Group → we abstract operations

$(G, *)$

- associativity
- identity
- two-sided inverse.
- closure included in $*: G * G \to G$.

Lagrange's Theorem

$|H| \mid |G|$

The order of an element is $\underbrace{g * g \cdots * g}_{m \text{ times}} = \varepsilon$

for a finite group, an element will always come back to identity (ε)

Multiplicative Group Modulo.

$G_n = \{i : 1 \le i \le n,\ i \text{ is coprime to } n\}$.

Define. $(x * y)$ as $x \cdot y \bmod n$.

$n = 15$

$G_n = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Euler's Totient Function $\phi(n)$

$\phi(n) = |\{i : 1 \le i \le n, i \text{ is coprime with } n\}|$

$\phi(9) = |\{1, 2, 4, 5, 7, 8\}| = 6$

$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots$

$\phi(9) = 9 \times \left(1 - \frac{1}{3}\right) = 6.$

$\phi(120) = 120 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{5}\right)$

$= 120 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5}$

$= 32.$

Recall $|G_n| = \phi(n)$ if $x \in G_n$.

$x^{\phi(n)} = 1 \pmod n$ ← ε

$x^{-1} = x^{\phi(n)-1} \pmod n$

Example. $8x = 5 \pmod{11}$

$\phi(11) = 10$, so $8^{10} = 1 \pmod{11}$

$8^9 = 8^{-1} \pmod{11}$

	8^k
1	8
2	9
3	6
4	4
5	10
6	3
7	2
8	5
9	7

$\Rightarrow 8^{-1} \equiv 7 \pmod{11}$

$x = 5 \times 7 \pmod{11}$

$\equiv 2 \pmod{11}$

$(x = 2, 13, 24 \ldots$
$-9, -20 \ldots)$