"Congruence"的概念是对 equality relation 的 generalization.

$a,b\in\mathbb{Z}\Rightarrow \boxed{a=b}$ iff $a-b=0$

而 $\boxed{a\equiv b\ (\mathrm{mod}\ n)}$ iff $a-b=nk$ for some $k\in\mathbb{Z}$.

即 $n\mid(a-b)$

Thm ①

Thm ① (2.1) Thm ① 是对于 equality 的三个性质的类比.

equality:
1. reflexive: $\forall a\in\mathbb{Z}$ $a=a$
2. symmetric: $a=b\Rightarrow b=a$ (易证)
3. transitive: $a=b$ AND $b=c\Rightarrow a=c$

congruence modulo n:
1. reflective: $a\equiv a\ (\mathrm{mod}\ n)$
2. symmetric: $a\equiv b\ (\mathrm{mod}\ n)\Rightarrow b\equiv a\ (\mathrm{mod}\ n)$
3. transitive: $a\equiv b\ (\mathrm{mod}\ n)$ AND $b\equiv c\ (\mathrm{mod}\ n)\Rightarrow a\equiv c\ (\mathrm{mod}\ n)$

Def ② Congruent class $[a]_N$

易见有 N 个 $[a]_N$，把 $\mathbb{Z}$ 切分为 N 份

比如 $[a]_3$ 有3个: $[0]_3$, $[1]_3$, $[2]_3$

$[0]_3=\{0,3,6,9,\dots\}$, $[1]_3=\{1,4,7,10,\dots\}$, $[2]_3=\{2,5,8,11,\dots\}$

C(2) 证明 $[a]_N$ 和 $[b]_N$ 不是相等就是 disjoint. (Collary ① 2.4)

Pf. Suppose $[a]_N\cap[b]_N\neq\emptyset$

那么 let $x\in[a]_N\cap[b]_N$

$\Rightarrow x\equiv a\ \mathrm{mod}\ N$,

$x\equiv b\ \mathrm{mod}\ N$

by Thm①, $\boxed{a\equiv b\ \mathrm{mod}\ N}$ (1)

WTS: $[a]_N\subseteq[b]_N$

那么就随便取一个 $y\in[a]_N\Rightarrow y\equiv a\ \mathrm{mod}\ N$

又(1) $\Rightarrow y\equiv b\ \mathrm{mod}\ N$

$\Rightarrow y\in[b]_N$

同样可证明 $[b]_N\subseteq[a]_N$

$\Rightarrow [a]_N=[b]_N$

因而要么 disjoint 要么 equiv.

D(4) $\forall a\in\mathbb{Z}$, $[a]_{60}\subseteq[a]_{10}$

Let $a+60k$ be an arbi elem $\in[a]_{60}$

write $a+60k=a+10(6k)$

$\Rightarrow (a+60k)\in[a]_{10}\Rightarrow[a]_{60}\subseteq[a]_{10}$

E(2) 这个 rule 是否为一个 function?

$[a]_7\mapsto\left[\text{"round down } a \text{ to 最近的10的倍数"}\right]_7$

答案是不是.

Consider: $x=[0]_7$ $(=[14]_7=[35]_7=\dots)$

a 可以是 0, 14, 35, ...,

$[0]_7$, $[10]_7$, $[30]_7$ 不同

一个 x 有多个 $f(x)$. X

E(3) 这个 rule 是否为一个函数?

$[a]_7\mapsto[-a]_7$

是的.

问题即: 如果 $x=[a]_7=[b]_7=\dots$

那么会得到同一个 $y=[-a]_7=[-b]_7=\dots$

这个问题就是求证:

如果 $[a]_7=[b]_7$

那么 $[-a]_7=[-b]_7$

实际上容易证明:

$[a]_7=[b]_7\Rightarrow 7\mid(a-b)$

$(a-b)=7c$ for some $c\in\mathbb{Z}$

$\Rightarrow (-a)-(-b)=-(a-b)=-7c$

F(1),(2) Show if $a\equiv c\ \mathrm{mod}\ N$

$b\equiv d\ \mathrm{mod}\ N$

$\Rightarrow (a+b)\equiv(c+d)\ \mathrm{mod}\ N$

$ab\equiv(cd)\ \mathrm{mod}\ N$

(Thm 2.2)

Pf 条件即 $a-c=nk$, $b-d=nt$ for some $k,t\in\mathbb{Z}$.

$\Rightarrow$ (1)

$(a+b)-(c+d)=nk+nt=n(k+t)$

(2)

$ab-cd = ab-bc+bc-cd$
$= b(a-c)+c(b-d)$
$= bnk + cnt = n(bk+ct)$

E(3) 即课本的 Def ④.
并且其是 well-defined 的. (即 Pf: Thm 2.6)

这里定义: $[a] \oplus [c] = [a+c]$
$[a] \otimes [c] = [ac]$

Pf of well-definedness:
(即证明如果 $[a]=[b]$, $[c]=[d]$ $\in \mathbb{Z}_n$,
那么 $[a+c]=[b+d]$
$[ac]=[bd]$)
其实就是复述 Thm 2.2.