Chapitre 1

Arithmétique

Ce texte est une liste d'exercices avec un résumé succinct des principaux résultats et définitions du cours. Il ne remplace donc pas le cours ! Pour le contenu du chapitre "Arithmétique", on peut se reporter au chapitre 9 du Cours de mathématiques – Algèbre 1re année de F. Liret et D. Martinais (éditions Dunod).

1.1 Division euclidienne, divisibilité

La *division euclidienne* est la "division avec reste" des entiers naturels. On rappelle ce qui la caractérise.

Proposition 1.1 *Soient a et b deux entiers naturels avec $b \neq 0$. Alors il existe deux entiers naturels q (*quotient*) et r (*reste*) tels que*

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b\ .$$

De plus il n'y a qu'un couple d'entiers (q, r) qui vérifie cette propriété.

La division euclidienne peut se généraliser aux entiers relatifs : étant donnés deux entiers relatifs a et b, avec $b \neq 0$, il existe un unique couple (q, r), où q est un entier relatif et r un entier tel que $0 \leq r < |b|$, tel que $a = bq + r$.

Soient a et b deux entiers relatifs. Par définition, on dit que b *divise* a quand il existe un entier naturel q tel que $a = bq$ (la division "tombe juste", son reste est nul). On dit aussi que b est un *diviseur* de a, ou que a est un *multiple* de b.

Exercice 1.1

Montrer qu'un et un seul des trois entiers naturels n, $n + 2$ et $n + 4$ est divisible par 3.

Exercice 1.2

Montrer que, si n est un entier qui n'est divisible ni par 2, ni par 3, alors $n^2 + 23$ est divisible par 24. (Utiliser la division de n par 6.)

Exercice 1.3

Montrer que, si a et b sont deux entiers et $b \neq 0$, alors il existe des entiers q et r uniques tels que $a = bq + r$ et $-\dfrac{|b|}{2} < r \leq \dfrac{|b|}{2}$.

Exercice 1.4

Montrer que, si l'entier relatif m divise les entiers relatifs $8n + 7$ et $6n + 5$, alors $m = \pm 1$.

Exercice 1.5

Montrer que, si m et n sont deux entiers strictement positifs tels que $\dfrac{1}{m} + \dfrac{1}{n}$ est entier, alors $m = n$. En déduire les valeurs possibles de m et de n.

Exercice 1.6

Soit $N = \overline{mcdu}$ un nombre de quatre chiffres. On note $P = \overline{udcm}$. Montrer que $N + P$ est divisible par 11 et donner le quotient.

Exercice 1.7

Soit n un entier relatif, a et b deux entiers strictement positifs. Démontrer que si q est le quotient de n par a et q' le quotient de q par b, alors q' est aussi le quotient de n par le produit ab.

Exercice 1.8

Soit deux entiers naturels $a \geq 3$ et $b \geq 2$. Connaissant le quotient de la division de $a - 1$ par b, calculer le quotient de la division de $ab^n - 1$ par b^{n+1}, pour tout entier naturel n.

1.2 Plus grand commun diviseur, Bezout, entiers premiers entre eux

Soient a et b deux entiers relatifs. Le *plus grand commun diviseur* de a et b, est l'entier naturel d qui vérifie

1. d est un diviseur commun de a et b,
2. tout diviseur commun de a et b divise d.

On notera $\text{pgcd}(a, b)$ le plus grand commun diviseur de a et b. L'unicité du pgcd est facile. L'existence est établie par *l'algorithme d'Euclide*, qui permet de calculer le pgcd.

Soient a et b deux entiers naturels. On pose

$$r_0 = a \qquad r_1 = b$$

et, pour $n \geq 1$, tant que r_n est non nul, on définit r_{n+1} comme le reste de la division euclidienne de r_{n-1} par r_n :

$$r_{n-1} = r_n q_n + r_{n+1} \quad \text{avec } 0 \leq r_{n+1} < r_n.$$

L'algorithme s'arrête au bout d'un nombre fini N d'étapes, avec $r_{N+1} = 0$, puisque la suite $r_1, r_2, \ldots$ est une suite d'entiers naturels strictement décroissante.

Théorème 1.2 $\text{pgcd}(a, b) = r_N$ *(c'est le dernier reste non nul, si a et b sont différents de 0).*

Si a et b sont tous les deux nuls, $\text{pgcd}(a, b) = 0$. Sinon, le pgcd est le plus grand des entiers naturels qui divisent à la fois a et b (c'est souvent comme cela que le pgcd est défini, par exemple chez Liret-Martinais).

Si a et b sont des entiers relatifs, le pgcd de a et b est celui des entiers naturels $|a|$ et $|b|$.

L'algorithme d'Euclide a la propriété suivante : pour tout entier $n \geq 0$, il existe des entiers relatifs u_n et v_n tels que $r_n = u_n a + v_n b$. En particulier, on obtient :

Théorème 1.3 (Bezout) *Soient a et b deux entiers relatifs. Il existe des entiers relatifs u et v tels que*

$$\text{pgcd}(a, b) = ua + vb\ .$$

Traitons un exemple : trouver le pgcd de 4641 et de 1898 et une identité de Bezout comme ci-dessus.

$$\begin{aligned}
& & r_0 &= 4641 \\
& & r_1 &= 1898 \\
4641 &= 1898 \times 2 + 845 & r_2 &= 845 = 4641 - 2 \times 1898 \\
1898 &= 845 \times 2 + 208 & r_3 &= 208 = 1898 - 2 \times 845 = -2 \times 4641 + 5 \times 1898 \\
845 &= 208 \times 4 + 13 & r_4 &= 13 = 845 - 4 \times 208 = 9 \times 4641 - 22 \times 1898 \\
208 &= 13 \times 16 & r_5 &= 0
\end{aligned}$$

Le pgcd de 4641 et de 1898 est 13, et on obtient une identité de Bezout $13 = 9 \times 4641 - 22 \times 1898$.

Deux entiers relatifs a et b sont dits *premiers entre eux* quand $\text{pgcd}(a, b) = 1$, autrement dit si et seulement si le seul entier naturel diviseur commun de a et b est 1. Du théorème de Bezout on déduit facilement la propriété suivante :

Théorème 1.4 *Deux entiers a et b sont premiers entre eux si et seulement s'il existe des entiers relatifs u et v tels que $ua + vb = 1$.*

L'identité de Bezout est une traduction utile du fait que deux nombres sont premiers entre eux, comme par exemple pour établir le résultat suivant, qui sert entre autres pour la décomposition en facteurs premiers.

Théorème 1.5 (Théorème de Gauss) *Soient a, b et c des entiers tels que a et b soient premiers entre eux et que a divise le produit bc. Alors a divise c.*

Un thème qui revient dans plusieurs exercices (10, 11, 14 et 15) est celui de la résolution de l'équation $ax + by = c$, où a, b, c sont des entiers donnés et x, y des inconnues entières. Une fois ces exercices traités, Il est conseillé de systématiser le travail fait pour décrire un algorithme général de résolution de telles équations (l'identité de Bezout est ici un outil essentiel).

Le *plus petit commun multiple* (ppcm) de deux entiers a et b est l'unique entier naturel m tel que

1. m est un multiple commun de a et b,
2. tout multiple commun de a et b est multiple de m.

Si a ou b est nul, $\text{ppcm}(a, b) = 0$. Si a et b sont deux entiers strictement positifs, on a $\text{ppcm}(a, b) = ab/\text{pgcd}(a, b)$.

Exercice 1.9

Calculer $d = \text{pgcd}(a, b)$ ainsi que des entiers u et v vérifiant $au + bv = d$ dans les cas suivants

1. $a = 806$ et $b = 102$.
2. $a = 7700$ et $b = 2233$.
3. $a = 126$ et $b = 198$.

Exercice 1.10

On considère les couples (x, y) d'entiers relatifs qui vérifient l'équation (E) $26x + 15y = 1$.

1. Ecrire l'algorithme d'Euclide pour les nombres 26 et 15.
2. En déduire une solution particulière de l'équation (E), puis l'ensemble de toutes les solutions.
3. Utiliser ce qui précède pour résoudre l'équation $26x + 15y = 4$.

Exercice 1.11

1. Calculer $\text{pgcd}(15, 21)$.
2. L'équation $15x - 21y = 5$ admet-elle des solutions dans $\mathbb{Z} \times \mathbb{Z}$?

Exercice 1.12

Soit a un entier naturel. Montrer que $n = 14a + 3$ et $m = 21a + 4$ sont premiers entre eux et trouver deux entiers u et v tels que $un + vm = 1$.

Exercice 1.13

Soit a et b deux entiers premiers entre eux.

1. Montrer que le pgcd de $a + b$ et $a - b$ vaut 1 ou 2. Préciser, suivant la parité respective de a et b, dans quels cas on obtient chacune de ces valeurs.
2. Montrer que le pgcd de $2a + b$ et $a + 2b$ vaut 1 ou 3.

Exercice * 1.14

Examen de janvier 1997

1. (a) Montrer que 15 et 28 sont premiers entre eux.
   (b) Trouver une solution particulière dans $\mathbb{Z} \times \mathbb{Z}$ de l'équation

$$28x - 15y = 1 \ .$$

(c) En déduire une solution particulière dans $\mathbb{Z} \times \mathbb{Z}$ de l'équation

$$28x - 15y = 11 .$$

(d) Trouver l'ensemble des couples d'entiers relatifs (x, y) vérifiant :

$$28x - 15y = 11 .$$

On définit une application f

$$f : \begin{cases} \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ (x, y) & \longrightarrow & 28x - 15y \end{cases}$$

3. (a) Montrer que f est surjective.
   (b) L'application f est-elle injective ?
4. (a) Calculer le pgcd de 15 et 21.
   (b) L'équation $15x - 21y = 5$ admet-elle des solutions dans $\mathbb{Z} \times \mathbb{Z}$?

Exercice 1.15

Examen de septembre 1997

1. Déterminer $\text{pgcd}(15, 21)$.
2. Trouver tous les couples d'entiers relatifs (x, y) tels que $15y - 21x = 3$.
3. Trouver tous les couples d'entiers relatifs (x, y) tels que $15y - 21x = 5$.
4. En déduire toutes les solutions dans $\mathbb{Z}$ de l'équation $(15y - 21x - 4)(2y - x + 4) = 1$.

Exercice 1.16

Soit a, b, c et d quatre entiers naturels tels que $\text{pgcd}(a, b) = \text{pgcd}(c, d) = 1, b > 0, d > 0$ et $a/b + c/d$ est entier. Montrer que $b = d$.

Exercice 1.17

Soit n un entier naturel, on pose $a = 12n^2 + 16n + 6$ et $b = 6n + 5$. Calculer $\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$.

1.3 Nombres premiers. Décomposition en facteurs premiers

Un *nombre premier* est un entier $p \geq 2$ tel que les seuls entiers naturels qui le divisent soient 1 et p.

Proposition 1.6 *Soit p un nombre premier, et a un entier naturel. Si p ne divise pas a, alors p est premier avec a. En particulier deux nombres premiers distincts sont premiers entre eux.*

Soit n un entier supérieur ou égal à 2. Un nombre premier qui divise n s'appelle un *facteur premier* de n. Tout entier $n \geq 2$ a un facteur premier. Soit n est premier, soit il a un facteur premier $\leq \sqrt{n}$.

Proposition 1.7 *Il y a une infinité de nombres premiers : étant donnés n nombres premiers $p_1, \ldots, p_n$, on peut toujours en trouver un $n+1$-ème p_{n+1}, différent des n autres.*

Théorème 1.8 *Soit a un entier supérieur ou égal à 2. Alors on peut décomposer a sous la forme d'un produit*

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

où $p_1, \ldots, p_k$ sont des nombres premiers vérifiant $p_1 < \ldots < p_k$, et les exposants $\alpha_1, \ldots, \alpha_k$ sont des entiers strictement positifs. De plus, une telle décomposition est unique.

Soient a et b deux entiers supérieurs ou égaux à 2. La décomposition en facteurs premiers de $\text{pgcd}(a, b)$ s'obtient en prenant les facteurs premiers qui figurent à la fois dans la décomposition de a et dans celle de b, avec pour puissance la plus petite des deux. Les entiers a et b sont premiers entre eux si et seulement s'il n'ont pas de facteur premier commun.

Exercice 1.18

1. Décomposer en facteurs premiers $a = 4725$, $b = 3718$ et $c = 3234$.
2. Calculer $\text{pgcd}(a, c), \text{ppcm}(a, c), \text{pgcd}(b, c)$ et $\text{ppcm}(b, c)$.

Exercice 1.19

On dit qu'un entier naturel a est un carré parfait s'il existe un entier n tel que $a = n^2$.

1. Montrer que l'entier $a > 1$ est un carré parfait si et seulement si dans sa décomposition en facteurs premiers tous les exposants sont pairs.
2. Montrer que l'entier a est un carré parfait si et seulement s'il a un nombre impair de diviseurs positifs.

Exercice 1.20

Déterminer l'exposant de 3 dans la décomposition en facteurs premiers de 100!. Par combien de zéros le nombre 100! se termine-t-il ?

Exercice 1.21

Montrer que, si $p > 5$ est premier, alors $p^4 - 1$ est divisible par 240.

Exercice 1.22

Examen de janvier 1998

Si a et b sont deux entiers naturels non nuls, on note d leur pgcd et m leur ppcm. On pose $a = da'$ et $b = db'$ et on note $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

1. Montrer que a' et b' sont premiers entre eux.
2. On considère le problème suivant

$$(S) \qquad \begin{cases} a & < b \\ a+b & = 51 \\ m & = 216 \end{cases}$$

   (a) Décomposer 51 et 216 en produits de facteurs premiers. En déduire $\text{pgcd}(51, 216)$. Donner toutes les décompositions de 216 en produit de deux entiers naturels x et y premiers entre eux.

   (b) Montrer que, si $(a, b) \in {\mathbb{N}^*}^2$ est solution de (S), alors d divise $\text{pgcd}(51, 216)$. En déduire les valeurs possibles de d.

   (c) Trouver toutes les solutions dans ${\mathbb{N}^*}^2$ du système (S).

Exercice 1.23

1. Montrer que, si deux entiers a et b sont premiers entre eux, il en est de même de $a+b$ et ab. Etudier la réciproque.
2. Montrer que le pgcd de deux entiers naturels est le même que celui de leur somme et de leur ppcm. En déduire deux entiers naturels connaissant leur somme 68 et leur ppcm 240.

1.4 Congruences

Soit n un entier supérieur ou égal à 2. On dit que deux entiers relatifs a et b sont *congrus modulo* n quand n divise $a-b$. On note $a \equiv b \pmod{n}$. Deux entiers relatifs sont congrus modulo n si et seulement s'ils ont même reste dans la division euclidienne par n.

La *classe de congruence modulo* n d'un entier relatif a est l'ensemble de tous les entiers relatifs qui sont congrus à a modulo n. Autrement dit, c'est l'ensemble des entiers relatifs de la forme $a+nq$ où q est un entier relatif quelconque. On utilisera la notation $\overline{a}$ pour désigner la classe de congruence de a. Deux entiers a et b sont congrus modulo n si et seulement si leurs classes de congruences sont égales. Il y a n classes de congruence modulo n, qui sont $\overline{0}$, $\overline{1}$,...,$\overline{n-1}$. L'ensemble des n classes de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$.

Théorème 1.9 *Soient a, b, c et d quatre entiers relatifs qui vérifient $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$. Alors*

$$\begin{aligned} -a &\equiv -b \pmod{n}, \\ a+c &\equiv b+d \pmod{n}, \\ ac &\equiv bd \pmod{n}. \end{aligned}$$

Les règles qui figurent dans le théorème permettent de faire rapidement des "calculs modulo n". Par exemple, calculons $1!+2!+3!+4!+5!+6!$ modulo 7. On a (toutes les congruences sont modulo 7) :

$$4! \equiv 3 \quad 5! \equiv 3 \times 5 \equiv 1 \quad 6! \equiv 5! \times 6 \equiv 6,$$

d'où

$$1!+2!+3!+4!+5!+6! \equiv 1+2+6+3+1+6 \equiv 5,$$

autrement dit le reste de la division euclidienne de $1!+2!+3!+4!+5!+6!$ par 7 est 5.

Les résultats du théorème permettent de définir l'addition et la multiplication de classes de congruence modulo n. On pose

$$\overline{a} + \overline{c} = \overline{a+c}$$

et

$$\overline{a} \times \overline{c} = \overline{ac}$$

. Ces opérations font de $\mathbb{Z}/n\mathbb{Z}$ un anneau commutatif.

Si a est premier avec n, alors on peut simplifier par a dans les congruences modulo n.

Proposition 1.10 *Supposons que l'entier relatif a est premier avec n. Alors il existe un entier relatif u tel que $au \equiv 1 \pmod{n}$. En conséquence, si $ab \equiv ac \pmod{n}$, alors $b \equiv c \pmod{n}$.*

Proposition 1.11 (Petit théorème de Fermat) *Soit p un nombre premier, et a un entier qui n'est pas divisible par p. Alors p divise $a^{p-1}-1$.*

Le petit théorème de Fermat peut servir à des calculs de puissances modulo un entier. Ce thème des calculs de puissances se retrouve dans plusieurs exercices.

Un thème différent, qui se retrouve dans les exercices 36, 37 et 38, est celui de la résolution de systèmes du genre

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{k} \end{cases}$$

L'identité de Bezout (pour n et k) est ici l'outil principal.

Exercice 1.24

Montrer que le produit de trois entiers consécutifs est divisible par 3.

Exercice 1.25

Montrer que tout entier premier > 3 est de la forme $6k \pm 1$.

Exercice 1.26

Quel est le reste de la division par 7 de 247^{349}, de la division par 13 de 100^{1000} ?

Exercice 1.27

Montrer que $2^{70}+3^{70}$ est divisible par 13.

Exercice 1.28

Montrer que, pour tout n entier naturel, $2^{2^{6n+2}}+3$ est divisible par 19.

Exercice 1.29

Quel est le chiffre des unités du nombre 7^{7^7}, du nombre $3548^9 \times 2537^{31}$?

Exercice 1.30

Montrer que tout chiffre peut être chiffre des unités d'un cube.

Exercice 1.31

1. Soit m et n deux entiers. Montrer que, si m divise $35n + 26$ et $7n + 3$, et, si $m > 1$, alors $m = 11$.
2. Pour $m = 11$, n existe-t-il ?

Exercice 1.32

Si $a \equiv b \mod n$, a-t-on $a^a \equiv b^b \mod n$?

Exercice 1.33

Montrer que deux entiers naturels a et b sont divisibles par 7 si et seulement si $a^2 + b^2$ l'est.

Exercice 1.34

Trouver trois entiers impairs consécutifs dont la somme des carrés s'écrit comme un nombre à quatre chiffres identiques.

Exercice 1.35

Examen de janvier 1997

On note E l'ensemble des entiers x dont le carré est congru à 2 modulo 7 et F l'ensemble des entiers x dont le carré est congru à 2 modulo 49, c'est-à-dire

$$E = \{x \in \mathbb{Z} \mid x^2 \equiv 2\,[7]\} \text{ et } F = \{x \in \mathbb{Z} \mid x^2 \equiv 2\,[49]\}.$$

1. (a) Calculer les carrés des éléments de $\mathbb{Z}/7\mathbb{Z}$.
   (b) En déduire l'ensemble E.
2. Montrer que l'ensemble F est inclus dans l'ensemble E.
3. (a) Trouver tous les entiers relatifs k tels que $3 + 7k$ appartienne à F.
   (b) Déterminer F.

Exercice 1.36

Examen de juin 1995

Résoudre dans $\mathbb{Z}$ le système

$$\begin{cases} x & \equiv 2 \pmod 6 \\ x & \equiv 4 \pmod 5 \\ x & \equiv 0 \pmod 4 \end{cases}$$

Exercice 1.37

Examen de janvier 1995

Si $x \in \mathbb{Z}$, on note $\bar{x}$ la classe de congruence de x modulo 4 et $\hat{x}$ la classe de congruence de x modulo 3. On considère l'application

$$f : \left[\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\ x & \longmapsto & (\bar{x}, \hat{x}) \end{array} \right.$$

1. (a) Soit $E = \{x \in \mathbb{Z} \mid f(x) = (\bar{0}, \hat{0})\}$. Montrer que $E = 12\mathbb{Z}$ (c'est-à-dire que E est l'ensemble des multiples de 12).
   (b) f est-elle injective ?
2. (a) Soit x_1 et x_2 deux entiers relatifs, calculer $f(4x_2 - 3x_1)$.
   (b) En déduire que f est surjective.

Exercice 1.38

Dix-sept pirates s'emparent d'un lot de pièces d'or toutes identiques. Leur loi exige un partage à égalité. Chacun doit recevoir le même nombre de pièces d'or et, s'il y a un reste, celui-ci est attribué au cuisinier de bord. Dans le cas présent la part du cuisinier serait de trois pièces mais les pirates se querellent et six d'entre eux sont tués, ce qui porte la part du cuisinier à quatre pièces. Au cours d'une tempête terrible le bateau fait naufrage et ne survivent que six pirates et le cuisinier. Par bonheur le butin est sauvé. La part du cuisinier est maintenant de cinq pièces.

Que peut espérer gagner le cuisinier lorsqu'il décide d'empoisonner le reste de l'équipage sachant que c'est la plus petite des solutions possibles ?

Exercice 1.39

Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation $3x + 4 = 0$. Cette équation a-t-elle des solutions dans $\mathbb{Z}/6\mathbb{Z}$? Quel est le nombre de solutions de $6x = 4$ dans $\mathbb{Z}/10\mathbb{Z}$?