

## Lecture 3 Congruences §1.3

2022/4/1

(See also §2.5 w/ a short intro to groups  
§2.10.1 w/ a short intro to rings)

Goal Diffie-Hellman & Discrete log problem  
Next Friday.

Today & Monday we'll be talking about the algebra background we need for Diffie-Hellman.

On Wednesday, we'll discuss a bit more about the theory of cryptosystems.

### Last time

- Euclidean algorithm computing  $\gcd(a, b)$
- Extended Euclidean algorithm computing  $u$  &  $v$  w/  
 $au + bv = \gcd(a, b)$ .

Def Suppose  $a, b$ , &  $m \in \mathbb{Z}$ ,  $m \geq 1$ .

Say  $a$  &  $b$  are equivalent mod  $m$  or

'eg 1 8  
Congruent mod m if  $m \mid (b-a)$ .  
7  $\mid$  (1-8)

Notation  $a \equiv b \pmod{m}$   
1  $\equiv$  8  $\pmod{7}$

m is called the modulus.

$$[a]_m = \{ b \in \mathbb{Z} : b \equiv a \pmod{m} \}$$
$$= \{ a + km : k \in \mathbb{Z} \}$$

is the Congruence class of a.

$$a \equiv b \pmod{m} \Leftrightarrow [a]_m = [b]_m.$$

Let  $\mathbb{Z}/m\mathbb{Z}$  or  $\mathbb{Z}/m$  denote the set of congruence classes mod m.

By division algorithm, can write

$$a = mq + r \quad w/ \quad 0 \leq r < m.$$

$a - r = mq$  is divisible by  $m$ , so

$$a \equiv r \pmod{m}.$$

$$\Rightarrow \mathbb{Z}/m\mathbb{Z} = \{ [0]_m, [1]_m, \dots, [m-1]_m \}$$

Every congruence class has a representative between 0 &  $m-1$ .

Congruence mod  $m$  is an equivalence relation.

It is:

• reflexive: for all  $a \in \mathbb{Z}$ ,  $a \equiv a \pmod{m}$

$$[\text{Proof: } m \mid (a-a) = 0.]$$

• symmetric for all  $a, b \in \mathbb{Z}$ ,

$$a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$$

$$[\text{Proof } m \mid (b-a) \Leftrightarrow m \mid (a-b).]$$

• transitive: for all  $a, b, c \in \mathbb{Z}$ ,

$$a \equiv b \pmod{m} \ \& \ b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$$

Proof If  $m \mid (b-a)$  &  $m \mid (c-b)$   
 then  $m \mid [(c-b) + (b-a)] = c-a$

So congruence mod  $m$  is reasonable to use like equality.

We can define  $+$ ,  $\times$  on  $\mathbb{Z}/m\mathbb{Z}$ .

Ex  $\mathbb{Z}/4\mathbb{Z} = \{ [0]_4, [1]_4, [2]_4, [3]_4 \}$ .

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

To check that this makes sense, need:

Prop if  $a \equiv a' \pmod{m}$  &  $b \equiv b' \pmod{m}$

then (1)  $a + b \equiv a' + b' \pmod{m}$

(2)  $a \cdot b \equiv a' \cdot b' \pmod{m}$

Proof (1)  $m \mid a - a'$  &  $m \mid b - b'$

$\Rightarrow m \mid a - a' + b - b' = (a+b) - (a'+b')$ .

$$(2) \quad m \mid (a-a')b + a'(b-b') = ab - a'b + a'b - a'b' \\ = ab - a'b'$$

Def A ring is a set  $R$  w/ operations

$+$  &  $\cdot$  &lt;math>\{0, 1\}</math> satisfying:

$$\bullet (a+b)+c = a+(b+c) \quad (+ \text{ is associative})$$

$$\bullet a+0 = a = 0+a \quad (0 \text{ is the unit for } +)$$

$$\bullet \text{For all } a, \exists b \text{ st. } a+b=0 \quad (\text{additive inverses})$$

$$\bullet a+b = b+a \quad (+ \text{ is commutative})$$

$$\bullet (a \cdot b) \cdot c = a \cdot (b \cdot c) \quad (\cdot \text{ is associative})$$

$$\bullet a \cdot 1 = a = a \cdot 1 \quad (1 \text{ is the unit for } \cdot)$$

$$\bullet a(b+c) = ab+ac \quad (\text{distributivity}) \\ (b+c)a = ba+ca$$

Ex  $\mathbb{Z}/m\mathbb{Z}$  is a ring.

This is our main example, but there are a lot more.

Ex  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \text{Mat}_{2 \times 2}(\mathbb{R}) \leftarrow$   $2 \times 2$  matrices of real #s.

$\text{Mat}_{2 \times 2}(\mathbb{Z}) \leftarrow 2 \times 2$  matrices of integers.

Note • Not required that non-zero elements have multiplicative inverses

• Not required that multiplication is commutative  
(for example, matrix multiplication is not commutative.)

We call an element that has a multiplicative inverse a unit.

Def An element  $a$  of a ring  $R$  is a unit if

$\exists b \in R$  s.t.  $ab = ba = 1$ .

We denote the set of units in  $R$  by  $R^\times$ .

In this case the inverse  $b$  is unique, so we write

$$a^{-1} = b.$$

Ex  $\mathbb{Z}/4\mathbb{Z}$ .

$x$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

1 & 3 are units, 0 & 2 are not.

(can tell if something is a unit by looking for a 1 in the column).

$$3 \cdot 3 = 1 \Rightarrow 3 = 3^{-1}.$$

$$(\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}. \quad \forall$$

x	1	3
1	1	3
3	3	1

We can multiply units to get a unit but adding units doesn't necessarily give a unit.

Prop  $a \in \mathbb{Z}/m\mathbb{Z}$  has an inverse if and only if  $\gcd(a, m) = 1$ .

In other words,  $(\mathbb{Z}/m\mathbb{Z})^\times = \{a \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1\}$

PF

$\Rightarrow$ ) Suppose  $u \in \mathbb{Z}/m\mathbb{Z}$  is the inverse of  $a$ .

$$\text{Then } ua \equiv 1 \pmod{m}$$

$$\Rightarrow ua = 1 + km \text{ for some } k \in \mathbb{Z}.$$

$$\Rightarrow ua - km = 1$$

$$\gcd(a, m) \mid a \ \& \ m \Rightarrow \gcd(a, m) \mid ua - km = 1$$

$$\Rightarrow \gcd(a, m) = 1.$$

$\Leftrightarrow$ )  $\gcd(a, m) = 1$  implies by the extended Euclidean algorithm that  $\exists u, v \in \mathbb{Z}$  s.t.  $au + mv = 1$

$$\text{So } au - 1 = -mv \quad \text{so } m \mid au - 1.$$

$$\text{So } au \equiv 1 \pmod{m}.$$

So  $u$  is the inverse of  $a$  &  $a$  is a unit.  $\square$

$$\text{Ex } (\mathbb{Z}/12\mathbb{Z})^\times \quad \gcd(a, 12) = 1 \Rightarrow 2 \nmid a \ \& \ 3 \nmid a.$$

~~0~~   1   ~~2~~ ~~3~~ ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11

$$(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}.$$

Def  $\phi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times$ , the Euler Totient function.

Note The word "totient" was introduced in a paper in  $\sim 1880$ . No explanation was given for where



"totient" comes from ----

$$\begin{aligned} \text{Ex } \phi(12) = 4 &= 12 - \underbrace{12\left(\frac{1}{2}\right)}_{\substack{\# \text{ of elts} \\ \text{divisible by 2}}} - \underbrace{12\left(\frac{1}{3}\right)}_{\substack{\text{elts div} \\ \text{by 3}}} + \underbrace{12\left(\frac{1}{6}\right)}_{\substack{\text{elts div} \\ \text{by 2 and 3.}}} \\ &= 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right). \end{aligned}$$

In general if  $m = p_1^{e_1} \cdots p_r^{e_r}$  where

$e_i \geq 1$  for all  $i$ , then

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$