CSE 16 7-20-22

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

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

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

By lemma 2

$$\gcd(30, 75) = 2^0 \cdot 3^1 \cdot 5^1 = 15$$

$$\text{lcm}(30, 75) = 2^1 \cdot 3^1 \cdot 5^2 = 150$$

Proof of lemma 2

Let

$$d = \text{RHS of (1)}$$

and

$$m = \text{RHS of (2)}$$

we must show d, m satisfy defns. of $\gcd(a,b)$ and $\text{lcm}(a,b)$ resp.

since $\min(x_i, y_i) \leq x_i$ for $1 \leq i \leq n$, lemma 1 gives $d \mid a$. similarly, $\min(x_i, y_i) \leq y_i$ $(1 \leq i \leq n)$, 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 both $z_i \leq x_i$ and $z_i \leq y_i$ $(1 \leq i \leq n)$.

$\therefore z_i \leq \min(x_i, y_i)$ for $1 \leq i \leq n$, again by lemma 1,

$$e \mid d.$$

Hence $e \leq d$. $\therefore d = \gcd(a, b)$

Exercise

complete this proof by showing that m (i.e. the RHS of (2)) satisfies the defn. of lcm(a,b).

■

Thm

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

Proof

let

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

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

as in lemma 2. Referring to (*)

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

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

observe, for $1 \le i \le n$:

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

Therefore

$$LHS = RHS$$

of (*), as required ∎

Ex.

$a = 16,200$

$b = 756$

$\gcd(a,b) = \boxed{108}$

$\therefore \operatorname{lcm}(a,b) = \dfrac{(16200)(756)}{108} = \boxed{113,400}$

note: factoring a number is computationally intensive.

Euclid invented an efficient algorithm for $\gcd(\cdot,\cdot)$.

Ex. $\gcd(16200, 756) = 108$

$16200 = 21 \cdot 756 + 324$

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

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

In Pseudo-code:

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

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

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 and b are <u>relatively prime</u> iff $\gcd(a, b) = 1$. Equivalently, a and b have no prime-factors in common.

Goal: Prove Correctness of Euclids' algorithm.

- Exercise (hw)

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

Lemma 3

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

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

Proof:

$d|a \Rightarrow a = kd$ for some $k \in \mathbb{Z}$

$\Rightarrow na = (nk)d$

$\Rightarrow d|na$ (since $nk \in \mathbb{Z}$).

■

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:

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

$d \mid a \Rightarrow d \mid na$ and $d \mid b \Rightarrow d \mid mb$: by lemma 3

$\Rightarrow d \mid (na + mb)$: by exercise

Lemma 5

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

Then

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

Proof.

note:

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

also:

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

$\therefore$ for any $d \in \mathbb{Z}$:

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

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

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

Proof of correctness of Euclidean algorithm

The 1st division

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

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

$$r_0 = q_1 r_1 + r_2 \qquad (0 \le r_2 < r_1)$$
$$r_1 = q_2 r_2 + r_3 \qquad (0 \le r_3 < r_2)$$
$$r_2 = q_3 r_3 + r_4 \qquad (0 \le r_4 < r_3)$$
$$\vdots$$

The seq. of remainders is strictly decreasing: $r_1 > r_2 > r_3 > \dots \ge 0$, and must therefore reach zero. Let r_n be the last non-zero remainder.

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

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 $a, b, m \in \mathbb{Z}$ where $m > 0$. 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 $3 \mid (10-7)$

$25 \equiv 11 \pmod 7$ " $7 \mid (25-11) = 14$

$-13 \equiv 106 \pmod{17}$ " $17 \mid (-13-106) = -119 = (-7)\cdot 17$

$18 \not\equiv 5 \pmod 4$ " $4 \nmid (18-5) = 13$

Lemma 6

$$a \equiv b \pmod m \iff a = b + km \quad (\text{some } k \in \mathbb{Z})$$

Proof: exercise.

Theorem

$a \equiv b \pmod m \iff a$ and b have the same remainder upon division by m.

Proof

($\Leftarrow$) assume a, b have same rem. on div. by m. i.e.

$$a = q_1 m + r \qquad 0 \le r < m$$
$$b = q_1 m + r \qquad "$$

Then $a - b = (q_1 m + r) - (q_2 m + r)$

$$= q_1 m - q_2 m$$
$$= (q_1 - q_2) m$$

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

$\therefore$ $a \equiv b \pmod{m}$.

($\Rightarrow$) next time ....