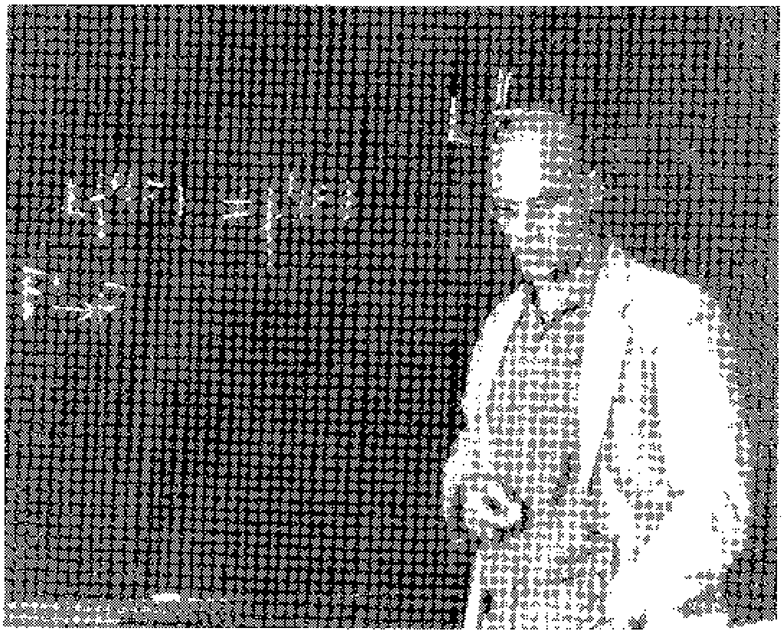
Chapitre 24

Arithmétique



Alexandre Grothendieck (1928 - 2014)

L'arithmétique, c'est l'étude du nombre (et, en premier lieu, c'est l'étude des nombres entiers, des ensembles $\mathbb{N}$ et $\mathbb{Z}$). Gauss disait de l'arithmétique que c'est la « reine des mathématiques ». Les nombreuses questions soulevées par cette discipline (par exemple, la preuve du théorème de Fermat, qui a tenu en échec les mathématiciens pendant plus de 350 ans) sont à l'origine de très nombreuses théories mathématiques.

Grothendieck

Alexandre Grothendieck est un mathématicien français du vingtième siècle dont l'œuvre, immense par la taille et la profondeur, a révolutionné les mathématiques. Il s'est intéressé à de nombreux domaines, dont l'arithmétique. Ses travaux ont permis de réaliser une unification de la géométrie et de l'arithmétique dans une théorie qu'on appelle désormais « géométrie arithmétique ».

Sommaire

I. Inversibles dans $\mathbb{Z}$

Définition 24.1
Soit $a \in \mathbb{Z}$. On dit que a est inversible (dans $\mathbb{Z}$) $\overset{\Delta}{\text{ssi}}$

1-

$$\exists b \in \mathbb{Z} : ab = 1.$$

Proposition 24.2
Les inversibles de $\mathbb{Z}$ sont -1 et 1.

Démonstration. — Soient $a, b \in \mathbb{Z}$ tq $a \cdot b = 1$
En passant à $|\cdot|$, on a $|a| \cdot |b| = 1$ donc $a, b \neq 0$ donc $|a| \geqslant 1, |b| \geqslant 1$
donc $|a| = \frac{1}{|b|} \leqslant \frac{1}{1} \leqslant 1$ donc $|a| = 1$, de m̂ $|b| = 1$

ie $a = \pm 1$ $b = \pm 1$ ■

Exercice 24.3
Montrer que

$$\forall k, k' \in \mathbb{Z},\ kk' = 1 \implies k = k'.$$

II. Division euclidienne

Théorème 24.4
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors,

2-

$$\exists!(q, r) \in \mathbb{Z} \times \mathbb{N} : \begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}.$$

- *L'entier q est appelé* quotient de la division euclidienne de a par b.
- *L'entier r est appelé* reste de la division euclidienne de a par b.

Remarques

- L'entier a est appelé *dividende de la division euclidienne de a par b.*
- L'entier $b \neq 0$ est appelé *diviseur de la division euclidienne de a par b.*

Exemple

- La division euclidienne de 1729 par 42.

3-

$$\begin{array}{r|l} 1729 & 42 \\ \hline 168 & 41 \\ 49 & \\ 42 & \\ 7 & \end{array}$$

$$1729 = \underbrace{41}_{q} \times 42 + \underbrace{7}_{r}$$

III. Diviseurs et multiples

1. Définition et exemples

Définition 24.5
Soient $a, b \in \mathbb{Z}$.

On dit que a divise *b et on note $a \mid b$* $\overset{\Delta}{\text{ssi}}$

$$\exists k \in \mathbb{Z} : b = k \times a.$$

Dans ce cas, on dit aussi que b est un multiple de a

On note

$$\operatorname{Div}(b) := \left\{ k \in \mathbb{Z} \mid k \mid b \right\}.$$

Exemples

4-

- On a $8 \mid 16$.
- On a $\forall n \in \mathbb{Z}, 1 \mid n$ et $-1 \mid n$.
- Soit $n \in \mathbb{N}$. Si $0 \mid n$ alors $n = 0$.
- **Diviseurs de 0.**
  On a $\forall n \in \mathbb{Z}, n \mid 0$. Donc $\operatorname{Div}(0) = \mathbb{Z}$.
- **Diviseurs de 1.**
  On a $\operatorname{Div}(1) = \{-1, 1\}$.

2. Premières propriétés

Fait 24.6
Soient $a, b \in \mathbb{Z}$.

- *On suppose $a \neq 0$. Alors, $a \mid b \iff \dfrac{b}{a} \in \mathbb{Z}$.*
- *Soit $k \in \mathbb{Z}_{\neq 0}$. Alors, $a \mid b \iff ka \mid kb$.*
- *Soit $c \in \mathbb{Z}$. Alors, $a \mid b \implies a \mid bc$.*

3. Divisibilité et combinaisons linéaires

Proposition 24.7
Soient $n, a, b \in \mathbb{Z}$. Alors,

$$\left.\begin{matrix} n \mid a \\ n \mid b \end{matrix}\right\} \implies \forall k, \ell \in \mathbb{Z},\ n \mid ka + \ell b.$$

4. La divisibilité est une relation de (pré)ordre

Proposition 24.8
Soient $a, b, c \in \mathbb{Z}$. Alors,
- $a \mid a$;
- $(a \mid b \text{ et } b \mid a) \implies a = b \text{ ou } a = -b$;
- $(a \mid b \text{ et } b \mid c) \implies a \mid c$.

Démonstration. — • ok car $a = a \times 1$
• si $a = 0$: $\hat{c}$ $a \mid b$, on a $0 \mid b$ et donc $b = 0$
de $\hat{m}$ $b = 0 \Rightarrow a = 0$
Osq. $a, b \neq 0$ et $a \mid b$ et $b \mid a$. Soient donc $k, k' \in \mathbb{Z}$ tq : $a = bk$, $b = k'a$
donc $a = a \cdot k \cdot k'$ or $a \neq 0$: on a $kk' = 1$
donc (cf 24.2) $k = \pm 1$ et $a = \pm b$
• exo ■

Remarques
- Ainsi, la relation « $\mid$ » de divisibilité est une relation d'ordre sur $\mathbb{N}$.
- C'est un préordre sur $\mathbb{Z}$.

5. Ordre et inégalité

Fait 24.9 !!
Soient $a, b \in \mathbb{Z}$. Alors,

$$\left.\begin{matrix} a \mid b \\ b \neq 0 \end{matrix}\right\} \implies |a| \leqslant |b|.$$

Démonstration. — Osq $a \mid b$ et $b \neq 0$
Soit $k \in \mathbb{Z}$ tq $b = k \cdot a$. On a $k \neq 0$
donc $|b| = \underbrace{|k|}_{\geqslant 1 \text{ car } k \in \mathbb{Z} \setminus \{0\}} \cdot |a|$ donc $|a| \leqslant |b|$ ■

IV. Nombres premiers

1. Définition

Définition 24.10

- *Soit $p \in \mathbb{N}$.*

  On dit que p est premier $\overset{\Delta}{\text{ssi}}$ *p possède exactement deux diviseurs dans $\mathbb{N}$.*
- *On note $\mathscr{P}$ l'ensemble des nombres premiers.*
- *Un nombre $n \in \mathbb{N}_{\geqslant 2}$ qui n'est pas premier est dit* composé.

5.

Remarque

- On a donc p est premier $\iff$ $\Big(\mathrm{Div}(p) \cap \mathbb{N}$ est fini et $\big|\mathrm{Div}(p) \cap \mathbb{N}\big| = 2\Big)$.

Exemples

- On a $\boxed{1 \notin \mathscr{P}}$ car $\big|\mathrm{Div}(p) \cap \mathbb{N}\big| = 1$. 6.
- Voilà la liste des premiers nombres premiers :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 \in \mathscr{P}.$$

- En revanche, $91 \notin \mathscr{P}$. En effet, $91 = 7 \times 13$.

Remarque

- Déterminer si un nombre $n \in \mathscr{P}$ et, si non, trouver une factorisation de n est un problème algorithmique compliqué. C'est sur la difficulté de factoriser un nombre composé qu'est construite toute la sécurité des échanges de données en informatique.

2. Lemme d'Ératosthène

Lemme 24.11 (d'Ératosthène)
Soit $N \in \mathbb{N}_{\geqslant 2}$ un nombre composé. Alors,

$$\exists p \in \mathscr{P} : \ \Big(p \mid N \text{ et } p \leqslant \big\lfloor \sqrt{N} \big\rfloor\Big).$$

Démonstration. — On procède par récurrence forte

On note, pour $N \geq 2$, $P(N)$: " $N \notin P \Rightarrow \exists p \in P : \begin{cases} p \mid N \\ p \leq \lfloor \sqrt{N} \rfloor \end{cases}$

. $N = 2$: ok car $2 \in P$

. Rérédité forte : Soit $N \geq 2$ tq $\forall k \in [\![2, N]\!]$, $P(k)$ vraie

Mq $P(N+1)$ est vraie.

On distingue deux cas :

. $N+1 \in \mathcal{P}$: ok

. $N+1 \notin \mathcal{P}$: on écrit $N+1 = a \times b$ avec $a \neq 1$ et $b \neq N+1$

Si $a > \sqrt{N+1}$ et $b > \sqrt{N+1}$, on aurait $ab > N+1$. absurde

donc on a $a \leqslant \sqrt{N+1}$ ou $b \leqslant \sqrt{N+1}$ de plus, on a

$a \geqslant 2$ et $b \geqslant 2$

On suppose par ex. que $a \leqslant \sqrt{N+1}$

donc par croissance de $\lfloor \cdot \rfloor$ $a \leqslant \lfloor \sqrt{N+1} \rfloor$

donc $a \in [\![2, \lfloor \sqrt{N+1} \rfloor]\!]$

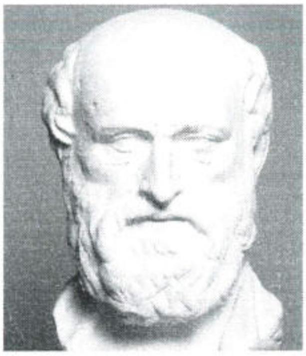
On applique l'hyp. de récurrence à a

* si $a \in \mathcal{P}$: ok
* si $a \notin \mathcal{P}$ on peut trouver $p \in \mathcal{P}$ tq $p \mid a$

On a $p \leqslant a \leqslant \lfloor \sqrt{N+1} \rfloor$

■

3. Crible d'Ératosthène



ÉRATOSTHÈNE de Cyrène (276 av. JC – 194 av. JC)

a) Description de l'algorithme

Soit $N \in \mathbb{N}_{\geqslant 2}$.
Pour déterminer les nombres premiers inférieurs ou égaux à N, on procède comme suit :

1) On détermine les nombres premiers $p_1, p_2, \ldots, p_\ell$ inférieurs ou égaux à $\left\lfloor \sqrt{N} \right\rfloor$.
2) On exclut de $[\![2, N]\!]$ tous les multiples de $p_1, p_2, \ldots, p_\ell$.
3) Les nombres restants sont exactement les nombres premiers inférieurs ou égaux à N.

Cet algorithme est donc naturellement récursif.

b) Détermination des premiers nombres premiers

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

4. L'ensemble $\mathscr{P}$ est infini

Théorème 24.12 (Euclide)
$\mathscr{P}$ est infini.

Démonstration. On raisonne par l'absurde et on écrit

$$\mathscr{P} = \left\{p_1, p_2, \ldots, p_\ell\right\},$$

avec $p_1 < p_2 < p_3 < \cdots < p_\ell$. On considère alors $N := p_1 \times p_2 \times \cdots \times p_\ell - 1$. Comme $\forall j,\ p_j \geqslant 1$, on a

$$p_1 \times p_2 \times \cdots \times p_\ell \geqslant p_k > p_k$$

pour tout $k \in [\![1, \ell]\!]$. En particulier, N n'est égal à aucun des p_k. Donc, $N \notin \mathscr{P}$.
Ainsi, d'après le lemme d'Ératosthène, N possède un diviseur premier. Soit donc $k \in [\![1, \ell]\!]$ tel que $p_k \mid N$.
Ainsi, on a

$$\left.\begin{array}{l} p_k \mid N \\ p_k \mid p_1 \times p_2 \times \cdots \times p_\ell \end{array}\right\} \text{ donc } p_k \mid (N - p_1 \times p_2 \times \cdots \times p_\ell).$$

Donc $p_k \mid 1$. Donc, $p_k \in \{\pm 1\}$. C'est absurde. ∎

5. Décomposition en produit de nombres premiers

a) L'énoncé

Théorème 24.13
Tout entier $n \geqslant 2$ s'écrit de façon unique (à l'ordre près des facteurs) comme produit de nombres premiers.

Démonstration. —

- **Existence :** elle se fait par récurrence forte (exercice).
- **Unicité :** on l'admet. On a besoin pour cette démonstration du résultat :

$$\forall p \in \mathscr{P},\ \forall a, b \in \mathbb{Z},\quad p \mid ab \implies (p \mid a \text{ ou } p \mid b).$$

∎

Exemples

- On a $42 = 6 \times 7 = 2 \times 3 \times 7$.
- On a $1\,729 = 7 \times 13 \times 19$.
- On a $1\,515 = 3 \times 5 \times 101$.
- On a

$$\begin{aligned} 840 &= 2 \times 420 \\ &= 2^2 \times 210 \\ &= 2^3 \times 105 \\ &= 2^3 \times 5 \times 21 \\ &= 2^3 \times 5 \times 3 \times 7 \\ &= \boxed{2^3 \times 3 \times 5 \times 7} \end{aligned}$$

b) Algorithme

Voici un algorithme pour déterminer la décomposition en facteurs premiers d'un entier.
Soit $n \in \mathbb{N}$.

1) Si $n \in \mathscr{P}$ (grâce à l'algorithme d'Ératosthène) : c'est terminé.
2) a) Sinon, le crible d'Ératosthène nous donne un nombre premier p tel que $p \mid n$.
   b) On écrit $n = p \times m$ et on réapplique cet algorithme à m.

Exercice 24.14
Implémenter cet algorithme en `Python`.

6 !!!. Valuations p-adiques

a) Définition

Définition 24.15
Soit $n \in \mathbb{Z} \setminus \{0\}$ et soit $p \in \mathscr{P}$.
La valuation p-adique de n, *notée $v_p(n)$, est le plus grand entier $k \in \mathbb{N}$ tel que p^k divise n.*
Ie, *on pose*

$$v_p(n) := \max\left\{k \in \mathbb{N} \mid p^k \mid n\right\}.$$

Dit autrement, la valuation p-adique d'un entier n est la puissance à laquelle est élevé p dans la décomposition en facteurs premiers de n.

Exercice 24.16
Soient $p \in \mathscr{P}$ et $n \in \mathbb{Z} \setminus \{0\}$. On note

$$A := \left\{k \in \mathbb{N} \mid p^k \mid n\right\}.$$

1) Montrer que A est non vide.
2) Montrer que A est majoré.

Exemples

7

- 60
- 1024
- 105

Remarque

- Par convention, on pose $v_p(0) = +\infty$ pour tout nombre premier p. Cette convention est cohérente puisque tous les entiers divisent 0 et qu'on a donc

$$\left\{k \in \mathbb{N} \mid p^k \mid 0\right\} = \mathbb{N}.$$

b) Valuation p-adique et décomposition en facteurs premiers

Soit $n \geqslant 2$. On décompose n en produit de nombres premiers en écrivant

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

où les p_i sont des nombres premiers deux à deux distincts et que $\forall i, \alpha_i \in \mathbb{N}^*$.

- On peut déjà remarquer que les seuls nombres premiers p qui divisent n sont les p_i.
- De plus, on a
$$\forall i \in [\![1, r]\!],\ v_{p_i}(n) = \alpha_i.$$
De plus, si p ne divise pas n, on a $v_p(n) = 0$.
- Ainsi, on peut écrire
$$n = \prod_{\substack{p \in \mathscr{P} \\ p \mid n}} p^{v_p(n)}.$$
- De plus, si $p \nmid n$, on a $v_p(n) = 0$ et donc $p^{v_p(n)} = p^0 = 1$. Ainsi, on peut écrire :

Théorème 24.17
Soit $n \in \mathbb{N}_{\geqslant 1}$. On a

$$\boxed{n = \prod_{p \in \mathscr{P}} p^{v_p(n)}.}$$

8- dans ce produit, il y a un nb fini de termes ≠ 1

c) Valuation p-adique du produit et de la somme

Proposition 24.18
Soient $n, m \in \mathbb{Z}$ et soit $p \in \mathscr{P}$. On a

9-

1) $v_p(n \times m) = v_p(n) + v_p(m)$;
2) $v_p(n + m) \geqslant \min\big(v_p(n), v_p(m)\big)$.

d) Valuation p-adique et divisibilité

Proposition 24.19
Soient $n, m \in \mathbb{Z}$. On a

$$n \mid m \iff \forall p \in \mathscr{P},\ v_p(n) \leqslant v_p(m).$$

10-

Exercice 24.20
Soit $n \in \mathbb{N}_{\geqslant 2}$. Combien n possède-t-il de diviseurs ?

V. Pgcd et algorithme d'Euclide

1. Définition

Définition 24.21
Soient $a, b \in \mathbb{N}$ avec $a \neq 0$ ou $b \neq 0$.
On appelle pgcd de a et b *et on note* $\operatorname{pgcd}(a,b)$ *le plus grand entier $d \in \mathbb{Z}$ tel que $d \mid a$ et $d \mid b$.*
Autrement dit, on pose
$$\operatorname{pgcd}(a,b) := \max\left\{d \in \mathbb{Z} \quad d \mid a \text{ et } d \mid b\right\}.$$

Remarques
- On note également $a \wedge b := \operatorname{pgcd}(a,b)$.
- Évidemment, le pgcd de a et b est le plus grand diviseur commun entre a et b.
- En Python, pour calculer le pgcd de a et b, il faut importer le module `math` (as `mt` par exemple) et exécuter la commande `mt.gcd(a, b)`.

  En effet, en anglais, le pgcd est *greatest common divisor*.

Exercice 24.22
Soient $a, b \in \mathbb{N}^*$ tels que $a \mid b$. Combien vaut $\operatorname{pgcd}(a,b)$?

Exercice 24.23
Soit $a \in \mathbb{N}^*$. Combien vaut $\operatorname{pgcd}(a,0)$?

2. Pgcd et valuation p-adique

Proposition 24.24
Soient $a, b \in \mathbb{N}^*$. Alors, on a
$$\operatorname{pgcd}(a,b) = \prod_{p \in \mathscr{P}} p^{\min(v_p(a), v_p(b))}.$$

Exemples
- Calculons $\operatorname{pgcd}(27, 105)$.
  - ▷ On a $27 = 3^3$.
  - ▷ On a $105 = 3 \times 5 \times 7$.

  Donc, on a $\operatorname{pgcd}(27,105) = 3^{\min(3,1)} \times 5^{\min(0,1)} \times 7^{\min(0,1)} = 3$.
- Calculons $\operatorname{pgcd}(27, 105)$.
- Calculons $\operatorname{pgcd}(2020, 4243)$. → lng si c'est grand

11

On voit que cette méthode du calcul du pgcd n'est réalisable que si les entiers a et b sont petits ou que l'on connaît leurs décompositions en facteurs premiers.

3. Algorithme d'Euclide : présentation

L'algorithme d'Euclide permet de calculer efficacement pgcd(a, b), en faisant des divisions euclidiennes et en considérant les restes successifs.

a) Description de l'algorithme

Voici l'algorithme d'Euclide.

- On place a et b dans les deux premières lignes.
- On calcule le reste r et le quotient q de la division euclidienne de a par b.
- Puis, on reporte dans la ligne suivante :
  - ▷ le « b » de la ligne n devient le a de la ligne $n+1$;
  - ▷ le « r » de la ligne n devient le b de la ligne $n+1$.
- On continue jusqu'à ce que $r = 0$.
- Le pgcd est alors le dernier reste non nul.

a	b	r	q

b) Pratique de l'algorithme sur un exemple

Calculons pgcd$(1927, 2013)$.

a	b	r	q
2013	1927	86	1
1927	86	35	22
86	35	16	2
35	16	3	2
16	3	1	5
3	1	0	3

pgcd(2013, 1927) = 1

Exercice 24.25
Implémenter en `Python` *l'algorithme d'Euclide.*

4. Algorithme d'Euclide étendu

Définition 24.26
Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$.
Une relation de Bézout entre a et b *est un couple* $(u, v) \in \mathbb{Z}^2$ *tel que*

$$au + bv = \operatorname{pgcd}(a, b).$$

L'algorithme d'Euclide étendu permet de calculer le pgcd de a et b ainsi qu'une relation de Bézout.

a) Description de l'algorithme

Voici l'algorithme d'Euclide.

- On ajoute deux colonnes au tableau précédent pour u et v.
- On initialise ces deux colonnes avec les données :

u	v
1	0
0	1

- On remplit les quatre premières colonne de l'algorithme d'Euclide non étendu jusqu'au reste nul.
- On remplit ensuite les deux dernières colonnes à l'aide du motif :

	α
	β
q	$\alpha - q\beta$

- Les valeurs finales de u et v sur la ligne du dernier reste non nul vérifient alors

$$au + bv = \operatorname{pgcd}(a, b).$$

b) Pratique de l'algorithme sur un exemple

Calculons une relation de Bézout entre 2013 et 1927.

α

β

$q \quad \alpha - q\beta$

a	b	r	q	u	v
				1	0
				0	1
2013	1927	86	1	1	-1
1927	86	35	22	-22	23
86	35	16	2	45	-47
35	16	3	2	-112	117
16	3	1	5	605	-632
3	1	0	3		

$$2013 \times 605 - 632 . 1927 = \text{pgcd}(2013, 1927) = 1$$

Remarques

- On remarque que u et v changent de signe à chaque ligne ; ceci peut être prouvé.
- De même, on remarque que les signes de u et v sont toujours opposés.
- Ces deux remarques peuvent aider à déceler des erreurs de calculs dans l'application de l'algorithme d'Euclide étendu.

Exercice 24.27
Trouver une relation de Bézout entre votre année de naissance et 4 243.

Exercice 24.28
Implémenter en `Python` *l'algorithme d'Euclide étendu.*

5. Preuve de l'algorithme d'Euclide étendu

a) Un lemme

Lemme 24.29
Soient $a, b \in \mathbb{N}^*$.

1) *Soient $q, r \in \mathbb{Z}$ tels que* $\boxed{a = bq + r.}$ *Alors,* $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$.
2) *Soit $r \in [\![0, b-1]\!]$ le reste dans la division euclidienne de a par b. Alors,*

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

Démonstration. — 1) Soit $d \in \mathbb{Z}$ tq $d|a$ et $d|b$ donc $d|a-bq$
donc $d|r$ donc $d|b$ et $d|r$, donc $d \leq \mathrm{pgcd}(b,r)$
pour $d = \mathrm{pgcd}(a,b)$ on trouve $\mathrm{pgcd}(a,b) \leq \mathrm{pgcd}(b,r)$
Soit $\delta \in \mathbb{Z}$ tq $\delta | b$ et $\delta | r$ on a $\delta | bq+r$ donc $\delta | a$
ĉ $\delta | b$, on a $\delta \leq \mathrm{pgcd}(a,b)$ d'où $\mathrm{pgcd}(b,r) \leq \mathrm{pgcd}(a,b)$
donc $\mathrm{pgcd}(a,b) = \mathrm{pgcd}(b,r)$

■

b) Description mathématique de l'algorithme

Soient $a, b \in \mathbb{N}^*$.

- On construit par récurrence les suites $(a_i)_i$, $(b_i)_i$, $(q_i)_i$ et $(r_i)_i$ de la façon suivante :
  - ▷ On pose $a_0 := a$ et $b_0 := b$.
  - ▷ Tant que $b_i \neq 0$, on effectue la division euclidienne de a_i par b_i, qu'on écrit

$$\boxed{a_i = b_i q_i + r_i.}$$

  - ▷ Puis, on pose $a_{i+1} := b_i$ et $b_{i+1} := r_i$.
- On a, par définition du reste dans la division euclidienne, $0 \leqslant r_i < b_i$, donc

$$0 \leqslant b_{i+1} < b_i.$$

Ainsi, d'après l'exercice qui suit, on peut affirmer que la suite $(b_i)_i$ finit par s'annuler.

Exercice 24.30
Montrer qu'il n'existe pas de suite $(u_n)_{n \in \mathbb{N}}$ strictement décroissante telle que $\forall n \in \mathbb{N},\ u_n \in \mathbb{N}$.

- Soit donc $N \in \mathbb{N}$ tel $b_N = 0$. On a donc $r_{N-1} = 0$, *ie* $\boxed{b_{N-1} \mid a_{N-1}.}$
- Donc, on a $\mathrm{pgcd}(a_{N-1}, b_{N-1}) = b_{N-1} = r_{N-2}$.

- Or, d'après le lemme 24.29, comme on a $\forall i \in [\![0, N-1]\!],\ a_i = b_i q_i + r_i$, on a

$$\begin{aligned} & \forall i \in [\![0, N-1]\!],\ \operatorname{pgcd}(a_i, b_i) = \operatorname{pgcd}(b_i, r_i) \\ \text{donc} \quad & \forall i \in [\![0, N-1]\!],\ \operatorname{pgcd}(a_i, b_i) = \operatorname{pgcd}(a_{i+1}, b_{i+1}). \end{aligned}$$

- Ainsi, on a $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(a_0, b_0) = \operatorname{pgcd}(a_{N-1}, b_{N-1}) = r_{N-2}$, qui est le dernier reste non nul.
- Pour résumer, $\boxed{\operatorname{pgcd}(a, b) = r_{N-2} = b_{N-1}.}$

6 *. Lecture matricielle de l'algorithme

Gardons les notations précédente.
Pour $i \in [\![0, N]\!]$, on a

$$\begin{cases} a_{i+1} = b_i \\ b_{i+1} = r_i = a_i - q_i b_i \end{cases}$$

Ce qu'on peut écrire

$$\begin{pmatrix} a_{i+1} \\ b_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} a_i \\ b_i \end{pmatrix}.$$

Donc, on a

$$\begin{aligned} \begin{pmatrix} a_{N-1} \\ b_{N-1} \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-2} \end{pmatrix} \begin{pmatrix} a_{N-2} \\ b_{N-2} \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-3} \end{pmatrix} \begin{pmatrix} a_{N-3} \\ b_{N-3} \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-3} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \begin{pmatrix} a_0 \\ b_0 \end{pmatrix} \end{aligned}$$

Notons $A := \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-3} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}$ et écrivons

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

On a donc

$$\begin{pmatrix} a_{N-1} \\ b_{N-1} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}.$$

Comme on a $b_{N-1} = \operatorname{pgcd}(a, b)$, on en déduit

$$\boxed{\operatorname{pgcd}(a, b) = \gamma \times a + \delta \times b.}$$

Remarque

- Cette analyse matricielle permet de prouver la justesse de l'algorithme d'Euclide étendu.
- Notons $(u_i)_{i \geqslant -2}$ et $(v_i)_{i \geqslant -2}$ les coefficients des deux dernières colonnes. Notons également :

$$M_i := \begin{pmatrix} u_i & v_i \\ u_{i+1} & v_{i+1} \end{pmatrix}.$$

Les relations de récurrence définissant les $(u_i)_{i \geqslant -2}$ et les $(v_i)_{i \geqslant -2}$ sont

$$\begin{cases} u_{i+1} = u_{i-1} - q_{i+1} u_i \\ v_{i+1} = v_{i-1} - q_{i+1} v_i \end{cases} \quad \text{et } M_{-2} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

- Maintenant, calculons

$$\begin{aligned}
\begin{pmatrix} 0 & 1 \\ 1 & -q_{i+2} \end{pmatrix} M_i &= \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+2} \end{pmatrix} \begin{pmatrix} u_i & v_i \\ u_{i+1} & v_{i+1} \end{pmatrix} \\
&= \begin{pmatrix} u_{i+1} & v_{i+1} \\ u_i - q_{i+2} u_{i+1} & v_i - q_{i+2} v_{i+1} \end{pmatrix} \\
&= \begin{pmatrix} u_{i+1} & v_{i+1} \\ u_{i+2} & v_{i+2} \end{pmatrix} \\
&= M_{i+1}.
\end{aligned}$$

- Donc,

$$\begin{aligned}
A &= \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-3} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-3} \end{pmatrix} \cdots \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \times M_{-2}}_{M_{-1}} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-3} \end{pmatrix} \cdots \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \times M_{-1}}_{M_0} \\
&= \cdots = \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-2} \end{pmatrix} \times M_{N-4} \\
&= M_{N-3} \\
&= \begin{pmatrix} u_{N-3} & v_{N-3} \\ u_{N-2} & v_{N-2} \end{pmatrix}
\end{aligned}$$

$M_{-2} = I_2$

- Donc, on a

$$\boxed{\mathrm{pgcd}(a, b) = u_{N-2} \times a + v_{N-2} \times b}$$

les coefficients u_{N-2} et v_{N-2} étant ceux sur la ligne de r_{N-2}, le dernier reste non nul.

7. Théorème de Bachet-Bézout

Ainsi, on a montré

Théorème 24.31 (Bachet-Bézout)
Soient $a, b \in \mathbb{N}^*$. Alors,

$$\exists u, v \in \mathbb{Z} : \ au + bv = \mathrm{pgcd}(a, b).$$

8. Le pgcd est aussi le plus grand diviseur commun pour la relation de divisibilité sur $\mathbb{N}$

Rappelons que la relation de divisibilité est une relation d'ordre sur $\mathbb{N}$. On dipose donc de deux relations d'ordre sur $\mathbb{N}$. On peut donc naturellement se poser la question : le pgcd est-il le plus grand diviseur commun pour ces deux relations d'ordre ?

- Par définition, il l'est pour $\leqslant$.
  Cela veut dire :
$$\forall d \in \mathbb{N}, \; \left(d \mid a \text{ et } d \mid b\right) \implies d \leqslant \operatorname{pgcd}(a,b).$$
- On va voir dans la proposition suivante que le pgcd l'est également pour la relation « $\mid$ » de divisibilité.
  Cela veut dire :
$$\forall d \in \mathbb{N}, \; \left(d \mid a \text{ et } d \mid b\right) \implies d \mid \operatorname{pgcd}(a,b).$$

Proposition 24.32
Soient $a, b \in \mathbb{N}^*$ et soit $d \in \mathbb{Z}$. Alors, on a
$$\begin{cases} d \mid a \\ d \mid b \end{cases} \iff d \mid \operatorname{pgcd}(a,b).$$

(thm de Bézout)

Démonstration. — $\Rightarrow$ Osq $d|a$ et $d|b$. Soient $u, v \in \mathbb{Z}$ tq
$\operatorname{pgcd}(a,b) = au + bv$. On a $d \mid au+bv$
donc $d \mid \operatorname{pgcd}(a,b)$
$\Leftarrow$ Osq $d \mid \operatorname{pgcd}(a,b)$. On a $\operatorname{pgcd}(a,b) \mid a$ donc $d \mid a$
de même $d \mid b$ ∎

12.

Remarque

- Cette proposition nous permet de donner un sens à $\operatorname{pgcd}(0,0)$.
- En effet, on a $\forall n \in \mathbb{Z}, n \mid 0$. Donc, $\operatorname{Div}(0) = \mathbb{Z}$
- Donc, le pgcd de 0 et 0 devrait être le plus grand élément de $\mathbb{Z}$: évidemment, on sait que $\mathbb{Z}$ ne possède pas de plus grand élément pour $\leqslant$.
- Cependant, comme on a
$$\forall n \in \mathbb{Z}, \; n \mid 0,$$
  cela veut dire que 0 est le plus grand élément de $\mathbb{Z}$ pour la relation de divisibilité !
- Ainsi, en toute logique, on pose
$$\boxed{\operatorname{pgcd}(0,0) := 0.}$$

9. Nombres premiers entre eux

Définition 24.33
Soient $a, b \in \mathbb{Z}$.

On dit que a et b sont premiers entre eux $\overset{\Delta}{\text{ssi}}$ $\operatorname{pgcd}(a, b) = 1$.

Exemples

- 12 et 15 ne sont pas premiers entre eux. $3 \mid 12$ et $3 \mid 15$
- 7 et 20 sont premiers entre eux.

VI. Ppcm

1. Définition

On définit de même le ppcm entre deux entiers $a, b \in \mathbb{N}^*$. On le note $\operatorname{ppcm}(a, b)$ ou $a \vee b$.

2. Ppcm et valuation p-adique

Proposition 24.34
Soient $a, b \in \mathbb{N}^*$. Alors,

$$\operatorname{ppcm}(a, b) = \prod_{p \in \mathscr{P}} p^{\max(v_p(a), v_p(b))}.$$

Corollaire 24.35
Soient $a, b \in \mathbb{N}^*$. Alors,

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

13

3. Être multiple commun équivaut à être multiple du ppcm

Proposition 24.36
Soient $a, b \in \mathbb{N}^*$ et soit $n \in \mathbb{Z}$. Alors, on a

$$\begin{cases} a \mid n \\ b \mid n \end{cases} \iff \operatorname{ppcm}(a, b) \mid n.$$

Chapitre 26 : Arithmétique

1_ cf la déf des matrices inversibles :

$A \in M_n(\mathbb{K})$ tq $\exists B : AB = BA = I_n$

cf aussi la déf de la réciproque d'une fct.

2_ on peut prendre $b \in \mathbb{Z} \setminus \{0\}$

on aurait eu $0 \leq r \leq |b|$

3_ div. eucli de 1729 par 42

4_ Soit n tq $0 | n$

Soit donc $k \in \mathbb{Z}$ tq $n = k.0$

donc $n = 0$

5_ si $p \geq 2$ est premier, on a $\mathrm{div}(p) \cap \mathbb{N} = \{1, p\}$

6_ Soit A un anneau

$x \in A$. On dit que x est irréductible ssi

$x \notin \mathcal{U}(A)$ (inversibles de A) noté aussi $A^\times$

$\forall y, z \in A$, $x = yz \Rightarrow y \in \mathcal{U}(A)$ ou $z \in \mathcal{U}(A)$

7_ . $60 = 6 \times 10 = 2 \times 3 \times 2 \times 5 = 2^2 \times 3 \times 5$

$\hookrightarrow v_2(60) = 2$; $v_3(60) = 1$; $v_5(60) = 1$; $v_7(60) = 0$

$\forall p > 5, v_p(60) = 0$

. $1024 = 2^{10}$ $\quad v_2(1024) = 10$. $\forall p \in \mathcal{P}, p \geq 3 \Rightarrow v_p(1024) = 0$

. $105 = 5 \times 21 = 3 \times 5 \times 7$

$v_3(105) = 1$; $v_5(105) = 1$; $v_7(105) = 1$

9_ $n = p^{v_p(n)} \cdot k$
$m = p^{v_p(m)} \cdot k'$

$\alpha = \min(v_p(n), v_p(m))$

on a $n = p^{\alpha} \cdot l$ et $m = p^{\alpha} \cdot l'$

donc $n + m = p^{\alpha}(l + l')$

10_ Osq $n \mid m$ on a $m = k \cdot n$

Si $p \in \mathcal{P}$, $v_p(m) = v_p(k) + v_p(n)$
$\geqslant v_p(n)$

$\Leftarrow$ Osq $\forall p$ $v_p(n) \leqslant v_p(m)$

$$m = \prod_{p \in \mathcal{P}} p^{v_p(m)} = \prod_{p \in \mathcal{P}} p^{\overbrace{v_p(m) - v_p(n)}^{\geqslant 0}} \cdot p^{v_p(n)}$$

$$= \prod_{p \in \mathcal{P}} p^{v_p(m) - v_p(n)} \cdot \underbrace{\prod_{p \in \mathcal{P}} p^{v_p(n)}}_{= n}$$

donc $\exists k \in \mathbb{Z} : m = k \cdot n$ ie $n \mid m$

11_ $27 = 3^3$
$105 = 3 \times 5 \times 7$
$\mathrm{pgcd}(27, 105) = 3^1 \cdot 5^0 \cdot 7^0 = 3$

12_ Soient $a, b \in \mathbb{N}^*$, soit $d \in \mathbb{Z}$
On sait par déf que :

$$\left.\begin{matrix} d \mid a \\ d \mid b \end{matrix}\right\} \Rightarrow d \leqslant \mathrm{pgcd}(a, b)$$

On a mieux :

$$\left.\begin{array}{l} d \mid a \\ d \mid b \end{array}\right\} \Rightarrow d \mid pgcd(a,b) \Rightarrow d \leq pgcd(a,b)$$

13. Fait : Soient $x, y \in \mathbb{R}$

Alors, $max(x+y) + min(x+y) = x+y$

ici $min(v_p(a), v_p(b)) + max(v_p(a) + v_p(b))$
$= v_p(a) + v_p(b)$

donc si $p \in \mathcal{P}$

$$p^{min(\ldots)} \cdot p^{max(\ldots)} = p^{v_p(a)} \cdot p^{v_p(b)}$$

donc : $$\underbrace{\prod_{p \in \mathcal{P}} p^{min(\ldots)}}_{pgcd} \cdot \underbrace{\prod p^{max(\ldots)}}_{ppcm} = \underbrace{\prod_{p \in \mathcal{P}} p^{v_p(a)}}_{a} \cdot \underbrace{\prod_{p \in \mathcal{P}} p^{v_p(b)}}_{b}$$

14. Exemple

ppcm $(60, 28)$?

$60 = 10 \times 6 = 2^2 \times 5 \times 3$

$28 = 14 \times 2 = 2^2 \times 7$

ppcm $(60, 28) = 2^2 \times 3 \times 5 \times 7 = 420$

15. 1) $a, b \in \mathbb{Z}$: $a \mid b \Leftrightarrow \forall p \in \mathcal{P}, v_p(a) \leq v_p(b)$

2) $a, b \in \mathbb{N}^*$

On pose : $ppcm(a,b) := min \left\{ m \in \mathbb{N}^* \;\middle|\; \begin{array}{l} a \mid m \\ b \mid m \end{array} \right\}$

$\neq \emptyset$ car contient a, b

3) On pose $\pi := \prod_{p \in P} p^{\max(v_p(a),\, v_p(b))}$

On a $a \mid \pi$ et $b \mid \pi$ d'après 1)

car $\forall p \in P$, $\begin{cases} v_p(\pi) \geq v_p(a) \\ v_p(\pi) \geq v_p(b) \end{cases}$

donc $\text{ppcm}(a, b) \leq \pi$

4) On a $a \mid \text{ppcm}(a,b)$
$b \mid \text{ppcm}(a,b)$

Soit $p \in P$

On a : $\begin{cases} v_p(\text{ppcm}(a,b)) \geq v_p(a) \\ v_p(\text{ppcm}(a,b)) \geq v_p(b) \end{cases}$

donc, $v_p(\text{ppcm}(a,b)) \geq \max(v_p(a), v_p(b))$

Supposons que $v_p(\text{ppcm}(a,b)) > \max(v_p(a), v_p(b))$

Osq $\max(v_p(a), v_p(b)) = v_p(a)$

donc $\dfrac{\text{ppcm}(a,b)}{p} \in \mathbb{N}$ car $v_p(\text{ppcm}(a,b)) \geq 1$

On a $\dfrac{\text{ppcm}(a,b)}{b} < \text{ppcm}(a,b)$

Mq $a \mid \dfrac{\text{ppcm}(a,b)}{p}$

ok car si $p' \in P$ avec $p' \neq p$

$v_{p'}\left(\dfrac{\text{ppcm}(a,b)}{p}\right) = v_{p'}(\text{ppcm}(a,b)) \geq v_{p'}(a)$

car $a \mid \text{ppcm}(a,b)$

car $v_{p'}(p) = 0$

$v_p(n \times m) = v_p(n) + v_p(m)$

$v_{p'}\left(\dfrac{\text{ppcm}}{p}\right) = v_{p'}(\text{ppcm}) - \underbrace{v_{p'}(p)}_{0}$

$$v_p\left(\frac{ppcm(a,b)}{p}\right) = v_p(ppcm(a,b)) - 1$$

$$\geq v_p(a) - 1$$

$$\geq v_p(a)$$

donc $a \mid \frac{ppcm(a,b)}{p}$