Université Paris 13, Institut Galilée
Département de Mathématiques
Licence 2ème année Informatique
2013-2014

Cours de Mathématiques pour l'Informatique
Des nombres aux structures
Sylviane R. Schwer

Leçon du 21 janvier 2014 : Divisibilité dans $\mathbb{N}$

Contrairement à l'approche de beaucoup d'ouvrages, nous étudions d'abord la divisibilité dans $\mathbb{N}$, puis nous aborderons le problème de l'extension de $\mathbb{N}$ à $\mathbb{Z}$.

1 Définition et premières propriétés

Définition 1.1 *Etant donné deux entiers naturels a et b, on dit que a* divise *b ou que b est un* multiple *de a - et l'on note $a|b$ - s'il existe un entier naturel c - appelé quotient - tel que $b = a \times c$, noté aussi $b = ac$.*
On note $a\mathbb{N}$ l'ensemble des multiples de a dans $\mathbb{N}$ et $D_{\mathbb{N}}(a)$ l'ensemble des diviseurs de a.

Exemples :
$D_{\mathbb{N}}(12) = \{1, 2, 3, 4, 6, 12\}$; $12\mathbb{N} = \{12k, k \in \mathbb{N}\} = \{0, 12, 24, 36, \cdots\}$
$D_{\mathbb{N}}(7) = \{1, 7\}$; $7\mathbb{N} = \{7k, k \in \mathbb{N}\} = \{0, 7, 14, 21, \cdots\}$
$\mathbb{N}$ a deux éléments particuliers pour le produit :
L'élément neutre 1 : c'est un diviseur de tout élément de $\mathbb{N}$, y compris de lui-même.
L'élément absorbant 0 : c'est un multiple de tout élément de $\mathbb{N}$ y compris de lui-même.
C'est pourquoi la division de 0 par 0 est *indéterminée.*

On en déduit que pour tout entier naturel a, $a\mathbb{N}$ et $D_{\mathbb{N}}(a)$ sont des parties non vides de $\mathbb{N}$.

$$0\mathbb{N} = \{0\} \ ; \ 1\mathbb{N} = \mathbb{N} \ ; \ D_{\mathbb{N}}(0) = \mathbb{N} \ ; \ D_{\mathbb{N}}(1) = \{1\}.$$

En revanche,

$$(a \neq 0 \quad \text{et} \quad a|b) \Longrightarrow (\exists! c \in \mathbb{N},\, c \leq b \quad \text{tel que} \quad b = ca)$$

En effet, supposons que $\exists c_1 \in \mathbb{N}$ et $c_2 \in \mathbb{N}$ tels que $b = ac_1 = ac_2$. Comme $a \neq 0$, il est régulier pour le produit, donc $c_1 = c_2$. $\square$

1.1 Etude de la relation | dans $\mathbb{N}$

Les propriétés du produit dans $\mathbb{N}$ font que la relation de divisibilité dans $\mathbb{N}$ est

une relation d'ordre

l'ordre est partiel $\exists n, m \in \mathbb{N}$, tel que ni $n|m$ ni $m|n$, par exemple, 2 et 5 ne sont pas comparables pour la divisiblité dans $\mathbb{N}$.

avec un plus petit élément :1.

avec un plus grand élément : 0.

discret sur $\mathbb{N}^*$.

non discret sur $\mathbb{N}$: 0 n'a pas de plus proche voisin, puisque $\forall a \in \mathbb{N}*, a|2a|0$, l'ordre | n'est pas discret sur $\mathbb{N}$.

1.1.1 |-Intervalles de $\mathbb{N}$

Etant donnés $a, b \in \mathbb{N}, a \leq b$, $[a, b]_| = \{n \in \mathbb{N}, a|n \text{ et } n|b\} = a\mathbb{N} \cap D_{\mathbb{N}}(b)$.

Lemme 1.1 *$\forall n \in \mathbb{N}$, $0, n \in n\mathbb{N}$ et $1, n \in D_{\mathbb{N}}(n)$. De plus, pour la relation de divisibilité,*

1. *n est le plus petit élément de $n\mathbb{N}$*
2. *0 est le plus grand élément de $n\mathbb{N}$*
3. *1 est le plus petit élément de $D_{\mathbb{N}}(n)$*
4. *n est le plus grand élément de $D_{\mathbb{N}}(n)$*
5. *Si $n \geq 2$, $D_{\mathbb{N}}(n)$ possède au moins deux éléments*
6. *Si $n \geq 1$, $n\mathbb{N}$ possède une infinité d'éléments*

•$D_{\mathbb{N}}(n) = \{k \in \mathbb{N}, 1|k|n\}$. $D_{\mathbb{N}}(n)$ est donc le |-intervalle $[1, n]$ mais ce n'est pas un $\leq$-intervalle pour $n > 2$.
• De même, si $a \in \mathbb{N}_*$, $a\mathbb{N}$ est un ensemble infini, c'est le |-intervalle $[n, 0]$ mais ce n'est pas un $\leq$-intervalle.

Définition 1.2 (Nombres Premiers) *Soit $n \in \mathbb{N}$ n est dit premier si $\#D_{\mathbb{N}}(n) = 2$. On note $\mathbb{P}$ l'ensemble des nombres premiers.*

Cette définition exclut 1 des nombres premiers. $2, 3, 5, 7, 11$ sont des nombres premiers.

1.1.2 Diagramme de Hasse de $< D_{\mathbb{N}}(n), | >$, pour $n \in \mathbb{N}_*$.

$D_{\mathbb{N}}(n)$ étant fini, on peut le représenter par un graphe qui exprime la relation de *divisibilité directe*, c'est-à-dire sans représenter[1]les flèches de transitivité et de réflexivité. C'est son diagramme de Hasse.

[1]Une propriété qui est commune à tous les éléments d'un ensemble, n'a pas à être représentée dans l'ensemble, mais sur l'ensemble.

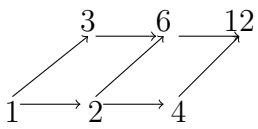

Figure 1: Diagramme de Hasse de $D_{\mathbb{N}}(12)$

1.2 Etude de | vis à vis des opérations de $\mathbb{N}$

Stabilité de la division par linéarité : Soit a, b, c trois entiers naturels,

$$(a|b \quad \text{et} \quad a|c) \Rightarrow (\forall \lambda, \mu \in \mathbb{N}, \quad a|\lambda.b + \mu.c)$$

$$(a|b \quad \text{et} \quad a|c) \text{ et si } \lambda.b \geq \mu.c \text{ alors } a|\lambda.b - \mu.c)$$

Attention, si $a|c$ et $b|c$, alors il est faut d'affirmer que $\lambda.a + \mu.b|c$ comme on pourra s'en convaincre avec $2|6$ et $3|6$ mais $2 + 3$ ne divise pas 6 !

Stabilité de la division par produit : Soit a, b, c, d quatre entiers naturels,

$$(a|b \quad \text{et} \quad c|d) \Rightarrow (a.c|b.d)$$

Régularité de tout entier naturel non nul pour la division : Soit a, b, u trois entiers naturels,

$$(au|bu) \Leftrightarrow (u = 0) \quad \text{ou} \quad (a|b)$$

2 Division entière dans $\mathbb{N}$

Nous allons définir une opération de division définie pour tous les entiers naturels non nuls.

Théorème 2.1 (division euclidienne) *Soit $a \in \mathbb{N}$ et $b \in N_*$, il existe un couple unique $q_{a,b} \in \mathbb{N}$ et $r_{a,b} \in \mathbb{N}$ qui satisfont*

$$a = b.q_{a,b} + r_{a,b} \quad \textbf{\textit{et}} \quad 0 \leq r_{a,b} < b$$

Attention : il peut exister plusieurs écritures de a sous la forme $bq + r$ si l'on supprime la contrainte $0 \leq r_{a,b} < b$. Par exemple $20 = 3 \times 6 + 2 = 3 \times 5 + 5 = 3 \times 4 + 8 = 3 \times 3 + 11 = 3 \times 2 + 14 = 3 \times 1 + 17 = 3 \times 0 + 20$.

Preuve : Soit $0 \leq a < b$, alors $a = b \times 0 + a$ est la seule décomposition possible dans $\mathbb{N}$ de la forme $b \times u = r$.

Soit $0 < b \leq a$.

• Existence du couple $q_{a,b} \in \mathbb{N}$.

Considérons alors l'ensemble $A = \{n \in b\mathbb{N}_* \text{ tels que } n > a\}$, ensemble des multiples de b

strictement supérieurs à a. Cet ensemble est non vide, car $2ba \in A$. Il possède donc un plus petit élément strictement positif que nous écrivons $b(q+1)$.
$0 < b \leq a < b(q+1)$ donc $q \geq 1$. Posons $r_q = a - bq$. $r_q \in \mathbb{N}$. Donc (q, r_q) convient.
• Unicité du couple.
Supposons qu'il existe (q, r) et (q', r') deux candidats possibles avec $r < r'$.
$(*) a = bq + r = bq' + r'$ avec $(**) 0 \leq r < b$ et $0 \leq r' < b$.
De $(*)$ on déduit $b(q - q') = r' - r$ c'est-à-dire que $(r' - r) \in b\mathbb{N}$ et de $(**)$ on déduit que $0 < r' - r < b - r \leq b$, soit $0 < r' - r < b$. Or le seul multiple de b strictement inférieur à b est 0, donc $r = r'$ et $q = q'$.□
Remarque : a est multiple de b ou b divise a si et seulement si $r_{a,b} = 0$

Application : Montrons que si n est un carré, alors le reste de la division par 4 de n est 0 ou 1.
Soit $n = a^2$. $\forall a \in \mathbb{N}, \exists! q \in \mathbb{N}, \exists! r_{a,4}, 0 \leq r_{a,4} < 4, a = 4q_{a,4} + r_{a,4}$. $a^2 = 4[4q_{a,4} + 2q_{a,4}r_{a,4}] + r_{a,4}^2$. Or Remarques

Table 1: Les carrés de $r \in [0, 4[_{\mathbb{N}}$

r	0	1	2	3
r^2	$4 \times 0 + 0$	$4 \times 0 + 1$	$4 \times 1 + 0$	$4 \times 2 + 1$

• On en déduit par contraposée que si le reste de la division par 4 d'un entier n est 2 ou 3, alors n n'est pas un carré de $\mathbb{N}$.
• On aurait pu être plus rapide en posant $a = 2q + r, r = 0$ ou $r = 1$, mais la preuve ne peut pas être généralisée (cf. TD).

Définition 2.1 *Soient $a \in \mathbb{N}$ et $b \in N_*$. Soit le couple unique $q_{a,b} \in \mathbb{N}$ et $r_{a,b} \in \mathbb{N}$ qui satisfont*

$$a = b.q_{a,b} + r_{a,b} \quad \textbf{\textit{et}} \quad 0 \leq r_{a,b} < b$$

$q_{a,b}$ est appelé division entière de a par b *et est noté $DIV(a, b)$. C'est une opération de $\mathbb{N} \times \mathbb{N}_* \to \mathbb{N}$.*
$r_{a,b}$ est appelé le résidu de a modulo b.

2.1 Décomposition en base b d'un nombre naturel

Une application importante de la division euclidienne est l'écriture unique de tout nombre dans une base b.

Théorème 2.2 *Soit b un entier naturel strictement supérieur à 1. Tout $n \in \mathbb{N}_*$ s'écrit de façon unique sous la forme d'un polynôme non nul en b à coefficients dans $[[b-1]]$.*

$$\forall n \in \mathbb{N}_*, \exists! u \in \mathbb{N}, \exists! (n_0, n_1, \cdots, n_u), \forall i \in [0, u], 0 \leq n_i < b, n_u \neq 0, n = \sum_{i=0}^{u} n_i b^i$$

.

Ainsi en base $b = 10$, on a : $2014 = 2 \times 10^3 + 0 \times 10^2 + 1 \times 10^1 + 3 \times 10^0$ ou $2 \times 10^3 + 10^1 + 4 \times 10^0$ que l'on écrit $\underline{2014}_{10}$ si l'on veut préciser la base.
En base $b = 8$, on a $2014 = 3 \times 8^3 + 7 \times 8^2 + 3 \times 8 + 6$ soit $\underline{3736}_8$.

Preuve

Existence de u. Soit $A = \{k \in \mathbb{N}, b^k > n\}$. A est non vide car $n \in A$ puisque $b \geq 2$, $b^n > n$ (cf TD 1). Donc A possède un plus petit élément strictement positif, que nouss notons $u + 1$ tel que

$$(*) \quad b^u \leq n < b^{u+1}$$

Calcul des coefficients. Par récurrence (ou induction) finie.
Si $n < b$ alors $u = 0$, $n_0 = n$, et $n = n_0$ donne la décomposition.
Sinon, d'après le théorème 2.1, il existe un couple unique d'entiers naturels (q_1, n_0) tel que $n = q_1 b + n_0$ avec $0 \leq n_0 < b$. Si $q_1 < b$ c'est terminé, $u = 1$, $n_1 = q_1$ et $n = n_1 b + n_0$, noté $\underline{n_1 n_0}_b$.
Sinon, on construit, toujours en utilisant le théorème 2.1, deux suites d'entiers naturels $q_0 = n, q_1, \cdots, q_p$ et $n_0, n_1, \cdots, n_p$ tels que :
$\forall i \in \mathbb{N}, 0 \leq i < p, q_i = bq_{i+1} + n_i$, avec $0 \leq n_i < b$, et $0 < n_p < b$.
La suite (q_i) est strictement décroissante, donc finie.
La suite des (n_i) est composée d'éléments strictement inférieurs à b.
En substituant dans $n = q_0$ répétitivement les q_i par leur valeur $q_i = bq_{i+1}$, on obtient : $n = b^p n_p + b^{p-1} n_{p-1} + \cdots + bn_1 + n_0$.

unicité de la décomposition. Montrons que $p = u$. Raisonnons par l'absurde.
Si $p < u$, alors $n = \sum_{i=0}^{p} b^i n_i \leq (b-1) \sum_{i=0}^{p} b^i = (b-1)\dfrac{b^{p+1} - 1}{b-1} < b^{p+1} \leq b^u \leq n$.
Si $p > u$ alors $n = b^p n_p + \sum_{i=0}^{p-1} b^i n_i \geq b^p n_p \geq b^p > b^{u+1} > n$.
Donc $p = u$.
S'il existait deux décompositions, $n = \sum_{i=0}^{u} b^i n_i$ et $n = \sum_{i=0}^{u} b^i n'_i$, $n_0 - n'_0$ ou $n'_0 - n_0$ serait un entier naturel divisible par b et strictement inférieur à b, donc nul, soit $n_0 = n'_0$ et $\sum_{i=1}^{u} b^{i-1} n_i = \sum_{i=1}^{u} b^{i-1} n'_i$. Par induction descendante on obtient $n_i = n'_i$, $\forall i \in [[u]]$. □

Exemple : Ecrire 532 dans la base 5. Posons $a_0 = q_0 = n$

Table 2: calcul de la représentation de 532 en base 5

	$a_i = q_i$	q_{i+1}	n_i	l_i	n=532
i=0	532	106	2	2	532=5x$\underline{106}$+2
i=1	106	21	1	1,2	532=5[5x$\underline{21}$ + 1] +2
i=2	21	4	1	1,1,2	532=5[5(5x$\underline{4}$+1) + 1] +2
					n= $\underline{4112}_5$

D'où l'algorithme de calcul :

```
données : n : IN, b:IN, b>1
variables : A (tampon),  N, Q : IN; L: liste
initialisation : A:= n; Q:=DIV(n,b) ;  N:=n-bDIV(n,b) ;  L:=N
SI $n<b$ ALORS AFFICHER : "la représentation de" n " en base" b "est" L
SINON
TANT QUE Q supérieur ou égal à b FAIRE
A:=Q ; Q:= DIV(Q,b) ; N:=  A- bQ ; L:= N,L
FIN FAIRE
L:=Q,L
AFFICHER : "la représentation de" n " en base" b "est" L
FIN SI
```

La décroissance de la suite des entiers naturels q_i assure la terminaison de l'algorithme.

3 Plus Grand Commun Diviseur, Plus Petit Commun Multiple

Théorème 3.1 *Soient a et b deux entiers naturels dont l'un au moins est non nul.*

PGCD *L'ensemble des diviseurs communs à a et b, qui est $D_{\mathbb{N}}(a,b) = D_{\mathbb{N}}(a) \cap D_{\mathbb{N}}(b)$, possède un $\leq$ plus grand élément, appelé le Plus Grand Commun Diviseur de a et b. On le note $PGCD(a,b)$ ou $a \wedge b$.*

PPCM *L'ensemble des multiples communs à a et b, qui est $= a\mathbb{N} \cup b\mathbb{N}$ possède un plus grand élément, appelé le Plus Petit Commun Multiple de a et b. On le note $PPCM(a,b)$ ou $a \vee b$.*

Exemple : $12 \wedge 8 = 4$, $12 \vee 8 = 24$.

Preuve

• L'intersection des ensembles de diviseurs n'est pas vide car elle contient 0. Puisque l'un des entiers est non nul, son ensemble de diviseurs est fini, donc l'intersection des ensembles de diviseurs est une partie non vide et finie de $< \mathbb{N}, \leq >$, elle admet un plus grand élément.

• L'intersection des ensembles de multiples n'est pas vide car elle contient $a \times b$, donc elle possède un plus petit élément $\square$

Table 3: propriétés comparées des opérations $\wedge$ et $\vee$ sur $\mathbb{N}_*$

	$\wedge$	$\vee$
loi interne	Oui	Oui
commutative	Oui	Oui
associative	Oui	Oui
élément neutre	Non	1
élément absorbant	1	Non
idempotence	$\forall n \in \mathbb{N}_*, a \wedge a = a$	$\forall n \in \mathbb{N}_*, a \vee a = a$
distributivité de $\times$	$n(a \wedge b) = na \wedge nb$	$n(a \vee b) = na \vee nb$
divisiblité	$b\|a \Leftrightarrow D_{\mathbb{N}}(b) \subseteq D_{\mathbb{N}}(a) \Leftrightarrow b \wedge a = b$	$b\|a \Leftrightarrow a\mathbb{N} \subseteq b\mathbb{N} \Leftrightarrow b \vee a = a$
	$(a \wedge b)\|a$ et $(a \wedge b)\|b$	$a\|(a \vee b)$ et $b\|(a \vee b)$
	$\forall c \in \mathbb{N}$, si $c\|a$ et $c\|b$ alors $c\|a \wedge b$	$\forall c \in \mathbb{N}$, si $a\|c$ et $b\|c$ alors $a \vee b\|c$ et soit $c = 0$ soit $a \vee b \leq c$

4 Algorithme d'Euclide

Trois cent ans avant l'ère commune, dEuclide à proposé, pour calculer $a \wedge b$ sur $\mathbb{N}_*$ une méthode qui repose sur le

Lemme 4.1 *Si $0 < b \leq a$, alors $a \wedge b = (a - b) \wedge b = r_{a,b} \wedge b$*

preuve : d'après la stabilité de | par combinaison linéaire, la première égalité est triviale et tout diviseur de a et b divise $r_{a,b} = a - bq_{a,b}$ et b.

Cela permet par division euclidienne successive de construire une suite strictement décroissante sur $\mathbb{N}$, $r_0 = b > r_1 > r_2 \cdots \geq 0$ de longueur au plus b telle que : $a = r_0q_1 + r_1$, si $r_1 \neq 0$, $r_0 = r_1q_2 + r_2$, si $r_2 \neq 0$, en continuant le schéma $r_{i-2} = q_ir_{i-1} + r_i$ avec n plus petit indice tel que $r_n = 0$, la dernière division euclidienne est $r_{n-2} = q_nr_{n-1} + r_n$. On a

$$a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \cdots r_{n-2} \wedge r_{n-1} = r_{n-1} \wedge 0 = r_{n-1}$$

Table 4: Calcul de $1492 \wedge 1066$ par la méthode d'Euclide

	a	q	b	r
i=0	1492	1	1066	426
i=1	1066	2	426	214
i=2	426	1	214	212
i=3	214	1	212	2
i=4	212	106	2	0

Un humain s'arrête dès qu'il aperçoit la réponse, et au pire sur l'avant-dernière ligne. Un programme qui implémente l'algorithme ne s'arrêtera qu'à $r = 0$.

```
données : a et b deux entiers naturels non suls
résultat : PGCD(a, b)
variable A, B, Q, R
traitement
A:= sup(a,b)
B:=inf(a,b)
Q:= DIV(a,b)
R:=A-BQ
TANT QUE R strictement supérieur à 0 FAIRE
A:=B (remplacer le contenu de A par le contenu de B)
B:=R (remplacer le contenu de B par le contenu de R)
Q:=DIV(A,B)
R:= A-QB (sch\'ema de la division euclidienne)
FIN TANT QUE
AFFICHER B
```

Preuve de l'algorithme : la terminaison donnée par la stricte décroissance des valeurs reçues par R à chaque passage dans la boucle. L'invariance de boucle est donnée par le lemme 3.1.

Proposition 4.1 *Soit* $a, b \in \mathbb{N}_*$, $a \vee b | c \iff a|c \quad et \quad b|c$.

Preuve : $\Longrightarrow$: Par (2) et la transitivité de $|$
$\Longleftarrow$ La division euclidienne de c par $a \vee b$ nous fournit un unique couple (q, r) tel que $c = (a \vee b)q + r$ avec $0 \leq r < a \vee b$. Montrons que $r = 0$. Mais $a|a \vee b$ et $a|c$ donc $a|r$. de même $b|r$. Donc d'après (3) $r = 0$ $\square$

5 Nombres premiers entre eux

Définition 5.1 *Soit* $a, b \in \mathbb{N}$ n. a *et* b *sont* premiers entre eux *si leur seul diviseur commun est* 1, *c'est-à-dire ssi* $D_{\mathbb{N}}(a) \cap D_{\mathbb{N}}(b) = \{1\}$. *Autrement dit,* a *et* b *sont premiers entre eux* $\Leftrightarrow b \wedge a = 1$

$\dfrac{a}{a \wedge b}$ et $\dfrac{b}{a \wedge b}$ sont premiers entre eux.

Remarque $a, b \in \mathbb{P} \Rightarrow a \wedge b = 1$.
La réciproque est fausse : $5 \wedge 14 = 1$ et $14 \notin \mathbb{P}$.

Théorème 5.1 (de Gauss) [2] *Soit* $a, b, c \in \mathbb{N}_*$,

$$[(a|bc) \quad et \quad (a \wedge b = 1)] \Rightarrow (a|c)$$

[2]Enoncé dans les *Disquisitiones Arithmeticae* paru en 1801. Jean Prestet (1689) l'énonce déjà en ces termes.

Preuve. $a = b\,q_1 + b_1$ avec $0 \leq b_1 < b$, d'où $a\,c = b\,c\,q_1 + b_1\,c$. Comme $a|bc \wedge ac$, $a \mid b_1\,c$.

Par divisions euclidiennes successives, on construit une suite (q_i) et une suite strictement décroissante (b_i), tels que $b_0 = b$, $b_{i-2} = b_{i-1}\,q_2 + b_i$ et $b_{i-2}\,c = b_{i-1}\,c\,q_i + b_i\,c$ avec $a|b_i\,c$.

Comme a et b sont premiers entre eux, le dernier b_i non nul vaut 1 – pour $i = n$ – soit $b_{n-2} = b_{n-1}\,q_n + 1$ et $b_{n-2}\,c = b_{n-1}\,c\,q_n + c$. Et comme $a|b_{n-2}\,c$ et $a|b_{n-1}\,c$, on en déduit que $a \mid c$.□ On montrera que dans $\mathbb{Z}$ on peut faire une preuve plus élégante. Mais nous pouvons dès à présent montrer le théorème fondamental de l'arithmétique.

6 Nombres premiers et théorème fondamental de l'arithmétique

Rappelons que $n \in \mathbb{N}$ n est dit premier si et seulement si $\#D_{\mathbb{N}}(n) = 2$. $\mathbb{P}$ est l'ensemble des nombres premiers.

Attention : ne pas confondre *nombre premier* qui est une propriété d'être d'un nombre et *nombres premiers entre eux*, qui est une relation externe entre deux nombres. 8 et 15 sont premiers entre eux, mais aucun des deux n'est premier.

Théorème 6.1 (test de primalité) *Tout entier $n > 1$ admet un diviseur premier. Si n n'est pas premier, il admet un diviseur premier inférieur à $\sqrt{n}$.*

Preuve : si n est premier, c'est lui-même. Si n n'est pas premier, alors il possède un diviseur k tel que $1 < k < n$. Soit A l'ensemble des diviseurs de n autres que 1 et n. A est non vide donc admet un plus petit élément, que nous notons p. Si p n'était pas premier, il aurait lui-même un diviseur p' tel que $1 < p' < p < n$ qui serait (transitivité) dans A et contredirait le fait que p est le plus petit élément de A.
Donc $n = qp$ avec $p \in \mathbb{P}$ et $q \in A$ donc $p \leq q$, et $p^2 \leq pq = n$.□

Exemple : si $n = 97$, il suffit de tester la divisibilité pour les nombres premiers inférieurs à 9.

Théorème 6.2 *$\mathbb{P}$ est un ensemble infini.*

Preuve : Supposons que l'ensemble $\mathbb{P}$ est fini. $\mathbb{P} = \{p_1, \ldots p_n\}$. Soit $N = (\prod_{i=1}^{n} p_i) + 1$. Montrons qu'aucun élément de $\mathbb{P}$ ne divise N, c'est-à-dire que N est lui-même un nombre premier. Raisonnons par l'absurde. L'un au moins des p_i divise N. Par commutativité, on peut toujours supposer, par réindexation, que p_1 divise N. Or p_1 divise aussi $\prod_{i=1}^{n} p_i$ donc il divise $N - \prod_{i=1}^{n} p_i$ c'est-à-dire qu'il divise 1, ce qui est absurde. donc $\mathbb{P}$ est une partie infinie de $\mathbb{N}$ □

Théorème 6.3 (décomposition en facteurs premiers) *Tout nombre naturel $n > 1$ se décompose de façon unique, à une permutation près, en un produit fini de puissance finie de facteurs premiers.*

$$n = \prod_{p \in \mathbb{P}} p^{n_p} \text{ avec les } n_p \text{tous nuls sauf un nombre fini d'entre eux.}$$

Preuve.

Existence d'une décomposition. Soit $p_1 \in \mathbb{P}, p|n$, $n = n_1 p_1$ et $n_1 < n$. Par régression, on construit une suite descendante finie de facteurs (n_k) qui possède un plus petit élément, minoré par 1 atteint à un ordre u. on obtient une suite de facteurs premiers $p_1, \cdots p_u$. En regroupant les facteurs premiers égaux, on obtient le résultat.

Unicité à une permutation près. application directe de la régularité des nombres premiers pour le produit et du théorème de Gauss (Théorème 5.1.) □

Corollaire 6.1 *Soit m et n tels que $\prod_{p\in\mathbb{P}} p^{n_p}$ et $m = \prod_{p\in\mathbb{P}} p^{m_p}$*

caractérisation de la divisibilité

$$m|n \Longleftrightarrow \forall p \in \mathbb{P}, m_p \leq n_p$$

calcul du PGCD

$$m \wedge n = \prod_{p\in\mathbb{P}} p^{inf(n_p,m_p)}$$

calcul du PPCM

$$m \vee n = \prod_{p\in\mathbb{P}} p^{sup(n_p,m_p)}$$

cardinal de $D_{\mathbb{N}}(n)$

$$\#D_{\mathbb{N}}(n) = \prod_{p\in\mathbb{P}, n_p\neq 0} (n_p + 1)$$

calcul de $D_{\mathbb{N}}(n)$

$$D_{\mathbb{N}}(n) = \prod_{p\in\mathbb{P}, n_p\neq 0} \{1, p, \cdots, p^{n_p}\}$$

Son diagramme de Hasse est une grille de $\mathbb{N}^u$, où u est le nombre de facteurs premiers de n.

Exemple n= 120, m= 70. $m = 2^3\times3\times5 = 2^3\times3^1\times5^1\times7^0$, $n = 2\times5\times7 = 2^1\times3^0\times5^1\times7^1$

caractérisation de la divisibilité : m ne divise pas n.

calcul du PGCD : $m \wedge n = 2 \times 5$

calcul du PPCM : $m \vee n = 2^3 \times 3^1 \times 5^1 \times 7^1$,

cardinal de $D_{\mathbb{N}}(n)$: $\#D_{\mathbb{N}}(n) = 4 \times 2 \times 2 = 1$

calcul de $D_{\mathbb{N}}(n)$: $D_{\mathbb{N}}(n) = \{1, 2, 4, 8\}\{1, 3\}\{1, 5\} = \{1, 2, 4, 8, 3, 6, 12, 24, 5, 10, 20, 40, 15, 30, 60, 120\}$

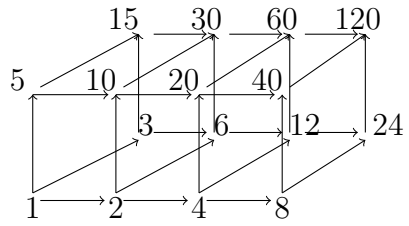

Figure 2: Diagramme de Hasse de $D_{\mathbb{N}}(120)$

Théorème 6.4 *Soit* $a, b \in \mathbb{N}_*$, $(a \vee b)(a \wedge b) = ab$

Preuve :

• si a et b sont premiers entre eux, montrons que $a \vee b = ab$.

Sinon, $\exists k \in \mathbb{N}, k > 1, ab = k(a \vee b)$. D'après le théorème de Gauss, k divise soit a soit b. Disons que k divise a, alors $a = a_1 k$, $a_1 < a$ et $ab = ka_1 b = k(a \vee b) \iff a_1 b = (a \vee b)$. Ce qui implique que $a|a_1 b$. Or $a \wedge b = 1$ donc $a_1 \wedge b = 1$ et d'après le lemme de Gauss, $a|a_1$ d'où $k = 1$, en contradiction avec l'hypothèse de départ.

• Or $a = (a \wedge b)\dfrac{a}{a \wedge b}$ et $b = (a \wedge b)\dfrac{b}{a \wedge b}$.

$\dfrac{a}{a \wedge b}$ et $\dfrac{b}{a \wedge b}$ sont premiers entre eux, donc d'après ce qui précède, et les propriétés de $\wedge$:

$(a \vee b)(a \wedge b) = [(a \wedge b)\dfrac{a}{a \wedge b} \vee (a \wedge b)\dfrac{b}{a \wedge b})][(a \wedge b)\dfrac{a}{a \wedge b} \wedge (a \wedge b)\dfrac{b}{a \wedge b})]$

$=[(a \wedge b)(\dfrac{a}{a \wedge b}.\dfrac{b}{a \wedge b})][(a \wedge b)1] = ab$ □

Exemple : Calculons $2048 \vee 1066$. Comme $1492 \wedge 1066 = 2$ $(2048 = 2^{11})$,

$2048 \vee 1066 = \dfrac{2048\ 1066}{2} = 1\ 091\ 584.$