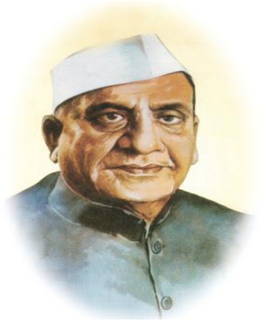

Mahatma Fule Arts, Commerce, and Sitaramji Chaudhari Science Mahavidyalaya, Warud

Department of Mathematics

Topic: Extended Euclidian Algorithm

Dr. R. S. Wadbude
Associate Professor

Greatest common divisor

Definition: The greatest common divisor of two non zero integer a and b is the largest common divisor of a and b .we denote this integer by gcd(a, b).

A greatest common divisor of two integer a and b is a positive integer d such that

i). $d \mid a$ and $d \mid b$
ii). if, for an integer c, $c \mid a$ and $c \mid b$, then $c \mid d$

GCD of a and b denoted by $(a, b) = d$

Example:

i) $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12$ are common divisors of 24 and 60

ii) 12 is the greatest common divisor of 24 and 60. i.e. $12 = (24, 60)$

Well ordering principle:
Every non empty set of positive integers contains a smallest member.

Extended Euclidian Algorithm/GCD is a Linear combination

Theorem:

For any non zero integers a and b, there exist integers s and t such that gcd(a, b) = as + bt .

Moreover, gcd (a, b) is the smallest positive integer of the form as + bt.

Proof:

Consider the set S = { am + bn : m, n are integers and am + bn >0}. Since S is non empty set, the well ordering principle asserts that S has a smallest member, say member is d such that d = as + bt. We claim that d = (a, b).

By DAT for a and b, $a = dq + r$, where $0 \le r < d$.

If $r > 0$, then $r = a - dq = a - (as + bt)q = a - asq - btq = a(1 - sq) + b(-tq) \in S$, but $r<d$

This is contradicting the fact that d is a smallest member of S. So r = 0.

Then $a = dq \Rightarrow d \mid a$. analogously $d \mid b$. This proves that d is a common divisor of a and b.

Now suppose that d' is another divisor of a and b i.e. $d' | a$ and $d' | b$

$\Rightarrow a = d' h$ and $b = d' k$ for some $h, k \in Z$. then

$d = as + bt = (d' h)s + (d' k)t = d'(hs + kt)$,

so that , d' is a divisor of d.

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

Theorem: If $a, b \in I$, $b \neq 0$ and $a = bq + r$, where $0 \leq r < b$, then $(a, b) = (b, r)$.

Proof: let $(a, b) = c$ and $(b, r) = d$. Now $(a, b) = c \Rightarrow c \mid a$ and $c \mid b \Rightarrow c \mid (a - bq)$

Then $c \mid r$ $(r = a - bq)$

Hence we have $c \mid b$ and $c \mid r$ i.e. c is a common divisor of both b and r.

therefore $c \leq (b, r) \Rightarrow c \leq d$ ….1

Similarly $(b, r) = d \Rightarrow d \mid b$ and $b \mid r \Rightarrow c \mid (bq + r)$

Then $d \mid a$

Thus $d \mid a$ and $d \mid b$ i.e. d is a common divisor of both a and b.

therefore $d \leq (a, b) \Rightarrow d \leq c$ …2

$\Rightarrow c = d$ i.e. $(a, b) = (b, r)$

The Euclidian algorithm

Theorem: Let $a = r_0$ and $b = r_1$ be positive integers. If the division algorithm is successively Applied to obtain

$$\mathbf{r_i = r_{i+1} q_{i+1} + r_{i+2} \quad \text{with } 0 \leq r_{i+2} < r_{i+1}} \quad i = 1, 2, 3, \ldots n-1 \qquad \ldots\ldots..1$$

and $r_{n+1} = 0$, Then $(a, b) = r_n$; the last non zero integer.

Proof: Let $a = r_0$ and $b = r_1$ be positive integers with $a > b$. Now put $i = 1, 2, 3, \ldots n-1$ till the remainder becomes zero. We can tabulate the result as follow

$$r_0 = r_1 q_1 + r_2 \qquad 0 \leq r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3 \qquad 0 \leq r_3 < r_2$$

$$r_2 = r_3 q_3 + r_4 \qquad 0 \leq r_4 < r_3$$

. . . . . .

. . . . . .

.

$$r_{n-2} = r_{n-1} q_{n-1} + r_n \qquad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_n q_n + r_{n+1} \qquad (r_{n+1} = 0)$$

Example: Find the GCD of 26 and 118 and express it in the form 26s + 118 t.

Solution:

By Euclidean algorithm, we have

118 = 26. 4 + 14

26 = 14. 1 + 12

14 = 12.1+ **2**

12 = 6. 2 + 0

Hence **(26, 118) = 2**

Now from the last but one equation i.e. $d = as + bt$

$$
\begin{aligned}
2 &= 14 - 12.1 \\
&= 14 - [26 - 14.1].1 \\
&= 14 - 26.1 + 14.1 \\
&= [118 - 26.4\ ].2 - 26.1 \\
&= 118.2 - 26.8 - 26.\ 1 \\
&= 118.2 - 26.9 \\
&= 118.(2) + 26.(-\ 9)
\end{aligned}
$$

Therefore **$s = 2$ and $t = -9$**

by previous theorem each of the above equation ,we get

$$(r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots\ldots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

therefore $(a, b) = r_n,$ where $r_0 = a$ and $r_1 = b$.

Example: Find the GCD of 427 and 616 and express it in the form 427 s + 616 t.

Solution:

By Euclidean algorithm, we have

616 = 427. 1 + 189

427 = 189. 2 + 49

189 = 49. 3 + 42

49 = 42. 1 + **7**

42 = 7.6 + 0

Hence **(427, 616) = 7**

Now from the last but one equation i.e. $d = as + bt$

$$7 = 49 + 42.1$$

$$= 49 – [189 – (49).3].1$$

$$= (49).4 – 189.1$$

$$= [427 – (189).2].4 – 189.1$$

$$= (427).4 –(189).9$$

$$= (427).4 – [616 – (427).1].9$$

$$\mathbf{7 = 427.13 + 161. (-9)}$$

Therefore $s = 13$ and $t = -9$

References

- Joseph. A. Gallian
  Contemporary Abstract Algebra
  Narosa publising House New Delhi IV edition
- Burton D.M.
  Elementary Number theory
  Universal book stall, New Delhi, II Edition 2003
- A. R. Vasishtha
  Dept. of Mathematics, Meerut
  Krushna Prakaskan mandir
- T. M. Karade
  Elemetary Number theory
  Sonu- Nilu Publication Nagpur

THANK YOU