Université de la Réunion. 1re année de licence de mathématiques. Année universitaire 2021/2022.

**Contrôle terminal d'arithmétique et de cryptographie**

Mardi 10 mai 2022

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.**
Soient $m, n \in \mathbb{Z}$. Citer une condition nécessaire et suffisante pour que $mn$ soit impair.

**Question de cours 2.**
Énoncer le lemme de Gauss.

**Exercice 1.**

1) Soit $k \in \mathbb{N}$. Montrer que $8 \mid 5^{2k+1} + 2.3^{2k} + 1$.
2) Soit $k \in \mathbb{N}$. Montrer que $8 \mid 5^{2k+2} + 2.3^{2k+1} + 1$.
3) Soit $n \in \mathbb{N}$. Montrer que $8 \mid 5^{n+1} + 2.3^{n} + 1$.

**Exercice 2.**
Soient $u, v \in \mathbb{Z}$. Montrer que les assertions suivantes sont équivalentes :

i) $u$ et $v$ sont premiers entre eux ;
ii) il existe $\alpha \in \mathbb{Z}$ tel que $\alpha u \equiv 1\ [v]$.

**Exercice 3.**
Soient $a, b, c, d \in \mathbb{Z}$. On suppose que $ad - bc = 1$. Soient $\alpha, \beta \in \mathbb{Z}$.

1) Montrer que $\mathrm{Div}(\alpha a + \beta b) \cap \mathrm{Div}(\alpha c + \beta d) = \mathrm{Div}(\alpha) \cap \mathrm{Div}(\beta)$.
2) Quelle équivalence peut-on déduire de la question 1) ?

**Exercice 4.**
Soient $p$ et $q$ des nombres premiers. On suppose $p \neq q$.

A] Soit $x \in \mathbb{N}$. On suppose que $x \mid pq$.
   1) On suppose que $p \nmid x$.
      a) Justifier que $x \mid q$.
      b) Que peut-on en déduire pour $x$ ?
   2) On suppose que $p \mid x$.
      On note $k$ le quotient de $x$ par $p$.
      a) Montrer que $k = 1$ ou $k = q$.
      b) Que peut-on dire en déduire pour $x$ ?

B] Écrire $\mathrm{Div}_+(pq)$ en extension.

**Exercice 5.**
Soit $a \in \mathbb{Z}$. Que vaut $\mathbb{Z}a + \mathbb{N}$ ?