# PSTAT 8 Extra Materials for Division

Haosheng Zhou

Feb, 2023

# Definition

Let's first introduce some useful notations you are likely to encounter in the future study.

For integers $a, b, n$, we call $a \equiv b \ (mod\ n)$ meaning that if we divide $a$ and $b$ by $n$, they have the same remainder. This is the **congruence relationship** on the set of integers. In the language of mathematics, it means that

$$\exists q_a \in \mathbb{Z}, r_a \in \{0, 1, ..., n-1\}, a = q_a \cdot n + r_a \tag{1}$$

$$\exists q_b \in \mathbb{Z}, r_b \in \{0, 1, ..., n-1\}, b = q_b \cdot n + r_b \tag{2}$$

$$r_a = r_b \tag{3}$$

from those two division representations, it can be seen that $a - b = (q_a - q_b) \cdot n + (r_a - r_b)$, so we conclude that $a \equiv b \ (mod\ n)$ if and only if $a - b = (q_a - q_b) \cdot n$ if and only if $n|(a-b)$, which provides the connection with division.

For two integers $a, b$, we have already defined the greatest common divisor $\gcd(a, b)$ as the greatest common divisor of $a, b$, i.e.

$$\gcd(a, b) = \max \{n \in \mathbb{Z} : n|a, n|b\} \tag{4}$$

it's natural to think on the other side, i.e. whether we can define some similar concept for common multiples. Since the common multiples of $a, b$ can be large enough, defining the greatest common multiple won't make sense. Instead, we define the **least common multiple** of our interest.

$$\mathrm{lcm}(a, b) = \min \{m \in \mathbb{N} : a|m, b|m, m \neq 0\} \tag{5}$$

notice that here we require $m$ to be natural number instead of integer since the multiple of $a, b$ can be as little as possible by taking negative values. For example, $\mathrm{lcm}(2, 3) = 2 \times 3 = 6, \mathrm{lcm}(6, 9) = 18$.

# Property

Let's form the properties as theorems and provide the proofs below, we always assume that all letters $a, b, m, n, ...$ in the following context stand for non-zero integers without specification.

**Theorem 1.** *If* $a \equiv b \ (mod\ n)$*, then* $\gcd(a, n) = \gcd(b, n)$.

*Proof.* Since $a \equiv b \ (mod\ n)$, by definition

$$\exists q_a \in \mathbb{Z}, r_a \in \{0, 1, ..., n-1\}, a = q_a \cdot n + r_a \tag{6}$$

$$\exists q_b \in \mathbb{Z}, r_b \in \{0, 1, ..., n-1\}, b = q_b \cdot n + r_b \tag{7}$$

$$r_a = r_b \tag{8}$$

by Euclidean algorithm, $\gcd(a, n) = \gcd(n, r_a) = \gcd(n, r_b) = \gcd(b, n)$, proved. □

**Theorem 2.** *If $a|n, b|n$, then $lcm(a,b)|n$.*

*Proof.* Denote $d = \text{lcm}(a,b)$ and consider dividing $n$ by $d$ to get

$$\exists q \in \mathbb{Z}, r \in \{0, 1, ..., d-1\}, s.t.\ n = q \cdot d + r \tag{9}$$

since $a|d, b|d$ by the definition of least common multiple, we have $a|qd, b|qd$. Notice that now $a|n, b|n$, so by the property of dividion, $a|(n-qd), b|(n-qd)$ so $a|r, b|r$.

Now $r < d$ is a common multiple of $a, b$ so $r = 0$. We can prove this fact by proving by contradiction. If $\exists r \in \{1, 2, ..., d-1\}$ is a common multiple of $a, b$, then $r$ is less than $d = \text{lcm}(a,b)$, the least common multiple of $a, b$. This is a contradiction with the definition of the least common multiple!

So $r = 0$ and $\exists q \in \mathbb{Z}, n = qd$ so we conclude that $\text{lcm}(a,b) = d|n$.

□

**Remark.** *This property is telling us that the common multiple must be a multiple of the least common multiple. Similar property holds for* gcd *that the common divisor must be a divisor of the greatest common divisor.*

**Theorem 3.** $\gcd(a,b) = 1$ *if and only if* $\exists u, v \in \mathbb{Z}, ua + vb = 1$.

*Proof.* Recall that we have already proved in class that $\forall a, b \in \mathbb{Z}, a, b \neq 0, \exists u, v \in \mathbb{Z}, ua+vb = \gcd(a,b)$ (by Euclidean algorithm). As a result, if $\gcd(a,b) = 1$, then $\exists u, v \in \mathbb{Z}, ua + vb = \gcd(a,b) = 1$.

Conversely, if $\exists u, v \in \mathbb{Z}, ua+vb = 1$, notice that by the definition of greatest common divisor, $\gcd(a,b)|a, \gcd(a,b)|b$, so $\gcd(a,b)|ua, \gcd(a,b)|vb$. By the property of division, $\gcd(a,b)|(ua+vb) = 1$, so $\gcd(a,b) = 1$.

□

**Remark.** *If* $\gcd(a,b) = 1$*, we generally call $a, b$ to be* ***coprime****. This is a very important and useful* ***characterization of being coprime****. If you are going to conduct further study in mathematics, you will definitely see a lot of variants and generalizations of this theorem. We will try to illustrate by examples why this theorem is useful.*

**Theorem 4.** *If* $\gcd(a,b) = 1$ *and* $a|bn$*, then* $a|n$.

*Proof.* By the characterization of coprime integers, $\exists u, v \in \mathbb{Z}, ua + vb = 1$, so $uan + vbn = n$.

Since $a|bn$, $a|vbn$. Since $a|uan$, we see that $a|(uan + vbn) = n$, proved. □

**Remark.** *This is the general case for problem 5 we have proved in worksheet 3 that if* $7|4a$*, then* $7|a$*. Now we know that the essential reason is that* $\gcd(4,7) = 1$.

**Theorem 5.** $\forall n \in \mathbb{Z}, n \geq 1, \gcd(n, n+1) = 1$.

*Proof.* By the characterization of coprime integers, we just have to prove that $\exists u, v \in \mathbb{Z}, un + v(n+1) = 1$.

Notice that $1 \times (n+1) + (-1) \times n = 1$, so $\exists u = -1, v = 1$ such that $un + v(n+1) = 1$, proved. □

**Remark.** *Any two consecutive positive integers are coprime.*

**Theorem 6.** $\gcd(a,b) \cdot lcm(a,b) = ab$.

*Proof.* Denote $d = \gcd(a, b)$ so $\frac{ab}{d}$ is a common multiple of $a, b$ since $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$, thus $\text{lcm}(a, b) \leq \frac{ab}{d}$ by the definition of lcm.

Now we only have to prove that $\text{lcm}(a, b) \geq \frac{ab}{d}$. Since $\frac{\text{lcm}(a,b)}{a}, \frac{\text{lcm}(a,b)}{b} \in \mathbb{Z}$, $\frac{ab}{\text{lcm}(a,b)} | a$, $\frac{ab}{\text{lcm}(a,b)} | b$ so $\frac{ab}{\text{lcm}(a,b)}$ is a common divisor of $a, b$ and $d \geq \frac{ab}{\text{lcm}(a,b)}$ so it's proved. □

**Remark.** *This show some kind of 'duality' between greatest common divisor and least common multiple that their product is always the product of two integers. This enables us to calculate least common multiple for even very large* $a, b$ *since* $\gcd(a, b)$ *can always be computed efficiently using the Euclidean algorithm and* $lcm(a, b) = \frac{ab}{\gcd(a,b)}$.