GREATEST COMMON DIVISOR

View the lecture on YouTube: https://youtu.be/IfLqUhTNQ3c

Greatest Common Divisor (GCD)

The greatest common divisor (GCD) of two integers a and b, not both zero, is the largest positive integer that divides both a and b; it is denoted by (a, b). For example, (12, 18) = 6, (12, 25) = 1, (11, 19) = 1, (−15, 25) = 5, and (3, 0) = 3.

Important Results

A positive integer d is the gcd of two positive integers a and b, if

(i) $d|a$ and $d|b$.

(ii) If $c|a$ and $c|b$ then $c|d$, where c is the positive integer .

Theorem 1: The GCD of positive integers a and b is the linear combination with respect to a and b.

Proof:

Let $S = \{xa + yb / xa + yb > 0, x, y \epsilon Z\}$.

For $x = 1$ and $y = 0$, $S = a \Rightarrow S$ is non empty.

Therefore by well ordering principle, let S has the least positive integer d.

$d = la + mb$ for some positive integers l and m.

To Prove: $d = gcd(a, b)$.

Since $d > 0$, by the division algorithm a and d, there exist an integers q and r such that

$$a = qd + r, \qquad 0 \le r < d \qquad (1)$$

$$r = a - qd$$

$$= a - q(la + mb)$$

$$= (1 - ql)a + (-qm)b.$$

This shows r is the linear combination of a and b.

If $r \neq 0,$ then $r > 0,$ and so $r \epsilon S$. Further $r < d$.

Which is a contradiction that d is the least positive integer of S.

Put $r = 0,$ in equation (1), so $a = qd \Rightarrow d|a$.

similarly we can prove that $d|b$.

Thus, d is the common divisor of a and b.

Hence $d = gcd(a, b)$.

Theorem 2: Prove that two positive integers a and b are relatively prime iff there exist an integers α and β such that $\alpha a + \beta b = 1$.

Proof:

If a and b are relatively prime then $(a, b) = 1$.

we know that, there exist an integers α and β such that $\alpha a + \beta b = 1$.

Conversely, let $\alpha a + \beta b = 1$.

To Prove: (a, b)=1.

If $d = gcd(a, b),$ then $d|a$ and $d|b$.

$\Rightarrow \quad d|\ \alpha a + \beta b$

$\Rightarrow \quad d|1$

$\therefore \quad (a, b)$=1 $\Rightarrow$ a and b are relatively prime.

Theorem 3: If $a|c$ and $b|c$ and (a, b)=1, then prove that $ab|c$.

Proof:

Given: $a|c$ and $b|c$

$\therefore \quad c = ma$ and $c = nb$.

Also given that (a, b)=1. $\Rightarrow \alpha a + \beta b = 1$, for some integers α and β.

$$\alpha ac + \beta bc = c$$

$$\alpha a(nb) + \beta b(ma) = c$$

$$(\alpha n + \beta m)ab = c$$

$$\Rightarrow \quad ab|c.$$

Theorem 4: Prove that $(a, a-b) = 1 \; iff \; (a.b) = 1$.

Proof:

Let $(a.b)$=1.

To Prove: $(a, a-b) = 1$.

$\exists$ an integer l and m such that $la + mb = 1$.

$\Rightarrow \quad la + ma + mb - ma = 1$

$\Rightarrow \quad (l+m)a - m(a-b) = 1$.

$\Rightarrow \quad (l+m)a + (-m)(a-b) = 1$.

$\therefore (a, a-b) = 1$.

Conversely,

Let $(a, a-b) = 1$.

To Prove: $(a.b)$=1.

$\exists$ an integer α and β such that

$\alpha a + \beta(a-b) = 1$.

$(\alpha+\beta)a + (-\beta)b = 1$.

Therefore, $(a.b)$=1.

The Euclidean Algorithm

Suppose a and b are positive integers $a \geq b$.

If $a = b$, then (a, b) =(a, a)=a.

So, assume $a > b$

Then by successive application of division algorithm, we have

$a = q_1 b + r_1, \quad 0 \leq r_1 \leq d$

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

$\vdots$

r_{n-1}=$q_{n+1}\, r_n$+0

The sequence of remainders terminate with remainder 0.

Thus, (a, b)=r_n, where r_n is the non zero remainder.

Example 1: Evaluate (2076,1776) or Find the GCD of 2076 and 1776.

Solution:

Apply the division algorithm with 2076 (the larger of the two numbers) as the dividend and 1776 as the divisor. Applying the division algorithm successively, continue this procedure until a zero remainder is reached.

$$2076 = 1 \,.\, 1776 + 300$$

$$1776 = 5 \,.\, 300 + 276$$

$$300 = 1 \,.\, 276 + 24$$

$$276 = 11 \,.\, 24 + 12$$

$$24 = 2 \,.\, 12 + 0$$

$\therefore$ (2076, 1776) = 12.

Example 2: Using the Euclidean algorithm, express (4076, 1024) as a linear combination of 4076 and 1024.

Solution:

By applying the division algorithm successively,

$$4076 = 3(1024)+1004$$

$$1024 = 1(1004)+ 20$$

$$1004 = 50(20)+ 4$$

$$20 = 5(4)+ 0$$

The last non zero remainder is 4.

$\therefore$ (4076, 1024) = 4.

Using the above equations in reverse order, we can express the gcd(4076, 1024)=4 as a linear combination of 1024 and 4076.

$$4 = 1004 - 50 \cdot 20$$

$$= 1004 - 50(1024 - 1 \cdot 1004) \text{ (substitute for 20)}$$

$$= 51 \cdot 1004 - 50 \cdot 1024$$

$$= 51(4076 - 3 \cdot 1024) - 50 \cdot 1024 \text{ (substitute for 1004)}$$

$$= 51 \cdot 4076 + (-203) \cdot 1024$$

∴ The gcd 4 is the linear combination of the numbers 1024 and 4076.

Example 3: Apply Euclidean algorithm to express the gcd of 1976 and 1776 as a linear combination of them.

Solution:

Applying the division algorithm successively, we get

$$1976 = 1(1776)+200$$

$$1776 = 8(200)+176$$

$$200 = 1(176)+ 24$$

$$176 = 7(24)+ 8$$

$$24 = 3(8)+ 0$$

The last non zero remainder is 8.

∴ gcd(1976,1776)=8.

Now we shall express (1976,1776)= 8 as a linear combination of 1976 and 1776.

.

8 = 176 – 7(24)

= 176 – 7(200 - 1(176))

= 8(176) – 7(200)

= 8(1776 - 8(200)) - 7(200)

= 8(1776) – 71(200)

= 8(1776) – 71(1976 – 1(1776))

= 79(1776) – 71(1976)

= 79(1776)+ (-71) (1976).

∴ The gcd is the linear combination of the numbers 1776 and 1976.

Theorem: (The Euclid's Lemma)

Statement: If p is a prime and $p|ab$, then $p|a$ or $p|b$.

Proof:

Given that p is a prime.

To Prove that either $p|a$ or $p|b$.

Suppose p is not a factor of a.

Then p and a are relatively prime, (p, a)=1

there are integers α and β such that $\alpha p + \beta a = 1$.

Multiply both sides of this equation by b, we get $\alpha pb + \beta ab = 1$.

Since $p|\ p$ and $p\ |\ ab \ \Rightarrow \ p|\ \alpha pb + \beta ab$.

$\therefore p|(\alpha p + \beta a)b \Rightarrow \ p|b$. (since $\alpha p + \beta a = 1$.)

FUNDAMENTAL THEOREM OF ARITHMETIC

Theorem: (The Fundamental theorem of Arithmetic)

Statement:

Every integer n ≥ 2 either is a prime or can be expressed as a product of primes. The factorization into primes is unique except for the order of the factors.

Proof:

First, we will show by strong induction that n either is a prime or can be expressed as a product of primes. Then we will establish the uniqueness of such a factorization.

Let P(n) denote the statement that n is a prime or can be expressed as a product of primes.

To show that P(n) is true for every integer n ≥ 2.

Since 2 is a prime, clearly P(2) is true.

Now assume P(2),P(3),...,P(k) are true; that is, every integer ≥ 2 through k either is a prime or can be expressed as a product of primes.

If k + 1 is a prime, then P(k + 1) is true.

Suppose k + 1 is composite.

Then k + 1 = ab for some integers a and b, where 1 < a, b< k + 1.

By the inductive hypothesis, a and b either are primes or can be expressed as products of primes.

In any event, k +1 = ab can be expressed as a product of primes.

Thus, P(k +1) is also true. Thus, by strong induction, the result holds for every integer n ≥ 2.

.