

Partie I

1. Si $\mathbb{P} = \{p_1, \dots, p_N\}$ est fini, avec $p_1 < p_2 < \dots < p_N$, soit l'entier $q = \prod_{i=1}^N p_i + 1$, alors pour tout $p \in \mathbb{P}$, on a : p divise $\prod_{i=1}^N p_i$ et donc $q \equiv 1 \pmod p$ et par suite q est premier et $q > p_N$. ce qui contredit l'hypothèse \mathbb{P} fini. On conclut que \mathbb{P} est infini.

a) Pour $n \geq 2$, on a : $(1 - \frac{1}{n^s})^{-1} = \sum_{k=0}^{\infty} \frac{1}{n^{ks}}$: série géométrique de raison $\frac{1}{n^s} \in]0, 1[$.

b) Pour tout $(i, j) \in \mathbb{N} \times \mathbb{N}$, $u_{ij} = \frac{1}{a^{is}b^{js}} > 0$. Pour chaque $i \in \mathbb{N}$, la famille $(u_{ij})_j$ est sommable de somme $s_i = \sum_{j=0}^{\infty} \frac{1}{a^{is}b^{js}} = \frac{1}{a^{is}} \sum_{j=0}^{\infty} \frac{1}{b^{js}}$ (comparaison à une série de Reimann). La famille $(s_i)_i$

est aussi sommable et $\sum_{i=0}^{\infty} s_i = \sum_{i=0}^{\infty} \left(\frac{1}{a^{is}} \sum_{j=0}^{\infty} \frac{1}{b^{js}} \right) = \left(\sum_{i=0}^{\infty} \frac{1}{a^{is}} \right) \left(\sum_{j=0}^{\infty} \frac{1}{b^{js}} \right)$.

Donc la famille $(u_{ij})_{(i,j)}$ est sommable et $\sum_{(i,j) \in \mathbb{N} \times \mathbb{N}} u_{ij} = \left(\sum_{i=0}^{\infty} \frac{1}{a^{is}} \right) \left(\sum_{j=0}^{\infty} \frac{1}{b^{js}} \right)$.

c) On note $M_n = \{m / m = \prod_{i=1}^n p_i^{\alpha_i}, \alpha_i \in \mathbb{N}\}$, l'application $\varphi : \mathbb{N}^n \rightarrow M_n$ est $(\alpha_1, \dots, \alpha_n) \mapsto \prod_{i=1}^n p_i^{\alpha_i}$

injective en effet : si $\varphi(\alpha_1, \dots, \alpha_n) = \varphi(\beta_1, \dots, \beta_n)$ alors $\prod_{i=1}^n p_i^{\alpha_i} = \prod_{i=1}^n p_i^{\beta_i}$ et puis $\alpha_i = \beta_i$ pour tout i car sinon, il existerait $k \in \llbracket 1, n \rrbracket$ tel que $\alpha_k \neq \beta_k$, par exemple $\alpha_k < \beta_k$. En écrivant : $\prod_{i=1, i \neq k}^n p_i^{\alpha_i} = p_k^{s(\beta_k - \alpha_k)} \prod_{i=1, i \neq k}^n p_i^{\beta_i}$, on a : $\prod_{i=1, i \neq k}^n p_i^{\alpha_i} \equiv 0 \pmod{p_k}$ ce qui absurde. D'où le résultat cherché.

Etude d'exemples :

Pour $s = 1$ et $n = 2$:

i	1	2	3	4	5	6	7	8	9	10	11	12
m_i	1	2	3	4	6	8	9	12	16	18	24	27

Pour $s = 1$ et $n = 3$:

i	1	2	3	4	5	6	7	8	9	10	11	12
m_i	1	2	3	4	5	6	8	9	10	12	15	20

d) Pour tout $n \in \mathbb{N}^*$, on a : $\{k^s / k \in \llbracket 1, n \rrbracket\} \subset M_n$ (décomposition d'un entier en facteurs premiers), donc : $\prod_{i=1}^n (1 - \frac{1}{p_i^s})^{-1} = \prod_{p \in \mathbb{P}, p \leq n} (1 - \frac{1}{p^s})^{-1} = \sum_{m \in M_n} \frac{1}{m} \geq \sum_{k=1}^n \frac{1}{k^s}$.

Pour $s = 1$, $\prod_{i=1}^n (1 - \frac{1}{p_i})^{-1} \geq \sum_{k=1}^n \frac{1}{k} \xrightarrow{n \rightarrow \infty} +\infty$, le retrouve le résultat de la question. **I-a)**...

e) Par décomposition d'un entier en facteurs premiers, on a : $M_N \subset \{k^s / k \in \mathbb{N}^*\}$, donc $\sum_{k=1}^n \frac{1}{k^s} \leq \prod_{i=1}^N (1 - \frac{1}{p_i^s})^{-1} = \sum_{m \in M_n} \frac{1}{m} \leq \sum_{k=1}^{\infty} \frac{1}{k^s}$ et puis $\lim_{n \rightarrow \infty} f_n(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}$.

3. Pour $s = 1$, par $\prod_{i=1}^N (1 - \frac{1}{p_i})^{-1} \geq \sum_{k=1}^n \frac{1}{k} \xrightarrow{n \rightarrow \infty} +\infty$, on a : $\sum_{i=1}^N v_i = -\ln(\prod_{i=1}^N (1 - \frac{1}{p_i})^{-1}) \rightarrow -\infty$, donc $\sum v_i$ diverge. On sait que $p_i \rightarrow +\infty$ quand $i \rightarrow \infty$, donc $v_i = \ln(1 - \frac{1}{p_i}) \sim -\frac{1}{p_i} = -w_i < 0$ et par le théorème de comparaison $\sum w_i$ diverge.

4. $\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}$ est définie pour tout $s > 1$ (série de Riemann).

Pour tout $a > 1$ et tout $s \geq a$, on a : $\forall k \in \mathbb{N}^*$, $0 < \frac{1}{k^s} \leq \frac{1}{k^a}$ et $\sum \frac{1}{k^a}$ converge, donc la série de fonctions continues $\sum_{k \geq 1} (s \mapsto \frac{1}{k^s})$ converge normalement (donc uniformément) sur $[a, +\infty[$ et par suite ζ est continue sur $]1, +\infty[$.

Etude du caractère C^1 .

L'application $s \mapsto \frac{1}{k^s}$ est C^1 (même C^∞) sur $]1, +\infty[$ et $\frac{d}{ds}(\frac{1}{k^s}) = -\ln(k)\frac{1}{k^s}$. On a donc, pour tout $a > 1$ et $s \geq a$, $|\ln(k)\frac{1}{k^s}| \leq \frac{\ln(k)}{k^a}$. Si $\alpha \in]1, a[$, alors $k^\alpha \frac{\ln(k)}{k^a} = \frac{\ln(k)}{k^{a-\alpha}} \xrightarrow{n \rightarrow \infty} 0$, donc la série numérique $\sum_{k \geq 1} \frac{\ln(k)}{k^a}$ est convergente et par suite la série de fonctions $\sum (s \mapsto -\ln(k)\frac{1}{k^s})$ converge normalement (donc uniformément) sur $[a, +\infty[$. On conclut alors que ζ est de classe C^1 sur $]1, +\infty[$ et $\zeta'(s) = -\sum_{k=2}^{\infty} \ln(k)\frac{1}{k^s}$.

Partie II

1. Majoration du produit P_n

a) Valeurs de N , p_N , P_n et 4^n pour $n = 2, 3, 4, 5$

n	2	3	4	5
N	1	2	2	3
p_N	2	3	3	5
P_n	2	6	6	25
4^n	16	64	256	124

b) Soit $n \in \mathbb{N}^*$ et supposons $n+1$ non premier et que $P_n \leq 4^n$, alors

$N = \text{card}\{p \in \mathbb{P} / p \leq n\} = \text{card}\{p \in \mathbb{P} / p \leq n+1\}$ donc $p_{n+1} = p_n \leq 4^n \leq 4^{n+1}$.

c) Si $n+1$ est premier, alors $n+1$ est impair, donc il existe $m \in \mathbb{N}^*$ tel que $n+1 = 2m+1$.

On a : $\mathfrak{C}_{2m+1}^m = \frac{(m+2)\dots(2m+1)}{m!} = \frac{N}{D}$, donc tout nombre premier $p \in \llbracket m+2, 2m+1 \rrbracket$ divise N et les seuls diviseurs p premiers de D sont $\leq m$ et par suite : tout nombre premier $p \in \llbracket m+2, 2m+1 \rrbracket$ divise \mathfrak{C}_{2m+1}^m . Par application de la formule du binôme, on a : $2\mathfrak{C}_{2m+1}^m = \mathfrak{C}_{2m+1}^m + \mathfrak{C}_{2m+1}^{m+1} \leq (1+1)^{2m+1} = 2^{2m+1}$, donc $\mathfrak{C}_{2m+1}^m \leq 2^{2m} = 4^m$.

Avec $n+1 = 2m+1$ premier, on a : $P_{n+1} = \underbrace{\left(\prod_{p \in \mathbb{P}, p \leq m+1} p \right)}_{p_{m+1}} \underbrace{\left(\prod_{p \in \mathbb{P}, m+2 \leq p \leq 2m+1} p \right)}_Q = P_{m+1}Q$.

par ce qui précède Q divise \mathfrak{C}_{2m+1}^m donc $Q \leq \mathfrak{C}_{2m+1}^m$ et par suite $Q \leq 4^m$.

Si $P_{m+1} \leq 4^{m+1}$, alors : $P_{n+1} = P_{m+1}Q \leq 4^{m+1}4^m = 4^{2m+1} = 4^{n+1}$.

d) Une récurrence s'impose :

Pour $n = 2$, on a : $N = 1$ et $P_n = p_1 = 2 \leq 4^2$.

Soit $n \in \mathbb{N}$ tel que $n \geq 2$, supposons (HR) : $P_n \leq 4^n$, alors par b) et c) on a : $P_{n+1} \leq 4^{n+1}$

2. Posons $\alpha_i = \max_j \{j / p_i^j \leq n\}$, alors $d_n = \prod_{i=1}^N p_i^{\alpha_i}$ en effet : Si $k = \prod_{i=1}^N p_i^{\alpha_{i,k}} \in \llbracket 1, n \rrbracket$, alors $\alpha_{i,k} \leq \alpha_i$

et k divise $\prod_{i=1}^N p_i^{\alpha_i}$. Donc $\prod_{i=1}^N p_i^{\alpha_i}$ est un multiple commun à tous les $k \in \llbracket 1, n \rrbracket$. Si $k = p_i^{\alpha_i}$, alors

$k \in \llbracket 1, n \rrbracket$ et k divise d_n , donc $\prod_{i=1}^N p_i^{\alpha_i}$ divise d_n . Par définition de d_n on a bien l'égalité.

Par $\alpha_i = \max_j \{j / p_i^j \leq n\}$, par $p_i^j \leq n$ on a : $j \leq \frac{\ln(n)}{\ln(p_i)}$ et puis $\alpha_i = \lfloor \frac{\ln(n)}{\ln(p_i)} \rfloor$

Autre façon :

Soit $k = \prod_{i=1}^N p_i^{\alpha_{i,k}} \in \llbracket 1, n \rrbracket$ et $D_n = \prod_{i=1}^N p_i^{\alpha_i}$ avec $\alpha_i = \max_{1 \leq k \leq n} \alpha_{i,k}$, on a : $\alpha_i \geq 1$ (car $\alpha_{i,k} \geq 1$ pour k

premier) et k divise D_n ($D_n = k \cdot \prod_{i=1}^N p_i^{\alpha_i - \alpha_{i,k}}$), donc D_n est un multiple commun des $k \in \llbracket 1, n \rrbracket$.

Comme d_n est le plus petit commun multiples des k , on a : d_n divise D_n : $D_n = d_n \prod_{i=1}^N p_i^{\gamma_i}$ avec

$\gamma_i \geq 0$ et si $d_n = \prod_{i=1}^N p_i^{\beta_i}$ alors $\alpha_i = \beta_i + \gamma_i$ pour tout i .

Supposons qu'il existe i_0 tel que $\gamma_{i_0} \geq 1$, alors $\alpha_{i_0} = \alpha_{i_0, k_0} = \beta_{i_0} + \gamma_{i_0}$ avec $k_0 = \left(\prod_{i=1, i \neq i_0}^N p_i^{\alpha_i} \right) \cdot p_{i_0}^{\alpha_{i_0, k_0}} \in \llbracket 1, n \rrbracket$

$p_{i_0}^{\alpha_{i_0}} = p_{i_0}^{\alpha_{i_0, k_0}}$ est un diviseur de k_0 , donc de d_n et comme $d_n = \left(\prod_{i=1, i \neq i_0}^N p_i^{\beta_i} \right) \cdot p_{i_0}^{\beta_{i_0}}$, on a :

$\alpha_{i_0} \leq \beta_{i_0} < \beta_{i_0} + \gamma_{i_0} = \alpha_{i_0}$ ce qui est absurde. En conséquence : $\forall i, \alpha_i = \beta_i$ et puis $d_n = D_n$.
Remarquons que $\alpha_i = \max_k \{k / p_i^k \leq n\}$, par $p_i^k \leq n$ on a : $k \leq \frac{\ln(n)}{\ln(p_i)}$ et puis $\alpha_i = \lfloor \frac{\ln(n)}{\ln(p_i)} \rfloor$

3. Une minoration de d_{2n+1}

a) L'étude de la fonction $f_n : [0, 1] \rightarrow \mathbb{R}, x \mapsto x^n(1-x)^n$ montre que f_n est continue et bornée sur $[0, 1]$ et $\|f_n\|_\infty = \sup_{x \in [0, 1]} |f_n(x)| = \frac{1}{4^n}$. D'où $I_n = \int_0^1 f_n(x) dx \leq \frac{1}{4^n}$.

b) \triangleright Par sa définition d_{2n+1} est divisible par tous les entiers $n+k+1$ avec $k \in \llbracket 0, n \rrbracket$

\triangleright On a : $(1-x)^n = \sum_{k=0}^n \mathcal{C}_n^k (-1)^k x^k$, donc $I_n = \int_0^1 \sum_{k=0}^n \mathcal{C}_n^k (-1)^k x^{n+k} dx = \sum_{k=0}^n \mathcal{C}_n^k (-1)^k \frac{1}{n+k+1}$

et puis $d_{2n+1} \cdot I_n = \sum_{k=0}^n \mathcal{C}_n^k (-1)^k \frac{d_{2n+1}}{n+k+1}$ et comme $\frac{d_{2n+1}}{n+k+1}$ est un entier, on a aussi $d_{2n+1} \cdot I_n$ est un entier (somme d'entiers).

\triangleright On a $I_n \cdot d_{2n+1} = m \in \mathbb{N}^*$, car I_n et d_{2n+1} sont strictement positifs, donc $d_{2n+1} = m \cdot \frac{1}{I_n} \geq \frac{m}{4^n} \geq \frac{1}{4^n}$.

Partie III

Pour $x \in \mathbb{R}$ tel que $x \geq 2$, posons $\pi(x) = \text{card}\{p \in \mathbb{P} / p \leq x\} = \sum_{p \in \mathbb{P}, p \leq x} 1$ et

$$\theta(x) = \sum_{p \in \mathbb{P}, p \leq x} \ln(p) = \sum_{i=1}^{\pi(x)} \ln(p_i)$$

1. Un résultat auxiliaire : On pose $a_0 = 0$ et $p_0 = 1$

$\triangleright H_A$ est une fonction en escalier, de constante égale à $\sum_{k=0}^N a_k$ sur $[p_N, p_{N+1}[$, donc continue sur les intervalles $[p_N, p_{N+1}[$ pour $N \in \mathbb{N}$.

Etude en les points p_N , $N \in \mathbb{N}^*$: on a : $H_A(x) = \begin{cases} \sum_{k=0}^{N-1} a_k & \text{si } x \in [p_{N-1}, p_N[\\ \sum_{k=0}^N a_k & \text{si } x \in [p_N, p_{N+1}[\end{cases}$, donc H_A est

continue en p_N si et seulement si $a_N = 0$ et lorsque $a_N \neq 0$, H_A est discontinue en p_N et on a : $H_A(p_N) - H_A(p_N - 0) = a_N$.

\triangleright Formule sommatoire d'Abel : pour $x \geq 2$, avec $p_N \leq x < p_{N+1}$, on a :

$$H_A(x)f(x) = \left(\sum_{i=1}^N a_i \right) f(x) \text{ et } \sum_{1 \leq i \leq N} a_i f(p_i) = a_1 f(p_1) + \dots + a_N f(p_N).$$

D'autre part $\int_2^x H_A(t)f'(t)dt = \sum_{2 \leq k \leq N} \int_k^{k+1} H_A(t)f'(t)dt + \int_N^x H_A(t)f'(t)dt$, mais :

$$\int_k^{k+1} H_A(t)f'(t)dt = \int_{[k, k+1[} H_A(t)f'(t)dt = \left(\sum_{i=1}^k a_i \right) (f(p_{i+1}) - f(p_i)) \text{ et}$$

$$\int_N^x H_A(t)f'(t)dt = \left(\sum_{i=1}^N a_i \right) (f(x) - f(p_N)), \text{ donc}$$

$$\begin{aligned} \int_2^x H_A(t) f'(t) dt &= \sum_{2 \leq k \leq N} \left(\sum_{i=1}^{k-1} a_i \right) f(p_k) - \sum_{2 \leq k \leq N} \left(\sum_{i=1}^k a_i \right) f(p_k) + \left(\sum_{i=1}^N a_i \right) (f(x) - f(p_N)) \\ &= - \sum_{1 \leq i \leq N} a_i f(a_i) + \left(\sum_{i=1}^N a_i \right) f(x) \end{aligned}$$

D'où le résultat demandé.

2. Une majoration de la fonction π .

a) Pour tout x réel tel que $x \geq 2$, et $p_N \leq [x] \leq x < p_{N+1}$, on a $p_N \leq [x] \leq x < p_{N+1}$ et par la question II-1.d) : $\prod_{i=1}^N p_i \leq 4^{[x]} \leq 4^x$ et par suite $\theta(x) = \sum_{i=1}^N \ln(p_i) \leq \ln(4^x) = x \ln(4)$.

b) Si la suite $A = (a_n)_n$ est telle que : $a_n = \ln(p_n)$, avec $p_0 = 1$ et $f : x \mapsto \frac{1}{\ln(x)}$, alors les hypothèses de formule sommatoire d'ABEL sont toutes justifiées, et on a :

$$\pi(x) = \sum_{i=1}^N 1 = \sum_{i=1}^N a_i f(p_i) = H_A(x) f(x) - \int_2^x H_A(t) f'(t) dt.$$

Or $H_A(x) = \sum_{i=1}^N a_i = \sum_{i=1}^N \ln(p_i) = \theta(x)$ et $f'(x) = -\frac{1}{x(\ln(x))^2}$ donc :

$$\pi(x) = \theta(x) f(x) + \int_2^x \frac{\theta(t)}{t(\ln t)^2} dt \leq \frac{x \ln(4)}{\ln(x)} + \int_2^x \frac{t \ln(4)}{t(\ln t)^2} dt \text{ ce qui montre que :}$$

$$\pi(x) \leq \ln(4) \left(\frac{x}{\ln(x)} + \int_2^x \frac{1}{(\ln t)^2} dt \right)$$

c) Pour $x \geq 4$, on a : $R(x) = \frac{\ln(x)}{x} \int_2^x \frac{1}{(\ln t)^2} dt = \frac{\ln(x)}{x} \int_2^{\sqrt{x}} \frac{1}{(\ln t)^2} dt + \frac{\ln(x)}{x} \int_{\sqrt{x}}^x \frac{1}{(\ln t)^2} dt$, mais la fonction \ln est croissante et strictement positive sur $[2; +\infty[$, donc :

$$\begin{aligned} 0 &\leq \frac{\ln(x)}{x} \int_2^{\sqrt{x}} \frac{1}{(\ln t)^2} dt \leq \frac{\ln(x)}{x} \int_2^{\sqrt{x}} \frac{1}{(\ln 2)^2} dt = \frac{\ln x}{x} \frac{\sqrt{x}-2}{\ln^2 2} \xrightarrow{x \rightarrow +\infty} 0 \text{ et } 0 \leq \frac{\ln(x)}{x} \int_{\sqrt{x}}^x \frac{1}{(\ln t)^2} dt \leq \\ &\frac{\ln(x)}{x} \int_{\sqrt{x}}^x \frac{1}{(\ln \sqrt{x})^2} dt = \frac{4}{(\ln x)x} (x - \sqrt{x}) \xrightarrow{x \rightarrow +\infty} 0 \text{ et par suite } \lim_{x \rightarrow +\infty} R(x) = 0 \end{aligned}$$

d) Par la question précédente on a : $\int_2^x \frac{1}{(\ln t)^2} dt \underset{x \rightarrow +\infty}{=} o\left(\frac{x}{\ln(x)}\right)$, et avec $\varepsilon = \ln(4) > 0$, il existe $x_0 > 2$ tel que : $\forall x \geq x_0$; $0 \leq \int_2^x \frac{1}{(\ln t)^2} dt \leq \ln(4) \frac{x}{\ln(x)}$ et puis : $0 \leq \pi(x) \leq \ln(4) \left(\frac{x}{\ln(x)} + \int_2^x \frac{1}{(\ln t)^2} dt \right) \leq \ln(4) \left(\frac{x}{\ln(x)} + \frac{x}{\ln(x)} \right) = 4 \ln(2) \frac{x}{\ln(x)}$

3. Une majoration de la fonction π

Pour tout $x \geq 2$, avec $N = \pi(x)$, on a : $d_{2[\frac{x}{2}]+1} = \prod_{i=1}^N p_i^{\alpha_i}$ où $\alpha_i = \left[\frac{\ln([\frac{x}{2}])}{\ln(p_i)} \right]$, donc : $\ln(d_{2[\frac{x}{2}]+1}) =$

$$\ln\left(\prod_{i=1}^N p_i^{\alpha_i}\right) = \sum_{i=1}^N \alpha_i \ln(p_i) \leq \sum_{i=1}^N \frac{\ln([\frac{x}{2}])}{\ln(p_i)} \ln(p_i) \leq N \ln([\frac{x}{2}]) \leq N \ln\left(\frac{x}{2}\right).$$

D'autre part $d_{2[\frac{x}{2}]+1} \geq 4^{[\frac{x}{2}]}$, donc $\ln(d_{2[\frac{x}{2}]+1}) \geq [x] \cdot \ln(4) \geq (x-2) \ln(2) \geq x \ln(2)$ et par suite $x \ln(2) \leq N \ln\left(\frac{x}{2}\right)$, donc $N \geq \frac{x \ln(2)}{\ln\left(\frac{x}{2}\right)} = \frac{\ln(2)}{2} \frac{x}{\ln(x)} \left(\frac{2}{1 - \frac{\ln 2}{\ln(x)}} \right)$, mais $\lim_{x \rightarrow +\infty} \left(\frac{2}{1 - \frac{\ln 2}{\ln(x)}} \right) = 2$, il existe donc $x_1 > 2$ tel que : $\forall x \geq x_1$; $\frac{2}{1 - \frac{\ln 2}{\ln(x)}} \geq 2 - 1 = 1$.

En conclusion : $\exists x_1 > 2, \forall x \geq x_1 : \pi(x) = N \geq \frac{\ln(2)}{2} \frac{x}{\ln(x)} \left(\frac{2}{1 - \frac{\ln 2}{\ln(x)}} \right) \geq \frac{\ln(2)}{2} \frac{x}{\ln(x)}$

Partie IV

1. Théorème d'Euler

a) \Rightarrow Si \bar{a} est inversible dans $\mathbb{Z}/n\mathbb{Z}$; il existe $b \in \mathbb{Z}/n\mathbb{Z}$ tel que :

$$ab \equiv 1 \pmod{n} \quad (1)$$

$$(1) \iff \exists k \in \mathbb{Z}, ab = 1 + kn \iff \exists k \in \mathbb{Z}, ab - kn = 1$$

D'après le théorème de *Bezout*, a et n sont alors premiers entre eux.

\Leftarrow) Réciproquement, si a et n sont premiers entre eux, il existe des entiers u et v tels que : $au + nv = 1$.

Donc $au \equiv 1 \pmod{n}$ et \bar{u} est alors l'inverse de \bar{a} dans $\mathbb{Z}/n\mathbb{Z}$.

Valeurs de $\varphi(n)$ lorsque n prend toutes ses valeurs entières dans $\llbracket 2, 7 \rrbracket$:

n	2	3	4	5	6	7
$\varphi(n)$	1	2	1	4	2	6

b) Cours : $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe multiplicatif et $\text{card}((\mathbb{Z}/n\mathbb{Z})^*) = \varphi(n)$.

Soit n un entier ($n \geq 2$), et a un entier premier avec n . Montrons (théorème d'Euler) que :

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad (2)$$

L'application $\Psi : (\mathbb{Z}/n\mathbb{Z})^* \rightarrow (\mathbb{Z}/n\mathbb{Z})^*, \bar{b} \mapsto \bar{m} = \bar{b} \cdot \bar{a}$ est injective et $\text{card}() = \varphi(n)$ est fini, donc Ψ est surjective et par suite bijective. L'élément $c = \prod_{\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*} \bar{b} \cdot \bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, peut

s'écrire : $c = \left(\prod_{\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*} \bar{b} \right) \cdot \bar{a}^{\varphi(n)}$, mais $c = \prod_{\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*} \bar{b} \cdot \bar{a} = \prod_{\bar{m} \in (\mathbb{Z}/n\mathbb{Z})^*} \bar{m}$ car Ψ est bijective.

D'où $\prod_{\bar{m} \in (\mathbb{Z}/n\mathbb{Z})^*} \bar{m} = \left(\prod_{\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*} \bar{b} \right) \cdot \bar{a}^{\varphi(n)}$, et par suite $\bar{a}^{\varphi(n)} = \bar{1}$.

Autre façon : Il suffit d'appliquer le théorème de *Lagrange* au groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$: a étant premier avec n , donc $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$, et son ordre d divise $\varphi(n)$, ordre de $(\mathbb{Z}/n\mathbb{Z})^*$. On peut alors écrire : $\varphi(n) = dk$, où $k \in \mathbb{N}^*$. D'où $a^{\varphi(n)} = (a^d)^k \equiv 1 \pmod{n}$.

c) Application : Reste de la division euclidienne de 251^{311} par 6 : Il suffit de calculer $\overline{251^{311}}$ dans $\mathbb{Z}/6\mathbb{Z}$ et comme 251 est premier avec 6 et que $\overline{311} = 5$, $\varphi(6) = 2$, on a : $\overline{251^{311}} = \overline{251^5} = \overline{251^3} = \overline{251} = 5$ car $251^2 \equiv 1 \pmod{6}$.

2. Principe de cryptographie :

Soit n un entier ≥ 2 et p, q deux entiers premiers tels que : $n = pq$

a) L'application $h : (\mathbb{Z}/pq\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*, \bar{x} \mapsto (\bar{a}, \bar{b})$, où \bar{a} (resp. \bar{b}) est la classe de $x \pmod{p}$ (resp. classe de $x \pmod{q}$, est bijective, en effet : soit $(a, b) \in \llbracket 1, p-1 \rrbracket \times \llbracket 1, q-1 \rrbracket$, $(\mathbb{Z}/p\mathbb{Z})^* = \llbracket 1, p-1 \rrbracket \dots$). Comme $p \wedge q = 1$, par l'identité de *Bezout*, il existe $(u, v) \in \mathbb{Z}^2$ tel que $up + vq = 1$, donc $pu(a-b) + qv(p-q) = a-b$. Si l'on pose $k = u(a-b)$ et $k' = v(a-b)$, alors l'entier : $x = a + kp = b + k'q$ vérifie : $\begin{cases} x \equiv a \pmod{p} \\ x \equiv b \pmod{q} \end{cases}$, donc h est surjective

Soient maintenant x et x' deux solutions entières de système de congruence :

$$\begin{cases} x \equiv a \pmod{p} \\ x \equiv b \pmod{q} \end{cases} \quad \text{et} \quad \begin{cases} x' \equiv a \pmod{p} \\ x' \equiv b \pmod{q} \end{cases}$$

Alors $x - x' \equiv 0 \pmod{p}$ et $x - x' \equiv 0 \pmod{q}$.

Le théorème de *Gauss* montre qu'alors : $x - x' \equiv 0 \pmod{pq}$ et par conséquent h est injective.

Conclusion : h est une bijection de $(\mathbb{Z}/pq\mathbb{Z})^*$ sur $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$

Donc $\varphi(pq) = \text{card}((\mathbb{Z}/pq\mathbb{Z})^*) = \text{card}((\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*) = \varphi(p)\varphi(q) = (p-1)(q-1)$.

b) On suppose e entier tel que e est premier avec $(p-1)(q-1)$

On se place dans $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$, l'élément e est premier avec $(p-1)(q-1)$, donc inversible dans $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$, il existe donc $d \in \mathbb{Z}$ tel que $\bar{e} \cdot \bar{d} \equiv 1 \pmod{(p-1)(q-1)}$.

Exemple : $n = 6 = (2-1) \times (7-1) = (p-1)(q-1)$ $e = 5$ est premier avec 6

\bar{a}	0	1	2	3	4	5
\bar{a}^{ed}	0	1	2	3	4	5

c) Soit $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, on a : $\bar{a}^{\varphi(n)} \equiv 1 \pmod{n}$, comme $\bar{e} \cdot \bar{d} \equiv 1 \pmod{\varphi(n)}$ il existe $k \in \mathbb{Z}$ tel que $ed = 1 + k \cdot \varphi(n)$ et donc $\bar{a}^{ed} = \bar{a}^{1+k \cdot \varphi(n)} = \bar{a} \cdot (\bar{a}^{\varphi(n)})^k = \bar{a} \cdot 1 = \bar{a}$