

Introduction à l'arithmétique

1. Divisibilité

Notation (rappel)

Soit $(A, +, \times)$ un anneau intègre.

Soit $x \in A$. On note $xA = \{xa \text{ où } a \in A\}$ et $Ax = \{ax \text{ où } a \in A\}$.

Remarque

Si A est commutatif, $xA = Ax$ et c'est l'idéal engendré par x dans A (c'est un idéal principal). C'est pourquoi nous allons uniquement considérer des anneaux commutatifs.

Exemples

$2\mathbb{Z} = \{2p \text{ où } p \in \mathbb{Z}\} = \{\text{entiers relatifs "pairs"}\}$ et $-1\mathbb{Z} = -\mathbb{Z} = \mathbb{Z}$.

$i\mathbb{R} = \{iy \text{ où } y \in \mathbb{R}\} = \{\text{imaginaires purs}\}$ et $2\mathbb{R} = \mathbb{R}$.

Propriété

Si x est un élément inversible d'un anneau commutatif intègre $(A, +, \times)$, alors $xA = A$.

Démonstration

- On a $xA \subset A$.
- Il faut donc montrer que $A \subset xA$.
Soit x^{-1} l'inverse de x .
Soit $b \in A$, on a $b = 1 \cdot b = (xx^{-1})b = x(x^{-1}b)$.
 b peut donc se mettre sous la forme xa où $a \in A$. Donc $b \in xA$.

Définition

Soit $(A, +, \times)$ un anneau commutatif intègre. Soient a et $b \in A$.

On dit que a divise b ou que b est divisible par a ou que b est un multiple de a et on note a/b si et seulement si $b \in aA$ c'est-à-dire si et seulement si $\exists c \in A / b = ac$.

Remarque

Si l'anneau n'était pas commutatif, on pourrait parler de divisibilité à droite et à gauche. L'égalité $b = ac$ signifie que a divise b à gauche.

Exemples

- Dans \mathbb{Z} , 2 divise 4 car $4 = 2 \times 2$ 2 divise -8 car $-8 = 2 \times (-4)$
-2 divise 6 car $6 = -2 \times -3$ 0 divise 0 car $0 = 0 \times 2$
-7 divise 0 car $0 = -7 \times 0$
- Dans $\mathbb{R}[X]$, $X + 1$ divise $X^2 - 1$ car $X^2 - 1 = (X + 1)(X - 1)$
 $X + 1$ divise $2X + 2$ car $2X + 2 = 2 \times (X + 1)$
 $-2X - 2$ divise $5X + 5$ car $5X + 5 = -\frac{5}{2}(-2X - 2)$

Remarques

- En particulier dans \mathbb{Z} , on a
0 est multiple de tout nombre car $\forall n \in \mathbb{Z}, n \cdot 0 = 0$.
1 est diviseur de tout nombre car, comme \mathbb{Z} est un anneau, $\forall n \in \mathbb{Z}, n \cdot 1 = n$.
-1 est diviseur de tout nombre car $(-1) \cdot (-1) = 1$ donc $\forall n \in \mathbb{Z}, (-1) \cdot (-n) = n$.
- Si $a \neq 0$ et a/b l'élément $c \in A$ tel que $b = ac$ est unique.
On suppose qu'il existe c et c' tels que $b = ac$ et $b = ac'$
 $\Rightarrow ac = ac' \Rightarrow ac - ac' = 0 \Rightarrow a(c - c') = 0 \Rightarrow c - c' = 0 \Rightarrow c = c'$
- Dans un anneau A , tout élément inversible divise tout élément de A .
car si $x, y \in A$ et x inversible alors x^{-1} existe et $y = x(x^{-1}y)$
- Dans un anneau A , tout élément divise 0_A .
car si $x \in A$ alors $0_A = x \cdot 0_A$

Rappel

- Dans \mathbb{Z} , les seuls éléments inversibles sont 1 et -1.
- Dans $\mathbb{R}[X]$, les seuls éléments inversibles sont les polynômes constants non nuls (identifiés à \mathbb{R}^*).

Propriété

Soit $(A, +, \times)$ un anneau commutatif intègre et soient a et $b \in A$.

$$a|b \Leftrightarrow bA \subset aA$$

Démonstration

- (\Rightarrow) On suppose $\exists c \in A / b = ac$.
Soit $x \in bA \Leftrightarrow \exists y \in A / x = by$
 $\Leftrightarrow \exists y \in A / x = acy = a(cy)$ et on a $cy \in A$
 $\Rightarrow x \in aA$.
- (\Leftarrow) On suppose $bA \subset aA$. On a $b \in bA \Rightarrow b \in aA \Rightarrow \exists c \in A / b = ac$.

Remarque

$$2\mathbb{Z} = -2\mathbb{Z} \text{ et } (X + 1)\mathbb{R}[X] = (-2X - 2)\mathbb{R}[X].$$

Propriété

Soit $(A, +, \times)$ un anneau commutatif intègre. Soient a et $b \in A$.

Si l'on a, à la fois, $a|b$ et $b|a$ c'est-à-dire si l'on a $bA = aA$, alors il existe un élément inversible γ de A tel que $b = a\gamma$. Réciproquement si il existe un élément inversible γ de A tel que $b = a\gamma$ alors $bA = aA$.

Démonstration

$$(\Rightarrow) \quad a|b \Leftrightarrow \exists c \in A / b = ac \quad (1)$$

$$b|a \Leftrightarrow \exists d \in A / a = bd \quad (2)$$

Si $a = 0, b = 0$ et tout élément inversible convient.

Si $a \neq 0, b \neq 0$ et (1) et (2) $\Rightarrow a = acd \Rightarrow cd = e$ où e est l'élément unité de A .

$\Rightarrow c$ et d sont des unités de A .

$$(\Leftarrow) \quad x \in bA \Leftrightarrow \exists c \in A / x = bc$$

$$\Leftrightarrow \exists c \in A / x = a\gamma c$$

et on a $\gamma c \in A$

$$\Rightarrow x \in aA.$$

De la même façon :

$$x \in aA \Leftrightarrow \exists c \in A / x = ac$$

$$\Leftrightarrow \exists c \in A / x = a\gamma(\gamma^{-1}c)$$

et on a $\gamma^{-1}c \in A$

$$\Leftrightarrow \exists c \in A / x = b(\gamma^{-1}c)$$

$$\Rightarrow x \in bA.$$

Propriété

La relation de divisibilité dans un anneau est une relation de préordre c'est-à-dire réflexive et transitive.

Démonstration

- $a|a$ car $a = a \times 1$
- $a|b \Leftrightarrow \exists \lambda \in A / b = a\lambda$
- $b|c \Leftrightarrow \exists \mu \in A / c = b\mu \Rightarrow c = a\lambda\mu$ avec $\lambda\mu \in A \Rightarrow a|c$.

Remarques

- Etude de la symétrie et de l'antisymétrie dans \mathbb{Z} .
Si $a|b$ et $b|a$ alors il existe c et d , deux entiers relatifs tels que $a.c = b$ et $b.d = a$.
On a alors $(a.c).d = a.(c.d) = a$.
donc $c.d = 1$ ou encore, puisque c et d appartiennent à \mathbb{Z} : $c = d = 1$ ou $c = d = -1$
- Sur \mathbb{N} , la restriction de la relation de divisibilité de \mathbb{Z} fournit une relation d'ordre mais qui n'est pas total car :
1 est le seul inversible de \mathbb{Z} qui appartienne à \mathbb{N} donc $a|b$ et $b|a \Rightarrow a = b$.
On a ni $2|3$, ni $3|2$.
- La relation de divisibilité dans les polynômes unitaires est un relation d'ordre.

Propriété

Soit $(A, +, \times)$ un anneau commutatif intègre. Soient a, b et $c \in A$.

Si $a|b$ et $a|c$ alors $a|(b+c)$.

Démonstration

$$a|b \Leftrightarrow \exists \lambda \in A / b = a\lambda \quad \text{et} \quad a|c \Leftrightarrow \exists \mu \in A / c = a\mu$$

$$\text{Donc } b+c = a\lambda + a\mu = a(\lambda + \mu).$$

Remarque

La réciproque est fautive en général mais intéressante à étudier.

Propriété

Soit $(A, +, \times)$ un anneau commutatif intègre. Soient $(a_i)_{i \in I}$ et $(b_i)_{i \in I}$ deux familles finies d'éléments de A .
Si $a_i | b_i$, pour tout $i \in I$, alors $\prod_{i \in I} a_i | \prod_{i \in I} b_i$.

Remarques

- Cela donne, par exemple, $2 | 4$ et $3 | 12$ donc $6 | 48$.
- On peut dire aussi que la relation de divisibilité est compatible avec la multiplication.

Démonstration

Pour tout $i \in I$, $a_i | b_i \Leftrightarrow \exists \lambda_i \in A / b_i = a_i \lambda_i$
Donc $\prod_{i \in I} b_i = \prod_{i \in I} a_i \prod_{i \in I} \lambda_i$.

2. Arithmétique

Rappel

Un anneau commutatif (<-- cette propriété est nécessaire pour les idéaux) intègre A est dit principal si et seulement si $\forall I$ idéal de A , $\exists i \in A / I = iA$.
On dit alors que i est un générateur de I .

Remarque

Ce i n'est pas unique mais tout autre j vérifiant $I = jA$ est obtenue de i en le multipliant par un inversible.

Définition

Soit A un anneau principal. Soient a, b deux éléments de A .
On appelle plus petit multiple commun de a et de b et on note $\text{ppcm}(a, b)$ tout générateur de $aA \cap bA$.

Remarques

- L'intersection de deux idéaux est un idéal.
- $x \in aA \cap bA \Leftrightarrow x \in aA$ et $x \in bA$
 $\Leftrightarrow x$ est un multiple de a et x est un multiple de b .
 $\Leftrightarrow x$ est un multiple commun à a et b .
 $c = \text{ppcm}(a, b) \Leftrightarrow$ Tout multiple commun à a et b est un multiple de c .

Propriété

Soient I et J deux idéaux d'un anneau principal A .
L'ensemble $I + J = \{i + j \text{ où } i \in I \text{ et } j \in J\}$ est un idéal de A .

Démonstration

- I et J sont non-vides donc $I + J$ est non vide.
- Soient $x, y \in I + J$. Donc $\exists x_i \in I$ et $\exists x_j \in J / x = x_i + x_j$ et $\exists y_i \in I$ et $\exists y_j \in J / y = y_i + y_j$.
D'où $x - y = (x_i + x_j) - (y_i + y_j) = (x_i - y_i) + (x_j - y_j)$.
Or $x_i - y_i \in I$ et $x_j - y_j \in J$ car I et J sont des sous-groupes.
On a donc $x - y \in I + J$.
- $\forall y \in A, \forall x \in I + J,$
 $\exists x_i \in I$ et $\exists x_j \in J / x = x_i + x_j$
 $xy = (x_i + x_j)y = x_i y + x_j y$ or $x_i y \in I$ car I idéal et $x_j y \in J$ car J idéal. Donc $xy \in I + J$

Définition

Soit A un anneau principal. Soient a, b deux éléments de A .

On appelle plus grand diviseur commun de a et de b et on note $\text{pgcd}(a, b)$ tout générateur de $aA + bA$.

Propriété

Soient a, b deux éléments de A et $d = \text{pgcd}(a, b)$.

- On a :
- (i) $d \mid a$ et $d \mid b$.
 - (ii) $\forall D \in A / D \mid a$ et $D \mid b$ alors $D \mid d$.

Remarque

D'où la dénomination de plus grand diviseur commun.

Démonstration

- $a = a \times 1 + b \times 0 \in aA + bA = dA$ d'où le résultat.
De la même façon, $b = a \times 0 + b \times 1 \in aA + bA = dA$
- $D \mid a \Leftrightarrow a = D \times x$ avec $x \in A$.
 $D \mid b \Leftrightarrow b = D \times y$ avec $y \in A$.
Or $\exists u, v \in A / d = a.u + b.v$ car $d \in aA + bA$.
D'où $d = D.x.u + D.y.v = D(x.u + y.v)$.

Remarque

On étend sans aucune difficulté toutes les définitions et toutes les propriétés au cas d'une famille non plus réduite à deux éléments mais en possédant un nombre finis n .

3. Cas particulier des entiers relatifs

Propriété

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

Alors $\exists q \geq 0$ et $\exists 0 \leq r < a / b = aq + r$.

On dit que l'on a effectué la division euclidienne de b par a .

Remarques

- C'est la division que l'on apprend à l'école primaire : $14 = 2 \times 5 + 4$.

- Si $r = 0$, on dit que a divise b .

Corollaire

Si $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}$, alors $\exists q \in \mathbb{Z}$ et $\exists 0 \leq r < |a|$ / $b = aq + r$.

Exemples

$$-17 = -4 \times 5 + 3 \quad \text{et} \quad -21 = 5 \times (-5) + 4.$$

Propriété

\mathbb{Z} est un anneau principal.

Démonstration

Soit I un idéal de \mathbb{Z} , I est un sous-groupe de \mathbb{Z} .

- si $I = \{0\}$, on a bien $I = 0\mathbb{Z}$.
- si $I \neq \{0\}$, soit $I' = \{x \in I / x > 0\}$. On a $I = \{0\} \cup I' \cup (-I')$.
Soit a le plus petit élément de I' (on veut donc montrer que $I = a\mathbb{Z}$).

$a\mathbb{N} \subset I$ car I est un sous-groupe de \mathbb{Z} .

$a\mathbb{N} \subset I'$ car tous les éléments sont positifs.

Soit $b \in I'$, $\exists q \geq 0$ et $\exists 0 \leq r < a$ / $b = aq + r \quad \Rightarrow \quad r = b - aq$

Or $b \in I' (\subset I)$ et $aq \in I' (\subset I)$ donc $r \in I$

Puisque $r \geq 0$, on a $r \in I'$ ou $r = 0$.

Or $r < a$ et a est le plus petit élément de I' donc r ne peut appartenir à I' .

Donc $r = 0 \Rightarrow b = aq \Rightarrow ba \in \mathbb{N}$.

Donc $a\mathbb{N} = I'$ et $I = a\mathbb{Z}$.

Remarque

Nous verrons que $\mathbb{R}[X]$ est aussi un anneau principal.

Rappel

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$.

- Un élément de $a\mathbb{Z} \cap b\mathbb{Z}$ est, à la fois un multiple de a et de b .
On appelle plus petit multiple commun de a et de b tout générateur de $a\mathbb{Z} \cap b\mathbb{Z}$.
Tout multiple commun à a et b est un multiple du ppcm(a, b).
- On appelle plus grand diviseur commun de a et de b tout générateur de $a\mathbb{Z} + b\mathbb{Z}$.
Le pgcd(a, b) est un diviseur commun à a et à b .
Tout diviseur autre commun à a et à b divise le pgcd(a, b).

Propriété

Soient a et b deux entiers relatifs. Un pgcd de (a, b) est unique au signe près.

Donc, dans le cas des relatifs, nous prendrons pour pgcd le nombre positif.

Démonstration

Soit d un pgcd de (a, b) et d' un autre pgcd de (a, b) .

On a $d'\mathbb{Z} = d\mathbb{Z}$ donc il existe un élément inversible γ de \mathbb{Z} tel que $d' = d\gamma$.

C'est-à-dire $d' = d$ ou $d' = -d$.

Exemple

$\text{pgcd}(12,18) = 6$.

Propriété (Identité de Bezout)

Soient a et b deux entiers relatifs et $d = \text{pgcd}(a,b)$.

Il existe alors u et v deux entiers relatifs tels que $a.u + b.v = d$.

Démonstration

Soient a et b deux entiers relatifs. Soit $d = \text{pgcd}(a,b)$.

Par définition $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} = \{a.j + b.k \mid (j,k) \in \mathbb{Z}^2\}$

Or, on a $d \in d\mathbb{Z} = \{a.j + b.k \mid (j,k) \in \mathbb{Z}^2\}$ d'où le résultat.

Remarques

- Il n'y a pas unicité du couple (u,v) .
Contre-exemple : Si on considère le couple $(2,4)$ on a $\text{pgcd}(2,4) = 2$
et pourtant : $2 = 2 \times 1 + 4 \times 0 = 2 \times 3 - 4 \times 1$
- On n'a pas la réciproque de $d = \text{pgcd}(a,b) \Rightarrow \exists (u,v) \in \mathbb{Z}^2 \mid a.u + b.v = d$
Sinon on pourrait prendre n'importe quel couple (u,v) .
Cette remarque peut sembler évidente maintenant mais il pourra y avoir des confusions lorsque nous aurons vu le théorème de Bezout.
On a $2 = 2 \times 0 + 4 \times 0$ et bien entendu $\text{pgcd}(2,4) = 2$ mais, par exemple $-14 = 2 \times 3 + 4 \times (-5)$.

Propriété

Soient a et b deux entiers relatifs.

$\text{pgcd}(a,b) = \text{pgcd}(|a|,|b|)$

Démonstration

Posons $d = \text{pgcd}(a,b)$ et $D = \text{pgcd}(|a|,|b|)$

On a $a\mathbb{Z} = |a|\mathbb{Z}$ et $b\mathbb{Z} = |b|\mathbb{Z}$.

On obtient alors $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} = |a|\mathbb{Z} + |b|\mathbb{Z} = D\mathbb{Z}$.

Etant donné que d et D sont de même signe et qu'ils engendrent le même sous-groupe de \mathbb{Z} , on a déjà montré que $D = d$.

Propriété

Soient a,b et v trois entiers relatifs.

On a : $\text{pgcd}(v.a, v.b) = |v|. \text{pgcd}(a,b)$.

Démonstration

On peut déjà remarquer que $\text{pgcd}(v.a, v.b) = \text{pgcd}(|v.a|,|v.b|) = \text{pgcd}(|v|.|a|,|v|.|b|)$

et que $|v|. \text{pgcd}(a,b) = |v|. \text{pgcd}(|a|,|b|)$.

On peut donc travailler avec a,b et v positifs.

Soient $d = \text{pgcd}(a,b)$ et $D = \text{pgcd}(v.a, v.b)$, on veut montrer que $D = v.d$. c'est-à-dire $D\mathbb{Z} = (v.d)\mathbb{Z}$ puisque D et $v.d$ sont positifs.

- Soit $x \in (v.d)\mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z} / x = v.d.k$
 $\exists p, q \in \mathbb{Z} / d = a.q + b.p$ car $d = \text{pgcd}(a,b)$ et identité de Bezout.
 D'où $v.d = (v.a).q + (v.b).p$ et $x = (v.a).(q.k) + (v.b).(p.k)$
 Donc $x \in (v.a)\mathbb{Z} + (v.b)\mathbb{Z} = D\mathbb{Z}$.
- Soit $m \in D\mathbb{Z}$.
 D'après la définition de $(v.a)\mathbb{Z} + (v.b)\mathbb{Z}$, il existe alors deux entiers relatifs f et g tels que
 $m = (v.a).f + (v.b).g = v.(a.f + b.g)$.
 Or $a.f + b.g \in d\mathbb{Z}$ donc $m \in (v.d)\mathbb{Z}$.

Remarques

- Les deux propriétés précédentes montrent que, en général, on peut travailler avec des positifs.
- Soit a un entier relatif non nul, on a : $\text{pgcd}(0,a) = a$.
 En effet $0\mathbb{Z} = \{0\}$, donc $0\mathbb{Z} + a\mathbb{Z} = \{0\} + a\mathbb{Z} = a\mathbb{Z}$.
- Soit a un entier relatif, on a : $\text{pgcd}(1,a) = 1$.
 En effet $a\mathbb{Z} \subset \mathbb{Z} = 1\mathbb{Z}$, d'où $1\mathbb{Z} + a\mathbb{Z} = 1\mathbb{Z}$.

Propriété

Soient a et b deux entiers relatifs. On a : $(a,b) \neq (0,0) \Leftrightarrow \text{pgcd}(a,b) \neq 0$

Démonstration

- $\text{pgcd}(0,0) = 0$. En effet $0\mathbb{Z} = \{0\}$, donc $0\mathbb{Z} + 0\mathbb{Z} = \{0\} + \{0\} = \{0\} = 0\mathbb{Z}$.
- Si $\text{pgcd}(a,b) = 0$, alors $a\mathbb{Z} + b\mathbb{Z} = \{0\}$.
 Donc $a\mathbb{Z} \subset \{0\}$ et $b\mathbb{Z} \subset \{0\}$.
 On a alors $(a\mathbb{Z} = \emptyset \text{ ou } a\mathbb{Z} = \{0\})$ et $(b\mathbb{Z} = \emptyset \text{ ou } b\mathbb{Z} = \{0\})$.
 Comme $a\mathbb{Z}$ et $b\mathbb{Z}$ ne peuvent être vides, on a alors obligatoirement : $a\mathbb{Z} = b\mathbb{Z} = \{0\}$.
 Donc $a = b = 0$.

Lemme d'Euclide

Soient a et b deux entiers relatifs.

S'il existe deux entiers relatifs $q \geq 0$ et $0 \leq r < b$ tels que $a = b.q + r$ alors $\text{pgcd}(a,b) = \text{pgcd}(b,r)$.

Démonstration

Soit $d = \text{pgcd}(a,b)$ et $d' = \text{pgcd}(b,r)$

- $d = \text{pgcd}(a,b) \Rightarrow d|a$
 $d = \text{pgcd}(a,b) \Rightarrow d|b$ et donc $d|b.q$ donc $d|(a-b.q)$ c'est-à-dire $d|r$.
 D'où $d|b$ et $d|r \Rightarrow d|d'$.
- $d' = \text{pgcd}(b,r) \Rightarrow d'|r$
 $d' = \text{pgcd}(b,r) \Rightarrow d'|b$ et donc $d'|b.q$ alors $d'|(b.q + r)$ donc $d'|a$.
 D'où $d'|a$ et $d'|b \Rightarrow d'|d$.

Comme d et d' sont positifs, $d = d'$

Algorithme d'Euclide

Soient a et b deux entiers relatifs non nuls.

Effectuons la division euclidienne de a par b : $\exists (q_1, r_1) \in \mathbb{Z}^2$ tels que $(0 \leq r_1 < b)$ et $(a = b \cdot q_1 + r_1)$.
 D'après le lemme d'Euclide, $\text{pgcd}(a, b) = \text{pgcd}(b, r_1)$.

- Si $r_1 = 0$ alors $\text{pgcd}(b, r_1) = b = \text{pgcd}(a, b)$.
- Sinon, on réitère le processus sur (b, r_1) , puis (r_1, r_2) , (r_2, r_3) ... jusqu'à ce que le reste de la division euclidienne soit nul, ce qui se produit forcément, puisque chaque reste est un entier naturel strictement inférieur au précédent (on a au plus $|b|$ étapes). Le pgcd de (a, b) est alors le dernier reste non nul (car $\text{pgcd}(a, b) = \text{pgcd}(r_n, 0) = r_n$).

Exemple

$$\begin{aligned} a &= 36465 \text{ et } b = 585 \\ 36465 &= 62 \times 585 + 195 \\ 585 &= 3 \times 195 + 0 \end{aligned} \quad \text{d'où } \text{pgcd}(a, b) = 195$$

Remarque

$$\begin{aligned} a &= 40392 \text{ et } b = 42 \\ 40392 &= 961 \times 42 + 30 \\ 42 &= 1 \times 30 + 12 \\ 30 &= 2 \times 12 + 6 \\ 12 &= 2 \times 6 + 0 \end{aligned} \quad \text{d'où } \text{pgcd}(a, b) = 6$$

$$\begin{aligned} 6 &= 30 - 2 \times 12 \\ 6 &= 30 - 2 \times (42 - 30) \\ 6 &= 3 \times 30 - 2 \times 42 \\ 6 &= 3 \times (40392 - 961 \times 42) - 2 \times 42 \\ 6 &= 40392 \times 3 - 2885 \times 42 \end{aligned}$$

De façon plus générale, nous allons voir comment on peut déterminer un couple (u, v) vérifiant l'identité de Bezout.

Algorithme d'Euclide appliqué à l'identité de Bezout

Soient a et b deux entiers relatifs.

Posons $d = \text{pgcd}(a, b)$.

D'après l'identité de Bezout, il existe deux entiers relatifs u et v tels que : $a \cdot u + b \cdot v = d$

Mais nous n'avons aucun moyen pratique de les calculer; nous allons voir que l'algorithme d'Euclide va nous permettre de les trouver. Il y a donc une double utilité à cet algorithme : la recherche du pgcd et son expression en fonction de a et b .

Supposons avoir appliqué l'algorithme à (a, b) ; on a donc les $n + 1$ étapes suivantes :

$$\begin{aligned} a &= b \cdot q_1 + r_1 \\ b &= r_1 \cdot q_2 + r_2 \\ &\dots \\ r_{n-2} &= r_{n-1} \cdot q_n + r_n \\ r_{n-1} &= r_n \cdot q_{n+1} + 0 \end{aligned}$$

En notant $a = r_{-1}$ et $b = r_0$, on voit que chaque reste d'ordre k (avec $k \geq 1$) peut s'exprimer comme une combinaison linéaire de r_{k-1} et r_{k-2}

C'est-à-dire $r_k = l \cdot r_{k-1} + m \cdot r_{k-2}$ avec $(l, m) \in \mathbb{Z}^2$.

Ainsi r_n est une combinaison linéaire de r_{n-1} et de r_{n-2} et, comme r_{n-1} est une combinaison linéaire de r_{n-2} et r_{n-3} , on peut exprimer à son tour r_n comme une combinaison linéaire de r_{n-2} et r_{n-3} . En procédant ainsi avec les restes successifs, on trouve explicitement r_n comme combinaison linéaire de r_{-1} et r_0 , les coefficients étant des sommes et produits des quotients successifs.

On a ainsi :

$$r_n = r_{n-2} - q_n \cdot r_{n-1}$$

$$r_{n-1} = r_{n-3} - q_{n-1} \cdot r_{n-2}$$

donc : $r_n = r_{n-2} - q_n \cdot (r_{n-3} - q_{n-1} \cdot r_{n-2})$
 soit : $r_n = (1 + q_n \cdot q_{n-1}) \cdot r_{n-2} - q_n \cdot r_{n-3}$

Et on réitère le processus jusqu'à trouver r_n comme CL de r_{-1} et de r_0 , c'est-à-dire $d = u \cdot a + v \cdot b$.

Remarque

Si les valeurs des quotients n'ont aucun rôle lorsqu'on utilise l'algorithme pour trouver le pgcd, elles sont indispensables pour calculer u et v et il faut donc les conserver.

Définition

Soient a et b deux entiers relatifs.

On dit que a et b sont premiers entre eux si et seulement si $\text{pgcd}(a,b) = 1$

Exemple

Les nombres 6 et 55 sont premiers entre eux.

Définition

On dit qu'un entier relatif p est premier s'il admet exactement quatre diviseurs : $1, -1, p$ et $-p$.

Remarques

- Un entier $p > 0$ est premier si et seulement si il admet exactement deux diviseurs positifs.
- Il n'y a qu'un nombre premier pair.

Propriété

Soient $p, m \in \mathbb{Z}$ tels que p soit un nombre premier.

Alors m n'est pas un multiple de $p \Leftrightarrow p$ et m sont premiers entre eux.

C'est-à-dire : $m \notin p\mathbb{Z} \Leftrightarrow \text{pgcd}(m,p) = 1$.

Démonstration

Soit $d = \text{pgcd}(p,m)$. On a, par caractérisation du pgcd, $d|p$ et $d|m$.

Comme $d|p$ alors $d = 1$ ou $d = p$.

- Si $m \in p\mathbb{Z}$, alors $p|m$ et donc $p|d$, car d est le plus grand des diviseurs communs à p et m .
Donc $d = p$ et $\text{pgcd}(p,m) \neq 1$.
- Si $m \notin p\mathbb{Z}$, alors on ne peut avoir $d = p$ car comme $d|m$, on aurait $p|m$ ce qui est absurde.
Donc $d = 1$, soit $\text{pgcd}(p,m) = 1$

Théorème (de Bezout)

Soient a et b deux entiers relatifs.

On a : $\text{pgcd}(a,b) = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2 / a.u + b.v = 1$.

Démonstration

(\Rightarrow) déjà fait.

(\Leftarrow) $a.u + b.v = 1$ et soit $d = \text{pgcd}(a,b)$.

On a $d | a \Rightarrow d | au$

$d | b \Rightarrow d | bv \Rightarrow d | a.u + b.v \Rightarrow d | 1 \Rightarrow d = 1$.

Exemple

6 et 55 sont premiers entre eux et $1 \times 55 - 9 \times 6 = 1$.

Remarque

Il ne faut surtout pas confondre l'identité et le théorème de Bezout.

Théorème (de Gauss)

Soient a, b et c trois entiers relatifs. Si $a | b.c$ et $\text{pgcd}(a,b) = 1$ alors $a | c$.

Démonstration

$\text{pgcd}(a,b) = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2 / a.u + b.v = 1$

$\Rightarrow a.c.u + b.c.v = c$.

Or $a | a.c.u$ et $a | b.c.v$ car $a | b.c$ donc $a | c$.

Exemple

$6 | 5610 = 55 \times 102$ et $\text{pgcd}(55,6) = 1$ donc $6 | 102$ en effet $102 = 17 \times 6$.

Remarques

- Ce théorème s'énonce aussi sous la forme :
"Si a divise un produit de deux facteurs et s'il est premier avec l'un des facteurs, il divise l'autre".
- Ce théorème n'a jamais signifié :
"Si $a | b.c$ et si a ne divise pas b alors $a | c$ "
Ce qui est totalement FAUX, comme le montre le contre-exemple suivant :
 $6 | 3 \times 4 = 12$ et pourtant 6 ne divise ni 3 ni 4.

Théorème (d'Euclide)

Soient a et b deux entiers relatifs et p un nombre premier.

Si p divise $a.b$ alors p divise a ou p divise b .

Démonstration

- Si $a \in p\mathbb{Z}$, alors $p | a$.
- Si $a \notin p\mathbb{Z} \Rightarrow \text{pgcd}(a,p) = 1$ or $p | a.b$ donc $p | b$.

Remarques

- Si ces trois théorèmes semblent découler chacun du précédent, il est toutefois nécessaire de les connaître tous. Il faut de plus remarquer que s'ils semblent n'être qu'une version "allégée" du précédent, historiquement c'est le théorème d'Euclide qui a été trouvé en premier, puis celui de Gauss et enfin celui de Bezout.
- Ce théorème se généralise à un produit de n facteurs
Soient a_1, a_2, \dots, a_n n entiers relatifs.
Soit p un nombre premier.
Si $p \mid a_1 a_2 \dots a_n$ alors $p \mid (a_1 a_2 \dots a_{n-1}) \cdot a_n$.
Donc, d'après le théorème que l'on vient de démontrer, $p \mid a_n$ ou $p \mid a_1 a_2 \dots a_{n-1}$.
Quitte à réitérer le même processus $n - 1$ fois, on montre ainsi qu'il existe i tel que $p \mid a_i$.

Propriété

Soient $a, b \in \mathbb{Z} / (a, b) \neq (0, 0)$.

On a $\text{pgcd}(a, b) = d \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2 / a \cdot u + b \cdot v = d$ et $\text{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Démonstration

On a bien $d = \text{pgcd}(a, b) \neq 0$.

On sait que $d \mid a$ donc $\frac{a}{d} \in \mathbb{Z}$. De même $\frac{b}{d} \in \mathbb{Z}$.

Si $d' = \text{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right) \neq 1$, alors $\frac{a}{d} = d'k$ et $\frac{b}{d} = d'k'$ avec $k, k' \in \mathbb{Z}$.

Donc $a = (dd')k$ et $b = (dd')k'$ avec $k, k' \in \mathbb{Z}$.

C'est-à-dire $dd' \mid a$ et $dd' \mid b$ absurde de par la définition du pgcd.

Théorème (fondamental de l'arithmétique)

Tout entier strictement supérieur à 1 se décompose de façon unique en produit fini de facteurs premiers.

Remarques

- La décomposition est unique "à l'ordre près", car on peut évidemment intervertir l'ordre des facteurs du produit.
- Pour les entiers 0 et 1, il n'y a aucun besoin de chercher à les décomposer.
- Pour les entiers négatifs, on utilise celle de leur valeur absolue, affectée d'un signe moins.
- Bien que ce théorème semble évident, sa démonstration n'est pas aussi aisée qu'il y paraît. De plus, il est nécessaire de l'avoir toujours en tête car il permet de démontrer la plupart des résultats de divisibilité; c'est en cela qu'il est "fondamental".

Démonstration

Le résultat est évidemment vrai pour $n = 2$.

Supposons que le résultat soit vrai pour tous les entiers inférieurs ou égaux à n .

Si $n + 1$ est premier, alors il se décompose en produit d'un seul nombre premier, lui-même.

Sinon, $n + 1$ n'étant pas premier, il vient : $\exists c, d \in \mathbb{Z}$ et $n + 1 = c \cdot d$ avec $c \leq n$ et $d \leq n$.

D'après l'hypothèse de récurrence, c et d admettent une décomposition en produit de facteurs premiers, il en est donc de même pour leur produit.

Il reste à montrer que les facteurs sont uniques (à l'ordre près).

Supposons qu'il existe deux décompositions en produit de nombres premiers, on a alors :

$$\begin{aligned} n+1 &= a_1 a_2 \dots a_p && \text{avec } a_i \text{ premier } \forall i = 1, p \\ &= b_1 b_2 \dots b_q && \text{avec } b_i \text{ premier } \forall i = 1, q \end{aligned}$$

On a $a_1 | n+1$ donc $a_1 | b_1 b_2 \dots b_q$

D'après le théorème d'Euclide (voir la remarque), $\exists l \in \{1, \dots, q\}$ tel que $a_1 | b_l$

On a alors obligatoirement $a_1 = b_l$ (découle directement de la notion de nombre premier).

On reindice les $b_1 b_2 \dots b_q$ de façon à placer b_l en premier.

On a $\frac{n+1}{a_1} = \frac{n+1}{b_1} = a_2 a_3 \dots a_p = b_1 b_2 \dots b_q$ et $\frac{n+1}{a_1} \leq n$, par hypothèse de récurrence, on a l'unicité de la décomposition de $\frac{n+1}{a_1}$ donc $p = q$ et $a_i = b_i \forall i = 1, p$.

La décomposition de $n+1$ est donc unique.

Remarques

- C'est à nouveau les décompositions que l'on apprend au collège
Par Exemple :

132	2
66	2
33	3
11	11
1	
- Grâce au théorème fondamental que nous venons d'énoncer, nous allons pouvoir préciser la notion de divisibilité, notamment avec la notion de valuation.

Définition

Soit n un entier naturel strictement supérieur à 1. Soit p un nombre premier.

On appelle valuation en p de l'entier naturel n , noté $v_p(n)$, l'entier qui correspond à la plus haute puissance de p qui divise n .

Remarques

- Si p ne divise pas n , $v_p(n) = 0$.
- Soit P l'ensemble des nombres premiers.
En utilisant le théorème fondamental de l'arithmétique, tout entier naturel n strictement supérieur à

1 peut donc s'écrire sous la forme : $n = \prod_{p \in P} p^{v_p(n)}$.

Propriété

Soient a et b deux entiers naturels non nuls et soit P l'ensemble des nombres premiers.

$$a | b \iff v_p(a) \leq v_p(b) \quad \forall p \in P.$$

Démonstration

On peut écrire $a = \prod_{i=1}^r p_i^{v_{p_i}(a)}$ et $b = \prod_{j=1}^s q_j^{v_{q_j}(b)}$ mais aussi $a = \prod_{p \in P} p^{v_p(a)}$ et $b = \prod_{p \in P} p^{v_p(b)}$.

(\Rightarrow) Par l'absurde, si $v_p(a) > v_p(b)$ pour un nombre premier p fixé.

$$\text{On a } \frac{a}{p^{v_p(b)}} = p^{v_p(a)-v_p(b)} c \text{ et } \frac{b}{p^{v_p(b)}} = d \quad \text{où } c, d \in \mathbb{Z}^* \text{ et } v_p(c) = v_p(d) = 0.$$

Si $a | b$ alors $b = ae$, on a $d = p^{v_p(a)-v_p(b)} ce$: Absurde.

(\Leftarrow) Si $v_p(a) \leq v_p(b) \quad \forall p \in \left\{ \bigcup_{i=1}^r p_i \cup \bigcup_{j=1}^s q_j \right\}$.

On a alors $p^{v_p(b)} = p^{v_p(a)} p^{v_p(b)-v_p(a)}$ c'est-à-dire $p^{v_p(a)} | p^{v_p(b)}$. Et donc $\prod_{i=1}^r p_i^{v_{p_i}(a)} | \prod_{j=1}^s q_j^{v_{q_j}(b)}$.

Propriété

Un ppcm d'un couple d'entiers relatifs est unique au signe près, nous prendrons le nombre positif.

Démonstration

Soient a et b deux entiers relatifs et soient m et m' deux ppcm de (a,b) .

On a $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} = m'\mathbb{Z}$.

Donc il existe un élément inversible γ de \mathbb{Z} tel que $m' = m\gamma$. C'est-à-dire $m' = m$ ou $m' = -m$.

Remarque

On a $\text{ppcm}(a,b) = \text{ppcm}(|a|,|b|)$.

Propriété

Soient a,b et λ des entiers relatifs.

On a $\text{ppcm}(\lambda.a,\lambda.b) = |\lambda|. \text{ppcm}(a,b)$.

Démonstration

Soient a, b et λ des entiers relatifs.

Puisque $\text{ppcm}(\lambda.a,\lambda.b) = \text{ppcm}(|\lambda|.a,|\lambda|.b)$ et $\text{ppcm}(a,b) = \text{ppcm}(|a|,|b|)$, on peut supposer a,b et λ positifs.

Posons $m = \text{ppcm}(a,b)$ et $L = \text{ppcm}(\lambda.a,\lambda.b)$.

$$\begin{aligned} x \in L\mathbb{Z} &\Leftrightarrow x \in (\lambda a)\mathbb{Z} \cap (\lambda b)\mathbb{Z} \\ &\Leftrightarrow \exists u,v \in \mathbb{Z} \text{ et } x = (\lambda a).u = (\lambda b).v \\ &\Leftrightarrow \exists u,v \in \mathbb{Z} \text{ et } x = \lambda(a.u) = \lambda(b.v) \\ &\Leftrightarrow x = \lambda y \text{ où } y \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} \\ &\Leftrightarrow x \in (\lambda.m)\mathbb{Z}. \end{aligned}$$

Donc $(\lambda.m)\mathbb{Z} = L\mathbb{Z}$ et $\lambda.m = L$.

Propriété

Soient a et b des entiers relatifs. On a $|a.b| = \text{ppcm}(a,b).\text{pgcd}(a,b)$.

Démonstration

On suppose a et b positifs. Posons $d = \text{pgcd}(a,b)$ et $m = \text{ppcm}(a,b)$.

On peut écrire $a = \prod_{i=1}^r p_i^{v_{p_i}(a)}$, $b = \prod_{j=r+1}^{r+s} p_j^{v_{p_j}(b)}$ et $ab = \prod_{i=1}^r p_i^{v_{p_i}(a)} \prod_{j=r+1}^{r+s} p_j^{v_{p_j}(b)}$.

On peut réorganiser les indices : $ab = \prod_{i=1}^t p_i^{v_{p_i}(a)+v_{p_i}(b)}$.

On pose $D = \prod_{i=1}^t p_i^{k_i}$ où $k_i = \min\{v_{p_i}(a) + v_{p_i}(b)\}$

$M = \prod_{i=1}^t p_i^{l_i}$ où $l_i = v_{p_i}(a) + v_{p_i}(b) - \min\{v_{p_i}(a) + v_{p_i}(b)\}$.

On a $ab = MD$ et $l_i = \max\{v_{p_i}(a) + v_{p_i}(b)\}$.

Rappel : $c|d \Leftrightarrow v_p(c) \leq v_p(d) \quad \forall p \in P.$

On constate que D est un diviseur commun à a et à b et M est un multiple commun à a et b .

On a donc $D|d$.

Supposons que $D \neq d$, alors il existe $p \in P$ tel que $v_p(D) < v_p(d)$.

Quitte à inverser a et b , on peut supposer que $\min(v_p(a), v_p(b)) = v_p(a)$.

On a $v_p(a) = v_p(D) < v_p(d)$ et puisque $d|a$, $v_p(d) \leq v_p(a)$: ce qui est absurde.

D'où $D = d = \text{pgcd}(a, b)$.

Nous allons maintenant démontrer que $M = m$ de manière analogue à la démonstration précédente.

On a donc $m|M$.

Supposons que $m \neq M$, alors il existe $p \in P$ tel que $v_p(m) < v_p(M)$.

Quitte à inverser a et b , on peut supposer que $\max(v_p(a), v_p(b)) = v_p(a)$.

On a $v_p(m) < v_p(M) = v_p(a)$ et puisque $a|m$, $v_p(a) \leq v_p(m)$: ce qui est absurde.

Enfin $M = m = \text{ppcm}(a, b)$.

Exemple

On a donc une autre méthode pour déterminer le ppcm et le pgcd.

132	2	110	2
66	2	55	5
33	3	11	11
11	11	1	
1			

C'est-à-dire $132 = 2 \times 2 \times 3 \times 11$

et $110 = 2 \times 5 \times 11$

Donc $\text{pgcd}(132, 110) = 2 \times 11 = 22$.

$\text{ppcm}(132, 110) = 2 \times 2 \times 3 \times 5 \times 11 = 660$

Définition (Généralisation)

Soient $a_1, \dots, a_n, n (\geq 2)$ entiers relatifs.

- On note $d = \text{pgcd}(a_1, \dots, a_n)$ le générateur positif de $a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$.
- $m = \text{ppcm}(a_1, \dots, a_n)$ le générateur positif de $a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \dots \cap a_n\mathbb{Z} = d\mathbb{Z}$.
- Si $\text{pgcd}(a_1, \dots, a_n) = 1$, les (a_i) sont dit premiers dans leur ensemble.
- Si, $\forall i, j / i \neq j$, $\text{pgcd}(a_i, a_j) = 1$, les (a_i) sont dits premiers deux à deux.

Propriété

Soient $a_1, \dots, a_n, n (\geq 2)$ entiers relatifs.

Soit $d = \text{pgcd}(a_1, \dots, a_n)$ d est le plus grand entier divisant tous les $a_i, i = 1, n$.

Soit $m = \text{ppcm}(a_1, \dots, a_n)$ m est le plus petit entier multiple de tous les $a_i, i = 1, n$.