Order 6
Abelian C_6
Not Abelian S_3

Abelian case
elts have order 1, 2, 3

If order $\{1,2\}$ $a \neq 1$
$\{1, a\}$ is a subgroup of order 2
$b \in G - \{1,a\}$ $\{1, a, b, ab\}$ is a subgroup of order 4 But $4 \nmid 6$.

$\exists\, g \in G$, $g^3 = 1$ $g^2 \neq 1$ order 3
Pick $b \in G - \{1, g, g^2\}$ $g^3 = 1$

$\{1, g, g^2, b, bg, bg^2\}$ all are distinct

$G = H \cup bH$ $H \cap bH = \phi$

either $b^2 = 1$ or $(b^3 = 1$ $b^2 \neq 1)$

If $b^2 = 1$ & G is abelian
ab has order 6

~~$1, a, b, a^2 b = a^2$~~
~~$a^3 b = b$, $a^4 b = a$, $a^5 b$~~
~~$= ab = ba^2$~~

$1, bg, b^2 g^2 = g^2$, $b^3 g^3 = b$, $b^4 g^4 = g$, $b^5 g^5 = bg^2$

b is either order 2 or 3. Showed $b^2 \neq 1$
$b^3 = 1$ $b^4 = b$
What's b^2? $1, g, g^2, bg, bg^2, b$
$b^2 \neq 1, b, gb, b^2 = gb$ $g^2 b$

$b^2 = a$ $\quad b^4 = a^2 = b \neq a$

$b^2 = a^2$ $\quad b^4 = a \Rightarrow b \neq a$

G is not abelian

1) $\exists$ an elt of order 6. Why? Cyc.

2) $\exists$ an elt of order 3. Why? Cyc

If only order 2 $(ab)^2 = 1$ $\quad abab = 1$

$a(abab)b = ab$

$ba = ab$

Let a have order 3

$\{1, a, a^2\} < G$

Pick $b \in G - \{1, a, a^2\}$

$G = \{1, a, a^2, b, ab, a^2b\}$

Not abelian $ab \neq ba$

What is ba? $\quad ba = 1$?

if $ba = 1 \Rightarrow b = a^2$ Contr

$ba = b \Rightarrow a = 1$ "

$ba = a \Rightarrow b = 1$ "

$ba = a^2 \Rightarrow b = a$

$ab \neq ba$ (Not abelian)

$ba = a^2b$

$a^2b\,a^2b = a^2(ba)ab = a^2a^2bab$

$= a^4b^2 = b^2$

$b^2 = ?$

$b^2 = b$? $\Rightarrow b = 1$ Contra

$b^2 = ab \Rightarrow b = a$ "

$b^2 = a^2 b \implies b = a^{-1}$

$b^2 = 1, \quad b^2 = a, \quad b^2 = a^2$

If $b^2 = a$ then $b^3 = 1$ Why?

$b^4 = b$

$b^2 = a$

$b = b^4 = a^2$ Contra

$b^2 = a^2$

$b = b^4 = a^4 = a$ Contra

$b^2 = 1$

$\{1, a, a^2, b, ab, a^2 b\}$

$abab = a a^2 b^2 = 1$

$a^2 b a^2 b = a^2 a^4 b^2 = 1$

$f : S_3 \longrightarrow \{1, a, a^2, b, ab, a^2 b\}$

$f((123)) = a \quad f((13)) = b \quad f((23)) = ab$

$f((132)) = a^2 \quad (123)(13) = (23) \quad f((12)) = a^2 b$

$(132)(13) = (12)$

---

p is a prime $\quad \mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$

$\mathbb{Z}_p^* = R \cup N$

disjoint union

$|R| = |N|$

$x^2 = a$

$(-x)^2 = a$

$(p-x)^2 = a$

$\Gamma = \mathbb{Z}_p^* \times \mathbb{Z}_p^* = \{(a, b) \mid a, b \in \mathbb{Z}_p^*\}$

$|\Gamma| = (p-1)^2$

R

$\overline{R \times N} \cup \overline{N \times R} \cup N \times N$

$|R| = \frac{p-1}{2}$ $|N| = \frac{p-1}{2}$

$T = (R \cup N) \times (R \cup N)$

$T = R \times R \cup R \times N \cup N \times R \cup N \times N$

Claim $a, b \in R \Rightarrow ab \in R$

$a = x^2 \pmod p$ $b = y^2 \pmod p$ $ab = x^2 y^2 = (xy)^2 \pmod p$

Claim $a \in R, b \in N$ $ab \notin R$

$ab \in R$ $a = x^2$ $ab = y^2$ $x^2 b = y^2$ $b = y^2 x^{-2} = (yx^{-1})^2 \in R$

$x^2 = a$

$a^{-1} = (x^{-1})^2$

$a \in R \& b \in N \Rightarrow ab \in N$

$a \in N \& b \in R \Rightarrow ab \in N$

Define equiv rel $\equiv$ on T

$(a,b) \equiv (c,d)$ iff $ab = cd$

$T = E_1 \cup E_2 \cdots$

$|E_1|$

Pick $x \in \mathbb{Z}_p^*$ how a, b s.t. $ab = x$

$b = a^{-1} x$

$ab = x$

$b = a^{-1} x$

$|E_1| = |\mathbb{Z}_p^*| = p-1$

The # of equiv classes is $p-1$

$T = R \times R \cup R \times N \cup N \times R \cup N \times N$

If $a \in G \cong \mathbb{Z}_p^*$, $\exists\ E_i = \{(x,y) \mid xy = a\} = C_a$

$|C_a| = p-1$ so

$\frac{(p-1)^2}{2}$ $\quad (\bigcup_{a \in R} C_a) \cup (\bigcup_{a \in N} C_a)$ $\quad \frac{(p-1)^2}{2}$

$|R \times R| = \frac{(p-1)^2}{4}$ $\quad |R \times N| = \frac{(p-1)^2}{4}$ $\quad |N \times R| = \frac{(p-1)^2}{4}$

$\frac{(p-1)^2}{2}$ non residue pairs

$|N \times N| = \frac{(p-1)^2}{4}$ non RES pairs

$$\left(\frac{r}{p}\right)\left(\frac{s}{p}\right) = \left(\frac{rs}{p}\right)$$