Devoir maison 4

Exercice 1 :

Soit $f: E \to F$ une application, où $CardE = CardF$

Montrer que les trois propriétés suivantes sont équivalentes

(i) f est injective

(ii) f est surjective

(iii) f est bijective

Correction

On pose $E = \{e_1, e_2, \dots, e_n\}$ et $F = \{f_1, f_2, \dots, f_n\}$, et bien sur tous les e_j sont distincts ainsi que tous les f_i.

On rappelle que le fait que f soit une application entraine que $\{f(e_1), f(e_2), \dots, f(e_n)\} \subset \{f_1, f_2, \dots, f_n\}$

On suppose que f est injective, on va montrer que f est surjective.

On va montrer la contraposée, c'est-à-dire que l'on va montrer que si f n'est pas surjective alors f n'est pas injective.

Soit $f_i \in F$ et on suppose qu'il n'existe pas de $e_j \in E$ tel que $f_i = f(e_j)$ (f n'est pas surjective)

Donc $\{f(e_1), f(e_2), \dots, f(e_n)\} \subset \{f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_n\}$, il y a n éléments dans le premier ensemble et $n-1$ dans le second, donc il existe j_1 et j_2, avec $j_1 \neq j_2$ dans $\{1,2, \dots, n\}$ tels que $f(e_{j_1}) = f(e_{j_2})$, or $e_{j_1} \neq e_{j_2}$ donc f n'est pas injective.

On suppose que f est surjective et on va montrer que f est injective.

On va montrer la contraposée, c'est-à-dire que l'on va montrer que si f n'est pas injective alors f n'est pas surjective.

Si $f(e_i) = f(e_j) = u$ avec $e_i \neq e_j$ alors

$\{f(e_1), \dots, f(e_{i-1}), u, f(e_{i+1}), \dots, f(e_{j-1}), u, f(e_{j+1}) \dots, f(e_n)\} \subset \{f_1, f_2, \dots, f_n\}$, le premier ensemble a $n-1$ éléments et le second n donc il existe un f_j qui n'a pas d'antécédent, cela montre que f n'est pas surjective.

On a montré que $(i) \Leftrightarrow (ii)$, par définition $(iii) \Rightarrow (i)$ et $(iii) \Rightarrow (ii)$. Si on a (i) alors on a (ii) et $(i)\ et\ (ii)$ entraine (iii) de même si on a (ii) alors on a (i) et $(i)\ et\ (ii)$ entraine (iii). Ce qui achève de montrer les trois équivalences.

Exercice 2 :

On considère l'application $f: \mathbb{N} \to \mathbb{N}$ définie pour tout $n \in \mathbb{N}$ par $f(n) = n^2$

1°) Existe-t-il $g: \mathbb{N} \to \mathbb{N}$ telle que : $f \circ g = Id_{\mathbb{N}}$?

2°) Existe-t-il $h: \mathbb{N} \to \mathbb{N}$ telle que : $h \circ f = Id_{\mathbb{N}}$?

Correction

1°) supposons que g existe, $f \circ g = Id_{\mathbb{N}} \Leftrightarrow \forall n \in \mathbb{N}, f(g(n)) = n \Leftrightarrow \forall n \in \mathbb{N}, (g(n))^2 = n$

Si n n'est pas un carré cela ne marche pas, par exemple si $n = 2$, $(g(2))^2 = 2$ donc $g(2) = \pm\sqrt{2} \notin \mathbb{N}$

Il n'existe pas de fonction $g: \mathbb{N} \to \mathbb{N}$ telle que : $f \circ g = Id_{\mathbb{N}}$.

2°) supposons que h existe, $h \circ f = Id_{\mathbb{N}} \Leftrightarrow \forall n \in \mathbb{N}, h(f(n)) = n \Leftrightarrow \forall n \in \mathbb{N}, h(n^2) = n$

Les valeurs $h(p)$ prennent les valeurs qu'elles veulent sauf lorsque p est un carré auquel cas $h(p) = \sqrt{p}$, donnons une fonction h qui répond à la question :

Si $p \neq n^2$ alors $h(p) = 0$ et si $p = n^2$ alors $h(p) = \sqrt{p} = n$.

Exercice 3 :

On considère un entier $n \geq 3$.

1°) Montrer que, quelque soit l'entier x, les carrés des nombres x et $n - x$ sont congrus modulos n.

2°) On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble $\{0,1, \dots, n-1\}$ des restes modulo n, et c l'application de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ qui a un reste associe son carré. Cette application est-elle injective ? surjective ?

3°) Dresser la table des carrés modulo 7.

4°) Montrer que l'équation $x^2 - 6xy + 2y^2 = 7003$ n'a pas de solutions (x, y) entière. (Exprimer le premier membre comme un carré modulo 7)

Correction

1°) $(n-x)^2 = n^2 - 2nx + x^2 \equiv x^2 \ \ [n]$

2°) Précisons un peu $\mathbb{Z}/n\mathbb{Z}$, si $m \in \mathbb{Z}$ d'après la division euclidienne, il existe un unique couple $(b, r) \in \mathbb{Z} \times \{0,1, \dots, n-1\}$ tel que $m = bn + r$, r est un reste donc un élément de $\mathbb{Z}/n\mathbb{Z}$.

Soit $r \in \{0,1, \dots, n-1\}$, $c(r)$ est le reste de la division de r^2 par n, donc $r^2 = bn + c(r)$ ce qui équivaut à $r^2 \equiv c(r) \ \ [n]$ et $c(r) \in \{0,1, \dots, n-1\}$.

Comme $c(1) \equiv 1^2 \ \ [n] \equiv 1 \ \ [n]$, on a $c(n-1) \equiv (n-1)^2 \ \ [n] \equiv 1^2 \ \ [n] \equiv c(1) \ [n]$

Puisque $c(n-1) \in \{0,1, \dots, n-1\}$ et $c(1) \in \{0,1, \dots, n-1\}$ et que $c(n-1) \equiv c(1) \ [n]$, on a

$$c(1) = c(n-1)$$

Et pourtant $1 \neq n-1$, sauf si $n = 2$, mais $n \geq 3$.

Donc c n'est pas injective.

On utilise l'exercice 1, c n'est pas surjective. Sinon on refait une démonstration semblable.

3°)

n	0	1	2	3	4	5	6
n^2	0	1	4	$9 \equiv 2 \ \ [7]$	$16 \equiv 2 \ \ [7]$	$25 \equiv 4 \ \ [7]$	$36 \equiv 1 \ \ [7]$

4°)

$$x^2 - 6xy + 2y^2 = (x-3y)^2 - 9y^2 + 2y^2 = (x-3y)^2 + 7y^2 \equiv (x-3y)^2 \ \ (7]$$

Et $7003 \equiv 3 \ \ [7]$, d'après le 3°) il n'y a pas de carré qui soit congru à 3 modulo 7 donc il n'y a pas de solution.