33 Modular Arithmetic,

~~Def:~~ (1) $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

(2) $a \oplus b = (a+b) \bmod n$

(3) $a \otimes b = (ab) \bmod n$

eg.: $n = 7$

$1 \oplus 3 = 4$ $\qquad$ $2 \otimes 3 = 6$

$4 \oplus 5 = 2$ $\qquad$ $2 \otimes 5 = 3$

Prop. 33.3: Let $a, b \in \mathbb{Z}_n$. Then $a \oplus b$, $a \otimes b \in \mathbb{Z}_n$

Pf: When dividing by n the remainder is between 0 & $n-1$. Thus, for any $x \in \mathbb{Z}$, $x \bmod n \in \mathbb{Z}_n$ ∎

[redacted] [redacted] 152

Prop 36.4 [redacted]: $\$ \; n \geq 2$.

1.) $\forall a, b \in \mathbb{Z}_n$, $\quad a \oplus b = b \oplus a$; $a \otimes b = b \otimes a$.

2.) $\forall a, b, c \in \mathbb{Z}_n$, $\quad a \oplus (b \oplus c) = (a \oplus b) \oplus c$; $(a \otimes b) \otimes c = a \otimes (b \otimes c)$

3.) $\forall a \in \mathbb{Z}_n$, $\quad a \oplus 0 = a$; $a \otimes 1 = a$; $a \otimes 0 = 0$.

4.) $\forall a, b, c \in \mathbb{Z}_n$, $\quad a \otimes (b \oplus c) = (a \otimes b) + (b \otimes c)$,

Pf: We will show that $\oplus$ is associative. The proofs of the other assertions are similar.

- **Prop 365:**
  Let $n>0$; $a,b \in \mathbb{Z}_n$. Then there is one and only one $x \in \mathbb{Z}_n$ s.t. $a = b \oplus x$.
- **Pf:** Put $x = (a-b) \pmod n$

Def: (Modular Subtraction)
Let $n>0$; $a,b \in \mathbb{Z}_n$. We define $a \ominus b$ to be the unique $x \in \mathbb{Z}_n$ so that $a = b \oplus x$.

Prop 36.7:

$$a \ominus b = a - b \pmod{n}$$

Pf: Follows immediately from Prop 36.5

Modular Division:

eg: Take $n = 10$. In $\mathbb{Z}_{10}$ we have

$$5 \otimes 2 = 5 \otimes 4$$

However $2 \neq 4$.

* We must take care when performing division in $\mathbb{Z}_n$.

Def: (Modular Reciprocal (or inverse))

1. Let $n \geq 1$ & $a \in \mathbb{Z}_n$. A reciprocal or inverse of a is an element $b \in \mathbb{Z}_n$ s.t.

$$a \otimes b = 1.$$

2. An element $a \in \mathbb{Z}_n$ which has an inverse is said to be invertible.

- eg.! In $\mathbb{Z}_6$, we have

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Note: Only 1 and 5 are invertible.

- Prop 38.10: Let $n \geq 1$; $a \in \mathbb{Z}_n$. If a is invertible, then its inverse is unique.

- Pf: Suppose $a \otimes b = 1$; $a \otimes c = 1$

Then

$$b = b \otimes 1 = b \otimes (a \otimes c) = (b \otimes a) \otimes c$$

$$= (a \otimes b) \otimes c = 1 \otimes c = c \quad \blacksquare$$

Prop 36.11: $\$$ $n \geq 1$; $a \in \mathbb{Z}_n$. $\$$ a is invertible. If $b = a^{-1}$ then $a = b^{-1}$. That is,

$(a^{-1})^{-1} = a$.

Pf: exercise.

Def: Let $n \geq 1$ and let $b \in \mathbb{Z}_n$ be invertible. If $a \in \mathbb{Z}_n$ then

$$a \oslash b = a \otimes b^{-1}$$

eg: In $\mathbb{Z}_{10}$, calculate

$5 \oslash 3$.

Thm 36.14:

Let $n \geq 1$; $a \in \mathbb{Z}_n$. a is inv. iff $(a,n)=1$.

Pf: