3. INTEGERS

3.1. Natural numbers.

The set $\mathbf{N}$ consiting of numbers 1,2,3,... is called the *set of all natural numbers*. The *well ordering property* of the set $\mathbf{N}$ states that

every non-empty subset of $\mathbf{N}$ *contains a least element.*

This means that if S be a non-empty subset of $\mathbf{N}$ there is some natural number a in S such that $a \leq x$ for all x in S.

3.1.1. Principle of induction.

Let S be a subset of $\mathbf{N}$ with the properties -

(i) 1 belongs to S, and

(ii) whenever a natural number k belongs to S, then $k+1$ belongs to S.

Then $S = \mathbf{N}$.

Proof. Let T be the set of all those natural numbers which are not in S. The theorem will be proved if we can prove that T is an empty set.

Let us assume that T is a non-empty set. Then by the well ordering property T possesses a least element, say m. Since $1 \in S, m > 1$ and so $m-1$ is a natural number. Again since m is the least element in $T, m-1$ is not in T and so $m-1$ is in S.

Since $m-1$ is in S, by (ii) $(m-1)+1$ is in S, i.e., m is in S which is a contradiction.

Therefore our assumption is wrong and T is empty and the theorem is proved. □

Theorem 3.1.2. Let E_n be a statement involving a natural number n. If

(i) E_1 is true, and

(ii) E_{k+1} is true whenever E_k is true, where k is a natural number, then E_n is true for all natural numbers.

Proof. Let S be the set of those natural numbers n for which the statement E_n is true.

Then S has the properties -

(i) $1 \in S$, and
(ii) $k+1 \in S$ whenever $k \in S$.

Then by the principle of induction $S = \mathbf{N}$.

Thus E_n is true for all $n \in \mathbf{N}$. □

Note. To establish a theorem (or a proposition) involving natural numbers by the principle of induction, both the conditions (i) and (ii) must be established.

The condition (i) is called the *basis of induction* and the assumption made in the condition (ii) is called the *induction hypothesis*.

Worked Examples.

1. Use the principle of induction to prove that
$1+2+\cdots+n = \frac{n(n+1)}{2}$, for all natural numbers n.

Step 1. For $n = 1$ the statement is true because $1 = \frac{1(1+1)}{2}$.

Step 2. Let us assume that the statement is true for some natural number k. Then $1+2+\cdots+k = \frac{k(k+1)}{2}$.

Therefore $1+2+\cdots+k+(k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$.

This shows that the statement is true for the natural number $k+1$ if it is true for k.

By the principle of induction, the statement is true for all natural numbers n.

2. Prove that $3^{2n} - 8n - 1$ is divisible by 64.

We use the principle of induction to prove the statement. Let $f(n) = 3^{2n} - 8n - 1$.

Step 1. $f(1) = 9 - 8 - 1 = 0$. $f(1)$ is divisible by 64. Therefore the statement is true for $n = 1$.

Step 2.
$$\begin{aligned} f(k+1) - f(k) &= [3^{2k+2} - 8(k+1) - 1] - [3^{2k} - 8k - 1] \\ &= 8(3^{2k} - 1) = 8(9^k - 1) \\ &= 8.8(9^{k-1} + 9^{k-2} + \cdots + 1) \\ &= 64p \text{ where } p \text{ is an integer.} \end{aligned}$$

Therefore $f(k+1)$ is divisible by 64 if $f(k)$ is so.
This proves that the statement is true for $k+1$ if it is true for k.

By the principle of induction, the statement is true for all natural numbers n.

3. Use the principle of induction to prove that for all natural numbers n, $(a_1 a_2 \ldots a_{2^n})^{\frac{1}{2^n}} \leq \frac{a_1+a_2+\cdots+a_{2^n}}{2^n}$, where a_i's are positive real numbers

for $i = 1, 2, \ldots, 2^n$.

The statement is true for $n = 1$, since $(a_1 a_2)^{\frac{1}{2}} \leq \frac{a_1 + a_2}{2}$ ... (i)

Let us assume that the statement is true for $n = k$, where k is a natural number.

Then $(a_1 a_2 \ldots a_{2^k})^{\frac{1}{2^k}} \leq \frac{a_1 + a_2 + \cdots + a_{2^k}}{2^k} = p$, say.

Let $b_i = a_{2^k + i}$ for $i = 1, 2, \ldots, 2^k$.

Then $(b_1 b_2 \ldots b_{2^k})^{\frac{1}{2^k}} \leq \frac{b_1 + b_2 + \cdots + b_{2^k}}{2^k} = q$, say.

Now $\{(a_1 a_2 \ldots a_{2^k})^{\frac{1}{2^k}} (b_1 b_2 \ldots b_{2^k})^{\frac{1}{2^k}}\}^{\frac{1}{2}} = (pq)^{\frac{1}{2}}$

$$\leq \frac{p+q}{2} \quad \ldots \text{by (i)}$$

or, $(a_1 a_2 \ldots a_{2^{k+1}})^{\frac{1}{2^{k+1}}} \leq \frac{(a_1 + a_2 + \cdots + a_{2^k}) + (b_1 + b_2 + \cdots + b_{2^k})}{2^{k+1}}$

i.e., $(a_1 a_2 \ldots a_{2^{k+1}})^{\frac{1}{2^{k+1}}} \leq \frac{(a_1 + a_2 + \cdots + a_{2^{k+1}})}{2^{k+1}}$.

This shows that the statement is true for $n = k + 1$, if it be true for $n = k$.

By the principle of induction, the statement is true for all natural numbers n.

There is a variation of the principle of induction.

Let S be a non-empty subset of $\mathbb{N}$ such that

(i) $n_0 \in S$, and

(ii) if $k (\geq n_0) \in S$ then $k + 1 \in S$.

Then $S = \{n \in \mathbb{N} : n \geq n_0\}$.

We can utilise this principle to prove that if $P(n)$ be a statement involving a natural number n satisfying the following conditions-

'(i) $P(n_0)$ is true (n_0 being the least possible natural number), and (ii) for $k \geq n_0$, $P(k + 1)$ is true whenever $P(k)$ is true.

Then $P(n)$ is true for all $n \geq n_0$.

Worked Example (continued).

4. Prove that $n! > 2^n$ for all natural numbers $n \geq 4$.

Let $P(n)$ be the statement $n! > 2^n$.

The statements $P(1), P(2)$ and $P(3)$ are not true.

The statement $P(4)$ is true, since $4! > 2^4$.

Let us assume that $P(k)$ is true where k is a natural number ≥ 4. Then $k! > 2^k$.

Multiplying both sides by $k+1$, we have $(k+1)! > 2^k.(k+1) > 2^{k+1}$, since $k + 1 > 2$.

This shows that $P(k+1)$ is true whenever $P(k)$ is true.

Since the statement $P(n)$ is true for $n = 4$ (the least possible natural number), by the principle of induction the statement $P(n)$ is true for all natural numbers $n \geq 4$.

3.1.3. Second principle of induction.

Let S be a subset of $\mathbf{N}$ such that

(i) $1 \in S$, and

(ii) if $\{1, 2, \ldots, k\} \subset S$, then $k+1 \in S$.

Then $S = \mathbf{N}$.

Proof. Let $T = \mathbf{N} - S$. We prove that $T = \phi$. If not, T being a non-empty subset of $\mathbf{N}$ must have a least element, say m, by the well ordering property of $\mathbf{N}$.

Since $1 \in S, m \neq 1$. Therefore $m > 1$.

By the choice of m, all natural numbers less than m belongs to S. Hence $1, 2, \ldots, m-1 \in S$.

By (ii) $m \in S$, a contradiction.

This proves $T = \phi$ and therefore $S = \mathbf{N}$. □

Worked Example (continued).

5. Prove that for all $n \in \mathbf{N}$, $(2+\sqrt{3})^n + (2-\sqrt{3})^n$ is an even integer.

Let $P(n)$ be the statement $(2+\sqrt{3})^n + (2-\sqrt{3})^n$ is an even integer.

The statement $P(1)$ is true, since $(2+\sqrt{3})^1 + (2-\sqrt{3})^1 = 4$ and it is an even integer.

Let assume that $P(n)$ is true for $n = 1, 2, \ldots, k$.

$(2+\sqrt{3})^{k+1} + (2-\sqrt{3})^{k+1}$

$= a^{k+1} + b^{k+1}$, where $a = 2+\sqrt{3}, b = 2-\sqrt{3}$

$= (a^k + b^k)(a+b) - (a^{k-1} + b^{k-1})ab$

$= 4(a^k + b^k) - (a^{k-1} + b^{k-1})$.

This is an even integer, since $a^k + b^k$ and $a^{k-1} + b^{k-1}$ are even integers, by assumption.

This shows that $P(k+1)$ is true whenever $P(1), P(2), \ldots, P(k)$ are true.

By the second principle of induction, the statement $P(n)$ is true for all natural numbers n.

3.2. Integers.

The set of all integers, denoted by $\mathbb{Z}$, consists of whole numbers $0, \pm 1, \pm 2, \pm 3, \ldots$ ... The set of all positive integers (a proper subset of $\mathbb{Z}$) is identified with the set $\mathbb{N}$. We shall use the properties and principles of $\mathbb{N}$ in connection with the proof of any theorem about positive integers.

Theorem 3.2.1. Division algorithm.
Given integers a and b with $b > 0$, there exist unique integers q and r such that $a = bq + r$, where $0 \leq r < b$.

Proof. Let us consider the subset of integers

$$S = \{a - bx : x \in \mathbb{Z}, a - bx \geq 0\}.$$

First we show that S is non-empty.

Since $b \geq 1, \mid a \mid b \geq \mid a \mid$. Therefore $a + \mid a \mid b \geq a + \mid a \mid \geq 0$.

This shows that $a - b(-|a|) \in S$ and therefore S is non-empty.

Since S is a non-empty set of non-negative integers, either

(i) S contains 0 as its least element, or

(ii) S contains a smallest positive inetger as its least element by the well ordering property of the set $\mathbb{N}$.

In either case, we call it r. Therefore there exists an integer q such that $a - bq = r$, $r \geq 0$.

We assert that $r < b$. Because if $r \geq b$, then

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

This shows that $a - (q+1)b$ belongs to S and also $a - (q+1)b = r - b < r$. This leads to a contradiction to the fact that r is the least element in S.

Hence $r < b$ and consequently, $a = bq + r$ where $0 \leq r < b$.

In order to establish uniqueness of q and r, let us suppose that a has two representations: $a = bq + r$, $a = bq_1 + r_1$ where $0 \leq r < b$, $0 \leq r_1 < b$.

Then $b(q - q_1) = r_1 - r$ or, $b \mid q - q_1 \mid = \mid r_1 - r \mid$.

But $0 \leq r_1 < b$ and $-b < -r \leq 0$ yield $-b < r_1 - r < b$, i.e., $\mid r_1 - r \mid < b$. Consequently, $\mid q - q_1 \mid < 1$.

Since q and q_1 are integers, the only possibility is $q = q_1$ and therefore $r = r_1$. □

Definition. q is called the *quotient* and r is called the *remainder* in the division of a by b.

A more general version of the Division algorithm is obtained by taking b a non-zero integer.

Theorem 3.2.2. Given integers a and b, with $b \neq 0$, there exist unique integers q and r such that $a = bq + r$, $0 \leq r < |b|$

Proof. With the previous theorem already established, it is enough to consider the case in which b is negative. Then $|b| > 0$. By the previous theorem, there exist unique integers q_1 and r such that

$$\begin{aligned} a &= |b| q_1 + r, 0 \leq r < |b| \\ &= -bq_1 + r. \end{aligned}$$

Therefore $a = bq + r$ where $q = -q_1$. □

To illustrate the division algorithm, let us take $b = 3, a = -20, 2, 10$.

$$\begin{aligned} -20 &= 3.-7+1 \text{ gives} \quad q = -7, r = 1 \\ 2 &= 3.0+2 \text{ gives} \quad q = 0, r = 2 \\ 10 &= 3.3+1 \text{ gives} \quad q = 3, r = 1. \end{aligned}$$

Let us take $b = -3, a = -20, 2, 10$.

$$\begin{aligned} -20 &= -3.7+1 \text{ gives} \quad q = 7, r = 1 \\ 2 &= -3.0+2 \text{ gives} \quad q = 0, r = 2 \\ 10 &= -3.-3+1 \text{ gives} \quad q = -3, r = 1. \end{aligned}$$

When the remainder in the division algorithm turns out to be 0, the case is of special interest to us.

Definition. An integer a is said to be *divisible* by an integer $b \neq 0$ if there exists some integer c such that $a = bc$.

We express this in symbol $b \mid a$ and read "b divides a" We also express this by the statements "b is a divisor of a", "a is a multiple of b"

If b is a divisor of a, then $-b$ is also a divisor of a, because $a = bc \Rightarrow a = (-b)(-c)$. Thus divisors of an integer occur in pairs.

The following properties are immediate (assuming that a divisor is always a non-zero integer).

(i) $a \mid b$ and $b \mid c \Rightarrow a \mid c$,

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

Theorem 3.2.3. If $a \mid b$ and $a \mid c$ then $a \mid (bx + cy)$ for arbitrary integers x and y.

Proof. Since $a \mid b$, $b = ad$ for some integer d.
Since $a \mid c$, $c = ae$ for some integer e.

Therefore $bx + cy = adx + aey = a(dx + ey)$.
This shows that $a \mid bx + cy$ whatever integers x, y may be. □

Worked Examples.

1. Prove that the product of any m consecutive integers is divisible by m.

Let the consecutive integers be $c, c+1, c+2, \ldots, c+(m-1)$.
Let q be the quotient and r be the remainder when c is divided by m.

$$\text{Then } c = mq + r, \quad 0 \leq r < m.$$

When $r = 0$, $c = mq$ and therefore $m \mid c$;
when $r = 1$, $c + (m-1) = m(q+1)$ and therefore $m \mid c + (m-1)$:
when $r = 2$, $c + m - 2 = m(q+1)$ and therefore $m \mid c + (m-2)$;
... ...
when $r = m-1$, $c + 1 = m(q+1)$ and therefore $m \mid c + 1$.

Therefore whatever integer r may be, m divides one of the integers $c, c+1, \ldots, c+(m-1)$ and it follows that the product $c(c+1)(c+2)\ldots(c+m-1)$ is always divisible by m.

2. Use division algorithm to prove that the square of an odd integer is of the form $8k+1$, where k is an integer.

By division algorithm every integer, upon division by 4, leaves one of the remainders $0, 1, 2, 3$. Therefore any integer is one of the forms $4q, 4q+1, 4q+2, 4q+3$, where q is an integer.

Odd integers are of the forms $4q+1, 4q+3$.

$$\begin{aligned} \text{Now } (4q+1)^2 &= 8(2q^2+q)+1 \text{ is of the form } 8k+1, \\ (4q+3)^2 &= 8(2q^2+3q+1)+1 \text{ is of the form } 8k+1. \end{aligned}$$

Hence the square of an odd integer is of the form $8k+1$.

Definition. If a and b are integers then an integer d is said to be a *common divisor* of a and b if $d \mid a$ as well as $d \mid b$.

Since 1 is a divisor of every integer, 1 is a common divisor of a and b.

Therefore, for an arbitrary pair of integers a, b there exists always a common divisor.

If both of a and b be 0 then each integer is a common divisor of a and b. But if at least one of a and b is non-zero there is only a finite number of *positive* common divisors. Of these positive common divisors, there is a greatest one, called the greatest common divisor and is denoted by $gcd(a, b)$.

Definition. If a and b are integers, not both zero, the *greatest common divisor* of a and b, denoted by $gcd(a, b)$ is the *positive integer* d satisfying

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

(ii) if $c \mid a$ and $c \mid b$ then $c \mid d$.

For example, let $a = 12, b = -18$. Then the positive divisors of 12 are $1, 2, 3, 4, 6, 12$ and those of -18 are $1, 2, 3, 6, 9, 18$.

Therefore the positive common divisors are $1, 2, 3, 6$ and $gcd(12, -18) = 6$.

Similarly $gcd(15, 8) = 1$, $gcd(20, -50) = 10$, $gcd(0, 5) = 5$.

Note. It follows from the definition that $gcd(a, -b) = gcd(-a, b) = gcd(-a, -b) = gcd(a, b)$, where a, b are integers, not both zero.

Theorem 3.2.4. If a and b are integers, not both zero, then there exist integers u and v such that $gcd(a, b) = au + bv$.

Proof. Let $S = \{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0\}$. First we show that S is a non-empty set.

Since at least one of a, b is non-zero, let $a \neq 0$. Then $| a | > 0$.

Therefore $| a | = a.x + b.0$ is an element of S, where we choose $x = 1$ if $a > 0$ and $x = -1$ if $a < 0$.

Since S is a non-empty set of positive integers, by the well ordering property of the set $\mathbb{N}$, S contains a least element, say d.

Then $d = au + bv$ for some integers u, v.

By division algorithm, $a = dq + r$ where q and r are integers with $0 \leq r < d$.

$$\begin{aligned} \text{Therefore } r &= a - dq \\ &= a - (au + bv)q \\ &= a(1 - uq) + b(-vq). \end{aligned}$$

This representation shows that if $r > 0$ then $r \in S$.

But d is the least element in S and since $r < d$, $r \notin S$.

Consequently, $r = 0$.

This proves that $a = dq$, i.e., d is a divisor of a.

By similar arguments we can prove that d is a divisor of b.

Therefore d becomes a common divisor of a and b.

To prove that d is the $gcd(a, b)$, let us assume that c is a common divisor of a and b.

Then $c \mid a$ and $c \mid b$ and therefore $c \mid au + bv$, by Theorem 3.2.3 i.e., $c \mid d$ and this proves that d is the greatest common divisor. □

For example,

$gcd(-4, 20) = 4$ and $4 = -4.(-1) + 20.0$
$gcd(55, 35) = 5$ and $5 = 55.2 + 35.(-3)$
$gcd(0, 9) = 9$ and $9 = 0.0 + 9.1$
$gcd(-9, 13) = 1$ and $1 = -9.(-3) + 13. - 2.$

Note 1. The $gcd(a, b)$ is the *least positive* value of $ax + by$ where x, y are integers.

But x and y are not uniquely determined integers for which the integer $ax + by$ is least positive. Because if $d = au + bv$, where u and v are integers then d can also be expressed as $d = a(u + kb) + b(v - ka)$ where k is an integer.

For example, let $a = 15, b = 24$. Then $d = 3$. d can be expressed as $d = 15(-3) + 24.2$, or as $d = 15.(-3 + 24k) + 24(2 - 15k)$ for any integer k.

Note 2. Guaranteed by the theorem it is always possible to express $gcd(a, b)$ as a linear combination of a and b. But the theorem gives no clue how to express $gcd(a, b)$ in the desired form $au + bv$, i.e., how to determine u and v. This will be discussed in a subsequent article.

Worked Example (continued.)

3. Show that $gcd(a, a + 2) = 1$ or 2 for every integer a.

Let $d = gcd(a, a + 2)$. Then $d \mid a$ and $d \mid a + 2$.

Therefore $d \mid ax + (a + 2)y$ for all integers x, y.

Taking $x = -1$ and $y = 1$, it follows that $d \mid 2$. i.e., d is either 1 or 2.

Theorem 3.2.5. If k be a positive integer, $gcd(ka, kb) = k.gcd(a, b)$.

Proof. Let $d = gcd(a, b)$. Then there exist integers u and v such that $d = au + bv$.

Since $d = gcd(a, b)$, $d \mid a$ and $d \mid b$.

$d \mid a \Rightarrow kd \mid ka, d \mid b \Rightarrow kd \mid kb$.

Therefore kd is a common divisor of ka and kb.

Let c be a common divisor of ka and kb.

$c \mid ka \Rightarrow ka = pc$ for some integer p and $c \mid kb \Rightarrow kb = qc$ for some integer q.

Now $kd = k(au + bv) = pcu + qcv = (pu + qv)c$.

As $pu + qv$ is an integer, it follows that $c \mid kd$.

Consequently, $kd = gcd(ka, kb)$, i.e., $gcd(ka, kb) = k.gcd(a, b)$. □

Definition. Two integers a and b, not both zero, are said to be *prime to each other* (*or relatively prime*) if $gcd(a, b) = 1$.

Theorem 3.2.6. Let a and b be integers, not both zero. Then a and b are prime to each other if and only if there exist integers u and v such that $1 = au + bv$.

Proof. Let a and b be prime to each other. Then $gcd(a, b) = 1$. Therefore there exist integers u and v such that $1 = au + bv$.

Conversely, let us suppose that there are integers u and v such that $1 = au + bv$ and let $d = gcd(a, b)$.

Since $d \mid a$ and $d \mid b$ then $d \mid ax + by$ for all integers x and y.

Hence $d \mid 1$ and this implies $d = 1$, since d is a positive integer. □

Theorem 3.2.7. If $d = gcd(a, b)$, then $\frac{a}{d}$ and $\frac{b}{d}$ are integers prime to each other.

Proof. Since $d \mid a$, there exists an integer m such that $md = a$.

Since $d \mid b$, there exists an integer n such that $nd = b$.

As $\frac{a}{d} = m$ and $\frac{b}{d} = n$, $\frac{a}{d}$ and $\frac{b}{d}$ are integers.

Since $d = gcd(a, b)$, it is possible to find integers u and v such that $d = au + bv$.

$$\text{Therefore } 1 = \left(\frac{a}{d}\right)u + \left(\frac{b}{d}\right)v.$$

This form of representation shows that $\frac{a}{d}$ and $\frac{b}{d}$ are integers prime to each other. □

Theorem 3.2.8. If $a \mid bc$ and $gcd(a, b) = 1$, then $a \mid c$.

Proof. Since $gcd(a, b) = 1$, there exist integers u and v such that $1 = au + bv$. Therefore $c = acu + bcv$.

Since $a \mid ac$ and $a \mid bc$, it follows that $a \mid \{(ac)u + (bc)v\}$ which means $a \mid c$. □

Corollary. If $ap = bq$ and a is prime to b then $a \mid q$ and $b \mid p$.

Theorem 3.2.9. If $a \mid c$ and $b \mid c$ with $gcd(a, b) = 1$, then $ab \mid c$.

Proof. Since $a \mid c$ and $b \mid c$, there exist integers m and n such that $c = am = bn$.

Since $gcd(a, b) = 1$, there exist integers u, v such that $1 = au + vb$.

Therefore $c = (au)c + (bv)c$

$= ab(un + vm) \Rightarrow ab \mid c$. □

Note. Without the condition $gcd(a, b) = 1$, $a \mid c$ and $b \mid c$ together may not imply $ab \mid c$.

For example, $4 \mid 12$ and $6 \mid 12$ do not imply $4.6 \mid 12$.

Theorem 3.2.10. If a is prime to b and a is prime to c then a is prime to bc.

Proof. Since a is prime to b, $au + bv = 1$ for some integers u, v ... (i)
Since a is prime to c, $am + cn = 1$ for some integers m, n ... (ii)
From (i) $acun + bcvn = cn = 1 - am$ by (ii).
or, $a(m + cun) + bc(vn) = 1$.
Since $m + cun$ and vn are integers, it follows that a is prime to bc.

Worked Examples (continued).

4. If a is prime to b, prove that $a + b$ is to prime to ab.

Since a is prime to b, there exist integers u and v such that $au + bv = 1$. This can be expressed as $a(u - v) + (a + b)v = 1$.
Since $u - v$ and v are integers, it follows that a is prime to $a + b$.

Again, $au + bv = 1$ can be expressed as $(a + b)u + b(v - u) = 1$.
Since $v - u$ and u are integers, it follows that $a + b$ is prime to b.
By Theorem 3.2.10, $a + b$ is prime to ab.

5. If a is prime to b, prove that

(i) a^2 is prime to b,

(ii) a^2 is prime to b^2.

(i) Since a is prime to b, there exist integers u and v such that $au + bv = 1$. Then $au = 1 - bv$
or, $a^2u^2 = 1 - 2bv + b^2v^2$
or, $a^2u^2 + b(2v - bv^2) = 1$.
Since u^2 and $2v - bv^2$ are integers, it follows that a^2 is prime to b.

(ii) Since a^2 is prime to b, there exist integers m and n such that $a^2m + bn = 1$. Then $bn = 1 - a^2m$
or, $b^2n^2 = 1 - 2a^2m + a^4m^2$
or, $a^2(2m - a^2m^2) + b^2n^2 = 1$.
Since n^2 and $2m - a^2m^2$ are integers, it follows that a^2 is prime to b^2.

6. If $d = gcd(a, b)$, show that $gcd(a^2, b^2) = d^2$.

Since $d = gcd(a, b)$, $a = dp$ and $b = dq$, where p, q are integers prime to each other.

Therefore $a^2 = d^2p^2, b^2 = d^2q^2$ and this shows that d^2 is a common divisor of a^2 and b^2.

Let $gcd(a^2, b^2) = d^2u$, where u is a positive integer. Then $d^2u | d^2p^2$ and $d^2u | d^2q^2$ and therefore $u | p^2$ and $u | q^2$.

But $gcd(p, q) = 1 \Rightarrow gcd(p^2, q^2) = 1$.

Since u is a common divisor of p^2 and q^2 and $gcd(p^2, q^2) = 1$, it follows that $u = 1$. Hence $gcd(a^2, b^2) = d^2$.

7. If $gcd(a, b) = 1$, show that $gcd(a + b, a^2 - ab + b^2) = 1$ or 3.

Let $d = gcd(a+b, a^2 - ab+b^2)$. Then $d \mid a+b$ and $d \mid (a^2 - ab+b^2)$. This implies $d \mid (a + b)(a + b) - (a^2 - ab + b^2)$, i.e., $d \mid 3ab$.

Therefore $d \mid a + b$ and $d \mid 3ab$. Since $gcd(a, b) = 1$, it follows that $gcd(a + b, ab) = 1$. Since $d \mid a + b$ and $gcd(a + b, ab) = 1$, we prove that $gcd(d, ab) = 1$.

There exist integers u and v such that $u(a + b) + v(ab) = 1$. Since $d \mid a + b$, $a + b = dp$ for some integer p. Therefore $(up)d + v(ab) = 1$ and this shows that d is prime to ab.

$d \mid 3ab$ and d is prime to ab implies $d \mid 3$. Therefore $d = 1$ or $d = 3$.

8. Prove that the product of any three consecutive integers is divisible by 6.

By division algorithm, any integer, upon division by 3, leaves one of the remainders $0, 1, 2$. Therefore any integer n is one of the forms $3k, 3k + 1, 3k + 2$.

When $n = 3k$, n is divisible by 3.
When $n = 3k + 1$, $n + 2$ is divisible by 3.
When $n = 3k + 2$, $n + 1$ is divisible by 3.

It follows that for any integer $n, n(n + 1)(n + 2)$ is divisible by 3.

Again, the product of two consecutive integers is divisible by 2.
Therefore $2 \mid n(n + 1)(n + 2)$ and $3 \mid n(n + 1)(n + 2)$.
Since $gcd(2, 3) = 1$, it follows that $2.3 \mid n(n + 1)(n + 2)$, i.e., $6 \mid n(n + 1)(n + 2)$.

3.2.11. Euclidean algorithm.

Euclidean algorithm is an efficient method of finding the greatest common divisor of two given integers. The method involves repeated application of the division algorithm.

Let a and b be two integers whose g.c.d. is required.

Since $gcd(a, b) = gcd(|a|, |b|)$, it is enough to assume that a and b are positive integers. Without loss of generality, we assume $a > b > 0$.

By division algorithm, $a = bq_1 + r_1$ where $0 \leq r_1 < b$.
If it happens that $r_1 = 0$, then $b \mid a$ and $gcd(a, b) = b$.
If $r_1 \neq 0$, then by division algorithm, $b = r_1q_2 + r_2$ where $0 \leq r_2 < r_1$.

If $r_2 = 0$, the process stops.If $r_2 \neq 0$, by division algorithm
$r = r_2q_3 + r_3$ where $0 \leq r_3 < r_2$.

The process continues until some zero remainder appears. This must happen because the remainders $r_1, r_2, r_3, \ldots$ form a decreasing sequence of integers and since $r_1 < b$, the sequence contains at most b non-negative integers.

Let us assume that $r_{n+1} = 0$ and r_n is the last non-zero remainder.

We have the following relations

$$\begin{aligned}
a &= bq_1 + r_1 && 0 < r_1 < b \\
b &= r_1q_2 + r_2 && 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3 && 0 < r_3 < r_2 \\
&\ldots \quad \ldots && \ldots \quad \ldots \\
r_{n-2} &= r_{n-1}q_n + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1} + 0.
\end{aligned}$$

We assert that r_n is the $gcd(a, b)$. First of all we prove the lemma- If $a = bq + r$, then $gcd(a, b) = gcd(b, r)$.

Proof. Let $d = gcd(a, b)$. Then $d \mid a$ and $d \mid b$.

This implies $d \mid a - bq$, i.e., $d \mid r$. This shows that d is a common divisor of b and r.

Let c be a common divisor of b and r. Then $c \mid bq + r$, i.e., $c \mid a$.

This shows that c is a common divisor of a and b.

Since $d = gcd(a, b)$, it follows from the property of the g.c.d. that $c \mid d$ and this gives $d = gcd(b, r)$.

We utilise the lemma to show that $r_n = gcd(a, b)$.

$r_n = gcd(0, r_n) = gcd(r_{n-1}, r_n) = gcd(r_{n-2}, r_{n-1}) = \quad \cdots \quad \cdots =$ $gcd(b, r_1) = gcd(a, b)$.

Also we have $r_n = r_{n-2} - r_{n-1}q_n$

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

r_n is expressed as a linear combination of r_{n-2} and r_{n-3}. Proceeding backwards we can express r_n as a linear combination of a and b.

Worked Examples (continued).

9. Calculate $gcd(567, 315)$ and express $gcd(567, 315)$ as $567u + 315v$, where u, v are integers.

By division algorithm,

$\frac{567}{315} = 1 + \frac{252}{315}$, $\quad \frac{315}{252} = 1 + \frac{63}{252}$, $\quad \frac{252}{63} = 4$.

Then $567 = 315.1 + 252$, $315 = 252.1 + 63$, $252 = 63.4 + 0$.
The last non-zero remainder is 63. Therefore $gcd(567, 315) = 63$.

$$\begin{aligned} \text{We have } 63 &= 315 - 252.1 \\ &= 315 - (567 - 315) \\ &= 567.(-1) + 315.2 \\ &= 567u + 315v, \text{ where } u = -1, v = 2. \end{aligned}$$

10. Find two integers u and v satisfying $63u + 55v = 1$.

63 and 55 are integers prime to each other and therefore there exist integers u, v such that $63u + 55v = 1$.

By division algorithm,

$63 = 55.1 + 8$, $55 = 8.6 + 7$, $8 = 7.1 + 1$.

We have $1 = 8 - 7 = 8 - (55 - 8.6) = 8.7 - 55$

$= (63 - 55).7 - 55 = 63.7 + 55.(-8)$.

Therefore $u = 7, v = -8$.

11. Find two integers u and v satisfying $54u + 24v = 30$.

Let us find the $gcd(54, 24)$.

By division algorithm, $54 = 24.2 + 6$, $24 = 6.4 + 0$.

Therefore $gcd(54, 24) = 6$.

Now $6 = 54 - 24.2 = 54.1 + 24.(-2)$.

Consequently, $30 = 54.5 + 24.(-10)$. Therefore $u = 5, v = 10$.

The Diophantine equation.

An equation in one or more unknowns which is to be solved in integers is said to be a Diophantine equation, named after the Greek mathematician Diophantus, who initiated the study of such problems.

A given linear Diophantine equation of the form $ax + by = c$ may have many solutions in integers or may not have even a single solution.

For example, the equation $2x+4y = 6$ has many solutions in integers, since $2.1 + 4.1 = 6$, $2.5 + 4.(-1) = 6$, $2.9 + 4.(-3) = 6$,...

Whereas, the equation $2x+4y = 3$ cannot have a solution in integers, since the left hand side is always an even integer for every pair of integers x, y, while the right hand side is odd.

First of all, we discuss the condition for solvability of the linear equation $ax + by = c$ in integers, where a, b, c are integers and a, b are not both zero.

Theorem 3.2.15. If a, b, c are integers and a, b are not both zero, the equation $ax + by = c$ has an integral solution if and only if d is a divisor of c, where $d = gcd(a, b)$. If (x_0, y_0) be any particular solution of the equation, then all integral solutions are given by $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$ for different integers t.

Proof. Let (x_1, y_1) be an integral solution of the equation $ax + by = c$.
Then $ax_1 + by_1 = c$, where x_1, y_1 are integers.
Let $gcd(a, b) = d$. Then $d \mid a$ and $d \mid b$.
This implies $d \mid ax_1 + by_1$, i.e., $d \mid c$.

Conversely, let $gcd(a, b)$ be a divisor of c.
Let $gcd(a, b) = d$. Then $d = au + bv$ for some integers u, v.
Let $c = dp$ where p is an integer.

Then $c = (au + bv)p = a(up) + b(vp)$.

This shows that (up, vp) is a solution of the equation $ax + by = c$. Clearly, up and vp are integers. So the equation $ax + by = c$ has an

integral solution.

To prove the second part, let (x', y') be any other solution. Then $ax_0 + by_0 = c = ax' + by'$, which gives $a(x' - x_0) = b(y_0 - y')$.

Since $d = gcd(a, b)$, there exist relatively prime integers p, q such that $a = dp$ and $b = dq$. Therefore we have $p(x' - x_0) = q(y_0 - y')$.

This shows that $p \mid q(y_0 - y')$ with $gcd(p, q) = 1$ and therefore $p \mid (y_0 - y')$. Therefore $y_0 - y' = pt$ for some integer t. Also we have $x' - x_0 = qt$.

This gives $x' = x_0 + qt = x_0 + \frac{b}{d}t$, $y' = y_0 - pt = y_0 - \frac{a}{d}t$.

Thus there are infinite number of solutions, one for each integral value of t.

Note. In particular, if a and b are prime to each other then all integral solutions of the equation are given by

$$x = x_0 + bt, y = y_0 - at \text{ for all integral values of } t.$$

3.2.16. Integral solution of the equation $ax + by = c$ where a, b, c are positive integers and $gcd(a, b) = 1$.

Since $gcd(a, b) = 1$, there exist integers u and v such that $au + bv = 1$.

Therefore $ax + by = c(au + bv)$

or, $a(x - cu) = -b(y - cv)$.

Since a and b are prime to each other, $x - cu$ is divisible by b and $y - cv$ is divisible by a and therefore

$\frac{x-cu}{-b} = \frac{y-cv}{a} = t$, where t is an integer

or, $x = cu - bt$

$y = cv + at$, where $t = 0, \pm 1, \pm 2, \cdots$

This is the general solution in integers.

Note. For positive integral solution, we must have $cu - bt > 0$ and $cv + at > 0$ simultaneously. Hence $\frac{-cv}{a} < t < \frac{cu}{b}$.

If $\frac{cu}{b} = m + f$ where m is an integer and $0 < f \leq 1$, then $t \leq m$.

If $\frac{-cv}{a} = n + f'$ where n is an integer and $0 \leq f' < 1$, then $t > n$.

The total number of solutions in positive integers is $m - n$.

3.2.17. Integral solution of the equation $ax - by = c$ where a, b, c are positive integers and $gcd(a, b) = 1$.

Since $gcd(a, b) = 1$, there exist integers u and v such that $au + bv = 1$.

Therefore $ax - by = c(au + bv)$

or, $a(x - cu) = b(y + cv)$.

Since a and b are prime to each other, $x - cu$ is divisible by b and $y + cv$ is divisible by a and therefore

$\frac{x-cu}{b} = \frac{y+cv}{a} = t$, where t is an integer

or, $x = cu + bt$

$y = -cv + at$, where $t = 0, \pm 1, \pm 2, \cdots$

This is the general solution in integers.

Note. For a positive integral solution, we must have $cu + bt > 0$ and $-cv + at > 0$ simultaneously. Hence $t > \frac{-cu}{b}$ and $t > \frac{cv}{a}$.

Let the integral part of max $\left\{\frac{-cu}{b}, \frac{cv}{a}\right\}$ be m. Then the solutions in positive integers correspond to $t = m+1, m+2, \ldots$ Clearly, the number of positive integral solutions is infinite.

Worked Examples (continued).

11. Find the general solution in integers of the equation $7x + 11y = 1$.

Since 7 and 11 are prime to each other, there exist integers u and v such that $7u + 11v = 1$. Here $u = 8, v = -5$.

Then $7x + 11y = 7.8 - 11.5$

or, $7(x - 8) = -11(y + 5)$.

Since 7 and 11 are prime to each other, $x - 8$ is divisible by 11 and $y + 5$ is divisible by 7 and therefore

$\frac{x-8}{-11} = \frac{y+5}{7} = t$, where t is an integer

or, $x = 8 - 11t$

$y = -5 + 7t$, where $t = 0, \pm 1, \pm 2, \cdots$

This is the general solution in integers.

Note. For a positive integral solution, we must have $8 - 11t > 0$ and $-5 + 7t > 0$ simultaneously. Hence $\frac{5}{7} < t < \frac{8}{11}$.

No such integer t exists. Hence there is no solution of the equation in positive integers.

12. Find the general solution in integers of the equation $5x + 12y = 80$. Examine if there is a solution in positive integers.

Since 5 and 12 are prime to each other, there exist integers u and v such that $5u + 12v = 1$. Here $u = 5, v = -2$.

Then $5x + 12y = 80(5.5 - 12.2)$

or, $5(x - 400) = -12(y + 160)$.

Since 5 and 12 are prime to each other, $x - 400$ is divisible by 12 and $y + 160$ is divisible by 5 and therefore

$\frac{x-400}{-12} = \frac{y+160}{5} = t$, where t is an integer

or, $x = 400 - 12t$
$y = 5t - 160$, where $t = 0, \pm 1, \pm 2, \cdots$

This is the general solution in integers.

For a positive integral solution, we must have $400 - 2t > 0$ and $5t - 160 > 0$ simultaneously. Hence $32 < t < \frac{100}{3}$.

The only solution in positive integers corresponds to $t = 33$ and the solution is $x = 4, y = 5$.

13. Find the general solution in positive integers of the equation $12x - 7y = 8$.

Since 12 and 7 are prime to each other, there exist integers u and v such that $12u + 7v = 1$. Here $u = 3, v = -5$.

Then $12x - 7y = 8(12.3 - 7.5)$

or, $12(x - 24) = 7(y - 40)$.

Since 12 and 7 are prime to each other, $x - 24$ is divisible by 7 and $y - 40$ is divisible by 12 and therefore

$\frac{x-24}{7} = \frac{y-40}{12} = t$, where t is an integer

or, $x = 7t + 24$
$y = 12t + 40$, where $t = 0, \pm 1, \pm 2, \cdots$

This is the general solution in integers.

For a solution in positive integers we must have $7t + 24 > 0$ and $12t + 40 > 0$. Hence $t > \frac{-24}{7}$ and $t > \frac{-10}{3}$.

The least integral value of t is -3. Hence the general solution in positive integers is given by $x = 7t + 24$
$y = 12t + 40$, where t is an integer ≥ -3.

Note. The solution corresponding to $t = -3$ is given by $x = 3, y = 4$. The general solution in positive integers can be expressed as
$x = 7t + 3 \quad y = 12t + 4$, where t is an integer ≥ 0.

3.3. Prime numbers.

An integer $p > 1$ is said to be a *prime number*, or simply a *prime*, if its only positive divisors are 1 and p.

An integer > 1 which is not a prime is said to be a *composite* number.

The integers $2, 3, 5, 7, 11, \ldots$ are prime numbers, while the integers $4, 6, 8, 9, \ldots$ are composite numbers.

The integer 1 is regarded as neither prime nor composite.

2 is the only even prime number. All other prime numbers are necessarily odd.

Theorem 3.3.1. If p be a prime number and $1 \leq a < p$ then p is prime to a.

Proof. Let $d = gcd(a, p)$. Then $d \mid a$ and $d \mid p$.

Since p is a prime and $d \mid p$, either $d = p$ or $d = 1$.

But since $a < p$ and $d \mid a$, d cannot be p. Therefore $d = 1$ and p is prime to a. □

Theorem 3.3.2. If p be a prime number and a is an integer $> p$ such that p is not a divisor of a, then p is prime to a.

Proof. Let $d = gcd(a, p)$. Then $d \mid a$ and $d \mid p$.

Since p is a prime and $d \mid p$, either $d = p$ or $d = 1$.

But $d \neq p$ since p is not a divisor of a. Therefore $d = 1$ and p is prime to a. □

Theorem 3.3.3. If p be a prime number and a is an integer $> p$ such that p is a divisor of a, then $gcd(a, p) = p$.

Proof. Since p is a divisor of a, $a = pk$ where k is an integer.

Hence $gcd(a, p) = gcd(pk, p) = p.gcd(k, 1) = p$. □

Theorem 3.3.4. If p be a prime number and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof. If $p \mid a$ then the theorem is done.

If p is not a divisor of a then $gcd(a, p) = 1$, since 1 and p are the only divisors of p.

Since $gcd(a, p) = 1$, there exist integers u and v such that $au + pv = 1$. Then $abu + pbv = b$.

Now $p \mid ab$ and $p \mid pb \Rightarrow p \mid (ab)u + (pb)v$, since u and v are integers. That is, $p \mid b$.

This completes the proof.

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

Proof. If $p \mid a_1$ we need not go further. If p is not a divisor of a_1 then by the theorem, $p \mid a_2 a_3 \ldots a_n$.

If p is not a divisor of a_2 then $p \mid a_3 a_4 \ldots a_n$. Proceeding in a similar manner, in a finite number of steps we arrive at the desired result.

Theorem 3.3.5. A composite number has at least one prime divisor.

Proof. Let n be a composite number. Since n is not a prime, it has a positive divisor other than 1 and n.

Let S be the set of those positive divisors of n which are different from 1 and n. Then S is non-empty. By the well ordering property of the set $\mathbf{N}$, S contains a least element, say d. Then $1 < d < n$.

We prove that d is a prime. if d be not a prime then d has a divisor d' other than d and 1; and $1 < d' < d < n$. But $d' \mid d$ and $d \mid n \Rightarrow d' \mid n$. Therefore $d' \in S$ and this contradicts that d is the least element of S.

Therefore d is a prime and the theorem is done. □

Worked Examples.

1. Prove that for $n > 3$, the integers n, $n+2$, $n+4$ cannot be all primes.

Any integer n is one of the forms $3k$, $3k+1$, $3k+2$, where k is an integer.

If $n = 3k$, then n is not a prime.

If $n = 3k+1$, then $n+2 = 3(k+3)$ and it is not a prime.

If $n = 3k+2$, then $n+4 = 3(k+2)$ and it is not a prime.

Thus in any case. the integers n, $n+2$, $n+4$ are not all primes.

2. If $p \geq q \geq 5$ and p, q are both primes, prove that $24 \mid p^2 - q^2$.

Since p and q are primes > 3, p and q are of the form $3k+1$ or $3k+2$, where k is an integer.

If both p and q are either of the forms $3k+1$ or $3k+2$, then $3 \mid p-q$.

If one of p and q is of the form $3k+1$ and the other is of the form $3k+2$, them $3 \mid p+q$.

Thus in any case, $3 \mid p^2 - q^2$.

Since p and q are odd primes, p and q are of the form $4k+1$ or $4k+3$, where k is an integer.

If both p and q are of the form $4k+1$, then $2 \mid p+q$ and $4 \mid p-q$.

If both p and q are of the form $4k+3$, then $2 \mid p+q$ and $4 \mid p-q$.

If one of p and q is of the form $4k+1$ and the other is of the form $4k+3$, then $4 \mid p+q$ and $2 \mid p-q$..

Thus in any case, $8 \mid p^2 - q^2$.

Since 3 and 8 are prime to each other, $24 \mid p^2 - q^2$.

3. If p and p^2+8 are both prime numbers, prove that $p = 3$.

Any integer p is one of the forms $3k$, $3k+1$, $3k+2$, where k is an integer.

If $p = 3k+1$, then $p^2+8 = 3(3k^2+2k+3)$. Since p^2+8 is a prime, $3k^2+2k+3$ must be 1 for some integer k and in that case p^2+8 must be 3.

But for no integer k, $3k^2+2k+3$ can be 1 and for no integer k, p^2+8 can be 3. Therefore $p = 3k+1$ is an impossibility.

If $p = 3k + 2$, then $p^2 + 8 = 3(3k^2 + 4k + 4)$. Since $p^2 + 8$ is a prime, $3k^2 + 4k + 4$ must be 1 for some integer k and in that case $p^2 + 8$ must be 3.

By similar arguments, $p = 3k + 2$ is an impossibility.

Therefore $p = 3k$, where k is an integer. Since p is a prime, k must be 1 and therefore $p = 3$.

4. If $2^n - 1$ be a prime, prove that n is a prime.

Let n be composite. Then $n = p.q$ where p and q are integers each greater than 1.

$2^n - 1 = 2^{pq} - 1 = (2^p - 1)(2^{p(q-1)} + 2^{p(q-2)} + \cdots + 2^p + 1)$.

Each factor on the right is evidently greater than 1 and therefore $2^n - 1$ is composite.

Contrapositively, $2^n - 1$ is a prime implies n is a prime.

5. Prove that $n^4 + 4^n$ is a composite number for all natural numbers $n > 1$.

Case 1. Let n be even.

Then $n^4 + 4^n$ is divisible by 4 and so it is a composite number.

Case 2. Let n be odd and $n = 2k + 1$, where k is a natural number.

Then $n^4 + 4^n = n^4 + 4.4^{2k} = n^4 + 4a^4$, where $a = 2^k$

$$= (n^2+2a^2)^2-(2an)^2 = (n^2+2an+2a^2)(n^2-2an+2a^2)$$

$(n^2+2an+2a^2) = (n+a)^2+a^2$ and $(n^2-2an+2a^2) = (n-a)^2+a^2$.

Each is a positive integer greater than 1, since a is a positive integer > 1. Consequently, $n^4 + 4^n$ is a composite number when n is odd.

Hence $n^4 + 4^n$ is a composite number for all $n > 1$.

6. Let p be a prime and a be a positive integer. Prove that a^n is divisible by p if and only if a is divisible by p.

Let a be divisible by p. Then $a = pk$ for some integer k.

$a^n = p^n k^n = p(p^{n-1}k^n) = pm$, where m is an integer.

This shows that a^n is divisible by p... ... (i)

Let a be not divisible by p. Since p is a prime, $gcd(a,p) = 1$. Therefore there exist integers u and v such that $au + pv = 1$.

Then $a^n u^n = (1 - pv)^n = 1 - ps$ where s is an integer

or, $a^n r + ps = 1$ where r, s are integers.

This shows that $gcd(a^n, p) = 1$ and therefore a^n is not divisible by p. Hence a is not divisible by $p \Rightarrow a^n$ is not divisible by p.

Contrapositively, $p \mid a^n \Rightarrow p \mid a$... (ii)

From (i) and (ii) the desired result is obtained.

Theorem 3.3.6. (Fundamental theorem of Arithmetic)

Any positive integer is either 1, or a prime, or it can be expreesed as a product of primes, the representation being unique except for the order of the prime factors.

Proof. Let n be a positive integer. Either $n = 1$ or $n > 1$. Let $P(n)$ be the statement that $n(> 1)$ is either a prime, or it can be expressed as a product of primes.

$P(2)$ is true, since 2 is a prime.

Let us assume that $P(n)$ is true for all n, where n is a positive integer such that $2 \leq n \leq k$.

If $k+1$ be itself a prime then $P(k+1)$ is true and by the second principle of induction, $P(n)$ is true for all positive integers $n > 1$.

If $k+1$ be not a prime then it is a composite number. Let $k+1 = rs$ where r, s are integers with $2 \leq r < k+1, 2 \leq s < k+1$.

By induction hypothesis, $P(r)$ and $P(s)$ are both true. Then

$r = p_1 p_2 \dots p_i$ where $p_1, p_2, \dots, p_i$ are primes, $i \geq 1$;

$s = q_1 q_2 \dots q_j$ where $q_1, q_2, \dots, q_j$ are primes, $j \geq 1$.

Thus $k+1$ is expressed as the product of primes and $P(k+1)$ is proved to be true. By the second principle of induction $p(n)$ is true for all positive integers $n > 1$.

Hence the first part of the theorem is established.

In order to prove uniqueness of the representation, let us assume that $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_m$, where p_i and q_i are all primes.

Since $p_1 \mid n$, it follows that $p_1 \mid q_1 q_2 \dots q_m$.

Since p_1 is a prime, $p_1 \mid q_r$ for some r where $1 \leq r \leq m$. But since p_1 and q_r are both primes, $p_1 = q_r$.

We obtain $p_2 p_3 \dots p_k = q_1 q_2 \dots q_{r-1} q_{r+1} \dots q_m$.

We repeat the argument with p_2 and obtain $p_2 = q_s$ for some s where $1 \leq s \leq m, s \neq r$. Then

$$p_3 p_4 \dots p_k = q_1 q_2 \dots q_{r-1} q_{r+1} \dots q_{s-1} q_{s+1} \dots q_m.$$

If $k < m$, then after k steps the left hand side reduces to 1 and the right hand side becomes the product of $m - k$ q's, each of which is a prime. This cannot happen. Therefore $k \geq m$.

If $k > m$, then after m steps the right hand side reduces to 1 and the left hand side becomes the product of $k - m$ p's, each of which is a prime. This cannot happen. Therefore $k \leq m$.

Hence $k = m$ and the products $p_1 p_2 \dots p_m, q_1 q_2 \dots q_k$ give the same representation except for the order of the factors.

Thus $n(> 1)$ is expressed as the product of a number of primes, the representation being unique except for the order of the factors. □

3.3.9. The number of positive divisors of a positive integer.

Let n be a positive integer greater than 1. Then n can be expressed as $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where the primes p_i are distinct with $p_1 < p_2 < \cdots < p_r$ and the exponents α_i are all positive.

If m be a positive divisor of n then m is of the form $p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}$, where $0 \le u_1 \le \alpha_1, 0 \le u_2 \le \alpha_2, \dots, 0 \le u_r \le \alpha_r$.

Thus the positive divisors of n are in one-to-one correspondence with the totality of r-tuples $(u_1, u_2, \dots, u_r)$, where $0 \le u_1 \le \alpha_1, 0 \le u_2 \le \alpha_2, \dots, 0 \le u_r \le \alpha_r$.

The number of such r-tuples is $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$.

Hence the total number of positive divisors of n is $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$.

If $n = 1$, then there is only one positive divisor.

Note. The total number of positive divisors $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$ include both the divisors 1 and n.

Definition. The number of positive divisors of a positive integer n is denoted by $\tau(n)$. (*tau n*)

If the canonical form of a positive integer $n(> 1)$ be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

then $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$; and $\tau(1) = 1$.

For example, $\tau(48) = \tau(2^4 3) = (4 + 1)(1 + 1) = 10$.

Theorem 3.3.10. The total number of positive divisors of a positive integer n is odd if and only if n is a perfect square.

Proof. Let $n(> 1)$ be a perfect square and let the canonical form of n be $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where $p_1 < p_2 < \cdots < p_r$ and α_i are all positive.

Then each of $\alpha_1, \alpha_2, \dots, \alpha_r$ is an even integer and $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$ is odd.

If however, $n = 1$, a perfect square, then $\tau(n) = 1$ and it is odd.

Conversely, let $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$ be odd. Then each of the factors $\alpha_1 + 1, \alpha_2 + 1, \dots, \alpha_r + 1$ must be odd. Consequently, each of $\alpha_1, \alpha_2, \dots, \alpha_r$ must be even and n is therefore a perfect square.

This completes the proof.

3.3.11. The sum of all positive divisors of a positive integer.

Let n be a positive integer greater than 1. Then n can be expressed as $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where the primes p_i are distinct with $p_1 < p_2 < \dots < p_r$ and $\alpha_i > 0$.

Every positive divisor of n is a term in the product

$$(1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1})(1 + p_2 + \dots + p_2^{\alpha_2}) \dots (1 + p_r + \dots + p_r^{\alpha_r})$$

and conversely, each term in the product is a divisor of n.

Hence the sum of all positive divisors of n

$$= (1+p_1+p_1^2+\dots+p_1^{\alpha_1})(1+p_2+p_2^2+\dots+p_2^{\alpha_2}) \dots (1+p_r+p_r^2+\dots+p_r^{\alpha_r})$$

$$= \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \dots \cdot \frac{p_r^{\alpha_r+1}-1}{p_r-1}.$$

If $n = 1$, the sum $= 1$.

Definition. The sum of all positive divisors of a positive integer n is denoted by $\sigma(n)$. (*sigma n*).

If the canonical form of a positive integer $n(> 1)$ be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

then $\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \dots \cdot \frac{p_r^{\alpha_r+1}-1}{p_r-1}$; and $\sigma(1) = 1$.

Definition. A function whose domain is the set of all positive integers is said to be a *number-theoretic function* (or an *arithmetic function*). The range of a number-theoretic function need not be the set of all positive integers. We shall encounter some simple number-theoretic functions which assume positive integral values.

The functions τ and σ are examples of number-theoretic functions.

A number-theoretic function f is said to be *multiplicative* if $f(mn) = f(m)f(n)$ for all integers m, n such that m, n are prime to each other.

Theorem 3.3.12. The functions τ and σ are both multiplicative functions.

Proof. Let m, n be relatively prime integers.

$\tau(mn) = \tau(m)\tau(n)$ holds trivially if either m or n is 1.

We assume $m > 1$ and $n > 1$.

Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ and $n = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$, where p_i, q_j are primes and $\alpha_i \geq 1$, $\beta_j \geq 1$.

Since m, n are relativey prime, each p_i is different from each q_j.

Therefore the prime factorisation of mn is

$$mn = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}.$$

$$\tau(mn) = (\alpha_1+1)(\alpha_2+1)\dots(\alpha_r+1)(\beta_1+1)(\beta_2+1)\dots(\beta_s+1)$$
$$= \tau(m)\tau(n).$$

$$\sigma(mn) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_r^{\alpha_r+1}-1}{p_r-1}\cdot\frac{q_1^{\beta_1+1}-1}{q_1-1}\cdot\frac{q_2^{\beta_2+1}-1}{q_2-1}\cdots\frac{q_s^{\beta_s+1}-1}{q_s-1};$$
$$= \sigma(m)\sigma(n).$$

Hence τ and σ are multiplicative functions.

Definition. Perfect number. A positive integer n is said to be a *perfect number* if $\sigma(n) = 2n$, i.e., if n be the sum of all its positive divisors excluding itself.

For example, 6 is a perfect number. 28 is another.

Worked Examples.

1. Find $\tau(360)$ and $\sigma(360)$.

$360 = 2^3.3^2.5$. Therefore $\tau(360) = (1+3).(1+2).(1+1) = 24$.

$\sigma(360) = \frac{2^4-1}{2-1}.\frac{3^3-1}{3-1}.\frac{5^2-1}{5-1} = 15.13.6 = 1170$.

2. Find the number of odd positive divisors of 2700.

$2700 = 2^2.3^3.5^2$. Every positive divisor of 2700 is of the form $2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}$, where $0 \le \alpha_1 \le 2, 0 \le \alpha_2 \le 3, 0 \le \alpha_3 \le 2$.

Therefore each term in the product $(1+2+2^2)(1+3+3^2+3^3)(1+5+5^2)$ is a positive divisor of 2700 and conversely.

The odd positive divisors of 2700 are given by the terms of the product $1.(1+3+3^2+3^3)(1+5+5^2)$.

The number of odd positive divisors are $(3+1)(2+1)$, i.e.,12.

3. Find the sum of all even positive divisors of 2700.

From the previous example it follows that the even positive divisors of 2700 are given by the different terms of the product

$$(2+2^2)(1+3+3^2+3^3)(1+5+5^2).$$

The sum of the even positive divisors

$$= (2+2^2)(1+3+3^2+3^3)(1+5+5^2) = 6.40.31 = 7440.$$

4. Let $k > 1$ and $2^k - 1$ is a prime. If $n = 2^{k-1}(2^k-1)$ then show that n is a perfect number.

$2^k - 1$ is an odd prime, say p.

$\sigma(n) = \sigma(2^{k-1}p) = \sigma(2^{k-1})\sigma(p)$, since 2^{k-1} and p are prime to each other.

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

Therefore $\sigma(n) = (2^k-1)(1+p) = (2^k-1)2^k = 2n$.

This proves that n is a perfect number.

Note. This example shows that if $2^n - 1$ $(n > 1)$ is a prime, then the number $2^{n-1}(2^n - 1)$ is a perfect number.

The numbers of the form $M_n = 2^n - 1$ $(n > 1)$ are called Mersenne numbers, named after Mersenne (1588-1648), a French monk and an amateur of mathematics.

The primality of M_n requires n must be a prime.

If M_n be a prime then M_n is called a Mersenne prime and in that case a perfect number $2^{n-1}(2^n - 1)$ is obtained.

5. If $d_1, d_2, \ldots, d_k$ be the list of all positive divisors of a positive integer n, prove that $\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k} = \frac{\sigma(n)}{n}$.

d_i is a positive divisor $\Rightarrow \frac{n}{d_i}$ is also a positive divisor. As d runs through the set of all positive divisors of n, $\frac{n}{d}$ also does so.

Therefore $\frac{n}{d_1} + \frac{n}{d_2} + \cdots + \frac{n}{d_k} = d_1 + d_2 + \cdots + d_k = \sigma(n)$

or, $\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k} = \frac{\sigma(n)}{n}$.