Prpas G.S High Tech, Rabat

Résumé de cours: *Arithmétique*

7 mars 2010

Blague du jour :
Un prof dit ses élèves : Les hommes intelligents sont toujours dans le doute. Seuls les imbéciles sont constamment affirmatifs.
- Vous en tes certain, monsieur ? demande une élève.
- Absolument certain !

Mathématicien du jour **Bezout**
tienne Bézout (1730-1783), est un mathématicien français. Il est l'auteur d'une Théorie générale des équations algébriques sur la théorie de l'élimination et des fonctions symétriques sur les racines d'une équation

1 Généralités.

Division dans $\mathbb{N}$.

Définition 1 .
Soit $(a,b) \in \mathbb{N}^{*2}$, on dit que a divise b si et seulement si : $\exists k \in \mathbb{N}^*$ tel que $b = ka$

Remarque 1 . *Si c divise a et b, alors c divise $ua + vb$, $\forall u, v \in \mathbb{Z}$.*

Division euclidienne.

Théorème 1 .
$\forall (a,b) \in \mathbb{N}^2 \quad \exists !(q,r) \in \mathbb{N}^2$ *tel que $a = bq + r$ avec $0 \leq r < b$, q s'appelle le quotient de la division euclidienne de a par b et r son reste.*

Propriétés. Soit $(a,b) \in \mathbb{N}^2$ et $(q,r) \in \mathbb{N}^2$ tel que $a = bq + r$, avec $0 \leq r < b$, alors :
– a divise b si et seulement si $r = 0$.
– $a \equiv r \quad [b]$, en particulier $\overline{a} = \overline{r}$ dans $\mathbb{Z}/b\mathbb{Z}$, plus précisément $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \ldots, \overline{n}\}$.

Algorithme d'Euclide. Soit $(a,b) \in \mathbb{N}^{*2}$, on effectue les divisions euclidienne successive de a par b, en divisant chaque fois le dernier quotient par son reste, jusqu' trouver un reste nul. Soit r_n le dernier reste non nul, alors :

1) r_n est un diviseur commun de a et b.

2) Si d divise a et b, alors d divise r_n.

3) $\exists u, v \in \mathbb{Z}$ tel que $r_n = ua + vb$.

2 Plus Grand Commun Diviseur, PGCD de deux entiers naturels.

Définition 2 .
Soit $a, b \in \mathbb{N}$, l'ensemble des diviseurs communs de a et b dans $\mathbb{N}$ est une partie de $\mathbb{N}$ non vide (contenant 1) majore par a et b, donc admet un plus grand, appel PGCD de a et b, on le note par $a \wedge b$.

Théorème 2 .
Soit $(a,b) \in \mathbb{N}^2$ et r_n le dernier reste non nul dans les divisions euclidiennes successives de a par b, alors $r_n = a \wedge b$.
En particulier :

1) *$a \wedge b$ est un diviseur commun de a et b.*

2) *Si d divise a et b, alors d divise $a \wedge b$.*

3) *$d = a \wedge b \exists u, v \in \mathbb{Z}$ tel que $d = ua + vb$.*

4) *Si $\exists u, v \in \mathbb{Z}$ tel que $d = ua + vb$, alors $a \wedge b$ divise d.*

Théorème 3 *Propriété caractéristique du PGCD.*
Soit $(a,b) \in \mathbb{N}^{*2}$ et $d \in \mathbb{N}^*$ alors :
$d = a \wedge b \iff$ *i)* *d divise a et b*
ii) *Pour tout autre diviseur commun d' de a et b on a : d' divise d aussi*

Propriétés. $\forall (a,b,c) \in \mathbb{N}^{*3}$ on a les propriétés suivantes

1) $a \wedge b = b \wedge a$, commutativité du PGCD.

2) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, associativité du PGCD.

3) $a \wedge b = a \iff a$ divise b.

Nombres premiers entre eux.

Définition 3 .
Soit $(a,b) \in \mathbb{N}^2$, lorsque $a \wedge b = 1$ on dit que a et b sont premiers entre eux.

Théorème 4 . *Théorème de Bezout.*
Soit $(a,b) \in \mathbb{N}^2$, alors : $a \wedge b = 1 \iff \exists (u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Théorème 5 . *Théorème de Gauss.*
Soit $a, b, c \in \mathbb{N}$ tel que a divise bc et $a \wedge b = 1$, alors a divise c.

Propriétés.

1) $ab \wedge ac = a(b \wedge c)$, distributivité du produit par rapport au pgcd.

2) Si d divise a et b on a : $\dfrac{a \wedge b}{d} = \dfrac{a}{d} \wedge \dfrac{b}{d}$.

3) Si $d = a \wedge b$ alors $\dfrac{a}{d} \wedge \dfrac{b}{d} = 1$, plus précisément $a = \alpha d, b = \beta d$ avec $\alpha \wedge \beta = 1$.

4) $a \wedge b = a \wedge c = 1 \Longrightarrow a \wedge bc = 1$.

5) $a \wedge b \iff a^n \wedge b^m = 1$.

3 PPCM de deux entiers naturels.

Définition 4 .
Soit $a, b \in \mathbb{N}$, l'ensemble des multiples communs de a et b dans $\mathbb{N}$ est une partie de $\mathbb{N}$ non vide (contenant ab) donc admet un plus petit élément, appel ppcm de a et b et not $a \vee b$.

Théorème 6 . *Propriété caractéristique du PPCM.*
Soit $(a,b) \in \mathbb{N}^{*2}$ et $m \in \mathbb{N}^*$ alors :
$d = m = a \vee b \iff$ *i)* *m multiple a et b*
ii) *Pour tout autre multiple commun m' de a et b on a : m' multiple de m aussi*

Propriété.

1) $a \vee b = b \vee a$, commutativité du PPCM.
2) $(a \vee b) \vee c = a \vee (b \vee c)$, associativité.
3) $\forall (a,b) \in \mathbb{N}^{*2}$ on a : $(a \wedge b)(a \vee b) = ab$
En particulier : $a \vee b = ab \Longleftrightarrow a \wedge b = 1$

4 Nombres premiers.

Définition 5 .
On appelle nombre premier, tout nombre différent de 1, dont les seuls diviseurs dans $\mathbb{N}^*$ sont 1 et lui même. Dans le cas contraire il est dit composé.

Théorème 7 .
Tout entier naturel supérieur 2 admet au moins un diviseur premier.

Théorème 8 .
L'ensemble des nombres premiers est infini.

Théorème 9 .
Tout entier naturel n supérieur 2 s'écrit de faon unique sous la forme :
$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, *avec $p_1, p_2, \dots, p_r$ des nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_r$ des entiers naturels non nuls.*
Cette écriture s'appelle décomposition primaire de n.

Théorème 10 .
Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $m = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$, avec $p_1, p_2, \dots, p_r$ des nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_r$ des entiers naturels éventuellement nuls, alors :
$n \wedge m = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_r^{\min(\alpha_r,\beta_r)}$
$n \vee m = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_r^{\max(\alpha_r,\beta_r)}$

Le plus grand nombre premier.
De nombreuses applications industrielles (systèmes cryptographiques, méthodes de transmission de l'information de,...) , d'où une course infernale pour trouver le plus grand nombre premier.
En 2006 l'*Electronic Frontier Foundation*, a annoncé une récompense de 100, 000$ pour qui trouverait un nombre premier plus d'un million de chiffres. Le 23 Août 2008, un américain (*Edson Smith*) trouva un formé par 12,978,189 chiffres, c'est $2^{43,112,609} - 1$, le 45 me nombre de *Mersenne* premier découvert, la méthode utilisé s'appelle *GIMPS* (*Great Internet Mersenne Prime Search*), qui consiste utiliser plusieurs serveurs distants connectés via internet.

Fin
à la prochaine