Chapitre 3 PGCD

1) Définition Soient a et b deux entiers non nuls. Les ensembles de diviseurs D_a et D_b sont finis donc $D_a \cap D_b$ l'est aussi. 1 est dans $D_a \cap D_b$ qui est donc non vide. Cet ensemble a donc un plus grand élément qu'on appelle PGCD de a et b. On le note PGCD (a, b) ou parfois simplement (a, b).

PGCD signifie Plus Grand Diviseur Commun.

Exemple : D_{15} = {-15, -5, -3, -1, 1, 3, 5, 15} et D_{20} = {-20, -10, -5, -4, -2, -1, 1, 2, 4, 5, 10, 20}.

PGCD (15, 20) = 5.

Définition : Cas particulier important : si PGCD (a, b) = 1, on dit que a et b sont premiers entre eux.

(ça ne signifie pas qu'ils sont premiers ! Définition : p est premier s'il a exactement deux diviseurs : 1 et lui-même.)

Exemple : (15, -14) = 1 donc 15 et -14 sont premiers entre eux.

Evidences : D_1 = {-1 ; 1} donc pour tout a, PGCD (a , 1) = . D_0 = IN donc si a ≠ 0, PGCD (a , 0) = .

PGCD (0 , 0) n'est pas défini. Pour tous a > 0 et k, PGCD (a , ka) = . Si a > 0, PGCD (a , b) = a ⇔

2) Algorithme d'Euclide (-300 av JC)

On dit parfois algorithme d'Euclide « étendu ». **Il donne en sortie le PGCD** de a et b quand a et b sont saisis en entrée. Il utilise plusieurs fois le fait suivant : quand on effectue la division euclidienne de a par b, a = bq + r, alors tout diviseur de a et b divise r et tout diviseur de b et r divise a, et du coup PGCD (a, b) = PGCD (b, r).

Théorème 1 : Soit a et b deux naturels non nuls tels que b ne divise pas a.
La suite des divisions euclidiennes suivantes finit par s'arrêter. Le dernier reste non nul est alors le $\text{pgcd}(a,b)$

$$\begin{array}{rll} a \text{ par } b & a = bq_0 + r_0 & \text{avec } b > r_0 \geqslant 0 \\ b \text{ par } r_0 & b = r_0 q_1 + r_1 & \text{avec } r_0 > r_1 \geqslant 0 \\ r_0 \text{ par } r_1 & r_0 = r_1 q_2 + r_2 & \text{avec } r_1 > r_2 \geqslant 0 \\ \vdots & \vdots & \\ r_{n-2} \text{ par } r_{n-1} & r_{n-2} = r_{n-1} q_n + r_n & \text{avec } r_{n-1} > r_n \geqslant 0 \\ r_{n-1} \text{ par } r_n & r_{n-1} = r_n q_{n+1} + 0 & \end{array}$$

On a alors $\text{pgcd}(a,b) = r_n$.

Démonstration :

- La suite des restes : $r_0, r_1, r_2, \ldots, r_n$ est une suite strictement décroissante dans $\mathbb{N}$ car $r_0 > r_1 > r_2 > \cdots > r_n$.
  Cette suite est donc finie. Il existe alors n tel que $r_{n+1} = 0$.
- De proche en proche, on en déduit que :

$$\text{pgcd}(a,b) = \text{pgcd}(b,r_0) = \cdots = \text{pgcd}(r_{n-2},r_{n-1}) = \text{pgcd}(r_{n-1},r_n)$$

or r_n divise r_{n-1}, donc $\text{pgcd}(r_{n-1},r_n) = r_n$
Conclusion : $\text{pgcd}(a,b) = r_n$. Le dernier reste non nul est le pgcd.

(cours de Paul Milan)

En Python :

```
def pgcd (a,b) :
    while b != 0 :
        a,b = b,a%b
    return a
#
print(pgcd(370,50))
# donne l'impression 10.
```

Noter la double affectation !
(elles sont simultanées, la première n'a pas d'incidence sur l'autre)
Exercice 1 : l'écrire sans double affectation :

```
 …
a = …
b =…
```

Exercice 2 : modifier ce code pour avoir en plus :
Si on tape pgcd(370,50) sur la console, on obtient l'impression suivante : PGCD(370,50) = 10.

Exemples :

59 = 27*2 + 5
27 = 5*5 + 2
5 = 2*2 + 1
donc PGCD(59 ; 27) = 1.

4539 = 1958*2 + 623
1958 = 623*3 + 89
623 = 89*7
donc PGCD(4539 ; 1958) = 89.

3) Identité de Bezout (1730- 1783)

Théorème : **Soient a et b deux entiers non nuls. Soit D = PGCD (a, b). Alors il existe des entiers u et v vérifiant : au + bv = D.**

Preuve : soit E l'ensemble des entiers n vérifiant deux conditions : n s'écrit sous la forme n = au + bv et n > 0. Cet ensemble est évidemment non vide et il a un plus petit élément qu'on désigne par d. On a donc l'existence de deux entiers, disons U et V, vérifiant aU + bV = d. On effectue la division euclidienne de a par d : a = qd + r avec $0 \leq r < d$.

On a donc r = a – qd = a – q (aU+bV) donc r = a (1-qU) + (-qV) b.

On voit que r vérifie la première condition d'appartenance à E et r < d = l'élément min de E donc r ne vérifie pas la deuxième condition, c'est-à-dire que $r \leq 0$, donc que r = 0. On a prouvé que d divise a. On prouverait de même que d divise b. d est un diviseur commun à a et b donc $d \leq$ PGCD (a, b) = D.

Par ailleurs D = PGCD (a, b) divise a et b donc divise aU + bV = d, ce qui implique $D \leq d$.

On voit que **D = PGCD (a, b) est le plus petit nombre (strictement) positif vérifiant une égalité du type au + bv = D**. Pour PGCD (15, 20) = 5, l'égalité est (-1).15 + 1.20 = 5. En revanche une égalité du type aU + bV = d n'implique évidemment pas que d est le PGCD de a et b : (-2).15 + 2.20 = 10.

Cependant si on a une égalité du type aU + bV = d, on est certain que **d est un multiple du PGCD de a et b** : en effet, ce PGCD divise a et b donc il divise aU + bV = d. Notamment : aU+bV = 1 => PGCD (a,b) = 1, d'où avec le théorème qui donne la réciproque : **il existe U et V tels que a U + b V = 1 <=> PGCD (a,b) = 1.**

Remarques : facile à prouver : si c divise a et b, alors c divise PGCD (a,b).

PGCD (a,b) = 1 => PGCD (da,db) = d.

3) Détermination pratique des coefficients u et v

Méthode 1 : avec l'algorithme d'Euclide, a = 4539, b = 1958

On effectue les divisions euclidiennes suivantes :

$$4\,539 = 1\,958 \times 2 + 623$$
$$1\,958 = 623 \times 3 + 89$$
$$623 = 89 \times 7$$

Conclusion : $\text{pgcd}(4\,539, 1\,958) = 89$

On écrit les restes successifs en fonction de a et b en commençant par le haut :
a = 2b + 623 donc 623 = a -2b.
89 = b -3.623 = b -3(a-2b) = -3a + 7b.
On a obtenu u = -3 et b = 7 :
-3*4539 + 7*1958 = 89.

Méthode 2 : l'algorithme suivant donne u et v.

a et b étant fixés, avec b > 0, et D = PGCD (a, b) étant connu, on part de u = 0 et tant que a*u n'est pas congru à D modulo b, on incrémente u de 1 (c'est-à-dire qu'on ajoute 1 à u : u ← u +1). On a alors trouvé u et on fait v ← (D-au)/b, c'est-à-dire qu'on affecte la valeur (D-au)/b à v.

Exercice : Ecrire ça en Python. Cet algorithme pose-t-il un problème ? (réponse oui : il suppose que le u à trouver est positif, mais on peut facilement le régler ! : on prouve facilement qu'il y a une infinité de couples (u,v) qui fonctionnent…dont certains avec u > 0.)

Méthode 3 : bricolage avec la calculatrice : on rentre la fonction Y = (89 – X*4539)/1958 et on demande un tableau de valeurs de pas 1, on cherche X tel que Y soit un entier : Y = (D – aX)/b, alors X = u et Y = v.

4) Théorème de Gauss (1777-1855)

Théorème : si a divise b*c et (a,b) = 1, alors a divise c. Preuve :…

Exercices : 1) si a et b, premiers entre eux, divisent c, alors ab divise c.

2) Si d = PGCD(a, b), alors il existe a' et b' premiers entre eux tels que a = da' et b = db'.

3) Soit m le PPCM(Plus Petit Commun Multiple) de a et b. Prouver que ab=m*PGCD(a, b). (utiliser le 2))

4) L'équation (« diophantienne ») : ax + by = c, a, b et c fixés, on cherche x et y (entiers !)… B-A BA à connaître…