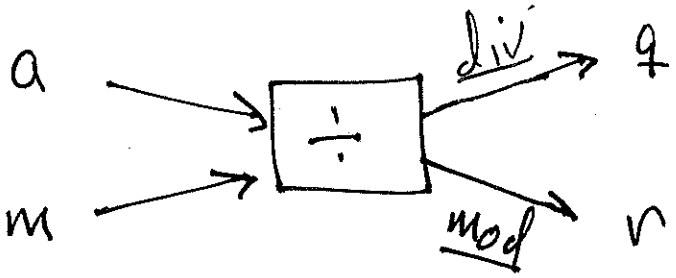
Defn

We define operations mod and div as

- a mod m = rem. of a on division by m
- a div m = quotient " " " " " m.



Thus

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

Prev. Thm:

$a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$

Theorem

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

(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)

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

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

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) $a - c \equiv_m b - c$

(3) $ac \equiv_m bd$

Exercise Prove (1) and (2).

Proof of (3)

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= (a-b)c + (c-d)b \\ &= k_1 m \cdot c + k_2 m \cdot b \quad \left\{ \begin{matrix} \text{by} \\ \text{hypothesis} \end{matrix} \right. \\ &= (k_1 c + k_2 b) m \end{aligned}$$

$\therefore m \mid (ac - bd) \quad \therefore \quad ac \equiv_m bd.$ ∎

From (3) We know

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

But

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

In general, no. Depends on m and d.

Warning

Students are tempted to think

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

In general * is false!!

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

$2 + 4 \stackrel{?}{=} 1$

$6 \neq 1$

4.3 Primes and GCD

Defn

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

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

composites: 1, 4, 6, 8, 9, 10, 12, ...

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 order doesn't count. i.e. $2 \cdot 3 = 3 \cdot 2 = 6$ are not different prime factorizations of 6.
- 'zero or more' prime factors:

  zero factors: 1 (empty product)

  one factor: 2, 3, 5 (primes)

  more factors: 4, 8, 6 (composites)

Ex.

- $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$.
- $17 = 17$
- $1 = 1$

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. $n = 113$

$2 \nmid 113$, $3 \nmid 113$, $5 \nmid 113$, $7 \nmid 113$ hence 113 is Prime. There is no need 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.

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

Assume that both $a > \sqrt{n}$ and $b > \sqrt{n}$.

Then $n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$ $\dot{-}\dot{\times}$

$\therefore$ 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 (by FTA) satisfying $p < a \leq \sqrt{n}$. since $p \mid a$ and $a \mid n$, we have $p \mid n$. so n has a prime factor p s.t. $p \leq \sqrt{n}$. ∎

Theorem (Euclid)
The set of primes is infinite.

Proof (contradiction)
Assume there are only finitely many primes

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

Let

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

By the FTA there is some prime $q \in \{p_1, p_2, \ldots, p_n\}$ s.t. $q \mid m$, since $m > 1$. But also $q \mid (p_1 p_2 \cdots p_n)$. Thus

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

i.e. $q \mid 1$, which is impossible since 1 has no prime factors.

$\therefore$ there are infinitely many primes

Defn GCD

Let $a, b \in \mathbb{Z} - \{0\}$. The greatest common divisor of a and b is the largest $d \in \mathbb{Z}^+$ s.t. both $d|a$ and $d|b$. i.e.

$d = GCD(a,b)$ iff both:

(i) $d|a \wedge d|b$

(ii) $e|a \wedge e|b \rightarrow e \leq d$

Ex.

- $GCD(12,18) = 6$ ✓

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

div of 12 div. of 18 comm. div.

- $GCD(13, 44) = 1$

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

Def^n

$a, b \in \mathbb{Z} - \{0\}$ are said to be relatively prime (or co-prime) iff $GCD(a, b) = 1$. Equivalently: a and b have no prime factors in common.

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

Let $a, b \in \mathbb{Z}$. The least common multiple (LCM) of a and b is the smallest $m \in \mathbb{Z}^+$ s.t. $a|m$ and $b|m$.

Ex.

- LCM$(30, 75) = 150$

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

  Pos. mult. of 75: $\{75, \underline{150}, \ldots\}$

- GCD$(30, 75) = 15$

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

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

• observe

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

Theorem

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

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

Ex. $a = 16,200$

$b = 756$

$GCD(a,b) = 108$

$$\therefore LCM(a,b) = \frac{a \cdot b}{GCD(a,b)} = \frac{16,200 \cdot 756}{108}$$

$$= \boxed{113,400}$$