

Corrigé du devoir

Exercice:

1°. R réflexive car $e \in G$, symétrique car $x^{-1} \in G$, transitive car G est stable (3)

Si on prend $\pi = (1, 2)$, on a: $(1, 2, 3) = (1, 2)(1, 3, 2)(1, 2)$ c.q.f.d. (3)

2°. $C_e = \{e\}$ $C_a = \{a\}$ (3)

3°. $x \in x^{-1}Hx \Rightarrow x^{-1}Hx \neq \emptyset$; si $x^{-1}Hx \in Hx$ alors $(x^{-1}Hx)^{-1} = x^{-1}H^{-1}x \in x^{-1}Hx$
(car $H^{-1} = H$)
et $(x^{-1}Hx).(x^{-1}Hx) = x^{-1}.(HH).x \in x^{-1}Hx$: $x^{-1}Hx$ est un sous-groupe de G (2)

$x \in N_H$, si $x \in N_H$: $x^{-1}Hx = H \Leftrightarrow Hx = xH \Leftrightarrow H = xHx^{-1} \Rightarrow x^{-1} \in N_H$

et si $y \in N_H$: $(xy)^{-1}H(xy) = y^{-1}(x^{-1}Hx)y = y^{-1}Hy = H \Rightarrow xy \in N_H$.

N_H est un sous-groupe de G (4)

H est distingué dans N_H : évident! (1)

Problème: $p > 2$

1°. Th. de Fermat: c.f. cours! (7)

2°. On a: (1) $\Leftrightarrow \left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$ (2)

3°. On a: $a^p = a$ or $a \neq 0 \Rightarrow a^{p-1} = 1$ $p-1$ est pair $\Rightarrow \left(a^{\frac{p-1}{2}}\right)^2 = 1$

Or, les seules solutions de $x^2 = 1$ sur $\mathbb{Z}/p\mathbb{Z}$ sont $\pm 1 \Rightarrow \boxed{a^{\frac{p-1}{2}} = \pm 1}$ (3)

$\gamma: a \mapsto a^{\frac{p-1}{2}}$: Homomorphisme de groupe: évident! (1)

4°. A chaque carré de $(\mathbb{Z}/p\mathbb{Z})^*$, on peut faire correspondre 2 él^s distincts.

Comme il y a $p-1$ él^s dans $(\mathbb{Z}/p\mathbb{Z})^*$, il y a en tout $\frac{p-1}{2}$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$. (3)

Grâce au 3°, on a: $(\mathbb{Z}/p\mathbb{Z})^* \xrightarrow{\gamma} \{-1, +1\}$ donc, $(\mathbb{Z}/p\mathbb{Z})^*/\ker \gamma$ contient 2 classes
d'équivalence $\Rightarrow \text{card}(\ker \gamma) = \frac{1}{2} \text{card}(\mathbb{Z}/p\mathbb{Z})^* = \frac{p-1}{2}$

Comme $\{x^2, x \in (\mathbb{Z}/p\mathbb{Z})^*\} \subset \ker \gamma$ et que ces 2 ensembles ont même nombre d'éléments,
ils sont égaux et on a bien: a carré dans $(\mathbb{Z}/p\mathbb{Z})^* \Leftrightarrow a^{\frac{p-1}{2}} = 1$ (2)

5°. a). Il faut $\left(-1\right)^{\frac{p-1}{2}} = 1$ i.e. $p \equiv 1 \pmod{4}$ d'où:

$p = 5, 13, 17, 29, 37, 41$ (4)

b). Pour que cette équation soit possible, il faut et il suffit que

$\Delta' = b'^2 - ac$ soit un carré dans $\mathbb{Z}/41\mathbb{Z}$: i.e.: $\Delta' = -8$ carré dans $\mathbb{Z}/41\mathbb{Z}$. (2)

$\Leftrightarrow (-8)^{20} \equiv 1 [41] \Leftrightarrow (64)^{10} \equiv 1 [41] \Leftrightarrow (23)^{10} \equiv 1 [41] \Leftrightarrow (529)^5 \equiv 1 [41] \Leftrightarrow (-4)^5 \equiv 1 [41]$

$\Leftrightarrow -1024 \equiv 1 [41]$ or: $1025 = 25 \times 41$ c.q.f.d.

Résolution de l'équation: $-8 = 369 - 9 \times 41 \equiv 19^2 [41]$

D'où les solutions: $x = 22$ or $x = -16$ (3)