# Colles MP*

Jad ABOU YASSIN

5 janvier 2023

**Topologie**
**Arithmétique**

## Table des matières

# Questions de cours

## Topologie

**Exercice 1 - Application linéaire continue (solution 👈)**
Soient $(E, ||\cdot||_E)$ et $(F, ||\cdot||_F)$ deux espaces vectoriels normés, et $f \in \mathcal{L}(E, F)$. Montrez que $f$ est continue si et seulement si

$$\exists C \geq 0,\ \forall x \in E,\ ||f(x)||_F \leq C\,||x||_E$$

---

**Exercice 2 - Théorème des valeurs intermédiaires (solution 👈)**
Énoncez et démontrez le théorème des valeurs intermédiaires pour une fonction définie sur un espace vectoriel normé.

Bonus : pourquoi les parties connexes par arcs de $\mathbb{R}$ sont les intervalles ?

---

## Arithmétique

**Exercice 3 - Idéaux de $\mathbb{Z}$ (solution 👈)**
Quels sont tous les idéaux de $\mathbb{Z}$ ? Si $a\mathbb{Z}$ et $b\mathbb{Z}$ sont deux idéaux, est-ce que $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$ ? Et $a\mathbb{Z} \cup b\mathbb{Z}$ ? Et $a\mathbb{Z} \cap b\mathbb{Z}$ ? Dans le cas où ce sont des idéaux, exprimez-les sous la forme $c\mathbb{Z}$.

---

**Exercice 4 - Théorème des restes chinois (solution 👈)**
Énoncez les deux versions du théorème des restes chinois vues en cours et démontrez l'une des deux versions. Résoudre le système

$$\begin{cases} x \equiv 2[5] \\ x \equiv 3[7] \end{cases}$$

---

# Exercices

## Topologie

**Exercice 5 - (**) $\mathbb{R}^d \setminus \mathbb{Q}^d$ (solution 👇)**
Montrez que $\mathbb{R}^d \setminus \mathbb{Q}^d$ est connexe par arcs si $d \geq 2$.

---

**Exercice 6 - (**) Ouverts de $\mathbb{R}$ (solution 👇)**
Soit $U$ un ouvert de $\mathbb{R}$.

1. Montrez que les composantes connexes par arcs de $U$ sont des intervalles ouverts
2. En déduire que $U$ est réunion au plus dénombrable disjointe d'intervalles ouverts

---

**Exercice 7 - (**) Connexité par arcs de la sphère unité (solution 👇)**
Soit $E$ un espace vectoriel normé de dimension au moins 2, et éventuellement infinie. Montrez que la sphère unité est connexe par arcs.

---

**Exercice 8 - (**) Connexité dans les espaces de matrices (solution 👇)**

1. Montrez que $GL_n(\mathbb{R})$ n'est pas connexe par arcs.
2. Est-ce que $GL_n(\mathbb{C})$ est connexe par arcs ?
   *Indication :* *On pourra considérer l'application polynomiale* $t \in \mathbb{C} \mapsto \det(tB + (1-t)A)$
3. Montrez que $SL_n(\mathbb{R})$ est connexe par arcs. On admet que les transvections engendrent $SL_n(\mathbb{R})$. Quelles sont les composantes connexes par arcs de $GL_n(\mathbb{R})$ ?

---

**Solution 8 - (**) Connexité dans les espaces de matrices (👉 exercice)**

1. L'application $M \in GL_n(\mathbb{R}) \mapsto \det(M) \in \mathbb{R}^*$ est continue et surjective. Or, $\mathbb{R}^*$ n'est pas connexe par arcs, donc $GL_n(\mathbb{R})$ n'est pas connexe par arcs.
2. Soient $A \neq B \in GL_n(\mathbb{C})$. L'application $\varphi : t \in \mathbb{C} \mapsto \det(tB + (1-t)A)$ est polynomiale, donc n'admet qu'un nombre fini de zéros. De plus, 0 et 1 n'annulent pas $\varphi$ car $\det(A), \det(B) \in \mathbb{C}^*$. Or, $\mathbb{C}$ privé d'un ensemble fini de points est connexe par arcs (pourquoi ?). Ainsi, il existe un chemin $\gamma$ reliant 0 à 1 dans $\mathbb{C}$ tel que pour tout $t \in [0,1]$, $\det(\gamma(t)B + (1-\gamma(t))A) \neq 0$. En particulier, le chemin $\Gamma : t \mapsto \gamma(t)B + (1-\gamma(t))A$ est un chemin reliant $A$ à $B$ dans $GL_n(\mathbb{C})$. Donc $GL_n(\mathbb{C})$ est connexe par arcs.

3. Comme les transvections engendrent $SL_n(\mathbb{R})$, alors pour tout $A, B \in SL_n(\mathbb{R})$, il existe $T_1(\lambda_1), \dots, T_r(\lambda_r)$ et $T_1(\lambda'_1), \dots, T_r(\lambda'_r)$ des transvections telles que $A = T_1(\lambda_1) \dots T_r(\lambda_r)$ et $B = T_1(\lambda'_1) \dots T_r(\lambda'_r)$. Alors le chemin

$$\begin{array}{rccc} \gamma : & [0,1] & \to & SL_n(\mathbb{R}) \\ & t & \mapsto & T_1(t\lambda'_1 + (1-t)\lambda_1) \dots T_r(t\lambda_r + (1-t)\lambda'_r) \end{array}$$

est un chemin continu reliant $A$ à $B$ dans $SL_n(\mathbb{R})$, qui est donc connexe par arcs.

$GL_n(\mathbb{R})$ n'est pas connexe par arcs car tout chemin reliant une matrice de $GL_n(\mathbb{R})^+$ à une matrice de $GL_n(\mathbb{R})^-$ fournit un chemin reliant un élément de $\mathbb{R}_+^*$ à un élément de $\mathbb{R}_-^*$ dans $\mathbb{R}^*$, ce qui n'est pas possible. Montrons que $GL_n(\mathbb{R})^+$ et $GL_n(\mathbb{R})^-$ sont les composantes connexes par arcs de $GL_n(\mathbb{R})$. On le fait seulement pour $GL_n(\mathbb{R})^+$, c'est analogue pour l'autre.

Soit $A$ une matrice de $GL_n(\mathbb{R})^+$. Alors $A = DU$ où $D = \mathrm{diag}(\det(A), 1, \dots, 1)$ et $U \in SL_n(\mathbb{R})$. On peut alors interpoler toute matrice de $GL_n(\mathbb{R})^+$ en une autre matrice de $GL_n(\mathbb{R})^+$, d'où la connexité par arcs.

---

## Arithmétique

**Exercice 9 - (**) Idéaux de $\mathbb{C}[X]$, racines et radicaux (solution ☞)**

Montrez qu'on a une application surjective

$$\{\text{idéaux non triviaux de } \mathbb{C}[X]\} \longrightarrow \{\text{parties finies de } \mathbb{C}\}$$

Cette application est-elle injective ?

Soit $I$ un idéal de $\mathbb{C}[X]$. On appelle le radical de $I$, noté $\mathrm{rad}(I)$, le sous-ensemble de $\mathbb{C}[X]$ défini par :

$$\mathrm{rad}(I) = \{f \in \mathbb{C}[X] \ ; \ \exists n \in \mathbb{N}^*, \ f^n \in I\}$$

Montrez que $\mathrm{rad}(I)$ est un idéal contenant $I$. On dit qu'un idéal est radical s'il est égal à son radical. Montrez que $\mathrm{rad}(I)$ est un idéal radical.

Finalement, montrez qu'un idéal $I$ de $\mathbb{C}[X]$ est radical si et seulement s'il existe $P \in \mathbb{C}[X]$ sans facteurs carrés tel que $I = P\mathbb{C}[X]$. En déduire qu'on a une bijection

$$\{\text{idéaux radicaux non triviaux de } \mathbb{C}[X]\} \longrightarrow \{\text{parties finies de } \mathbb{C}\}$$

---

**Exercice 10 - (**) Bonne année (solution )**

Montrez qu'il n'existe pas de fonction $f : \mathbb{N} \to \mathbb{N}$ telle que pour tout $n \in \mathbb{N}$, $f \circ f(n) = n + 2023$.

---

**Exercice 11 - (**) Cryptosystème RSA (solution )**

Soient $p, q$ deux nombre premiers impairs distincts, et $n = pq$.

1. Rappelez la définition de l'indicatrice d'Euler, puis calculez $\varphi(n)$ en fonction de $p$ et $q$.
2. Soit $e \in (\mathbb{Z}/\varphi(n)\mathbb{Z})^\times$. Comment peut-on calculer $d$ un inverse de $e$ ?
3. Application : Cryptosystème RSA. Soit $M \in \mathbb{Z}/n\mathbb{Z}$ un message qu'Alice veut envoyer à Bob, sans qu'il puisse être lu par autrui. Bob connaît $p$, $q$ et $e$ (qu'on appelle la clé privée, et qui permet en particulier de calculer $n$ et $d$), et envoie $n$ et $d$ à Alice, qu'on appelle la clé publique. Alice calcule ensuite $N = M^d\ [n]$, et envoie le résultat à Bob. Montrez que Bob peut retrouver le message en calculant $N^e\ [n]$. Pourquoi il sera très difficile pour une personne ne connaissant pas la clé privée de modifier le message ?

---

# Solutions des exercices

**Solution 1 - Application linéaire continue (☞ exercice)**
TODO

---

**Solution 2 - Théorème des valeurs intermédiaires (☞ exercice)**
Soit $X$ une partie connexe par arcs d'un espace vectoriel normé, et $f : X \to \mathbb{R}$ continue. Alors l'image de $f$ est un intervalle. En particulier, si $a < b \in f(X)$, alors $[a, b] \in f(X)$.

Preuve : L'image d'un connexe par arcs par une application continue est connexe par arcs. En effet, soit $f(x), f(y) \in f(X)$. Comme $X$ est connexe par arcs, alors il existe $\gamma : [0, 1] \to X$ un chemin continu reliant $x$ à $y$. Alors $f \circ \gamma$ est un chemin continu reliant $f(x)$ à $f(y)$ dans $f(X)$. Donc $f(X)$ est connexe par arcs.

---

**Solution 3 - Idéaux de $\mathbb{Z}$ (☞ exercice)**
$\mathbb{Z}$ est un anneau principal, donc tous ses idéaux sont de la forme $c\mathbb{Z}$ où $c \in \mathbb{Z}$. La somme de deux idéaux est un idéal, en effet, si $I, J$ sont deux idéaux d'un anneau $A$, alors $I + J$ est un sous-groupe additif de $A$ et et si $x \in A$, $i + j \in I + J$, alors $x(i + j) = xi + xj \in I + J$. De même pour l'intersection, $I \cap J$ est un sous-groupe additif de $A$ et si $x \in A$ et $y \in I \cap J$, alors $xy \in I$ et $xy \in J$ donc $xy \in I \cap J$. Pour l'union, c'est faux cependant, simplement parce que l'union de deux groupes n'est en général pas un groupe (en fait, c'est le cas si et seulement si l'un est contenu dans l'autre). En fait, $I + J$ est l'idéal engendré par $I \cup J$.

De plus, on a : $a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a, b)\mathbb{Z}$. En effet,

$$x \in a\mathbb{Z} \cap b\mathbb{Z} \Leftrightarrow x \in a\mathbb{Z} \text{ et } x \in b\mathbb{Z} \Leftrightarrow a|x \text{ et } b|x \Leftrightarrow \text{ppcm}(a, b)|x \Leftrightarrow x \in \text{ppcm}(a, b)\mathbb{Z}$$

et

$$x \in a\mathbb{Z} + b\mathbb{Z} \Leftrightarrow \exists n, m \in \mathbb{Z},\ x = an + bm \Leftrightarrow \text{pgcd}(a, b)|x \Leftrightarrow x \in \text{pgcd}(a, b)\mathbb{Z}$$

---

**Solution 4 - Théorème des restes chinois (☞ exercice)**
Preuve : Il suffit de montrer que l'application

$$\begin{array}{rccc} \varphi : & \mathbb{Z}/(nm)\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & [x]_{nm} & \mapsto & ([x]_n, [x]_m) \end{array}$$

est injective si $n \wedge m = 1$. On a $([x]_n, [x]_m) = (0,0)$ si et seulement si $n|x$ et $m|x$. Comme $n \wedge m = 1$, alors $nm|x$. Donc $[x]_{nm} = 0$.

Pour résoudre ce système, on calcule l'application réciproque de $\varphi$. On résout d'abord les deux systèmes

$$\begin{cases} x_1 \equiv 1[5] \\ x_1 \equiv 0[7] \end{cases} \quad \text{et} \quad \begin{cases} x_2 \equiv 0[5] \\ x_2 \equiv 1[7] \end{cases}$$

On trouve $x_1 = 21$ par l'algorithme d'EUCLIDE, et $x_2 = 15$. Donc $x = 2x_1 + 3x_2 = 87$ convient. On peut aussi réduire $x$ modulo 35 pour obtenir 17 comme solution dans $[\![0, 34]\!]$.

---

**Solution 5 - (**) $\mathbb{R}^d \setminus \mathbb{Q}^d$ (☞ exercice)**

Soient $x, y \in \mathbb{R}^d \setminus \mathbb{Q}^d$. On considère $H$ l'hyperplan affine de $\mathbb{R}^d$ orthogonal à $x - y$ et passant par $(x+y)/2$. On considère pour tout $z \in H$, le chemin $\gamma_z$ défini par :

$$\forall t \in [0,1], \quad \gamma_z(t) = \begin{cases} 2tz + (1-2t)x & \text{si } t \leq 1/2 \\ (2t-1)y + 2(1-t)z & \text{si } t \geq 1/2 \end{cases}$$

Soit $I_z = \gamma_z(]0,1[)$. Il est clair que si $z \neq z' \in H$, alors $I_z \cap I_{z'} = \emptyset$. On suppose par l'absurde que pour tout $z \in H$, il existe $q_z \in \mathbb{Q}^d$ tel que $q_z \in I_z$. On a donc une injection $H \hookrightarrow \mathbb{Q}^d$ $(z \mapsto q_z)$. Or, $H$ est un hyperplan de $\mathbb{R}^d$, donc de dimension $\geq 1$ car $d \geq 2$. Ainsi, il est infini non dénombrable, ce qui est absurde. Donc il existe $z \in H$ tel que $I_z \cap \mathbb{Q}^d = \emptyset$, donc le chemin $\gamma_z$ est à valeurs dans $\mathbb{R}^d \setminus \mathbb{Q}^d$ et relie $x$ à $y$. Donc $\mathbb{R}^d \setminus \mathbb{Q}^d$ est connexe par arcs.

---

**Solution 6 - (**) Ouverts de $\mathbb{R}$ (☞ exercice)**

1. Soit $C$ une composante connexe par arcs de $U$. Soit $x \in C$. Comme $U$ est ouvert, il existe $r > 0$ tel que $B(x,r) \subset U$. Or, une boule est connexe par arcs, donc $B(x,r) \subset C$. Donc $C$ est voisinage de tous ses points, donc $C$ est ouvert. De plus, $C$ étant une partie connexe par arcs de $\mathbb{R}$, $C$ est un intervalle. Donc c'est un intervalle ouvert.
2. $U$ est réunion disjointe de ses composantes connexes par arcs (car l'intersection de deux composantes connexes par arcs distinctes sont disjointes), donc réunion d'intervalles ouverts. Il reste à montrer que cette réunion est finie ou dénombrable. Par densité de $\mathbb{Q}$ dans $\mathbb{R}$, on a une application injective

$$\begin{array}{rccc} \varphi : & \{\text{composantes connexes de } U\} & \longrightarrow & \mathbb{Q} \\ & C & \longmapsto & \text{un élément quelconque} \end{array}$$

Donc $U$ n'admet qu'un nombre fini de composantes connexes par arcs.

---

**Solution 7 - (**) Connexité par arcs de la sphère unité (☞ exercice)**

Soient $x, y \in \mathbb{S}$. On suppose dans un premier temps que $y \notin \{x, -x\}$. Alors l'application $t \in [0,1] \mapsto ||ty + (1-t)x||$ ne s'annule pas et est continue. On considère alors le chemin

$$\begin{array}{rccc} \gamma : & [0,1] & \to & \mathbb{S} \\ & t & \mapsto & \dfrac{ty + (1-t)x}{||ty + (1-t)x||} \end{array} \tag{1}$$

qui est bien défini par ce qui précède, continue, à valeurs dans $\mathbb{S}$ et relie $x$ à $y$.

Il reste à traiter le cas où $x = -y$. Comme $E$ est de dimension $\geq 2$, il existe $z \in \mathbb{S} \setminus \{x, -x\}$. Par ce qui précède, on peut relier $x$ à $z$ et $z$ à $-x$

---

**Solution 9 - (**) Idéaux de $\mathbb{C}[X]$, racines et radicaux (☞ exercice)**

Comme $\mathbb{C}[X]$ est principal, tous ses idéaux sont principaux. Soit $I$ un idéal de $\mathbb{C}[X]$ non trivial. Il existe $P \in \mathbb{C}[X]$ non nul tel que $I = P\mathbb{C}[X]$. On associe à $I$ l'ensemble des racines de $P$, c'est une partie finie de $\mathbb{C}$. Cet ensemble est bien défini (ne dépend que de $I$, pas du $P$ choisi) car $P\mathbb{C}[X] = Q\mathbb{C}[X] \Leftrightarrow P = \alpha Q$ où $\alpha \in \mathbb{C}^*$, donc $P$ et $Q$ ont même ensemble de racines. Cette application est surjective car si $\{z_1, \ldots, z_k\}$ est une partie finie de $\mathbb{C}$, alors l'idéal $(X - z_1) \ldots (X - z_k)\mathbb{C}[X]$ en est un antécédent.

Par contre, elle n'est pas injective, car $X\mathbb{C}[X]$ et $X^2\mathbb{C}[X]$ ont même image (le singleton $\{0\}$) mais ne définissent pas les mêmes idéaux, car $X \in X\mathbb{C}[X]$ mais $X \notin X^2\mathbb{C}[X]$.

$\mathrm{rad}(I)$ contient évidemment $I$ en prenant $n = 1$ dans la définition de l'idéal radical de $I$. De plus, c'est bien un idéal car si $f, g \in \mathrm{rad}(I)$, on a $n, m \in \mathbb{N}^*$ tels que $f^n \in I$ et $g^m \in I$, alors :

$$(f+g)^{n+m} = \sum_{k=0}^{n+m} \binom{n}{k} f^k g^{n+m-k} = \underbrace{\sum_{k=0}^{n} \binom{n}{k} f^k \underbrace{g^{n+m-k}}_{\in I}}_{\in I} + \underbrace{\sum_{k=n+1}^{n+m} \binom{n}{k} \underbrace{f^k}_{\in I} g^{n+m-k}}_{\in I} \in I$$

Donc $f + g \in \mathrm{rad}(I)$ est bien un sous-groupe de $\mathbb{C}[X]$. Et de plus, si $f \in \mathrm{rad}(I)$ et $g \in \mathbb{C}[X]$, alors $(fg)^n = f^n g^n \in I$ si $n$ est tel que $f^n \in I$. Donc $fg \in \mathrm{rad}(I)$. C'est donc bien un idéal de $\mathbb{C}[X]$.

Montrons que $\mathrm{rad}(\mathrm{rad}(I)) = \mathrm{rad}(I)$. L'inclusion $\boxed{\supset}$ est claire par ce qui précède. Soit $f \in \mathrm{rad}(\mathrm{rad}(I))$. Alors il existe $n \in \mathbb{N}^*$ tel que $f^n \in \mathrm{rad}(I)$. Donc il existe $m \in \mathbb{N}^*$ tel que $f^{nm} \in I$. Donc $f \in \mathrm{rad}(I)$. Donc les radicaux d'idéaux sont des idéaux radicaux.

Soit maintenant $I$ un idéal radical de $\mathbb{C}[X]$. On a $P \in \mathbb{C}[X]$ tel que $I = P\mathbb{C}[X]$ car $\mathbb{C}[X]$ est un

idéal principal. On note $P = \prod (X - \alpha_i)^{m_i}$ où les $\alpha_i$ sont deux à deux distincts. Montrons que tous les $m_i$ sont égaux à 1. Soit $Q$ le polynôme radical de $P$ (oui ça s'appelle aussi radical, et ça va être très clair pourquoi), c'est-à-dire $P$ mais auquel on a retiré toutes les multiplicités des facteurs : $Q = \prod (X - \alpha_i)$. Alors $Q \in \mathrm{rad}(I)$ car $Q^{\max m_i} \in I$. Or, $I$ est radical, donc $Q \in I$. Mais alors, $P$ divise $Q$. Ceci n'est possible que si tous les $m_i$ valent 1 (par un argument de degré par exemple). Donc $P$ est sans facteurs carrés.

Réciproquement, si $P$ est sans facteurs carrés, et si $Q \in \mathbb{C}[X]$ vérifie $Q^n \in P\mathbb{C}[X]$ pour un certain $n \in \mathbb{N}^*$, alors $P$ divise $Q^n$. On écrit $P = \prod (X - \alpha_i)$ (où les $\alpha_i$ sont deux à deux distincts). Alors pour tout $i$, $X - \alpha_i$ divise $Q^n$, donc divise $Q$. Ainsi, $P$ divise $Q$ et donc $Q \in I$. Donc $I$ est radical.

Finalement, si on restreint l'ensemble de départ aux idéaux radicaux (non triviaux), l'application devient injective. En effet, si $P$ et $Q$ sont sans facteurs carrés (pour définir des idéaux radicaux) et non proportionnels (pour définir deux idéaux distincts), alors ils ont des racines distinctes. L'application reste surjective car les antécédents construits au début de l'exercice sont des idéaux radicaux. Ainsi, on obtient bien la bijection voulue.

---

**Solution 10 - (**) Bonne année (☞ exercice)**

On a pour tout $n \in \mathbb{N}$, $f(n + 2023) = f(f(f(n))) = f(n) + 2023$. Ainsi, l'application $f$ définit une application $\overline{f} : \mathbb{Z}/2023\mathbb{Z} \to \mathbb{Z}/2023\mathbb{Z}$ par $\overline{f}(\overline{n}) = \overline{f(n)}$.

Comme $f(f(n)) = n$ [2023], alors $\overline{f}^2 = \mathrm{id}_{\mathbb{Z}/2023\mathbb{Z}}$. Ainsi, $\overline{f} \in \mathfrak{S}_{2023}$ est d'ordre 2, donc admet un point fixe car 2023 est impair.

Ainsi, il existe $n_0 \in \mathbb{N}$ tel que $\overline{f}(\overline{n_0}) = \overline{n_0}$, c'est-à-dire que $\overline{f(n_0)} = \overline{n_0}$, et donc que $f(n_0) = n_0 + 2023k$ pour un certain $k \in \mathbb{Z}$. Donc $f \circ f(n_0) = f(n_0 + 2023k) = f(n_0) + 2023k = n_0 + 2023$. Donc $f(n_0) = n_0 + 2023(1 - k)$ : c'est absurde. Donc une telle fonction ne peut pas exister.

---

**Solution 11 - (**) Cryptosystème RSA (☞ exercice)**

1. Si $n \in \mathbb{N}^*$, on définit $\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$. De manière équivalente, il s'agit du nombre d'éléments de $[\![1, n]\!]$ premiers à $n$. En particulier, on a $\varphi(pq) = (p-1)(q-1)$. En effet, les seuls éléments de $[\![1, pq]\!]$ non premiers à $pq$ sont les multiples de $p$ ou de $q$, et il y en a $p + q - 1$ (ce sont $p, 2p, \ldots, qp$ et $q, 2q, \ldots qp$, moins $qp$ qu'on a compté deux fois). Donc $\varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$. Une autre méthode pour démontrer cette égalité et de montrer que $\varphi$ est multiplicative, et que pour $p$ premier on a $\varphi(p) = p - 1$.
2. On peut utiliser l'algorithme d'Euclide pour trouver un inverse de $e$ modulo $n$.

3. On a

$$N^e \equiv M^{de}\ [p] \equiv M^{1+k\varphi(n)}\ [p] \equiv M(M^{k(q-1)})^{p-1}\ [p] \equiv M\ [p]$$

De même avec $q$. Comme $p$ et $q$ sont premiers entre eux, alors par le théorème des restes chinois, on a

$$N^e \equiv M\ [n]$$

Bob peut donc retrouver le message. Il sera très difficile pour une tierce personne de modifier le message car celle-ci doit calculer $d$, un inverse de $e$ modulo $\varphi(n)$, et donc pouvoir calculer $\varphi(n)$ sans connaître $p$ et $q$. Si $p$ et $q$ sont assez grands, il s'agit d'une opération très difficile à faire. Ceci permet d'assurer la sécurité du cryptosystème RSA.