Université de la Réunion. 1re année de licence de mathématiques. Année universitaire 2023/2024.

Contrôle terminal d'arithmétique et de cryptographie

Lundi 13 mai 2024

Durée : 2 heures

La consultation de documents est interdite.
L'utilisation d'appareils électroniques est interdite.
Les questions de cours doivent être rendues dès la première sortie de la salle d'examen.

Question de cours 1. Énoncer le théorème de division euclidienne.

Question de cours 2. Soit $n \in \mathbb{Z}$. Justifier que n et $n+1$ sont premiers entre eux.

Question de cours 3. Énoncer le théorème de Bézout.

Question de cours 4. Énoncer le lemme de Gauss.

Exercice 1. Soient $a, b \in \mathbb{N}$. On suppose $a \neq 0$. On suppose que $\mathbb{Z}a \subset \mathbb{Z}b$. Montrer que $b \leqslant a$.

Exercice 2. Soit $n \in \mathbb{N}$. On suppose n pair. Montrer que $45 \mid 7^n - 2^n$.

Exercice 3. Soit $n \in \mathbb{Z}$. Montrer que $9n+8$ et $6n+5$ sont premiers entre eux.

Exercice 4.

A] Soit $n \in \mathbb{Z}$. On suppose n pair.
   1) Justifier que n et 2 ne sont pas premiers entre eux.
   2) Justifier que n et $n+2$ ne sont pas premiers entre eux.

B] Soit $n \in \mathbb{Z}$. On suppose n impair.
   1) Justifier que n et 2 sont premiers entre eux.
   2) Montrer que n et $n+2$ sont premiers entre eux.

C] Soit $a \in \mathbb{Z}$. On suppose que $2023 \mid a$, $2024 \mid a$ et $2025 \mid a$.
   Montrer que $(2023 \times 2024 \times 2025) \mid a$.

Exercice 5. Les deux questions peuvent se traiter indépendamment l'une de l'autre.

1) Soient A, B et C des parties de $\mathbb{Z}$. On suppose $A \subset B$.
   Vérifier que $A + C \subset B + C$.
2) Soient F, G et H des parties de $\mathbb{Z}$.
   Montrer que $(F \cap G) + H \subset (F + H) \cap (G + H)$.

Exercice 6. On définit $f\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ par $\forall (x, y) \in \mathbb{Z} \times \mathbb{Z}\ f(x, y) = 4x + 9y$.

1) Justifier que f est surjective.
2) Justifier que f n'est pas injective.