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

Feuille d'exercices 4

Arithmétique

<u>Exercice 4.1. Algorithme d'Euclide</u>
Pour les entiers a et b suivants, calculer $\mathrm{pgcd}(a, b)$ 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 $b = n$

<u>Exercice 4.2. Division euclidienne</u>
1. Calculer $\mathrm{pgcd}(1995, 2975)$.

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 ?

<u>Exercice 4.4. Pgcd, ppcm</u>
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.

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

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

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.

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 ?

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 $7 | 2^{4^n} - 2$