Prof : SAKAT	**ARITHMETIQUE**	1°BAC . SM

Division Euclidienne-divisibilité :

Division Euclidienne :

$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{N}^*)(\exists!\,(q,r) \in \mathbb{Z}^2)$:

$0 \le r < b$ et $a = bq + r$.

a est appelé dividende, b :diviseur, q :quotient et r:le reste.

Divisibilité :

Soit $(a, b) \in \mathbb{Z}^2$.

On dit que :a est divisible par b , b divise a où a un multiple de b,et on écrit a/b si :

$[a/b] \Leftrightarrow [(\exists q \in Z): a = bq]$

Propriétés

a/a ; $(a/b \text{ et } b/c) \Rightarrow a/c$

$(a/b \text{ et } b/a) \Rightarrow |a| = |b|$

$(a/b \text{ et } c/d) \Rightarrow ac/bd$

$a^n/b \Rightarrow a/b$

$(a/b \text{ et } a/c) \Rightarrow (a/bc \text{ et } a/b + c)$

$(a/b \text{ et } a/c) \Rightarrow (\forall(\alpha,\beta)\epsilon\mathbb{Z}^2): a/\alpha b + \beta c$

PPCM – PGCD :

PGCD: Symbole

$a \wedge b$: *le plus grand diviseur commun strictement positif de a et b.*

Propriétés

$d = a\wedge b \Leftrightarrow (\exists (a', b') \in \mathbb{Z}^2): \begin{cases} a = d.a' \\ b = d.b' \end{cases}$ et $a'\wedge b' = 1$

$\begin{cases} c/a \\ c/b \end{cases} \Rightarrow c/a\wedge b$; $(ca)\wedge(cb) = |c|.a\wedge b$

PPCM : Symbole

$a \vee b$: *le plus petit multiple commun strictement positif de a et b.*

Propriétés

$\begin{cases} a/c \\ b/c \end{cases} \Rightarrow a\vee b/c$

$\forall (a,b) \in \mathbb{Z}^2 : (a\wedge b).(a\vee b) = |ab|$

NOMBRES PREMIERS:

Définition :

Un nombre entier p est dit premier si :

$|p| \neq 1$ et $D_p = \{-1, 1, -p, p\}$

D_p désigne l'ensemble des diviseurs de p.

Propriétés:

Soit p un nombre premier ;on a :

$(p/ab) \Rightarrow (p/a \text{ ou } p/b)$; $(p/a^n) \Rightarrow p/a$

$(p/a_1 a_2 \dots a_n) \Rightarrow \exists i \in (1, 2 \dots n): p/a_i$

$(p/a) \Rightarrow (p\wedge a = p)$; $(p \text{ ne divise pas } a) \Rightarrow (p\wedge a = 1)$

DECOMPOSITION EN PRODUIT DE NOMBRES PREMIERS :

$\forall n \in \mathbb{Z} - \{-1, 1\}$, n s'écrit de facon unique sous la forme :$n = \varepsilon\, p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ *ou* $(p_1, p_2 \dots p_k)$ *des nombres premiers distincts* Et $\alpha_1, \alpha_2 \dots \alpha_k$ *des éléments de* $\mathbb{N}^*$

Soit $a = \varepsilon\, p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ la décomposition d'un entier naturel non nul en produit de facteurs premiers.Le nombre de diviseurs de a est : $(1 + \alpha_1)(1 + \alpha_1) \dots (1 + \alpha_k)$

Si $|a| = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ et $|b| = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$

alors $a\wedge b = p_1^{c_1} p_2^{c_2} \dots p_k^{c_k}$ et $a\vee b = p_1^{d_1} p_2^{d_2} \dots p_k^{d_k}$ où $c_i = inf(a_i, b_i)$ et $d_i = sup(a_i, b_i)$ $\forall i \in \{1, 2 \dots k\}$

NOMBRES PREMIERS ENTRE EUX:

Définition :

a et b premiers entre eux $\Leftrightarrow (a\wedge b = 1)$

Théorème de Gauss:

$(c/ab \text{ et } c\wedge a = 1) \Rightarrow (c/b)$

Propriétés:

$(a/c\,;\, b/c \text{ et } a\wedge b = 1) \Rightarrow (a.b/c)$

$(a\wedge b = 1 \text{ et } a\wedge c = 1) \Rightarrow (a\wedge(b.c) = 1)$

$(a\wedge b = 1) \Leftrightarrow \forall (m, n) \in \mathbb{N}^* \times \mathbb{N}^* : a^n \wedge b^m = 1$

Algorithme d'Euclide :

$(a = bq + r \text{ et } 0 \le r < b) \Rightarrow (a\wedge b = b\wedge r)$

CONGRUANCE MODULO N :

Congruance modulo n :

Soient : $n \in \mathbb{N}, (a, b) \in \mathbb{Z}^2$. On dit que a est congru à b modulo n et on écrit :$a \equiv b[n]$

$a \equiv b[n] \Leftrightarrow (\exists k \in \mathbb{Z}): a - b = nk$

Propriétés:

$a \equiv b[n] \Leftrightarrow (\exists k \in \mathbb{Z}): a - b = nk \Leftrightarrow n/a - b$

$\begin{cases} a \equiv b[n] \\ c \equiv d[n] \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d[n] \\ a.c \equiv b.d[n] \end{cases}$

ENSEMBLE DES CLASSES D'EQUIVALENCE :

Définition :

Soit n un entier naturel non nul.La classe d'équivalence de l'entier relatif a est l'ensemble $\bar{a}$ tel que : $\bar{a} = \{b \in \mathbb{Z} \,/\, b \equiv a[n]\}$

On pose : $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2} \dots, \overline{n-2}, \overline{n-1}\}$

Et on a : $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \dots \cup \overline{n-2} \cup \overline{n-1}$

$(\forall a \in \mathbb{Z})(\exists!\, r \in \{1, 2 \dots n-1\}): \bar{a} = \bar{r}$

On définit la somme et le produit dans $\mathbb{Z}/n\mathbb{Z}$ Comme suit :

$\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \times \bar{b} = \overline{a \times b}$

Propriétés:

$(\bar{a} = \bar{b}) \Leftrightarrow (a \equiv b[n])$

$(\bar{a} \cap \bar{b} = \emptyset) \Leftrightarrow (a \not\equiv b[n])$

$(0 \le a < n \text{ et } 0 \le c < n) \Rightarrow (\bar{a} = \bar{c} \Leftrightarrow a = c)$