Bharathidasan University
Tiruchirappalli - 620 024
Tamil Nadu, India

Programme: M.Sc., Mathematics

Course Title :Theory of Numbers
COurse Code : 21M04CC

Bezout's Identity

Dr. V. Piramanantham
Professor
Department of Mathematics

GCD g is the gcd of a & b if

(1) $g \mid a$ & $g \mid b$

(2) If $d \mid a$ & $d \mid b$, $d \leq g$.

Property: For any, nonzero integer m

$$a \mid b \iff ma \mid mb.$$

Proof of the property:

$a \mid b \Rightarrow \exists\, x \in \mathbb{Z}$ s.t. $b = ax$

$$\Rightarrow \quad mb = max$$

$$\Rightarrow \quad ma \mid mb$$

Conversely

$$ma \mid mb$$

$$\Rightarrow \exists\, y \in \mathbb{Z} \text{ s.t. } \quad mb = may$$

cancelling m from both sides

$$\Rightarrow \quad b = ay$$

$$\Rightarrow a \mid b$$

$a \mid b \iff ma \mid mb$ for any $m > 0$

Recall

$$\left\{ \begin{array}{l} d \mid a \ \& \ d \mid b \\ \Rightarrow \quad d \mid ax+by \Rightarrow d \le ax+by \end{array} \right.$$

$d > 0$

$ax+by > 0$

smallest

$\{A = \{ax+by \mid \text{for all integers } x \ \& \ y\}$ $\quad ax+by \geq 0$

$g = (a,b) > 0 \rightarrow$

d is a common divisor

$$\left. \begin{array}{l} g \mid ax+by \\ d \mid ax+by \end{array} \right\} \Rightarrow$$

$g \le ax+by$

$g = ax+by$

$g < ax+by$

Bezout's identity

Let a & b be given integers, not both zero. Then if g is the greatest common divisor of a and b, then there exist integers x_0 and y_0 such that

$$g = ax_0 + by_0$$

(ie) gcd of a & b can be expressed as a integer-linear combination of a and b.

Proof of Bezout's identity

Consider the set A of integers:

$$A = \{ax+by \,/\, x, y \in \mathbb{Z}\}$$

For the choice $x=0$ & $y=0$, $ax+by = 0 \in A$

So, A is nonempty set.

By well-ordering principle,

A has a smallest +ve integer ax_0+by_0 for some $x_0, y_0 \in \mathbb{Z}$

put $g = ax_0 + by_0$. Then

g is the smallest element of

A (a)

$$g \leq ax+by \quad \forall\, x, y \in \mathbb{Z}$$

with $ax+by > 0$

Clearly g is a +ve integer.

We show that g is the gcd of a & b

① g is a common divisor of a & b

By division Algorithm on a & g,

$\exists\ q$ & $r \in \mathbb{Z}$ such that

$$a = q \cdot g + r, \quad 0 \le r < g.$$

If $r = 0$, $g \mid a$

$r \neq 0$, $g \nmid a$

Suppose $r \neq 0$.

Then $\boxed{0 < r < g}$

and
$$r = a - q \cdot g$$
$$= a - q \cdot (ax_0 + by_0)$$
$$= (1 - qx_0)\, a + (-y_0)\, b$$

$\Rightarrow$ r is in the form $ax + by$

so $\boxed{r \in A}$

which contradicts to the fact that g is the smallest +ve integer in A.

$\therefore\ r = 0$

$\&\ g \mid a$

$|||^{ly}$ we can show that $g \mid b$.

g is a positive common divisor of a & b.

Next we prove that g is the greatest common divisor of a and b.

Let l be a +ve common divisor of a and b.

(i.e) $l \mid a$ & $l \mid b$

$$l \mid ax+by \quad \text{for any} \quad x, y \in \mathbb{Z}$$

In particular,

$$l \mid ax_0+by_0$$

$$\Rightarrow l \mid g \quad \text{———} \quad (*)$$

Since $l > 0$, $g > 0$,

$$l \leq g$$

$\therefore g$ is the greatest common divisor of a and b.

If $g=(a,b)$, $\exists\ x_0\ \&\ y_0 \in \mathbb{Z}$

s.t. $g = ax_0 + by_0$

(*) Say that any +ve common divisor of a and b is a divisor of the greatest common divisor of a and b.

Suppose that $g=(a,b)$. If $d|a$, $d|b$ then $d|g$.

Corollary: (Characterization of gcd)

① The gcd of a and b is the smallest +ve integer in the form

$$ax+by$$

② Any common divisor of a & b is a divisor of greatest common divisor of a & b.

Result: For any +ve int m,

$$(ma, mb) = m(a, b).$$

Proof of Result

$$\text{Let } g = (ma, mb)$$

$$d = (a, b)$$

To prove that $(ma, mb) = m(a, b)$, we prove that

$$g = md.$$

Since $d \mid a$ & $d \mid b$

$\Rightarrow md \mid ma \;\&\; md \mid mb$

$\Rightarrow md$ is a common divis[or] of ma & mb

By corollary (2)

Any +ve common divisor of a & b is a divisor of gcd of a & b.

$\Rightarrow md \mid g$

$\exists\, y \in \mathbb{Z}$ s.t. $g = mdy \Rightarrow y \geq$ [1]

claim: $y = 1$.

$mdy \mid ma \;\&\; mdy \mid mb$

$\Rightarrow \quad dy \mid a \quad \& \quad dy \mid b$

$\Rightarrow$ dy is a common divisor of a & b

Since $d = (a,b)$, $\quad dy \le d$

$\Rightarrow \quad y \le 1$

$0 < y \le 1$

$\Rightarrow y = 1$

$\therefore \; g = md$

Corollary: If $d|a$ & $d|b$ & $d>0$, then

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}$$

If $g=(a,b)$, then $\left(\frac{a}{g}, \frac{b}{g}\right)=1$

Proof $m>0$, $(ma, mb) = m(a,b)$

$m=d$, $a \Rightarrow a/d$ $b \Leftarrow\Rightarrow b/d$

$$\left(d\cdot\frac{a}{d}, d\cdot\frac{b}{d}\right) = d\left(\frac{a}{d}, \frac{b}{d}\right)$$

$$\Rightarrow (a, b) = d\left(\frac{a}{d}, \frac{b}{d}\right)$$

$$\Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}.$$

If $g = (a,b)$, $\left(\frac{a}{g}, \frac{b}{g}\right) = \frac{(a,b)}{g} = 1$

$$\therefore \left(\frac{a}{g}, \frac{b}{g}\right) = 1$$

$a = 18$, $b = 24$. , $g = (18, 24) = 6$

$$6 = 18x_0 + 24y_0$$

suitable $x_0 = -1$, $y_0 = 1$

There is no method available (in the proof of Bezout's identity) to find x_0 & y_0

Note: Suppose that $a_1, a_2, \ldots, a_n$ are given integers, not all a's zero. Then if $g = (a_1, a_2, \ldots, a_n)$, then there exists integers $x_1, x_2, \ldots, x_n$ such that

$$g = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$$

$n=2$, $a_1 = a$, $b_1 = b$

Corollary: If $d \mid a$ & $d \mid b$

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}.$$

In particular if $g = (a, b)$, then

$$\left(\frac{a}{g}, \frac{b}{g}\right) = 1.$$

Theorem: Suppose that $(a, b) = 1$. Then

$\exists\ x_0$ & $y_0 \in \mathbb{Z}$ s.t.

$$a x_0 + b y_0 = 1$$

It follows from Bezout's identity.

Converse: Suppose that there exist two integer x & y such that

$$ax + by = 1$$

Then $(a, b) = 1$.

Cor: 1 g = smallest +ve int in form $ax+by$

Suppose that a +ve integer $d = ax+by$

for some integers x & y, then
d need not be the gcd of a & b.

Definition Let a & b be integers.
Then if the gcd of a and b is 1
then a & b are called relatively
prime integers (or) a & b are coprimes
(or) a is coprime to b.

Result: If $(a, m) = 1$ & $(b, m) = 1$, then

$$(ab, m) = 1.$$

Proof:

$(a, m) = 1$ $\quad \exists\; x_1 \;\&\; y_1 \in \mathbb{Z}$ s.t.

$$a x_1 + m y_1 = 1 \qquad \text{--- (1)}$$

$(b, m) = 1 \Rightarrow \exists\; x_2, y_2 \in \mathbb{Z}$ s.t.

$$b x_2 + m y_2 = 1 \qquad \text{--- (2)}$$

$(ab, m) = 1$

$abx + my = 1$

From ① & ②,

$$ax_1 = 1 - my_1$$

$$bx_2 = 1 - my_2$$

$$abx_1x_2 = (ax_1)(bx_2)$$

$$= (1 - my_1)(1 - my_2)$$

$$= 1 - my_1 - my_2 + m^2y_1y_2$$

$$abx_1x_2 = 1 - m(y_1 + y_2 - my_1y_2)$$

$$\Rightarrow ab(x_1 x_2) + m(y_1 + y_2 - m y_1 y_2) = 1$$

put. $x_0 = x_1 x_2$ & $y_0 = y_1 + y_2 - m y_1 y_2$.

$$(ab) x_0 + m y_0 = 1$$

$$\Rightarrow (ab, m) = 1 \quad //$$

$$g = a x_0 + b y_0$$

we could not find x_0 & y_0

Theorem: Let a, b be two integers, not both zero. Then

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

(2) $(a, b) = (a, b + ax)$ for any integer x.

Proof (i) Trivial

$(a, b+ax) = (a, b)$