Arithmétique et groupes 5 novembre 2024
L3 Parcours Mathématiques pour l'enseignement Contrôle continu 1
Université Claude Bernard (Lyon 1) Durée : **90 minutes**

Corrigé

Exercice 1. (**3 points**) Soit $n = 2^{1137}$.

1. Calculer le reste de la division de n par 13 et par 17.
2. En déduire le reste de la division de n par 221.

Solution. 1. Par le petit théorème de Fermat, on a

$$2^{12} \equiv 1 \pmod{13}, \quad 2^{16} \equiv 1 \pmod{17}.$$

De $1137 \equiv 9 \pmod{12}$ et $1137 \equiv 1 \pmod{16}$, on déduit que

$$n = 2^{1137} \equiv 2^9 \equiv 5 \pmod{13}, \quad n = 2^{1137} \equiv 2^1 \equiv 2 \pmod{17}.$$

2. On note que $221 = 13 \times 17$ et que $\mathrm{pgcd}(13, 17) = 1$. En effectuant deux divisions euclidiennes : $17 = 13 + 4$ et $13 = 3 \cdot 4 + 1$, on déduit l'identité de Bézout : $1 = 4 \cdot 13 - 3 \cdot 17$. Par le théorème des restes chinois on a

$$n \equiv \mathbf{5} \cdot (-3) \cdot 17 + \mathbf{2} \cdot 4 \cdot 13 \equiv 70 \pmod{221}.$$

Donc, le reste de la division de n par 221 est 70.

Exercice 2. (**4 points**) On s'interroge sur une réciproque possible du petit théorème de Fermat comme suit :
- *Si n est un entier naturel tel que pour tout entier naturel a premier avec n on a $a^{n-1} \equiv 1 \pmod{n}$, alors n est premier.* -

1. Soit $n = 561$. Vérifier que n n'est pas premier en le factorisant en produit de nombres premiers.
2. Montrer que pour tout $a \in \mathbb{Z}$ premier avec n, on a : $a^{n-1} \equiv 1 \pmod{n}$.
3. Conclure.

Solution. 1. On a $561 = 3 \times 11 \times 17$.

2. Par le petit théorème de Fermat, pour tout entier naturel a premier avec 3, 11 et 17 respectivement, on a :

$$a^2 \equiv 1 \pmod 3, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}.$$

En élévant les deux membres des équations aux puissances 280, 56 et 35 respectivement, on obtient

$$a^{560} \equiv 1 \pmod 3, \quad a^{560} \equiv 1 \pmod{11}, \quad a^{560} \equiv 1 \pmod{17}.$$

Comme 3, 11, 17 sont deux à deux premiers entre eux, par le théorème d'Euclide-Gauss, on déduit que $a^{560} \equiv 1 \pmod{561}$.

3. Pour tout $a \in \mathbb{Z}$ premier avec 561, on a montré que $a^{561-1} \equiv 1 \pmod{561}$, or 561 n'est pas premier. Donc, la réciproque du petit théorème de Fermat est inexacte.

Exercice 3. (**5 points**)

1. Trouver tous les couples d'entiers $(x, y) \in \mathbb{Z}^2$ tels que

$$7x + 4y = 100.$$

2. En déduire tous les triplets d'entiers positifs $(x, y, z) \in \mathbb{N}^3$ tels que

$$\begin{cases} x + y + z = 100, \\ 5x + 3y + \frac{1}{3}z = 100. \end{cases}$$

Solution. 1. On observe que $7(-1) + 4(2) = 1$, d'où on déduit une solution particulière $(-100, 200)$ et puis la solution générale de l'équation :

$$\begin{cases} x = -100 + 4k \\ y = 200 - 7k \end{cases} \qquad (k \in \mathbb{Z}).$$

2. En retranchant la première équation de la seconde multipliée par 3 on obtient $7x + 4y = 100$. De la solution de 1. on tire

$$\begin{cases} x &= -100 + 4k \geq 0 \Longrightarrow k \geq 25 \\ y &= 200 - 7k \geq 0 \Longrightarrow k \leq \lfloor \frac{200}{7} \rfloor = 28 \Longrightarrow k \in \{25, 26, 27, 28\}. \\ z &= 100 - (x + y) = 3k \Longrightarrow k \geq 0 \end{cases}$$

Il s'en suit que l'ensemble des solutions positives est :

$$\{(0, 25, 75), \quad (4, 18, 78), \quad (8, 11, 81), \quad (12, 4, 84)\}.$$

Exercice 4. (5 **points**)
Soit E un ensemble. On note $\mathcal{P}(E)$ l'ensemble de parties de E. Soit $A \in \mathcal{P}(E)$. On note $\overline{A} = E \setminus A$, le complémentaire de A dans E. Pour tout $A \subset E$ on note $\mathbf{1}_A$ sa fonction indicatrice sur E.

1. Soient E un ensemble et $A, B \in \mathcal{P}(E)$. Démontrer les propriétés de la fonction indicatrice :

$$\begin{aligned}\mathbf{1}_{A\cap B} &= \mathbf{1}_A \cdot \mathbf{1}_B;\\ \mathbf{1}_{A\cup B} &= \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A \cdot \mathbf{1}_B.\end{aligned}$$

2. Soit E un ensemble fini de cardinal $|E| = n$. Exprimer les deux sommes suivantes en fonction d'indicatrice et puis calculer leurs sommes :

$$\sum_{A,B\subset E} |A \cap B|, \qquad \sum_{A,B\subset E} |A \cup B|.$$

Solution. 1. Pour tout $x \in E$, on a

$$\mathbf{1}_{A\cap B}(x) = \begin{cases} 1 & \text{si x} \in \text{A} \cap \text{B};\\ 0 & \text{sinon,}\end{cases}$$

ce qui coincide avec les valeurs de $\mathbf{1}_A \cdot \mathbf{1}_B : x \mapsto \mathbf{1}_A(x) \cdot \mathbf{1}_B(x)$ pour tout $x \in E$.

2. Pour tout $x \in E$, on a l'équivalence

$$[\mathbf{1}_A(x) = 1] \Longleftrightarrow [A = \{x\} \cup B \quad \text{avec} \quad \text{B} \subset \text{E} \setminus \{\text{x}\}].$$

Il s'en suit que

$$\sum_{A\subset E} \mathbf{1}_A(x) = \#\{B : B \subset E \setminus \{x\}\} = 2^{n-1}.$$

Par suite, on a

$$\begin{aligned}\sum_{A,B\subset E} |A \cap B| &= \sum_{A,B\subset E} \sum_{x\in E} \mathbf{1}_A(x) \cdot \mathbf{1}_B(x)\\ &= \sum_{x\in E} \left(\sum_{A\subset E} \mathbf{1}_A(x)\right) \left(\sum_{B\subset E} \mathbf{1}_B(x)\right)\\ &= \sum_{x\in E} 2^{n-1} \cdot 2^{n-1}\\ &= n\, 2^{2n-2}.\end{aligned}$$

De même on a

$$\sum_{A,B\subset E} |A\cup B| = \sum_{A,B\subset E}\sum_{x\in E} \left(\mathbf{1}_A(x) + \mathbf{1}_B(x) - \mathbf{1}_A(x)\cdot \mathbf{1}_B(x)\right).$$

Il est clair que

$$\sum_{A,B\subset E}\sum_{x\in E} \mathbf{1}_A(x) = \sum_{x\in E}\left(\sum_{B\subset E}\sum_{A\subset E} \mathbf{1}_A(x)\right) = \sum_{x\in E} 2^n\cdot 2^{n-1} = n\,2^{2n-1}.$$

De même, on a

$$\sum_{A,B\subset E}\sum_{x\in E} \mathbf{1}_B(x) = n2^{2n-1}.$$

D'autre part, on a

$$\sum_{A,B\subset E}\sum_{x\in E} \mathbf{1}_A(x)\cdot\mathbf{1}_B(x) = n2^{2n-2}.$$

En récapitulant, on obtient

$$\sum_{A,B\subset E} |A\cap B| = 2\cdot n2^{2n-1} - n2^{2n-2} = 3n\,4^{n-1}.$$

Exercice 5. (**5 points**) Pour un entier $a > 1$, on note $M_a = 2^a - 1$.

1. Vérifier que M_2, M_3, M_5 et M_7 sont premiers.
2. Montrer que si M_a est un nombre premier alors a l'est aussi.
3. Soit p un nombre premier impair et q un nombre premier tel que $q \mid M_p$.
   Montrer que $q \equiv 1[p]$; en déduire que $q \equiv 1[2p]$.
   [*On pourra se servir de l'égalité* : $\mathrm{pgcd}(a^m - 1, a^n - 1) = a^{\mathrm{pgcd}(m,n)} - 1$.]
4. M_{11} est-il un nombre premier ?

Solution. 1. On a : $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ and $M_7 = 127$. Il est clair que 3,7 et 31 sont tous premiers. On montre que 127 est premier. Si 127 n'était pas premier, alors il devait posséder un diviseur premier majoré par $\sqrt{127} < 12$, or 127 n'est pas divisible par $3, 5, 7$ ni 11, donc 127 est premier.

2. Par contraposée, on suppose que a n'est pas premier. Alors il existe des entiers $p, q > 1$ tels que $a = pq$. Par suite,

$$M_a = 2^{pq} - 1 = (2^p - 1)Q, \quad \text{avec} \quad Q = \sum_{k=0}^{q-1} (2^p)^k.$$

Comme $2^p - 1 \geq 3$ et $Q \geq 2^p$, l'entier M_a n'est pas premier.

3. Soit p un nombre premier impair et q un diviseur premier de M_p. Alors q est un diviseur de $2^p - 1$, ce qui implique que $2^p \equiv 1 \pmod{q}$ et que q est impair.

   Par le petit théorème de Fermat, on a $2^{q-1} \equiv 1 \pmod{q}$. Donc q est un diviseur premier de $\mathrm{pgcd}(2^{\mathrm{p}} - 1, 2^{\mathrm{q}-1} - 1) = 2^{\mathrm{pgcd}(\mathrm{p},\mathrm{q}-1)} - 1$, ce qui implique que $\mathrm{pgcd}(\mathrm{p}, \mathrm{q} - 1) = \mathrm{p}$ car p est premier et $\mathrm{pgcd}(\mathrm{p}, \mathrm{q} - 1) \neq 1$. Il s'en quit que p divise $q - 1$, et que 2 est un diviseur du nombre pair $q - 1$. Par le théorème d'Euclide-Gauss, on a $q \equiv 1 \pmod{2p}$.

4. D'après ce qui précède, s'il existe un diviseur premier q de $M_{11} = 2^{11} - 1 = 2047$, alors $q < \sqrt{M_{11}} < 2^{12/2} = 64$ et $q \equiv 1 \pmod{22}$, c'est-à-dire que $q = 22k + 1$ avec $k \in \mathbb{N}^*$. Le plus petit tel entier est donc 23. Comme $M_{11} = 2047 = 23 \times 89$, l'entier M_{11} n'est pas premier.