Chapitre 7

PGCD

7.1 Introduction historique

Étant donnés deux nombres non premiers entre eux, trouver leur plus grande commune mesure.

Euclide, *Éléments*, livre VII, proposition 2 (vers 300 av. J.-C.)

Lors du chapitre sur les congruences, on a pu travailler sur la résolution particulière de certaines équations à deux inconnues, dont on cherche une solution **entière**. Une équation à plusieurs inconnues dont on cherche des solutions entières ou du moins rationnelles, c'est une **équation diophantienne**, du nom du mathématicien **Diophante d'Alexandrie** (III^{e} siècle). Si Gauss était particulièrement charmé par ce type de problème, omniprésent en théorie abstraite des nombres, sa résolution peut s'avérer extrêmement difficile.

7.1.1 Identité de Bézout

Pour s'attaquer aux cas particuliers les plus simples des équations diophantiennes, un nouvel outil est introduit (probablement par Euclide) : le PGCD, ou Plus Grand Commun Diviseur... En s'appuyant sur cet outil, **Claude-Gaspard Bachet de Méziriac** démontre en 1624, dans la seconde édition de ses *Problèmes plaisants et délectables qui se font par les nombres*, qu'il existe une combinaison linéaire à coefficients entiers de deux entiers premiers entre eux égale à 1. Le mathématicien français **Étienne Bézout** (1730-1783) étend ce résultat aux polynômes dans sa *Théorie générale des équations algébriques* (1779) ; on parle d'ailleurs aussi de théorème de Bachet-Bézout. Ce théorème a aujourd'hui une portée considérable en théorie des nombres, jusqu'en cryptographie.

7.1.2 Lemme de Gauss

Le prince des mathématiques, qui écrivait de l'arithmétique supérieure qu'une grande partie de ses théories tire un charme particulier de ce que des propositions importantes, d'apparence simple, se découvrent aisément par induction, alors que leurs démonstrations sont si profondes qu'on ne les trouve qu'après bien des tentatives infructueuses (introduction aux *Mathematische Abhandlungen* d'Eisenstein, 1847), travailla énormément sur le sujet et proposa lors de ses recherches une généralisation du Lemme d'Euclide dans son ouvrage *Disquisitiones arithmeticae* (1801), en reprenant la définition de deux entiers **premiers entre eux**, qui sera la notion fondamentale de ce chapitre.

La cryptographie moderne, sans doute le versant le plus lucratif des mathématiques appliquées, repose essentiellement sur les résultats de ce chapitre, notamment le chiffrement RSA, clef de voûte du système bancaire mondial...

~



7.2 PGCD

Définition :
Soient a et b deux entiers relatifs non tous deux nuls.
On appelle **plus grand commun diviseur de a et b**, noté $\text{PGCD}(a,b)$ le plus grand élément de l'ensemble des diviseurs communs à a et b.

ex : *On a :* $\text{PGCD}(35,15)=5$ *ou* $\text{PGCD}(39,26)=13$.

Proposition 1 :
Soient a, b deux entiers relatifs non nuls. Alors :

- $\text{PGCD}(a,b)=\text{PGCD}(b,a)$
- $\text{PGCD}(a,b)=\text{PGCD}(-a,b)$
- $\text{PGCD}(a,0)=|a|$
- $b|a \Rightarrow \text{PGCD}(a,b)=|b|$

∘ Démonstration :

- Trivial.
- a partage les mêmes diviseurs que $-a$, d'où le résultat.
- 0 admet tous les entiers comme diviseurs, donc le PGCD recherché est le plus grand diviseur de a, soit $|a|$.
- Le plus grand diviseur de b est $|b|$, donc si b divise a alors $|b|$ est un diviseur commun, et c'est le plus grand possible, d'où le résultat.

□

Définition :
Soient a et b deux entiers relatifs non nuls.
On dit que a et b sont **premiers entre eux** si et seulement si $\text{PGCD}(a,b)=1$.

ex : *On a :* $\text{PGCD}(25,16)=1$ *donc les entiers* 25 *et* 16 *sont premiers entre eux.*

Proposition 2 :
Soient a, b deux entiers naturels non nuls avec $a>b$, et r le reste de la division euclidienne de a par b. Alors :

$$\text{PGCD}(a,b)=\text{PGCD}(b,r)$$

∘ Démonstration : Soit $q\in\mathbb{Z}$ tel que la division euclidienne de a par b soit $a=bq+r$.

— Soit d un diviseur de a et b. Alors d divise $a-bq$, donc divise r. Ainsi d est un diviseur commun de b et r.

— Soit d' un diviseur de b et r. Alors d' divise $bq+r$, donc divise a. Ainsi d' est un diviseur commun de a et b.

On en déduit que a et b ont les mêmes diviseurs communs que b et r, donc en particulier :

$$\text{PGCD}(a,b)=\text{PGCD}(b,r)$$

□

Théorème 1 : Algorithme d'Euclide
Soient a, b deux entiers naturels non nuls avec $a>b$.
On définit par récurrence la suite $(r_n)_{n\in\mathbb{N}}$ par :

- r_0 est le reste de la division euclidienne de a par b.
- Si $r_0\neq 0$, alors r_1 est le reste de la division euclidienne de b par r_0.
- Pour tout $k\in\mathbb{N}^*$, si $r_k\neq 0$, alors r_{k+1} est le reste de la division euclidienne de r_{k-1} par r_k.

Alors cette suite d'entiers est strictement décroissante, nulle à partir d'un certain rang, et la dernière valeur non nulle de cette suite est $\text{PGCD}(a,b)$ (si $r_0=0$, c'est-à-dire si b divise a, on a directement $\text{PGCD}(a,b)=b$).

∘ Démonstration :

- Par définition du reste d'une division euclidienne, la suite est nécessairement décroissante car $r_0 < b$, et pour tout $k \in \mathbb{N}$ tel que $r_k \neq 0$, $r_{k+1} < r_k$.
  Or une suite strictement décroissante d'entiers positifs atteint nécessairement 0.
- Posons N le rang tel que $r_N \neq 0$ et $r_{N+1} = 0$.
  D'après la proposition 2, $\text{PGCD}(a,b) = \text{PGCD}(b,r_0) = \text{PGCD}(r_0,r_1) = \cdots = \text{PGCD}(r_N, r_{N+1})$.
  Or $r_{N+1} = 0$, donc $\text{PGCD}(r_N, r_{N+1}) = r_N$ d'après la proposition 1.
- Ainsi, on a bien $\text{PGCD}(a,b) = r_N$, le dernier reste non nul de l'algorithme.

□

ex : Cet algorithme permet de trouver rapidement et manuellement le PGCD de deux nombres, sans avoir à lister les diviseurs de chaque nombre, cherchons :

- *Le PGCD de* 326 *et* 126 *:*

$$\begin{aligned} & 326 = 126 \times 2 + 74 \\ \Rightarrow \quad & 126 = 74 \times 1 + 52 \\ \Rightarrow \quad & 74 = 52 \times 1 + 22 \\ \Rightarrow \quad & 52 = 22 \times 2 + 8 \\ \Rightarrow \quad & 22 = 8 \times 2 + 6 \\ \Rightarrow \quad & 8 = 6 \times 1 + 2 \\ \Rightarrow \quad & 6 = 2 \times 3 + 0 \end{aligned}$$

  On en déduit donc que $\text{PGCD}(326, 126) = 2$.

- *Le PGCD de* 255 *et* 68 *:*

$$\begin{aligned} & 255 = 68 \times 3 + 51 \\ \Rightarrow \quad & 68 = 51 \times 1 + 17 \\ \Rightarrow \quad & 51 = 17 \times 3 + 0 \end{aligned}$$

  On en déduit donc que $\text{PGCD}(255, 68) = 17$.

Proposition 3 :
Soient a, b deux entiers naturels non nuls avec $a > b$, et $k \in \mathbb{N}^*$. Alors :

$$\text{PGCD}(ka, kb) = k \times \text{PGCD}(a,b)$$

∘ Démonstration : Si $a = bq + r$ avec $0 \leqslant r < b$, alors $ka = (kb)q + kr$ avec $0 \leqslant kr < kb$: le reste de la division de ka par kb est kr. Ainsi, l'algorithme d'Euclide appliqué à ka et kb produit les mêmes quotients et des restes tous multipliés par k. Son dernier reste non nul est donc $k \times \text{PGCD}(a,b)$.

□

ex :

$$\begin{aligned} \text{PGCD}(7800, 5200) &= 200 \times \text{PGCD}(39, 26) \\ &= 200 \times 13 \\ &= 2600 \end{aligned}$$

7.3 Théorème de Bézout

Théorème 2 : Identité de Bézout
Soient a et b deux entiers non nuls et $D = \text{PGCD}(a,b)$.
Alors il existe un couple (u,v) d'entiers relatifs tels que :

$$au + bv = D$$

◦ Démonstration : Soit E l'ensemble des combinaisons linéaires de a et b à coefficients entiers qui sont strictement positives. Cet ensemble de nombres entiers naturels n'est pas vide car $|a| \in E$. Il admet donc un plus petit élément, notons le d. Ainsi il existe u et v deux entiers relatifs tels que

$$d = au + bv$$

Montrons en deux temps que $d = D$:

- Dans un premier temps, on remarque que $D|a$ et $D|b$, donc D divise tout élément de E et en particulier $D|d$.
- Si on effectue la division euclidienne de a par d, il existe q et r deux entiers tels que $0 \leqslant r < d$ et :

$$a = dq + r$$

Or ceci implique que :

$$\begin{aligned} r &= a - dq \\ &= a - (au + bv)q \\ &= a - auq - bvq \\ &= a(1 - uq) + b(-vq) \end{aligned}$$

Si r était non nul, r serait donc un élément de E strictement inférieur à d, ce qui contredit le fait que d est le plus petit élément de E. Le reste est donc nécessairement nul, ce qui prouve que d divise a.
De la même manière, on prouve que d divise b. Ainsi d est un diviseur commun de a et b, donc $d \leqslant D$.

Comme $D|d$ et $d > 0$, on a aussi $D \leqslant d$, donc $d = D$. D'où :

$$au + bv = D = \text{PGCD}(a, b)$$

□

Proposition 4 :
Soient a, b deux entiers naturels non tous nuls. Alors :

Tout diviseur d de a et b divise $\text{PGCD}(a, b)$

◦ Démonstration : Conséquence de l'identité de Bézout et du fait que tout diviseur de a et b divise toute combinaison linéaire de a et b. □

Théorème 3 : Théorème de Bézout
Deux entiers relatifs a et b sont premiers entre eux si et seulement s'il existe deux entiers relatifs u et v tels que $au + bv = 1$. Autrement dit :

$$\text{PGCD}(a, b) = 1 \quad \Leftrightarrow \quad \exists u, v \in \mathbb{Z},\ au + bv = 1$$

◦ Démonstration : On procède par double implication :

- $\Rightarrow$: Supposons que $\text{PGCD}(a, b) = 1$, alors d'après l'identité de Bézout, il existe bien u et v deux entiers relatifs tels que $au + bv = \text{PGCD}(a, b) = 1$.
- $\Leftarrow$: Supposons qu'il existe u et v deux entiers relatifs tels que $au + bv = 1$. Alors $\text{PGCD}(a, b)$ divisant a et b, il divise toute combinaison linéaire de a et b, et donc il divise $au + bv = 1$. Le seul entier non nul divisant 1 est 1, donc $\text{PGCD}(a, b) = 1$.

□

ex : Montrons que pour tout entier naturel n, $2n + 1$ et $3n + 2$ sont premiers entre eux :

$$\begin{aligned} \forall n \in \mathbb{N}, \qquad -3 \times (2n + 1) + 2 \times (3n + 2) &= -6n - 3 + 6n + 4 \\ &= 1 \end{aligned}$$

Donc d'après le théorème de Bézout, $\text{PGCD}(2n + 1, 3n + 2) = 1$, ces deux nombres sont premiers entre eux.

✠ Méthode : Algorithme d'Euclide étendu

Les résultats précédents peuvent être utilisés pour trouver un couple de Bézout à l'aide de l'algorithme d'Euclide. Par exemple, comment trouver un couple d'entiers (x, y) tels que $59x + 27y = 1$?

- Premièrement, on vérifie que 59 et 27 sont premiers entre eux, à l'aide de l'algorithme d'Euclide :

$$\begin{aligned} & 59 = 27 \times 2 + 5 \quad (L_1) \\ \Rightarrow \quad & 27 = 5 \times 5 + 2 \quad (L_2) \\ \Rightarrow \quad & 5 = 2 \times 2 + 1 \quad (L_3) \end{aligned}$$

  Nécessairement 1 sera le dernier reste non nul, donc $\text{PGCD}(59, 27) = 1$.

- Maintenant vient l'idée de l'algorithme étendu pour trouver le couple recherché : on remonte l'algorithme en isolant le 1, de façon à faire réapparaître 59 et 27 :

$$\begin{aligned} 1 &= 5 - 2 \times 2 \qquad \text{or d'après la ligne } L_2,\ 2 = 27 - 5 \times 5 \\ &= 5 - (27 - 5 \times 5) \times 2 \\ &= 5 - 27 \times 2 + 10 \times 5 \\ &= 11 \times 5 - 27 \times 2 \qquad \text{or d'après la ligne } L_1,\ 5 = 59 - 27 \times 2 \\ &= 11 \times (59 - 27 \times 2) - 27 \times 2 \\ &= 11 \times 59 - 27 \times 22 - 27 \times 2 \\ &= 11 \times 59 - 27 \times 24 \end{aligned}$$

  On a donc bien trouvé $(x, y) = (11, -24)$ tels que $59x + 27y = 1$.
  Maîtriser cet algorithme rapidement est essentiel pour la suite du chapitre.

Proposition 5 : Corollaire de Bézout

Soient a et b deux entiers relatifs non tous deux nuls, et c un entier relatif. Alors :

L'équation $ax + by = c$ admet des solutions entières si et seulement si $\text{PGCD}(a, b) | c$.

◦ Démonstration : Notons $D = \text{PGCD}(a, b)$. Si (x, y) est une solution, D divise a et b, donc $ax+by = c$. Réciproquement, si $c = kD$ avec $k \in \mathbb{Z}$, l'identité de Bézout fournit u et v tels que $au + bv = D$, et le couple (ku, kv) est solution : $a(ku) + b(kv) = kD = c$. □

ex : $4x + 9y = 2$ *admet des solutions car* $\text{PGCD}(4, 9) = 1$ *et* 2 *est multiple de* 1.
Mais $9x - 15y = 2$ *n'admet pas de solution car* $\text{PGCD}(9, 15) = 3$ *et* 2 *n'est pas multiple de* 3.

7.4 Théorème de Gauss

Théorème 4 : Théorème de Gauss

Soient a, b et c trois entiers relatifs non nuls. Alors :

$$\left.\begin{array}{l} a \text{ divise } bc \\ a \text{ et } b \text{ premiers entre eux} \end{array}\right\} \Rightarrow a \text{ divise } c$$

◦ Démonstration : Si a divise bc, alors il existe un entier $k \in \mathbb{Z}$ tel que $ak = bc$. Or si a et b sont premiers entre eux, alors d'après le théorème de Bézout, il existe u et v deux entiers relatifs tels que :

$$\begin{aligned} & au + bv = 1 \\ \Rightarrow \quad & acu + bcv = c \\ \Rightarrow \quad & acu + akv = c \\ \Rightarrow \quad & a(cu + kv) = c \end{aligned}$$

Donc a divise c.

□

ex : *Trouver un couple d'entiers relatifs* (x, y) *tels que* $5(x - 1) = 7y$.

- 7 *divise* $5(x - 1)$ *mais* $\text{PGCD}(5, 7) = 1$, *donc d'après le théorème de Gauss,* 7 *divise* $(x - 1)$. *Autrement dit il existe* $k \in \mathbb{Z}$ *tel que* $x - 1 = 7k$, *ou* $x = 7k + 1$. *Si on remplace* $(x - 1)$ *par* $7k$ *dans l'équation, on trouve rapidement* $y = 5k$.
- *Ainsi tous les couples solutions sont de la forme* $(7k + 1; 5k)$ *où* $k \in \mathbb{Z}$.

Proposition 6 : Corollaire de Gauss
Soient a, b et c trois entiers relatifs, b et c non nuls. Alors :

$$\left.\begin{array}{l} b \text{ et } c \text{ divisent } a \\ b \text{ et } c \text{ premiers entre eux} \end{array}\right\} \Rightarrow bc \text{ divise } a$$

∘ Démonstration : Si b et c divisent a, alors il existe k et k' entiers relatifs tels que : $a = kb$ et $a = k'c$. On a alors $kb = k'c$, donc b divise $k'c$, or $\text{PGCD}(b, c) = 1$, donc d'après le théorème de Gauss, b divise k'.

Ceci signifie qu'il existe $k'' \in \mathbb{Z}$ tel que : $k' = k''b$.

On a alors : $a = k'c = k''bc$, ce qui prouve que bc divise a.

□

✠ Méthode : Résolution d'équation diophantienne

On appelle **équation diophantienne** toute équation du type $ax+by = c$, où a, b et c sont des entiers, et dont on cherche un couple d'entiers solution. On sait d'après les résultats précédents que cette solution existe si et seulement si $\text{PGCD}(a, b)$ divise c. Pour la résoudre, on suivra plusieurs étapes, supposons que $\text{PGCD}(a, b) = 1$:

- On cherche une solution particulière (x_0, y_0) à l'équation.

  Si cette solution n'est pas immédiate, on cherche alors une solution (x_1, y_1) à l'équation $ax + by = 1$ en utilisant l'algorithme d'Euclide étendu.

  Une solution de l'équation originale est alors $(x_0, y_0) = (cx_1, cy_1)$.
- Soit (x, y) une solution de l'équation, on soustrait terme à terme dans l'équation la solution (x, y) à la solution particulière (x_0, y_0).
- On applique le théorème de Gauss pour déterminer l'expression de (x, y).
- On vérifie que les solutions trouvées vérifient bien l'équation originale.

Cherchons à résoudre l'équation diophantienne suivante :

$$17x - 33y = 1$$

On sait que cette équation admet au moins un couple solution car $\text{PGCD}(17, 33) = 1$.

- On remarque une solution évidente, car : $17 \times 2 - 33 \times 1 = 1$, donc le couple $(2; 1)$ est solution particulière de l'équation.
- Soit (x, y) un couple solution. On a alors :

  $$\left\{\begin{array}{l} 17x - 33y = 1 \\ 17 \times 2 - 33 \times 1 = 1 \end{array}\right.$$

  On soustrait alors la deuxième égalité à la première terme à terme :

  $$(17x - 33y) - (17 \times 2 - 33 \times 1) = 0$$

  Ce qui nous donne rapidement :

  $$17(x - 2) = 33(y - 1)$$

  Or 17 est premier avec 33, et 17 divise $33(y - 1)$, donc d'après le théorème de Gauss, 17 divise $(y - 1)$. Il existe donc un entier relatif k tel que $y - 1 = 17k$, ou $y = 17k + 1$. On trouve ensuite rapidement que $x = 33k + 2$. Le couple solution est donc de la forme :

  $$(33k + 2; 17k + 1) \text{ où } k \in \mathbb{Z}$$

- On vérifie que les solutions sont correctes :

  $$\begin{aligned} 17 \times (33k + 2) - 33 \times (17k + 1) &= 17 \times 2 - 33 \times 1 \\ &= 1 \end{aligned}$$

  La vérification est essentielle car on raisonne par implication.