Chapitre mpsi: arithmétique

HEI 1 - 2011/2012

I. Divisibilité et division euclidienne dans $\mathbb{Z}$

1. Divisibilité

Définition.

Etant donnés a et b deux entiers relatifs, on dit que a est un diviseur de b ou que b est un multiple de a s'il existe $k \in \mathbb{Z}$ tel que $b = ka$.

Notation.
- Si a divise b, on note $a|b$
- L'ensemble des diviseurs de b est noté $\mathcal{D}(b)$
- L'ensemble des multiples de a est noté $a\mathbb{Z}$

Exemple.
- 1 et -1 divisent tous les entiers mais ne sont divisibles que par 1 et -1
- 0 est multiple de tous les entiers mais n'est diviseur que de lui-même

Remarque. La relation de divisibilité dans $\mathbb{Z}$ est réflexive et transitive mais n'est pas une relation d'ordre car elle n'est pas antisymétrique, contrairement à la divisibilité dans $\mathbb{N}$. D'ailleurs, pour cet ordre (partiel), le plus petit élément est 1 et le plus grand est 0. Enfin, la divisibilité dans $\mathbb{N}^*$ est liée à l'ordre (total) naturel de $\mathbb{N}^*$:

$$a|b \Rightarrow a \leq b$$

2. Division euclidienne

Propriété.

Etant donné $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tel que :

$$a = bq + r, \;\; 0 \leq r < |b|$$

Définition.

Déterminer les entiers q et r, c'est effectuer la division euclidienne de a par b.
a est le dividende, b le diviseur, q le quotient et r le reste dans la division euclidienne de a par b.

Exemple.
- Division de -56 par 17
- Division de 32 par -7

II. PGCD - PPCM

1. PGCD

a. Définition et caractérisation

Définition.

Le PGCD de a et b, noté $a \wedge b$, est le plus grand commun diviseur de a et b si $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, et 0 si $(a, b) = (0, 0)$.

Propriété.

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

$$d = a \wedge b \Leftrightarrow \begin{cases} d \geq 0 \\ d|a \text{ et } d|b \\ \forall d' \in \mathbb{Z},\ (d'|a \text{ et } d'|b) \Rightarrow d'|d \end{cases}.$$

Remarque.
- $\forall (a, b) \in \mathbb{Z}^2,\ a \wedge b = |a| \wedge |b|$
- $\forall a \in \mathbb{Z},\ a \wedge 0 = |a|$

Définition.

Deux entiers a et b non nuls sont dits premiers entre eux lorsque $a \wedge b = 1$.

b. Théorème de Bézout et théorème de Gauss

Théorème (de Bézout)**.**

Etant donnés a et b des entiers non nuls,

$$a \wedge b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2,\ ua + vb = 1$$

Théorème (de Gauss)**.**

Etant donnés a, b et c des entiers non nuls,

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

c. Théorème d'Euclide et Algorithme d'Euclide

Théorème (d'Euclide)**.**

Etant donnés a, b, q et r des entiers non nuls,

$$a = bq + r \Rightarrow a \wedge b = b \wedge r$$

L'algorithme d'Euclide qui a pour objet le calcul du pgcd de deux entiers naturels est basé sur le théorème précédent, dans le cas particulier où $a = bq + r$ exprime la division euclidienne de a par b, c'est à dire lorsque $0 \leq r < b$:
- On divise a par b, en notant q_1 et r_1 respectivement les quotient et reste.
- Si $r_1 = 0$, alors $a \wedge b = b$.
  Sinon, on utilise le théorème d'Euclide : $a \wedge b = b \wedge r_1$ pour être ramené au cas précédent.
- En itérant cette opération, on obtient un reste nul au bout d'un nombre fini s d'étapes (la suites des restes successifs étant strictement décroissante et minorée par 0).
- On a alors :

$$a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = ... = r_{s-1} \wedge r_s = r_{s-1}$$

En résumé, le PGCD de a et b est le dernier reste non nul dans la suite des divisions euclidiennes successives.

Exemple. Le PGCD de $a = 18480$ et $b = 9828$ est 84.
En "remontant" la suite des divisions euclidiennes successives, on obtient : $84 = 25a - 47b$

d. Equations diophantiennes

Etant donnés A, B et C des entiers non nuls, on donne une méthode de résolution de :

$$Ax + By = C,\ (x, y) \in \mathbb{Z}^2$$

Propriété.

L'équation $Ax + By = C$ a des solutions entières si et seulement si $A \wedge B$ divise C.

Exemple. Résoudre l'équation $29x - 25y = -3,\ (x, y) \in \mathbb{Z}^2$

2. PPCM

Définition.

Le PPCM de a et b, noté $a \vee b$, est le plus petit commun multiple strictement positif de a et b si $ab \neq 0$, et 0 sinon.

Propriété.

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

$$m = a \vee b \Leftrightarrow \begin{cases} m \geq 0 \\ a|m \text{ et } b|m \\ \forall m' \in \mathbb{Z},\ (a|m' \text{ et } b|m') \Rightarrow m|m' \end{cases}.$$

Remarque.
- $\forall (a, b) \in \mathbb{Z}^2,\ a \vee b = |a| \vee |b|$
- $\forall a \in \mathbb{Z},\ a \vee 0 = 0$

Théorème.

Etant donnés a et b des entiers non nuls,

$$(a \wedge b)(a \vee b) = |ab|$$

III. Nombres premiers

On se limite ici à $\mathbb{N}$.

1. Définitions et premières propriétés

Définition.

Un entier est dit premier lorsqu'il admet exactement deux diviseurs : 1 et lui-même.

Propriété.

Tout entier $n \geq 2$ admet au moins un diviseur premier.

Corollaire.

L'ensemble $\mathbb{P}$ des entiers naturels premiers est infini.

Propriété.

Un nombre premier est premier avec tous les entiers qu'il ne divise pas.
En particulier, si p est premier, alors $p \wedge k = 1$ pour tout $k \in \{1, ..., p-1\}$.

Théorème.

Si un nombre premier divise un produit fini d'entiers non nuls, alors il divise l'un d'eux.

2. Décomposition en produit de facteurs premiers

Théorème.

Tout entier $n \geq 2$ admet une unique décomposition en produit fini de nombres premiers (à l'ordre des facteurs près) de la forme :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$$

où les p_k sont des nombres premiers deux à deux distincts et les α_k des enties naturels non nuls.

Remarque. Cette décomposition peut aussi s'écrire $n = \prod_{p \in \mathbb{P}} p^{\alpha_p}$ en attribuant l'exposant 0 aux nombres premiers qui ne sont pas dans la famille $\left(p_k\right)_{k \in \{1,...,r\}}$

3. Application aux diviseurs

Théorème.

Les diviseurs de $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ sont les entiers :

$$d = p_1^{\delta_1} p_2^{\delta_2} ... p_r^{\delta_r}$$

avec $\forall k \in \{1, ..., r\}$, $0 \leq \delta_k \leq \alpha_k$

Propriété.

Soit a et b des entiers supérieurs à 2 : $a = \prod_{p \in \mathbb{P}} p^{\alpha_p}$ et $b = \prod_{p \in \mathbb{P}} p^{\beta_p}$. Alors,

$$a \wedge b = \prod_{p \in \mathbb{P}} p^{inf(\alpha_p, \beta_p)} \text{ et } a \vee b = \prod_{p \in \mathbb{P}} p^{sup(\alpha_p, \beta_p)}$$

Exemple. PGCD et PPCM de 360 et 21.

IV. Congruences

Définition.

Etant donnés deux entiers relatifs x, y et un entier naturel n, on dit que x est congru à y modulo n si $x - y \in n\mathbb{Z}$ ou encore s'il existe $k \in \mathbb{Z}$ tel que $x = y + kn$. On note alors $x \equiv y\,[n]$.

Remarque.
- $x \equiv 0\,[n] \Leftrightarrow n|x$
- $x \equiv y\,[0] \Leftrightarrow x = y$
- $x \equiv y\,[n] \Leftrightarrow x$ et y ont le même reste dans la division euclidienne par n
- Si r est le reste dans la division euclidienne de x par n, alors $x \equiv r\,[n]$

Propriété.

La relation de congruence est une relation d'équivalence.

Propriété.

Soit x, y, x', y' des entiers relatifs et n, p des entiers naturels.
Si $x \equiv x'\,[n]$ et si $y \equiv y'\,[n]$, alors

$$\begin{array}{rcll} x + y & \equiv & x' + y' & [n] \\ xy & \equiv & x'y' & [n] \\ x^p & \equiv & x'^p & [n] \end{array}$$

Définition.

Etant donnés un entier relatif x et un entier naturel n, l'ensemble des entiers relatifs congrus à x modulo n est appelé la classe d'équivalence de x modulo n et notée $\bar{x}$.

Remarque. $x \equiv y\,[n] \Leftrightarrow \bar{x} = \bar{y}$