# Number Theory & Mathematical Reasoning
Instructor: Dr. Daniel Saracino

Note Taken by Daniel Jeong

from 2024-08-29 to 2024-12-20

**Theorem 1**

For all integers $a$, $b$, $c$, $d$:

(i) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(ii) If $a \mid b$ and $a \mid c$, then for all $x, y \in \mathbb{Z}$, $a \mid (xb + yc)$.

(iii) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

**Theorem 2**

Suppose $a$ and $b$ are integers that are not both 0, so that $(a, b)$ exists. Then for every $n \in \mathbb{Z}$,

$$(a, b) = (a + nb, b) = (a, b + na)$$

**Theorem 3**

Every integer $n \geqslant 2$ is the product of one or more primes.

**Theorem 4**

There exist infinitely many primes.

**Theorem 5**

For every integer $n \geqslant 2$, the factorization of $n$ into primes is unique, except for the order in which the factors are written.

**Theorem 6**

Suppose $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$. Then the following are equivalent:

(i) $a \equiv b \pmod{m}$; that is, $m \mid (a - b)$.

(ii) $a = b + m\ell$ for some $\ell \in \mathbb{Z}$.

(iii) $\overline{a}^m = \overline{b}^m$.

Thus, the remainders are equal, and any one of (i), (ii), or (iii) proves the other two.

**Theorem 7**

Basic Properties of Congruence Modulo $m$:
Suppose $m \in \mathbb{Z}^+$, then the following all hold:

(i) **Reflexivity**: For every $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$.

(ii) **Symmetry**: For all $a, b \in \mathbb{Z}$, if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

(iii) **Transitivity**: For all $a, b, c \in \mathbb{Z}$, if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

When a relationship between elements of a set $S$ is reflexive, symmetric, and transitive, the relationship is called an equivalence relation on $S$.
Thus, **** says that ”congruence modulo $m$” is an equivalence relation on the set $\mathbb{Z}$.

**Theorem 8**

Suppose $m \in \mathbb{Z}^+$, and let $a, b, c, d \in \mathbb{Z}$.
Then, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, we have:

1. $a + c \equiv b + d \pmod{m}$.
2. $ac \equiv bd \pmod{m}$.

**Lemma 1** Bezout's Lemma

If $m$ and $n$ are integers that are not both zero, then there exist $x, y \in \mathbb{Z}$ such that $xm + yn = (m, n)$.

**Lemma 2** Euclid's Lemma

Suppose $a$, $b$, $c$ are integers such that $a \mid bc$ and $(a, b) = 1$. Then $a \mid c$.

**Lemma 3** Division Lemma

If $a$ and $m$ are integers and $m$ is positive, then there exist integers $q$ and $r$ such that $a = qm + r$ and $0 \leq r \leq m$

**Definition 1: Coprime**

We say integers $a$ and $b$ are relatively prime (or "coprime") if $(a, b) = 1$.

**Definition 2: Prime**

An integer $p$ is prime if $p > 1$ and the only positive integers that divide $p$ are 1 and $p$.

**Corollary 1**

Every integer $n \geq 2$ has a unique representation in the form:

$$n = p_1^{e_1} \times p_2^{e_2} \times p_3^{e_3} \times \cdots \times p_k^{e_k}$$

where the $p$'s are distinct primes and each $e_i \geq 1$. This is called the prime-power decomposition of $n$.

**Corollary 2**

Suppose $n \geqslant 2$ and the prime-power decomposition (ppd) of $n$ is:

$$n = p_1^{e_1} \times p_2^{e_2} \times p_3^{e_3} \times \cdots \times p_k^{e_k}.$$

Then if $m$ is any positive integer that divides $n$,

$$m = p_1^{f_1} \times p_2^{f_2} \times p_3^{f_3} \times \cdots \times p_k^{f_k}$$

for some integers $f_1, \cdots, f_k$ such that $0 \leqslant f_i \leqslant e_i$.

**Corollary 3**

If

$$n = p_1^{c_1} \times p_2^{c_2} \times p_3^{c_3} \times \cdots \times p_k^{c_k}$$

and

$$m = p_1^{d_1} \times p_2^{d_2} \times p_3^{d_3} \times \cdots \times p_k^{d_k},$$

where $p_1, \cdots, p_k$ are distinct primes, and the $c_i$'s and $d_i$'s are nonnegative integers, then:

$$(m, n) = p_1^{\min(c_1,d_1)} \times p_2^{\min(c_2,d_2)} \times \cdots \times p_k^{\min(c_k,d_k)}.$$

**Corollary 4**

If $n$ is an integer such that $n \geqslant 2$, then there exists a positive integer $m$ such that $n = m^2$ if and only if all the exponents in the ppd of $n$ are even.

**Corollary 5** Theorem 8-1

Suppose $a \equiv b \pmod{m}$. Then:

$$\begin{aligned} a &\equiv b \pmod{m}, \\ a^2 &\equiv b^2 \pmod{m}, \\ a^3 &\equiv b^3 \pmod{m}, \\ &\vdots \\ a^k &\equiv b^k \pmod{m} \quad \text{for every } k \in \mathbb{Z}^+. \end{aligned}$$

Thus, using part (ii) of Theorem 8 repeatedly, we get: If $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$ for every $k \in \mathbb{Z}^+$.

**Corollary 6** Theorem 8-2

If $p(x)$ is a polynomial with integer coefficients and $a \equiv b \pmod{m}$, then $p(a) \equiv p(b) \pmod{m}$.