Dev 36 - Équations quadratiques dans $\mathbb{F}_p$. (Algèbre)

Soit $p \in \mathbb{P}$. Soient $a, b, c \in \mathbb{F}_p$ avec $a \neq 0$.

a) L'équation quadratique $ax^2+bx+c=0$ admet des solutions ssi $\Delta := b^2-4ac \in (\mathbb{F}_p^*)^2$

Le cas échéant, les solutions sont $\frac{-b \pm \delta}{2a}$ où $\delta \in \mathbb{F}_p$ est tel que $\delta^2 = \Delta$

b) Supposons $p \geq 3$. Soit $\alpha \in \mathbb{F}_p^*$. Alors $\alpha \in (\mathbb{F}_p^*)^2 \iff \alpha^{\frac{p-1}{2}} = 1$

Preuve :

a) Soit $x \in \mathbb{F}_p$. On a :

$$ax^2+bx+c=0 \iff a\left(x^2+2\frac{b}{2a}x\right)+c=0 \iff a\left(\left(x+\frac{b}{2a}\right)^2-\left(\frac{b}{2a}\right)^2\right)+c=0$$

$$\iff a\left(x+\frac{b}{2a}\right)^2 - \frac{b^2-4ac}{4a} = 0 \iff \left(x+\frac{b}{2a}\right)^2 = \frac{\Delta}{4a^2} \quad (*)$$

- "$\Rightarrow$" (Contraposition)

Si $\Delta \notin (\mathbb{F}_p^*)^2$, alors $\frac{\Delta}{4a^2} = \left(\frac{1}{2a}\right)^2 \Delta \notin (\mathbb{F}_p^*)^2$ (sinon $\Delta = (2a)^2\left(\frac{\Delta}{4a^2}\right) \in (\mathbb{F}_p^*)^2$, absurde) ($\mathbb{F}_p^*$ sous-ensemble de $\mathbb{F}_p$),

mais $\left(x+\frac{b}{2a}\right)^2 \in (\mathbb{F}_p^*)^2$ d'autre part, donc $(*)$ est faux et donc l'équation quadratique n'a pas de solution

Donc on a "$\Rightarrow$" par contraposition

- "$\Leftarrow$" Supposons $\Delta \in (\mathbb{F}_p^*)^2$. Alors il existe $\delta \in \mathbb{F}_p$ tel que $\delta^2 = \Delta$. D'où :

$$ax^2+bx+c=0 \iff \left(x+\frac{b}{2a}\right)^2 = \left(\frac{\delta}{2a}\right)^2 \iff \left(x+\frac{b}{2a}\right)^2 - \left(\frac{\delta}{2a}\right)^2 = 0$$

$$\iff \left(x+\frac{b}{2a}-\frac{\delta}{2a}\right)\left(x+\frac{b}{2a}+\frac{\delta}{2a}\right) = 0 \overset{(\mathbb{F}_p \text{ est un corps, donc intègre})}{\iff} x \in \left\{\frac{-b \pm \delta}{2a}\right\}$$

Donc l'équation quadratique admet les solutions, qui sont celles attendues.

b) $\mathbb{F}_p$ est un corps fini donc $\mathbb{F}_p^*$ est cyclique fini

Également, $d := \frac{p-1}{2}$ divise $p-1 = |\mathbb{F}_p^*|$.

Ainsi, $\mathbb{F}_p^*$ possède un unique sous-groupe H d'ordre d, donné par $H = \{x \in \mathbb{F}_p^* \mid x^d = 1\}$.

Il nous reste à montrer que $(\mathbb{F}_p^*)^2 = H$, en montrant que $(\mathbb{F}_p^*)^2$ est un sous-groupe de $\mathbb{F}_p^*$ d'ordre d.

Pour ce faire, considérons le morphisme de groupes $f : \mathbb{F}_p^* \ni y \mapsto y^2 \in \mathbb{F}_p^*$

On a naturellement $\mathrm{Im}(f) = (\mathbb{F}_p^*)^2$, ce qui montre au passage que $(\mathbb{F}_p^*)^2 < \mathbb{F}_p^*$.

De plus, $\ker(f) = \{\pm 1\}$ car $y \in \ker(f) \iff y^2 = 1 \iff y^2-1 = 0 = (y-1)(y+1) \iff y \in \{\pm 1\}$

Donc $\mathbb{F}_p^* / \{\pm 1\} \simeq (\mathbb{F}_p^*)^2$ par le 1er théorème d'isomorphisme.

Ainsi $|(\mathbb{F}_p^*)^2| = \frac{|\mathbb{F}_p^*|}{|\{\pm 1\}|} = \frac{p-1}{2} = d$. Donc $(\mathbb{F}_p^*)^2$ est un sous-groupe de $\mathbb{F}_p^*$ d'ordre d.

Ainsi $(\mathbb{F}_p^*)^2 = H$. CQFD.