Example. Simplify $13^{453^{2022}} \pmod{100}$.

$a^{b^c} = a^{(b^c)}$ since $(a^b)^c = a^{bc}$

$\varphi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 40.$

Check: 13 is coprime to 100, so Euler's Thm applies.

First, attack exponent:

$$453^{2022} \pmod{40}$$
$$\equiv 13^{2022}$$

$\varphi(40) = 40\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 16.$

Check: 13 is coprime to 40, so Euler's Thm applies.

So $13^{2022} \equiv 13^6 \pmod{40}$

Use successive squaring.

$$13^2 \equiv 9 \pmod{40}$$
$$13^4 \equiv 1 \pmod{40}$$

So $453^{2022} \equiv 13^6 \equiv 13^4 \cdot 13^2 \equiv 9 \pmod{40}$.

Returning to original problem,

$$13^{453^{2022}} \equiv 13^9 \pmod{100}.$$

Again by successive squaring:

$$13^2 \equiv 69, \quad 13^4 \equiv 61, \quad 13^8 \equiv 21$$

$$13^9 \equiv 13^8 \cdot 13 \equiv 21 \cdot 13 \equiv 273 \equiv 73 \pmod{100}.$$

Summary. p = prime.

$(\mathbb{Z}/p\mathbb{Z})^*$ = invertible elts of $\mathbb{Z}/p\mathbb{Z}$.

① a group (a number system)

② a is invertible $\iff \gcd(a,p)=1$

$\iff p \nmid a$

$\iff x \longmapsto ax$ is a bijection on $\mathbb{Z}/p\mathbb{Z}$

$\iff x \longmapsto ax$ " " " $(\mathbb{Z}/p\mathbb{Z})^*$

③ The mult. order of $a \in (\mathbb{Z}/p\mathbb{Z})^*$ is the smallest positive k s.t. $a^k \equiv 1 \pmod{p}$

④ $a^{p-1} \equiv 1 \pmod{p}$ for $a \in (\mathbb{Z}/p\mathbb{Z})^*$

⑤ If a has mult. order $p-1$, we call it a <u>primitive root</u>.

⑥ Such a primitive root always exists.

MORAL: Exponents mod p "live" mod p-1.

Eg. mod 7, $3^6 \equiv 1$

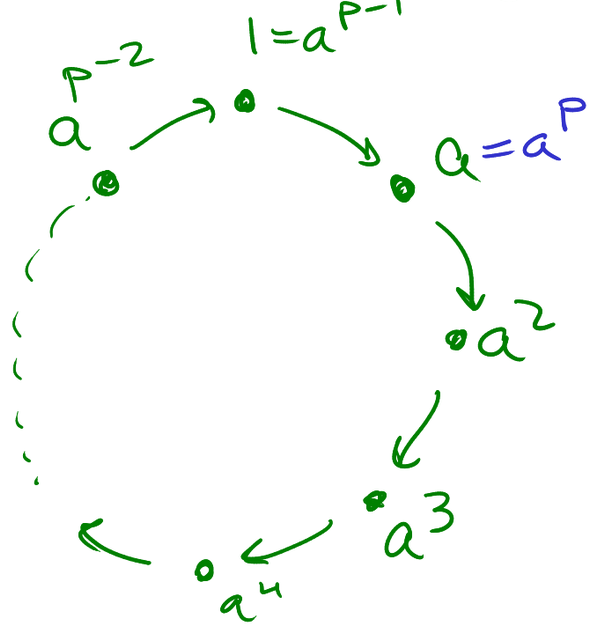
$3^8 \equiv 3^{6+2} \equiv 3^6 3^2 \equiv 1 \cdot 3^2 \equiv 3^2$

($8 \to 2 \pmod 6$)

So $3^8 \equiv 3^2 \equiv 9 \equiv 2 \pmod 7$

(7 = prime)

We will use this big cycle mod p:



there's one big cycle

$\Longleftrightarrow$ (mult.)

a has order p-1

$\Longleftrightarrow$

a is called a primitive root.

great place for crypto

Diffie-Hellman Key Exchange

Public (known) Setup Info: { prime p (large!!), primitive root $g \pmod p$

Alice

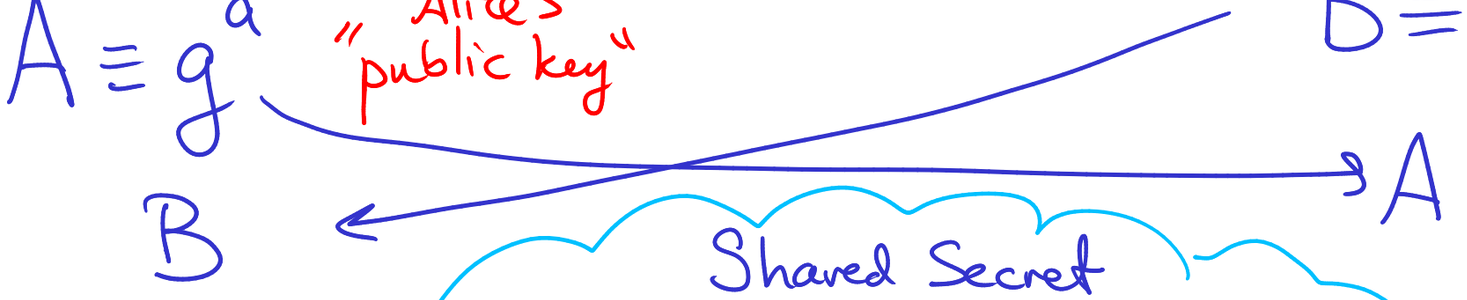
Secret: $0 < a < p-1$ "Alice's private key"

$A \equiv g^a$ "Alice's public key"

Bob

Secret: $0 < b < p-1$ "Bob's private key"

$B \equiv g^b$ "Bob's public key"



Shared Secret

$$B^a = g^{ab} = A^b$$

Hard Problems.

Computational Diffie-Hellman Problem (CDHP)

Let p be prime, g a primitive root mod p.
Given $g^a \pmod p$, and $g^b \pmod p$, compute $g^{ab} \pmod p$.

Discrete Logarithm Problem (DLP)

Let p be prime, g a primitive root mod p.
Given $g^a \pmod p$, compute $a \pmod{p-1}$.

If we solve DLP then we can solve CDHP.