Arithmétique et groupes 9 janvier 2024
L3 Parcours Mathématiques pour l'enseignement Contrôle Terminal
Université Claude Bernard (Lyon 1) Durée : **120 minutes**

Barème : 4+7+6+8=25

Exercice 1 ($4 = 0,5 + 1 + 2,5$ points)**.**
a) Soit $k \in \mathbb{N}^*$. Donner un multiple commun des nombres $1, 2, \ldots, k$.
b) Pour tout $k \in \mathbb{N}^*$, montrer qu'il est possible de trouver un entier n tel que les nombres $n+1, n+2, \ldots, n+k$ soient tous composés.
c) En déduire que pour tout entier $k \in \mathbb{N}^*$, il existe un nombre premier p tel que les nombres $p+1, p+2, \ldots, p+k$ soient tous composés.

Correction.
a) Le factoriel $k!$ est un multiple commun de $1, 2, \ldots, k$.
b) Pour tout $k \in \mathbb{N}^*$, soit $n = (k+1)! + 1$, alors le nombre $n+i$ est divisible par $i+1$ pour $i = 1, \ldots, k$.
c) D'après b), pour tout $k \in \mathbb{N}^*$, il existe un entier $n \geq 3$ tel que les nombres $n+1, n+2, \ldots, n+k$ soient tous composés. Soit p le plus grand nombre premier majoré par n. Alors tout entier dans $[p+1, n+k]$ est un nombre composé. En particulier, les nombres $p+1, \ldots, p+k$ sont tous composés.

Exercice 2 ($7 = 2 + 2 + (1 + 1 + 1)$ points)**.**
a) Calculer le reste de la division euclidienne de 10^{100} par 247.
b) Calculer $\mathrm{pgcd}(198, 75)$ et trouver un couple d'entiers (u, v) tel que

$$\mathrm{pgcd}(198, 75) = 198u + 75v.$$

c) Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ les équations suivantes :
1. $198x + 75y = 0$;
2. $198x + 75y = 3$;
3. $198x + 75y = 5$.

Correction. a) On observe que $247 = 13 \times 19$ et que 13 et 19 sont premiers entre eux. Comme $100 \equiv 4 \pmod{12}$ et $100 \equiv 10 \pmod{18}$, par le PTF, on a

$$10^{100} \equiv 10^4 \equiv 3^4 \equiv 3 \pmod{13},$$
$$10^{100} \equiv 10^{10} \equiv 5^5 \equiv 9 \pmod{19}.$$

D'autre part, on a la relation de Bézout $3 \cdot 13 + (-2) \cdot 19 = 1$. Par le théorème des restes chinois, on a

$$10^{100} \equiv 9 \cdot 3 \cdot 13 + 3 \cdot (-2) \cdot 19 \equiv 3 \cdot 79 \equiv 237 \pmod{247}.$$

On peut aussi chercher une puissance de 10 qui est $\pm 1 \pmod{247}$ comme suit :

$$10^3 \equiv 12 \Longrightarrow 10^9 \equiv 1728 \equiv 7 \times 247 - 1 \equiv -1 \Longrightarrow 10^{100} = 10^{9\times 11+1} \equiv -10 \equiv 237.$$

b) On effectue les divisions euclidiennes :

$$\begin{aligned} 198 &= 75 \times 2 + 48 \\ 75 &= 48 \times 1 + 27 \\ 48 &= 27 \times 1 + 21 \\ 27 &= 21 \times 1 + 6 \\ 21 &= 6 \times 3 + 3 \\ 6 &= 3 \times 2 \Longrightarrow \operatorname{pgcd}(198, 75) = 3, \end{aligned}$$

et en déduit que

$$\begin{aligned} 3 &= 21 - (27 - 21) \times 3 \\ &= -27 \times 3 + (48 - 27) \times 4 \\ &= -(75 - 48) \times 7 + 48 \times 4 \\ &= (198 - 75 \times 2) \times 11 - 75 \times 7 \Longrightarrow 198 \times 11 + 75 \times (-29) = 3. \end{aligned}$$

b) 1. On cherche $(x, y) \in \mathbb{Z}\times\mathbb{Z}$ tels que $198x+75y = 0 \Longleftrightarrow 66x+25y = 0$ avec $\operatorname{pgcd}(66, 25) = 1 \Longleftrightarrow 25|x$ et $66|y$. En substituant $x = 25k$ avec $k \in \mathbb{Z}$ dans la dernière équation, on tire $y = -66k$. Donc la solution générale est

$$(x, y) = (25, -66)k \quad \text{avec} \quad \mathrm{k} \in \mathbb{Z}.$$

2. Pour tout $(x, y) \in \mathbb{Z}\times\mathbb{Z}$, d'après a), on a $198x+75y = 3 \Longleftrightarrow 198(x-11)+75(y+29) = 0$, on déduit de a) que

$$(x, y) = (11, -29) + (25, -66)k, \quad k \in \mathbb{Z};$$

3. Comme $\operatorname{pgcd}(198, 75) = 3$ et $3 \nmid 5$, l'équation $198x + 75y = 5$ n'a pas de solution dans $\mathbb{Z} \times \mathbb{Z}$.

Exercice 3 ($6 = 3 + 3$ points)**.** Soient les polynômes dans $\mathbb{R}[X]$:

$$\begin{aligned} A &= X^5 - X^4 + 2X^3 + 1, \\ B &= X^5 + X^4 + 2X^2 - 1. \end{aligned}$$

1. Calculer leur PGCD unitaire et en déduire une relation de Bézout entre A et B.
2. Déterminer tous les couples de polynômes (U, V) vérifiant cette identité.

Correction. a) On effectue les divisions eucliennes : $A - B = -2X^4 + 2X^3 - 2X^2 + 2$,

$$B = (-2X^4 + 2X^3 - 2X^2 + 2)(-\frac{1}{2}X - 1) + X^3 + X + 1,$$

$$-2X^4 + 2X^3 - 2X^2 + 2 = (X^3 + X + 1)(-2X + 2).$$

D'où $\text{pgcd}(A,B) = X^3 + X + 1$ et

$$X^3 + X + 1 = B - (A - B)\left(-\frac{1}{2}X - 1\right) = \left(\frac{1}{2}X + 1\right)A + \left(-\frac{1}{2}X\right)B.$$

On factorise $A = (X^3+X+1)(X^2-X+1)$ et $B = (X^3+X+1)(X^2+X-1)$ par la division euclidienne ou la méthode de coefficients à déterminer. Donc,

$$(X^2 - X + 1)U_0 + (X^2 + X - 1)V_0 = 1 \tag{1}$$

où $U_0 = \frac{1}{2}X + 1$ et $\mathrm{V}_0 = -\frac{1}{2}\mathrm{X}$.
b) On cherche les couples de polynômes (U, V) tels que

$$(X^2 - X + 1)U + (X^2 + X - 1)V = 1.$$

En soustrayant (1) on a

$$(X^2 - X + 1)(U - U_0) + (X^2 + X - 1)(V - V_0) = 0.$$

Comme $X^2 - X + 1$ et $X^2 + X - 1$ sont premiers entre eux, on en déduit que

$$U = U_0 + (X^2 + X - 1)P,$$
$$V = V_0 - (X^2 - X + 1)P,$$

où $P \in \mathbb{R}[X]$.

Exercice 4 ($8 = 2 + 1,5 + 1,5 + 1,5 + 1,5$ points)**.** Soit G un groupe d'ordre $\ell = mn$ avec $m, n \in \mathbb{N}^*$. On suppose que H et K sont deux sous-groupes de G d'ordre m et n respectivement tels que $H \cap K = \{e\}$.

1. Soit $\varphi : H \times K \to G$ l'application définie par $(h, k) \mapsto hk$. L'application φ est-elle un morphisme ?
2. Montrer que l'application φ est injective et en déduire que tout élément g de G peut s'écrire de façon unique comme $g = hk$, où $h \in H$ et $k \in K$.
3. Rappeler la définition d'un sous-groupe distingué ou normal. Si K est un sous-groupe distingué de G, montrer que H est isomorphe à G/K.
4. Rappeler la définition du centre d'un groupe. Si K est un sous-groupe du centre de G. Est-ce que G est isomorphe à $H \times K$?
5. Supposons que G est abélien et $\psi : G \to H$ est un morphisme tel que $K = \operatorname{Ker}\psi$. Montrer que G est isomorphe à $H \times K$.

Correction. 1. Soit l'application $\varphi : H \times K \longrightarrow G$ telle que $(h, k) \mapsto hk$. Pour tout $(h, k), (h', k') \in H \times K$, on a

$$\varphi((h, k) \cdot (h', k')) = \varphi((hh', kk')) = hh'kk'.$$

Or $\varphi((h,k)) \cdot \varphi((h',k')) = hkh'k'$. Donc, φ est un morphisme ssi $h'k = kh'$ pour tout $h' \in H$ et $k \in\in K$, ce qui n'est pas vrai en général . Par exemple, soit

$$G = \mathfrak{S}_3 = \{e,\ (1\,2\,3),\ (1\,3\,2),\ (1\,2),\ (1\,3),\ (2\,3)\},$$

$H = \{e, (1\,2)\}$ et $K = \{e, (1\,2\,3), (1\,3\,2)\}$. Si $h = k' = e$, $h' = (12)$ et $k = (123)$, alors $h'k = (12)(123) = (13)$ or $kh' = (123)(12) = (23)$.

2. Soit $\varphi(h,k) = hk = e$ avec $k \in K$, alors $h = k^{-1}$. Il s'ensuit que $h = k \in H \cap K = \{e\}$. Donc Ker$\varphi = \{(e,e)\}$ et φ est injective. Comme $|H \times K| = |G| = mn$, on déduit que φ est aussi surjective et donc bijective. Par suite, tout élément $g \in G$ peut s'écrire de façon unique comme $g = hk$ avec $(h,k) \in H \times K$.

3. Soit G un groupe et $H \leq G$. On dit que H est normal si $xHx^{-1} = H$ ou $xH = Hx$ pour tout $x \in G$.
   Par 2. on a $G = HK = \{hk : h \in H, k \in K\}$. Soit $\phi : G = HK \to H$ l'application telle que $hk \mapsto h$ pour tout $h \in H$ et $k \in K$. Il est clair que ϕ est surjective. D'autre part, pour tout $h, h' \in H$ et $k, k' \in K$, comme $K \lhd G$, il existe $k_1 \in K$ tel que $kh' = h'k_1$. C'est-à-dire que

$$\phi((hk)(h'k')) = \phi((hh')(k_1k')) = hh' = \phi(hk)\phi(h'k').$$

   Donc ϕ est un morphisme surjectif avec $\mathrm{Ker}(\phi) = K$. Il existe donc un isomorphisme $\bar{\phi} : G/K \to H$ définie par $hK \mapsto h$ pour tout $h \in H$.

4. Soit G un groupe. L'ensemble des éléments de G qui commutent avec tous les éléments de G est le centre de G, noté $Z(G)$, qui est un sous-groupe de G.
   Si $K \leq Z(G)$, alors les éléments de K commutent avec tous les éléments de G. Donc, $\forall h, h' \in H$ et $k, k' \in K$ on a

$$\varphi((h,k) \cdot (h',k')) = \varphi((hh', kk')) = hh'kk' = hkh'k = \varphi((h,k)) \cdot \varphi((h',k')).$$

   Ceci prouve que φ est un morphisme. D'après 2., l'application φ est bijective, par suite c'est un isomorphisme.

5. Si G est abélien, le centre de G est égal à G. Comme K est un sous-groupe de G, d'après 4., G est isomorphe à $H \times K$.
