Correction CC2 Arithmétique

Exercice 1

1. cf cours
2. $\varphi(4) = \varphi(2^2) = 2^2 - 2 = 2$
   $\varphi(5) = 5 - 1 = 4$
   $\varphi(20) = \varphi(4) \times \varphi(5) = 2 \times 4 = 8$
   $\varphi(64) = \varphi(2^6) = 2^6 - 2^5 = 32$
3. Remarque : Une démonstration est proposée ici mais le mieux est de se référer à ce que vous avez dans votre cours.
   Soit $n \geq 2$. Par définition (question 1), on a
   $$\varphi(n) = \left|\mathbb{Z}/n\mathbb{Z}^\times\right| = |\{1 \leq k \leq n-1 \mid \text{pgcd}(k,n) = 1\}|.$$
   En particulier, on a les équivalences :
   $$\begin{aligned} \varphi(n) = n-1 &\iff \text{pour tout } 1 \leq k \leq n-1,\ \text{pgcd}(k,n) = 1 \\ &\iff \text{pour tout nombre premier } p \leq n-1,\ p \text{ ne divise pas } n \\ &\iff n \text{ est premier.} \end{aligned}$$
   Le sens réciproque de la deuxième équivalence n'est *a priori* pas immédiat. Démontrons-le par contraposée : supposons qu'il existe $1 \leq k \leq n-1$ tel que $\text{pgcd}(k,n) \neq 1$. En prenant un diviseur premier de ce pgcd, on obtient un nombre premier p tel que $p|n$ et $p|k$, donc $p \leq k \leq n-1$.

Exercice 2

1. (i) Supposons que n est pair. Il existe alors $q \in \mathbb{N}$ tel que $n = 2q$. Notons que l'on a :
   $$3^2 = 9 \equiv 1 \pmod 8$$
   Ainsi,
   $$3^n = \left(3^2\right)^q \equiv 1 \pmod 8$$
   On a ainsi montré que si n est pair, alors $3^n \equiv 1 \pmod 8$.
   (ii) Supposons désormais que n est impair. Il existe donc $q \in \mathbb{N}$, tel que $n = 2q+1$. On a alors
   $$3^n = \left(3^2\right)^q \times 3 \equiv 3 \pmod 8$$
   On a ainsi montré que si n est impair, alors $3^n \equiv 3 \pmod 8$.
2. Soit $m \geq 3$. Il existe $q \in \mathbb{N}$ tel que $m = 3 + q$. Puisque $2^3 = 8$, alors $2^m = 8 \times 2^q$, donc
   $$2^m \equiv 0 \pmod 8.$$
   En particulier, pour tout $n \in \mathbb{N}$, on a
   $$2^m - 3^n \equiv -3^n \pmod 8.$$
   Or, la question précédente nous donne les valeurs des puissances de 3 modulo 8. Si n est pair, on sait que
   $$-3^n \equiv -1 \equiv 7 \pmod 8,$$
   et si n est impair, on sait que
   $$-3^n \equiv -3 \equiv 5 \pmod 8.$$

Dans les deux cas, on a $-3^n \not\equiv 1 \pmod 8$. En particulier, on a

$$2^m - 3^n \neq 1.$$

On en conclut que si un couple $(m, n) \in \mathbb{N}^2$ est solution de (1), alors $m \leq 2$.

Remarque : Il faut faire attention aux passages de $\mathbb{Z}$ à modulo 8 et réciproquement. Si une égalité est vraie dans $\mathbb{Z}$, elle est vraie modulo 8, mais la réciproque n'est pas toujours vraie, par exemple, $8 \equiv 0 \pmod 8$ mais $8 \neq 0$. En revanche, c'est l'inverse pour une non-égalité : si deux entiers ne sont pas congrus modulo 8, ils ne sont pas égaux dans $\mathbb{Z}$, mais la réciproque est fausse (même contre-exemple : $0 \neq 8$ mais $0 \equiv 8 \pmod 8$).

3. On vient de voir que pour avoir une solution, il faut que m soit inférieur ou égal à 2. On peut donc faire une disjonction de cas sur m.

• Cas 1 : $m = 0$

On a alors

$$2^m - 3^n = -3^n$$

ce qui ne peut en aucun cas faire 1. Il n'y a donc pas de solution dans ce cas.

• Cas 2 : $m = 1$

On a alors

$$2^m - 3^n = 2 - 3^n$$

et

$$2 - 3^n = 1 \iff 3^n = 1 \iff n = 0$$

Ainsi, $(m, n) = (1, 0)$ est solution et c'est la seule solution lorsque $m = 1$.

• Cas 3 : $m = 2$

On a alors

$$2^m - 3^n = 4 - 3^n$$

et

$$4 - 3^n = 1 \iff 3^n = 3 \iff n = 1$$

Ainsi, $(m, n) = (2, 1)$ est solution et c'est la seule solution lorsque $m = 2$.

Finalement, on obtient que l'ensemble de solution de (1) est $\{(1, 0), (2, 1)\}$.

Exercice 3

1. Utilisons les décompositions en produits de facteurs premiers :

$$512 = 2^9, \quad 98 = 2 \times 49 = 2 \times 7^2.$$

Ainsi, $\text{pgcd}(512, 98) = 2$ et $\text{ppcm}(512, 98) = 2^9 \times 7^2 = 25088$.

2. On a $375 = 3 \times 5^3$. Comme le pgcd de a et b divise $b = 375$, il existe $n \in \{0, 1\}$ et $m \in \{0, 1, 2, 3\}$ tels que $\text{pgcd}(a, b) = 3^n \times 5^m$.

Or, $\sum_{i=0}^{8} 10^k$, n'est pas divisible par 5, on peut le voir à l'aide du critère de divisibilité par 5 (son chiffre des unités n'est ni 0 ni 5). On a donc $m = 0$.

Cependant, $\sum_{i=0}^{8} 10^k$ est divisible par 3 grâce au critère de divisibilité par 3 (la somme des chiffres est égale à 9 qui est divisible par 3). Ainsi, $n = 1$.

Finalement, on a donc que $\text{pgcd}(a, b) = 3$.

Exercice 4

Remarque : On rappelle qu'il y a beaucoup de façons de résoudre un tel système. On présente ici une méthode, ainsi que le résultat mais nous n'étions pas obligé de procéder ainsi.
On cherche à résoudre dans $\mathbb{Z}$ le système :

$$\begin{cases} x & \equiv 3 \pmod 7 \\ x & \equiv 4 \pmod 9 \\ x & \equiv 1 \pmod{11} \end{cases}$$

Les nombres $7, 9$ et 10 sont deux-à-deux premiers entre eux, il existe donc une unique solution modulo 693 d'après le théorème des restes chinois.

Étape 1 : Trouvons $u \in \mathbb{Z}$, une solution du système :

$$(E_1) : \begin{cases} u & \equiv 1 \pmod 7 \\ u & \equiv 0 \pmod 9 \\ u & \equiv 0 \pmod{11} \end{cases} \iff \begin{cases} u & \equiv 1 \pmod 7 \\ u & \equiv 0 \pmod{99} \end{cases}$$

Supposons que u vérifie ce système. Il existe $q \in \mathbb{Z}$ tel que $u = 99q$. Avec la première ligne du système, ceci nous donne :

$$\begin{aligned} 99q &\equiv 1 \pmod 7 \\ q &\equiv 1 \pmod 7 \end{aligned}$$

car $99 \equiv 1 \pmod 7$. Ainsi, $u = 99 \times 1 = 99$ convient.

Étape 2 : Trouvons $v \in \mathbb{Z}$, une solution du système :

$$(E_2) : \begin{cases} v & \equiv 1 \pmod 9 \\ v & \equiv 0 \pmod 7 \\ v & \equiv 0 \pmod{11} \end{cases} \iff \begin{cases} v & \equiv 1 \pmod 9 \\ v & \equiv 0 \pmod{77} \end{cases}$$

Supposons que v soit solution de (E_2). Il existe $q \in \mathbb{Z}$ tel que $v = 77q$. Avec la première ligne du système, ceci nous donne :

$$\begin{aligned} 77q &\equiv 1 \pmod 9 \\ 5q &\equiv 1 \pmod 9 \\ 10q &\equiv 2 \pmod 9 \\ q &\equiv 2 \pmod 9 \end{aligned}$$

(On effectue une multiplication par 2 à la troisième ligne car 2 est l'inverse de 5 modulo 9)
Ainsi, $v = 77 \times 2 = 154$ convient.

Étape 3 : Trouvons $w \in \mathbb{Z}$, solution du système :

$$(E_3) : \begin{cases} w & \equiv 1 \pmod{11} \\ w & \equiv 0 \pmod 7 \\ w & \equiv 0 \pmod 9 \end{cases} \iff \begin{cases} w & \equiv 1 \pmod{11} \\ w & \equiv 0 \pmod{63} \end{cases}$$

Supposons que w soit solution de (E_3). Il existe $q \in \mathbb{Z}$ tel que $w = 63q$. Avec la première ligne du système, ceci nous donne :

$$\begin{aligned} 63q &\equiv 1 \pmod{11} \\ 8q &\equiv 1 \pmod{11} \\ 56q &\equiv 7 \pmod{11} \\ q &\equiv 7 \pmod{11} \end{aligned}$$

(On effectue une multiplication par 7 à la troisième ligne car 7 est l'inverse de 8 modulo 11)
Ainsi, $w = 63 \times 7 = 441$ convient.

Étape 4 : Conclusion.
Ainsi, $3 \times u + 4 \times v + 1 \times w = 297 + 616 + 441 = 1354$ est solution du système.
De plus, $1354 \equiv 661 \pmod{693}$.
L'ensemble de solution dans $\mathbb{Z}$ est donc :

$$S = \{x \in \mathbb{Z} \mid x \equiv 661 \pmod{693}\}$$

Exercice 5

1. Soit $a \in \mathbb{Z}$. L'équation (2) admet des solutions si et seulement si $\text{pgcd}(20, 50)$ divise a, c'est-à-dire si et seulement si 10 divise a. Ainsi,

$$A = \{10q \mid q \in \mathbb{Z}\}$$

Soit $a \in A$. Il existe $q \in \mathbb{Z}$ tel que $a = 10q$. Cherchons à résoudre (2).
Cherchons tout d'abord une solution particulière. Pour cela, comme $\text{pgcd}(20, 50) = 10$, on peut se ramener à regarder

$$\frac{20}{10}x + \frac{50}{10}y = \frac{10q}{10}$$

c'est-à-dire,

$$2x + 5y = q.$$

Notons qu'une égalité de Bézout pour 2 et 5 est :

$$2 \times (-2) + 5 \times 1 = 1$$

Ainsi,

$$2 \times (-2q) + 5 \times q = q$$

Donc $(-2q, q)$ est une solution particulière de (2). On obtient alors que l'ensemble de solution de (2), pour $a = 10q$, est :

$$S = \{(-2q + 5k, q - 2k) | k \in \mathbb{Z}\}$$

2. Procédons par contraposée. Soit $a \in \mathbb{Z}$. Supposons que $a \notin B$ et montrons qu'il n'existe pas de solution $(x, y) \in \mathbb{N}^2$ à (2).

Si $a \notin A$, par la question précédente, l'équation (2) n'admet pas de solution dans $\mathbb{Z}^2$ donc, comme $\mathbb{N}^2 \subset \mathbb{Z}^2$, on en déduit qu'elle n'admet pas de solution dans $\mathbb{N}^2$.

Supposons alors $a \in A$. On a $a \in A \setminus B$, c'est-à-dire $a \in \{10, 30\}$. Procédons par disjonction de cas.
• Cas : 1 $a = 10$.
Supposons par l'absurde que $(x, y) \in \mathbb{N}^2$ soit une solution de (2). Par la question 1, il existe alors $k \in \mathbb{Z}$ tel que $x = -2 + 5k$ et $y = 1 - 2k$.
D'une part, comme $x \geqslant 0$, on a :

$$-2 + 5k \geqslant 0 \iff 5k \geqslant 2 \iff 10k \geqslant 4$$

D'autre part, $y \geqslant 0$, d'où :

$$1 - 2k \geqslant 0 \iff 1 \geqslant 2k \iff 5 \geqslant 10k$$

En combinant ces deux inégalité, on obtient :

$$5 \geqslant 10k \geqslant 4$$

Or, il n'existe aucun multiple de 10 compris entre 4 et 5, ceci est donc absurde !
Ainsi, si $a = 10$, (2) n'admet pas de solution $(x, y) \in \mathbb{N}^2$.

• Cas 2 : $a = 30$.
De même, supposons par l'absurde que $(x, y) \in \mathbb{N}^2$ soit une solution de (2). Par la question 1, il existe alors $k \in \mathbb{Z}$ tel que $x = -6 + 5k$ et $y = 3 - 2k$.
D'une part, comme $x \geqslant 0$, on a :

$$-6 + 5k \geqslant 0 \iff 5k \geqslant 6 \iff 10k \geqslant 12$$

D'autre part, $y \geqslant 0$, d'où :

$$3 - 2k \geqslant 0 \iff 3 \geqslant 2k \iff 15 \geqslant 10k$$

En combinant ces deux inégalité, on obtient :

$$15 \geqslant 10k \geqslant 12$$

Or, il n'existe aucun multiple de 10 entre 12 et 15, ceci est donc absurde !
Ainsi, si $a = 30$, (2) n'admet pas de solution $(x, y) \in \mathbb{N}^2$.

Finalement, on a bien obtenu le résultat souhaité, et par contraposée, on en conclut que si l'équation (2) admet une solution $(x, y) \in \mathbb{N}^2$, alors $a \in B$.

3. Soit $a \in B$. Montrons que (2) admet une solution $(x, y) \in \mathbb{N}^2$.
Notons tout d'abord qu'il existe $q \in \mathbb{N} \setminus \{1, 3\}$ tel que $a = 10q$.
De plus, par la question 1, les solutions de (2) dans $\mathbb{Z}^2$ sont de la forme $(-2q + 5k, q - 2k)$, avec $k \in \mathbb{Z}$. Une solution dans $\mathbb{N}^2 \subset \mathbb{Z}^2$ aura donc la même forme.

Faisons une disjonction de cas :
• Cas 1 : Supposons que q est nombre pair.
Il existe alors $n \in \mathbb{N}$ tel que $q = 2n$. On a dans ce cas,

$$-2q + 5k \geqslant 0 \iff -4n + 5k \geqslant 0 \iff 5k \geqslant 4n \iff 10k \geqslant 8n$$

et,

$$q - 2k \geqslant 0 \iff 2n - 2k \geqslant 2n \geqslant 2k \iff 10n \geqslant 10k.$$

Ainsi,

$$\begin{cases} -2q + 5k \geqslant 0 \\ q - 2k \geqslant 0 \end{cases} \iff 10n \geqslant 10k \geqslant 8n \iff n \geqslant k \geqslant \frac{4}{5}n$$

En prenant $k = n$, on a que $(x, y) = (-2q + 5n, q - 2n) \in \mathbb{N}^2$ est solution de (2).

• Cas 2 : Supposons que q est un nombre impair.
Il existe alors $n \in \mathbb{N}$ tel que $q = 2n + 1$. Notons également que comme $q \notin \{1, 3\}$, alors $n \geqslant 2$.
On a dans ce cas,

$$-2q + 5k \geqslant 0 \iff -4n - 2 + 5k \geqslant 0 \iff 5k \geqslant 4n + 2 \iff 10k \geqslant 8n + 4$$

et,

$$q - 2k \geqslant 0 \iff 2n + 1 - 2k \geqslant 2n + 1 \geqslant 2k \iff 10n + 5 \geqslant 10k.$$

Ainsi,

$$\begin{cases} -2q + 5k \geqslant 0 \\ q - 2k \geqslant 0 \end{cases} \iff 10n + 5 \geqslant 10k \geqslant 8n + 4$$

Remarquons que, comme $n \geqslant 2$, on a :

$$10n = 8n + 2n \geqslant 8n + 4$$

Ainsi, en prenant $k = n$, on obtient une nouvelle fois que $(x, y) = (-2q + 5n, q - 2n) \in \mathbb{N}^2$ est solution de (2).

4. On cherche à trouver toutes les solutions dans $\mathbb{N}^2$ de l'équation

$$20x + 50y = 150.$$

Par les questions précédentes, cette équation admet des solutions dans $\mathbb{N}^2$ car $150 = 10 \times 15 \in B$, et ce sont tous les couples $(-2 \times 15 + 5k, 15 - 2k)$ avec $-30 + 5k \geq 0$ et $15 - 2k \geq 0$. De plus,

$$\begin{cases} 5k \geqslant 30 \\ 15 \geqslant 2k \end{cases} \iff \begin{cases} 10k \geqslant 60 \\ 75 \geqslant 10k \end{cases} \iff 75 \geqslant 10k \geqslant 60 \iff 12 \leq 2k \leq 15$$

Il y a donc exactement deux solutions, pour $k = 6$ et $k = 7$, qui sont respectivement $(0, 3)$ et $(5, 1)$.
Ainsi, les combinaisons possibles que la machine peut donner sont : 0 billets de 20 € et 3 billets de 50 € ; 5 billets de 20 € et 1 billet de 50 €.
Remarque : on aurait pu trouver cette réponse directement sans faire toutes les questions de l'exercice ! Le nombre de billets de 50 € est 0, 1, 2 ou 3. Mais comme ni 150 ni 50 sont des multiples de 20, ça ne peut pas être 0 ni 2. On vérifie ensuite que les deux autres cas fonctionnent.

Exercice 6

1. Soit $x \in \mathbb{Z}$. Supposons que x est impair. Il existe donc $q \in \mathbb{N}$ tel que $x = 2q + 1$. On a alors :

$$x^2 = 4q^2 + 4q + 1 \equiv 1 \pmod 4.$$

Ainsi, pour tout $x \in \mathbb{Z}$ impair, on a $x^2 \equiv 1 \pmod 4$.

Soit $x \in \mathbb{Z}$ tel que $\text{pgcd}(x, 5) = 1$. Comme $5^2 = 25$, on a également $\text{pgcd}(x, 25) = 1$. Ainsi, par le théorème d'Euler, on a :

$$x^{\varphi(25)} \equiv 1 \pmod{25}.$$

On a de plus que :

$$\varphi(5^2) = 5^2 - 5 = 20$$

d'où,

$$x^{20} \equiv 1 \pmod{25}.$$

On en conclut que tout $x \in \mathbb{Z}$ tel que $\text{pgcd}(x, 5) = 1$ vérifie $x^{20} \equiv 1 \pmod{25}$.

2. Supposons que x est solution entière de (3).

   (a) Par hypothèse, x vérifie :

$$x^7 \equiv 27 \pmod{100}$$

Comme 4 divise 100, on a

$$\begin{aligned} x^7 &\equiv 27 \pmod 4 \\ \left(x^2\right)^3 x &\equiv 3 \pmod 4 \\ x &\equiv 3 \pmod 4 \qquad \text{d'après la question 1} \end{aligned}$$

De même, 25 divise 100 donc

$$\begin{aligned} x^7 &\equiv 27 \pmod{25} \\ x^7 &\equiv 2 \pmod{25} \\ \left(x^7\right)^3 &\equiv 2^3 \pmod{25} \\ x^{21} &\equiv 8 \pmod{25} \\ x &\equiv 8 \pmod{25} \qquad \text{d'après la question 1} \end{aligned}$$

Finalement, on a bien obtenu que $x \equiv 3 \pmod 4$ et $x \equiv 8 \pmod{25}$.

(b) Supposons que x soit solution de (3). Par la question précédente, on a que x est solution de

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 8 \pmod{25} \end{cases}$$

Comme 4 et 25 sont premier-entre-eux, alors par le théorème des restes chinois, il existe une unique solution modulo 100. Trouvons là !
La deuxième ligne nous donne $x = 25q + 8$ avec $q \in \mathbb{Z}$. En injectant dans la première, on obtient alors

$$\begin{aligned} 25q + 8 &\equiv 3 \pmod 4 \\ q &\equiv 3 \pmod 4 \end{aligned}$$

Ainsi, $x = 25 \times 3 + 8 = 83$ est solution du système, et l'ensemble des solution est

$$S = \{x \in \mathbb{Z} \mid x \equiv 83 \pmod{100}\}$$

On a ainsi que si x est solution de (3), alors $x \equiv 83 \pmod{100}$.

Réciproquement, supposons que $x \equiv 83 \pmod{100}$.
On veut montrer que $x^7 \equiv 27 \pmod{100}$, ce qui est équivalent, par le théorème des restes chinois, à montrer que $x^7 \equiv 27 \pmod 4$ et $x^7 \equiv 27 \pmod{25}$.
• Comme $x \equiv 83 \pmod{100}$, alors

$$x \equiv 83 \pmod 4$$

c'est-à-dire $x \equiv 3 \equiv -1 \pmod 4$. Ainsi,

$$x^7 \equiv (-1)^7 \equiv -1 \equiv 3 \pmod 4.$$

Comme $27 \equiv 3 \pmod 4$, alors

$$x^7 \equiv 27 \pmod 4.$$

• De même, comme $x \equiv 83 \pmod{100}$, alors $x \equiv 83 \pmod{25}$, c'est-à-dire $x \equiv 8 \pmod{25}$. Calculons les premières puissances de 8 modulo 25 :

$$8 \equiv 8 \pmod{25}; \quad 8^2 \equiv 14 \pmod{25}; \quad 8^3 \equiv 12 \pmod{25}; \quad 8^4 \equiv 21 \equiv -4 \pmod{25}.$$

Or, $8^7 = 8^4 \times 8^3$, donc $8^7 \equiv -48 \equiv 2 \pmod{25}$. Mais $27 \equiv 2 \pmod{25}$, donc

$$x^7 \equiv 27 \pmod{25}.$$

Finalement, on obtient bien que $x^7 \equiv 27 \pmod{100}$. L'ensemble des solutions entières de (3) est donc

$$S = \{83 + 100k \mid k \in \mathbb{Z}\}.$$

Exercice 7

On montre le résultat par double implication.

$\boxed{\Leftarrow}$ On suppose que $n = 2^k$ pour un certain $k \in \mathbb{N}^*$. On sait alors que $\varphi(n) = 2^k - 2^{k-1}$. Or,

$$2^k - 2^{k-1} = 2^{k-1} = \frac{2^k}{2} = \frac{n}{2}.$$

Donc $\varphi(n) = \frac{n}{2}$.

$\boxed{\Rightarrow}$ On suppose que $\varphi(n) = \frac{n}{2}$. Comme $\varphi(1) = 1 \neq \frac{1}{2}$, on sait que $n \geq 1$. On écrit la décomposition en produit de facteurs premiers de n :

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

où $r \in \mathbb{N}^*$, $p_1, \ldots, p_r$ sont des nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_r$ sont des entiers non-nuls [1].

On a alors :

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

Comme $\varphi(n) = \frac{n}{2}$, alors

$$\prod_{i=1}^{r} \left(1 - \frac{1}{p_i} \right) = \frac{1}{2}$$

ce qui se réécrit en passant à l'inverse

$$\prod_{i=1}^{r} \frac{p_i}{p_i - 1} = 2. \qquad (\star)$$

D'un autre côté, on sait que n est pair puisque $\varphi(n) = \frac{n}{2}$ donc $n = 2\varphi(n)$. Donc parmi les p_i, 2 apparaît. Disons que c'est p_1 (quitte à les renuméroter). L'équation $(\star)$ devient :

$$\frac{2}{2-1} \prod_{i=2}^{r} \frac{p_i}{p_i - 1} = 2 \iff \prod_{i=2}^{r} \frac{p_i}{p_i - 1} = 1 \iff \prod_{i=2}^{r} p_i = \prod_{i=2}^{r} (p_i - 1). \qquad (\star\star)$$

Supposons par l'absurde que $r > 1$, c'est-à-dire qu'il y a des termes dans les produit apparaissant dans $(\star\star)$, on a donc pour tout $2 \leq i \leq r$, $0 < p_i - 1 < p_i$, et alors

$$0 < \prod_{i=2}^{r} (p_i - 1) < \prod_{i=2}^{r} p_i.$$

Ceci est absurde d'après $(\star\star)$. Donc $r = 1$, et on a alors $n = p_1^{\alpha_1} = 2^{\alpha_1}$. Donc n est bien de la forme 2^k avec $k \in \mathbb{N}^*$.

1. Souvent, on autorise les exposants α_i à être nuls pour simplifier les calculs de pgcd et ppcm, ici, on veut faire apparaître uniquement les nombres premiers qui divisent n.