cse 16 7-22-21

Lemma 1

Let $p_1, p_2, \ldots, p_n$ be primes, and let

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

and

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

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

Then $a \mid b$ iff $x_i \leq y_i$ $(1 \leq i \leq n)$ ($\Rightarrow$ / $\Leftarrow$)

Proof.

observe

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

$$= a \cdot K$$

($\Leftarrow$) If $x_i \leq y_i$ then $y_i - x_i \geq 0$ $(1 \leq i \leq n)$,

so is an integer. $\therefore$ $a \mid b$.

($\Rightarrow$) If $a|b$, then $b = ak'$ for some $k' \in \mathbb{Z}$. Then $ak = ak'$, $\therefore k = k'$

$\therefore k$ is an integer

$\therefore x_i \leq y_i$ for $1 \leq i \leq n$. ∎

Lemma 2

Let $a, b \in \mathbb{Z}^+$ and let

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

be the set of primes that divide a, or b, or both. i.e.

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

and

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

for some $x_i \geq 0$, $y_i \geq 0$.

Then

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

and

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

Illustrate with: $a=30$, $b=75$

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

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

so

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

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

Proof of Lemma 2

Let

d = RHS of (1)

and

m = RHS of (2)

we must show d, m satisfy definitions of gcd & lcm resp. i.e.

gcd (i) $d|a$ and $d|b$ ✓

(ii) if $e|a$ and $e|b$, then $e \leq d$

lcm (i) $a|m$ and $b|m$

(ii) if $a|k$ and $b|k$, then $m \leq k$

we have $\min(x_i, y_i) \leq x_i$ for $1 \leq i \leq n$. So by lemma 1, we have $d|a$. also $\min(x_i, y_i) \leq y_i$ for $1 \leq i \leq n$, so by lemma 1, we have $d|b$.

Now suppose $e|a$ and $e|b$. by unique ~~factorization~~ factorization:

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

where $z_i \geq 0$ $(1 \leq i \leq n)$. by lemma 1

$$\left.\begin{array}{l} e|a \Rightarrow z_i \leq x_i \\ e|b \Rightarrow z_i \leq y_i \end{array}\right\} 1 \leq i \leq n$$

$\therefore z_i \leq \min(x_i, y_i)$ for $1 \leq i \leq n$.

Again by lemma 1, we have

$$e \mid d .$$

It follows that $d = \gcd(a,b)$, proving (1). ∎

Exercise.

Prove part (2), i.e. m satisfies defn. of $\operatorname{lcm}(a,b)$.

Recall:

Thm

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

Proof

let $p_1, \ldots, p_n$ be as in previous

Proof, > 0

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

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

for $x_i \geq 0$, $y_i \geq 0$ and $1 \leq i \leq n$

Refering to (*)

$$LHS = a \cdot b = p_1^{x_1+y_1} p_2^{x_2+y_2} \ldots p_n^{x_n+y_n}$$

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

using lemma 2. But

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

for $1 \leq i \leq n$ $\therefore$ LHS = RHS,

as required. ∎

Ex. $a = 16,200$

$b = 756$

$\gcd(a,b) = 108$

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

Euclid's Algorithm for $\gcd(a,b)$

Ex. $\gcd(16\,200, 756) = 108$

$16\,200 = 21 \cdot 756 + 324$

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

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

↑ stop

Pseudo-code:

```
r = remainder 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. $\gcd(136, 235) = 1$

(a, b)

$$\underset{a}{136} = 0 \cdot \underset{b}{235} + \underset{r}{136}$$

$$235 = 1 \cdot 136 + 99$$

$$136 = 1 \cdot 99 + 37$$

$$99 = 2 \cdot 37 + 25$$

$37 = 1 \cdot 25 + 12$

$25 = 2 \cdot 12 + 1$

$12 = 12 \cdot \boxed{1} + 0 \leftarrow$ stop

↑ gcd

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 (hw ?)

Prove that: if $d|a \wedge d|b$,

then $d|(a+b)$.

Lemma 3

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

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

Proof.

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

$$\Rightarrow na = n(kd) = (nk)d$$

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

■

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:

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

↑ by lemma 3

↑ exercise

■

Exercise

- Prove lemma 4 directly from defn. of divisibility, i.e. don't use exercise and lemma 3.
- Prove lemma 3 & exercise from lemma 4

Lemma 5

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

Then

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

Proof: let $d \in \mathbb{Z}$. Then

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

↑ Lemma 4, $n = 1$, $m = -q$

Also

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

↑ Lemma 4, $a = b$, $b = r$, $n = q$, $m = 1$

Thus

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

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

■

Proof of correctness of Euclid's Alg.

The 1st division gives

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

Let $r_0 = a,\ q_1 = q,\ r_1 = b,\ r_2 = r \quad . > 0$

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

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

$$\vdots$$

The seq. of remainders is strictly decreasing

$$r_1 > r_2 > r_3 > r_4 > \cdots \geq 0,$$

and therefore reach 0. Let r_n be the last non-zero remainder.

$$\vdots$$

$$r_{n-2} = q_{n-1} r_{n-1} + \boxed{r_n} \quad (0 \leq r_n < r_{n-1})$$

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

By lemma 5:

$$\gcd(a,b) = \gcd(r_0, r_1)$$
$$= \gcd(r_1, r_2)$$

$$\vdots$$

$$= \gcd(r_{n-1}, r_n)$$

$$= \gcd(r_n, 0)$$

$$= r_n$$

■

Defn

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

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

notation: $a \equiv b \pmod{m}$

Alternate notation: $a \equiv_m b$.