Préparation DS N° 5

Structures Algébriques

EXERCICE 2: Un anneau d'extension quadratique

Soit α l'une des deux racines complexes[1] du polynôme $P(z) = z^2 + z + 2$.
On désigne par $\mathbf{Z}[\alpha]$ l'ensemble des nombres complexes défini par

$$\boxed{\mathbf{Z}[\alpha] = \left\{p + \alpha q\,;\ (p,q) \in \mathbf{Z}^2\right\}}$$

1. Montrez que $\mathbf{Z}[\alpha]$ est un sous-anneau de $\mathbf{C}$.

2.a. Montrez[2] que $\alpha + \bar{\alpha} = -1$ et $\alpha\,\bar{\alpha} = 2$.

b. Montrez que pour tout $z \in \mathbf{Z}[\alpha]$, $\bar{z} \in \mathbf{Z}[\alpha]$.

c. Montrez que pour tout $z \in \mathbf{Z}[\alpha]$, $z\,\bar{z} \in \mathbf{N}$.

3.a. Soit $z = p + \alpha q$ un élément de $\mathbf{Z}[\alpha]$. Montrez que z est inversible dans $\mathbf{Z}[\alpha]$ *si et seulement si* (p,q) vérifie :

$$p^2 + 2q^2 - pq = 1 \qquad (1)$$

b. Montrez que l'équation (2) est impossible lorsque $pq < 0$.

c. Montrez que l'équation (2) est impossible lorsque $pq > 0$.

d. Déduisez des questions précédentes l'ensemble des éléments inversibles de $\mathbf{Z}[\alpha]$.

Exercice 1 : Idéaux et sous-anneaux de $\mathbb{Z}^2$

Soit $\mathcal{A}$ un anneau commutatif, $\mathcal{I}$ une partie de $\mathcal{A}$. On dit que $\mathcal{I}$ est un *idéal* de $\mathcal{A}$ si $\mathcal{I}$ est un sous-groupe de $(\mathcal{A},+)$, stable par multiplication par un élément quelconque de $\mathcal{A}$, *i.e.* :

$$\forall (a,i)\in\mathcal{A}\times\mathcal{I},\quad ai\in\mathcal{I}.$$

1 Soit $x\in\mathcal{A}$. On pose $x\mathcal{A}=\{xa, a\in\mathcal{A}\}$. Montrer que $x\mathcal{A}$ est un idéal de $\mathcal{A}$.
Soit $\mathcal{I}$ un idéal de $\mathcal{A}$. On dit que $\mathcal{I}$ est *principal* s'il existe $x\in\mathcal{A}$ tel que $\mathcal{I}=x\mathcal{A}$.

2 Montrer que tout idéal de $\mathbb{Z}$ est principal.
On travaille maintenant dans l'anneau produit $\mathbb{Z}^2$.

3 Soit $\mathcal{I}$ un idéal de $\mathbb{Z}^2$. On pose

$$\mathcal{I}_1=\{x\in\mathbb{Z},(x,0)\in\mathcal{I}\}\quad\text{et}\quad\mathcal{I}_2=\{y\in\mathbb{Z},(0,y)\in\mathcal{I}\}.$$

a Montrer que $\mathcal{I}=\mathcal{I}_1\times\mathcal{I}_2$.
b En déduire que $\mathcal{I}$ est principal.

4 Pour tout $d\in\mathbb{N}$, on pose

$$A_d=\{(x,y)\in\mathbb{Z}^2, d|y-x\}.$$

a Préciser A_0 et A_1.
b Montrer que pour tout entier naturel d, A_d est un sous-anneau de $\mathbb{Z}^2$.
Soit A un sous-anneau de $\mathbb{Z}^2$, distinct de A_0.
c Montrer que $\{n\in\mathbb{N}^*,(0,n)\in A\}$ est non vide. On note d son plus petit élément.
d Montrer que $A=A_d$.

Problème : L'anneau $\mathbb{Z}/n\mathbb{Z}$

Le but de ce problème est d'introduire les anneaux $\mathbb{Z}/n\mathbb{Z}$, fondamentaux en arithmétique.

Pour tout n entier naturel $\geqslant 2$, on définit la *relation de congruence modulo n* sur $\mathbb{Z}$, par :

$$\forall x, y \in \mathbb{Z}, \quad (y \equiv x\,[n]) \Leftrightarrow (\exists k \in \mathbb{Z}, \quad y = x + kn)$$

(autrement dit, $y - x$ est un multiple entier de n, ou encore n divise $y - x$).

On rappelle que relation de congruence modulo n est une relation réflexive, symétrique, transitive (on dit que c'est une *relation d'équivalence*).

Partie A – L'anneau $\mathbb{Z}/n\mathbb{Z}$

Pout tout entier relatif x, on note $\bar{x}$ la *classe d'équivalence de x* pour la relation de congruence modulo n, *i.e.* :

$$\bar{x} = \{y \in \mathbb{Z}, \quad y \equiv x[n]\}$$

A.1 Montrer que si $x \equiv x'[n]$, alors $\bar{x} = \bar{x}'$. Montrer que l'ensemble $\{\bar{x}, x \in \mathbb{Z}\}$ est fini, de cardinal n. On note cet ensemble $\mathbb{Z}/n\mathbb{Z}$.

A.2 On définit des lois d'addition et de multiplication sur $\mathbb{Z}/n\mathbb{Z}$:

$$\forall \bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}, \quad \bar{x} + \bar{y} = \overline{x + y}$$

et

$$\forall \bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}, \quad \bar{x} \cdot \bar{y} = \overline{xy}$$

Montrer que ces opérations sont effectivement bien définies (il s'agit de prouver que la définition ne dépend pas des représentants x et y choisis pour les classes d'équivalence $\bar{x}$ et $\bar{y}$), puis qu'elles confèrent à $\mathbb{Z}/n\mathbb{Z}$ une structure d'anneau commutatif.

A.3 Montrer que si n est composé (*i.e.* n'est pas premier), l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

A.4 Montrer que l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si n est premier.

A.5 *Petit théorème de Fermat :* soit $a \in \mathbb{Z}$, et p un nombre premier. Montrer que $a^p \equiv a\,[p]$.

Indication : utiliser la question précédente, et un exercice de la feuille de TD sur les structures algébriques.

Partie B – Carrés dans $\mathbb{Z}/p\mathbb{Z}$

B.1 Soit $a \in \mathbb{Z}$, et p un nombre premier *impair*. On dit que a est un *carré modulo p* (ou que a ou $\bar{a}$ est un *carré* dans $(\mathbb{Z}/p\mathbb{Z})$) s'il existe $x \in \mathbb{Z}$ tel que

$$a \equiv x^2\,[p]$$

Montrer que dans $\mathbb{Z}/p\mathbb{Z}$ il y a $\frac{p+1}{2}$ carrés.

Indication : utiliser le morphisme carré sur $(\mathbb{Z}/p\mathbb{Z})^*$, pour montrer qu'il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$.

B.2 Montrer que $x \in \mathbb{Z}$ tel que $\bar{x} \neq \bar{0}$ est un carré modulo p si et seulement si $x^{\frac{p-1}{2}} \equiv 1\,[p]$.

B.3 Montrer que -1 est un carré modulo p si et seulement si $p \equiv 1\,[4]$.

CORRIGE

EXERCICE 2

Soit α l'une des deux racines complexes du polynôme $P(z) = z^2 + z + 2$.
On désigne par $\mathbf{Z}[\alpha]$ l'ensemble des nombres complexes défini par

$$\boxed{\mathbf{Z}[\alpha] = \left\{p + \alpha q\,;\ (p,q) \in \mathbf{Z}^2\right\}}$$

0. **remarque préliminaire** P est un polynôme à coefficients réels de discriminant strictement négatif. Il admet deux racines complexes conjuguées qui vérifient

$$\left\|\begin{array}{lcr} \alpha + \bar{\alpha} & = & -1 \\ \alpha \times \bar{\alpha} & = & 2 \\ \alpha^2 + \alpha + 2 & = & 0 \end{array}\right.$$

1. Pour montrer que $\mathbf{Z}[\alpha]$ est un sous-anneau de $\mathbf{C}$, utilisons la **caractérisation des sous-anneaux** :

- $1 = 1 + 0\ \alpha \in \mathbf{Z}[\alpha]$
- soit $(z_1, z_2) \in \mathbf{Z}[\alpha]^2$. Par construction, il existe des couples (p_1, q_1) et (p_2, q_2) d'entiers relatifs tels que $z_1 = p_1 + \alpha q_1$ et $z_2 = p_2 + \alpha q_2$. On a alors

$$\begin{array}{rcl} z_1 - z_2 & = & \big(p_1 + \alpha q_1\big) - \big(p_2 + \alpha q_2\big) \\ & = & \underbrace{(p_1 - p_2)}_{\in \mathbf{Z}} + \alpha \underbrace{(q_1 - q_2)}_{\in \mathbf{Z}} \end{array}$$

- soit $(z_1, z_2) \in \mathbf{Z}[\alpha]^2$. Avec les notations précédentes,

$$\begin{array}{rcl} z_1 \times z_2 & = & \big(p_1 + \alpha q_1\big) \times \big(p_2 + \alpha q_2\big) \\ & = & p_1 p_2 + \alpha^2 q_1 q_2 + \alpha(p_1 q_2 + p_2 q_1) \\ & = & p_1 p_2 - (\alpha + 2) q_1 q_2 + \alpha(p_1 q_2 + p_2 q_1) \\ & = & \underbrace{(p_1 p_2 - 2 q_1 q_2)}_{\in \mathbf{Z}} + \alpha \underbrace{(p_1 q_2 + p_2 q_1 - q_1 q_2)}_{\in \mathbf{Z}} \end{array}$$

D'après la **caractérisation des sous-anneaux**, $\mathbf{Z}[\alpha]$ est uun sous-anneau de $(\mathbf{C}, +, \times)$. ▲

2.a. D'après la remarque préliminaire (somme et produit des racines) $\alpha + \bar{\alpha} = -1$ et $\alpha\,\bar{\alpha} = 2$. ▲

b. Soit $z \in \mathbf{Z}[\alpha]$. Par construction, il existe $(p, q) \in \mathbf{Z}^2$ tel que $z = p + \alpha q$. En utilisant la remarque préliminaire (ou la question précédente), il vient

$$\begin{array}{rcl} \bar{z} & = & \overline{p + \alpha q} = p + \bar{\alpha} q \\ & = & p - (\alpha + 1) q = \underbrace{(p - q)}_{\in \mathbf{Z}} - \alpha \underbrace{q}_{\in \mathbf{Z}} \end{array}$$

▲

c. Soit $z \in \mathbf{Z}[\alpha]$. Avec les notations précédentes, on a

$$\begin{aligned} z\,\bar{z} &= (p+\alpha q)(p+\bar{\alpha} q) \\ &= p^2 + |\alpha|^2 q^2 + pq(\alpha+\bar{\alpha}) \\ &= p^2 + 2q^2 - pq \end{aligned}$$

Sous cette forme il apparait clairement que $z\,\bar{z}$ est un entier relatif. Comme de plus $z\,\bar{z} = |z]|^2$, ce produit est positif. Ainsi $z\,\bar{z} \in \mathbf{N}$. ▲

3.a. Soit $z = p + \alpha q$ un élément de $\mathbf{Z}[\alpha]$.

- Supposons que $z \in \mathbf{Z}[\alpha]^\times$ soit inversible. Notons $w = z^{-1}$. Comme $z\,w = 1$ il vient
$$|z|^2\,|w|^2 = 1$$
D'après la question précédente, $|z|^2$ et $|w|^2$ sont des entiers naturels, qui divisent 1. Ceci entraîne que $|z|^2 = |w|^2 = 1$. En utilisant l'expression obtenue à la question précédente pour le produit $z\,\bar{z}$, il s'ensuit :
$$p^2 + 2q^2 - pq = 1$$

- Réciproquement, supposons que $p^2 + 2q^2 - pq = 1$. Compte-tenu de l'expression obtenue à la question précédente pour le produit $z\,\bar{z}$, l'hypothèse se traduit par $z\,\bar{z} = 1$. Par conséquent, z est inversible et son inverse est son conjugué $\bar{z}$.

Par double-implication on a prouvé que z est inversible dans $\mathbf{Z}[\alpha]$ *si et seulement si* (p,q) vérifie :

$$p^2 + 2q^2 - pq = 1 \qquad (2)$$

▲

b. Soit $(p,q) \in \mathbf{Z}^2$ tel que $pq < 0$. Montrons par l'absurde que (p,q) ne peut être solution de (2).
Supposons *au contraire* que (p,q) vérifie (2). En ce cas, $0 \leqslant p^2 + 2q^2 = 1 + pq$. Comme pq est strictement négatif, il en résulte successivement que $0 \leqslant p^2 + 2q^2 < 1$, puis que $p = q = 0$. Substituons dans (2) pour obtenir $0 = 1$. *Absurde !*
Ainsi, l'équation (2) est impossible lorsque $pq < 0$. ▲

c. Soit $(p,q) \in \mathbf{Z}^2$ tel que $pq > 0$. Montrons par l'absurde que (p,q) ne peut être solution de (2).
Supposons *au contraire* que (p,q) vérifie (2).

$$\begin{aligned} p^2 + 2q^2 - pq = 1 &\iff p^2 - 2pq + q^2 + q^2 + pq = 1 \\ &\iff (p-q)^2 + q^2 = 1 - pq. \end{aligned}$$

Comme précédemment, l'encadrement $0 \leqslant (p-q)^2 + q^2 < 1$ entraîne que $q = 0$ et $p = q$, soit $p = 0$ et $q = 0$. Substituons dans (2) pour obtenir $0 = 1$. *Absurde !*
Ainsi, l'équation (2) est impossible lorsque $pq > 0$. ▲

d. D'après les questions précédentes, $\mathbf{Z}[\alpha]^\times \subset \{p+\alpha q \mid pq = 0\}$. Réciproquement,

- si $p = 0$, l'équation (2) s'écrit $2q^2 = 1$ qui est impossible dans $\mathbf{Z}$.

Exercice 1 : Idéaux et sous-anneaux de $\mathbb{Z}^2$

1 $x\mathcal{A}$ est bien sûr une partie non vide de $\mathcal{A}$, et, pour tout $a, a' \in \mathcal{A}$:

$$xa - xa' = x(a - a') \in x\mathcal{A} \quad \text{et} \quad (xa)a' = x(aa') \in x\mathcal{A},$$

par structure d'anneau de $\mathcal{A}$.

$x\mathcal{A}$ est donc bien un idéal de $\mathcal{A}$.

2 Soit $\mathcal{I}$ un idéal de $\mathbb{Z}$. C'est en particulier un sous-groupe de $(\mathbb{Z}, +)$, donc de la forme $x\mathbb{Z}$ pour un certain entier x (cf. le cours) : tout idéal de $\mathbb{Z}$ est principal.

3

a Soit $(x, y) \in \mathcal{I}_1 \times \mathcal{I}_2$. Les couples $(x, 0)$ et $(0, y)$ appartiennent à $\mathcal{I}$, donc leur somme (x, y) également : ceci montre $\mathcal{I}_1 \times \mathcal{I}_2 \subset \mathcal{I}$.

Réciproquement, soit $(x, y) \in \mathcal{I}$. En multipliant par $(1, 0) \in \mathcal{A}$, il vient $(x, 0) \in \mathcal{I}$, *i.e.* $x \in \mathcal{I}_1$, et, de même, $(0, y) \in \mathcal{I}$, *i.e.* $y \in \mathcal{I}_2$: ceci montre l'inclusion réciproque, puis l'égalité.

b $\mathcal{I}_1$ et $\mathcal{I}_2$ sont principaux : soit $n_1, n_2 \in \mathbb{Z}$ tels que $\mathcal{I}_1 = n_1\mathbb{Z}$ et $\mathcal{I}_2 = n_2\mathbb{Z}$. On vérifie aisément que $\mathcal{I} = (n_1, n_2)\mathbb{Z}^2$: $\mathcal{I}$ est principal.

4

a $A_0 = \{(x, x), x \in \mathbb{Z}\}$ et $A_1 = \mathbb{Z}^2$ (car 1 divise tout entier, et 0 ne divise que lui-même).

b Soit $d \in \mathbb{N}$. A_d est une partie de $\mathbb{Z}^2$, comprenant $(1, 1)$, et, si (x, y) et (x', y') en sont des éléments, alors d divise $y - x$ et $y' - x'$, donc d divise $(y - y') - (x - x')$, *i.e.* $(x, y) - (x', y') \in A_d$ et d divise $yy' - xx' (= y(y' - x') + x'(y - x))$, *i.e.* $(x, y)(x', y') \in A_d$: A_d est bien un sous-anneau de $\mathbb{Z}^2$.

c Puisque $A \neq A_0$, on peut trouver des entiers distincts x et y tels que $(x, y) \in A_d$. Quitte à prendre l'opposé de (x, y) (également élément de A_d), on peut supposer $y > x$. Comme $(1, 1) \in A$, on a $(x, x) \in A$, puis en posant $n = y - x$ (entier naturel non nul), $(0, n) = (x, y) - (x, x) \in A$.

d A est un sous-anneau de $\mathbb{Z}^2$ comprenant $(0, d)$ et $(1, 1)$, donc contenant $\{(x, x + kd), (x, k) \in \mathbb{Z}\}$, *i.e.* $A_d \subset A$.

Réciproquement, si $(x, y) \in A$, alors $(x, y) \in A_d$ si $x = y$ (car d divise 0), et, si $x \neq y$ on a vu lors de la question précédente que $(0, |y - x|)$ appartenait à A. On effectue la division euclidienne de $|y - x|$ par $d (\in \mathbb{N}^*)$: $|y - x| = dq + r$. On a $(0, r) = (0, |y - x|) - q(0, d) \in A$, d'où $r = 0$ par minimalité de d (on rappelle que $0 \leqslant r < d$) : d divise $y - x$, $(x, y) \in A_d$.

Il vient bien : $A = A_d$.

L'anneau $\mathbb{Z}/n\mathbb{Z}$

Partie A – L'anneau $\mathbb{Z}/n\mathbb{Z}$

A.1 Soit $y \in \bar{x}$. On a donc $y \equiv x\,[n]$, puis $y \equiv x'\,[n]$ (par transitivité de la relation de congruence modulo n), et enfin $y \in \bar{x}'$ (par définition de $\bar{x}'$). Il vient donc $\bar{x} \subset \bar{x}'$. Comme la relation de congruence est symétrique, on a également $x' \equiv x\,[n]$, ce qui permet d'échanger les rôles de x et de x', et de montrer l'inclusion réciproque.

En conclusion, $\bar{x} = \bar{x'}$.

Considérons les classes de 0, 1, ...,$n-1$. Ces classes sont distinctes deux à deux (si $i, j \in [\![0, n-1]\!]$, $i \neq j$, alors $i - j \in [\![-(n-1), n-1]\!]$, et $i - j \neq 0$. Par conséquent, n ne divise pas $i - j$, puis $\bar{i} \neq \bar{j}$), et toute classe de congruence modulo n est de ce type (grâce à la division euclidienne, tout entier définit la même classe que son reste par la division euclidienne par n).

L'ensemble $\{\bar{x}, x \in \mathbb{Z}\}$ est donc fini, de cardinal n.

A.2 Pour définir par exemple $\bar{x} + \bar{y}$, on choisit arbitrairement des représentants des classes $\bar{x}$ et $\bar{y}$ (par exemple $x + 3n$ et $y - 2n$). Le problème réside dans ce choix arbitraire. Qui nous dit que le résultat n'aurait pas été autre si nous avions pris d'autres représentants (par exemple $x - 6n$ et $y + 9n$) ? L'objet de cette question est donc de s'assurer de la validité de cette définition.

Si $x' = x + kn$ et $y' = y + ln$ $(x, y, k, l \in \mathbb{Z})$, alors $x' + y' = x + y + (k + l)n$ et $x'y' = xy + (kln + ky' + lx')n$, et par conséquent $\overline{x' + y'} = \overline{x + y}$, et $\overline{x'y'} = \overline{xy}$:

Les opérations d'addition et de multiplication dans $\mathbb{Z}/n\mathbb{Z}$ sont bien définies.

On vérifie aisément que muni de ces lois, $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif.

A.3 Si n est composé, on peut écrire $n = pq$, où $p, q \geqslant 2$. Les classes $\bar{p}$ et $\bar{q}$ sont non nulles, leur produit est cependant la classe nulle : l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ comporte au moins un diviseur de zéro.

Si n est composé, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

A.4 Si n n'est pas premier, *i.e.* si n est composé (on a supposé $n \geqslant 2$), alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre, donc n'est sûrement pas un corps.

Si n est premier, alors tout nombre $m \in [\![1, n-1]\!]$ est premier avec n, et la relation de Bézout donne deux entiers u et v tels que $um + vn = 1$, ce qui après réduction modulo n donne $\bar{u}\bar{m} = \bar{1}$: tout élément *non nul* est inversible, et l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ (commutatif et non nul) est un corps.

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

A.5 Soit $a \in \mathbb{Z}$, et p un nombre premier. D'après la question précédente, $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe fini d'ordre $p-1$, l'ordre de chacun de ses élements divise donc $p-1$, et par conséquent, si p ne divise pas a, alors $a^{p-1} \equiv 1\,[p]$ puis $a^p \equiv a\,[p]$. Cette relation est clairement vérifiée si $a \equiv 0\,[p]$ (puisqu'alors $a^p \equiv 0[p]$).

Pour tout nombre premier p, tout entier relatif a, $\quad a^p \equiv a\,[p]$.

Partie B – Carrés dans $\mathbb{Z}/p\mathbb{Z}$

B.1 On a $\bar{x}^2 = \bar{y}^2$ si et seulement si $(\bar{x} - \bar{y})(\bar{x} + \bar{y}) = \bar{0}$. Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps, c'est un anneau intègre, et donc $\bar{x}^2 = \bar{y}^2$ si et seulement si $\bar{x} = \bar{y}$ ou $\bar{x} = -\bar{y}$. L'ensemble $\mathbb{Z}/p\mathbb{Z}$ est constitué des classes de $-\frac{p-1}{2}$, ..., $\frac{p-1}{2}$ (cela a un sens car p est impair), donc l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$ est constitué des carrés de ces classes, et donc, d'après ce qui précède, des classes $\bar{0}^2, \bar{1}^2, \ldots, \overline{\frac{p-1}{2}}^2$, qui sont distinctes deux à deux (toujours d'après ce qui précède) :

il y a $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.

Voilà une autre démonstration, plus abstraite :

Soit p un nombre premier *supérieur ou égal à* 3. On considère l'application carré sur $(\mathbb{Z}/p\mathbb{Z})^*$: cette application est bien définie (car $\mathbb{Z}/p\mathbb{Z}$ est sans diviseur de zéro) et est en fait un morphisme (car $\mathbb{Z}/p\mathbb{Z}$ est un anneau commutatif). Un élément x appartient à son noyau si et seulement si $x^2 = \bar{1}$, *i.e.* $(x - \bar{1})(x + \bar{1}) = \bar{1}$,

i.e. $x \in \{\pm\bar{1}\}$. Cette application n'est donc pas injective, et donc pas surjective (puisque $(\mathbb{Z}/p\mathbb{Z})^*$ est fini), et il existe un élément y de $(\mathbb{Z}/p\mathbb{Z})^*$ qui ne soit pas un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$. On vérifie immédiatement que la multiplication par y dans $(\mathbb{Z}/p\mathbb{Z})^*$ est une application bijective qui envoie l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$ sur son complémentaire, et réciproquement : il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$, et donc $\frac{p-1}{2}$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$. Comme 0 est un carré dans $(\mathbb{Z}/p\mathbb{Z})$, il y a $\frac{p+1}{2}$ carrés dans $(\mathbb{Z}/p\mathbb{Z})$.

B.2

Si $x \in (\mathbb{Z}/p\mathbb{Z})^*$ est un carré y^2 modulo p alors $x^{\frac{p-1}{2}} \equiv (y^2)^{\frac{p-1}{2}} \equiv y^{p-1} \equiv 1\,[p]$. Nous avons donc trouvé $\frac{p-1}{2}$ solutions à l'équation polynomiale $x^{\frac{p-1}{2}} \equiv 1\,[p]$ de degré $\frac{p-1}{2}$.

Pour pouvoir conclure, montrons qu'une équation polynomiale de degré $k \geqslant 0$ dans $\mathbb{Z}/p\mathbb{Z}$ (à une inconnue) admet au plus k solutions distinctes.

On peut d'abord montrer qu'un polynôme P à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ admettant $\bar{x}$ pour racine est divisible par $(X - \bar{x})$ (par récurrence forte sur le degré, si P est de coefficient dominant $\bar{\alpha}$, de degré k, et admet $\bar{x}$ pour racine, alors $P - \bar{\alpha}X^{k-1}(X - \bar{x})$ est de degré inférieur à celui de P, on peut lui appliquer l'hypothèse de récurrence).

On montre ensuite par récurrence qu'un polynôme de degré k dans $\mathbb{Z}/p\mathbb{Z}$ admet au plus k racines distinctes. Il n'y a rien à prouver pour l'amorçage. Supposons la propriété vérifiée pour $k \geqslant 0$ fixé, montrons la pour $k+1$. Soit donc P un polynôme de degré $k+1$. Si P n'admet pas de racine, le résultat est évident. Si $\bar{x}$ est une racine de P, alors on peut écrire $P = (X - \bar{x})Q$, où Q est de degré $k-1$, et l'hypothèse de récurrence permet alors de conclure.

L'équation polynomiale $x^{\frac{p-1}{2}} \equiv 1\,[p]$ possède donc au plus $\frac{p-1}{2}$ racines : ce sont celles que l'on a trouvées.

x non congru à 0 modulo p est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $x^{\frac{p-1}{2}} \equiv 1\,[p]$.