Cours du 13 novembre

vendredi 13 novembre 2020 07:59

a, b entiers

$PGCD(a,b)$ = plus grand diviseur commun

obtenu soit - par l'algo d'EUCLIDE

- par la factorisation de a et b.

DÉFINITION $a, b \in \mathbb{Z}$

a et b sont premiers entre eux si $PGCD(a,b) = 1$.

$\Updownarrow$

le seul diviseur commun ≥ 0 à a et b est 1.

Théorème : Identité de BÉZOUT.

Soient a, b deux entiers non nuls.

Alors il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = PGCD(a,b)$$

En particulier, si a et b sont premiers entre eux

$\exists u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

EX $a = 7$, $b = 17$ par exemple $u = 5$ $v = -2$ convient

car $7 \times 5 + 17 \times (-2) = 1$

Remarque si $a, b > 0$ alors u et v sont de signes opposés.

Pour trouver u et v (qui s'appellent les coefficients de BÉZOUT), on "remonte" l'algorithme d'EUCLIDE.

- Calculons $PGCD(17,7)$ par l'algorithme d'Euclide

$$17 = 2 \times 7 + 3$$
$$7 = 2 \times 3 + 1 \quad \leftarrow \text{dernier reste non nul.}$$
$$3 = 3 \times 1 + 0$$

$17 - 14 = 3$ | 7 | 2

$$1 = 7 - 2 \times 3 = 7 - 2 \times [17 - 2 \times 7]$$
$$= 7 - 2 \times 17 + 4 \times 7 = 5 \times 7 - 2 \times 17$$

- Autre exemple $a = 600$ $b = 124$

On effectue l'algorithme d'Euclide

$600 - 496 = 104$ | 124 | 4

$$600 = 4 \times 124 + 104$$
$$124 = 1 \times 104 + 20$$
$$104 = 5 \times 20 + 4$$
$$20 = 5 \times 4 + 0$$

$PGCD(600, 124) = 4$

On remonte l'algorithme

$4 = 104 - 5 \times 20$ ← identité de Bézout pour 104 et 20

$= 104 - 5 \times (124 - 104)$

$= 6 \times 104 - 5 \times 124$ ← identité de Bézout pour 124 et 104

$= 6 \times (600 - 4 \times 124) - 5 \times 124$

$= 6 \times 600 - 29 \times 124$ ← identité de Bézout pour 600 et 124

Ainsi $\begin{cases} u = 6 \\ v = -29 \end{cases}$ vérifient $au + bv = \text{PGCD}(a,b)$

Remarque : il n'y a pas un unique couple (u,v) qui convient, mais une infinité.

Si $au + bv = 1$

$au + bv + ab - ab = 1$

$a(u+b) + b(v-a) = 1$

On a l'équivalence

a et b premiers entre eux $\iff$ $\exists\, u, v \in \mathbb{Z}$ tels que $au + bv = 1$

(Bézout $\Rightarrow$)

$\Leftarrow$ Si $p \mid a$ et $p \mid b$ alors $p \mid au$ et $p \mid bv$ donc $p \mid au + bv$ soit $p \mid 1$ et donc $p = 1$

THÉORÈME de GAUSS

Soient a, b, c dans $\mathbb{Z}^*$.
On suppose a et b premiers entre eux
Si $a \mid bc$ alors $a \mid c$.

Preuve Par le théorème de Bézout, il existe u, v tels que $au + bv = 1$

$auc + bvc = c$

$a(uc) + (bc)v = c$

($a(uc)$: divisible par a ; $(bc)v$: divisible par a)

donc $a \mid c$.

COROLLAIRE

Si p est un nombre premier
et m, n deux entiers.
Si $p \mid mn$ alors $p \mid m$ ou $p \mid n$ [ou éventuellement les deux]

Preuve Si p ne divise pas m.
Alors le seul diviseur commun à p et m est 1
donc $PGCD(p,m) = 1$
Par le théorème de GAUSS $p \mid mn$ donc $p \mid n$.

Avec ce corollaire, on peut démontrer l'unicité de la décomposition en facteurs premiers.

CONGRUENCES

Soit $n \in \mathbb{N}^*$
On dit que $a, b \in \mathbb{Z}$ sont congrus modulo n si n divise $a-b$
$(\Leftrightarrow \exists k \in \mathbb{Z}$ tel que $a = b + kn)$

On écrit $a \equiv b \ [n]$
c'est aussi équivalent à dire que les divisions euclidiennes de a par n et de b par n donnent le même reste.

Proposition

Soit $n \in \mathbb{N}^*$, soient a, b, c, d dans $\mathbb{Z}$

① Si $a \equiv b \ [n]$ et $c \equiv d \ [n]$ alors $a+c \equiv b+d \ [n]$
② Si $a \equiv b \ [n]$ et $c \equiv d \ [n]$ alors $ac \equiv bd \ [n]$
③ Si $a \equiv b \ [n]$ alors $\forall k \in \mathbb{N}^*$ $a^k \equiv b^k \ [n]$.

Preuve ① $n \mid a-b$, $n \mid c-d$ donc $n \mid (a-b+c-d)$
autrement dit $n \mid (a+c-(b+d))$

② $n \mid a-b$, $n \mid c-d$

$$ac - bd = ac - bc + bc - bd$$
$$= (a-b)c + b(c-d)$$

$(a-b)c$: divisible par n ; $b(c-d)$: divisible par n

donc $n \mid ac - bd$

③ Se montre à partir de ② par récurrence sur k. (EXO)

BASES de NUMÉRATION

Théorème

Soit $b \geq 2$.
Tout entier $x \in \mathbb{N}$ peut s'écrire d'une manière unique sous la forme

$$x = a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0$$

où $n \in \mathbb{N}$ et $a_0, \dots a_n$ sont dans $\{0, \dots, b-1\}$.

On dit que $\overline{a_n \dots a_0}^{\,b}$ est l'écriture de x

où $n \in \mathbb{N}$ et $a_0, \dots a_n$ sont dans $\{0, \dots, b-1\}$.

On dit que $x = \overline{a_n a_{n-1} \dots a_0}^{\,b}$ est l'écriture de x en base b.

Pour $b=10$, c'est l'écriture habituelle (décimale)

$b=2 \rightarrow$ écriture binaire.

$105 = \overline{105}^{10} = \overline{1101001}^{2}$

2^6 2^5 2^4 2^3 2^2 2^0

plus grande puissance de 2 inférieure à 105

$105 = 64 + 41$ $\quad 64 = 2^6$

$= 64 + 32 + 9$

$= 64 + 32 + 8 + 1$

$= 2^6 + 2^5 + 2^3 + 2^0$

Exercice :

Calculer des coefficients de BÉZOUT pour

$a = 14 \quad b = 9$