4/18/ Discrete

1. $\underline{38 = 7 \cdot \overset{q}{5} + \overset{r}{3}}$

(a) $38 \text{ div } 7 = 5$

(b) $38 \bmod 7 = 3$

$-38 = 7 \cdot \overset{q}{\underline{-6}} + \overset{r}{\underline{4}}$

$-42 +$

(c) $-38 \text{ div } 7 = -6$

(d) $-38 \bmod 7 = 4$

2. $13 \equiv -8 \pmod 3$

Defn: $a \equiv b \pmod m \iff m \mid b - a$

(a) $13 - (-8) = 21$ $\quad 3 \mid 21$ $\quad$ T

(b) $5 \mid 21$? $\quad$ F

CCI 7/21 ? T

Last time Modular Arithmetic

I.e. Arithmetic in

$$\mathbb{Z}_n = \{0, 1, \ldots n-1\}$$

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

$$a \ominus b = (a-b) \bmod n$$

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

might not exist → $a \oslash b = \frac{a}{b} \bmod n$

But if b is invertible in $\mathbb{Z}_n$

then

① $\frac{1}{b}$ exists and it's unique

② $\frac{a}{b} = a \otimes \frac{1}{b}$

$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : x \text{ invertible}\}$

$= \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}$

<u>Ex 1</u> Find $\frac{1}{9}$ in $\mathbb{Z}_n$ if possible.

(a) <u>$n = 14$</u> $\quad \mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$

$$14 = 2 \cdot 7$$

$\frac{1}{9} = ?$ $\quad 9 \otimes x = 1$

$x = 1$ $\quad 9 \otimes 1 = 9 \neq 1$ ✗

$x = 3$ $\quad 9 \otimes 3 = 27 = 13$ ✗

$x = 5$ $\quad 9 \otimes 5 = 45 \equiv 3$ ✗

$x = 9 =$ $\quad 9 \otimes 9 = 81 = 11$

$x = 11$ $\quad 9 \otimes 11 = 99 \equiv 1 \pmod{14}$

$$\frac{1}{9} = 11.$$

(b) $n = 27$

$$\mathbb{Z}_{27}^{*} = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23\}$$

$\frac{1}{9}$ DNE

(c) $n = 545 = 5 \cdot 109$

$$\mathbb{Z}_{545} = \{1, 2, 3, 4, 6, 7, 8, 9 \ldots$$

$$|\mathbb{Z}_{545}^{*}| = 432 \quad \text{big!}$$

Use Euclidean Algorithm:

$\gcd(545, 9) = 1$

① $545 = 9(60) + 5$

② $9 = \underline{5}(1) + \underline{\underline{4}}$

③ $5 = 4(1) + 1 \leftarrow \gcd = 1$

3 $\to$ $1 \overset{2}{=} 5-4$

$= 5-(9-5)$

$= 2(5)-1(9)$

$\overset{1}{=} 2(545-60(9))-1(9)$

$2\cdot 545 - 121(9) = 1$

$-121\cdot 9 \equiv 1 \pmod{545}$

so $\boxed{\frac{1}{9} \equiv -121 \equiv 424}$

<u>Euler's phi function:</u>

For $n>1$,

$\phi(n) = |\mathbb{Z}_n^*|$

Thm: ϕ can be computed as follows:

(a) If p prime, $\phi(p^n) = p^{n-1}(p-1)$

(b) If $\gcd(m,n)=1$, then
$$\phi(mn) = \phi(m)\,\phi(n)$$

Proof of (a):

$$\mathbb{Z}_{p^n}^* = \{x \in \mathbb{Z}_{p^n} \mid \gcd(x, p^n) = 1\}$$
$$= \{x \in \mathbb{Z}_{p^n} \mid p \nmid x\}$$

$$|\{x \in \mathbb{Z}_{p^n} \mid p \nmid x\}| =$$

$$|\mathbb{Z}_{p^n}| - |\{x \in \mathbb{Z}_{p^n} : p \mid x\}|$$

$$p^n - |\{0, p, 2p, 3p, \dots \dots \underline{\underline{p^n - p}}\}|$$

$$\{px \mid x = 0, 1, 2, \ldots, p^{n-1} - 1\}$$

$$\underbrace{1, 2, \ldots, p^{n-1}-1}_{\#\ p^{n-1}}$$

So

$$|\mathbb{Z}_{p^n}^{*}| = p^n - p^{n-1} = p^{n-1}(p-1) \checkmark$$

Ex (a) $\phi(14) = \phi(2 \cdot 7) \overset{(b)}{=} \phi(2)\,\phi(7) = (2-1)(7-1) = 1 \cdot 6 = 6 \checkmark$

(b) $\phi(27) = \phi(3^3) \overset{(a)}{=} 3^2(3-1) = 9(2) = 18 \checkmark$

(c) $\phi(595) = \phi(5 \cdot 109) = \phi(5) \cdot \phi(109) = 4 \cdot 108 = 432 \checkmark$

(d) $\phi(20) = \phi(2^2 \cdot 5) \overset{(5)}{=}$

$$\phi(2^2) \cdot \phi(5) =$$

$$2^1(2-1) \cdot (5-1) = 8$$

Check : $\mathbb{Z}_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$

Exponential in $\mathbb{Z}_n$

$a^b \to \infty$ as $b \to \infty$ ($a > 1$ Calculus)

In $\mathbb{Z}_n$?!

Ex) Calculate 3^{100} in $\mathbb{Z}_n$

$3^{100} = 5.15 \times 10^{47}$

(a) $n = 10$:

$3^0 = 1$, $3^1 = 3$, $3^2 = 9$, $3^3 = 27 \equiv 7$

$3^4 = \underline{\underline{3^3}} \cdot 3 = 7 \cdot 3 = 21 \equiv 1$.

$$3^5 \equiv 3 \cdot 3^4 = 3 \cdot 1 = 3$$

$$3^6 \equiv 3 \cdot 3 = 9$$

n	0	1	2	3	4	5	6	7	8	9			
3^n mod 10	1	3	9	7	1	3	9	7	1	3	9	7	1.

See $3^{4m} \equiv 1 \pmod{10}$

for all $m \geq 1$

$m = 25 \propto \quad 3^{100} \equiv 1$

(b) $\underline{n = 7}$ $\qquad \mathbb{Z}_7$

$$3^0 = 1, \quad 3^1 = 3, \quad 3^2 = 9 \equiv 2$$

$$3^3 = 2 \cdot 3 = 6$$

$$3^4 = 6 \cdot 3 = 18 \equiv 4$$

$$3^5 \equiv 4 \cdot 3 = 12 \equiv 5 \pmod{7}$$

$$3^6 \equiv 3 \cdot 5 \equiv 15 \equiv 1 \pmod{7}$$

0	1	2	3	4	5	6	7	8	9	
1	3	2	6	4	5	1	3	2	6	...

repetition in 6-cycles

$3^6 \equiv 1$ in $\mathbb{Z}_7$

$3^{96} = (3^6)^{16} \equiv 1^{16} \equiv 1$

$3^{100} = \underbrace{3^{96}}_{1} \cdot \underbrace{3^4}_{4} = 4.$

$100 \equiv 4 \pmod 6$

$3^{500} \equiv 2 \pmod 7$

$500 = 6(83) + 2$

<u>$n = 23$</u> $3^0 = 1,\ 3^1 = 3,\ 3^2 = 9,\ 3^3 = 27$ $\overset{\shortparallel}{4}$

$3^4 = 3 \cdot 4 = 12$ - - —

$3^{100} = 3^{64} 3^{32} \cdot 3^4$

$3^{64} = (3^{32})^2$

$3^{32} = (3^{16})^2$

$3^{16} = (3^8)^2$

$3^4 = (3^2)^2$

4

9

$(3^8) = (3^4)^2$

$12^2 = 144 = 6$

$9^2 = 81 = 12$

$18 \cdot 8 \cdot 12 =$

$3 \pmod{23}$

Thm If $x \in \mathbb{Z}_n^*$, then

$$x^{\phi(n)} \equiv 1 \pmod{n}$$

(Group Theory)

$n = 23$: $x = 3$

o   23 prime

$\phi(23) = 22$

Thm $3^{\phi(23)} = 3^{22} \equiv 1 \pmod{23}$

$$3^{100} = (3^{22})^{4} \cdot 3^{12}$$