Devoir Maison (16 Fevrier 2018)
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 $p \equiv 1\,[4]$.

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 $x^{\frac{p-1}{2}} \equiv 1\,[p]$.