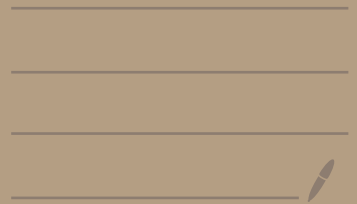


Day 4: Modular Arithmetic and Cyclic Groups.



Today

① Remainders

② Modular Arithmetic

③ Cyclic Groups

① Remainders.

Recall: Division is not always clean

$$8/2 = 4 \checkmark$$

$$7/2 = 3.5 \times$$

For unclear division, we say there is a remainder

$$7/2? \rightarrow 7 = \underline{3} \cdot 2 + \underline{1}$$

quotient remainder

$$15/4 \rightarrow 13 = 3 \cdot 4 + \underline{3}$$

 remainder

definition: For integer n and positive integer d , if

$$n = q \cdot d + r$$

for integers q, r with $0 \leq r < d$,
 r is the remainder when d divides n .

alternate definition:

the **remainder** when d divides n is the least non-negative r such that d cleanly divides $n-r$.

if r is the remainder when d divides n , we also say:

- r is " n reduced modulo d "
- r is " $n \bmod d$ "
- r is " $n \% d$ "

Python:

```
>>> 7 % 2
1
>>> 13 % 3
1
```

Q: What about negative n ?

```
>>> -1 % 6
5
>>> -3 % 7
4
```

A: They work too!

[2] Modular Arithmetic

• A new kind of arithmetic where you reduce all numbers modulo some fixed integer p .

→ For us, p will be prime, like 2, 3, 5, 7, or $2^{255}-19$

• Examples: (mod 5)

• $4 + 2 = 1$ ($4 + 2 = 6, 6 \% 5 = 1$)

• $3 + 4 = 2$ ($3 + 4 = 7, 7 \% 5 = 2$)

• $2 \times 4 = 3$

• $4 \times 4 = 1$

• $7 - 3 = 4$

• $2 - 4 = 3$ ($2 - 4 = -2, -2 \% 5 = 3$)

It really is prime! ↴

How does \div work?

We treat $3/2$ as $3 \times \boxed{\frac{1}{2}}$ ← what is this?

Key fact: for all n , $\frac{1}{n} \cdot n = 1 \pmod{p}$.

How do we find y s.t. $y = \frac{1}{n}$ or $y = n^{-1}$?

Python can do it!

pow function: `pow(base, exponent, modulus)`

`pow(n, -1, p)` gives n^{-1} (a.k.a. $\frac{1}{n}$)

`>>> pow(2, -1, 7)` $4 \cdot 2 = 8, 8 \% 7 = 1 \checkmark$

`>>> pow(3, -1, 13)` $3 \cdot 9 = 27, 27 \% 13 = 1 \checkmark$

Recap: Modular arithmetic

$+$, $-$, \times : normal operation, followed by $\% p$.

$\times / y : (x \cdot \text{pow}(y, -1, p)) \% p$

"Theorem": arithmetic "works" modulo primes:

- $+$, \times are commutative & associative
- $\frac{1}{n}$ always exists (when $n \neq 0$).
- $x + 0 = x$ • associative property ✓
- $x \cdot 1 = x$ • ...

2a) Groups.

A commutative group is:

- a set of objects, G
- a way to multiply them
- a way to take inverses
- an identity $1 \in G$ s.t.

for any $G \in G$, $1 \cdot G = G$.

example: integers mod 7 (except 0)

$\{1, 2, 3, 4, 5, 6\}$

$$x \cdot y = (x \times y) \% 7$$

$$x^{-1} = \text{pow}(x, -1, 7)$$

1.

Fact: The integers modulo any prime p (if we exclude 0) are a commutative group. This group is written $\sum_{\substack{* \\ \text{integers} \\ P \leftarrow \text{mod } p}}$ \leftarrow multiplication

Q: Why not 0?

A: It has no inverse $0 \cdot \text{any } x = 0 \neq 1$

Definition: For $G \in G$ and positive integer $n \in \mathbb{N}$,

$$G^n = \underbrace{G \times G \times \dots \times G}_{n \text{ times}}$$

ex: (mod 5)

$$4^4 = \underbrace{4 \cdot 4}_{16} \cdot \underbrace{4 \cdot 4}_{16} = 1 \pmod{5}$$

256 \nearrow

Definition: The order of a group is the size of the set.

The order of $G \in G$ is the least positive integer

n s.t. $G^n = 1$.

Example: order of 2 in \mathbb{Z}_5^*

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8 \rightarrow 3$$

$$2^4 = 16 \rightarrow 1 \quad \checkmark \text{ order is 4.}$$

Definition: a **cyclic group** is a group G where all elements are powers of a **generator** $g \in G$.

Example: $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ are all

generated by 2: $\left. \begin{array}{l} 2^1 = 2 \\ 2^2 = 4 \\ 2^3 = 3 \\ 2^4 = 1 \end{array} \right\} \text{ all of the integers} \\ \text{mod } 5, \text{ save } 0.$

So, \mathbb{Z}_5^* is a cyclic group with generator 2.

Consider just $\{1, 4\}$ from \mathbb{Z}_5^* , 4 generates

this (sub) group: $4^1 = 4$
 $4^2 = 1$

For public-key cryptography we will use

cyclic groups of prime order. The order

will be **HUGE**: approximately 2^{255} (256 bits).