(version dimanche 19 mai 2002 : 6h52)

nom :

spé MP1 carnot DIJON

Épreuve controlée et corrigé fait par LEGROS (Pierre Corneille ROUEN) et VIDIANI (CARNOT DIJON). *(Le but de chaque partie est donné en clair, le thème principal des questions est mis en évidence en caractères gras, la fin du problème est signalée ; la pagination est normalisée : numéro de page en cours / nombre total de pages : tout est fait pour donner de bonnes conditions matérielles aux candidats, et les placer dans un cadre bien construit).*

(Mais comme il y a peu de résultats à obtenir, qui ne sont pas donnés par l'énoncé, la rigueur et le précision de l'énoncé, favorise les élèves de MP, par rapport à ceux de MP)*

(Les maladresses de l'énoncé sont signalées par  *au fur et à mesure de leur apparition)*

Partie I : Nombres premiers

La suite des nombres premiers est illimitée : Raisonnons par l'absurde, supposons qu'il n'y ait qu'un (I-1) nombre fini de tels nombres $p_1, .., p_n$, alors Q donné dans l'énoncé, admet un diviseur premier (qui peut être lui même, s'il n'est pas factorisable), mais qui n'est pas dans la liste, sinon il diviserait $Q - p_1..p_n = 1$.

Relation à justifier : Il suffit d'appliquer l'identité de la série géométrique (de rayon 1) $\frac{1}{1-x} = \sum_{k=0}^{+\infty} x^k$, en (I-2-a) la spécialisant à $0 < x = \frac{1}{n^s} \leq \frac{1}{2} < 1$.

Somme d'une série double : On sait que si la série double est absolument convergente pour une bijection (I-2-b) particulière de $\mathbb{N}^2$, ce fait est indépendant de la bijection choisie et les sommes correspondantes sont les mêmes. En sommant par piles d'abcisse $i = constante$ on a $\sum_{(i,j)\in\mathbb{N}^2} \frac{1}{a^{is}}\frac{1}{b^{js}} = \sum_{i=0}^{\infty} \frac{1}{a^{is}} \sum_{j=0}^{\infty} \frac{1}{b^{js}} = \sum_{i=0}^{\infty} \frac{1}{a^{is}}(1 - \frac{1}{b^s})^{-1} = (1 - \frac{1}{b^s})^{-1} \sum_{i=0}^{\infty} \frac{1}{a^{is}} = (1 - \frac{1}{b^s})^{-1}(1 - \frac{1}{ab^s})^{-1} < +\infty$. Ainsi $\boxed{\mathbf{S = \frac{1}{1-a^s}\frac{1}{1-b^s}}}$ 

L'application donnée est injective : Cela résulte immédiatement de l'unicité de la décomposition en (I-2-c) facteurs premiers de tout nombre entier de $\mathbb{N}^*$ et de l'injectivité de l'application définie sur $\mathbb{R}+$ qui à x associe x^s.

Son image M_n est donc une partie infinie de $\mathbb{N}$. Il suffit de numéroter les nombres obtenus dans l'ordre naturel. Si l'on veut être plus précis on peut définir la suite $(m_i)_{i\geq 1}$ par récurrence en définissant $m_{i+1} = min\{M_n - \{m_1, ..., m_i\}\}$.

Pour $n = 2$; M_2 est constituée des éléments admettant uniquement 2 et 3 pour facteurs premiers : on commence la liste des éléments de M_2

puissances de 2 seul : 1, 2, 4, 8, 16, 32
puissances de 3 seul : 3, 9, 27, 81, 243
puissances mixtes : 6, 12, 24, 48, 96, ..., 18, 54,

puis de les placer dans l'ordre naturel :

numéro	1	2	3	4	5	6	7	8	9	10	11	12
élément de M_2	1	2	3	4	6	8	9	12	16	18	24	27

Pour $n = 3$; M_3 est constituée des éléments admettant uniquement 2 et 3 et 5 pour facteurs premiers : on commence la liste des éléments de M_3

puissances de 2 seul : 1, 2, 4, 8, 16, 32
puissances de 3 seul : 3, 9, 27, 81, 243
puissances de 5 seul : 5, 25, 125, 625,
puissances mixtes : 6, 10, 12, 15, 20, 24,

puis de les placer dans l'ordre naturel :

numéro	1	2	3	4	5	6	7	8	9	10	11	12
élément de M_3	1	2	3	4	5	6	8	9	10	12	15	16

(Les points admis dans l'énoncé se trouvent dans les thèmes séries ou arithmétiques, de tous les livres classiques d'exercices : Spm 2 p 81, Leichtnam p 150; Tauvel ronéo Poitiers p 98, Tauvel Livre, Br 72 p 55 ; Br 83 p 75, Serre Puf cours d'arithmétique p 83, Itard les nombres premiers Puf p 29-30, Dony)

Inégalité à prouver : Nous savons que $\prod_{i=1}^{N} \left(1 - \frac{1}{(p_i)^s}\right)^{-1} = \sum_{m\in M_N} \frac{1}{m}$. Comme pour tout entier k compris (I-2-d) entre 1 et n, k^s est élément de M_N (dans la décomposition en produit de facteurs premier de k, tous les

facteurs sont au plus égaux à k, donc a fortiori à p_N), nous obtenons :

$$\sum_{k=1}^{n} \frac{1}{k^s} \leq \sum_{m \in M_N} \frac{1}{m} = \prod_{i=1}^{N} \left(1 - \frac{1}{(p_i)^s}\right)^{-1}.$$

■ **Suite des nombres premiers illimitée :**

Si la suite des nombres premiers n'était pas illimitée, N serait majoré par le nombre N_0 de nombres premiers. En choisissant $s = 1$ dans l'inégalité précédente, nous obtiendrions que la suite des sommes partielles de la série HARMONIQUE est majorée !

N.B : il y a une maladresse dans l'énoncé, le N (dépendant de n) devenant n.

■ **Limite de $\mathbf{f_n(s)}$.**

Nous avons, pour tout $n \in \mathbf{N}^*$:

$$\sum_{k=1}^{p_n} \frac{1}{k^s} \leq f_n(s).$$

Quand $0 < s \leq 1$, la série de terme général $1/k^s$ diverge vers $+\infty$ (série de RIEMANN avec l'exposant $s \leq 1$) et donc $f_n(s)$ tend vers $+\infty$ quand n tend vers l'infini (en remarquant que p_n tend vers l'infini quand n tend vers l'infini).

N.B.: il y a une nouvelle maladresse dans l'énoncé, qui nous définit un N qui dépend de n, puis un N qui dépend de x, pour reprendre dans la question (e) le N dépendant de n.

(I-2-e) **Encadrement et limite :** Il suffit de remarquer que M_N est contenu dans $\mathbf{N}^*$ pour obtenir l'inégalité qui manque. On en déduit que pour $s > 1$, la suite $f_n(s)$ converge vers $\zeta(s)$.

N.B.: Il y a une maladresse, j'aurais introduit la fonction zéta dès cette question, puisqu'on l'utilise, alors qu'elle n'est définie qu'avec la question (4).

(I-3) **Nature de la série des inverses des nombres premiers :** Comme $\displaystyle\prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right)^{-1}$ tend vers $+\infty$ quand N tend vers l'infini, on en déduit en prenant le logarithme que la série de terme général v_i diverge. Comme v_i est équivalent à $-1/p_i$ quand i tend vers l'infini, la série de terme général $1/p_i$ est également divergente (th. de comparaison des séries de signe constant).

■ Ceci prouve que les nombres premiers sont relativement nombreux dans l'ensemble $\mathbb{N}$, i.e. que p_i ne tend pas trop vite vers l'infini (on peut comparer aux carrés, qui sont "moins nombreux" que les nombres premiers puisque la série de terme général $1/i^2$ converge).

(I-4) **Zéta est de classe $\mathbf{C^1}$:** Il suffit d'appliquer le théorème de dérivation sous le signe $\sum$ à la série : $\zeta(s) = \displaystyle\sum_{k=1}^{\infty} \frac{1}{k^s}.$,

La série proposée converge en effet normalement - donc uniformément (de même que sa série dérivée de terme général $u'_k(s) = -\frac{\ln k}{k^s}$ aussi pour tout s dans $[1+u, +\infty[$, avec $u > 0$ fixé.

Partie II : Majorer $\mathbf{P_n}$

(II-1-a) **Tableau donnant $\mathbf{N, p_N, P_n, 4^n}$:** On obtient directement le tableau suivant :

n	2	3	4	5
N	1	2	2	3
$\mathbf{p_N}$	2	3	3	5
$\mathbf{P_n}$	2	6	6	30
$\mathbf{4^n}$	16	64	256	1024

Inégalité impliquant une autre : Si $n+1$ n'est pas premier, $N(n+1) = N(n)$ et $P_n = P_{n+1}$. Nous (II-1-b) aurons donc $P_{n+1} = P_n \leq 4^n \leq 4^{n+1}$ si l'on suppose que $P_n \leq 4^n$.

Existence de m : Comme $n+1$ est premier et supérieur à 3, il est impair et peut donc s'écrire $2m+1$ (II-1-c) avec $m \geq 1$.

■ **Divisibilité du coefficient du binôme :** Soit p un nombre premier compris entre $m+2$ et $n+1$. Nous avons alors $(2m+1)! = m!\,(m+1)!\,C_{2m+1}^m$. Comme p divise $(2m+1)!$ et est premier avec $m!\,(m+1)!$, il divise C_{2m+1}^m.

■ **Inégalité, majoration du coefficient du binôme :** L'inégalité $C_{2m+1}^m \leq 4^m$ se prouve facilement par récurrence sur m.

■ **Inégalité numéro m+1 implique celle n+1 :** Si nous supposons que $P_{m+1} \leq 4^{m+1}$, alors :

$$P_n = P_{m+1} \prod_{\substack{p \text{ premier} \\ m+2 \leq p \leq n+1}} p \leq 4^{m+1} C_{2m+1}^m \leq 4^{2m+1} = 4^n$$

puisque tous les facteurs p du produit divisent C_{2m+1}^m et sont des entiers premiers deux à deux distincts.

Majoration de $\mathbf{P_n}$: Cette majoration se prouve par récurrence (forte) sur n, en utilisant le b ou le c (II-1-d) selon que $n+1$ est composé ou premier.

Expression de $\mathbf{d_n}$: Pour k entier compris entre 1 et n, nous pouvons écrire
(II-2)

$$k = p_1^{\alpha_1(k)}\, p_2^{\alpha_2(k)} \ldots p_N^{\alpha_N(k)}$$

où les $\alpha_i(k)$ sont des entiers naturels. Nous avons alors :

$$d_n = \prod_{i=1}^{N} p_i^{\alpha_i}$$

où pour tout i, α_i est le maximum des $\alpha_i(k)$ pour k décrivant $\{1, \ldots, n\}$. Mais si, pour i fixé, nous notons $\alpha_i' = \left[\frac{\ln n}{\ln p_i}\right]$, nous avons :

- pour tout $k \in \{1, \ldots, n\}$, $p_i^{\alpha_i(k)} \leq k \leq n$ donc $\alpha_i(k) \leq \alpha_i'$;
- $p_i^{\alpha_i'}$ est un entier compris entre 1 et n et $\alpha_i\left(p_i^{\alpha_i'}\right) = \alpha_i'$.

Ceci prouve donc que $\alpha_i = \alpha_i'$.

Majoration de l'intégrale $\mathbf{I_n}$: Il suffit de remarquer que pour tout $x \in [0,1]$, $x(1-x) \leq 1/4$.
(II-3-a)

Divisibilité du ppcm : d_{2n+1} est divisible par tous les entiers compris entre 1 et $2n+1$, donc en particulier
(II-3-b) par tous les entiers compris entre $n+1$ et $2n+1$. Nous avons d'autre part :

$$\begin{aligned} d_{2n+1}\, I_n &= d_{2n+1} \sum_{k=0}^{n} C_n^k (-1)^{n-k} \int_0^1 x^{n+k}\, \mathrm{d}x \\ &= \sum_{k=0}^{n} C_n^k (-1)^{n-k} \underbrace{\frac{d_{2n+1}}{n+k+1}}_{\in \mathbb{N}} \end{aligned}$$

et donc $d_{2n+1}\, I_n$ est un entier.

■ **Minoration du ppcm :** Nous en déduisons que $d_{2n+1}\, I_n$ est au moins égal à 1, puis :

$$d_{2n+1} \geq \frac{1}{I_n} \geq 4^n.$$

Partie III : Fonctions arithmétiques

Continuité de $\mathbf{H_A}$? Précisons $H_A(x)$ pour mieux cerner la fonction H_A $H_A(x) = \begin{cases} 0 & \text{pour } 1 \leq x < 2 \\ a_1 & \text{pour } 2 \leq x < 3 \text{ (ra} \\ a_1 + a_2 & \text{pour } 3 \leq x < 5,\ N \\ a_1 + a_2 + a_3 & \text{pour } 5 \leq x < 7,\ N \end{cases}$
(III-1)

H_A est constante sur chaque intervalle $[p_N, p_{N+1}[$, donc y est continue. Les points de discontinuité éventuels, sont les points p_N où $a_N \neq 0$, et alors pour ces N, $\boxed{\mathbf{H_A(x) - H_A(x-0) = a_N}}$

■ **La formule sommatoire d'ABEL :** *(Elle est un outit très puissant en théorie analytique des nombres. Il permet de remplacer des sommes par des intégrales, ce qui, bien souvent simplifie considérablement les calculs. Pour les gens informés elle revient à une intégration part parties d'une intégrale de STIELTJES).*

Laissons nous guider par la relation de CHASLES, et le fait que H_A est constante par paliers : On pose $n = E(x)$ (partie entière).

$$\begin{aligned}
\int_2^x f'(t)H_A(t) &=_{\text{Chasles}} \sum_{k=2}^{n-1}\int_k^{k+1} f'(t)H_A(t)dt + H_A(n)(f(x)-f(n)) \\
&=_{\text{H constante par intervalles}} \sum_{k=2}^{n-1} H_A(k)(f(k+1)-f(k)) + H_A(n)(f(x)-f(n)) \\
&=_{\text{distributivité et H(n)=H(x)}} \sum_{k=2}^{n-1} H_A(k)f(k+1) - \sum_{k=2}^{n} H_A(k)f(k) + H_A(x)f(x) \\
&=_{\text{changement d'indice}} \sum_{k=3}^{n} H_A(k-1)f(k) - \sum_{k=2}^{n} H_A(k)f(k) + H_A(x)f(x) \\
&=_{\text{par définition de H}} \sum_{k=3}^{n} \underbrace{\big[H_A(k-1) - H_A(k)\big]}_{=-a_k} f(k) + H_A(x)f(x)
\end{aligned}$$

D'où l'égalité la formule sommatoire d'ABEL demandée.

(III-2-a) **Majoration de $\theta(\mathbf{x})$:** On a, avec une notation plus commode (p comme "Premier") $\theta(x) = \sum_{p\leq x} \ln p \leq_{\text{En prenant le logarithme des deux membres de l'inégalité (II-1-d)}} n\ln 4 \leq x\ln 4$.

(III-2-b) **Majoration de $\pi(\mathbf{x})$:** *(D'après le dictionnaire Weisstein p 1427 π est appelée fonction compteur des nombres premiers $\leq x$, pour des terminologie d'autres fonctions arithmétiques voir aussi Polya et Szegö II p 1118-119, θ est la fonction arithmétique sommatoire de MANGOLDT)*

En faisant ce qui indiqué, la formule sommatoire d'ABEL établie en (III-1) donne $\pi(x) = \theta(x)\frac{1}{\ln(x)} + \int_2^x \frac{\theta(t)}{t(\ln(t))^2}dt$ qui donne bien l'inégalité demandée en majorant $\theta(x)$ et $\theta(t)$ par $x\ln 4$ et $t\ln 4$, respectivement.

(III-2-c) **R(x) tend vers zéro :** ⚠En opérant comme il est dit dans l'énoncé, on a par CHASLES : $R(x) = \frac{\ln x}{x}\Big(\int_2^{\sqrt{x}} \frac{dt}{(\ln(t))^2} + \int_{\sqrt{x}}^x \frac{dt}{(\ln(t))^2}\Big) \leq \frac{\ln x}{x}\big(\frac{\sqrt{x}}{(\ln(2))^2} + \frac{x-\sqrt{x}}{(\ln(\sqrt{x}))^2}\big) \to 0$ d'après la prépondérance au voisinage de $+\infty$ de $x^k,\ k>0$ par rapport à $(\ln x)^s$.

(III-2-d) **Déduction :** ⚠D'après ce qu'il vient d'être fait : $\pi(x) = 2\ln(2)\frac{x}{\ln x}\big(1+R(x)\big)$. En choisissant, compte tenu de la question précédente, x_0 réel, pour que pour tout x supérieur ou égal à x_0 on ait $|R(x)-0| \leq 1 = \varepsilon$, on a bien la majoration exigée.

(III-3) **Minoration de $\pi(\mathbf{x})$:** Pour $x \geq 3$, soit n l'entier vérifiant $2n+1 \leq x < 2n+3$. Remarquons tout d'abord que le N de $2n+1$ est égal au N de x, puisque $2n$ n'est pas premier. Nous avons donc $p_N \leq 2n+1 \leq x < p_{N+1}$. Nous savons d'après la partie II que $d_{2n+1} \geq 4^n$, donc :

$$n\ \ln 4 \leq \ln d_{2n+1} = \sum_{i=1}^{N} \left[\frac{\ln(2n+1)}{\ln p_i}\right] \ln p_i.$$

Comme $x < 2n+3$, $\frac{x-3}{2} < n$, et donc (en majorant chaque $\left[\frac{\ln(2n+1)}{\ln p_i}\right]$ par $\frac{\ln(2n+1)}{\ln p_i}$) :

$$\frac{x-3}{2}\ \ln 4 \leq \sum_{i=1}^{N} \frac{\ln(2n+1)}{\ln p_i}\ \ln p_i = N\ln(2n+1).$$

Il reste à remarquer que $N = \pi(x)$, pour obtenir :

$$\frac{x-3}{2\ln x}\ \ln 4 \leq \pi(x).$$

Enfin, $\frac{x-3}{2\ln x}\ln 4$ étant équivalent à $\frac{x}{\ln x}\ln 2$ quand x tend vers $+\infty$, on a

$$\frac{x}{\ln x}\frac{\ln 2}{2} \leq \frac{x-3}{2\ln x}\ln 4 \leq \pi(x)$$

pour x suffisamment grand.

En fait, nous avons démontré des résultats un peu plus précis : il existe deux fonctions $m(x)$ et $M(x)$ telles que $m(x) \leq \pi(x) \leq M(x)$ avec :

$$m(x) \sim_{+\infty} \ln 2\ \frac{x}{\ln x} \qquad \text{et} \qquad M(x) \sim_{+\infty} 2\ln 2\ \frac{x}{\ln x}.$$

Partie IV : Fonctions d'EULER et RSA

CNS d'inversibilité : (IV-1-a) Pour des raisons de facilité de typographie a désigne aussi bien l'élément a de $\mathbb{Z}$, que sa classe ; Si $a = sr$ n'est pas premier avec $n = st$ ($1 < s < n$ diviseur commun), alors $at = rn = 0$, a est non nul et n'est pas inversible puisqu'il est diviseur de 0.

Réciproquement si a et n sont premiers entre eux, d'après BEZOUT, il existe $u, v \in \mathbb{Z}$ tels que $au + nv = 1$, en langage de classe $au = 1$, et a est bien inversible.

Lorsque n est premier il est immédiat que $\boxed{\varphi(\mathbf{n}) = \mathbf{n-1}}$, d'où le tableau :

n	2	3	4	5	6	7	8	9	10	11	12
$\varphi(\mathbf{n})$	1	2	2	4	2	6	4	6	4	10	4

(Pour des tables plus complètes, voir Comtet PUF analyse combinatoire page 28, Warusfel structure algébrique finie Hachette 1971 p 70, un tableau latin de valeurs de 1 à 100 ; Maple donne par exemple with(numtheory): phi(2002); qui donne $\varphi(2002) = 720$)

Les éléments inversibles forment un groupe : (IV-1-b) Plongé dans $\mathbb{Z}\backslash n\mathbb{Z}$, l'ensemble proposé en possède tous les propriétés (associativité, élement neutre,..) de plus il est stable puisque classiquement le produit de deux éléments inversibles est inversible grâce à $(ab)^{-1} = b^{-1}a^{-1}$. Son cardinal est par définition $\varphi(n)$.

■ **Relation à démontrer :** Comme γ est injective, donc une bijection sur $(\mathbb{Z}\backslash n\mathbb{Z})$, on retrouve tous les éléments b à l'ordre près : $c = a^{\varphi(n)}c$, d'où le résultat annoncé.

Reste de $\mathbf{251^{311}}$ par 6 : (IV-1-c) Comme $\varphi(6) = 2$, on a $251^{311} = 251^{2*155+1} = 251 = 5$ modulo 6.

Calculer $\varphi(\mathbf{pq})$: (IV-2-a) Pour qu'un élément de $\mathbb{Z}$ soit inversible dans $\mathbb{Z}\backslash pq\mathbb{Z}$ il faut et il suffit qu'il soit premier avec pq, Mais comme p et q sont premiers, une conséquence des théorèmes de BEZOUT et GAUSS est qu'il soit premier séparément avec p et q : or le nombre de multiples de p est p (en comptant 0) et celui des multiples de q est $q-1$ (en ne comptant plus 0 une nouvelle fois). Par conséquent $\varphi(pq) = pq-p-q+1 = (p-1)(q-1) = pq(1-\frac{1}{p})(1-\frac{1}{q})$; *(Pour la formule générale voir par exemple Fraysse page 137 et 148)*

Existence de d : (IV-2-b) D'après BEZOUT, il existe des entiers u et v tels que $eu + v(p-1)(q-1) = 1$: La classe de u répond à la question.

■ **Exemple :** Ici $p = 2$, $q = 3$, on vérifie bien que $\varphi(6) = (2-1)(3-1) = 2$ comme $5 = 2*2+1$ on n'a pas besoin de BEZOUT pour voir que $u = 1 = e$ convient. $\boxed{\mathbf{e=1}}$.

■ $a^{ed} = a^{1+\varphi(6)k} = a$: (c'est le décodage RSA).

Relation à vérifier : (IV-2-c) ⚠ C'est le même calcul que dans le cas particulier précédent : $a^{ed} = a^{1+\varphi(n)k} =_{(*)} = a*1 = a$.

(*) En effet, et c'est justement l'intérêt d'un tel codage, en choisissant n QUADRATFREI, cette relation $x^k = x$ est valable pour tout x (et pas seulement pour ceux premiers avec n), ce qui serait génant pour la pratique du codage, - il faudrait en effet sinon vérifier que tout bloc message x est bien premier avec n ! -) dès lors que k est congru à 1 modulo φ(n) : Voici une démonstration Flash MP1 de ce fait :

D'abord on a le lemme Chinois : si a et b sont premiers entre eux, alors $\mathbb{Z}\backslash$abZ est isomorphe à $\mathbb{Z}\backslash a\mathbb{Z} \times \mathbb{Z}\backslash b\mathbb{Z}$; Considérons en effet l'application naturelle : $\mathbb{Z} \mapsto \mathbb{Z}\backslash a\mathbb{Z} \times \mathbb{Z}\backslash b\mathbb{Z}$ qui à un entier x fait correspondre le couple (x mod a, y mod b). Il s'agit d'un homomorphisme d'anneaux. Son noyau est

constitué par les entiers congrus à zéro modulo a et modulo b, donc d'après le théorème de GAUSS (puisque a et b sont premiers entre eux) par les multiples de ab. L'homomorphisme considéré est donc injectif, c'est même une bijection car les deux membres ont le même nombre ab d'éléments.

Par une récurrence triviale (et associativité du produit de groupes) si $p_1, ..., p_h$, sont h nombres premiers distincts, alors $\mathbb{Z}\backslash p_1\mathbb{Z} \times .... \times \mathbb{Z}\backslash p_h\mathbb{Z}$ est isomorphe à $\mathbb{Z}\backslash p_1...p_h\mathbb{Z}$.

n étant QUADRATFREI $n = p_1...p_h$, alors $\varphi(n) = (p_1 - 1)...(p_h - 1)$. Alors soit k un entier congru à 1 modulo $\varphi(n)$.

Or $x^k = x$ pour k congru à 1 modulo p-1 (p premier) (c'est trivial pour x multiple de p, les deux membres étant nuls modulo p), sinon cela résulte de la multiplication par x de la formule du peit théorème de FERMAT $x^{k-1} = 1$. puisqu'alors par Bezout k est de la forme u(p-1)+1 ; L'isomorphisme mis en évidence permet de conclure $x^k = x$ dès lors que $k = 1 + V(p_1 - 1)...(p_h - 1)$.

Pour des exemples voir le TP Maple codage RSA de MP1.

BIBLIOGRAPHIE COMMENTÉE

Ens Cloud physique 1975 énoncé rms 1 75-76 p 49 ; Mines 2 1990 ; RMS février 1996 question et réponses p608-615 pour $ppcm(1..n) \leq 3^n$; ; Ulm lyon cachan 96 P' , DUVERNEY théorie des nombres cours et exercices corrigés Dunod 1998 isbn 2 10 004102 9 page 89-90 inégalité de HANSON (1972) ; Concrete Mathematics GRAHAM, KNUTH ET PATASHNIK Addison Wesley 1994 isbn 0 201 55802 5 page 500 (exercice 21) où il semble qu'il y ait un lien entre probabilité et valeur moyenne de ce ppcm ;

Pour la partie III : Francinou et Gianella exercices de mathématiques pour l'agrégation algèbre 1 Masson 1993 isbn 2 225 84366 X pages 89,95, 97, 101-104 ; Apostol introduction to analystic Number Theory Springer Verlag 1984 isbn 0 387 90163 9 p 77 et sqq ; pour mémoire Hardy et Wright , De Bruyn ; Ellison et Mendes France ; Itard que sais je : théorie des nombres premiers ;

Pour la partie IV et surtout (IV 2 c) Gazette Aout 1979 Article de Maurice MIGNOTTE p61-69 en particulier p 64 la relation $x^k = x$ est valable POUR TOUT x premier ou non avec n (ce qui serait génant, car sinon, il faudrait vérifier pour chaque "bloc message" que le bloc x est premier avec n), sous la seule réserve que k soit congru à 1 modulo $\varphi(n)$.