LEÇON 11 :

(PGCD de deux entiers naturels. Nombres premiers entre eux. Applications. L'exposé pourra être illustré par un ou des exemples faisant appel à l'utilisation d'une calculatrice.)

I PGCD de deux entiers naturels.

prérequis : - La division Euclidienne dans $\mathbb{N}$.
- Ensemble $\mathbb{N}$ et $\mathbb{Z}$.
- Relation de divisibilité.

Notations : Pour tout $a \in \mathbb{N}$, on notera $D_a = \{x \in \mathbb{N} \mid x|a\}$ l'ensemble des diviseurs de a (dans $\mathbb{N}$).

1) Théorème fondamental et définitions :

• Théorème : Soient $a, b \in \mathbb{N}$. Il existe un et un seul entier naturel d noté $a \wedge b$ tel que $D_a \cap D_b = D_d$.

preuve : • Existence :

- si $b = 0$ alors $D_a \cap D_0 = D_a$ car tout nbre divise 0
- De même si $a = 0$ alors $D_0 \cap D_b = D_b$.
- Supposons maintenant $0 < b \leq a$.
  - si $b|a$ alors $D_a \cap D_b = D_b$ on peut donc prendre $d = b$.
  - Sinon on écrit la division euclidienne de a et de b, soit $a = bq + r \quad 0 \leq r < b$ et on constate que $D_a \cap D_b = D_b \cap D_r$
    on divise à nouveau b par r pour obtenir $b = rq_1 + r_1 \quad 0 \leq r_1 < r$
    Et ainsi de suite.

On obtient ainsi une liste finie de divisions euclidiennes appelé l'algorithme d'Euclide.

$$(E):\begin{cases} a = bq + r & 0 < r < b \\ b = rq_1 + r_1 & 0 < r_1 < r \\ r = r_1 q_2 + r_2 & 0 < r_2 < r_1 \\ \vdots & \vdots \\ r_{n-2} = r_{n-1} q_n + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = r_n \cdot q_n + 0 \end{cases}$$

Avec $D_a \cap D_b = D_b \cap D_r = \dots = D_{r_{n-1}} \cap D_{r_n} = D_{r_n}$.

Rmq :

On montre que le reste s'annule au bout d'un nombre fini de pas de calcul : $\rightarrow$ on a une suite (des) d'entiers naturels strictement décroissante

Unicité :

si $D_a \cap D_b = D_d$ et $D_a \cap D_b = D_{d'}$

alors d divise d' et d' divise d

donc $d = d'$

* Corollaire : $d = a \wedge b \iff \begin{cases} d \mid a \text{ et } d \mid b \\ \text{tout diviseur de } a \text{ et de } b \text{ divise } d \end{cases}$

* Définition : L'entier naturel d est appelé le "plus grand commun diviseur" (au sens de la divisibilité et aussi au sens de l'ordre habituel sauf si $a = b = 0$) de a et de b. on note $d = pGCD(a,b)$ ou $d = a \wedge b$.

2) Propriétés : $\forall a \in \mathbb{N}^*$, $\forall (b,c) \in \mathbb{N}^2$

i) $a \wedge b = b \wedge a$ (commutativité du pgcd)
ii) $a \wedge 0 = a$ et $a \wedge 1 = 1$.
iii) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (associativité)
iv) $a \cdot c \wedge bc = c\,(a \wedge b)$.

Preuve : i) on a $D_a \cap D_b = D_b \cap D_a$.
ii) comme $D_0 = \mathbb{N}$ et comme $D_1 = \{1\}$ est inclus dans D_a pour tout entier a, on obtient :
$D_a \cap D_0 = D_a$ et $D_a \cap D_1 = D_1$.

iii) traduit l'égalité $(D_a \cap D_b) \cap D_c = D_a \cap (D_b \cap D_c)$
iv) on multiplie par c toutes les divisions qui interviennent dans l'algorithme d'Euclide :

restes)

$$(E') : \begin{cases} ca = cbq_1 + cr \\ cb = cr q_1 + cr_1 \\ \vdots \\ cr_{n-2} = cr_{n-1} q_n + cr_n \\ cr_{n-1} = cr_n q_n + 0 \end{cases}$$

par suite $ac \wedge bc = cr_n = c \times (a \wedge b)$.

3) Méthode de Calcul : (du PGCD).

- Euclide (algorithme) → (exemple programme calculatrice)

$$\begin{cases} 60 = 42 \times 1 + 18 \\ 42 = 18 \times 2 + 6 \\ 18 = 6 \times 3 + 0 \end{cases} \Rightarrow 60 \wedge 42 = 6.$$

- ~~Calculatrice avec la fonction gcd(a,b).~~
- Décomposition en facteurs premiers : (utilise le théorème fondamental d'arithmétique : tout nombre $a \in \mathbb{N}$ s'écrit : $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$)

$$\prod_{i}^{n} p_i^{a_i}$$

Exemple : $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n} = \prod_{i=1}^{n} p_i^{\alpha_i}$ premier

$b = p_1^{\beta_1} \cdots p_n^{\beta_n} = \prod_{i=1}^{n} p_i^{\beta_i}$ p premier

$a \wedge b = p_1^{\min(\alpha_1, \beta_1)} \times \cdots \times p_n^{\min(\alpha_n, \beta_n)} = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$

II Nombres premiers entre eux ;

* **Définition** : Soit $(a,b) \in \mathbb{N}^2$. a et b sont dits premiers entre eux si $pgcd(a,b) = 1$.

* **Théorème de BEZOUT** :
Soit $(a,b) \in \mathbb{N}^2$. a et b sont premiers entre eux si et seulement si il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Rmq : le couple (u,v) n'est pas unique.
exple : $pgcd(9,5) = 1$ le couple
$(-1, 2)$ vérifie $9 \times (-1) + 2 \times 5 = 1$.
$(9, -16)$ ——— $9 \times 9 - 16 \times 5 = 1$.

→ Calculatrice (progme de recherche de u_0 et v_0)

* **Exercice** : Montrer que : si $a \wedge b = 1$ et $a \wedge c = 1$
alors $a \wedge bc = 1$.
Réponse : le théorème de BEZout montre qu'il existe u, v, u', v' tels que $au + bv = 1$ et
$au' + cv' = 1$
par suite (en multipliant membre en membre) :
$a(auu' + ucv' + u'bv) + bc \cdot vv' = 1$
et les entiers a et bc sont premiers entre eux.

LEcon 11 Suite:

Preuve: Thm de BEZOUT:

⇐) $\exists (u,v) \in \mathbb{Z}^2$ t.q $au+bv = 1$

on pose $a \wedge b = d$.

donc il existe k_1 et k_2 t.q $a = d.k_1$ et $b = d.k_2$.

d'où $d(uk_1 + v.k_2) = 1$

donc d divise 1, donc $d = 1$.

⇒) Un couple (u,v) est donné en remontant l'algorithme d'Euclide.

Théorème de Gauss:

soit $(a,b,c) \in \mathbb{N}^3$.

si $a \wedge b = 1$ et si a divise bc alors a divise c

preuve: $a \wedge b = 1$, donc d'après BEZOUT $\exists (u,v) \in \mathbb{Z}^2$ t.q

$au + bv = 1$ ce qui entraine:

$acu + bvc = c$ et a divise le premier membre

donc a divise c.

Corollaire: $(a,b,c) \in \mathbb{N}^3$ si a divise n, b divise n, et $a \wedge b = 1$ } alors ab divise n

III Applications

1°) Equation Diophantienne:

définition: soit $(a,b) \in (\mathbb{Z}^*)^2$, $c \in \mathbb{Z}$, on appelle équation diophantienne une équation de la forme: $ax+by = c$

proposition : Une solution générale de (E) est la somme d'une solution particulière de (E) et de la solution générale à l'équation $ax + by = 0$.

Exercice : Soit une cible : 

: quelles sont toutes les possibilités d'obtenir 100 points.

2°) fraction irréductible

définition : Soit $(a,b) \in \mathbb{N}^2$. on dit que la fraction $\frac{a}{b}$ est irréductible si et seulement si $a \wedge b = 1$.

prop : Tout nbre rationnel $r > 0$ s'écrit de façon unique $r = \frac{a}{b}$ où $a \wedge b = 1$ et $b \neq 0$.

3°) inversion modulaire :

définition : Soit $(n,m) \in \mathbb{N}^2$. Si $n \wedge m = 1$, alors on appelle inverse de m modulo n le nombre v tel que : $m \cdot v = 1 \ [n]$.

- Inverse dans $\mathbb{Z}/n\mathbb{Z}$.

Soit $n \in \mathbb{N} \setminus \{0,1\}$. Soit $\dot{x}$ la classe de $x \in \mathbb{Z}$ dans l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$:
Les propriétés suivantes sont équivalentes :
i) $\dot{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$
ii) $x \wedge n = 1$

4°) L'irrationnalité de $\sqrt{2}$.

Par l'absurde, on suppose $\sqrt{2}$ rationnelle.
Il existe donc $p \in \mathbb{N}$, $q \in \mathbb{N}^*$ tel que : $\sqrt{2} = \frac{p}{q}$ avec $p \wedge q = 1$.

(En effet si $d = \text{pgcd}(p,q)$ et si on écrit $p = dp'$ et $q = d \cdot q'$ on a $\text{pgcd}(p';q') = 1$ car :
$d = \text{pgcd}(p,q) = \text{pgcd}(dp', dq') = d \cdot \text{pgcd}(p',q)$).

$\sqrt{2} = \frac{p}{q} \Rightarrow p^2 = 2q^2$.

donc 2 divise p^2, donc divise p et on l'en peut écrire $p = 2 \cdot p'$. Ainsi $(2 \cdot p')^2 = p^2 = 2q^2$, soit

$2p'^2 = q^2$

donc 2 divise q^2 $\Rightarrow$ 2 divise q. C'est absurde car $\text{pgcd}(p,q) = 1$