Algèbre – Arithmétique, Polynômes

Christophe Mouilleron

ensIIE

Division euclidienne dans $\mathbb{Z}$

Théorème (division euclidienne)

Pour tout $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, il existe des entiers q et r tels que :

1. $a = b\,q + r$
2. $0 \leq r < |b|$.

q = quotient
r = reste

Division euclidienne dans $\mathbb{Z}$

Théorème (division euclidienne)

Pour tout $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, il existe des entiers q et r tels que :

1. $a = b\,q + r$
2. $0 \leq r < |b|$.

q = quotient
r = reste

Lorsque $r = 0$, on a l'égalité $a = b\,q$ et on dit que :

- a est un multiple de b — $a \in b\mathbb{Z}$
- b est un diviseur de a — $b \mid a$

Notation *modulo*

Notation (modulo)

Si a et b sont des entiers, et $m \in \mathbb{N}^*$, on note

$$a \equiv b \bmod m \qquad \text{ou} \qquad a \equiv b\,[m]$$

lorsque m divise $a - b$.

Remarques :

- il existe $q \in \mathbb{Z}$ tel que $a = b + m\,q$
- a et b ont le même reste après division par m

Calculs modulo un entier

Si a_1, a_2, b_1, b_2 sont des entiers, si $m \in \mathbb{N}^*$, et si

$$a_1 \equiv b_1 \bmod m$$
$$a_2 \equiv b_2 \bmod m$$

alors :

$$\begin{aligned} a_1 + a_2 &\equiv b_1 + b_2 \bmod m \\ a_1\, a_2 &\equiv b_1\, b_2 \bmod m \\ {a_1}^n &\equiv {b_1}^n \bmod m \qquad\qquad \text{pour tout } n \in \mathbb{N} \end{aligned}$$

Calculs modulo un entier

Si a_1, a_2, b_1, b_2 sont des entiers, si $m \in \mathbb{N}^*$, et si

$$a_1 \equiv b_1 \mod m$$
$$a_2 \equiv b_2 \mod m$$

alors :

$$a_1 + a_2 \equiv b_1 + b_2 \mod m$$
$$a_1\, a_2 \equiv b_1\, b_2 \mod m$$
$${a_1}^n \equiv {b_1}^n \mod m \qquad \text{pour tout } n \in \mathbb{N}$$

De plus, si d divise a_1, b_1 et m, alors $\dfrac{a_1}{d} \equiv \dfrac{b_1}{d} \mod \dfrac{m}{d}$.

Nombres premiers

Définition (nombre premier)

On dit qu'un entier $n \in \mathbb{N}$ est premier lorsque l'ensemble de ses diviseurs est $\{1, n\}$.

Remarques :

- il existe une infinité de nombres premiers
- 1 n'est pas premier

Factorisation d'un entier

Soit a un entier positif.

On peut trouver des nombres premiers p_i tels que :

$$a = \prod_{i=1}^{k} p_i$$

unicité si (p_i) croissante

$$= \prod_{i=1}^{\ell} p_i^{\alpha_i} \text{ avec } \alpha_i \in \mathbb{N}^*$$

unicité si (p_i) strict. croissante

PGCD et PPCM – Définitions

Définition (PGCD)

Pour $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$, le plus grand entier $d \in \mathbb{N}^*$ divisant à la fois a et b est appelé Plus Grand Commun Diviseur de a et b.

On le note $d = \mathrm{pgcd}(a, b)$. ou $\mathrm{gcd}(a, b)$ ou $a \wedge b$

PGCD et PPCM – Définitions

Définition (PGCD)

Pour $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$, le plus grand entier $d \in \mathbb{N}^*$ divisant à la fois a et b est appelé Plus Grand Commun Diviseur de a et b.

On le note $d = \mathrm{pgcd}(a, b)$. ou $\gcd(a, b)$ ou $a \wedge b$

Définition (PPCM)

Pour $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$, le plus petit entier $m \in \mathbb{N}^*$ qui est multiple à la fois de a et b est appelé Plus Petit Commun Multiple de a et b.

On le note $m = \mathrm{ppcm}(a, b)$. ou $\mathrm{lcm}(a, b)$ ou $a \vee b$

PGCD et PPCM – Définitions

Définition (PGCD)

Pour $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$, le plus grand entier $d \in \mathbb{N}^*$ divisant à la fois a et b est appelé Plus Grand Commun Diviseur de a et b.

On le note $d = \text{pgcd}(a, b)$. ou $\text{gcd}(a, b)$ ou $a \wedge b$

Définition (PPCM)

Pour $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$, le plus petit entier $m \in \mathbb{N}^*$ qui est multiple à la fois de a et b est appelé Plus Petit Commun Multiple de a et b.

On le note $m = \text{ppcm}(a, b)$. ou $\text{lcm}(a, b)$ ou $a \vee b$

- $\text{pgcd}(a, b) = \text{pgcd}(b, a)$ et $\text{ppcm}(a, b) = \text{ppcm}(b, a)$
- $0 \leq \text{pgcd}(a, b) \leq \min(a, b) \leq \max(a, b) \leq \text{ppcm}(a, b)$
- $\text{pgcd}(a, 0) = a$ et $\text{ppcm}(a, 0) = 0$ par convention

PGCD et PPCM – Propriétés

Si $$a = \prod_{i=1}^{k} p_i^{\alpha_i} \qquad b = \prod_{i=1}^{k} p_i^{\beta_i}$$

$$a = 42 = 2^1 \times 3^1 \times 5^0 \times 7^1$$
$$b = 60 = 2^2 \times 3^1 \times 5^1 \times 7^0$$

avec

- p_i des nombres premiers distincts
- $\alpha_i \geq 0$ et $\beta_i \geq 0$

alors, on a :

$$\mathrm{pgcd}(a, b) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}$$

$$\mathrm{ppcm}(a, b) = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$$

PGCD et PPCM – Propriétés

Si $a = \prod_{i=1}^{k} p_i^{\alpha_i}$ $b = \prod_{i=1}^{k} p_i^{\beta_i}$

$a = 42 = 2^1 \times 3^1 \times 5^0 \times 7^1$
$b = 60 = 2^2 \times 3^1 \times 5^1 \times 7^0$

avec

- p_i des nombres premiers distincts
- $\alpha_i \geq 0$ et $\beta_i \geq 0$

alors, on a :

$$\text{pgcd}(a, b) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}$$

$$\text{pgcd}(42, 60) = 2^1 \times 3^1 \times 5^0 \times 7^0 = 6$$

$$\text{ppcm}(a, b) = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$$

$$\text{ppcm}(42, 60) = 2^2 \times 3^1 \times 5^1 \times 7^1 = 420$$

De plus :

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

PGCD – Algorithme d'Euclide – Idée

Soit a et b deux entiers positifs. gérer les signes à part

1. Si u, v et n sont des entiers, alors

$$\begin{cases} n \text{ divise } a \\ n \text{ divise } b \end{cases} \Rightarrow n \text{ divise } a\,u + b\,v$$

PGCD – Algorithme d'Euclide – Idée

Soit a et b deux entiers positifs. gérer les signes à part

1. Si u, v et n sont des entiers, alors

$$\begin{cases} n \text{ divise } a \\ n \text{ divise } b \end{cases} \Rightarrow n \text{ divise } a\,u + b\,v$$

2. Division euclidienne

   On a l'égalité $a = q\,b + r$ avec q et r entiers, et $0 \leq r < b$

PGCD – Algorithme d'Euclide – Idée

Soit a et b deux entiers positifs. gérer les signes à part

1. Si u, v et n sont des entiers, alors

$$\begin{cases} n \text{ divise } a \\ n \text{ divise } b \end{cases} \Rightarrow n \text{ divise } a\,u + b\,v$$

2. Division euclidienne

   On a l'égalité $a = q\,b + r$ avec q et r entiers, et $0 \leq r < b$

$$\begin{cases} \text{pgcd}(a, b) \text{ divise } a \\ \text{pgcd}(a, b) \text{ divise } b \end{cases} \Rightarrow \text{pgcd}(a, b) \text{ divise } r = a \times 1 + b \times (-q)$$

PGCD – Algorithme d'Euclide – Idée

Soit a et b deux entiers positifs. gérer les signes à part

1. Si u, v et n sont des entiers, alors

$$\begin{cases} n \text{ divise } a \\ n \text{ divise } b \end{cases} \Rightarrow n \text{ divise } a\,u + b\,v$$

2. Division euclidienne

   On a l'égalité $a = q\,b + r$ avec q et r entiers, et $0 \leq r < b$

$$\begin{cases} \text{pgcd}(a, b) \text{ divise } a \\ \text{pgcd}(a, b) \text{ divise } b \end{cases} \Rightarrow \text{pgcd}(a, b) \text{ divise } r = a \times 1 + b \times (-q)$$

$\leadsto$ approche récursive $\text{pgcd}(a, b) = \text{pgcd}(b, r)$

PGCD – Algorithme d'Euclide

Algorithme 1 : `pgcd`

Entrée : deux entiers positifs a et b
Sortie : PGCD de a et b

$r_0 \leftarrow a$
$r_1 \leftarrow b$
si $r_0 < r_1$ **alors** échanger r_0 et r_1 `// facultatif`
tant que $r_1 > 0$ **faire**
    Calculer q, r tels que $r_0 = q\,r_1 + r$ `// div. euclidienne`
    $r_0 \leftarrow r_1$
    $r_1 \leftarrow r$
retourner r_0

PGCD – Algorithme d'Euclide – Exemple

Calcul du PGCD de 42 et 60 :

PGCD – Algorithme d'Euclide – Exemple

Calcul du PGCD de 42 et 60 :

r_0	r_1	
42	60	$42 = 0 \times 60 + 42$
60	42	$60 = 1 \times 42 + 18$
42	18	$42 = 2 \times 18 + 6$
18	6	$18 = 3 \times 6 + 0$
6	0	

$\rightsquigarrow \mathrm{pgcd}(42, 60) = 6$

PGCD – Algorithme d'Euclide – Exemple

Calcul du PGCD de 42 et 60 :

r_0	r_1	
42	60	$42 = 0 \times 60 + 42$
60	42	$60 = 1 \times 42 + 18$
42	18	$42 = 2 \times 18 + 6$
18	6	$18 = 3 \times 6 + 0$
6	0	

$\rightsquigarrow \text{pgcd}(42, 60) = 6$

Résultat obtenu sans factoriser 42 et 60

Coefficients de Bezout

Théorème (Bezout)

Pour tout entier a et tout entier b, on peut trouver u et v entiers tels que

$$a\,u + b\,v = \operatorname{pgcd}(a, b).$$

On dit que u et v sont les coefficients de Bezout associés à a et b.

Remarques :

- calcul possible en adaptant l'algorithme d'Euclide
- plusieurs couples (u, v) conviennent

$$20 \times (-1) + 30 \times 1 = 10$$
$$20 \times 2 + 30 \times (-1) = 10$$

Algorithme d'Euclide étendu

Algorithme 2 : `pgcd_etendu`

Entrée : deux entiers positifs a et b
Sortie : g, u et v tels que $a\,u + b\,v = g = \mathrm{pgcd}(a, b)$

$$\begin{pmatrix} r_0 & u_0 & v_0 \\ r_1 & u_1 & v_1 \end{pmatrix} \leftarrow \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$$

si $r_0 < r_1$ **alors** échanger (r_0, u_0, v_0) et (r_1, u_1, v_1) `//facultatif`

tant que $r_1 > 0$ **faire**

Calculer q, r tels que $r_0 = q\,r_1 + r$ `// div. euclidienne`

$$\begin{pmatrix} r_0 & u_0 & v_0 \\ r_1 & u_1 & v_1 \end{pmatrix} \leftarrow \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} r_0 & u_0 & v_0 \\ r_1 & u_1 & v_1 \end{pmatrix}$$

retourner (r_0, u_0, v_0)

Algorithme d'Euclide étendu – Exemple

Calcul de coefficients de Bezout pour 42 et 60 :

Algorithme d'Euclide étendu – Exemple

Calcul de coefficients de Bezout pour 42 et 60 :

r	u	v		
42	1	0	L_1	
60	0	1	L_2	
42	1	0	$L_3 = L_1 - 0\, L_2$	$42 = 60 \times 0 + 42$
18	-1	1	$L_4 = L_2 - 1\, L_3$	$60 = 42 \times 1 + 18$
6	3	-2	$L_5 = L_3 - 2\, L_4$	$42 = 18 \times 2 + 6$
0	-10	7	$L_6 = L_4 - 3\, L_5$	$18 = 6 \times 3 + 0$

$\rightsquigarrow 42 \times 3 + 60 \times (-2) = 6$

Algorithme d'Euclide étendu – Exemple

Calcul de coefficients de Bezout pour 42 et 60 :

r	u	v		
42	1	0	L_1	
60	0	1	L_2	
42	1	0	$L_3 = L_1 - 0\,L_2$	$42 = 60 \times 0 + 42$
18	-1	1	$L_4 = L_2 - 1\,L_3$	$60 = 42 \times 1 + 18$
6	3	-2	$L_5 = L_3 - 2\,L_4$	$42 = 18 \times 2 + 6$
0	-10	7	$L_6 = L_4 - 3\,L_5$	$18 = 6 \times 3 + 0$

$\rightsquigarrow 42 \times 3 + 60 \times (-2) = 6$

À chaque étape, on peut vérifier que $r = 42\,u + 60\,v$.

Équations du type $a\,u + b\,v = c$

Méthode :

1. Trouver $g = \text{pgcd}(a, b)$ et des coefficients de Bezout (u, v)
$$a\,u + b\,v = g$$
2. Si g ne divise pas c, pas de solutions
Sinon, $c = g\,q$ et on multiplie tout par q :
$$a\,\underbrace{q\,u}_{u_0} + b\,\underbrace{q\,v}_{v_0} = c$$
3. Utiliser la solution particulière (u_0, v_0) pour trouver toutes les solutions

Équations du type $a\,u + b\,v = c$ – Exemple

Pour résoudre $42\,u + 60\,v = 12$:

1. On a vu que $\quad 42 \times 3 + 60 \times (-2) = 6$
2. Donc $\quad 42 \times 6 + 60 \times (-4) = 12 \qquad \times 2$

Équations du type $a\,u + b\,v = c$ – Exemple

Pour résoudre $42\,u + 60\,v = 12$:

1. On a vu que $42 \times 3 + 60 \times (-2) = 6$
2. Donc $42 \times 6 + 60 \times (-4) = 12$ $\times 2$
3. On a

$$\begin{array}{rlcl} & 42 \times u & + & 60 \times v = 12 \\ - & 42 \times 6 & + & 60 \times (-4) = 12 \\ \hline & 42 \times (u-6) & + & 60 \times (v+4) = 0 \end{array}$$

Équations du type $a\,u + b\,v = c$ – Exemple

Pour résoudre $42\,u + 60\,v = 12$:

1. On a vu que $\quad 42 \times 3 + 60 \times (-2) = 6$
2. Donc $\quad 42 \times 6 + 60 \times (-4) = 12 \qquad \times 2$
3. On a

$$\begin{array}{rlcl} & 42 \times u & + & 60 \times v = 12 \\ - & 42 \times 6 & + & 60 \times (-4) = 12 \\ \hline & 42 \times (u-6) & + & 60 \times (v+4) = 0 \end{array}$$

$$\begin{array}{rrcll} \text{D'où} & 42 \times (6-u) & = & 60 \times (v+4) & \\ & 7 \times (6-u) & = & 10 \times (v+4) & /\ \mathrm{pgcd}(42,60) \\ & v+4 & = & 7k \text{ avec } k \in \mathbb{Z} & \text{car } \mathrm{pgcd}(7,10) = 1 \\ & 7 \times (6-u) & = & 10 \times 7k & \text{substitution + simplification} \end{array}$$

$\rightsquigarrow$ Solutions = $\left\{(6-10k, 7k-4),\ k \in \mathbb{Z}\right\}$

Calcul d'inverse modulo n

Théorème

Pour tout $m \in \mathbb{N}^*$, si a est un entier tel que $\mathrm{pgcd}(a, m) = 1$, alors il existe un entier b tel que $a\,b \equiv 1 \mod m$.

On dit alors que b est un inverse de a modulo m.

Remarques :

- L'ensemble des inverses de a modulo m est de la forme $\{b_0 + k\,m\ ,\ k \in \mathbb{Z}\}$ où b_0 est un inverse quelconque.
- Si (u, v) sont les coefficients de Bezout associés à a et m
  - $a\,u + m\,v = 1$, d'où $a\,u = 1 + m \times (-v) \equiv 1 \mod m$
  - donc u est un inverse de a modulo m

Exemple : $25\,b \equiv 1 \mod 42 \;\Rightarrow$

Calcul d'inverse modulo n

Théorème

Pour tout $m \in \mathbb{N}^*$, si a est un entier tel que $\text{pgcd}(a, m) = 1$, alors il existe un entier b tel que $a\,b \equiv 1 \mod m$.

On dit alors que b est un inverse de a modulo m.

Remarques :

- L'ensemble des inverses de a modulo m est de la forme $\{b_0 + k\,m\ ,\ k \in \mathbb{Z}\}$ où b_0 est un inverse quelconque.
- Si (u, v) sont les coefficients de Bezout associés à a et m
  - $a\,u + m\,v = 1$, d'où $a\,u = 1 + m \times (-v) \equiv 1 \mod m$
  - donc u est un inverse de a modulo m

Exemple : $25\,b \equiv 1 \mod 42 \;\Rightarrow\; b \equiv -5 \equiv 37 \mod 42$

Théorème des restes chinois

Théorème (restes chinois)

Soit m_1 et m_2 deux entiers positifs tels que $\text{pgcd}(m_1, m_2) = 1$.

Si $\begin{cases} x \equiv y_1 \mod m_1 \\ x \equiv y_2 \mod m_2 \end{cases}$, alors $x \equiv y_1\, m_2\, v + y_2\, m_1\, u \mod (m_1\, m_2)$

où (u, v) sont les coefficients de Bezout associés à m_1 et m_2.

Exemple : $\begin{cases} x \equiv 4 \mod 42 \\ x \equiv 5 \mod 25 \end{cases}$

Comme $42 \times 3 + 25 \times (-5) = 1$, on a

Théorème des restes chinois

Théorème (restes chinois)

Soit m_1 et m_2 deux entiers positifs tels que $\mathrm{pgcd}(m_1, m_2) = 1$.

Si $\begin{cases} x \equiv y_1 \bmod m_1 \\ x \equiv y_2 \bmod m_2 \end{cases}$, alors $x \equiv y_1\, m_2\, v + y_2\, m_1\, u \bmod (m_1\, m_2)$

où (u, v) sont les coefficients de Bezout associés à m_1 et m_2.

Exemple : $\begin{cases} x \equiv 4 \bmod 42 \\ x \equiv 5 \bmod 25 \end{cases}$

$$130 = 42 \times 3 + 4$$
$$130 = 25 \times 5 + 5$$

Comme $42 \times 3 + 25 \times (-5) = 1$, on a

$$x \equiv 4 \times 25 \times (-5) + 5 \times 42 \times 3 \equiv 130 \bmod 1050$$

Théorème (division euclidienne)

Pour tout polynôme $A \in \mathbb{R}[X]$ et tout polynôme $B \in \mathbb{R}[X]$ non nul, il existe des polynômes Q et R de $\mathbb{R}[X]$ tels que :

1. $A(X) = B(X)\,Q(X) + R(X)$
2. $0 \leq \deg(R) < \deg(B)$.

Arithmétique pour les polynômes

Théorème (division euclidienne)

Pour tout polynôme $A \in \mathbb{R}[X]$ et tout polynôme $B \in \mathbb{R}[X]$ non nul, il existe des polynômes Q et R de $\mathbb{R}[X]$ tels que :

1. $A(X) = B(X)\,Q(X) + R(X)$
2. $0 \leq \deg(R) < \deg(B)$.

Remarques :

- si $R(X) = 0$, on dit que B divise A
- on peut aussi définir $\mathrm{pgcd}(P, Q)$
- l'algorithme d'Euclide étendu donne $\mathrm{pgcd}(P, Q)$ et des coefficients de Bezout pour P et Q