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

Contrôle continu d'arithmétique et de cryptographie

Mercredi 10 avril 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. Compléter, sans justification, les deux énoncés se trouvant ci-dessous.

a) Proposition. Soient $a, b \in \mathbb{N}$. On suppose que $a \mid b$. On suppose $b \neq 0$.
Alors ....

b) Corollaire. Soient $a, b \in \mathbb{N}$. On suppose que $a \mid b$ et $b \mid a$.
Alors ....

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) ....

Question de cours 3. Compléter, sans justification, l'énoncé se trouvant ci-dessous.
Proposition. Soit $a \in \mathbb{Z}$. On suppose $a \neq 0$.
Soit $b \in \mathbb{Z}$. Notons r le reste dans la division euclidienne de b par a.
Soit $b' \in \mathbb{Z}$. Notons r' le reste dans la division euclidienne de b' par a.
Alors les assertions suivantes sont équivalentes :

i) ... ;
ii) ....

Exercice 1. Soit $n \in \mathbb{N}$. Montrer que $17 \mid 2^{6n+3} + 3^{4n+2}$.

Exercice 2. Soient $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$.
On note q le quotient dans la division euclidienne de $b - 1$ par a. Soit $n \in \mathbb{N}$.
Que vaut le quotient dans la division euclidienne de $ba^n - 1$ par a^{n+1} ?

Exercice 3. Montrer que $\forall n \in \mathbb{N}^*$ $21 \mid 2^{4^n} + 5$.

Exercice 4. Soit $a \in \mathbb{Z}$. On suppose $a \neq 0$.
On définit $\varphi \colon \mathbb{Z} \times [\![0, |a| - 1]\!] \to \mathbb{Z}$ par $\forall (q, r) \in \mathbb{Z} \times [\![0, |a| - 1]\!]$ $\varphi(q, r) = qa + r$.
Que peut-on dire de φ ? Justifier.

Exercice 5. On note $S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x^2 - y^2 - 4x - 2y = -2\}$.
Écrire S en extension, en justifiant.