$$\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n : GCD(a, n) = 1 \}$$

$$|\mathbb{Z}_n^*| = \varphi(n)$$

$a, b \in \mathbb{Z}_n^*$, $GCD(a, n) = GCD(b, n) = 1$.

$\therefore GCD(ab, n) = 1$

Thm ① $\varphi(p^\alpha) = p^\alpha\left(1-\frac{1}{p}\right)$, p is prime.

② 가 $\gcd(m,n)=1$, then

$$\varphi(mn) = \varphi(m)\varphi(n)$$

(ⅰ) 만약 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then

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

pf $\phi(3)$.

Consider $\mathbb{Z}_{mn}^*$, $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$

Clearly, $|\mathbb{Z}_{mn}^*| = \phi(mn)$.

$|\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = \phi(m)\phi(n)$

Define a map $\overline{\Phi} : \mathbb{Z}_{mn}^* \longrightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^*$

For any $x \in \mathbb{Z}_{mn}^*$ define

$\overline{\Phi}(x) = \langle x \bmod m, x \bmod n \rangle$.

Check that $(x \bmod m, x \bmod n) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

For any $(a, b) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$

By CRT, $\exists X$ s.t.

$$X \equiv a \bmod m$$

$$X \equiv b \bmod n.$$

Clearly, $X \in \mathbb{Z}_{mn}^*$

Also, X is unique modulo mn.

Hence Φ is 1-1 & onto.

$$\therefore \quad |\mathbb{Z}_{mn}^{*}| = |\mathbb{Z}_m^{*}| \cdot |\mathbb{Z}_n^{*}|.$$

i.e. $\varphi(mn) = \varphi(m)\varphi(n)$.

(c) $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$

$$= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right) p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right)$$

$$= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\left(1-\frac{1}{p_1}\right) \cdots \left(1-\frac{1}{p_k}\right)$$

$$= n\left(1-\frac{1}{p_1}\right) \cdots \left(1-\frac{1}{p_k}\right)$$

Pollard's ρ factoring algorithm.

---

n

Assume that p is the smallest prime divisor of n

$\exists$ integers $x \neq x'$ s.t. $x \equiv x' \bmod p$

then $p \leq GCD(x - x', n) < n$.

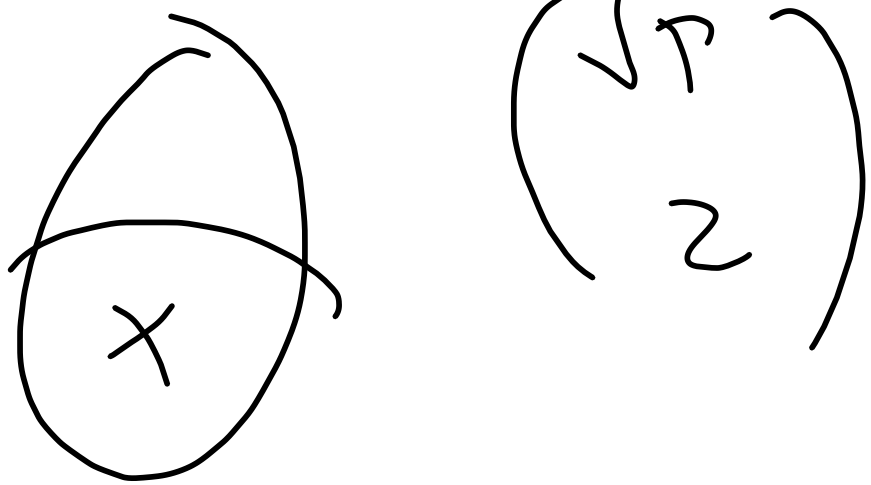
i.e we require a collision for the f:

$x \longrightarrow x \bmod p$

By Birthday paradox

Select a random subset

of cardinality approx $\sqrt{p}$



Pollard's ρ algorithm

tries to minimize

the GCD computations.

Consider the fn $f(x) = x^2 + 1$

We assume that $x \longrightarrow f(x) \bmod n$

behaves like a random fn

Pick a random $x_1 \in \mathbb{Z}_n$ & compute

the seq $x_1, x_2, \ldots$ as follows:

$$x_1 \equiv x \bmod n$$

$$x_{i+1} = f(x_i) \bmod n.$$

Our aim is to find $j > i$ s.t.

$x_i \equiv x_j \mod p$

Suppose $\exists\, j > i$ s.t. $x_i \equiv x_j \mod p$.

$$f(x_i) \equiv f(x_j) \mod p.$$

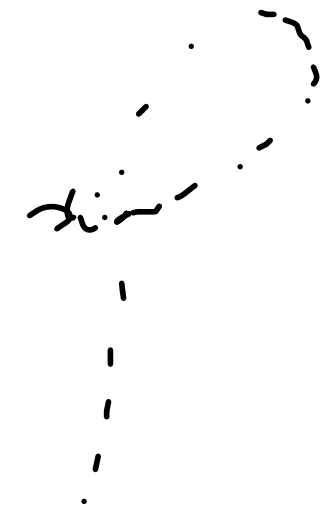
We have $x_{i+1} \equiv f(x_i) \mod n \Rightarrow x_{i+1} \equiv f(x_i) \mod p$.

Similarly $x_{j+1} \equiv f(x_j) \mod p$.

$$x_{i+1} \equiv x_{j+1} \mod p$$

Repeating this we obtain $\forall k \geq 0$

$$x_{i+k} \equiv x_{j+k}$$



Set $l = j - i$

$$x_{i+k} \equiv x_{i+k+l} \quad \forall k \geq 0.$$

This means that the seq^n is periodic with period l after i

Hence if $j' > i' \geq i$ & $j' - i' \equiv 0 \bmod l$ } (1)

$$\boxed{x_{i'} \equiv x_{j'}}$$

$$\underbrace{i, i+1, i+2, \ldots, j}_{\ell \text{ consecutive integers}}$$

$\exists\ \underline{i' < j}$ s.t. $i' \equiv 0 \mod \ell$.

$$\implies x_{i'} \equiv x_{2i'} \mod p.$$

In at most j iterations we have found a collision. Expected value of j is $\sqrt{p} \le n^{1/4}$

Pollard's ρ - factoring Algorithm (n)

- Let $f(x) = x^2 + 1$
- $x_1 \xleftarrow{R} Z_n$.
- $x \leftarrow x_1$
- $x' \leftarrow f(x) \bmod n$.
- $p \leftarrow GCD(x - x', n)$

While $p = 1$ do

{
$x \leftarrow f(x) \bmod n$

$x' \leftarrow f(x') \bmod n$

$x' \leftarrow f(x') \bmod n$

$p \leftarrow GCD(x - x', n)$

Comment: In the i^{th} iteration $x \equiv x_i$, $x' \equiv x_{2i}$.
}

If $p = n$ return ("failure")

else return (p)

Ex Choose $x_1 = 1$ & use Pollard's

alg. to factorize 1717

Primality test

If n is prime, then by Fermat,

$$x^{n-1} \equiv 1 \mod n \quad \forall x \in \mathbb{Z}_n.$$

The converse need not be true

Carmichael's number

Miller-Rabin tries to find a "witness" to the compositeness of n by showing $a^{n-1} \not\equiv 1 \bmod n$

Miller-Rabin (n, s)

- Write $n-1 = 2^k m$, where m is odd
- Choose a random integer a, $1 \le a \le n-1$
- $b \leftarrow a^m \bmod n$
- if $b \equiv 1 \bmod n$ then return ("n is prime")
- for $i \leftarrow 0$ to $k-1$ do
  - if $b \equiv -1 \bmod n$ return ("n is prime")
  - else $b \leftarrow b^2 \bmod n$
- return ("n is composite")
- Repeat s times

Thm Miller-Rabin for COMPOSITE is a YES-biased Monte-Carlo Algorithm.

pf We shall show that if Miller-Rabin returns "n is composite", then n has to be composite

Observe that Miller-Rabin computes the seq^n $a^m, a^{2m}, a^{2^2 m}, \ldots, a^{2^t m}$

Since the algorithm returns "n is composite" we must have

$$a^{2^{k-1} \cdot m} \not\equiv -1 \bmod n.$$

Assume n is prime. By Fermat,

$$a^{n-1} \equiv \boxed{a^{2m} \equiv 1 \bmod n.}$$

Clearly $a^{2^{k-1}\cdot m}$ is a square-root of 1 modulo n. Since $a^{2^{k-1}\cdot m} \not\equiv -1 \mod n$, & n is prime,

$$a^{2^{k-1}\cdot m} \equiv +1 \mod n.$$

$$a^{2^{k-2}\cdot m} \not\equiv -1 \mod n$$

$$a^{2^{k-2}\cdot m} \equiv +1 \mod n$$

Repeating we obtain

$$a^m \equiv 1 \mod n$$

Contradiction!

Repeating we obtain

$$Q^m \equiv 1 \mod n$$

Contradiction!

This shows that n cannot be prime.

Remark: If n is prime, Miller-Rabin will return "n is prime"

Hence Miller-Rabin is likely to err when n is composite & it returns "n is prime".

Thm The no. of witnesses for the compositeness of n is at least $\frac{n-1}{2}$

If we shall prove that the no. of non-witnesses is at most $\frac{n-1}{2}$

Fix a non-witness $a \in \mathbb{Z}_n$.

Claim $a \in \mathbb{Z}_n^*$

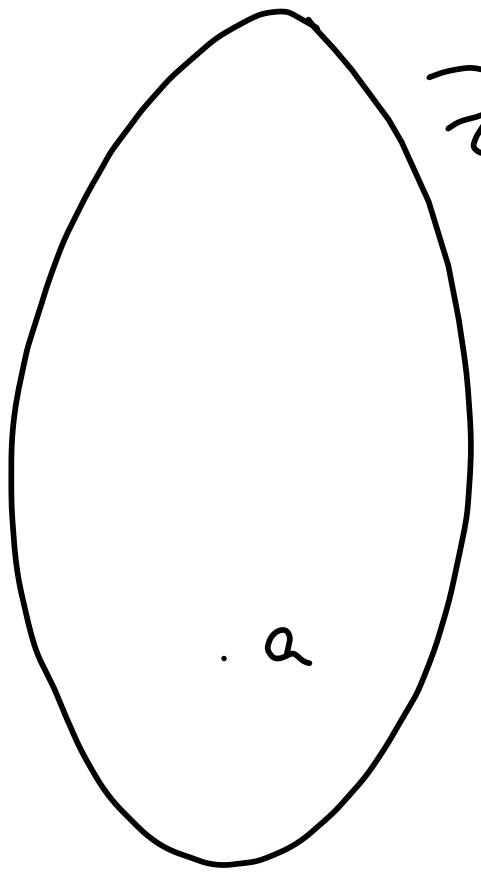
Note that $a^{n-1} \equiv 1 \bmod n$ (Why?)

(O.w. a is a witness).

$a^{2^k \cdot m} \equiv 1 \bmod n$.

$a^{2 \cdot m} \equiv 1 + rn$. Any prime divisor p of a & n will divide $a^{2^k \cdot m} - rn = 1$

$\Rightarrow a \in \mathbb{Z}_n^*$



We shall show that

C is proper subgroup of $\mathbb{Z}_n^\times$