Chinese remainder

if $\gcd(a,b) = 1$ then for any remainder r_a modulo a and any remainder r_b modulo b there exists integer n, such that $n \equiv r_a \pmod{a}$ and $n \equiv r_b \pmod{b}$

if n_1 and n_2 are 2 such

$$n_1 \equiv n_2 \pmod{(ab)}$$

∴ each x in

$0, 1, 2 \cdots ab-1$

corresponds to a pair

(r_a, r_b)

Simple algo to find n giving pair (r_a, r_b)

$\gcd(a,b) = 1$

use extended Euclid Algo to find x, y in

$1 = ax + by$

Take $n = r_a \cdot by + r_b \cdot ax$

Fermat's little theorem

if prime no $p \nmid a$, then

$$a^{p-1} = 1 \bmod p$$

just diff order maybe

Consider all non-zero remainders of p

$\Rightarrow 1, 2, 3 \cdots p-1$

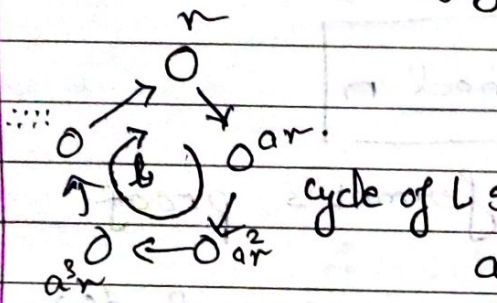
multiply with a is invertible [will still give all rems when mod p]

Let a rem r $[1 \le r \le p-1]$

multiply with a

forms a graph: edge from r to ar

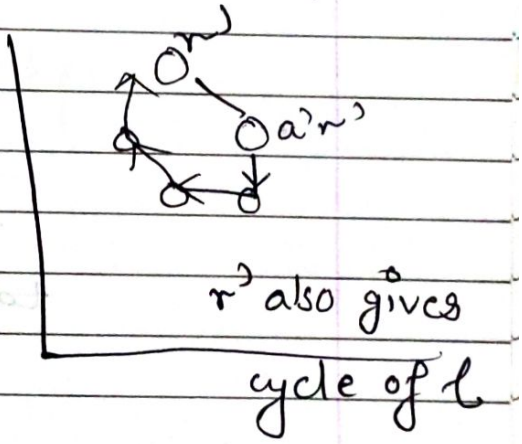
keep multiplying and taking rem with modulo p



cycle of l sides

$$a^l r = r \bmod p$$

$$a^l = 1 \bmod p$$



$\Rightarrow$ These cycle don't intersect and totally contain all $p-1$ rems

Let total cycles be c

$$cl = p-1$$

$$a^{cl} = 1^c \bmod p = 1 \bmod p$$

$$a^{p-1} = 1 \bmod p$$

Eulers totient function

$\phi(n)$ → integers between 0 and n-1 coprime with n

if p is prime

$$\phi(p) = p-1$$

if p and q are prime

$$\phi(pq) = (p-1)(q-1)$$

Eulers theorem

if a coprime with n,

$$a^{\phi(n)} = 1 \bmod n$$

Similar to fermat's proof

take all non zero rems of $\phi(n) \bmod n$

(actually all $\phi(n)$ numbers themselves)

cycles of l length

c cycles

$cl = \phi(n)$

$a^{\phi(n)} = 1 \bmod n$

★ Fermat's is used to optimize modular exponentiation

if $p \nmid a$, $a^{p-1} \equiv 1 \bmod p$

$$a^n = a^{n \bmod (p-1)} \bmod p$$

$n = q(p-1) + r$

$a^n = a^{q(p-1)+r}$

$= a^{(p-1)q} \cdot a^{n \bmod (p-1)}$

$= 1^q \bmod p \cdot a^{n \bmod (p-1)}$

if $p \mid a$, $a^n \equiv 0 \equiv a^{n \bmod (p-1)} \bmod p$

∴ works better

RSA

Asymmetric / Public key

⇒ If Bob wants to receive he generates keys - public, private

⇒ public is sent to whoever wants to send him msgs, private is kept secret by Bob

If Alice wants to, she encrypts message using Bob's public key to ciphertext
↓
This can only be decrypted by Bob via his private key which is kept secret.

Algorithm

(1) Bob generates 2 big, random, prime numbers p and q → hundreds of thousands of digits
computes $n = p \cdot q$

(2) random e is generated thats coprime with $\phi(n)$
Euler totient func
$\phi(n) = (p-1)(q-1)$

(3) Public key pair is (n, e)
Private key pair is (p, q)

∴ product of p and q = n is known but we can't factorize really huge numbers

(4) message m is encoded into bits and converted to integer (m)

needs to be between 0 and p-1

so choose p, q wisely

(5) ciphertext $c \equiv m^e \bmod (n)$

↳ using fast modular expo ~~theo~~ algorithm

(6) Decryption: $c^d \equiv m \bmod (n)$

d is only known by Bob

we need

$c^d \equiv m \bmod n$

$m^{ed} \equiv m \bmod n$

$n = pq$, p and q coprime

so by Chinese remainder theorem

$m^{ed} \equiv m \bmod p$, $m^{ed} \equiv m \bmod q$

since p, q are prime

By Fermat's Little theorem

$m^k \equiv m^{k \bmod (p-1)} \bmod p$

~~this holds if~~

we need

$k \bmod (p-1) \equiv 1 \bmod (p-1)$

$ed \equiv 1 \bmod (p-1)$

& $ed \equiv 1 \bmod (q-1)$

Page No.:

$ed \equiv 1 \bmod (p-1)$, $ed \equiv 1 \bmod (q-1)$

This is true

if

$ed \equiv 1 \bmod (p-1)(q-1)$

→ e is coprime with $(p-1)(q-1)$

remember Euclids Lemma

a coprime with n

$ax = 1 \bmod (n)$

find ↳ by extended euclids algo

∴ d can be computed

★ This is how Bob computes d

after generating p, q, e

Only he knows p, q and hence knows $(p-1)(q-1)$

we don't, we know n

but can't factorize huge n

⇒ we rely on difficulty of factorization

★★ Decryption

can also be explained using

Eulers theorem

$m^{k \bmod \phi(n)} = m \bmod n$