Chapitre 17 — "L'essentiel" sur l'arithmétique

Préambule. Un rapide tour d'horizon du cours d'arithmétique de cette année.

Table des matières

1. Divisibilité

On commence par la définition fondamentale de ce chapitre :

Définition. Soient a et b dans $\mathbb{Z}$.

On dit que a **divise** b s'il existe un entier relatif k tel $b = ka$.

Dans ce cas, on note : $a|b$.

On dit aussi que a est **un diviseur** de b, ou que b est **un multiple** de a.

Quelques exemples. [1]

$2|651794$; $3|324195$; $4|78659348$; $5|78659345$; $10|765210$; $11|12324213$

Au passage, on a utilisé sur ces exemples le critère de divisibilité par 3, et le critère de divisibilité par 11 qui font l'objet des exercices 20 et 21.

Les propriétés les plus remarquables de la relation de divisibilité sont les suivantes :

Propriétés de la relation de divisibilité.

➢ **La relation de divisibilité est réflexive**. Tout entier a se divise lui-même.

➢ **La relation de divisibilité est transitive**. Si un entier a divise un entier b qui divise un entier c, alors a divise c.

➢ **La relation de divisibilité est... "presque antisymétrique"...**. Soient a et b deux entiers. Si a divise b, et b divise a, alors $|a| = |b|$.

➢ **Conséquence** : la relation de divisibilité dans $\mathbb{N}$ est une relation d'ordre. Mais ce n'est pas une relation d'ordre dans $\mathbb{Z}$ puisque l'axiome d'antisymétrie n'est pas vérifié alors.

➢ **Une propriété algébrique**. Soient a, b et c trois entiers. Si a divise b et c, alors a divise $nb + mc$ pour tout couple d'entiers (n, m).

De toutes ces propriétés, la dernière est celle qui rend le plus de services, que ce soit en théorie (notamment dans la preuve du théorème de Bezout), ou en pratique (cf exemple suivant).

Exemple d'application. Déterminer tous les entiers n tels que $(n + 5)$ divise $3n + 19$.

Si n est un entier solution du problème, alors :

$$(n+5)|(n+5) \text{ (waouh !)} \qquad \text{et} \qquad (n+5) \,|\, (3n+19)$$

Par suite :

$$(n+5) \,|\, [(3n+19) - 3(n+5)] \iff (n+5) \,|4$$

Or les diviseurs de 4 sont exactement : -4, -2, -1, 1, 2 et 4.

On en déduit que $n \in \{-9, -7, -6, -4, -3, -1\}$.

On a donc établi l'implication : $[(n+5) \,|\, (3n+19)] \Longrightarrow [n \in \{-9, -7, -6, -4, -3, -1\}]$.

L'implication réciproque est une vérification aisée qui permet de conclure.

Conclusion. Il existe exactement 6 entiers n tels que $(n + 5) \,|\, (3n + 19)$, qui sont $-9, -7, -6, -4, -3$, et -1.

1. Pour réviser des critères de divisibilité que vous connaissez sans doute.

2. Division euclidienne dans $\mathbb{Z}$

Le théorème de la division euclidienne formalise une opération que vous connaissez depuis votre enfance !

Théorème (de la division euclidienne dans $\mathbb{Z}$).

$$\forall\,(a,b)\in\mathbb{Z}\times\mathbb{N}^*,\ \exists!\ (q,r)\in\mathbb{Z}\times\mathbb{N},\ [a=bq+r]\wedge[0\leqslant r<b]$$

Exemples d'application. Le TDE est un ingrédient-clef dans la preuve :

➢ du résultat donnant l'ensemble des racines n-èmes de l'unité :

$$\mathbb{U}_n=\left\{\mathrm{e}^{2\mathrm{i}k\pi/n},\ k\in[\![\,0,n-1\,]\!]\right\}$$

➢ du théorème de Bezout (voir plus loin dans ce chapitre) ;

➢ de propriétés concernant les groupes finis (l'an prochain, en MP).

3. PGCD

3.1. Définition et algorithme d'Euclide.

Définition. Soient a et b deux entiers non nuls.

Le **plus grand commun diviseur (PGCD)** de a et b est le plus grand (au sens de la relation d'ordre $\leqslant$) entier divisant à la fois a et b. Il sera noté $a\wedge b$.

Par convention, $0\wedge 0=0$.

Remarque. Un certain nombre de propriétés proviennent directement de cette définition de PGCD, et des propriétés de la divisibilité. L'une d'elles permet de se restreindre, pour le calcul des PGCD, aux couples d'entiers naturels (et non relatifs). En effet :

$$\forall\,(a,b)\in\mathbb{Z}^2,\ a\wedge b=|a|\wedge|b|$$

Algorithme d'Euclide. Le PGCD de a et b est le dernier reste non nul obtenu dans la suite de divisions euclidiennes effectuées dans l'algorithme décrit ci-dessous.

Exemple. Calcul du PGCD de 25 et 72.

$$72=25\times 2+22$$

$$25=22\times 1+3$$

$$22=3\times 7+1$$

$$3=3\times 1+0$$

On en déduit que $\boxed{25\wedge 72=1}$.

3.2. **Théorème de Bezout.** L'énoncé de ce résultat signifie que le PGCD de deux entiers a et b peut s'écrire comme somme d'un multiple de a et d'un multiple de b.

Théorème de Bezout.

$$\forall\ (a,b) \in \mathbb{Z}^2,\ \exists\ (u,v) \in \mathbb{Z}^2,\ au + bv = a \wedge b$$

Terminologie. Les entiers u et v ci-dessus peuvent être appelés *coefficients de Bezout* des entiers a et b. Il n'y a pas unicité de ce couple.

Enfin, on peut déterminer de tels entiers en "remontant" l'algorithme d'Euclide.

A titre d'exemple, on détermine ci-dessous des coefficients pour les entiers 25 et 72.

$1 = 22 - 7 \times 3$

$1 = 22 - 7 \times (25 - 22) = 8 \times 22 - 7 \times 25$

$1 = 8 \times (72 - 2 \times 25) - 7 \times 25$ soit finalement :

$\boxed{1 = 8 \times 72 - 23 \times 25}$

On a donc obtenu une relation de Bezout pour les entiers 25 et 72, c'est à dire deux entiers u et v tels que $25u + 72v = 25 \wedge 72$ avec $\boxed{u = -23 \text{ et } v = 8}$.

Une conséquence du théorème de Bezout est que le PGCD de a et b est également le plus grand diviseur commun de a et b, pour la relation de divisibilité ; c'est ce que formalise l'énoncé ci-dessous.

Corollaire. Soient a, b et d trois entiers.

Si $d|a$ et $d|b$, alors $d|\ (a \wedge b)$.

4. Congruences

4.1. **Généralités.**

Définition. Soient a et b deux entiers, et n un entier $\geqslant 2$.

On dit que a **est congru à** b **modulo** n si $b - a$ est multiple de n, c'est à dire s'il existe $k \in \mathbb{Z}$ tel que : $b = a + kn$.

On le note $a \equiv b\ [n]$.

Remarque 1. La définition de congruence dans $\mathbb{Z}$ est très proche de la définition de congruence énoncée dans le chapitre de trigonométrie au début de cette année. En particulier, elle jouit des mêmes propriétés (réflexivité, symétrie et transitivité) permettant d'affirmer que la relation de congruence modulo n est une relation d'équivalence dans $\mathbb{Z}$.

Remarque 2. Tout entier est congru modulo n est à son reste dans la division euclidienne par n. Lorsque l'on travaille modulo n, on peut donc se restreindre à considérer les n entiers 0, 1,..., $n - 1$.

Remarque 3. Soient a et n deux entiers. On a l'équivalence :

$$(n \text{ divise } a) \iff (a \equiv 0\ [n])$$

Cette équivalence peut s'avérer très utile lorsque l'on vous demande d'établir qu'un certain entier est multiple d'un autre. A ce sujet, voir notamment les exos 10, 14 et 15 de la feuille d'exos.

Propriétés algébriques des congruences. Soit n un entier, $n \geqslant 2$; et soient a, b, c et d quatre entiers tels que $a \equiv b\ [n]$ et $c \equiv d\ [n]$. Alors :

1/ $a + c \equiv b + d\ [n]$ 2/ $ac \equiv bd\ [n]$ 3/ $\forall N \in \mathbb{N},\ a^N \equiv b^N\ [n]$

Exemples d'application. "Montrer que $2^{3000} - 1$ est multiple de 7" ; "Montrer que l'équation $5x^2 + 2y^4 = 9999$" n'a pas de solution dans $\mathbb{Z}^2$" ; "Montrer que $7|n$ et $7|m$ SSI $7|n^2 + m^2$".

4.2. Entiers inversibles modulo n.

Définition. Soit a et n deux entiers, avec $n \geqslant 2$.

On dit que a est **inversible modulo** n s'il existe un entier b tel que $ab \equiv 1\ [n]$.

Dans ce cas, b est appelé **un inverse de** a **modulo** n

Exemples. 3 a pour inverse 5 modulo 7. Mais 12 et -2 sont aussi des inverses de 3 modulo 7. Plus généralement :

Si b est un inverse de a modulo n, alors $b + kn$ est un inverse de a modulo n (pour tout $k \in \mathbb{Z}$).

En d'autres termes, un entier admet une infinité d'inverses modulo n dès qu'il en admet un. Mais à l'opposé, il peut très bien ne pas exister d'inverse du tout : par exemple, 8 n'a pas d'inverse modulo 4, 6 n'a pas d'inverse modulo 9...

L'énoncé ci-dessous donne une condition nécessaire et suffisante pour que a soit inversible modulo n.

Propriété. Soit n un entier, $n \geqslant 2$, et $a \in \mathbb{Z}$.

L'entier a est inversible modulo n si et seulement si $a \wedge n = 1$.

Remarque. La preuve de ce résultat, pas trop difficile, est un excellent moyen de vérifier que vous avez bien intégré les parties du cours les plus récentes (sur les congruences et la notion d'inversibilité modulo n).

5. Entiers premiers entre eux

5.1. Généralités.

Définition. Deux entiers a et b sont **premiers entre eux** si $a \wedge b = 1$.

Exemples. 75 et 22 sont premiers entre eux ; 4 et 15 sont premiers entre eux ; deux entiers consécutifs sont premiers entre eux.

L'énoncé ci-dessous joue un rôle important dans la preuve des résultats concernant les équations diophantiennes, et dans certains exercices (comme les exos 30, 31 et 34 de la feuille).

Lemme. Soient a et b deux entiers non nuls. On note $d = a \wedge b$.

Il existe un unique couple d'entiers relatifs tels que $a = da'$, $b = db'$ et $a' \wedge b' = 1$.

Enfin, un excellent exercice sur cette notion (et celle du paragraphe précédent) consiste à établir la propriété suivante.

Lemme. Si a et b sont premiers entre eux, alors a^n et b^m sont premiers entre eux pour tout couple $(n, m) \in \mathbb{N}^2$.

5.2. Le lemme de Gauss et ses conséquences.

Théorème ("lemme de Gauss"). Soient a, b et c trois entiers.

Si $a|bc$ et $a \wedge b = 1$ alors $a|c$.

Une application de ce résultat est l'énoncé donnant la solution générale d'une équation diophantienne "homogène" ($ax + by = 0$) ; une seconde application est la preuve du théorème de Fermat (dans le paragraphe consacré aux nombres premiers).

Une autre conséquence du lemme de Gauss est la suivante :

Corollaire. Soient a et b deux entiers tels que $a \wedge b = 1$.

Si $a|c$ et $b|c$, alors $ab|c$.

Conséquence. Si n est multiple de 3 et de 25, alors n est multiple de 75.

6. L'équation diophantienne $ax + by = c$

Problématique. Soient a, b et c trois entiers. Déterminer l'ensemble des couples (x, y) d'**entiers** tels que : $ax + by = c$.

L'aspect remarquable est que la méthode pour parvenir à cet objectif est très similaire à celle rencontrée dans le cadre des équations différentielles.

Explicitement, la méthode pour résoudre l'équation (E) : $ax + by = c$ est la suivante.

➢ **Etape 0** — On vérifie que l'équation a des solutions : $(a \wedge b)|c$

➢ **Etape 1** — Solution générale de l'équation homogène associée

➢ **Etape 2** — Solution particulière de (E) (l'équation "avec second membre")

➢ **Etape 3** — Solution générale de (E) = "Etape 1 + Etape 2"

6.1. L'équation homogène $ax + by = 0$.

Propriété. Soient a et b deux entiers non nuls.

On note $d = a \wedge b$, $a = da'$ et $b = db'$.

L'ensemble des solutions (la solution générale) de l'équation (H) $ax + by = 0$ est :

$$\{(kb',\ -ka')\ /\ k \in \mathbb{Z}\}.$$

6.2. **Structure des solutions de $ax + by = c$.**

Propriété. Soient a, b et c trois entiers non nuls.
On note $d = a \wedge b$, $a = da'$ et $b = db'$.
On suppose qu'il existe un couple $(x_0, y_0) \in \mathbb{Z}^2$ solution de (E) : $ax + by = c$.
Alors l'ensemble des solutions (la solution générale) de (E) est :

$$\{(x_0 + kb',\ y_0 - ka')\ /\ k \in \mathbb{Z}\}$$

Cet énoncé donne la justification théorique de la méthode décrite précédemment ; explicitement, il justifie que l'on obtient la solution générale de l'équation avec second membre en faisant la somme d'une solution particulière de cette équation, et de la solution générale de l'équation homogène associée.

6.3. **CNS d'existence d'un couple solution.** La dernière propriété décrit l'ensemble des solutions de $ax + by = c$, **sous réserve** de l'existence d'une solution particulière.

Une telle solution particulière (x_0, y_0) existe SSI $a \wedge b | c$, en vertu de la propriété suivante.[2]

Propriété. Soient a et b deux entiers.
On a :

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\,\mathbb{Z}$$

Explication de texte. $a\mathbb{Z}$ désigne l'ensemble des multiples de a :

$$a\mathbb{Z} = \{ka,\ k \in \mathbb{Z}\}$$

$b\mathbb{Z}$ et $(a \wedge b)\,\mathbb{Z}$ désignent donc les ensembles des multiples de b et $a \wedge b$ respectivement.

La notation $a\mathbb{Z} + b\mathbb{Z}$ désigne l'ensemble des entiers sommes d'un multiple de a et d'un multiple de b :

$$a\mathbb{Z} + b\mathbb{Z} = \{au + bv,\ (u, v) \in \mathbb{Z}^2\}$$

La propriété signifie donc que tout entier multiple du PGCD de a et b est la somme d'un multiple de a et d'un multiple de b, et réciproquement.

En conclusion. Pour résoudre l'équation $ax + by = c$, on commence par vérifier que $a \wedge b | c$. Si tel est le cas, on applique la méthode décrite à la page précédente. En particulier, on détermine une solution (x_0, y_0) de l'équation à l'aide de coefficients de Bezout pour a et b.

Pour des illustrations de cette méthode, voir exos 36 à 39 de la feuille ; voir aussi les 200 exemples du document "spécial équations diophantiennes".

2. Dont la preuve sera au programme de colle, en MPSI et en MP.

7. PPCM

Définition. Soient a et b deux entiers non nuls. Le **plus petit commun multiple (PPCM)** de a et b est le plus petit (au sens de la relation d'ordre $\leqslant$) entier naturel non nul multiple à la fois de a et de b.

Le PPCM de a et b est noté $a \vee b$.

Convention. $\forall (a,b) \in \mathbb{Z}^2,\ a \vee 0 = 0 \vee b = 0$.

Le PPCM de deux entiers possède un certain nomnbre de propriétés élémentaires :

- $\forall (a,b) \in \mathbb{Z}^2,\ a \vee b = b \vee a$
- $\forall (a,b) \in \mathbb{Z}^2,\ a \vee b = |a| \vee |b|$
- $\forall (a,b,n) \in \mathbb{Z}^2 \times \mathbb{N},\ na \vee nb = n\,(a \vee b)$

Enfin, le très joli énoncé suivant donne le lien entre le PGCD et le PPCM de deux entiers.

Propriété. Soient a et b deux entiers.

On a :

$$(a \wedge b)\,(a \vee b) = |ab|$$

En particulier, le PPCM peut se déduire directement du PGCD (que l'on sait déterminer grâce à l'algorithme d'Euclide).

8. Nombres premiers

8.1. Généralités.

Définition. Un nombre **premier** est un entier admettant exactement deux diviseurs dans $\mathbb{N}$: 1 et lui-même.

Notation. On note $\mathscr{P}$ l'ensemble des nombres premiers.

Exemples. 2, 3, 5, 7, 11, 13, -17, 19, 59 sont premiers. 0, 1, 1341, 745, 3883 ne le sont pas.

La propriété ci-dessous donne une caractérisation des nombres premiers.

Propriété. Soit $p \in \mathbb{N}$. LASSE :

1/ p est premier

2/ p est premier avec tout entier qu'il ne divise pas.

3/ p est premier avec tout entier compris entre 2 et $p-1$.

8.2. Le "petit" théorème de Fermat.

Le théorème faisant l'objet de ce paragraphe permet de simplifier beaucoup d'exos relatifs aux congruences ; c'est également un ingrédient de base dans l'algorithme de codage RSA utilisé en cryptographie.

"Petit" théorème de Fermat. Soit $p \in \mathscr{P}$.

$$\forall n \in \mathbb{Z}, \qquad n^p \equiv n\ [p]$$