3. INTEGERS

3.1. Natural numbers.

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

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

This means that if S be a non-empty subset of $\mathbb{N}$ 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 $\mathbb{N}$ 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 $S = \mathbb{N}$.

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 $S = \mathbb{N}$.

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

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

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, $(a_1a_2\ldots a_{2^n})^{\frac{1}{2^n}} \leq \frac{a_1+a_2+\cdots+a_{2^n}}{2^n}$, where a_i 's are positive real numbers for $i = 1, 2, \ldots, 2^n$.

The statement is true for $n = 1$, since $(a_1a_2)^{\frac{1}{2}} \leq \frac{a_1+a_2}{2}$ $\cdots$ (i)

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

Then $(a_1a_2\ldots a_{2^k})^{\frac{1}{2^k}} \leq \frac{a_1+a_2+\cdots+a_{2^k}}{2^k} = p$, say.

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

Then $(b_1b_2\ldots b_{2^k})^{\frac{1}{2^k}} \leq \frac{b_1+b_2+\cdots+b_{2^k}}{2^k} = q$, say.

Now $\{(a_1a_2\ldots a_{2^k})^{\frac{1}{2^k}}(b_1b_2\ldots b_{2^k})^{\frac{1}{2^k}}\}^{\frac{1}{2}} = (pq)^{\frac{1}{2}}$

$\leq \frac{p+q}{2}$ $\cdots$ by (i)

or, $(a_1a_2\ldots a_{2^{k+1}})^{\frac{1}{2^{k+1}}} \leq \frac{(a_1+a_2+\cdots+a_{2^k})+(b_1+b_2+\cdots+b_{2^k})}{2^{k+1}}$

i.e., $(a_1a_2\ldots a_{2^{k+1}})^{\frac{1}{2^{k+1}}} \leq \frac{(a_1+a_2+\cdots+a_{2^{k+1}})}{2^{k+1}}$.

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

By the principle of induction, the statement is true for all $n \in \mathbb{N}$.

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) $k(\geq n_0) \in S$ implies $k + 1 \in S$.
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 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 $n \geq 4$.

3.2. Integers.

The set of all integers, denoted by $\mathbb{Z}$, consists of whole numbers $0, \pm1, \pm2, \pm3, \ldots \quad \ldots$ 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 $\quad a = bq + r$, 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: $\quad a = bq + r$, $a = bq_1 + r_1$ where $0 \leq r < b$, $0 \leq r_1 < b$.

Then $b(q - q_1) = r_1 - r \quad$ 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 $b = 3, a = -20, 2, 10$.

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

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

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

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 $m \mid c + (m-2)$;
$\ldots \quad \ldots \quad \ldots \quad \ldots$
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 $1 = au + vb$.

$$\begin{aligned} \text{Therefore } c &= (au)c + (bv)c \\ &= ab(un + vm) \Rightarrow ab \mid c. \ \square \end{aligned}$$

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 $0 \le r_1 < b$.
If it happens that $r_1 = 0$, then $b \mid a$ and $gcd(a, b) = b$.

If $r_1 \ne 0$, then by division algorithm, $b = r_1 q_2 + r_2$ where $0 \le r_2 < r_1$.

If $r_2 = 0$, the process stops.If $r_2 \neq 0$, by division algorithm

$$r = r_2q_3 + r_3 \text{ where } 0 \leq r_3 < r_2.$$

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 $567 = 315.1 + 252$, $\quad 315 = 252.1 + 63$, $\quad 252 = 63.4 + 0$.
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 $\quad 63u + 55v = 1$.

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

By division algorithm,
$63 = 55.1 + 8$, $\quad 55 = 8.6 + 7$, $\quad 8 = 7.1 + 1$.
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 $\quad 54u + 24v = 30$.

Let us find the $gcd(54, 24)$.
By division algorithm, $\quad 54 = 24.2 + 6$, $\quad 24 = 6.4 + 0$.
Therefore $gcd(54, 24) = 6$.
Now $6 = 54 - 24.2 = 54.1 + 24.(-2)$.
Consequently, $30 = 54.5 + 24.(-10)$. Therefore $u = 5, v = 10$.