1. hw4: cancel sec. 5.1 this week.
    only 2 sections on hw4.

2. Defn
   Let \( a, b \in \mathbb{Z}, m \in \mathbb{Z}^+ \). We say \( a \) is congruent to \( b \) modulo \( m \) if

\[
m \mid (a - b)
\]

Notation: \( a \equiv b \pmod{m} \)

Better: \( a \equiv_m b \)
Example:

\[ 8 \equiv 22 \pmod{7} \text{ since } 7 \mid (8 - 22) \]

\[ 51 \equiv 18 \pmod{11} \text{ since } 11 \mid (51 - 18) \]

\[ 13 \equiv -7 \pmod{10} \text{ since } 10 \mid (13 - (-7)) \]

Observe:

- \( a \equiv b \pmod{m} \) iff \( b \equiv a \pmod{m} \) (symmetric)

since

\[ m \mid (a - b) \text{ iff } m \mid (b - a). \]

- \( a \equiv a \pmod{m} \) for any \( a \in \mathbb{Z} \) (reflexive)

since

\[ m \mid (a - a) \text{ i.e. } m \mid 0. \]

- \( a \equiv b \pmod{m} \) \& \( b \equiv c \pmod{m} \) \( \Rightarrow \) \( a \equiv c \pmod{m} \) (transitive)

Proof: later
Theorem

\[ a \equiv b \pmod{m} \iff a = b + km \text{ for some } k \in \mathbb{Z}. \]

Proof:

\[ a \equiv b \pmod{m} \iff m \mid (a - b) \]

\[ \iff a - b = km, \text{ some } k \in \mathbb{Z} \]

\[ \iff a = b + km, \ldots \]

Theorem

\[ a \equiv b \pmod{m} \iff a \text{ and } b \text{ have the same remainder upon division by } m \]
(\Rightarrow) \text{ assume } a \equiv b \pmod{m}, \text{ so that } a - b = km \text{ for some } k \in \mathbb{Z}.

By the division algorithm:

\[
\begin{align*}
a &= q_1 m + r_1, \quad 0 \leq r_1 < m \\
b &= q_2 m + r_2, \quad 0 \leq r_2 < m
\end{align*}
\]

Thus

\[
k m = a - b = (q_1 m + r_1) - (q_2 m + r_2)
\]

\[
= (q_1 - q_2) m + (r_1 - r_2)
\]

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

\[
\therefore \quad m \mid r_1 - r_2, \text{ and likewise } m \mid r_2 - r_1.
\]

Note: note one of \( r_1 - r_2 \) and \( r_2 - r_1 \) is non-negative.
Say \( r_1 - r_2 \geq 0 \), also \( r_1 - r_2 < m \)

\[ \therefore \quad 0 \leq r_1 - r_2 < m \]

and also \( m \mid (r_1 - r_2) \). Therefore

\[ r_1 - r_2 = 0 \quad \therefore \quad r_1 = r_2. \]

\((\Leftarrow)\) assume \( a \) and \( b \) have the same remainder upon division by \( m \), i.e.

\[ a = q_1 m + r \quad \mid \quad 0 \leq r < m \]

\[ b = q_2 m + r \]

\[ \therefore \quad a - b = (q_1 - q_2) m \]

\[ \therefore \quad m \mid (a-b) \quad \therefore \quad a \equiv b \pmod{m}. \]
Define operations

\[ a \mod m = \text{remainder of } a \text{ on div. by } m. \]

\[ a \div m = \text{quotient of } a \text{ on div. by } m. \]

\begin{align*}
  a &= m \left( a \div m \right) + (a \mod m) \\
  \underbrace{\text{quotient}} & \quad \underbrace{\text{remainder}}
\end{align*}

Preceding them:

\[ a \equiv b \pmod{m} \iff a \mod m = b \mod m \]
If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \), then \( a+c \equiv b+d \pmod{m} \).

**Proof:**

\[
\begin{align*}
\frac{a \equiv b \pmod{m}}{\Rightarrow m \mid (a-b)} \\
\frac{c \equiv d \pmod{m}}{\Rightarrow m \mid (c-d)} \end{align*}
\]

\[\Rightarrow m \mid (a-b)+(c-d)\]

\[\therefore m \mid (a+c)-(b+d)\]

\[\therefore a+c \equiv b+d \pmod{m} \]
If \(a \equiv b \pmod{m}\) and \(c \equiv d \pmod{m}\), then \(ac \equiv bd \pmod{m}\).

\[
ac - bd = ac - bc + bc - bd
\]
\[
= (a - b)c + (c - d)b
\]
\[
= (k_1m)c + (k_2m)b
\]
\[
= (k_1c + k_2b)m
\]

\[\therefore \quad m \mid (ac - bd)\]

\[\therefore \quad ac \equiv bd \pmod{m}.\]
Thus (transitivity)

If \( a \equiv b (\text{mod} m) \) and \( b \equiv c (\text{mod} m) \)

then \( a \equiv c (\text{mod} m) \).

Proof.

\[
\begin{align*}
a \equiv b (\text{mod} m) & \Rightarrow m \mid (a - b) \\
b \equiv c (\text{mod} m) & \Rightarrow m \mid (b - c)
\end{align*}
\]

\[
\therefore m \mid (a - b) + (b - c)
\]

\[
\therefore m \mid (a - c)
\]

\[
\therefore a \equiv c (\text{mod} m).
\]
Students sometimes think that

\[
\begin{align*}
\text{Since } \quad & a \equiv c \pmod{m} \quad \text{and} \quad b \equiv d \pmod{m} \\
\implies & a + b \equiv c + d \pmod{m}
\end{align*}
\]

It must also be true that

\[
(a \pmod{m}) + (b \pmod{m}) = (a + b) \pmod{m}
\]

Counter-example:

\[
\left( 1 \pmod{5} \right) + \left( 4 \pmod{5} \right) \overset{?}{=} \left( 1 + 4 \right) \pmod{5}
\]

\[
1 + 4 \overset{?}{=} 5 \pmod{5}
\]

\[
5 \overset{?}{=} 0
\]

\[
5 \neq 0
\]
4.3 Prime and Composite

**Defn**

Let \( p \in \mathbb{Z}, p > 1 \). We say \( p \) is *prime* iff its positive factors are 1 and \( p \), a pos. int.

That is, not prime is **composite**.

**Primes**

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

**Composite**

1, 4, 6, 8, 9, 10, 14, 15, 16...

Note: 1 is not prime.
Every positive integer can be expressed uniquely (up to order) as a product of (zero or more) primes.

Remark:
- 'up to order' means order does not count, i.e. 2, 3, and 3, 2 are the same factorization of 6.
- Product may contain, 0, 1, or more factors.
- The 'empty product' is 1.
  - 0 factors: 1
  - 1 factor: 2, 3, 5, ... primes
  - 2 or more factors: ... composite
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:

\[
\begin{align*}
2 \nmid 113, \quad 3 \nmid 113, \quad 5 \nmid 113, \quad 7 \nmid 113 \\
\therefore 113 \text{ is prime, not necessary to check } 11 \nmid 113 \text{ since } 11^2 = 121 > 113.
\end{align*}
\]

See Proof in book.
**Theorem (Euclid)**

The set of prime numbers is infinite.

**Proof (contradiction)**

Assume there are only finitely many primes, say \( p_1, p_2, \ldots, p_n \).

Let \( m = (p_1 \cdot p_2 \cdot p_3 \cdots p_n) + 1 \). By the FTA there is some prime \( q \) such that \( q \mid m \) since \( m > 1 \). Now \( q \not\in \{p_1, p_2, \ldots, p_n\} \), so \( q \mid (p_1 \cdot p_2 \cdots p_n) \).

Thus \( q \mid m - (p_1 \cdots p_n) \vdash q \mid 1 \).
But 1 has no prime factors so \( g \neq 1 \). This shows our assumption was false, and the set of primes is infinite.

\[ \text{Defn} \]

\[ \text{let } a, b \in \mathbb{Z} - \{0\}. \text{ The Greatest Common Divisor (GCD) of } a \text{ and } b \text{ is the largest } d \in \mathbb{Z}^+ \text{ such that } d \mid a \text{ and } d \mid b. \]

\[ \text{Ex: GCD}(12, 18) = 6 \]

\[ \{1, 2, 3, 4, 6, 12\} \cap \{1, 2, 3, 6, 9, 18\} = \{1, 2, 3, 6\} \]
Ex: $\text{GCD}(13, 44) = 1$

\[
\{1, 13\} \cap \{1, 2, 4, 11, 44\} = \emptyset
\]

**Note:**
1. $\text{GCD}(a, a) = a$ for any $a \geq 1$.
2. $\text{GCD}(p, a) = \begin{cases} 1 & \text{if } p \text{ prime, } p \nmid a \\ p & \text{if } p \text{ prime, } p \mid a \end{cases}$

**Defn**

$a, b \in \mathbb{Z}$ for $a$ and $b$ are said to be relatively prime if $\text{GCD}(a, b) = 1$.

Equivalently: $a$ and $b$ have no prime factors in common.
\[ \text{Ex: } \gcd(13, 44) = 1 \]
\[ \gcd(12, 25) = 1 \]
\[ \gcd(27, 104) = 1 \]

**Theorem**

Let the prime factors of either \(a\) or \(b\) be listed

\[ p_1, p_2, \ldots, p_n \]

so that

\[ a = p_1^{x_1} p_2^{x_2} \ldots p_n^{x_n} \quad \text{and} \quad b = p_1^{y_1} p_2^{y_2} \ldots p_n^{y_n} \]

where \( x_i \geq 0 \) and \( y_i \geq 0 \) \((1 \leq i \leq n)\).

Then

\[ \gcd(a,b) = p_1^{\min(x_1,y_1)} p_2^{\min(x_2,y_2)} \ldots p_n^{\min(x_n,y_n)} \]

**Proof:** See book.
Let $a, b \in \mathbb{Z}$. The Least Common Multiple of $a$ and $b$ is the smallest $m$ s.t. both $a|m$ and $b|m$.

Notation: $m = \text{LCM}(a, b)$.

Then

Same hypotheses. Then

$$\text{LCM}(a, b) = \prod_{i=1}^{n} \left( \max(x_i, y_i) \right) \cdot p_2 \cdot \ldots \cdot p_n$$

Proof: See book.
Thm:

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

$$a \cdot b = \gcd(a, b) \cdot \operatorname{LCM}(a, b)$$

Proof exercise.

Hint: $\min(x, y) + \max(x, y) = x + y$.

next: Euclidean Algorithm.