Lecture 1

Recap:

1) GCD (a, b)
2) primes & factorization
3) FTA $\forall n \; \exists p_i$ s.t.

$\forall n = p_1 \cdots p_k$

Congruence & Modular arithmetic

Recall: " a divides $b \Leftrightarrow a \mid b$. "

Today: we say $a \equiv b \mod n$

$\boxed{n > 0}$ if $n \mid a - b$

In words, we say: " a is congruent to b mod n "

Ex: $27 \equiv 0 \mod 3$, $35 \equiv 1 \mod 17$

Prob 1: Congruence is an equivalence relation.

Recall, a relation " $\equiv$ " is equivalence iff it satisfies

1) $a \equiv a \quad \forall a$
2) $a \equiv b \Leftrightarrow b \equiv a, \; \forall b$
3) $a \equiv b,\; b \equiv c \Rightarrow a \equiv c$ $\forall a, b, c$.

Proof: Indeed, $a \equiv a \mod n$

as $n \mid 0 = a - a$

If $a \equiv b \mod n$ then

$n \mid a - b \Rightarrow n \mid b - a \Rightarrow b \equiv a \mod n$

If $a \equiv b \mod n$ & $b \equiv c \mod n$

$\Downarrow$ $\Downarrow$

$n \mid a - b$ $n \mid b - c$

$\Rightarrow n \mid a - b + b - c = a - c$

$\Rightarrow a \equiv c \mod n$. $\blacksquare$

Thus we can divide $\mathbb{Z}$ in congruence class modulo n.

Ex: Let $n = 5$

$-4 \equiv 1$	$1 \equiv 1$	$6 \equiv 1$	$\cdots$
$-3 \equiv 2$	$2 \equiv 2$	$7 \equiv 2$	$\cdots$
$-2 \equiv 3$	$3 \equiv 3$	$8 \equiv 3$	
$-1 \equiv 4$	$4 \equiv 4$	$9 \equiv 4$	$\vdots$
$0 \equiv 0$	$5 \equiv 0$	$10 \equiv 0$	

Thus $\mathbb{Z} = \{\ldots, -4, 1, 6, \ldots\} \cup \{\ldots, -3, 2, 7, \ldots\}$

$\cup \{\ldots, -2, 3, 8, \ldots\} \cup \{\ldots, -1, 4, 9, \ldots\}$

$\cup \{\ldots, 0, 5, 10, \ldots\}$

We can write $\mathbb{Z} = [1]_5 \cup [2]_5 \cup [3]_5$
$[4]_5 \cup [0]_5$

where $[a]_n := \{ z \in \mathbb{Z} \mid z \equiv a \mod n \}$
$= \{ \dots, a-n, a, a+n, \dots \}$

In general, there are n congruence classes mod n, namely

$[0], [1], \dots, [n-1]$

We denote $\mathbb{Z}/n\mathbb{Z} := \{ [i]_n \mid 0 \leq i \leq n \}$

It is a ring, i.e. $[i]_n + [j]_n = [i+j]_n$
$[i]_n \cdot [j]_n = [ij]_n$

Exercise 1) Check the above.

2) If $a \equiv a'$ & $b \equiv b' \mod n$ then prove that $[a]_n + [b]_n$
$= [a']_n + [b']_n$

& $[ab]_n = [a'b']_n$.

$\Rightarrow$ Congruence arithmetic is independent of choice of a representative.

Check with mod 3.

It has 3 congruence class : $[0]$, $[1]$, $[2]$.

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

×	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Finally, check that $\forall n > 0$

$$\mathbb{Z} = [0]_n \sqcup [1]_n \sqcup \cdots \sqcup [n-1]_n$$

disjoint union

Of course, $\forall a \in \mathbb{Z}$ by Euclid

we write $a = qn + r$, $0 \leq r \leq n-1$

$\Leftrightarrow$ $a \equiv r \mod n \Leftrightarrow [a]_n = [r]_n$

OTOH, if $[r_1]_n = [r_2]_n$ $\quad 0 \leq r_i \leq n-1$, $i = 1, 2$

$\Rightarrow$ $n \mid r_1 - r_2$ $\qquad$ Let $r_1 > r_2$

But $0 \leq r_1 - r_2 \leq n-1 \Rightarrow r_1 - r_2 = 0$

<u>Prob 2</u>: Let p be a prime then $\mathbb{Z}/p\mathbb{Z}$ is a field.

F is a field : All non-zero element have inverses.

What is identity in $\mathbb{Z}/p\mathbb{Z}$?

Ans : $[1]_p$

Pf: It suffices to show that

$\forall [x]_p \neq [0]_p \quad \exists [y]_p$ s.t.

$[xy]_p = [1]_p$.

$\iff \quad xy \equiv 1 \mod p$.

If $[x]_p \neq [0]_p \Rightarrow p \nmid x$

$\Rightarrow GCD(x, p) = 1$ [why ??]

$\overset{\text{Bezout}}{\Rightarrow} \exists y, s \in \mathbb{Z} : xy + sp = 1$

$\Rightarrow xy \equiv 1 \mod p$.

$\boxtimes$

Conversely, if n is not a prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Ex: $\mathbb{Z}/4\mathbb{Z}$ is not a field.

$[2] \neq [0]$. What is the inverse of $[2]$?

$\mathbb{Z}/7\mathbb{Z}$ is a field. What is the inverse of $[3]$?

<u>Ans:</u> We can check case by case:

$$[3] \times [1] = [3]$$
$$\text{—} \quad [2] = [6]$$
$$\text{—} \quad [3] = [2]$$
$$\text{—} \quad [4] = [5]$$
$$[5] = [1] \checkmark$$

$$\Rightarrow [3]^{-1} = [5]$$

Inverse is unique: If $[ab] = 1$ & $[ac] = 1$

then $[b] = [c]$

$$[ab] = [ac]$$
$$\Rightarrow p \mid a(b-c) \underset{\text{Lemma week 1}}{\Rightarrow} p \mid a \text{ or } p \mid b-c$$

But $[a] \neq [0] \Rightarrow [b] = [c]$.

Is there a slick way to find inverse?

e.g. What is the inverse of $[225]^{-1}$

in $\mathbb{Z}/157\mathbb{Z}$?

i.e. we want q s.t.

$157 \mid 225q - 1 \iff$ want q, r s.t.

$225q + 157r = 1$

Very tedious to solve.!!

There is a better way:

<u>Theorem</u> [Fermat little theorem]
(FLT) (NOT Fermat Last Theorem)

$\forall a \in \mathbb{Z}$, we have

$a^p \equiv a \mod p$.

<u>Note</u>: If $p \nmid a \iff GCD(a, p) = 1$

then $p \mid a^p - a \iff p \mid a(a^{p-1} - 1)$

$\underset{p \nmid a}{\iff} p \mid a^{p-1} - 1 \iff a^{p-1} \equiv 1 \mod p$

$\iff [a] \times [a^{p-2}] = [1]$ if $[a] \neq [0]$
in $\mathbb{Z}/p\mathbb{Z}$.

Check for 3

$[a]=[0]$ ✓ $\quad [a]=[1] \Rightarrow [a^3-a]$

$= [1^3-1] = [0]$

$[a]=[2] \Rightarrow [2^3-2]$

$= [8-2] = [0]$

Conversely, if $\exists\ a \in \mathbb{Z}$ s.t.

$a^n \not\equiv a \mod n$

$\Rightarrow n$ is not prime.

<u>Ex.</u>: • Show that $3^{10} \equiv -1 \mod 5$

<u>Pf</u>: $3^{10} = 3^{5\times 2}$

$= 3^5 \times 3^5$

$\equiv 3 \times 3 \mod 5$

$\equiv -1 \mod 5$

<u>Exercise</u>: Find $[2^{2023}]_{17}$

Hint: Find prime factors of 2023.

Proof: Let $p \mid a$. Then it is trivial.

So we assume $p \nmid a \Leftrightarrow GCD(p, a) = 1$.

Consider $\{a, 2a, \ldots, (p-1)a\}$.

We claim the above set is the same as $\{1, 2, \ldots, p-1\}$ mod p.

Both sets have $p-1$ elements.

Thus it is enough to show that the elements in the former set are distinct mod p. Indeed, if

$$ra \equiv sa \mod p \qquad 1 \leq r, s \leq p$$

$$\Leftrightarrow p \mid a(r-s) \underset{p \nmid a}{\Longleftrightarrow} p \mid r - s$$

$$\Leftrightarrow r = s.$$

Thus $\{a, 2a, \ldots, (p-1)a\}$ is a permutation of $\{1, 2, \ldots, p-1\}$. Hence,

$$a \times 2a \times \cdots \times (p-1)a \equiv \overbrace{1 \times 2 \times \cdots \times (p-1)}^{=:P} \mod p$$

$$\| $$

$$a^{p-1}(1 \times 2 \times \cdots \times p-1).$$

$$\Rightarrow p \mid (a^{p-1} - 1)P. \underset{p \nmid P}{\Longrightarrow} p \mid a^{p-1} - 1. \quad \square$$