Ch2 Defs & Thms

Def ① congruent modular N

let $a, b \in \mathbb{Z}$, $N \in \mathbb{Z} \neq 0$

Say: a is congruent to b mod N

$\boxed{a \equiv b \mod N}$

if $\boxed{N \mid (a-b)}$

($\equiv$ mod N is one piece, like =)

Def ② congruent class

$$\boxed{[a]_N = \{ b \in \mathbb{Z} \mid b \equiv a \mod N \}}$$

Thm ① 2.1

(1) $a \equiv a \mod N$ (reflective)

(2) $a \equiv b \mod N \Leftrightarrow b \equiv a \mod N$ (symmetric)

(3) $\begin{cases} a \equiv b \mod N \\ b \equiv c \mod N \end{cases} \Rightarrow a \equiv c \mod N$ (transitive)

Def ③

$\mathbb{Z}_n$: The set of all congru classes mod N

(by Collary ② 2.5 (2), $\boxed{|\mathbb{Z}_n| = n}$ (have n elements))

Def ④ Congruent Class +, ×.

(简写 $\mathbb{Z}_n$ 中的 $[a]_n$ 为 $[a]$).

$\mathbb{Z}_n$ 上,

(def: $[a]^k = [a] \odot [a] \odot \cdots \odot [a]$ (k 个))

def: $\boxed{\begin{aligned} [a] \oplus [c] &= [a+c] \\ [a] \odot [c] &= [ac] \end{aligned}}$

Thm ③ 2.6

if $\mathbb{Z}_n$ 上, $[a]=[c]$, $[b]=[d]$

$$\Rightarrow \boxed{\begin{cases} [a+c] = [b+d] \\ [ac] = [bd] \end{cases}}$$

Thm ② 2.2

(1) $\begin{cases} a \equiv c \mod N \\ b \equiv d \mod N \end{cases} \Rightarrow (a+c) \equiv (b+d) \mod N$

(2) $\begin{cases} a \equiv c \mod N \\ b \equiv d \mod N \end{cases} \Rightarrow (ab) \equiv (cd) \mod N$

Collary ① 2.4

$[a]_N$ and $[b]_N$ are either identical or disjoint

($[a]_N = [b]_N$) ($[a]_N \cap [b]_N = \emptyset$)

iff $b = a + kN$, $k \in \mathbb{Z}$.

Collary ② 2.5

(1) Let $N \in \mathbb{Z}_{>1}$, $a \in \mathbb{Z}$

if $a = kN + r$, $k \in \mathbb{Z}$

$\Rightarrow [a] = [r]$

(2) There are N distinct congru classes mod N : $\boxed{[0], [1], \ldots, [N-1]}$

(dividing $\mathbb{Z}$ into N subsets)

Thm ④ 2.7 Properties of Modular Arithmetic

$\forall [a], [b], [c] \in \mathbb{Z}_n$,

A

1. $[a], [b] \in \mathbb{Z}_n \Rightarrow ([a] + [b]) \in \mathbb{Z}_n$ (closure)
2. $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$ (asso)
3. $[a] \oplus [b] = [b] \oplus [a]$ (comm)
4. $[a] \oplus [0] = [a]$ (0_e)
5. $\forall [a] \in \mathbb{Z}_n$, $\exists X \in \mathbb{Z}_n$ s.t. $[a] \oplus X = [0]$ ($+^{-1}$)

M

(比field 少条 $\times^{-1}$)

6. $[a], [b] \in \mathbb{Z}_n \Rightarrow [a] \odot [b] \in \mathbb{Z}_n$ (closure)
7. $[a] \odot ([b] \odot [c]) = ([a] \odot [b]) \odot [c]$ (asso)
8. $[a] \odot [b] = [b] \cdot [a]$ (comm)
9. $[a] \odot [1] = [a]$ (1_e)

D

10. $[a] \odot ([b] \oplus [c]) = [a] \odot [b] + [a] \odot [c]$ AND $([a] \oplus [b]) \odot [c] = [a] \odot [c] \oplus [b] \odot [c]$ (distri)

Thm ⑤ 2.8 $\mathbb{Z}_p$中存在M. x^{-1} 的条件

let $p \in \mathbb{Z}_{>1}$

$\Rightarrow$ The three condition are equiv.

(1) p is prime (∃ multi^{-1})

(2) $\boxed{\forall [a] \neq [0] \in \mathbb{Z}_p,\ \exists X \in \mathbb{Z}_p \text{ s.t } [a]X = 1}$

(3) Whenever $[b] \odot [c] = [0]$ ($\in \mathbb{Z}_p$)

$\Rightarrow [b] = [0]$ or $[c] = [0]$.

Thm ⑥ 2.9

Let $a, n \in \mathbb{Z}$, $n > 1$.

$\Rightarrow$ $\boxed{[a]X = [1]}$ has sol X $\boxed{\text{in } \mathbb{Z}_n}$

iff $\boxed{(a,n) = 1}$

Def ⑤ Unit, Inverse.

$[a] \in \mathbb{Z}_n$ is called a $\boxed{\text{unit}}$

if $[a]X = 1$ has sol in $\mathbb{Z}_n$.

(I.O.W, $\exists [b] \in \mathbb{Z}_n$ s.t. $[a] \odot [b] = 1$)

称 $[b]$ (即解出的 X) 为$[a]$的 inverse

(注意，那么$[b]$也是一个 unit)

($\Rightarrow$ by def ⑤, Thm ⑥ 2.9 可写为

$[a] \in \mathbb{Z}_n$ is a unit

iff $(a,n) = 1$.)