Arithmétique : PGCD, Bézout et Gauss

Prélude - Historique et contexte

L'algorithme d'Euclide, décrit dans les *Éléments* vers 300 av. J.-C., est l'un des plus anciens algorithmes encore utilisés : il calcule le plus grand diviseur commun de deux entiers sans les décomposer. Au XVII^{e} siècle, Bachet de Méziriac établit l'identité qu'on attribue aujourd'hui à Étienne Bézout (XVIII^{e} siècle). Ces résultats sont au cœur du chiffrement RSA, qui sécurise les échanges sur Internet.

I PGCD et algorithme d'Euclide

Définition

Soit a et b deux entiers non tous deux nuls. Le plus grand des diviseurs communs positifs de a et b est le **PGCD** de a et b, noté PGCD$(a\,;\,b)$.
a et b sont **premiers entre eux** si PGCD$(a\,;\,b)=1$.

Propriété

Si $a=bq+r$, alors les diviseurs communs de a et b sont ceux de b et r, donc PGCD$(a\,;\,b)=$ PGCD$(b\,;\,r)$.

Méthode - Algorithme d'Euclide

On effectue des divisions euclidiennes successives ; le PGCD est le dernier reste non nul.
PGCD(462 ; 180) :
$462=180\times2+102$
$180=102\times1+78$
$102=78\times1+24$
$78=24\times3+6$
$24=6\times4+0$
Donc PGCD(462 ; 180) = 6.

```
def pgcd(a, b):
    while b != 0:
        a, b = b, a % b
    return a
```

II Théorèmes de Bézout et de Gauss

Propriété - Identité de Bézout

Si $d=$ PGCD$(a\,;\,b)$, il existe des entiers relatifs u et v tels que $au+bv=d$.
On les obtient en « remontant » l'algorithme d'Euclide.

Propriété - Théorème de Bézout

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

Exemple

$7\times(-2)+5\times3=1$, donc 7 et 5 sont premiers entre eux. Deux entiers consécutifs sont premiers entre eux : $(n+1)\times1+n\times(-1)=1$.

Propriété - Théorème de Gauss

Si a divise bc et si a est premier avec b, alors a divise c.
Démonstration : $au+bv=1$ donne $c=acu+bcv$; a divise acu et bcv, donc c.

Propriété - Corollaire

Si a et b sont premiers entre eux et divisent tous deux n, alors ab divise n.

III Équations diophantiennes $ax + by = c$

Propriété

L'équation $ax + by = c$ d'inconnues entières x et y a des solutions si et seulement si PGCD$(a\ ;\ b)$ divise c.

Méthode - Résoudre $5x - 3y = 2$

- Solution particulière : $(1\ ;\ 1)$ convient.
- Si $(x\ ;\ y)$ est solution, par soustraction $5(x-1) = 3(y-1)$. 5 divise $3(y-1)$ et est premier avec 3, donc d'après le théorème de Gauss, 5 divise $y-1$: $y = 1+5k$, $k \in \mathbb{Z}$. Puis $5(x-1) = 15k$, donc $x = 1+3k$.
- Réciproquement, $5(1+3k) - 3(1+5k) = 2$. Les solutions sont les couples $(1+3k\ ;\ 1+5k)$, $k \in \mathbb{Z}$.

Exemple - Remonter l'algorithme d'Euclide

PGCD$(17\ ;\ 5)$: $17 = 5\times 3+2$; $5 = 2\times 2+1$. Donc $1 = 5-2\times 2 = 5-2(17-5\times 3) = 7\times 5-2\times 17$: $u = -2$, $v = 7$ conviennent pour $17u+5v = 1$.