Divisibilité dans N et Z

I. Quelques rappels

1. L'ensemble des entiers naturels

a. Définition

$$\mathbb{N} = \{0;1;2;3;4;5;6;.....\}$$

$\mathbb{N}$ est l'ensemble des entiers positifs ou nuls.

b. Stabilité

Propriété 01

$\mathbb{N}$ est stable par addition et multiplication seulement.

$$\forall n \in \mathbb{N}, \forall m \in \mathbb{N},\ n+m \in \mathbb{N} \text{ et } n \times m \in \mathbb{N}$$

Par contre $\mathbb{N}$ n'est pas stable pour la soustraction et la division.

c. Quelques axiomes

Axiome 01 :
Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
Axiome 02 :
Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand Elément.
Axiome 03 :
Toute suite d'entiers naturels strictement décroissante est stationnaire à partir d'un certain rang.

2. L'ensemble des entiers relatifs

a. Définition

$$\mathbb{Z} = \{.....;-5;-4;-3;-2;-1;0;1;2;3;4;5;.....\}$$

b. Propriétés

Propriété 02 :

$\mathbb{Z}$ est stable par addition, soustraction et multiplication seulement.

$$\forall n \in \mathbb{Z}, \forall m \in \mathbb{Z},\ n+m \in \mathbb{Z}, n-m \in \mathbb{Z} \text{et } n \times m \in \mathbb{Z}$$

Par contre $\mathbb{Z}$ n'est pas stable pour la division.

Propriété 03 :

Tout nombre entiers relatif, admet un opposé entier relatif

$$\forall n \in \mathbb{Z},\quad -n \in \mathbb{Z}$$

Propriété 04 :

Tout entier naturel est un entier relatif. $\mathbb{N} \subset \mathbb{Z}$

$$\forall n \in \mathbb{N},\quad n \subset \mathbb{Z}$$

c. Quelques axiomes

Dans $\mathbb{Z}$, l'axiome 01 et l'axiome 03 sont faux mais par contre l'axiome 03 reste vrai.

Axiome 03 bis :

Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément

II. Divisibilité dans $\mathbb{Z}$

1. Multiple d'un entier.

On note n et m deux entiers relatifs

Définition :

On dit que ***m* est un multiple de *n*** si et seulement si il existe un entier relatif k tel que $m = nk$

2. Diviseur d'un entier

On note n et m deux entiers relatifs avec $n \neq 0$

Définition :

On dit que ***n* est un diviseur de *m*** (ou **que *n* divise *m***) si et seulement si il existe un entier relatif k tel que $m = nk$. (m est un multiple de n)

Notation :

On notera $n \mid m$ pour dire que n divise m

Quelques remarques :

- $\forall n \in \mathbb{Z},\quad 1 \mid n$ et $-1 \mid n$
- $\forall n \in \mathbb{Z},\quad n \mid 0$
- $\forall n \in \mathbb{Z}$, n admet au moins quatre diviseurs $\{-n;-1;1;n\}$

3. Propriétés sur la divisibilité.

Propriété 05

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}^*,\quad b \mid a \Rightarrow -b \mid a$$

Propriété 06

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}^*,\quad b \mid a \text{ et } a \neq 0 \Rightarrow |b| \leq |a|$$

Propriété 07

$$\forall a \in \mathbb{Z}^*, \forall b \in \mathbb{Z}^*, c \in \mathbb{Z},\quad b \mid a \text{ et } a \mid c \Rightarrow b \mid c$$

Propriété 08

$$\forall a \in \mathbb{Z}^*, \forall b \in \mathbb{Z}^*,\quad b \mid a \text{ et } a \mid b \Rightarrow a = -b \text{ ou } a = b$$

Propriété 08

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}^*,\quad b \mid a \Rightarrow \forall c \in \mathbb{Z}, b \mid ac$$

Propriété 09

$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}^*, c \in \mathbb{Z}, \quad b \mid a$ et

$b \mid c \Rightarrow \forall u \in \mathbb{Z}, \forall v \in \mathbb{Z}, \quad b \mid au + cv$

On dit que si $b \mid a$ et $b \mid c$ alors b divise toute combinaison linéaire de a et de c.

Propriété 10

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}^*, \quad b \mid a \Rightarrow \forall c \in \mathbb{Z}^*, bc \mid ac$$

III. La division Euclidienne dans $\mathbb{N}$ et $\mathbb{Z}$

1. La division euclidienne dans $\mathbb{N}$

a. Théorème

On note $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$

Théorème

Il existe un couple unique (q,r) d'entiers naturels tels que

$$a = bq + r \text{ avec } 0 \leq r < b$$

On dit alors que q est le **quotient** et r le **reste** de la division euclidienne de b par a.

2. Le division euclidienne dans $\mathbb{Z}$

a. Théorème

On note $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$

Théorème

Il existe un couple unique (q,r) d'entiers relatifs tels que

$$a = bq + r \text{ avec } 0 \leq r < |b|$$

Remarque : r est toujours positif

On dit alors que q est le **quotient** et r le **reste** de la division euclidienne de b par a.

3. Application au changement de système de numération.

En base 10 (**système décimal**, le système de numération que l'on utilise) les nombres s'expriment à l'aide des puissances de 10 et des chiffres

$$\{0;1;2;3;4;5;6;7;8;9\}$$

Théorème :

Pour tout $m \in \mathbb{N}$, il existe $n \in \mathbb{N}$ tel que

$$m = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \ldots + a_2 \times 10^2 + a_1 \times 10 + a_0 = \sum_{k=0}^{n} a_k 10^k$$

Où la suite (a_n) est une suite d'éléments de $\{0;\ldots;8;9\}$

On peut écrire m, en base 2 (**système binaire**), en base 3 (**système trinaire**), en base 16 (**système hexadécimal**), en base 60 (**système sexagésimal** : système horaire), etc…

La base 2 (**système binaire**) avec les chiffres 0 et 1, est souvent utilisé en électronique et en informatique. (le courant passe ou ne passe pas)

La base 16 (**système hexadécimal**) est souvent utilisée en informatique(Exemple : le codage des couleurs des écrans) .
Les chiffres de ce système sont :
$\{0,1,2,3,4,5,6,7,8,9,A;B;C;D;E;F\}$

- Dans le système binaire, les nombres s'écrivent sous la forme :

$$\overline{m}^{2} = a_n \times 2^n + a_{n-1} \times 2^{n-1} + \ldots + a_2 \times 2^2 + a_1 \times 2 + a_0 = \sum_{k=0}^{n} a_k 2^k$$

Où la suite (a_n) est une suite d'éléments de $\{0;1\}$

- Dans le système hexadécimal, les nombres s'écrivent sous la forme :

$$\overline{m}^{16} = a_n \times 16^n + a_{n-1} \times 16^{n-1} + \ldots + a_2 \times 6^2 + a_1 \times 16 + a_0 = \sum_{k=0}^{n} a_k 16^k$$

Où la suite (a_n) est une suite d'éléments de

$$\{0;1;2;3;4;5;6;7;8;9;A;B;C;D;E;F\}$$

Congruence dans Z

IV. Congruence dans $\mathbb{Z}$

1. Définition

Définition

On note $n \geq 2$ un entier naturel et a et b deux entiers relatifs. On dit que a et b sont congrus modulo n et on note $a \equiv b\,[n]$ si la différence $a-b$ est un multiple de n ou si $n \mid (a-b)$

2. Propriétés

On note n et n' deux entiers naturels ≥ 2 et a et b deux entiers relatifs.

Propriété 01

$$a \equiv 0\,[n] \quad \Leftrightarrow \quad n \mid a$$

Propriété 02

Si $n' \mid n$ alors $a \equiv b\,[n] \quad \Rightarrow \quad a \equiv b\,[n']$

Propriété 03

$a \equiv b\,[n] \quad \Leftrightarrow$ les divisions euclidiennes de a et b par n ont le même reste.

V. Congruences et opérations

On note a, a', b et b' quatre entiers relatifs quelconques.

1. Addition.

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

2. Soustraction.

$$\begin{cases} a \equiv a'\,[n] \\ b \equiv b'\,[n] \end{cases} \Rightarrow a-b \equiv a'-b'\,[n]$$

3. Produit par un entier relatif.

$$\begin{cases} a \equiv a'\,[n] \\ k \in \mathbb{Z} \end{cases} \Rightarrow ka \equiv ka'\,[n]$$

4. Produit.

$$\begin{cases} a \equiv a'\,[n] \\ b \equiv b'\,[n] \end{cases} \Rightarrow a \times b \equiv a' \times b'\,[n]$$

5. Puissance d'un entier naturel.

$$\begin{cases} a \equiv a'\,[n] \\ p \in \mathbb{N} \end{cases} \Rightarrow a^p \equiv a'^p\,[n]$$

PGCD et PPCM

VI. PGCD et PPCM de deux entiers relatifs

1. Définition

Définition :

On note $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}^*$

- Le $PGCD(a,b)$ est le plus grand diviseur commun de a et b
- Le $PPCM(a,b)$ est le plus petit multiple commun de a et b

Définition : Nombres étrangers ou **premiers entre eux**

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

Le seul diviseur commun positif est 1.

2. Méthodes de calcul du PGCD

a. Liste des diviseurs

Il suffit de faire la liste des diviseurs des deux nombres et de trouver le plus grand des diviseurs communs.

b. Algorithme d'Euclide

On effectue des divisions euclidiennes successives en prenant à chaque fois le diviseur et le reste de la division précédente.

$$\begin{aligned} a &= bq_1 + r_1 \quad \textbf{avec} \quad 0 \le r_1 < b \\ &\vdots \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \quad \textbf{avec} \quad 0 \le r_n < r_{n-1} \end{aligned}$$

Théorème :

On note $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}^*$

$$PGCD(a,b) = PGCD(b, MOD(a,b))$$

Où $MOD(a,b)$ est le reste de la division euclidienne de a par b.

c. Algorithme des soustractions

On effectue des soustractions successives.

$$a - b = r_1$$

Si $b < r_1$ $b \to c$ $r_1 \to b$ $c \to r_1$ et $b - r_1 = r_2$

Si $r_1 < r_2$ $r_1 \to c$ $r_2 \to r_1$ $c \to r_2$ et $r_1 - r_2 = r_3$

$\vdots$

$\vdots$

Si $r_{n-2} < r_{n-1}$ $r_{n-2} \to c$ $r_{n-1} \to r_{n-2}$ $c \to r_{n-1}$ et

$$r_{n-2} - r_{n-1} = r_n$$

Théorème :

On note $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}^*$

$$PGCD(a,b) = PGCD(b, a-b)$$

d. Décomposition en facteurs premiers

Exemple $a = 2^3 \times 3^2 \times 5 \times 7^2$ et $b = 2^1 \times 3^3 \times 5^4 \times 7 \times 11$

3. Méthodes de calcul du PPCM

a. Liste des multiples

Exemple : $PPCM(6,4)$

b. Décomposition en facteurs premiers

Exemple : $PPCM(2^3 \times 3^1, 2^2 \times 3^2 \times 5^3)$

c. Formule reliant le PGCD et le PPCM

Théorème : a et b sont deux entiers relatifs non nuls

$$PGCD(a,b) \times PPCM(a,b) = ab$$

VII. Théorèmes importants en arithmétique

1. Théorème de BEZOUT

Théorème de BEZOUT

Pour tout couple $(a,b) \in \mathbb{Z}^{*2}$, il existe un couple $(u,v) \in \mathbb{Z}^2$ tel que

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

2. Propriété de BEZOUT

Propriété de BEZOUT

a et b sont premiers entre eux

$\Leftrightarrow$

$\exists (u,v) \in \mathbb{Z}$ tel que $au + bv = 1$

3. Théorème de GAUSS

Théorème de GAUSS

a, b *et* c sont des entiers relatifs non nuls

$$a \mid bc \quad et \quad PGCD(a,b) = 1 \quad \Rightarrow \quad a \mid c$$

Equations Diophantiennes

VIII. Définition

1. Définition

Définition

Une équation diophantienne est une équation à coefficients entiers et dont les inconnues sont des entiers.

Cette année, de terminale, nous ne résolvons que les équations de la forme $ax+by=k\times PGCD(a,b)$

2. Exemples de l'année de terminale

- $5x+7y=1$
- $6x+15y=3$
- $5x-8y=2$

IX. Méthode de résolution

1. Méthode théorique

On souhaite résoudre l'équation diophantienne

$$ax+by=k\times PGCD(a,b) \quad (E)$$

- **Première étape :** Recherche d'une solution particulière de (E)

  On calcule le $PGCD(a,b)$ par l'algorithme d'Euclide.

  On cherche une solution particulière (x_1,y_1) telle que

  $$ax_1+by_1=PGCD(a,b)$$

  Le couple $(\ldots\ldots,\ldots\ldots)$ est donc une solution particulière de (E)

  On note (x_0,y_0) ce couple

- **Deuxième étape :** Recherche de toutes les solutions de (E)

  On note (x,y) un couple solution donc

  $$ax+by=k\times PGCD(a,b)$$

  (x_0,y_0) est une solution particulière de (E) donc

  $$ax_0+by_0=k\times PGCD(a,b)$$

  Par soustraction des deux équations, on obtient :

  $$a(x-x_0)+b(y-y_0)=\ldots\ldots$$

  On a donc $a(x-x_0)=b(y_0-y_0)$ et en divisant par $PGCD(a,b)$

  on obtient que $a'(x-x_0)=b'(y_0-y_0)$ avec $PGCD(a,b')=1$

On a alors $b' \mid a'(x-x_0)$ avec a' et b' premiers entre eux.

D'après le théorème de Gauss : $b' \mid (x-x_0)$ donc il existe un

entier relatif δ tel que $x = x_0 + \delta b'$

de plus

$a'(x-x_0) = b'(y_0 - y) \Leftrightarrow a'b'\delta = b'(y_0 - y) \Leftrightarrow y = y_0 - a'\delta$

On obtient donc $S = \left\{ \left(x_0 + \delta b', y_0 - a'\delta \right), \delta \in \mathbb{Z} \right\}$

- **Vérification :**

$ax + by = a(x_0 + \delta b') + b(y_0 - a'\delta) = ax_0 + by_0 + \delta ab' - \delta ba'$

or $a = PGCD(a,b) \times a'$ et $b = PGCD(a,b) \times b'$ donc

$\delta ab' - \delta ba' = 0$

De plus $ax_0 + by_0 = k \times PGCD(a,b)$

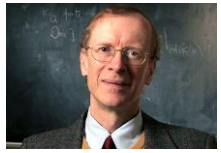
Donc $ax + by = k \times PGCD(a,b)$

Quelques personnalités importantes du chapitre

GAUSS

BEZOUT

D'ALEMBERT



WILES