CSE 16 2-15-22

Ex (gcd & lcm)

find gcd(30, 75), lcm(30, 75)

divisors of 30: 1, 2, 3, 5, 10, 15, 30

divisors of 75: 1, 3, 5, 15, 25, 75

common divisors: 1, 3, 5, (15)

$\therefore \gcd(30, 75) = \boxed{15}$

Pos. mult. of 30: 30, 60, 90, 120, (150), 180, ...

" " " 75: 75, (150), ...

$\therefore \operatorname{lcm}(30, 75) = \boxed{150}$

Notice: $30 \cdot 75 = 2250 = 15 \cdot 150$

Theorem

for any $a, b \in \mathbb{N}$:

$$a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$$

Lemma 1

Let $a, b \in \mathbb{N}$ and let $p_1, p_2, \ldots, p_n$ be primes. Suppose

$$a = p_1^{x_1} \cdot p_2^{x_2} \cdot \ldots \cdot p_n^{x_n}$$

and

$$b = p_1^{y_1} \cdot p_2^{y_2} \cdot \ldots \cdot p_n^{y_n}$$

for some integers $x_i \geq 0$, $y_i \geq 0$ $(1 \leq i \leq n)$.

Then $a \mid b$ $\overset{\Rightarrow}{\underset{\Leftarrow}{\text{iff}}}$ $x_i \leq y_i$ $(1 \leq i \leq n)$.

Proof.

Observe

$$b = (p_1^{x_1} p_2^{x_2} \cdots p_n^{x_n})(p_1^{y_1-x_1} p_2^{y_2-x_2} \cdots p_n^{y_n-x_n})$$

$$= a \cdot \kappa$$

where $\kappa = p_1^{y_1-x_1} p_2^{y_2-x_2} \cdots p_n^{y_n-x_n}$

($\Leftarrow$) If $x_i \le y_i$, then $y_i - x_i \ge 0$ $(1 \le i \le n)$.

Then κ is an integer, and $a \mid b$.

($\Rightarrow$) If $a \mid b$, then $b = a\kappa'$ for some $\kappa' \in \mathbb{Z}$.

But also $b = a\kappa$, $\therefore a\kappa' = a\kappa$, $\therefore \kappa' = \kappa$,

$\therefore \kappa \in \mathbb{Z}$. It follows that

$y_i - x_i \ge 0$, $\therefore x_i \le y_i$ $(1 \le i \le n)$.

∎

Lemma 2

Let $a, b \in \mathbb{N}$ and let

$$S = \{p_1, p_2, \ldots, p_n\}$$

be all primes that divide either a or b (or both). Thus

$$a = p_1^{x_1} p_2^{x_2} \cdots p_n^{x_n}$$

and

$$b = p_1^{y_1} p_2^{y_2} \cdots p_n^{y_n}$$

with $x_i \geq 0$, $y_i \geq 0$ $(1 \leq i \leq n)$. Then ...

(1) $$\gcd(a,b) = p_1^{\min(x_1,y_1)} \cdot p_2^{\min(x_2,y_2)} \cdots p_n^{\min(x_n,y_n)}$$

(2) $$\operatorname{lcm}(a,b) = p_1^{\max(x_1,y_1)} p_2^{\max(x_2,y_2)} \cdots p_n^{\max(x_n,y_n)}$$

Ex. $a = 30$, $b = 75$

$$30 = 2 \cdot 3 \cdot 5 = 2^1 \cdot 3^1 \cdot 5^1$$
$$75 = 3 \cdot 5 \cdot 5 = 2^0 \cdot 3^1 \cdot 5^2$$

$$\gcd(30,75) = 2^0 \cdot 3^1 \cdot 5^1 = 15 \quad \checkmark$$
$$\operatorname{lcm}(30,75) = 2^1 \cdot 3^1 \cdot 5^2 = 150 \quad \checkmark$$

Proof of Lemma 2

Let d = RHS of (1) and

m = RHS of (2).

Must show that d & m satisfy definitions of gcd & lcm respectively.

since $\min(x_i, y_i) \le x_i$ $(1 \le i \le n)$, lemma1 says $d \mid a$. similarly $\min(x_i, y_i) \le y_i$ $(1 \le i \le n)$ so $d \mid b$.

Now suppose $e \mid a$ and $e \mid b$. Then by lemma 1, we have

$$e = p_1^{z_1} p_2^{z_2} \cdots p_n^{z_n}$$

where $z_i \le x_i$ and $z_i \le y_i$ $(1 \le i \le n)$

Therefore $z_i \le \min(x_i, y_i)$ $(1 \le i \le n)$.

Again by lemma 1, $e \mid d$.

Hence $e \le d$, and $d = \gcd(a, b)$.

Exercise: show that m satisfies the definition of $\operatorname{lcm}(a, b)$

Proof of theorem

(*) $a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$.

As in statement of lemma 2, let

$$a = p_1^{x_1} p_2^{x_2} \cdots p_n^{x_n}$$

and

$$b = p_1^{y_1} p_2^{y_2} \cdots p_n^{y_n}.$$

Then LHS of (*) is

$$\text{LHS} = p_1^{x_1+y_1} p_2^{x_2+y_2} \cdots p_n^{x_n+y_n}$$

By lemma 2, RHS of (*) is

$$\text{RHS} = p_1^{\min(x_1,y_1)+\max(x_1,y_1)} \cdots p_n^{\min(x_n,y_n)+\max(x_n,y_n)}$$

BUT $x_i + y_i = \min(x_i, y_i) + \max(x_i, y_i)$

for $1 \le i \le n$. $\therefore$ LHS = RHS.

Better algorithm for gcd(a, b)

Ex. (Euclid's algorithm)

$\gcd(16200, 756) = \boxed{108}$.

$16200 = 21 \cdot 756 + 324$

$756 = 2 \cdot 324 + \boxed{108}$

$324 = 3 \cdot \boxed{108} + 0$ stop

In Pseudo-code

```
r = rem. of a on div. by b
while r > 0
    a = b
    b = r
    r = rem. of a on div. by b
end while
return b
```

Ex. $\gcd(136, 235) = \boxed{1}$

a		b		r
136	$=$	$0 \cdot 235$	$+$	136
235	$=$	$1 \cdot 136$	$+$	99
136	$=$	$1 \cdot 99$	$+$	37
99	$=$	$2 \cdot 37$	$+$	25
37	$=$	$1 \cdot 25$	$+$	12
25	$=$	$2 \cdot 12$	$+$	$\boxed{1}$
12	$=$	$12 \cdot \boxed{1}$	$+$	0 stop

Defn

we say $a, b \in \mathbb{Z}$ are relatively prime iff $\gcd(a,b) = 1$. Equivalently, a and b have no prime factors in common.

Goal: Prove correctness of Euclid's algorithm.

Exercise

show $d|a$ and $d|b \Rightarrow d|(a+b)$

Lemma:

let $a, d, n \in \mathbb{Z}$. Then

$$d|a \Rightarrow d|na$$

Proof:

$$\begin{aligned} d|a &\Rightarrow a = kd \quad (\text{some } k \in \mathbb{Z}) \\ &\Rightarrow na = n(kd) \\ &\Rightarrow na = (nk)d \\ &\Rightarrow d|na \quad (\text{since } nk \in \mathbb{Z}.) \end{aligned}$$

Lemma 4

Let $a, b, n, m, d \in \mathbb{Z}$. Then

$$d \mid a \wedge d \mid b \Rightarrow d \mid (na + mb)$$

Proof.

$$\left.\begin{array}{l} d \mid a \Rightarrow d \mid na \\ d \mid b \Rightarrow d \mid mb \end{array}\right\} \Rightarrow d \mid (na + mb)$$

↑ by lemma 3 ↑ by exercise

Lemma 5

Suppose $a = qb + r$ (some $q, r \in \mathbb{Z}$).

Then

$$\gcd(a, b) = \gcd(b, r)$$

Proof:

$$d|a \wedge d|b \Rightarrow d|(a-qb)=r$$

$$\Rightarrow d|b \wedge d|r$$

$a|=0$

$$d|b \wedge d|r \Rightarrow d|(qb+r)=a$$

$$\Rightarrow d|a \wedge d|b$$

$\therefore d|a \wedge d|b \iff d|b \wedge d|r$.

$\therefore \{\text{com. div. of } a,b\} = \{\text{com. div. of } b,r\}$

$\therefore \quad gcd(a,b) = gcd(b,r)$.

∎

Proof of correctness of Euclid's Alg.

The 1st division gives

$$a = qb + r \qquad (0 \le r < b)$$

Let $r_0 = a$, $q_1 = q$, $r_1 = b$, $r_2 = r$

$$r_0 = q_1 \cdot r_1 + r_2 \qquad (0 \le r_2 < r_1)$$

$$r_1 = q_2 r_2 + r_3 \qquad (0 \le r_3 < r_2)$$

$$r_2 = q_3 \cdot r_3 + r_4 \qquad (0 \le r_4 < r_3)$$

$$\vdots$$

since $r_1 > r_2 > r_3 > \cdots \ge 0$,

some $r_{n+1} = 0$.

$$\vdots$$

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

$$r_{n-1} = q_n \boxed{r_n} + 0$$

By lemma 5 :

$$\begin{aligned} \gcd(a,b) &= \gcd(r_0, r_1) \\ &= \gcd(r_1, r_2) \\ &= \gcd(r_2, r_3) \\ &\vdots \\ &= \gcd(r_{n-1}, r_n) \\ &= \gcd(r_n, 0) \\ &= r_n \end{aligned}$$

∎

Defn

Let $a, b, m \in \mathbb{Z}$, $m > 0$. We say that a and b are congruent modulo m iff

$$m \mid (a - b)$$

Notation: $a \equiv b \pmod{m}$.

Alternate notation: $a \equiv_m b$

Ex

- $10 \equiv 7 \pmod 3$ since $3 \mid (10-7)$
- $25 \equiv 11 \pmod 7$ $\because$ $7 \mid (25-11) = 14$
- $-13 \equiv 106 \pmod{17}$ $\because$ $17 \mid (-13-106) = 119$
  $= (-7)\,17$
- $18 \not\equiv 5 \pmod 4$ $\because$ $4 \nmid 18-5 = 13$