Chapter 2 part 7

Th 2.9 Let $n>1$, $a\in\mathbb{Z}$.

The equation $[a]\odot x=[1]$ has a solution iff $(a,n)=1$.
in $\mathbb{Z}_n$

$a\in\mathbb{Z}$ is called unit if the equation $ax=1$ has a solution in $\mathbb{Z}_n$
in $\mathbb{Z}_n$

Th 2.10 Let $n>1$ be an integer

$a\in\mathbb{Z}_n$ is a unit in $\mathbb{Z}_n$ iff $(a,n)=1$ (in $\mathbb{Z}$)

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

If $(a,n)=1$, then $(b,n)=1$ for any b such that $[b]=[a]$.

Special case $n=p$ is a prime

Theorem 2.10 reads:

In $\mathbb{Z}_p$ every non-zero element is a unit.

$0=[0]$ – all integers divisible by p

$[1],\dots,[p-1]$ – non-zero classes; for any of them, $[r]$, we have $(r,p)=1$

because $0 < r < p$, therefore $p \nmid r$.

Equivalently, Th 2.10 tells us that for any $a \in \mathbb{Z}_p$, $a \neq 0$, the equation $ax = 1$ in $\mathbb{Z}_p$ has a (unique) solution

<u>Th 2.8</u> The following statements are equivalent:

(1) p is prime

(2) for any $a \neq 0$, the equation $ax = 1$ has a solution in $\mathbb{Z}_p$

(3) $bc = 0$ in $\mathbb{Z}_p$ implies $b = 0$ or $c = 0$ (or both)

<u>Pf</u> (1) implies (2); (2) implies (3); (3) implies (1)

<u>(1) implies (2)</u> follows from Th 2.10 as above.

<u>(2) implies (3)</u>

Let $bc = 0$. <u>If $b \neq 0$, then</u> b is a unit in $\mathbb{Z}_p$.

Therefore b has an inverse, a so that $ab = 1$.

$$abc = 0 \quad \text{in } \mathbb{Z}_p$$

$$1 \cdot c = 0$$

$$\underline{c = 0} \quad \text{in } \mathbb{Z}_p$$

(3) implies (1)

Example $\mathbb{Z}_6$:

$\dot{2} \neq \dot{0} \quad \dot{3} \neq \dot{0} \quad \dot{2}\cdot\dot{3} = \dot{6} = \dot{0}$

Counterpositive: if p is not a prime, then (3) is not true in $\mathbb{Z}_p$

$p = bc$ as integers (in $\mathbb{Z}$) (positive) $b < p$, $c < p$ implies $p \nmid b$ and $p \nmid c$

as congruence classes (in $\mathbb{Z}_p$) $\dot{b} \neq \dot{0}$ and $\dot{c} \neq \dot{0}$.

while $\dot{b}\dot{c} = \dot{p} = \dot{0}$ in $\mathbb{Z}_p$