4.3 Recherche du pgcd et résolution d'équations diophantiennes

4.3.1 Lemme

Soient a et b 2 entiers tels que $a = bq + r$, alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$

Démonstration

1. Soit c un diviseur quelconque *(et pourquoi pas le* pgcd *?)* de a et b ; alors, $a = a'c$ et $b = b'c$; or, $r = a - bq = a'c - bb'cq = c(a' - bb'q)$, c'est à dire que c divise r
   On montre ainsi qu'un diviseur quelconque de a et b divise aussi r, et donc, en particulier, $\text{pgcd}(a, b)$ divise r
2. Réciproquement, soit c un diviseur commun à b et r, c'est à dire que nous avons $b = b'c$ et $r = r'c$; alors, $a = bq + r = b'cq + r'c = c(b'q + r')$, et donc c divise a et c est un diviseur commun à a, b et r

On vient ainsi de montrer qu'un diviseur commun à a et à b est aussi un diviseur commun à b et r

Exercice résolu

Montrer que pour tout $n \in \mathbb{Z}$, $(5n^3 - n) \wedge (n + 2) = (n + 2) \wedge 38$

Et si nous faisions la division euclidienne de $5n^3 - n$ par $n + 2$?
Nous avons : $(5n^3 - n) = (5n^2 - 10n + 19)(n + 2) - 38$
Nous avons donc bien $(5n^3 - n) \wedge (n + 2) = (n + 2) \wedge 38$

4.3.2 Description de l'algorithme

On suppose a et b strictement positifs

1. **Si b divise a, c'est à dire si $a = bq$, alors $b = \text{pgcd}(a, b)$**
2. **Si b ne divise pas a, il existe alors un unique couple d'entiers (q, r) tels que $a = bq + r$ avec $0 < r < b$, et nous avons $\text{pgcd}(a, b) = \text{pgcd}(b, r)$**

Exemple 1 :

1. $\text{pgcd}(795, 53) = 53$ car 53 divise 795
2. Recherche de $\text{pgcd}(1971, 63)$.
   Cette fois ci, 63 ne divise pas 1971 ; on effectue la division euclidienne de 1971 par 63
   — $1971 = (31 \times 63) + 18$, donc $\text{pgcd}(1971, 63) = \text{pgcd}(63, 18)$
   — Il n'y a aucune raison de s'arrêter là ! !
   — On ré-effectue donc la division euclidienne de 63 par 18
   — $63 = (3 \times 18) + 9$, donc $\text{pgcd}(1971, 63) = \text{pgcd}(63, 18) = \text{pgcd}(18, 9)$
   — 9 divise 18, donc $\text{pgcd}(1971, 63) = \text{pgcd}(63, 18) = \text{pgcd}(18, 9) = 9$
   On arrive donc à la généralisation qui suit.

4.3.3 Généralisation

Le pgcd de a et b est le dernier reste non nul dans la méthode des divisions successives de a par b

Démonstration

1. Si on divise a par b, on obtient $a = bq_1 + r_1$ avec $0 < r_1 < b$ et $\text{pgcd}(a, b) = \text{pgcd}(b, r_1)$
2. On divise b par r_1 et nous obtenons $b = r_1q_2 + r_2$ avec $0 < r_2 < r_1$ et

$$\text{pgcd}(a, b) = \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2)$$

3. En itérant, on construit ainsi une suite décroissante $(r_n)_{n\in\mathbb{N}}$ d'entiers positifs tels que $\text{pgcd}\,(a,b) = \text{pgcd}\,(b,r_1) = \text{pgcd}\,(r_1,r_2) = \cdots = \text{pgcd}\,(r_n,r_{n-1})$
4. Au bout d'un certain nombre de divisions, on obtient un reste nul ; supposons $r_{n+1} = 0$, alors, $r_{n-1} = q_{n+1}r_n$ d'où

$$\text{pgcd}\,(a,b) = \text{pgcd}\,(b,r_1) = \text{pgcd}\,(r_1,r_2) = \cdots = \text{pgcd}\,(r_n,r_{n-1}) = r_n$$

Exercice résolu

Recherche du pgcd **de 2375 et 75**

On utilise donc la méthode des divisions successives :

$$\begin{array}{ll} 2375 = 31\times 75 + 50 & \text{donc } \text{pgcd}\,(2375,75) = \text{pgcd}\,(75,50) \\ 75 = 1\times 50 + 25 & \text{donc } \text{pgcd}\,(75,50) = \text{pgcd}\,(50,25) \\ 50 = 2\times 25 & \text{donc } \text{pgcd}\,(50,25) = 25 \end{array}$$

Donc, $\text{pgcd}\,(2375,75) = 25$

Il y a une façon de présenter les résultats sous forme de tableau :

	31	1	2	⟵ quotient
2375	75	50	25	⟵ diviseur
50	25	0		⟵ reste
	↑ pgcd			

Exercice 21 :

1. Rechercher le pgcd de 4641 et 1898
2. Ecrire un algorithme de recherche du pgcd de 2 nombres
   A l'aide de cet algorithme, rechercher :

— $\text{pgcd}\,(871,533)$ — $\text{pgcd}\,(285,322)$ — $\text{pgcd}\,(1812,537)$

Exercice 22 :

Calculez

1. $\text{pgcd}\,(1980,546)$
2. $\text{pgcd}\,(46488,2379)$
3. $\text{pgcd}\,(13860,4488)$

4.3.4 Proposition

Le pgcd **est associatif, c'est à dire que, pour tout $a\in\mathbb{Z}$, tout $b\in\mathbb{Z}$ et tout $c\in\mathbb{Z}$:**

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

Démonstration

Soit D_a l'ensemble des diviseurs de a, D_b l'ensemble des diviseurs de b et D_c l'ensemble des diviseurs de c.
L'ensemble $D_a\cap D_b$ est l'ensemble des diviseurs communs à a et b auquel appartient $\text{pgcd}\,(a,b)$. Ainsi, si $c\in D_a\cap D_b$, alors c divise $\text{pgcd}\,(a,b)$. Et donc, $D_a\cap D_b = D_{\text{pgcd}(a,b)}$.
En faisant le même raisonnement, nous avons :

— $(D_a\cap D_b)\cap D_c = D_{\text{pgcd}(\text{pgcd}(a,b),c)}$
— $D_a\cap(D_b\cap D_c) = D_{\text{pgcd}(a,\text{pgcd}(b,c))}$
— $D_a\cap D_b\cap D_c = D_{\text{pgcd}(a,b,c)}$

L'associativité du pgcd est totalement liée à l'associativité de l'intersection. En effet, nous avons :

$$D_a\cap D_b\cap D_c = (D_a\cap D_b)\cap D_c = D_a\cap(D_b\cap D_c)$$

Généralisation : pgcd de plusieurs nombres

On peut alors étendre la notion de pgcd à un nombre fini d'entiers : $d = \text{pgcd}\,(a_1 \cdots a_n)$ où d est un diviseur commun à $a_1, \cdots, a_n$, et tel que tout diviseur de ces entiers divise d.

4.3.5 Application : résolution d'une équation diophantienne

Résoudre l'équation : $437x - 241y = 1$

Résolution

1. Il faut d'abord vérifier que 437 et 241 sont des nombres premiers entre eux ; pour ce faire, on utilise l'algorithme d'Euclide ; si le pgcd de 437 et 241 n'est pas 1, cette équation n'a pas de solution.

$$\begin{cases} 437 = 1 \times 241 + 196 \\ 241 = 1 \times 196 + 45 \\ 196 = 4 \times 45 + 16 \\ 45 = 2 \times 16 + 13 \\ 16 = 1 \times 13 + 3 \\ 13 = 4 \times 3 + 1 \end{cases}$$

   donc, $\text{pgcd}\,(437, 241) = 1$

2. **Recherchons une solution particulière de l'équation**
   L'idée est d'exprimer 1 **en fonction** de 437 et 241.

$$\begin{cases} 13 = 4 \times 3 & +1 \\ -4 \times 16 = -4 \times 13 & +-4 \times 3 \\ 5 \times 45 = 10 \times 16 & +5 \times 13 \\ -14 \times 196 = (-14) \times 4 \times 45 & +(-14) \times 16 \\ 61 \times 241 = 61 \times 196 & +61 \times 45 \\ (-75) \times 437 = (-75) \times 241 & +(-75) \times 196 \end{cases}$$

   En additionnant les égalités, des simplifications arrivent, et on obtient :

$$61 \times 241 + (-75) \times (437) = 1 + (-75) \times 241$$

   C'est à dire $(136) \times 241 + (-75) \times (437) = 1$.
   On obtient donc comme solution particulière : $x_0 = -75$, $y_0 = -136$

3. **Recherchons une solution générale :**
   Soit $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ une solution générale.
   Nous avons alors :

$$437x - 241y = 437x_0 - 241y_0$$

   C'est à dire :

$$437\,(x - x_0) = 241\,(y - y_0)$$

   Nous avons 437 qui divise $241\,(y - y_0)$; or 437 est premier avec 241, donc, **d'après le lemme de Gauss,** 437 divise $(y - y_0)$.
   Nous avons donc : $(y - y_0) = 437 \times k$, et de la même manière, $(x - x_0) = 241 \times k'$.
   On a donc : $x = -75 + 241k'$ et $y = -136 + 437k$
   Nous avons $k = k'$.
   En effet,

$$(437(-75 + 241k') - 241\,(-136 + 437k) = 1) \Rightarrow (437 \times 241\,(k' - k) = 0)$$

   Donc $k = k'$
   L'ensemble des solutions est donc : $\begin{cases} x = -75 + 241k \\ y = -136 + 437k \end{cases}$ avec $k \in \mathbb{Z}$

4.3.6 Quelques exercices

Exercice 23 :

1. Calculer le pgcd de 5145, 4410, 3675
2. Résoudre l'équation : $3675x - 5145y = 4410$

Exercice 24 :

Résoudre dans $\mathbb{Z}$, les équations

$\star$ $65x = 16y$ $\star$ $65x - 16y = 1$ $\star$ $65x - 16y = 7$

Exercice 25 :

Un pays décide de ne mettre en circulation que des pièces de 3 et 5 euros.

1. Combien de prix sont impraticables entre 1 et 20 euros, si le commerçant ne veut pas être obligé de rendre la monnaie ?
2. Tous les prix supérieurs à 20 euros sont-ils admissibles ?
3. Quels sont les prix admissibles si le commerçant accepte de rendre la monnaie ?

Exercice 26 :

Trouver tous les couples $(x, y) \in \mathbb{Z}^2$ tels que :

$\triangleright$ $5x + 7y = 1$ $\triangleright$ $48x + 60y = 30$ $\triangleright$ $20x + 25y = 1$ $\triangleright$ $21x - 56y = 49$

Exercice 27 :

Résoudre dans $\mathbb{Z}$ le système d'équation d'inconnue x

$$\begin{cases} x \equiv 4\,[7] \\ x \equiv 5\,[15] \end{cases}$$

Exercice 28 :

Deux entiers naturels a et b s'écrivent dans le système de numération de base n :

$$a = \overline{(2310)}_n \qquad b = \overline{(252)}_n$$

On appelle $d = \text{pgcd}\,(a, b)$

1. (a) Démontrer que $2n + 1$ divise a et b
   (b) Démontrer que, si n est pair, alors $d = \text{pgcd}\,(a, b) = 2\,(2n + 1)$, et que, si n est impair, alors $d = \text{pgcd}\,(a, b) = 2n + 1$
2. On suppose que $n = 6$. Résoudre alors dans $\mathbb{Z} \times \mathbb{Z}$ l'équation diophantienne $ax + by = -26$

Exercice 29 :

Un exercice d'arithmétique et de codage

1. (a) Déterminer deux entiers relatifs u et v tels que $7u - 13v = 1$
   (b) Déterminer tous les couples (a, k) d'entiers relatifs tels que $14a - 26k = 4$
2. On considère deux entiers naturels a et b. Pour tout entier n, on note $\rho\,(n)$ le reste 1e la division euclidienne de $an + b$ par 26.

   On décide de coder un message, en procédant comme suit :
   — À chaque lettre de l'alphabet on associe un entier compris entre 0 et 25 (A est numéroté 0, B numéroté 1. . . etc . . .)

— Pour chaque lettre α du message, on détermine l'entier n associé puis on calcule $\rho(n)$.
— La lettre α est alors codée par la lettre associée à $\rho(n)$.
Dans cette question, on ne connaît pas les entiers a et b, mais on sait que la lettre F est codée par la lettre K et la lettre T est codée par la lettre O.

(a) Montrer que les entiers a et b sont tels que $5a+b \equiv 10\,[26]$ et $19a+b \equiv 14\,[26]$

(b) En déduire qu'il existe un entier $k \in \mathbb{Z}$ tel que $14a - 26k = 4$

(c) Déterminer tous les couples d'entiers (a,b), avec $0 \leqslant a \leqslant 25$ et $0 \leqslant b \leqslant 25$,tels que :

$$\begin{array}{l} 5a+b \equiv 10\,[26] \\ 19a+b \equiv 14\,[26] \end{array}$$

3. On suppose que $a = 17$ et $b = 3$.
   (a) Coder le message « GAUSS »
   (b) Soient n et p deux entiers naturels quelconques. Montrer que, si $\rho(n) = \rho(p)$, alors $17(n-p) \equiv 0\,[26]$
   (c) En déduire que deux lettres distinctes de l'alphabet sont codées par deux autres lettres distinctes
4. On suppose toujours que $a = 17$ et $b = 3$
   (a) Soit n un entier naturel. Calculer le reste de la division euclidienne de $23\rho(n) + 9 - n$ par 26
   (b) En déduire un procédé de décodage
   (c) En déduire le décodage du message « KTGZDO »