

Section 36 - modular arithmetic

Def: Let  $n$  be a positive integer. Then  $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$

Def: Let  $n$  be a positive integer and let  $a, b \in \mathbb{Z}_n$ . Then the *modular addition* and *modular multiplication* operators are defined by

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

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

Exs: If  $n = 5$ , then

$$2 \oplus 1 = 3 \bmod 5 = 3$$

$$2 \oplus 4 = 6 \bmod 5 = 1$$

$$2 \oplus 3 = 5 \bmod 5 = 0$$

$$2 \otimes 1 = 2 \bmod 5 = 2$$

$$2 \otimes 4 = 8 \bmod 5 = 3$$

We can use a table to summarize:

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Note that the modular addition table has Suduko property (no repeats in any row or column). The modular multiplication table does not. In  $\mathbb{Z}_6$ , we can see this even more clearly.

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	0	0	1
3	3	4	0	1	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\otimes_6$	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

Thus,  $\forall a, y \in \mathbb{Z}_n, \exists$  a unique  $x \in \mathbb{Z}_n$  so that  $a \oplus x = y$ . We may write  $x = y \ominus a$ .

However, there is not necessarily  $x \in \mathbb{Z}_n$  so that  $a \otimes x = y$ . For example, in  $\mathbb{Z}_6, 2 \otimes x \neq 3$  for any  $x \in \mathbb{Z}_6$ . And, while there is  $x \in \mathbb{Z}_6$  so that  $2 \otimes x = 4$ , it is not unique.

Def: Let  $n$  be a positive integer and let  $a \in \mathbb{Z}_n$ . Then a *reciprocal* of  $a$  is defined as  $b \in \mathbb{Z}_n$  such that  $a \otimes b = 1$ . If an element has a reciprocal, the element is called invertible and we denote its reciprocal by  $a^{-1}$ . Thus, in  $\mathbb{Z}_5, 2^{-1} = 3$  and in  $\mathbb{Z}_6, 2^{-1}$  does not exist.

Prop: Let  $n$  be a positive integer and let  $a \in \mathbb{Z}_n$ . If  $a$  has a reciprocal, it is unique.

(Sneaky) Proof : Suppose  $\exists b, c \in \mathbb{Z}_n$  with  $a \otimes b = 1$  and  $a \otimes c = 1$ .

$$\text{Then } b = b \otimes 1 = b \otimes (a \otimes c) = (b \otimes a) \otimes c = 1 \otimes c = c.$$

Def: Let  $n$  be a positive integer and let  $a \in \mathbb{Z}_n$  with  $a$  invertible. Then  $b \odot a = b \otimes a^{-1}$ .

Ex: In  $\mathbb{Z}_6$ ,  $4 \odot 2 = 4 \otimes 2^{-1} = 4 \otimes 3 = 0$ .

Theorem: Let  $n$  be a positive integer and let  $a \in \mathbb{Z}_n$ . Then  $a$  is invertible if and only if  $a$  and  $n$  are relatively prime.

Proof :  $(\implies)$  Hyp:  $a$  is invertible.

Then  $\exists b \in \mathbb{Z}_n$  so that  $a \otimes b = 1$ .

Thus  $(ab) \bmod n = 1$ .

So,  $ab = qn + 1$  for some  $q \in \mathbb{Z}$ .

Hence,  $ab - qn = 1$ .

Thus  $\gcd(a, n) = 1$  (by gcd Theorem from last time).

$(\impliedby)$  Hyp :  $\gcd(a, n) = 1$

Then  $\exists x, y \in \mathbb{Z}$  such that  $ax + ny = 1$ .

Let  $b = x \bmod n$ .

Then  $b - x = kn$  for some  $k \in \mathbb{Z}$ .

So  $x = b - kn$ .

So  $ax + ny = a(b - kn) + ny = ab - akn + ny = ab + n(y - ak)$ .

So  $ab = n(y - ak) + 1$  and  $y - ak \in \mathbb{Z}$ .

Thus  $a \otimes_n b = 1$ .

Homework: Section 36, P. 318 #1-4,12,13