# Licence Math-Info

# Exercices d'Arithmétique

TD LMI2
Pascal Lefèvre

# 1 Révisions : Théorie élémentaire des ensembles

**Exercice 1.1** a) Ecrire la négation de la phrase suivante: “La nuit, tous les chats sont gris."

b)(“on peut toujours rêver !") Un enseignant dit à ses étudiants: "Chaque étudiant qui fera tous ses exercices de TD aura 20." Les étudiants n'ayant pas fait leurs exercices reçoivent un 20. Est-ce illogique ?

c) Dans un restaurant pour mathématiciens, un client choisit le menu avec “fromage ou dessert". A la fin du repas on lui sert un plateau de fromages et une tarte. Est-ce illogique?

**Exercice 1.2** Démontrons que dans une boîte de crayons de couleurs, tous les crayons sont de la même couleur. Soit $n \geq 1$ et $\mathcal{P}_n$ la propriété “Dans toute boîte contenant $n$ crayons de couleurs, tous les crayons sont de la même couleur.”

Pour $n = 1$, $\mathcal{P}_1$ est trivialement vraie.

Supposons que $\mathcal{P}_n$ est vraie, où $n \geq 1$ et considérons une boîte contenant $n + 1$ crayons de couleurs. Retirons un crayon de cette boîte, nous avons maintenant une boîte contenant $n$ crayons de couleurs. Comme $\mathcal{P}_n$ est vraie, tous ces crayons sont de la même couleur. On remet le crayon mis à l'écart pour en reprendre un autre. À nouveau, nous avons encore une boîte contenant $n$ crayons de couleurs et d'après $\mathcal{P}_n$, vraie, tous ces crayons sont de la même couleur. Ainsi, tous les crayons considérés sont de la même couleur.

Donc $\mathcal{P}_{n+1}$ est vraie et, par récurrence, $\mathcal{P}_n$ est vraie pour tout $n \geq 1$.
*Où est le problème ?*

**Exercice 1.3** Un facteur fait sa tournée. A part délivrer des lettres, il aime les jeux mathématiques. Le mathématicien chez qui il arrive lui pose cette devinette :

- J'ai trois filles. Le produit de leurs âges est 36 et leur somme est égale au numéro de la maison d'à côté, quels sont les âges de mes 3 filles ?

Le facteur regarde la maison voisine et dit:

- Mais, je ne peux pas vous répondre !

Le mathématicien est gêné, recalcule et s'écrie:

- Ah oui... j'ai oublié de vous dire : mon ainée est blonde !

Quels sont les âges des 3 filles ?

**Exercice 1.4** Un groupe de $N \geq 2$ personnes se réunit. Montrer qu'au moins deux personnes ont serré le même nombre de mains. On pourra séparer les deux cas suivants : soit tout le monde a serré au moins une main, soit il existe quelqu'un qui n'a serré aucune main.

**Exercice 1.5** Soit $(P)$ la proposition suivante: $(\exists n \in \mathbb{N})(\forall p \in \mathbb{N}),\ p \leq n$.

Que veut-elle dire? Ecrire sa négation. Laquelle des propositions $(P)$ ou non $(P)$ est vraie?

**Exercice 1.6** Soient $f_1, f_2, f_3$ trois fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Traduire graphiquement les propriétés suivantes:

a) $(\forall j \in \{1,2,3\})(\exists a \in \mathbb{R}),\ f_j(a) = 1$.
b) $(\exists j \in \{1,2,3\})(\forall a \in \mathbb{R}),\ f_j(a) = 1$.
c) $(\exists a \in \mathbb{R})(\forall j \in \{1,2,3\}),\ f_j(a) = 1$.
d) $(\forall a \in \mathbb{R})(\exists j \in \{1,2,3\}),\ f_j(a) = 1$.

**Exercice 1.7** Soient $A, B$ des parties de $E$.

a) Trouver une condition nécessaire et suffisante pour que le problème "$A \cap X = B$ , où $X \in \mathcal{P}(E)$" ait une solution puis le résoudre.

b) idem pour $A \cup X = B$.

**Exercice 1.8** Soit $A$ une partie de $E$. On appelle fonction caractéristique de $A$ l'application $f$ de $E$ dans l'ensemble $\{0, 1\}$, telle que: $f(x) = 0$ si $x \notin A$ et $f(x) = 1$ si $x \in A$.

Soient $A$ et $B$ deux parties de $E$, $f$ et $g$ leurs fonctions caractéristiques. Montrer que les fonctions suivantes sont les fonctions caracteristiques d'ensembles que l'on déterminera:

a) $1 - f$.

b) $fg$.

c) $f + g - fg$.

**Exercice 1.9** Soient $E$, $F$ des ensembles et $f : E \to F$ une application. Montrer que:

a) $f$ est injective si et seulement s'il existe $g : F \to E$ telle que $g \circ f = Id_E$.

b) $f$ est surjective si et seulement s'il existe $g : F \to E$ telle que $f \circ g = Id_F$.

c) $f$ est bijective si et seulement s'il existe $g : F \to E$ telle que $g \circ f = Id_E$ et $f \circ g = Id_F$.

**Exercice 1.10** Soient $f$ une application de $E$ dans $F$, $A$ une partie de $E$ et $B$ une partie de $F$

1)a) Montrer que $\forall A \in \mathcal{P}(E)$, $A \subset f^{-1}(f(A))$.

b) Montrer que: [pour tout $A \in \mathcal{P}(E)$, $f^{-1}(f(A)) = A$] $\Longleftrightarrow$ $f$ injective.

2)a) Montrer que pour tout $B \in \mathcal{P}(F)$, $f(f^{-1}(B)) \subset B$.

b) Montrer que: [pour tout $B \in \mathcal{P}(F)$, $f(f^{-1}(B)) = B$] $\Longleftrightarrow$ $f$ surjective.

**Exercice 1.11** Soient $A, B$ des parties d'un ensemble $E$. Soit $f : \mathcal{P}(E) \longrightarrow \mathcal{P}(A) \times \mathcal{P}(B)$ tel que $\forall X \in \mathcal{P}(E)$, $f(X) = (X \cap A, X \cap B)$.

Montrer que : $f$ injective $\Longleftrightarrow A \cup B = E$.

A quelle condition est-elle surjective ?

**Exercice 1.12** Soit $E$ un ensemble non vide. Montrer que $E$ est infini si et seulement si pour toute application $f : E \to E$, il existe $A \subset E$, non vide, distinct de $E$ vérifiant $f(A) \subset A$.

Indication: pour cela, on pourra s'intéresser d'une part à une permutation sur un ensemble fini et d'autre part à un ensemble du type $\{f^n(x) |\ n \in \mathbb{N}^*\}$.

**Exercice 1.13** (Olympiades 1977)

Soit $f$ une application de $\mathbb{N}^*$ dans $\mathbb{N}^*$ telle que pour tout $n$ de $\mathbb{N}^*$, on ait : $f(n+1) > f(f(n))$.

Montrer que: $\forall n \in \mathbb{N}^*$, $f(n) = n$.

Indication: on pourra montrer que pour tout $n$, $x \geq n \Rightarrow f(x) \geq n$.

# 2 Relations

**Exercice 2.1** Prouver les affirmations laissées en exercice dans le cours: déf. de plus petit élément, borne inf.,...; partitions,...

**Exercice 2.2** Soient $A$ et $B$ deux parties d'un ensemble $E$. La relation d'ordre considérée est l'inclusion. Déterminer $\sup(\{A, B\})$ et $\inf(\{A, B\})$.

**Exercice 2.3** Soit $n \geq 1$ un entier. On dit que $x$ et $y$ (deux entiers) sont congruents modulo $n$ si $n$ divise $x - y$. Auquel cas , on note $x \equiv y[n]$. Montrer que c'est une relation d'équivalence.

**Exercice 2.4** Soient $(E, \leq)$ et $(F, \prec)$ deux ensembles ordonnés isomorphes par la bijection $f$ (Cela signifie que, $\forall x, y \in E$, on a: $x \leq y \Leftrightarrow f(x) \prec f(y)$). Soit $X$ une partie de $E$ admettant la borne supérieure $b$ pour l'ordre sur $E$. Montrer que $f(b)$ est la borne supérieure dans $F$ de $f(X)$ .

**Exercice 2.5** Soit $\mathcal{I}$ l'ensemble des intervalles fermés $[a, b]$ de $\mathbb{R}$ ($a \leq b$), ensemble ordonné par inclusion.

a) Existe-t-il des éléments maximaux, minimaux?

b) Montrer que sur $\mathcal{I}$, on peut définir $sup\{[a, b], [c, d]\}$ pour toute paire d'intervalles.

c) Quelles conditions $[a, b]$ et $[c, d]$ doivent-ils vérifier pour que l'on puisse définir sur $\mathcal{I}$ la borne inférieure de ces intervalles?

**Exercice 2.6** Soient $E$ et $F$ deux ensembles donnés. A toute partie $X$ de $E$, on associe l'ensemble $\mathcal{F}(X, F)$ des applications de $X$ dans $F$. Soit $\Phi$ l'ensemble de ces applications: $\Phi = \{f \mid f \in \mathcal{F}(X, F) \text{ et } X \in \mathcal{P}(E)\}$.

On définit sur $\Phi$ la relation binaire suivante: $f\mathcal{R}f' \Longleftrightarrow X \subset X'$, où $f' \in \mathcal{F}(X', F)$ et $f$ est la restriction de $f'$ à $X$.

Montrer que $\mathcal{R}$ est une relation d'ordre partiel. Quels sont les éléments maximaux de $\Phi$ pour cet ordre ?

# 3 Ensembles finis, dénombrement.

**Exercice 3.1** Démontrer la formule du crible (faire une récurrence).

**Exercice 3.2** Montrer que dans un ensemble infini, on peut trouver des parties de cardinal $n$, pour tout $n \in \mathbb{N}$.

**Exercice 3.3** Soit $E$ un ensemble. Montrer

$$E \text{ fini } \Longleftrightarrow \forall P \subset \mathcal{P}(E),\ P \neq \emptyset, \text{ possède un élément maximal pour l'inclusion.}$$

Indication: pour $\Leftarrow$: considérer l'ensemble des parties finies.

**Exercice 3.4** Soient $N$ un entier naturel non nul et $r \in \mathbb{N}$ . Déterminer le nombre de $N$-uplets d'entiers $(a_1, \cdots, a_N)$ tels que $a_1 + \cdots + a_N = r$.

**Exercice 3.5** Etablir les formules suivantes :

a) $\mathcal{C}_p^p + \mathcal{C}_{p+1}^p + \ldots + \mathcal{C}_n^p = \mathcal{C}_{n+1}^{p+1}$.

b) $\mathcal{C}_n^k \cdot \mathcal{C}_{n-k}^{p-k} = \mathcal{C}_p^k \cdot \mathcal{C}_n^p$.

c) $\mathcal{C}_n^0 \cdot \mathcal{C}_n^p + \mathcal{C}_n^1 \cdot \mathcal{C}_{n-1}^{p-1} + \mathcal{C}_n^2 \cdot \mathcal{C}_{n-2}^{p-2} + \ldots + \mathcal{C}_n^p \cdot \mathcal{C}_{n-p}^0 = 2^p \mathcal{C}_n^p$.

d) $\mathcal{C}_n^0 \cdot \mathcal{C}_n^p - \mathcal{C}_n^1 \cdot \mathcal{C}_{n-1}^{p-1} + \mathcal{C}_n^2 \cdot \mathcal{C}_{n-2}^{p-2} + \ldots (-1)^p \mathcal{C}_n^p \cdot \mathcal{C}_{n-p}^0 = 0$

**Exercice 3.6** Soit $n$ un entier naturel; calculer $\sum_{p=0}^{n} (\mathcal{C}_n^p)^2$.

Plus généralement, établir la formule de Vandermonde:

$$\sum_{l=0}^{min(k,n)} \mathcal{C}_m^{k-l} \mathcal{C}_n^l = \mathcal{C}_{m+n}^k.$$

**Exercice 3.7** Soient $E$ et $F$ deux ensembles de cardinal $n$ et $k$ respectivement.

Déterminer le nombre de surjections $f|E \to F$ (on suppose $n \geq k$). On pourra suivre la démarche suivante.

$*$ Montrer que pour $n \geq k \geq 1$ on a $\sum_{i=1}^{k} C_k^i S_n^i = k^n$, où $S_n^i$ désigne le nombre de surjections d'un ensemble à $n$ éléments sur un ensemble à $i$ éléments.

$*$ Montrer que les égalités précédentes peuvent être décrites par une égalité $AX = Y$, où $A$ est une matrice d'ordre $n \times n$ et $X$ et $Y$ sont deux vecteurs.

$*$ Montrer que $A$ est inversible et que les coefficients $(b_{ij})$ de $A^{-1}$ sont $b_{ij} = (-1)^{i+j} C_i^j$. Expliquer comment on pouvait trouver $A^{-1}$ ?

$*$ Montrer que $S_n^k = \sum_{i=1}^{k} (-1)^{k+i} C_k^i i^n$

**Exercice 3.8** Montrer que $[0,1]$ n'est pas dénombrable. Pour cela, on commencera par construire une application surjective de $[0,1]$ dans $\{0,1\}^{\mathbb{N}}$ (l'ensemble des suites à valeurs dans $\{0,1\}$): penser à la décomposition triadique. Puis justifier qu'il n'y a pas d'application surjective de $\mathbb{N}$ sur $\{0,1\}^{\mathbb{N}}$ ("diagonale de Cantor"). Conclure.

Preuve alternative: supposer que $[0,1] = \{a_n | n \in \mathbb{N}\}$. En coupant $[0,1]$ en trois, un des intervalles (deux le plus souvent) ne contient pas $a_0$, on choisit un de ces intervalles: $I_0$ (on a donc $a_0 \notin I_0$). On coupe $I_0$ en trois et on a de même $a_1 \notin I_1 \subset I_0$. Et ainsi de suite... Conclure.

# 4 Séries Numériques à termes positifs.

**Exercice 4.1** Quelle est la nature de la série de terme général $u_n$ dans les cas suivants

a) $u_n = \dfrac{1}{n+n^2}$.

b) $u_n = \dfrac{1}{n+1}$ si $n$ est pair; et $u_n = \dfrac{1}{n^2}$ si $n$ est impair.

c) $u_n = \dfrac{a^n}{n!}$ où $a \in \mathbb{R}^+$.

d) $u_n = \dfrac{n^n}{n!}$

e) $u_n = \dfrac{(\sqrt{n})^n}{n!}$

**Exercice 4.2** Etudier la série de terme général $u_n = \dfrac{n^\alpha}{(1+a)\dots(1+a^n)}$ où $a > 0$ et $\alpha \in \mathbb{R}$.

**Exercice 4.3** Etudier la série de terme général $u_n = e^{an^2}(1-\dfrac{a}{n})^{n^3}$ où $a > 0$.

**Exercice 4.4** Etudier la série de terme général $u_n = \cos\dfrac{\pi n^2}{2n^2+an+1}$ où $a \geq 0$.

**Exercice 4.5** Etudier la série de terme général $u_n = e^{-\sqrt{n}}$.

**Exercice 4.6** a) Soit $(u_n)$ une suite décroissante de réels telle que $u_n > 0$ pour tout entier $n$. On suppose qu'il existe une suite $(n_k)$ strictement croissante telle que $\forall k$, $u_{n_k} \geq \dfrac{1}{n_k}$. Montrer que la série $\sum_n u_n$ diverge.

b) Soit $(a_n)$ une suite décroissante de réels positifs telle que la série $\sum a_n$ converge. Montrer que $\lim na_n = 0$. Montrer que ce résultat est faux si la suite $(a_n)$ n'est pas décroissante.

**Exercice 4.7** Soit $(a_n)$ une suite de réels positifs.

**a)** On suppose que la série $\sum a_n$ converge. Etudier la convergence des séries de terme général $a_n^2$ ; $\dfrac{\sqrt{a_n}}{n}$ ; $\dfrac{a_n}{1+a_n}$ ; $a_n a_{2n}$.

**b)** On suppose que la série $\sum a_n$ diverge. Etudier la convergence des séries de terme général $a_n^2$ ; $\dfrac{a_n}{1+a_n}$ ; $\dfrac{a_n}{1+na_n}$ ; $\dfrac{a_n}{1+n^2a_n}$ ; $\dfrac{a_n}{a_0+\ldots+a_{n-1}}$ (Indication : comparer $(x-y)/y$ à une intégrale).

**Exercice 4.8** Critère de Duhamel. Soit $(a_n)$ une suite de réels strictement positifs telle que au voisinage de l'infini $\dfrac{a_{n+1}}{a_n} = 1 + \dfrac{\alpha}{n} + o(\dfrac{1}{n})$.

Montrer que si $\alpha < -1$, la série $\sum a_n$ converge; si $\alpha > -1$, la série $\sum a_n$ diverge et pour si $\alpha = -1$, on ne peut conclure.

**Exercice 4.9** Soit $u_n > 0$ le terme général d'une série convergente. On note $C_k$ le cardinal de l'ensemble des entiers $n$ tels que $u_n \geq \dfrac{1}{k}$. Montrer que $C_k = o(k)$.

**Exercice 4.10** Soit $\varphi$ une bijection de $\mathbb{N}$ sur $\mathbb{N}$. Nature de la série $\sum \frac{\varphi(n)}{(n+1)^2}$.

**Exercice 4.11** *Produits infinis.*

1) Soit $(u_n)_n$ une suite de réels avec $u_n > -1$. Montrer que la série de terme général $\log(1 + u_n)$ est absolument convergente si, et seulement si, la série de terme général $u_n$ est absolument convergente.

2) Etant donnée une suite $(a_n)_n$ de réels strictement positifs, on lui associe la suite $P_n = \prod_{k=1}^{n} a_k$. On dit que le produit infini de facteur général $a_n$ converge si la suite $(P_n)_n$ est convergente, sa limite $P$ est appelée le produit infini de la suite $(a_n)_n$ et on note $P = \prod_{k\geq 1} a_k$. On dit que le produit infini est strictement convergent s'il est convergent et $P > 0$.

a) - Montrer que si le produit infini de facteur général $a_n$ est strictement convergent alors la suite $(a_n)_n$ converge vers 1.

b) - Montrer que le produit infini de facteur général $a_n$ est strictement convergent si, et seulement si, la série de terme $\log(a_n)$ est convergente.

**Exercice 4.12** Soit $q_1(n)$ le nombre de chiffres de $n \geq 1$ dans son écriture décimale. On pose $q_k = q_1 \circ q_{k-1}$ pour $k \geq 2$. Nature de la série de terme général

$$a_n = \frac{1}{nq_1(n)\dots q_n(n)}$$

# 5 Arithmétique élémentaire.

**Exercice 5.1** Pour $x \in \mathbb{N}$, montrer que $\sqrt{x} \in \mathbb{Q}$ si et seulement si $x$ est un carré dans $\mathbb{N}$.

**Exercice 5.2** Montrer que $\dfrac{\ln(2)}{\ln(3)} \notin \mathbb{Q}$.

**Exercice 5.3** Montrer que pour chaque entier naturel $n$, 49 divise $2^{3n+3} - 7n - 8$.

**Exercice 5.4** Trouver tous les entiers positifs $a$ tels que $a^{10} + 1$ est divisible par 10.

**Exercice 5.5** Quel est le chiffre des unités de $20082008^{10}$ ? '

**Exercice 5.6** Trouver deux nombres sachant que leur somme est 581 et que le quotient de leur PPCM par leur PGCD est 240.

**Exercice 5.7** Montrer que :

1. Si un entier est de la forme $6k + 5$, alors il est nécessairement de la forme $3k - 1$, alors que la réciproque est fausse.
2. Le carré d'un entier de la forme $5k + 1$ est aussi de cette forme.
3. Le carré d'un entier est de la forme $3k$ ou $3k + 1$, mais jamais de la forme $3k + 2$.
4. Le carré d'un entier est de la forme $4k$ ou $4k + 1$, mais jamais de la forme $4k + 2$ ni de la forme $4k + 3$.
5. Le cube de tout entier est de la forme $9k$, $9k + 1$ ou $9k + 8$.
6. Si un entier est à la fois un carré et un cube, alors c'est une puissance sixième, et il est de la forme $7k$ ou $7k + 1$.

**Exercice 5.8** Déterminer le pgcd des couples d'entiers suivants : $a = 325$ et $b = 312$. $a = 1225$ et $b = 972$. $a = 1104$ et $b = 1260$.

**Exercice 5.9** On souhaite trouver tous les couples $(x, y) \in \mathbb{Z}^2$ vérifiant l'équation

$$325x + 299y = 39. \tag{E}$$

**1)** Quel est le pgcd de 325 et 299 ? Simplifier l'équation $(E)$ sous la forme $ax + by = c$ où $a$ et $b$ sont premiers entre eux.
**2)** Trouver une relation de Bézout entre $a$ et $b$.
**3)** En déduire une solution particulière de $(E)$.
**4)** Trouver toutes les solutions de $(E)$.
**5)** Interprétation géométrique du résultat.

**Exercice 5.10** Résoudre l'équation en nombres entiers : $315x + 273y = 63$.

**Exercice 5.11** On souhaite trouver tous les $q \in \mathbb{Z}$ tels que $e^{i\pi(\frac{1}{6}+\frac{5q}{8})}$ soit une racine neuvième de l'unité.
**1)** Montrer que cela revient à résoudre $16k - 45q = 12$ où $q, k \in \mathbb{Z}$.
**2)** Résoudre cette équation en utilisant la méthode des exercices précédents.

**Exercice 5.12** *Critères de divisibilité.*

Soit $N$ un entier naturel. On note $\rho(N)$ la somme des chiffres dans son écriture décimale.

a) Montrer que $N$ est divisible par 3 si seulement si $\rho(N) \equiv 0[3]$.

b) Montrer que $N$ est divisible par 9 si seulement si $\rho(N) \equiv 0[9]$.

c) Justifier que: pour savoir qu'un entier est divisible par 2, il suffit de savoir que le dernier chiffre de son écriture décimale l'est; pour savoir qu'un entier est divisible par 4, il suffit de savoir que le nombre obtenu avec les deux derniers chiffres de son écriture décimale l'est; pour savoir qu'un entier est divisible par 8, il suffit de savoir que le nombre obtenu avec les trois derniers chiffres de son écriture décimale l'est;...

d) Montrer que $N$ est divisible par 11 si seulement si la différence entre la somme des chiffres de rang pair dans son écriture décimale et la somme des chiffres de rang impair est divisible par 11.

e) Application: calculer $\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)^{20082008}$.

**Exercice 5.13** Soit $n \geq 1$ un entier. Déterminer le nombre de diviseurs de $n$. En déduire que ce nombre est impair si et seulement si $n$ est un carré.

**Exercice 5.14** *Nombres de Mersenne*

Soient $(p, q) \in \mathbb{N}$. Montrer que $2^p - 1$ et $2^q - 1$ divisent $2^{pq} - 1$. En déduire que si $2^n - 1$ est premier, alors $n$ est premier. Étudier la réciproque pour $n = 11$.

**Exercice 5.15** *Nombres parfaits pairs.* On appelle nombre parfait tout entier $N$ égal à la somme de ses diviseurs autres que lui-même (par exemple $6 = 1 + 2 + 3$).

Soit $n \in \mathbb{N}^*$, on note $\sigma(n)$ la somme de tous les diviseurs de $n$.

**1)** Soit $n \in \mathbb{N}^*$, on suppose que $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ est sa décomposition en produits de nombres premiers. Montrer que

$$\sigma(n) = [1 + p_1 + \cdots + p_1^{\alpha_1}] \cdots [1 + p_r + \cdots + p_r^{\alpha_r}]$$

En déduire une expression de $\sigma(n)$ en fonction des diviseurs premiers de $n$ et de leur ordre de multiplicité.

**2)** En déduire que, si $a$ et $b$ sont premiers entre eux, alors $\sigma(ab) = \sigma(a).\sigma(b)$.

**3)** Soit $n \in \mathbb{N}$, montrer que si $2^{n+1} - 1$ est premier alors $2^n(2^{n+1} - 1)$ est parfait.

**4)** Montrer que, réciproquement, tout nombre parfait pair $N$ s'écrit $N = 2^n(2^{n+1} - 1)$ où $2^{n+1} - 1$ est premier.

(Indication : on écrira $N = 2^r.m$ avec $r \geq 1$ et $m$ impair)

Remarque : le problème de déterminer les nombres parfaits impairs est ouvert. En fait, on ne sait même pas s'il en existe.

**Exercice 5.16** Soit $\varphi$ la fonction caractéristique d'Euler : $\varphi(m) = \#\{1 \leq k \leq m |\ k \wedge m = 1\}$ où $m \in \mathbb{N} \setminus \{0\}$.

**a)** Calculer $\varphi(p^\alpha)$ si $p$ est premier et $\alpha \geq 1$.

**b)** Montrer que si $n \wedge m = 1$ alors $\varphi(nm) = \varphi(n)\varphi(m)$. En déduire $\varphi(m)$.

**c)** Soit $n \geq 1$ un entier. Montrer que $\sum_{d|n} \varphi(d) = n$.

**d)** En déduire $\det[i \wedge j]_{1 \leq i,j \leq n}$.

**Exercice 5.17** Montrer qu'un entier $p \geq 2$ est premier si et seulement si $\varphi(p) = p - 1$.

**Exercice 5.18** Montrer que $\underline{\lim}\dfrac{\varphi(n)}{n} = 0$ et $\overline{\lim}\dfrac{\varphi(n)}{n} = 1$.

**Exercice 5.19** Formule d'inversion de Möbius:

Pour tout entier $n \geq 1$, on considère la fonction définie par $\mu(n) = (-1)^r$ si $n$ s'écrit comme produit de $r$ entiers premiers distints; et $\mu(n) = 0$ sinon. On remarque que $\mu(1) = 1$.

1) Calculer $\displaystyle\sum_{\substack{1\leq d\leq n\\ d|n}} \mu(d)$.

Soient $f$ et $g$ deux fonctions définies sur $\mathbb{N}$ à valeurs complexes.

2) Montrer que les deux propriétés suivantes sont équivalentes:

i) Pour tout $n \geq 1$, on a $f(n) = \displaystyle\sum_{\substack{1\leq d\leq n\\ d|n}} g(d)$.

ii) Pour tout $n \geq 1$, on a $g(n) = \displaystyle\sum_{\substack{1\leq d\leq n\\ d|n}} \mu(\frac{n}{d})f(d)$.

3) En déduire que $\displaystyle\sum_{\substack{1\leq d\leq n\\ d|n}} d\mu(\frac{n}{d}) = \varphi(n)$.

**Exercice 5.20** On admet le théorème des nombres premiers:

$$\text{card}\left\{p \,|\, p \text{ premier }, 1 \leq p \leq x\right\} \sim \frac{x}{\ln(x)}$$

quand $x$ tend vers l'infini. En déduire

a) $p_n \sim n\ln(n)$.

b) $\displaystyle\sum_{1<n\leq x} \frac{d_n}{\ln(n)} \sim x$, où $d_n$ est l'écart $p_{n+1} - p_n$.

c) $\underline{\lim}\dfrac{d_n}{\ln(n)} \leq 1 \leq \overline{\lim}\dfrac{d_n}{\ln(n)}$.

d) L'ensemble des quotients de deux nombres premiers est dense dans $\mathbb{R}^+$. Indication: on pourra montrer que pour tout $\alpha > 0$, on peut trouver une suite croissante d'entiers $(n_j)_j$ (mais pas strictement croissante a priori !) telle que $p_{n_j} \sim \alpha j$.

**Exercice 5.21** Résoudre le problème chinois généralisé: soient $m_1, \ldots, m_p$ des entiers premiers entre eux deux à deux. Soient $a_1, \ldots, a_p$ des entiers. Trouver tous les entiers $x$ tels que, pour tout $1 \leq k \leq p$, on a $x \equiv a_k[m_k]$.

Indication : montrer que l'ensemble des solutions est $\{a_1b_1M_1 + \ldots + a_kb_kM_k + NM |\ N \in \mathbb{Z}\}$, où $M_i = \displaystyle\prod_{j\neq i} m_j$; $M = \displaystyle\prod_j m_j$ et $b_i$ est l'inverse de $M_i$ modulo $m_i$.

**Exercice 5.22** (Examen 2007). Dans tout le sujet, la notation $\bar{x}$ désigne la classe de $x$ dans l'ensemble quotient considéré.

I] Soit $p$ un nombre premier impair. On se place dans $\mathbb{Z}/p\mathbb{Z}$. On notera $d = \dfrac{p-1}{2}$.

On considère $S$ l'ensemble des racines du polynôme $X^d - \bar{1}$. On rappelle qu'en raison du degré, le cardinal de $S$ est inférieur à $d$.

Enfin $K = \left\{a^2 |\ a \in \mathbb{Z}/p\mathbb{Z}\right\}$ est l'ensemble des carrés dans $\mathbb{Z}/p\mathbb{Z}$.

1)a) Montrer que l'application $\chi : \{0, \dots, d\} \to K$, qui à un entier $x$ associe $\bar{x}^2$, est bijective.

b) En déduire que $\text{card}(K) = \dfrac{p+1}{2}$.

2) Montrer que $K \setminus \{\bar{0}\} \subset S$. En déduire que $K = \{\bar{0}\} \cup S$.

3) Montrer que $\overline{-1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1[4]$.

II] On introduit l'ensemble $E$ des nombres premiers congrus à 1 modulo 4. On veut montrer que l'ensemble $E$ est infini.

On suppose qu'il est fini et on note $n = \max E$, puis on définit $N = (n!)^2 + 1$.

1) Justifier l'existence de $n$.

2) Montrer qu'il existe un nombre premier impair $p$ divisant $N$.

3) Montrer que $p \in E$.

4) Conclure.

**Exercice 5.23** Soit $p$ un nombre premier. On a vu que $x^{p-1} = \bar{1}$ pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, non nul. Soit $m$ un entier.

1) Montrer que, si $p-1$ ne divise pas $m$ alors il existe $a \in \mathbb{Z}/p\mathbb{Z}$ tel que $a^m \notin \{\bar{0}, \bar{1}\}$.

2) Calculer $\displaystyle\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^m$.

**Exercice 5.24** Soit $n \geq 1$ un entier.

On définit le polynôme cyclotomique $\Phi_d(X) = \displaystyle\prod_{\substack{1 \leq k \leq d \\ k \wedge d = 1}} \left(X - \mathrm{e}^{\frac{2ik\pi}{d}}\right)$.

Montrer que $X^n - 1 = \displaystyle\prod_{d|n} \Phi_d$.

**Exercice 5.25** *Nombres de Carmichaël.* Le (petit) théorème de Fermat affirme que si $n$ premier, on a pour tout entier $a$: $n$ divise $a^n - a$. On appelle nombre de Carmichaël un entier $n$ ayant la même propriété. On qualifie cet entier de *menteur de Fermat* si de plus cet entier n'est pas un nombre premier: ainsi 561 est un menteur de Fermat. On peut le vérifier avec le critère suivant que l'on se propose de démontrer.

I] On va démontrer le *théorème de Korselt*: $n$ est un nombre de Carmichaël si et seulement si $n$ est sans facteur carré et pour tout diviseur premier $p$ de $n$, $p-1$ divise $n-1$.

1) Soit $n$ est un nombre de Carmichaël. On considère un nombre premier $p$ qui divise $n$.

a)i) Justifier que $(p+1)^n \equiv 1[p^2]$.

ii) En déduire que $p^2$ ne divise pas $n$. Indication: remarquer que $(p+1)^n \equiv p+1[n]$.

b)i) Soit $a \geq 2$.

i) Justifier que $a^{n-1} \equiv 1[p]$ pour tout entier $1 \leq a \leq p-1$.

ii) Montrer que $p-1$ divise $n-1$. Indication: faire la division euclidienne.

2) Réciproquement: On suppose que $n = p_1 \dots p_r$, où les $p_i$ sont tous distincts et $r \geq 2$.

i) Montrer que pour tout $a \in \mathbb{Z}$, $a \equiv a^n[p_i]$.

ii) Conclure.

II] Montrer que les menteurs de Fermat ont au moins trois facteurs premiers distincts.