09/29/22:

Chinese Remainder Theorem Tricks:-

we know,

$$\boxed{\begin{array}{l} \text{divid} = \text{divisor} \cdot q + r \\ q \in \mathbb{Z},\ 0 \le r < \text{divisor} \end{array}}$$

$2^{53} \pmod 3 \Rightarrow$ let us say, $-1 \bmod 3$

$$-1 = 3 \cdot q + r$$

$$q = -1,\ \boxed{r = 2}$$

$$-1 \pmod 3 = 2.$$

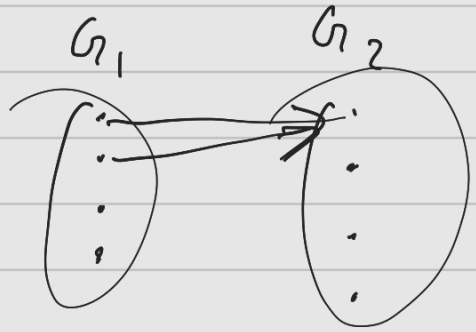
where as, From Group order Rule;

$2^{53} \pmod 3$; $\mathbb{Z}_3^* = \{1, 2\}$; $|\mathbb{Z}_3^*| = 2$

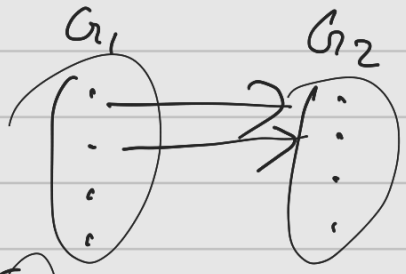
$$= 2^{53} \pmod 3 = 2 \bmod 3 = 2.$$

Isomorphisms:-

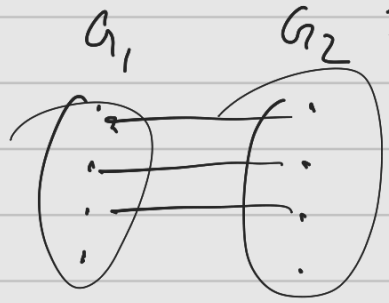
(i) Many-to-one:- (epimorphism)



(ii) **One-to-one:-**



(iii) **Subjunction:-**



Direct Product:- set of integers co-prime with ($\mathbb{Z}_p \to$ 'p')

$\mathbb{Z}_3^* = \{1, 2\}$; $|\mathbb{Z}_3^*| = 2$.

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$; $|\mathbb{Z}_5^*| = 4$.

$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$; $|\mathbb{Z}_{15}^*| = 8$.

Pairing Assumptions (DLIN):-

↳ Decision Linear Diffie-Hellman Assumption (DLIN)
Here $G = H$.

→ $\Pr[A(u, v, h, u^a, v^b, h^{a+b}) = 1 ; u, v, h \in G ; a, b \in \mathbb{Z}_p]$

→ $\Pr[A(u, v, h, u^a, v^b, \eta) = 1 ; u, v, h, \eta \in G ; a, b \in \mathbb{Z}_p]$

$\leq 1/2 + negl(\epsilon)$

10/04/22 **Factoring:-**

Complexity:- $O(\log n)$ Polynomial.

$O(\log^K n), K \geq 1.$

(Heuristic Method)
$\hookrightarrow O(2^{n/2} \cdot \text{Polylog}(2^n))$; $n = \#$ of bits in N

$n = \log_2 N.$

Prime Generation:

- **Fermat's Little Theorem (FLT):-** (Primality Test)

Attempt 1:-

Ex:- $\mathbb{Z}_7^+ = \{1, 2, 3, 4, 5, 6\}$

It should be a prime

$2^6 \bmod 7 = 2$

$3^6 \bmod 7 = 1$

$\vdots$

$6^6 \bmod 7 = 1$

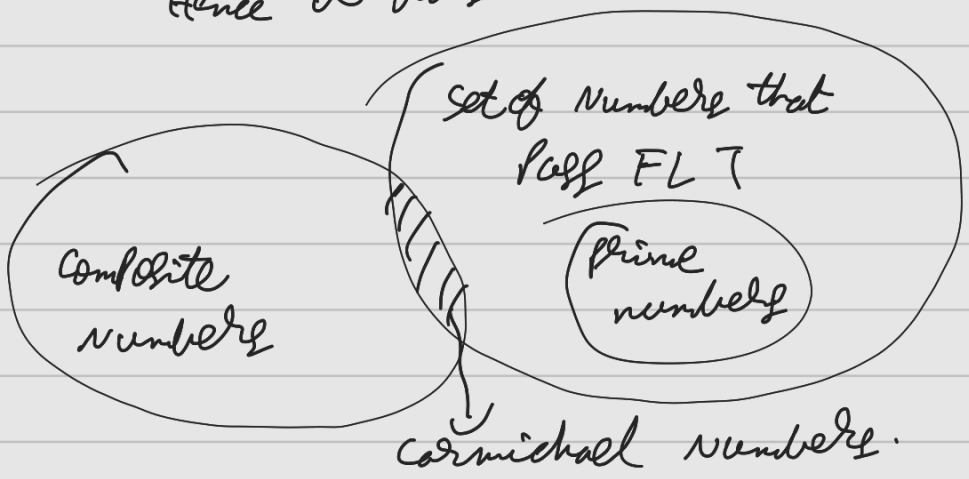
$\rightarrow$ FLT can be fooled by Carmichael numbers!

Ex for Carmichael number:-

$\mathbb{Z}_{561}^* = \{1, \ldots, 560\}$

$\forall a \in [1, \ldots, 560]$; $a^{n-1} \pmod n = 1$

Hence it fools that every number is a prime.



Ex:- (For FLT)

Test if $n = 9$ is a prime.

$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$

$|\mathbb{Z}_9^*| = 6$

If 9 is a prime for $a \in \mathbb{Z}_9^*$,

$a^8 \pmod 9 = 1.$

i.) $a = 2$

$2^8 \bmod 9 = 4$

2-witness of 9 being composite.

ii.) $a = 4$

$4^8 \bmod 9 = 7$

4-witness of 9.

iii.) $a = 5$

$5^8 \bmod 9 = 7$

5-witness of 9.

10/06/22.

iv.) $a = 7$

$7^8 \bmod 9 = 4.$

7-witness of 9.

v.) $a = 8$

$8^8 \bmod 9 = 1.$

$\therefore$ "8 is a strong liar".

$\therefore$ witnesses of composit-ness $= \{2, 4, 5, 7\}$.

$\therefore |\mathbb{Z}_9^*| = 6$

$\therefore$ 4-witnesses $> \frac{6}{2}$.

Wilson Primality Test:- (Primality test)

$(n-1)! \equiv -1 \pmod{n}$

iff n is prime

check 2 $(2-1)! \bmod 2 = 1 \bmod 2 \equiv -1 \pmod{2}$

$-1 = 2 \cdot -1 + 1$ $\quad$ $1 = 2 \cdot 0 + 1$

Remainder is same.

If n is a prime, $(n-1)$ has to be even.

So, $(n-1) = 2^r \cdot u$, $r \geq 1$, u is odd.

Known results:

For all $a \in \{1, \dots, n-1\}$, if n is prime then,

- either $a^u \pmod{n} = 1$,
- (or) $a^{2^r \cdot u} \pmod{n} = -1$.

(Miller-Rabin is based on this)

$\Rightarrow$ So, if n is composite then,

- $a^u \bmod n \neq 1$
- and $a^{2^r \cdot u} \bmod n \neq -1$

Miller-Rabin Test:- (Composite Test)

$a \in \{1, \ldots, n-1\}$

If $(a^u \bmod n \neq 1)$ AND

$(a^{2^1 u} \bmod n \neq -1)$ AND

AND $(a^{2^r \cdot u} \bmod n \neq -1)$

then a is a "strong witness" of n being composite, else a is a "strong liar".

$\Downarrow$

If $a^u \pmod n \neq 1$, return composite.

else if $a^{2^r \cdot u} \pmod n \neq -1$, return composite.

$\vdots$

else if $a^{2^r} \cdot u \pmod n \neq -1$, return composite.

Theorem: If $n \geq 3$ and n is odd and composite, there are at least $\frac{(n-1)}{4}$ elements of $a \in \mathbb{Z}_n$; for which Miller-Rabin returns composite.