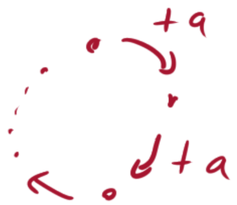
Theorem. $(\mathbb{Z}/n\mathbb{Z})^* = \{ a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1 \}$.

Pf. Suppose $\gcd(a,n) = 1$. (We'll show it is invertible.)

Consider the additive dynamics of $+a \bmod n$.

This has 1 cycle (since gcd = 1).



So every element appears in the cycle

So 0 and 1 appear.

So $\exists$ x s.t. $0 + \underline{ax \equiv 1} \pmod n$.

So x is the inverse of a.

Conversely, suppose a is invertible, so $0 + ax \equiv 1 \pmod n$ for some x.

Let $k \in \mathbb{Z}$. Therefore $0 + akx \equiv k \pmod n$.

So the cycle containing 0 contains k (take kx steps of $+a$).

So there is 1 cycle. So $\gcd(a,n) = 1$.

□

Corollary. Let p be prime.
Then $\left|(\mathbb{Z}/p\mathbb{Z})^*\right| = p-1$,

since $(\mathbb{Z}/p\mathbb{Z})^* = \{ x \in \mathbb{Z}/p\mathbb{Z} : x \not\equiv 0 \pmod{p} \}$

a coprime to b
$\iff \gcd(a,b) = 1$

Def^n. The Euler phi function,

$$\varphi(n) := \#\{ x : 1 \le x < n \text{ such that } x \text{ is coprime to } n \}$$

Ex. $\varphi(p) = p-1$ for any prime p.

Ex. $\varphi(6) = 2$

(Q (for later): formula for $\varphi(n)$)

We saw **Theorem.** The map $x \mapsto ax$ is bijective on $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(a,n) = 1$.

We get from this... **Corollary.** $(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1\}$.

Pf. (of Cor) If $x \mapsto ax$ is bijective, then it is surjective, so $\exists\ x_0$ s.t. $ax_0 \equiv 1 \pmod{n}$.

So a is invertible.

Conversely, if a is invertible, then it has an inverse a^{-1}.

$a^{-1} \longmapsto 1$ under $x \mapsto ax$

$ka^{-1} \longmapsto k$ for any $k \in \mathbb{Z}/n\mathbb{Z}$.

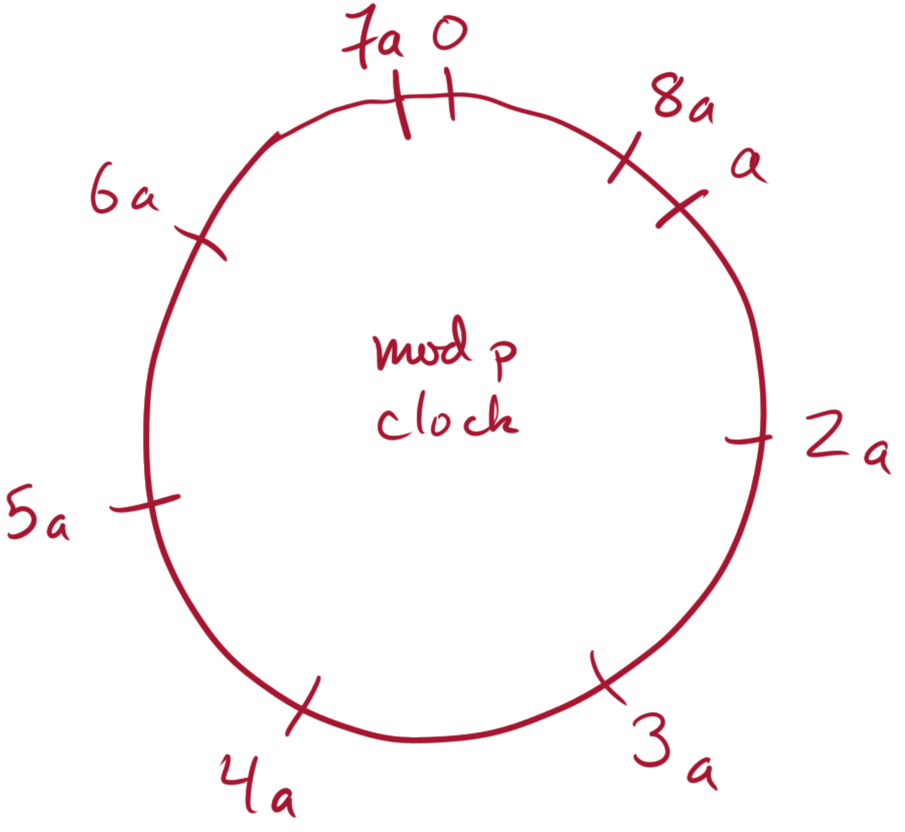
So the map $x \mapsto ax$ is surjective.

$\Rightarrow$ it is bijective. ∎

Modular Inverse via Gauss (for prime modulus p).

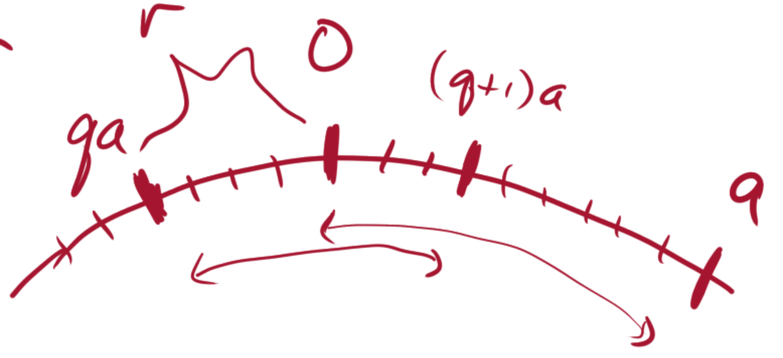
Goal: find the inverse of $a \pmod p$, $a \in (\mathbb{Z}/p\mathbb{Z})^*$.

i.e. solve $ax \equiv 1 \pmod p$.



Key idea: First time multiples of a wrap around the clock, it hits something smaller (closer to 0) than a.

$p = qa + r$



So: replace a w/ $a' = qa$ or $(q+1)a$

and try again!

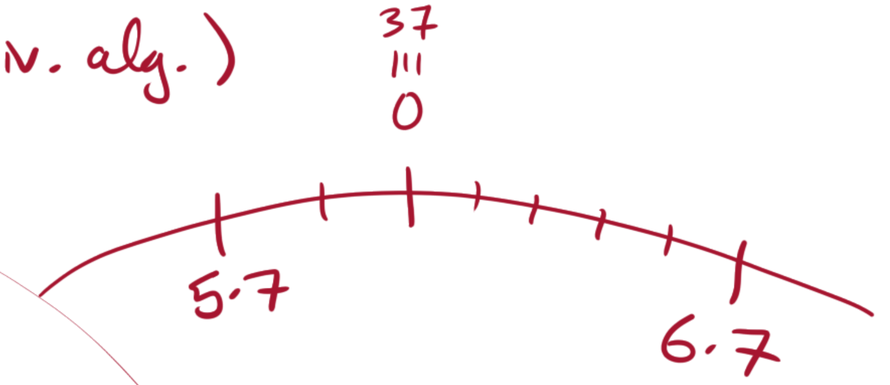
Keep getting smaller a's, until we hit 1.

Example.

Example. $p = 37$, $a = 7$ (Find inverse of 7 mod 37)

Step 1. $37 = 5 \cdot 7 + 2$ (div. alg.)

We learn: $2 \equiv (-5) \cdot 7 \pmod{37}$



Step 2. $37 = 18 \cdot 2 + 1$

We learn: $1 \equiv (-18) \cdot 2 \pmod{37}$

We've reached 1!

So $1 \equiv (-18) \cdot 2$

$\equiv (-18)(-5) \cdot 7$

So inverse of 7 is $(-18)(-5) \equiv 18 \cdot 5 \equiv 90 \equiv 16$

Check:

$7 \cdot 16$

$\equiv 1 \pmod{37}$

Another Example. $p = 37, \quad a = 8$

Step 1. $37 = 4 \cdot 8 + 5$

$= 5 \cdot 8 - 3$

So $3 \equiv 5 \cdot 8 \pmod{37}$

Step 2. $37 = 12 \cdot 3 + 1$

So $1 \equiv (-12) \cdot 3 \pmod{37}$

So $1 \equiv (-12) \cdot 3$

$\equiv (-12) \cdot 5 \cdot 8$

The inverse of 8 is $-12 \cdot 5 \equiv -60$

$\equiv 14$.

Check:

$8 \cdot 14 \equiv 1 \pmod{37}$

Algorithm for inverse of a mod p.

(Gauss)

(1) Let $a_0 = a$.

(2) While $a_i > 1$:

Write $p = a_i q + r$ (div. alg.)

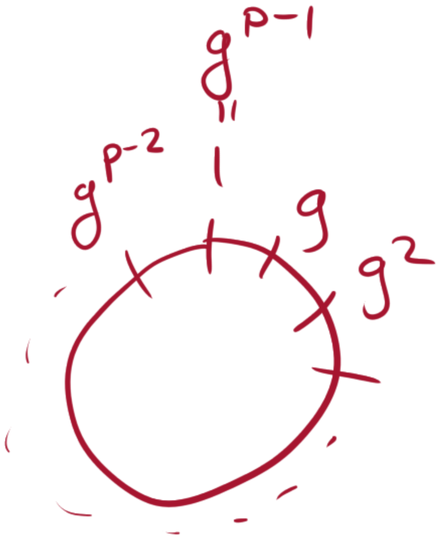
Set $(a_{i+1}, q_i) = \begin{cases} (r, -q) & \text{if } r < p-r \\ (p-r, q+1) & \text{o/w} \end{cases}$

(3) The inverse is $q_0 q_1 \cdots q_{i-1}$.

Computing the discrete log: $h = g^x$, what is x?

Warm-up question:

If I know $h^3 = g^2$, then what is h?



Sub in: $(g^x)^3 \equiv g^2 \pmod{p}$

$g^{3x} \equiv g^2 \pmod{p}$

$\Rightarrow 3x \equiv 2 \pmod{p-1}$

Find 3^{-1}, then

$3^{-1} \cdot 3 \cdot x \equiv 3^{-1} \cdot 2 \pmod{p-1}$

$x \equiv 3^{-1} \cdot 2 \pmod{p-1}$

Computing the discrete log:

$h = g^x$, what is x?

(g primitive root)

Warm-up question:

If I know $h^3 = g^2$, then what is h?

Sub in: $(g^x)^3 \equiv g^2 \pmod{p}$

$g^{3x} \equiv g^2 \pmod{p}$

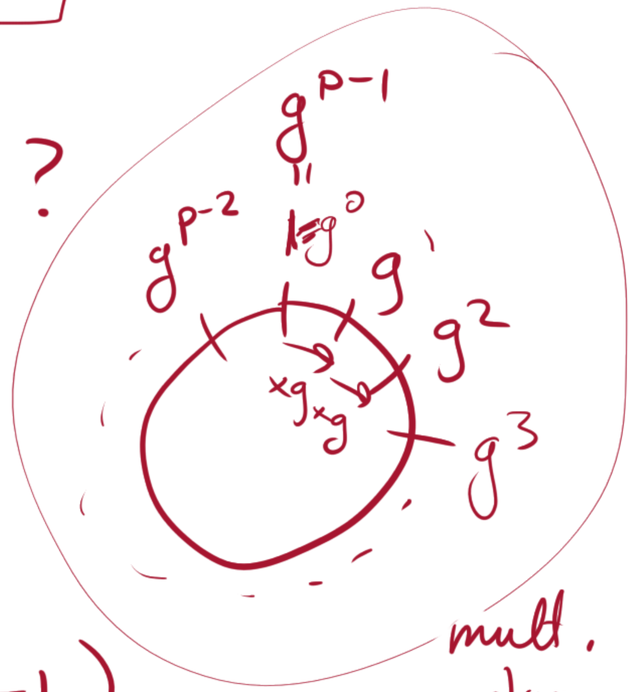
$\Leftrightarrow \quad 3x \equiv 2 \pmod{p-1}$

$p-1$ = order(g)

Find 3^{-1}, then

$3^{-1} \cdot 3 \cdot x \equiv 3^{-1} \cdot 2 \pmod{p-1}$

$x \equiv 3^{-1} \cdot 2 \pmod{p-1}$



mult. dyn. of $\cdot g$