PGCD et applications

Lycée du parc

Année 2020-2021

I PGCD et algorithme d'Euclide

On commence par rappeler des choses « évidentes » :

Simplifier la fraction : $\frac{30}{42} =$

Comment a-t-on choisi le nombre qui a permis la simplification ?

Additionner de manière « économique » les fractions : $\frac{9}{35} + \frac{3}{14} =$

Quelle propriété possède le nouveau dénominateur ?

Définition (Diviseurs communs, PGCD)

Soient a et b deux entiers relatifs non simultanément nuls.
L'ensemble des diviseurs communs à a et b est noté $\mathcal{D}(a, b)$. On a ainsi :

$$\mathcal{D}(a, b) = \mathcal{D}_{\mathbb{Z}}(a) \cap \mathcal{D}_{\mathbb{Z}}(b).$$

L'ensemble $\mathcal{D}(a, b)$ admet un plus grand élément appelé Plus Grand Commun Diviseur de a et b et que l'on note $\text{PGCD}(a, b)$ ou $a \wedge b$.

Exercice 1

Déterminer $\mathcal{D}(15, 40)$, en déduire $\text{PGCD}(15, 40)$.

Entraînement 1

Déterminer $\mathcal{D}(104, 182)$, en déduire $\text{PGCD}(104, 182)$.

Propriété

a et b étant deux entiers relatifs non simultanément nuls, on a toujours :

1. $\text{PGCD}(a,b) = \text{PGCD}(b,a) = \text{PGCD}(|a|,|b|)$
2. $\text{PGCD}(a,b) \geqslant 1$, $\text{PGCD}(a,0) = |a|$ et $\text{PGCD}(a,1) = 1$.
3. a divise b si, et seulement si, $\text{PGCD}(a,b) = |a|$.
4. $\text{PGCD}(a,b) = \text{PGCD}(a-b,b)$.

Preuve :

Exercice 2

Soit $n \in \mathbb{N}^*$, déterminer $\text{PGCD}(n-1, n+1)$.

Entraînement 2

Pour $n \in \mathbb{N}^*$, déterminer $\text{PGCD}(3n+2, 3n-1)$.

La notion de PGCD est très importante en arithmétique car le PGCD de deux nombres mesure, en quelque sorte, ce que ces nombres ont en (facteur) commun. Pour le calculer on dispose, heureusement, d'un algorithme efficace qui utilise les divisions euclidiennes.

C'est l'occasion d'un petit rappel :

Propriété-Définition (Division euclidienne)

Soit a un entier relatif quelconque et b un entier naturel non nul, il existe un unique couple d'entier relatif $(q;r)$ tel que

$$a = bq + r \text{ et } 0 \leq r < b$$

On dit alors que q est le quotient de la division et r son reste.

La propriété suivante indique comment une division euclidienne permet de simplifier le calcul d'un PGCD :

Propriété (Lemme d'Euclide [1])

Soient a et b deux entiers naturels non nuls.

Si q et r sont tels que $a = bq + r$ alors $\mathcal{D}(a, b) = \mathcal{D}(b, r)$.

Et le plus grand élément de ces ensembles est le même, c'est à dire :

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

Preuve :

Théorème (Algorithme d'Euclide)

Soient $a, b \in \mathbb{N}^*$. On considère la suite d'entiers (r_n) définie par :
$r_0 = b$
r_1 est le reste de la division euclidienne de a par r_0
si $r_1 \neq 0$ alors r_2 est le reste de la division euclidienne de r_0 par r_1
si $r_2 \neq 0$ alors r_3 est le reste de la division euclidienne de r_1 par r_2
$\vdots$
En continuant tant que le reste obtenu est non nul.
Alors, il existe un entier N tel que $r_N = 0$ et alors :

$$\text{PGCD}(a, b) = r_{N-1} \quad \text{et} \quad \mathcal{D}(a, b) = \mathcal{D}(a \wedge b)$$

Remarques :
— On se ramènera toujours au cas positif par $\text{PGCD}(a, b) = \text{PGCD}(|\ a\ |, |\ b\ |)$.
— Sur les calculatrices Numworks, le reste de la division euclidienne de p par q se calcule à l'aide de `rem(p, q)` qui s'obtient dans la boîte à outils.
— Sur les calculatrices TI-83, grâce à la touche `math`, on accède à un menu NBRE qui propose la fonction : `reste(`.

1. Un lemme est un résultat intermédiaire sur lequel on s'appuie pour conduire la démonstration d'un théorème plus important. Certains ont eu un destin plus brillant que prévu comme le lemme de Zorn, le lemme d'Abel et bien d'autres encore.

Preuve :

Exercice 3 : Algorithme d'Euclide en Python

Écrire une fonction python qui calcule le PGCD par l'algorithme d'Euclide.

Exercice 4

Calculer PGCD$(4095, 98)$ et PGCD$(754, -611)$

Entraînement 3

Calculer PGCD$(378, 294)$ et PGCD$(758, -631)$

Propriété (Propriétés du PGCD)

Pour $a, b \in \mathbb{Z}^*$,

1. Pour $n \in \mathbb{Z}$, $\text{PGCD}(a, b) = \text{PGCD}(a, b - na)$.
2. $\mathcal{D}(a, b) = \mathcal{D}_{\mathbb{Z}}(\text{PGCD}(a, b))$. (Cette propriété est d'usage **très** fréquent.)
   «Les diviseurs communs à a et b sont exactement les diviseurs de $\text{PGCD}(a, b)$».
3. Pour $k \in \mathbb{Z}^*$, $\text{PGCD}(ka, kb) = |k|\text{PGCD}(a, b)$. (Propriété d'homogénéité)

Preuve :

II Les théorèmes de Bézout et de Gauss

Définition (Nombres premiers entre eux, fraction irréductible)

On dit que deux nombres a et b sont premiers entre eux si leur PGCD est égal à 1 ou, de manière équivalente, si leur seul diviseur commun (dans $\mathbb{N}$) est 1.

On dit qu'une fraction est écrite de manière irréductible lorsque le numérateur et le dénominateur sont premiers entre eux .

Remarque : D'après cette définition, pour montrer que a et b sont premier entre eux, il suffit de prouver que si $d > 0$ est un diviseur commun alors $d = 1$.

Exercice 5

Montrer que, quel que soit $n \in \mathbb{N}$, la fraction $\dfrac{2n+3}{3n+4}$ est irréductible.

Entraînement 4

Même consigne pour $\dfrac{5n+3}{2n+1}$.

Pour bien comprendre les notions qui suivent il est utile de faire quelques expériences à l'aide d'un tableur. On s'intéresse aux combinaisons linéaires entières de deux entiers donnés, c'est à dire à l'ensemble des nombres de la forme $au+bv$ où a et b sont **fixés** et où u, v prennent toutes les valeurs entières.

Quelle conjecture peut-on faire ?

Théorème de Bézout [2]

Soient a et b deux entiers relatifs non simultanément nuls,
a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Remarque : Cette propriété permet de montrer que des nombres sont premiers entre eux sachant que d'autres le sont en combinant les relations du type $au + bv = 1$ pour en obtenir de nouvelles.

Preuve :

Exercice 6 : non unicité du couple de Bézout.

Soient a et b deux nombres premiers entre eux et (u_0, v_0) est un couple vérifiant $au_0+bv_0 = 1$.

Montrer qu'il existe une infinité d'autres couples (u, v) tels $au + bv = 1$.

Exercice 7

Montrer que si un entier a est premier avec deux entiers b et c alors il est premier avec leur produit.

2. Étienne Bézout est un mathématicien français né à Nemours le 31 mars 1730 et mort à Avon le 27 septembre 1783. Ses recherches portèrent principalement sur les équations algébriques, la divisibilité des polynômes, la rectification des courbes planes et leurs intersections qui lui valurent d'entrer à 28 ans à l'Académie des sciences.

Entraînement 5 

À l'aide du résultat de l'exercice précédent, montrer que si a et b sont premiers entre eux alors a^n et b^p le sont aussi pour tout $n \geq 1$ et $p \geq 1$.

Corollaire (Identité de Bézout)

Soient a et b deux entiers relatifs non tous les deux nuls et $d = PGCD(a, b)$.

L'ensemble des nombres de la forme $au + bv$ où u et v sont des relatifs quelconques est exactement l'ensemble des multiples de d.

$$\{au + bv \mid (u, v) \in \mathbb{Z}^2\} = (a \wedge b)\mathbb{Z}$$

Remarques :

— En particulier, il existe toujours un couple (u, v) d'entiers relatifs tel que $au + bv = a \wedge b$.

— C'est ce qu'on a constaté expérimentalement à l'aide du tableur.

Preuve :

La détermination effective d'un couple se fait en "remontant" dans l'algorithme d'Euclide, par exemple pour $a = 71$ et $b = 19$, cela donne :

Propriété (Caractérisation du PGCD)

Soient a et b des entiers relatifs non nuls, alors pour g entier naturel non nul les propositions suivantes sont équivalentes :

1. g est le PGCD de a et b.
2. Il existe des entiers a' et b' premiers entre eux tels que $a = ga'$ et $b = gb'$.
3. g est un diviseur commun à a et b et il existe $u, v \in \mathbb{Z}$ tels que $au + bv = g$.

Preuve :

Exercice 8 : Algorithme d'Euclide étendu

Attention cet algorithme fait partie du cours.

III Applications de l'identité de Bezout

Propriété (Existence d'un inverse en congruence)

Soit $n \geqslant 2$ un entier naturel et $a \in Z$.

Il existe $c \in Z$ tel que $ac \equiv 1 \ \ [n]$ si, et seulement si, a est premier avec n.

Preuve :

Exercice 9

Résoudre l'équation dans $\mathbb{Z}$: $\quad 4x \equiv 2 \ \ [9]$

Entraînement 6

Résoudre l'équation dans $\mathbb{Z}$: $\quad -5x \equiv -3 \ \ [7]$

Une erreur classique est de croire que si a divise un produit bc mais ne divise pas l'un des deux facteurs (b par exemple) il divise forcément l'autre (donc c dans l'exemple). On trouve facilement un contre-exemple :

qui montre que l'implication « si $a \mid bc$ et $a \nmid b$ alors $a \mid c$ » est **fausse !**

On pourra éviter de commettre cette erreur à l'aide du théorème suivant qui montre que la condition $a \nmid b$ n'est pas assez forte ; il faut que a et b soient premiers entre eux.

Théorème de Gauss [3]

Pour a, b et c des entiers relatifs non nuls, si $a \mid bc$ et $a \wedge b = 1$ alors $a \mid c$.

Preuve :

Corollaire

Pour a, b et n des entiers relatifs non nuls, si $a \mid n$, $b \mid n$ et $a \wedge b = 1$ alors $ab \mid n$.

Preuve :

Exercice 10 Montrer que pour tout $n \in \mathbb{N}$, $n(5n^2 + 1)$ est divisible par 6.

3. Johann Carl Friedrich Gauss (30 avril 1777 — 23 février 1855) est un mathématicien, astronome et physicien allemand. Ce bas de page est trop petit pour un exposé même succinct de ses contributions scientifiques...

Le théorème de Gauss est d'usage très fréquent. Il permet, par exemple, de résoudre les équations diophantiennes du type $ax + by = c$. On se propose ici de résoudre quatre équations de ce type, représentatives des différents cas possibles.

On verra qu'il est aussi possible de les résoudre avec des congruences.

Exercice 11

a. $15x + 21y = 7$

b. $8x + 3y = 1$

c. $3x - 7y = 3$

d. $49x + 35y = 14$