

$$a^{p-1} = 1 \pmod p \quad \text{for } a \not\equiv 0 \pmod p$$

חוקי פסגה פשוטים

אגרגט G היא חבורה סופית אם מוגדרת בה כחבורה פסגה פשוטה. $(ab)c = a(bc)$ וכן לכל a חבורה יש
 יחיד e ויחיד a^{-1} כך $e = aa^{-1} = a^{-1}a$, e הוא היחיד
 זהה לכל הנכסל כך $ea = ae = a$

אגרגט G חבורה סופית $H \subseteq G$ וכל H סגורה תחת
 פעולה הנכסל. H קבוצת חבורה של G .

דוגמה: $G = \mathbb{Z}_6$ ופעולה גורם $+$, חבורה חצונית G .

$$3+3=2 \pmod 6$$

וקבוצה $H = \{0, 2, 4\}$ היא חבורה של G .

$$|H|=3, |G|=6$$

למה $H \subseteq G$ והיא סגורה לכל ופעולה הנכסל H $a, b \in H$

$a \in H, c \in H$, $a^{-1}c \in H$ חבורה של G .

הוכחה הפעולה המוגדרת על H היא פעולה הנכסל של G . H סגורה

פעולה זו ופעולה מוגדרת חסמה.

יווין $a, b, c \in H$ נניח $(ab)c = a(bc)$ זה המקרה G -
 וכל $a \in H$.

נניח $a \in H$ ויש $a^{-1} \in H$ ויחידה e וכל a חבורה של G

נניח $a \in H$ $a^{-1} \in H$ ויחידה e וכל a חבורה של G

$$e = aa^{-1} \in H$$