Résumé de cours : *Arithmétique*

MPSI-Maths.
Mr Mamouni : *myismail1@menara.ma*

بِسمِ اللَّهِ الرَّحمَنِ الرَّحِيمِ
وَ قُلِ إِعمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُم وَ رَسُولُهُ وَ المُؤ مِنِين
صَدَقَ اللَّهُ العَظِيم

1 Division dans $\mathbb{N}$.

Définition.

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

Division euclidienne.

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

Théorème.

a divise b si et seulement si le reste de la division euclidienne de b par a est nul.

2 Congruence dans $\mathbb{Z}$

Définition.

Soit $(a,b) \in \mathbb{Z}^2$ et $n \in \mathbb{N}^*$, on dit que a est congru à b modulo n *si et seulement si :* $\exists k \in \mathbb{Z}$ tel que $: b-a = kn$, c'est à dire n divise $b-a$ dans $\mathbb{Z}$, on écrit alors $a \equiv b \quad [n]$.

Propriétés.

1) **Soit $(a,n) \in \mathbb{Z} \times \mathbb{N}^*$, et r le reste de la division euclidienne de a par n, alors $a \equiv r \quad [n]$, on peut en conclure par conséquence que $\forall\,(a,n) \in \mathbb{Z} \times \mathbb{N}^*$ les seuls cas possibles sont : $a \equiv 0 \quad [n], a \equiv 1 \quad [n], \ldots, a \equiv n-1 \quad [n]$.**
2) **Soit $(a,b,c) \in \mathbb{Z}^3, n \in \mathbb{N}^*$ tel que $(a \equiv b \quad [n])$ et $(b \equiv c \quad [n])$ alors $(a \equiv c \quad [n])$**
3) **Soit $(a,b,c,d) \in \mathbb{Z}^4, n \in \mathbb{N}^*$ tel que $(a \equiv c \quad [n])$ et $(b \equiv d \quad [n])$ alors $(a+b \equiv c+d \quad [n])$, $(ab \equiv cd \quad [n])$ et $\forall k \in \mathbb{N}$ on a aussi : $(a^k \equiv c^k \quad [n])$.**

3 PGCD de deux entiers naturels.

Définition.

le PGCD de deux entiers naturels non nuls a et b est le plus grand parmi leurs diviseurs communs, on le note par $a \wedge b$.

Algorithme d'Euclide.

Soit $(a,b) \in \mathbb{N}^{*2}$, on effectue les divisions euclidienne successive de a par b, on divise le dernier quotient par son reste, jusqu'à trouver un reste nul, alors le dernier reste non nul est exactement le PGCD de a et b.

Propriété caractéristique du PGCD.

$(a,b) \in \mathbb{N}^{*2}$ 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) $a \wedge b = b \wedge a, \quad (a \wedge b) \wedge c = a \wedge (b \wedge c)$, **commutativité et associativité du PGCD.**
2) $d = a \wedge b \Longrightarrow \exists (u,v) \in \mathbb{Z}^2$ **tel que** $au + bv = d$, **la réciproque est evidement fausse toute fois on a le résultat suivant :**
3) **Théorème de Bezout.**

$$a \wedge b = 1 \Longleftrightarrow \exists (u,v) \in \mathbb{Z}^2 \text{ tel que } au + bv = 1$$

Vocabulaire.

Lorsque $a \wedge b = 1$ **on dit que** a **et** b **sont premiers entre eux.**

4) $ab \wedge ac = a(b \wedge c)$.
5) **Si** d **divise** a **et** b **on a :** $\dfrac{a \wedge b}{d} = \dfrac{a}{d} \wedge \dfrac{b}{d}$, **en particulier si** $d = a \wedge b$ **alors** $\dfrac{a}{d} \wedge \dfrac{b}{d} = 1$ **ou que** $a = kd, b = k'd$ **avec** $k \wedge k' = 1$.
6) **Théorème de Gauss :** a **divise** bc **et** $a \wedge b = 1 \Longrightarrow a$ **divise** c.
7) $a \wedge b = a \wedge c = 1 \Longrightarrow a \wedge bc = 1$.
8) $a \wedge b \Longleftrightarrow a^n \wedge b^m = 1$.

4 PPCM de deux entiers naturels.

Définition.

le PPCM de deux entiers naturels non nuls a **et** b **est le plus petit parmi leurs multiples communs, on le note par** $a \vee b$.

Propriété caractéristique du PPCM. $(a,b) \in \mathbb{N}^{*2}$ **et** $m \in \mathbb{N}^*$ **alors :**

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

$$a \vee b = ab \Longleftrightarrow a \wedge b = 1$$

5 Nombres premiers.

Définition.

Un nombre est dit premier différent de 1 ***si et seulement si*** **ses seuls diviseurs dans** $\mathbb{N}^*$ **sont 1 et lui même, dans le cas contraire il est dit composée.**

Théorème 1.

Tout entier naturel superieur à 2 admet au moins un diviseur premier.

Théorème 2.

L'ensemble des nombres premiers est infini.

Théorème 3.

Tout entier naturel n **superieur à 2 s'écrit de façon 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 4.

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 eventuellement 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 :

Le 11 Septembre 2006 fût découvert le plus grand nombre premier connu jusqu'à nos jours, c'est le nombre de Mersenne $M_{232\,582\,657} = 2^{232\,582\,657} - 1 = 12457502601536945540 \dots 11752880154053967871$, **formé par** $9\,808\,358$, **c'est le 44 ème nombre de Mersenne premier découvert, la méthode utilisé s'appelle GIMPS (Great Internet Mersenne Prime Search), qui consiste à utiliser plusieurs serveurs distants connectés via internet.**

Fin.