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

Contrôle continu d'arithmétique et de cryptographie

Vendredi 14 avril 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.
Énoncer le théorème de division euclidienne.

Question de cours 2.
Soient $m, n \in \mathbb{Z}$. Citer une condition nécessaire et suffisante pour que $m + n$ soit pair.

Question de cours 3.
Soient A et B des parties de Z.

1) Dire ce que signifie la notation $A + B$.
2) On suppose $0 \in A$. Dire (sans justifier) ce que l'on peut en déduire concernant $A + B$.

Exercice 1. Soit $m \in \mathbb{Z}$. Montrer que $m^2 + m$ est pair.

Exercice 2. Soit $a \in \mathbb{Z}$. Montrer que $\forall n \in \mathbb{N}\ a^2 \mid (a+1)^n - an - 1$.

Exercice 3. Les questions sont deux à deux indépendantes.

1) Soient $a, b \in \mathbb{Z}$.
   Vérifier que $\mathrm{Div}(a) \cap \mathrm{Div}(b) \subset \mathrm{Div}(a + b)$.
2) Trouver $a, b \in \mathbb{Z} \setminus \{0\}$ tels que $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(a + b)$. Justifier.
3) Soient $a, b \in \mathbb{N}$.
   Montrer que les assertions suivantes sont équivalentes :
   i) $a = 0$ ou $b = 0$;
   ii) $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(a + b)$.

Exercice 4. Soient $k, \ell \in \mathbb{N}$. Montrer que $13 \mid 3^{3k} + 5^{4\ell+2}$.

Exercice 5. Soit $a \in \mathbb{Z}$. On suppose $a \neq 0$.
Quels sont le reste et le quotient dans la division euclidienne de $a^2 - 1$ par a ? Justifier.
(On pourra distinguer deux cas : $a \geqslant 1$ et $a \leqslant -1$.)

Exercice 6. Soient $\ell, m, n \in \mathbb{N}$. On suppose que $\ell \leqslant m \leqslant n$.
Montrer que les assertions suivantes sont équivalentes :

i) $\ell \mid m + n$ et $m \mid n + \ell$ et $n \mid m + \ell$;
ii) $\big(m = \ell$ et $n = \ell\big)$ ou $\big(m = \ell$ et $n = 2\ell\big)$ ou $\big(m = 2\ell$ et $n = 3\ell\big)$.