Université Paris Saclay **MDD 102**
L1S1 **Algèbre**

Feuille d'exercices 4. Corrigé

Arithmétique

Exercice 4.1. Algorithme d'Euclide
Pour les entiers a et b suivants, calculer pgcd(a, b) et trouver $u, v \in \mathbb{Z}$ tels que $au + bv = pgcd(a, b)$.
1. $a = 13$ et $b = 17$

2. $a = 32$ et $b = 27$

3. $a = 98$ et $b = 18$

4. pour un entier $n \geq 1$ quelconque, $a = n + 1$ et $b = n$

Exercice 4.2. Division euclidienne
1. Calculer pgcd$(1995, 2975)$.

2. Soit un entier $n \geq 1$ tel que le reste de le division euclidienne de 2003 par n est 8 et le reste de la division euclidienne de 3002 par n est 27. En utilisant la question précédente, trouver la valeur de n.

Exercice 4.3. Identité de Bézout
Au rugby, on peut marquer 3 points (drop/pénalité), 5 points (essai non transformé) ou 7 points (essai transformé). On se demande quels sont les scores qu'il est possible d'atteindre.
1. On ne regarde pour l'instant que les scores qu'on peut obtenir avec 3 et 5 points.

a. Donner les scores ≤ 9 qu'on peut atteindre.
b. Écrire deux relations $3u + 5v = 1$ avec u et v entiers, l'une avec $u > 0$ et l'autre avec $u < 0$.
c. Montrer par récurrence que tous les scores ≥ 9 peuvent être atteints.
2. On autorise maintenant 3, 5 et 7 points. Quels sont les scores qu'on peut atteindre ?

Réponse : 1.a. On peut atteindre $3, 5, 6 = 3 + 3, 8 = 5 + 3, 9 = 3 \times 3$.
1.b. À partir d'une identité de Bézout, obtenue par exemple avec l'algorithme d'Euclide, on peut en trouver une autre en ajoutant et en soustrayant 3×5. Par exemple, $1 = 3 \times 2 + 5 \times (-1)$ et $1 = 3 \times (-3) + 5 \times 2$.
1.c. On montre par récurrence sur $n \geq 9$ que le score n peut être atteint. Initialisation : le cas $n = 9$ a été vu en 1.a. Hérédité : si on peut atteindre n pour un certain $n \geq 9$, il existe a et b dans $\mathbb{N}$ tels que $n = 3a + 5b$. On doit montrer qu'on peut atteindre $n + 1$, c'est-à-dire trouver a' et b' dans $\mathbb{N}$ tels que $n + 1 = 3a' + 5b'$. Pour cela, on va ajouter 1 sous une des formes de la question 1.b :

$$n + 1 = 3(a + 2) + 5(b - 1) \text{ et } n + 1 = 3(a - 3) + 5(b + 2).$$

On voudrait qu'au moins une de ces écritures ait ses deux coefficients dans $\mathbb{N}$; c'est toujours le cas sauf si on a à la fois $b < 1$ et $a < 3$. Mais dans ce cas, $a \leq 2$ et $b = 0$ donc $n = 3a + 5b \leq 6$, contradiction. Donc soit $a \geq 3$, et $n + 1 = 3(a - 3) + 5(b + 2)$ convient, soit $b \geq 1$ et $n + 1 = 3(a + 2) + 5(b - 1)$ convient. Donc la propriété est vrai au rang $n + 1$, et donc pour tout $n \geq 9$ par

récurrence.
2. On ajoute simplement 7 par rapport à la liste précédente.

Exercice 4.4. Pgcd, ppcm
Pour les entiers a et b suivants, donner la décomposition en facteurs premiers de a et b et en déduire $pgcd(a,b)$ et $ppcm(a,b)$.

1. $a = 66$ et $b = 21$

2. $a = 54$ et $b = 12$

3. $a = 70$ et $b = 91$

Exercice 4.5. Nombres premiers
On veut montrer qu'il existe une infinité de nombres premiers. On suppose par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers, que l'on dénote par $p_1, \ldots, p_n$. On note $q = p_1 \ldots p_n + 1$.

1. Montrer que q n'est divisible par aucun des nombres premiers $p_1, \ldots, p_n$.

2. Conclure.

Réponse : 1. Si q est divisible par un nombre premier p_i, puisque le produit $p_1 \ldots p_n$ est lui aussi clairement divisible par p_i, on obtient en faisant la différence que 1 est divisible par p_i, ce qui est absurde.
2. Par le théorème fondamental, on peut décomposer q en un produit de nombres premiers, donc q est au moins divisible par un nombre premier, mais les seuls possibles sont $p_1, \ldots, p_n$ par hypothèse. Cela contredit la question précédente. Donc l'hypothèse que $p_1, \ldots, p_n$ sont les seuls nombres premiers est fausse, et donc il existe une infinité de nombres premiers.

Exercice 4.6. Diviseurs premiers
Soit un entier $n \geq 2$. On suppose que n n'est pas premier.

1. Montrer qu'il existe un entier m tel que $2 \leq m \leq \sqrt{n}$ et qui divise n.

2. Montrer qu'il existe un nombre premier p tel que $2 \leq p \leq \sqrt{n}$ et qui divise n.

3. Application : comment vérifie-t-on si un entier $n \leq 100$ est premier ?

Exercice 4.7. Compter les nombres premiers
Le but de l'exercice est de compter les nombres premiers compris entre 1 et 48. Pour tout entier $d \geq 1$, on notera dans la suite

$$A_d = \{n \in \mathbb{N}; 1 \leq n \leq 48 \text{ et } d|n\}$$

On pourra utiliser la formule suivante, vue au TD 2 : si X, Y, Z sont des ensembles finis, alors

$$\text{card}(X \cup Y \cup Z) = \text{card}(X) + \text{card}(Y) + \text{card}(Z) - \text{card}(X \cap Y) - \text{card}(X \cap Z) - \text{card}(Y \cap Z) + \text{card}(X \cap Y \cap Z)$$

1. Soit $2 \leq n \leq 48$. Montrer que si n n'est pas premier, alors n est divisible par 2 ou par 3 ou par 5.

2. Calculer le cardinal de A_d.

3. Montrer que $A_2 \cap A_3 = A_6$.

4. Trouver des formules semblables pour $A_2 \cap A_5$, $A_3 \cap A_5$ et $A_2 \cap A_3 \cap A_5$.

5. Déduire des questions précédentes le nombre de nombres premiers entre 1 et 48.

6. Confirmer le résultat obtenu en faisant la liste des nombres premiers entre 1 et 48.

Réponse : 1. On utilise l'exercice 4.6 : si n n'est pas premier, il est divisible par un nombre premier p avec $2 \leq p \leq \sqrt{n}$. Comme $\sqrt{n} < \sqrt{49} = 7$, les seules possibilités sont 2, 3 et 5.
2. Les éléments de A_d s'écrivent sous la forme dk, avec $k \in \mathbb{N}$. Comme $1 \leq n \leq 48$, on doit avoir $1 \leq k \leq \frac{48}{d}$. Comme k est entier, il faut que $k \leq \lfloor \frac{48}{d} \rfloor$, où $\lfloor - \rfloor$ désigne la partie entière inférieure. Comme toutes ces valeurs de k donnent bien kd entre 1 et 48, on obtient $\mathrm{card}(A_d) = \lfloor \frac{48}{d} \rfloor$.
3. Soit n un entier entre 1 et 48. Alors $n \in A_2 \cap A_3$ ssi n est un multiple commun de 2 et 3. Or, comme 2 et 3 sont premiers entre eux, le plus petit multiple commun de 2 et 3 est 6, ce qui signifie que ($2|n$ et $3|n$) ssi $6|n$. Ainsi, $A_2 \cap A_3 = A_6$.
4. Comme 2 et 5 sont premiers entre eux, et de même pour 3 et 5, on obtient par le même argument $A_2 \cap A_5 = A_{10}$ et $A_3 \cap A_5 = A_{15}$. Pour $A_2 \cap A_3 \cap A_5$, on peut faire une étape supplémentaire :

$$A_2 \cap A_3 \cap A_5 = (A_2 \cap A_3) \cap A_5 = A_6 \cap A_5 = A_{30}$$

puisque 6 et 5 sont premiers entre eux.
5. 1 n'est pas premier.
Soit n entre 2 et 48. Si n n'est pas premier, il est dans $A_2 \cup A_3 \cup A_5$ d'après la question 1. Réciproquement, si $n \in A_2 \cup A_3 \cup A_5$, il n'est pas premier sauf si $n = 2$, 3 ou 5.
Le nombre de nombre premiers entre 1 et 48 est donc 47 (le nombre d'entiers entre 2 et 48) $-\mathrm{card}(A_2 \cup A_3 \cup A_5)$ (les nombres entre 2 et 48 divisibles par 2, 3 ou 5) $+3$ (car on a retiré 2, 3 et 5 alors qu'ils sont premiers). Or, par la formule du TD2 et les questions précédentes,

$$\begin{aligned}\mathrm{card}(A_2 \cup A_3 \cup A_5) &= \mathrm{card}(A_2) + \mathrm{card}(A_3) + \mathrm{card}(A_5) - \mathrm{card}(A_2 \cap A_3) - \mathrm{card}(A_2 \cap A_5) - \mathrm{card}(A_3 \cap A_5) \\ &\quad + \mathrm{card}(A_2 \cap A_3 \cap A_5) \\ &= \mathrm{card}(A_2) + \mathrm{card}(A_3) + \mathrm{card}(A_5) - \mathrm{card}(A_6) - \mathrm{card}(A_{10}) - \mathrm{card}(A_{15}) + \mathrm{card}(A_{30}) \\ &= 24 + 16 + 9 - 8 - 4 - 3 + 1 = 35\end{aligned}$$

Cela donne $47 - 35 + 3 = 15$ nombres premiers entre 1 et 48.
6. Voici la liste des 15 nombres premiers entre 1 et 48 : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$.

Exercice 4.8. Divisibilité

Soit p un nombre premier > 3.

1. Montrer que 3 divise $(p-1)p(p+1)$. En déduire que 3 divise $p^2 - 1$.

2. Montrer que 24 divise $p^2 - 1$.

Exercice 4.9. $\mathbb{Z}/d\mathbb{Z}$

1. Écrire les tables de multiplication de $\mathbb{Z}/5\mathbb{Z}$ et de $\mathbb{Z}/6\mathbb{Z}$.

2. Vérifier que pour tout élément $x \neq \overline{0}$ dans $\mathbb{Z}/5\mathbb{Z}$, il existe $y \in \mathbb{Z}/5\mathbb{Z}$ tel que $xy = \overline{1}$.

3. Trouver x et y dans $\mathbb{Z}/6\mathbb{Z}$, distincts de $\overline{0}$, tels que $xy = \overline{0}$.

Exercice 4.10. $\mathbb{Z}/d\mathbb{Z}$

Soit un entier $d \geq 2$ qui n'est pas premier. Montrer qu'il existe x et y dans $\mathbb{Z}/d\mathbb{Z}$, distincts de $\overline{0}$, tels que $xy = \overline{0}$.

Exercice 4.11. $\mathbb{Z}/p\mathbb{Z}$

Soit un nombre premier p.

1. Soit $1 \leq a \leq p-1$. Montrer qu'il existe u et v dans $\mathbb{Z}$ tels que $au+pv=1$.

2. En déduire que pour tout x dans $\mathbb{Z}/p\mathbb{Z}$, distinct de $\overline{0}$, il existe y dans $\mathbb{Z}/p\mathbb{Z}$ tel que $xy=\overline{1}$.

3. En déduire qu'on ne peut pas trouver x et y dans $\mathbb{Z}/p\mathbb{Z}$, distincts de $\overline{0}$, tels que $xy=\overline{0}$.

Exercice 4.12. Critères de divisibilité

Soit $n \in \mathbb{N}$. Pour éviter la confusion avec un produit, on note $n=[a_k \dots a_1 a_0]$ l'écriture en base 10 de n : a_0 est le chiffre des unités, a_1 celui des dizaines, ...

1. Soit $n=[a_k \dots a_1 a_0]$, écrire n en fonction de $a_0, \dots, a_k$ et des puissances de 10.

2. On veut justifier le critère de divisibilité des entiers par 3.

a. Calculer $\overline{10^i}$ pour tout $i \in \mathbb{N}$ dans $\mathbb{Z}/3\mathbb{Z}$.

b. Pour $n=[a_k \dots a_1 a_0]$, montrer que $n \equiv a_0 + \dots + a_k$ [3].

c. En déduire que n est divisible par 3 ssi la somme de ses chiffres est divisible par 3.

3. Justifier que l'argument précédent fonctionne aussi pour la divisibilité par 9 : n est divisible par 9 ssi la somme de ses chiffres est divisible par 9.

4. Divisibilité par 11.

a. Soit $n=[a_k \dots a_1 a_0]$. Montrer que n est divisible par 11 ssi $\sum_{i=0}^{k}(-1)^i a_i$ est divisible par 11.

b. Application : est-ce que 5472819 est divisible par 11 ?

Réponse : 1.

$$n = \sum_{i=0}^{k} a_i 10^i$$

2.a. Dans $\mathbb{Z}/3\mathbb{Z}$, $\overline{10}=\overline{1}$ donc $\overline{10^i}=\overline{10}^i=\overline{1}^i=\overline{1^i}=\overline{1}$.

2.b. On déduit des deux questions précédentes que

$$\overline{n} = \overline{\sum_{i=0}^{k} a_i 10^i} = \sum_{i=0}^{k} \overline{a_i}\,\overline{10^i} = \sum_{i=0}^{k} \overline{a_i} = \overline{\sum_{i=0}^{k} a_i}.$$

Cela signifie exactement que $n \equiv a_0 + \dots + a_k$ [3].

2.c. Le reste de la division euclidienne de n par 3 est nul ssi celui de la division euclidienne de la somme des chiffres $a_0 + \dots + a_k$ l'est, ce qui donne le résultat.

3. On peut prendre le raisonnement précédent pour la divisibilité par 9, le point essentiel étant qu'on a encore $\overline{10}=\overline{1}$ dans $\mathbb{Z}/9\mathbb{Z}$.

4.a. C'est encore une fois le même raisonnement, mais avec cette fois $\overline{11}=\overline{-1}$ dans $\mathbb{Z}/11\mathbb{Z}$.

4.b. On doit regarder la somme alternée des chiffres de cet entier : $9-1+8-2+7-4+5=22$, qui est divisible par 11, donc 5472819 est divisible par 11.

Exercice 4.13. Calcul de puissances

1. Dans $\mathbb{Z}/10\mathbb{Z}$, calculer les premières puissances $\overline{7}^n$, jusqu'à trouver un entier $n \geq 1$ tel que $\overline{7}^n=\overline{1}$.

2. En déduire que pour tous q et r dans $\mathbb{N}$, $\overline{7}^{4q+r}=\overline{7}^r$ dans $\mathbb{Z}/10\mathbb{Z}$.

3. Quel est le chiffre des unités de 2017^{2019} ?

Exercice 4.14. Divisibilité

En effectuant les calculs dans $\mathbb{Z}/d\mathbb{Z}$ pour un entier d approprié, montrer que pour tout $n \geq 0$:

1. $7|3^{2n+1} + 2^{n+2}$

2. $11|2^{6n+3} + 3^{2n+1}$

3. $3|4^n - 1$ puis $7|2^{4^n} - 2$