Préparation à l'agrégation interne de mathématiques
Arithmétique dans Z - Résumé de résultats de base

Pour référence : par exemple les livres [Mon06] et [WAC+02] pour plus de détails et de démonstrations.
Sur ce thème, le travail sur un manuel de Terminale S (programme de l'enseignement de spécialité) peut s'avérer très profitable également.

1 Divisibilité dans Z, congruences

Proposition 1.1.

1. *Un sous-ensemble non-vide de* $\mathbf{N}$ *possède un plus petit élément.*
2. *Un sous-ensemble non-vide et minoré de* $\mathbf{Z}$ *possède un plus petit élément.*
3. *Quels que soient l'entier naturel* b *non nul et l'entier naturel* a*, il existe un entier naturel* n *tel que* $a < nb$*. (*$\mathbf{N}$ *est* archimédien*).*

Une liste de définitions/vocabulaires :

1. Un entier b divise un entier a (on note $b|a$) s'il existe un nombre entier k tel que $a = b \times k$.
2. L'ensemble $\mathcal{D}_a$ des diviseurs positifs d'un entier a est non vide (et fini si a est non nul).
3. L'entier a est *premier* si $\mathcal{D}_a$ contient exactement deux éléments (qui sont alors 1 et $|a|$).
4. L'ensemble des multiples de a est $a\mathbf{Z}$.
5. La notion de diviseur commun, de multiple commun à deux (ou plus) nombres est naturelle.
6. Deux entiers a et b (ou plus...) sont *premiers entre eux* si $\mathcal{D}_a \cap \mathcal{D}_b = \{1\}$.

Propriété 1.1. *Si* c *divise* a *et* b*, alors* c *divise toutes les combinaisons linéaires* $\alpha a + \beta b$ *avec* α *et* β *entiers relatifs.*

Propriété 1.2 (Sur l'existence des nombres premiers).

1. *Tout nombre entier naturel* $n \geqslant 2$ *admet pour diviseur un nombre premier.*
2. *Tout nombre entier naturel* $n \geqslant 2$ *non premier admet un diviseur premier* p *vérifiant* $p^2 \leqslant n$*.*
3. *L'ensemble des nombres premiers est infini.*

Théorème 1 (Division euclidienne). *Soient* a *et* b *deux entiers avec* $b \neq 0$*.*
Il existe un unique couple $(q; r)$ *(quotient ; reste) d'entiers vérifiant :*

$$a = bq + r \ \textbf{\textit{et}}\ 0 \leqslant r < |b|.$$

Définition 1.1. *Deux entiers relatifs* a *et* b *sont dits* congrus modulo l'entier n *si* n *divise* $b - a$*.*
On note $a \equiv b \pmod{n}$*.*

Remarque 1.1. *Il est équivalent de dire que* a *et* b *ont même reste dans la division euclidienne par* n *(si* $n \neq 0$*).*

Propriété 1.3. *La congruence est compatible avec les opérations usuelles (*$+$ *;* $-$ *;* $\times$ *; exponentiation).*

La congruence modulo n est une relation d'équivalence sur $\mathbf{Z}$ constituée de n classes (si $n > 0$). L'ensemble quotient est (l'anneau) $\mathbf{Z}/n\mathbf{Z} = \left\{\overline{0}; \overline{1}; \ldots; \overline{n-1}\right\}$.

2 Décomposition, $PGCD$, $PPCM$, Euclide, Bézout, Gauss

Théorème 2 (**Décomposition en produit de facteurs premiers**). *Tout entier naturel $n \geqslant 2$ peut s'écrire de façon unique comme un produit :*

$$n = \prod_{i=1}^{i=m} p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$$

où $p_1, p_2, \dots, p_m$ sont des nombres premiers vérifiant $2 \leqslant p_1 < p_2 < \dots < p_m$
et $\alpha_1, \alpha_2, \dots, \alpha_m$ sont des nombres entiers naturels non nuls.

Les deux définitions suivantes ne sont pas les plus habituelles mais ont l'avantage de ne pas nécessiter d'hypothèses de non-nullité sur a et b.

Propriété et définition 2.1 (**Plus Grand Commun Diviseur**). *Soient a et b deux entiers relatifs. Il existe un unique entier naturel $\delta = PGCD(a;b) = PGCD(b;a)$ vérifiant :*

- *δ est un diviseur commun à a et b ;*
- *tout autre diviseur commun à a et b divise δ.*

Si a et b sont non nuls, le nombre $PGCD(a;b)$ est le dernier reste non nul obtenu en appliquant l'algorithme d'Euclide aux entiers a et b.

Propriété et définition 2.2 (**Plus Petit Commun Multiple**). *Soient a et b deux entiers relatifs. Il existe un unique entier naturel $\mu = PPCM(a;b) = PPCM(b;a)$ vérifiant :*

- *μ est un multiple commun à a et b ;*
- *tout autre multiple commun à a et b est un multiple de μ.*

Remarque 2.1. *Le nombre $\mu = PPCM(a;b)$ vérifie $a\mathbf{Z} \cap b\mathbf{Z} = \mu\mathbf{Z}$.*

Théorème 3 (**Bézout**). *Soient a et b deux entiers relatifs.*

1. *il existe des entiers relatifs u et v tels que $au + bv = PGCD(a;b)$.*
2. *(Corollaire) Les entiers a et b sont premiers entre eux si et seulement s'il existe des entiers relatifs u et v tels que $au + bv = 1$.*

Propriété 2.1. *Soient a, b, c, d et k des entiers relatifs.*

1. *Si $a|c$ et $b|d$, alors $PGCD(a;b)|PGCD(c;d)$ et $PPCM(a;b)|PPCM(c;d)$.*
2. *$PGCD(ka;kb) = |k| \times PGCD(a;b)$ et $PPCM(ka;kb) = |k| \times PPCM(a;b)$*
3. *$PGCD(a;b) \times PPCM(a;b) = |ab|$*

Théorème 4 (**Gauss**). *Soient a, b et c trois entiers relatifs.*

1. $\left.\begin{array}{r} a \mid bc \\ PGCD(a;c) = 1 \end{array}\right\} \Longleftrightarrow a \mid b$
2. *Plus généralement : si $PGCD(a;c) = 1$ alors $PGCD(a;bc) = PGCD(a;b)$.*
3. *(Corollaire) Un nombre premier p divise ab si et seulement si p divise a ou p divise b.*

Références

[Mon06] Jean-Marie Monier. Algèbre MPSI, Cours, méthodes et exercices corrigés, 4eédition. J'intègre. Dunod, Paris, 2006.

[WAC+02] André Warusfel, Paul Attali, Michel Collet, Christian Gautier, and Serge Nicolas. Arithmétique. Mathématiques, Cours et exercices TS. Vuibert, Paris, 2002.