Q: A formula for $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ in general?

Sps $\boxed{n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}}$ (p_i's distinct, but w/ repeats (exponents e_i))

$n = 9 = 3^2$

~~0~~, 1, 2, ~~3~~, 4, 5, ~~6~~, 7, 8

eg. $\varphi(n) = 9\left(\frac{2}{3}\right) = 6$

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right)$$

all #s mod n

prob it is coprime to p_1 (or p_1^2 or p_1^3)

eg. $\varphi(27) = 27\left(1-\frac{1}{3}\right) = 27\left(\frac{2}{3}\right) = 18$

$27 = 3^3$

$\varphi(270) = 270\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$= 2\cdot 3^3\cdot 5$ $= \cancel{2}\cdot 3^{\cancel{3}^2}\cdot\cancel{5}\left(\frac{1}{\cancel{2}}\right)\left(\frac{2}{3}\right)\left(\frac{4}{\cancel{5}}\right) = 72$

Facts about $(\mathbb{Z}/n\mathbb{Z})^*$: "the multiplicative group mod n" (unit group)

① If $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$, then $ab \in (\mathbb{Z}/n\mathbb{Z})^*$

"closed under multiplication"

② $1 \in (\mathbb{Z}/n\mathbb{Z})^*$ "the identity" s.t. $a \cdot 1 \equiv a \equiv 1 \cdot a$

"does nothing"

③ If $a \in (\mathbb{Z}/n\mathbb{Z})^*$ then $a^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*$

s.t. $aa^{-1} = 1$ "inverses" "can undo"

This, together with associativity $(ab)c = a(bc)$,

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

$\mathbb{Z}/6\mathbb{Z} = \{0,1,2,3,4,5\}$

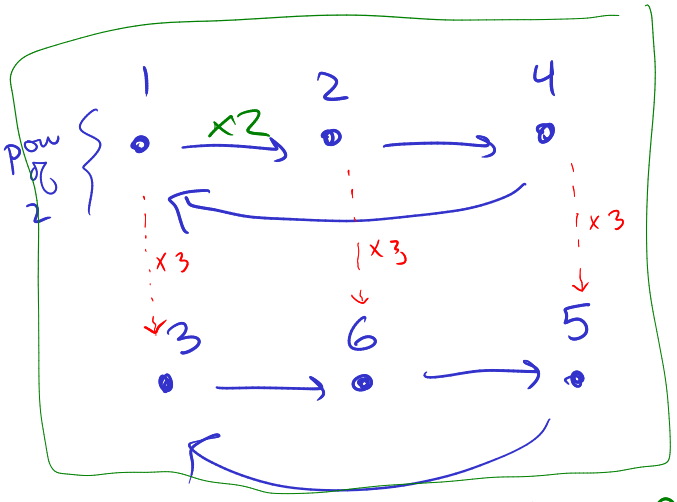
$+, \times$

$(\mathbb{Z}/6\mathbb{Z})^* = \{1,5\}$

only $\times$

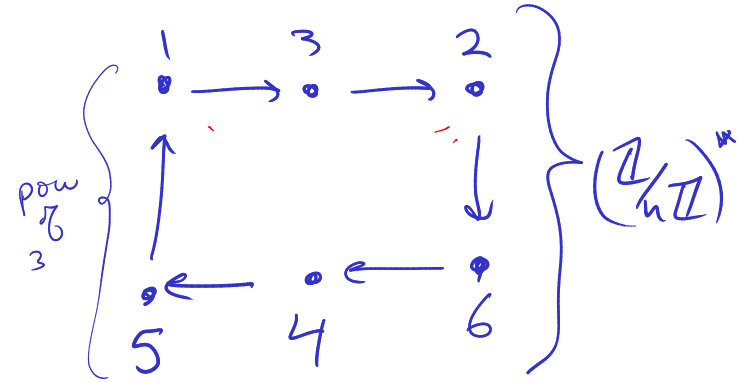
Dynamical portraits

$\times 2 \mod 7$



order of 2 mod 7 is 3

$\times 3 \mod 7$



order of 3 mod 7 is 6

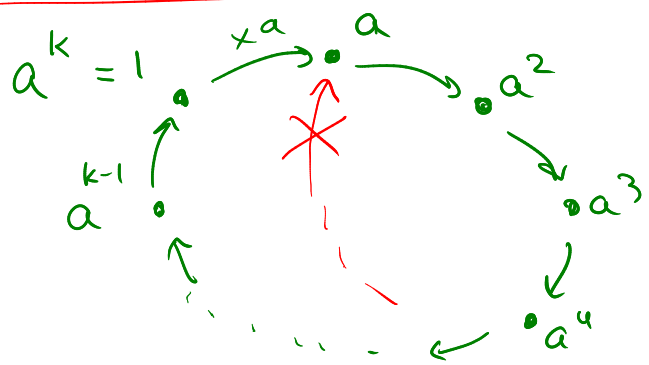
observations:

① $a \in (\mathbb{Z}/n\mathbb{Z})^*$ acting on $(\mathbb{Z}/n\mathbb{Z})^*$ is a bijection

$\Rightarrow$ cycles

② cycles are the same size

cycle including 1 $a \in (\mathbb{Z}/n\mathbb{Z})^*$



there exists such that

$\exists$ k s.t.

$1, a, a^2, \ldots, a^{k-1}, 1 = a^k$

Def' k is called the **multiplicative order** of a modulo n.

Note: since the cycles in $(\mathbb{Z}/n\mathbb{Z})^*$ under $x \mapsto ax$ are all the same size

implies that the (multiplicative) order of a modulo n divides $\varphi(n)$.

Theorem. (Fermat's Little Theorem)
Let p be prime.
Let $a \in (\mathbb{Z}/p\mathbb{Z})^*$.
Then $a^{p-1} \equiv 1 \pmod{p}$

Theorem. (Euler's Theorem)
Let $n \in \mathbb{Z}$.
Let $a \in (\mathbb{Z}/n\mathbb{Z})^*$
Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Pf. The multiplicative order k of a divides $\varphi(n)$,
so write $\varphi(n) = k\ell$, for some $\ell \in \mathbb{Z}$.

So $a^{\varphi(n)} \equiv a^{k\ell} \equiv (a^k)^\ell \equiv 1^\ell \equiv 1$. ∎

eg. mod 11

If $\gcd(3,11)=1$ ✓

then $3 \in (\mathbb{Z}/11\mathbb{Z})^\times$ $\quad \varphi(11)=10$ $\quad \varphi(p)=p\left(1-\frac{1}{p}\right)=p-1$

So $3^{10} \equiv 1$

taking exponent modulo $\varphi(n)$

So $3^{519} \equiv 3^{510}3^{9} \equiv 1 \cdot 3^{9} \pmod{11}$