Devoir Maison N°8

Arithmétique

Problème 1 — Les bases du codage RSA

1) **Congruences et exponentiation rapide**

   a) Déterminer le PGCD et les coefficients de Bezout des entiers 27 et 112.

   b) On pose $a = 12$. Calculer a^2, puis a^4, puis a^8 et enfin a^{16} modulo 145.

   c) Déduire de ce qui précède la valeur de 12^{27} modulo 145.

2) **Questions de cours**

   a) Rappeler la définition d'entiers premiers entre eux. Rappeler la définition de nombre premier.

   b) Soient a et b deux entiers. A quelle condition sur a et b l'entier a est-il inversible modulo b ? Donner, en justifiant brièvement votre réponse, un inverse de 27 modulo 112, ainsi qu'un inverse de 112 modulo 27.

   c) Etablir que si p et q sont deux nombres premiers distincts, alors ils sont premiers entre eux.

   d) Soit p un nombre premier. Le petit théorème de Fermat affirme que : $\forall\, a \in \mathbb{Z},\ a^p \equiv a\ [p]$.

   Redémontrer alors que : $\forall\, a \in \mathbb{Z}\backslash p\mathbb{Z},\ a^{p-1} \equiv 1\ [p]$.

3) **Une nouvelle conséquence du théorème de Fermat**. Soient p et q deux nombres premiers distincts, et soit $N = pq$.

   a) Montrer que a est premier avec N si et seulement si a est premier avec p et avec q.

   b) On suppose que a est premier avec N. Montrer que $a^{(p-1)(q-1)} \equiv 1\ [p]$ et $a^{(p-1)(q-1)} \equiv 1\ [q]$.

   c) Déduire de la question précédente que $a^{(p-1)(q-1)} \equiv 1\ [N]$.

4) On pose $\varphi(N) = (p-1)(q-1)$. Soit e un entier naturel premier avec $\varphi(N)$. Justifier qu'il existe un entier d tel que $ed \equiv 1\ [\varphi(N)]$.

5) Soit m un entier naturel.

   a) Montrer que si m est premier avec N, alors $m^{ed} \equiv m\ [N]$.*

   b) Montrer que pour tout entier m, on a $m^{ed} \equiv m\ [N]$.

   c) **"Vérification"**. Dans cette question, on prend $p = 5$, $q = 29$, $m = 12$ et $e = 27$. Donner sans justification la valeur de d. Déterminer la valeur de m^e modulo N, puis détailler le calcul de $(m^e)^d$ modulo N.

---

*. Où e et d sont ceux définis dans la question 4, et $N = pq$ avec p et q premiers distincts.

Problème 2 — Indicatrice d'Euler et probabilités

Notations et rappels de terminologie. On appelle espace probabilisé (Ω, P) la donnée d'un ensemble Ω (appelé univers) et d'une probabilité P sur $\mathscr{P}(\Omega)$. Les éléments de Ω sont appelés issues, et les parties de Ω évènements.

Un évènement A étant donné, on note $\Omega\backslash A$ (plutôt que $\overline{A}$) l'évènement contraire de A.

Deux évènements A et B sont dits indépendants lorsque : $P(A\cap B) = P(A)\times P(B)$. Cette définition admet la généralisation suivante.

Définition. Soit n un entier $\geqslant 2$, et soit $A_1,\ldots, A_n$ une famille de n évènements.
Les évènements $A_1,\ldots, A_n$ sont **mutuellement indépendants** si pour tout entier j compris entre 2 et n, et pour toute famille d'indices deux à deux distincts $i_1,\ldots, i_j$ dans $[\![\, 1, n\,]\!]$ on a :

$$P\left(\bigcap_{k=1}^{j} A_{i_k}\right) = \prod_{k=1}^{j} P\left(A_{i_k}\right)$$

Partie I — Probabilités

Soit (Ω, P) un espace probabilisé.(deux parties de Ω)

1) Soient A et B deux évènements.

a) Etablir que : $A\cap(\Omega\backslash B) = A\backslash(A\cap B)$.

b) Etablir que A et B sont indépendants si et seulement si A et $\Omega\backslash B$ sont indépendants.

c) En déduire que A et B sont indépendants si et seulement si $\Omega\backslash A$ et $\Omega\backslash B$ sont indépendants.

2) Soit $(A_i)_{i\in[\![1,n]\!]}$ une famille de n évènements (avec $n\in\mathbb{N}$, $n\geqslant 2$) mutuellement indépendants.

a) Etablir que les évènements $\Omega\backslash A_1,\ A_2,\ldots,\ A_n$ sont mutuellement indépendants.

b) En déduire que les évènements $\Omega\backslash A_1, \Omega\backslash A_2,\ldots,\Omega\backslash A_n$ sont mutuellement indépendants.

Partie II — Indicatrice d'Euler

Soit $n\geqslant 2$ un entier naturel. On choisit de manière équiprobable un entier compris entre 1 et n.

Soient p un diviseur positif de n, et A_p l'évènement : "l'entier choisi est divisible par p".

3) Calculer $P(A_p)$.

4) On note $p_1,\ldots, p_r$ les diviseurs premiers de n.

a) Soit m un entier naturel. Etablir que $[\forall\, i\in[\![\, 1, r\,]\!],\ p_i|m\,] \iff \left[\left(\prod_{i=1}^{r} p_i\right)|m\right]$

b) Etablir que les évènements $A_{p_1}, \ldots, A_{p_r}$ sont mutuellement indépendants.

5) On note $\varphi(n)$ (l'indicatrice d'Euler) le nombre d'entiers compris entre 1 et $(n-1)$ qui sont premiers avec n :

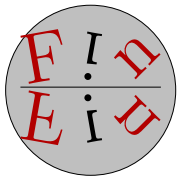
$$\varphi(n) = \text{Card}\left\{k \in [\![\, 1, n-1 \,]\!] \ / \ k \wedge n = 1\right\}$$

On note désormais A l'évènement "l'entier choisi est premier avec n".

Calculer $P(A)$, et en déduire que : $\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

6) Dans cette ultime question, n et m désignent deux entiers $\geqslant 2$.

Etablir que : $[n \wedge m = 1] \Longrightarrow [\varphi(nm) = \varphi(n)\varphi(m)]$



Corrigé

Problème 2 — Les bases du codage RSA

1) 1) a) On applique l'algorithme d'Euclide aux entiers 27 et 112.

$112 = 27 \times 4 + 4$
$27 = 4 \times 6 + 3$
$4 = 3 \times 1 + 1$
$3 = 3 \times 1 + 0$

On en déduit déjà que $\boxed{27 \wedge 112 = 1}$.

$1 = 4 - 3 \times 1$
$1 = 4 - \times(27 - 4 \times 6) = 7 \times 4 - 1 \times 27$
$1 = 7 \times (112 - 4 \times 27) - 1 \times 27$ soit finalement :
$\boxed{1 = 7 \times 112 - 29 \times 27}$

On a donc obtenu une relation de Bezout pour les entiers 27 et 112, c'est-à-dire deux entiers u et v tels que $27u + 112v = 27 \wedge 112$ avec $\boxed{u = -29 \text{ et } v = 7}$.

b) $\boxed{a = 12 \text{ donc } a \equiv 12\ [145]}$; $a^2 = 144$ donc $\boxed{a^2 \equiv -1\ [145]}$.

Il s'ensuit que $\boxed{a^4 \equiv a^8 \equiv a^{16} \equiv 1\ [145]}$.

c) On peut observer que : $27 = 16+8+2+1$ pour écrire : $a^{27} = a^{16} \times a^8 \times a^2 \times a$ d'où : $a^{27} \equiv 12 \times -1\ [145]$. Par suite : $\boxed{12^{27} \equiv -12\ [145]}$.

2) a) Deux entiers a et b sont premiers entre eux si leur PGCD est égal à 1 (il est équivalent de dire que leurs seuls diviseurs communs sont 1 et -1, ou encore que leur seul diviseur commun dans $\mathbb{N}$ est 1).

Un entier naturel n est premier s'il admet exactement deux diviseurs dans $\mathbb{N}$: 1 et lui-même.

b) D'après le cours, un entier a est inversible modulo b si et seulement si a et b sont premiers entre eux.

D'après la question 1-a, un inverse de 27 modulo 112 est -29, et un inverse de 112 modulo 27 est 7.

c) Puisque p (*resp.* q) est premier, il admet exactement 1 et p (*resp.* 1 et q) comme diviseurs dans $\mathbb{N}$. Par conséquent, p et q admettent 1 comme unique diviseur commun dans $\mathbb{N}$. Donc $\boxed{p \text{ et } q \text{ sont premiers entre eux}}$.

d) Soient p un nombre premier, et a un entier tel que p ne divise pas a.

D'après le théorème de Fermat : $a^p \equiv a\ [p]$. Il est équivalent de dire que : $p|a^p - a$, soit : $p|a\,(a^{p-1} - 1)$. Comme p ne divise pas a et que p est premier, p est premier avec a (en vertu de la propriété : "tout nombre premier est premier avec tout entier qu'il ne divise pas"). D'après le lemme de Gauss, il s'ensuit que $p|a^{p-1} - 1$, c'est à dire : $\boxed{a^{p-1} \equiv 1\ [p]}$.

3) a) Sens direct : supposons a premier avec pq. Alors (théorème de Bezout), il existe deux entiers u et v tels que : $au + vpq = 1$. En écrivant cette relation $au + p(vq) = 1$, on en déduit que a et p sont premiers entre eux ; et en l'écrivant $au + q(vp) = 1$, on en déduit que a et q sont premiers entre eux.

Conclusion : (a premier avec $N = pq$) implique (a premier avec p et q).

Réciproquement : supposons a premier avec p et a premier avec q. Les diviseurs de pq dans $\mathbb{N}$ sont 1, p, q et pq. On sait déjà que p ne divise pas a (a et p étant premiers entre eux) et que q ne divise pas a (a et q étant premiers entre eux). A fortiori, pq ne divise pas a, puisque si tel était le cas p et q diviseraient a. Il s'ensuit que a et pq ont un unique diviseur commun dans $\mathbb{N}$ (qui est 1). Donc a et pq sont premiers entre eux.

Conclusion : (a premier avec p et q) implique (a premier avec $N = pq$).

$\boxed{\text{En résumé : } (a \text{ premier avec } p \text{ et } q) \text{ SSI } (a \text{ premier avec } N = pq)}$.

b) Puisque a est premier avec N, alors d'après la question précédente, a est premier avec p et q.

Par suite : $a^{p-1} \equiv 1\ [p]$ et $a^{q-1} \equiv 1\ [q]$.
On en déduit que : $a^{(p-1)(q-1)} \equiv (a^{p-1})^{q-1} \equiv 1^{q-1} \equiv 1\ [p]$; et symétriquement : $a^{(p-1)(q-1)} \equiv 1\ [q]$.

En déduit de ces deux congruences que : $p|a^{(p-1)(q-1)}-1$ et $q|a^{(p-1)(q-1)}-1$. Or les entiers p et q sont premiers entre eux, puisque ce sont deux nombres premiers distincts. Donc : $(pq)\,|a^{(p-1)(q-1)}-1$, ce qui se traduit par la congruence : $\boxed{a^{(p-1)(q-1)} \equiv\ 1\ [pq]}$.

4) Puisque e est premier avec $\varphi(N)$, il existe d'après le théorème de Bezout deux entiers d et v tels que : $ed + v\varphi(N) = 1$. Cette égalité implique la congruence : $\boxed{ed \equiv\ 1\ [\varphi(N)]}$, d'où la conclusion.

5) a) Par définition des entiers e et d, il existe un entier k tel que : $ed = 1 + k\varphi(N)$, soit encore : $1 + k\,(p-1)\,(q-1)$.
On peut ainsi écrire : $m^{ed} = m^{1+k(p-1)(q-1)}$ soit : $m^{ed} = \left(m^{(p-1)(q-1)}\right)^k \times m$. Or $m^{(p-1)(q-1)} \equiv 1\ [pq]$ d'après la question 3-b et puisque m est premier avec N. On en déduit que $\boxed{m^{ed} \equiv m\ [N]}$.

b) Supposons à présent que m ne soit pas premier avec N. D'après la question 3-a, il revient au même de dire que $p|m$ ou $q|m$. Supposons donc que m soit divisible par p. Alors $m \equiv 0\ [p]$ donc $m^{1+(p-1)(q-1)} \equiv 0\ [p]$. en particulier $m^{ed} \equiv m\ [p]$. Si m est également divisible par q, alors le même raisonnement entraîne : $m^{ed} \equiv m\ [q]$. Et si q ne divise pas m, alors $m^{ed} \equiv m\ [q]$ (conséquence du théorème de Fermat).

En résumé, dans tous les cas, on a $m^{ed} \equiv m\ [p]$ et $m^{ed} \equiv m\ [q]$. Il s'ensuit que p et q divisent $m^{ed} - m$, donc (p et q étant premiers entre eux) pq divise $m^{ed} - m$. D'où $\boxed{\forall\, m \in \mathbb{Z},\ m^{ed} \equiv m\ [N]}$.

c) Avec les notations et données de l'énoncé : $p - 1 = 4$ et $q - 1 = 28$ d'où $\varphi(N) = 112$. En outre, on a $e = 27$ et l'entier d recherché doit vérifier $ed \equiv 1\ [\varphi(N)]$, càd : $27d \equiv 1\ [112]$. D'après la question 1-a), $d = -29$ fait l'affaire, tout comme $d = 83$ (puisque $-29 \equiv 83\ [112]$).

En posant $m = 12$, on a : $m^e = 12^{27}$, et on sait d'après la question $12^{27} \equiv -12\ [145]$.

Calculons à présent $(m^e)^d$ modulo 145. D'après ce qui précède $(m^e)^d \equiv (-12)^{83}\ [145]$.

Or : $(-12)^{83} \equiv \underbrace{\left[(-12)^4\right]^{20}}_{\equiv 1\ [145]} (-12)^3 \equiv -12^3 \equiv 12^2 \times (-12) \equiv (-1) \times (-12) \equiv 12\ \ [145]$

Par suite : $\boxed{\left(12^{27}\right)^{83} \equiv 12\ [145]}$

Problème 3 — Indicatrice d'Euler et probabilités

Partie I — Probabilités

1. Soient A et B deux évènements.

a. Soit $x \in A \cap (\Omega \backslash B)$. Alors $x \in A$ et $x \notin B$. Donc : $x \in A$ et $x \notin A \cap B$. D'où : $x \in A \backslash (A \cap B)$. Ce qui prouve l'inclusion : $\boxed{A \cap (\Omega \backslash B) \subset A \backslash (A \cap B)\ \ (\spadesuit)}$.

Réciproquement, soit $x \in A \backslash (A \cap B)$. Alors $x \in A$ et $x \notin B$. Donc $x \in A$ et $x \in \Omega \backslash B$. Donc : $x \in A \cap (\Omega \backslash B)$. D'où : $\boxed{A \backslash (A \cap B) \subset A \cap (\Omega \backslash B)\ \ (\clubsuit)}$.

D'après ($\spadesuit$), ($\clubsuit$) et la règle de double inclusion : $\boxed{A \backslash (A \cap B) = A \cap (\Omega \backslash B)}$.

b. Supposons A et B indépendants. Alors :

$$P\left(A\cap(\Omega\backslash B)\right)=P\left(A\backslash(A\cap B)\right)=P(A)-P\left(A\cap B\right)=P(A)-P(A)P(B)=P(A)\left(1-P(B)\right).$$

D'autre part : $P(A)P(\Omega\backslash B)=P(A)\left(1-P(B)\right)$.

Donc : $P\left(A\cap(\Omega\backslash B)\right)=P(A)P(\Omega\backslash B)$. Ce qui signifie que les évènements A et $\Omega\backslash B$ sont indépendants.

Ainsi : $\boxed{[A \text{ et } B \text{ indépendants}]\Longrightarrow[A \text{ et } \Omega\backslash B \text{ indépendants}]\ (\spadesuit)}$.

Réciproquement, supposons A et $\Omega\backslash B$ indépendants. Alors d'après l'implication précédente, les évènements A et $\Omega\backslash\left(\Omega\backslash B\right)$ sont indépendants. Puisque $\Omega\backslash\left(\Omega\backslash B\right)=B$, on en déduit que A et B sont indépendants. Ce qui prouve : $\boxed{[A \text{ et } \Omega\backslash B \text{ indépendants}]\Longrightarrow[A \text{ et } B \text{ indépendants}]\ (\clubsuit)}$.

$\boxed{\textbf{Conclusion}.\ [A \text{ et } B \text{ indépendants}]\Longleftrightarrow[A \text{ et } \Omega\backslash B \text{ indépendants}]}$.

c. D'après la question précédente, les évènements A et B sont indépendants SSI les évènements A et $\Omega\backslash B$ sont indépendants.

D'après cette même question, les évènements A et $\Omega\backslash B$ sont indépendants SSI les évènements $\Omega\backslash A$ et $\Omega\backslash B$ sont indépendants. §

On en déduit que : $\boxed{[A \text{ et } B \text{ indépendants}]\Longleftrightarrow[\Omega\backslash A \text{ et } \Omega\backslash B \text{ indépendants}]}$.

2. Soit $(A_i)_{i\in[\![1,n]\!]}$ une famille de n évènements (avec $n\in\mathbb{N}$, $n\geqslant 2$) mutuellement indépendants.

a. Notons $A'_1=\Omega\backslash A_1$, et pour tout entier $i\in[\![\,2,n\,]\!]$, $A'_i=A_i$.

Soit J une partie non vide de $[\![\,1,n\,]\!]$ (J est une famille d'indices).

Si $1\notin J$, alors : $P\left(\bigcap_{j\in J}A'_j\right)=P\left(\bigcap_{j\in J}A_j\right)=\prod_{j\in J}P\left(A_j\right)$; la première égalité provenant de la définition des A'_j, la seconde de l'hypothèse suivant laquelle la famille $(A_i)_{i\in[\![1,n]\!]}$ est constituée d'évènements mutuellement indépendants.

Si $1\in J$ (et si $\mathrm{card}(J)\geqslant 2\ldots$), on a :

$$\bigcap_{j\in J}A'_j=A'_1\cap\left(\bigcap_{j\in J\backslash\{1\}}A'_j\right)=(\Omega\backslash A_1)\cap\left(\bigcap_{j\in J\backslash\{1\}}A_j\right)=\left(\bigcap_{j\in J\backslash\{1\}}A_j\right)\backslash\left(\left(\bigcap_{j\in J\backslash\{1\}}A_j\right)\cap A_1\right)$$

D'où : $\bigcap_{j\in J}A'_j=\left(\bigcap_{j\in J\backslash\{1\}}A_j\right)\backslash\left(\bigcap_{j\in J}A_j\right)$.

On en déduit que :

$$P\left(\bigcap_{j\in J}A'_j\right)=P\left(\bigcap_{j\in J\backslash\{1\}}A_j\right)-P\left(\bigcap_{j\in J}A_j\right)=\prod_{j\in J\backslash\{1\}}P\left(A_j\right)-\prod_{j\in J}P\left(A_j\right)$$

$$=\prod_{j\in J\backslash\{1\}}P\left(A_j\right)-P\left(A_1\right)\prod_{j\in J\backslash\{1\}}P\left(A_j\right)=\left(1-P(A_1)\right)\prod_{j\in J\backslash\{1\}}P\left(A_j\right)=\prod_{j\in J}P\left(A'_j\right)$$

§. Pour s'en convaincre, faire jouer dans la propriété précédente le rôle de A à $\Omega\backslash B$ et le rôle de B à A.

Dans les deux cas, on a établi que : $P\left(\bigcap_{j\in J} A'_j\right) = \prod_{j\in J} P(A_j)$. Puisque cette égalité tient pour tout famille J de $[\![\, 1, n \,]\!]$, on peut conclure que :

les évènements $\Omega\backslash A_1$, A_2,..., A_n sont mutuellement indépendants.

b. Supposons les évènements A_1, A_2,..., A_n mutuellement indépendants.

D'après la question précédente, les évènements $\Omega\backslash A_1$, A_2,..., A_n sont mutuellement indépendants.

Donc les évènements A_2,..., A_n, $\Omega\backslash A_1$ sont mutuellement indépendants.

D'après la question précédente, les évènements $\Omega\backslash A_2$, A_3,..., A_n, $\Omega\backslash A_1$ sont mutuellement indépendants.

Donc les évènements A_3,..., A_n, $\Omega\backslash A_1$, $\Omega\backslash A_2$ sont mutuellement indépendants.

Etc... Au final, les évènements $\Omega\backslash A_1$,..., $\Omega\backslash A_n$ sont mutuellement indépendants.

Partie II — Indicatrice d'Euler

3. Soit p un diviseur de n. Il existe un entier q tel que $n = pq$. Les multiples de p compris entre 1 et n sont : p, $2p$,..., qp. Il existe donc exactement q entiers compris entre 1 et n qui sont divisibles par p. On en déduit que la probabilité qu'un entier choisi au hasard entre 1 et n soit multiple de p est : $q/n = 1/p$.

Conclusion. $P(A_p) = \dfrac{1}{p}$.

4. On note p_1,..., p_r les diviseurs premiers de n.

a. Soit m un entier naturel (non nul, sinon il n'y a pas grand chose à prouver).

Supposons que $\forall\, i \in [\![\, 1, r \,]\!],\ p_i | m$. Alors : $\forall\, i \in [\![\, 1, r \,]\!],\ v_{p_i}(m) > 0$. La décomposition en facteurs premiers de m peut donc s'écrire :

$$m = \prod_{i=1}^{r} p_i^{v_{p_i}(m)} \times \prod_{p\in\mathscr{P}\backslash\{p_1,\dots,p_r\}} p^{v_p(m)} = \prod_{i=1}^{r} p_i \times \underbrace{\left(\prod_{i=1}^{r} p_i^{v_{p_i}(m)-1} \times \prod_{p\in\mathscr{P}\backslash\{p_1,\dots,p_r\}} p^{v_p(m)}\right)}_{\in\mathbb{N}}$$

On déduit de cette écriture que : $\prod_{i=1}^{r} p_i \,|m$. Par suite : $[\forall\, i \in [\![\, 1, r \,]\!],\ p_i|m] \Longrightarrow \left[\prod_{i=1}^{r} p_i \,|m\right]$.

La réciproque est triviale, et on peut conclure : $\left[\forall\, i \in [\![\, 1, r \,]\!],\ p_i|m\right] \Longleftrightarrow \left[\prod_{i=1}^{r} p_i \,|m\right]$.

b. Supposons $r \geqslant 2$ (sinon il n'y a pas grand chose à faire), et soit J une partie de $[\![\, 1, r \,]\!]$ de cardinal c supérieur ou égal à 2 (sinon...).

Quitte à renuméroter les p_i, on peut supposer que $J = \{1, 2, \dots, c\}$. D'après la question précédente on a : $\bigcap_{i=1}^{c} A_{p_i} = A_{\prod_{i=1}^{c} p_i}$. D'où : $P\left(\bigcap_{i=1}^{c} A_{p_i}\right) = P\left(A_{\prod_{i=1}^{c} p_i}\right) = \dfrac{1}{\prod_{i=1}^{c} p_i} = \prod_{i=1}^{c} \dfrac{1}{p_i} = \prod_{i=1}^{c} P(A_{p_i})$

Conclusion. Les évènements A_{p_1},..., A_{p_r} sont mutuellement indépendants.

5. Soit m un entier compris entre 1 et n. L'entier m est premier avec n si et seulement si il est premier avec tout diviseur premier p_i de n. Puisque les p_i sont premiers(!), il revient au même de dire qu'aucun des p_i ne divise n. De ce raisonnement on déduit que : $A = \bigcap_{i=1}^{r} (\Omega \backslash A_{p_i})$.

Or, puisque les évènements A_{p_i} sont mutuellement indépendants (d'après 4-b), les évènements $\Omega \backslash A_{p_i}$ le sont également (d'après 2-b). Il s'ensuit que :

$$P(A) = P\left(\bigcap_{i=1}^{r} (\Omega \backslash A_{p_i})\right) = \prod_{i=1}^{r} P\left(\Omega \backslash A_{p_i}\right) = \prod_{i=1}^{r} \left(1 - P\left(A_{p_i}\right)\right)$$

D'où finalement : $\boxed{P(A) = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \quad (\spadesuit)}$

Par ailleurs, et par définition de l'indicateur d'Euler : $\boxed{P(A) = \frac{\varphi(n)}{n} \quad (\clubsuit)}$

On déduit alors de ($\spadesuit$) et de ($\clubsuit$) que : $\boxed{\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)}$.

6. Soient n et m deux entiers strictement plus grands que 1. Supposons que n et m sont premiers entre eux. Alors aucun facteur premier intervenant dans la décomposition de n n'intervient dans celle de m, et réciproquement. En d'autres termes il existe $(r+s)$ nombres premiers $p_1, \ldots, p_r$, $q_1, \ldots, q_s$ et (r+s) entiers naturels non nuls $\alpha_1, \ldots, \alpha_r$, $\beta_1, \ldots, \beta_s$ tels que :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} \quad \text{et} \quad m = \prod_{j=1}^{s} q_j^{\beta_j}$$

Puisque les p_i et les q_j sont des nombres premiers deux à deux distincts, la décomposition en facteurs premiers de nm est : $nm = \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{j=1}^{s} q_j^{\beta_j}$.

On déduit alors de la question précédente que :

$$\varphi(nm) = nm \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \prod_{j=1}^{s} \left(1 - \frac{1}{q_j}\right) = \left(n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)\right) \left(m \prod_{j=1}^{s} \left(1 - \frac{1}{q_j}\right)\right) = \varphi(n)\varphi(m)$$

Conclusion. $\boxed{\forall\, (n,m) \in \left(\mathbb{N} \backslash \{0,1\}\right)^2,\ [n \wedge m = 1] \Longrightarrow [\varphi(nm) = \varphi(n)\varphi(m)]}$.