1. $\mathbb{Z}_n$ 上 $+, \times$ operation 的 well-definedness.

$+$ 显然, $\times$: (1) $[a]_N \cdot [b]_N = [ab]_N$

$\forall x \in [a], y \in [b]$

$\Rightarrow x = a + ka$
$y = b + lb$

$\Rightarrow xy = ab + (k+l)ab + kl\,ab = (1+k+l+kl)ab$

$ab \mid xy$.

2. $\mathbb{Z}_n$ 具有 除 X^{-1} 外所有 field 的性质 $(\overset{3}{A}, \overset{5-1}{M}, \overset{2}{D})$

易证.

C. (3) Show: if $(a, N) = 1$, then $[a]X = [1]$ has a sol in $\mathbb{Z}_n$ (Thm 6 2.9 Part 1)

By Thm 1.2 : $(a, N) = 1$

$\Rightarrow \exists\, r, s \in \mathbb{Z}$ s.t. $ar + Ns = (a, N) = 1$

$\Rightarrow Ns = 1 - ar \Rightarrow ar = -s \cdot N + 1$

$\Rightarrow ar \bmod N = 1$ $\quad [a]_N [r]_N = [1]_N$

(4) Corollary 1: 证明这个 sol 是 unique 的.

Pf. assume $[a][x_1] = [a][x_2] = [1]$

$\Rightarrow [a][x_1 - x_2] = [0]$

由(2) (也是易知), $\because [a] \neq 0 \quad \therefore [x_1 - x_2] = [0]$

$\Rightarrow [x_1] = [x_2]$

(4) Corollary 2: 不仅 $[a]X = [1]$ 有 unique sol, $[a]X = [b]$ 也有 unique sol.

Pf (易证) 我们已证: $\exists\, r$ 使 $[a][r] = 1$

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

$[a][br] = [b]$

$\therefore X = [br]$ 为 sol.

For uniqueness, 和 (3) 完全相同.

C. 补充证明:

如果 $[a]X = 1$ 有 sol, 那么 $(a, N) = 1$ ($[r]$)

$\Downarrow$

$\exists k$, 使 $ar - 1 = kN$

$1 = ar + kN$

因而 1 是 a, N 的一个 linear combination

我们知道 a, N 的 linear combination 一定会被 (a, N) 整除. (by hw 1)

$\Rightarrow$ 因而 $(a, N) \mid 1$

所以 (a, N) 只可能为 1.

D (Proof of Thm 5 2.8)

(1) 如果 p 是 prime 且 $[a] \neq [0]$, then $[a]x = [1]$ 在 $\mathbb{Z}_p$ 上有 sol.

p 是 prime 且 $[a]_p \neq [0]_p \Rightarrow p \nmid a$ ($a = kp + c,\ 0 < c < p$)

因而 $(a, p) = 1$ $\Rightarrow$ By C 即得 $[a]X = [1]$ 有 sol

E. (2) Let $a, n \in \mathbb{Z}$, not both 0.

Prove: $\{ra + sn \mid r, s \in \mathbb{Z}\}$

$= \{k \cdot (a, n) \mid k \in \mathbb{Z}\}$

就是说: 任意两个 int (不都为 0) 的任何 linear comb 都是它们 gcd 的倍数. 并且 gcd 的任何倍数都是这两个数的 linear comb

Denote: $P = \{ra + sn \mid r, s \in \mathbb{Z}\}$

$Q = \{k(a, n) \mid k \in \mathbb{Z}\}$

(1) $Q \subseteq P$: By Bezout, $(a, n) = au + nv$ for some u, v

$\Rightarrow k(a, b) = (ku)a + (kv)n \in Q$

(2) $P \subseteq Q$: $(a, n) \mid a$, $(a, n) \mid n$

$\Rightarrow (a, n) \mid$ 任意 $ra + sn$.

$\Rightarrow \exists k \in \mathbb{Z}$, 使 $k(a, n) = ra + sn$.

(3) 何时 $[a]_N X = [b]_N$ 有sol，
何时有多个sol？

由(2)可总结：任何两 int
linear comb = gcd 倍数

因而 $b = ra + sN$ (即 $[a]_N = [b]_N$ 有sol)

iff $b = k(a,N)$ (即 $(a,N) \mid b$.)

例如：$[9]_{12} X = [3]_{12}$

有sol $\{[3], [7], [11]\}$

(3 是 $(9,12)=3$ 的倍数)

我们发现：每个 sol 间隔为 4
而 $4 \cdot (3,12)$ 即 $4 \cdot 3 = 12$.

何时有多个sol？
(N如果是(a,N)的d倍)

如果有 $d \in \mathbb{Z}$ 使 $d(a,N) = N$

$\Rightarrow ad = a \cdot \frac{N}{(a,N)}$

$\because (a,N) \mid a$

$\therefore ad$ 是 N 的倍数 $\Rightarrow [ad]_N = [0]_N$

$\Rightarrow [a](X + [d]) = [0]$

因为 $[r+kd]_N$ 也是解 (r满足 $r+kd<N$)