Mathématiques pour l'informatique 1

Cours 6 - Division euclidienne et PGCD

Émilie Charlier

Université de Liège

Division euclidienne dans $\mathbb{N}$

- On ne peut pas 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 : $30 = (-4) \cdot (-7) + 2.$
- -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

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

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 $k \in \mathbb{Z}$, nous avons $(k+1)|d| - k|d| = |d| > 0$.

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 $r = r'$. $\square$

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 :

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

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 $r_1, \dots, r_j$ 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 $r_j \geq d$. $\square$

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 :

- $r_1 = a - q_1 b$
- $r_2 = b - q_2 r_1$
  $= b - q_2(a - q_1 b)$
  $= -q_2 a + (1 + q_1 q_2) b$
- $r_3 = r_1 - q_3 r_2$
  $= a - q_1 b - q_3(-q_2 a + (1 + q_1 q_2) b)$
  $= (1 + q_2 q_3) a + (-q_1 - q_3 - q_1 q_2 q_3) b$

Retour à la démonstration

Formellement, on montre ceci par récurrence (forte) 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 que pour tout $k < i$, il existe $m_k, n_k \in \mathbb{Z}$ tels que

$$r_k = m_k a + n_k b.$$

Alors

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

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 $r_i = m_i a + n_i b$. $\square$

Suite de l'exemple

Exemple

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

En remontant les calculs obtenus précédemment, on calcule successivement :

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

D'où

$$3 \cdot 1078 - 10 \cdot 322 = 14 = \mathrm{pgcd}(1078, 322).$$

Coefficients de Bézout pas uniques

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

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

Dans notre exemple, on a

$$3 \cdot 1078 - 10 \cdot 322 = \mathrm{pgcd}(1078, 322)$$

donc aussi

$$(3 + 322) \cdot 1078 + (-10 - 1078) \cdot 322 = \mathrm{pgcd}(1078, 322)$$

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 non nuls 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 $\mathrm{pgcd}(a, b) = 1$. $\square$

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. $\square$

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. $\square$