CSE 16 7-18-24

- Quiz 2 today: 12:35-1:00 PM

Theorem
Let $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. 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) & (2)

Proof of (3)

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= (a-b)c + b(c-d) \\ &= k_1 m \cdot c + b \cdot k_2 m \end{aligned}$$

for some $k_1, k_2 \in \mathbb{Z}$, by hypothesis.

Thus

$$ac - bd = (k_1 c + k_2 b) m$$

$$\therefore \quad ac \equiv_m bd$$ ∎

Question:

Is it valid to cancel a number from a congruence

i.e. does

$$ad \equiv_m bd \overset{?}{\longrightarrow} a \equiv_m b$$

we know

$$a \equiv_m b \longrightarrow ad \equiv_m bd$$

Answer: no!

warning: don't think that since

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

it would also be true that

$$(a \bmod m) + (b \bmod m) = (a+b) \bmod m$$

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

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

$6 \neq 1$

4.3 Primes & 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*.

note: 1 is neither prime nor composite.

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

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

Theorem (Fund. Thm. 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 order does not count, i.e. $2 \cdot 3 = 3 \cdot 2 = 6$ are not different prime-factorizations of 6.

- 'zero or more'

zero-factors: 1 (empty product)
one-factor: 2, 3, 5, .. (primes)
more-factors: 4, 6, 8, .. (composites)

Ex.

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

Theorem

Let $n \in \mathbb{Z}^+$ be composite. Then n has a prime factor p satisfying $p \leq \sqrt{n}$.

Corollary (contrapositive)

If $n > 1$ is not divisible by any prime $p \leq \sqrt{n}$, then n is prime.

Ex

$2 \nmid 113$, $3 \nmid 113$, $5 \nmid 113$, $7 \nmid 113$, therefore 113 is prime.

don't have to check $11 \nmid 113$ since

$$11^2 = 121 > 113 \rightarrow 11 > \sqrt{113}$$

Proof

Since n is composite, there exist $a, b \in \mathbb{Z}$ s.t.

$1 < a < n$, $1 < b < n$, and $n = a \cdot b$

Assume, to get a $\cdot\dot{X}\cdot$, that both $a > \sqrt{n}$ and $b > \sqrt{n}$. Then

$$n = ab > \sqrt{n} \cdot \sqrt{n} = n \quad \cdot\dot{X}\cdot$$

Therefore either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Say $a \leq \sqrt{n}$.

If a is prime, we're done. If a is composite, a has a prime factor p (by F.T.A.) satisfying

$$1 < p < a \leq \sqrt{n}$$

Since $p \mid a$ and $a \mid n$, we have $p \mid n$.

Theorem (Euclid)

The set of prime numbers is infinite.

Proof (contradiction)

Assume there are only finitely many primes, say n.

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

Let $m = (p_1 \cdot p_2 \cdots p_n) + 1$. By the FTA there exists

$$q \in \{p_1, p_2, \ldots, p_n\}$$

that divides m, since $m > 1$

But also $q \mid (p_1 p_2 \cdots p_n)$. So we have

$$q \mid m \text{ and } q \mid (p_1 \cdots p_n)$$

$$\therefore q \mid m - (p_1 \cdots p_n) \quad \therefore q \mid 1$$

But 1 has no prime factors. This $\lightning$ shows our assumption was false, so there are infinitely many primes.

$\blacksquare$

Defn

Let $a, b \in \mathbb{Z} - \{0\}$. The greatest common divisor (GCD) of a and b is the largest $d \in \mathbb{Z}^+$ such that

$$d \mid a \quad \text{and} \quad d \mid b$$

Ex

- $\text{GCD}(12, 18) = 6$

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

- $GCD(13, 44) = 1$

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

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

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

Defn

$a, b \in \mathbb{Z} - \{0\}$ are called relatively prime (or co-prime) iff

$$GCD(a, b) = 1.$$

Equivalently: a and b have no prime factors in common.

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

$$a \mid m \quad \text{and} \quad b \mid m$$

Ex $\text{LCM}(30, 75) = 150$

Pos. mult of 30: 30, 60, 90, 120, (150), 180, ...
" " " 75: 75, (150), ...

$\text{GCD}(30, 75) = 15$

divisors of 30: $\{1, 2, 3, 5, 10, (15), 30\}$
" " 75: $\{1, 3, 5, (15), 25, 75\}$

observe

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

Theorem

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

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

more to come . . .