Mathématiques pour l'informatique 1

Division euclidienne et PGCD, Bases entières, Arithmétique modulaire

Émilie Charlier

Universitfé de Liège

19-26 octobre et 9-16 novembre 2021

Division euclidienne dans $\mathbb{N}$

- On ne peut diviser 30 par 7 de façon exacte.
- Division euclidienne : $30 = 4 \cdot 7 + 2$.
- 4 est appelé le quotient de la division euclidienne de 30 par 7.
- 2 est appelé le reste de la division euclidienne de 30 par 7.
- Ce quotient et ce reste sont uniques : on ne peut pas écrire $30 = q \cdot 7 + \cdot r$ pour d'autres entiers q et r tels que $0 \leq r < 7$.

Quelques divisions euclidiennes dans $\mathbb{Z}$

Division euclidienne de

- 30 par 7 : $30 = 4 \cdot 7 + 2$.
- 30 par -7 :

Quelques divisions euclidiennes dans $\mathbb{Z}$

Division euclidienne de

- 30 par 7 : $30 = 4 \cdot 7 + 2.$
- 30 par -7 : $30 = (-4) \cdot (-7) + 2.$

Quelques divisions euclidiennes dans $\mathbb{Z}$

Division euclidienne de

- 30 par 7 : $30 = 4 \cdot 7 + 2$.
- 30 par -7 : $30 = (-4) \cdot (-7) + 2$.
- -30 par 7 :

Quelques divisions euclidiennes dans $\mathbb{Z}$

Division euclidienne de

- 30 par 7 : $30 = 4 \cdot 7 + 2$.
- 30 par -7 : $30 = (-4) \cdot (-7) + 2$.
- -30 par 7 : $-30 = (-5) \cdot 7 + 5$.

Quelques divisions euclidiennes dans $\mathbb{Z}$

Division euclidienne de

- 30 par 7 : $30 = 4 \cdot 7 + 2$.
- 30 par -7 : $30 = (-4) \cdot (-7) + 2$.
- -30 par 7 : $-30 = (-5) \cdot 7 + 5$.
- -30 par -7 :

Quelques divisions euclidiennes dans $\mathbb{Z}$

Division euclidienne de

- 30 par 7 : $30 = 4 \cdot 7 + 2$.
- 30 par -7 : $30 = (-4) \cdot (-7) + 2$.
- -30 par 7 : $-30 = (-5) \cdot 7 + 5$.
- -30 par -7 : $-30 = 5 \cdot (-7) + 5$.

Théorème (Division euclidienne)

Soient $n \in \mathbb{Z}$ et $d \in \mathbb{Z}_0$. Alors n se décompose de façon unique sous la forme

$$n = qd + r, \text{ avec } q \in \mathbb{Z} \text{ et } r \in \{0, \ldots, |d| - 1\}.$$

Autrement dit, il existe un unique couple d'entiers (q, r) tels que $n = qd + r$ et $0 \leq r < |d|$.

Existence de tels q et r

Démonstration

Montrons tout d'abord l'existence d'une telle décomposition.

La suite $(k|d|)_{k\in\mathbb{Z}}$ est strictement croissante puisque pour tout $k \in \mathbb{Z}$, $(k+1)|d| - k|d| = |d| > 0$.

Il existe donc $k \in \mathbb{Z}$ tel que $k|d| \leq n < (k+1)|d|$.

On vérifie facilement que

$$r = n - k|d| \quad \text{et} \quad q = \begin{cases} k & \text{si } d > 0 \\ -k & \text{si } d < 0. \end{cases}$$

conviennent pour la thèse.

En effet, on a bien $0 \leq r < |d|$.

De plus, si $d > 0$, alors $n = k|d| + r = kd + r = qd + r$,
et si $d < 0$, alors $n = k|d| + r = -kd + r = qd + r$.

Unicité de tels q et r

Montrons maintenant l'unicité de la décomposition.

Supposons que $n = qd + r = q'd + r'$, avec $q, r, q', r' \in \mathbb{Z}$, $0 \leq r < |d|$ et $0 \leq r' < |d|$.

Alors on a $(q - q')d = r' - r$.

On a donc $0 \leq |q - q'||d| = |(q - q')d| = |r' - r| < |d|$.

En divisant par $|d|$, on obtient $0 \leq |q - q'| < 1$.

Puisque $|q - q'|$ est un entier, cela entraîne que $|q - q'| = 0$.

Ceci démontre que $q = q'$, et par conséquent, que $r = r'$. □

Les notations des théorèmes précédents n'ont pas été choisies au hasard puisque d est appelé le diviseur, q le quotient et r le reste de la division euclidienne de n par d.

Definition

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}_0$. On note

- $\mathrm{DIV}(a, b)$ le quotient de la division euclidienne de a par b
- $\mathrm{MOD}(a, b)$ le reste de la division euclidienne de a par b.

Algorithme d'Euclide

La division euclidienne porte son nom en raison de l'algorithme d'Euclide qui permet de calculer le PGCD (plus grand commun diviseur) de deux naturels.

En effet, cet algorithme, datant d'environ 300 avant J.C., calcule le PGCD en réalisant des divisions euclidiennes successives, jusqu'à arriver à une condition d'arrêt.

Algorithme d'Euclide

Require: $a, b \in \mathbb{N}_0$
Ensure: $\mathrm{pgcd}(a, b)$
  $r \leftarrow \max(a, b)$, $s \leftarrow \min(a, b)$
  while $s > 0$ **do**
    $(r, s) \leftarrow (s, \mathrm{MOD}(r, s))$
  end while
  return r

Exemple

Calculons le PGCD de 1078 et de 322 à l'aide de l'algorithme d'Euclide.

Initialisation : $(r, s) \leftarrow (1078, 322)$.

On calcule successivement les divisions euclidiennes suivantes :

$$\begin{aligned} 1078 &= 3 \cdot 322 + 112 & (r, s) &\leftarrow (322, 112) \\ 322 &= 2 \cdot 112 + 98 & (r, s) &\leftarrow (112, 98) \\ 112 &= 1 \cdot 98 + 14 & (r, s) &\leftarrow (98, 14) \\ 98 &= 7 \cdot 14 + 0 & (r, s) &\leftarrow (14, 0). \end{aligned}$$

La sortie de l'algorithme est le dernier reste non nul de cette suite de divisions euclidiennes, soit 14.

Théorème

L'algorithme d'Euclide est correct et se termine toujours.

Démonstration

1/ L'algorithme d'Euclide se termine toujours.

En effet, la variable s contient toujours un nombre naturel et à chaque étape de la boucle, la valeur de s décroît strictement puisque $\mathrm{MOD}(r, s) < s$.

La condition de la boucle ($s > 0$) finira donc par être violée et l'algorithme se terminera.

2/ L'algorithme d'Euclide est correct.

Détaillons les divisions euclidiennes successives de l'algorithme d'Euclide (en supposant que $a \geq b$) :

$$\begin{aligned}
a &= q_1 \cdot b + r_1 && \text{étape 1} \\
b &= q_2 \cdot r_1 + r_2 && \text{étape 2} \\
r_1 &= q_3 \cdot r_2 + r_3 && \text{étape 3} \\
r_2 &= q_4 \cdot r_3 + r_4 && \text{étape 4} \\
&\vdots \\
r_{j-2} &= q_j \cdot r_{j-1} + r_j && \text{étape j} \\
r_{j-1} &= q_{j+1} \cdot r_j + 0 && \text{étape j+1}
\end{aligned}$$

où les q_i et r_i sont les quotient et reste de la division euclidienne de l'étape i (où $1 \leq i \leq j+1$), avec $r_1, \ldots, r_j$ non nuls.

On pose $r_{-1} = a$ et $r_0 = b$.

La sortie de l'algorithme est le dernier reste non nul, soit r_j.

Pour montrer que l'algorithme d'Euclide est correct, nous devons démontrer que $r_j = \mathrm{pgcd}(a, b)$.

Pour cela, on doit montrer deux choses :

i) que r_j est un diviseur de a et de b

ii) que r_j est plus grand que tous les autres diviseurs de a et de b.

Montrons i). Ceci s'obtient de proche en proche, en remontant les égalités.

- La dernière égalité montre que r_j divise r_{j-1}.
- L'avant-dernière égalité montre que r_j divise r_{j-2}.
- Successivement, on obtient que r_j divise $r_{j-3}, \ldots, r_1, r_0 = b$ et enfin $r_{-1} = a$.

Montrons ii). Supposons à présent que d soit un diviseur commun de a et de b. Ici, on va descendre les égalités.

- De la première égalité, on obtient que d divise $r_1 = a - q_1 \cdot b$.
- De la deuxième égalité, on obtient que d divise $r_2 = b - q_2 \cdot r_1$.
- En continuant de proche en proche vers le bas jusque l'avant-dernière égalité, on obtient que d divise r_j.

On a donc bien $r_j \geq d$. □

Coefficients de Bézout

Théorème de Bachet-Bézout

Pour tous $a, b \in \mathbb{N}_0$, il existe $m, n \in \mathbb{Z}$ tels que

$$ma + nb = \mathrm{pgcd}(a, b).$$

Démonstration

On garde les mêmes notations que précédemment.

Il suffit d'observer que l'on peut exprimer chaque r_i (avec $-1 \leq i \leq j$) sous la forme $r_i = m_i a + n_i b$ où $m_i, n_i \in \mathbb{Z}$.

En effet, puisque le PGCD de a et b est donné par r_j, les entiers $m = m_j$ et $n = n_j$ conviendront pour la thèse.

Parenthèse (utile pour comprendre, mais inutile dans la démonstration)

Calculs des trois premières étapes :

- $r_1 = a - q_1 b$
- $\begin{aligned} r_2 &= b - q_2 r_1 \\ &= b - q_2(a - q_1 b) \\ &= -q_2 a + (1 + q_1 q_2) b \end{aligned}$
- $\begin{aligned} r_3 &= r_1 - q_3 r_2 \\ &= a - q_1 b - q_3(-q_2 a + (1 + q_1 q_2) b) \\ &= (1 + q_2 q_3) a + (-q_1 - q_3 - q_1 q_2 q_3) b \end{aligned}$

Retour à la démonstration

Formellement, on montre ceci par une récurrence d'ordre 2 sur $i \geq -1$.

Cas de base ($i = -1$ et $i = 0$) : on a $r_{-1} = a = 1 \cdot a + 0 \cdot b$ et $r_0 = b = 0 \cdot a + 1 \cdot b$.

Supposons maintenant que i soit tel que $1 \leq i \leq j$, et qu'il existe $m_{i-2}, n_{i-2}, m_{i-1}, n_{i-1} \in \mathbb{Z}$ tels que

$$r_{i-2} = m_{i-2}a + n_{i-2}b \qquad \text{et} \qquad r_{i-1} = m_{i-1}a + n_{i-1}b.$$

Alors on calcule

$$\begin{aligned} r_i &= r_{i-2} - q_i r_{i-1} \\ &= m_{i-2}a + n_{i-2}b - q_i(m_{i-1}a + n_{i-1}b) \\ &= (m_{i-2} - q_i m_{i-1})a + (n_{i-2} - q_i n_{i-1})b. \end{aligned}$$

Ainsi les entiers $m_i = m_{i-2} - q_i m_{i-1}$ et $n_i = n_{i-2} - q_i n_{i-1}$ sont tels que $r_i = m_i a + n_i b$. □

Coefficients de Bézout pas uniques

L'égalité $ma + nb = \mathrm{pgcd}(a, b)$ implique que pour tout $k \in \mathbb{Z}$, on a aussi

$$(m + kb)a + (n - ka)b = \mathrm{pgcd}(a, b).$$

Exemple

Continuons l'exemple précédent pour obtenir des entiers m et n tels $m \cdot 1078 + n \cdot 322 = 14$.

On calcule successivement :

$$\begin{aligned} 14 &= 112 - 98 \\ &= 112 - (322 - 2 \cdot 112) \\ &= 3 \cdot 112 - 322 \\ &= 3 \cdot (1078 - 3 \cdot 322) - 322 \\ &= 3 \cdot 1078 - 10 \cdot 322. \end{aligned}$$

On appelle algorithme d'Euclide étendu l'algorithme décrit dans la preuve du théorème de Bachet-Bézout qui permet d'obtenir le PGCD de deux naturels a et b non nuls ainsi que des coefficients de Bézout, c'est-à-dire des entiers m et n tels que $ma + nb = \mathrm{pgcd}(a, b)$.

Exercice

Modifier l'algorithme d'Euclide pour obtenir l'algorithme d'Euclide étendu. La sortie attendue est le triplet de nombres $(\mathrm{pgcd}(a, b), m, n)$.

Théorème de Bézout

Definition

Deux naturels sont premiers entre eux lorsque leur PGCD vaut 1.

Théorème de Bézout

Deux naturels non nuls a et b sont premiers entre eux si et seulement s'il existe des entiers m et n tels que $ma + nb = 1$.

Démonstration.

Soient $a, b \in \mathbb{N}_0$.

Si $\mathrm{pgcd}(a, b) = 1$, alors par le théorème de Bachet-Bézout, il existe des entiers m et n tels que $ma + nb = 1$.

Inversement, supposons qu'il existe $m, n \in \mathbb{Z}$ tels que $ma + nb = 1$.

Comme $\mathrm{pgcd}(a, b)$ divise à la fois a et b, on obtient de cette égalité que $\mathrm{pgcd}(a, b)$ divise 1, ce qui implique que $\mathrm{pgcd}(a, b) = 1$. □

Lemmes de Gauss et d'Euclide

Lemme de Gauss

Si a, b, c sont des naturels non nuls tels que c divise ab et $\mathrm{pgcd}(a, c) = 1$, alors c divise b.

Démonstration.

Soient $a, b, c \in \mathbb{N}_0$ tels que c divise ab et $\mathrm{pgcd}(a, c) = 1$.

D'une part, il existe $q \in \mathbb{N}_0$ tel que $ab = qc$.

D'autre part, par le théorème de Bézout, il existe $m, n \in \mathbb{Z}$ tels que $ma + nc = 1$.

On obtient que

$$b = (ma + nc)b = mab + ncb = mqc + ncb = (mq + nb)c,$$

ce qui montre que c divise b. □

Lemme d'Euclide

Soient a et b des naturels non nuls. Si un nombre premier p divise ab, alors p divise a ou b.

Démonstration.

Il s'agit de la démonstration d'une alternative.

Soit p un nombre premier divisant ab mais ne divisant pas a.

Alors $\mathrm{pgcd}(a, p) = 1$.

Par le lemme de Gauss, on obtient que p divise b. □

Numération en bases entières

L'algorithme suivant permet d'obtenir une suite de nombres

$$(c_\ell, c_{\ell-1}, \ldots, c_0)$$

telle que

$$n = \sum_{i=0}^{\ell} c_i \, b^i.$$

Nous montrerons ensuite que, en ajoutant certaines contraintes sur les coefficients c_i, cette décomposition est unique.

Ceci nous permettra de définir les représentations des entiers en base b.

Exemples de représentations en bases 2, 3 et 10

$b = 10$	$b = 2$	$b = 3$	$b = 10$	$b = 2$	$b = 3$
1	1	1	11	1011	102
2	10	2	12	1100	110
3	11	10	13	1101	111
4	100	11	14	1110	112
5	101	12	15	1111	120
6	110	20	16	10000	121
7	111	21	17	10001	122
8	1000	22	18	10010	200
9	1001	100	19	10011	201
10	1010	101	20	10100	202

Algorithme glouton de décomposition en base b

Require: $n, b \in \mathbb{N}_0$ avec $b \geq 2$
Ensure: $(c_\ell, \ldots, c_0)$ tel que
1. $n = \sum_{i=0}^{\ell} c_i \, b^i$
2. $c_\ell \neq 0$
3. pour tout $i \in \{0, \ldots, \ell\}$, $c_i \in \{0, \ldots, b-1\}$.

$i \leftarrow \lfloor \log_b(n) \rfloor$, $r \leftarrow n$, ListeChiffres $\leftarrow ()$
while $i \geq 0$ **do**
  $r \leftarrow \mathrm{MOD}(r, b^i)$
  ListeChiffres $\leftarrow$ (ListeChiffres, $\mathrm{DIV}(r, b^i)$)
  $i \leftarrow i - 1$
end while
return ListeChiffres

Action de l'algorithme glouton sur l'entrée $n = 177$ en base $b = 2$

Puisque $2^7 = 128 \leq 177 < 2^8 = 256$, on a $\lfloor \log_2(177) \rfloor = 7$.

Initialisation : $i \leftarrow 7,\ r \leftarrow 177$, ListeChiffres $\leftarrow ()$

Boucle :

$$
\begin{aligned}
177 &= 1 \cdot 128 + 49 && r \leftarrow 49,\ \text{ListeChiffres} \leftarrow (1),\ i \leftarrow 6 \\
49 &= 0 \cdot 64 + 49 && r \leftarrow 49,\ \text{ListeChiffres} \leftarrow (1,0),\ i \leftarrow 5 \\
49 &= 1 \cdot 32 + 17 && r \leftarrow 17,\ \text{ListeChiffres} \leftarrow (1,0,1),\ i \leftarrow 4 \\
17 &= 1 \cdot 16 + 1 && r \leftarrow 1,\ \text{ListeChiffres} \leftarrow (1,0,1,1),\ i \leftarrow 3 \\
1 &= 0 \cdot 8 + 1 && r \leftarrow 1,\ \text{ListeChiffres} \leftarrow (1,0,1,1,0),\ i \leftarrow 2 \\
1 &= 0 \cdot 4 + 1 && r \leftarrow 1,\ \text{ListeChiffres} \leftarrow (1,0,1,1,0,0),\ i \leftarrow 1 \\
1 &= 0 \cdot 2 + 1 && r \leftarrow 1,\ \text{ListeChiffres} \leftarrow (1,0,1,1,0,0,0),\ i \leftarrow 0 \\
1 &= 1 \cdot 1 + 0 && r \leftarrow 0,\ \text{ListeChiffres} \leftarrow (1,0,1,1,0,0,0,1),\ i \leftarrow -1.
\end{aligned}
$$

Sortie : $(1,0,1,1,0,0,0,1)$.

Action de l'algorithme glouton sur l'entrée $n = 177$ en bases $b = 3$

Puisque $3^4 = 81 \leq 177 < 3^5 = 243$, on a $\lfloor \log_3(177) \rfloor = 4$.

Initialisation : $i \leftarrow 4,\ r \leftarrow 177$, ListeChiffres $\leftarrow ()$

Boucle :

$$
\begin{aligned}
177 &= 2 \cdot 81 + 15 && r \leftarrow 15,\ \text{ListeChiffres} \leftarrow (2),\ i \leftarrow 3 \\
15 &= 0 \cdot 27 + 15 && r \leftarrow 15,\ \text{ListeChiffres} \leftarrow (2,0),\ i \leftarrow 2 \\
15 &= 1 \cdot 9 + 6 && r \leftarrow 6,\ \text{ListeChiffres} \leftarrow (2,0,1),\ i \leftarrow 1 \\
6 &= 2 \cdot 3 + 0 && r \leftarrow 0,\ \text{ListeChiffres} \leftarrow (2,0,1,2),\ i \leftarrow 0 \\
0 &= 0 \cdot 1 + 0 && r \leftarrow 0,\ \text{ListeChiffres} \leftarrow (2,0,1,2,0),\ i \leftarrow -1
\end{aligned}
$$

Sortie : $(2,0,1,2,0)$.

Théorème

Soit b un entier ≥ 2. L'algorithme glouton de décomposition en base b est correct et se termine toujours.

Démonstration

1) L'algorithme se termine toujours.

En effet, la variable i est initialisée à $\lfloor \log_b(n) \rfloor$ et diminue d'une unité à chaque étape de la boucle.

La condition $i \geq 0$ sera donc violée après exactement $\lfloor \log_b(n) \rfloor + 1$ étapes.

2) L'algorithme est correct.

Détaillons les divisions euclidiennes successives de l'algorithme glouton.

Soit $\ell = \lfloor \log_b(n) \rfloor$ et $r_\ell = n$.

On a successivement

$$\begin{aligned} r_\ell &= c_\ell \cdot b^\ell + r_{\ell-1} \\ r_{\ell-1} &= c_{\ell-1} \cdot b^{\ell-1} + r_{\ell-2} \\ r_{\ell-2} &= c_{\ell-2} \cdot b^{\ell-2} + r_{\ell-3} \\ &\vdots \\ r_1 &= c_1 \cdot b^1 + r_0 \\ r_0 &= c_0 \cdot b^0 + 0 \end{aligned}$$

où les c_i et r_{i-1} sont les quotient et reste de la division euclidienne de l'étape $\ell - i + 1$ (où $0 \leq i \leq \ell$).

La sortie de l'algorithme est la suite des chiffres $(c_\ell, c_{\ell-1}, \ldots, c_1, c_0)$.

Pour montrer que l'algorithme est correct, nous devons démontrer que

$$n = \sum_{i=0}^{\ell} c_i \, b^i, \quad c_\ell \neq 0 \quad \text{et} \quad \forall i \in \{0, \ldots, \ell\}, \; c_i \in \{0, \ldots, b-1\}.$$

En descendant toutes les égalités, nous obtenons successivement

$$\begin{aligned} r_\ell &= c_\ell b^\ell + r_{\ell-1} \\ &= c_\ell b^\ell + c_{\ell-1} b^{\ell-1} + r_{\ell-2} \\ &\vdots \\ &= c_\ell b^\ell + c_{\ell-1} b^{\ell-1} + c_{\ell-2} b^{\ell-2} + \cdots + c_1 b + r_0 \\ &= c_\ell b^\ell + c_{\ell-1} b^{\ell-1} + c_{\ell-2} b^{\ell-2} + \cdots + c_1 b + c_0. \end{aligned}$$

Puisque $\ell = \lfloor \log_b(n) \rfloor$, nous avons

$$b^\ell \leq n < b^{\ell+1}$$

et donc

$$1 \leq c_\ell = \mathrm{DIV}(n, b^\ell) < b.$$

De plus, pour tout $i \in \{0, \ldots, \ell - 1\}$, nous avons

$$r_i = \mathrm{MOD}(r_{i+1}, b^{i+1}) < b^{i+1},$$

et donc

$$c_i = \mathrm{DIV}(r_i, b^i) < b.$$

Ainsi, tous les coefficients c_i sont compris entre 0 et $b - 1$ et $c_\ell \neq 0$. □

Définition

Les chiffres de la base b sont $0, \ldots, b-1$.

La représentation de n en base b est la suite de chiffres $(c_\ell, c_{\ell-1}, \ldots, c_1, c_0)$ produits par l'algorithme glouton.

Quand il n'y a pas d'ambiguïté, on écrit simplement $c_\ell \cdots c_0$.

Remarque

En base 10, on retrouve bien nos 10 chiffres $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$.

En base 2, seuls deux chiffres sont autorisés : 0 et 1.

Proposition

Soit $n, b \in \mathbb{N}_0$ avec $b \geq 2$. Le nombre de chiffres de la représentation de n en base b est égal à $\lfloor \log_b(n) \rfloor + 1$.

Démonstration.

Ceci découle de l'algorithme glouton. □

Si l'on impose que les coefficients c_i soient compris entre 0 et $b-1$ et que de plus le coefficient c_ℓ de b^ℓ soit différent de 0, alors la décomposition en base entière fournie par l'algorithme glouton est en fait la seule possible.

C'est l'objet du théorème suivant.

Théorème de décomposition en base entière

Soit b un naturel ≥ 2. Tout nombre $n \in \mathbb{N}_0$ se décompose de façon unique sous la forme

$$n = \sum_{i=0}^{\ell} c_i\, b^i, \quad \text{avec} \quad c_\ell \neq 0 \quad \text{et} \quad \forall i \in \{0, \ldots, \ell\},\ c_i \in \{0, \ldots, b-1\}.$$

Démonstration de l'existence

L'existence de la décomposition est donnée par l'algorithme glouton.

Démonstration de l'unicité

Supposons que $n = \sum_{i=0}^{\ell} c_i\, b^i$, où les chiffres c_i vérifient les conditions de l'énoncé. Il suffit de montrer que chaque c_i est univoquement déterminé par n et b. Nous procédons par récurrence sur n.

Si $n < b$, on doit avoir $\ell = 0$ et donc $c_0 = n$.

Supposons maintenant que $n \geq b$ et que l'unicité de la décomposition est vérifiée pour tout entier m tel que $1 \leq m < n$.

On a $\ell \geq 1$ et on peut donc écrire

$$n = \left(\sum_{i=1}^{\ell} c_i \, b^{i-1} \right) b + c_0.$$

Comme $c_0 \in \{0, \ldots, b-1\}$, nous obtenons que

$$c_0 = \mathrm{MOD}(n, b) \quad \text{et} \quad \sum_{i=1}^{\ell} c_i \, b^{i-1} = \mathrm{DIV}(n, b).$$

Considérons $m = \mathrm{DIV}(n, b) = c_\ell \, b^{\ell-1} + \cdots + c_2 b + c_1$.

Comme $b \geq 2$, on a $m < n$ et par hypothèse de récurrence, on obtient que les coefficients $c_\ell, \ldots, c_2, c_1$ sont univoquement déterminés par m et b, et donc par n et b (puisque n et b déterminent m). □

Remarque

On aurait pu également utiliser l'algorithme glouton pour démontrer l'unicité de la décomposition en base entière, en montrant successivement que les coefficients c_ℓ, puis $c_{\ell-1}, \cdots, c_0$ étaient univoquement déterminés par n et b.

La démonstration n'aurait pas été plus ou moins difficile.

Celle que nous avons présentée ci-dessus a l'avantage de mettre en lumière un deuxième algorithme de décomposition.

Exercice

Adapter la preuve de l'unicité de la décomposition en base entière présentée ci-dessus pour obtenir un algorithme de décomposition qui produit les chiffres de la représentation de n en base b de droite à gauche, c'est-à-dire dans l'ordre $(c_0, c_1, \ldots, c_\ell)$.

Exercice

Montrer l'unicité de la décomposition en base entière en utilisant l'algorithme glouton.

Arithmétique modulaire

Definition

Pour tout naturel $m \geq 2$, nous notons $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$. Nous définissons deux opérations binaires sur cet ensemble, appelée addition modulo m et multiplication modulo m :

$$+_m \colon \mathbb{Z}_m \times \mathbb{Z}_m, (i, j) \mapsto \mathrm{MOD}(i + j, m)$$

et

$$\cdot_m \colon \mathbb{Z}_m \times \mathbb{Z}_m, (i, j) \mapsto \mathrm{MOD}(i \cdot j, m).$$

Autrement dit, pour tous $i, j \in \mathbb{Z}_m$, on a

$$i +_m j = \mathrm{MOD}(i + j, m) \quad \text{et} \quad i \cdot_m j = \mathrm{MOD}(ij, m).$$

Tables d'addition et de multiplication dans $\mathbb{Z}_5$ et $\mathbb{Z}_6$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Dans la suite de cette section, m désigne toujours un entier ≥ 2.

Faire des calculs dans $\mathbb{Z}_m$ peut rapidement s'avérer fastidieux si l'on ne remarque pas qu'il revient au même d'effectuer les calculs dans $\mathbb{Z}$ et de "réduire modulo m" à la fin (ou à n'importe quel moment qui nous arrange d'ailleurs). Ceci est l'objet du résultat pratique suivant.

Proposition

Soient $x, y, k \in \mathbb{Z}$. Alors

1. $\mathrm{MOD}(x, m) = \mathrm{MOD}(y, m) \iff x - y$ est multiple de m.
2. $\mathrm{MOD}(x + km, m) = \mathrm{MOD}(x, m)$.
3. $\mathrm{MOD}(x + y, m) = \mathrm{MOD}(\mathrm{MOD}(x, m) + y, m)$
4. $\mathrm{MOD}(x \cdot y, m) = \mathrm{MOD}(\mathrm{MOD}(x, m) \cdot y, m)$

Démonstration

Supposons que

$$x = qm + r \quad \text{et} \quad y = q'm + r',$$

avec $q, q' \in \mathbb{Z}$ et $r, r' \in \mathbb{Z}_m$.

On a donc

$$r = \mathrm{MOD}(x, m) \quad \text{et} \quad r' = \mathrm{MOD}(y, m).$$

Démonstration

Supposons que

$$x = qm + r \quad \text{et} \quad y = q'm + r',$$

avec $q, q' \in \mathbb{Z}$ et $r, r' \in \mathbb{Z}_m$.

On a donc

$$r = \mathrm{MOD}(x, m) \quad \text{et} \quad r' = \mathrm{MOD}(y, m).$$

1. $\mathrm{MOD}(x, m) = \mathrm{MOD}(y, m) \iff x - y$ est multiple de m.

On a $x - y = (q - q')m + r - r'$.

Comme $|r - r'| < m$, on obtient que $x - y$ est multiple de m si et seulement si $r - r' = 0$.

Démonstration

Supposons que

$$x = qm + r \quad \text{et} \quad y = q'm + r',$$

avec $q, q' \in \mathbb{Z}$ et $r, r' \in \mathbb{Z}_m$.

On a donc

$$r = \mathrm{MOD}(x, m) \quad \text{et} \quad r' = \mathrm{MOD}(y, m).$$

1. $\mathrm{MOD}(x, m) = \mathrm{MOD}(y, m) \iff x - y$ est multiple de m.

On a $x - y = (q - q')m + r - r'$.

Comme $|r - r'| < m$, on obtient que $x - y$ est multiple de m si et seulement si $r - r' = 0$.

2. $\mathrm{MOD}(x + km, m) = \mathrm{MOD}(x, m)$.

Le point 2 découle directement du point 1.

3. $\mathrm{MOD}(x+y,m) = \mathrm{MOD}(\mathrm{MOD}(x,m)+y,m)$
4. $\mathrm{MOD}(x\cdot y,m) = \mathrm{MOD}(\mathrm{MOD}(x,m)\cdot y,m)$

On a

$$x+y = qm+r+y \quad \text{et} \quad xy = qmy+ry.$$

En utilisant le point 2, on obtient

$$\mathrm{MOD}(x+y,m) = \mathrm{MOD}(r+y,m) \quad \text{et} \quad \mathrm{MOD}(xy,m) = \mathrm{MOD}(ry,m),$$

comme souhaité. □

Ce résultat implique que toute égalité dans $\mathbb{Z}$ est aussi vérifiée "modulo m".

Par exemple, l'égalité $27 = 2 \cdot 8 + 11$ donne

- $1 = 0 \cdot_2 0 +_2 1$ dans $\mathbb{Z}_2$
- $0 = 2 \cdot_3 2 +_3 2$ dans $\mathbb{Z}_3$
- $3 = 2 \cdot_4 0 +_4 3$ dans $\mathbb{Z}_4$
- $2 = 2 \cdot_5 3 +_5 1$ dans $\mathbb{Z}_5$
- etc.

Propriétés de l'addition et la multiplication modulaires

Proposition

Pour tout $i, j, k \in \mathbb{Z}_m$, nous avons

1.	$(i +_m j) +_m k = i +_m (j +_m k)$	associativité de $+_m$
2.	$(i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k)$	associativité de $\cdot_m$
3.	$i \cdot_m (j +_m k) = i \cdot_m j \ +_m \ i \cdot_m k$	distributivité de $\cdot_m$ sur $+_m$
4.	$i +_m j = j +_m i$	commutativité de $+_m$
5.	$i \cdot_m j = j \cdot_m i$	commutativité de $\cdot_m$
6.	$0 +_m i = i +_m 0 = i$	0 est neutre pour $+_m$
7.	$1 \cdot_m i = i \cdot_m 1 = i$	1 est neutre pour $\cdot_m$
8.	$i +_m (m - i) = 0$ si $i \neq 0$	l'opposé de $i \neq 0$ est $m - i$

Démonstration

Laissée en exercice.

Remarques

- L'associativité permet de donner du sens aux écritures

$$i +_m j +_m k \quad \text{et} \quad i \cdot_m j \cdot_m k$$

puisque l'ordre dans lequel on effectue ces opérations n'a pas d'importance.

- L'addition par un élément de $\mathbb{Z}_m$ est injective :

$$i +_m j = i +_m k \implies j = k.$$

- On ne peut pas définir un ordre $<$ de $\mathbb{Z}_m$ tel que

$$x < y \implies x + z < y + z.$$

Nous avons facilement identifié les opposés des éléments de $\mathbb{Z}_m$: l'opposé d'un élément i de $\mathbb{Z}_m$ est simplement $m - i$ si $i \neq 0$ et 0 sinon.

Déterminer les inverses est par contre plus délicat.

Lemme

Soient $i, j, j' \in \mathbb{Z}_m$. Alors $i \cdot_m j = i \cdot_m j' = 1 \implies j = j'$.

Démonstration.

Supposons que $i \cdot_m j = i \cdot_m j' = 1$.

En utilisant la proposition précédente, on en déduit que

$$\begin{aligned} j &= j \cdot_m 1 \\ &= j \cdot_m (i \cdot_m j') \\ &= (j \cdot_m i) \cdot_m j' \\ &= (i \cdot_m j) \cdot_m j' \\ &= 1 \cdot_m j' \\ &= j'. \end{aligned}$$

Le lemme précédent nous dit que si un élément possède un inverse, alors celui-ci est unique.

Definition

Un élément i de $\mathbb{Z}_m$ est inversible modulo m s'il existe j dans $\mathbb{Z}_m$ tel que $i \cdot_m j = 1$.

Au vu du lemme précédent, il ne peut exister qu'un seul tel élément j et lorsqu'il existe, celui-ci est appelé l'inverse de i modulo m.

On dit aussi que i est un élément inversible de $\mathbb{Z}_m$.

Exemples

- Dans le cas de $\mathbb{Z}_6$, seuls 1 et 5 sont inversibles modulo 6.

  On vérifie en effet que dans la table de multiplication modulo 6, les lignes correspondants aux éléments 0, 2, 3 et 4 ne contiennent pas l'élément 1, mais que 1 apparaît bien dans les lignes correspondants à 1 et 5.

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- Dans le cas de $\mathbb{Z}_5$, toutes les lignes de la table de multiplication modulo 5, excepté celle de 0, contient 1.

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Ceci montre que tous les éléments non nuls de $\mathbb{Z}_5$ sont inversibles.

Caractérisation des éléments inversibles de $\mathbb{Z}_m$

Théorème

Un élément i de $\mathbb{Z}_m$ est inversible modulo m si et seulement si i et m sont premiers entre eux.

Démonstration.

Soit i un élément inversible de $\mathbb{Z}_m$.

Alors il existe $j \in \mathbb{Z}_m$ tel que $i \cdot_m j = 1$, càd tel que $\mathrm{MOD}(ij, m) = 1$.

Il existe donc $q \in \mathbb{N}$ tel que $ij = qm + 1$, et donc tel que $ij - qm = 1$.

Par le théorème de Bézout, i et m sont premiers entre eux.

Réciproquement, soit i un élément de $\mathbb{Z}_m$ premier avec m.

Par le théorème de Bézout, il existe $a, b \in \mathbb{Z}$ tels que $ai + bm = 1$.

On obtient que $\mathrm{MOD}(a, m) \cdot_m i = \mathrm{MOD}(ai, m) = \mathrm{MOD}(1 - bm, m) = 1$.

L'élément $\mathrm{MOD}(a, m)$ est donc l'inverse de i dans $\mathbb{Z}_m$. □

Exemples

- Dans le cas de $\mathbb{Z}_6$, seuls 1 et 5 sont inversibles modulo 6.

  En effet, les éléments de $\mathbb{Z}_6$ premiers avec 6 sont exactement 1 et 5.
- Dans le cas de $\mathbb{Z}_5$, tous les éléments non nuls sont inversibles modulo 5.

  En effet, tous les éléments non nuls de $\mathbb{Z}_5$ sont premiers avec 5.

Remarque importante
La preuve du théorème précédent montre que la recherche d'un inverse modulaire peut de faire à l'aide de l'algorithme d'Euclide.

Ceci sera très utile pour résoudre des équations dans $\mathbb{Z}_m$.

Ces exemples sont des cas particuliers du résultat général suivant.

Théorème

Tous les éléments non nuls de $\mathbb{Z}_m$ sont inversibles si et seulement si m est un nombre premier.

Démonstration.

Ceci découle directement du théorème précédent et du fait que m est premier avec $1, 2, \ldots, m-1$ si et seulement si m est un nombre premier. □

Remarque

La multiplication par un élément quelconque de $\mathbb{Z}_m$ n'est pas toujours injective !

Par exemple, on a $2 \cdot_6 1 = 2 \cdot_6 4$ dans $\mathbb{Z}_6$.

Néanmoins, il est vrai que la multiplication par un élément inversible de $\mathbb{Z}_m$ est injective.

Proposition

Pour tout $i \in \mathbb{Z}_m$ inversible modulo m, la fonction

$$\mathbb{Z}_m \to \mathbb{Z}_m,\ j \mapsto i \cdot_m j$$

est injective.

Démonstration.

Soit k l'inverse de i dans $\mathbb{Z}_m$ et soient $j, j' \in \mathbb{Z}_m$ tels que $i \cdot_m j = i \cdot_m j'$.

Alors $j = k \cdot_m i \cdot_m j = k \cdot_m i \cdot_m j' = j'$. □

Consignes pour les exercices

- Vous n'avez pas le droit d'utiliser de calculatrice !

  Il faudra donc d'être efficace, et ne pas passer en revue toutes les valeurs possibles pour x.
- Lorsqu'on demande de résoudre une équation du type

$$ax + b = 0$$

  dans $\mathbb{Z}_m$, les opérations de multiplication et d'addition doivent être interprétées comme étant réellement $\cdot_m$ et $+_m$.

Exercices

1. Résoudre l'équation $10x + 8 = 0$ dans $\mathbb{Z}_{21}$.

   Comme $\mathrm{pgcd}(10, 21) = 1$, nous savons que 10 est inversible dans $\mathbb{Z}_{21}$.

   Puisque $21 - 2 \cdot 10 = 1$, on obtient que $\mathrm{MOD}(-2, 21) = 19$ est l'inverse de 10 dans $\mathbb{Z}_{21}$.

   Ainsi, en supposant que $x \in \mathbb{Z}_{21}$, on a les équivalences suivantes :

$$\begin{aligned} 10 \cdot_{21} x +_{21} 8 = 0 &\iff 10 \cdot_{21} x = 13 \\ &\iff x = 19 \cdot_{21} 13 \\ &\iff x = \mathrm{MOD}(19 \cdot 13, 21) \\ &\iff x = \mathrm{MOD}((-2) \cdot (-8), 21) \\ &\iff x = 16. \end{aligned}$$

   L'équation $10x + 8 = 0$ a donc 16 comme unique solution dans $\mathbb{Z}_{21}$.

2. Résoudre l'équation $10x + 8 = 0$ dans $\mathbb{Z}_{12}$.

Comme $\mathrm{pgcd}(10, 12) = 2$, 10 n'est pas inversible dans $\mathbb{Z}_{12}$.

En supposant que $x \in \mathbb{Z}_{12}$, on a les équivalences suivantes :

$$
\begin{aligned}
10 \cdot_{12} x +_{12} 8 = 0 \quad &\Longleftrightarrow \quad 10 \cdot_{12} x = 4 \\
&\Longleftrightarrow \quad \mathrm{MOD}(10x, 12) = 4 \\
&\Longleftrightarrow \quad \exists q \in \mathbb{Z},\ 10x = 12q + 4 \\
&\Longleftrightarrow \quad \exists q \in \mathbb{Z},\ 5x = 6q + 2 \\
&\Longleftrightarrow \quad \mathrm{MOD}(5x, 6) = 2 \\
&\Longleftrightarrow \quad 5 \cdot_6 \mathrm{MOD}(x, 6) = 2.
\end{aligned}
$$

Comme $\mathrm{pgcd}(5,6) = 1$, nous savons que 5 est inversible dans $\mathbb{Z}_6$.

L'inverse de 5 dans $\mathbb{Z}_6$ est 5 puisque $5 \cdot_6 5 = 1$.

On obtient les équivalences suivantes :

$$\begin{aligned} 5 \cdot_6 \mathrm{MOD}(x,6) = 2 &\iff \mathrm{MOD}(x,6) = 5 \cdot_6 2 \\ &\iff \mathrm{MOD}(x,6) = 4 \\ &\iff \exists q \in \mathbb{Z},\ x = 6q + 4 \\ &\iff x = 4 \ \text{ ou } \ x = 10. \end{aligned}$$

Les solutions de l'équation $10x + 8 = 0$ dans $\mathbb{Z}_{12}$ sont donc 4 et 10.

3. Résoudre l'équation $10x + 8 = 0$ dans $\mathbb{Z}_{15}$.

Comme $\mathrm{pgcd}(10, 15) = 5$, 10 n'est pas inversible dans $\mathbb{Z}_{15}$.

En supposant que $x \in \mathbb{Z}_{15}$, on a les équivalences suivantes :

$$\begin{aligned} 10 \cdot_{15} x +_{15} 8 = 0 &\iff 10 \cdot_{15} x = 7 \\ &\iff \mathrm{MOD}(10x, 15) = 7 \\ &\iff \exists q \in \mathbb{Z},\ 10x = 15q + 7 \end{aligned}$$

Mais si on a $7 = 10x - 15q$ avec $x, q \in \mathbb{Z}$, alors 7 doit nécessairement être un multiple de $\mathrm{pgcd}(10, 15) = 5$.

Comme ce n'est pas le cas (7 n'est pas multiple de 5), on obtient donc qu'il ne peut exister d'entiers x et q tels que $10x = 15q + 7$.

Par conséquent, l'équation $10x + 8 = 0$ n'a pas de solution dans $\mathbb{Z}_{15}$.