

Corrigé du devoir n° 1

Exercice 1.

1. Si f est une injection de E dans \mathbb{N} , alors E est en bijection avec son image $f(E)$, et l'on est ramené à montrer qu'une partie de \mathbb{N} est finie ou dénombrable. Soit donc A une partie infinie de \mathbb{N} . On définit récursivement une suite $(a_n)_{n \in \mathbb{N}} \subset A$ en posant $a_0 := \min A$ (toute partie non vide de \mathbb{N} admet un plus petit élément...), puis, pour $n \geq 1$, $a_n = \min A \setminus \{a_0, \dots, a_{n-1}\}$ (noter que $A \setminus \{a_0, \dots, a_{n-1}\}$ est *non vide* pour tout $n \geq 1$ puisque A est infinie). On vérifie alors facilement que l'application $n \mapsto a_n$ est une bijection de \mathbb{N} sur A .
2. Soit g une surjection de \mathbb{N} sur E . On définit une application f de E dans \mathbb{N} de la façon suivante : à $x \in E$ on associe $f(x) := \min \{n \in \mathbb{N}, | g(n) = x\}$. L'ensemble image $f(E)$ est alors un système de représentants des classes d'équivalence dans \mathbb{N} modulo la relation \sim_g et f est à l'évidence une injection de E dans \mathbb{N} . On peut donc conclure grâce à la question précédente.

Exercice 2. *Le problème des scores.*

1. Puisque a et b sont premiers entre eux, il existe deux entiers u et v tels que $au + bv = 1$. Si c est un entier quelconque, le couple $(x, y) = (uc, vc)$ est alors solution de l'équation $ax + by = c$.
2. Si $ax + by = c$, alors pour tout $k \in \mathbb{Z}$ on a $a(x + kb) + b(y - ka) = ax + by = c$. Soit q le quotient de la division euclidienne de y par a . Alors $y - qa = r$ est le reste de cette division, de sorte que l'on a $0 \leq r \leq a - 1$. Ainsi, le couple $(x', y') = (x + qb, y - qa)$ est une solution de l'équation initiale vérifiant $0 \leq y' \leq a - 1$.
3. Soit (x, y) une solution de l'équation $ax + by = c$ vérifiant $0 \leq y \leq a - 1$ (un tel couple existe d'après la question précédente). On a alors $ax = c - by > ab - a - b - b(a - 1) = -a$, d'où $x > -1$. Or x est un entier (relatif), donc la dernière inégalité équivaut à $x \geq 0$. On a donc bien trouvé un couple (x, y) d'entiers positifs ou nuls solution de l'équation $ax + by = c$.
4. Supposons qu'il existe $(x, y) \in \mathbb{N}^2$ tel que $ax + by = ab - a - b$. En particulier $ax = a(b - 1) - b < a(b - 1)$, donc $x < b - 1$, soit

$$1 \leq x + 1 < b. \tag{1}$$

Par ailleurs, $ax + by = ab - a - b \Leftrightarrow a(x + 1) = b(a - 1 - y)$, ce qui impose, puisque a et b sont premiers entre eux, que b divise $x + 1$. Ceci est incompatible avec (1), d'où la conclusion.

5. En appliquant ce qui précède, on voit que tout score supérieur strictement à $7 = 3 \cdot 5 - 3 - 5$ est réalisable avec des pénalités (3 points) et des essais non transformés (5 points). Ensuite, 7 est réalisable avec un essai transformé, 6 avec deux pénalités, 3 avec une et 5 avec un essai non transformé. Les seuls scores non réalisables sont donc 1, 2 et 4.

Exercice 3. *Test de Lucas - Nombres de Fermat*

1. (a) Si n est premier, un générateur α du groupe (cyclique) $(\mathbb{Z}/n\mathbb{Z})^\times$ est un élément d'ordre exactement $n - 1$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ et satisfait donc trivialement le test de Lucas.
 (b) Inversement, soit $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$ satisfaisant le test de Lucas et soit m son ordre dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Puisque $\alpha^{n-1} \equiv 1 \pmod n$, on peut affirmer que m divise $n - 1$. Si m était un diviseur strict de $n - 1$, il existerait un premier p tel que m divise $\frac{n-1}{p}$. On aurait alors $\alpha^{\frac{n-1}{p}} \equiv 1 \pmod n$, en contradiction avec la deuxième partie du test de Lucas. Ainsi, α est d'ordre $n - 1$, ce qui implique que $(\mathbb{Z}/n\mathbb{Z})^\times$ contient au moins $n - 1$ éléments. Comme $|(\mathbb{Z}/n\mathbb{Z})^\times| \leq n - 1$, on conclut que tous les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles, ce qui est une façon de caractériser le fait que n est premier.

2. Si a est impair, alors a^n l'est également (quel que soit $n \in \mathbb{N}$) et $a^n + 1$ est pair, donc non premier, sauf si $a^n = 1$, ce qui est incompatible avec la condition $a \geq 2$. Posons alors $n = 2^l m$ avec m impair, et montrons que $m = 1$. Pour cela, remarquons que $a^n + 1 = (a^{2^l})^m - (-1)^m$ puisque m est impair, et donc

$$a^n + 1 = (a^{2^l})^m - (-1)^m = (a^{2^l} + 1) \left((a^{2^l})^{m-1} + \dots + 1 \right)$$

ce qui fournit une factorisation non triviale, sauf si $m = 1$.

3. (a) Si $n > m$, alors on peut écrire $F_n = 2^{2^n} + 1 = (2^{2^m})^{2^{n-m}} + 1$. on en déduit, en appliquant l'identité $b^{2^{n-m}} + 1 = (b + 1) (b^{2^{n-m}-1} - b^{2^{n-m}-2} + \dots + b - 1) + 2$ à $b = 2^{2^m}$, que le reste de la division euclidienne de F_n par F_m vaut 2, donc $F_n \wedge F_m = F_m \wedge 2 = 1$.

Remarque : on peut aussi s'appuyer sur la relation $F_n = \prod_{i=0}^{n-1} F_i + 2$, qui s'établit facilement par récurrence.

- (b) S'il existe $k \in \mathbb{Z}$ tel que $k^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$, alors $k^{F_n-1} = \left(k^{\frac{F_n-1}{2}}\right)^2 \equiv 1 \pmod{F_n}$. Par ailleurs, le seul diviseur premier de $F_n - 1 = 2^{2^n}$ est 2. On voit donc que le test de Lucas est satisfait (avec $\alpha = k$), et donc F_n est premier. Inversement, si F_n est premier, alors $(\mathbb{Z}/F_n\mathbb{Z})^\times$ est cyclique d'ordre $F_n - 1 = 2^{2^n}$, et si k en est un générateur, on a $\left(k^{\frac{F_n-1}{2}}\right)^2 = k^{F_n-1} \equiv 1 \pmod{F_n}$ et donc $k^{\frac{F_n-1}{2}}$ est la seule racine carrée non triviale de 1 dans le corps $\mathbb{Z}/F_n\mathbb{Z}$, c'est-à-dire -1 .