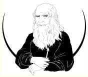
Arithmétique

Cours de PTSI

Lycée Jules Garnier

Février 2024



Sommaire I

À l'heure où j'écris ces pages, le plus grand nombre premier connu est $2^{82\,589\,933}-1$ obtenu par Patrick Laroche dans le cadre du programme GIMPS et trouvé le 7 décembre 2018. Écrit en base 10, ce nombre comporte 24 862 048 chiffres, soit près d'un million de chiffres supplémentaires par rapport à l'ancien record qui datait de janvier 2018 .

I. Rudiments d'arithmétique dans $\mathbb{N}$

Définition 1 (Divisibilité dans $\mathbb{Z}$) :

Soient a et b des entiers relatifs.

On dit que a **divise** b, noté $a|b$, s'il existe un entier relatif k tel que $b = ka$.

On dit alors que :

- a est **un diviseur** de b. On note $\mathcal{D}(b)$ leur ensemble.
- b est **un multiple** de a. On note $a\mathbb{Z}$ leur ensemble.

Comme a et $-a$ ont les mêmes diviseurs dans $\mathbb{Z}$, on se restreindra le plus souvent, sans le dire, à l'étude de la divisibilité dans $\mathbb{N}$. C'est le parti pris par le programme donc, à partir de maintenant, sauf remarques intéressantes, on ne considèrera plus que la divisibilité dans $\mathbb{N}$.

Exemples 1 :

- $3|12$ et $5\nmid 12$.
- L'ensemble des diviseurs de 12 est $\mathcal{D}(12) = \{1, 2, 3, 4, 6, 12\}$.
- Tous les nombres divisent 0 *i.e.* 0 est multiple de tout entier : $\mathcal{D}(0) = \mathbb{N}$.
- 0 n'est diviseur d'aucun entier (non nul) : $0\mathbb{Z} = \{0\}$.

- $a|b \iff b\mathbb{Z} \subset a\mathbb{Z}$.

- Un multiple de 2 est aussi appelé un nombre pair. Ceux qui ne le sont pas sont appelés nombre impair. L'ensemble des nombres pairs est noté $2\mathbb{N}$. (cf le corollaire (2.1) pour les nombres impairs)

Exercice 1 :

On appelle nombre parfait tout nombre égal à la somme de ses diviseurs stricts.

Par exemple $\mathcal{D}(6) = \{1, 2, 3, 6\}$ et $6 = 1 + 2 + 3$, donc 6 est parfait.

Montrer que 28 est parfait.

Méthode 1 :

Pour les problèmes donnés sous forme additive, on essaiera de se ramener à une forme multiplicative du type $\mathrm{A} \times \mathrm{B} = \mathrm{C}$, où on connaît les diviseurs de C.

Exercice 2 :

Déterminer les couples $(x,\ y)$ d'entiers naturels qui vérifient $x^2 = y^2 + 21$.

Proposition 1 (Relation de divisibilité) :

1. $\forall\, a \in \mathbb{N}, \quad a|a$ et $1|a$. (« $a|b$ » est réflexive)
2. $\forall\, a, b \in \mathbb{N}, \quad \begin{cases} a|b \\ b|a \end{cases} \implies a = b.$ (« $a|b$ » est antisymétrique sur $\mathbb{N}$)
3. $\forall\, a, b, c \in \mathbb{N}, \quad \begin{cases} a|b \\ b|c \end{cases} \implies a|c.$ (« $a|b$ » est transitive)

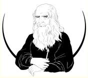
La relation « $a\mathcal{R}b \iff a|b$ », réflexive, antisymétrique et transitive est appelée une relation d'ordre sur $\mathbb{N}$. C'est un ordre non total.

ATTENTION

Sur $\mathbb{Z}$, la relation $a|b$ est seulement réflexive et transitive.

On perd l'antisymétrie :

$$\forall\, a, b \in \mathbb{Z}, \quad \begin{cases} a|b \\ b|a \end{cases} \iff |a| = |b|\,.$$



Proposition 2 (Compatibilité) :

1. $$\begin{matrix}\forall\, a,b,c\in\mathbb{N}\\ \forall\, m,n\in\mathbb{N}\end{matrix},\quad \begin{cases}a|b\\ a|c\end{cases}\Longrightarrow a|mb+nc$$

   (« $a|b$ » est compatible avec les combinaisons linéaires entières)

2. $$\forall\, a,b,a',b',c\in\mathbb{N},\quad \begin{cases}a|b\\ a'|b'\end{cases}\Longrightarrow a|bc \text{ et } aa'|bb'$$

   (« $a|b$ » est compatible avec le produit)

   En particulier, $\forall\, a,b,n\in\mathbb{N},\quad a|b \Longrightarrow a^n|b^n$

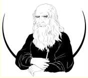
ATTENTION

- $\begin{cases}a|c\\ b|c\end{cases}\ \cancel{\Longrightarrow}\ ab|c$:

  $2|12$ et $4|12$ mais

- $a|bc\ \cancel{\Longrightarrow}\ a|b$:

  $10|210=14\times15$ mais $10\nmid 14$ (et $10\nmid 15$)



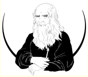
Exemple 2 :

Si $a \in \mathbb{Z}$ divise $3n+2$ et $n-3$ alors $a|11$.

En effet, a divise alors $(3n+2)-3(n-3)=11$.

Exercice 3 :

Trouver les entiers n pour lesquels $\dfrac{n+15}{n+2}$ est entier.

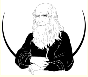


Corollaire 2.1 :

Les nombres impairs sont exactement les entiers de la forme $2p + 1$ où $p \in \mathbb{Z}$.

Exercice 4 :

Montrer que pour tout entier impair n, $n^2 - 1$ est multiple de 8.



Théorème 3 :

Pour tout $(a,b) \in \mathbb{N} \times \mathbb{N}^*$, il existe un unique couple $(q,r) \in \mathbb{N}^2$ tel que :

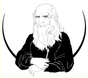
$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b. \tag{1}$$

Lorsqu'on a obtenu cette écriture, on dit qu'on a effectué la division euclidienne de a par b.

Rappel (Vocabulaire) :

- q s'appelle le quotient,
- r s'appelle le reste,
- a s'appelle le dividende
- et b s'appelle le diviseur.

Combien de fois peut-on soustraire 7 de 83 et combien reste-t-il ?



Réponse : autant de fois que l'on veut et il reste 76 à chaque fois.

Exercice 5 :

Montrer que tout entier n non divisible par 5 a un carré de la forme $5p+1$ ou $5p-1$.

Proposition 4 :

Soient a et b deux entiers naturels avec b non nul.

$$b|a \iff \text{le reste dans la division euclidienne de } a \text{ par } b \text{ est nul.}$$

Exercice 6 :

Le 1er mai 2022 tombait un dimanche. Quel jour tombe le 1er mai 2023 ?

Définition 2 :

Un entier naturel est dit premier lorsqu'il admet exactement deux diviseurs (1 et lui-même).

On note $\mathbb{P}$ l'ensemble des nombres premiers.

Exemples 3 :

- $0 \notin \mathbb{P}$: il admet une infinité de diviseurs.
- $1 \notin \mathbb{P}$: il n'admet qu'un seul diviseur.
- $2 \in \mathbb{P}$: c'est le plus petit nombre premier, et il est pair. C'est le seul nombre premier pair.
- Une curiosité et un jeu des siècles passés, le polynôme $\mathrm{P}(n) = n^2 - n + 41$ associé à Euler donne des nombres premiers pour n prenant les valeurs 0 à 39 mais $\mathrm{P}(40) = 1681 = 41^2$!

Théorème 5 (Critère d'arrêt) :

- Tout entier naturel n, $n \geqslant 2$, admet un diviseur premier.
- Si n n'est pas premier, alors il admet un diviseur premier p tel que :

$$2 \leqslant p \leqslant \sqrt{n}.$$

Exemple 4 :

Comment montrer que 109 est un nombre premier ?

- On a $10 < \sqrt{109} < 11$.
  On teste donc tous les nombres premiers strictement inférieurs à 11, soit : 2, 3, 5 et 7.
- Des règles de divisibilité, on déduit que 109 n'est divisible ni par 2, ni par 3, ni par 5.
- Soit, on se rappelle le critère de divisibilité par 7, soit on effectue la division euclidienne de 109 par 7, on obtient :

$$109 = 7 \times 15 + 4 \implies 109 \text{ n'est pas divisible par } 7.$$

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Figure 1 – Les nombres premiers inférieurs à 100 par le crible d'Ératosthène

Théorème 6 :

L'ensemble des nombres premiers est infini.

Exercice 7 :

Soit $n \in \mathbb{N}$. On suppose $n \geqslant 2$.

Montrer qu'il n'existe aucun nombre premier entre $n! + 2$ et $n! + n$.

I. Rudiments d'arithmétique dans $\mathbb{N}$

3. Nombres premiers

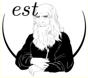
Un peu d'histoire : *En mathématiques, et plus précisément en théorie analytique des nombres, le théorème des nombres premiers, démontré indépendamment par Hadamard et La Vallée Poussin en 1896, est un résultat concernant la distribution asymptotique des nombres premiers.*

Théorème 7 :

La fonction π qui à un réel x associe $\mathcal{P}(x)$ le nombre de nombres premiers inférieurs ou égaux à x, est équivalente lorsque x tend vers $+\infty$, au quotient de x par son logarithme népérien :

$$\pi(x) \underset{x\to+\infty}{\sim} \frac{x}{\ln(x)}.$$

- *Le théorème des nombres premiers a été conjecturé dans la marge d'une table de logarithmes par Gauss en 1792 ou 1793 alors qu'il avait seulement 15 ou 16 ans (selon ses propres affirmations ultérieures).*
- *Le Russe Pafnouti Tchebychev a établi en 1851 que si x est assez grand, $\mathcal{P}(x)$ est compris entre* $\dfrac{0,92129x}{\ln(x)}$ *et* $\dfrac{1,10556x}{\ln(x)}$.



- *Le théorème a finalement été démontré indépendamment par Hadamard et La Vallée Poussin en 1896 à l'aide de méthodes d'analyse complexe, utilisant en particulier la fonction ζ de Riemann.*
- *Un approximant de $\pi(x)$ nettement meilleur que $\dfrac{x}{\ln(x)}$ est la fonction logarithme intégral*
$$li(x) = \int_0^x \frac{\mathrm{d}t}{\ln(t)}$$
ou sa variante, la fonction d'écart logarithmique intégrale
$$Li(x) = li(x) - li(2) = \int_2^x \frac{\mathrm{d}t}{\ln(t)}$$
$$\pi(x) \underset{x\to+\infty}{\sim} li(x) \underset{x\to+\infty}{\sim} Li(x).$$
- *En 1899, La Vallée Poussin a affiné son résultat en montrant que :*
$$\pi(x) \underset{x\to+\infty}{=} li(x) + O\left(x\,\mathrm{e}^{-\sqrt{\frac{\ln(x)}{2\mathrm{V}}}}\right),$$
pour une certaine constante V.
Landau (en 1909) puis bien d'autres ont travaillé à réduire la taille admissible cette constante V.

- *L'hypothèse de Riemann est même équivalente à l'estimation* $\pi(x) \underset{x\to+\infty}{=} li(x) + O\big(\sqrt{x}\ln(x)\big)$.

  Surprenant ! Magnifique ! et pourtant encore si loin ...

Théorème 8 (Théorème fondamental de l'arithmétique) :

Tout entier n supérieur à 2 admet une et une seule (à l'ordre des facteurs près) décomposition en facteurs premiers.

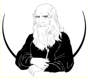
$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \text{ avec } p_i \in \mathbb{P} \text{ deux à deux distincts et } \alpha_i \in \mathbb{N}^*.$$

On l'appelle **décomposition primaire** de n et les exposants α_i s'appellent les valuations associées aux nombres premiers p_i.

Lemme 1 :

Un nombre premier divise un produit s'il divise l'un des facteurs du produit.

ATTENTION $4 | (14 \times 10)$ mais 4 ne divise ni 14, ni 10.



Exemple 5 :

Décomposons 16 758 en produit de facteurs premiers :

$$\begin{array}{r|l}
16758 & 2 \\
8379 & 3 \\
2793 & 3 \\
931 & 7 \\
133 & 7 \\
19 & 19 \\
1 &
\end{array}$$

Pour décomposer un entier, on effectue des divisions successives par des nombres premiers dans l'ordre croissant.

On obtient :

$$16758 = 2 \times 3^2 \times 7^2 \times 19.$$

Exemples 6 :

- $510510 = 1001 \times 510 = (7 \times 11 \times 13) \times (2 \times 3 \times 5 \times 17).$
  $= (2)(3)(5)(7)(11)(13)(17)$
- $80000 = 8 \times 10^4 = (2)^7(5)^4.$

Corollaire 8.1 :

Soient a et b deux entiers supérieurs à 2 dont les décompositions primaires s'écrivent $a = \displaystyle\prod_{p\in\mathbb{P}} p^{\alpha_p}$ et $b = \displaystyle\prod_{p\in\mathbb{P}} p^{\beta_p}$.

Alors :

$$a|b \quad \iff \quad \forall\, p \in \mathbb{P},\ \alpha_p \leqslant \beta_p.$$

Corollaire 8.2 :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \text{admet} \quad \prod_{i=1}^{k} (1+\alpha_i) \text{ diviseurs.}$$

Exercice 8 :

Trouver le nombre de diviseurs de 120 et déterminer tous ces diviseurs.

II. PGCD et PPCM

II. PGCD et PPCM
1. PGCD

Définition 3 :

Soient a et b deux entiers naturels non nuls.

On appelle **PGCD de a et b**, noté $\text{pgcd}\,(a\,;b)$ ou $a \wedge b$, le plus grand diviseur commun à a et b.

Remarques :

- Comme 1 divise tous les nombres entiers $\text{pgcd}\,(a\,;b) \geqslant 1$.
  De même, il est évident que si a et b sont non nuls, $\text{pgcd}\,(a\,;b) \leqslant a$ et $\text{pgcd}\,(a\,;b) \leqslant b$.
- $\text{pgcd}\,(a\,;b) = \text{pgcd}\,(b\,;a)$
- Si $a > 0$, $\text{pgcd}\,(a\,;0) = a$. Par convention, on posera $\text{pgcd}\,(0\,;0) = 0$.

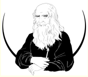
II. PGCD et PPCM
1. PGCD

Dans la pratique, on se bornera souvent au cas où a et b sont dans $\mathbb{N}^*$ et tels que $a > b$. Cette condition n'est pas restrictive car les diviseurs d'un nombre et de son opposé sont les mêmes, donc $\operatorname{pgcd}(a\,;b) = \operatorname{pgcd}(|a|\,;|b|)$ pour a et b dans $\mathbb{Z}$.

Et, par ailleurs, parmi deux entiers naturels a et b, il y en a toujours un qui est plus grand que l'autre. Il suffira donc de commencer par diviser le plus grand par le plus petit.

Exemple 7 :

- $\operatorname{pgcd}(24\,;18) = 6$.
- $\operatorname{pgcd}(60\,;84) = 12$.
- $\operatorname{pgcd}(150\,;240) = 30$.
- $\operatorname{pgcd}(27\,;140) = 1$.
- $\operatorname{pgcd}(6\,;72) = 6$.
- $\operatorname{pgcd}(31\,;45) = 1$.
- $\operatorname{pgcd}(5\,;7) = 1$.



Exercice 9 :

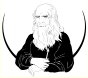
Pour tout entier n non nul, on définit la suite $(u_n)_{n\in\mathbb{N}}$ par :

$$u_n = \frac{1}{n}\,\text{pgcd}\,(24\,;n)\,.$$

La suite $(u_n)_{n\in\mathbb{N}}$ est-elle convergente ?

Proposition 9 :

- $\text{pgcd}\,(a\,;a) = |a|$ et $\text{pgcd}\,(1\,;a) = 1$.
- Si $b|a$ alors $\text{pgcd}\,(a\,;b) = |b|$.



Théorème 10 (Fondamental) :

Soient a et b deux entiers non nuls tels et un couple d'entiers $(q\,;r)$ tels que $a = bq + r$. Alors,

$$\operatorname{pgcd}(a\,;b) = \operatorname{pgcd}(b\,;r).$$

Remarques : Même si l'énoncé du théorème (10) fait fortement penser à la division euclidienne de a par b, il n'est nullement besoin que ce soit le cas pour que ce théorème soit vrai.

Ce théorème est fondamental par ses applications et notamment dans l'algorithme d'Euclide du paragraphe (2) .

Méthode 2 :

Soit d et D, deux quantités. Pour montrer que $d = \mathrm{D}$, il suffit :

- de montrer successivement que $d \leqslant \mathrm{D}$ puis $\mathrm{D} \leqslant d$.
- dans le cas de nombres entiers positifs, on pourra aussi montrer que $d | \mathrm{D}$ puis $\mathrm{D} | d$.

Exercice 10 :

Soient a et b deux entiers naturels non nuls. Soient $x = 7a + 5b$ et $y = 4a + 3b$.

Montrer que $\mathrm{pgcd}\,(x\,;y) = \mathrm{pgcd}\,(a\,;b)$.

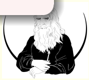
Théorème II (Le pgcd est le dernier reste non nul) :

Soient a et b deux naturels non nuls tels que b ne divise pas a. La suite des divisions euclidiennes suivantes finit par s'arrêter.

Le dernier reste non nul est alors le pgcd $(a\,;b)$.

$$\begin{array}{llll}
a \text{ par } b & a = bq_0 + r_0 & \text{avec} & b > r_0 \geqslant 0 \\
b \text{ par } r_0 & b = r_0 q_1 + r_1 & \text{avec} & r_0 > r_1 \geqslant 0 \\
r_0 \text{ par } r_1 & r_0 = r_1 q_2 + r_2 & \text{avec} & r_1 > r_2 \geqslant 0 \\
 & & \vdots & \\
r_{n-2} \text{ par } r_{n-1} & r_{n-2} = r_{n-1} q_n + r_n & \text{avec} & r_{n-1} > r_n \geqslant 0 \\
r_{n-1} \text{ par } r_n & r_{n-1} = r_n q_{n+1} + 0 & &
\end{array}$$

On a alors pgcd $(a\,;b) = r_n$.



Exemple 8 :

Calculer le $\operatorname{pgcd}(4539\,;1958)$. On effectue les divisions euclidiennes suivantes :

$$\begin{aligned} 4539 &= 1958 \times 2 + 623 \\ 1958 &= 623 \times 3 + 89 \\ 623 &= 89 \times 7 + 0 \end{aligned}$$

Conclusion : $\operatorname{pgcd}(4539\,;1958) = 89$.

Remarque : Le petit nombre d'étapes montre la performance de cet algorithme. Celui-ci porte le nom d'un père des mathématiques car il était effectivement connu d'Euclide six siècles avant notre ère !!!

Exercice 11 :

Calculer le pgcd de 162 et 207.

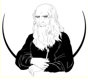
Théorème 12 :

Soient a et b deux entiers non nuls. Les diviseurs communs de a et b sont **exactement** les diviseurs de $\operatorname{pgcd}(a\,;b)$:

$$d|\operatorname{pgcd}(a\,;b) \iff \begin{cases} d|a \\ d|b \end{cases}$$

De manière équivalente : $\mathcal{D}(a \wedge b) = \mathcal{D}(a) \cap \mathcal{D}(b)$.

Remarque : Avant ce théorème, nous n'avions que l'inclusion $\mathcal{D}(a \wedge b) \subset \mathcal{D}(a) \cap \mathcal{D}(b)$.



Proposition 13 :

Pour tout entier naturel k non nul, $\quad \operatorname{pgcd}(ka\,;kb) = k \times \operatorname{pgcd}(a\,;b)$.

Exemple 9 :

- $\operatorname{pgcd}(800\,;500) = \operatorname{pgcd}(100 \times 8\,;100 \times 5)$
  $= 100 \times \operatorname{pgcd}(8\,;5) = 100.$
- $\operatorname{pgcd}(36\,;24) = \operatorname{pgcd}(12 \times 3\,;12 \times 2) = 12 \times \operatorname{pgcd}(3\,;2) = 12.$

Proposition 14 :

Soient a et b deux entiers supérieurs à 2 dont les décompositions primaires s'écrivent $a = \prod_{p \in \mathbb{P}} p^{\alpha_p}$ et $b = \prod_{p \in \mathbb{P}} p^{\beta_p}$.

Alors,

$$a \wedge b = \prod_{p \in \mathbb{P}} p^{\min(\alpha_p, \beta_p)}.$$

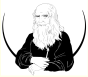
Dans le cas de deux nombres a et b pas trop grands, on pourra ainsi réviser ses tables de multiplication et décomposer les deux nombres a et b en facteurs premiers et trouver, « à la main », le plus grand diviseur commun.

Exemples 10 :

- $$\begin{aligned} 510510 \wedge 80000 &= (2)(3)(5)(7)(11)(13)(17) \wedge (2)^7(5)^4 \\ &= (2)(5) = 10. \end{aligned}$$
- $9100 \wedge 1848 = (2)^2(5)^2(7)(13) \wedge (2)^3(3)(7)(11) = (2)^2(7) = 28.$

Exercice 12 :

Déterminer le PGCD de 1960 et de 34300.



II. PGCD et PPCM
3. PPCM

Définition 4 :

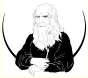
Soient a et b deux entiers naturels non nuls.

On appelle **PPCM de a et b**, noté $\operatorname{ppcm}(a\,;b)$ ou $a \vee b$, le plus petit multiple commun de a et b.

Remarques :

- Le seul multiple de 0 est 0 donc, pour tout entier a, $\operatorname{ppcm}(a\,;0) = 0$.
- Comme tous les entiers sont multiples de 1, $\operatorname{ppcm}(a\,;b) \geqslant 1$.
  De même, il est évident que si a et b sont non nuls, $\operatorname{ppcm}(a\,;b) \geqslant a$ et $\operatorname{ppcm}(a\,;b) \geqslant b$.
- $\operatorname{ppcm}(a\,;b) = \operatorname{ppcm}(b\,;a)$.

Au collège, pour additionner deux fractions, on recherchait le dénominateur commun le plus petit qui n'était rien d'autre que $\operatorname{ppcm}(a\,;b)$.



Exemple 11 :

- $\operatorname{ppcm}(18\,;12) = 36$.
- $\operatorname{ppcm}(24\,;40) = 120$.
- $\operatorname{ppcm}(11\,;17) = 11 \times 17 = 187$.
- $\operatorname{ppcm}(19\,;5) = 19 \times 5 = 195$.

Proposition 15 :

Soient a et b deux entiers naturels non nuls.

- $\operatorname{ppcm}(a\,;a) = a$ et $\operatorname{ppcm}(1\,;a) = a$.
- Si $b|a$ alors $\operatorname{ppcm}(a\,;b) = a$.

Théorème 16 :

Soient a et b deux entiers non nuls.

Les multiples communs de a et b sont **exactement** les multiples de $\operatorname{ppcm}(a\,;b)$:

$$\operatorname{ppcm}(a\,;b)\,|m \iff \begin{cases} a|m \\ b|m \end{cases}$$

De manière équivalente : $(a \vee b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

En pratique, on sait calculer le PGCD de deux nombres mais moins leur PPCM. Le théorème (17) donne un moyen de le calculer :

Théorème 17 :

Soient a et b deux entiers naturels.

$$ab = \operatorname{ppcm}(a\,;b) \times \operatorname{pgcd}(a\,;b)\,.$$

Remarque : La notion de PPCM peut aisément s'étendre aux entiers relatifs en prenant comme définition, le plus petit multiple de $|a|$ et $|b|$. Dans ce cas, on aurait également :

$$|ab| = \operatorname{ppcm}(a\,;b) \times \operatorname{pgcd}(a\,;b)\,.$$

Exemple 12 :

Le PGCD de 42 et 60 est 6. Si on note m leur PPCM, alors $6m = 42 \times 60$ d'où $m = 420$.

Exercice 13 :

Déterminer $m = 44100 \vee 36036$.

Corollaire 17.1 :

Si k est un entier naturel : $\quad \text{ppcm}\,(ka\,;kb) = k \times \text{ppcm}\,(a\,;b)$.

Proposition 18 :

Soient a et b deux entiers supérieurs à 2 dont les décompositions primaires s'écrivent $a = \prod_{p\in\mathbb{P}} p^{\alpha_p}$ et $b = \prod_{p\in\mathbb{P}} p^{\beta_p}$.

Alors,

$$a \vee b = \prod_{p\in\mathbb{P}} p^{\max(\alpha_p,\beta_p)}.$$

Méthode 3 :

Pour des entiers a et b pas « trop grands », une méthode enfantine mais souvent suffisante est de décomposer a et b en facteurs premiers.

Le ppcm de a et b est alors égal au produit de tous les facteurs premiers de a et b pris avec l'exposant le plus grand apparaissant dans les décompositions.

Exercice 14 :

Déterminer $\operatorname{ppcm}(240\,;756)$.