Nombres entiers

Antoine Louatron

Table des matières

I Diviseurs

I.1 Multiples et diviseurs

I.1.1 Définition

Soient $a, b \in \mathbb{N}$. On dit que a divise *b ou que b est un* multiple *de a si il existe un entier $k \in N$ tel que*

$$ak = b$$

. On note $a|b$.

I.1.2 Remarque

1. Tout entier divise 0. Il suffit en effet de prendre $k = 0$. De plus 1 divise tout entier.
2. Si $a|b$ et $b \neq 0$, alors $a \leqslant b$.

I.1.3 Exemple

Trouver tous les diviseurs de 24.

I.1.4 Proposition

Soient $a, b, c, d \in \mathbb{N}$.

1. *$a|b$ et $b|a \Rightarrow a = b$.*
2. *Pour tout $u, v \in \mathbb{N}$, si $d|a$ et $d|b$ alors $d|au + bv$.*
3. *Si $a|b$ et $c|d$ alors $ac|bd$. En particulier sous ces conditions on a pour tout $n \in \mathbb{N}$: $a^n|b^n$.*
4. *Si $d \neq 0$ on a $a|b \iff ad|bd$.*

Preuve.

1. Supposons que $a|b$ et $b|a$. La propriété est vraie si un des deux entiers est nul, car 0 est le seul entier divisé par 0. On suppose donc $a, b \neq 0$. Par définition il existe α et β entiers tels que
$$a\alpha = b \text{ et } b\beta = a$$
on en déduit que $a\alpha\beta = a$ et donc que $\alpha\beta = 1$ (par intégrité). Les seuls diviseurs de 1 étant ± 1, on en déduit $\alpha = \beta = \pm 1$ et la conclusion désirée.
2. Soient $u, v \in \mathbb{N}$. Par définition de la divisibilité on peut prendre $\alpha, \beta \in \mathbb{N}$ tels que $d\alpha = a$ et $d\beta = b$. Ainsi $d\alpha u = au$ et $d\beta v = bv$ et donc
$$d(\alpha u + \beta v) = au + bv.$$
Donc $d|au + bv$.
3. On note comme d'habitude $a\alpha = b$ et $c\gamma = d$. Alors $ac\alpha\gamma = cd$ et donc $ac|bd$. En particulier, par récurrence immédiate $a^n|b^n$.
4. Soit $d \in \mathbb{N} - \{0\}$. On a alors $a\alpha = b \iff ad\alpha = bd$ pour tout triplet d'entiers. ∎

I.2 PGCD

I.2.1 Définition-Proposition

Soient $a, b \in \mathbb{N}$, non tous les deux nuls.

1. *Le plus grand entier d qui divise à la fois a et b est appelé Plus Grand Commun Diviseur ou PGCD de a et b, on ne note* $\text{pgcd}(a, b)$.
2. *Le plus petit entier d qui soit à la fois multiple de a et b est appelé Plus Petit Commun Multiple ou PPCM de a et b, on ne note* $\text{ppcm}(a, b)$.

Preuve.

On doit prouver l'existence d'un maximum et d'un minimum.

Considérons $G = \{d \in \mathbb{N} |\ d|a \text{ et } d|b\}$. Alors $1 \in G$ donc G est non vide. De plus, si $d \in G$, alors $d \leqslant a$ et $d \leqslant b$ (ou une seule condition si l'un est nul), donc G est majoré. Ainsi G admet un maximum.

Pour l'existence du PPCM, il suffit de remarquer qu'il existe un multiple commun : ab. ∎

I.2.2 Exemple

Calculer $\text{pgcd}(12, 42)$, $\text{ppcm}(6, 14)$.

I.2.3 Application aux fractions

Si $\frac{p}{q} \in \mathbb{Q}$, alors on peut réduire la fraction en divisant p et q par leur pgcd. On obtient encore des entiers. De plus, si $\alpha|p$ et $\alpha|q$ alors $pgcd(\frac{p}{\alpha}, \frac{q}{\alpha}) = \frac{1}{\alpha}\,\text{pgcd}(p,q)$

Pour calculer $\frac{a}{b} + \frac{c}{d}$, le meilleur dénominateur commun est $\text{ppcm}(b,d)$.

II Division d'entiers

II.1 Division euclidienne

II.1.1 Théorème
Soit $(a,b) \in \mathbb{N} \times \mathbb{N} - \{0\}$. Alors il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r \text{ et } 0 \leqslant r < b$$

Preuve.

— Existence On le prouve d'abord pour $a \geqslant 0$.

Considérons l'ensemble $E = \{a - bq | q \in \mathbb{N} \text{ et } a - bq \geqslant 0\}$. C'est un ensemble non vide car contenant 0 et donc il admet un minimum que l'on note r. Maintenant on pose $r = a - bq$ pour un certain $q \in \mathbb{N}$ et on a $r \geqslant 0$ par définition. Mais $r < b$ car sinon $r - b = a - b(q+1) \geqslant 0$ et donc $r - b \in E$ et $r > r - q$ ce qui est impossible par définition du minimum.

— Unicité Si $a = bq + r = bq' + r'$ (possédant les bonnes propriétés) alors $b(q - q') = r' - r$. Mais $-b < r' - r < b$ donc $q - q' = 0$ et finalement $r' - r = 0$. ∎

II.1.2 Remarque

Il s'agit de la première division que l'on apprend à faire à l'école : la division avec reste.

II.1.3 Exercice
Calculer le quotient et le reste de la division euclidienne de 15478 par 38.

II.1.4 Proposition
$b|a$ ssi le reste dans la division euclidienne de a par b est nul.

Preuve.
On écrit $a = bq + r$ la division euclidienne de a par b. Si $r = 0$ alors $a = bq$ et donc $b|a$.

Réciproquement si $b|a$ alors on peut écrire $a = bk$ qui est une division euclidienne de a par b dont le reste vaut 0. Par unicité du reste... ∎

II.2 Algorithme d'Euclide

II.2.1 Lemme
Soient $a, b \in \mathbb{N}\backslash\{0\}$. On note $d = \text{pgcd}(a,b)$ et $a = bq + r$ la division euclidienne de a par b. Alors $d|r$.

Preuve.
Immédiat : $r = a - bq$ et d divise à la fois a et b. Voir les propriétés de début de cours. ∎

II.2.2 Algorithme

Données : a, b deux entiers naturels non nuls. Sortie : $d = \text{pgcd}(a,b)$

On note $r_{-1} = a$, $r_0 = b$ et pour tout $n \in \mathbb{N}$, r_{n+2} est le reste de la division de r_{n+1} par r_n. Le pgcd de a et b est le dernier reste non nul obtenu.

On a donc pour les premières étapes, en notant q_n le quotient à l'étape n

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\dots \end{aligned}$$

sachant que le quotient n'est d'aucune utilité pour le calcul.

```
def pgcd(a,b):
    u, v = a, b
    while v != 0:
        u, v = v, u % v
    return u
```

Preuve.
Si $d = \text{pgcd}(a, b)$, alors d divise tous les restes obtenus par applications successives du lemme
Notons r_{k+1} le dernier reste non nul. Alors $r_{k+1}|r_k$. Mais on avait $r_{k-1} = r_kq_{k+1} + r_{k+1}$ donc $r_{k+1}|r_{k-1}$ car c'est un diviseur des deux termes de la somme. Par récurrence immédiate, r_{k+1} divise tous les restes précédents donc r_{k+1} divise à la fois a et b et donc $r_{k+1} \leqslant d$ et $d|r_{k+1}$ donc $d = r_{k+1}$. ∎

Coin culture Cet algorithme est fondamental en informatique, et plus particulièrement en sécurité.

II.2.3 Exemple
A l'aide de python, calculer pgcd(1458, 7788).
Calculer à la main pgcd(741, 51)

III Nombres premiers

III.1 Vocabulaire

III.1.1 Définition
Un entier naturel $\geqslant 2$ est dit premier s'il ne possède pas d'autres diviseurs que 1 et lui même.

III.1.2 Exemple
2,3,5,7,11,13,17,19,23,29,31....

III.1.3 Exercice
Ecrire tous les nombres de 2 à 100 et en extraire les nombres premiers par l'algorithme du crible d'Erathostène : 2 est premier, on raye tous ses multiples. Le premier nombre non rayé est alors premier. On raye tous ses multiples.... On s'arrête à $10 = \sqrt{100}$ et tous les nombres non rayés sont premiers.
En effet, si $n = pq$ est une vraie factorisation, alors l'un de p ou q est inférieur à $\sqrt{n}$...

III.1.4 Algorithme

Donnée : un entier n Sortie : la liste de tous les nombres premiers inférieur à n

```
def erathostene(n):
    l = list(range(2, n + 1))
    a = 2
    res = []
    while a *a <= n:
        l = [m for m in l if m % a != 0]
        res.append(a)
        a = l[0]
    res.extend(l)
    return res
```

III.1.5 Proposition
L'ensemble des nombres premiers est infini.

Preuve.
Supposons le contraire et soient $p_1, \dots, p_n$ l'ensemble des nombres premiers.

Alors $A = p_1 p_2 \dots p_n + 1 \in \mathbb{N}$ et donc admet un diviseur premier noté p_i (c'est un nombre premier donc l'un de ceux que l'on connaît). Mais alors, vu que $p_i | p_1 \dots p_n$ on a $p_i | A - p_1 \dots p_n$ donc $p_i | 1$ ce qui est impossible.

Donc l'ensemble des nombres premiers n'est pas fini. ∎

III.2 Factorisation

III.2.1 Lemme

Soit $n \in \mathbb{N} \backslash \{0, 1\}$. Alors n possède un diviseur premier.

Preuve.
On prouve la propriété $P(n)$: n possède un diviseur premier par récurrence pour les entiers $\geqslant 2$.

— P(2) est vraie car $2|2$.

— Supposons $P(k)$ vraie pour tous les entiers $k \leqslant n$ où n est un naturel fixé.
Montrons que $P(n+1)$ est vraie. Deux cas se présentent :

1. Si $n+1$ est premier alors il possède un diviseur premier : lui même.
2. Sinon $n+1$ possède un diviseur $1 < q < n+1$. Par hypothèse de récurrence q possède un diviseur premier p. On a donc $p|q$ et $q|n+1$ donc $p|n+1$.

— Finalement, par récurrence, tout $n \geqslant 2$ possède un diviseur premier.

III.2.2 Décomposition en facteur premiers

Soit $n \in \mathbb{N}$ et $n > 1$. Alors n possède un diviseur premier p_1 et donc $n = p_1 q_1$ avec $q_1 \in \mathbb{N}$. Si $q_1 > 1$ alors il possède lui aussi un diviseur premier $q_1 = p_2 q_2$ et donc $n = p_1 p_2 q_2$.

On voit ainsi que l'on peut continuer jusqu'à ce que $q = 1$ (on s'arrête à un moment car la suite des q_i est décroissante donc stationnaire !)

III.2.3 Théorème
Soit $n \in Z - \{0\}$. Alors il existe une unique famille fine de nombre premiers $(p_i)_{i \in [\![1,k]\!]}$ et une unique famille d'entiers $(\alpha_i)_{i \in [\![1,k]\!]}$ telles que

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

C'est la décomposition en facteurs premiers de n.

Preuve.
Hors programme ∎

III.2.4 Exemple

La décomposition en facteurs premiers de 60 est

$$60 = 2^2 \times 3 \times 5$$

III.2.5 Exercice

Montrer que $\sqrt{2}, \sqrt{3}$ sont irrationnels.