Ch 1.6 Theory of Congruences (Y)

1.6.1 Basic Concepts and Properties of Congruences

Let a be an integer and n a positive integer greater than 1. We define "$a \mod n$" to be the remainder r when a is divided by n, that is
$r = a \mod n = a - \lfloor a/n \rfloor n.$

- We may also say that "r is equal to a reduced modulo n".

Let a be an integer and n a positive integer. We say that "a is *congruent* to b modulo n", denoted by $a \equiv b \pmod{n}$

- if n is a divisor of $a - b$, or equivalently, if $n \mid (a - b)$. Similarly, we write $a \not\equiv b \pmod{n}$
  if a is not congruent (or incongruent) to b modulo n, or equivalently, if $n \nmid (a - b)$. Clearly, for $a \equiv b \pmod{n}$ (resp. $a \not\equiv b \pmod{n}$), we can write $a = kn - b$ (resp. $a \neq kn - b$) for some integer k. The integer n is called the *modulas*.
- $$\begin{aligned} a \equiv b \pmod{n} &\iff n \mid (a - b) \\ &\iff a = kn + b,\ k \in \mathbb{Z} \\ a \not\equiv b \pmod{n} &\iff n \nmid (a - b) \\ &\iff a \neq kn + b,\ k \in \mathbb{Z} \end{aligned}$$

Theorem Let n be a positive integer. Then the congruence modulo n is
1. *reflexive*: $a \equiv a \pmod{n},\ \forall a \in \mathbb{Z}$;
2. *symmetric*: if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n},\ \forall a, b \in \mathbb{Z}$;
3. *transitive*: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n},\ \forall a, b, c \in \mathbb{Z}$.

- $a \mid b$ is *reflexive*, and *transitive* but not *symmetric*. if $a \mid b$ and $b \mid a$ then $a = b$, so it's not an *equivalence relation*.

If $x \equiv a \pmod{n}$, then a is called a *residue* of x modulo n. The *residue class* of a modulo n, denoted by $[a]_n$ (or just $[a]$ if no confusion caused), is the set of all those integers that are congruent to a modulo n.

- Writing $a \in [b]_n$ is the same as writing $a \equiv b \pmod{n}$.

▼ Example: Name the sets of modulo 5.

There are five residue classes:

$$\begin{aligned} [0]_5 &= \{\dots, -15, -10, -5, 0, 5, 10, 15, 20, \dots\} \\ [1]_5 &= \{\dots, -14, -9, -4, 1, 6, 11, 16, 21, \dots\} \\ [2]_5 &= \{\dots, -13, -8, -3, 2, 7, 12, 17, 22, \dots\} \\ [3]_5 &= \{\dots, -12, -7, -2, 3, 8, 13, 18, 23, \dots\} \\ [4]_5 &= \{\dots, -11, -6, 1, 4, 9, 14, 19, 24, \dots\} \end{aligned}$$

▼ Example: In congruence modulo 5, we have...

$$\begin{aligned} [9]_5 &= \{9 + 5k : k \in \mathbb{Z}\} = \{9, 9 \pm 5, 9 \pm 10, 9 \pm 15, \dots\} \\ &= \{\dots, -11, -6, -1, 4, 9, 14, 19, 24, \dots\} \end{aligned}$$

We also have

$$\begin{aligned} [4]_5 &= \{4 + 5k : k \in \mathbb{Z}\} = \{4, 4 \pm 5, 4 \pm 10, 4 \pm 15, \dots\} \\ &= \{\dots, -11, -6, -1, 4, 9, 14, 19, 24, \dots\} \end{aligned}$$

So, clearly, $[4]_9 = [9]_5$.

If $x \equiv a \pmod{n}$ and $0 \leq a \leq n - 1$, then a is called the *least (nonnegative) residue* of x modulo n.

1.6.2 Modular Arithmetic

Theorem For all $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
1. $a \pm b \equiv c \pm d \pmod{n}$,
2. $a \cdot b \equiv c \cdot d \pmod{n}$,
3. $a^m \equiv b^m \pmod{n}, \ \forall m \in \mathbb{N}$

Theorem For all $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
1. $[a \pm b]_n = [c \pm d]_n$,
2. $[a \cdot b]_n = [c \cdot d]_n$,
3. $[a^m]_n = [b^m]_n, \ \forall m \in \mathbb{N}$

- $$\begin{aligned} [a]_n + [b]_n &= [a+b]_n \\ [a]_n - [b]_n &= [a-b]_n \\ [a]_n \cdot [b]_n &= [a \cdot b]_n \end{aligned}$$

▼ Example: Let $n = 12$, then

$$\begin{aligned} &[7]_{12} +_{12} [8]_{12} = [7+8]_{12} = [15]_{12} = [3]_{12}, \\ &[7]_{12} -_{12} [8]_{12} = [7-8]_{12} = [-1]_{12} = [11]_{12}, \\ &[7]_{12} \cdot_{12} [8]_{12} = [7 \cdot 8]_{12} - [56]_{12} = [8]_{12}. \end{aligned}$$

$$\hookrightarrow \begin{aligned} &7+8 = 15 \equiv 3 \pmod{12} \\ &7-8 = -1 \equiv 11 \pmod{12} \\ &7 \cdot 8 = 56 \equiv 8 \pmod{12} \end{aligned}$$

Theorem The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n has the following properties with respect to addition:
1. Closure: $[x] + [y] \in \mathbb{Z}/n\mathbb{Z}$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
2. Associative: $([x] + [y]) + [z] = [x] + ([y] + [z])$, for all $[x], [y], [z] \in \mathbb{Z}/n\mathbb{Z}$.
3. Commutative: $[x] + [y] = [y] + [x]$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
4. Identity, namely, $[0]$.
5. Additive inverse: $-[x] = [-x]$, for all $[x] \in \mathbb{Z}/n\mathbb{Z}$.

Theorem The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n has the following properties with respect to multiplication:
1. Closure: $[x] \cdot [y] \in \mathbb{Z}/n\mathbb{Z}$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
2. Associative: $([x] \cdot [y]) \cdot [z] = [x] \cdot ([y] \cdot [z])$, for all $[x], [y], [z] \in \mathbb{Z}/n\mathbb{Z}$.
3. Commutative: $[x] \cdot [y] = [y] \cdot [x]$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
4. Identity, namely, $[1]$.
5. Distributivity of multiplication over addition: $[x] \cdot ([y] + [z]) = ([x] \cdot [y]) + ([x] \cdot [z])$, for all $[x], [y], [z] \in \mathbb{Z}/n\mathbb{Z}$.

Two integers x and y are said to be multiplicative inverses if $xy \equiv 1 \pmod{n}$, where n is a positive integer greater than 1.

Theorem The multiplicative inverse $1/b$ modulo n exists *iff* $gcd(b, n) = 1$.

Corollary There are $\phi(n)$ numbers b for which $1/b \pmod{n}$ exists.

Corollary The division a/b modulo n (assume that a/b is in lowest terms) is possible *iff* $1/b \pmod{n}$ exists.

Theorem $\mathbb{Z}/n\mathbb{Z}$ is a field *iff* n is prime.

Let $1/a \pmod n = x$, which is equivalent to $ax \equiv 1 \pmod n$.
Since $ax \equiv 1 \pmod n \iff ax - ny = 1$.

So finding the inverse becomes finding the solution of the linear Diophantine equation $ax - ny = 1$.

▼ Example: Find...

▼ $1/154 \pmod{801}$

find x and y in $154x - 801y = 1$.

$$\begin{aligned} 801 &= 154 \cdot 5 + 31 \\ 154 &= 31 \cdot 4 + 30 \\ 31 &= 30 \cdot 1 + 1 \\ 30 &= 10 \cdot 3 + 0. \end{aligned}$$

Since gcd(154, 801) = 1, and the equation $154x - 801y = 1$ is soluble.

we now work backwords from the above equations

$$\begin{aligned} 1 &= 31 - 30 * 1 \\ &= 31 - (154 - 31 * 4) * 1 \\ &= 31 - 154 + 4 * 31 \\ &= 5 * 31 - 154 \\ &= 5 * (801 - 154 * 5) - 154 \\ &= 5 * 801 - 26 * 154 \\ &= 801 * 5 - 154 * 26 \end{aligned}$$

So, $x \equiv -26 \equiv 775 \pmod{801}$, that is, $1/154 \mod 801 = 775$.

▼ $4/154 \pmod{801}$

Since $4/154 \equiv 4 \cdot 1/154 \pmod{801}$, then $4/154 \equiv 4 \cdot 775 \equiv 697 \pmod{801}$.

$$\begin{aligned} 777, &\quad 154 \cdot 777 \equiv 11 \pmod{803} \\ 777 + 803/11 \equiv 47, &\quad 154 \cdot 47 \equiv 11 \pmod{803} \\ 777 + 2 \cdot 803/11 \equiv 120, &\quad 154 \cdot 120 \equiv 11 \pmod{803} \\ 777 + 3 \cdot 803/11 \equiv 193, &\quad 154 \cdot 193 \equiv 11 \pmod{803} \\ 777 + 4 \cdot 803/11 \equiv 266, &\quad 154 \cdot 266 \equiv 11 \pmod{803} \\ 777 + 5 \cdot 803/11 \equiv 339, &\quad 154 \cdot 339 \equiv 11 \pmod{803} \\ 777 + 6 \cdot 803/11 \equiv 412, &\quad 154 \cdot 412 \equiv 11 \pmod{803} \\ 777 + 7 \cdot 803/11 \equiv 485, &\quad 154 \cdot 485 \equiv 11 \pmod{803} \\ 777 + 8 \cdot 803/11 \equiv 558, &\quad 154 \cdot 558 \equiv 11 \pmod{803} \\ 777 + 9 \cdot 803/11 \equiv 631, &\quad 154 \cdot 631 \equiv 11 \pmod{803} \\ 777 + 10 \cdot 803/11 \equiv 704, &\quad 154 \cdot 704 \equiv 11 \pmod{803}. \end{aligned}$$

Theorem (Fermat's little theorem) Let a be a positive integer, and p prime. If gcd(a, p) = 1, then $a^{p-1} \equiv 1 \pmod p$.

Theorem (Euler's theorem) Let a and n be positive integers with gcd(a, n) = 1. Then $a^{\phi(n)} \equiv 1 \pmod n$.

Theorem (Carmichael's theorem) Let a and n be positive integers with gcs(a, n) = 1. Then $a^{\lambda(n)} \equiv 1 \pmod n$.