Welcome to Section!

$(G, \cdot)$ **Groups!**

1. There is an identity $e \in G$

$$a \cdot e = a \quad \text{for all } a \in G$$

2. Every element $a \in G$ has an inverse $a^{-1} \in G$

$$a \cdot a^{-1} = e$$

3. Associativity

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

4. Closure: if $a, b \in G$ then

$$a \cdot b \in G$$

$\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$

$\mathbb{Z}_{11}^* = \{1, 2, \ldots, 10\}$

$2^1 = 2$ $\quad 2^5 = 10$ $\quad 2^9 = 6$

$2^2 = 4$ $\quad 2^6 = 9$ $\quad 2^{10} = 1$

$2^3 = 8$ $\quad 2^7 = 7$

$2^4 = 5$ $\quad 2^8 = 3$

$\mathbb{Z}_{11}^*$ is cyclic; 2 is a generator

$3^1 = 3$ $\quad 3^4 = 4$

$3^2 = 9$ $\quad 3^5 = 1$

$3^3 = 5$ $\quad 3^6 = 3$

$Z_{11}^* = \langle 2 \rangle$ ↺ group generated by 2 ← order 10

$\langle 3 \rangle = \{3, 9, 5, 4, 1\}$ ← order 5

group

$H \subseteq G$ and H is a group

↑ subset H is a subgroup of G

$G \subseteq G \rightarrow G$ is a subgroup of G

$\emptyset \subseteq G \rightarrow \emptyset$ is a subgroup of any group

Subgroups have order (size)

that divides the order of G!

$\langle 1 \rangle \rightarrow \{1\}$

Subgroups of cyclic groups are cyclic!

G is cyclic, H subgroup of G.

Suppose for cont. that H is not cyclic.

$\exists$ generator g for G (i.e. $G = \langle g \rangle$)

$\exists\ a, b \in H \to a = g^j,\ b = g^k$

such that j, k are rel. prime

$\gcd(j,k) = 1 \to \alpha j + \beta k = 1$

$(g^j)^\alpha \cdot (g^k)^\beta \to g^{j\alpha + k\beta} = g^1 = g$

$a \in H$, $b \in H$

but $g \in H \to H = G$!

but G is cyclic! ⁂

$g \in G$

$$g^{|G|} = 1 \quad ??$$

g has order $\text{ord}(g)$

$$g^{|G|} = \left(g^{\text{ord}(g)}\right)^{|G| / \text{ord}(g)}$$

$$= (1)^{|G| / \text{ord}(g)} = 1$$

(mod 5)

order 2?

$2^1 = 2$

$2^2 = 4$

$2^3 = 3$

$2^4 = 1$

$$\mathbb{Z}_p^* \rightarrow |\mathbb{Z}_p^*| = p - 1$$

$$g \in \mathbb{Z}_p^* \Rightarrow g^{p-1} = 1$$ — Fermat's Little Theorem

$3^6 = 1$ in $\mathbb{Z}_7^*$

$23^{12} = 10^{12} = 1$ in $\mathbb{Z}_{13}^*$

Euler's Theorem: uses Euler phi/totient fn

$\varphi(n) = \#$ of $a \in \{1, \ldots, n\}$ s.t. $\gcd(a, n) = 1$

or just $n-1$

$\varphi(p) = p-1$ ← prime

$\varphi(7) = 6$

$1, \ldots, 6$ ✓

Euler's Theorem: If $\gcd(a, n) = 1$ then

$$a^{\varphi(n)} \equiv 1 \bmod n$$

$\mathbb{Z}_n^*$ ← has order $\varphi(n)$

↑ Group of things rel. prime to n mod n

$$a^{\varphi(n)} \quad a^{\text{ord}(\mathbb{Z}_n^*)} \equiv 1 \bmod n$$

Examples of Euler's Thm

$$Z_{12}^* = \{1, 5, 7, 11\} \quad \varphi(12) = 4$$

$$1^{\varphi(12)} \to 1^4 \equiv 1 \bmod 12 \qquad 5^4 = 625 \equiv 1 \bmod 12$$

$$7^4 = 2401 \equiv 1 \bmod 12 \qquad 11^4 \equiv (-1)^4 \equiv 1 \bmod 12$$

$$Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\} \quad \varphi(15) = 8$$

$$13^8 \to 1 \bmod 15$$

$$\varphi(15) \to \varphi(3) \cdot \varphi(5)$$

$$2 \cdot 4 = 8$$

Computing Roots

G – finite cyclic group

$|G| = q \leftarrow$ prime

$h \in G \quad 1 < e < q : \; h^{1/e}$

Alg:

$\gcd(e, q) = 1$

1. $\boxed{\alpha = e^{-1}} \pmod q \rightarrow \alpha \cdot e \equiv 1 \pmod q$
2. $y = h^{\alpha} \rightarrow y = h^{1/e}$

$y^e = h$

$\boxed{y^e} = (h^{\alpha})^e = h^{\alpha e} = h^{kq+1}$

$= h \cdot (h^q)^k$

$= h \cdot (1)^k = \boxed{h}$

$\langle 3 \rangle \leq Z_{11}^*$

$|Z_{11}^*| = 5$

$\{3, 9, 5, 4, 1\}$

What is $\sqrt{4}$?

$2^{-1} \equiv 3 \pmod 5$

$4^3 = 9 \rightarrow 9^2 = 4$

What is $\sqrt[3]{5}$

$3^{-1} \equiv 2 \pmod 5$

$5^2 = 3 \rightarrow 3^3 = 5$

What is $\sqrt[4]{9}$

$4^{-1} \equiv 4 \pmod 5$

$9^4 = 5 \rightarrow 5^4 = 9$

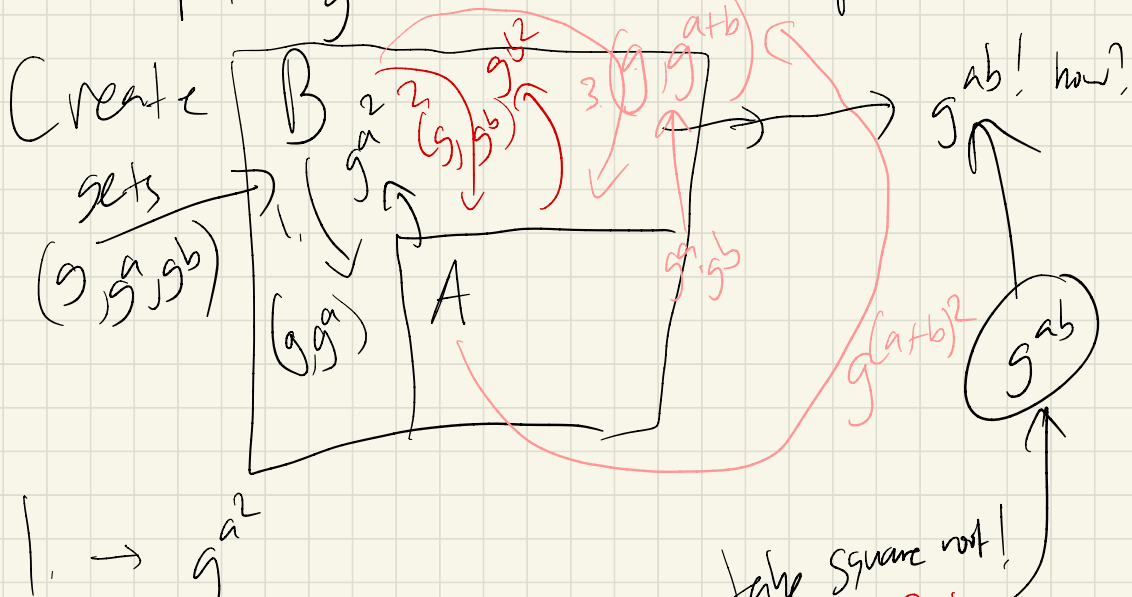
CDH $\Rightarrow$ it is hard to get g^{x^2} from g, g^x

$\downarrow$

hard for Adv to get g^{ab} given g, g^a, g^b

prove by contrapositive!

Suppose $\exists$ Adv A who, given (g, g^x) can output g^{x^2} with non-negl. probability



1. $\rightarrow g^{a^2}$

2. $\rightarrow g^{b^2}$

3. $\rightarrow g^{(a+b)^2} \Rightarrow g^{a^2+2ab+b^2}$ / g^{a^2} and / g^{b^2}