Section 9.1

Recall Euler's Thm: If $(a,m)=1$, then

$$a^{\varphi(m)} \equiv 1 \mod m$$

Note: (Almost) Everything in this section follows from the fact that $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is a finite abelian group.

Q: Given $a, n \in \mathbb{Z}_{>0}$ with $(a,n)=1$, which values of x yield $a^x \equiv 1 \mod n$?

↳ smallest x?

Ex: $n=9$ $\rightarrow$ $\varphi(9)=6$

x	1	2	3	4	5	6
1^x	1	1	1	1	1	1
2^x	2	4	8	7	5	1
4^x	4	7	1	4	7	1
5^x	5	7	8	4	2	1
7^x	7	4	1	7	4	1
8^x	8	1	8	1	8	1

all members of $(\mathbb{Z}/9\mathbb{Z})^{\times}$

inverses

Observations

- Some rows contain 1 before col. 6
- Some rows don't contain 1 until col. 6
- Orders of all elts. are divisors of $\varphi(9)$
  ↳ every divisor shows up

"Def:" the order of $a \bmod 9$ is the least x s.t. $a^x \equiv 1 \bmod 9$

- order of 1 mod 9 : 1
- order of 2 mod 9 : 6

  4 : 3

  5 : 6

  7 : 3

  8 : 2

Questions

① For any modulus n, will there be elts. $\neq \pm 1$ with order $< \varphi(n)$?

② For any n, will there be elts with order $= \varphi(n)$?

③ For any n, will the set of orders of elts. constitute the set of divisors of $\varphi(n)$?

④ For any n and a of order $\varphi(n)$, will $\{a^x : 1 \le x \le \varphi(n)\}$ be a reduced residue system mod n?

Ex. $n = 8 \to \varphi(n) = 4$

X	1	2	3	4
1	1	1	1	1
3	3	1	3	1
5	5	1	5	1
7	7	1	7	1

There is no elt. of order $\underset{\varphi(8)}{\overset{4}{\shortparallel}}$!

$\hookrightarrow$ So A2: No

A3: No

Q3': Is the order of every elt. a divisor of $\varphi(n)$?

Lead-in to def: Let $n, a \in \mathbb{Z}_{>0}$, $(a, n) = 1$. Set $S = \{x \in \mathbb{Z}_{>0} : a^x \equiv 1 \bmod n\}$

$S \neq \emptyset$ because $\varphi(n) \in S$.

Hence, by well-ordering, S has a least elt.

Def: The <u>order</u> of a modulo n is the minimal elt. of S.

$\mathrm{ord}_n(a)$

Ex: $\mathrm{ord}_8(1) = 1 = \mathrm{ord}_9(1)$

$\mathrm{ord}_9(2) = 6$ $\quad$ ($2^6 \equiv 1 \mod 9$ but if $1 \le x < 6$, $2^x \not\equiv 1 \pmod 9$)

$\mathrm{ord}_8(3) = 2$

$\mathrm{ord}_9(4) = 3$

Facts

- $S = \{ x \in \mathbb{Z}_{>0} : a^x \equiv 1 \mod n \}$

Ex: What is S when $n = 9$, $a = 4$?

$$4^3 \equiv 1 \mod 9$$

$$4^6 \equiv 1 \mod 9$$

powers of 4: $4, 7, 1, 4, 7, 1, 4, 7, 1, \ldots$

$$S = \{3, 6, 9, 12, \ldots\} = \{3k : k \in \mathbb{Z}_{>0}\}$$

S = multiples of 3 $(\mathrm{ord}_9(4))$

Thm: Suppose $n \in \mathbb{Z}_{>0}$, $a \in (\mathbb{Z}/n\mathbb{Z})^{\times}$

Then for any $x \in \mathbb{Z}_{>0}$, $a^x \equiv 1 \mod n$

if and only if $\mathrm{ord}_n(a) \mid x$

Pf: Suppose $\mathrm{ord}_n(a) \mid x$

Goal: $a^x \equiv 1 \mod n$

$\mathrm{ord}_n(a) \mid x \rightarrow \exists k \in \mathbb{Z} : k \cdot \mathrm{ord}_n(a) = x$

$a^x = a^{k \cdot \mathrm{ord}_n(a)} = \left(a^{\mathrm{ord}_n(a)}\right)^k \equiv 1^k \equiv 1 \mod n$

Suppose $a^x \equiv 1 \mod n$

Goal: $\mathrm{ord}_n(a) \mid x$

Use: $\mathrm{ord}_n(a)$ is the smallest exp.
to which $a^{???} \equiv 1 \bmod n$.

Write $x = q \cdot \mathrm{ord}_n(a) + r$
where $0 \leq r < \mathrm{ord}_n(a)$

$1 \equiv a^x \equiv a^{q \cdot \mathrm{ord}_n(a) + r} \equiv \left(a^{\mathrm{ord}_n(a)}\right)^q a^r$
$\equiv a^r \mod n$

Since $r < \mathrm{ord}_n(a)$ and $\mathrm{ord}_n(a)$
is smallest pos. exp. s.t. $a^{???} \equiv 1 \bmod n$,
we must have $r = 0$.

So $x = q \cdot \mathrm{ord}_n(a)$, i.e. $\mathrm{ord}_n(a) \mid x$

Consequences:

Note that $a^{\varphi(n)} \equiv 1 \mod n$

So $\mathrm{ord}_n(a) \mid \varphi(n)$

More generally:

$n=9$

x	1	2	3	4	5	6	...	9
4^x	4	7	1	4	7	1	...	...

We just showed: $4^x \equiv 1 \mod 9$

when $x \equiv 0 \mod 3$

Also: $4^x \equiv 4^1 \mod 9$ when $x \equiv 1 \mod 3$

$4^x \equiv 7 \mod 9$ when $x \equiv 2 \mod 3$

$\equiv 4^2$

Thm: Suppose $n \in \mathbb{Z}_{>0}$ and $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then $\forall x, y \in \mathbb{Z}_{>0}$, $a^x \equiv a^y \mod n$ if and only if $x \equiv y \mod \mathrm{ord}_n(a)$

Primitive Roots

Q: When is there an $a \in (\mathbb{Z}/n\mathbb{Z})^\times$

s.t. $\text{ord}_n(a) = \varphi(n)$?

Q: If such an a exists,

what do we learn about it?

→ Substantial applications to cryptography.

Def: If $n \in \mathbb{Z}_{>0}$, $a \in (\mathbb{Z}/n\mathbb{Z})^\times$,

then a is a <u>primitive root</u>

if $\text{ord}_n(a) = \varphi(n)$.

Ex: Show that 3 is a primitive root mod 17

Naive method: ($\varphi(17) = 16$)

x	1	2	3	4	......	16
3^x	3	9	10			1

Clever method ($\varphi(17) = 16$)

$$\mathrm{ord}_{17}(3) \mid \varphi(17) = 16.$$

Only possible orders of 3 are 1, 2, 4, 8, 16

$3^1 \equiv 3 \mod 17$ $\qquad$ $\mathrm{ord}_{17}(3) \neq 1$

$3^2 \equiv 9 \mod 17$ $\qquad$ $\mathrm{ord}_{17}(3) \neq 2$

$3^4 \equiv 81 \equiv 13 \mod 17$ $\qquad$ $\mathrm{ord}_{17}(3) \neq 4$

$3^8 \equiv 169 \equiv 16 \mod 17 \quad \text{ord}_{17}(3) \neq 8$

So $\underline{\text{ord}_{17}(3)} = 16 = \underline{\varphi(17)}$

So 3 is a primitive root of 17.

Q: Do 10, 11, 12, 13 have primitive rts?