Chapitre

M

Cours et exercices

Arithmétique dans l'ensemble des entiers naturels

L'objectif de ce chapitre est de consolider les capacités et connaissances partiellement acquises concernant l'arithmétique dans $\mathbb{N}$: divisibilité, division euclidienne, PGCD et PPCM et nombres premiers.
Paradoxalement, notre programme va moins loin que celui de la spécialité Mathématiques de la classe de Terminale. Mais comme tout les étudiants ne l'ont pas nécessairement suivi, cela sera l'occasion de mettre tout le monde à niveau.
Pour être honnête, l'arithmétique n'est pas au cœur du programme de mathématiques de la filière PTSI/PT. En revanche, nous profiterons de ce chapitre pour faire de l'algorithmique et de la programmation en Python car l'arithmétique est un thème extrêmement prisé des examinateurs d'un des deux oraux de la Banque PT (« Mathématiques et algorithmique »).

Sommaire

NB – On rappelle que toute partie non vide de $\mathbb{N}$ possède un plus petit élément et que toute partie non vide et majorée de $\mathbb{N}$ possède un plus grand élément.

I – Divisibilité

I.1 – Relation de divisibilité

I.1.1 – Définition (Relation de divisibilité dans $\mathbb{N}$)

Soit $(a,b) \in \mathbb{N}^2$. On dit que b ***divise*** a (ou que a est ***divisible*** par b ou encore que a est un ***multiple*** de b) s'il existe $k \in \mathbb{N}$ tel que $a = kb$. On note alors $b \mid a$ (et $b \nmid a$ dans le cas contraire).

Remarques

1 ▶ Conformément au programme, nous nous limitons ici aux entiers naturels (c'est-à-dire positifs). Mais la relation de divisibilité se définit de la même manière pour les entiers relatifs.

2 ▶ Avec cette définition (la seule, la vraie) on remarque que tout entier b divise 0 car on a $0 = 0 \times b$.

3 ▶ Avec cette définition (la seule, la vraie) on remarque que le seul entier divisible par 0 est 0 lui même. En effet $a = k \times 0$ implique $a = 0$.

4 ▶ On démontre facilement que la relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre (symétrique, transitive et antisymétrique). Il s'agit d'un ordre partiel car, par exemple, 2 et 3 ne sont pas comparables : $2 \nmid 3$ et $3 \nmid 2$.

I.1.2 – Définition (Ensemble des diviseurs d'un entier donné)

Pour tout entier $n \in \mathbb{N}$, on note $\mathscr{D}(n)$ l'ensemble des diviseurs de n.

Exemples

1 ▶ Écrivons $\mathscr{D}(10)$:

$$\mathscr{D}(10) = \{1, 2, 5, 10\}$$

2 ▶ Écrivons $\mathscr{D}(7)$:

$$\mathscr{D}(7) = \{1, 7\}$$

3 ▶ Écrivons $\mathscr{D}(12)$:

$$\mathscr{D}(12) = \{1, 2, 3, 4, 6, 12\}$$

4 ▶ Comme évoqué précédemment, tout entier naturel divise 0, donc on a $\mathscr{D}(0) = \mathbb{N}$.

I.1.3 – Proposition

Pour tout $n \neq 0$ on a $\mathscr{D}(n) \subset [\![1, n]\!]$. En particulier $\mathscr{D}(n)$ est fini et son plus grand élément est n.

Démonstration

Soit d un diviseur de n. Par définition il existe $k \in \mathbb{N}$ tel que $n = kd$. Comme $n \neq 0$ on a nécessairement $k \neq 0$ et donc $k \geqslant 1$. En multipliant par d (positif) on en déduit que $kd \geqslant d$ c'est à dire $d \leqslant n$. Comme par ailleurs $d \neq 0$ (sinon n serait nul) on a $d \in [\![1, n]\!]$. On a donc bien démontré l'inclusion $\mathscr{D}(n) \subset [\![1, n]\!]$.

I.1.4 – Proposition et Définition (Multiples d'un entier donné)

Soit $n \in \mathbb{N}$ un entier donné.

(i) Les multiples de n sont les nombres de la forme nk avec $k \in \mathbb{N}$.

(ii) L'ensemble des multiples de n est naturellement noté $n\mathbb{N}$.

Démonstration

Cela provient directement de la définition de la divisibilité.

Exemples

1 ▶ Les multiples de 2 sont les entiers de le forme $2k$ avec $k \in \mathbb{N}$. Pour cette raison, l'ensemble de ces nombres est noté $2\mathbb{N}$.

2 ▶ L'ensemble des multiples de 5 est l'ensemble $5\mathbb{N}$. Il est constitué des entiers suivants de la forme $5k$ avec $k \in \mathbb{N}$.

3 ▶ Bien entendu, 0 est le seul multiple de 0 et on a $0\mathbb{N} = \{0\}$.

I.2 – Division euclidienne

I.2.1 – Théorème (Division euclidienne)

Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Il existe alors un unique couple $(q, r) \in \mathbb{N}^2$ tel que :

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$$

On dit que q et r sont respectivement le quotient et le reste de la division euclidienne de a par b.

Remarque – Nous avons revu en début d'année comment poser en pratique une telle division.

Démonstration (pas tout à fait complète)

La preuve n'est pas explicitement au programme. Mais pas non plus hors programme!

Nous admettrons (bien que cela soit très facile) l'unicité. En ce qui concerne l'existence, une jolie preuve s'appuie sur l'algorithmique et sur la méthode pratique que l'on utilise pour poser une division. Nous avons fait cela en début d'année, pensez à la réviser.

Citation – « *Un algorithme est un objet mathématique comme les autres.* » Luc BOUGÉ, professeur dans le *Département Informatique et Télécommunications* de l'ÉNS Rennes.

En voici un version un peu plus formalisée mais il manque (volontairement) quelques détails. Les différentes étapes de la division conduisent (mais ce n'est pas totalement évident) à des égalités de la forme :

$$\begin{aligned}
&a = b \times q_0 + r_0 \qquad \text{avec} \quad q_0 = 0 \quad r_0 = a\\
&a = b \times q_1 + r_1\\
&\qquad \vdots\\
&a = b \times q_k + r_k\\
&\qquad \vdots\\
&a = b \times q_{n-1} + r_{n-1}\\
&a = b \times q_n + r_n \qquad \text{avec} \quad q_n = q \quad r_n = r
\end{aligned}$$

L'essentiel est de prouver la ***terminaison*** et la ***correction*** de cet algorithme. La correction est basée sur un ***invariant de boucle*** qui n'est rien d'autre que les égalités successives que l'on a écrites (mais il manque un détail essentiel!). La terminaison est basée sur un ***variant*** de boucle qui est le nombre r_k (le reste) qui est un entier positif strictement décroissant. ***Et voilà***!

Attention, comme annoncé, il manque quelques détails. Un peu plus précisément, ce qu'il manque c'est la condition que satisfait le reste r_k. Nous passons volontairement sous silence ce détail (qui n'en ai pas un). Vous pouvez prendre l'infinitive de chercher par vous même.

I.2.2 – Proposition

Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^*$ et q, r le quotient et le reste de la division euclidienne de a par b. Il y a alors équivalence entre :

(i) b divise a ;

(ii) $r = 0$.

Résultat admis (mais démonstration très facile).

Exercice M.1

1. Le nombre 366546 est-il divisible par 47?

2. Le nombre 5801868 est-il divisible par 127?

Exercice M.2

1. Décomposer 1148 en facteurs premiers.

2. Décomposer 45320 en facteurs premiers.

Exercice M.3 (⋆)

Pour tout entier $n \in \mathbb{N}$, montrer que n^2 divise $(n+1)^n - 1$.

Exercice M.4 (Très classique ⋆)

Soient a et n deux entiers naturels supérieurs au égaux à 2.

1. Démontrer que si $p = a^n - 1$ est premier alors nécessairement $a = 2$ et n est premier.

2. La réciproque est-elle vraie ?
Utilisez un ordinateur (par exemple avec l'application en ligne Wolfram|Alpha) ou une calculatrice.

I.2.3 – Application à l'écriture en base a (où $a \in \mathbb{N}^*$)

Exemples

1 ▶ Pour écrire par exemple 38 en base 2 on effectue des divisions euclidiennes successives par 2 jusqu'à obtenir un quotient nul.

$$\begin{array}{rcrcr} 38 & = & 2\times 19 & + & 0 \\ 19 & = & 2\times 9 & + & 1 \\ 9 & = & 2\times 4 & + & 1 \\ 4 & = & 2\times 2 & + & 0 \\ 2 & = & 2\times 1 & + & 0 \\ 1 & = & 2\times 0 & + & 1 \end{array}$$

L'écriture en base 2 est alors donné par les restes, en partant de la fin : il s'agit de 100110.

Cette écriture signifie (par définition de l'écriture en base 2) que

$$38 = 1\times 2^5 + 0\times 2^4 + 0\times 2^3 + 1\times 2^2 + 1\times 2^1 + 0\times 2^0.$$

2 ▶ Pour écrire 736 en hexadécimal (base 16) on effectue des divisions euclidiennes successive par 16 jusqu'à obtenir un quotient nul.

$$\begin{array}{rcrcr} 736 & = & 16\times 46 & + & 0 \\ 46 & = & 16\times 2 & + & 14 \\ 2 & = & 16\times 0 & + & 2 \end{array}$$

Rappelons que l'écriture hexadécimale utilise 16 symboles : les chiffres de 0 à 9 et les lettres de A à F. En héxadécimal A désigne le nombre 10, B le nombre 11, et F le nombre 15.

On obtient l'écriture hexadécimale de 736 en écrivant les restes 2, 14 et 0 avec la convention précédente : il s'agit donc de 2E0.

Cette écriture signifie (par définition de l'écriture héxadécimale) que

$$736 = 2\times 16^2 + 14\times 16^1 + 0\times 16^0.$$

Exercice M.5

Déterminer les écritures binaire et hexadécimale du nombre 2020.

II – PGCD et PPCM

II.1 – PGCD

II.1.1 – Théorème et Définition

Soit a et b deux entiers naturels dont l'un au moins est non nul.

(i) L'ensemble des diviseurs communs à a et b est l'ensemble $\mathscr{D}(a,b) = \mathscr{D}(a) \cap \mathscr{D}(b)$.

(ii) Cet ensemble $\mathscr{D}(a,b)$ est non vide et majoré.

(iii) Le plus grand élément de $\mathscr{D}(a,b)$ est appelé **PGCD** (**Plus Grand Commun Diviseur**) de a et de b. Il est noté $\mathrm{PGCD}(a,b)$ ou $a \wedge b$.

Résultat admis mais démonstration très facile.

Exemples

1 ► Quel est le PGCD de 15 et 12 ?

On a $\mathscr{D}(15) = \{1,3,5,15\}$ et $\mathscr{D}(12) = \{1,2,3,4,6,12\}$ d'où $\mathscr{D}(15,12) = \{1,3\}$ et donc :

$$\text{PGCD}(15,12) = 15 \wedge 12 = \max(\{1,3\}) = 3$$

2 ► Quel est le PGCD de 15 et 28 ?

On a $\mathscr{D}(15) = \{1,3,5,15\}$, $\mathscr{D}(28) = \{1,2,4,7,14,28\}$ d'où $\mathscr{D}(15,28) = \mathscr{D}(15) \cap \mathscr{D}(28) = \{1\}$ et donc :

$$\text{PGCD}(15,28) = 15 \wedge 28 = \max(\{1\}) = 1$$

Remarques

1 ► La méthode précédente consistant à énumérer tous les diviseurs n'est ***pas du tout efficace***. Nous ferrons beaucoup mieux, soit à l'aide de l'***algorithme d'Euclide***, soit à l'aide de la ***décomposition en facteurs premiers***.

2 ► Lorsque le PGCD de deux entiers est égal à un, on dit que ces entiers sont ***premiers entre-eux***. Cela revient à dire qu'ils n'ont pas de diviseurs communs autre que 1.

II.2 – Algorithme d'Euclide et conséquences

II.2.1 – Lemme

Soit $(a,b) \in (\mathbb{N}^*)^2$. Notons q et r le quotient et le reste de la division euclidienne de a par b. Si $r \neq 0$ alors on a :

(i) $\mathscr{D}(a,b) = \mathscr{D}(b,r)$

(ii) $a \wedge b = b \wedge r$ ou avec l'autre notation $\text{PGCD}(a,b) = \text{PGCD}(b,r)$

*Le point **(i)** se démontre facilement par double inclusion.*

II.2.2 – Lemme

Pour tout $a \in \mathbb{N}^*$ on a : $\text{PGCD}(a,0) = a \wedge 0 = a$.

Démonstration

On a vu que tous les entiers divisent 0 c'est-a-dire $\mathscr{D}(0) = \mathbb{N}$. On a donc :

$$\mathscr{D}(a,0) = \mathscr{D}a \cap \mathscr{D}(0) = \mathscr{D}a \cap \mathbb{N} = \mathscr{D}(a)$$

Et comme a est le plus grand diviseur de lui même :

$$\text{PGCD}(a,0) = a \wedge 0 = \max(\mathscr{D}(a)) = a$$

Exemple – Pour déterminer le PGCD de 456 et 135 effectuons les divisions euclidiennes suivantes :

$$\begin{aligned} 456 &= 135 \times 3 + 51 \\ 135 &= 51 \times 2 + 33 \\ 51 &= 33 \times 1 + 18 \\ 33 &= 18 \times 1 + 15 \\ 18 &= 15 \times 1 + \boxed{3} \\ 15 &= 3 \times 5 \end{aligned}$$

En utilisant les lemmes précédents on obtient :

$$\begin{aligned} \text{PGCD}(456,135) &= \text{PGCD}(135,51) \\ &= \text{PGCD}(51,33) \\ &= \text{PGCD}(33,18) \end{aligned}$$

$$\begin{aligned} &= \text{PGCD}(18,15)\\ &= \text{PGCD}(15,3)\\ &= \text{PGCD}(3,0)\\ &= 3 \end{aligned}$$

On a donc PGCD(456, 135) = 3 et on observe que le résultat est le ***dernier reste non nul*** dans la succession de divisions euclidiennes effectuées précédemment.

II.2.3 – Description de l'algorithme d'Euclide

On désire calculer le PGCD de deux entiers naturels a et b (dont l'un des deux au moins est non nul). Quitte à échanger a et b, ce qui ne change pas leur PGCD, on peut supposer que $b \leqslant a$ et donc $a \neq 0$.

- Si $b = 0$ alors $\text{PGCD}(a,b) = a$ et il n'y a aucun calcul à faire.
- Sinon on pose $r_0 = a$, $r_1 = b$ et on effectue la division euclidienne de r_0 par r_1 : il existe un unique couple (q_1, r_2) tel que :
$$r_0 = r_1 q_1 + r_2 \quad \text{avec} \quad 0 \leqslant r_2 < r_1.$$
On a alors $\text{PGCD}(a,b) = \text{PGCD}(r_0,r_1) = \text{PGCD}(r_1,r_2)$ (en utilisant l'un des lemmes précédents).
- Si $r_2 = 0$ le calcul est terminé car $\text{PGCD}(a,b) = \text{PGCD}(r_1,0) = r_1$.
- Sinon on effectue la division euclidienne de r_1 par r_2 : il existe un unique couple (q_2, r_3) tel que :
$$r_1 = r_2 q_2 + r_3 \quad \text{avec} \quad 0 \leqslant r_3 < r_2.$$
- On a alors $\text{PGCD}(a,b) = \text{PGCD}(r_0,r_1) = \text{PGCD}(r_1,r_2) = \text{PGCD}(r_2,r_3)$.
- Si $r_3 = 0$ le calcul est terminé et $\text{PGCD}(a,b) = \text{PGCD}(r_2,0) = r_2$.
- Sinon on continue ce procédé de manière itérative en construisant les nombres r_k et q_k tels que $a = r_0$, $b = r_1$ et :

$$\begin{array}{rcll} r_0 &=& r_1 q_1 + r_2 & \text{avec} \quad 0 < r_2 < r_1\\ r_1 &=& r_2 q_2 + r_3 & \text{avec} \quad 0 < r_3 < r_2\\ \vdots && \vdots & \vdots\\ r_{n-2} &=& r_{n-1} q_{n-1} + \boxed{r_n} & \text{avec} \quad 0 < r_n < r_{n-1}\\ r_{n-1} &=& r_n q_n & (\textit{i.e. } r_{n+1} = 0) \end{array}$$

Le point essentiel est que la suite (r_k) étant constituée d'entiers positifs strictement décroissants, il existe $n \in \mathbb{N}$ tel que $r_{n+1} = 0$ et l'algorithme s'arrête donc à cette étape (***variant de boucle*** démontrant la ***terminaison*** dans la langage de l'algorithmique).

À chaque étape on a $\text{PGCD}(r_{k-1}, r_k) = \text{PGCD}(r_k, r_{k+1})$ (***invariant de boucle*** dans le langage de l'algorithmique) donc :

$$\text{PGCD}(a,b) = \text{PGCD}(r_0,r_1) = \cdots = \text{PGCD}(r_n, r_{n+1}) = \text{PGCD}(r_n, 0) = r_n$$

On a donc ***démontré*** (et oui) le théorème suivant :

II.2.4 – Théorème

> Avec les notations précédentes, le PGCD de a et b est précisément ***le dernier reste non nul dans l'algorithme d'Euclide***.

Exercice M.6

Soient $a = 31682$ et $b = 11417$.

1. Déterminer le PGCD de a et b par l'algorithme d'Euclide.

2. Déterminer le PGCD de a et b en les décomposant préalablement en facteurs premiers.

3. Quelle méthode préférez-vous ?

Exercice M.7 (- Algorithme d'Euclide en Python)

Écrire une fonction Python `pgcd(a,b)` prenant en entrée deux entiers naturels dont l'un au moins est non nul et qui retourne le PGCD de a et b par utilisation de l'algorithme d'Euclide (si $b > a$ on commence par échanger a et b).

*Dans l'objectif de l'oral du concours Banque PT, il est **absolument impensable** de ne pas savoir faire cela.*

II.2.5 – Proposition (Propriétés du PGCD)

Soit $(a,b,k) \in (\mathbb{N}^*)^3$.

(i) On a : $(ka) \wedge (kb) = k(a \wedge b)$ ou écrit autrement $\text{PGCD}(ka,kb) = k\,\text{PGCD}(a,b)$

(ii) Les diviseurs communs de a et b sont précisément les diviseurs de $a \wedge b = \text{PGCD}(a,b)$:

$$\forall d \in \mathbb{N},\ \Big(d \mid a \ \text{ET}\ d \mid b\Big) \Longleftrightarrow d \mid (a \wedge b) = \text{PGCD}(a,b)$$

Résultat admis (mais à connaître).

Remarques

1 ▶ Le deuxième résultat peut s'écrire sous une forme plus concise (mais pas forcément plus claire) :

$$\mathscr{D}(a,b) = \mathscr{D}(a \wedge b)$$

2 ▶ En divisant un couple d'entiers par leur PGCD on les rend premiers entre eux. Si $(a,b) \in (\mathbb{N}^*)^2$ est donné et que l'on note $d = a \wedge b$ alors on sait que d divise a et b donc il existe $(\alpha,\beta) \in (\mathbb{N}^*)^2$ tel que :

$$a = d\alpha \quad b = d\beta$$

On a alors :

$$d = a \wedge b = (d\alpha) \wedge (d\beta) = d(\alpha \wedge \beta)$$

D'où en simplifiant par d :

$$\text{PGCD}(\alpha,\beta) = \alpha \wedge \beta = 1$$

3 ▶ Soit r un nombre rationnel non nuls (positifs pour simplifier). Ce nombre peut donc s'écrire :

$$r = \frac{a}{b}$$

avec $(a,b) \in (\mathbb{N}^*)^2$. Si, comme dans la remarque précédente on divise a et b par leur PGCD d on a alors :

$$r = \frac{d\alpha}{d\beta} = \frac{\alpha}{\beta}$$

avec $\text{PGCD}(\alpha,\beta) = \alpha \wedge \beta = 1$. Cette deuxième écriture est dite ***irréductible*** car son numérateur et son dénominateur n'ont pas de diviseur commun (autre que 1). Elle a l'avantage d'être ***unique***.

4 ▶ Les professeurs un peu sérieux (et/ou psychorigide) exigent que les nombres rationnels soient toujours écrits sous forme irréductible. Pensez donc toujours à simplifier.

II.3 – De l'arithmétique un peu plus sérieuse

Exercice M.8 (Algorithme d'Euclide étendu)

On reprend les notations utilisées dans la description de l'algorithme d'Euclide. Et on définit les suites (u_k) et (v_k) par récurrence (double) :

$$\begin{cases} u_0 = 1 & v_0 = 0 \\ u_1 = 0 & v_0 = 1 \\ u_{k+1} = -q_k u_k + u_{k-1} \\ v_{k+1} = -q_k v_k + v_{k-1} \end{cases}$$

1. Démontrer, par récurrence double, que la propriété :

$$\mathscr{P}(k) = \text{« } au_k + bv_k = r_k \text{ »}$$

est vraie pour tout $k \in [\![0, n+1]\!]$. Dans la langage de l'algorithmique il s'agit simplement d'un ***invariant de boucle***.

2. Compte-tenu de ce que l'on sait déjà pour l'algorithme d'Euclide classique, quelle relation obtient-t-on au rang n ?
3. Adapter votre algorithme d'Euclide de l'exercice **N.7** en écrivant une fonction Python `euclide_etendu(a,b)` prenant comme argument deux entiers naturels dont l'un au moins est non nul et qui renvoie la liste $[\delta, u, v]$ avec $\delta = \text{PGCD}(a,b)$, $u = u_n$ et $v = v_n$.

Exercice M.9

Soient $a = 394485$ et $b = 9548$

1. À l'aide da la fonction `pgcd(a,b)` de l'exercice **N.7**, déterminer $\delta = \text{PGCD}(a,b)$.
2. À l'aide da la fonction `euclide_etendu(a,b)` de l'exercice précédent **N.8**, déterminer deux entiers relatifs u et v tels que $\delta = au + bv$.
   Vérifier la cohérence des résultats obtenus.

Exercice M.10 (En avant pour les résultats classiques d'arithmétique! ⋆)

Démontrer les théorèmes suivants

1. **Théorème de Bézout** - Soient a et b deux entiers naturels dont l'un au moins est non nul. Alors il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = \text{PGCD}(a,b) = a \wedge b$.
2. **Corollaire** - Soient a et b deux entiers naturels dont l'un au moins est non nul. Alors a et b sont premiers entre eux si et seulement si il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.
   On rappelle que deux entiers sont dit premiers entre eux si leur PGCD vaut 1.
3. **Lemme d'Euclide** - Si p est un nombre premier divisant un produit ab alors p divise a ou p divise b.
4. **Théorème de Gauss** - Si a divise bc et que a est premier avec b, alors a divise c.

II.4 – PPCM

II.4.1 – Proposition et Définition

Soit a et b deux entiers naturels non nuls.

(i) On note $\mathcal{M}(a)$ l'ensemble des multiples **non nuls** de a.

(ii) L'ensemble $\mathcal{M}(a,b) = \mathcal{M}(a) \cap \mathcal{M}(b)$ des multiples communs **non nuls** de a et de b est un ensemble non vide.

(iii) Le plus petit élément de $\mathcal{M}(a,b)$ est appelée PPCM (Plus Petit Commun Multiple) de a et b. Il est noté $\text{PPCM}(a,b)$ ou $a \vee b$.

Démonstration

L'ensemble $\mathcal{M}(a,b)$ est non vide car il contient le produit ab. Étant une partie non vide de $\mathbb{N}$, l'ensemble $\mathcal{M}(a,b)$ possède un plus petit élément. La définition précédente est donc valide.

Exemples

1 ▶ Quel est le PPCM de 6 et 10 ?

$$\mathcal{M}(6) = \{6, 12, 18, 24, \boxed{30}, 36, \ldots\}$$
$$\mathcal{M}(10) = \{10, 20, \boxed{30}, 40, 50, 60 \ldots\}$$

D'où $\text{PPCM}(6,10) = 30$.

2 ▶ Quel est le PPCM de 12 et 30 ?

$$\mathcal{M}(12) = \{12, 24, 36, 48, \boxed{60}, 72, \ldots\}$$
$$\mathcal{M}(30) = \{30, \boxed{60}, 90, 120, 150, \ldots\}$$

D'où $\text{PPCM}(12,30) = 60$.

Remarques

1 ▶ Dans les deux cas précédents, on remarque que le PPCM n'est pas (comme on pourrait naïvement le penser) le produit des deux entiers :

$$\text{PPCM}(6,10) = 30 \neq 6 \times 10 = 60$$
$$\text{PPCM}(12,30) = 60 \neq 12 \times 30 = 360$$

2 ▶ La méthode précédente consistant à énumérer tous les multiples n'est ***pas du tout efficace***. Nous ferrons beaucoup mieux, soit en utilisant le ***lien entre PGCD et PPCM***, soit à l'aide de la ***décomposition en facteurs premiers***.

II.4.2 – Proposition (Propriétés élémentaires du PPCM)

Soit a et b deux entiers naturels non nuls.

(i) On a : $a \vee a = a$ et $a \vee 1 = a$

(ii) On a : $\max(a,b) \leqslant a \vee b \leqslant ab$

(iii) Si $a \mid b$ alors $a \vee b = b$. Et la réciproque est vraie !

Résultat admis, mais à connaître.

II.4.3 – Proposition

Soit a et b deux entiers naturels non nuls. Alors les multiples communs de a et b sont les multiples de $a \vee b$. Autrement dit on a :

$$\mathscr{M}(a,b) = (a \vee b).\mathbb{N}$$

Résultat admis, mais à connaître absolument.

II.4.4 – Théorème (Lien entre PGCD et PPCM)

Soit a et b deux entiers naturels non nuls. On a alors :

$$(a \wedge b)(a \vee b) = ab$$

c'est-à-dire :

$$\text{PGCD}(a,b) \times \text{PPCM}(a,b) = ab$$

Résultat admis, mais à connaître absolument.

II.4.5 – Proposition

Soit $(a,b,k) \in \left(\mathbb{N}^*\right)^3$. On a alors :

$$(ka) \vee (kb) = k(a \vee b) \qquad \text{c'est-à-dire} \qquad \text{PPCM}(ka,kb) = k\,\text{PPCM}(a,b)$$

Résultat admis, mais à connaître.

III – Nombres premiers

III.1 – Notion de nombre premier

III.1.1 – Définition (Nombre premier)

Un entier naturel p est dit premier s'il possède exactement deux diviseurs (1 et lui-même).

Remarques

1 ▶ Avec cette définition, le nombre 1 n'est ***pas premier*** car il n'a qu'un seul diviseur.

2 ▶ Les nombres 2, 3, 5, 7, 11, 13, 17 sont premiers.

3 ▶ Le ***plus grand nombre premier connu à ce jour*** (c'est-à-dire vérifié d'une manière indiscutable) est le nombre (dit de Mersenne) :

$$M_{82\,589\,933} = 2^{82\,589\,933} - 1$$

Ce record date du 21 décembre 2018. Pour information, les précédent records dataient du 26 décembre 2017 et de janvier 2016.

Bien sûr il y en a de plus grand (voir plus loin). Mais à ce jour on ne les connait pas!

Celui-ci possède « beaucoup » de chiffres en écriture décimale. Nous y consacrerons un exercice.

Pour plus de détails sur la recherche effective de très grands nombres premiers, vous pouvez consultez le le site du projet **GIMPS** (***the Great Internet Mersenne Prime Search***) : www.mersenne.org.

4 ▶ Cette course, à la recherche de grands nombres premiers, est tout sauf un jeux de mathématiciens.

C'est d'abord un moyen très concret de mettre à l'épreuve notre savoir et notre technologie existante, tant au niveau mathématique que d'informatique ***software*** et d'informatique ***hardware***. Et les challenges font, de fait, progresser la science et la technologie.

C'est aussi et surtout un sujet ***crucial*** en cryptographie (et plus généralement en cryptologie). Pour faire simple, tout ce qui a un rapport avec la sécurité des communications (confidentialité, authenticité et intégrité).

Attention, nous ne sommes ***pas du tout*** dans le monde des bisounours : quand on parle de sécurité des communications, on parle de paiements par carte bancaire, de protocoles sécurisés sur internet (PGP, SSH, SSL, TLS, ...) mais aussi, par exemple, de communication entre le chef d'un état muni de l'***arme nucléaire*** et sa hiérarchie militaire!

Précisément on a besoin de (***très***) gros nombres premiers dans le système de ***chiffrement à clefs publiques*** appelé **RSA** (du nom de leurs inventeurs Rivest, Shamir and Adleman qui ont présenté ce système en 1977).

Effectivement, 1977, c'est loin. Mais contrairement à ce que l'on peut parfois entendre **RSA** est encore utilisé de nos jours, en général conjointement à d'autres systèmes de chiffrements (typiquement à ***clefs privées***).

Exercice M.11

Soit n un entier naturel supérieur ou égal à 2 et $d \in [\![2, n]\!]$ son plus petit diviseur autre que 1.

1. Démontrer que d est un nombre premier.
2. En déduire que tout entier supérieur ou égal à 2 possède au moins un diviseur premier.
3. Écrire une fonction Python `plus_petit_diviseur(n)` prenant en entrée un entier n supérieur ou égal à 2 et renvoyant son plus petit diviseur autre que 1.

   Remarque - *D'après la première question le résultat sera toujours un nombre premier.*

III.1.2 – Théorème (Euclide)

L'ensemble des nombres premiers est infini.

Déjà démontré (par l'absurde) en cours d'année.

III.2 – Décomposition en facteurs premiers

III.2.1 – Théorème (Théorème fondamental de l'arithmétique - le Graal!)

Tout entier supérieur ou égal à 2 peut s'écrire de manière unique (à l'ordre prêt des facteurs) comme un produit de nombres premiers.

Résultat admis conformément au programme officiel.

Remarques

1 ▶ En regroupant les nombres premiers égaux et en les ordonnant on obtient donc une décomposition de la forme :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

avec $(\alpha_1, \alpha_2 ..., \alpha_k) \in \left(\mathbb{N}^*\right)^k$ et $p_1 < p_2 < \dots < p_k$.

2 ▶ Si on dispose de deux entiers a et b, on peut écrire leurs décompositions avec les ***mêmes facteurs premiers*** en autorisant ***certains exposants à être nuls*** :

$$\begin{cases} a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \\ b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} \end{cases}$$

où les exposants α_i et β_j peuvent éventuellement être nuls.

Exemples

1 ▶ Les décompositions de 15 et 12 sont les suivantes :

$$\begin{cases} 15 = 3^1 \times 5^1 \\ 12 = 2^2 \times 3 \end{cases}$$

2 ▶ Si l'on veut écrire ces deux nombres à l'aide des mêmes facteurs premiers, il suffit d'écrire :

$$\begin{cases} 15 = 2^0 \times 3^1 \times 5^1 \\ 12 = 2^2 \times 3^1 \times 5^0 \end{cases}$$

III.2.2 – Théorème

Soit a et b deux entiers naturels non nuls dont les décompositions en facteurs premiers sont les suivantes :

$$\begin{cases} a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \\ b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} \end{cases}$$

Il y a alors équivalence entre :

(i) $a \mid b$;

(ii) $\forall i \in [\![1, k]\!],\ \alpha_i \leqslant \beta_i$.

Résultat admis.

Exemples

1 ▶ Décomposons le nombre 90 en facteurs premiers.

On y va de proche en proche : il est d'abord divisible par 2 et on a $90 = 2 \times 45$. Puis $45 = 5 \times 9$ (ça c'est dans les tables de multiplication : école primaire CE2).

La décomposition en facteurs premiers de 90 est donc :

$$90 = 2 \times 3^2 \times 5$$

2 ▶ D'après la proposition précédente, les diviseurs de 90 sont exactement les nombres de le forme

$$d = 2^a \times 3^b \times 5^c$$

avec $0 \leqslant a \leqslant 1$, $0 \leqslant b \leqslant 2$ et $0 \leqslant c \leqslant 1$. Il y a donc autant de diviseurs que de choix possibles pour le triplet $(a, b, c) \in [\![0, 1]\!] \times [\![0, 2]\!] \times [\![0, 1]\!]$. Autrement dit il y a $2 \times 3 \times 2 = 12$ diviseurs.

III.2.3 – Théorème

Soit a et b deux entiers naturels non nuls dont les décompositions en facteurs premiers sont les suivantes :

$$\begin{cases} a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \\ b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} \end{cases}$$

On a alors :

$$\begin{cases} \text{PGCD}(a,b) = a \wedge b = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k} \\ \text{PPCM}(a,b) = a \vee b = p_1^{\text{M}_1} p_2^{\text{M}_2} \dots p_k^{\text{M}_k} \end{cases}$$

où $\forall i \in [\![1,k]\!]$, $m_i = \min(\alpha_i, \beta_i)$ et $\text{M}_i = \max(\alpha_i, \beta_i)$.

Résultat admis.

Exemples

1 ▶ Recherchons à nouveau le PGCD de 15 et 12.
Les décompositions en facteurs premiers de 15 et 12 sont :

$$15 = 3 \times 5 = 2^0 \times 3^1 \times 5^1 \qquad 12 = 2^2 \times 3 = 2^2 \times 3^1 \times 5^0$$

D'après le théorème précédente on a :

$$\text{PGCD}(15,12) = 2^{\min(0,2)} \times 3^{\min(1,1)} \times 5^{\min(1,0)} = 2^0 \times 3^1 \times 5^0 = 3$$

2 ▶ Recherchons à nouveau le PPCM de 12 et 30.
Les décompositions en facteurs premiers de 12 et 30 sont :

$$12 = 2^2 \times 3 = 2^2 \times 3^1 \times 5^0 \qquad 30 = 2 \times 3 \times 5 = 2^1 \times 3^1 \times 5^1$$

D'après le théorème précédente on a :

$$\text{PPCM}(12,30) = 2^{\max(2,1)} \times 3^{\max(1,1)} \times 5^{\max(0,1)} = 2^2 \times 3^1 \times 5^1 = 60$$

Exercice M.12

Démontrer que ***la longueur d'un entier*** en base 10 (*i.e.* son nombre de chiffres) vaut $\ell(n) = \lfloor \log_{10}(n) \rfloor + 1$.

Exercice M.13 (Longueur de $\text{M}_{82\,589\,933}$)

1. En négligeant le -1, c'est à dire en admettant que $\left\lfloor \log_{10}\left(2^{82\,589\,933} - 1\right) \right\rfloor = \left\lfloor \log_{10}\left(2^{82\,589\,933}\right) \right\rfloor$, calculer la longueur de $\text{M}_{82\,589\,933}$.
2. On dispose de cahiers A4 (21 cm × 29,7 cm) grands formats à petits carreaux de 192 pages. En écrivant un chiffre par petit carreau, combien de cahiers faut-il pour écrire $\text{M}_{82\,589\,933}$?

Exercice M.14 (Facile mais incontournable)

1. Démontrer qu'un entier naturel $n \geqslant 2$ est premier si et seulement s'il ne possède aucun diviseur entre 2 et $\lfloor \sqrt{n} \rfloor$.
2. Écrire une fonction Python `est_premier(n)` prenant en entrée un entier naturel non nul et renvoyant le booléen `True` ou `False` suivant que n est premier ou pas.
   On utilisera la question précédente pour optimiser ce ***test de primalité****.*
3. Écrire une fonction Python `premiers(n)` prenant en entrée un entier naturel non nul et renvoyant la liste de tous les nombres premiers inférieurs au égaux à n.
   On utilisera une boucle, la fonction `est_premiers(n)` *et la méthode* `append()`.

Exercice M.15 (Décomposition en facteurs premiers ⋆)

On sait que tout entier naturel $n \geqslant 2$ s'écrit de manière unique :

$$n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_r^{e_r}$$

avec $p_1 < p_2 < \cdots < p_r$, tous ces nombres étant premiers et pour tout $i \in [\![1,r]\!]$, $e_i \geqslant 1$.

On souhaite écrire une fonction Python `decomposition(n)` prenant en entrée un entier n supérieur ou égal à 2 en renvoyant la liste `[`$(p_1, e_1), (p_2, e_2), \cdots, (p_r, e_r)$`]`.

Voici quelques consignes un peu plus précises.

1. Commencer, pour être tranquille en faisant une copie de n : `m = n` et déclarer une liste vide `D = []`.
2. On considère tout d'abord p_1 = `plus_petit_diviseur(m)`. À l'aide d'une boucle, calculer la plus grande puissance

de p_1 qui divise m : on obtient ainsi l'exposant e_1.
Ajouter alors le couple (p_1, e_1) à la liste `D` et remplacer m par $\dfrac{m}{p_1^{e_1}}$

3. Continuez itérativement (ou récursivement) ce procédé jusqu'à ce que m soit égal à 1.
4. Tester votre fonction `decomposition(n)` avec le nombre $n = 419879824$.

Exercice M.16 (Nombre de Fermat ⋆)

1. Soit $n \in \mathbb{N}$ et on suppose que $N = 2^n + 1$ est un nombre premier. Démontrer que n est une puissance de deux, c'est-à-dire qu'il existe $k \in \mathbb{N}$ tel que $N = 2^{2^k} + 1$.
2. On appelle k-ième nombre de Fermat le nombre $F_k = 2^{2^k} + 1$. Écrire une fonction Python `fermat(k)` prenant en entrée un entier naturel (éventuellement nul) et renvoyant la valeur de F_k.
3. Faites afficher (par Python) les 6 premiers nombres de Fermat F_0, ... F_5.
4. Fermat avait émis l'hypothèse que tous ces nombres étaient premiers. Mais Euler est venu mettre son grain de sel... Et vous, en utilisant, la fonction `est_premier(n)` de l'exercice **N.14**, qu'en pensez-vous ?

Fin du chapitre