

18.781

7 Feb 2003

Def. An integer a is a common divisor of b and c if $a|b$ and $a|c$

The greatest common divisor exists and is denoted (b, c) .

Thrm. The number (b, c) can be characterized as follows:

- 1) It is the least positive value of $bx+cy$, x, y integers.
- 2) It is the unique common divisor of b and c divisible by every other common divisor.

Proof:

- 1) Consider $\{bx+cy\}$. Set of integers, has smallest pos. elt.

Let $l = bx_0 + cy_0$ be this smallest elt.

l divides b & c . Enough to show $l|b$, $l|c$ is the same.

$$b = lq + r \quad 0 \leq r < l \quad \text{by division with remainder.}$$

If $l \nmid b$, then $0 < r < l$

$$r = b - lq = b - (bx_0 + cy_0)q = b(1 - x_0q) + c(y_0q),$$

so $r \in \{bx+cy\}$ and $r < l$; contradicts minimality of l .

$$l|b, l|c \Rightarrow l \leq (b, c) = g.$$

Show $g \leq l$

$$b = gB \quad c = gC \quad (B, C \text{ integers})$$

$$l = gBx_0 + gCy_0 = g(Bx_0 + Cy_0) \Rightarrow g|l \Rightarrow g \leq l$$

- 2) Suppose d is common divisor of b, c .

$$b = Bd \quad c = Cd$$

$$(b, c) = bx_0 + cy_0 \quad (\text{part 1})$$

$$= Bdx_0 + Cdy_0 = d(Bx_0 + Cy_0) \Rightarrow d|(b, c)$$

uniqueness:

if $g \neq (b, c)$, $g|b, g|c$, then $g < (b, c)$, so $(b, c) \nmid g$.

Cor. For every $m > 0$, $m(b, c) = (mb, mc)$

Proof: $(mb, mc) =$ smallest pos. elt in $\{mbx + mcy\} = m\{bx + cy\}$

\Rightarrow smallest pos. elt in $\{mbx + mcy\} = m(\text{smallest pos. elt in } \{bx + cy\})$

Cor. If $d|a, d|b, d > 0$, then $(\frac{a}{d}, \frac{b}{d}) = \frac{1}{d}(a, b)$

Proof. Special case of previous corollary.

Prop: If $(a, m) = (b, m) = 1$ then $(ab, m) = 1$

Proof: Enough to write $1 = ax_0 + my_0$, $x_0, y_0 \in \mathbb{Z}$

$$1 = ax_0 + my_0 \quad 1 = bx_1 + my_1$$

$$(ax_0)(bx_1) + (1 - my_0)(1 - my_1) = 1 - m(y_0 + y_1) + m^2 y_0 y_1$$

$$1 = abx_0 x_1 + m(y_0 + y_1 - my_0 y_1)$$

Cor: if $(a, m) = 1$, then $(ab, m) = (b, m)$

Proof: let $g = (b, m)$ $(a \frac{b}{g}, \frac{m}{g}) = 1 \Rightarrow g(a \frac{b}{g}, \frac{m}{g}) = g \Rightarrow (ab, m) = g$.

Def: Two integers a & b are relatively prime if $(a, b) = 1$

Prop: For every n , $(a, b) = (b, a) = (a, -b) = (a, b + an)$

Proof: consider set $\{ax + by\}$. This is the same as $\{bx + ay\}$,
and $\{ax + (-b)y\}$ and $\{ax + (b + an)y\} = \{a(x + ny) + by\}$

Prop: If (a, b) , and $(b, c) = 1$ then (a, c) .

Proof: $(ab, ac) = a(b, c) = a$

(a, b) and (a, c) , so by part 2 of 1st thrm, (a, c) .

Question: Given $a, b \in \mathbb{Z}$. How do we compute $g = (a, b)$ and

$$x_0, y_0 \text{ s.t. } g = ax_0 + by_0$$

Ex: $a = 7472$ $b = 2464$

$$7472 = 3 \cdot 2464 + 80$$

claim: $(2464, 80) = (7472, 2464)$

by above prop: $= (80 + 2464 \cdot 3, 2464)$

$$2464 = 30 \cdot 80 + 64 \Rightarrow (2464, 80) = (80, 64) = (64, 16) = 16$$

$$80 = 64 \cdot 1 + 16 \quad 64 = 4 \cdot 16$$

$$\therefore (7472, 2464) = 16.$$

$$16 = 80 - 1 \cdot 64 = 80 - (2464 - 30 \cdot 80) = 31 \cdot 80 - 2464 = 31 \cdot (7472 - 3 \cdot 2464) - 2464 \Rightarrow$$

$$16 = 7472 \cdot (31) + 2464 \cdot (-94).$$