Correction du Devoir n°1

Exercice 1. On utilise l'algorithme suivant pour coder un mot : on remplace chaque lettre par sa position dans l'alphabet (a par 1, b par 2, ...), on multiplie cette position par 7 puis on prend le reste de la division euclidienne par 26.

a) Coder le mot "JAZZ".

- Les lettres J, A et Z ont respectivement pour position 10, 1 et 26. La division euclidienne par 26 de leur produit par 7 donne : $10 \times 7 = 70 = 26 \times 2 + 18$, $1 \times 7 = 26 \times 0 + 7$ et $26 \times 7 = 26 \times 7 + 0$. D'où le résultat du codage : 18,7,0,0.

b) Expliquer pourquoi deux mots différents seront codés différemment.

- Associer, à une lettre de l'alphabet, sa position x est une bijection de l'ensemble des lettres de l'alphabet dans l'ensemble des entiers $\{1, 2, \cdots, 26\}$.

  Associer, à un entier x compris entre 1 et 26, sa classe $\overline{x}$ modulo 26 définit une bijection de l'ensemble $\{1, 2, \cdots, 26\}$ dans l'anneau $\mathbb{Z}/26\mathbb{Z}$.

  La classe de 7 est inversible dans l'anneau $\mathbb{Z}/26\mathbb{Z}$, car 7 est premier à 26. Par conséquent, la multiplication par 7 est une bijection de cet anneau dans lui-même.

  L'image de $\overline{7x}$ par la bijection

  Associer, à la classe $\overline{y} \in \mathbb{Z}/26\mathbb{Z}$, le reste de la division euclidienne de y par 26 définit une bijection de $\mathbb{Z}/26\mathbb{Z}$ sur l'ensemble $\{0, 1, \cdots, 25\}$.

  L'algorithme de codage, qui est la composition de ces bijections, définit ainsi une bijection de l'ensemble des lettres de l'alphabet sur l'ensemble $\{0, 1, \cdots, 25\}$. Donc deux lettres différentes sont codées différemment et il en est de même pour les mots.

c) Donner l'algorithme (très similaire à celui de départ) permettant de décoder.

- La relation $7 \times 15 - 26 \times 4 = 1$ montre que l'inverse de $\overline{7} \in \mathbb{Z}/26\mathbb{Z}$ est $\overline{15}$. La réciproque de la multiplication par $\overline{7}$ dans $\mathbb{Z}/26\mathbb{Z}$ est donc la multiplication par $\overline{15}$.

  Pour décoder un nombre $z \in \{0, 1, \cdots, 25\}$, il faut prendre le représentant de $\overline{15z} \in \mathbb{Z}/26\mathbb{Z}$ dans $\{1, 2, \cdots, 26\}$, puis la lettre correspondant à cette position.

Exercice 2. Soient $p \geqslant 3$ et $q \geqslant 3$ deux nombres premiers distincts.

a) Combien de solutions l'équation $x^2 = 1$ possède-t-elle dans $\mathbb{Z}/pq\mathbb{Z}$?

- Les nombres premiers p et q étant distincts, le lemme chinois s'applique à $\mathbb{Z}/pq\mathbb{Z}$ et donne l'isomorphisme d'anneaux naturel α: $\mathbb{Z}/pq\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ définit par $\alpha(n \bmod pq) = (n \bmod p, n \bmod q)$.

  Soit $a \in \mathbb{Z}/pq\mathbb{Z}$. Si on note $\alpha(a) = (b, c)$. On a les équivalences suivantes :

$$a^2 = 1 \Leftrightarrow \alpha(a^2) = \alpha(1) \Leftrightarrow \alpha(a)^2 = (1, 1) \Leftrightarrow (b, c)^2 = (1, 1) \Leftrightarrow (b^2, c^2) = (1, 1) \Leftrightarrow b^2 = c^2 = 1$$

  Ainsi α induit une bijection entre les solutions a de l'équation $x^2 = 1$ dans $\mathbb{Z}/pq\mathbb{Z}$ et les couples (b, c) formés d'une solution de la même équation dans $\mathbb{Z}/p\mathbb{Z}$ et d'une solution dans $\mathbb{Z}/q\mathbb{Z}$. La factorisation $x^2 - 1 = (x - 1)(x + 1)$ montre que l'équation $x^2 = 1$ a pour solution ± 1 dans tout corps. D'après les hypothèses, $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ sont des corps dans lesquels $1 \neq -1$, si bien que l'équation $x^2 = 1$ y possède exactement deux solutions : 1 et -1. D'où exactement $2 \times 2 = 4$ solutions dans $\mathbb{Z}/pq\mathbb{Z}$.

b) Soit $I = \prod_{x \in (\mathbb{Z}/pq\mathbb{Z})^*} x$ le produit de tous les éléments de $(\mathbb{Z}/pq\mathbb{Z})^*$.

En calculant I de deux façons différentes, montrer l'identité

$$\frac{(pq-1)!}{p^{q-1}(q-1)!q^{p-1}(p-1)!} \equiv 1 \mod pq$$

- Par définition, le produit d'un élément x de $(\mathbb{Z}/pq\mathbb{Z})^*$ et de son inverse x^{-1} vaut 1. Dans le produit I, chaque terme x peut être rapproché de son inverse x^{-1} (s'il lui est disctinct bien sûr), si bien que dans I ne subsistent que les x égaux à leur propre inverse, c'est-à-dire les solutions de l'équation $x^2=1$. Par conséquent, $I=\prod_{x^2=1} x$. Pour déterminer ce produit, appliquons α : $\alpha(I)=\prod_{x^2=1} \alpha(x)$. Selon la question précédente, les valeurs prises par $\alpha(x)$ dans ce produit sont $(1,1)$, $(1,-1)$, $(-1,1)$ et $(-1,-1)$. D'où $\alpha(I)=(1,1)(1,-1)(-1,1)(-1,-1)=(1,1)$ et $I=\alpha^{-1}(1,1)=1$.

  Par ailleurs les éléments inversibles de l'anneau $\mathbb{Z}/pq\mathbb{Z}$ correspondent aux entiers 1, 2, $\cdots$, pq qui ne sont pas multiples de p, ni de q. Le produit de ces représentants vaut donc

$$\frac{\prod_{a=1}^{pq-1} a}{(\prod_{a=1}^{q-1} pa)(\prod_{a=1}^{p-1} qa)} = \frac{(pq-1)!}{p^{q-1}(q-1)!\,q^{p-1}(p-1)!}$$

  D'où la congruence de l'énoncé.

c) Comment faut-il corriger cette congruence lorsque $p=2$?

- Si $p=2$, l'équation $x^2=1$ dans $\mathbb{Z}/p\mathbb{Z}$ a pour seule solution $x=2$, si bien que, dans ce cas, $\alpha(I)=(1,1)(1,-1)=(1,-1)=(-1,-1)=\alpha(-1)$. D'où $I=-1$ et la congruence doit être corrigée en remplaçant le membre de droite par -1.

Exercice 3. Soient $r \geqslant 1$ un entier, p un nombre premier et $q=p^r$.

Un élément $x \in \mathbb{F}_q^*$ étant fixé, on considère les deux propriétés suivantes :

i. L'élément x engendre l'extension $\mathbb{F}_q/\mathbb{F}_p$.

ii. L'élément x engendre le groupe $\mathbb{F}_q^*$.

a) Démontrer que l'une des implication est vraie : $\forall x, (\mathrm{i} \Rightarrow \mathrm{ii})$ ou $\forall x, (\mathrm{ii} \Rightarrow \mathrm{i})$.

- Soit $x \in \mathbb{F}_q^*$. Montrons $\mathrm{ii} \Rightarrow \mathrm{i}$. On suppose donc que x engendre $\mathbb{F}_q^*$ et l'on va prouver que tout sous-corps $K \subset \mathbb{F}_q$ contenant x est égal à $\mathbb{F}_q$.

  Puisque K^* est un sous-groupe de $\mathbb{F}_q^*$ qui contient x, selon ii, K contient $\mathbb{F}_q^*$. Comme tout sous-corps de $\mathbb{F}_q$, le corps K contient aussi 0. Par conséquent, K contient $\mathbb{F}_q$.

b) Rappeler quels sont les sous-corps de $\mathbb{F}_q$.

- Les sous-corps de $\mathbb{F}_q$ sont les corps $\mathbb{F}_{p^s}$, où s parcourt les diviseurs de r.

c) On considère dorénavant les cas $q=2^3$, $q=2^6$.

Dénombrer séparément les générateurs du type i et du type ii.

Dans quel cas a-t-on l'équivalence $\forall x, (\mathrm{i} \Leftrightarrow \mathrm{ii})$?

- Soit $q=2^3$. Puisque 3 est premier, le seul sous-corps de $\mathbb{F}_8$ est $\mathbb{F}_2$. Donc $x \in \mathbb{F}_8$ engendre $\mathbb{F}_8$ si et seulement si $x \in \mathbb{F}_8 \smallsetminus \mathbb{F}_2$. D'où $8-2=6$ générateurs du type i. Par ailleurs, $\mathbb{F}_8^*$ est un groupe cyclique à 7 éléments, isomorphe à $\mathbb{Z}/7\mathbb{Z}$, lequel possède $\varphi(7)=6$ générateurs. D'où à nouveau 6 générateurs du type ii. Dans ce cas, on a donc $\forall x$, $(\mathrm{i} \Leftrightarrow \mathrm{ii})$.

  Soit maintenant $q=2^6$. Les diviseurs non triviaux de 6 étant 2 et 3, les sous-corps de $\mathbb{F}_{64}$ sont $\mathbb{F}_2$, $\mathbb{F}_4$ et $\mathbb{F}_8$. Donc $x \in \mathbb{F}_{64}$ engendre $\mathbb{F}_{64}$ si et seulement si $x \in \mathbb{F}_{64} \smallsetminus (\mathbb{F}_2 \cup \mathbb{F}_4 \cup \mathbb{F}_8)$. De plus, d'après la question précédente, $\mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_2$ si bien que $\mathbb{F}_2 \cup \mathbb{F}_4 \cup \mathbb{F}_8$ possède $4+8-2=10$ éléments. D'où $64-10=54$ générateurs du type i. Par ailleurs, $\mathbb{F}_{64}^*$ est un groupe cyclique à 63 éléments, isomorphe à $\mathbb{Z}/63\mathbb{Z}$, lequel possède $\varphi(63)=\varphi(3^2 \times 7)=6 \times 6=36$ générateurs. D'où 36 générateurs du type ii. Dans ce cas, on n'a donc pas l'équivalence $\forall x, (\mathrm{i} \Leftrightarrow \mathrm{ii})$.