MODULE-2

Division Algorithm

suppose an integer a is divided by a positive integer b, Then we get a unique quotient q and a unique remainder r, where the remainder r satisfies the common condition $0 \leq r < b$, a is the dividend and b the divisor.

Theorem: (Division Algorithm)

Given integers a and b, with $b > 0$, there exist unique integers q and r satisfing,

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

Proof,

The proof consists of two parts. First, we must establish the existence of the integers q and r and then we must show they are indeed unique.

Existence part:

consider the set

$$S = \{ a - xb : x \text{ is an integer and } a - xb \geq 0 \}$$

well ordering principle:

Every nonempty set S of nonnegative integers contains a least element, ie, there is some integer a in S such that $a \leq b$ for all b's belonging to S.

First we will prove that S is nonempty. ↓ To perform well ordering property

To do this we have to consider two cases.

case 1: Let $a \geq 0$, Then $a - b \cdot 0 = a \geq 0$. Hence $a \in S$ and so S is nonempty.

case 2: Let $a < 0$, since b is a positive integer $b \geq 1$ and so

$|a|b \geq |a|$ → $|a|$ - +ve, b - +ve, $|a|b \geq |a|$

eg: $a = -2$ $b = 3$, $|a|b = 6$, $|a| = 2$, $6 \geq 2$ //

since $a < 0$, $|a| = -a$ and so the above inequality implies that.

$-ab \geq -a$ ie $ab \leq a$

$\therefore a - ab \geq 0$ and consequently, $a - ab \in S$ and so S is nonempty.

Thus S is a nonempty set of nonnegative integers. Then by well ordering principle, S contains a least element r.

since $r \in S$, by the definition of S, there exists an integer q such that,

$r = a - qb$

ie, $a = qb + r \quad r \geq 0$

it possible let $r \geq b$ Then $r - b \geq 0$ and so

~~$a - qb - b$~~

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

hence $a - (q+1)b \in S$. But $a - (q+1)b = r - b < r$ (r is min, r-b < min violate well ordering)

leading to a contradiction of the choice of r as the smallest member of S. hence $r < b$.

$\therefore \quad a = qb + r, \quad 0 \le r < b$

uniqueness part:

suppose that a has a representation of the desired form, say

$a = qb + r$ and $a = q_1 b + r_1$

where q, q_1, r and r_1 are integers and $0 \le r, r_1 < b$

then $qb + r = q_1 b + r_1$ and hence $r - r_1 = b(q_1 - q)$ $(\because b \neq 0)$

$\therefore \quad |r - r_1| = b\,|q_1 - q|$

Now $0 \le r < b$ and $0 \le r_1 < b \Rightarrow 0 \le r < b$ and $-b < -r_1 \le 0$

~~$\Rightarrow -b < -r_1 \le 0 \le r < b$~~

~~$\Rightarrow -b < -r_1 \le r < b$~~

~~$\Rightarrow -b < r$~~ add 2 inequalities.

$\Rightarrow -b < r - r_1 < b \Rightarrow |r - r_1| < b$

$\therefore |r - r_1| = b\,|q_1 - q| < b$, which $|q_1 - q| = 1$

$b \times 1 < b$, $b < b$ not poss'ble

$|q_1 - q|$ must be < 1

which implies $|q_1 - q| < 1$.

only possibility $|q_1 - q| = 0$

since $|q_1 - q|$ is a nonnegative integer the only possibility is that $|q_1 - q| = 0$. $\therefore q = q_1$ and this, in turn, gives $r = r_1$. Hence the above representation is unique. $q_1 = q$ & $r_1 = r$

corollary.

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

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

To illustrate the division Algorithm, when $b < 0$, let us take $b = -7$, Then, for the choices of $a = 1, -2, 61$, and -59, we obtain the expressions

$$1 = 0 \times -7 + 1$$

$$-2 = 1 \times -7 + 5$$

$$61 = -8 \times -7 + 5$$

$$-59 = 9 \times (-7) + 4$$

? Show that the power of every odd integer leave remainder 1 when divided by 4

A Generally,

odd integer is of the form, $2n+1$

power of odd integer $= (2n+1)^2$

$$= 4n^2 + 4n + 1$$

$$= \underbrace{4k + 4k}_{\text{multiple of } 4} + 1$$

$$= 8k + 1$$

so remainder $= 1$ //

? S.T the square of any odd integer is of the form $8k+1$.

A. By division algorithm, any integer, when divided by 4 leaves 0 or 1 or 2 or 3 as remainder. Hence any integer can be represented as one of the forms, $4q+0$, $4q+1$, $4q+2$, $4q+3$, where q is an integer in this classification, only those integers of the forms $4q+1$ and $4q+3$ are odd.

squaring these numbers we get

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

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

hence the square of any odd integer is of the form $8k+1$.

2. show that the expression $\frac{a(a^2+2)}{3}$ is an integer for all $a \geq 1$

A). By division algorithm when a is divided by 3, it leaves 0 or 1 or 2 as remainder. Hence a can be written as one of the three forms.

$3q$, $3q+1$, $3q+2$, where q is an integer.

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

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

$= q(9q^2+2)$, an integer

when $a = 3q+1$,

$$\frac{a(a^2+2)}{3} = \frac{(3q+1)\left[(3q+1)^2+2\right]}{3}$$

$$= \frac{(3q+1)\left[9q^2+6q+1+2\right]}{3}$$

$$= \frac{(3q+1)\left[9q^2+6q+3\right]}{3}$$

$= (3q+1)(3q^2+2q+1)$, an integer

when $a = 3q+2$,

$$\frac{a(a^2+2)}{3} = \frac{(3q+2)\left[(3q+2)^2+2\right]}{3}$$

$$= \frac{(3q+2)\left[9q^2+12q+4+2\right]}{3}$$

$= (3q+2)(3q^2+4q+2)$, an integer

Hence the given expression is always an integer.

GCD

Let a and b be given integers with atleast one of them different from zero. The greatest common divisor of a and b, denoted by gcd(a,b) is the positive integer d satisfying the following

(a) d is a divisor of both a and b ie, $d|a$ and $d|b$

(b) if $c|a$ and $c|b$ then $c \leq d$

DIVISIBILITY

Theorem:

for integers a, b, c, the following hold:

a) $a|0$, $1|a$, $a|a$

b) $a|1$ iff $a = \pm 1$

c) if $a|b$ and $c|d$, then $ac|bd$

d) if $a|b$ and $b|c$, then $a|c$

e) $a|b$ and $b|a$, iff $a = \pm b$

f) if $a|b$ and $b \neq 0$, then $|a| \leq |b|$

g) if $a|b$ and $a|c$, then $a|(bx+cy)$ for arbitrary integers x and y.

Proof,

(b) since $0 = a \cdot 0$, for every integer a, we see that every integer is a divisor of 0 ie, $a|0$, $\forall$ integer a.

since $a = a \cdot 1$, $1|a$ and $a|a$ $\forall$ integer a.

(e)

for any integer a, we've

$a|1 \Rightarrow 1 = ab$, for some integer b

$\Rightarrow a = 1$ and $b = 1$ or $a = -1$ and $b = -1$

$\Rightarrow a = \pm 1$

conversely, let $a = \pm 1$, if $a = 1$, then $1 = a \cdot 1$ and if $a = -1$, then $1 = a \cdot -1$. Thus in either case $a|1$.

(c) Let $a|b$ and $c|d$. Now $a|b \Rightarrow b = ar$, for some integer r and $c|d \Rightarrow d = cs$, for some integer s.

Then $bd = (ar)(cs)$

$= (ac)(rs)$, where rs is an integer.

hence $ac|bd$.

(d) Let $a|b$ and $b|c$

$a|b \Rightarrow b = ar$

$b|c \Rightarrow c = bs$

$\Rightarrow c = ars$, rs is an integer

$\Rightarrow a|c$

(e) $a|b$ and $b|a$

$a|b \Rightarrow b = ar$

$b|a \Rightarrow a = bs$

$\Rightarrow b = bsr$

$\Rightarrow b = b(rs)$

$\Rightarrow rs = 1$

$\Rightarrow r = 1$ or $r = -1$ and $s = 1$ or $s = -1$

$\Rightarrow r = s = \pm 1$

~~$\Rightarrow b = \pm 1 \times b$~~

$\therefore a = bs$

$\Rightarrow a = \pm b$ ($\because s = \pm 1$)

Conversily, $a = \pm b$. Then $a = (\pm 1)b$ and so $b|a$.

Also $a = \pm b$ implies $b = \pm a$ and consequently $b = (\pm 1)a$

$\Rightarrow a|b$ //

(f) Let a|b and b≠0 Now, a|b ⇒ b=ar, for some integer r and b≠0 implies that r≠0

Then |b| = |a||r|

since r≠0, |r| ≥ 1 and so |b| = |a||r| ≥ |a|,

ie, |a| ≤ |b|

(g) Let a|b and a|c.

a|b ⇒ b=ar, for some integer r

a|c ⇒ c=as, " "

Then for any arbitrary integers x and y, we get, bx+cy = (ar)x + (as)y

= a(rx+sy), where rx+sy is an integer. Hence a|bx+cy.

(h) Theorem:

Given integers a and b, not both of which are zero, there exist integers x and y such that

gcd(a,b) = ax+by

Note:

* If a|b and b|c then a|c ⇒ This statement is false.

eg: 8|24 and 8|24 but 8×6 = 48 doesn't divides 24

* corollary of Euclid's lemma.

If p|ab then p|a or p|b, where p is a prime no.

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

(i) *d is a divisor of both a and b i. e., $d \mid a$ and $d \mid b$*

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

For example, the positive divsors of -12 are 1, 2, 3, 4, 6, 12, whereas those of 30 are 1, 2, 3, 5, 6, 10, 15, 30; hence the positive common divisors of -12 and 30 are 1, 2, 3, 6. Since 6 is the largest of these integers, it follows that gcd $(-12, 30) = 6$. In the same way we can show that

$$\gcd(-5, 5) = 5, \quad \gcd(12, 25) = 1, \quad \gcd(-8, -32) = 8.$$

The next theorem establishes that for any two integers a and b, gcd (a, b) can be represented by a linear combination of a and b. By a linear combination of a and b we mean an expression of the form $ax + by$, where x and y are integers.

Theorem 1. *Given integers a and b, not both of which are zero, there exist integers x and y such that*

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

Proof. Let S be the set of all positive linear combinations of a and b i. e., $S = \{ax + by : x \text{ and } y \text{ are integers and } ax + by > 0\}$.

Since at least one of a and b is nonzero, let us assume with out loss of generality that $a \neq 0$. If $a > 0$, then $a = a \cdot 1 + b \cdot 0 > 0$ and hence $a \in S$. If $a < 0$, then $-a = a \cdot (-1) + b \cdot 0 > 0$ and hence $-a \in S$. Thus in either case S is nonempty.

Thus S is a nonempty set of nonnegative integers. Then by 'Well-ordering Principle' S contains a least element d.

Since $d \in S$, by the definition of S, there exists integers x and y such that $d = ax + by$.

To show that $d = \gcd(a, b)$

By Division Algorithm, there exists integers q and r such that

$$a = qd + r, \quad \text{where} \quad 0 \le r < d.$$

Then r can be written in the form

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

If $r > 0$, then this representation would imply that r is a member of S, contradicting the fact that d is the least integer in S. Therefore $r = 0$ and so $a = qd$ or equivalently $d \mid a$.

Similarly, by Division Algorithm, there exists integers q_1 and r_1 such that $b = q_1 d + r_1$, where $0 \le r_1 < d$.

Then r_1 can be written in the form

$$r_1 = b - q_1 d = b - q_1(ax + by) = a(-q_1 x) + b(1 - q_1 y).$$

If $r_1 > 0$, then this representation would imply that r_1 is a member of S, contradicting the fact that d is the least integer in S. Therefore $r_1 = 0$ and so $b = q_1 d$ or equivalently $d \mid b$.

Thus d is a common divisor of a and b.

Now let c be an arbitrary positive common divisor of the integers a and b. But $c \mid a$ and $c \mid b$ implies $c \mid ax + by$ i.e., $c \mid d$. Also $c \mid d$ implies $c = |c| \le |d| = d$. Thus d is greater than any other common divisor of a and b. Hence d is the greatest common divisor of a and b.

$$\therefore \qquad d = \gcd(a, b).$$

Remark. A persual of the proof of the above theorem reveals that the greatest common divisor of a and b may be described as the smallest positive integer of the form $ax + by$. Consider the case in which $a = 8$ and $b = 12$. Here the set S becomes

$$S = \{8(-1) + 12 \cdot 1,\ 8 \cdot 0 + 12 \cdot 1, 8 \cdot 1 + 12 \cdot 0, \ldots\} = \{4, 12, 8, \ldots\}.$$

Here 4 is the smallest integer in S and $4 = \gcd(8, 12)$.

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

$$T = \{ax + by : x, y \text{ are integers}\}$$

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

Proof. Since $d = \gcd(a, b)$, d is a common divisor of a and b i.e., $d \mid a$ and $d \mid b$. We know that $d \mid a$ and $d \mid b$ implies $d \mid ax + by$, for all integers x and y. Hence every member of T is a multiple of d.

Now let c be any multiple of d. Then $c = nd$, for some integer n. By the theorem, we can write d as

$$d = au + bv, \text{ for some integers } u \text{ and } v.$$

Then $$c = nd = n(au + bv) = a(nu) + b(nv).$$

Hence c is a linear combination of a and b and hence is an element of T. Thus T is precisely the set of all multiples of d.

Procedure for finding the g.c.d. (Euclidean Algorithm)

The Euclidean Algorithm presents a systematic step-by step process for obtaining the greatest common divisor of two given numbers.

Let a and b be the two integers whose greatest common divisor is desired. Since $\gcd(|a|, |b|) = \gcd(a, b)$, let us assume with out loss of generality that $a \geq b > 0$. Now divide a by b. Let q_1 be the quotient and r_1 be the remainder obtained.

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

If $r_1 = 0$, then $b|a$ and hence $\gcd(a, b) = b$. If $r_1 \neq 0$, we now divide b by r_1, to produce integers q_2 and r_2 satisfying

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

If $r_2 = 0$, then we stop. If $r_2 \neq 0$, we now divide r_1 by r_2, getting

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

Repeat this process. Since $r_1 > r_2 > r_3 > \ldots$, and all these remainders are non-negative integers, we must eventually get a zero remainder. If r_{n+1} is the first zero remainder, we then have the following system of equations.

$$\begin{aligned}
a &= q_1 b + r_1, & 0 < r_1 < b \\
b &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2 \\
r_2 &= q_4 r_3 + r_4, & 0 < r_4 < r_3 \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
r_{n-2} &= q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
\text{and} \quad r_{n-1} &= q_{n+1} r_n.
\end{aligned}$$

We now assert that r_n (the last non-zero remainder) is the greatest common divisor of a and b. Our proof is based on the lemma given below:

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

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

$$\gcd(a,b) = d \Rightarrow d \mid a \text{ and } d \mid b \Rightarrow d \mid (a - qb) \text{ and } d \mid b$$
$$\Rightarrow d \mid r \text{ and } d \mid b. \qquad [\because r = a - qb]$$

Thus d is a common divisor of both b and r. Now let c be an arbitrary common divisor of b and r. Then $c \mid (qb + r)$ and so $c \mid a$. Then c is a common divisor of a and b and so $c \leq d$ (since $d = \gcd(a, b)$). Thus every other common divisor of b and r is less than or equal to d. Therefore d is the greatest common divisor of b and r.

$$\therefore \qquad \gcd(a, b) = d = \gcd(b, r).$$

Using the result of this lemma, we simply work down the displayed system of equations, obtaining

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

Hence r_n is the greatest common divisor of a and b.

Remark. Theorem 1 asserts that $\gcd(a, b)$ can be expressed in the form $ax + by$, but the proof of the theorem gives no hint as to how to determine the integers x and y. For this, we fall back on the Euclidean algorithm. Starting with the next to last equation arising from the algorithm, we write

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

Now solve the preceding equation in the algorithm for r_{n-1} and substitute to obtain

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

This represents r_n as a linear combination of r_{n-2} and r_{n-3}. Continuing backward through the system of equations, we successively eliminate the remainders $r_{n-1}, r_{n-2}, \ldots, r_2, r_1$ until a stage is reached where $r_n = \gcd(a, b)$ is expressed as a linear combination of a and b. The following problems illustrate the method.

Problem 3. *Find the g.c.d. of* 26 *and* 382 *and express it as a linear combination* 26 *and* 382.

Solution. Applying Division Algorithm successively, as in Euclidean

Algorithm, we get the following system of equations :

$$382 = 14 \cdot 26 + 18,$$
$$26 = 1 \cdot 18 + 8,$$
$$18 = 2 \cdot 8 + 2,$$

and
$$8 = 4 \cdot 2.$$

In this case, 2 is the greatest common divisor of 382 and 26, since it is the last non-zero remainder. To express 2 as a linear combination of 382 and 26, we start with the next to last of the displayed equations and successively eliminate the remainders 8 and 18 :

$$2 = 18 - 2 \cdot 8$$
$$= 18 - 2 \cdot (26 - 1 \cdot 18) = 3 \cdot 18 - 2 \cdot 26$$
$$= 3 \cdot (382 - 14 \cdot 26) - 2 \cdot 26 = 3 \cdot 382 - 44 \cdot 26.$$

$\therefore$
$$2 = 3 \cdot 382 - 44 \cdot 26.$$

Theorem 2. *If $k > 0$, then* gcd $(ka, kb) = k$ gcd (a, b).

Proof. The system of equations in the Euclidean Algorithm for finding greatest common divisor of a and b are as follows :

$$\begin{aligned} a &= q_1 b + r_1, && 0 < r_1 < b \\ b &= q_2 r_1 + r_2, && 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, && 0 < r_3 < r_2 . \\ r_2 &= q_4 r_3 + r_4, && 0 < r_4 < r_3 \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ r_{n-2} &= q_n r_{n-1} + r_n, && 0 < r_n < r_{n-1} \end{aligned}$$

and $\quad r_{n-1} = q_{n+1} r_n.$

Then g.c.d. of a and b is the last nonzero remainder r_n i.e., gcd $(a, b) = r_n$. Multiplying each equations of the above system by k, we get

$$\begin{aligned} ak &= q_1 (bk) + r_1 k, && 0 < r_1 k < bk \\ bk &= q_2 (r_1 k) + r_2 k, && 0 < r_2 k < r_1 k \\ r_1 k &= q_3 (r_2 k) + r_3 k, && 0 < r_3 k < r_2 k \\ r_2 k &= q_4 (r_3 k) + r_4 k, && 0 < r_4 k < r_3 k \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ r_{n-2} k &= q_n (r_{n-1} k) + r_n k, && 0 < r_n k < r_{n-1} k \end{aligned}$$

and $\quad r_{n-1} k = q_{n+1} (r_n k).$

But this is clearly Euclidean Algorithm for finding greatest common divisor of ka and kb. Hence the greatest common divisor of ka and kb is the last nonzero remainder $r_n k$.

$\therefore \qquad$ gcd $(ka, kb) = k$ gcd (a, b).

§ 4. RELATIVELY PRIME NUMBERS

Two integers a and b, not both of which are zero, are said to be ***relatively prime*** (or ***prime to each other***) if their greatest common divisor is 1, that is, if gcd $(a, b) = 1$.

The following theorem characterises relatively prime integers in terms of linear combinations.

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

Corollary 1. *If* gcd $(a, b) = d$, *then* gcd $(a/d, b/d) = 1$.

Proof. Let gcd $(a, b) = d$. Then, by theorem 1, of section § 3, it follows that there exist integers x and y such that $d = ax + by$.

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

Since gcd $(a, b) = d$, $d \mid a$ and $d \mid b$. Hence a/d and b/d are integers and so by the above theorem, $1 = (a/d)\,x + (b/d)\,y$ implies that a/d and b/d are relatively prime. Therefore gcd $(a/d, b/d) = 1$.

Corollary 2. *If* $a \mid c$ *and* $b \mid c$, *with* gcd $(a, b) = 1$, *then* $ab \mid c$.

Proof. Let $a \mid c$ and $b \mid c$. Then there exist integers r and s such that $c = ar = bs$. Since gcd $(a, b) = 1$, there exist integers x and y such that $1 = ax + by$. Multiplying this equation by c, we get

$$c = c \cdot 1 = c(ax + by) = acx + bcy$$
$$= a\,(bs)\,x + b\,(ar)\,y = ab(sx + ry). \qquad [\because\ c = ar = bs]$$

Since $sx + ry$ is an integer, above equation implies that $ab \mid c$.

Theorem 2. (***Euclid's lemma***) *If* $a \mid bc$, *with* gcd $(a, b) = 1$, *then* $a \mid c$.

Proof. Since gcd $(a, b) = 1$, there exist integers x and y such that $1 = ax + by$. Multiplying this equation by c, we get

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

Since $a \mid ac$ and $a \mid bc$, it follows that $a \mid acx + bcy$, which is equivalent to saying $a \mid c$.

§5. LEAST COMMON MULTIPLE

The *least common multiple* (l.c.m.) of two positive integers a and b is closely related to their g.c.d. In fact we use the l.c.m. every time we add and subtract fractions.

An integer c is said to be a ***common multiple*** of two nonzero integers a and b whenever $a \mid c$ and $b \mid c$. Evidently, zero is a common multiple of a and b. To see there exist common multiples that are not trivial, just note that the products ab and $-(ab)$ are both common multiples of a and b, and one of these is positive. By the Well-Ordering Principle, the set of positive common multiples of a and b must contain a smallest integer and we call

it the least common multiple of a and b. The precise definition of l.c.m. is as given below :

Definition. *The least common multiple two nonzero integers a and b, denoted by* lcm (a, b), *is the positive integer m satisfying the following conditions* :

(a) $a \mid m$ *and* $b \mid m$.

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

Usually, we use two methods to find l.c.m. of two nonzero integers. The first method emloys canonical decomposition of the integers (which we will discuss later in section § 7) and the second employs their g.c.d. The following theorem establishes a relationship between the ideas of greatest common divisor and least common multiple.

Theorem. *For positive integers a and b*

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

Proof. Let $d = \gcd(a, b)$. Then by definition, $d \mid a$ and $d \mid b$ and so $a = dr$ and $b = ds$, for some integers r and s.

Let $m = ab/d$.

Then $m = as = rb$, which implies that $a \mid m$ and $b \mid m$ i.e., m is a common multiple of a and b.

Now let c be any positive integer that is a common multiple of a and b. Let $c = au = bv$, where u and v are positive integers. Since $d = \gcd(a, b)$, there exist integers x and y such that $d = ax + by$.

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

Since u, v, x, y are all integers from the above equation, it follows that $m \mid c$, allowing us to conclude that $m \leq c$. Hence lcm $(a, b) = m$.

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

and so $$\gcd(a, b) \cdot \text{lcm}(a, b) = ab.$$

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

The above corollary follows directly from the theorem.

§ 6. LINEAR DIOPHANTINE EQUATIONS

Often we are interested in integral solutions of equations with integral coefficients. Such equations are called ***Diophantine equations***. The name honors the Greek mathematician ***Diophantus***, who initiated the study of such equations.

For example, when we restrict the solutions to integers, the equations $2x + 3y = 4$, $x^2 + y^2 = 1$ and $x^2 + y^2 = z^2$ are Diophantine equations.

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

$$x = x_0 + (b/d)t, \qquad y = y_0 - (a/d)t,$$

where t is an arbitrary integer.

Proof. Let $d = \gcd(a, b)$. Then by definition, $d \mid a$ and $d \mid b$ and so $a = dr$ and $b = ds$, for some integers r and s.

First let us assume that the linear Diophantine equation $ax + by = c$ has a solution and let the solution be x_0 and y_0. Then $ax_0 + by_0 = c$.

$$\therefore \qquad c = a x_0 + b y_0 = dr\, x_0 + ds\, y_0 = d\,(r x_0 + s y_0),$$

which implies that $d \mid c$.

Conversely, assume that $d \mid c$, so that $c = dt$, for some integer t. Since $\gcd(a, b) = d$, there exist integers u and v such that $d = au + bv$.

$$\therefore \qquad c = dt = (au + bv)t = a(ut) + b(vt).$$

Hence the Diophantine equation $ax + by = c$ has $x_0 = ut$ and $y_0 = vt$ as a particular solution.

Thus the linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$, where $d = \gcd(a, b)$.

Now suppose that a solution x_0, y_0 of the given Diophantine equation is known. Let x_1, y_1 be any other solution of the given equation. Then

$$ax_0 + by_0 = c = ax_1 + by_1,$$

which is equivalent to $a(x_1 - x_0) = b(y_0 - y_1)$. ...(1)

If $d = \gcd(a, b)$, then we know that $d \mid a$ and $d \mid b$ and so $a = dr$ and $b = ds$, for some integers r and s. Also $r = a/d$ and $s = b/d$ are numbers prime to each other (refer corollary 1 to Theorem 1 of section § 4). In (1) substituting $a = dr$ and $b = ds$, and cancelling the common factor d, we get

$$r(x_1 - x_0) = s(y_0 - y_1). \quad \ldots(2)$$

Now equation (2) implies that $r \mid s(y_0 - y_1)$. Since r and s are prime to each other, $\gcd(r, s) = 1$ and hence by Euclids lemma (Theorem 2 of section § 4), we get $r \mid (y_0 - y_1)$. Therefore $y_0 - y_1 = rt$, for some integer t. When $y_0 - y_1 = rt$, from equation (2), we get $x_1 - x_0 = st$.

$$\therefore \quad x_1 = x_0 + st = x_0 + \left(\frac{b}{d}\right)t \quad \text{and} \quad y_1 = y_0 - rt = y_0 - \left(\frac{a}{d}\right)t.$$

It is easy to see that these values satisfy the given Diophantine equation, regardless of the choice of the integer t; for

$$a x_1 + b y_1 = a\left[x_0 + \left(\frac{b}{d}\right)t\right] + b\left[y_0 - \left(\frac{a}{d}\right)t\right]$$

$$= (ax_0 + by_0) + \left(\frac{ab}{d} - \frac{ab}{d}\right)t = c.$$

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

Corollary. *If* $\gcd(a, b) = 1$ *and if* x_0, y_0 *is a particular solution of the linear Diophantine equation* $ax + by = c$, *then all solutions are given by*

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

for integral values of t.

The above corollary follows directly from the theorem.

these exhaust the divisors of a, then it is said to be a ***prime number***. The precise definition of prime number is as given below :

Definition. *An integer $p > 1$ is called a* ***prime number*** *or simply a* ***prime****, if its only positive divisors are 1 and p. An integer greater than 1 that is not a prime is termed* ***composite****.*

From the above definition it is clear that 1 is neither a prime nor a composite. It is just the multiplicative identity or the ***unit***. It also follows from the definition that the set of positive integers can be partitioned into three disjoint classes : the set of primes, the set of composites and $\{1\}$.

The first 10 primes are 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29. The first 10 composite numbers are 4, 6, 8, 9, 10, 12, 14, 15, 16 and 18.

In testing the primality of a specific integer $a > 1$, it is sufficient to divide a by those primes not exceeding $\sqrt{a}$ (pesuming, of course, the availability of a list of primes up to $\sqrt{a}$). This may be clarified by considering the integer $a = 509$. Since $22 < \sqrt{509} < 23$, we need only try out the primes that are not larger than 22 as possible divisors, namely, the primes 2, 3, 5, 7, 11, 13, 17 and 19. By dividing 509 by each of these, in turn, we find that none serves as a divisor of 509. The conclusion is that 509 must be a prime number.

The sieve of Eratosthenes. We have seen that if an integer $a > 1$ is not divisible by any prime $p \leq \sqrt{a}$, then a is necessarily a prime. Eratosthenes (276 - 194 B.C.) used this fact as the basis of a clever technique, called the ***Sieve of Eratosthenes***, for finding all primes below a given integer. The method consists in writing down all the integers upto the given number in their natural succession and then striking out all the multiples of 2, then the multiples of 3, then those of 5 and so on. The numbers that are left out (placed within circles) are the primes less than the given number. The Sieve for primes less than 100 is given below.

	(2)	(3)	~~4~~	(5)	~~6~~	(7)	~~8~~	~~9~~	~~10~~
(11)	~~12~~	(13)	~~14~~	~~15~~	~~16~~	(17)	~~18~~	(19)	~~20~~
~~21~~	~~22~~	(23)	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	(29)	~~30~~
(31)	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	(37)	~~38~~	~~39~~	~~40~~

Corollary 2. *If $p, q_1, q_2, \ldots, q_n$ are all primes and $p \mid q_1 q_2 \cdots q_n$, then $p = q_k$ for some k, where $1 \le k \le n$.*

Proof. By virtue of Corollary 1,

$$p \mid q_1 q_2 \cdots q_n \Rightarrow p \mid q_k, \text{ for some } 1 \le k \le n.$$

Since q_k is a prime number, q_k is not divisible by any positive integer other than 1 or q_k itself. Since $p > 1$, $p \mid q_k$ implies that $p = q_k$.

Theorem 2. (***Unique Factorisation Theorem* or *Fundamental Theorem of Arithmetic***) *Every positive integer $n > 1$ can be expressed as a product of primes; this representation is unique, apart from the order in which the factors occur.*

Proof. Let n be an integer greater than 1. Then either n is a prime number or is a composite number. If n is a prime number, then there is nothing to prove.

If n is composite, then there exist an integer d satisfying $d \mid n$ and $1 < d < n$. Among all such integers d, choose p_1 to be the smallest (this is possible by Well-Ordering Principle). Then we can show that p_1 is a prime.

If p_1 is not a prime number, then there exist an integer q satisfying $q \mid p_1$ and $1 < q < p_1$.

But $$q \mid p_1 \text{ and } p_1 \mid n \Rightarrow q \mid n,$$

which contradicts the choice of p_1 as the smallest positive divisor, not equal to 1, of n. Therefore p_1 is a prime number.

We therefore may write $n = p_1 n_1$, where p_1 is prime and $1 < n_1 < n$. If n_1 happens to be a prime, then there is nothing more to prove. Otherwise the argument is repeated to produce a second prime number p_2 such that

$$n_1 = p_2 n_2 \quad \text{that is} \quad n = p_1 p_2 n_2 \quad 1 < n_2 < n_1.$$

If n_2 is a prime, then it is not necessary to go further. Otherwise write $n_2 = p_3 n_3$ with p_3 prime so that

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

The decreasing sequence

$$n > n_1 > n_2 > \cdots > 1$$

cannot continue indefinitely, so that after a finite number of steps n_{k-1} is a prime, call it p_k. This leads to the factorization

$$n = p_1 p_2 p_3 \cdots p_k$$

where $p_1, p_2, \ldots, p_k$ are all prime numbers and $p_1 \le p_2 \le \cdots \le p_k$.

If possible, let n be expressed as the product of prime factors in another way, so that

$$n = q_1 q_2 q_3 \cdots q_m$$

where $q_1, q_2 \cdots q_m$ are all prime numbers and $q_1 \leq q_2 \leq \cdots \leq q_m$.

Then $$p_1 p_2 p_3 \cdots p_k = q_1 q_2 q_3 \cdots q_m. \quad \ldots (1)$$

The above equation implies that $p_1 \mid q_1 q_2 q_3 \cdots q_m$. Hence, by corollary 2 of theorem 1, we get $p_1 = q_s$ for some $1 \leq s \leq m$. Therefore $p_1 \geq q_1$. Similarly since $q_1 \mid p_1 p_2 p_3 \cdots p_k$, we get $q_1 = p_r$ for some $1 \leq r \leq k$ and therefore $q_1 \geq p_1$. Hence $p_1 = q_1$. We may cancel this common factor from equation (1) and we get

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_m.$$

We now repeat the process to get $p_2 = q_2$ and in turn

$$p_3 p_4 \cdots p_k = q_3 q_4 \cdots q_m.$$

Continuing in this fashion, if the inequality $k < m$ were to hold, we would eventually arrive at

$$1 = q_{k+1} q_{k+2} \cdots q_m,$$

which is absurd, since each $q_i > 1$. Similar is the case with $k > m$. Hence $k = m$ and $p_1 = q_1$, $p_2 = q_2, \ldots, p_k = q_k$, making the two factorizations of n identical. Thus every positive integer $n > 1$ can be expressed uniquely as a product of primes.

Corollary. *Any positive integer $n > 1$ can be written uniquely in a* ***canonical form***

lcm (90, 168). The canonical form of 90 and 168 are
$90 = 2 \cdot 3^2 \cdot 5$ and $168 = 2^3 \cdot 3 \cdot 7$.
Looking at the prime powers, it follows that their l.c.m. must be a multiple of 2^3, 3^2, 5 and 7 and so lcm (90, 168) $= 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$. The above observation can be written as

$$\text{lcm}(90, 168) = 2^{\max\{1,3\}} \cdot 3^{\max\{2,1\}} \cdot 5^{\max\{1,0\}} \cdot 7^{\max\{0,7\}}.$$

This leads to the following generalization.

Let a and b be two positive integers with the following cannonical form:

$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $a = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ where $a_i, b_i \geq 0$.

(In the above decomposition we assume that both decompositions contain exactly the same prime bases p_i. This is possible by taking, if p_i is not a factor of a, $a_i = 0$ and if p_i is not a factor of b, $b_i = 0$.)

Then $\text{lcm}(a, b) = p_1^{\max\{a_1, b_1\}} \cdot p_2^{\max\{a_2, b_2\}} \cdots p_n^{\max\{a_n, b_n\}}$.

Infinitude of Primes. One of the questions that arise concerning the class of primes is whether the number of primes is finite or infinite. Euclid prove that the number of primes is infinite.

Theorem 3. (*Euclid*) *The number of Primes is infinite.*

Proof. If possible, let the number of primes be finite, say n. Let $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ be primes in ascending order and p_n be the last prime. Then all the other numbers are composite and therefore should be exactly divisible by at least one of the prime numbers $p_1, p_2, \ldots, p_n$. Now consider the number

$$P = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1.$$

When this number is divided by p_1 or p_2 or p_3, ..., or by p_n, the remainder is 1. Hence P is not exactly divisible by any of the prime numbers $p_1, p_2, \ldots, p_n$; i.e. P is a prime number greater than $p_1, p_2, \ldots, p_n$, which is contrary to our assumption. Hence our supposition that the number of primes is finite, is absurd. Therefore the number of primes is infinite.

Remark 2. For a prime p, define $p^{\#}$ to be the product of all primes that are less than or equal to p. Numbers of the form $p^{\#} + 1$ might be termed *Euclidean numbers*, because they appear in Euclid's scheme for proving the infinitude of primes. It is interesting to note that in forming these

2. Find the gcd (12378, 3054)

$$3054 \overline{)12378}\ 4 \quad \text{rem} = 162$$

$12378 = 4 \times 3054 + 162$

$3054 = 18 \times 162 + 138$

$162 = 1 \times 138 + 24$

$138 = 5 \times 24 + 18$

$24 = 1 \times 18 + 6 \rightarrow \gcd = 6$ ——— a)

$18 = 3 \times 6 + 0$

$\gcd(12378, 3054) = 6$

Here 6 can be written as $6 = x \times 12378 + y \times 3054$

From a),

$6 = 24 - 1 \times 18$

$= 24 - (138 - 5 \times 24)$

$= 1 \times 24 - 138 + 5 \times 24$

$= 6 \times 24 - 138$

$= 6 \times 24 - 138$

$= 6 \times (162 - 138) - 138$

$= 6 \times 162 - 6 \times 138 - 1 \times 138$

$= 6 \times 162 - 7 \times 138$

$= 6 \times 162 - 7 (3054 - 18 \times 162)$

$= 132 \times 162 - 7 \times 3054$

$= 132 \times (12378 - 4 \times 3054) - 7 \times 3054$

$= 132 \times 12378 - (132 \times 4) \times 3054 - 7 \times 3054$

$6 = 132 \times 12378 - 535 \times 3054$

Consider the linear Diophantine equation

$172x + 20y = 1000$

$\gcd(172, 20) = 4$

here $4 \mid 1000$,

$a = 172, \quad b = 20$

$172 = 8 \times 20 + 12$

$20 = 1 \times 12 + 8$

$12 = 1 \times 8 + 4$

$8 = 2 \times 4 + 0$

$4 = 12 - 8$

$= 12 - (20 - 1 \times 12)$

$= 2 \times 12 - 20$

$= 2 \times (172 - 8 \times 20) - 20$

$= 2 \times 172 - 16 \times 20 - 1 \times 20$

$4 = 2 \times 172 - 17 \times 20$

$172x + 20y = 1000 \quad \text{---(1)}$

$172 \times 2 - 20 \times 17 = 4 \quad \text{---(2)}.$

$(2) \times 250 \Rightarrow 172 \times 500 - 20 \times (17 \times 500) = 1000$

$(x_0 = 500, \; y_0 = -4250)$

$1000 = 500 \times 172 + (-4250) 20$

So that $x = 500$, $y = -4250$ provide one solution to the Diophantine eqn on question. All other solutions are expressed by,

$x = 500 + (99/4)t = 500 + 5t$

$y = -4950 - (179/4)t = -4950 - 43t$ for some integer t.

Recurrence Relations

A recurrence relation is an equation that recursively defines a sequence where the next term is a function of the previous terms.

Initial condition uniquely determine a sequence in terms of recurrence relation.

Solution:

General solution:

particular solution:

? Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} + 3$ for $n = 1, 2, 3, \ldots$ and suppose that $a_0 = 2$. what are a_1, a_2 and a_3?

A). Initial condition $a_0 = 2$

order = 1

$a_1 = 5, a_2 = 8, a_3 = 11$

solution → 2, 5, 8, 11, ...

2. $a_n = a_{n-1} - a_{n-2}$ for $n = 2, 3, 4 \ldots$

$a_0 = 0$ and $a_1 = 5$, what are a_2 and a_3?

A). $a_2 = a_1 - a_0$

$= 5$

order = 2

$a_3 = a_2 - a_1$

$= 5 - 5 = 0$

* order = " no. of terms used to define the recurrence relation

order = difference of largest term and the relation and smallest term on the relation.

eg: $a_n = a_{n-1} - a_{n-2}$

order = $n - (n-2)$

$= 2$ //

? ~~$a_n = a_{n-1} - a_{n-2}$ for $n = 2, 3, 4$ ...~~

~~$a_0 = 3$ and $a_1 = 5$.~~

~~a_{n+1}~~ $a_0 = 3$

$a_1 =$

? $a_{n+1} = 3a_n$, $n \geq 0$, $a_0 = 5$

$a_0 = 5$

$a_1 = 3a_0 = 3(5)$

$a_2 = 3a_1 = 3(3a_0)$

$= 3^2(5)$

$a_3 = 3^3(5)$

$a_n = 3^n 5 \Rightarrow$ solution

$a_{n+1} = da_n \quad n \geq 0$

$a_0 = A$

general solution $\Rightarrow a_n = d^n A \quad n \geq 0$

? solve the recurrence relation $a_n = 7a_{n-1}$, where $n \geq 1$ and $a_2 = 98$

$a_n = 7a_{n-1}$

$a_2 = 7a_1 = 98$

$a_1 = 98/7 = 14$

$a_0 = 14/7 = 2$ //

general solution $= Ad^n$

$A = 2$

$d = 7$

$a_n = 2 \times 7^n$ 2A)

2. Find a recurrence relation with initial condition that uniquely determines each of the following geometric progressions.

a) 2, 10, 50, 250

A). 2, 2×5, 10×5 . . . .

$a_{n+1} = a_n \cdot 5$ where $a_0 = 2$.

b) 6, −18, 54, −162 . . .

A) $a_{n+1} = -3 \times a_n$, where $a_0 = 6$ 3A).

c) 7, 14/5, 28/25, 56/125 . . . .

A) $a_{n+1} = 2/5 \times a_n$, where $a_0 = 7$

3. Find the unique solution for each of the following recurrence relations.

a) $a_{n+1} - 1.5a_n = 0$, $n \geq 0$

b) $4a_n - 5a_{n-1} = 0$, $n \geq 1$

c) $3a_{n+1} - 4a_n = 0$, $n \geq 0$, $a_1 = 5$ 4A).

d) $2a_n - 3a_{n-1} = 0$, $n \geq 1$, $a_4 = 81$

1A). $a_{n+1} - 1.5a_n = 0$.

$a_0 = ?$

$a_1 = 1.5a_0$

$a_2 = (1.5)^2 a_0$

general solution =

$a_n = (1.5)^n \cdot a_0$

2A) $4a_n - 5a_{n-1} = 0$

$a_0 = ?$

$4a_1 - 5a_0 = 0$

$4a_1 = 5a_0$

$a_1 = 5/4\, a_0$

$4a_2 - 5a_1 = 0$

$4a_2 - 5(5/4 a_0) = 0$

$a_2 = \left(\frac{5}{4}\right)^2 a_0$

general solution,

$a_n = (5/4)^n a_0$

3A). $3a_{n+1} - 4a_n = 0$, $a_1 = 5$

$3a_1 - 4a_1 = 0$

$3a_2 = 20$

$a_2 = 20/3$

$3a_1 - 4a_0 = 0$

$15 = 4a_0$

$a_0 = 15/4$

$a_n = (4/3)^n \, 15/4$

4A). $2a_n - 3a_{n-1} = 0$ $a_4 = 81$

$2a_n = 3a_{n-1}$

$a_n = 3/2\, a_{n-1}$

$a_4 = 3/2\, a_3 = 81$

$a_3 = 2 \times 81/3 = 54$

$a_3 = 3/2\, a_2$

$54 = 3/2\, a_2$

$a_2 = 2/3 \times 54$

$= \frac{108}{3} = 36$

$a_2 = 3/2\, a_1$

$a_1 = 2/3\, a_2$

$= 2/3 \times 36$

$= 24$

$a_0 = 2/3\, a_1$

$= 16$ //

$a_n = (3/2)^n \cdot 16$ //

? The no. of bacteria in a culture is 1000 (approximately) and this number increases 250% every two hours. Use a recurrence relation to determine the no. of bacteria present after one day.

A). $a_0 = 1000$

$a_1 = 1000 + \frac{250}{100} \times 1000$

$= 1000 \left[1 + \frac{250}{100}\right]$

$= (1.25)\, 1000$

$a_2 = (1.25)\, a_1$

$\boxed{a_{n+1} = (1.25)\, a_n}$

$a_n = (1.25)^n a_0$

$a_n = (1.25)^n 1000$

After one day (after 24 hrs)

$a_{12} = (1.25)^{12} \cdot 1000$

? solve the relation $a_n = n \cdot a_{n-1}$, where $n \geq 1$ and $a_0 = 1$

A) $a_1 = 1 \cdot 1$

$a_2 = 2 \cdot 1$

$a_3 = 3 \cdot 2 \cdot 1$

$a_n = n!$

Linear recurrence Relation.

Linear recurrence relation is a relation in which all terms have degree one and they are not multiplied together.

eg: $a_{n+1}^2 - a_n = 2$ this is not a linear recurrence relation.

Linear homogeneous recurrence relation

$c_0 a_{n+1} + c_1 a_n + c_2 a_{n-1} + \cdots + c_{n+1} a_0 = f(n)$

eg: $2a_{n+1} - 3a_n + 4a_{n-1} = n^2$

for homogenous recurrence relation, $f(n) = 0$

eg: $2a_{n+1} - 3a_n + 4a_{n-1} = 0$

Second order linear homogeneous recurrence relation:

$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} = 0, \quad n \geq 2.$ ——— (1)

solution: $a_n = cr^n$ r same as d

substitute $a_n = cr^n$ in (1)

$c_0 cr^n + c_1 cr^{n-1} + c_2 cr^{n-2} = 0$

$cr^{n-2}(c_0 r^2 + c_1 r + c_2) = 0$

$c_0 r^2 + c_1 r + c_2 = 0$ => characteristic equation

2. $3a_n + 4a_{n-1} + 6a_n = 0$ find characteristic equation.

A). $a_n = cr^n$

$3(cr^n) + 4(cr^{n-1}) + 6(cr^n) = 0$.

$cr^{n-2}(3r^2 + 4r + 6) = 0$

$3r^2 + 4r + 6 = 0$

To find solution, find the roots of characteristic equation.
roots may be real and distinct or real and equal or complex.

case1. (DISTINCT Real Roots)

the general solution is of the form,

$a_n = c_1 r_1^n + c_2 r_2^n$

where r_1 & r_2 are distinct real roots.

2. solve the recurrence relation $a_n + a_{n-1} - 6a_{n-2} = 0$, where $n \geq 2$ and $a_0 = -1$, $a_1 = 8$

A). characteristic equation = $r^2 + r - 6$

root = 2, -3

gen solution is,

$a_n = c_1 r_1^n + c_2 r_2^n$

$a_n = c_1 2^n + c_2 (-3)^n$

a The value of a_0 and a_1 can be used to find value of c_1 & c_2.

$a_0 = c_1 2^0 + c_2 (-3)^0$

$a_0 = c_1 + c_2$

$c_1 + c_2 = -1$ ——— (1)

$a_1 = c_1 2 + c_2(-3)$

$2c_1 - 3c_2 = 8$ ——— (2).

multiply (1) with 2.

$2c_1 + 2c_2 = -2$. ——— (3)

(2) − (3) $= 7 \quad -5c_2 = 10$

$c_2 = -2$ //

$c_1 - 2 = -1$

$c_1 = 1$ //

∴ solution is,

$a_n = 2^n(-2)(-3)^n$

Case 2: (Complex Roots)

$z^n = r^n(\cos n\theta + i \sin n\theta)$ (polar form)

? solve the recurrence relation $a_n = 2(a_{n-1} - a_{n-2})$, where $n \geq 2$ and $a_0 = 1$, $a_1 = 2$.

A). $a_n - 2(a_{n-1}) + 2a_{n-2} = 0$

characteristic eqn = $r^2 - 2r + 2 = 0$

roots are, $r = \frac{2 \pm \sqrt{4 - 4 \times 1 \times 2}}{2}$

$= \frac{2 \pm \sqrt{-4}}{2}$

$= \frac{2 \pm 2i}{2}$

$r = 1 \pm i$

$a_n = c_1(1+i)^n + c_2(1-i)^n$

First convert $(1+i)$ & $(1-i)$ on to polar form.

$(1+i) = r(\cos\theta + i\sin\theta)$

$= \sqrt{2}(\cos\pi/4 + i\sin\pi/4)$

~~$= \sqrt{2}($~~

$r = \sqrt{a^2+b^2}$

$\theta = \tan^{-1}(b/a)$

$r = \sqrt{2}$

$\theta = \tan^{-1}(1)$

$= \pi/4$

~~$(1-i) = \sqrt{2}(\cos 7\pi/4 + i\sin 7\pi/4)$~~ ~~$\theta = -1$~~

~~$= \sqrt{2}$~~

$(1-1) = \sqrt{2}(\cos -\pi/4 + i\sin -\pi/4)$ $\left(\theta = \tan^{-1}(-1) = -\pi/4 \text{ or } 7\pi/4\right)$

solution,

~~$a_n = \sqrt{2}(\cos\pi/4 + is$~~

$a_n = c_1[(\sqrt{2})^n(\cos\pi/4 + i\sin\pi/4)^n] + c_2[(\sqrt{2})^n(\cos -\pi/4 + i\sin(-\pi/4)^n]$

$= c_1[(\sqrt{2})^n(\cos n\pi/4 + i\sin n\pi/4)] + c_2[(\sqrt{2})^n(\cos -n\pi/4 + i\sin(-n\pi/4)]$

$= (\sqrt{2})^n[c_1\cos n\pi/4 + c_1 i\sin n\pi/4 + c_2\cos n\pi/4 - c_2 i\sin n\pi/4]$

$= (\sqrt{2})^n[\cos n\pi/4(c_1+c_2) + i\sin n\pi/4(ic_1 - ic_2)]$

$a_n = (\sqrt{2})^n[A\cos n\pi/4 + Bi\sin n\pi/4]$

where,

$A = c_1 + c_2$

$B = i(c_1 - c_2)$

$a_0 = \cos 0(c_1 + c_2)$

$a_0 = c_1 + c_2$

$c_1 + c_2 = 1 = A$ ——— a)

$a_1 = \sqrt{2}\left[\frac{1}{\sqrt{2}}(c_1 + c_2) + i\frac{1}{\sqrt{2}}(c_1 - c_2)\right]$

$= c_1 + c_2 + i(c_1 - c_2)$

$c_1 + c_2 + i(c_1 - c_2) = 2$

$1 + i(c_1 - c_2) = 2$

$i(c_1 - c_2) = 1$

$B = 1$

$\therefore a_n = (\sqrt{2})^n \left(\cos 3\pi/4 + \sin n\pi/4 \right)$

case 3: Repeated real roots.

general solution:

$a_n = c_1 r^n + c_2 n r^n$

or

$a_n = (c_1 + c_2 n) r^n$

2. solve the recurrence relation $a_{n+2} = 4a_{n+1} - 4a_n$, where $n \geq 0$ and $a_0 = 1$, $a_1 = 3$

characteristic eqn $\Rightarrow r^2 - 4r + 4 = 0$

$r = 2, 2$

general soln $\Rightarrow$

$a_n = (c_1 + c_2 n) 2^n$.

$a_0 = (c_1 + c_2 \times 0)\, 2^0$

$a_0 = c_1$

$c_1 = 1$

$a_1 = (c_1 + c_2) 2$

$= 2(c_2 + c_1)$ $\quad 3 = (1 + c_2) 2$

$3/2 = 1 + c_2$

$c_2 = 3/2 - 1$

$= 1/2$

$a_n = (1 + 1/2 n) 2^n$

? Solve the following recurrence relations.

a) $a_n = 5a_{n-1} + 6a_{n-2}$, $n \geq 2$, $a_0 = 1$, $a_1 = 3$

b) $2a_{n+2} - 11a_{n+1} + 5a_n = 0$, $n \geq 0$, $a_0 = 2$, $a_1 = -8$

c) $a_{n+2} + a_n = 0$, $n \geq 0$, $a_0 = 0$, $a_1 = 3$

d) $a_n - 6a_{n-1} + 9a_{n-2} = 0$, $n \geq 2$, $a_0 = 5$, $a_1 = 12$

e) $a_n + 2a_{n-1} + 2a_{n-2} = 0$, $n \geq 2$, $a_0 = 1$, $a_1 = 3$.

NON Homogeneous recurrence relation

* $c_0 a_n + c_1 a_{n-1} + \cdots + c_n a_0 = F(n)$
* the solution (a_n) of a non-homogeneous recurrence relation has two parts.
* First part is the solution (a_h) of the associated homogeneous recurrence relation and the second part is the particular solution (a_t).

$$a_n = a_h + a_t$$

* solution to the first part is done using the procedures discussed in the previous ese section.
* To find the particular solution, we find an appropriate trial solution.
* Let $f(n) = cx^n$; let $x^2 = Ax + B$ be the characteristic equation of the associated homogeneous recurrence relation and let x_1 and x_2 be its roots.
* If $x_1 \neq x_1$ and $x \neq x_2$, then,

$$a_t = Ax^n$$

* If $x = x_1$, $x \neq x_2$, then

$$a_t = Anx^n$$

If $\alpha = \alpha_1 = 2, 1$ then,

$a_k = An^2 \alpha^n$

	$a_n^{(p)}$
c, a constant	A, a constant
n	$A_1 n + A_0$
n^2	$A_2 n^2 + A_1 n + A_0$
$n^k, k \in Z^+$	$A_k n^k + A_{k-1} n^{k-1} + \dots + A_1 n + A_0$
$r^n, r \in R$	$A r^n$
$\sin \omega n$	$A \sin \omega n + B \cos \omega n$
$\cos \omega n$	$A \sin \omega n + B \cos \omega n$
$n^k r^n$	$r^n (A_k n^k + A_{k-1} n^{k-1} + \dots + A_1 n + A_0)$
$r^n \sin \omega n$	$A r^n \sin \omega n + B r^n \cos \omega n$
$r^n \cos \omega n$	$A r^n \sin \omega n + B r^n \cos \omega n$

2. $a_{n+2} + 3a_{n+1} + 2a_n = 3^n, \; n \geq 0 \quad a_0 = 0, \; a_1 = 1$

A $\quad a_n = a_n^{(h)} + a_n^{(p)}$

$a_n^{(h)} \Rightarrow \quad a_{n+2} + 3a_{n+1} + 2a_n = 0$

$r^2 + 3r + 2 = 0$

$r = -2, -1$

$a_n^{(h)} = c_1 (-2)^n + c_2 (-1)^n$

$a_n^{(p)} \Rightarrow$ RHS $= 3^n \; (r^n)$

$a_n^{(p)} = A r^n$

$A 3^{n+2} + 3A \cdot 3^{n+1} + 2A \cdot 3^n = 3^n$

$9A + 9A + 2A = 1$

$20A = 1$

$A = 1/20$

$a_n^{(p)} = A r^n$

$= (1/20)\, 3^n$

$\therefore$

$a_n = c_1(-2)^n + c_2(-1)^n + (1/20)\, 3^n$

$a_0 = c_1 + c_2 + 1/20 = 0 \Rightarrow c_1 + c_2 = -1/20.$

$c_1 = -1/20 - c_2$

$a_1 = -2c_1 - c_2 + \frac{3}{20} = 1$

$= -2(-1/20 - c_2) - c_2 + 3/20 = 1$

$2(c_2 + 1/20) - c_2 + 3/20 = 1$

$2c_2 + 2/20 - c_2 + 3/20 = 1$

$c_2 + 5/20 = 1$

$c_2 + 1/4 = 1$

$c_2 = 1 - 1/4$

$c_2 = 3/4 //$

$c_1 = -1/20 - 3/4$

$= \frac{-4 - 60}{80}$

$= -\frac{64}{80} = -8/10 = -4/5$

$a_n = -4/5(-2)^n + 3/4(-1)^n + (1/20)\, 3^n$

2. $a_{n+1} - 2a_n = 2^n \quad n \geq 0, \quad a_0 = 1$

characteristic eqn: $a_{n+1} - 2a_n = 0$

$r^{n+1} - 2r^n = 0$

$r = 2 //$

$a_n^{(h)} = c_1 2^n$

$a_n^{(p)} = A 2^n \rightarrow$ but 2^n is already present in $a_n^{(h)}$

$\therefore a_n^{(p)} = An2^n$

$a_{n+1} - 2a_n = 2^n$

$\Rightarrow A(n+1)2^{n+1} - 2[An\,2^n] = 2^n.$

$A(n+1)2^{n+1} - An\,2^{n+1} = 2^n.$

$2A(n+1) - 2An = 1$

$2An + 2A - 2An = 1$

$2A = 1$

$A = 1/2$ //

$a_n^{(p)} = 1/2\, n\, 2^n$

$= n2^{n-1}$

$a_n = c_1 2^n + n2^{n-1}$

$a_0 = c_1$

$c_1 = 1$

$\therefore a_n = 2^n + n2^{n-1}$

2. $a_{n+2} + 4a_{n+1} + 4a_n = 7.\ n \geq 0,\ a_0 = 1,\ a_1 = 2$

$a_n^{(H)} = 7 \quad a_{n+2} + 4a_{n+1} + 4a_n = 0$

$r^2 + 4r + 4 = 0$

$r = -2, -2$ //

$a_n^{(h)} = c_1(-2)^n + c_2 n(-2)^n$

$a_n^{(p)} = A$

$a_n^{(p)} = A + 4A + 4A = 7$

$9A = 7$

$A = 7/9$

$\therefore a_n = c_1(-2)^n + c_2 n(-2)^n + 7/9.$

$a_0 = c_1 + 0 + 7/9$

$c_1 + 7/9 = 1$

$c_1 = 1 - 7/9$

$= 2/9$ //

$a_1 = c_1(-2) + c_2(-2) + 7/9$

$-2c_1 - 2c_2 + 7/9 = 2.$

$-4/9 - 2c_2 + 7/9 = 2.$

$3/9 - 2C_2 = 2$

$1/3 - 2C_2 = 2$

$2C_2 = 2 - 1/3$

$= 5/3$

$C_2 = 5/6$ //

$\therefore a_n = 2/9(-2)^n + 5/6(n(-2)^n) + 7/9$

2. Solve the recurrence relation $a_{n+2} - 6a_{n+1} + 9a_n = 3(2^n) + 7(3^n)$, where $n \geq 0$ and $a_0 = 1$, $a_1 = 4$.

A). $a_n^{(h)} \Rightarrow a_{n+2} - 6a_{n+1} + 9a_n = 0$

$r^2 - 6r + 9 = 0$

$a_n^{(h)} = c_1 3^n + c_2 n 3^n$

$a_n^{(p)} = A(2^n) + B(3^n)$ X (3^n & $n3^n$ are present in $a_n^{(h)}$)

$a_n^{(p)} = A(2^n) + B(3^n)n^2$

$A2^{n+2} + B3^{n+2}(n+2)^2 - 6[A(2^{n+1}) + B(3^{n+1})(n+1)^2] + 9[A2^n + Bn^2 3^n] = 3(2^n) + 7(3^n)$

$A2^{n+2} + B3^{n+2}(n+2)^2 - 6A(2^{n+1}) - 6B(3^{n+1})(n+1)^2 + 9A2^n + 9Bn^2 3^n = 3(2^n) + 7(3^n)$

$A2^{n+2} - 6A(2^{n+1}) + 9A2^n + B3^{n+2}(n+2)^2 - 6B(3^{n+1})(n+1)^2 + 9Bn^2 3^n$

$2^n[4A - 12A + 9A] + 3^n[9B(n+2)^2 - 18B(n+1)^2 + 9Bn^2] = 3(2^n) + 7(3^n)$

$\Rightarrow A = 3$ & $9B(n+2)^2 - 18B(n+1)^2 + 9Bn^2 = 7$

$9B(n^2 + 4n + 4) - 18B(n^2 + 2n + 1) + 9Bn^2 = 7$

$9Bn^2 + 36Bn + 36B - 18Bn^2 - 36Bn - 18B + 9Bn^2 = 7$

$18B = 7$

$B = 7/18$

$a_n = c_1 3^n + c_2 n 3^n + 3(2^n) + 7/18 (3^n) n^2$

2. $a_{n+2} - 4a_{n+1} + 3a_n = -200$, $n \geq 0$ $a_0 = 3000$, $a_1 = 3300$

Ans. $a_n^{(h)} = a_{n+2} - 4a_{n+1} + 3a_n = 0$.

$r^2 - 4r + 3 = 0$

$r = 3, 1$,

$a_n^{(h)} = c_1 3^n + c_2$.

$a_n^{(p)} = A \times$ there exist a constant in $a_n^{(h)}$

$\therefore$

$a_n^{(p)} = An$.

$A(n+2) - 4A(n+1) + 3An = -200$

$An + 2A - 4An - 4A + 3An = -200$

$-2A = -200$

$A = 100$

$a_n = c_1 3^n + c_2 + 100n$.

$a_0 = c_1 + c_2$

$c_1 + c_2 = 3000$

$c_1 = 3000 - c_2$.

$a_1 = 3c_1 + c_2 + 100$

$3300 = 3c_1 + c_2 + 100$

$3200 = 3(3000 - c_2) + c_2$.

$3200 = 9000 - 3c_2 + c_2$.

$3200 = 9000 - 2c_2$.

$2c_2 = 9000 - 3200$

$= 5800$

$c_2 = 2900$ $c_1 = 100$

$$a_n = 1003^n + 2900 + 100n$$