

18781

10 Feb 2003

Recall: $a, b \in \mathbb{Z}$ greatest common divisor (a, b) • Equiv. characterizations of (a, b) 1) the smallest pos. integer in $\{ax+by\}$, $x, y \in \mathbb{Z}$ 2) the pos. common div. of a, b div. by every other divisor.• compute (a, b) and x_0, y_0 s.t. $(a, b) = ax_0 + by_0$ • ex: $(2689, 4001) = (2689, 1312) = (1312, 65) = (65, 12) = (12, 5) = (5, 2) = 1$

$$4001 = 1 \cdot 2689 + 1312$$

$$2689 = 2 \cdot 1312 + 65$$

$$1312 = 20 \cdot 65 + 12$$

$$65 = 5 \cdot 12 + 5$$

$$12 = 2 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$\text{Note: } (a, b+na) = (a, b)$$

$$1 = 5 - 2 \cdot 2$$

$$= 5 - 2(12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12$$

$$= 5(65 - 5 \cdot 12) - 2 \cdot 12 = 5 \cdot 65 - 27 \cdot 12$$

$$= 5 \cdot 65 - 27(1312 - 20 \cdot 65) = -27(1312) + 545 \cdot 65$$

$$= -27(1312) + 545(2689 - 2 \cdot 1312) = -1117 \cdot 1312 + 545 \cdot 2689$$

$$= -1117 \cdot 4001 + 1662 \cdot 2689 = 1$$

Thrm: Euclidean algorithm:

Given b and c , compute

$$b = cq_1 + r_1 \quad 0 < r_1 < c$$

$$c = r_1 q_2 + r_2 \quad 0 < r_2 < r_1$$

$$\vdots$$

$$r_{j-2} = r_{j-1} q_j + r_j$$

$$r_{j-1} = r_j q_{j+1}$$

Since r_i strictly decreasing & positive, eventually goes to zero:Then $r_j = (b, c)$ and you can solve for x_0, y_0 by "unscrewing" the equations, as in above example.Proof: By induction on j , # of steps to finish. $j=0$ In this case, $b = cq_1$, so $\text{g.c.d.}(b, c) = c (=r_0)$ Assume that if the Euclidean algorithm stops in $j-1$ or fewer steps.Apply thrm to c, r_1 (algorithm finishes in $j-1$ steps)

$$\Rightarrow r_j = (c, r_1) = (c, b - cq_1) = (c, b)$$

Thus, algorithm holds for finishing in j stepsDef: c is a common multiple of a and b if $a|c$ and $b|c$ The smallest common multiple is the smallest positive common multiple, written $[a, b]$

Thrm.

a) For all $m > 0$, $[ma, mb] = m \cdot [a, b]$

b) $[a, b] = \frac{|ab|}{(a, b)}$

Proof.

a) Let $H = [ma, mb]$, $h = [a, b]$

Show: $H \geq mh$ and $mh \geq H$

$mh \geq H$. Show $ma | mh$ and $mb | mh$

$$a | h, b | h \quad h = a \cdot n_a \quad h = b \cdot n_b$$

$$mh = ma n_a \quad mh = mb n_b$$

$$\Rightarrow mh = (ma) n_a \quad \text{and} \quad mh = (mb) n_b \Rightarrow ma | mh \quad \text{and} \quad mb | mh.$$

$\therefore mh \geq H$, since H is the smallest pos. numb. for which this holds.

$H \geq mh$. There exist r, s s.t. $H = ram \quad H = sbm$

$$\Rightarrow \frac{H}{m} = ra \quad \frac{H}{m} = sb \Rightarrow \frac{H}{m} \geq h, \text{ since } \frac{H}{m} \text{ comm. mult. of } a, b.$$

$$\Rightarrow H \geq mh.$$

$$\therefore mh = H.$$

b) Reduce to case when $(a, b) = 1$

$$g = (a, b)$$

$$[a, b] = g \left[\frac{a}{g}, \frac{b}{g} \right] = g \cdot \frac{|\frac{a}{g}, \frac{b}{g}|}{1} = \frac{|ab|}{g}, \text{ assuming true for } (a, b) = 1.$$

So can assume $(a, b) = 1$. Then reduces to $[a, b] = |ab|$.

$$\text{Suppose } [a, b] = m \cdot a \Rightarrow b | m \cdot a \Rightarrow b | m \Rightarrow m \geq |b| \Rightarrow ma \geq |ab|.$$

But $|ab|$ is a common mult., so by minimality, $ma = |ab|$

Def. An integer $p > 1$ is prime iff it has no divisors d with

$$1 < d < p.$$