

Devoir n° 1

À rendre pour la semaine du 20 octobre

Exercice 1. On rappelle qu'un ensemble E est dénombrable s'il est en bijection avec \mathbb{N} .

1. Montrer que s'il existe une *injection* $f : E \longrightarrow \mathbb{N}$ alors E est fini ou dénombrable.
2. Montrer que s'il existe une *surjection* $g : \mathbb{N} \longrightarrow E$ alors E est fini ou dénombrable (on pourra par exemple considérer le quotient \mathbb{N}/\sim_g de \mathbb{N} par la relation d'équivalence $n \sim_g m$ si $g(n) = g(m)$ et se ramener à la question précédente).

Exercice 2. *Le problème des scores.* Soient a et b deux entiers naturels non nuls et premiers entre eux. Pour tout entier relatif c fixé, on considère l'équation

$$ax + by = c, \quad (x, y) \in \mathbb{Z}^2 \quad (1)$$

1. Montrer que quel que soit l'entier c , l'équation (1) admet des solutions dans \mathbb{Z}^2 .
2. Montrer que si le couple (x, y) est solution de (1), alors pour tout $k \in \mathbb{Z}$, le couple $(x + kb, y - ka)$ est également solution. En déduire que pour tout entier c , l'équation (1) admet une solution $(x, y) \in \mathbb{Z}^2$ avec $0 \leq y \leq a - 1$.
3. En déduire que si $c > ab - a - b$, il existe (au moins) un couple (x, y) d'entiers *positifs ou nuls* solution de l'équation (1).
4. Montrer enfin que si $c = ab - a - b$, l'équation (1) n'a pas de solution avec x et y entiers naturels.
5. Application : quels sont les scores réalisables au rugby ? On rappelle qu'une pénalité ou un drop rapportent 3 points, un essai 5 et un essai transformé 7.

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

1. On rappelle que si p est un nombre premier, le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ des éléments inversibles modulo p est cyclique d'ordre $p - 1$ (la démonstration de ce résultat classique sera rappelée en TD). On se propose de montrer dans cette question qu'un entier n est premier si et seulement si il existe $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que

- $\alpha^{n-1} \equiv 1 \pmod{n}$
- $\alpha^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$ pour tout diviseur premier p de $n - 1$.

Ce critère est souvent appelé *test de Lucas* dans la littérature.

- (a) Montrer que si n est premier, tout générateur α du groupe (cyclique) $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$ convient.
 - (b) Inversement, montrer qu'un élément α satisfaisant les conditions ci-dessus est nécessairement d'ordre $n - 1$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ et conclure.
2. Soit a un entier ≥ 2 , et n un entier ≥ 1 . Montrer que si $a^n + 1$ est premier, alors a est pair et n est une puissance de 2.
 3. On définit pour $n \in \mathbb{N}$ le nombre $F_n = 2^{2^n} + 1$ ("n^{ième} nombre de Fermat").
 - (a) Montrer que si $n \neq m$, F_n et F_m sont premiers entre eux.
 - (b) En utilisant le test de Lucas, montrer que F_n est premier si et seulement si il existe $k \in \mathbb{Z}$ tel que $k^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.