Devoir facultatif n° 4

Dans tout ce problème, p désignera un nombre premier supérieur ou égal à 3. L'objet de ce problème est d'étudier l'existence de racines carrées modulo p.

Si $a, b \in \{0, 1, \ldots, p-1\}$, on note $a * b$ l'unique entier $r \in \{0, 1, \ldots, p-1\}$ vérifiant $ab \equiv r\ [p]$. On remarquera donc que $a * b$ est le reste de la division euclidienne de ab par p et que

$$a * b \equiv ab\ [p].$$

On remarquera que $*$ est associative ainsi que commutative sur $\{0, 1, \ldots, p-1\}$, et qu'elle possède 1 pour élément neutre.
Si $a \in \{0, 1, \ldots, p-1\}$, on note

$$a^2 = a * a,\ a^3 = a * a * a\ \textit{etc.}$$

Si $a, b \in \{0, 1, \ldots, p-1\}$, on dit que b est une *racine carrée* de a si

$$b^2 = a.$$

Remarquons que $0^2 = 0$. On notera C l'ensemble des carrés non nuls de $\{1, 2, \ldots, p-1\}$ et NC l'ensemble des éléments de $\{1, 2, \ldots, p-1\}$ qui ne sont pas des carrés, c'est-à-dire

$$\begin{aligned} C &= \left\{ a \in \{1, 2, \ldots, p-1\} \;\middle|\; \exists b \in \{1, 2, \ldots, p-1\},\ a = b^2 \right\} \\ &= \left\{ b^2 \;\middle|\; b \in \{1, 2, \ldots, p-1\} \right\} \end{aligned}$$

et

$$\begin{aligned} NC &= \{1, 2, \ldots, p-1\} \setminus C \\ &= \left\{ a \in \{1, 2, \ldots, p-1\} \;\middle|\; \forall b \in \{1, 2, \ldots, p-1\},\ a \neq b^2 \right\}. \end{aligned}$$

1) Un exemple. Dans cette question, on suppose que $p = 7$.

- **a)** Calculer $2 * 6$ et $3 * 5$.
- **b)** Déterminer x^2 et x^3 pour tout $x \in \{0, 1, \ldots, 6\}$.
- **c)** En déduire C et NC et observer les valeurs de x^3 pour chaque $x \in C$ puis pour chaque $x \in NC$.

Lorsque vous répondrez aux questions suivantes, vous penserez à comparer vos réponses à l'exemple ci-dessus.

2) Résultats préliminaires. Ces questions sont élémentaires, vous devez bien les détailler.

a) Montrer que $\dfrac{p-1}{2}$ est un entier.

b) Montrer que pour tout $a, b \in \{0, 1, \dots, p-1\}$:

$$a * b = 0 \Rightarrow (a = 0 \text{ ou } b = 0).$$

c) En déduire que pour tout $a \in \{1, \dots, p-1\}$ et tout $b, c \in \{0, 1, \dots, p-1\}$:

$$a * b = a * c \Rightarrow b = c.$$

d) Soit $a \in \{1, \dots, p-1\}$. Montrer qu'il existe un unique $b \in \{1, \dots, p-1\}$ vérifiant

$$a * b = 1.$$

On notera dorénavant cet élément a^{-1}.
On manipulera naïvement la notion de *nombre d'éléments* d'un ensemble. Notamment, on admettra les deux propriétés suivantes :

— si A, B sont deux ensembles ayant autant d'élements et vérifient $A \subset B$, alors $A = B$;

— si un ensemble A a un nombre fini d'éléments et si φ est une fonction injective, alors $\varphi(A)$ a autant d'éléments que A.

3) Nombre de racines carrées.

a) Soit $a, b \in \{1, \dots, p-1\}$, montrer que

$$a^2 = b^2 \Leftrightarrow (a = b \text{ ou } a = p - b).$$

b) En déduire que C possède exactement $\dfrac{p-1}{2}$ éléments puis que NC possède aussi exactement $\dfrac{p-1}{2}$ éléments.

4) Lien entre C et NC.
Soit $a \in NC$. On considère la fonction

$$\varphi_a \; : \; \begin{array}{ccc} \{1, \dots, p-1\} & \to & \{1, \dots, p-1\} \\ x & \mapsto & a * x \end{array}.$$

a) Montrer que φ_a est bijective.

b) Montrer que $\varphi_a(C) \subset NC$ puis que $\varphi_a(C) = NC$.

c) En déduire que $\varphi_a(NC) = C$.

On remarquera que l'on vient de démontrer que le produit de deux nombres qui ne sont pas des carrés est un carré.

5) Théorème de Wilson.

On montre dans cette question le théorème de Wilson : pour tout entier $p \geqslant 2$, p est premier si et seulement si

$$(p-1)! \equiv -1 \ [p].$$

a) Dans cette question seulement, on ne suppose pas que p est premier.
Montrer que si $(p-1)! \equiv -1 \ [p]$, alors p est premier.
Indication : on pourra considérer les diviseurs de p et ceux de $(p-1)!+1$.

b) Montrer que si $a \in \{2, 3, \ldots, p-2\}$, alors $a^{-1} \in \{2, 3, \ldots, p-2\}$ et $a^{-1} \neq a$.

c) En déduire la réciproque : si p est premier, alors $(p-1)! \equiv -1 \ [p]$.

6) Caractérisation des résidus quadratiques.

a) Déterminer les deux racines carrées de 1.

b) Montrer que, si $a \in C$, alors

$$a^{(p-1)/2} \equiv 1 \ [p].$$

Montrer de même que, si $a \in NC$, alors

$$a^{(p-1)/2} \equiv 1 \ [p] \ \text{ ou } \ a^{(p-1)/2} \equiv -1 \ [p].$$

c) Montrer que

$$(p-1)! \equiv (-1)^{(p-1)/2} \prod_{k \in C} k \ [p]$$

Indication : pour $k \in C$ et a une racine carrée de k, on pourra remarquer que l'autre racine carrée de k est $p-a$.

d) Soit $a \in NC$. En reprenant les résultats de la partie **4)**, montrer que

$$\prod_{k \in NC} k \equiv a^{(p-1)/2} \prod_{k \in C} k \ [p].$$

e) En utilisant le théorème de Wilson, en déduire que pour tout $a \in NC$:

$$a^{(p-1)/2} \equiv -1 \ [p].$$

— FIN —