Voyage au coeur de l'arithmétique

Notations

On appelle **fonction arithmétique** toute fonction de $\mathbb{N}^*$ dans $\mathbb{R}$. L'objectif du problème est d'étudier deux fonctions arithmétiques célèbres : la fonction indicatrice d'Euler et la fonction μ de Möbius, puis d'étudier une opération sur les fonctions arithmétiques : le produit de convolution.

Si a et b sont deux entiers, on note $a \wedge b$ le plus grand commun diviseur de a et b. On notera bien que pour tout $a \geq 1$, $0 \wedge a = a$.

En l'absence de précisions supplémentaires, lorsque que l'on parle de décomposition de $n \in \mathbb{N}^*$ en facteurs premiers :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

il sera implicite que pour tout $i \in [\![1, r]\!]$, les α_i sont des entiers non nuls et les p_i des nombres premiers distincts.

On dit que $n \in \mathbb{N}^*$ a un facteur carré si et seulement s'il existe $k \in \mathbb{N}^*$ tel que k^2 divise n.

On rencontrera souvent le symbole $\sum_{d|n}$, cela signifiera que la somme porte sur les entiers $d \geq 1$ qui divisent n.

A-L'indicatrice d'Euler

Soit $n \in \mathbb{N}^*$, on définit **l'indicatrice d'Euler** par :

$$\varphi(n) = \text{Card}\{k \in [\![0, n-1]\!],\ k \wedge n = 1\}.$$

Autrement dit, $\varphi(n)$ est le nombre d'entiers naturels premiers avec n et inférieurs strictement à n.

1. Calculer $\varphi(n)$ pour $1 \leq n \leq 12$, on présentera les résultats sous forme de tableau et on détaillera le calcul uniquement pour $n = 12$.
2. Montrer que p est premier si et seulement si $\varphi(p) = p - 1$.
3. Soit p premier et $\alpha \in \mathbb{N}^*$.
   (a) Soit $k \in \mathbb{N}^*$, montrer que k et p^α ne sont pas premiers entre eux si et seulement si p divise k.
   (b) Dénombrer les multiples de p compris entre 0 et $p^\alpha - 1$.
   (c) En déduire $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
4. Dans la suite de cette partie, on souhaite trouver une formule pour calculer $\varphi(n)$ pour n quelconque sachant que d'après la question précédente, on connaît une expression de $\varphi(p^\alpha)$ pour p premier. Pour ce faire nous allons d'abord démontrer que φ est une fonction multiplicative, c'est-à-dire que pour $(m, n) \in (\mathbb{N}^*)^2$, on a :

$$m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n).$$

On définit pour tout $n \in \mathbb{N}^*$, l'ensemble :

$$\mathcal{A}(n) = \{k \in [\![0, n-1]\!],\ k \wedge n = 1\}.$$

On se donne désormais $(m, n) \in (\mathbb{N}^*)^2$ premiers entre eux et on définit l'application :

$$\begin{array}{rccc} f & : & \mathcal{A}(mn) & \to & \mathcal{A}(m) \times \mathcal{A}(n) \\ & & x & \mapsto & (r, s) \end{array}$$

où r est le reste de la division euclidienne de x par m et s est le reste de la division euclidienne de x par n.

(a) Justifier que f est bien définie.

(b) On veut montrer que f est injective, pour cela on suppose que $f(x) = f(y) = (r, s)$ avec $(x, y) \in \mathcal{A}(mn)^2$.

i. Ecrire les divisions euclidiennes de x puis y par m et n.

ii. En déduire que mn divise $x - y$.

iii. Démontrer que $|x - y| \leq mn - 1$.

iv. Justifier alors que f est injective.

(c) On veut montrer que f est surjective, pour cela on se donne $(r, s) \in \mathcal{A}(m) \times \mathcal{A}(n)$.

i. Justifier l'existence de deux entiers relatifs u et v tels que $um + vn = 1$.

ii. Vérifier que $a = sum + rvn$ satisfait : $a = r\ [m]$ et $a = s\ [n]$.

iii. En déduire que f est surjective.

(d) Démontrer que φ est multiplicative.

5. Soit $n \geq 2$ et $r \geq 1$, on suppose que la décomposition de n en facteurs premiers s'écrit : $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.

(a) Démontrer que :

$$\varphi(n) = n \prod_{i=1}^{r} \Big(1 - \frac{1}{p_i}\Big).$$

(b) Calculer $\varphi(105)$, $\varphi(120)$ et $\varphi(1000)$.

(c) Démontrer que pour tout $n \geq 3$, $\varphi(n)$ est pair.

6. Le but de cette question est de démontrer le théorème d'Euler qui s'énonce ainsi : soit $n \geq 2$ et $a \in \mathbb{N}$ tel que $a \wedge n = 1$ alors :

$$a^{\varphi(n)} = 1\ [n].$$

(a) Expliquer pourquoi le théorème d'Euler généralise le petit théorème de Fermat.

(b) Soit $a \in [\![0, n-1]\!]$, on dit que a est inversible modulo n si et seulement s'il existe $b \in [\![0, n-1]\!]$ tel que $ab = 1\ [n]$. Démontrer que a est inversible modulo n si et seulement si a est premier avec n.

(c) On note $U(n)$ l'ensemble des éléments inversibles modulo n. Démontrer que $U(n)$ muni de la multiplication modulo n est un groupe. Quel est son cardinal ?

(d) En déduire le théorème d'Euler.

On reviendra à la fonction φ en fin de devoir en démontrant la formule :

$$\sum_{d|n} \varphi(d) = n$$

mais pour cela il va nous falloir introduire dans les parties suivantes des outils plus sophistiqués.

B-Fonctions multiplicatives

Soit f une fonction arithmétique, on dit que f est **multiplicative** si $f(1) \neq 0$ et $f(mn) = f(m)f(n)$ pour tout $(m,n) \in (\mathbb{N}^*)^2$ premiers entre eux. On définit la fonction arithmétique : e_1 qui vaut 1 si $n = 1$ et 0 sinon. On pose également id la fonction arithmétique définie par $id(n) = n$ pour tout $n \in \mathbb{N}^*$. Enfin, on note $\mathbb{1}$ la fonction arithmétique constante égale à 1.

1. Démontrer que e_1, id et $\mathbb{1}$ sont multiplicatives. On notera que d'après la question 4. de la partie A, la fonction φ est également multiplicative.
2. (a) Montrer que si $f(1) = 1$ et si pour tout $n \geq 2$:

$$f\Big(\prod_{i=1}^{r} p_i^{\alpha_i}\Big) = \prod_{i=1}^{r} f(p_i^{\alpha_i}) \quad (*)$$

où $p_1^{\alpha_1}...p_r^{\alpha_r}$ est la décomposition de n en facteurs premiers, alors f est multiplicative.

(b) Réciproquement, montrer que si f est multiplicative alors $f(1) = 1$ et f vérifie $(*)$.

C-La fonction de Möbius

Nous allons à présent définir et étudier une nouvelle fonction arithmétique, **la fonction μ de Möbius**. Elle est définie par $\mu(1) = 1$ et pour tout $n \geq 2$:

$$\mu(n) = \begin{cases} -1 & \text{si } n \text{ est sans facteur carré et a un nombre impair de facteurs premiers distincts} \\ 1 & \text{si } n \text{ est sans facteur carré et a un nombre pair de facteurs premiers distincts} \\ 0 & \text{si } n \text{ a un facteur carré} \end{cases}$$

1. Donner, en détaillant les calculs, les valeurs de $\mu(10)$, $\mu(20)$ et $\mu(210)$.
2. Démontrer que μ est multiplicative.
3. Soit $n \in \mathbb{N}^*$, on considère la décomposition de n en facteurs premiers : $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.
   (a) Donner l'écriture générale d'un diviseur de n en fonction de l'écriture précédente de n en produit de facteurs premiers. A quelle condition un tel diviseur est-il sans facteur carré ?
   (b) Combien y-a-t-il de façons de choisir j nombres premiers distincts parmi les $(p_i)_{1 \leq i \leq r}$ où $j \in [\![0, r]\!]$?
   (c) En déduire que pour tout $n \in \mathbb{N}^*$, $\sum_{d|n} \mu(d) = e_1(n)$.

D-Produit de convolution de Dirichlet

Soient f et g deux fonctions arithmétiques. On pose $f \star g$ que l'on appelle **produit de convolution** de f et g, la fonction arithmétique définie pour tout $n \in \mathbb{N}^*$ par :

$$(f \star g)(n) = \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big).$$

1. Dans cette question, on étudie les propriétés du produit de convolution.
   (a) Montrer que le produit de convolution est commutatif.
   (b) Montrer que e_1 est l'élément neutre du produit de convolution.
   (c) On considère f, g et h des fonctions arithmétiques.

i. Vérifier que pour tout $n \in \mathbb{N}^*$, on a :

$$(f \star (g \star h))(n) = \sum_{d|n} f(d) \sum_{\delta | \frac{n}{d}} g(\delta) h\Big(\frac{n}{d\delta}\Big).$$

ii. En effectuant le changement de variables $d' = d\delta$, montrer que le produit de convolution est associatif.

(d) Pour toute fonction arithmétique f telle que $f(1) \neq 0$, on définit de façon récursive la fonction arithmétique g par $g(1) = \dfrac{1}{f(1)}$ et pour tout $n \geq 2$:

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d \neq n}} g(d) f\Big(\frac{n}{d}\Big).$$

Démontrer que $f \star g = g \star f = e_1$.

2. Soient $(m, n) \in (\mathbb{N}^*)^2$ deux entiers premiers entre eux.

(a) Montrer que tout diviseur positif d de mn peut s'écrire sous la forme $d = ab$ avec a et b deux entiers non nuls premiers entre eux tels que $a|m$ et $b|n$.

(b) En déduire que si f et g sont deux fonctions arithmétiques multiplicatives alors $f \star g$ est multiplicative.

3. Montrer que $\mu \star \mathbb{1} = e_1$, on pourra, en justifiant cela, se contenter de vérifier l'égalité pour les puissances de nombres premiers. Retrouver ainsi le résultat de la question 3.(c) de la partie C : $\displaystyle\sum_{d|n} \mu(d) = 0$, si $n \geq 2$ et vaut 1 si $n = 1$.

4. Démontrer que $\varphi = \mu \star id$, on pourra commencer par remarquer que $\varphi(n) = \displaystyle\sum_{\substack{1 \leq m \leq n \\ m \wedge n = 1}} 1$ et utiliser l'identité démontrée à la question précédente.

E-Formule d'inversion de Möbius

1. Soit f une fonction arithmétique, on définit F une nouvelle fonction arithmétique par :

$$\forall n \in \mathbb{N}^*,\ F(n) = \sum_{d|n} f(d).$$

Démontrer que pour tout : $n \in \mathbb{N}^*$, on a :

$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) F(d).$$

On utilisera de préférence le produit de convolution et les résultats obtenus dans la partie précédente pour traduire puis démontrer les expressions proposées. Cette formule est connue sous le nom **formule d'inversion de Möbius.**

2. En déduire que pour tout $n \in \mathbb{N}^*$, on a :

$$\sum_{d|n} \varphi(n) = n.$$

Vérifier cette formule pour $n = 12$.

A-L'indicatrice d'Euler

Le but de cette partie est d'étudier l'indicatrice d'Euler nommée ainsi en l'honneur du mathématicien suisse qui l'a étudiée en premier. Le point clé est le caractère multiplicatif de φ démontré à la question 4., il suffit ainsi de décomposer un entier n en facteurs premiers pour connaître $\varphi(n)$.

1. Voici les premières valeurs de l'indicatrice d'Euler :

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

Pour $n = 12$, il y a uniquement 4 entiers compris entre 0 et 11 qui sont premiers avec 12, ce sont : 1, 5, 7 et 11.

2. On procède par double implication :

(⇒) On suppose que p est premier, alors pour tout $i \in [\![1, p-1]\!]$, on a $p \wedge i = 1$. Par contre $0 \wedge p = p \neq 1$. Ceci montre que $\varphi(p) = p - 1$.

(⇐) Réciproquement, on suppose que $\varphi(p) = p - 1$ avec $p \in \mathbb{N}^*$. On remarque déjà que $p \geq 2$ puisque $\varphi(1) = 1$. On a alors pour tout $k \in [\![1, p-1]\!]$, $p \wedge k = 1$, ce qui démontre que p n'a pas de diviseur positif autre que 1 ou lui-même. Ceci implique que p est premier.

Finalement :

$$\boxed{p \text{ premier} \Leftrightarrow \varphi(p) = p - 1}$$

3. (a) On procède par double implication :

(⇒) On suppose que k et p^α ne sont pas premiers entre eux, il existe un entier $a \geq 2$ tel que $a|k$ et $a|p^\alpha$. Les seuls diviseurs positifs de p^α sont les p^i où $i \in [\![0, \alpha]\!]$, ainsi $a = p^\beta$ avec $1 \leq \beta \leq \alpha$ et par suite $p|a$. Par transitivité de la relation de divisibilité, on a bien $p|k$.

(⇐) Réciproquement, on suppose que p divise k alors il est clair que k et p^α ne sont pas premiers entre eux, puisque tous deux divisibles par p.

On a montré que :

$$\boxed{k \wedge p^\alpha \neq 1 \Leftrightarrow p|k}$$

(b) Les multiples de p compris entre 0 et $p^\alpha - 1$ sont les cp où c est un entier compris entre 0 et $p^{\alpha-1} - 1$. Déjà il est clair que ces entiers sont bien des multiples de p qui n'excèdent pas $p^\alpha - 1$ puisque :

$$(p^{\alpha-1} - 1)p = p^\alpha - p \leq p^\alpha - 1.$$

Ce sont les seuls car le suivant $p^{\alpha-1}p$ est supérieur à $p^\alpha - 1$. D'où :

$$\boxed{\text{il y a } p^{\alpha-1} \text{ multiples de } p \text{ entre 0 et } p^\alpha - 1}$$

(c) Parmi les p^α entiers $k \in [\![0, p^\alpha - 1]\!]$, ceux qui ne sont pas premiers avec p^α sont les multiples de p d'après la question 3.(a), il y en a $p^{\alpha-1}$ d'après la question 3.(b). Les entiers $k \in [\![0, p^\alpha - 1]\!]$ premiers avec p^α sont donc au nombre de $p^\alpha - p^{\alpha-1}$. Cela revient à dire que :

$$\boxed{\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}}$$

On remarque que l'on retrouve le résultat de la question 2. lorsque $\alpha = 1$.

4. (a) Il s'agit de montrer que $r \in \mathcal{A}(m)$ et $s \in \mathcal{A}(n)$. Démontrons uniquement la première assertion, la seconde s'en déduira par symétrie. Soit $x \in \mathcal{A}(mn)$, effectuons la division euclidienne de x par m, cela donne :

$$x = am + r, \quad \text{avec } a \in \mathbb{N} \text{ et } r \in [\![0, m-1]\!].$$

On a immédiatement $r \in [\![0, m-1]\!]$. De plus r est premier avec m, en effet par l'absurde si $b \geq 2$ est un diviseur commum de m et r alors b divise aussi x, ceci est exclu puisque x est premier avec mn. On vient de montrer que $r \in \mathcal{A}(m)$. Ainsi :

$$\boxed{f \text{ est bien à valeurs dans } \mathcal{A}(m) \times \mathcal{A}(n)}$$

(b) i. D'après le théorème de la division euclidienne, il existe $(a, \tilde{a}, b, \tilde{b}) \in \mathbb{N}^4$ tels que :

$$x = am + r, \quad x = bn + s, \quad y = \tilde{a}m + r \quad \text{et} \quad y = \tilde{b}n + s.$$

ii. On a avec les notations précédentes : $x - y = (a - \tilde{a})m$ et $x - y = (b - \tilde{b})n$.
Ceci montre que $m|x - y$ et $n|x - y$, or m et n sont premiers entre eux donc d'après un corollaire du théorème de Gauss, on a : $mn|x - y$.

iii. Comme x et y appartiennent à $\mathcal{A}(mn)$, on a : $0 \leq x \leq mn - 1$ et $0 \leq y \leq mn - 1$. Par soustraction, on obtient :

$$-(mn-1) \leq x - y \leq mn - 1 \Leftrightarrow |x - y| \leq mn - 1.$$

iv. D'après les deux questions précédentes, on sait que $mn|x - y$ et que $x - y \in [\![-(mn-1), mn-1]\!]$, cela implique que $x - y = 0$. On a montré finalement que pour tout $(x, y) \in \mathcal{A}(mn)^2$, $f(x) = f(y) \Rightarrow x = y$, d'où :

$$\boxed{f \text{ est injective}}$$

(c) i. Les entiers m et n sont premiers entre eux, on a donc la relation de Bézout :

$$um + vn = 1$$

avec $(u, v) \in \mathbb{Z}^2$.

ii. On a les égalités suivantes modulo m :

$$a = sum + rvn = rvn = r(1 - um) = r - rum = r \ [m].$$

De même :

$$a = sum + rvn = sum = s(1 - vn) = s - svn = s \ [n].$$

Ce qui donne le résultat souhaité.

iii. L'entier a semble être un antécédent de (r, s) cependant il n'appartient pas à priori à $\mathcal{A}(mn)$. Effectuons la division euclidienne de a par mn, il existe $q \in \mathbb{Z}$ tel que :

$$a = qmn + \hat{a}, \quad \text{avec} \quad \hat{a} \in [\![0, mn-1]\!].$$

Montrons que $\hat{a}$ est un antécédent de (r, s) par f, on a :

$$\hat{a} = a - qmn = a = r \ [m] \quad \text{et} \quad \hat{a} = a - qmn = a = s \ [n].$$

De plus $\hat{a}$ est premier avec mn, pour le démontrer raisonnons par l'absurde. Si t est un nombre premier qui divise $\hat{a}$ et mn, alors $t|a$ puisque $a = qmn + \hat{a}$. De plus comme t est premier $t|mn \Rightarrow t|m$ ou $t|n$, disons m sans perte de généralité. On reprend alors la relation $a = r \ [m]$ qui montre que t divise également r, ceci est absurde puisque par hypothèse $r \in \mathcal{A}(m)$ donc m et r sont premiers entre eux.
Finalement, on a bien $\hat{a} \in \mathcal{A}(mn)$ et $f(\hat{a}) = (r, s)$, on a démontré que :

$$\boxed{f \text{ est surjective}}$$

(d) Finalement f est bijective, or deux ensembles finis qui sont en bijection ont le même nombre d'éléments, ainsi :

$$\mathrm{Card}(\mathcal{A}(mn)) = \mathrm{Card}(\mathcal{A}(m)) \times \mathrm{Card}(\mathcal{A}(n)).$$

Par définition, cette dernière égalité est exactement :

$$\varphi(mn) = \varphi(m)\varphi(n).$$

On a bien démontré que :

$$\boxed{m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)}$$

On remarque que la réciproque ne tient pas, d'après le tableau de valeurs de la question 1., on a $\varphi(2)\varphi(4) = \varphi(8)$ mais 2 et 4 ne sont pas premiers entre eux.

5. (a) D'après 3.(c), on connaît une expression de $\varphi(p_i^{\alpha_i})$ pour $i \in [\![1, r]\!]$, il s'agit de montrer que :

$$\varphi\Big(\prod_{i=1}^{r} p_i^{\alpha_i}\Big) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i})$$

pour ainsi avoir une formule donnant $\varphi(n)$. Pour ceci on considère l'hypothèse de récurrence pour $r \geq 1$:

$$H_r \ : \text{ Si } (m_i)_{1\leq i\leq r} \in (\mathbb{N}^*)^r \text{ sont premiers entre eux deux à deux alors } \ \varphi\Big(\prod_{i=1}^{r} m_i\Big) = \prod_{i=1}^{r} \varphi(m_i).$$

⋆ Initialisation : la propriété est évidente pour $r = 1$.

⋆ Hérédité : supposons H_r vraie et démontrons H_{r+1}. Pour ceci, considérons une famille d'entiers premiers entre eux deux à deux : $(m_i)_{1\leq i\leq r+1} \in (\mathbb{N}^*)^{r+1}$. On note $m = \prod_{i=1}^{r} m_i$, on va démontrer par l'absurde que m et m_{r+1} sont premiers entre eux. Soit p un nombre premier tel que $p|m$ et $p|m_{r+1}$, alors p divise l'un des $(m_i)_{1\leq i\leq r}$, ceci est absurde car tous les $(m_i)_{1\leq i\leq r}$ sont premiers avec m_{r+1}. La fonction φ étant multiplicative d'après la question 4., on a $m \wedge m_{r+1} = 1$ qui implique que :

$$\varphi(mm_{r+1}) = \varphi(m)\varphi(m_{r+1}) \Leftrightarrow \varphi\Big(\prod_{i=1}^{r+1} m_i\Big) = \varphi\Big(\prod_{i=1}^{r} m_i\Big)\varphi(m_{r+1}) \Leftrightarrow \varphi\Big(\prod_{i=1}^{r+1} m_i\Big) = \Big(\prod_{i=1}^{r} \varphi(m_i)\Big)\varphi(m_{r+1}).$$

En utilisant l'hypothèse de récurrence pour la dernière équivalence. Ce qui achève la récurrence. Revenons à la question, on applique la propriété H_r avec pour tout $i \in [\![1, r]\!]$, $m_i = p_i^{\alpha_i}$ sachant que les entiers de la famille $(p_i^{\alpha_i})_{1\leq i\leq r}$ sont bien premiers entre eux deux à deux. On obtient :

$$\varphi(n) = \varphi\Big(\prod_{i=1}^{r} p_i^{\alpha_i}\Big) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{r} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = \prod_{i=1}^{r} p_i^{\alpha_i}\Big(1 - \frac{1}{p_i}\Big) = n\prod_{i=1}^{r}\Big(1 - \frac{1}{p_i}\Big).$$

On a bien démontré que :

$$\boxed{\varphi(n) = n\prod_{i=1}^{r}\Big(1 - \frac{1}{p_i}\Big)}$$

(b) D'après la proposition précédente, il s'agit dans un premier temps de décomposer les nombres proposés en facteurs premiers :

⋆ $105 = 3 \times 5 \times 7$ d'où $\varphi(105) = \varphi(3)\varphi(5)\varphi(7) = 2 \times 4 \times 6 = 48$.

⋆ $120 = 2^3 \times 3 \times 5$ d'où $\varphi(120) = \varphi(2^3)\varphi(3)\varphi(5) = 4 \times 2 \times 4 = 32$.

⋆ $1000 = 2^3 \times 5^3$ d'où $\varphi(1000) = \varphi(2^3)\varphi(5^3) = 4 \times (5^3 - 5^2) = 4 \times 100 = 400$.

Récapitulons :

$$\boxed{\begin{array}{ccc} \varphi(105) & = & 48 \\ \varphi(120) & = & 32 \\ \varphi(1000) & = & 400 \end{array}}$$

(c) Réutilisons la formule suivante qui a été vue au cours de la démonstration de la question 5.(a) :

$$\varphi(n) = \prod_{i=1}^{r}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1).$$

Il y a deux cas à distinguer :

⋆ S'il existe $i \in [\![1, r]\!]$ tel que p_i soit impair alors $p_i - 1$ est pair et la formule ci-dessus montre que $\varphi(n)$ est pair.

⋆ Dans le cas contraire $n = 2^\beta$ où $\beta \geq 2$, ainsi $\varphi(n) = 2^{\beta-1}$ est pair.

On a montré que :

$$\boxed{\forall n \geq 3,\ \varphi(n) \text{ est pair}}$$

6. (a) Le petit théorème de Fermat est un cas particulier du théorème d'Euler avec n un nombre premier. L'hypothèse $a \wedge n = 1$ se réécrit alors $n \not| a$ et on a bien $\varphi(n) = n - 1$ lorsque n est premier.

(b) On va démontrer ce résultat par double implicitation :

($\Rightarrow$) Supposons l'existence de $b \in [\![0, n-1]\!]$ tel que $ab = 1\ [n]$ alors :

$$\exists k \in \mathbb{Z} \text{ tel que } ab = 1 + kn \Leftrightarrow ab - kn = 1.$$

L'égalité précédente est une relation de Bézout entre a et n, montrant que $a \wedge n = 1$.

($\Leftarrow$) Réciproquement, supposons $a \wedge n = 1$, alors il existe une relation de Bézout : $au + nv = 1$ avec $(u, v) \in \mathbb{Z}^2$. Modulo n la relation devient $au = 1\ [n]$. Prenons $\hat{u}$ le reste de la division euclidienne de u par n, on a toujours $a\hat{u} = 1\ [n]$ et à présent $\hat{u} \in [\![0, n-1]\!]$ comme souhaité. Ceci montre que a est inversible modulo n.

Finalement :

$$\boxed{a \text{ est inversible modulo } n \Leftrightarrow a \text{ est premier avec } n}$$

(c) Vérifions les différentes propriétés requises pour avoir un groupe :

⋆ L'élément neutre est 1 qui est bien inversible modulo n puisque $1.1 = 1\ [n]$.

⋆ La multiplication modulo n est associative.

⋆ Soit $(a, a') \in U(n)^2$, montrons que aa' est inversible modulo n. Il existe $(b, b') \in [\![0, n-1]\!]^2$ tels que $ab = 1\ [n]$ et $a'b' = 1\ [n]$. Ainsi :

$$aa'(b'b) = a.1.b = 1\ [n].$$

Ainsi $aa' \in U(n)$. Il est à noter que si $(a, a') \in [\![0, n-1]\!]^2$, a priori $aa' \notin [\![0, n-1]\!]$, mais il faut comprendre ici que l'on considère toutes les opérations effectuées modulo n, de même pour bb'. On vient de montrer la stabilité par produit.

⋆ Enfin si $a \in U(n)$ alors il existe $b \in [\![0, n-1]\!]$ tel que $ab = 1\ [n]$, ainsi $a^{-1} = b$ et $b \in U(n)$. D'où la stabilité par passage à l'inverse.

$$\boxed{U(n) \text{ est un groupe pour la multiplication modulo } n}$$

D'après la question précédente a est inversible modulo n si et seulement si $a \wedge n = 1$ le cardinal de $U(n)$ est donc $\varphi(n)$.

$$\boxed{\text{Card}(U(n)) = \varphi(n)}$$

(d) D'après le théorème de Lagrange, si G est un groupe fini noté multiplicativement et e son élement neutre, alors pour tout $a \in G$, on a $a^{\text{Card}(G)} = e$. On applique ici ce résultat avec $G = U(n)$ qui est fini et de cardinal $\varphi(n)$, ainsi lorsque $a \wedge n = 1$, on a :

$$\boxed{a^{\varphi(n)} = 1\ [n]}$$

B-Fonctions multiplicatives

Le but de cette courte partie est de généraliser la notion de fonction multiplicative entrevue avec l'exemple de la fonction φ dans la partie précédente.

1. Pour e_1 : il y a deux cas à distinguer, soient m et n deux entiers premiers entre eux :

⋆ Si $m = n = 1$, alors $e_1(mn) = e_1(1) = 1 = e_1(m)e_1(n)$.

⋆ Sinon, sans perte de généralité, supposons que $m \geq 2$. On a $mn \geq 2$, d'où $e_1(mn) = 0 = e_1(m)e_1(n)$ puisque $e_1(m) = 0$.

De plus $e_1(1) \neq 0$ comme réclamé dans la définition d'une fonction multiplicative, d'où :

$$\boxed{e_1 \text{ est multiplicative}}$$

Pour id : On a pour tout $(m, n) \in (\mathbb{N}^*)^2$ premiers entre eux : $id(mn) = mn = id(m)id(n)$. De plus $id(1) \neq 0$, ce qui démontre que :

$$\boxed{id \text{ est multiplicative}}$$

Pour $\mathbb{1}$: On a pour tout $(m, n) \in (\mathbb{N}^*)^2$ premiers entre eux : $\mathbb{1}(mn) = 1 = \mathbb{1}(m)\mathbb{1}(n)$. En outre $\mathbb{1}(1) \neq 0$, on obtient :

$$\boxed{\mathbb{1} \text{ est multiplicative}}$$

2. (a) Déjà, on a bien $f(1) \neq 0$. On considère $(m, n) \in (\mathbb{N}^*)^2$ premiers entre eux, traitons d'abord le cas où l'un des deux, disons m, vaut 1, on a $f(mn) = f(n) = f(1)f(n) = f(m)f(n)$ ce qui est bien l'égalité souhaitée. Supposons à présent que m et n soient supérieurs ou égaux à 2, on considère leurs décomposition en facteurs premiers :

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

Puisque m et n sont premiers entre eux, les $(p_i)_{1\leq i\leq r}$ et les $(q_j)_{1\leq j\leq s}$ sont distincts, ainsi d'après l'hypothèse de la question :

$$f(mn)=f\Big(\Big[\prod_{i=1}^{r}p_i^{\alpha_i}\Big]\Big[\prod_{j=1}^{s}q_j^{\beta_j}\Big]\Big)=\Big[\prod_{i=1}^{r}f(p_i^{\alpha_i})\Big]\Big[\prod_{j=1}^{s}f(q_j^{\beta_j})\Big]=f(m)f(n).$$

Ainsi :

$$\boxed{f \text{ est multiplicative}}$$

(b) On suppose f multiplicative comme $1\wedge 1=1$, on a $f(1)=f(1)f(1)$, or $f(1)\neq 0$ d'où en simplifiant $f(1)=1$. Pour montrer la propriété $(*)$ c'est exactement la même démarche qu'à la question 5.(a) de la partie A, c'est-à-dire à l'aide d'une récurrence, en remplaçant la fonction φ par f. On renvoie à cette question pour plus de détails. Finalement, on a démontré que :

$$\boxed{f \text{ est multiplicative } \Leftrightarrow f(1)=1 \text{ et } f \text{ vérifie } (*)}$$

C-La fonction de Möbius

On va à présent découvrir la fonction de Möbius qui est l'une des fonctions arithmétiques les plus importantes, comme la formule d'inversion de Möbius présentée dans la partie E le mettra en évidence. Möbius est un mathématicien allemand du XIXème siècle, notamment connu pour sa découverte du ruban de Möbius qui est une surface possédant une unique face.

1. La définition de μ indique qu'il va falloir décomposer les entiers proposés en facteurs premiers, on a :
   - $\star$ $10=2\times 5$, d'où $\mu(10)=1$ puisque 10 est sans facteur carré et possède 2 diviseurs premiers.
   - $\star$ $20=2^2\times 5$, d'où $\mu(20)=0$ puisque 20 est divisible par 2^2 donc possède un facteur carré.
   - $\star$ $210=2\times 3\times 5\times 7$, d'où $\mu(210)=1$ puisque 210 est sans facteur carré et possède 4 diviseurs premiers.

   Récapitulons :

$$\boxed{\begin{array}{ccc}\mu(10)&=&1\\ \mu(20)&=&0\\ \mu(210)&=&1\end{array}}$$

2. On va utiliser la caractérisation d'une fonction multiplicative démontrée dans la question 2. de la partie B. Déjà $\mu(1)=1$, il reste à démontrer que μ vérifie $(*)$. Soit $n=\displaystyle\prod_{i=1}^{r}p_i^{\alpha_i}$, montrons que $\mu\Big(\displaystyle\prod_{i=1}^{r}p_i^{\alpha_i}\Big)=\displaystyle\prod_{i=1}^{r}\mu(p_i^{\alpha_i})$.

   Par définition de la fonction μ, on a pour tout $i\in[\![1,r]\!]$, on a :

$$\mu(p_i^{\alpha_i})=\begin{cases}-1 & \text{si } \alpha_i=1\\ 0 & \text{si } \alpha_i\geq 2\end{cases}$$

   Ainsi, on obtient :

$$\prod_{i=1}^{r}\mu(p_i^{\alpha_i})=\begin{cases}(-1)^r & \text{si } \alpha_1=\alpha_2=...=\alpha_r=1\\ 0 & \text{s'il existe } i\in[\![1,r]\!] \text{ tel que } \alpha_i\geq 2\end{cases}$$

C'est exactement la définition de $\mu\Big(\prod_{i=1}^{r} p_i^{\alpha_i}\Big)$. On a utilisé implicitement dans cette étude que :

$$n=\prod_{i=1}^{r} p_i^{\alpha_i} \text{ est sans facteur carré si et seulement si pour tout } i\in[\![1,r]\!],\ \alpha_i=1$$

On vient de démontrer que μ vérifie $(*)$, par suite :

$$\boxed{\mu \text{ est multiplicative}}$$

3. (a) D'après le cours, les diviseurs de n sont tous les entiers de la forme :

$$\prod_{i=1}^{r} p_i^{\beta_i} \text{ avec pour tout } i\in[\![1,r]\!]:\ 0\leq\beta_i\leq\alpha_i.$$

Comme dit précédemment, un tel diviseur est sans facteur carré si et seulement si pour tout $i\in[\![1,r]\!]$: $0\leq\beta_i\leq 1$.

(b) Pour tout $j\in[\![0,r]\!]$, il y a $\binom{r}{j}$ façons de choisir j nombres premiers parmi les $(p_i)_{1\leq i\leq r}$.

(c) Traitons tout de suite le cas particulier où $n=1$, on a $\sum_{d|1}\mu(d)=\mu(1)=1=e_1(1)$.

Supposons à présent $n\geq 2$. Soit d un diviseur de n, si d a un facteur carré comme $\mu(d)=0$ la contribution dans la somme est nulle. Ainsi, en abrégeant sans facteur carré par s.f.c, on a :

$$\sum_{d|n}\mu(d)=\sum_{\substack{d|n\\ d \text{ s.f.c}}}\mu(d)=\sum_{(\beta_i)_{1\leq i\leq r}\in\{0,1\}^r}\mu\Big(\prod_{i=1}^{r}p_i^{\beta_i}\Big).$$

La dernière égalité étant obtenue à l'aide de la caractérisation des diviseurs sans facteur carré de n donnée à la question 3.(a).
D'après la question 3.(b), on obtient :

$$\sum_{d|n}\mu(d)=\sum_{j=0}^{r}\binom{r}{j}(-1)^j=(1-1)^r=0$$

puisque décrire tous les diviseurs de n sans facteur carré revient à énumérer les façons de choisir j diviseurs parmi les $(p_i)_{1\leq i\leq r}$; de plus si t est un produit de j facteurs premiers disctints, on a bien $\mu(t)=(-1)^j$ par définition.
Finalement :

$$\boxed{\sum_{d|n}\mu(d)=e_1(n)}$$

D-Produit de convolution de Dirichlet

Dans cette partie, on étudie une loi de composition interne sur les fonctions arithmétiques qui préserve notamment les fonctions multiplicatives. Dirichlet est un mathématicien allemand du XIXème siècle dont les travaux en arithmétique et sur les séries de Fourier furent primordiaux. Il a en particulier démontré que si a et b sont deux entiers premiers entre eux, il existe une infinité de nombres premiers congrus à a modulo b.

1. (a) Pour montrer la commutativité du produit de convolution, on va effectuer un changement de variable en posant $d' = \dfrac{n}{d}$ où d est un diviseur positif de n. Cette correspondance est bijective car si $d|n$, il existe un unique d' tel que $dd' = n$, avec $(d, d') \in [\![1, n]\!]^2$. Ainsi pour tout $n \in \mathbb{N}^*$, on a :

$$(f \star g)(n) = \sum_{d|n} f(d)g\Big(\frac{n}{d}\Big) = \sum_{d'|n} f\Big(\frac{n}{d'}\Big)g(d') = \sum_{d'|n} g(d')f\Big(\frac{n}{d'}\Big) = (g \star f)(n).$$

Ce qui montre que :

le produit de convolution est commutatif

(b) Soit f une fonction arithmétique, il s'agit de montrer que $f \star e_1 = e_1 \star f = f$. Par commutativité, il suffit de ne montrer qu'une seule de ces relations, on a pour tout $n \in \mathbb{N}^*$:

$$(e_1 \star f)(n) = \sum_{d|n} e_1(d)f\Big(\frac{n}{d}\Big) = e_1(1)f(n) = f(n)$$

ceci puisque la fonction e_1 est nulle sauf en 1. On a montré que $e_1 \star f = f \star e_1 = f$, d'où :

e_1 est l'élément neutre du produit de convolution

(c) i. Soit $n \in \mathbb{N}^*$, on a par définition :

$$(f \star (g \star h))(n) = \sum_{d|n} f(d)(g \star h)\Big(\frac{n}{d}\Big) = \sum_{d|n} f(d) \sum_{\delta|\frac{n}{d}} g(\delta)h\Big(\frac{n}{d\delta}\Big).$$

Ce qui est l'expression souhaitée.

ii. Reprenons l'expression précédente :

$$(f \star (g \star h))(n) = \sum_{d|n} f(d) \sum_{\delta|\frac{n}{d}} g(\delta)h\Big(\frac{n}{d\delta}\Big) = \sum_{\substack{(d,\delta)\in[\![1,n]\!]^2 \\ d\delta|n}} f(d)g(\delta)h\Big(\frac{n}{d\delta}\Big).$$

en effet : $\Big\{(d, \delta) \in [\![1, n]\!]^2,\ d|n \text{ et } \delta|\dfrac{n}{d}\Big\} = \Big\{(d, \delta) \in [\![1, n]\!]^2,\ d\delta|n\Big\}$.

Comme indiqué dans l'énoncé, on effectue le changement d'indice $d' = d\delta$, cela donne :

$$(f \star (g \star h))(n) = \sum_{d'|n} \sum_{d|d'} f(d)g\Big(\frac{d'}{d}\Big)h\Big(\frac{n}{d'}\Big) = \sum_{d'|n} (f \star g)(d')h\Big(\frac{n}{d'}\Big) = ((f \star g) \star h)(n).$$

Le produit de convolution est associatif

(d) Par commutativité du produit de convolution, vérifions uniquement que $g \star f = e_1$. On a :

$$(g \star f)(1) = \sum_{d|1} g(d)f\Big(\frac{1}{d}\Big) = g(1)f(1) = 1 \ \text{ puisque } g(1) = \frac{1}{f(1)}.$$

Pour $n \geq 2$, cela donne :

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d\neq n}} g(d)f\Big(\frac{n}{d}\Big) \Leftrightarrow -g(n)f(1) = \sum_{\substack{d|n \\ d\neq n}} g(d)f\Big(\frac{n}{d}\Big) \Leftrightarrow 0 = \sum_{d|n} g(d)f\Big(\frac{n}{d}\Big) \Leftrightarrow 0 = (g \star f)(n).$$

Finalement :

$$\boxed{f \star g = g \star f = e_1}$$

Dans la question 1, nous avons finalement démontré que l'ensemble des fonctions arithmétiques muni du produit de convolution est un groupe d'élement neutre e_1.

2. (a) On va utiliser la décomposition en facteurs premiers, on a :

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

Comme $m \wedge n = 1$, les $(p_i)_{1\leq i\leq r}$ et les $(q_j)_{1\leq j\leq s}$ sont distincts. L'entier d est un diviseur de mn, ainsi d'après le cours, on a :

$$d = \prod_{i=1}^{r} p_i^{\gamma_i} \prod_{j=1}^{s} q_j^{\delta_j} \quad \text{avec } \forall i \in [\![1, r]\!] : \ 0 \leq \gamma_i \leq \alpha_i \text{ et } \forall j \in [\![1, s]\!] : \ 0 \leq \delta_j \leq \beta_j.$$

On pose alors :

$$a = \prod_{i=1}^{r} p_i^{\gamma_i} \quad \text{et} \quad b = \prod_{j=1}^{s} q_j^{\delta_j}.$$

Il est clair que $a \wedge b = 1$, $a|m$ et $b|n$.

(b) Soient f et g deux fonctions arithmétiques multiplicatives et $(m, n) \in (\mathbb{N}^*)^2$ premiers entre eux, on a :

$$(f \star g)(mn) = \sum_{d|mn} f(d) g\Big(\frac{mn}{d}\Big) = \sum_{a|m} \sum_{b|n} f(ab) g\Big(\frac{m}{a}\frac{n}{b}\Big).$$

On a cette égalité grâce à la question précédente qui démontre que tout diviseur d de mn peut s'écrire $d = ab$ avec $a|m$ et $b|n$ et la réciproque étant bien entendu vraie : $a|m$ et $b|n$ implique que $d = ab|mn$. D'autre part , on sait que $a \wedge b = 1$ et $\dfrac{m}{a} \wedge \dfrac{n}{b} = 1$, d'après la question précédente car m et n sont premiers entre eux. Comme f et g sont multiplicatives, on a :

$$(f \star g)(mn) = \sum_{a|m} \sum_{b|n} f(a) f(b) g\Big(\frac{m}{a}\Big) g\Big(\frac{n}{b}\Big) = \Big[\sum_{a|m} f(a) g\Big(\frac{m}{a}\Big)\Big]\Big[\sum_{b|n} f(b) g\Big(\frac{n}{b}\Big)\Big] = (f \star g)(m) \times (f \star g)(n)$$

De plus $(f \star g)(1) = f(1)g(1) \neq 0$ puisque $f(1) \neq 0$ et $g(1) \neq 0$. On a montré que :

$$\boxed{f \text{ et } g \text{ multiplicatives } \Rightarrow \ f \star g \text{ multiplicative}}$$

3. Les fonctions arithmétiques μ et $\mathbb{1}$ sont multiplicatives, ainsi d'après la question précédente $\mu \star \mathbb{1}$ est multiplicative. D'autre part e_1 est également multiplicative. Pour montrer que deux fonctions multiplicatives sont égales, il suffit de vérifier qu'elles coïncident sur les puissances des nombres premiers, ceci d'après la question 2. de la partie B. On a déjà :

$$(\mu \star \mathbb{1})(1) = \mu(1)\mathbb{1}(1) = 1 = e_1(1).$$

Soit p un nombre premier et $\alpha \geq 1$, on a :

$$\mu \star \mathbb{1}(p^\alpha) = \sum_{d|p^\alpha} \mu(d)\mathbb{1}\Big(\frac{p^\alpha}{d}\Big) = \sum_{d|p^\alpha} \mu(d) = \sum_{i=0}^{\alpha} \mu(p^i) = \mu(1) + \mu(p) = 1 - 1 = 0 = e_1(p^\alpha).$$

D'où l'égalité :

$$\boxed{\mu \star \mathbb{1} = e_1}$$

Ainsi pour tout $n \geq 2$, on a :

$$\mu \star \mathbb{1}(n) = \sum_{d|n} \mu(d) = e_1(n) = 0$$

comme souhaité et si $n = 1$, on a bien $\mu(1) = 1$. Ce qui permet de retrouver les relations de la question 3.(c) de la partie C.

4. Il est clair que $\varphi(n) = \sum_{\substack{1 \leq m \leq n \\ m \wedge n}} 1$, puisque cette somme fait justement le compte des nombres premiers avec n appartenant à $[\![1, n]\!]$. D'autre part, d'après la relation démontrée à la question précédente, on a :

$$\sum_{d|m\wedge n} \mu(d) = \begin{cases} 1 & \text{si } m \wedge n = 1 \\ 0 & \text{si } m \wedge n \geq 2 \end{cases}$$

Ainsi en regroupant les deux formules, on a pour tout $n \geq 1$:

$$\varphi(n) = \sum_{1 \leq m \leq n} \sum_{d|m\wedge n} \mu(d) = \sum_{d|n} \mu(d) \sum_{\substack{1 \leq m \leq n \\ d|m}} 1$$

ceci en intervertissant les deux sommes.
L'expression $\sum_{\substack{1 \leq m \leq n \\ d|m}} 1$ compte le nombre de multiples de d qui sont inférieurs ou égaux à n, il y en a $E\Big(\frac{n}{d}\Big) = \frac{n}{d}$ puisque d divise n. Ce qui donne :

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = \sum_{d|n} \mu(d) id\Big(\frac{n}{d}\Big)$$

Cela s'écrit plus simplement :

$$\boxed{\varphi = \mu \star id}$$

E-Formule d'inversion de Möbius et applications

Cette partie démontre la très importante formule d'inversion de Möbius. La démonstration est quasiment immédiate avec l'étude précise du produit de convolution faite dans la partie précédente. Quelques applications de cette formule sont ensuite présentées.

1. Soit $n \in \mathbb{N}^*$, on a d'après l'énoncé :

$$F(n) = \sum_{d|n} f(d) = \sum_{d|n} f(d)\mathbb{1}\Big(\frac{n}{d}\Big) = (f \star \mathbb{1})(n).$$

Ainsi F et f sont liées par la relation : $F = f \star \mathbb{1}$. Multiplions cette relation par μ et utilisons l'associativité du produit de convolution :

$$F \star \mu = (f \star \mathbb{1}) \star \mu = f \star (\mathbb{1} \star \mu) = f \star e_1 = f$$

ceci puisque $\mathbb{1} \star \mu = e_1$ d'après la question 3. de la partie D.

Explicitons la formule obtenue, pour tout $n \in \mathbb{N}^*$, on a :

$$f(n) = (F \star \mu)(n) = \sum_{d|n} F(d)\mu\Big(\frac{n}{d}\Big).$$

On vient de démontrer la formule d'inversion de Möbius :

$$\boxed{F(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)F(d)}$$

C'est bien une équivalence, puisque la démonstration consiste à effectuer le produit de convolution par μ, on peut remonter les calculs en multipliant par μ^{-1} qui existe d'après la question 1.(d) de la partie D. On va avoir besoin de cette équivalence dans la question suivante.

2. On a démontré à la question 4. de la partie D que pour tout $n \in \mathbb{N}^*$, on a :

$$\varphi(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) id(d).$$

On reconnaît la formule d'inversion de Möbius avec $F = id$ et $f = \varphi$. Ainsi d'après la question précédente pour tout $n \in \mathbb{N}^*$, on a :

$$id(n) = \sum_{d|n} \varphi(d).$$

On a démontré que pour tout $n \in \mathbb{N}^*$, on a :

$$\boxed{\sum_{d|n} \varphi(d) = n}$$

On a bien $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$.

Toutes les fonctions arithmétiques et formules démontrées dans ce devoir sont primordiales en théorie des nombres qui est la branche des mathématiques qui s'intéresse aux nombres entiers et plus particulièrement aux nombres premiers et à leur répartition. Pour en savoir plus les premiers chapitre du livre suivant sont accessibles à un élève de classe préparatoire :

-Thèmes d'arithmétique avec 85 exercices corrigés d'Olivier Bordellès aux éditions Ellipses.