Arithmétique, deuxième partie

Terminale S (enseignement de spécialité)
Lycée Charles PONCET

Février 2014

Table des matières

Le symbole ✏ indique les exemples à traiter, des démonstrations à trouver.
Le symbole ☛ indique des points importants, des pièges possibles, des notations particulières, etc.

1 PGCD de deux nombres entiers

1.1 Diviseurs communs à deux nombres entiers

Les *diviseurs communs* à deux entiers relatifs a et b sont les entiers relatifs qui divisent à la fois a et b.

✏ Déterminer les diviseurs communs à 12 et -20.

Remarques

1. Les diviseurs communs à 0 et $a \in \mathbb{Z} - \{0\}$ sont les diviseurs de a.
2. Les diviseurs communs à 1 et a sont 1 et -1, pour tout entier relatif a.

Proposition 1.1.1 (réduction)
Si $\Delta(a\ ;\ b)$ *est l'ensemble des diviseurs communs à deux entiers relatifs* a *et* b*, alors :*

$$\Delta(a\ ;\ b) = \Delta(a - b\ ;\ b) = \Delta(a + kb\ ;\ b),\ \textit{pour tout entier } k \in \mathbb{Z}.$$

✏ Démontrer la proposition 1.1.1.

Proposition 1.1.2 (corollaire de la proposition 1.1.1)
a *et* b *sont deux entiers relatifs.*

1. *Si* $0 < b \leqslant a$ *alors* $\Delta(a\ ;\ b) = \Delta(r\ ;\ b)$ *où* r *est le reste de la division euclidienne de* a *par* b.
2. *Si* b *divise* a *alors* $\Delta(a\ ;\ b) = \Delta(b)$ *où* $\Delta(b)$ *est l'ensemble des diviseurs de* b.

✏ Démontrer la proposition 1.1.2.

1.2 PGCD de deux nombres entiers

Théorème 1.2.1 (admis)
Toute partie finie non vide de $\mathbb{Z}$ *possède un plus grand élément.*

Théorème 1.2.2 (et définition)
a *et* b *étant deux entiers relatifs non tous les deux nuls, l'ensemble* $\Delta(a\ ;\ b)$ *des diviseurs communs à* a *et* b *adment un plus grand élément appelé le* plus grand commun diviseur *de* a *et* b *et noté* $\text{PGCD}(a\ ;\ b)$ *ou* $a \wedge b$.

✏ Démontrer le théorème 1.2.2.

Remarques

a et b sont deux entiers relatifs non tous les deux nuls.

1. $\text{PGCD}(a\ ;\ b)$ est un entier naturel non nul.
2. $\text{PGCD}(a\ ;\ b) = \text{PGCD}(b\ ;\ a) = \text{PGCD}(|a|\ ;\ |b|)$.
3. Si $0 < b \leqslant a$ alors $\text{PGCD}(a\ ;\ b) \leqslant b$.
4. $\text{PGCD}(1\ ;\ b) = 1$.
5. Pour tout $b \neq 0$, $\text{PGCD}(0\ ;\ b) = |b|$.

Proposition 1.2.1
Deux entiers relatifs non tous les deux nuls sont premiers entre eux si, et seulement si, leur PGCD *est égal à* 1.

☛ La proposition 1.2.1 peut être prise comme définition de deux nombres entiers premiers entre eux.

Proposition 1.2.2
a et b étant deux entiers relatifs non tous les deux nuls, pour tout entier relatif k :

$$\text{PGCD}(a\,;\,b) = \text{PGCD}(a-b\,;\,b) = \text{PGCD}(a+kb\,;\,b).$$

En particulier, si $0 < b \leqslant a$ alors $\text{PGCD}(a\,;\,b) = \text{PGCD}(r\,;b)$ où r est le reste de la division euclidienne de a par b.

☛ La proposition 1.2.2 est une conséquence directe des propositions 1.1.1 et 1.1.2.

Lorsque b est un diviseur strictement positif de a, on peut écrire $a = kb$ avec k un entier relatif non nul donc $\text{PGCD}(a\,;\,b) = \text{PGCD}(a-kb\,;\,b) = \text{PGCD}(0\,;\,b) = b$.

Exercice d'application

p et q sont deux entiers naturels non nuls. On pose $a = 9p + 4q$ et $b = 2p + q$.

1. Montrer que $\text{PGCD}(a\,;\,b) = \text{PGCD}(p\,;\,q)$.
2. Montrer que $9p + 4$ et $2p + 1$ sont premiers entre eux.
3. Déterminer $\text{PGCD}(9p + 4\,;\,2p - 1)$ en fonction des valeurs de p.
   Vérifier pour $p = 5$ et $p = 9$.

1.3 Algorithme d'EUCLIDE [1]

Théorème 1.3.1 (algorithme d'EUCLIDE)
a et b sont deux entiers naturels tels que $0 < b \leqslant a$.

1. *On calcule le reste r de la division euclidienne de a par b.*
2. *Si $r = 0$ alors $\text{PGCD}(a\,;\,b) = b$.*
3. *Si $r \neq 0$ on reprend la première étape en remplaçant a par b et b par r.*

Ainsi quand b ne divise pas a, le PGCD de a et b est le dernier reste non nul.

✏ Utiliser l'algorithme d'EUCLIDE pour $a = 11222$ et $b = 279$.

Preuve du théorème 1.3.1

Pour cette démonstration, on utilise les théorèmes suivants :

Théorème 1.3.2
Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

Théorème 1.3.3 (principe de la descente infinie)
Si (a_n) est une suite infinie d'entiers naturels décroissante (au sens large) alors (a_n) est stationnaire (c'est-à-dire constante) à partir d'un certain rang.

Théorème 1.3.4 (corollaire du théorème 1.3.3 dû à FERMAT)
Toute suite strictement décroissante d'entiers naturels est finie.

On écrit les divisions euclidiennes successives :

$$a = bq_0 + r_0 \;\text{ avec }\; 0 \leqslant r_0 < b.$$

Si $r_0 = 0$, on s'arrête car $\text{PGCD}(a\,;\,b) = b$ puisque b divise a.

1. EUCLIDE, mathématicien grec du III^{e} siècle av. J.-C. Connu pour la rédaction des *Éléments*, traité qui est passé pendant deux millénaires comme un modèle de rigueur et comme une description du monde physique.

Si $r_0 \neq 0$, on remplace a par b et b par r_0 :

$$b = r_0 q_1 + r_1 \text{ avec } 0 \leqslant r_1 < r_0.$$

Si $r_1 \neq 0$, on remplace b par r_0 et r_0 par r_1 :

$$r_0 = r_1 q_2 + r_2 \text{ avec } 0 \leqslant r_2 < r_1.$$

Si $r_2 \neq 0$, on remplace r_0 par r_1 et r_1 par r_2 :

$$r_1 = r_2 q_3 + r_3 \text{ avec } 0 \leqslant r_3 < r_2.$$

On construit ainsi une suite (r_n) d'entiers naturels strictement décroissante car cette suite vérifie $0 \leqslant \cdots < r_3 < r_2 < r_1 < r_0$.
Cette suite est finie car il n'existe qu'un nombre fini d'entiers naturels entre 0 et r_0. Il existe donc un reste nul, c'est-à-dire qu'il existe $k \in \mathbb{N}$ tel que $r_k \neq 0$ et $r_{k+1} = 0$. Il y a donc un nombre fini d'étapes, l'algorithme s'arrête.
En utilisant les propriétés de réduction du PGCD on a alors :
$\text{PGCD}(a\,;\,b) = \text{PGCD}(b\,;\,r_0) = \text{PGCD}(r_0\,;\,r_1) = \cdots = \text{PGCD}(r_k\,;\,r_{k+1}) = \text{PGCD}(r_k\,;\,0) = r_k$ car $r_k \neq 0$ et $r_{k+1} = 0$.

Théorème 1.3.5 (corollaire de l'algorithme d'EUCLIDE)
Les diviseurs communs à deux entiers naturels non nuls sont les diviseurs de leur PGCD.

✏ Déterminer les diviseurs communs à 11222 et 279.

✏ Démontrer le théorème 1.3.5.

1.4 Autres propriétés du PGCD

Proposition 1.4.1 (homogénéité)
a *et* b *sont deux entiers relatifs non tous les deux nuls. Pour tout entier naturel* α *non nul :*

$$\text{PGCD}(\alpha a\,;\,\alpha b) = \alpha\,\text{PGCD}(a\,;\,b).$$

✏ Utiliser la proposition 1.4.1 pour calculer $\text{PGCD}(300\,;\,375)$.

✏ Démontrer la proposition 1.4.1.

Proposition 1.4.2 (propriété caractéristique, corollaire de la proposition 1.4.1)
On considère deux entiers relatifs a *et* b *non tous les deux nuls et* d *un entier naturel non nul.*

$d = \text{PGCD}(a\,;\,b)$ *si et seulement si* $a = da'$ *et* $b = db'$ *avec* a' *et* b' *premiers entre eux.*

✏ Démontrer la proposition 1.4.2.

Proposition 1.4.3 (conséquence de la proposition 1.4.2)
Tout nombre rationnel peut s'écrire sous la forme d'une fraction irréductible.

✏ Démontrer la proposition 1.4.3.

Proposition 1.4.4
a, b, c, d *sont des entiers relatifs non nuls. Si* a *divise* c *et* b *divise* d *alors* $\text{PGCD}(a\,;\,b)$ *divise* $\text{PGCD}(c\,;\,d)$.

✏ Démontrer la proposition 1.4.4.

Exercice sur le PGCD

Déterminer tous les couples $(a\,;\,b)$ d'entiers naturels tels que $ab = 7776$ et $\text{PGCD}(a\,;\,b) = 18$.

2 Théorème de BÉZOUT [2]

2.1 Égalité de BÉZOUT (ou de BACHET [3])

Théorème 2.1.1
Si a *et* b *sont deux entiers relatifs non tous les deux nuls et si* $d = \text{PGCD}(a\,;\,b)$ *alors il existe deux entiers relatifs* u *et* v *tels que* $au + bv = d$.

Preuve du théorème 2.1.1

Soit E l'ensemble des entiers naturels de la forme $au + bv$ avec u et v deux entiers relatifs.

$E \neq \varnothing$ car $|a| \in E$ en effet, $|a| = a \times 1 + b \times 0$ si $a \geqslant 0$ et $|a| = a \times (-1) + b \times 0$ si $a \leqslant 0$.

E est une partie non vide de $\mathbb{N}$ donc E possède un plus petit élément d, donc il existe un couple $(u\,;\,v)$ d'entiers relatifs tels que $au + bv = d$.

On démontre maintenant que $d = \text{PGCD}(a\,;\,b)$ c'est-à-dire que d divise a et b et que tout diviseur commun de a et b divise d.
La division euclidienne de a par d s'écrit $a = dq + r$ avec $0 \leqslant r < d$.
On a donc $r = a - dq = a - (au + bv)q = a(1 - qu) + b(-qv) = ax + by$ avec $x = 1 - qu$ et $y = -qv$.
Comme x et y sont des entiers relatifs, $r \in E$.
$r = 0$ car sinon $r > 0$ et $r \in E$ donc $r \geqslant d$ ce qui est absurde car $0 \leqslant r < d$ d'après la division euclidienne de a par d.
Finalement $a = dq$ donc d divise a.
On démontre de même que d divise b, donc d est un diviseur commun à a et b.

Soit d' un diviseur commun à a et b, alors a divise toute combinaison linéaire de a et b donc d' divise $au + bv = d$.

Conclusion : $d = \text{PGCD}(a\,;\,b)$.

☛ Le théorème 1.4.2 donne l'existence de u et v mais il n'y a pas unicité, par exemple $\text{PGCD}(6\,;\,8) = 2$ et $2 = 6 \times (-1) + 8 \times 1 = 6 \times 3 + 8 \times (-2)$.

✏ Utiliser l'algorithme d'EUCLIDE pour calculer le PGCD de $a = 960$ et $b = 245$.
En utilisant les divisions euclidiennes de l'algorithme d'EUCLIDE, déterminer un couple $(u\,;\,v)$ d'entiers relatifs tels que $960u + 245v = \text{PGCD}(960\,;\,245)$.

2.2 Théorème de BÉZOUT

Théorème 2.2.1
Deux entiers relatifs a *et* b *sont premiers entre eux si et seulement s'il existe des entiers relatifs* u *et* v *tels que* $au + bv = 1$.

✏ Démontrer le théorème 2.2.1 (théorème de BÉZOUT).

✏ Utiliser le théorème de BÉZOUT pour démontrer que $6n + 4$ et $2n + 1$ sont premiers entre eux, quel que soit $n \in \mathbb{Z}$.

2. Étienne BÉZOUT, mathématicien français, Nemours, 1730 – Les Basses-Loges, 1783.
3. Claude-Gaspard BACHET dit de MÉZIRIAC, mathématicien, poète et traducteur français, auteur de « Les problèmes plaisants et délectables », Bourg-en-Bresse, 1581 – *idem*, 1638.

3 Théorème de GAUSS [4]

3.1 Théorème de GAUSS

Théorème 3.1.1
a, b, c sont trois entiers relatifs non nuls.
Si a divise bc et si a et b sont premiers entre eux alors a divise c.

✏ Utiliser le théorème de BÉZOUT pour démontrer le théorème 3.1.1 (théorème de GAUSS).

Conséquences

Proposition 3.1.1
a, b, c sont trois entiers relatifs non nuls.
Si a et b divisent c et si a et b sont premiers entre eux alors ab divise c.

✏ Démontrer la proposition 3.1.1.

Proposition 3.1.2
Si un entier relatif non nul a est premier avec chacun des entiers relatifs non nuls b_1, b_2, …, b_n alors a est premier avec le produit $b_1 \times b_2 \times \cdots \times b_n$.

✏ En utilisant un raisonnement par récurrence, démontrer la proposition 3.1.2.

Proposition 3.1.3
Si un nombre premier p divise le produit ab de deux entiers relatifs alors p divise au moins l'un des facteurs a ou b.

' ✏ Démontrer la proposition 3.1.3.

Proposition 3.1.4
Si un nombre premier p divise un produit de nombres premiers alors p est l'un d'entre eux.

✏ Démontrer la proposition 3.1.4.

Proposition 3.1.5
Un entier n est premier avec les entiers a et b si, et seulement si, n est premier avec le produit ab.

✏ Démontrer la proposition 3.1.5.

3.2 Exemples d'équations diophantiennes [5]

Une équation diophantienne est une équation algébrique à coefficients dans $\mathbb{Z}$ à plusieurs inconnues, dont on cherche les solutions dans $\mathbb{Z}$.

On considère l'équation $(E) : 17x - 33y = 1$, où x et y sont des entiers relatifs.

1. Déterminer « à vue » une solution particulière de (E).
2. En déduire une solution particulière $(x_0\,;\,y_0)$ de $(E') : 17x - 33y = 5$.
3. Résoudre dans $\mathbb{Z}^2$ l'équation (E'). Pour cela on montrera que l'équation (E') est équivalente à $17(x - x_0) = 33(y - y_0)$ et on utilisera le théorème de GAUSS.
4. Résoudre de la même façon l'équation $51x + 54y = 2004$ dans $\mathbb{Z}^2$, puis déterminer les couples d'entiers naturels solutions de cette équation.

4. Carl Friedrich GAUSS, astronome, mathématicien et physicien allemand, Brunswick, 1777 – Göttingen, 1855. Ses travaux mathématiques concernent la théorie des nombres, le théorème fondamental de l'algèbre, le calcul des probabilités, la géométrie...
5. DIOPHANTE, mathématicien grec, v. 200/214 – v. 284/298.

Remarque

On considère l'équation $ax + by = c$ avec a, b, c des entiers relatifs non nuls.
Démontrer que si c n'est pas un multiple du PGCD de a et b alors l'équation $ax + by = c$ n'a pas de solution dans $\mathbb{Z}^2$.

4 PPCM de deux nombres entiers

La notion de PPCM *n'est plus dans le programme de 2012. Elle peut néanmoins apparaître dans certains exercices.*

4.1 Définition

Théorème 4.1.1 (et définition)
Si a et b sont deux entiers relatifs non nuls, l'ensemble des multiples communs strictement positifs de a et b admet un plus petit élément m appelé plus petit commun multiple *de a et b et on note $m = \text{PPCM}(a\ ;\ b)$ ou $m = a \vee b$.*

☛ L'ensemble des multiples communs strictement positifs de a est b est une partie non vide de $\mathbb{N}$, car il contient $|ab|$, donc cet ensemble possède un plus petit élément m.

✏ Déterminer le PPCM de 9 et 12.
Pour additionner deux fractions on peut choisir comme dénominateur commun le PPCM des deux dénominateurs, par exemple $\frac{10}{9} + \frac{7}{12} = \cdots$

Remarques

a et b sont deux entiers relatifs non nuls.

1. $\text{PPCM}(a\ ;\ b) = \text{PPCM}(b\ ;\ a) = \text{PPCM}(|a|\ ;\ |b|)$.
   Dans la pratique on se ramène donc au cas où a et b sont des entiers strictement positifs.
2. $\text{PPCM}(1\ ;\ a) = |a|$.
3. Si $b|a$ alors $\text{PPCM}(a\ ;\ b) = |a|$.

4.2 Propriétés

Proposition 4.2.1
Si a et b sont deux entiers naturels non nuls, l'ensemble des multiples communs à a et b est l'ensemble des multiples de $\text{PPCM}(a\ ;\ b)$.

✏ Démontrer la proposition 4.2.1.

Proposition 4.2.2 (relation entre le PGCD et le PPCM)
Si a et b sont deux entiers naturels non nuls alors $\text{PGCD}(a\ ;\ b) \times \text{PPCM}(a\ ;\ b) = a \times b$.

✏ Démontrer la proposition 4.2.2.

Proposition 4.2.3 (premier corollaire de la proposition 4.2.2)
Deux entiers naturels non nuls a et b sont premiers entre eux si et seulement si $\text{PPCM}(a\ ;\ b) = ab$.

✏ Démontrer la proposition 4.2.3.

Proposition 4.2.4 (deuxième corollaire de la proposition 4.2.2)
Si a *et* b *sont deux entiers naturels non nuls alors, pour tout entier naturel* k *non nul :*

$$\text{PPCM}(ka\,;\,kb) = k \times \text{PPCM}(a\,;\,b).$$

✏ Démontrer la proposition 4.2.4.

4.3 Utilisation de la décomposition en produit de nombres premiers

Proposition 4.3.1
Si on connaît les décompositions en produit de nombres premiers des entiers naturels non nuls a *et* b *alors on peut déterminer la décomposition en produit de nombres premiers de* $d = \text{PGCD}(a\,;\,b)$ *et de* $m = \text{PPCM}(a\,;\,b)$.

- d *est égal au produit de* tous les facteurs premiers communs *aux deux décompositions, élevés chacun à* la plus petite des deux puissances *les concernant.*
- m *est égal au produit de* tous les facteurs premiers présents *dans les deux décompositions, élevés chacun à* la plus grande puissance *les concernant.*

✏ Déterminer le PGCD et le PPCM de 252 et 1176.