PROGRAMME DE COLLE S16

NB : **seules** les démonstrations des théorèmes, propositions étoilées ne sont pas exigées.

ENTIERS RELATIFS, ARITHMÉTIQUE

Division euclidienne dans Z

Théorème.— Division euclidienne dans Z —. Pour tout couple $(a, b) \in \mathbf{Z} \times \mathbf{N}^\star$ d'entiers tel que $b \neq 0$, il existe un couple $(q, r) \in \mathbf{Z}^2$, **unique** tel que

- $a = bq + r$
- $0 \leq r < b$

Proposition.— Soit $(a, b) \in \mathbf{Z} \times \mathbf{N}^\star$. b divise a *si et seulement si* le reste de la division euclidienne de a par b est nul.

PGCD de deux entiers

Soit $(a, b) \in \mathbf{Z}^2$ un couple d'entiers relatifs, on note $\mathcal{D}(a, b)$ l'ensemble des diviseurs communs à a et b.

Définition : *Soit $(a, b) \in \mathbf{Z}^2$ un couple d'entiers relatifs, tel que $(a, b) \neq (0, 0)$. Le plus grand élément de $\mathcal{D}(a, b)$ est appelé **plus grand diviseur commun** à a et b. Cet entier naturel est noté $PGCD(a, b)$ ou encore $a \wedge b$*

Proposition.— Lemme d'Euclide —. Soit $(a, b) \in \mathbf{Z} \times \mathbf{N}^\star$. Notons r le reste de la division euclidienne de a par b. Alors $a \wedge b = b \wedge r$.

Savoir-faire : l'**algorithme d'Euclide** pour déterminer $a \wedge b$, et établir une **égalité de Bezout** par *remontée.*

Théorème.— Caractérisations du PGCD —. Soit $(a, b) \in \mathbf{Z}^2$, $d \in \mathbf{N}$. On note $a\mathbf{Z} + b\mathbf{Z} = \{a.k + b.\ell,\ (k, \ell) \in \mathbf{Z}^2\}$. Les asse

$\Updownarrow$
- $d = a \wedge b$
- $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$
- $\mathcal{D}(a, b) = \mathcal{D}(d)$

Généralisation : Soit $a_1, a_2, \ldots, a_n$ des entiers non tous nuls. L'ensemble des diviseurs communs à a_1, a_2, …, a_n admet un plus grand élément, appelé **plus grand commun diviseur** et noté $PGCD(a_1, a_2, \ldots, a_n)$.

Proposition.— Relation de Bezout —. Soit $(a_1, \ldots, a_n) \in \mathbf{Z}^n$, $d = PGCD(a_1, \ldots, a_n)$. Alors il existe $(u_1, u_2, \ldots, u_n) \in \mathbf{Z}^n$ tel que $d = a_1u_1 + a_2u_2 + \cdots + a_nu_n$

PPCM de deux entiers

L'ensemble des multiples communs à a et b est noté $a\mathbf{Z} \cap b\mathbf{Z}$.

Définition : *Soit $(a, b) \in (\mathbf{Z}^\star)^2$ un couple d'entiers relatifs, non nuls. Le plus petit élément strictement positif de $a\mathbf{Z} \cap b\mathbf{Z}$ est appelé **plus petit multiple commun** à a et b. Cet entier naturel est noté $PPCM(a, b)$ ou encore $a \vee b$.*

Théorème.— Caractérisation du PPCM —. Soit $(a, b) \in \mathbf{Z}^2$. Pour tout entier **naturel** $m \in \mathbf{N}$, les asse :

$\Updownarrow$
- $m = a \vee b$
- $a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z}$

Entiers premiers entre eux

Définition : *Soit $(a, b) \in \mathbf{Z}^2$. On dit que a et b sont **premiers entre eux** si $\mathcal{D}(a, b) = \{\pm 1\}$.*

Remarque : a et b sont premiers entre eux si et seulement si $a \wedge b = 1$.

Théorème.— Théorème de Bezout —. Soit $(a, b) \in \mathbf{Z}^2$.

$$\boxed{a \wedge b = 1 \iff \exists (u, v) \in \mathbf{Z}^2,\ au + bv = 1}$$

Proposition.— Soit $(a, b, c) \in \mathbf{Z}^3$. a et le produit bc sont premiers entre eux *ssi* a est premier avec b et c.

Théorème.— Théorème de Gauss —. Soit $(a,b,c) \in \mathbf{Z}^3$.

$$\boxed{\left.\begin{array}{l}\bullet \quad a \mid b \times c \\ \bullet \quad a \wedge b = 1\end{array}\right) \Rightarrow a \mid c.}$$

Proposition.— Soit $(a,b,c) \in \mathbf{Z}^3$. Si a et b divisent c et $a \wedge b = 1$, alors $a \times b$ divise c.

Proposition*.— Produit du PGCD et du PPCM —. Soit $(a,b) \in \mathbf{Z}^2$, alors

$$\boxed{(a \wedge b) \times (a \vee b) = |ab|}$$

Application : résolution dans $\mathbf{Z}^2$ des équations diophantiennes $(E) \quad ax + by = c$.

■■■ Nombres premiers

Définition : *On appelle* ***nombre premier*** *tout entier naturel $p \geq 2$ dont les seuls diviseurs dans $\mathbf{N}$ sont 1 et p lui-même. Un entier naturel $n \geq 2$ qui n'est pas premier est dit* ***composé****. Dans ce cas, il existe un entier $k \in \mathbf{N}$, $1 < k < n$ tel que $k \mid n$. On note $\mathfrak{P}$ l'ensemble des nombres premiers.*

Proposition*.— Tout entier $n \geq 2$ admet au moins un diviseur premier. Si de plus n est composé, alors il admet un diviseur premier p vérifiant $p \leq \sqrt{n}$.

Théorème*.— L'ensemble $\mathfrak{P}$ des nombres premiers est infini.

Théorème*.— Décomposition primaire d'un entier —. Soit $n \in \mathbf{N}$, $n \geq 2$. Il existe alors des nombres premiers $p_1, p_2, \ldots, p_N$ (avec $p_1 < p_2 < \cdots < p_N$), et des entiers naturels non nuls $\alpha_1, \alpha_2, \ldots, \alpha_N$, uniques, tels que :

$$\boxed{n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_N^{\alpha_N}.}$$

Proposition*.— Diviseurs positifs d'un entier —. Soit $n \in \mathbf{N}$, $n \geq 2$, décomposé sous la forme d'un produit de facteurs premiers $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_N^{\alpha_N}$. Les diviseurs positifs de n sont tous les entiers naturels qui s'écrivent sous la forme

$$\boxed{d = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_N^{\beta_N}, \text{ où } 0 \leq \beta_i \leq \alpha_i}$$

Théorème*.— Factorisation du PGCD et du PPCM en produit de nombres premiers —. Soit $(a,b) \in \mathbf{N}^2$, deux entiers naturels supérieurs ou égaux à 2 donnés par $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_N^{\alpha_N}$ et $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_N^{\beta_N}$, où $p_1, p_2, \ldots, p_N$ sont des entiers premiers 2 à 2 distincts, et les exposants, (α_i), (β_i) sont des entiers naturels. Alors

$$\boxed{\bullet\ a \wedge b = p_1^{\min(\alpha_1,\beta_1)} \times p_2^{\min(\alpha_2,\beta_2)} \times \cdots \times p_N^{\min(\alpha_N,\beta_N)} \qquad \bullet\ a \vee b = p_1^{\max(\alpha_1,\beta_1)} \times p_2^{\max(\alpha_2,\beta_2)} \times \cdots \times p_N^{\max(\alpha_N,\beta_N)}}$$

■■■ Congruences

Définition : *Soit $n \in \mathbf{N}^\star$, $(a,b) \in \mathbf{Z}^2$. On dit que a* ***est congru à*** *b* ***modulo*** *n, et on note $a \equiv b\ [n]$ si n divise $b - a$.*

Proposition.— Compatibilité avec les opérations —. Soit $n \in \mathbf{N}^\star$, $(a,b,c,d) \in \mathbf{Z}^4$.
Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ **alors** $a + c \equiv b + d\ [n]$ et $a \times c \equiv b \times d\ [n]$.

Théorème.— Petit théorème de Fermat —. Soit $p \in \mathfrak{P}$ un nombre premier.

- ■ Pour tout entier $n \in \mathbf{Z}$, on a $n^p \equiv n\ [p]$.
- ■ Pour tout entier $n \in \mathbf{Z}$ tel que $p \wedge n = 1$, on a $n^{p-1} \equiv 1\ [p]$.