I. Division euclidienne/ divisibilité /congruence

Division euclidienne

Quels que soit le nombre entier relatif a, quel que soit l'entier naturel non nul b, il existe deux entiers uniques q et r tels que :

$a = b.q + r$ et $0 \le r \prec b$

Divisibilité

a et b sont deux entiers relatifs, on dit que b divise a (a est multiple de b) si et seulement si, il existe un entier k tel que :

$a = b.q$

congruence

n est un entier naturel non nul donné. a et b sont deux entiers relatifs. On dit que a est congrus à b modulo n si et seulement si, il existe k dans Z tel que : a – b = k.n

On écrit : a≡b[modulo]

II. Propriétés de la divisibilité et de la congruence

Divisibilité

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

$(\delta/a \text{ et } \delta/b) \Rightarrow (\forall(\alpha,\beta) \in Z^2)\ ;\ \delta/\alpha.a + \beta.b$

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

congruence

$a \equiv b\,[n] \Leftrightarrow a - b = k.n \Leftrightarrow n/a - b$

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

III. PGDC et PPMC

Plus grand diviseur commun

on le note : $d = pgdc(a,b) = a \wedge b$

Le pgcd vérifie les propriétés suivantes :

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

$\begin{cases} d'/a \\ d'/b \end{cases} \Rightarrow d'/a \wedge b$

Plus petit multiple commun

on le note : $m = ppmc(a,b) = a \vee b$

Le ppmc vérifie les propriétés suivantes :

$(m = a \vee b) \Rightarrow \begin{cases} a/m \\ b/m \end{cases}$

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

Propriété commune

$\forall(a,b) \in Z^2; (a \vee b).(a \wedge b) = |a.b|$

IV. Nombres premiers entre eux / Bezzout / Gauss/Propriétés

Nombres premiers entre eux

On dit que les entiers a et b sont premiers entre eux si et seulement si pgcd (a,b)=1.

Identité de Bezzout

$(a \wedge b = 1) \Leftrightarrow (\exists(u,v) \in Z^2\ ;\ a.u + b.v = 1)$

Conséquence :

$(a \wedge b = d) \Leftrightarrow (\exists(u,v) \in Z^2\ ;\ a.u + b.v = b)$

Théorème de Gauss :

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

Autres propriétés :

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

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

$(a \wedge b = 1) \Leftrightarrow \forall(m,n) \in IN^* x IN^*\ ;\ (a^m \wedge b^n = 1)$

$(a = b.q + r \text{ et } 0 \le r \prec b) \Rightarrow (a \wedge b = r \wedge b)$

V. Nombres premiers / Propriétés

Un nombre entier est premier s'il a exactement deux diviseurs positifs : 2, 3, 5 ,7 etc.... 1 et -1 ne sont pas premiers...

L'ensemble des nombres premiers est infini.

Propriétés : *soit p premier on a :*

$(p/a.b) \Rightarrow (p/a \text{ ou } p/b)$

$(p/a^n) \Rightarrow (p/a)$

$(p/a_1.a_2...a_n) \Leftrightarrow \exists i \in (1,2,...,n)\ ;\ (p/a_i)$

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

VI. Algorithme d'Euclide

Soient deux entiers naturels a et b tels que a > b :
On divise a (le plus grand) par b, on obtient :

(1) : $a = b.q_0 + r_0$ et $0 \le r_0 \prec b$

Si r_0=0 alors b divise a et pgcd(a,b)=b

Si r_0#0 On divise b par r_0, on obtient :

(2) : $b = r_0.q_1 + r_1$ et $0 \le r_1 \prec r_0 \prec b$

Si r_1=0 alors pgcd(a,b)=pgcd(b,r_0)=r_0

Si r_1#0 On divise r_0 par r_1, on obtient :

etc

Après un certains nombre d'opération, on obtient un reste nul (en effet la suite des restes est une suite décroissante de nombres entiers), soit r_n, le dernier reste non nul de cette suite, on alors :

pgcd(a,b)=pgcd(b,r_0)=…= pgcd(r_{n-1} , r_n)=r_n

VII. Décomposition d'un entier en un produit de facteurs premiers

Tout nombre entier naturel non nul et différent de 1 , se décompose d'une manière unique sous la forme :

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_n^{\alpha_n}$$

Où les nombres pi sont des nombres premiers et les αi sont des entiers naturels non nuls.

VIII. L'ensemble des classes d'équivalence Z/n.Z

La relation de congruence :

$$a \equiv b\,[n] \Leftrightarrow a - b = k.n \Leftrightarrow n \,/ a - b$$

Est une relation d'équivalence dans Z, compatible avec la somme et le produit:

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

La classe d'équivalence d'un entier relatif x est l'ensemble défini par :

$$\alpha = \bar{x} = \{ y \in Z \,/\; y \equiv x [\text{modulo } n] \}$$

L'ensemble qui contient toutes les classes d'équivalence modulo n est noté : Z/n.Z

$$Z/n.Z = \{ \bar{0} , \bar{1} , \bar{2} , \bar{3} , ..., \overline{n-2} , \overline{n-1} \}$$

Dans Z/n.Z, on définit la somme etr le produit des classes, de la façon suivante :

$$\begin{cases} \bar{a} + \bar{b} \equiv \overline{a+b} \\ \bar{a}.\bar{b} \equiv \overline{a.b} \end{cases}$$

(Z/n.Z , + , x) est un anneau commutatif unitaire, en général non intègre.

Si n est premier, alors Z/n.Z est un corps.

$$\left(\bar{a} \text{ inversible dans } Z/n.Z\right) \Leftrightarrow (a \wedge n = 1)$$

IX. La numération

Soit x un entier nature supérieur ou égal à 2.
Tout entier b de In peut s'écrire sous la forme :

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

Où

$$a_n \neq 0 \quad \text{et} \quad (\forall i \in [0, n]) \;;\; a_i \in [0, n-1]$$

On écrit :

(1) : $b = \overline{a_n a_{n-1} ... a_1 a_0}^{\,(x)}$

Et on dit que l'écriture (1) est l'écriture du nombre b dans le système de numération de base x .

X. Détermination du pgdc(a,b) et du ppmc(a,b)

Soient :

$$a = \prod_{i=1}^{n} p_i^{\alpha_i} \quad \text{et} \quad b = \prod_{i=1}^{n} p_i^{\beta_i}$$

La décomposition en facteurs premiers de a et b, on obtient :

$$a \wedge b = \prod_{i=1}^{n} p_i^{\inf(\alpha_i, \beta_{i'})}$$

$$a \vee b = \prod_{i=1}^{n} p_i^{\sup(\alpha_i, \beta_{i'})}$$