Multiplicative Structure Mod n

a is invertible if $\exists\, a^{-1}$ s.t. $a^{-1}a \equiv 1 \pmod n$

Recall: $(\mathbb{Z}/n\mathbb{Z})^*$ = the invertible elements of $\mathbb{Z}/n\mathbb{Z}$.

Thm. The elements of $(\mathbb{Z}/n\mathbb{Z})^*$ are closed under multiplication.

(AKA: If $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ then $ab \in (\mathbb{Z}/n\mathbb{Z})^*$.)

Note for abstract algebra:

$(\mathbb{Z}/n\mathbb{Z})^*$ is a group.

Pf. If $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ then they have inverses a^{-1} and b^{-1}:

$$a^{-1}a \equiv 1 \pmod n$$
$$b^{-1}b \equiv 1 \pmod n.$$

Then
$$\begin{aligned}(b^{-1}a^{-1})ab &\equiv b^{-1}(a^{-1}a)b \\ &\equiv b^{-1}\cdot 1 \cdot b \\ &\equiv b^{-1}b \\ &\equiv 1 \pmod n.\end{aligned}$$

Therefore ab is invertible, so $ab \in (\mathbb{Z}/n\mathbb{Z})^*$. ∎

Let $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

Def^n. The smallest positive integer k s.t. $a^k \equiv 1 \pmod{n}$, is called the **multiplicative order of a modulo n.**

$$a^0 \equiv 1,\ a^1 \equiv a,\ a^2,\ a^3, \ldots,\ a^k \equiv 1$$

Note: Exercise: Prove this exists. Hint: use the fact that $\mathbb{Z}/n\mathbb{Z}$ is finite.

Def^n. If $g \in (\mathbb{Z}/n\mathbb{Z})^*$ is such that

$$(\mathbb{Z}/n\mathbb{Z})^* = \{1, g, g^2, g^3, \ldots\} = \{g^k : k \in \mathbb{Z}\}$$

then g is called a **multiplicative generator** mod n or a **primitive root** mod n.

Note: This is equivalent to the multiplicative order of g being $|(\mathbb{Z}/n\mathbb{Z})^*|$.

Exercise: prove that.

Example.

Let $n = 5$

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$1 \cdot 1 \equiv 1$

$4 \cdot 4 \equiv 1$

$2 \cdot 3 \equiv 1$

$(\mathbb{Z}/n\mathbb{Z})^* = \{1, 2, 3, 4\}$

Exercise: try powers of 3, 1

Powers of 2

$2^0 \equiv 1$

$2^1 \equiv 2$

$2^2 \equiv 4$

$2^3 \equiv 3$

$2^4 \equiv 1$

the mult. order of 2 mod 5 is 4

this is a primitive root

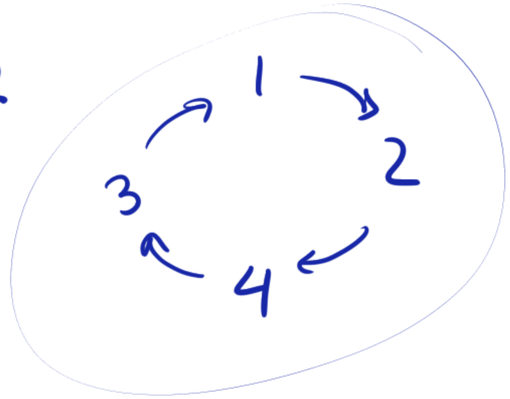
$2^5 \equiv 2$

$2^6 = 4$

$2^7 \equiv 3$

$\vdots$

$x \mapsto x \cdot 2$



Powers of 4

$4^0 \equiv 1$

$4^1 \equiv 4$

$4^2 \equiv 1$

$4^3 \equiv 4$

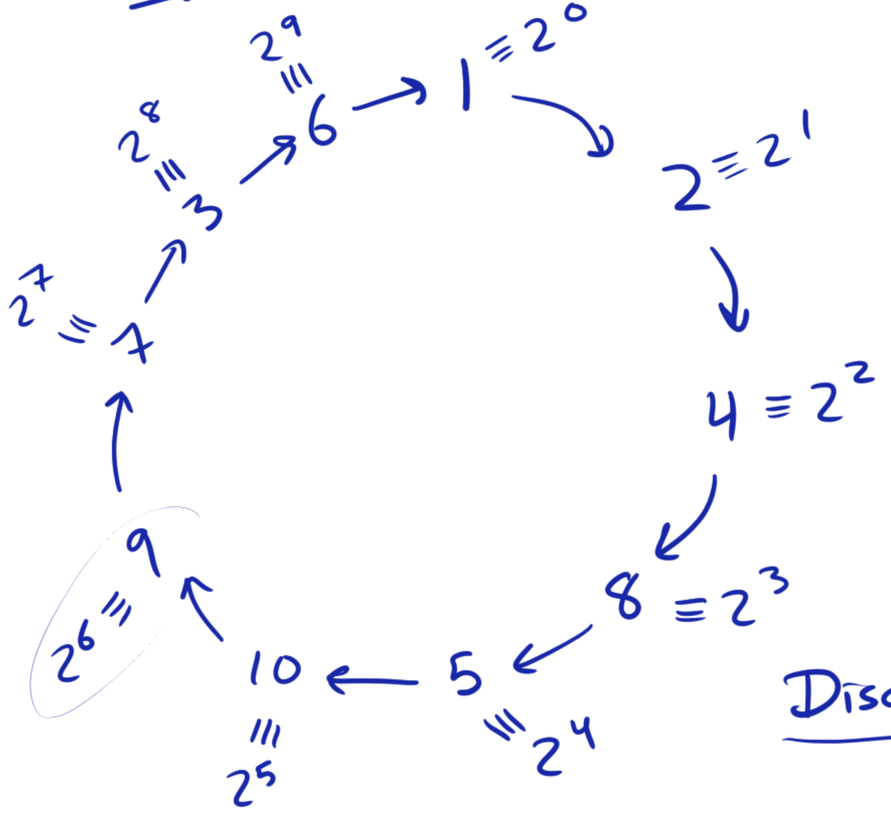
$4^4 \equiv 1$

the mult. order of 4 mod 5 is 2

this is not a primitive root

$x \mapsto x \cdot 4$

Bigger Example. Mod 11, 2 is a primitive root.
(order is 10)



$g = 2$
$n = 11$
$g^r = 9$
$\rightarrow$ find $r = 6$

Question: How do we know the ordering of the residues in this cycle?

How do I know, for example, if 9 is a small power of 2 (early in cycle) or a big one (later in cycle)

Discrete Logarithm Problem. Given g, a primitive root mod n, and given g^r, some power of g, find r.

g^r: given as its smallest positive residue eg. 9

Defⁿ. If $h \equiv g^r \pmod{n}$

then we say $r = L_g(h)$ in $(\mathbb{Z}/n\mathbb{Z})^*$.

"discrete logarithm to the base g of h" with respect to

Example. Look back at mod 5 data:

$L_2(3) = 3$ (or 7)

$L_2(1) = 0$ (or 4)

$L_2(4) = 2$

} answers actually live mod 4.

typically give smallest non-negative answer.

Discrete Logarithm Problem. What is $L_g(h)$ in $(\mathbb{Z}/n\mathbb{Z})^*$?

(We require this has an answer, i.e. h is a power of g.)

Example. $L_4(3)$ doesn't exist. (mod 5)