Module II

Algorithm:- An algorithm is a finite set of precise instructions for performing a computation or for solving a problem.

Division algorithm (one of the most important theorems in number theory).

Let a and b are any 2 integers, $b > 0$. Then there exists unique integers q and r such that

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

Proof:- Consider the infinite sequence of multiples of b, namely

$$-2b, -b, 0, b, 2b, \dots qb \dots$$

clearly a is equal to one of the multiples of b say bq in the sequence or a lies between two consecutive multiples say bq and $b(q+1)$. In either case we have $bq \leq a < b(q+1)$ for some q.

$$bq \leq a < b(q+1)$$

$$\text{i.e. } 0 \leq a - bq < b$$

Let us take $a = bq + r$, then we have,

$$a = bq + (a - bq) = bq + r, \quad 0 \leq r < b.$$

This proves the existence of two integers ~~a, b~~ q and r.

To prove the uniqueness of q & r, suppose they are not unique. Then it follows that

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

$$a = bq_1 + r_1 \quad 0 \leq r_1 < b$$

for some integer q, r, q_1, r_1.

ie $bq+r = bq_1 + r_1$

ie $bq - bq_1 = r_1 - r$

$b(q-q_1) = r_1 - r$

Hence b divides $r_1 - r$ which is a contradiction since both r and r_1 are positive and less than b. Hence $r = r_1$. Also $q = q_1$.

Therefore q and r are unique

Note: bq is the largest multiple of b, which does not exceed a, r is called the least remainder of a, when divided by b and q is called the quotient.

If $r=0$, then $a = bq$, and hence a is a multiple of b.

eg. Let $a=23$; $b=5$, then $23 = 5\times4+3$, $0<3<5$

Hence 5×4 is the largest multiple of 5, which does not exceed 23.

3 is the remainder of 23 when divided by 5; 4 is the quotient.

Note:- For integers a, b, c it is true that

(1) If a/b and a/c then $a/(b+c)$

eg. $3/6$ and $3/9$ then $3/15$.

(2). If a/b then a/bc for all integers c.

ie $5/10$ so $5/20$, $5/30$, $5/40$ . . .

(3) If a/b and b/c then a/c

eg. $4/8$ and $8/24$ then $4/24$.

Primes

A positive integer p greater than 1 is called **prime** if the only positive factors of p are 1 & p.

A positive integer p greater than 1 and is not prime is called composite.

Greatest Common Divisor (GCD)

Let a & b be integers. An integer $d (\neq 0)$ is said to be common divisor of a and b if d/a and d/b (ie d divides both a & b)

eg: ± 5 is the common divisor of 20 and 30.

If d is a common divisor of a and b, which is a multiple of every other common divisor of a & b (ie the largest of all common divisors of a & b). Then d is called the greatest common divisor of a and b, it is denoted by $gcd(a, b)$.

eg: The divisors of 12 are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$

The divisors of 16 are $\pm 1, \pm 2, \pm 4, \pm 8, \pm 16$.

The common divisors of 12 & 16 are $\pm 1, \pm 2, \pm 4$. Hence the greatest common divisor is 4.

Thus $gcd(12, 16) = 4$.

If $gcd(a, b) = 1$, then a & b are said to be relatively prime.

eg: $gcd(-2, 9) = 1$, so -2 & 9 are relatively prime.

If gcd$(a,b) = 1$, then a & b are said to be coprime, or by saying that a is prime to b.

If gcd$(a_1, a_2 \ldots a_n) = 1$ then $a_1, a_2 \ldots a_n$ are relatively prime.

We say that $a_1, a_2, \ldots a_n$ are relatively prime in pairs in case gcd$(a_i, a_j) = 1$ for all $i = 1, 2 \ldots n$ and $j = 1, 2 \ldots n$ with $i \neq j$

eg: The integers 21, 85, 92, 143 are relatively prime in pairs since,

$$\gcd(21, 85) = 1$$
$$\gcd(21, 92) = 1$$
$$\gcd(21, 143) = 1$$
$$\gcd(85, 92) = 1$$
$$\gcd(85, 143) = 1$$
$$\gcd(92, 143) = 1$$

The greatest common divisor (gcd) is also called the highest common factor (hcf)

Theorem — The GCD is unique

Proof - Let $a_1, a_2 \ldots a_k$ be the integers and let d_1 and d_2 be their two g.c.d. Then d_1 divides $a_1, a_2 \ldots a_k$ and d_2 is their g.c.d. It follows that d_1 divides d_2. Conversely it can be shown that in a similar manner that d_2 divides d_1. This implies $d_1 = d_2$; ie The GCD is unique.

The Euclidean Algorithm for Computation of GCD.

This is an efficient algorithm for finding the GCD.

Statement

If a and b are any two integers $(a > b)$, if r_1 is the remainder when a is divided by b, r_2 is the remainder when b is divided by r_1, r_3 is the remainder when r_1 is divided by r_2 and so on and if $r_{k+1} = 0$, then the last non-zero remainder r_k is the $\gcd(a, b)$.

Proof

When $a = qb + r$ where a, b, q and r are integers, we will first prove that

$\gcd(a, b) = \gcd(b, r)$

Let $d_1 = \gcd(a, b)$ — ①

and $d_2 = \gcd(b, r)$ — ②

Now, by (2), d_2 / b and d_2 / r

$\therefore d_2 / qb + r$ ie d_2 / a

Thus d_2 is a common divisor of a and b

Since d_1 is the gcd of (a, b) we have

$d_2 \leq d_1$. — ③

Now by ①, d_1 / a and d_1 / b.

ie $d_1 / (a - qb)$ ie d_1 / r

$\therefore d_1$ is a common divisor of b & r.

Since $d_2 = \gcd(b, r)$ we have $d_1 \leq d_2$ — ④

(5)

From (3) & (4) it follows that $d_1 = d_2$

$\therefore$ $gcd(a,b) = gcd(b,r)$ when $a = qb + r$. (5)

Now, since r_1 is the remainder when a is divided by b, we have $a = q_1 b + r_1$, $0 \leq r_1 < b$.

Similarly by the given data,

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

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

$$- - - \qquad - - -$$

$$r_{k-2} = q_k r_{k-1} + r_k \qquad 0 \leq r_k < r_{k-1}$$

$$r_{k-1} = q_{k+1} r_k + r_{k+1} \qquad 0 \leq r_{k+1} < r_k.$$

and since $r_1, r_2, r_3 \ldots$ form a decreasing set of non-negative integers, there must exist an r_{k+1} equal to zero.

Now by (5) proved above,

$$gcd(a,b) = gcd(b, r_1) = gcd(r_1, r_2) = \cdots$$

$$= gcd(r_{k-1}, r_k) = gcd(r_k, 0) = r_k$$

Hence $gcd(a,b) = r_k$, which is the last non-zero remainder.

eg: find the $gcd(1575, 231)$ by using Euclid algorithm.

$$1575 = 6 \times 231 + 189$$

$$231 = 1 \times 189 + 42$$

$$189 = 4 \times 42 + 21$$

$$42 = 2 \times 21 + 0.$$

$$\begin{array}{r} 4 \\ 42 \overline{)189} \\ 168 \\ \hline 21 \end{array} \qquad \begin{array}{r} 6 \\ 231 \overline{)1575} \\ 1386 \\ \hline 189 \end{array} \qquad \begin{array}{r} 1 \\ 189 \overline{)231} \\ 189 \\ \hline 42 \end{array}$$

Since the last non-zero remainder is 21,

$\gcd(1575, 231) = 21$

Note - $\gcd(a,b)$ can be expressed as an integral linear combination of a & b

ie $\gcd(a,b) = ma + nb$, where m & n are integers.

Prob ① Find the gcd of 2406 and 654

By applying division algorithm repeatedly

$$2406 = 3 \times 654 + 444$$

$$654 = 1 \times 444 + 210$$

$$444 = 2 \times 210 + 24$$

$$210 = 8 \times 24 + 18$$

$$24 = 1 \times 18 + 6$$

$$18 = 3 \times 6 + 0$$

Since the last nonzero remainder is 6,

$\gcd(2406, 654) = 6$

Prob ② Find the $\gcd(12378, 3054)$

$$12378 = 4 \times 3054 + 162$$

$$3054 = 18 \times 162 + 138$$

$$162 = 1 \times 138 + 24$$

$$138 = 5 \times 24 + 18$$

$$24 = 1 \times 18 + 6$$

$$18 = 3 \times 6 + 0.$$

The last non-zero integer is 6.

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

Using Euclidean algorithm,

HW① find the gcd of 595 and 252

② find gcd(7469, 2464)

③ gcd(272, 1479)

Some basic Properties of gcd

1. If c divides ab & gcd (a, c) = 1, then c divides b.

Since gcd (a, c) = 1, then there exists integers x & y such that $ax + cy = 1$.

Multiplying by b, we have,

$abx + bcy = b$.

Now c divides ab. Therefore c divides abx.

Also c divides bcy.

~~So~~ so c divides $abx + bcy$ which is ~~eq~~ b.

So c divides b.

2. If gcd(a, b) = 1 & gcd (a, c) = 1, then gcd(a, bc) = 1

3. Let k be any integer and a, b any integers at least one of which is non-zero,

Then gcd (ka, kb) = |k| gcd (a, b)

4. If gcd (a, b) = d then gcd (a/d, ~~b~~ b/d) = 1

5. If gcd (a, b) = 1, then for any c, gcd (ac, b) = gcd (c, b)

6. If $a_1, a_2 \ldots a_n$ are all relatively prime to b, then their product $a_1 \cdot a_2 \cdots a_n$ is also prime to b.

Factorization of primes

Fundamental theorem of arithmetic.

Every positive integer $n > 1$ can be expressed as a product of primes.

Apart from the order in which prime factors occur in the product, they are unique.

ie $n > 1$ can be written uniquely as $p_1 p_2 \dots p_n$ where $p_1 < p_2 < \dots < p_n$ are distinct primes that divide n.

The unique expression for the integer $n (\geq 2)$ as a product of primes is called the prime factorization or the prime decomposition of n.

eg: The prime factorization of 81, 100 & 289 are

$$81 = 3 \times 3 \times 3 \times 3 = 3^4$$

$$100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$$

$$289 = 17 \times 17 = 17^2$$

Let $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ and $n = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$

then $\gcd(m, n) = \prod p^{\min(a,b)}$

where $\min(a, b)$ represents the minimum of the 2 numbers a & b.

eg: Use prime factorization to find the gcd of 12 & 30.

Prime factorization of 12 & 130 are

$12 = 2^2 \times 3^1 \times 5^0$ and $30 = 2^1 \times 3^1 \times 5^1$

Hence $\gcd(12, 30) = 2^{\min(2,1)} \times 3^{\min(1,1)} \times 5^{\min(1,0)}$

$= 2^1 \times 3^1 \times 5^0 = 2 \times 3 = 6$

Theorem

The number of primes is infinite

Let us assume that the number of primes be finite and be equal to n. Let them be arranged in the order of magnitudes as

$p_1, p_2, p_3, \ldots p_n$.

Let the product $p_1 \cdot p_2 \cdot p_3 \cdot \times \ldots p_n = c$ and let us consider the integer $(c+1)$.

Since no one of the p's is a divisor of $(c+1)$, we conclude that either $(c+1)$ is a prime $> p_n$ or has a prime $> p_n$ as a factor.

But this is a contradiction to our assumption that p_n is the greatest prime.

Therefore the number of primes is infinite

Prime testing

If n has only few decimal digits, then one can show that it is prime by trial divisions up to square root.

if n is composite then it must have a prime divisor less than $\sqrt{n}$. This is based on the following theorem.

Theorem

If $n > 1$, be a composite integer, then there exists a prime p such that p/n (ie n has a prime divisor p) and $p \leq \sqrt{n}$.

Prob Show that 47 is a prime.

Take $n = 47$

Since $6 < \sqrt{47} < 7$, 2, 3 & 5 are the primes less than or equal to 6. But 47 is not

(10)

divisible by 2, 3, 5.

Therefore 47 must be a prime.

To express gcd(x, y) = d in the form $d = ax + by$.

Euclid's algorithm can be extended to express gcd(x, y) = d in the form $d = ax + by$ where $x, y \in \mathbb{Z}$ as follows.

$$r_n = r_{n-2} + (-q_n) r_{n-1}$$
$$= r_{n-2} + [r_{n-3} + r_{n-2}(-q_{n-1})](-q_n)$$
$$= r_{n-3}(-q_n) + r_{n-2}(1 + q_{n-1} q_n)$$

Now we substitute $r_{n-4} + r_{n-3}(-q_{n-2})$ for r_{n-2}.

Repeat this back substitution process until we reach $r_n = ax + by$ for some integers x & y.

Consider the problem.

Find the gcd of 595 and 252 and express it in the form $252m + 595n$

Applying division algorithm repeatedly, we have

$$595 = 2 \times 252 + 91$$
$$252 = 2 \times 91 + 70$$
$$91 = 1 \times 70 + 21$$
$$70 = 3 \times 21 + 7$$
$$21 = 3 \times 7 + 0$$

Since the last non-zero remainder is 7

gcd (595, 252) = 7

Now find m & n such that

$$7 = 252m + 595n.$$

To find m & n it is convenient to begin with the last non zero remainder.

$$7 = 70 - 3 \times 21$$
$$= 70 - 3(91 - 1 \times 70)$$
$$= 4 \times 70 - 3 \times 91$$
$$= 4 \times (252 - 2 \times 91) - 3 \times 91$$
$$= -11 \times 91 + 4 \times 252$$
$$= -11(595 - 2 \times 252) + 4 \times 252$$
$$= 26 \times 252 + -11 \times 595$$

$m = 26$ & $n = -11$

Diophantine equation

The simplest linear Diophantine equation takes the form $ax + by = c$, where a, b and c are given integers.

The solutions are described by the following theorem

This Diophantine equation has a solution (where x & y are integers) if and only if c is a multiple of the greatest common divisor of a & b.

Prob (1) Find the integers x & y such that $71x - 50y = 1$

$$71 = 1 \times 50 + 21$$
$$50 = 2 \times 21 + 8$$
$$21 = 2 \times 8 + 5$$
$$8 = 1 \times 5 + 3$$
$$5 = 1 \times 3 + 2$$
$$3 = 1 \times 2 + 1$$
$$2 = 1 \times 1 + 1$$
$$1 = 1 \times 1 + 0 \; ; \quad \gcd(71, 50) = 1$$

Thus

$$
\begin{aligned}
1 &= 2 - 1\times 1 = 2 - 1\times(3 - 1\times 2) \\
&\cancel{= 2 - 1\times 1} \\
&= 2\times 2 - 1\times 3 \\
&= 2\times(5 - 1\times 3) - 1\times 3 \\
&= 2\times 5 - 3\times 3 \\
&= 2\times 5 - 3\,(8 - 1\times 5) \\
&= 5\times 5 - 3\times 8 \\
&= 5\,(21 - 2\times 8) - 3\times 8 \\
&= 5\times 21 - 13\times 8 \\
&= 5\times 21 - 13\times(50 - 2\times 21) \\
&= 31\times 21 - 13\times 50 \\
&= 31\times(71 - 1\times 50) - 13\times 50 \\
&= 31\times 71 - 44\times 50.
\end{aligned}
$$

Hence $x = 31$ & $y = 44$

Prob(2) Solve the linear Diophantine equation,

$$172x + 20y = 1000$$

Applying Euclidean algorithm to find the $\gcd(172, 20)$. we have,

$$
\begin{aligned}
172 &= 8\times 20 + 12 \\
20 &= 1\times 12 + 8 \\
12 &= 1\times 8 + 4 \\
8 &= 2\times 4 + 0
\end{aligned}
$$

So $\gcd(172, 20) = 4$

Since 4 divides 1000, a solution to this equation exists.

To obtain the integer 4 as a linear combination of 172 and 20, working backward through the previous calculations, as follows.

$$4 = 12 - 1\times 8$$
$$= 12 - 1\times(20 - 1\times 12)$$
$$= 2\times 12 - 20$$
$$= 2\times(172 - 8\times 20) - 20$$
$$= 2\times 172 + (-17)\times 20$$

By multiplying this equation by 250, we have,

$$1000 = 250\times 4 = 250\left[2\times 172 + (-17)\times 20\right]$$
$$= 500\times 172 + -4250\times 20.$$

So $x = 500$ & $y = -4250$

is one solution to the Diophantine equation

H.W ① Solve the following linear Diophantine equations,

(i) $512x + 320y = 64$

(ii) $423x + 198y = 9$

(iii) $93x - 81y = 3$.

(iv) $256x + 116y = 2$.