Corrigé DM3

Problème 1. *(1) Soit $n \geqslant 2$ un entier. Montrez que les conditions suivantes sont équivalentes*

(i) *n est sans facteurs carrés et $p|n \Rightarrow p-1|n-1$, pour p premier;*

(ii) *$\forall a \in \mathbb{Z}$, on a $a^n \equiv a \bmod n$;*

(iii) *$\forall a \in \mathbb{Z}$ premier à n, on a $a^{n-1} \equiv 1 \bmod n$.*

(2) Un entier $n \in \mathbb{N}^*$ est dit pseudo-premier de base b si $b^{n-1} \equiv 1 \bmod n$.

(a) *Montrez que $n = 105 = 3.5.7$ est pseudo-premier de base 13 mais qu'il ne l'est pas de base 2.*

(b) *Le petit théorème de Fermat dit qu'un nombre premier p est pseudo-premier de base b pour tout b premier à p. Réciproquement un nombre n est dit de Carmichael s'il est pseudo-premier de base b pour tout b premier avec n, sans être premier. Montrez que $n = 561 = 3.11.17$ est un nombre de Carmichael.*

(c) *Un entier $n = 1 + 2^k q$ impair, q impair, est dit fortement pseudo-premier de base b si l'une des conditions suivantes est vérifiée:*

$$b^q \equiv 1 \bmod n \qquad \exists 0 \leqslant j < k,\ b^{2^j q} \equiv -1 \bmod n$$

(i) *Montrez que si n est premier alors il est fortement pseudo-premier de base b pour tout $1 \leqslant b < n$ et qui si n est fortement pseudo-premier de base b alors il est pseudo-premier de base b.*

(ii) *Montrez que $n = 561$ n'est pas fortement pseudo-premier de base 2.*

(iii) *Pour n impair soit*

$$B_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ n \text{ est fortement pseudo-premier de base } x\}.$$

On veut montrez le théorème de Rabin: si n est non premier alors $\frac{|B_n|}{\phi(n)} \leqslant 1/4$ sauf pour $n = 9$. Sous une autre forme, si $|B_n| \geqslant \phi(n)/4$ alors n est premier.

(α) *Considérons $p_1 \equiv 3 \bmod 4$ premier tel que $p_2 = 2p_1 - 1$ soit premier (exemple $p_1 = 40039, 41011, 42727$). Montrez alors que pour $n = p_1 p_2$, on a $4|B_n| = \phi(n)$.*

(β) *Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition en facteurs premiers de $n = 1 + 2^k q$, q impair; on écrit $p_i = 1 + 2^{k_i} q_i$ avec q_i impair et $k_1 \leqslant \cdots \leqslant k_r$. Montrez alors que*

$$|B_n| = (q, q_1) \cdots (q, q_r)(1 + \sum_{j=0}^{k_1 - 1} 2^{jr})$$

En déduire que $\frac{|B_n|}{\phi(n)} \leqslant \frac{1 + \frac{2^{k_1 r} - 1}{2^r - 1}}{2^{k_1 r}} K$, avec $K = \prod_{i=1}^r \frac{(q, q_i)}{q_i p_i^{\alpha_i - 1}}$. En outre si tous les k_i ne sont pas tous égaux, on peut améliorer l'inégalité précédente d'un facteur 2.

(γ) Montrez le résultat dans le cas où n est une puissance d'un nombre premier, puis traitez le cas général.

Remarque: Ainsi si n est fortement pseudo-premier dans m bases tirées au hasard, on peut présumer, avec une probabilité d'erreur inférieure à $1/4^m$, qu'il est premier.

(d) La méthode de cryptographie RSA: soit p et q deux nombres premiers distincts impairs et $n = pq$. Soit $0 \leqslant c < n$ un entier premier avec $\varphi(n)$. Etant donné un message en clair $0 \leqslant x < n$, $x \in \mathbb{N}$, on calcule $y = x^c$ qui représente le message codé.

(i) Expliquez comment décrypter le message.

(ii) On suppose maintenant que p et q sont fortement pseudo-premier pour r bases choisies au hasard. Que peut-on dire du système cryptographique précédent.

Preuve: (1) (i) implique (ii): Supposons $n = p_1.\cdots.p_s$ les p_i étant distincts deux à deux. Le théorème chinois donne alors $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s\mathbb{Z}$ et la congruence $a^n \equiv a \bmod n$ est équivalente à $a^n \equiv a \bmod p_i$ pour tout $i\cdot$ Pour i fixé, si p_i divise a le résultat est clair, sinon la congruence est équivalente à $a^{n-1} \equiv 1 \bmod p_i$. Par hypothèse $p_i - 1$ divise $n-1$, le petit théorème de Fermat donne alors $a^{p_i-1} \equiv 1 \bmod p_i$ soit $a^{n-1} \equiv 1 \bmod p_i$.

(ii) implique (iii): si a et n sont premiers entre eux l'implication est évidente car a est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

(iii) implique (i): Commençons par montrer que n est sans facteur carré: supposons par l'absurde que $n = p^r q$ avec $r > 1$, p premier et q non divisible par p. Pour a non divisible par p, on a $a^{n-1} \equiv 1 \bmod p^r$. On choisit alors un élément a de $(\mathbb{Z}/p^r\mathbb{Z})^\times$ d'ordre p (c'est possible car $r > 1$). On en déduit alors que p divise $p^r q - 1$ ce qui n'est pas. Montrons ensuite la deuxième propriété: soit p premier divisant n et soit a tel que sa classe modulo p engendre $(\mathbb{Z}/p\mathbb{Z})^\times$. La congruence $a^n \equiv a \bmod n$ implique $a^n \equiv a \bmod p$ soit $a^{n-1} \equiv 1 \bmod p$ et donc $p - 1$ divise $n - 1$ car $p - 1$ est l'ordre de a.

(2) (a) On a $13^{104} = (13^2)^{52} \equiv 1 \bmod 3$, $13^{104} = (13^4)^{26} \equiv 1 \bmod 5$ et $13^{104} = (13^6)^{17} \times 13^2 \equiv 1 \bmod 7$, de sorte que d'après le lemme chinois on a $13^{104} \equiv 1 \bmod 105$.
En revanche on a $2^{104} = (2^6)^{17} \times 2^2 \equiv 4 \bmod 7$.

(b) Il suffit de remarquer que 560 est multiple de $2, 10, 15$ et par suite $x^{560} \equiv 1$ dans $(\mathbb{Z}/3\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$, dans $(\mathbb{Z}/11\mathbb{Z})^\times \simeq \mathbb{Z}/10\mathbb{Z}$ et dans $(\mathbb{Z}/17\mathbb{Z})^\times \simeq \mathbb{Z}/16\mathbb{Z}$ et donc dans $(\mathbb{Z}/561\mathbb{Z})^\times$ d'après le lemme chinois.

(c) (i) Si n est premier alors $b^{2^k q} \equiv 1 \bmod n$ et soit donc $0 \leqslant i \leqslant k$ le plus petit entier tel que $b^{2^i q} \equiv 1 \bmod n$. Si $i = 0$, on a $b^q \equiv 1 \bmod n$ et si $i > 0$ alors $b^{2^{i-1} q} \equiv -1 \bmod n$ car dans un corps $x^2 = 1$ entraine $x = \pm 1$.
Si n est fortement premier de base b, il existe $0 \leqslant i \leqslant k$ tel que $b^{2^i q} \equiv 1 \bmod n$; or $2^i q$ divise $n - 1$ de sorte que $b^{n-1} \equiv 1 \bmod n$.

(ii) On a vu que $n = 561$ est pseudo-premier de base 2 mais il n'est pas fortement pseudo-premier de base 2; en effet $n - 1 = 2^4 35$ et $2^{352^3} \equiv 1 \bmod 561$ mais $2^{352^2} \equiv 67 \bmod 561$.

(iii) (α) On écrit $p_1 = 1 + 2q_1$ et $p_2 = 1 + 4q_1$ avec q_1 impair; $n - 1 = 2q_1(3 + 4q_1) = 2^k q$, soit $k = 1$ et $q = q_1(3 + 4q_1)$. L'ensemble B_n est la réunion disjointe de

$$P_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ x^q = 1\} \qquad Q_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ x^q = -1\}$$

Le théorème chinois donne avec des notations évidentes $|P_n| = |P_{p_1}||P_{p_2}|$ et $|Q_{p_1}||Q_{p_2}|$. Or comme $(\mathbb{Z}/p_1\mathbb{Z})^\times$ est cyclique d'ordre $p_1 - 1$, on a $|P_{p_1}| = (q, p_1 - 1) = (q, 2q_1) = (q, q_1) = q_1$. On calcule de même les autres cardinaux et on obtient $|B_n| = 2q_1^2$ et $\phi(n) = 8q_1^2$ d'où le résultat.

(β) L'ensemble B_n est la réunion disjointe de $P_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ x^q = 1\}$ et des $Q_n(j) = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ x^{2^j q} = -1\}$ pour $0 \leqslant j < k$.
- *calcul de* $|P_n|$: le théorème chinois donne $P_n \simeq \prod_{i=1}^r P_{p_i^{\alpha_i}}$ avec $|P_{p_i^{\alpha_i}}| = (q, \varphi(p_i^{\alpha_i})) = (q, q_i)$.
- *cacul de* $|Q_n(j)|$: à nouveau le théorème chinois nous ramène à calculer le cardinal de $Q_{p_i^{\alpha_i}}(j)$: or ce dernier ensemble est non nul si et seulement si $(-1)^{\frac{\varphi(p_i^{\alpha_i})}{(2^j q, \varphi(p_i^{\alpha_i}))}} = 1$ ce qui est équivalent à $\frac{2^{k_i} q_i}{2^{\inf(j,k_i)}(q,q_i)}$ car $(2^j q, \varphi(p_i^{\alpha_i})) = 2^{\inf(j,k_i)}(q, q_i)$; en effet comme p_i divise n, et que n est premier avec $n - 1 = 2^k q$ alors p_i est premier avec $n - 1$. Ainsi $Q_{p_i^{\alpha_i}}(j)$ est non vide si et seulement si $j < k_i$ et dans ce cas son cardinal est $2^j(q, q_i)$. Finalement si $j \geqslant k_1$ alors $Q_n(j)$ est vide et si $j < k_1$ alors $|Q_n(j)| = 2^{jr}(q, q_1) \cdots (q, q_r)$. En outre comme $p_i \equiv 1 \bmod 2^{k_i}$ alors $n \equiv 1 \bmod 2^{k_1}$ soit $k_1 \leqslant k$. Ainsi on obtient

$$\sum_{0 \leqslant j < k} |Q_n(j)| = \sum_{0 \leqslant j < k_1} |Q_n(j)| = \prod_{i=1} r(q, q_i) \sum_{0 \leqslant j < k_1} 2^{jr}$$

d'où le résultat en y ajoutant le calcul du cardinal de P_n.
exemple: pour $n = 561$, on obtient $|B_{561}| = 10$ de sorte qu'outre ± 1, il ne reste plus que 8 entiers qui font croire que 561 est premier et le rapport $\frac{|B_{561}|}{\varphi(561)} = 1/32$ est relativement faible.

On obtient ainsi

$$\frac{|B_n|}{\varphi(n)} = \frac{1 + \frac{2^{k_1 r} - 1}{2^r - 1}}{2^{k_1 + \cdots + k_r}} K$$

si l'on minore $k_1 + \cdots + k_r$ par rk_1, on obtient l'inégalité demandée; si en outre tous les k_i ne sont pas égaux k_1, on peut minorer $k_1 + \cdots + k_r$ par $rk_1 + 1$.

(γ) Dans le cas où $n = p^\alpha$, on obtient alors $\frac{|B_n|}{\varphi(n)} \leqslant (q, q_1)/q_1 \leqslant 1/p_1^{\alpha_1 - 1}$ ce qui donne si $p_1 \geqslant 5$, $\frac{|B_n|}{\varphi(n)} \leqslant 1/5$ et si $p_1 = 3$, $\frac{|B_n|}{\varphi(n)} \leqslant 1/9$ sauf pour $\alpha = 2$, i.e. $n = 9$ auquel cas $B_9 = \{1, -1\}$ et $\varphi(9) = 6$ soit $\frac{|B_9|}{\varphi(9)} = 1/3$.

Dans le cas général, le rapport $\frac{1 + \frac{2^{k_1 r} - 1}{2^r - 1}}{2^{rk_1}}$ qui intervient dans la majoration, est décroissant en k_1; on peut donc le remplacer par $1/2^{r-1}$, soit

$$\frac{|B_n|}{\varphi(n)} \leqslant \frac{1}{2^{r-1}} \prod_{i=1}^r \frac{1}{p_i^{\alpha_i}}$$

Si l'un des α_i est supérieur ou égal à 2, alors $\prod_{i=1}^r \frac{1}{p_i^{\alpha_i - 1}} \leqslant 1/3$ et donc $\frac{|B_n|}{\varphi(n)} \leqslant 1/6$. On suppose donc dans la suite que tous les α_i sont égaux à 1:
cas $r \geqslant 3$: l'inégalité $\frac{|B_n|}{\varphi(n)} \leqslant 1/4$ est alors immédiate et l'égalité est obtenue pour $r = 3, k_1 = k_2 = k_3 = 1$ et $q_i | q$ autrement dit si la décomposition primaire de n est $(1+2q_1)(1+2q_2)(1+2q_3)$.
cas $r = 2$ *et* $k_1 < k_2$ d'après ce qui précède on a la majoration $\frac{|B_n|}{\varphi(n)} \leqslant \frac{1}{2^2} \prod_{i=1}^2 \frac{(q,q_i)}{q_i} \leqslant 1/4$, l'égalité étant obtenue si et seulement si $k_1 = 1, k_2 = k_1 + 1 = 2$, q_1 et q_2 divisent q soit $q_1 = q_2$ et la décomposition primaire de n est $(1 + 2q_1)(1 + 4q_1)$, ce qui est le cas étudié plus haut.
cas $r = 2$ *et* $k_1 = k_2$ on a la majoration $\frac{|B_n|}{\varphi(n)} \leqslant \frac{1}{2} \prod_{i=1}^2 \frac{(q,q_i)}{q_i}$. Or q_1 et q_2 ne peuvent pas tous deux diviser q; en effet on a

$$n - 1 = 2^k q = p_1 p_2 - 1 = (1 + 2^{k_1} q_1)(1 + 2^{k_1} q_2) - 1 = 2^{k_1}(q_1 + q_2) + 2^{2k_1} q_1 q_2$$

et si $q_1 | q$ (resp. $q_2 | q$) entraine $q_1 | q_2$ (resp. $q_2 | q_1$) soit $q_1 = q_2$ puis $p_1 = p_2$ ce qui n'est pas. On en déduit alors $\frac{(q,q_i)}{q_i} \leqslant 1/3$ pour $i = 1$ ou 2 soit $\frac{|B_n|}{\varphi(n)} \leqslant 1/6$.

□

Exercice 1. *Montrez que si $a^n - 1$ est premier alors $a = 2$ et n est premier; $M_p = 2^p - 1$ est appelé un nombre de Mersenne pour p premier. On veut montrer le test de primalité de Lucas-Lehmer: M_q est premier ($q \geqslant 3$ premier) si et seulement si $(2+\sqrt{3})^{2^{q-1}} \equiv -1 \bmod M_q$.*

(i) Montrez que l'anneau $A = \mathbb{Z}[\sqrt{3}]$ est euclidien et caractérisez les unités.

(ii) Remarquez que pour q impair, $M_q \equiv 7 \bmod 12$ et en déduire qu'il existe un premier $p \not\equiv \pm 1 \bmod 12$ divisant M_q et remarquer que p reste irréductible dans $\mathbb{Z}[\sqrt{3}]$. Montrez que si M_q vérifie la congruence ci-dessus, alors $p = M_q$.

(iii) En utilisant la loi de réciprocité quadratique, montrez que 3 est un résidu quadratique modulo $p \neq 2, 3$ si et seulement si $p \equiv \pm 1 \bmod 12$. En supposant M_q est premier, montrez le petit théorème de Fermat suivant dans $\mathbb{Z}[\sqrt{3}]$: $(x+y\sqrt{3})^p \equiv x - y\sqrt{3} \bmod p$. En remarquant que 2 est un carré modulo p, on définit dans $\mathbb{Z}[\sqrt{3}]/(p)$: $\tau = \frac{1+\sqrt{3}}{\sqrt{2}}$ et $\overline{\tau} = \frac{1-\sqrt{3}}{\sqrt{2}}$. A partir des relations $\tau^2 = 2+\sqrt{3}$ et $\tau\overline{\tau} = -1$, en déduire la congruence de l'énoncé.

(iv) Montrez le test de primalité suivant sur M_q pour $q \geqslant 3$ premier: soit $(L_i)_{i \geqslant 0}$ la suite de Lucas-Lehmer définie par $L_0 = 4$ et $L_{i+1} = L_i^2 - 2 \bmod M_q$, alors M_q est premier si et seulement si $L_{q-2} \equiv 0 \bmod M_q$.

Preuve: La factorisation $a^{pq} - 1 = (a^p - 1)(a^{p(q-1)} + \cdots + a^p + 1)$ donne l'implication M_n irréductible alors $a = 2$ et n premier.

(i) On considère le sthasme $v : x + y\sqrt{3} \mapsto |x^2 - 3y^2|$, soit la valeur absolue de la norme N. Soient alors $\alpha, \beta \in\in \mathbb{Z}[\sqrt{3}]$; $\alpha/\beta = r + s\sqrt{3}$ avec $r, s \in \mathbb{Q}$ que l'on approxime par des entiers x, y avec une erreur inférieure à $1/2$: $|x - r| \leqslant 1/2$ et $|y - s| \leqslant 1/2$. On obtient alors $-3/4 \leqslant (r-x)^2 - 3(s-y)^2 \leqslant 1/4$ soit $v(\alpha/\beta - (x+y\sqrt{3})) \leqslant 3/4$ et donc $v(\alpha - \beta(x+y\sqrt{3})) < v(\beta)$.

Si $z \in \mathbb{Z}[\sqrt{3}]$ est inversible alors $N(zz^{-1}) = N(z)N(z^{-1})$ et donc $N(z) \in \mathbb{Z}^\times = \{\pm 1\}$. Réciproquement si $N(x+y\sqrt{3}) = \epsilon = \pm 1$ alors $\epsilon(x - y\sqrt{3})$ est son inverse. En particulier $2+\sqrt{3}$ est inversible d'inverse $2 - \sqrt{3}$.

(ii) On a $M_3 \equiv 7 \bmod 12$; par récurrence supposons $M_n \equiv 7 \bmod 12$ alors $M_{n+2} = (M_n + 1)^4 - 1 \equiv 8^4 - 1 \bmod 12$; or $8^4 - 1 \equiv 3 \bmod 12$, d'où le résultat. Remarquons que 2 et 3 ne divise pas M_q pour q impair, de sorte que si p divise M_q alors $p \equiv \pm 1, \pm 5 \bmod 12$; tous les diviseurs p de M_q ne peuvent pas être congrus à $\pm 1 \bmod 12$ car sinon il en serait de même de M_q. Soit donc p premier divisant M_q avec $p \not\equiv \pm 1 \bmod 12$ et montrons que p reste irréductible dans $\mathbb{Z}[\sqrt{3}]$. On raisonne par l'absurde: $p = \alpha\beta$ soit $p^2 = N(\alpha)N(\beta)$ et $p = \pm N(\alpha)$ car β n'est pas inversible. On en déduit alors $p = \pm(x^2 - 3y^2)$; or comme $x^2 - 3y^2$ est un nombre premier distinct de $\pm 2, \pm 3$, on a alors $x^2 - 3y^2 \equiv 1 \bmod 3$ et $x^2 - 3y^2 \equiv 1 \bmod 4$ soit $p \equiv \pm 1 \bmod 12$ ce qui n'est pas.

Supposons que $(2+\sqrt{3})^{2^{q-1}} \equiv -1 \bmod M_q$, on va alors montrer que $p = M_q$. Comme $\mathbb{Z}[\sqrt{3}]$ est principal, et p est irréductible, alors le quotient $(\mathbb{Z}[\sqrt{3}]/(p))^\times$ est un corps de cardinal p^2. La congruence $(2+\sqrt{3})^{2^{q-1}} \equiv -1 \bmod M_q$ montre alors que l'ordre de $2+\sqrt{3}$ est d'ordre 2^q dans $(\mathbb{Z}[\sqrt{3}]/(p))^\times$; donc 2^q divise $p^2 - 1$. On écrit $M_q = pa$, soit $p^2 \equiv 1 \bmod M_q$ et $ap \equiv -1 \bmod 2^q$ soit $ap \equiv -p^2 \bmod 2^q$. Comme p est inversible modulo 2^q, on obtient $a + p \equiv 0 \bmod 2^q$, or $ap < 2^q \leqslant a + p$ soit $(a-1)p \leqslant a - 1$ soit $a = 1$ et $p = M_q$.

(iii) La loi de réciprocité quadratique donne $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}$; donc 3 est résidu quadratique modulo p si et seulement si $\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}$. Le seul carré modulo 3 autre que 0 est 1, soit $p \equiv 1 \bmod 3$ et $p \equiv 1 \bmod 4$ ou bien $p \equiv 2 \bmod 3$ et $p \equiv 3 \bmod 4$, soit en définitive $p \equiv \pm 1 \bmod 12$.

Comme $p = M_q$ premier est congru à 7 modulo 12, on en déduit que 3 n'est pas un carré modulo p et par conséquent $\sqrt{3}^p = 3^{(p-1)/2}\sqrt{3} \equiv -\sqrt{3} \bmod p$ et donc $(x+y\sqrt{3})^p \equiv x-y\sqrt{3} \bmod p$. On considère les éléments $\tau, \overline{\tau}$ de l'énoncé; $\tau^p = \overline{\tau}$ soit $\tau^{p+1} = -1$ ce qui donne la congruence de l'énoncé $(\tau^2)^{(p+1)/2} \equiv -1 \bmod p$ car $\tau^2 = 2 + \sqrt{3}$.

(iv) En posant $\alpha = 2 + \sqrt{3}$ et $\overline{\alpha} = 2 - \sqrt{3}$, en remarquant que $\alpha\overline{\alpha} = 1$, on montre aisément par récurrence que $L_i = \alpha^{2^i} + \overline{\alpha}^{2^i}$; la congruence $L_i \equiv 0 \bmod n$ est ainsi équivalente à $\alpha^{2^{i+1}} \equiv -1 \bmod n$, d'où le résultat.

□

Exercice 2. *Soit μ la fonction de Möbius sur $\mathbb{N}$ définie comme suit*

$$\mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ s'il existe } p \text{ premier tel que } p^2|n \\ (-1)^r \text{ si } n \text{ est sans facteur carré et si } n = \prod_{i=1}^r p_i \end{cases}$$

Une fonction $f : \mathbb{N}^* \longrightarrow \mathbb{R}$ est dite multiplicative si $f(mn) = f(m)f(n)$ pour n et m premiers entre eux.

(i) Montrez que si f est multiplicative, il en est de même de $g(n) = \sum_{d|n} f(d)$.

(ii) Montrez que μ est multiplicative et que $\sum_{d|n} \mu(d)$ vaut 1 pour $n = 1$ et est nulle si $n > 1$.

(iii) Montrez que pour $g(n) = \sum_{d|n} f(d)$ avec $n \geqslant 1$, on a

$$f(n) = \sum_{d|n} \mu(\frac{n}{d})g(d)$$

c'est la première formule d'inversion de Möbius.

(iv) Réciproquement si $g : \mathbb{N}^* \longrightarrow \mathbb{R}$ est telle que $f(n) = \sum_{d|n} \mu(\frac{n}{d})g(d)$ pour tout n alors $g(n) = \sum_{d|n} f(d)$.

(v) Soit $F : [1, +\infty[\longrightarrow \mathbb{R}$ et $G(x) = \sum_{n=1}^{[x]} F(\frac{x}{n})$. Montrez la deuxième formule de Möebius

$$F(x) = \sum_{1 \leqslant n \leqslant x} \mu(n)G(\frac{x}{n})$$

pour $x \geqslant 1$ et prouvez la réciproque.

Preuve: (i) On calcule pour n et n' premiers entre eux

$$g(nn') = \sum_{k|nn'} f(k) = \sum_{\substack{d|n \\ d'|n'}} f(dd') = \sum_{\substack{d|n \\ d'|n'}} f(d)f(d') = (\sum_{d|n} f(d))(\sum_{d'|n'} f(d'))$$

soit $g(nn') = g(n)g(n')$.

(ii) La multiplicativité de μ est immédiate. Soit alors $n = \prod_{i=1}^r p_i^{\alpha_i} > 1$:

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{1 \leqslant i \leqslant r} \mu(p_i) + \sum_{1 \leqslant i \neq j \leqslant r} \mu(p_i p_j) + \cdots + \mu(p_1 \cdots p_r)$$

$$\sum_{d|n} \mu(d) = 1 - C_r^1 + C_r^2 + \cdots (-1)^r = (1-1)^r = 0$$

Le cas $n = 1$ est trivial.

(iii) Soit $n \geqslant 1$. On a

$$\begin{aligned} \textstyle\sum_{d|n} \mu(d) g(n/d) &= \textstyle\sum_{d|n} \mu(d) (\sum_{d'|\frac{n}{d}} f(d')) = \sum_{dd'|n} \mu(d) f(d') \\ &= \textstyle\sum_{d'|n} f(d') (\sum_{d|\frac{n}{d'}} \mu(d)) = f(n) \end{aligned}$$

(iv) Pour $n \geqslant 1$, on a

$$\begin{aligned} \textstyle\sum_{d|n} f(d) &= \textstyle\sum_{d|n} (\sum_{d'|\frac{n}{d}} \mu(d') g(\frac{n}{dd'})) = \sum_{dd'|n} \mu(d') g(\frac{n}{dd'}) \\ &= \textstyle\sum_{\substack{k|n \\ l|k}} \mu(l) g(\frac{n}{k}) = \sum_{k|n} g(\frac{n}{k}) (\sum_{l|k} \mu(l)) = g(n) \end{aligned}$$

(v) Pour $x \geqslant 1$, on a

$$\begin{aligned} \textstyle\sum_{n=1}^{[x]} \mu(n) G(\frac{x}{n}) &= \textstyle\sum_{n=1}^{[x]} \mu(n) (\sum_{m=1}^{[x/n]} F(\frac{x}{nm})) = \sum_{\substack{1 \leqslant n \leqslant x \\ 1 \leqslant m \leqslant x/n}} \mu(n) F(\frac{x}{nm}) \\ &= \textstyle\sum_{1 \leqslant mn \leqslant x} \mu(n) F(\frac{x}{nm}) = \sum_{\substack{1 \leqslant k \leqslant n \\ n|k}} \mu(n) F(\frac{x}{k}) \\ &= \textstyle\sum_{k=1}^{[x]} F(\frac{x}{k}) (\sum_{n|k} \mu(n)) = F(x) \end{aligned}$$

La réciproque se prouve de manière identique en intervertissant le rôle de F et G.

□

Exercice 3. *Pour d entier et x réel, soit $H_d^x = \{(u,v) \in \mathbb{N}^2 \ / \ 1 \leqslant u, v \leqslant x, \ (u,v) = d\}$. On va montrer le théorème de Dirichlet, à savoir que*

$$\lim_{n \to +\infty} \frac{|H_1^n|}{n^2} = \frac{6}{\pi^2}$$

(i) Montrez que $|H_1^x| = \sum_{k \geqslant 1} \mu(k) [x/k]^2$, où μ est la fonction de Möbius (cf. l'exercice précédent).

(ii) Montrez que $\lim_{n \to +\infty} \frac{|H_1^n|}{n^2} = \sum_{k=1}^{\infty} \mu(k)/k^2$ et conclure en remarquant que $(\sum_{k=1}^{\infty} \mu(k)/k^2)(\sum_{k=1}^{\infty} 1/k$ 1.

Preuve: (i) L'ensemble des couples d'entiers strictement positifs et inférieurs ou égaux à x est la réunion disjointe des ensembles H_d^x pour d variant de 1 à $[x]$, d'où l'égalité

$$[x]^2 = \sum_{d=1}^{[x]} |H_d^x| = \sum_{d=1}^{[x]} |H_1^{x/d}|$$

car H_d^x est en bijection avec $H_1^{x/d}$. En appliquant à cette expression, la formule d'inversion de Möbius aux fonctions $F(x) = [x]^2$ et $G(x) = |H_1^x|$, on obtient le résultat de l'énoncé.

(ii) Les séries de l'énoncé sont clairement absolument convergentes de sorte que pour prouver l'égalité des limites, il suffit d'évaluer la différence entre les termes génériques de ces deux suites et de montrer qu'elle tend vers 0. On a

$$\sum_{k=1}^{n} \frac{\mu(k)}{k^2} - \frac{q_n}{n^2} = \sum_{k=1}^{n} \mu(k) (1/k^2 - \frac{[n/k]^2}{n^2})$$

Or on a $0 \leqslant 1/k - [n/k]/n \leqslant n$ et donc

$$0 \leqslant \frac{1}{k^2} - \frac{1}{n^2} \times [\frac{n}{k}]^2 = (\frac{1}{k} - \frac{1}{n}[\frac{n}{k}])(\frac{1}{k} + \frac{1}{n}[\frac{n}{k}]) \leqslant \frac{1}{n}\frac{2}{k}$$

On obtient ainsi

$$|\frac{q_n}{n^2} - \sum_{k=1}^{n} \frac{\mu(k)}{k^2}| \leqslant \frac{2}{n} \sum_{k=1}^{n} \frac{1}{k} \leqslant \frac{2 \ln\ n}{n}$$

quantité qui tend vers 0 quand n tend vers l'infini.

Pour montrer l'égalité $(\sum_{k=1}^{\infty} \mu(k)/k^2)(\sum_{k=1}^{\infty} 1/k^2) = 1$, du fait que ces séries convergent absolument, on peut modifier l'ordre des sommations, en particulier de la manière suivante:

$$(\sum_{k=1}^{\infty} \mu(k)/k^2)(\sum_{m=1}^{\infty} 1/m^2) = \sum_{k=1}^{\infty} \sum_{m=1}^{\infty} \frac{\mu(k)}{m^2 k^2} = \sum_{d=1}^{\infty} (\sum_{k|d} \mu(k)) \times \frac{1}{d^2}$$

or la somme $\sum_{k|d} \mu(k)$ est nulle sauf pour $d = 1$; le résultat découle alors de l'égalité $\sum_{k=1}^{\infty} 1/k^2 = \pi^2/6$.

□