09/22/22: Groups:-

Group properties and tricks:-

use this method if and only if base is in the group and the exponential is greater than the length of the group.

If $a < b$, $a \pmod b = a$ (Since $a, b \in \mathbb{Z}^+$)

Num Theory - 4:-

Cyclic Groups:

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ Since,

↳ ($\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$). ($\mathbb{Z}_p^*$ is a cyclic group when 'p' is a prime number.)

If $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ Since,

↳ ($\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$).

Discrete Logarithms:-

$$h = g^x \pmod p$$

$$x = \log_g h \pmod p \quad ; x \in \{0, \ldots, p-1\}$$

09/27/22 CDH problem (Computational Diffie-Hellman Problem):-

$h_1 = g^{x_1}$, $h_2 = g^{x_2}$

$x_1 = \log_g h_1 \pmod p$

$x_2 = \log_g h_2 \pmod p$

$(g^{x_2})^{x_1}$.

Diffie-Hellman problems:-

If,

DL (easy)
- CDH (Easy)
- DDH (Easy)

DL (Hard)
- CDH (Hard?)

DDH (easy)
- CDH (Hard)
- DDH (Hard)

CDH (easy)
- DDH (easy)

Group Generation Algorithm:-

$G = (h^{2 = (p-1)/q} \bmod p)$.