Chapitre 20

Arithmétique

Le père Rouault vint apporter à Charles le paiement de sa jambe remise,
soixante-quinze francs en pièces de quarante sous.
Gustave FLAUBERT, Madame Bovary, 1857.

Pour bien aborder ce chapitre

Un très beau chapitre. Tellement beau que nous allons le traiter deux fois ! En effet, il a beaucoup de points communs avec le suivant. On peut expliquer ces points communs à l'aide de la théorie des idéaux d'un anneau, mais ce n'est pas l'objet ici.
Par ailleurs l'arithmétique a toujours fasciné les hommes, les mathématiciens comme les profanes. Avec un peu de curiosité et d'observation, n'importe qui peut conjecturer des propriétés qui peuvent s'avérer ardues à démontrer. On peut par exemple contempler le tableau des derniers chiffres de i^j pour $0 \leqslant i \leqslant 9$ et $1 \leqslant j \leqslant 5$. Une explication viendra plus tard...

$j \setminus i$	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	1	4	9	6	5	6	9	4	1
3	1	8	7	4	5	6	3	2	9
4	1	6	1	6	5	6	1	6	1
5	1	2	3	4	5	6	7	8	9

Par ailleurs, on peut s'émerveiller devant les nombres premiers, le mystère de leur répartition et la beauté gratuite de leur étude. Gratuite ? Rien n'est moins sûr ! La découverte d'un algorithme rapide de décomposition en facteurs premiers mettrait à mal bien des codes secrets et l'arithmétique est devenu un secteur d'étude stratégique.
Parmi les nombreux mathématiciens qui se sont intéressés à l'arithmétique, le nom de Gauss se détache. Toute sa vie durant il est revenu sur des problèmes d'arithmétique. Mais on peut citer Euclide, Diophante, Fermat, Legendre, Euler et Ramanujan.
L'arithmétique est une école de rigueur. Mais une fois les mécanismes acquis, ce chapitre devient une récréation.

20.1 Relation de divisibilité, division euclidienne

20.1.1 Relation de divisibilité

DÉFINITION 20.1 ♡ **Divisibilité**
Soient deux entiers relatifs $(a,b) \in \mathbb{Z}^2$. On dit que l'entier *a divise* l'entier b si et seulement si $\exists k \in \mathbb{Z}$ tq $b = ka$.

Notation 20.1 On notera $a \mid b$ (se lit « a divise b ») le fait que l'entier a divise l'entier b.

Remarque 20.1
– $\forall n \in \mathbb{N},\ n \mid 0$;
– $\forall n \in \mathbb{N},\ 0 \mid n \implies n = 0$;
– $\forall (a,b,c,d) \in \mathbb{Z}^4,\ [a \mid b \quad \text{et} \quad c \mid d] \implies ac \mid bd$.

PROPOSITION 20.1 **Propriétés de la divisibilité**

– La relation « divise » est réflexive : $\forall a \in \mathbb{Z},\quad a \mid a$.
– La relation « divise » est transitive : $\forall (a,b,c) \in \mathbb{Z}^3,\quad [a \mid b \quad \text{et} \quad b \mid c] \implies a \mid c$.
– La relation « divise » n'est ni symétrique, ni antisymétrique. Donc ce n'est ni une relation d''équivalence, ni une relation d'ordre sur $\mathbb{Z}$). Par contre : $[a \mid b \quad \text{et} \quad b \mid a] \iff a = \pm b$.

Démonstration

1. *Soit $a \in \mathbb{Z}$. Comme $a = 1 \times a$ il est clair que $a|a$.*
2. $$\begin{cases} a|b \\ b|c \end{cases} \implies \begin{cases} \exists k \in \mathbb{Z}, \quad b = ka \\ \exists k' \in \mathbb{Z}, \quad c = kb \end{cases} \implies c = kk'a \implies a|c$$
3. *On a : $[a|b \quad \text{et} \quad b|a] \implies \left[\exists (k,k') \in \mathbb{Z}^2 : \quad b = ka \quad \text{et} \quad a = k'b\right] \implies a = kk'a$. Il vient alors :*
   – *si $a = 0$ alors $b = ka = 0$ et donc $a = b$.*
   – *si $a \neq 0$, $kk' = 1$, comme k et k' sont des entiers, cette égalité n'est possible que si $k = k' = 1$ ou alors si $k = k' = -1$. On a finalement bien $a = \pm b$.*

   Réciproquement si $a = \pm b$, on a nécessairement $[a|b \quad \text{et} \quad b|a]$.

PROPOSITION 20.2
Soit $a, b, c \in \mathbb{Z}$ et $k_1, k_2 \in \mathbb{Z}$. Alors :

$$[a|b \quad \text{et} \quad a|c] \implies a|(k_1 b + k_2 c)$$

Démonstration *En effet :*

$$[a|b \quad \text{et} \quad a|c] \implies \begin{cases} \exists k \in \mathbb{Z}, \quad b = ka \\ \exists k' \in \mathbb{Z}, \quad c = ka \end{cases} \implies k_1 b + k_2 c = k_1 ka + k_2 k' a = \left(k_1 k + k_2 k'\right) a \implies a|(k_1 b + k_2 c)$$

20.1.2 Congruences

DÉFINITION 20.2 **Congruence**

Considérons un entier strictement positif $n \in \mathbb{N}^*$ et deux entiers $(a,b) \in \mathbb{Z}^2$. On dit que l'entier a est *congru* à l'entier b modulo n, et l'on note $a \equiv b\ [n]$ lorsque l'entier n divise l'entier $(b-a)$:

$$a \equiv b\ [n] \iff n/(b-a).$$

PROPOSITION 20.3 **Compatibilité des lois avec les congruences**
Soient quatre entiers $(a,b,c,d) \in \mathbb{Z}^4$ et un entier $n \in \mathbb{N}^*$. On suppose que

1. $a \equiv b\ [n]$;
2. $c \equiv d\ [n]$.

Alors

1. $a + c \equiv b + d\ [n]$;
2. $a \times c \equiv b \times d\ [n]$;
3. $\forall k \in \mathbb{N},\ a^k \equiv b^k\ [n]$.

Pour démontrer que $a \mid b$ il peut être intéressant de démontrer que $b \equiv 0\ [a]$.

Exemple 20.2
On veut démontrer que 641 divise $2^{32} + 1$.
On remarque que $n = 641 = 1 + 640 = 1 + 5 \times 2^7 = 625 + 16 = 5^4 + 2^4$.
On en déduit $5 \times 2^7 \equiv -1\ [n]$. En élevant à la puissance 4, on a $5^4 \times 2^{28} \equiv 1\ [n]$. Comme $5^4 \equiv -2^4\ [n]$, on obtient $-2^4 \times 2^{28} \equiv 1\ [n]$ soit en ajoutant 2^{32} aux deux membres, $0 \equiv 2^{32} + 1\ [n]$, ce qu'il fallait vérifier.
Cet exemple historique est dû à Euler et fournit un contre-exemple à une conjecture de Fermat :

$$\forall n \in \mathbb{N}, 2^{2^n} + 1 \text{ est premier.}$$

Exemple 20.3 Pour un nombre entier n (écrit en base 10) on a $n \equiv a\ [10]$ où a désigne le chiffre des unités de n. Ainsi la dernière ligne du tableau des i^j p. 748 peut se lire $i^5 \equiv i\ [10]$ pour tous entiers i.

Exemple 20.4 On a $10 \equiv 1\ [9]$ et donc $\forall k \in \mathbb{N}, 10^k \equiv 1\ [9]$. En particulier $\sum_{k=0}^{p} a_k 10^k \equiv \sum_{k=0}^{p} a_k\ [9]$. Autrement dit, un nombre entier $n = \sum_{k=0}^{p} a_k 10^k$ (écrit en base 10) est congru modulo 9 à la somme de ses chiffres, et donc aussi à la somme des chiffres de la somme de ses chiffres, etc. C'est le principe de la *preuve par neuf* enseignée autrefois à l'école élémentaire. Elle peut s'énoncer de la façon suivante : « Le produit des restes des deux facteurs modulo 9 est congru au reste du produit modulo 9 ».
L'exemple suivant est dû à Eugène Ionesco (La Leçon 1951).
LE PROFESSEUR
...combien font, par exemple, trois milliards sept cent cinquante-cinq millions neuf cent quatre-vingt-dix-huit mille deux cent cinquante et un, multiplié par cinq milliards cent soixante-deux millions trois cent trois mille cinq cent huit ? L'ÉLÈVE, *très vite*.
Ça fait dix-neuf quintillions trois cent quatre-vingt dix quadrillions deux trillions huit cent quarante quatre milliards deux cent dix-neuf millions cent soixante-quatre mille cinq cent huit...
On prend $a = 3755998251$, $b = 5162303508$. La somme des chiffres de a vaut 54 donc $a \equiv 0\ [9]$. De même la somme des chiffres de b vaut 33 donc $b \equiv 6\ [9]$. Donc le produit ab est congru à 0 modulo 9.
La somme des chiffres du produit $c = 19390002844219164508$ annoncé par l'élève vaut 76 donc $c \equiv 4\ [9]$.
Moralité, le résultat donné par l'élève est faux.

Exemple 20.5 On peut de demander quelle est valeur exacte du produit. Faute d'un logiciel de calcul formel qui donnerait la solution, on travaille avec une calculatrice qui donne quatorze chiffres significatif (en l'occurence il s'agit d'un tableur).
Il donne $3755998251 \times 5162303508 = 19389602947179200000$. Il est clair que les derniers chiffres sont faux. Pour les trouver, on travaille modulo 10^7, ce qui va donner les sept derniers chiffres : Soit $a' = 5998251$ et $b' = 2303508$. On a $a \equiv a'\ [10^7]$ et $b \equiv b'\ [10^7]$. On a donc $ab \equiv a'b'\ [10^7]$. Le tableur donne $a'b' = 13817019164508 \equiv 19164508 \pmod{10^7}$. On peut donc reconstituer $ab = 19389602947179164508$.
Bien entendu, on vérifie avec la preuve par neuf que $ab \equiv 0\ [9]$.

DÉFINITION 20.3 **Système complet de restes modulo m**
Soit m un entier $\geqslant 2$. On appelle système complet de restes modulo m un système d'entiers contenant un et un seul représentant de chaque classe.

Exemples : $[\![0, m-1]\!]$, système de m entiers consécutifs, m entiers non congrus modulo m deux à deux.

PROPOSITION 20.4
Soit $x \longmapsto f(x) = \sum_{i=0}^{n} a_i x^i$ une fonction polynôme où les $a_i \in \mathbb{Z}$.
On suppose que l'on a $f(r)$ non congru à 0 modulo m pour r décrivant un système complet de restes modulo m. On a alors $\forall x \in \mathbb{Z}, f(x)$ non congru à 0 modulo m.

Démonstration *En effet, soit $x \in \mathbb{Z}$, il existe un r appartenant au système complet de restes modulo m, tel que $x \equiv r\ [m]$. Comme par ailleurs, $\sum_{i=0}^{n} a_i x^i \equiv \sum_{i=0}^{n} a_i r^i\ [m]$, le résultat en découle.*

20.1.3 Division euclidienne

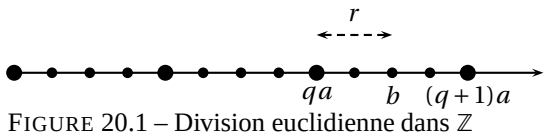


FIGURE 20.1 – Division euclidienne dans $\mathbb{Z}$

THÉORÈME 20.5 ♡♡♡ **Division Euclidienne**
Soient deux entiers $(a, b) \in \mathbb{Z} \times \mathbb{N}$ avec $b \neq 0$. Alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que :

1. $a = bq + r$
2. $0 \leqslant r < b$

On dit que l'entier q est le *quotient* et l'entier r le *reste* de la *division euclidienne* de a par b.

Démonstration

Unicité : *Soient $(q,r)\in\mathbb{Z}^2$ et $(q',r')\in\mathbb{Z}^2$ tels que $a=qb+r$, $0\leqslant r<b$ et $a=q'b+r'$, $0\leqslant r'<b$. Comme $0\leqslant r<b$ et $0\leqslant r'<b$, on a : $b\left|q'-q\right|=\left|r'-r\right|<b$ ce qui n'est possible que si $\left|q'-q\right|=0$, c'est a dire que si $q=q'$. Ceci entraîne $r=r'$ et donc $(q,r)=(q',r')$.*

Existence : *– Supposons que $a\in\mathbb{N}$ et considérons l'ensemble $\mathscr{M}=\{n\in\mathbb{N}\mid nb\leqslant a\}$ des multiples de b inférieurs à a. $\mathscr{M}$ est une partie de $\mathbb{N}$. De plus, $\mathscr{M}$ est :*

– non vide car $0\in\mathscr{M}$.

– majorée par a. En effet, si $n\in\mathscr{M}$ alors, comme $b\geqslant 1$, $n\leqslant nb\leqslant a$ donc $n\leqslant a$.

On en déduit que $\mathscr{M}$ admet un plus grand élément (voir page 304), noté q qui vérifie :

1. *$qb\leqslant a$ car $q\in\mathscr{M}$.*
2. *$(q+1)b>a$ car $q+1>q$ et q est le plus grand élément de $\mathscr{M}$, donc $q+1\notin\mathscr{M}$.*

Posons $r=a-bq$. On a bien $a=bq+r$. Par ailleurs $0\leqslant r$ car $a\geqslant bq$ et $r<b$ car $b=(q+1)b-qb>a-qb=r$.

– Supposons maintenant que $a\in\mathbb{Z}$. Si a est positif, on se ramène au cas précédent. Sinon $-a$ est positif et il existe $(q',r')\in\mathbb{Z}^2$ tel que $:-a=q'b+r'$ et $0\leqslant r'<b$. On a donc $a=b(-q')-r'$. Si $r'=0$ alors on pose $q=-q'$ et $r=0$. On obtient ainsi le couple recherché. Sinon, si $r'\neq 0$, alors $r'\in[\![1,b-1]\!]$ et $a=b(-q'-1)+(b-r')$. On pose alors $q=-q'-1$ et $r=b-r'$ et on obtient, ici encore, le couple recherché.

20.2 PGCD, théorèmes d'Euclide et de Bézout

DÉFINITION 20.4 ♡ **PGCD, PPCM**

Soient deux entiers non tous deux nuls $(a,b)\in\mathbb{Z}^{*2}$.

1. L'ensemble des diviseurs de $\mathbb{N}^*$ communs à a et b admet un plus grand élément noté $a\wedge b$. C'est le *plus grand commun diviseur* (PGCD) des entiers a et b.
2. L'ensemble des entiers de $\mathbb{N}^*$ multiples communs de a et b admet un plus petit élément noté : $a\vee b$. C'est le *plus petit commun multiple* (PPCM) des entiers a et b.

Si $a=b=0$, on pose $a\wedge b=a\vee b=0$.

THÉORÈME 20.6 ♡ **Théorème d'Euclide**

Soient deux entiers $(a,b)\in\mathbb{Z}^{*2}$. Effectuons la division euclidienne de l'entier a par l'entier b :

$$\exists!(q,r)\in\mathbb{N}^2\ :\quad a=bq+r\quad\text{et}\quad 0\leqslant r<b$$

Alors :

$$a\wedge b=b\wedge r$$

Démonstration *Comme $r=a-bq$, tout entier divisant à la fois a et b divise aussi r. L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs communs à b et r. En particulier, ces deux ensembles ont le même plus grand élément, ce qui s'écrit aussi : $a\wedge b=b\wedge r$.*

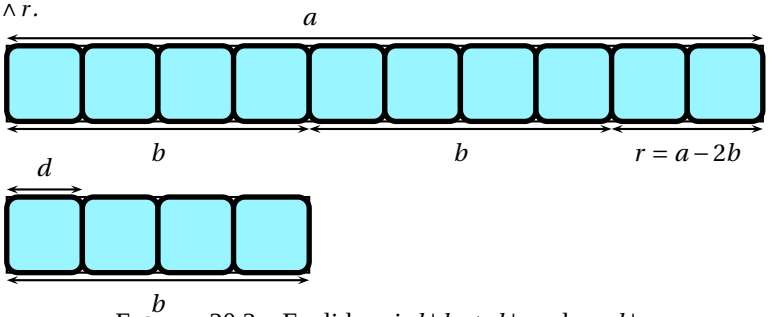


FIGURE 20.2 – Euclide : si $d\mid b$ et $d\mid a$, alors $d\mid r$

Le théorème précédent justifie l'algorithme d'Euclide pour trouver le pgcd de deux entiers non nuls $(a,b)\in\mathbb{N}^{*2}$. On pose $r_0=a$, $r_1=b$ et on définit ensuite $\forall k\geqslant 1$, les couples (q_k,r_k) en utilisant une division euclidienne :

$$\text{si } r_k\neq 0,\ \exists!(q_k,r_{k+1})\in\mathbb{Z}^2 \text{ tq } r_{k-1}=q_kr_k+r_{k+1} \text{ et } 0\leqslant r_{k+1}<r_k$$

Comme la suite d'entiers (r_k) est strictement décroissante, il existe un rang $n\geqslant 1$ tel que $r_n\neq 0$ et $r_{n+1}=0$. D'après le théorème d'Euclide, on a $\forall k\in[0,n-1]$, $a\wedge b=r_k\wedge r_{k+1}$. Comme r_n divise r_{n-1}, on a $r_n\wedge r_{n-1}=r_n$. Par conséquent, le dernier reste non-nul r_n est le pgcd des entiers (a,b).

Exemple 20.6 Déterminons le pgcd des entiers 366 et 43 en utilisant l'algorithme d'Euclide :

$$\begin{aligned} 366 &= 43 \times 8 + 22 \\ 43 &= 22 \times 1 + 21 \\ 22 &= 21 \times 1 + 1 \\ 21 &= 1 \times 21 + 0 \end{aligned}$$

donc $366 \wedge 43 = 1$.

- **Paramètres :** a, b (entiers).
- **Variables locales :** A, B, r.
- **Initialisation :**
  - A $\leftarrow a$,
  - B $\leftarrow b$,
- **Corps :** Tant que $b \neq 0$ faire :
  - $r \leftarrow$ A mod B,
  - A $\leftarrow$ B,
  - B $\leftarrow r$,

  Fin tant que
- Renvoyer A (A = pgcd(a, b)).

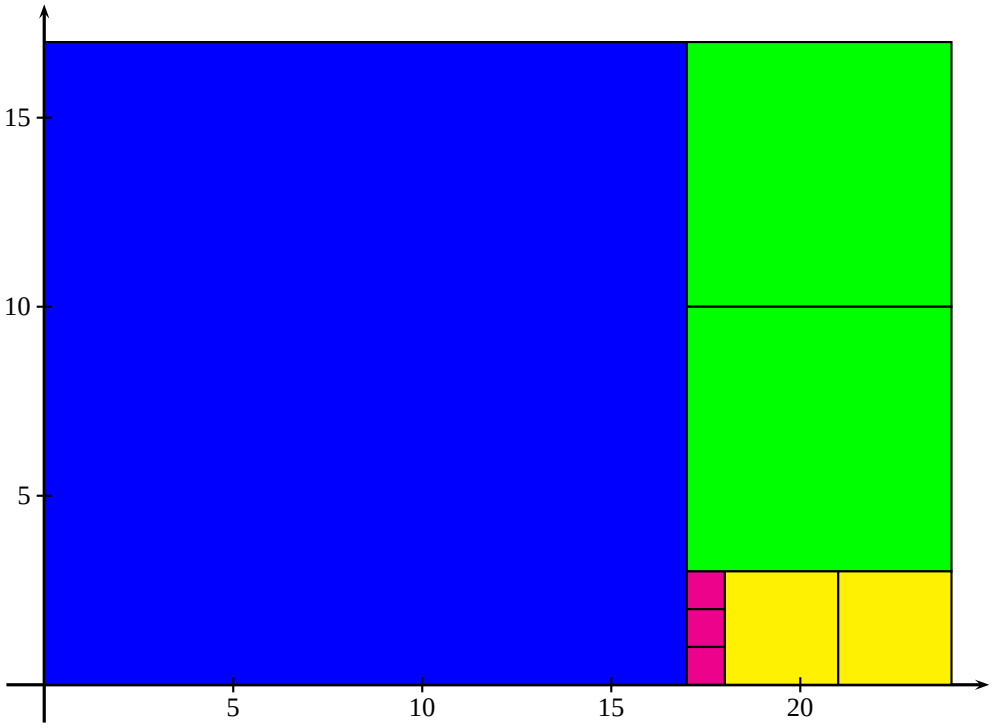
MAPLE

```
pgcd := proc(a, b)
  local A, B, r;
  A := a;
  B := b;
  while (b > 0) do
     r := irem(A, B);
     A := B;
     B := r;
  od;
  A;
end;
```

ou sous une forme récursive :

MAPLE

```
pgcd := proc(a, b)
  if b = 0 then a
  else
    pgcd(b,irem(a,b))
  fi;
end;
```



Le pgcd de 17 et 24 égale 1.

DÉFINITION 20.5 **Nombres premiers entre eux**
On dit que deux nombres a et b sont premiers entre eux si et seulement si leur plus grand diviseur commun est 1, autrement dit si et seulement si $a \wedge b = 1$.

BIO 17 Étienne Bézout, , né le 31 mars 1730 à Nemours, mort le 27 septembre 1783 à Basses-Loges)

Mathématicien français. Auteur de différents livres d'enseignement qu'il rédigea à l'attention des gardes de la marine ou des élèves du corps de l'artillerie. Il est surtout connu pour le théorème ci dessous mais il a travaillé également sur les déterminants et les équations algébriques. Son nom est attaché à d'autres théorèmes en géométrie algébrique et intersections de courbes.

THÉORÈME 20.7 ♡♡♡ **Coefficients de Bézout**
Soient deux entiers non nuls $(a,b) \in \mathbb{Z}^{*2}$. Il existe $(u,v) \in \mathbb{Z}^2$ tels que

$$au + bv = a \wedge b.$$

Un tel couple (u,v) est appelé *couple de coefficients de Bézout de a et b*.

Démonstration *Quitte à considérer $|a|$ et $|b|$ à la place de a et b, on peut supposer a et b positifs. La preuve se fait par récurrence sur b. Si $b = 0$, alors $a \wedge b = a$ et $1.a + 0.b = a$ donc un couple de coefficient de Bézout est $(1,0)$. On fixe $b \in \mathbb{N}^*$ et on suppose que la propriété est vraie pour tout $a \in \mathbb{N}$ et tout nombre n de l'intervalle d'entiers $[\![0, b-1]\!]$. Par division euclidienne, il existe $(q,r) \in \mathbb{N}^2$ tels que $a = bq + r$ et $0 \leqslant r \leqslant b-1$. D'après le théorème d'Euclide, on sait que $a \wedge b = b \wedge r$. On applique l'hypothèse de récurrence à b et r, il existe $(U,V) \in \mathbb{Z}^2$ tels que $Ub + Vr = b \wedge r$. Donc $Ub + V(a - bq) = a \wedge b$ et $Va + (U - Vq)b = a \wedge b$. La propriété est alors prouvée par récurrence.*

Remarque 20.2 Il n'y a pas unicité du couple de coefficients de Bézout de deux entiers. Voir exercice **??** p. **??**.

THÉORÈME 20.8 ♡♡♡ **Théorème de Bézout**
Soient deux entiers non nuls $(a,b) \in (\mathbb{Z}^*)^2$. On a

$$a \wedge b = 1 \iff \left[\exists (u,v) \in \mathbb{Z}^2 \ : \quad 1 = au + bv\right]$$

Démonstration

$\boxed{\Rightarrow}$ *C'est une conséquence directe du théorème précédent.*

$\boxed{\Leftarrow}$ *Supposons qu'il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. Si d est un diviseur commun à a et b alors d est un diviseur de 1. Il est alors clair que $a \wedge b = 1$.*

Remarque 20.3 Soient deux entiers $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ premiers entre eux. L'algorithme d'Euclide permet de trouver un couple de Bézout $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. On définit les suites (r_k) et (q_k) des restes dans l'algorithme d'Euclide. Notons $r_n = a \wedge b = 1$ le dernier reste non-nul. On pose $r_0 = a$, $r_1 = b$ et par récurrence, on définit

$$\forall k \geqslant 1,\ r_{k-1} = q_k r_k + r_{k+1} \text{ avec } 0 < r_{k+1} \leqslant r_k$$

On définit simultanément deux suites (u_k) et (v_k) telles que

$$\forall k \in [0,n],\ r_k = u_k a + v_k b$$

Pour que cette propriété soit vraie pour tout $k \in [\![0,n]\!]$, on doit poser :

$$(u_0,v_0) = (1,0),\ (u_1,v_1) = (0,1) \ \text{ et } \forall k \in [2,n],\ \begin{cases} u_{k+1} = u_{k-1} - q_k u_k \\ v_{k+1} = v_{k-1} - q_k v_k \end{cases}$$

On a alors $1 = au_n + bv_n$.

$r_0 = a$	$r_1 = b$	r_2	$\ldots$	r_k	$\ldots$	1
	q_1	q_2	$\ldots$	q_k	$\ldots$	q_n
1	0	u_2	$\ldots$	u_k	$\ldots$	$u_n = u$
0	1	v_2	$\ldots$	v_k	$\ldots$	$v_n = v$

Voici une procédure Maple qui prend comme paramètres a et b et qui retourne $a \wedge b$, ainsi qu'un couple de Bézout (U,V)

MAPLE

```
bezout := proc(a, b)
  local R, RR, Q, U, UU, V, VV, temp;
  R := a;
  RR := b;
  U := 1;
  UU := 0;
  V := 0;
  VV := 1;
  #Cond entrée :  R = r0, RR = r1, U = u0, V = v0, UU = u1, VV = v1
  while (RR > 0) do
    Q := iquo(R, RR);
    temp := UU;
    UU := U - Q * UU;
    U:=temp;
    temp := VV;
    VV := V - Q * VV;
    V := temp;
    temp := RR;
    RR := irem(R, RR);
    R := temp;
    #INV : R = rk, RR = r_{k+1}, U = uk, UU = u_{k+1}, V = vk, VV = v_{k+1},
    #    Q = qk,  k : nombre de passages dans la boucle while
  od;
    #Cond sortie : RR = u_{n+1}=0, R = r_n = pgcd(a, b), U = u_n, V = v_n
  R, U, V;
end;
```

Exemple 20.7 Déterminons grâce à l'algorithme d'Euclide un couple de Bézout pour $a = 22$ et $b = 17$.

$r_0 = 22$	$r_1 = 17$	$r_2 = 5$	$r_3 = 2$	$r_4 = 1$
	$q_1 = 1$	$q_2 = 3$	$q_3 = 2$	$q_4 = 2$
$u_0 = 1$	$u_1 = 0$	$u_2 = 1$	$u_3 = -3$	$u_4 = 7$
$v_0 = 0$	$v_1 = 1$	$v_2 = -1$	$v_3 = 4$	$v_4 = -9$

et $\boxed{1 = 7 \times 22 - 9 \times 17}$.

BIO 18 Carl Friedrich Gauss, né le 30 avril 1777 à Brunswick (Saint-Empire romain germanique), mort le 23 février 1855 à Göttingen (Royaume de Hanovre)

Mathématicien allemand. C'est un des plus grands mathématiciens de tous les temps. Certains l'ont même surnommé le « prince des mathématiques ». Alors âgé de trois ans, on raconte qu'il sut corriger son père dans un calcul de salaire. Il est remarqué par ses instituteurs qui le poussent à poursuivre ses études. Á dix-neuf ans, il résout un problème qui date d'Euclide, celui de la construction à la règle et au compas du polygône régulier à dix-sept côtés. Cette découverte fut à l'origine de sa décision de consacrer sa vie aux mathématiques. Il effectue sa thèse sous la direction de Johann Pfaff à l'université de Brunswick. Celle-ci porte sur une démonstration du théorème fondamental de l'algèbre 21.24 page 778. Gauss s'intéressa à de nombreuses branches des mathématiques : l'arithmétique, la géométrie, les probabilités, etc. Il a permis des avancées énormes en théorie des nombres, en géométrie non-euclidienne, ...Mais il s'est aussi intéressé, entre autres, à l'astronomie ou à la cartographie à chaque fois avec génie. Même si la portée de ses travaux ne fut pas complètement comprise par ses contemporains - Gauss ne publiant que très peu - ce fut la postérité qui comprit la profondeur et l'étendue de son travail à la lecture de son journal intime qui fut publié après sa mort. Il eut comme élèves Richard Dedekind et Bernhard Riemann.

THÉORÈME 20.9 ♡♡♡ **Théorème de Gauss**
Soient trois entiers non nuls $(a,b,c) \in \mathbb{Z}^{*3}$.

$$[a \mid bc \quad \text{et} \quad a \wedge b = 1] \implies a \mid c$$

Démonstration *Si $a \wedge b = 1$ alors, d'après le théorème de Bézout 20.8, il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. On a donc aussi $auc + bvc = c$. Mais comme a divise bc et que a divise auc, a divise $auc + bvc = c$.*

PROPOSITION 20.10 **Caractérisation des diviseurs et des multiples**
Soient deux entiers $(a,b) \in \mathbb{Z}^2$.

1. Soit un entier $d \in \mathbb{Z}$. $\begin{cases} d \mid a \\ d \mid b \end{cases} \iff d \mid (a \wedge b)$
2. soit un entier $m \in \mathbb{Z}$. $\begin{cases} a \mid m \\ b \mid m \end{cases} \iff (a \vee b) \mid m.$

Démonstration

1. *Supposons que que d divise a et b et notons $\delta = a \wedge b$. D'après le théorème 20.7, il existe $(u,v) \in \mathbb{Z}^2$ tels que $au + bv = \delta$. Comme $d \mid a$ et que $d \mid b$, on sait que $d \mid \delta$. La réciproque est facile.*
2. *Supposons que a et b divisent m et notons $\mu = a \vee b$. Il existe $k, k' \in \mathbb{N}$ tels que $\mu = ka$ et $\mu = k'b$. Il existe aussi $l, l' \in \mathbb{N}$ tels que $m = la$ et $m = l'b$. De plus, par application du théorème 20.5, il existe un unique couple $(q,r) \in \mathbb{N}^2$ tel que $m = p\mu + r$ et $0 \leqslant r < \mu$. On peut alors écrire $la = pka + r$ et $l'b = pk'b + r$ et donc $a \mid r$ et $b \mid r$. Si $r \neq 0$ alors r est un multiple commun à a et b. Par définition de μ, il vient $r \geqslant \mu$ ce qui est impossible. Donc $r = 0$ et μ divise m. La réciproque est évidente.*

PROPOSITION 20.11
Soient deux entiers non nuls $(a,b) \in \mathbb{Z}^{*2}$. Pour un entier $k \in \mathbb{N}^*$, $\begin{cases} (ka) \wedge (kb) = k(a \wedge b) \\ (ka) \vee (kb) = k(a \vee b) \end{cases}$.

Démonstration

- *Posons $\delta = a \wedge b$ et $\Delta = ka \wedge kb$. Il est clair que $k\delta \mid \Delta$. Montrons que $\Delta \mid k\delta$, ce qui prouvera la première égalité. Comme $k \mid \Delta$ il existe $m \in \mathbb{Z}$ tel que $\Delta = km$. Mais alors $km \mid ka$ et $m \mid a$. De même, $km \mid kb$ et donc $m \mid b$. L'entier m est donc un diviseur de δ et $\Delta = km \mid k\delta$.*
- *Posons maintenant $d = a \vee b$ et $\mathrm{D} = ka \vee kb$. L'entier kd est un multiple de ka et kb donc $\mathrm{D} \mid kd$. Si on montre de plus que $kd \mid \mathrm{D}$ alors la seconde égalité sera prouvée. Comme $ka \mid \mathrm{D}$ et que $kb \mid \mathrm{D}$, il existe des entiers m_1 et m_2 tels que $\mathrm{D} = kam_1 = kbm_2$. L'entier k est donc un diviseur de D et il existe un entier D' tel que $\mathrm{D} = k\mathrm{D}'$. Par suite, on a $\mathrm{D}' = am_1 = bm_2$ et D' est donc un multiple commun à a et b ce qui amène $d \mid \mathrm{D}'$ ainsi que $kd \mid \mathrm{D}$.*

PROPOSITION 20.12 ♡ **Autres propriétés du PGCD**
Soient trois entiers non nuls $(a,b,c) \in \mathbb{Z}^{*3}$.

1 Soient trois entiers $(\delta, a', b') \in \mathbb{N}^* \times \mathbb{Z}^2$ tels que $a = \delta a'$, $b = \delta b'$, alors

$$(\delta = a \wedge b) \iff (a' \wedge b' = 1)$$

2 $\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \iff a \wedge (bc) = 1$;

3 $\begin{cases} a \mid c \\ b \mid c \\ a \wedge b = 1 \end{cases} \implies ab \mid c$;

4 pour tout couple $(p,q) \in \mathbb{N}^{*2}$, si $a \wedge b = 1$, alors $a^p \wedge b^q = 1$;

5 pour tout entier $k \in \mathbb{N}^*$, $a^k \wedge b^k = (a \wedge b)^k$.

Démonstration

1 *C'est une conséquence directe de la proposition 20.10.*

2 ⇒ *Si $a \wedge b = 1$ et $a \wedge c = 1$, alors par application du théorème de Bézout 20.8, il existe des entiers s,t,u,v tels que $sa + tb = 1$ et $ua + vc = 1$. Si on multiplie membre à membre ces deux égalités, on obtient l'égalité de Bézout : $(sua + vsc + tub)\,a + (tvc)\,b = 1$ et en conclusion $a \wedge (bc) = 1$.*

⇐ *Réciproquement, si $a \wedge (bc) = 1$ alors il : est clair que a est premier à la fois avec b et c.*

3 *Comme $a \mid c$, il existe $k \in \mathbb{Z}$ tel que $c = ka$. Mais comme $b \mid c = ka$ et que $a \wedge b = 1$ alors par le théorème de Gauss 20.9, il vient que $b \mid k$. En conclusion $ab \mid c$.*

4 *Considérons $\mathrm{A}, \mathrm{B} \in \mathbb{N}^*$ tels que $\mathrm{A} \wedge \mathrm{B} = 1$ et $m \in \mathbb{N}^*$. Si on applique la deuxième règle avec $a = \mathrm{A}$, $b = \mathrm{B}$ et $c = \mathrm{B}$, on obtient : $\mathrm{A} \wedge \mathrm{B}^2 = 1$. En l'appliquant une nouvelle fois avec $a = \mathrm{A}$, $b = \mathrm{B}$ et $c = \mathrm{B}^2$, il vient que $\mathrm{A} \wedge \mathrm{B}^3 = 1$. Si on l'applique encore $m - 3$ fois, il vient que : $\mathrm{A} \wedge \mathrm{B}^m = 1$. En résumé, on a prouvé que si $\mathrm{A} \wedge \mathrm{B} = 1$ alors $\mathrm{A} \wedge \mathrm{B}^m = 1$. Considérons $a, b \in \mathbb{N}^*$ tels que $a \wedge b = 1$ et $p,q \in \mathbb{N}^*$. On applique ce résultat à $\mathrm{A} = a$, $\mathrm{B} = b$ et $m = q$. Il vient $a \wedge b^q = 1$. On l'applique alors une nouvelle fois mais à $\mathrm{A} = b^q$, $\mathrm{B} = a$ et $m = p$ et on trouve : $a^p \wedge b^q = 1$.*

5 *Soit $k \in \mathbb{N}^*$. Posons $\delta = a \wedge b$. Grâce à la première règle, on a : $\frac{a}{\delta} \wedge \frac{b}{\delta} = 1$ et grâce à la quatrième : $\left(\frac{a}{\delta}\right)^k \wedge \left(\frac{b}{\delta}\right)^k = 1$. En appliquant à nouveau la première règle, il vient que : $a^k \wedge b^k = \delta^k = (a \wedge b)^k$.*

THÉORÈME 20.13 ♡ **Relation entre PGCD et PPCM**
Soient deux entiers non nuls $(a, b) \in \mathbb{Z}^{*2}$.

1. Si $a \wedge b = 1$ alors $a \vee b = |ab|$;
2. $(a \wedge b)(a \vee b) = |ab|$.

Démonstration

1. *Supposons que a et b sont positifs et premiers entre eux. Soit d un multiple commun à a et b. Alors il existe $k \in \mathbb{N}$ tels que $d = ka$. Comme $b \mid d$ et que $a \wedge b = 1$, on en déduit, grâce au théorème de Gauss 20.9, que $b \mid k$ et qu'il existe donc $k' \in \mathbb{N}$ tel que $d = k'ab$. Comme d est le plus petit commun multiple de a et b, il vient forcément que $k' = 1$ et que $d = ab$. Si a et b ne sont pas tous deux positifs, on applique ce résultat à $|a|$ et $|b|$.*
2. *Notons $\delta = a \wedge b$ et $a = \delta a'$, $b = \delta b'$ avec $a', b' \in \mathbb{Z}$. Montrons que l'ensemble des multiples communs à a et b est l'ensemble des multiples de $\delta a'b'$. Il est clair que tout multiple de $\delta a'b'$ est un multiple commun à a et b. Réciproquement, si m est un multiple commun à a et b alors il existe $k, k' \in \mathbb{Z}$ tels que $m = ka = k'b$. On a aussi : $m = k\delta a' = k'\delta b'$. Comme a' et b' sont premiers entre eux, cette égalité implique, par application du théorème de Ga uss 20.9 que $b' \mid k$. Donc m est un multiple de $\delta a'b'$. Il s'ensuit que le ppcm de a et b est le plus petit multiple de $\delta a'b'$, c'est à dire que $a \vee b = |\delta a'b'|$. Il vient alors $\delta(a \vee b) = \delta|\delta a'b'| = |ab|$ d'où l'égalité.*

20.3 Nombres premiers

20.3.1 Nombres premiers

DÉFINITION 20.6 ♡ **Nombre premier, nombre composé**
Un entier $n \in \mathbb{N}$ est dit *premier* si $n \geqslant 2$ et si ses seuls diviseurs dans $\mathbb{N}$, sont 1 ou lui-même :

$$\forall k \in \mathbb{N}^*,\ k/n \implies k \in \{1, n\}$$

On note $\mathbb{P}$ l'ensemble des nombres premiers.
Si un entier $n \in \mathbb{N}$ n'est pas premier, on dit qu'il est *composé*.

Remarque 20.4 Un entier positif est premier si et seulement si le cardinal de l'ensemble de ses diviseurs est égal à 2.

PROPOSITION 20.14 ♡ **Propriétés des nombres premiers**

1. Soit un entier $p \in \mathbb{N}$ premier, et $a \in \mathbb{Z}$ un entier. Alors, $p \mid a$ ou bien $p \wedge a = 1$.
2. Si n et m sont deux nombres premiers distincts, ils sont premiers entre eux : $n \neq m \implies n \wedge m = 1$.
3. Si n est un nombre premier et si $(a_1, \ldots, a_k) \in \mathbb{Z}^k$,

$$n \mid a_1 \ldots a_k \implies [\exists i \in [\![1, n]\!] :\quad n \mid a_i]$$

Démonstration

1. *Si n et a ne sont pas premiers entre eux alors $\delta = n \wedge a > 1$. Mais comme $\delta \mid n$ et que n est premier, $\delta = 1$ ce qui n'est pas possible ou $\delta = n$. En conclusion, $n \mid a$.*
2. *n est premier et peut diviser m donc d'après le point précédent $n \wedge m = 1$.*
3. *D'après le théorème de Gauss et une petite récurrence.*

PROPOSITION 20.15 ♡
Tout entier supérieur à 2 admet un diviseur premier.

Démonstration *Effectuons une récurrence forte. Si $p = 2$ alors p possède un diviseur premier : lui même. Supposons la propriété vérifiée pour tout entier $p \in [\![2, n]\!]$ et montrons là pour $p = n+1$. Soit $\mathscr{A}$ l'ensemble des diviseurs de $n+1$. On a $|\mathscr{A}| \geqslant 2$. Si $|\mathscr{A}| = 2$ alors $n+1$ est premier et cela démontre la propriété sinon $\mathscr{A}$ contient un entier $q \in [\![2, n]\!]$ qui divise $n+1$. On applique l'hypothèse de récurrence à q : q possède un diviseur premier. Ce diviseur premier divise nécessairement aussi $n+1$ et donc $n+1$ possède un diviseur premier. La propriété est donc démontrée par récurrence.*

PROPOSITION 20.16 ♡
L'ensemble $\mathbb{P}$ des nombres premiers est infini.

Démonstration *Supposons que ce ne soit pas le cas. $\mathbb{P}$ forme alors une partie finie de $\mathbb{N}$. $\mathbb{P}$ possède donc un plus grand élément n. Considérons le nombre entier $N = n! + 1$. On a : $N > n$. D'après la proposition précédente, N possède un diviseur premier p différent de 1. Ce dernier est nécessairement élément de l'ensemble $[\![2, n]\!]$. p divise donc aussi $n!$. Mais alors p divise 1 ce qui est impossible. L'ensemble $\mathbb{P}$ des nombres premiers est donc infini.*

20.3.2 Décomposition en facteurs premiers

LEMME 20.17
Soit $m \in \mathbb{N}^*$. On considère m nombre premiers $p_1, \dots, p_m \in \mathbb{P}$ distincts deux à deux et des entiers naturels non nuls $\alpha_1, \dots, \alpha_m$. On forme le nombre entier $p_1^{\alpha_1} \dots p_m^{\alpha_m}$. Alors tout diviseur premier de n est l'un des p_i où $i \in [\![1, m]\!]$.

Démonstration *Considérons l'ensemble $\mathscr{A}$ des entiers de la forme $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ avec $m \in \mathbb{N}^*$, $p_1, \dots, p_m \in \mathbb{P}$ distincts deux à deux et $\alpha_1, \dots, \alpha_m \in \mathbb{N}^*$ qui admettent un diviseur premier différent de chacun des p_i. La propriété sera prouvée si on montre que $\mathscr{A}$ est vide. Supposons que ce n'est pas le cas. Alors comme $\mathscr{A}$ est une partie de $\mathbb{N}$, $\mathscr{A}$ admet un plus petit élément $n_0 = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ et d'après la proposition 20.15, n_0 admet un diviseur premier p qui n'est, par définition de $\mathscr{A}$, aucun des p_i. L'entier p divise donc le produit $p_1 . p_1^{\alpha_1 - 1} \dots p_m^{\alpha_m}$. Les entiers p et p_1 sont premiers entre eux car premiers. On en déduit, par application du lemme de Gauss, que $p \mid p_1^{\alpha_1 - 1} \dots p_m^{\alpha_m}$. Mais comme n_0 est le plus petit élément de $\mathscr{A}$, l'entier $p_1^{\alpha_1 - 1} \dots p_m^{\alpha_m}$ n'est pas élément de $\mathscr{A}$ et p est l'un des p_i pour $i \in [\![1, m]\!]$ ce qui rentre en contradiction avec l'hypothèse faite sur p. Le lemme est alors prouvé par l'absurde.*

THÉORÈME 20.18 ♡♡♡ **Décomposition en facteurs premiers**
Soit un entier $n \in \mathbb{N} \setminus \{0, 1\}$. Cet entier n s'écrit de façon unique de la manière suivante :

$$n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$$

où $m \in \mathbb{N}^*$, $p_1 < \dots < p_m$ sont m nombres premiers et où $\alpha_1, \dots, \alpha_m \in \mathbb{N}^*$. Ce résultat se formule aussi sous la forme suivante : n s'écrit de manière unique, à l'ordre des facteurs près, comme

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$$

où $\nu_p(n) \in \mathbb{N}$ est appelé la *p-valuation* de l'entier n.

Démonstration

Existence *La preuve se fait par récurrence sur n. Si $n = 2$ alors comme $2 \in \mathbb{P}$, la proposition est vraie. Soit $n \in \mathbb{N} \setminus \{0, 1\}$. Supposons que tout entier $< n$ se décompose comme indiqué dans le théorème. Si n est premier alors le théorème est vrai pour n. Sinon n admet un diviseur premier $p \in \mathbb{P}$ et il existe $0 < m < n$ tel que $n = pm$. Mais par application de l'hypothèse de récurrence, m se décompose comme indiqué dans le théorème et il en est alors de même de n. L'existence de la décomposition est alors prouvée par récurrence.*

Unicité *La preuve se fait à nouveau par récurrence. Supposons que $2 = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ avec pour tout $i \in [\![1, m]\!]$, $p_i \in \mathbb{P}$, $\alpha_i \in \mathbb{N}^*$ et $p_1 < \dots < p_m$. Comme 2 est le plus petit des nombres premiers, il vient : $2 = p_1^{\alpha_1} \dots p_m^{\alpha_m} \geqslant 2^{\alpha_1} \times \dots \times 2^{\alpha_m}$ ce qui n'est possible que si $m = 1$, $p_1 = 2$, $\alpha_1 = 1$. L'unicité de la décomposition de 2 en facteurs premiers est alors prouvée. Soit $n \in \mathbb{N}$. Supposons que tout entier $< n$ admet une unique décomposition en facteurs premiers et supposons que que ce ne soit pas le cas pour n, c'est à dire que n admet au moins deux décompositions en facteurs premiers : $n = p_1^{\alpha_1} \dots p_m^{\alpha_m} = p_1'^{\alpha'_1} \dots p_{m'}'^{\alpha'_{m'}}$. Par application du lemme précédent, il vient $p_1 = p'_i$ pour un certain $i \in [\![1, m']\!]$ et $p'_1 = p_j$ pour un certain $j \in [\![1, m]\!]$. Mais $p_1 \leqslant p_j = p'_1 \leqslant p'_i = p_1$ et forcément $p_1 = p'_1$. On peut alors écrire :*

$$\frac{n}{p_1} = p_1^{\alpha_1 - 1} \dots p_m^{\alpha_m} = p_1'^{\alpha'_1 - 1} \dots p_{m'}'^{\alpha'_{m'}}$$

L'hypothèse de récurrence nous permet d'affirmer que la décomposition de n/p_1 en facteurs premiers est unique donc : $m = m'$, $p_1 = p'_1$, $p_2 = p'_2$, …, $p_m = p'_m$, $\alpha_1 = \alpha'_1$, …, $\alpha_m = \alpha'_m$. Les deux décompositions de n en facteurs premiers sont donc égales. L'unicité est ainsi prouvée par récurrence.

Remarque 20.5 Tout entier relatif $n \in \mathbb{Z}$ non nul s'écrit de façon unique sous la forme :

$$n = \pm \prod_{p \in \mathbb{P}} p^{\nu_p(|n|)}.$$

Pour des entiers $a, b \in \mathbb{N}^*$, et $p \in \mathbb{P}$,

$$\nu_p(a \times b) = \nu_p(a) + \nu_p(b) \quad a \mid b \implies \nu_p(a) \leqslant \nu_p(b)$$

THÉORÈME 20.19 ♡ **Expression du PGCD et du PPCM à l'aide des facteurs premiers**
Soient deux entiers non-nuls $(a,b) \in \mathbb{N}^{*2}$. Leur décomposition en facteurs premiers s'écrit :

$$a = \prod_{p\in\mathbb{P}} p^{\nu_p(a)} \quad b = \prod_{p\in\mathbb{P}} p^{\nu_p(b)}$$

Alors la décomposition de $a \wedge b$ et de $a \vee b$ en facteurs premiers s'écrit :

$$a \wedge b = \prod_{p\in\mathbb{P}} p^{\min\{\nu_p(a),\nu_p(b)\}} \quad a \vee b = \prod_{p\in\mathbb{P}} p^{\max\{\nu_p(a),\nu_p(b)\}}$$

Démonstration *Posons $\delta = \prod_{p\in\mathbb{P}} p^{\min\{\nu_p(a),\nu_p(b)\}}$ et montrons que $\delta = a \wedge b$. Considérons $a', b' \in \mathbb{N}$ tels que $a = \delta a'$ et $b = \delta b'$. D'après la proposition 20.12, on aura montré que $\delta = a \wedge b$ si et seulement si $a' \wedge b' = 1$. Supposons que ce ne soit pas le cas alors il existe un diviseur $d \neq 1$ commun à a et b qu'on peut supposer premier. On a donc :*

$$d \mid \frac{a}{d} = \prod_{p\in\mathbb{P}} p^{\nu_p(a)-\min\{\nu_p(a),\nu_p(b)\}} \quad \text{et} \quad d \mid \frac{b}{d} = \prod_{p\in\mathbb{P}} p^{\nu_p(b)-\min\{\nu_p(a),\nu_p(b)\}}.$$

Il vient alors que d est un facteur de chacun des deux produits ci dessus et que $\nu_d(a) - \min\{\nu_d(a),\nu_d(b)\} \geqslant 1$ ainsi que $\nu_d(b) - \min\{\nu_d(a),\nu_d(b)\} \geqslant 1$ ce qui constitue une contradiction et prouve par l'absurde que $a' \wedge b' = 1$. La formule pour le pgcd est ainsi démontrée. On procède de même pour le ppcm.

Exemple 20.8

Soit $n \in \mathbb{N}$ non nul, $n = \prod_{p\in\mathbb{P}} p^{\nu_p(|n|)}$. Les diviseurs positifs d de n s'écrivent $d = \prod_{p\in\mathbb{P},p|n} p^{\nu_p(|d|)}$, avec $\forall p \in \mathbb{P}, \nu_p(|d|) \leqslant \nu_p(|n|)$. Pour chaque $p \in \mathbb{P}$ qui divise n, on a $\nu_p(|n|)+1$ choix pour $\nu_p(|d|)$, à savoir $0, 1, \ldots, \nu_p(|n|)$. On obtient ainsi

$$\prod_{p\in\mathbb{P},p|n} (\nu_p(|n|)+1)$$

diviseurs positifs de n. Ces diviseurs de n sont distincts deux à deux à cause du théorème de décomposition en facteurs premiers.