CSE 16 5-3-24

Supplemental Lecture

Theorem

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

Proof

($\Rightarrow$) Let $a \equiv_m b$. Then $a - b = km$ for some $k \in \mathbb{Z}$. By the division algorithm:

$$a = q_1 m + r_1 \quad \text{and} \quad 0 \leq r_1 < m$$

also

$$b = q_2 m + r_2 \quad \text{and} \quad 0 \leq r_2 < m$$

we must show $r_1 = r_2$.

so

$$km = a - b$$

$$= (q_1 m + r_1) - (q_2 m + r_2)$$

$$= (q_1 - q_2)m + (r_1 - r_2)$$

$\therefore \quad r_1 - r_2 = (k - q_1 + q_2)m$

$\therefore \quad m \mid (r_1 - r_2)$

similarly we have $m \mid (r_2 - r_1)$. At least one of $(r_1 - r_2)$ and $(r_2 - r_1)$ is non-negative. say

$$0 \leq r_1 - r_2 < m$$

Then $m \mid (r_1 - r_2) \Rightarrow r_1 - r_2 = 0 \Rightarrow r_1 = r_2$. □

($\Leftarrow$) Suppose a, b have the same remainder when divided by m. Then

$$a = q_1 m + r$$

$$b = q_2 m + r$$

$$\therefore \quad a - b = (q_1 - q_2)m + \cancel{(r - r)}^{0}$$

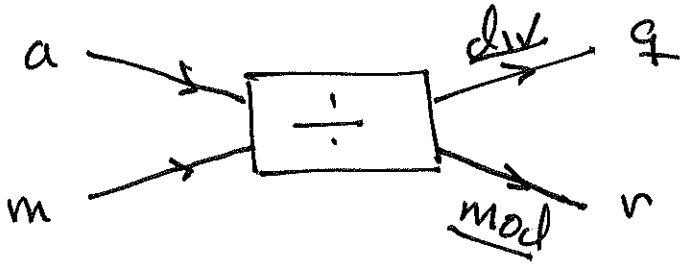
$$\therefore \quad m \mid (a-b)$$

$$\therefore \quad a \equiv_m b \; .$$ ∎

Defn

we define operations mod and div

- $a \bmod m$ = rem. of a on division by m.
- $a \operatorname{div} m$ = quotient of a on division by m.



≥ 0

$$a = (a \underline{\text{div}}\, m) \cdot m + (a \underline{\text{mod}}\, m)$$

last theorem says

$$a \equiv b \pmod{m} \quad \text{iff} \quad a \underline{\text{mod}}\, m = b \underline{\text{mod}}\, m$$

Theorem

Let $a, b, c \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Then

(1) reflexive: $a \equiv_m a$

(2) symmetric: $a \equiv_m b \rightarrow b \equiv_m a$

(3) Transitive: $a \equiv_m b \wedge b \equiv_m c \rightarrow a \equiv_m c$

Exercise:

Prove (1) and (2).

Proof of (3)

$$\left.\begin{array}{l} a \equiv_m b \to m \mid (a-b) \\ b \equiv_m c \to m \mid (b-c) \end{array}\right\} \to m \mid (a-b)+(b-c)$$

$\therefore \quad m \mid (a-c) \quad \therefore \quad a \equiv_m c.$ ∎

Theorem

Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Suppose $a \equiv_m b$ and $c \equiv_m d$. Then

(1) $a+c \equiv_m b+d$

(2) $a-c \equiv_m b-d$

(3) $ac \equiv_m bd$.

Exercise Prove (1) and (2).

Proof of (3)

$$ac - bd = ac - bc + bc - bd$$

$$= (a-b)c + (c-d)b$$

$$= k_1 m \cdot c + k_2 m \cdot b$$

($k_1, k_2 \in \mathbb{Z}$ since $a \equiv_m b$ and $c \equiv_m d$.)

$$= (k_1 c + k_2 b) m$$

Since $k_1 c + k_2 b \in \mathbb{Z}$, we have

$$m \mid (ac - bd)$$

$$\therefore \quad ac \equiv_m bd . \qquad \blacksquare$$

Question:

$$ad \equiv_m bd \xrightarrow{??} a \equiv_m b$$

i.e. can we cancel factors from a congruence?

warning:

don't think that since

$$\left.\begin{array}{l} a \equiv_m c \\ b \equiv_m d \end{array}\right\} \longrightarrow a+b \equiv_m c+d$$

is true, this

$*$ $(a \bmod m) + (b \bmod m) \not\equiv (a+b) \bmod m$

is true. $*$ is in general false

Ex $(2 \bmod 5) + (4 \bmod 5) \stackrel{?}{=} (2+4) \bmod 5$

$2 + 4 \stackrel{?}{=} 6 \bmod 5$

$6 \stackrel{?}{=} 1$

$6 \neq 1$

(skip 4.2)

4.3 Primes and GCD

Defn

Let $p \in \mathbb{Z}$, $p > 1$. We say p is Prime iff its only positive factors are 1 and p. A positive integer that is not prime is Composite

Primes

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

Composites

1, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, ...

note: 1 is not Prime.

Theorem (Fundamental Theorem of Arithmetic)

Every Positive Integer can be expressed uniquely (up to order) as a Product of (zero or more) Primes.

Rmks

- 'up to order' means that order doesn't count, i.e. $2 \cdot 3$ and $3 \cdot 2$ are the same Prime factorization of 6.
- 'zero or more' means:

  zero factors: 1 (empty Product)
  one factor: 2, 3, 5 ... (Primes)
  more factors: 4, 6, 8 ... (composites)

Ex

- $100 = 2 \cdot 2 \cdot 5 \cdot 5$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37$
- $1356 = 2 \cdot 2 \cdot 3 \cdot 113$
- $1357 = 23 \cdot 59$
- $17 = 17$
- $1 = 1$ (empty)

Theorem

Let $n \neq 1$ be composite. Then n has a prime factor p satisfying

$$p \leq \sqrt{n}.$$

Corollary (contrapositive)

If $n > 0$ is not divisible by any prime $p \leq \sqrt{n}$, then n is prime.

Ex is 113 prime?

check: $2 \nmid 113$, $3 \nmid 113$, $5 \nmid 113$, $7 \nmid 113$.
conclude 113 is prime. there is no need to check $11 \nmid 113$, since

$$11^2 = 121 > 113 \quad \text{so} \quad 11 > \sqrt{113}$$

Proof:
Since n is composite, there exist integers a, b such that

$$1 < a < n, \quad 1 < b < n, \quad \text{and} \quad n = a \cdot b$$

Assume (to get $\not\!\!\not$) that both $a > \sqrt{n}$ and $b > \sqrt{n}$. Then

$$n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n \quad \not\!\!\not$$

$\therefore$ our assumption was false, hence either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. say $a \leq \sqrt{n}$.

If a is prime we're done, otherwise a has a prime factor $p \mid a$ (by FTA). so $p \mid n$ and $p < a \leq \sqrt{n}$, so $p \leq \sqrt{n}$.

■

Theorem (Euclid)

The set of prime numbers is infinite.

Proof (contradiction)

Assume there are only finitely many primes, say n of them.

$$\{p_1, p_2, p_3, \ldots, p_n\}$$

Let

$$m = (p_1 \cdot p_2 \cdots p_n) + 1$$

By the FTA m has a prime factor,

say $q \in \{p_1, p_2, \ldots, p_n\}$ divides m since $m > 1$. But also

$$q \mid (p_1 p_2 \cdots p_m)$$

so both $q \mid m$ and $q \mid p_1 p_2 \cdots p_m$, hence

$$q \mid m - (p_1 p_2 \cdots p_n) = 1$$

$\therefore q \mid 1$, which is impossible since 1 has no prime factors. This contradiction shows our assumption was false, hence there are infinitely many primes.

Def'n

Let $a, b \in \mathbb{Z} - \{0\}$. The <u>Greatest common divisor</u> (GCD) of a and b is the largest $d \in \mathbb{Z}^+$ such that both $d|a$ and $d|b$.

Ex. $GCD(12, 18) = 6$

$\{1, 2, 3, 4, 6, 12\} \cap \{1, 2, 3, 6, 9, 18\} = \{1, 2, 3, \textcircled{6}\}$

Ex. $GCD(13, 44) = 1$

$\{1, 13\} \cap \{1, 2, 4, 11, 44\} = \{\textcircled{1}\}$

Def'n

$a, b \in \mathbb{Z} - \{0\}$ are said to be <u>relatively prime</u> (or <u>co-prime</u>) iff $GCD(a, b) = 1$.

<u>Equivalently</u>: a and b have no prime factors in common.

Def'n

Let $a, b \in \mathbb{Z}$. The <u>least common multiple</u> (LCM) of a and b is the smallest $m \in \mathbb{Z}^+$ such that both $a|m$ and $b|m$.

Note:

For any $a \in \mathbb{Z} - \{0\}$, p prime

- $GCD(a, a) = a$
- $GCD(a, p) = \begin{cases} 1 & \text{if } p \nmid a \\ p & \text{if } p | a \end{cases}$.

Ex.

- $LCM(30, 75) = 150$

  mult of 30: $\{30, 60, 90, 120, \underline{150}, 180, \ldots\}$

  " " 75: $\{75, \underline{150}, \ldots$

- $GCD(30, 75) = 15$

  divisors of 30: $\{1, 2, 3, 5, 10, \underline{15}, 30\}$

  " " 75: $\{1, 3, 5, \underline{15}, 25, 75\}$

- observe that

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

Theorem

for any $a, b \in \mathbb{Z}^+$

$$a \cdot b = GCD(a,b) \cdot LCM(a,b)$$

Euclidean Algorithm

Ex. $GCD(198, 84) = 6$

$198 = 84 \cdot 2 + 30$

$84 = 30 \cdot 2 + 24$

$30 = 24 \cdot 1 + \boxed{6}$ ← gcd

$24 = 6 \cdot 4 + 0$ ← stop

Pseudo-code

GCD(a, b)

1. $r = a \bmod b$
2. while $r > 0$
3. $\quad a = b$
4. $\quad b = r$
5. $\quad r = a \bmod b$
6. end-while
7. return b

Ex GCD(756, 16200) = 108

$$16200 = 756 \cdot 21 + 324$$
$$756 = 324 \cdot 2 + 108 \leftarrow \text{gcd}$$
$$324 = 108 \cdot 3 + 0 \leftarrow \text{stop}$$