Prépa CAPES UPMC 2009-2010 Matthieu Romagny

Résumé sur l'Arithmétique

Théorème de division euclidienne : *Étant donnés $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < b$.*

Corollaire : *Les sous-groupes de $\mathbb{Z}$ sont les sous-ensembles $n\mathbb{Z}$ pour un entier $n \geq 0$.*

Définition : Soient a, b deux entiers relatifs. On dit que b *divise* a, ou que a *est multiple de* b, si et seulement s'il existe un entier relatif k tel que $a = kb$. On note $b|a$.

Soient a, b deux entiers naturels non nuls. Il n'est pas difficile de montrer que l'ensemble de leurs diviseurs communs dans $\mathbb{N}$ possède un plus grand élément, et l'ensemble de leurs multiples non nuls communs dans $\mathbb{N}$ possède un plus petit élément. Ces remarques sont utilisées implicitement dans l'énoncé suivant.

Proposition et définition : *Soient a, b deux entiers naturels non nuls. 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 $\mathbb{Z}$, son générateur positif est aussi le plus grand des diviseurs communs dans $\mathbb{N}$ de a et b. On l'appelle un pgcd *de a et b.*

ii) l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ des multiples communs de a et de b est un sous-groupe de $\mathbb{Z}$, son générateur positif est aussi le plus petit des multiples communs dans $\mathbb{N}$ de a et b. On l'appelle un ppcm *de a et b.*

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

Dans les questions de divisibilité, les signes importent peu car 1 et -1 sont inversibles dans $\mathbb{Z}$. En conséquence, on considère parfois que a et b possèdent deux pgcd, et deux ppcm, opposés l'un l'autre. Lorsqu'on parle *du* pgcd, on parle de celui qui est > 0. Pour les mêmes raisons, l'extension des notions de pgcd et ppcm aux couples d'entiers relatifs non nuls est immédiate.

Théorème de Bézout : *Soient a et b entiers relatifs non nuls. Si $d = \mathrm{pgcd}(a,b)$ alors il existe $(u,v) \in \mathbb{Z}^2$ tels que $ua + vb = d$. Si u et v sont premiers entre eux, la réciproque est vraie : s'il existe $(u,v) \in \mathbb{Z}^2$ tels que $ua + vb = d$ alors $d = \mathrm{pgcd}(a,b)$.*

Théorème des restes chinois : *Soient m et n des entiers naturels non nuls premiers entre eux. Alors, on a un isomorphisme $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Lemme de Gauss : *Soient a, b, c entiers relatifs non nuls. On suppose que a et b sont premiers entre eux. Alors $a|bc$ implique $a|c$.*

Proposition : *Soient a, b, d entiers relatifs non nuls. Alors $d = \mathrm{pgcd}(a, b)$ ssi il existe des entiers relatifs a', b' tels que $a = da'$, $b = db'$ et $\mathrm{pgcd}(a', b') = 1$.*

Définition : On dit qu'un entier naturel $p \geq 2$ est *premier* si $\forall (a, b) \in \mathbb{N}^2$, $p = ab$ implique $p = a$ ou $p = b$.

Théorème de décomposition en facteurs premiers : *Tout entier $n \geq 2$ s'écrit comme un produit de nombres premiers, de façon unique à l'ordre près des facteurs. Plus précisément, on a une écriture $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec $r \geq 1$ entier, $p_1 < \dots < p_r$ premiers, et $\alpha_1, \dots, \alpha_r \geq 1$ entiers. Les entiers r, p_i, α_j sont uniques.*

Pour chaque nombre premier p, il est commode de noter $v_p(n)$ l'exposant de p dans la décomposition en facteurs premiers de n. On l'appelle la *valuation p-adique* de n.

Proposition : *Soient a, b entiers naturels non nuls. Alors :*

i) la décomposition en facteurs premiers de $d = \mathrm{pgcd}(a, b)$ est le produit (sur les p premiers) des $p^{\min(v_p(a), v_p(b))}$.

ii) la décomposition en facteurs premiers de $m = \mathrm{ppcm}(a, b)$ est le produit (sur les p premiers) des $p^{\max(v_p(a), v_p(b))}$.

Corollaire : *Soient a, b entiers naturels non nuls, $d = \mathrm{pgcd}(a, b)$ et $m = \mathrm{ppcm}(a, b)$. Alors, on a $dm = ab$.*

On termine ce résumé avec un fait classique qui résulte du théorème de Bézout :

Proposition : *Soient n, k entiers avec $n \geq 1$ et $1 \leq k \leq n$. On note $\overline{k}$ la classe de k dans le groupe $\mathbb{Z}/n\mathbb{Z}$. Alors, les conditions suivantes sont équivalentes :*

i) k est premier avec n,

ii) $\overline{k}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$,

iii) la classe de $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.