Arithmétique, première partie

Terminale S (enseignement de spécialité)
Lycée Charles PONCET

Septembre 2012

Table des matières

Le symbole ✏ indique les exemples à traiter, des démonstrations à trouver.
Le symbole ☛ indique des points importants, des pièges possibles, des notations particulières, etc.

1 Divisibilité dans $\mathbb{Z}$

$\mathbb{N} = \{0\ ;\ 1\ ;\ 2\ ;\ \cdots\}$ est l'ensemble des entiers naturels.
$\mathbb{Z} = \{\cdots\ ;\ -2\ ;\ -1\ ;\ 0\ ;\ 1\ ;\ 2\ ;\ \cdots\}$ est l'ensemble des entiers relatifs.

1.1 Définition

Définition 1.1.1
Pour deux entiers relatifs a *et* b*, s'il existe un entier relatif* k *tel que* $a = kb$ *on dit que* a est un multiple de b.
Si de plus $b \neq 0$*, on dit que* b est un diviseur de a *ou que* a est divisible par b *ou encore que* b divise a *et on note* $b|a$.

Exemples et remarques

1. On a $84 = -7 \times (-12)$ donc 84 est un multiple de -7, -7 divise 84.
2. Écrire l'ensemble des multiples de 5 que l'on note $5\mathbb{Z}$.
3. Déterminer les diviseurs de 18 puis ceux de 24 et enfin les diviseurs communs à 18 et 24.
4. Justifier que 0 est un multiple de tout entier mais qu'il n'a qu'un seul multiple.
5. Justifier que tout entier $a \neq 0$ possède comme diviseurs 1, -1, a et $-a$.
6. Justifier que 1 et -1 n'ont que deux diviseurs : 1 et -1.
7. Justifier que $b|a$ est équivalent à $b|(-a)$, $(-b)|a$ et $(-b)|(-a)$.

1.2 Propriétés de la divisibilité

Théorème 1.2.1 (transitivité)
Quels que soient les entiers relatifs non nuls a, b *et* c *:*

si $a|b$ *et* $b|c$ *alors* $a|c$.

✏ Démontrer le théorème 1.2.1.

Théorème 1.2.2
Quels que soient les entiers relatifs non nuls a *et* b *:*

1. *Si* a *divise* b *alors* $|a| \leqslant |b|$.
2. a *divise* b *et* b *divise* a *si, et seulement si,* $a = b$ *ou* $a = -b$.

✏ Démontrer le théorème 1.2.2.
Déduire du théorème 1.2.2 qu'un entier relatif non nul a un nombre fini de diviseurs.

Théorème 1.2.3 (combinaison linéaire)
Quels que soient les entiers relatifs non nuls a, b *et* c*, si* c *divise* a *et* b *alors* c *divise* $a + b$, $a - b$ *et toute combinaison linéaire (à coefficients entiers) de* a *et* b.

☛ Une combinaison linéaire de a et b est une expression de la forme $\alpha a + \beta b$ où α et β sont deux entiers relatifs.
✏ Démontrer le théorème 1.2.3.

Définition 1.2.1
On dit que deux entiers relatifs non nuls sont premiers entre eux *(ou* étrangers*) si leurs seuls diviseurs communs sont* 1 *et* -1.

✏ En écrivant les diviseurs de 12 et 25, jusitifier que 12 et 25 sont premiers entre eux.

2 Division euclidienne

2.1 Propriété d'ARCHIMÈDE [1]

Proposition 2.1.1
Toute partie non vide de $\mathbb{Z}$ minorée (resp. majorée) possède un plus petit (resp. plus grand) élément.

Proposition 2.1.2 (corollaire de la proposition 2.1.1)
Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

☛ En effet toute partie non vide de $\mathbb{N}$ est minorée par 0.

Proposition 2.1.3 (propriété d'ARCHIMÈDE)
L'ensemble $\mathbb{N}$ est archimédien *: pour un entier naturel b non nul, on peut rendre le produit nb aussi grand que l'on veut, c'est-à-dire que, quel que soit l'entier naturel a, il existe un entier naturel n tel que $a < nb$.*

☛ L'ensemble $\mathbb{R}$ des nombres réels est également archimédien.

2.2 Division euclidienne dans $\mathbb{N}$

Théorème 2.2.1
Soit a un entier naturel et soit b un entier naturel non nul. Il existe un unique couple $(q\ ;\ r)$ d'entiers naturels tels que :

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

a est le dividende, *b le* diviseur, *q le* quotient *et r est le* reste *de la* division euclidienne *de a par b.*

☛ Le nombre q est le quotient euclidien de a par b si et seulement si $bq \leqslant a < b(q+1)$.
Comme $b \neq 0$, on a $q \leqslant \dfrac{a}{b} < q+1$, q est la partie entière de $\dfrac{a}{b}$ notée $E\left(\dfrac{a}{b}\right)$.

✏ Écrire la division euclidienne de 165 par 7.

Preuve du théorème 2.2.1

Lorsque $a = 0$, il suffit de prendre $q = 0$ et $r = 0$.

Dans les autres cas, l'existence du couple $(q\ ;\ r)$ utilise la propriété d'ARCHIMÈDE (proposition 2.1.3).

Comme $a \in \mathbb{N}$ et $b \in \mathbb{N} - \{0\}$, l'ensemble des entiers naturels n tels que $a < nb$ n'est pas vide. Cet ensemble possède un plus petit élément $k \in \mathbb{N}$.

$k \neq 0$ car sinon $a < 0$ ce qui est absurde, donc $k \geqslant 1$ et k vérifie $(k-1)b \leqslant a < kb$.

En posant $q = k-1$, on a $q \in \mathbb{N}$ et $bq \leqslant a < (q+1)b$ donc $0 \leqslant a - bq < b$.

Finalement en posant $r = a - bq$ on a $a = bq + r$ et $0 \leqslant r < b$.

✏ Démontrer l'unicité du couple $(q\ ;\ r)$ par l'absurde.

2.3 Division euclidienne dans $\mathbb{Z}$

Théorème 2.3.1
Soit a un entier relatif et soit b un entier relatif non nul. Il existe un unique couple $(q\ ;\ r)$ d'entiers relatifs tels que :

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

✏ Justifier le théorème 2.3.1.

✏ Écrire les divisions eucliennes de 165 par -7, -165 par 7 et -165 par -7.

1. ARCHIMÈDE, mathématicien et physicien grec, Syracuse 287 – *id.* 212 av. J.-C..

Remarques générales

1. a et b sont des entiers relatifs non nuls.
   $b|a$ si et seulement si le reste de la division de a par b est nul.
2. $a = bq + r$ avec $0 \leqslant r < |b|$ donc $r \in \{0\ ;\ 1\ ;\ \cdots\ ;\ |b|-1\}$. Dans une division euclidienne de a par $b \neq 0$, il y a $|b|$ restes possibles.
3. b est un entier naturel supérieur ou égal à 2.
   Tout nombre entier s'écrit sous une, et une seule, des formes bq, $bq+1$, …, $bq+(r-1)$ où q est un entier relatif et r est un entier naturel tel que $0 \leqslant r < b$.
   - ☛ Tout nombre entier peut s'écrire sous la forme $2k$ ou $2k+1$.
     Tout nombre entier peut s'écrire sous la forme $3k$, $3k+1$ ou $3k+2$.
4. b est un entier naturel supérieur ou égal à 2.
   Parmi b entiers consécutifs, l'un est multiple de b.
   - ☛ k étant un nombre entier, parmi les nombres $k-1$, k et $k+1$, l'un est un multiple de 3.

3 Nombres premiers

3.1 Définition

Définition 3.1.1
Un nombre entier naturel est premier *s'il possède exactement deux diviseurs positifs :* 1 *et lui-même.*
Un entier naturel différent de 1 *non premier est un nombre* composé.

- ☛ 0 et 1 ne sont pas premiers. Le plus petit entier naturel premier est 2 (c'est le seul nombre pair et premier).

3.2 Propriétés des nombres premiers

Théorème 3.2.1
n est un entier naturel supérieur ou égal à 2.
Le plus petit diviseur de n compris entre 2 et n est premier.

Théorème 3.2.2
Tout entier naturel supérieur ou égal à 2 possède au moins un diviseur premier.

Théorème 3.2.3
Tout entier naturel non premier *supérieur ou égal à 2 possède un diviseur premier* $p \leqslant \sqrt{n}$.

Corollaire 3.2.4 (test de primalité)
n est un entier naturel supérieur ou égal à 2.
Si aucun nombre entier compris entre 2 et $\sqrt{n}$ ne divise n alors n est premier.

- ☛ Pour connaître la *primalité* (ou *primarité*) d'un nombre entier naturel, il suffit de tester sa divisibilité par tous les nombres premiers inférieurs à sa racine carrée.
- ✏ Utiliser cette méthode pour construire le crible d'ÉRATOSTHÈNE [2].

Théorème 3.2.5
Il existe une infinité de nombres premiers.

- ✏ Démontrer le théorème 3.2.5. Pour cela, raisonner par l'absurde en considérant p le plus grand nombre premier et en démontrant que $N = p!! + 1$ est premier.
  ($p!!$ désigne le produit de tous les nombres premiers de 2 jusqu'à p.)

2. ÉRATOSTHÈNE, astronome, géographe, mathématicien et philosophe grec, Cyrène v. 284 – Alexandrie, 192 av. J.-C..

3.3 Décomposition en un produit de nombres premiers

Théorème 3.3.1
Tout entier naturel supérieur ou égal à 2 possède une décomposition, unique à l'ordre près, en un produit de nombres premiers.

✏ Décomposer le millésime de votre année de naissance en un produit de nombres premiers.

Proposition 3.3.1
a *et* b *sont deux entiers naturels non nuls.*
b *divise* a *si, et seulement si, les exposants des facteurs premiers de* b *sont inférieurs ou égaux à ceux de la décomposition de* a.

✏ Déterminer les diviseurs positifs de 120.
✏ p, q, r sont des nombres premiers et $n = p^\alpha \times q^\beta \times r^\gamma$ (avec α, β, γ trois entiers naturels). Quel est le nombre de diviseurs positifs de n ?

4 Congruences

4.1 Définition

Définition 4.1.1
Soit n *un entier naturel supérieur ou égal à 2.*
Deux entiers relatifs a *et* b *sont* congrus modulo n *si* n *divise* $a - b$.
On note $a \equiv b \pmod{n}$ *ou* $a \equiv b \ (n)$ *ou* $a \equiv b \ [n]$.

✏ Comparer 13 et 40 modulo 3, 29 et -121 modulo 5, -623 et -473 modulo 10.
✏ Que se passe-t-il lorsque l'on compte de 7 en 7 à partir de 2 ?
☛ On peut étendre la définition des congruences à des entiers négatifs $n \leqslant -2$ mais cela n'a aucun intérêt car $n|(a - b)$ est équivalent à $-n|(a - b)$.

4.2 Propriétés des congruences

Théorème 4.2.1
On considère un entier naturel n *supérieur ou égal à 2.*
Deux entiers relatifs a *et* b *sont congrus modulo* n *si, et seulement si, les divisions euclidiennes de* a *et* b *par* n *ont le même reste.*

✏ Démontrer le théorème 4.2.1 en utilisant la division euclidienne de a et b par n (*distinguer la partie directe et la réciproque*).

Théorème 4.2.2
On considère deux entiers naturels n *et* n' *supérieurs ou égaux à 2 et deux entiers relatifs* a *et* b.
Si $n'|n$ *et* $a \equiv b \pmod{n}$ *alors* $a \equiv b \pmod{n'}$.

✏ Démontrer le théorème 4.2.2.

Proposition 4.2.1 (relation d'équivalence)
On considère un entier naturel n *supérieur ou égal à 2 et trois entiers relatifs* a, b *et* c.
- $a \equiv a \pmod{n}$ *(réflexivité).*
- *Si* $a \equiv b \pmod{n}$ *alors* $b \equiv a \pmod{n}$ *(symétrie).*
- *Si* $a \equiv b \pmod{n}$ *et* $b \equiv c \pmod{n}$ *alors* $a \equiv c \pmod{n}$ *(transitivité).*

✏ Justifier la proposition 4.2.1.
☛ La relation « être congru modulo n » est réflexive, symétrique et transitive tout comme l'égalité ou le parallélisme. On dit que c'est une *relation d'équivalence*.

Congruences et division euclidienne

Théorème 4.2.3
Soit n un entier naturel supérieur ou égal à 2. Tout entier relatif est congru modulo n à un unique entier r tel que $0 \leqslant r \leqslant n-1$.

✏ Démontrer le théorème 4.2.3.

Conséquences On peut définir une partition de $\mathbb{Z}$ en n classes dont chacune contient un élément et un seul de l'ensemble $\{0\ ;\ 1\ ;\ \cdots\ ;\ n-1\}$.
☛ Lorsque $n = 2$, il y a deux classes : les nombres pairs ($r = 0$) et les nombres impairs ($r = 1$).

Congruences et opérations

Théorème 4.2.4
Soit n un entier naturel supérieur ou égal à 2. La relation de congruence modulo n est compatible avec l'addition et la multiplication dans $\mathbb{Z}$. Cela signifie que si a, b, a', b' sont des entiers relatifs et si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ alors $a+b \equiv a'+b' \pmod{n}$ et $ab \equiv a'b' \pmod{n}$.

✏ Démontrer le théorème 4.2.4.

Théorème 4.2.5 (corollaire du théorème 4.2.4)
On considère un entier naturel n supérieur ou égal à 2 et deux entiers relatifs a et a'.

1. *Pour tout entier relatif k, si $a \equiv a' \pmod{n}$ alors $ka \equiv ka' \pmod{n}$.*
2. *Pour tout entier naturel $p \geqslant 1$, si $a \equiv a' \pmod{n}$ alors $a^p \equiv a'^p \pmod{n}$.*

✏ Démontrer le théorème 4.2.5 (*pour le deuxième item utiliser un raisonnement par récurrence*).
✏ Déterminer le reste de la division euclidienne de 17^{2013} par 4.

4.3 Critères de divisibilité

Proposition 4.3.1
On considère un entier naturel n supérieur ou égal à 2 et un entier relatif a.
$a \equiv 0 \pmod{n}$ *si, et seulement si, n divise a.*

Critères de divisibilité usuels

Dans ce qui suit, les nombres entiers sont écrits dans le système décimal.

1. Un nombre entier est divisible par 2 (c'est-à-dire pair) si, et seulement si, son chiffre des unités est 0, 2, 4, 6 ou 8.
2. Un nombre entier est divisible par 5 si, et seulement si, son chiffre des unités est 0 ou 5.
3. Un nombre entier est divisible par 3 si, et seulement si, la somme de ses chiffres est divisible par 3.
4. Un nombre entier est divisible par 9 si, et seulement si, la somme de ses chiffres est divisible par 9.
5. Un nombre entier est divisible par 4 si, et seulement si, le nombre formé par le chiffre des dizaines et celui des unités est divisible par 4.

✏ Justifier ces cinq critères de divisibilité.