 \leq i \leq 5\} \\ &= \{x : 1 < x < 6, i \neq 1, 2, 3, 4, 5\} \\ &= (1, 6) - \{1, 2, 3, 4, 5\}. \end{aligned}$$

$\cap_{i=1}^{5} A_i = \emptyset$ since the sets are pairwise disjoint.

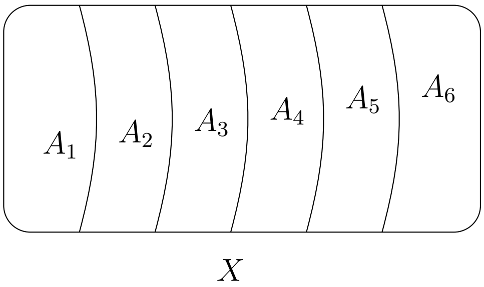
2. If for each $n \in \mathbb{N}$ if $A_n = (\frac{1}{n}, 4 + \frac{1}{n})$ find $\cup\{A_n : n \in \mathbb{N}\}$ and $\cap\{A_n : n \in \mathbb{N}\}$.

Let $A = \cup\{A_n : n \in \mathbb{N}\}$. Take $x \in \mathbb{R}$. If $x \leq 0$ then $x \notin A_n$ for any $n \in \mathbb{N}$, hence $x \notin A$. If $0 < x < 1$, then we can find $n \in \mathbb{N}$ such that $\frac{1}{n} < x$ and hence $x \in A_n \subset A$. If $1 \leq x \leq 4$, then $x \in A_n$ for all $n \in \mathbb{N}$. For $4 < x < 5$, $x \in A_1 \subset A$. For $x \geq 5, x \notin A_n$ for all $n \in \mathbb{N}$ and hence $x \notin A$. Thus $x \in A$ if and only if $0 < x < 5$, hence $A = \cup\{A_n : n \in \mathbb{N}\} = (0, 5)$.



Let $B = \cap\{A_n : n \in \mathbb{N}\}$. To find the intersection, note that $A_n \subset (1, 4]$ for all $n \in \mathbb{N}$ hence $(1, 4] \subset B$. If $x \leq 1$ then $x \notin A_1$ and hence $x \notin B$. If $x > 4$ we can find $n \in \mathbb{N}$ such that $4 + \frac{1}{n} < x$ and hence $x \notin A_n$ so that $x \notin B$. Thus $x \in B$ if and only if $1 < x \leq 4$. Hence $\cap\{A_n : n \in \mathbb{N}\} = (1, 4]$.

Definition. 1.22 Let X be a set. A collection $\mathcal{P} = \{A_i : i \in I\}$ is called a partition of the set X if (i) $X = \cup\{A_i : i \in I\}$ and for $i, j \in I, i \neq j \Rightarrow A_i \cap A_j = \emptyset$.



The set X is partitioned into disjoint subsets $A_1, A_2, \ldots, A_6$ of X.
$A_i \cap A_j = \emptyset$ for $i \neq j$; $i, j \in \{1, 2, \ldots, 6\}$ and $A_1 \cup A_2 \cup \cdots \cup A_6 = X$.

Example. 1.23

1. For each $n \in \mathbb{Z}$ define $I_n = (n, n + 1]$. Then we have $I_m \cap I_n = \emptyset$ for $m \neq n$, $m, n \in \mathbb{Z}$. Also $\bigcup_{n=-\infty}^{\infty} I_n = \cup\{I_n : n \in \mathbb{Z}\} = \mathbb{R}$. Thus $\{I_n : n \in \mathbb{Z}\}$ is a partition of $\mathbb{R}$.

2. For $i = 0, 1, 2, \ldots, 5$, define $A_i = \{6k + i : k \geq 0\}$.

$$A_0 = \{6, 12, 18, 24, \ldots\}, \quad A_1 = \{1, 7, 13, 19, \ldots\}, \quad A_2 = \{2, 8, 14, 20, \ldots\}$$
$$A_3 = \{3, 9, 15, 21, \ldots\}, \quad A_4 = \{4, 10, 16, 22, \ldots\}, \quad A_5 = \{5, 11, 17, 23, \ldots\}.$$

Here $A_i \cap A_j = \emptyset$ when $i \neq j$ and $A_0 \cup A_1 \cup \cdots \cup A_6 = \mathbb{N}$. Hence $\{A_0, A_1, \ldots, A_5\}$ is a partition of $\mathbb{N}$.

Theorem. 1.24 *Let X be a set ρ be an equivalence relation on X. Then ρ induces a partition $\mathcal{P}_\rho$ on the set X. On the other hand if $\mathcal{P}$ is a partition on the set X then there exists an equivalence relation $\rho_{\mathcal{P}}$ of X such that $\mathcal{P} = \mathcal{P}_{\rho_{\mathcal{P}}}$.*

Proof. Assume that ρ is an equivalence relation on X. For each $a \in X$ define a subset $\rho(a)$ of X by $\rho(a) = \{b \in X : a\rho b\}$. Then since $a\rho a$, $a \in \rho(a)$ and hence $\rho(a) \neq \emptyset$ for all $a \in X$. It also follows that $X = \cup\{\rho(a) : a \in X\}$.

We now show that for $a, b \in X$ either $\rho(a) = \rho(b)$ or $\rho(a) \cap \rho(b) = \emptyset$. If $\rho(a) \cap \rho(b) \neq \emptyset$ choose $x \in \rho(a) \cap \rho(b)$. Then $x \in \rho(a) \Rightarrow a\rho x \Rightarrow x\rho a$ (by symmetry) and $x \in \rho(b) \Rightarrow$

$b\rho x \Rightarrow x\rho b$ (by symmetry). Now, for any $y \in X$,

$$\begin{aligned}
y \in \rho(a) \;&\Rightarrow\; a\rho y \Rightarrow y\rho a \text{ (symmetry)}\\
y\rho a \text{ and } a\rho x \;&\Rightarrow\; y\rho x \text{ (transitivity)}\\
y\rho x \text{ and } x\rho b \;&\Rightarrow\; y\rho b \text{ (transitivity)} \;\Rightarrow\; b\rho y \text{ (symmetry)} \;\Rightarrow\; y \in \rho(b).
\end{aligned}$$

Hence $y \in \rho(a) \Rightarrow y \in \rho(b)$, thus $\rho(a) \subset \rho(b)$. Similarly, we can show for any $z \in X$, $z \in \rho(b) \Rightarrow z \in \rho(a)$, i.e., $\rho(b) \subset \rho(a)$. Hence $\rho(a) = \rho(b)$.

Hence X is expressed as $X = \cup\{\rho(a) : a \in X\}$, where the sets $\rho(a)$'s are disjoint or equal for different a's. Thus $\mathcal{P}_\rho = \{\rho(a) : a \in X\}$ is a partition of X.

Conversely, assume that $\mathcal{P} = \{A_i : i \in I\}$ is a partition of X. Define a relation ρ on X by, for all $a, b \in X$, $a\rho b$ if and only if $\{a, b\} \subset A_i$ for some $i \in I$, i.e. $a\rho b$ if and only if a and b belong to the same member A_i of the partition $\mathcal{P}$.

Reflexivity and symmetry of ρ follows immediately. To show transitivity, Let $a, b, c \in X$ such that $a\rho b$ and $b\rho c$. Then there are $A_i, A_j \in \mathcal{P}$ such that $\{a, b\} \subset A_i$ and $\{b, c\} \subset A_j$. This shows that $b \in A_i \cap A_j$, i.e., $A_i \cap A_j \neq \emptyset$. But $\mathcal{P}$ being a partition of X, either $A_i \cap A_j = \emptyset$ or $A_i = A_j$. Hence we must have $A_i = A_j$, i.e., $a, b, c \in A_i$. Hence $a\rho c$ thus ρ is transitive.

Let $a \in A_i$. Then $b \in \rho(a) \iff a\rho b \iff a$ and b belong to the same member of $\mathcal{P}$ $\iff b \in A_i$. Thus $\rho(a) = A_i$. Hence $\mathcal{P}_\rho = \mathcal{P}$. ■

Definition. 1.25 For an equivalence relation ρ on a set X and for $a \in X$ the set $\rho(a) = \{b \in X : a\rho b\}$ is called the equivalence class of ρ containing a. The equivalence class $\rho(a)$ is also denoted by $\bar{a}$ or by $[a]$ or by (a).

From the above theorem we see that the equivalence classes of an equivalence relation ρ on a set X has the following properties:

1. Equivalence class of an element contains that element, i.e., $a \in [a]$ for all $a \in X$.
2. For $a, b \in X$ either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.
3. $X = \cup\{[a] : a \in X\}$.

Definition. 1.26 For an equivalence relation ρ on a set X the set of all equivalence classes is called the *quotient set of* ρ and is denoted by X/ρ. Thus $X/\rho = \{\rho(a) : a \in X\}$.

Example. 1.27 Define a relation ρ_5 on $\mathbb{N}$ by $m\rho_5 n$ if and only if $|m-n|$ is divisible by 5. Show that ρ_5 is an equivalence relation on $\mathbb{N}$ and find its quotient set.

That ρ_5 is an equivalence relation has already been shown in a previous example. Note that $\rho_5(1) = \{m \in \mathbb{N} : 1\rho_5 m\} = \{m \in \mathbb{N} : |m-1| \text{ is divisible by } 5\} = \{1, 6, 11, 16, \ldots\}$. Similarly we can show that $\rho_5(2) = \{2, 7, 12, 17, \ldots\}$, $\rho_5(3) = \{3, 8, 13, 18, \ldots\}$, $\rho_5(4) = \{4, 9, 14, 19, \ldots\}$ and $\rho_5(5) = \{5, 10, 15, 20, \ldots\}$. We can see $\rho_5(6)$ is same as $\rho_5(1)$, $\rho_5(7)$ is same as $\rho_5(2)$ and so on. Hence $\mathbb{N}/\rho_5 = \{\rho_5(1), \rho_5(2), \rho_5(3), \rho_5(4), \rho_5(5)\}$.

1.3 Exercise

1. Let $X = \{a, b, c, d, e\}$, construct relation ρ on X such that ρ is (i) reflexive but not symmetric and transitive, (ii) reflexive and symmetric but not transitive, (iii) not reflexive but symmetric and transitive, (iv) reflexive and transitive but not symmetric.

2. If $X = \{1, 2, 3\}$ find all the equivalence relations on X, or equivalently all the partitions of X.

3. Let $X = \{a, b, c, d\}$ and $\mathcal{P} = \{\{a\}, \{b, c\}, \{d\}\}$. Find the equivalence relation induced by $\mathcal{P}$.

4. Verify which of the following relations on $\mathbb{Z}$ are equivalence relations:

   (a) $\rho = \{(a, b) : a^2 = b^2\}$.

   (b) $\rho = \{(a, b) : |a| \leq |b|\}$.

   (c) $\rho = \{(a, b) : |a| = |b|\}$.

   (d) $\rho = \{(a, b) : a - b \text{is divisible by} 9\}$.

   (e) $\rho = \{(a, b) : a^2 - b^2 \text{is divisible by} 5\}$.

   (f) $\rho = \{(a, b) : a = b^3\}$.

5. Let $\rho = \Delta_X \cup \{(p, q), (q, p), (p, t), (r, s), (r, t), (s, r), (s, t), (t, p), (t, r), (t, s)\}$ be a relation on the set $X = \{p, q, r, s, t\}$. Show that ρ is an equivalence relation on X and find the partition induced by ρ and the quotient set.

6. Let M_2 denote the set of all 2×2 matrices over the real numbers. Define a relation σ on M_2 by $A\sigma B$ if and only if there is a matrix P in M_2 such that $A = PBP^{-1}$. Verify whether σ is an equivalence relation on M_2.

2 Functions

2.1 Definition and Examples

Functions are special type of relations.

Definition. 2.1 Let X, Y be two nonempty sets, a subset $f \subset A \times B$ is called a *function* from X to Y, written as $f : X \to Y$, if it satisfies the following conditions:

1. For every $x \in X$ there exists $y \in Y$ such that $(x, y) \in f$,
2. for $x \in X$ if $(x, y_1) \in f$ and $(x, y_2) \in f$, where $y_1, y_2 \in Y$, then $y_1 = y_2$.

If $(x, y) \in f$ the it is written as $y = f(x)$.

The set X is called the *domain* of f and Y is called the *codomain* of f.

The *range* of f is the subset $f(X)$ of Y defined by

$$f(X) = \{f(x) : x \in X\} = \{y \in Y : \exists x \in X \text{ such that } y = f(x)\}.$$

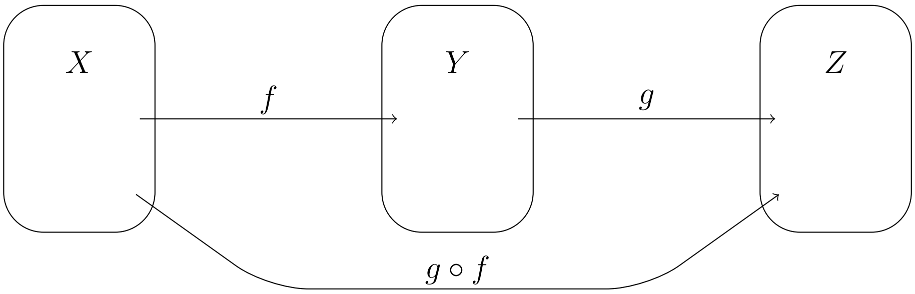
If $y = f(x)$ we say y is the *image* of x and x is called a *pre-image* of y.

It can be observed from the above definition that (i) condition 1 says that every element x in the domain has an image in the range and the condition 2 says that an element in the domain can not have more than one images. However different elements of the domain of a function can have same image.

Example. 2.2

1. For $A = \{a, b, c\}, B = \{x, y, z\}$, $f = \{(a, x), (b, y), (c, y)\} \subset A \times B$ is a function. We write it as $f(a) = x, f(b) = f(c) = y$. Here we see that b and c have the same image y, i.e., y has two pre-images b and c, the domain of f is A and the codomain of f is B. The set $\{x, y\} \subset B$ is the range of f.
2. Denote $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} : x \geq 0\}$. The relation $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ defined by $f(x) = \sqrt{x}$ is not a function, since any $x > 0$ has two images, $+\sqrt{x}$ and $-\sqrt{x}$. However $f(x) = +\sqrt{x}$ and $f(x) = -\sqrt{x}$ are functions. Hence whenever we write *the function* $f(x) = \sqrt{x}$ we mean the positive square root.
3. For any nonempty set X the function $i_X : X \to X$, defined by $i_X(x) = x$ for all $x \in X$, is called the identity function on X.

Definition. 2.3 Let $f : X \to Y$ and $g : Y \to Z$ be two functions. The *composition* of f and g is a function $g \circ f : X \to Z$ defined by $(g \circ f)(x) = g(f(x))$ for all $x \in X$.



Example. 2.4 1. $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ and $g(x) = e^x$, $x \in \mathbb{R}$. Then $(g \circ f)(x) = g(f(x)) = g(x^2) = e^{x^2}$ and $(f \circ g)(x) = f(g(x)) = f(e^x) = (e^x)^2 = e^{2x}$.

2. $f, g : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = ax^2 + bx + c$ and $g(x) = \sin x + \cos x$. Then $(g \circ f)(x) = g(f(x)) = g(ax^2 + bx + c) = \sin(ax^2 + bx + c) + \cos(ax^2 + bx + c)$ and $(f \circ g)(x) = f(g(x)) = f(\sin x + \cos x) = a(\sin x + \cos x)^2 + b(\sin x + \cos x) + c$.

Theorem. 2.5 *For function $f : X \to Y, g : Y \to Z, h : Z \to W$, $h \circ (g \circ f) = (h \circ g) \circ f$, i.e., the composition of functions obeys the associative laws.*

Proof. For $x \in X$, $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f))(x)$. Hence $h \circ (g \circ f) = (h \circ g) \circ f$. ■

Definition. 2.6 Let $f : X \to Y$ be a function, $A \subset X, B \subset Y$. Then we define

$$\begin{aligned} f(A) &= \{f(x) : x \in A\} = \{y \in Y : \exists x \in A \text{ such that } y = f(x)\} \\ f^{-1}(B) &= \{x \in X : f(x) \in B\} = \{x \in X : \exists y \in B \text{ such that } y = f(x)\} \end{aligned}$$

$f(A)$ is called the *image* of A under f and $f^{-1}(B)$ is called the *pre-image* of B under f. Thus the range of f is the set $f(X) \subset Y$.

Theorem. 2.7 *let $f : X \to Y$ be a function, $A_1, A_2 \subset X$, $B_1, B_2 \subset Y$. Then*

1. *If $A_1 \subset A_2$ then $f(A_1) \subset f(A_2)$.*
2. *$f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$,*
3. *$f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$,*
4. *If $B_1 \subset B_2$ then $f^{-1}(B_1) \subset f^{-1}(B_2)$.*
5. *$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$,*
6. *$f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.*

Proof. **1.** Assume $A_1 \subset A_2$. Then $y \in f(A_1) \Rightarrow \exists x \in A_1$ such that $y = f(x)$. Now $x \in A_1 \Rightarrow x \in A_2 \Rightarrow f(x) \in f(A_2) \Rightarrow y \in f(A_2)$. Hence $y \in f(A_a) \Rightarrow y \in f(A_2)$. Thus $A_1 \subset A_2 \Rightarrow f(A_1) \subset f(A_2)$.

2. $y \in f(A_1 \cup A_2) \Rightarrow y = f(x)$ for some $x \in A_1 \cup A_2$. Also

$$\begin{aligned} x \in A_1 \cup A_2 &\Rightarrow x \in A_1 \text{ or } x \in A_2 \Rightarrow f(x) \in f(A_1) \text{ or } f(x) \in f(A_2) \\ &\Rightarrow y \in f(A_1) \text{ or } y \in f(A_2 \Rightarrow y \in f(A_1) \cup f(A_2). \end{aligned}$$

Thus $y \in f(A_1 \cup A_2) \Rightarrow y \in f(A_1) \cup f(A_2)$, i.e., $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$.

Conversely, since $A_1 \subset A_1 \cup A_2$, by 1 above $f(A_1) \subset f(A_1 \cup A_2)$. Similarly $f(A_2) \subset f(A_1 \cup A_2)$. Hence $f(A_1) \cup f(A_2) \subset f(A_1 \cup A_2)$.

Combining, $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

3. Choose $y \in f(A_1) \cap f(A_2)$. Then there exists $x \in A_1 \cap A_2$ such that $y = f(x)$. Now, $x \in A_1 \cap A_2 \Rightarrow x \in A_1$ and $x \in A_2 \Rightarrow f(x) \in f(A_1)$ and $f(x) \in f(A_2) \Rightarrow f(x) \in f(A_1) \cap f(A_2) \Rightarrow y \in f(A_1) \cap f(A_2)$. Hence $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.

4. $x \in f^{-1}(B_1) \Rightarrow f(x) \in B_1 \Rightarrow f(x) \in B_2 \Rightarrow x \in f^{-1}(B_2)$. Hence the result follows.

5. $x \in f^{-1}(B_1 \cup B_2) \iff f(x) \in B_1 \cup B_2 \iff f(x) \in B_1$ or $f(x) \in B_2 \iff x \in f^{-1}(B_1)$ or $x \in f^{-1}(B_2) \iff x \in f^{-1}(B_1) \cup f^{-1}(B_2)$. Hence $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.

6. $x \in f^{-1}(B_1 \cap B_2) \iff f(x) \in B_1 \cap B_2 \iff f(x) \in B_1$ and $f(x) \in B_2 \iff x \in f^{-1}(B_1)$ and $x \in f^{-1}(B_2) \iff x \in f^{-1}(B_1) \cap f^{-1}(B_2)$. Hence $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$. ■

The inclusion in (3) of the above theorem may be proper. For example take $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 1 - x^2, x \in \mathbb{R}$. Let $A = [-1, 0]$ and $B = [0, 1]$. Then

$$f(A) = \{1 - x^2 : -1 \leq x \leq 0\} = [0, 1] \text{ and } f(B) = \{1 - x^2 : 0 \leq x \leq 1\} = [0, 1].$$

Hence $f(A) \cap f(B) = [0, 1]$. But $A \cap B = \{0\}$ and $f(A \cap B) = \{f(0)\} = \{1\}$. Hence $f(A \cap B) \subsetneqq f(A) \cap f(B)$

Definition. 2.8 1. A function $f : X \to Y$ is called *injective* or *one-one* if for all $x, y \in X$, $x \neq y \Rightarrow f(x) \neq f(y)$, or equivalently, $f(x) = f(y) \Rightarrow x = y$.

2. $f : X \to Y$ is called *surjective* or *onto* if the range of f is Y, i.e., for all $y \in Y$ there is $x \in X$ such that $y = f(x)$.

3. f is called *bijective* if it is both injective and surjective.

Example. 2.9 1. $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is neither injective nor surjective. For $a > 0$ $f(a) = f(-a) = a^2$ but $a \neq -a$, hence f is not injective. Also for $b < 0$ there exists no $a \in \mathbb{R}$ for which $f(a) = b$, hence f is not surjective.

However if the codomain has been changed to $\mathbb{R}_{\geq 0}$ then f becomes surjective.

2. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = ax + b, a \neq 0$ is bijective. If $x_1, x_2 \in \mathbb{R}$ such that $x_1 \neq x_2$. Then $ax_1 \neq ax_2$ and hence $ax_1 + b \neq ax_2 + b$, i.e., $f(x_1) \neq f(x_2)$. Hence f is surjective.

Also for $y \in \mathbb{R}$, take $x = \frac{y-b}{a}$ so that $f(x) = a \cdot \frac{y-b}{a} + b = y$. Hence f is surjective.

3. The function $f : [0, 2\pi] \to [-1, 1]$ defined by $f(x) = \sin x$ is surjective but not injective. For $y \in [-1, 1], x = \sin^{-1} y \in [0, 2\pi]$ so that $f(x) = y$. Hence f is surjective. Also $f(0) = f(\pi)$ shows that f is not injective.

Theorem. 2.10 *For the functions $f : X \to Y$ and $g : Y \to Z$,*

1. *If f and g are injective then $g \circ f$ is injective.*

2. *If f and g are surjective then $g \circ f$ is surjective.*

Proof. 1. Since f, g is injective, for $x_1, x_2 \in X$, $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \Rightarrow g(f(x_1)) \neq g(f(x_2))$. Hence $x_1 \neq x_2 \Rightarrow (g \circ f)(x_1) \neq (g \circ f)(x_2)$. Thus $g \circ f$ is injective,

2. For $z \in Z$, since g is surjective, there exists $y \in Y$ such that $g(y) = z$. Also since f is surjective there exists $x \in X$ such that $f(x) = y$. Hence $(g \circ f)(x) = g(f(x)) = g(y) = z$. Thus $g \circ f$ is surjective. ■

Theorem. 2.11 *For the functions $f : X \to Y$ and $g : Y \to Z$,*

1. *If $g \circ f$ is injective then f is injective.*

2. *If $g \circ f$ is surjective then g is surjective.*

Proof. 1. Take $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. Now $(g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2)$ and hence $x_1 = x_2$ since $g \circ f$ is injective. Thus $f(x_1) = f(x_2)$ implies that $x_1 = x_2$ which shows that f is injective.

2. Choose $z \in Z$. Since $g \circ f$ is surjective there exists $x \in X$ such that $(g \circ f)(x) = z$, i.e., $g(f(x)) = z$. Let $f(x) = y$. Then $g(y) = z$, thus y is a pre-image of z under g and hence g is surjective. ■

The following result follows immediately.

Corollary. 2.12 *If $f : X \to Y$ and $g : Y \to Z$ are functions such that $g \circ f$ is bijective then f is injective and g is surjective.*

Definition. 2.13 Let $fX \to Y$ be a function. A function $g : Y \to X$ is called a *left inverse* of f if $g \circ f = i_X$. A function $h : Y \to X$ is called a *right inverse* of f if $f \circ h = i_Y$. A function which is both left inverse and right inverse is called the inverse of f and is denoted by f^{-1}. Thus $f \circ f^{-1} = i_Y$ and $f^{-1} \circ f = i_X$.

Example. 2.14

1. Let $A = \{a, b, c, d\}$ and $B = \{u, v, w, x, y\}$. Define $f : A \to B$ by $f(a) = u, f(b) = v, f(c) = w, f(d) = x$. The function $g : B \to A$ is defined by $g(u) = a, g(v) = b, g(w) = c, g(x) = d, g(y) = a$.

   Then $(g \circ f)(a) = g(f(a)) = g(u) = a$, similarly, $(g \circ f)(b) = b, (g \circ f)(c) = c$ and $(g \circ f)(d) = d$. Thus $g \circ f = i_A$ and hence g is left inverse of f.

   On the other hand, $(f \circ g)(u) = f(g(u)) = f(a) = u$. Similarly, $(f \circ g)(v) = v, (f \circ g)(w) = w, (f \circ g)(x) = x$ and $(f \circ g)(y) = f(g(y)) = f(a) = u$. Hence $(f \circ g) \neq i_B$, thus g is not right inverse of f.

2. let $A = \{a, b, c, d\}$ and $B = \{x, y, z\}$. Define $f : X \to Y$ by $f(a) = f(b) = x, f(c) = y, f(d) = z$ and $h : B \to A$ by $h(x) = a, h(y) = c, h(z) = d$. Then $(f \circ h)(x) = f(h(x)) = f(a) = x$. Similarly, $(f \circ h)(y) = y, (f \circ h)(z) = z$, hence $f \circ h = i_B$.

   But $(h \circ f)(b) = h(f(b)) = h(x) = a$ shows that $h \circ f \neq i_A$. Thus h is right inverse of f by not a left inverse of f.

Theorem. 2.15 *Let $f : X \to Y$ be a function. then*

1. *f has a left inverse if and only if f is injective.*
2. *f has a right inverse if and only if f is surjective.*

Proof. 1. Assume that f has a left inverse $g : Y \to X$. Then $g \circ f = i_X$. Let $x_1, x_2 \in X$, such that $f(x_1) = f(x_2)$. Then $g(f(x_1)) = g(f(x_2))$, i.e., $(g \circ f)(x_1) = (g \circ f)(x_2) \Rightarrow i_X(x_1) = i_X(x_2) \Rightarrow x_1 = x_2$. Hence f is injective.

Conversely, assume that f is injective. Define $g : Y \to X$ as follows: for $y \in Y$ if y belongs to the range of f then there exists $x \in X$ such that $y = f(x)$, define $g(y) = x$. If y is not in the range of f then define $g(y)$ arbitrarily in X. Then for all $x \in X$, $(g \circ f)(x) = g(f(x)) = g(y) = x$. Hence $g \circ f = i_X$ and hence g is a left inverse of f.

2. Assume that f has a right inverse $h : Y \to X$. Then $f \circ h = i_Y$. let $y \in Y$. Then $y = i_Y(y) = (f \circ h)(y) = f(h(y))$. Thus $h(y)$ is a pre-image of y. Hence f is surjective.

Conversely, assume that f is surjective. For any $y \in Y$ there exists at least one $x \in X$ such that $y = f(x)$, i.e., the set $f^{-1}(\{y\})$ is non-empty. For each $y \in Y$ choose $x \in f^{-1}(\{y\})$ arbitrarily and define $h(y) = x$. (Such a choice is possible by *Axiom of Choice*). Then $(f \circ h)(y) = f(h(y)) = f(x) = y$, since $x \in f^{-1}(\{x\})$. Thus $f \circ h = i_Y$, i.e., h is right inverse of f. ■

Definition. 2.16 A function $f : X \to Y$ is called *left invertible* if it has a left inverse $g : Y \to X$ such that $g \circ f = i_X$. f is called *right invertible* if it has right inverse $h : Y \to X$ such that $f \circ h = i_Y$. The function f is called *invertible* if it it has an inverse f^{-1}, which is both left and right inverse.

Theorem. 2.17 *A function f is invertible if and only if f is a bijection.*

Proof. It follows from the theorem 2.15.

Students are requested to write the complete proof of this theorem using 2.15.

Remark. 2.18 It can be noted that if $f : A \to B$ is a bijection then $f^{-1} : B \to A$ is also a bijection, so without any loss of generality, instead of saying *there is a bijection from A to B*, we can say *there is a bijection between A and B*.

Definition. 2.19 Two sets A and B are said to be *equipotent* if there exists a bijection between A and B and is denoted by $A \sim B$. Two equipotent sets are said to be of the *same cardinality.*

Theorem. 2.20 *If X is an universal set and $P(X)$ denoted the set of all subsets of X, i.e., the power set of X, then $\sim$ is an equivalence relation on $P(X)$.*

Proof. For any set A, $i_A : A \to A$ is a bijection and hence $A \sim A$. So $\sim$ is reflexive. Also, for $A, B \subset X$, $A \sim B \Rightarrow \exists$ a bijection $f : A \to B \Rightarrow f^{-1} : B \to A$ is a bijection $\Rightarrow B \sim A$. Hence $\sim$ is symmetric. Finally, if $A \sim B$ and $B \sim C$, $A, B, C \subset X$, then there are bijections $f : A \to B$ and $g : B \to C$. So $g \circ f : A \to C$ is a bijection and hence $A \sim C$. Thus $\sim$ is transitive. So $\sim$ is an equivalence relation on $P(X)$. ■

Hence all the sets belonging to an equivalence class of $\sim$ have the same cardinality.

Definition. 2.21 For an integer $n \in \mathbb{N}$ the cardinal number of the set $I_n = \{1, 2, \ldots, n\}$ is defined to be n. Hence any set equipotent with I_n has the cardinal number n. Cardinal number of the empty set is defined as zero. For any set A the cardinal number of the set A is denoted by $|A|$ or by $n(A)$ or by $card(A)$.

Hence the cardinal number of a finite set is the number of elements in that set.

Theorem. 2.22 *A set can not be equipotent with its power set.*

Proof. If possible, let $A \sim P(A)$, where $P(A)$ is the power set of A. Then there exists a bijection $h : A \to P(A)$. Note that for all $x \in A$, $h(x)$ is a subset of A.

Define a set $D \subset A$ by $D = \{x \in A; x \notin h(x)\}$. Since h is surjective there exists $x_0 \in A$ such that $h(x_0) = D$. Now, if $x_0 \in D$ then by the property of D, $x_0 \notin h(x_0) = D$. Again, if $x_0 \notin D = h(x_0)$ then $x_0 \in D$. Hence a paradox arises.

So there is no $x_0 \in A$ such that $h(x_0) = D$ and hence h is not surjective. Thus there is no surjective map from A to $P(A)$, and hence A can not be equipotent with $P(A)$.

Definition. 2.23 A set is called *countable* if it is equipotent with $\mathbb{N}$. The cardinal number of a countable set is written as $\aleph_0$ (pronounced as "Alef zero", alef is the first letter of Hebrew alphabets).

Example. 2.24 The set $\mathbb{Z}$ is countable.

Define $f : \mathbb{N} \to \mathbb{Z}$ by $f(n) = \frac{n-1}{2}$ if n is odd and $f(n) = -\frac{n}{2}$ if n is even. Hence $f(1) = 0, f(2) = -1, f(3) = 1, f(4) = -2, f(5) = 2, \ldots$. It is easy to verify that f is a bijection. (Students are requested to verify by themselves).

Hence $|\mathbb{Z}| = \aleph_0$, i.e., $\mathbb{Z}$ is countable.

Example. 2.25 The open interval $(0, 1)$ is equipotent to $\mathbb{R}_{>0} = (0, \infty)$.

Define $f : (0, 1) \to \mathbb{R}_{>0}$ by $f(x) = \frac{x}{1-x}$, $x \in (0, 1)$.

For $x_1, x_2 \in (0, 1)$, $x_1 \neq x_2 \Rightarrow 1 - x_1 \neq 1 - x_2 \Rightarrow \frac{1}{1-x_1} \neq \frac{1}{x_2} \Rightarrow f(x_1) \neq f(x_2)$. Hence f is injective. Also if $y \in \mathbb{R}_{>0}$ put $x = \frac{y}{1+y}$. Then $0 < x < 1$ and $f(x) = f(\frac{y}{1+y}) = \frac{\frac{y}{1+y}}{1-\frac{y}{1+y}} = \frac{\frac{y}{1+y}}{\frac{1}{1+y}} = y$. Hence f is surjective. Thus f is a bijection between $(0, 1)$ and $\mathbb{R}_{>0}$.

Remark. 2.26 It has been observed from the above two examples that an infinite set can be equipotent with a proper subset of it. However it is not true that all infinite subsets are equipotent. If X is an infinite set then it is never be equipotent with its power set $P(X)$. It is known for a finite set A, if $|A| = n$ then $|P(A)| = 2^n$. Following it the cardinality of $P(\mathbb{N})$ is denoted by $2^{\aleph_0}$.

2.2 Exercise

1. Verify whether the following functions are injective, surjective or bijective.

   (a) $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = e^x$.

   (b) $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = \cos x$.

   (c) $f : [-1, 1] \to [0, 2\pi]$ by $f(x) = \sin^{-1} x$.

   (d) $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 + 8x + 15$.

   (e) $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^3$.

   (f) $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x|x|$.

   (g) $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x - [x]$.

2. Find $f(A)$ where f and A are given by

   (a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$, $A = [-1, 1]$.

   (b) $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ defined by $f(x) = \sqrt{x}$, $A = [2, 4]$.

   (c) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = [x]$, $A = [0, 4)$.

   (d) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x|x|$, $A = [-2, 2]$.

3. Find $f^{-1}(B)$ where f and B are given by

   (a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = ax^2 - 2bx - a$, $B = \{0\}$.

   (b) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \sin x$, $B = [0, \frac{1}{\sqrt{2}}]$.

   (c) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \tan x$, $B = [-1, 1]$.

4. For $f : X \to Y$ and $A \subset X$ prove that $A \subset f^{-1}(f(A))$.

5. For $f : X \to Y$ and $B \subset Y$ prove that $B = f(f^{-1}(B))$.

6. If $f : X \to Y$ is injective and $A, B \subset X$, prove that $f(A - B) \subset f(A) - f(B)$.

7. If $f : X \to Y$ and $C, D \subset Y$, prove that $f^{-1}(C - D) = f^{-1}(C) - f^{-1}(D)$.

8. Let $f : X \to Y$ be surjective and $g, h : Y \to X$ be such that $g \circ f = h \circ f$. Then prove that $g = h$.

9. Let $h : Y \to X$ be injective and $f, g : X \to Y$ be such that $h \circ f = h \circ g$. Then prove that $f = g$.

3 Theory of numbers

The natural numbers 1, 2, 3, ... are also called the positive integers. The set of positive integers is denoted by $\mathbb{N}$. The positive integers together with the negative of integers and zero are called integers and the set of integers is denoted by $\mathbb{Z}$.

THEOREM. 3.1 *The set* $\mathbb{N}$ *has the following properties:*

1. *Every natural number* n *has a successor* $n + 1$,
2. *Every natural number* n *except* $n = 1$ *has a predecessor* $n - 1$,
3. *Mathematical Induction: If* $M \subset \mathbb{N}$ *satisfying the properties (i)* $1 \in M$ *and (ii) if* $n \in M$ *then its successor* $n + 1 \in M$, *Then* $M = \mathbb{N}$.

The usual ordering relation $\leq$ on $\mathbb{N}$ is a total order. $\mathbb{N}$ also possesses the *well ordering property* which states that

THEOREM. 3.2 (WELL ORDERING PROPERTY) *Every non-empty subset of the set of non-negative integers has a least element (first element).*

THEOREM. 3.3 (ARCHIMEDEAN PROPERTY) *If* a, b *are a positive integers then there is a positive integer* n *such that* $an > b$.

We shall study the theorems stated above in future. Here we shall apply the above results whenever necessary.

3.0.1 Divisibility

DEFINITION. 3.4 If a, b are integers then b is called *divisible by* a or equivalently a *divides* b if there exists an integer n such that $b = an$. If a divides b it is denoted by $a \mid b$. If a does not divide b then it is written as $a \nmid b$.

EXAMPLE. 3.5 It is easy to see that $2 \mid 8, 11 \mid 132, 17 \mid 306$ etc. We also have $3 \nmid 10$, $12 \nmid 100$, $13 \nmid 122$ etc.

THEOREM. 3.6 *For integers* a, b, c, d *the following holds:*

1. $a \mid 0$, $1 \mid a$ *and* $a \mid a$.

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

3. *If $a \mid b$ and $c \mid d$ then $ac \mid bd$.*

4. *If $a \mid b$ and $b \mid c$ then $a \mid c$.*

5. *$a \mid b$ and $b \mid a$ if and only if $a = \pm b$.*

6. *If $a \mid b$ and $b \neq 0$ then $|a| \leq |b|$.*

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

Proof. Proof is 1 and 2 are immediate. For 3, there exists integers x, y such that $b = ax, d = cy$, hence $bd = (xy)(ac)$. Since xy is an integer we have $ac \mid bd$.

For 4, there are integers x, y such that $b = ax, c = by$, hence $c = a(xy)$ showing $a \mid c$.

For 5, there are integers x, y such that $b = ax$ and $a = by$. Thus $a = axy$, hence $xy = 1$, i.e., either $x = y = 1$ or $x = y = -1$, i.e., either $b = a$ or $b = -a$. Hence $a = \pm b$.

For 6, there exists integer x such that $b = ax$. Since $b \neq 0$, $x \neq 0$ and hence $|x| \geq 1$. So, $|b| = |a|.|x| \geq |a|$.

For 7, there are integers p, q such that $b = ap, c = aq$. Hence for any integers x, y, $bx + cy = apx + aqy = a(px + qy)$. Hence $a \mid (bx + cy)$. ■

Theorem. 3.7 (Division Algorithm) *If a, b are integers with $a > 0$ then there exist unique integers q, r such that $b = aq + r$ where $0 \leq r < a$.*

Proof. Consider the set

$$S = \{b - ax : x \text{ is integer and } b - ax \geq 0\}.$$

Since $a \geq 1$, we have $a|b| \geq |b|$. Thus taking $x = -|b|$, we have $b - a(-|b|) = b + a|b| \geq 0$ and hence $b - ax \in S$ when $x = -|b|$. Thus $S \neq \emptyset$.

By the well ordering property S has a least element say r. Let the value of x corresponding to r be q, i.e., $r = b - aq$. Thus we get $b = aq + r$. Since $r \in S$, $r \geq 0$. To show that $r < a$, assume that $r \geq a$ then $r_1 = b - a(q + 1) = b - aq - a = r - a \geq 0$ and hence $r_1 \in S$ and $r_1 \leq r$ contradicting that r is the least element of S. Thus $r < a$.

To check the uniqueness of r and q assume that there are integers q, q', r, r', $0 \leq r, r' < a$ such that $b = aq + r = aq' + r'$. Then $r - r' = a(q' - q)$, or $|r - r'| = a|q - q'|$.

Since $0 \leq r < a$ and $-a < -r' \leq 0$, adding $-a < r - r' < a$, i.e., $|r - r'| < a$. Hence $a|q - q'| = |r - r'| < a$ implies that $|q - q'| < 1$. Since q, q' are integers, $|q - q'|$ must be a non-negative integer and hence $|q - q'| = 0$, thus $q = q'$. This gives $a|q - q'| = 0$, i.e., $|r - r'| = 0$, hence $r = r'$. ■

DEFINITION. 3.8 For integers a, b, $a > 0$, if $b = aq + r$ by division algorithm, q ia called the *quotient* and r is called the *remainder* in the division of b by a.

EXAMPLE. 3.9

1. Taking $a = 12, b = 30$ we have $30 = 12 \cdot 2 + 6$. Hence quotient $q = 2$ and the remainder $r = 6$.

2. $a = 13, b = 1427$, $1427 = 13 \cdot 109 + 10$, so $q = 109, r = 10$.

3. $a = 7, b = -24$. So $-24 = 7 \cdot (-4) + 4$. Here $q = -4, r = 4$.

4. $a = 23, b = -1128$. So $-1128 = 23(-50) + 22$. Hence $q = -50, r = 22$.

COROLLARY. 3.10 *If a, b are integers with $a \neq 0$ then there exist unique integers q and r such that $b = aq + r$ where $0 \leq r < |a|$.*

PROOF. The result has already been proved for $a > 0$, now take $a < 0$. Then $|a| = -a > 0$, hence for b there exist unique q', r' such that $b = |a|q' + r'$ where $0 \leq r' < |a|$. Taking $q = -q'$ and $r = r'$ we have $b = qa + r$. ■

EXAMPLE. 3.11

1. The square of any integer of the form $9k$ or $3k + 1$.

   If n is any integer then dividing n by 3 we have $n = 3q + r$ where $0 \leq r < 3$. Squaring, $n^2 = 9q^2 + 6qr + r^2 = 3q(3q + 2r) + r^2$. Since r can be 0, 1 or 2,

$$\begin{aligned}
\text{When } r = 0 \quad &: \quad n^2 = 9q^2 = 9k, \text{ where } k = q^2. \\
\text{When } r = 1 \quad &: \quad n^2 = 3q(3q + 2r) + 1 = 3k + 1, \text{ where } k = q(3q + 2r). \\
\text{When } r = 2 \quad &: \quad n^2 = 3q(3q + 2r) + 4 = 3(3q^2 + 2qr) + 3 + 1 \\
&= \quad 3(3q^2 + 2qr + 1) + 1 = 3k + 1, \text{ where } k = 3q^2 + 2qr + 1.
\end{aligned}$$

   Thus in all cases $n^2 = 3k + 1$ or $n^2 = 9k$.

2. The cube of any integer of the form $9k$ or $9k + 1$ or $9k + 8$.

If n is any integer, dividing by 3 by division algorithm $m = 3q + r$ where $r = 0, 1$ or 2. So $m^3 = (3q + r)^3 = 27q^3 + 9qr(3q + r) + r^3 = 9(3q^3 + qr(3q + r)) + r^3$.

$$\begin{aligned} \text{When } r = 0 \ &: \ m^3 = (3q)^3 = 9k, \text{ where } k = 3q^3. \\ \text{When } r = 1 \ &: \ m^3 = 9(3q^3 + q(3q + 1)) + 1 = 9k + 1, \\ &\qquad \text{where } k = 9(3q^3 + q(3q + 1)) \\ \text{When } r = 2 \ &: \ m^3 = 9(3q^3 + 2q(3q + 2)) + 8 = 9k + 8, \\ &\qquad \text{where } k = 9(3q^3 + 2q(3q + 2)). \end{aligned}$$

Example. 3.12 If an integer is simultaneously a square and a cube then it must be either of the form $7k$ or $7k + 1$. [For example $64 = 8^2 = 4^3$]

Let $n = m^2 = l^3$. Now dividing m by 7 using division algorithm we have $m = 7q_1 + r_1$ where $0 \leq r_2 \leq 6$. Then $n = m^2 = 7(7q^2 + 2qr_1) + r_1^2$.

$$\begin{aligned} \text{when } r_1 = 0 \ &: \ m^2 \ = \ 7(7q^2) \\ \text{when } r_1 = 1 \ &: \ m^2 \ = \ 7(7q^2 + 2q) + 1 \\ \text{when } r_1 = 2 \ &: \ m^2 \ = \ 7(7q^2 + 4q) + 4 \\ \text{when } r_1 = 3 \ &: \ m^2 \ = \ 7(7q^2 + 6q) + 9 \ = \ 7(7q^2 + 6q + 1) + 2 \\ \text{when } r_1 = 4 \ &: \ m^2 \ = \ 7(7q^2 + 8q) + 16 \ = \ 7(7q^2 + 6q + 2) + 2 \\ \text{when } r_1 = 5 \ &: \ m^2 \ = \ 7(7q^2 + 10q) + 25 \ = \ 7(7q^2 + 6q + 3) + 4 \\ \text{when } r_1 = 6 \ &: \ m^2 \ = \ 7(7q^2 + 12q) + 36 \ = \ 7(7q^2 + 6q + 5) + 1. \end{aligned}$$

Thus $n = m^2$ can be expressed in the form of $7k$ or $7k + 1$ or $7k + 2$ or $7k + 4$.

Again dividing l by 7 using division algorithm we have $l = 7q + r_2$ where $0 \leq r_2 \leq 6$. Then $n = l^3 = (7q)^3 + 3.7qr_2(7q + r_2) + r_2^3 = 7(49q^3 + 3qr_2(7q + r_2)) + r_2^3$.

$$\begin{aligned} \text{when } r_2 = 0 \ &: \ l^3 = 7(49q^3) \\ \text{when } r_2 = 1 \ &: \ l^3 = 7(49q^3 + 3q(7q + 1)) + 1 \\ \text{when } r_2 = 2 \ &: \ l^3 = 7(49q^3 + 6q(7q + 2)) + 8 \ = \ 7(49q^3 + 6q(7q + 2) + 1) + 1 \\ \text{when } r_2 = 3 \ &: \ l^3 = 7(49q^3 + 9q(7q + 3)) + 27 \ = \ 7(49q^3 + 9q(7q + 2) + 3) + 6 \\ \text{when } r_2 = 4 \ &: \ l^3 = 7(49q^3 + 12q(7q + 4)) + 64 \ = \ 7(49q^3 + 12q(7q + 2) + 9) + 1 \\ \text{when } r_2 = 5 \ &: \ l^3 = 7(49q^3 + 15q(7q + 5)) + 125 \ = \ 7(49q^3 + 15q(7q + 2) + 17) + 6 \\ \text{when } r_2 = 6 \ &: \ l^3 = 7(49q^3 + 18q(7q + 2)) + 216 \ = \ 7(49q^3 + 18q(7q + 2) + 30) + 6. \end{aligned}$$

Thus $n = l^3$ must be of the form $7k$ or $7k + 1$ or $7k + 6$.

So combining these two, when $n = m^2 = l^3$ then n must be of the form $7k$ or $7k + 1$.

3.1 The Greatest Common Divisor

Divisibility of integers has already been defined and a number of properties has been mentioned in Theorem 3.6. Here we define and study the properties of greatest common divisors.

Definition. 3.13 Let a, b be two integers. An integer d is called a *common divisor* if $d \mid a$ and $d \mid b$. If at least one of a, b is non-zero, then the integer d is called the *greatest common divisor* or gcd of a and b if

1. $d > 0$, $d \mid a$ and $d \mid b$,
2. If $c \mid a$ and $c \mid b$ then $c \leq d$.

The gcd of a and b is denoted by $\gcd(a, b)$ or by (a, b).

Example. 3.14 For $a = -18$ and $b = 30$ the positive divisor of a are $2, 3, 6, 9$ and the positive divisors of b are $2, 3, 5, 6, 10, 15$. The common divisors are $2, 3$ and 6. hence the greatest common divisor is 6, i.e., $\gcd(-18, 30) = 6$.

Theorem. 3.15 *Given integers a, b, not both of them are zero, there exist integers x, y such that* $\gcd(a, b) = ax + by$.

Proof. Define a set $S = \{au + bv : u, v \text{ are integers}, au + bv > 0\}$. Since a and b are not both zero simultaneously, we may assume that $a \neq 0$. If $a > 0$ then taking $u = 1, v = 0$, $au + bv = a \in S$ and if $a < 0$ then taking $u = -1, v = 0$, $au + bv = -a \in S$. Thus $S \neq \emptyset$. By well ordering principle S has a least element, say d. So there exist integers $u = x, v = y$ such that $d = ax + by$.

By division algorithm, dividing a by d, we have $a = dq + r$ where $0 \leq r < d$. Hence $r = a - dq = a - (ax + by)q = a(1 - qx) + b(-yq) = ax' + by'$. If $r > 0$ then $r \in S$ which is a contradiction since d is the smallest element of S and $r < d$. Hence $r = 0$, i.e., $a = dq$, i.e., $d \mid a$. Similarly $d \mid b$. Thus d is a common divisor of a and b.

Let c be a positive common divisor of a and b, i.e., $c \mid a$ and $c \mid b$. Then by Theorem 3.6 $c \mid (ax + by)$, i.e., $c \mid d$. hence $c = |c| \leq |d| = d$.

Thus $\gcd(a, b) = d = ax + by$. ■

Corollary. 3.16 *For integers a, b, not both zero, $T = \{ax + by : x, y \text{ are integers}\}$ is precisely the set of all the multiples of $d = \gcd(a, b)$.*

Proof. Since $d \mid a$ and $d \mid b$ it follows that $d \mid (ax + by)$ for all integers x any y. Thus d divides every member of T, i.e., every member of T is a multiple of d.

Since $d = ax_0 + by_0$ for some integers x_0, y_0, a multiple of d is $cd = c(ax_0 + bx_0) = a(cx_0) + b(cy_0) = ax + by \in T$. Thus every multiple of d belongs to T. ■

Definition. 3.17 Two integers a, b are said to be relatively prime or *prime to each other* if $\gcd(a, b) = 1$.

Theorem. 3.18 *Two integers a, b are prime to each other if and only of there exist integers x, y such that $ax + by = 1$.*

Proof. If a, b are relatively prime then $\gcd(a, b) = 1$. So there exist integers x, y such that $ax + by = \gcd(a, b) = 1$.

Conversely, if there exist integers x, y such that $ax+by = 1$ and $\gcd(a, b) = d$ then $ax+by$ must be a multiple of d, i.e., $d \mid (ax + by)$, i.e., $d \mid 1$. Since $d > 0$ we have $d = 1$. Thus a and b are relatively prime. ■

Corollary. 3.19 *If $\gcd(a, b) = d$ then $\frac{a}{d}, \frac{b}{d}$ are relatively prime.*

Proof. Since $\gcd(a, b) = d$ there exist integers x, y such that $d = ax + by$. Hence $\frac{a}{d}x + \frac{b}{d}y = 1$. This shows that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, i.e., the integers $a/d, b/d$ are relatively prime. ■

Corollary. 3.20 *If $\gcd(a, b) = 1$ and $a \mid c, b \mid c$ then $(ab) \mid c$.*

Proof. Since $a \mid c, b \mid c$ we have $c = am, c = bn$ for some integers m, n. Also since $\gcd(a, b) = 1$ there exist integers x, y such that $ax + by = 1$. Now $c = c \cdot 1 = c(ax + by) = acx + bcy = a(bn)x + b(am)y = ab(nx + my)$. Thus $(ab) \mid c$.

Theorem. 3.21 (Euclid's Lemma) *If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.*

Proof. Since $\gcd(a, b) = 1$ there exist integers x, y such that $ax+by = 1$. Now $c = c\cdot 1 = c(ax + by) = acx + bcy$. Also since $a \mid bc$ there exist an integer m such that $bc = am$. Thus $c = acx + bcy = acx + amy = a(cx + my)$. Thus a is a factor of c, i.e., $a \mid c$. ■

The above result may not be true if $\gcd(a, b) \neq 1$. For example, take $a = 6, b = 9, c = 8$. Then $a \mid bc$ but $a \nmid b, a \nmid c$.

Example. 3.22 1. It immediately follows that: $\gcd(a, 0) = |a|$, $\gcd(a, a) = |a|$ and $\gcd(a, 1) = 1$.

2. If a is any integer and n is a positive integer then $\gcd(a, a+n)$ divides n.

   If $\gcd(a, a+n) = d$ then $d \mid a$ and $d \mid (a+n)$. Hence $d \mid (a+n-a)$, i.e., $d \mid n$. In particular taking $n = 1$, $\gcd(a, a+1) = 1$.

3. If for integers x, y, $\gcd(a, b) = ax + by$ then $\gcd(x, y) = 1$.

   Let $\gcd(a, b) = d = ax + by$. then $\frac{a}{d}x + \frac{b}{d}y = 1$, this shows that $\gcd(x, y) = 1$.

3.2 Euclid's Algorithm

In the present section we describe a practical method to find the ggc of two integers. We start with the following lemma.

Lemma. 3.23 *For integers a, b if $b = aq + r$, $0 \le r < a$ then* $\gcd(a, b) = \gcd(a, r)$.

Proof. Assume that $d = \gcd(a, b)$.Then $d \mid a$ and $d \mid b$ thus $d \mid (b - aq)$, i.e., $d \mid r$. Hence d is a common divisor of a and r. Let c be a positive common divisor of a and r. Then $c \mid a$ and $c \mid r$ which implies that $c \mid (aq + r)$, i.e., $c \mid b$. Thus c is a common divisor of a and b and hence $c \le b$. Thus $\gcd(a, r) = d$. ■

We now describe the Euclid's algorithm of finding gcd of two integers a and b. Since for any integers a, b, $\gcd(a, b) = \gcd(|a|, |b|)$ without any loss of generality we may assume that $b \ge a > 0$.

Divide b by a, then by division algorithm we have $b = aq_1 + r_1$, $0 \le r_1 < a$. If $r_1 = 0$ then $a \mid b$ and hence $\gcd(a, b) = a$. If $r_1 > 0$ then divide a by r_1 to get $a = r_1q_2 + r_2$. Again divide r_1 by r_2 and get $r_1 = r_2q_3 + r_3$. Proceed this process until the remainder r_n in some stage n vanishes. Hence we get,

$$\begin{aligned}
b &= aq_1 + r_1,\ 0 \le r_1 < a \\
a &= r_1q_2 + r_2,\ 0 \le r_2 < r_1 \\
r_1 &= r_2q_3 + r_3,\ 0 \le r_3 < r_2 \\
\vdots \quad & \quad \vdots \\
r_{n-2} &= r_{n-1}q_n + r_n,\ 0 \le r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1} + 0,
\end{aligned}$$

Then it has been claimed that $\gcd(a, b) = r_n$, the last non-zero remainder. This follows from the previous lemma $\gcd(a, b) = \gcd(a, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n)$.

Since $r_n \mid r_{n-1}$ it follows that $\gcd(r_{n-1}, r_n) = r_n$. Thus $\gcd(a, b) = r_n$.

Example. 3.24 1. Find the gcd of 14328 and 1732. Also find integers x, y such that $\gcd(14327, 1732) = 14327x + 1732y$.

By division algorithm we get

$$\begin{aligned} 14328 &= 1732 \cdot 8 + 472 \\ 1732 &= 472 \cdot 3 + 316 \\ 472 &= 316 \cdot 1 + 156 \\ 316 &= 156.2 + 4 \\ 156 &= 4 \cdot 39 + 0 \end{aligned}$$

Thus $\gcd(14328, 1732) = 4$. Now From the above divisions

$$\begin{aligned} \gcd(14328, 1732) &= 4 \;=\; 316 - 2 \cdot 156 \\ &= 316 - (472 - 316) \cdot 2 \;=\; -472 \cdot 2 + 316 \cdot 3 \\ &= -472 \cdot 2 + (1732 - 472 \cdot 3) \cdot 3 \;=\; 1732 \cdot 3 - 472 \cdot 11 \\ &= 1732 \cdot 3 - (14328 - 1732 \cdot 8) \cdot 11 \\ &= -14328 \cdot 11 + 1732 \cdot 91. \end{aligned}$$

Hence $x = -11$ and $y = 91$, i.e., $\gcd(14328, 1732) = 4 = 14328(-11) + 1732 \cdot 91$.

2. Find the gcd of 5304 and 48477. Also find integers x, y such that $\gcd(48477, 5304) = 48477x + 5304y$.

$$\begin{aligned} 48477 &= 5304 \cdot 9 + 741 \\ 5304 &= 741 \cdot 7 + 117 \\ 741 &= 117 \cdot 6 + 39 \\ 117 &= 39 \cdot 3 + 0. \end{aligned}$$

Hence $\gcd(5304, 48477) = 39$. Form the above divisions,

$$\begin{aligned} \gcd(5304, 48477) &= 39 \;=\; 741 - 117 \cdot 6 \\ &= 741 - (5304 - 741 \cdot 7) \cdot 6 \;=\; -5304 \cdot 6 + 741 \cdot 43 \\ &= -5304 \cdot 6 + (48477 - 5304 \cdot 9) \cdot 43 \\ &= 48477 \cdot 43 - 5304 \cdot 393. \end{aligned}$$

Hence $x = 43, y = -393$, i.e., $\gcd(48477, 5304) = 39 = 48477 \cdot 43 + 5304 \cdot (-393)$.

3.3 Congruences

Definition. 3.25 For integers a, b and $m > 0$ if $m \mid (a - b)$ then we say a *is congruent to* b *modulo* m and is denoted by $a \equiv b \pmod{m}$. If $m \nmid (a - b)$ we say that a is not congruent to b modulo m and write as $a \not\equiv b \pmod{m}$.

Example. 3.26 (i) $2 \equiv 22 \pmod{5}$. since $2 - 22 = -20$ is divisible by 5. Similarly, (ii) $5 \equiv -7 \pmod{6}$, (iii) $95 \equiv 0 \pmod{19}$, (iv) $-32 \equiv 19 \pmod{17}$ etc. Also $22 \not\equiv -17 \pmod{7}$, $-51 \not\equiv 10 \pmod{17}$, $89 \not\equiv 0 \pmod{12}$ etc.

Theorem. 3.27 *Let $m > 0$ and a, b, c, d be any integers. Then*

1. $a \equiv a \pmod{m}$.
2. *If* $a \equiv b \pmod{m}$ *then* $b \equiv a \pmod{m}$.
3. *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$ *then* $a \equiv c \pmod{m}$.
4. *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$ *then* $a + c \equiv b + d \pmod{m}$.
5. *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$ *then* $ac \equiv bd \pmod{m}$.
6. *If* $a \equiv b \pmod{m}$ *and* $d \mid m$*, where* $d > 0$ *then* $a \equiv b \pmod{d}$.
7. *If* $a \equiv b \pmod{m}$ *and where* $c > 0$ *then* $ac \equiv bc \pmod{mc}$.
8. *If* $a \equiv b \pmod{m}$ *then for any positive integer* k, $a^k \equiv b^k \pmod{m}$

Proof. 1. Immediate.

2. $a \equiv b \pmod{m} \Rightarrow m \mid (a - b) \Rightarrow m \mid (b - a) \Rightarrow b \equiv a \pmod{m}$.

3. $a \equiv b \pmod{m} \Rightarrow m \mid (a - b)$ and $b \equiv c \pmod{m} \Rightarrow m \mid (b - c)$. Hence $m \mid (a - b) + (b - c)$, i.e., $m \mid (a - c)$. Thus $a \equiv c \pmod{m}$.

4. $a \equiv b \pmod{m} \Rightarrow m \mid (a - b)$ and $c \equiv d \pmod{m} \Rightarrow m \mid (c - d)$. Thus m divides $(a - b) + (c - d)$, i.e., $m \mid (a + c) - (b + d)$. Hence $a + c \equiv b + d \pmod{m}$.

5. $a \equiv b \pmod{m} \Rightarrow m \mid (a - b) \Rightarrow a - b = km$ for some integer k and $c \equiv d \pmod{m} \Rightarrow m \mid (c - d) \Rightarrow c - d = lm$ for some integer l. Thus $ac = (b + km)(d + lm) = bd + m(bl + dk + klm)$, i.e., $ac - bd = m(bl + dk + klm)$, which shows that $m \mid (ac - bd)$. Thus $ac \equiv bd \pmod{m}$.

6. $a \equiv b \pmod{m} \Rightarrow m \mid (a - b)$. Since $d \mid m$, where $d > 0$ we have $d \mid (a - b)$. Hence $a \equiv b \pmod{d}$.

7. $a \equiv b \pmod{m} \Rightarrow m \mid (a-b)$. For $c > 0$ we have $mc \mid c(a-b)$, i.e., $mc \mid (ac-bc)$. Thus $ac \equiv bc \pmod{m}c$.

8. This follows by repeated application of 5 above taking $c = a$ and $d = b$. ■

Theorem. 3.28 *For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if a and b leave the same non-negative remainder when divided by m.*

Proof. Assume that $a \equiv b \pmod{m}$. Then $a - b = mk$ for some integer k, thus $a = b + mk$. Now, dividing b by m by division algorithm we have $b = mq + r$ where $0 \leq r < m$.

Hence $a = b + mk = mq + r + mk = m(q + k) + r$ where $0 \leq r < m$. Thus both of a, b leave the same remainder r when divided by m.

Conversely, assume that both of a, b leave the same remainder when divided by m. Then $a = mq_1 + r, b = mq_2 + r$ and hence $a - b = m(q_1 - q_2)$, i.e., $m \mid (a-b)$. Thus we have $a \equiv b \pmod{m}$. ■

Cancellation is allowed in congruences in some special conditions.

Theorem. 3.29 *If for integers a, b, c, $ac \equiv bc \pmod{m}$ then $a \equiv b \pmod{\frac{m}{d}}$ where $d = \gcd(c, m)$.*

Proof. $ac \equiv bc \pmod{m}$ implies that $ac - bc = km$ for some integer k. Since $\gcd(c, m) = d$ there exist integers p, q such that $c = pd, m = qd$ and $\gcd(p, q) = 1$. Thus $apd - bpd = kqd$, i.e., $(a-b)p = kq$. This shows that $q \mid (a-b)p$. Since $\gcd(p, q) = 1$, by Euclid's Lemma, $q \mid (a-b)$, i.e., $a \equiv b \pmod{q}$. But $q = \frac{m}{d}$. hence the result holds. ■

Two immediate consequences of the above result are the following.

Corollary. 3.30 *If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$ then $a \equiv b \pmod{m}$.*

Corollary. 3.31 *If $ac \equiv bc \pmod{p}$ where p is prime and $p \nmid c$ then $a \equiv b \pmod{p}$.*

Theorem. 3.32 *If f is a polynomial function with integer coefficient and $a \equiv b \pmod{m}$ then $f(a) \equiv f(b) \pmod{m}$.*

Proof. Let $f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$, where $c_0, c_1, \ldots, c_n$ are integers. Now $a \equiv b \pmod{m}$ implies that $a^k \equiv b^k \pmod{m}$ for all positive integer k. Also for integers c_k, $a^k \equiv b^k \pmod{m}$ gives $c_ka^k \equiv c_kb^k \pmod{m}$. Thus adding from $k = 0$ to n,

$$c_0 + c_1a + c_2a^2 + \cdots + c_na^n \equiv c_0 + c_1b + c_2b^2 + \cdots + c_nb^n \pmod{m},$$

i.e., $f(a) \equiv f(b) \pmod{m}$. ■

Example. 3.33 If $x_n x_{n-1} \ldots x_1 x_0$ is the decimal representation of a number m, where $x_0, x_1, \ldots x_n \in \{0, 1, 2, \ldots, 9\}$, then m is divisible by 9 if and only if $x_0 + x_1 + \cdots + x_n$ is divisible by 9.

Let $f(x) = x_0 + x_1 x + x_2 x^2 + \cdots + x_n x^n$. Then f is a polynomial with integer coefficients. We have $m = 10^n x_n + 10^{n-1} x_{n-1} + \cdots + 10 x_1 + x_0 = f(10)$ and $f(1) = x_0 + x_1 + \cdots + x_n$.

Since $10 \equiv 1 \pmod{9}$ we have $f(10) \equiv f(1) \pmod{9}$, i.e., $m \equiv (x_1 + x_2 + \cdots + x_n) \pmod{9}$. Hence m is divisible by 9 if and only if $m \equiv 0 \pmod{9}$ if and only if $x_1 + x_2 + \cdots + x_n \equiv 0 \pmod{9}$ if and only if $x_1 + x_2 + \cdots + x_n$ is divisible by 9.

For example, if $m = 403713 = 4 \cdot 10^5 + 0 \cdot 10^4 + 3 \cdot 10^3 + 7 \cdot 10^2 + 1 \cdot 10^1 + 3$. Then m is divisible by 9 if and only if $4 + 0 + 3 + 7 + 1 + 3 = 18$ is divisible by 9, which is true. Thus 403713 is divisible by 9.

Example. 3.34 If $x_n x_{n-1} \ldots x_1 x_0$ is the decimal representation of a number M, where $x_0, x_1, \ldots x_n \in \{0, 1, 2, \ldots, 9\}$, then M is divisible by 11 if and only if $x_0 - x_1 + \cdots + (-1)^n x_n$ is divisible by 11.

Let $f(x) = x_0 + x_1 x + x_2 x^2 + \cdots + x_n x^n$. Then f is a polynomial with integer coefficients.

Note that $10 \equiv -1 \pmod{11}$. Hence $f(10) \equiv f(-1) \pmod{11}$. But $f(10) = M$ and $f(-1) = x_0 - x_1 + x_2 - \cdots + (-1)^n x_n$. Hence M is divisible by 11 if and only if $x_0 - x_1 + \cdots + (-1)^n x_n$ is divisible by 11.

Example. 3.35 Find the remainder when 2^{20} is divided by 41.

Note that $2^5 = 32$ and $32 \equiv (-9) \pmod{41}$. Hence $(2^5)^2 \equiv (-9)^2 \pmod{41}$, i.e., $2^{10} \equiv 81 \pmod{41}$. Also $81 \equiv -1 \pmod{41}$. Hence $2^{10} \equiv (-1) \pmod{41}$. This gives $(2^{10})^2 \equiv (-1)^2 \pmod{41}$, i.e., $2^{20} \equiv 1 \pmod{41}$. Hence the remainder is 1 when 2^{20} is divided by 41, or equivalently, $2^{20} - 1$ is divisible by 41.

Example. 3.36 Find the remainder when 2^{50} is divided by 7.

$2^3 = 8$ and $8 \equiv 1 \pmod{7}$. Thus $2^3 \equiv 1 \pmod{7}$. Thus $(2^3)^{16} \equiv 1^{16} \pmod{7}$, i.e., $2^{48} \equiv 1 \pmod{7}$. Also $2^2 \equiv 2^2 \pmod{7}$. Thus $2^{48} \cdot 2^2 \equiv 1 \cdot 2^2 \pmod{7}$. Hence we have , $2^{50} \equiv 4 \pmod{7}$, i.e., the remainder is 4 when 2^{50} is divided by 7.

Example. 3.37 Find the remainder when 41^{65} is divided by 7.

Here $41 \equiv -1 \pmod 7$. Hence $41^{65} \equiv (-1)^{65} \pmod 7$, i.e., $41^{65} \equiv -1 \pmod 7$. Thus $41^{65}+1$ is divisible by 7. This gives $41^{65}+1-7$ is divisible by 7, i.e., $41^{65}-6$ is divisible by 7. Hence the remainder is 6 when 41^65 is divided by 7.

Example. 3.38 Find the remainder when $1!+2!+\cdots+100!$ is divided by 8.

For all $k \geq 4$, $k! = 4! \times 5 \times \cdots \times k$. Since $4! = 24$ is divisible by 8, $k!$ is divisible by 8 for all $k \geq 4$. Hence $k! \equiv 0 \pmod 8$ for all $k \geq 4$. Thus,

$$\begin{aligned} 1!+2!+3!+4!\cdots+100! &\equiv 1+2+6+0+\cdots+0 \pmod 8 \\ \text{or, } 1!+2!+3!+4!\cdots+100! &\equiv 9 \pmod 8. \end{aligned}$$

Also $9 \equiv 1 \pmod 8$. Hence $1!+2!+3!+4!\cdots+100! \equiv 1 \pmod 8$. Hence the remainder is 1 when $1!+2!+3!+4!\cdots+100!$ is divided by 8.

Example. 3.39 Find the remainder when $3^{12}+5^{12}$ is divided by 13.

$3^3 = 27 \equiv 1 \pmod{13}$. Hence $(3^3)^4 \equiv 1^4 \pmod{13}$, i.e., $3^{12} \equiv 1 \pmod{13}$.

Also $5^2 \equiv -1 \pmod{13}$, hence $(5^2)^6 \equiv (-1)^6 \pmod{13}$, i.e. $5^{12} \equiv 1 \pmod{13}$.

Adding $5^{12}+3^{12} \equiv 1+1 \pmod{13}$, or $5^{12}+3^{12} \equiv 2 \pmod{13}$. Hence the remainder is 2.

Example. 3.40 Find the last two digits of 9^{9^9}.

The last two digits of a number is the remainder when it is divided by 100.

Now, $9 \equiv -1 \pmod{10}$ therefore $9^8 \equiv (-1)^8 = 1 \pmod{10}$. Multiplying by 9, $9^9 \equiv 9 \pmod{10}$. Thus $9^9 = 9+10k$ for some integer k and hence $9^{9^9} = 9^{9+10k} = 9^9 \cdot 9^{10k}$.

$$\begin{aligned} 9^{10} &= (-1+10)^{10} = (-1)^{10} +^{10} C_1(-1)^9 \cdot 10^1 +^{10} C_2(-1)^8 \cdot 10^2 + \cdots + 10^{10} \\ &= 1 -^{10} C_1 \cdot 10^1 +^{10} C_2 \cdot 10^2 + \cdots + 10^{10} \\ &\equiv 1(\text{mod}100), \end{aligned}$$

since from the second term onward each term is congruent to zero mod 100. Hence for each positive integer k, $9^{10k} \equiv 1 \pmod{100}$.

Also

$$\begin{aligned} 9^9 &= (-1+10)^9 = (-1)^9 +^9 C_1(-1)^8 \cdot 10 +^9 C_2(-1)^7 \cdot 10^2 + \cdots + 10^9 \\ &= -1 + 90 +^9 C_2(-1)^7 \cdot 10^2 + \cdots + 10^9 \\ &\equiv 89(\text{mod}100), \end{aligned}$$

since from the third term onward each term is congruent to zero mod 100.

Hence $9^{9^9} = 9^9 \cdot 9^{10k} \equiv 89 \cdot 1 \pmod{100}$, i.e., $9^{9^9} \equiv 89 \pmod{100}$. Thus the last two digits of 9^{9^9} is 89.

3.3.1 Exercise

1. Find the remainder when 2^{24} is divided by 17.
2. Find the remainder when 3^{287} is divided by 23.
3. Find the remainder when 11^{35} is divided by 13.
4. Show that $2^{44} - 1$ is divisible by 89.
5. Find the remainder when 17^{341} is divided by 5.
6. If a is an odd integer then prove that $a^2 \equiv 1 \pmod 8$.

3.4 Linear Congruence Equation

Definition. 3.41 Let m be a fixed positive integer. A set of integers $\{a_1, a_2, \ldots, a_k\}$ is called a *complete residue system modulo m* if

1. $a_i \not\equiv a_j \pmod m$ for all $i \neq j$,
2. For every integer n there is unique a_i such that $n \equiv a_i \pmod m$.

Example. 3.42 1. For a fixed positive integer m, the numbers $0, 1, 2, \ldots, m-1$ form a complete residue system modulo m.

2. The numbers $2, 7, 10, 18, 22, 26, 34$ form a complete set of residues modulo 7. It can be observed that dividing each number by 7 leaves seven remainders 0 to 6.

Definition. 3.43 For integers $a \neq 0, b, n > 0$ an equation of the form $ax \equiv b \pmod n$ is called a *linear congruence.*

An integer x_0 is called a solution of the above linear congruence if $ax_0 \equiv b \pmod n$.

Example. 3.44 The expression $3x \equiv 9 \pmod{12}$ is a linear congruence equation. Here $x_0 = 3$, $x_1 = 7$ and $x_2 = 15$ are three solutions of the linear congruence. It can be observed that the solutions 3 and 15 are congruent modulo 12, however the solutions 3, 7 are not congruent modulo 12. They are called non-congruent solutions and treated as distinct solutions.

Theorem. 3.45 *A linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $\gcd(a,n) \mid b$. If $d = \gcd(a,n)$ then there are d non-congruent solutions.*

Proof. The congruence $ax \equiv b \pmod{n}$ has a solution if and only if $n \mid (ax - b)$, i.e., if and only if there is integer y such that $ax - b = ny$, or $ax - ny = b$.

Since $d = \gcd(a,n)$ there exist integers r, s such that $a = rd, n = sd$ and $\gcd(r,s) = 1$.

Assume that $d \mid b$. So $b = cd$ for some integer c. Since $d = \gcd(a,n)$ there exist integers x_0, y_0 such that $d = ax_0 + ny_0$. Multiplying by c we have, $cd = cax_0 + cny_0$, or, $b = a(cx_0) - n(-cy_0)$ which shows that $a(cx_0) \equiv b \pmod{n}$. Thus cx_0 is a solution of the congruence.

Conversely, let the linear congruence $ax \equiv b \pmod{n}$ have a solution, say x_0. Hence there exists integer y_0 such that $ax_0 - ny_0 = b$, i.e., $rdx_0 - sdy_0 = b$, i.e., $d(rx_0 - sy_0) = b$. Thus $d \mid b$.

Now, assume that x_0 and x_1 be two solutions of the linear congruence $ax \equiv b \pmod{n}$. Then $ax_0 \equiv b \pmod{n}$ and $ax_1 \equiv b \pmod{n}$ and hence $ax_1 - ax_0 \equiv 0 \pmod{n}$, or $n \mid a(x_1 - x_0)$, or $sd \mid rd(x_1 - x_0)$, i.e., $s \mid r(x_1 - x_0)$. Since $\gcd(r,s) = 1$ we have $s \mid (x_1 - x_0)$. We can write $x_1 - x_0 = st$, or $x_1 = x_0 + st = x_0 + \frac{n}{d}t$, where t is any integer.

For $t = t_1, t_2$, two solutions are $x_1 = x_0 + \frac{n}{d}t_1$ and $x_2 = x_0 + \frac{n}{d}t_2$. Then $x_1 \equiv x_2 \pmod{n}$ if and only if $n \mid \frac{n}{d}(t_1 - t_2)$ i.e., if and only if $d \mid (t_1 - t_2)$. Thus for $t = 0, 1, 2, \ldots, d-1$ we get the d incongruent solutions $x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{n(d-1)}{d}$. Since any integer t is congruent to one of $0, 1, 2, \ldots, d-1$, these are the only incongruent solutions of the linear congruence $ax \equiv b \pmod{n}$. ■

Corollary. 3.46 *If $\gcd(a,n) = 1$ then the linear congruence equation $ax \equiv b \pmod{n}$ has a unique solution modulo n.*

Proof. Here $d = \gcd(a,n) = 1$ and $1 \mid b$. Hence the result follows. ■

Example. 3.47 1. Solve the linear congruence equation: $9x \equiv 21 \pmod{30}$.

Here $\gcd(9,30) = 3$ and $3 \mid 21$. Hence the congruence has 3 incongruent solutions.

We shall find the gcd of 9 and 30.

$$\begin{aligned} 30 &= 9 \cdot 3 + 3 \\ 9 &= 3 \cdot 3 + 0. \end{aligned}$$

Hence $\gcd(9,30) = 3 = 9 \cdot (-3) + 30 \cdot 1$, i.e., $9 \cdot (-21) + 30 \cdot 7 = 21$. Hence $x_0 = -21$ is a solution of $9x \equiv 21 \pmod{30}$. Other solutions are $-21 + \frac{30}{3}t$ where $t = 1, 2$, i.e., $x_1 = -21 + 10 = -11$ and $x_2 = -21 + 20 = -1$. To get positive solutions we add multiples of 10 and get 9, 19 and 29 are incongruent solutions.

2. Solve the linear congruence equation: $25x \equiv 15 \pmod{29}$.

   Here $\gcd(25, 29) = 1$, hence the congruence has the unique solution. By division algorithm,

$$\begin{aligned} 29 &= 25 \cdot 1 + 4 \\ 25 &= 4 \cdot 6 + 1. \end{aligned}$$

   Hence $1 = 25 - 4 \cdot 6 = 25 - (29 - 25) \cdot 6 = 25 \cdot 7 - 29 \cdot 6$. Thus $25 \cdot 7 = 1 + 29 \cdot 6$, or, $25 \cdot (7 \cdot 15) = 15 + 29 \cdot 90$. Hence $25 \cdot 105 \equiv 15 \pmod{29}$, i.e., $x = 105$ is the solution of the congruence. Note that $105 - 29 \cdot 3 = 105 - 87 = 18$, hence $105 \equiv 18 \pmod{29}$. Thus $x = 18$ is a solution congruent modulo 29.

3. Solve the linear congruence equation: $6x \equiv 15 \pmod{21}$.

   Here $\gcd(6, 21) = 3$ and $3 \mid 15$. Hence the system has 3 incongruent solutions. By division algorithm, $21 = 6 \cdot 3 + 3$ which gives $\gcd(6, 21) = 3 = 21 \cdot 1 - 6 \cdot 3$. Multiplying by $15/3 = 5$, $15 = 21 \cdot 5 - 6 \cdot 18$, i.e., $6(-18) = 15 - 21 \cdot 5$. Hence $6(-18) \equiv 15 \pmod{21}$ and so $x = -18$ is a solution of the linear congruence.

   An arbitrary solution is $x = -18 + \frac{21}{3}t = -18 + 7t$, t is any integer. Thus the smallest positive solution is obtained by putting $t = 3$, i.e., $x = -18 + 21 = 3$. Other incongruent solutions are $3 + 7 = 10$ and $3 + 7 \times 2 = 17$.

4. Solve the linear congruence equation: $36x \equiv 8 \pmod{102}$.

   Here to find $\gcd(36, 102)$ we use Euclid's algorithm. By division algorithm,

$$\begin{aligned} 102 &= 36 \cdot 2 + 30 \\ 36 &= 30 \cdot 1 + 6 \\ 30 &= 6 \cdot 5 + 0 \end{aligned}$$

   which gives $\gcd(36, 102) = 6$ and $6 \nmid 8$. Hence the system has no solution.

5. Solve the linear congruence equation: $140x \equiv 133 \pmod{301}$.

We use Euclid's algorithm to find $\gcd(140, 301)$.

$$\begin{aligned} 301 &= 140 \cdot 2 + 21 \\ 140 &= 21 \cdot 6 + 14 \\ 21 &= 14 \cdot 1 + 7 \\ 14 &= 7 \cdot 2 + 0. \end{aligned}$$

Thus $\gcd(140, 301) = 7$ and $133/7 = 19$, i.e., $7 \mid 133$. Thus the congruence has seven incongruent solutions. Now,

$$\begin{aligned} 7 &= 21 - 14 \;=\; 21 - (140 - 21 \cdot 6) \\ &= -140 + 21 \cdot 7 \;=\; -140 + (301 - 140 \cdot 2) \cdot 7 \\ &= 301 \cdot 7 - 140 \cdot 15 \end{aligned}$$

Thus $-140 \cdot 15 = 7 - 301 \cdot 7$. Multiplying by $133/7 = 19$ both sides we have $140(-15 \times 19) = 133 - 301(7 \times 19)$, i.e., $140(-285) = 133 - 301 \times 133$. This shows that 301 divides $140(-285) - 133$ i.e., $140(-285) \equiv 133 \pmod{301}$. Hence $x_0 = -285$ is a solution of the linear congruence $140x \equiv 133 \pmod{301}$. The other incongruent solutions are $x = -285 + \frac{301}{7}t$, $t = 1, 2, \ldots, 6$. Hence a complete set of incongruent solutions is $x = -285 + 43t$, $t = 0, 1, 2, \ldots, 6$.

3.4.1 Exercise

1. Solve the linear congruence equation: $5x \equiv 2 \pmod{26}$.

2. Solve the linear congruence equation: $34x \equiv 60 \pmod{98}$.

3. Solve the linear congruence equation: $8x \equiv 15 \pmod{12}$.

4. Solve the linear congruence equation: $9x \equiv 16 \pmod{24}$.

5. Solve the linear congruence equation: $24x \equiv 9 \pmod{31}$.

3.5 Linear Diophantine Equations

A Diophantine equation is an equation whose coefficients are integers and the solutions are also integers. As an example consider the following problem.

Example. 3.48 A person has Rs 330 in cash, all in Rs 50/- and Rs 20/- notes. How many he has Rs 50 notes and Rs 20 notes?

This is an example of diophantine equation, as all of its solutions must be integers, in fact positive integers. There are several solutions as stated below:

Rs 50/- note	Rs 20 note	Total amount
1	14	330
3	9	330
5	4	330.

There are infinite many solutions, but for this purpose only these three solutions are applicable, as the number notes can not be negative.

A Diophantine equation is called linear if the variables appear in fiest degree only.

3.5.1 Solution of Linear Diophantine Equations

Theorem. 3.49 *A linear diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$ where $d = \gcd(a, b)$.*

Proof. Assume that $d \mid c$.

Since $d = \gcd(a, b)$ there exist integers x, y such that $d = ax+by$. Now by condition $d \mid c$, i.e., there exists integer k such that $c = kd$.

Hence $c = kd = k(ax + by) = a(kx) + b(ky) = ax_0 + by_0$. Thus $x_0 = kx, y_0 = ky$ is a solution set of the equation.

For the converse part, assume that the equation $ax + by = c$ has a solution x_0, y_0. Then $c = ax_0 + by_0$. Since $d = \gcd(a, b)$, $a = ud, b = vd$ for some integers u, v. Hence $c = udx_0 + vdy_0 = d(ux_0 + vy_0)$ which shows that $d \mid c$. ■

The general solutions can be obtained as follows: Let x_0, y_0 be an initial solution and x', y' be another set of solutions. Then $ax_0 + by_0 = c = ax' + by'$ which gives $a(x' - x_0) = b(y_0 - y')$. Since $d = \gcd(a, b)$ there are integers u, v such that $a = ud, b = vd$ and $\gcd(u, v) = 1$. Hence $ud(x' - x_0) = vd(y_0 - y')$, i.e., $u(x' - x_0) = v(y_0 - y')$.

The last identity shows that $u \mid v(y_0 - y')$. Since $\gcd(u, v) = 1$ by Euclid's Lemma $u \mid (y_0 - y')$. Thus there exists integer t such that $y_0 - y' = ut$.

Hence $u(x' - x_0) = vut$, i.e., $x' = x_0 + vt$, or, $x' = x_0 - (b/d)t$. Also we have $y' = y_0 - ut = y_0 - (a/d)t$. The general solution is written as,

$$x = x_0 + \frac{b}{d}t \quad \text{and} \quad y = y_0 - \frac{a}{d}t.$$

It can be shown taht for any integer t the above expression represents a solution.

EXAMPLE. 3.50 Solve the Diophantine Equation. $56x + 72y = 40$.

$\gcd(56, 72) = 8$ and $8 \mid 40$, hence the system has solutions.

Using Euclid's algorithm,

$$\begin{aligned} 72 &= 56 \cdot 1 + 16 \\ 56 &= 16 \cdot 3 + 8 \\ 16 &= 8 \cdot 2 + 0. \end{aligned}$$

Hence $8 = 56 - 16 \cdot 3 = 56 - (72 - 56) \cdot 3 = 56 \cdot 4 - 72 \cdot 3$. Multiplying by 5 (=40/8) we have, $40 = 56 \cdot 20 + 72 \cdot (-15)$. Hence $x_0 = 20, y_0 = -15$ is a solution of the equation.

The general solution is $x = x_0 + (72/8)t = 20 + 9t$ and $y = y_0 - (56/8)t = -15 - 7t$. Putting $t = 0, \pm 1, \pm 2$ etc. we write a few solutions:

$$\begin{aligned} t = 0, \quad & x = 20, \quad y = -15 \\ t = 1, \quad & x = 29, \quad y = -22 \\ t = -1, \quad & x = 11, \quad y = -8 \\ t = 2, \quad & x = 38, \quad y = -29 \\ t = -2, \quad & x = 2, \quad y = -1. \end{aligned}$$

EXAMPLE. 3.51 Solve the Diophantine Equation. $24x + 138y = 18$.

$\gcd(24, 138) = 6$ and $6 \mid 18$. Hence the equation has solutions. By Euclid's Algorithm, $138 = 24 \times 5 + 18, 24 = 18 \times 1 + 6, 18 = 6 \times 3 + 0$.

Hence, $6 = 24 - 18 = 24 - (138 - 24 \times 5) = 24 \times 6 - 138$, i.e., $24 \times 6 + 138 \times (-1) = 6$.

Multiplying by 3, $24 \times 18 + 136 \times (-3) = 18$. Hence $x = 18, y = -3$ is a solution.

The general solution is $x = 18 + \frac{138}{6}t, y = -3 - \frac{24}{6}t$, i.e., $x = 18 + 23t, y = -3 - 4t$, t is integer.

3.5.2 Exercises

Solve the following Diophantine Equations.

1. $221x + 91y = 117$.
2. $84x - 438y = 156$.
3. $30x + 17y = 300$.
4. $54x + 21y = 906$.
5. $123x + 360y = 99$.
6. $158x - 57y = 7$.

3.6 Prime Numbers

One of the most important theories and widely studied topics is the prime number. Here we mention only an introductory result of the theory.

DEFINITION. 3.52 An integer $p > 1$ is called a *prime number* or simply a *prime* if its only positive divisors are 1 and p itself. An integer greater than 1 which is not peime is called a *composite number*.

EXAMPLE. 3.53 The numbers 2, 3, 5, 7, 11, . . . are prime numbers, whereas 4, 9, 16, 25 etc are examples of composite numbers. It can be mentioned that the number 1 is neither prime nor composite. Also 2 is the only even prime number.

THEOREM. 3.54 *If p is a prime and $p \mid ab$ then either $p \mid a$ or $p \mid b$.*

PROOF. If $p \mid a$ then the result is proved. Assume that $p \nmid a$. Then $\gcd(p, a) = 1$ and hence by Euclid algorithm $p \mid b$. ■

COROLLARY. 3.55 *If $p \mid (a_1 a_2 \cdots a_n)$ then $p \mid a_k$ for some $k = 1, 2, \ldots, n$.*

PROOF. This can be proved by induction on n, left to the student as an exercise.

COROLLARY. 3.56 *If $p, q_1, q_2, \ldots, q_n$ are all primes and $p \mid (q_1 q_2 \ldots q_n)$ then $p = q_k$ for some $k = 1, 2, \ldots, n$.*

We conclude this section with the statement of Fundamental Theorem of Arithmetic.

THEOREM. 3.57 (FUNDAMENTAL THEOREM OF ARITHMETIC) *Every positive integer $n > 1$ can be expressed as a product of primes in a unique way up to the order of occurrence of the primes.*

— ∗ —