Université Pierre et Marie Curie
Master de Sciences et Technologies
Mention *Mathématiques et Applications*
Spécialité *Education et Formation*, Section CAPES, M1
Année 2011 - 2012

ARITHMÉTIQUE (résumé)

1. Division euclidienne

Théorème de division euclidienne. *Soit a un nombre entier, et soit b un nombre entier strictement positif. Alors, il existe un unique couple (q, r) de nombres entiers tel que $a = bq + r$ et $0 \leq r < b$.*

L'écriture $a = bq + r$ sappelle la *division euclidienne* de a par b.

Définition. Soient a et b deux nombres entiers tels que $b \neq 0$. On dit que b *divise* a (ou que a est un *multiple* de b), s'il existe un nombre entier k tel que $a = kb$. Si b divise a, on écrit $b|a$.

Soient a et b deux nombres entiers strictement positifs. L'ensemble des diviseurs communs positifs de a et b est non vide et fini. Le plus grand élément de cet ensemble s'appelle le *plus grand commun diviseur* de a et b, et est noté $pgcd(a, b)$. L'ensemble des multiples communs positifs de a et b est non vide. Le plus petit élément de cet ensemble s'appelle le *plus petit commun multiple* de a et b, et est noté $ppcm(a, b)$.

Dans les questions de divisibilité, les signes importent peu, car 1 et -1 sont inversibles dans $\mathbb{Z}$. Par conséquent, on considère parfois que deux nombres entiers strictement positifs a et b possèdent deux pgcd (opposés l'un à l'autre) et deux ppcm (opposés l'un à l'autre). Lorsqu'on parle du pgcd ou du ppcm, on parle de celui qui est supérieur à 0. L'extension des notions de pgcd et ppcm aux paires d'entiers relatifs non nuls est immédiate. De plus, si a est un nombre entier non nul, on pose $pgcd(a, 0) = a$ et $ppcm(a, 0) = 0$.

Lorsque $pgcd(a, b) = 1$, on dit que a et b *sont premiers entre eux.*

Algorithme d'Euclide. On a deux nombres entiers strictement positifs a et b tels que $a \geq b$. Le but de l'algorithme est de calculer le pgcd de a et b. A chaque étape de l'algorithme, un couple (a', b') de nombres entiers strictement positifs a' et b' tels que $a' \geq b'$ est remplacé par le couple (b', r), où r est le reste de a' dans la division par b'. L'algorithme s'arrête quand le plus petit nombre du couple est égal à 0. Le deuxième nombre du couple obtenu à la fin est égal au pgcd de a et b.

Théorème de Bézout. *Soient a et b des nombres entiers non tous les deux nuls. Posons $d = pgcd(a, b)$. Alors, il existe des nombres entiers u et v tels que $ua + vb = d$.*

Le théorème de Bézout permet de démontrer les énoncés suivants.

Proposition (Lemme de Gauss). *Soient a, b et c des nombres entiers strictement positifs tels que $pgcd(a, b) = 1$ et a divise bc. Alors, a divise c.*

Proposition. *Soient a, b et c des nombres entiers strictement positifs tels que a soit premier avec b et premier avec c. Alors, a est premier avec bc.*

Proposition. *Soient a et b deux nombres entiers non tous les deux nuls tels que $pgcd(a, b) = 1$, et soient m et n deux nombres entiers strictement positifs. Alors, $pgcd(a^m, b^n) = 1$.*

Proposition. *Soient a et b des nombres entiers non tous les deux nuls. Posons $d = pgcd(a, b)$. Alors, tout diviseur commun de a et b divise d.*

La proposition suivante donne une relation importante entre le pgcd et le ppcm de deux nombres.

Proposition. *Soient a et b deux nombres entiers strictement positifs. Posons $d = pgcd(a, b)$ et $m = ppcm(a, b)$. Alors, $ab = dm$.*

Démonstration. On a $a = da_0$ et $b = db_0$, où a_0 et b_0 sont des nombres entiers. De plus, $pgcd(a_0, b_0) = 1$. En effet, si d_0 est un diviseur commun de a_0 et b_0, alors dd_0 divise a et b, d'où $d_0 = 1$. On va montrer que $m = da_0b_0$. Tout d'abord, remarquons que $da_0b_0 = ab_0 = a_0b$ est un multiple commun de a et b. Étant donné un autre multiple commun strictement positif n de a et b, on va montrer que $da_0b_0 \leq n$, et même que da_0b_0 divise n. En effet, par hypothèse, il existe des nombres entiers n_1 et n_2 tels que $n = an_1 = bn_2$. Divisant par d, on obtient $a_0n_1 = b_0n_2$. En particulier, a_0 divise b_0n_2, donc, d'après le lemme de Gauss, il existe un nombre entier n_3 tel que $n_2 = a_0n_3$. Par conséquent, $n = ba_0n_3 = da_0b_0n_3$. En conclusion, $ab = da_0db_0 = dm$. □

Dans la démonstration de la proposition précédente, nous avons montré, en particulier, le lemme suivant.

Lemme. *Soient a et b des nombres entiers non tous les deux nuls. Posons $m = ppcm(a, b)$. Alors, m divise tout multiple commun de a et b.*

Proposition. *Soient a et b deux nombres entiers strictement positifs. Alors,*

(i) *l'ensemble $a\mathbb{Z} + b\mathbb{Z}$ des sommes d'un multiple de a et d'un multiple de b est un sous-groupe de $\mathbb{Z}$; le générateur positif de ce sous-groupe est $pgcd(a, b)$;*
(ii) *l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ des multiples communs de a et de b est un sous-groupe de $\mathbb{Z}$; le générateur positif de ce sous-groupe est $ppcm(a, b)$.*

On termine cette section par le théorème des restes chinois.

Théorème des restes chinois. *Soient k et n des nombres entiers strictement positifs et premiers entre eux. Alors, les groupes $\mathbb{Z}/kn\mathbb{Z}$ et $\mathbb{Z}/k \times \mathbb{Z}/n$ sont isomorphes.*

2. Nombres premiers

Définition. Soit p un nombre entier supérieur ou égal à 2. On dit que p est un *nombre premier* si ses seuls diviseurs positifs sont 1 et lui-même. Un nombre entier n supérieur ou égal à 2 qui n'est pas premier est dit *composé*.

Remarquons que si p et q deux nombres premiers distincts, on a $pgcd(p, q) = 1$.

Proposition. *Il y a une infinité de nombres premiers.*

Les nombres premiers jouent un rôle fondamental en arithmétique à cause du théorème suivant.

Théorème (Décomposition en facteurs premiers) *Tout nombre entier n supérieur ou égal à 2 s'écrit comme produit de nombres premiers, de façon unique à l'ordre près des facteurs. Une telle écriture est donc de la forme*

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r},$$

où $r \geq 1$ est un nombre entier, $p_1 < \dots < p_r$ sont des nombres entiers premiers distincts, et $\alpha_1, \dots, \alpha_r$ sont des nombres entiers strictement positifs.

Démonstration. Soit E l'ensemble des nombres premiers qui divisent n. Remarquons que E est non vide. De plus, E est fini, car chaque élément de E est inférieur ou égal à n. Soit $E = \{p_1, \dots, p_r\}$.

Pour chaque indice $1 \leq i \leq r$, il y a un nombre α_i maximal tel que $p_i^{\alpha_i}$ divise n. Puisque les nombres $p_1^{\alpha_1}, \dots, p_r^{\alpha_r}$ sont deux à deux premiers entre eux, le nombre n est divisible par $p_1^{\alpha_1} \dots p_r^{\alpha_r}$, cest-à-dire il existe un nombre entier k tel que

$$n = k p_1^{\alpha_1} \dots p_r^{\alpha_r} \ .$$

Si $k > 1$, le nombre k est divisible par un nombre premier p_s qui doit être dans E, pour un certain indice s. Donc, $p_s \times p_s^{\alpha_s}$ divise n. Ceci est est impossible car α_s a été choisi maximal, donc $k = 1$ et $n = p^{\alpha_1} \dots p_r^{\alpha_r}$. $\square$