

# Corrigé de devoir non surveillé

## 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  $0, 1, \dots, n-1$ . Ces classes sont distinctes deux à deux (si  $i, j \in \llbracket 0, n-1 \rrbracket$ ,  $i \neq j$ , alors  $i-j \in \llbracket -(n-1), n-1 \rrbracket$ , 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  $\overline{x' + y'} = \bar{x} + \bar{y}$ , et  $\overline{x'y'} = \bar{x}\bar{y}$  :

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

On vérifie aisément que  $\mathbb{Z}/n\mathbb{Z}$  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  $p, q \geq 2$ . 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  $n \geq 2$ ), alors  $\mathbb{Z}/n\mathbb{Z}$  n'est pas intègre, donc n'est sûrement pas un corps.

Si  $n$  est premier, alors tout nombre  $m \in \llbracket 1, n-1 \rrbracket$  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 éléments 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  $a$ ,  $a^p \equiv a [p]$ .

### 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  $-\frac{p-1}{2}, \dots, \frac{p-1}{2}$  (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  $\bar{0}^2, \bar{1}^2, \dots, \frac{p-1}{2}^2$ , 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.*  $x \in \{\pm 1\}$ . 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  $k \geq 0$  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  $k \geq 0$  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  $x^{\frac{p-1}{2}} \equiv 1 [p]$ .