Sorbonne Université
Année universitaire 2023-2024, master 1, *Théorie des nombres 1.* Corrigé de certains exercices de la feuille de TD numéro 3.

Exercice 1

Question (1). La théorie générale des morphismes depuis un groupe cyclique (corrigé de la feuille 2, exercice 4, préliminaires) assure que $\psi \mapsto \psi(1)$ établit un isomorphisme de groupes entre $\widehat{\mathbb{F}}_p$ et le groupe μ_p des racines p-ièmes de l'unité dans $\mathbb{C}^\times$, sa réciproque envoyant une racine ω sur $x \mapsto \omega^x$, qui est bien définie puisque ω est de p-torsion. Comme ξ est un générateur de μ_p l'application $a \mapsto \xi^a$ établit un isomorphisme de groupes entre $\mathbb{F}_p$ et μ_p. Il s'ensuit que $a \mapsto (x \mapsto (\xi^a)^x = \xi^{ax}$ établit un isomorphisme de groupes entre $\mathbb{F}_p$ et $\widehat{\mathbb{F}_p}$. Autrement dit, $a \mapsto \psi_a$ établit un isomorphisme de groupes entre $\mathbb{F}_p$ et $\widehat{\mathbb{F}_p}$, ce qu'il fallait démontrer.

Question (2). Soit $x \in \mathbb{F}_p$. On a

$$\begin{aligned}\sum_a \widehat{f}(a)\psi_a(x) &= \frac{1}{p}\sum_a\sum_t f(t)\psi_{-a}(t)\psi_a(x)\\ &= \frac{1}{p}\sum_a\sum_t f(t)\xi^{a(x-t)}\\ &= \frac{1}{p}\sum_t f(t)\sum_a(\xi^{(x-t)})^a.\end{aligned}$$

Or si ω est un élément de μ_p l'on a $\sum_{a\in\mathbb{F}_p}\omega^a = \sum_{a=0}^{p-1}\omega^a$. Si $\omega = 1$ cette somme vaut p, sinon elle vaut $(1-\omega^p)/(1-\omega) = 0$. Comme $\xi^{x-t} = 1$ si et seulement si $x = t$ (dans $\mathbb{F}_p$), il vient

$$\sum_a \widehat{f}(a)\psi_a(x) = \frac{1}{p}(pf(x)) = f(x).$$

Ceci valant pour tout x on a bien $f = \sum \widehat{f}(a)\psi_a$.

Question (3). On a les égalités

$$\begin{aligned}\widehat{f}(a) &= \frac{1}{p}\sum_t f(t)\xi^{-at}\\ &= \frac{1}{p}\sum_t \left(\frac{t}{p}\right)\xi^{-at}\\ &= g_{-a}.\end{aligned}$$

Il vient

$$\begin{aligned}\sum_a g_a &= \sum_a g_{-a}\\ &= \sum_a \widehat{f}(a)\end{aligned}$$

$$
\begin{aligned}
&= \sum_a \widehat{f}(a) \cdot 1 \\
&= \sum_a \widehat{f}(a)\psi_a(0) \\
&= f(0) \\
&= 0
\end{aligned}
$$

(l'avant-dernière égalité provient de la question 2).

Commentaires. Lorsqu'on munit le $\mathbb{C}$-espace vectoriel des applications de $\mathbb{F}_p$ dans $\mathbb{C}$ du produit hermitien

$$(f, g) \mapsto \langle f, g\rangle := \frac{1}{p}\sum_a f(a)\overline{g}(a),$$

les caractères de $\mathbb{F}_p$ en forment une base orthonormée (feuille 2, exercice 5). En remarquant que $\widehat{f}(a)$ est pour tout a égal à $\langle f, \psi_a\rangle$, on voit que la formule démontrée en (2) est simplement l'énoncé classique selon lequel on obtient les coordonnées d'un vecteur dans une base orthonormée en calculant son produit hermitien avec chacun des vecteurs de la base.

Exercice 2

Commençons par une remarque. Comme un caractère de Dirichlet prend ses valeurs dans le groupes des racines de l'unité, il est réel si et seulement s'il est à valeurs dans $\{-1, 1\}$. Le groupe $\mathbb{F}_p^\times$ est cyclique de cardinal $p-1$, et $(-1)^{p-1} = 1$ puisque p est impair. La théorie générale des morphismes depuis un groupe cyclique assure donc qu'il y a exactement deux caractères de $\mathbb{F}_p^\times$ à valeurs dans $\{-1, 1\}$ à savoir le caractère trivial, et celui qui envoie un générateur fixé de $\mathbb{F}_p^\times$ sur (-1). Il y a donc un et un seul morphisme non trivial de $\mathbb{F}_p^\times$ dans $\{-1, 1\}$, qui coïncide nécessairement avec $x \mapsto \left(\frac{x}{p}\right)$.

Le cas du caractère trivial Supposons que $\chi(k) = 1$ pour tout k. La somme étudiée, considérée modulo p, s'écrit alors $\sum_{k\in\mathbb{F}_p} k$. Soit E l'ensemble des orbites de $\mathbb{F}_p$ sous l'action de $\{-1, 1\}$ par multiplication. On a

$$\sum_{k\in F_p} k = \sum_{O\in E}\sum_{k\in O} k.$$

Or pour toute $O \in E$ on a $\sum_{k\in O} k = 0$ car O est ou bien égale à $\{0\}$, ou bien de la forme $\{x, -x\}$ avec x non nul (auquel cas $x \neq (-x)$ car $(-1) \neq 1$ puisque p est impair). La somme calculée est donc bien nulle modulo p. (Variante de l'argument : comme la multiplication par (-1) est une bijection de $\mathbb{F}_p$ sur lui-même, on a $\sum_{k\in\mathbb{F}_p} k = \sum_{k\in\mathbb{F}_p}(-k) = -\sum_{k\in\mathbb{F}_p} k$. Puisque $1 \neq (-1)$ dans $\mathbb{F}_p$, on en déduit que $\sum_{k\in\mathbb{F}_p} k = 0$.)

Le cas du symbole de Legendre Supposons maintenant que $\chi(k) = \left(\frac{k}{p}\right)$ pour tout k. La somme étudiée, considérée modulo p, s'écrit alors $\sum_{k\in\mathbb{F}_p}\left(\frac{k}{p}\right) k$,

et comme on a vu ci-dessus que $\sum_{k\in\mathbb{F}_p} k = 0$, on peut récrire cette somme

$$\sum_{k\in\mathbb{F}_p} \left(1+\left(\frac{k}{p}\right)\right) k.$$

Or $1+\left(\frac{k}{p}\right)$ vaut 1 si $k=0$, 0 si k n'est pas un carré et 2 si k est un carré. Or 0 a exactement une racine carrée (lui-même) dans $\mathbb{F}_p$ et tout carré non nul de $\mathbb{F}_p$ a exactement deux racines carrées dans $\mathbb{F}_p$. On peut donc écrire

$$\left(1+\left(\frac{k}{p}\right)\right) k = \sum_{y\in\mathbb{F}_p, y^2=k} y^2.$$

Par conséquent on a

$$\begin{aligned}
\sum_{k\in\mathbb{F}_p} \left(\frac{k}{p}\right) k &= \sum_{k\in\mathbb{F}_p} \left(1+\left(\frac{k}{p}\right)\right) k \\
&= \sum_{k\in\mathbb{F}_p} \sum_{y\in\mathbb{F}_p, y^2=k} y^2 \\
&= \sum_{y\in\mathbb{F}_p} y^2 \\
&= \sum_{y=0}^{p-1} y^2 \\
&= \frac{(p-1)p(2p-1)}{6}.
\end{aligned}$$

Or $(p-1)(2p-1)$ est pair puisque $(p-1)$ est pair, et il est multiple de 3 car comme $p \geqslant 5$ on a ou bien $p = 1$ modulo 3 ou bien $2p = -p = 1$ modulo 3, si bien que 3 divise $(p-1)(2p-1)$. En conséquence 6 divise $(p-1)(2p-1)$ (puisque 2 et 3 sont premiers entre eux), si bien que

$$\frac{(p-1)p(2p-1)}{6} = p \cdot \frac{(p-1)(2p-1)}{6}$$

est multiple de p, ce qu'il fallait démontrer.

Le cas $p = 3$. Le résultat établi ci-dessus ne vaut plus dans ce cas. On a en effet

$$\sum_{k\in\mathbb{F}_3} \left(\frac{k}{3}\right) k = 1 + 1 = 2$$

qui est non nul modulo 3. Notez que c'est uniquement à sa toute fin que la démonstration ci-dessus prend l'eau dans le cas $p = 3$, le problème venant du fait que $(3-1)(2\cdot 3-1) = 10$ n'est pas nul modulo 3.

Exercice 4

Nous allons commencer par l'exercice 4, dont l'exercice 3 sera une conséquence facile.

Question (1). Nous allons également montrer (ce n'était pas demandé) que le produit de convolution est commutatif.

La formule $f * g = (n) = \sum_{d_1,d_2,d_1d_2=n} f(d_1)g(d_2)$ est manifestement symétrique en f et g, ce qui montre la commutativité de $*$.

Donnons-nous trois fonctions f, g et h de $\mathbb{N}^\times$ vers $\mathbb{C}$. On a alors pour tout entier non nul n les égalités

$$\begin{aligned}
(f*(g*h))(n) &= \sum_{a,b,ab=n} f(a)(g*h)(b) \\
&= \sum_{a,ab=n} f(a) \sum_{c,d,cd=b} g(c)h(d) \\
&= \sum_{a,c,d,acd=n} f(a)g(c)h(d) \\
&= \sum_{e,d,ed=n} \left(\sum_{a,c,ac=e} f(a)g(c) \right) h(d) \\
&= \sum_{e,d,ed=n} (f*g)(e)h(d) \\
&= ((f*g)*h)(n).
\end{aligned}$$

On a bien ainsi $f*(g*h) = (f*g)*h$, et le produit de convolution est donc associatif.

On a enfin pour toute fonction f de $\mathbb{N}^\times$ vers $\mathbb{C}$ l'égalité

$$(f*\delta_1)(n) = \sum_{d|n} f(d)\delta_1(n/d) = f(n)$$

car $\delta(n/d) = 1$ si $d = n$ et 0 sinon. Ainsi $f*\delta_1 = f$ et on a aussi $\delta_1 * f = f$ par commutativité ; par conséquent, δ_1 est neutre pour la loi $*$.

Question (2). Notons $\mathbf{1}$ la fonction constante égale à 1. Soit n un entier. On souhaite montrer que $(\mu * \mathbf{1})(n) = \delta_1(n)$. Or on a

$$(\mu*\mathbf{1})(n) = \sum_{d|n} \mu(d)\cdot 1 = \sum_{d|n} \mu(d).$$

Il s'agit donc de montrer que ce dernier terme vaut 0 si $n > 1$ et 1 sinon. Écrivons $n = \prod_{1\leqslant i\leqslant r} p_i^{n_i}$ où les p_i sont des nombres premiers deux à deux distincts et les n_i des entiers strictement positifs. Les diviseurs de n sont les entiers de la forme $\prod p_i^{m_i}$ avec $m_i \leqslant n_i$ pour tout i et si d est un tel entier alors $\mu(d) = 0$ dès que l'un des m_i est supérieur où égal à 2. Il en résulte que $\sum_{d|n} \mu(d)$ peut se récrire

$$\sum_{I\subset\{1,\dots,r\}} \mu(\prod_{i\in I} p_i) = \sum_{I\subset\{1,\dots,r\}} (-1)^{|I|}.$$

Nous allons donner deux preuves du fait que cette dernière somme vaut 0 si $n > 1$, c'est-à-dire si $r > 0$, et 1 sinon.

La première preuve consiste à ranger les parties de $\{1,\dots,r\}$ selon leur cardinal. On écrit

$$\begin{aligned}\sum_{I\subset\{1,\dots,r\}}(-1)^{|I|} &= \sum_{a\leqslant r}\sum_{I\subset\{1,\dots,r\},|I|=A}(-1)^a\\ &= \sum_{a\leqslant r}\binom{r}{a}(-1)^a\\ &= (1-1)^r\end{aligned}$$

et ce dernier terme vaut 0 si $r>0$ mais vaut 1 si $r=0$ (en algèbre on utilise systématiquement la convention $0^0=1$).

La seconde preuve (proposée en TD par l'un d'entre vous) consiste à introduire l'ensemble E_0 des parties de $\{1,\dots,r\}$ de cardinal pair et l'ensemble E_0 des parties de $\{1,\dots,r\}$ e cardinal impair, et à remarquer que

$$\begin{aligned}\sum_{I\subset\{1,\dots,r\}}(-1)^{|I|} &= \sum_{I\in E_0}1+\sum_{I\in E_1}(-1)\\ &= |E_0|-|E_1|.\end{aligned}$$

Si $r=0$ alors $\{1,\dots,r\}$ est vide, et E_0 est alors de cardinal 1 (c'est le singleton $\{\varnothing\}$) alors que E_1 est vide ; la somme cherchée vaut donc bien 1 dans ce cas.

Si $r\geqslant 1$ alors $\{1,\dots,r\}$ est non vide (il contient 1). Soit Φ l'application de $\mathscr{P}(\{1,\dots,r\})$ dans lui-même qui envoie une partie F sur $F\cup\{1\}$ si $1\notin F$ et sur $F\setminus\{1\}$ sinon. Alors Φ est clairement une involution (et en particulier une bijection) qui échange E_0 et E_1, et l'existence de Φ assure que $|E_0|=|E_1|$; par conséquent, la somme étudiée est nulle.

Question (3). Si n est un entier non nul la formule $\sum_{d|n}\varphi(d)=n$ peut se récrire $\sum_{d|n}\varphi(d)\cdot 1=n$, soit encore $(\varphi*\mathbf{1})(n)=n$. On a donc $\varphi*\mathbf{1}=\mathrm{Id}$. Puisque μ est l'inverse de $\mathbf{1}$ pour la convolution par la question précédente il vient $\varphi=\mu*\mathrm{Id}$. (Concrètement cela veut dire qu'on a pour tout entier $n>0$ l'égalité $\varphi(n)=\sum_{d|n}\mu(d)\frac{n}{d}$.)

Question (3bis). Nous avons traité en TD la question suivante, qui ne figurait pas sur la feuille : *montrez que si f et g sont multiplicatives $f*g$ l'est aussi.*

Supposons donc données deux fonctions arithmétiques multiplicatives f et g. Nous allons montrer que $f*g$ est encore multiplicative. La clef de la preuve est le fait suivant, qu'on démontre aisément à l'aide de la décomposition en produit de facteurs premiers : *si a et b sont deux éléments de $\mathbb{N}^\times$ premiers entre eux, l'application $(c,d)\mapsto cd$ établit une bijections entre* $\mathrm{Div}(a)\times\mathrm{Div}(b)$ *et* $\mathrm{Div}(ab)$, où $\mathrm{Div}(\cdot)$ désigne l'ensemble des diviseurs.

Donnons-nous donc deux entiers a et b non nuls et premiers entre eux. On a

$$\begin{aligned}(f*g)(ab) &= \sum_{d|ab}f(d)g(ab/d)\\ &= \sum_{\lambda|a,\mu|db}f(\lambda\mu)g((a/\lambda)(b/\mu))\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\lambda|a,\mu|db} f(\lambda)f(\mu)g(a/\lambda)g(b/\mu) \\
&= \left(\sum_{\lambda|a} f(\lambda)g(a/\lambda)\right)\left(\sum_{\mu|b} f(\mu)g(b/\mu)\right) \\
&= (f*g)(a)\cdot(f*g)(b),
\end{aligned}
$$

où la seconde égalité utilise la bijection $\mathrm{Div}(a)\times\mathrm{Div}(b)\simeq\mathrm{Div}(ab)$ décrite ci-dessus, et la troisième le caractère multiplicatif de f et g. Par conséquent, $f*g$ est multiplicative, comme annoncé.

Question (4). Pour comprendre ce qui se passe, calculons tout d'abord la fonction $\mathbf{1}^{*2} := \mathbf{1}*\mathbf{1}$. On a pour tout entier $n>0$ l'égalité

$$\mathbf{1}^{*2}(n) = \sum_{d|n} 1\cdot 1 = |\mathrm{Div(n)}|.$$

Ainsi $\mathbf{1}^{*2}$ est la fonction de comptage des diviseurs.

Calculons maintenant $\mathbf{1}^{*3}$. On a pour tout entier $n>0$ l'égalité

$$\mathbf{1}^{*3}(n) = \sum_{d|n} \mathbf{1}^{*2}(d)\cdot 1 = \sum_{d|n} |\mathrm{Div}(d)|.$$

Pour bien comprendre ce qui se passe, nous allons réinterpréter le terme $\sum_{d|n}|\mathrm{Div}(d)|$. On peut le récrire $\sum_{d|n}\sum_{\delta|d}1$; c'est donc le nombre de couples (δ,d) formé de deux entiers >0 tels que $\delta|d|n$. Une récurrence immédiate montre alors que $\mathbf{1}^*k(n)$ est égal pour tout $k\geqslant 1$ à l'ensemble des $(k-1)$-uplets $d_1,d_2,\ldots,d_{k-1}$ d'entiers >0 tels que $d_1|d_2|\ldots|d_{k-1}|n$ (le cas limite $k=1$ correspond à celui des 0-uplets et il n'y en a qu'un, la *famille vide* ; si vous n'aimez pas ça, commencez à $k=2$).

Nous allons maintenant expliquer comment donner une formule explicite pour ce cardinal. Commençons par le cas où $n=p^r$ pour un certain p premier et un certain entier $r\geqslant 1$. L'ensemble des diviseurs de n est alors en bijection comme ensemble ordonné avec $\{0,\ldots,r\}$ (à un entier i de cet ensemble correspond le diviseur p^i). On cherche donc le cardinal de l'ensemble des suites d'entiers $i_1,\ldots,i_{k-1}$ telles que $0\leqslant i_1\leqslant i_2\ldots\leqslant i_{k-1}\leqslant r$. Le calcul semble *a priori* délicat en raison des inégalités larges et donc des multiples cas d'égalité à distinguer. L'astuce pour contourner l'obstacle consiste à remarquer que notre ensemble de suites croissantes $i_1\leqslant i_2\ldots\leqslant i_{k-1}$ est en bijection avec l'ensemble des suites *strictement croissantes* $j_1<j_2<\ldots j_{k-1}$ d'entiers compris entre 0 et $r+k-2$: la bijection envoie la suite croissante $i_1\leqslant i_2\ldots\leqslant i_{k-1}$ sur la suite strictement croissante $i_1<i_2+1<i_3+2<\ldots<i_{k-1}+k-2$, et sa réciproque envoie la suite strictement croissante $j_1<j_2\ldots<j_{k-1}$ sur la suite croissante $j_1\leqslant j_2-1\leqslant j_3-2\leqslant\ldots\leqslant j_{k-1}+k-2$. Or l'ensemble des suites strictement croissantes de longueur $k-1$ d'entiers compris entre 0 et $r+k-2$ s'identifie au nombre de parties à $k-1$ éléments de $\{0,\ldots,r+k-2\}$ (on fait correspondre à une partie la suite de ses éléments rangés dans l'ordre croissant), qui est de cardinal $\binom{r+k-1}{k-1}$.

On a donc démontré que

$$\mathbf{1}^{*k}(p^r) = \binom{r+k-1}{k-1}$$

pour tout $k \geqslant 1$.

Soit maintenant n un entier non nul quelconque. Écrivons $n = \prod p_i^{r_i}$, où les p_i sont premiers deux à deux distincts et les r_i sont des entiers > 0. Comme $\mathbf{1}$ est clairement multiplicative, il en va de même de $\mathbf{1}^{*k}$ pour tout $k \geqslant 1$ en vertu de la question (3bis) ci-dessus (et à l'aide d'une récurrence immédiate). Il vient

$$\begin{aligned}\mathbf{1}^{*k}(n) &= \mathbf{1}^{*k}(\prod_i p_i^{r_i}) \\ &= \prod_i \mathbf{1}^{*k}(p_i^{r_i}) \\ &= \prod_i \binom{r_i + k - 1}{k-1},\end{aligned}$$

où la seconde égalité provient de la multiplicativité et la troisième du cas p^r traité plus haut.

Question (5). Il fallait ici supposer que $\sum f(n)$ et $\sum g(n)$ convergent *absolument*. Dans ce cas la famille $((f(n)g(m))_{(n,m)\in(\mathbb{N}^\times)^2)}$ est sommable et

$$\sum_{(n,m)\in(\mathbb{N}^\times)^2)} f(n)g(m) = \left(\sum_{n>0} f(n)\right)\left(\sum_{m>0} g(m)\right).$$

Nous allons maintenant réarranger les termes de $\sum_{n,m} f(n)g(m)$ en les rangeant selon la valeur du produit nm, l'opération étant licite puisque la famille est sommable, et toutes les séries qui apparaissent au cours des calculs sont absolument convergentes. Il vient

$$\begin{aligned}\left(\sum_{n>0} f(n)\right)\left(\sum_{m>0} g(m)\right) &= \sum_{n,m} f(n)g(m) \\ &= \sum_{\ell\in\mathbb{N}^\times} \sum_{m,n,mn=\ell} f(m)g(n) \\ &= \sum_{\ell\in\mathbb{N}^\times} (f*g)(\ell).\end{aligned}$$

Par conséquent $\sum_\ell (f*g)(\ell)$ est absolument convergente et de somme $\left(\sum_{n>0} f(n)\right)\left(\sum_{m>0} g(m)\right)$, ce qu'il fallait démontrer.

Exercice 3

Les séries $\sum_n \frac{1}{n^s}$ et $\sum_n \frac{\mu(n)}{n^s}$ sont absolument convergentes. Pour tout entier n, on pose $f(n) = 1/n^s$ et $g(n) = \mu(n)/n^s$. On a alors pour tout n les égalités

$$\begin{aligned}(f*g)(n) &= \sum_{d_1,d_2,d_1d_2=n} f(d_1)g(d_2) \\ &= \sum_{d_1,d_2,d_1d_2=n} \frac{d_1}{d_1^s}\cdot\frac{\mu(d_2)}{d_2^s} \\ &= \frac{1}{n_s} \sum_{d_1,d_2,d_1d_2=n} 1\cdot\mu(d_2)\end{aligned}$$

$$\begin{aligned} &= \frac{1}{n^s}(\mu * \mathbf{1})(n) \\ &= \frac{\delta_1(n)}{n^s}, \end{aligned}$$

la dernière égalité provenant de la question (2) de l'exercice 4. Autrement dit, $(f * g)(n) = 1$ si $n = 1$, et 0 sinon. L'exercice 5 assure alors que

$$\left(\sum_{n>0} f(n)\right)\left(\sum_{m>0} g(n)\right) = \sum_{n>0}(f * g)(n) = 1,$$

où la dernière égalité résulte du calcul précédent. On a donc bien

$$\sum_{n>0} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)},$$

ce qu'il fallait démontrer.

Exercice subsidiaire

J'ai posé en TD l'exercice suivant. On fixe un entier $k \geqslant 1$. Pour tout entier $n \geqslant 1$, on note $r_k(n)$ le cardinal de l'ensemble des k-uplets $(a_1, \ldots, a_k)$ d'entiers appartenant à $\{1, \ldots, n\}$ et qui sont premiers entre eux dans leur ensemble.

(1) Montrez que $r_k(n) = \sum_{a=1}^{n} \mu(a) \left\lfloor \frac{n}{a} \right\rfloor^k$.

(2) Montrez que si $k \geqslant 2$ alors $\frac{r_k(n)}{n^k}$ tend vers $\frac{1}{\zeta(k)}$ quand n tend vers l'infini.

Question (1). Posons $E = \{1, \ldots, n\}^k$, et notons F le sous-ensemble de E constitué des k-uplets $(a_1, \ldots, a_k)$ tels que les a_i soient premiers entre eux dans leur ensemble. Soient $p_1, \ldots, p_r$ les nombres premiers inférieurs ou égaux à n. Pour tout i entre 1 et r, notons U_i le sous-ensemble de E formé des k-uplets $(a_1, \ldots, a_k)$ tels que chacun des a_i soit multiple de p_i.

La réunion des U_i pour $1 \leqslant i \leqslant r$ est le sous-ensemble de E constitué des k-uplets $(a_1, \ldots, a_k)$ tels que les a_j aient au moins un diviseur premier commun. Par conséquent, $F = E \setminus \bigcup_i U_i$.

Pour tout sous-ensemble I de $\{1, \ldots, r\}$, notons U_I le sous-ensemble $\bigcap_{i \in I} U_i$. Notons que $U_\varnothing = E$, et que U_I peut également se décrire comme le sous-ensemble de E formé des k-uplets $(a_1, \ldots, a_k)$ tels que tous les a_j soient multiples de $p_I := \prod_{i \in I} p_i$. On a alors

$$\begin{aligned} r_k(n) &= |F| \\ &= |E| - |\bigcup U_i| \\ &= |E| - \sum_{I \subset \{1,\ldots,r\}, I \neq \varnothing} (-1)^{|I|+1} |U_I| \\ &= |E| + \sum_{I \subset \{1,\ldots,r\}, I \neq \varnothing} (-1)^{|I|} |U_I| \\ &= \sum_{I \subset \{1,\ldots,r\}} (-1)^{|I|} |U_I|. \end{aligned}$$

Pour tout I, notons V_I le sous-ensemble de $\{1,\dots,n\}$ formé des multiples de p_I. Le cardinal de V_I est $\left\lfloor \frac{n}{p_I} \right\rfloor$, et $U_I = V_I^k$, si bien que $|U_I| = \left\lfloor \frac{n}{p_I} \right\rfloor^k$. Par ailleurs $(-1)^{|I|}$ est égal à $\mu(p_I)$ et si a est un entier compris entre 1 et n qui n'est pas l'un des p_I alors $\mu(a) = 0$ (car a est alors divisible par p_i^2 pour au moins un indice i). ll vient

$$\begin{aligned} r_k(n) &= \sum_{I \subset \{1,\dots,r\}} (-1)^{|I} |U_I| \\ &= \sum_{I \subset \{1,\dots,r\}} \mu(p_I) \left\lfloor \frac{n}{p_I} \right\rfloor^k \\ &= \sum_{a=1}^{n} \mu(a) \left\lfloor \frac{n}{a} \right\rfloor^k. \end{aligned}$$

Question (2). On sait d'après l'exercice 3 que $\sum_{a=1}^{+\infty} \frac{\mu(a)}{a^k} = \frac{1}{\zeta(k)}$. Il suffit donc de démontrer que

$$\left(\sum_{a=1}^{n} \frac{\mu(a)}{a^k} \right) - \frac{r_k(n)}{n^k}$$

tend vers zéro quand n tend vers l'infini. Cette différence est égale à

$$\sum_{a=1}^{n} \mu(a) \left(\frac{1}{a^k} - \frac{1}{n^k} \left\lfloor \frac{n}{a} \right\rfloor^k \right) = \frac{1}{n^k} \sum_{a=1}^{n} \mu(a) \left(\frac{n^k}{a^k} - \left\lfloor \frac{n}{a} \right\rfloor^k \right).$$

On a pour tout a compris entre 1 et n l'encadrement

$$\frac{n}{a} - 1 < \left\lfloor \frac{n}{a} \right\rfloor \leqslant \frac{n}{a}.$$

Il vient

$$\begin{aligned} \left| \frac{1}{n^k} \sum_{a=1}^{n} \mu(a) \left(\frac{n^k}{a^k} - \left\lfloor \frac{n}{a} \right\rfloor^k \right) \right| &\leqslant \frac{1}{n^k} \sum_{a=1}^{n} \left(\frac{n^k}{a^k} - \left\lfloor \frac{n}{a} \right\rfloor^k \right) \\ &\leqslant \frac{1}{n^k} \sum_{a=1}^{n} \left(\frac{n^k}{a^k} - \left(\frac{n}{a} - 1 \right)^k \right) \end{aligned}$$

et il suffit dès lors de montrer que ce dernier terme tend vers zéro quand n tend vers l'infini. On a pour tout a entre 1 et n l'égalité

$$\frac{n^k}{a^k} - \left(\frac{n}{a} - 1 \right)^k = \sum_{j=0}^{k-1} \binom{k}{j} (-1)^{k+1-j} \frac{n^j}{a^j}.$$

Le terme à étudier se récrit donc

$$\frac{1}{n^k} \sum_{j=0}^{k-1} \sum_{a=1}^{n} \lambda_j \frac{n^j}{a^j}$$

où λ_j est une constante ne dépendant ni de n ni de a que nous n'avons pas besoin d'expliciter. Il suffit donc désormais de démontrer que $n^{j-k} \sum_{a=1}^{n} \frac{1}{a^j}$ tend vers zéro quand n tend vers l'infini, pour tout j compris entre 0 et $k-1$. On distingue désormais trois cas :

- ◇ Si $j \geqslant 2$ la série $\sum \frac{1}{a^j}$ est convergente, et n^{j-k} tend vers zéro quand n tend vers l'infini car $j - k < 0$; par conséquent $n^{j-k} \sum_{a=1}^{n} \frac{1}{a^j}$ tend vers zéro quand n tend vers l'infini.
- ◇ Si $j = 1$ la série $\sum \frac{1}{a^j} = \sum \frac{1}{a}$ est divergente, et sa n-ième somme partielle est équivalente à $\log n$. L'expression étudiée est donc équivalente à $n^{1-k} \log n$, et tend dès lors vers zéro quand n tend vers l'infini car $k \geqslant 2$.
- ◇ Si $j = 0$ la série $\sum \frac{1}{a^j} = \sum 1$ est divergente, et sa n-ième somme partielle est égale à n. L'expression étudiée est donc égale à n^{1-k} et tend dès lors vers zéro quand n tend vers l'infini car $k \geqslant 2$.

Application numérique. En particulier la probabilité que deux entiers tirés au hasard soient premiers entre eux vaut $6/\pi^2$, soit 0,6079271…