Université de la Réunion. 1re année de licence de mathématiques. Année universitaire 2022/2023.

Contrôle terminal d'arithmétique et de cryptographie

Mercredi 17 mai 2023

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. Compléter l'énoncé se trouvant ci-dessous.
Proposition. Soient $a, b \in \mathbb{Z}$.
Alors les assertions suivantes sont équivalentes : i) $a \mid b$ et $b \mid a$, ii) $\cdots\cdots$.

Question de cours 2. Compléter l'énoncé se trouvant ci-dessous, puis démontrer le.
Proposition. Soient $a, b \in \mathbb{Z}$.
Alors les assertions suivantes sont équivalentes : i) $\mathbb{Z}b \subset \mathbb{Z}a$, ii) $\cdots\cdots$.

Question de cours 3. Citer la proposition appelée « Lemme d'Euclide ».

Question de cours 4. Citer le théorème d'existence d'une décomposition en produit de nombres premiers.

Exercice 1. Soit $n \in \mathbb{N}$. Montrer que $17 \mid 25^n + 2^{3n+4}$.

Exercice 2.

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

Exercice 3. Soit $n \in \mathbb{Z}$.

1) Justifier que $2 \mid n(n+1)$.
2) Montrer que $3 \mid n(n+1)(2n+1)$.
3) En déduire que $6 \mid n(n+1)(2n+1)$.

Exercice 4. Soient $a, b, c, d \in \mathbb{N}$. On suppose $ab = cd$.
On suppose que a et d sont premiers entre eux. On suppose que b et c sont premiers entre eux.
Montrer que $a = c$ et $b = d$.

Exercice 5. Soit $a \in \mathbb{Z}$. On suppose que $\forall p \in \mathcal{P}\ p \mid a$. Que peut-on dire de a ? Justifier.

Exercice 6.

1) Citer le théorème décrivant les sous-groupes de $\mathbb{Z}$.
2) Soient $a, b \in \mathbb{Z}$. On suppose $a \neq 0$ et $b \neq 0$. Montrer que les assertions suivantes sont équivalentes : i) a et b sont premiers entre eux, ii) $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}(ab)$.