# 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 <u>equivalent mod $m$</u> 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 $a$.

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

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

By division algorithm, can write

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

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

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

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

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

Congruence mod $m$ is an <u>equivalence relation</u>.

It is:

- reflexive: for all $a \in \mathbb{Z}$, $a \equiv a \bmod m$

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

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

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

  [Proof: $m \mid (b-a) \iff m \mid (a-b)$.]

- 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 |

| × | 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) $m \mid (a-a')b + a'(b-b') = ab - a'b + a'b - a'b'$

$= ab - a'b'$.

**Def** A ring is a set $R$ w/ operations $+$ & $\cdot$ & elts $0 \& 1$ satisfying:

- $(a+b)+c = a+(b+c)$ ($+$ is associative)
- $a+0 = a = 0+a$ ($0$ is the unit for $+$)
- For all $a$, $\exists\ b$ s.t. $a+b=0$ (additive inverses)
- $a+b = b+a$ ($+$ is commutative)
- $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ ($\cdot$ is associative).
- $a\cdot 1 = a = a\cdot 1$ ($1$ is the unit for $\cdot$)
- $a(b+c) = ab+ac$ (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** $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $Mat_{2\times 2}(\mathbb{R})$ ← 2x2 matrices of real #s.

$Mat_{2\times 2}(\mathbb{Z})$ ← $2\times 2$ matrices of integers.

Note · Not required that nonZero 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 $\mathbb{Z}/4\mathbb{Z}$.

| × | 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).

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

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

| $\times$ | 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 $a$.

Then $ua \equiv 1 \pmod m$

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

$\Rightarrow ua - km = 1$

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

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

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

So $au - 1 = -mv$ so $m \mid au - 1$.

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

So $u$ is the inverse of $a$ & $a$ is a unit. □

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

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 ~1880. No explanation was given for where

"totient" Comes from....

Ex $\phi(12) = 4 = 12 - \underbrace{12(1/2)}_{\#\text{ of elts divisible by 2}} - \underbrace{12(1/3)}_{\text{elts div by 3}} + \underbrace{12(1/6)}_{\text{elts div by 2 and 3.}}$

$= 12(1-1/2)(1-1/3).$

In general if $m = p_1^{e_1} \cdots p_r^{e_r}$ where $e_i \geq 1$ for all $i$, then

$$\phi(m) = m(1-1/p_1)\cdots(1-1/p_r)$$