Université Aix-Marseille 2021–2022

Licence – Mathématiques
Algèbre 2

Partiel
Correction

Exercice 1.

1. - Pour tout $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$ on appelle division euclidienne de a par b les uniques entiers $q \in \mathbb{Z}$ et $r \in [\![0, |b| - 1]\!]$ tels que $a = qb + r$.
   - On dit qu'un entier $n \in \mathbb{N}^*$ est premier s'il possède exactement quatre diviseurs.
   - Un groupe est un ensemble G munie d'opération $* : G \times G \to G$ telle que :
     - pour tous $a, b, c \in G$, $(a * b) * c = a * (b * c)$;
     - il existe $e \in G$ tel que pour tout $a \in G$, $e * a = a * e = a$;
     - pour tout $a \in G$, il existe $b \in G$ tel que $a * b = b * a = e$, où e est l'élément du point précédent.
2. Enoncé du lemme de Gauss : Soit $a, b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$ tels que a divise bc et a et b soient premiers entre eux, alors a divise c.

   Démonstration du lemme de Gauss : Puisque que a et b sont premiers entre eux, d'après le théorème de Bachet–Bézout, il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$. On a alors $uac + vbc = c$. Or a divise clairement uac, ainsi que vbc par hypothèse, il divise donc leur somme, laquelle est égale à c.

Exercice 2. Etre divisible par 7, cela revient à être égal à $\overline{0}$ dans $\mathbb{Z}/7\mathbb{Z}$. Or

$$\begin{aligned}
\overline{5^{n+2} + 3^{n+1}5^{2n}} &= \overline{25}.\overline{5}^n + \overline{3}.\overline{3}^n.\overline{25}^n \\
&= \overline{4}.\overline{5}^n + \overline{3}.\overline{3}^n.\overline{4}^n \\
&= \overline{4}.\overline{5}^n + \overline{3}.\overline{12}^n \\
&= \overline{4}.\overline{5}^n + \overline{3}.\overline{5}^n \\
&= (\overline{4} + \overline{3}).\overline{5}^n \\
&= \overline{0}.\overline{5}^n = \overline{0}.
\end{aligned}$$

Exercice 3.

1. Utilisons l'algorithme d'Euclide. Les divisions euclidiennes successives donnent :
   - $10001 = 5053 + 4948$;
   - $5053 = 4948 + 105$;
   - $4948 = 47.105 + 13$;
   - $105 = 8.13 + 1$.

   On en déduit que 10001 et 5053 sont premiers entre eux.
2. En remontant les calculs précédents, on trouve :

$$\begin{aligned}
1 &= 105 - 8.13 = 105 - 8(4948 - 47.105) \\
&= 377.105 - 8.4948 = 377.(5053 - 4948) - 8.4948 \\
&= 377.5053 - 385.4948 = 377.5053 - 385(10001 - 5053) \\
&= 762.5053 - 385.10001.
\end{aligned}$$

3. En considérant la relation de Bézout de la question précédente modulo 10001, on trouve

$$\overline{762}.\overline{5053} = \overline{1} + \overline{385}.\overline{10001} = \overline{1}.$$

   On en déduit que $\overline{762}$ est un inverse pour $\overline{5053}$ dans $\mathbb{Z}/10001\mathbb{Z}$.

4. Le problème revient à trouver $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ tels que

$$\begin{cases} \overline{53}.\overline{x} + \overline{y} = -\overline{2} \\ \overline{5000}.\overline{x} + \overline{10000}.\overline{y} = \overline{3} \end{cases}$$

dans $\mathbb{Z}/10001\mathbb{Z}$. En remplaçant la seconde ligne par la somme des deux, ce problème est équivalent à

$$\begin{cases} \overline{53}.\overline{x} + \overline{y} = -\overline{2} \\ \overline{5053}.\overline{x} + \overline{10001}.\overline{y} = \overline{1} \end{cases}$$

et donc à

$$\begin{cases} \overline{53}.\overline{x} + \overline{y} = -\overline{2} \\ \overline{5053}.\overline{x} = \overline{1} \end{cases}.$$

Dans la queston précédente, nous avons vu que $x = 762$ satisfait la seconde ligne. La première ligne devient alors

$$\overline{y} = -\overline{2} - \overline{53}.\overline{762} = -\overline{40388} = -\overline{384}.$$

Une solution possible est donc $x = 762$ et $y = -384$.

Exercice 4.

1. (a) L'entier 4 possède 1 et 2 comme diviseurs propres, mais n'est pas parfait car $1 + 2 \neq 3$.
   (b) L'entier 6 est parfait car ses diviseurs propres sont 1, 2 et 3 et $1 + 2 + 3 = 6$.
2. (a) Supposons que $n = ab$ avec $a, b \in \mathbb{N}^*$. Par identité remarquable, on a alors $2^n - 1 = (2^a)^b - 1^b = (2^a - 1)\sum_{k=0}^{b-1} 2^{ak}$ et $2^a - 1$ divise donc $2^n - 1$. Mais par primalité de $2^n - 1$, on a alors $2^a - 1 = 1$ ou $2^a - 1 = 2^n - 1$. Dans le premier cas, $a = 1$, et dans le second $a = n$. On en déduit que les seuls diviseurs positifs de n sont 1 et n, et donc que n est premier.
   (b) Soit d un diviseur de N_p. Puisque $2^p - 1$ est premir, si d n'est pas un multiple de $2^n - 1$, alors il est premier avec lui et d divise 2^{n-1} par le lemme de Gauss. Il est donc de la forme 2^k avec $0 \leq k \leq n - 1$. Si d est un multiple de $2^n - 1$, alors $d = (2^n - 1)r$ avec $r \in \mathbb{N}^*$, et r divise alors $\frac{2^{n-1}(2^n-1)}{2^n-1} = 2^{n-1}$; on a alors $r = 2^k$ avec $0 \leq k \leq n - 1$. Au final, les diviseurs de P_n sont

$$1, 2, 4, \ldots, 2^{n-1}, (2^n - 1), 2(2^n - 1), 4(2^n - 1), \ldots, 2^{n-1}(2^n - 1).$$

   (c) Les diviseurs propres de P_n sont tous les éléments de la liste ci-dessus sauf $2^{n-1}(2^p - 1)$, or leur somme vaut

$$\begin{aligned} \left(\sum_{k=0}^{n-1} 2^k\right) + \left(\sum_{k=0}^{n-2} (2^n - 1)2^k\right) &= \frac{2^n - 1}{2 - 1} + \left((2^n - 1)\sum_{k=0}^{n-2} 2^k\right) \\ &= 2^n - 1 + (2^n - 1)\frac{2^{n-1} - 1}{2 - 1} \\ &= (2^n - 1)(1 + 2^{n-1} - 1) \;=\; P_n. \end{aligned}$$

   L'entier P_n est donc parfait.