**Notes de Cours**

# AM : ATELIERS MATHÉMATIQUES

Clément Boulonne
Web : http://clementboulonne.new.fr
Mail : clement.boulonne@gmail.com

**Université des Sciences et Technologies de Lille**
**U.F.R de Mathématiques Pures et Appliquées**
Licence de Mathématiques — Semestre 1
2006 – 2007

# Table des matières

# PROGRAMME DU COURS

AM : **Ateliers Mathématiques** [S1, 5 ECTS]
Prérequis : Aucun

Cette option permet d'une part de renforcer certaines notions traitées dans les unités M101 et M102 et d'autre part d'initier à la recherche à travers quelques thèmes de mémoires tels que les nombres pythagoriciens et le problème de Fermat, Crytographie à clef publique, les décimales de $\pi$, comment calculait-on les logarithmes avant les ordinateurs ?

- Congruences.
  Définitions et propriétés. Divisibiltié. Relation d'équivalence. Polynômes. Classe d'équivalence. L'ensemble $\mathbf{Z}/n\mathbf{Z}$ et ses opérations. Structure de $\mathbf{Z}/n\mathbf{Z}$ : rappels sur les groupes, $(\mathbf{Z}/n\mathbf{Z}, \oplus)$ est un groupe, $((\mathbf{Z}/n\mathbf{Z})^\times, \otimes)$ est un groupe abélien. Théorème de Gauss. Fonction d'Euler. Théorème de Wilson.
  « Petit théorème de Fermat » : les deux versions. Théorème d'Euler.
  Résolution de congruences. Équations diophantiennes. Équations de congruences. Théorème chinois pour les systèmes d'équations de congruences.
  Applications aux codages des messages secrets. Applications sur les périodes d'un développement décimal.
- Fractions continues.
  Définition de fractions continues à coefficients entiers. Récurrences et calcul effectif.
  Fractions continues $1/a_n$, $a_n \in \mathbf{N}$ : encadrements de nombres, formule d'Euler, « meilleure » approximation par nombres rationnels, critère d'irrationnalité.
  Nombres quadratiques et leur fonction continue.

# CHAPITRE I

# CONGRUENCES

## I.1 Premières définitions et propriétés

**Définition I.1** (Divisibilité)**.** *Soient $a, b \in \mathbf{Z}$. On dit que $a$* divise *$b$ (qu'on notera $a \mid b$) s'il existe un entier $k$ tel que $b = ka$ (on dit aussi que $b$ est* multiple *de $a$). Si $a$ ne divise pas $b$, on notera $a \nmid b$.*

**Exemples I.2.**
1. On a $2 \mid 4$ car $4 = 2 \times 2$.
2. On a $3 \mid 9$ car $9 = 3 \times 3$.
3. On a $6 \mid 30$ car $30 = 6 \times 5$.

**Définition I.3** (Congruence)**.** *Soit $n$ un entier tel que $n > 1$ et soient $a$ et $b$ des entiers. On dit que $a$ et $b$ sont* congrus modulo *$n$ (noté $a \equiv b \pmod{n}$) si $n \mid a - b$.*

**Exemples I.4.**
1. On a $8 \equiv 1 \pmod{7}$ car $7 \mid 8 - 1$.
2. On a $122 \equiv 1 \pmod{11}$ car $11 \mid 122 - 1$ et $122 - 1 = 121 = 11 \times 11 - 1$.

**Définition I.5** (Relation d'équivalence)**.** *Soient $E$ un ensemble non vide et $\mathscr{R}$ une relation entre les éléments de $E$. On dit que $\mathscr{R}$ est une* relation d'équivalence *si :*
- *pour tout $x \in E$, $x\mathscr{R}x$ (réflexivité) ;*
- *pour tout $x, y \in E$, si $x\mathscr{R}y$ alors $y\mathscr{R}x$ (symétrique) ;*
- *pour tout $x, y, z \in E$, si $x\mathscr{R}y$ et $y\mathscr{R}z$ alors $x\mathscr{R}z$ (transitivité).*

**Exemples I.6.**
1. Soit $E = \{a, b, c, d, e\}$. On suppose qu'il existe une relation $\mathscr{R}$ telle que $a\mathscr{R}a$, $b\mathscr{R}b$, $c\mathscr{R}c$, $d\mathscr{R}d$ et $e\mathscr{R}e$. On peut vérifier que cette relation est bien une relation d'équivalence (voir la figure I.1 pour une représentation sagitale de la situation).

2. Soient $E = \{a, b, c, d, e\}$ et $\mathscr{R}$ la relation d'équivalence représentée sagitalement par la figure I.2. On peut montrer aussi que c'est une relation d'équivalence.
3. Soit $E = \mathbf{R}$. On considère la relation $\mathscr{R}$ « inférieur ou égal ». On montre que $\mathscr{R}$ n'est pas une relation d'équivalenc. On a bien, pour tout $x \in \mathbf{R}$, $x \leq x$ mais $\mathscr{R}$ n'est pas symétrique car si $1 \leq 2$, on n'a pas $2 \leq 1$. D'où $\mathscr{R}$ n'est pas une relation d'équivalence sur $\mathbf{R}$.

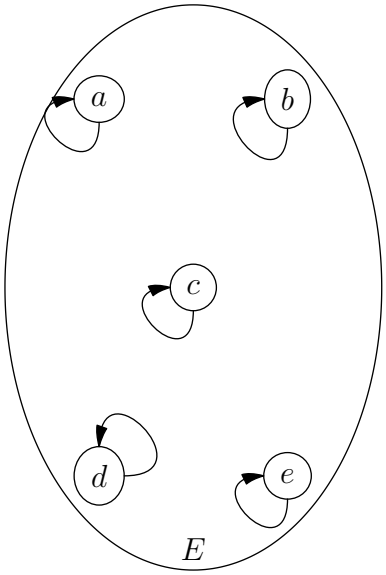


FIGURE I.1 – La relation $\mathscr{R}$ (exemple I.6-1) qui relie chaque élément à lui-même est une relation d'équivalence.

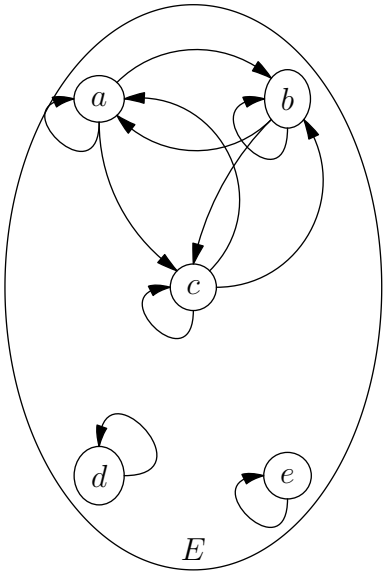


FIGURE I.2 – La relation $\mathscr{R}$ pour l'exemple I.6-2

4. Voir la proposition I.7.

**Proposition I.7.** *Soient $E = \mathbf{Z}$ et $n \in \mathbf{Z}^*$. La relation « congru modulo $n$ » est une relation d'équivalence.*

*Démonstration.* **Réflexivité** Pour tout $a \in \mathbf{Z}$, on a $a \equiv a \pmod{n}$ car, en effet, $a - a = 0 \times n$.

**Symétrie** On suppose que $a \equiv b \pmod{n}$. Il existe donc $k \in \mathbf{Z}$, $a - b = kn$. On a : $b - a = (-k)n$ et comme $-k \in \mathbf{Z}$, on obtient bien $b \equiv a \pmod{n}$.

**Transitivité** Soient $a, b, c \in \mathbf{Z}$ et on suppose que $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$. Il existe donc $k, k' \in \mathbf{Z}$ tel que $a = b + nk$ et $b = c + nk'$. Si on combine tout cela, on obtient :

$$a = b + nk = (c + nk') + nk = c + n(k + k')$$

et comme $k + k' \in \mathbf{Z}$, on obtient $a \equiv c \pmod{n}$.

D'où « congru modulo $n$ » est une relation d'équivalence. □

**Proposition I.8.** *Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors :*

*(i)* $a + c \equiv b + d \pmod{n}$,

*(ii)* $a \cdot c \equiv b \cdot d \pmod{n}$.

*Démonstration.* On a comme hypothèse $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, d'où il existe $k, k'$ tels que $a - b = nk$ et $c - d = nk'$.

(i) On a :

$$a + c - (b + d) = (a - b) + (c - d) = nk + nk' = n(k + k').$$

D'où $a + c \equiv b + d \pmod{n}$.

(ii) On a :

$$a \cdot c = kk'n^2 + (kd + k'd) \cdot n + bd = (kk'n + kd + k'b)n + b_1b_2.$$

D'où $a \cdot c \equiv b \cdot d \pmod{n}$.

□

**Définition I.9** (Polynômes)**.** *Soit $E$ un ensemble. On appelle* polynôme *à coefficients dans $E$, une expression du type :*

$$a_0 + a_1X + \cdots + a_nX^n, \quad a_i \in E,\ n \in \mathbf{N}.$$

*$X$ est appelée une* indeterminée. *On note $E(X)$ l'ensemble à coefficients dans $E$.*

**Exemples I.10.** Le polynôme $1 + 2X$ appartient à $\mathbf{Z}[X]$ et comme $\mathbf{Z} \subset \mathbf{R}$, on a : $1 + 2X \in \mathbf{R}[X]$. Le polynôme $X^3 + 3X^2 + \sqrt{2}X^5$ n'appartient pas à $\mathbf{Z}[X]$ car $\sqrt{2} \notin \mathbf{Z}$. Par contre, ce dernier polynôme appartient à $\mathbf{R}[X]$.

**Proposition I.11.** *Soit* $P \in \mathbf{Z}[X]$ *avec :*

$$P(X) = \sum_{i=0}^{n} \alpha_i X^i, \quad \alpha_i \in \mathbf{Z}.$$

*Soient* $a, b \in \mathbf{Z}$ *tels que* $a \equiv b \pmod{n}$ *alors* $P(a) \equiv P(b) \pmod{n}$.

*Démonstration.* Si $a \equiv b \pmod{n}$ alors il existe $k \in \mathbf{Z}$ tel que $a - b = nk$. D'après la proposition I.8-(ii), on a, pour tout $1 \leq k \leq n$, $a^k \equiv b^k \pmod{n}$ et de plus,

$$\alpha_k \equiv \alpha_k \pmod{n}, \quad \text{pour } 1 \leq k \leq n.$$

D'où, en faisant la somme, on obtient $P(a) \equiv P(b) \pmod{n}$. □

**Définition I.12** (Classes d'équivalence)**.** *Soient* $E$ *un ensemble non vide et* $\mathscr{R}$ *une relation d'équivalence. Soit* $a \in E$*, on appelle la* classe d'équivalence *de* $a$ *(qu'on note* $\overline{a}$*, l'ensemble de tous les éléments de* $E$ *qui sont en relation avec* $a$*.*

$$\overline{a} = \{x \in E,\ x \mathscr{R} a\}.$$

*Comme* $\mathscr{R}$ *est réflexive,* $a \in \overline{a}$ *donc* $\overline{a}$ *n'est pas l'ensemble vide.*

**Exemples I.13.**

1. Soit $E = \{a, b, c, d, e\}$ un ensemble et $\mathscr{R}$ une relation d'équivalence définie sagitalement par la figure I.3. On a :

$$\overline{a} = \{a, b, c\}.$$

2. On prend $E = \mathbf{Z}$ et on se fixe $n \in \mathbf{N}^*$. On définit par $\mathscr{R}$ la relation (d'équivalence) « congru modulo $n$ ». Soit $a \in \mathbf{Z}$ alors :

$$\overline{a} = \{b \in \mathbf{Z},\ b \equiv a \pmod{n}\} = \{a + nk,\ k \in \mathbf{Z}\}.$$

Si, par exemple, $n = 5$, on obtient :

$$\begin{aligned}
\overline{0} &= \{0, 5, 10, 15, 20, \ldots\} = \{5k,\ k \in \mathbf{Z}\} \\
\overline{1} &= \{1, 6, 11, 16, \ldots\} = \{5k + 1,\ k \in \mathbf{Z}\} \\
\overline{2} &= \{2, 7, 12, 17, \ldots\} = \{5k + 2,\ k \in \mathbf{Z}\} \\
\overline{3} &= \{3, 8, 13, 18, \ldots\} = \{5k + 3,\ k \in \mathbf{Z}\} \\
\overline{4} &= \{5k + 4,\ k \in \mathbf{Z}\} \\
\overline{5} &= \{5k + 5,\ k \in \mathbf{Z}\} = \{5(k + 1),\ k \in \mathbf{Z}\} = \overline{0}.
\end{aligned}$$

**Définition I.14** (Ensemble des classes)**.** *Soient* $E$ *un ensemble non vide et* $\mathscr{R}$ *une relation d'équivalence. L'*ensemble des classes *relativement à la relation* $\mathscr{R}$ *est noté :*

$$E/\mathscr{R} = \{\overline{a},\ a \in E\}.$$

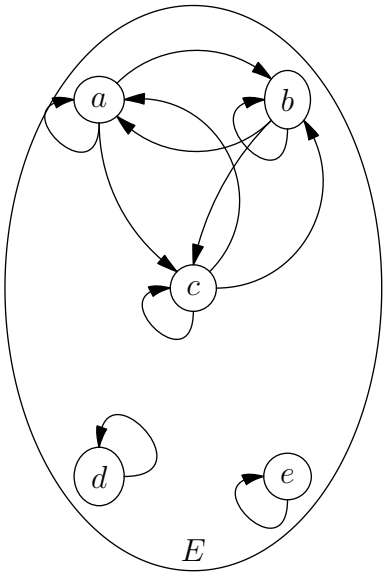


FIGURE I.3 – La relation $\mathscr{R}$ pour l'exemple I.13-1

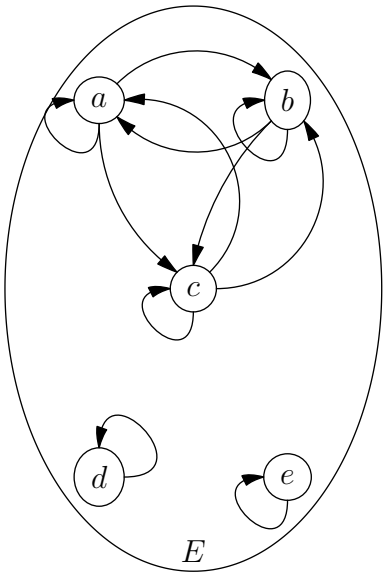


FIGURE I.4 – La relation $\mathscr{R}$ pour l'exemple I.15-1

**Exemples I.15.** 1. Soit $E = \{a, b, c, d, e\}$ un ensemble et $\mathscr{R}$ une relation d'équivalence définie sagitalement par la figure I.4. On a :

$$E/\mathscr{R} = \left\{\overline{a}, \overline{b}, \overline{c}, \overline{d}, \overline{e}\right\} = \left\{\overline{a}, \overline{b}, \overline{e}\right\}.$$

2. On se place dans $\mathbf{Z}$ et on considère la relation $\mathscr{R}$ « congru modulo $n$ ». On a :

$$\mathbf{Z}/\mathscr{R} = \{\overline{a},\ a \in \mathbf{Z}\} = \{a + nk,\ k \in \mathbf{Z}\ ; a \in \mathbf{Z}\}$$

On notera $\mathbf{Z}/n\mathbf{Z} := \mathbf{Z}/$« congru modulo $n$ ».

**Définition I.16** ($\mathbf{Z}/n\mathbf{Z}$)**.** *Soient $n \in \mathbf{N}$ et $\mathscr{R}$ la relation d'équivalence « congru modulo $n$ ». $\mathbf{Z}/n\mathbf{Z}$ constitue l'ensemble des classes de $\mathscr{R}$.*

**Proposition I.17.** *Soit $n \in \mathbf{N}$,*

$$\mathbf{Z}/n\mathbf{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

*et* $\operatorname{card}(\mathbf{Z}/n\mathbf{Z}) = n$.

*Démonstration.* 1. On a, par définition,

$$\mathbf{Z}/n\mathbf{Z} = \{\overline{a},\ a \in \mathbf{Z}\}.$$

On montre que :

$$\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} = \{\overline{a},\ a \in \mathbf{Z}\}.$$

On a déjà $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} \subset \{\overline{a},\ a \in \mathbf{Z}\}$. On montre alors que

$$\{\overline{a},\ a \in \mathbf{Z}\} \subset \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Soit $a \in \mathbf{Z}$, on fait une division euclidienne de $a$ par $n$. Il existe $q \in \mathbf{Z}$ tel que

$$a = nq + r, \quad 0 \leq r \leq n-1.$$

On a donc :

$$\begin{aligned}\overline{a} = \overline{nq + r} &= \{nq + r + nk,\ k \in \mathbf{Z}\} = \{r + n(q + k),\ k \in \mathbf{Z}\} \\ &= \{r + nk',\ k' \in \mathbf{Z}\} = \overline{r}.\end{aligned}$$

Donc $\overline{a} = \overline{r}$ et $0 \leq r \leq n-1$, d'où le résultat.

2. On va montre que $\operatorname{card}(\mathbf{Z}/n\mathbf{Z}) = n$. Soit $\overline{a}, \overline{b} \in \mathbf{Z}/n\mathbf{Z}$ avec $0 \leq a \leq n-1$ et $0 \leq b \leq n-1$. On montre que $\overline{a} \neq \overline{b}$ par l'absurde en rappelant que :

$$\overline{a} = \{a + nk,\ k \in \mathbf{Z}\} \quad \text{et} \quad \overline{b} = \{b + nk',\ k' \in \mathbf{Z}\}.$$

On suppose que $\overline{a} = \overline{b}$ alors il existe $k \in \mathbf{Z}$ tel que $a + nk \in \overline{b}$. Cela implique qu'il existe $k' \in \mathbf{Z}$ tel que $a + nk = b + n'$. On a donc :

$$a + nk = b + nk' \Rightarrow a - b = n(k' - k) \Rightarrow |a - b| \geq n,$$

c'est-à-dire que la distance entre $a$ et $b$ est supérieur ou égal à $n$. Or, on a supposé que $0 \leq a \leq n - 1$ et $0 \leq b \leq n - 1$. Mais $|a - b| \leq n - 1$, on aboutit donc à une contradiction et donc $\overline{a} \neq \overline{b}$, c'est-à-dire que $\text{card}(\mathbf{Z}/n\mathbf{Z}) = n$.

□

**Exemple I.18.** On se place dans $\mathbf{Z}/5\mathbf{Z}$ :

$$\mathbf{Z}/5\mathbf{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \{\overline{5}, \overline{-4}, \overline{7}, \overline{-2}, \overline{-1}\}.$$

Soit $n \in \mathbf{N}^*$, on va définir des opérations dans $\mathbf{Z}/n\mathbf{Z}$.

**Définition I.19** (Addition dans $\mathbf{Z}/n\mathbf{Z}$)**.** *Soient $\overline{a}, \overline{b} \in \mathbf{Z}/n\mathbf{Z}$. On définit une opération appelée « addition » par :*

$$\overline{a} \oplus \overline{b} = \overline{a + b}.$$

**Exemple I.20.** On se place dans $\mathbf{Z}/6\mathbf{Z}$ :

$$\overline{1} \oplus \overline{7} = \overline{8} = \overline{2},$$
$$\overline{8} \oplus \overline{13} = \overline{21} = \overline{3}.$$

*Démonstration.* On montre que cette opération est bien définie. Soient $a, a', b, b' \in \mathbf{Z}$ tels que :

$$\overline{a} = \overline{a'} \quad \text{et} \quad \overline{b} = \overline{b'}.$$

On montre que $\overline{a + b} = \overline{a' + b'}$. On a $\overline{a} = \overline{a'} \Leftrightarrow a \equiv a' \pmod{n}$ (voir la remarque I.21) et $\overline{b} = \overline{b'} \Leftrightarrow b \equiv b' \pmod{n}$. Donc, d'après la proposition I.8-(i) :

$$a + b \equiv a' + b' \pmod{n} \Leftrightarrow \overline{a + b} = \overline{b' + a'}.$$

□

**Remarque I.21.** Soit $E$ un ensemble non vide et $\mathscr{R}$ la relation d'équivalence dans $E$. Si $x, y \in E$ alors on a :

$$\overline{x} = \overline{y} \Leftrightarrow x \mathscr{R} y.$$

**Définition I.22** (Multiplication dans $\mathbf{Z}/n\mathbf{Z}$)**.** *Soient $\overline{a}, \overline{b} \in \mathbf{Z}/n\mathbf{Z}$. On définit une autre opération appelée « multiplication par $\overline{a} \otimes \overline{b} = \overline{a \cdot b}$.*

*Démonstration.* On vérifie que cette opération a un sens. Soient $a, a', b, b' \in \mathbf{Z}$ tel que $\overline{a} = \overline{a'}$ et $\overline{b'} = \overline{b}$. On a :

$$\overline{a} = \overline{a'} \Leftrightarrow a \equiv a' \pmod{n}, \tag{I.1}$$
$$\overline{b} = \overline{b'} \Leftrightarrow b \equiv b' \pmod{n}. \tag{I.2}$$

Si on multiple (I.1) et (I.2) et en utilisant la proposition I.8-(ii), on obtient :

$$a \cdot b \equiv a' \cdot b' \pmod{n}$$

donc : $\overline{ab} = \overline{a'b'}$. □

On rappelle la définition de structure de groupes.

**Définition I.23** (Groupe)**.** *Soit $G$ un ensemble muni d'une opération (ou d'une loi) noté $*$. On dit que $G$ est un* groupe *ou $(G, *)$ est un groupe si :*

1. *$G$ est* stable *par $*$, c'est-à-dire :*
$$\forall x, y \in G, \quad x * y \in G.$$
2. *L'opération $*$ est* associative *:*
$$\forall x, y, z \in G, \quad (x * y) * z = x * (y * z) = x * y * z.$$
3. *Il existe un unique élément $e \in G$ (qu'on appelle* élément neutre*) tel que pour tout $x \in G$,*
$$x * e = x = e * x.$$
4. *Pour tout $x \in G$, il existe un unique élément $x^{-1} \in G$ (qu'on appelle* élément inversible *de $x$) tel que :*
$$x * x^{-1} = x^{-1} * x = e.$$

*Si, de plus, on a :*

$$\forall x, y \in G, \quad x * y = y * x.$$

*Dans ce cas, on dit que la loi $*$ est commutative et le groupe $G$ est* abélien *(ou* commutatif*).*

**Exemples I.24.** 1. $(\mathbf{N}, -)$ n'est pas un groupe car on a bien $1 \in \mathbf{N}$ et $2 \in \mathbf{N}$ mais

$$1 - 2 \in \mathbf{Z} \notin \mathbf{N}.$$

2. $(\mathbf{Z}, +)$ est un groupe abélien. En effet,
   (1) Pour tout $a, b \in \mathbf{Z}$, $a + b \in \mathbf{Z}$.
   (2) Pour tout $a, b, c \in \mathbf{Z}$, on a : $(a + b) + c = (b + c) + a$.
   (3) Il existe $e \in \mathbf{Z}$ tel que pour tout $a \in \mathbf{Z}$,
   $$a + e = a \Leftrightarrow e = 0.$$
   (4) Soit $a \in \mathbf{Z}$, on a :
   $$a + (-a) = -a + a = 0.$$
   Tout élément de $\mathbf{Z}$ admet un inverse et l'inverse d'un élément $a$ est $-a$.
   De plus, on a : pour tout $a, b \in \mathbf{Z}$, $a + b = b + a$.

3. $(\mathbf{R}, \times)$ n'est pas un groupe car 0 n'admet pas d'inverse pour la multiplication. On suppose que 0 admet un inverse. Il existe donc un élément unique $x \in \mathbf{R}$ tel que $0 \times x = x \times 0 = 1$. Or $0 \times x = 0$, pour tout $x \in \mathbf{R}$ et $0 \neq 1$. D'où on obtient une contradiction.

**Proposition I.25.** *Soit $(G, *)$ un groupe. Alors :*

*(i) il existe un unique élément de $G$ qui vérifie, pour tout $x \in G$,*

$$x * e = e * x = x.$$

*(ii) Soit $x \in G$ alors il existe un unique $x' \in G$ tel que :*

$$x * x' = x' * x = e.$$

*Démonstration.* (i) On suppose qu'il existe $e, e' \in G$ tels que :

$$\forall x \in G, \quad x * e = e * x = x, \tag{I.3}$$
$$\forall x \in G, \quad x * e' = e' * x = x. \tag{I.4}$$

En prenant $x = e'$ dans (I.3), on obtient :

$$e * e' = e' * e = e.$$

et si on prend $x = e$ dans (I.4), on a :

$$e' * e = e * e' = e'.$$

D'où $e = e'$.

(ii) On suppose qu'il existe $x', x'' \in G$ tels que :

$$\exists x \in G, \quad x * x' = x' * x = e, \tag{I.5}$$
$$\exists x \in G, \quad x * x'' = x'' * x = e. \tag{I.6}$$

On obtient donc $x'' * (x * x') = x'' * (x' * x) = x''$. Comme la loi $*$ est associative, on a aussi :

$$(x'' * x) * x' = x'' * (x * x').$$

Or, d'après (I.6), $x'' * x = e$. On en déduit donc que :

$$x'' * (x * x') = e * x' = x'.$$

D'où $x' = x''$.

□

**Proposition I.26.** *Soit $n \in \mathbf{N}^*$. $(\mathbf{Z}/n\mathbf{Z}, \oplus)$ est un groupe commutatif.*

*Démonstration.* On montre que $(\mathbf{Z}/n\mathbf{Z}, \oplus)$ est un groupe.

**Stabilité** L'addition est bien définie sur $\mathbf{Z}/n\mathbf{Z}$ c'est-à-dire si $\overline{a}, \overline{b} \in \mathbf{Z}/n\mathbf{Z}$ alors :

$$\overline{a} \oplus \overline{b} = \overline{a+b} \in \mathbf{Z}/n\mathbf{Z}.$$

**Associativité** Soient $\overline{a}, \overline{b}, \overline{c} \in \mathbf{Z}/n\mathbf{Z}$ alors :

$$(\overline{a} \oplus \overline{b}) \oplus \overline{c} = \overline{a+b} \oplus \overline{c} = \overline{(a+b)+c}.$$

Comme l'addition est associative dans $\mathbf{Z}$, on a :

$$(a+b)+c = a+(b+c).$$

D'où :

$$\overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} \oplus \overline{b+c} = \overline{a} \oplus (\overline{b} \oplus \overline{c}).$$

**Élément neutre** On montre qu'il existe un unique élément $\overline{x} \in \mathbf{Z}/n\mathbf{Z}$ tel que pour tout $a \in \mathbf{Z}/n\mathbf{Z}$, $\overline{a} \oplus \overline{x} = \overline{a}$. On a :

$$\forall \overline{a} \in \mathbf{Z}/n\mathbf{Z}, \quad \overline{a+x} = a,$$

c'est-à-dire, pour $a \in \mathbf{Z}$, on a $a + x \equiv a \pmod{n}$. D'où $\overline{x} = 0$. L'élément neutre est donc $e = \overline{0}$.

**Élément inversible** Soit $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$. On montre qu'il existe $b \in \mathbf{Z}/n\mathbf{Z}$ tel que $\overline{a} \oplus \overline{b} = \overline{0}$. On a :

$$\overline{a} \oplus \overline{b} = 0 \Leftrightarrow \overline{a+b} = 0 \Leftrightarrow a + b \equiv 0 \pmod{n} \Leftrightarrow b \equiv -a \pmod{n} \Leftrightarrow \overline{b} = \overline{-a}.$$

On montre, de plus, que $(\mathbf{Z}/n\mathbf{Z}, \oplus)$ est un groupe abélien. La loi est commutative car si on considère $\overline{a}, \overline{b} \in \mathbf{Z}/n\mathbf{Z}$, on a, par commutativité de la loi + sur $\mathbf{Z}$ :

$$\overline{a} \oplus \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} \oplus \overline{a}.$$

□

**Proposition I.27.** $(\mathbf{Z}/n\mathbf{Z}, \otimes)$ *n'est pas un groupe.*

*Démonstration.* On montre que certaines propriétés sont vérifiés mais il y en aura une qui ne le sera pas.

**Stabilité** La multiplication est bien définie sur $\mathbf{Z}/n\mathbf{Z}$ donc si $\overline{a}, \overline{b} \in \mathbf{Z}/n\mathbf{Z}$ alors $\overline{a} \otimes \overline{b} = \overline{a \cdot b} \in \mathbf{Z}/n\mathbf{Z}$.

**Associativité** Soient $\overline{a}, \overline{b}, \overline{c} \in \mathbf{Z}/n\mathbf{Z}$. On a :

$$(a \otimes b) \otimes c = \overline{a \cdot b} \otimes \overline{c} = \overline{(a \cdot b) \cdot c}.$$

Comme la multiplication est commutative dans $\mathbf{Z}$, on obtient

$$\overline{(a \cdot b) \cdot c} = \overline{a \cdot (b \cdot c)}.$$

D'où :

$$\overline{a \cdot (b \cdot c)} = \overline{a} \otimes \overline{b \cdot c} = \overline{a} \otimes (\overline{b} \otimes \overline{c}).$$

**Commutative** La multiplication dans $\mathbf{Z}/n\mathbf{Z}$ est commutative (on peut le vérifier grâce à la commutativité de la multiplcation dans $\mathbf{Z}$).

**Élément neutre** On suppose $e = \overline{x} \in \mathbf{Z}/n\mathbf{Z}$ vérifiant, pour tout $a \in \mathbf{Z}/n\mathbf{Z}$,

$$\overline{a} \otimes \overline{x} = \overline{a}.$$

On a donc :

$$\overline{ax} = \overline{a} \Leftrightarrow ax \equiv a \pmod{n} \Leftrightarrow a(x-1) \equiv 0 \pmod{n}.$$

En particulier, si on prend $a = 1$, on en déduit que $x \equiv 1 \pmod{n}$. Réciproquement, si $x \equiv 1 \pmod{n}$ alors $ax \equiv a \pmod{n}$, pour tout $a \in \mathbf{Z}$. D'où $\overline{x} = \overline{1}$.

**Élément inversible** Soit $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$. On cherche $\overline{a'} \in \mathbf{Z}/n\mathbf{Z}$ tel que $\overline{a} \otimes \overline{a'} = \overline{1}$. On a :

$$\overline{a} \otimes \overline{a'} = \overline{1} \Leftrightarrow \overline{aa'} = \overline{1} \Leftrightarrow aa' \equiv 1 \pmod{n}.$$

Si on prend $\overline{a} = \overline{0}$, il n'existe pas d'élément $\overline{a'} \in \mathbf{Z}/n\mathbf{Z}$ tel que $\overline{0} \otimes \overline{a'} = \overline{1}$. On a bien, pour tout $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$, $\overline{0} \otimes \overline{a} = \overline{0}$ et $\overline{0} \neq \overline{1}$.

Donc, $(\mathbf{Z}/n\mathbf{Z}, \otimes)$ n'est pas un groupe. □

On considère l'ensemble des éléments inversibles pour la multiplication dans $\mathbf{Z}/n\mathbf{Z}$.

**Définition I.28.** *L'ensemble $\mathbf{Z}/\mathbf{Z}^{-1}n$ est l'ensemble des éléments de $\mathbf{Z}/n\mathbf{Z}$ inversibles pour la multiplication de $\mathbf{Z}/n\mathbf{Z}$.*

**Remarque I.29.** Pour tout $n \in \mathbf{N}^*$, l'élément $\overline{1}$ appartient à $(\mathbf{Z}/n\mathbf{Z})^\times$ car :

$$\overline{1} \times \overline{1} = \overline{1 \times 1} = \overline{1}.$$

Soit un élément $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$, $\overline{a}$ est inversible pour la multiplication si et seulement si

$$\begin{aligned}
\exists \overline{x} \in \mathbf{Z}/n\mathbf{Z},\ \overline{a} \otimes \overline{x} = \overline{1} &\Leftrightarrow \exists \overline{x} \in \mathbf{Z}/n\mathbf{Z},\ \overline{ax} = \overline{1} \\
&\Leftrightarrow \exists \overline{x} \in \mathbf{Z}/n\mathbf{Z},\ ax \equiv 1 \pmod{n} \\
&\Leftrightarrow \exists \overline{x} \in \mathbf{Z}/n\mathbf{Z},\ \exists k \in \mathbf{Z},\ ax = 1 + kn \\
&\Leftrightarrow \exists \overline{x} \in \mathbf{Z}/n\mathbf{Z},\ \exists k \in \mathbf{Z},\ ax - kn = 1.
\end{aligned}$$

Mais, cela ressemble fortement au théorème de Bézout :

**Théorème I.30** (Théorème de Bézout)**.** *Soient $a$ et $b$ des entiers non nuls. Les assertions suivantes sont équivalentes :*

1. $\mathrm{PGCD}(a, b) =$.
2. *Il existe des entiers $u$ et $v$ tels que :*

$$au + bv = 1.$$

*Démonstration.* En exercice ou [4, p. 31] □

Donc, d'après le théorème de Bézout, $\overline{a}$ est inversible pour la multiplication si et seulement $\mathrm{PGCD}(a,n)=1$. On a donc une autre définition de $(\mathbf{Z}/n\mathbf{Z})^\times$.

**Définition I.31** ($(\mathbf{Z}/n\mathbf{Z})^\times$)**.** *L'ensemble* $(\mathbf{Z}/n\mathbf{Z})^\times$ *est l'ensemble des éléments* $\overline{a}\in\mathbf{Z}/n\mathbf{Z}$ *tels que* $\mathrm{PGCD}(a,n)=1$*, c'est-à-dire :*

$$(\mathbf{Z}/n\mathbf{Z})^\times=\{\overline{a}\in\mathbf{Z}/n\mathbf{Z},\ \mathrm{PGCD}(a,n)=1\}\,.$$

**Exemples I.32.** 1. $(\mathbf{Z}/6\mathbf{Z})^\times=\{\overline{1},\overline{5}\}$.

2. $(\mathbf{Z}/5\mathbf{Z})^\times=\{\overline{1},\overline{2},\overline{3},\overline{4}\}$.

**Proposition I.33.** *Soit* $n\in\mathbf{N}^*$*.* $((\mathbf{Z}/n\mathbf{Z})^\times,\otimes)$ *est un groupe abélien.*

On montre la stabilité de la loi $\otimes$ par deux façons. Les autres propriétés sont évidentes (en partie parce que $(\mathbf{Z}/n\mathbf{Z})^\times\subset\mathbf{Z}/n\mathbf{Z}$).

*Démonstration de la stabilité de la loi, première méthode.* Soient $\overline{a},\overline{b}\in(\mathbf{Z}/n\mathbf{Z})^\times$.

On montre que

$$\overline{a}\otimes\overline{b}\in(\mathbf{Z}/n\mathbf{Z})^\times,\quad \text{c'est-à-dire } \overline{a\cdot b}\in(\mathbf{Z}/n\mathbf{Z})^\times.$$

Comme $\overline{a},\overline{b}\in(\mathbf{Z}/n\mathbf{Z})^\times$, on a $\mathrm{PGCD}(a,b)=\mathrm{PGCD}(b,n)=1$. On montre que

$$\mathrm{PGCD}(ab,n)=1.$$

On a :

$$\mathrm{PGCD}(a,n)=1\Leftrightarrow\exists u,v\in\mathbf{Z},\quad au+nv=1, \tag{I.7}$$
$$\mathrm{PGCD}(b,n)=1\Leftrightarrow\exists \alpha,\beta\in\mathbf{Z},\quad b\alpha+n\beta=1. \tag{I.8}$$

En faisant la multiplication de (I.7) et (I.8), on obtient :

$$ab(u\alpha)+n(au\beta+bv\alpha+vn\beta)=1.$$

Si on pose $X=u\alpha\in\mathbf{Z}$ et $Y=au\beta+bv\alpha+vn\beta\in\mathbf{Z}$, on a :

$$abX+nY=1.$$

Donc, d'après le théorème de Bézout, $\mathrm{PGCD}(ab,n)=1$. □

Avant de démontrer de la stabilité de la loi par une seconde méthode, on a besoin du théorème de Gauss.

**Théorème I.34** (Théorème de Gauss)**.** *Soient* $a$ *et* $b$ *des entiers et soit* $p$ *un nombre premier. Si* $p\mid ab$ *alors* $p\mid a$ *ou* $p\mid b$*.*

*Démonstration de la stabilité de la loi, seconde méthode.* Soient $\overline{a}, \overline{b} \in (\mathbf{Z}/n\mathbf{Z})^\times$.

On montre que

$$\overline{a} \otimes \overline{b} \in (\mathbf{Z}/n\mathbf{Z})^\times, \quad \text{c'est-à-dire } \overline{a \cdot b} \in (\mathbf{Z}/n\mathbf{Z})^\times.$$

On pose $d = \mathrm{PGCD}(ab, n)$ et on suppose que $d \geq 2$. Donc il existe un nombre premier tels que $p \mid d$ donc il existe $k \in \mathbf{Z}$ tel que $p = dk$. On a, d'une part, $d \mid ab$ et $n \mid$ et, d'autre part, $p \mid d$. D'où $p \mid ab$ et $p \mid n$. Comme $p$ est premier et $p \mid ab$ alors $p \mid a$ ou $p \mid b$. Supposons que $p \mid a$. Comme $p \mid n$, $\mathrm{PGCD}(a, n) \geq p$, ce qui est absurde car $\mathrm{PGCD}(a, n) = 1$. Supposons que $p \mid d$. Comme $p \mid n$, $\mathrm{PGCD}(b, n) \geq p$. Ce qui est absurde car $\mathrm{PGCD}(b, n) = 1$. □

Soit $n \in \mathbf{N}^*$. On s'intéresse maintenant au nombre d'éléments de $(\mathbf{Z}/n\mathbf{Z})^\times$.

**Définition I.35** (Fonction d'Euler)**.** *Soit $n \geq 1$ un entier. On appelle la* fonction d'Euler *de $n$ (qu'on note $\varphi(n)$) le nombre d'entiers $a$ tels que $1 \leq a \leq n$ et $\mathrm{PGCD}(a, n) = 1$.*

D'après la définition I.31, le nombre d'éléments dans $(\mathbf{Z}/n\mathbf{Z})^\times$ est le nombre d'entiers $a$ tels que $1 \leq a \leq n$ et $\mathrm{PGCD}(a, n) = 1$, c'est-à-dire, d'après la définition I.35, $\varphi(n)$. D'où :

**Définition I.36** (Nombre d'éléments dans $(\mathbf{Z}/n\mathbf{Z})^\times$)**.** *Soit $n \in \mathbf{N}^*$. Le* nombre d'éléments *dans $(\mathbf{Z}/n\mathbf{Z})^\times$ est :*

$$\mathrm{card}((\mathbf{Z}/n\mathbf{Z})^\times) = \mathrm{card}(\{a \in \mathbf{N}^*,\ 1 \leq a \leq n \text{ et } \mathrm{PGCD}(a, n) = 1\}) = \varphi(n).$$

**Exemple I.37.** $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$.

**Proposition I.38.** *Si $p$ est un nombre premier alors $\varphi(p) = p - 1$.*

*Démonstration.* Un nombre premier est premier avec tous les nombres *strictement* inférieurs à lui-même. D'où le résultat. □

**Proposition I.39.** *Soit $p$ un nombre premier et $\alpha \geq 1$ un entier. Alors :*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

*Démonstration.* On a :

$$\varphi(p^\alpha) = \mathrm{card}(\{a \in \mathbf{N}^*\}\, \mathrm{PGCD}(a, p^\alpha = 1).$$

Mais, puisque $p$ est un nombre premier, $\mathrm{PGCD}(a, p^\alpha) \neq 1$ si et seulement si $p \mid a$. Donc :

$$\begin{aligned}\varphi(p^\alpha) &= \mathrm{card}(\{a \in \mathbf{N}^*,\ 1 \leq a \leq p^\alpha\}) - \mathrm{card}(\{a \in \mathbf{N}^*,\ 1 \leq a \leq p^\alpha,\ p \mid a\}) \\ &= p^\alpha - \mathrm{card}(\{a \in \mathbf{N}^*,\ 1 \leq a \leq p^\alpha,\ p \mid a\}).\end{aligned}$$

Mais

$$\begin{aligned}\mathrm{card}(\{a \in \mathbf{N}^*,\ 1 \leq a \leq p^\alpha,\ p \mid a\}) &= \mathrm{card}(\{k \in \mathbf{N}^*,\ 1 \leq pk \leq p^\alpha\}) \\ &= \mathrm{card}(\left\{k \in \mathbf{N}^*,\ 1/p \leq k \leq p^{\alpha-1}\right\}) \\ &= \mathrm{card}(\left\{k \in \mathbf{N}^*,\ 1 \leq k \leq p^{\alpha-1}\right\}) = p^{\alpha-1}.\end{aligned}$$

D'où :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

□

**Théorème I.40.** *Soient $a, b \in \mathbf{N}^*$ tels que* $\mathrm{PGCD}(a,b) = 1$*, alors :*

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

**Exemple I.41.** On a : $100 = 4 \times 25$ et $\mathrm{PGCD}(25, 4) = 1$. D'où :

$$\begin{aligned}\varphi(100) &= \varphi(4 \times 25) = \varphi(4) \cdot \varphi(25) \\ &= \varphi(2^2) \cdot \varphi(5^2) = (4-2) \cdot (25-5) = 2 \times 20 = 40.\end{aligned}$$

**Définition I.42** (Ordre du groupe)**.** *Soit $G$ un groupe. On appelle* ordre du groupe *(et on note* $\mathrm{ord}(G)$*), son nombre d'éléments.*

**Remarque I.43.** Compte tenu qu'un groupe est aussi un ensemble, l'ordre d'un groupe $G$ est aussi le cardinal de cet ensemble $G$. Mais, dans toute la suite de cette section, on utilisera la notation ord plus adaptée à un groupe.

**Exemple I.44.** On cherche l'ordre de $(\mathbf{Z}/7700\mathbf{Z})^\times$. Avant de faire les calculs, on remarque que $7700 = 77 \times 100$ et comme $\mathrm{PGCD}(77, 100) = 1$, on obtient :

$$\begin{aligned}\mathrm{ord}((\mathbf{Z}/7700\mathbf{Z})^\times) &= \varphi(7700) = \varphi(77 \times 100) = \varphi(77) \cdot \varphi(100) \\ &= \varphi(7 \times 11) \cdot \varphi(10^2) \overset{\mathrm{PGCD}(7,11)=1}{=} \varphi(7) \cdot \varphi(11) \cdot 40 \\ &= 6 \times 10 \times 11 = 400 \times 6 = 1400.\end{aligned}$$

**Théorème I.45** (Théorème de Wilson)**.** *Soit $p$ un nombre premier. Alors :*

$$(p-1)! \equiv -1 \pmod{p}.$$

*Démonstration.* On a vu que $(\mathbf{Z}/p\mathbf{Z})^\times = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$. On montre alors que $(p-1)! \equiv -1 \pmod{p}$. Ceci revient à montrer que :

$$1 \times 2 \times \cdots \times (p-1) \equiv -1 \pmod{p}$$

ou aussi :

$$\overline{1} \otimes \overline{2} \otimes \cdots \otimes \overline{p-1} = \overline{-1}.$$

Dans le produit, en regroupant chaque $\overline{x}$ avec sa classe inverse pour la multiplication (c'est-à-dire la classe $\overline{x'}$ tel que $\overline{x} \otimes \overline{x'} = \overline{1}$), on obtient le produit des classes qui sont égales à leur classe inverse. Le problème revient, donc, à chercher les classes de $\overline{x} \in (\mathbf{Z}/p\mathbf{Z})^\times$ qui vérifie $\overline{x} \otimes \overline{x} = \overline{1}$. On a :

$$\begin{aligned}\overline{x^2} = 1 &\Leftrightarrow x^2 \equiv 1 \pmod{p} \Leftrightarrow x^2 - 1 \equiv 0 \pmod{p} \\ &\Leftrightarrow (x-1)(x+1) \equiv 0 \pmod{p} \Leftrightarrow p \mid (x-1)(x+1).\end{aligned}$$

Comme $p$ est premier, on a $p \mid x+1$ ou $p \mid x-1$, c'est-à-dire $x \equiv 1 \pmod{p}$ ou $x \equiv -1 \pmod{p}$. D'où $\overline{x} = \overline{1}$ ou $\overline{x} = \overline{-1}$ et :

$$\overline{1} \otimes \overline{2} \otimes \cdots \otimes \overline{p-1} = \overline{1} \otimes \overline{-1} = \overline{1 \times -1} = \overline{-1}.$$

□

## I.2 Petit théorème de Fermat

**Théorème I.46** (Théorème de Fermat, première version)**.** *Soit $p$ un nombre premier et $a \in \mathbf{Z}$ tels que $p$ ne divise pas $a$. Alors :*

$$a^p \equiv a \pmod{p}.$$

**Exemple I.47.** Le petit théorème de Fermat permet d'établir que

1. $\left(10^{10^{10}}\right)^7 \equiv 10^{10^{10}} \pmod 7$,
2. $15^{29} \equiv 15 \pmod{29}$.

Par contre, $2^4 = 16 \equiv 0 \pmod 4$ et non congru à 2 modulo 4.

Avant de démontrer la première version du petit théorème de Fermat, on va montrer le lemme suivant :

**Lemme I.48.** *Soit $p$ un nombre premier. Alors, pour tout $1 \leq k \leq p-1$, on a :*

$$\mathrm{C}_p^k \equiv 0 \pmod{p}.$$

*Démonstration du lemme I.48.* Déjà on a $\mathrm{C}_p^k \in \mathbf{N}$ et :

$$\mathrm{C}_p^k = \frac{p!}{k!(p-k)!} = \frac{(p-k+1)\cdot(p-k+2)\cdots p}{k!}.$$

On a :

$$k!\mathrm{C}_p^k = p\left(\frac{(p-k)(p-k+1)\cdot(p-1)}{k!}\right),$$

c'est-à-dire $p \mid k!\mathrm{C}_p^k$. D'où le résultat ! □

*Preuve de la première version du petit théorème de Fermat.* On montre que, pour tout $a \in \mathbf{N}$ et $p$ fixé, $a^p \equiv a \pmod p$. On fait une démonstration par récurrence sur $a$.

**Initialisation** Pour $a = 0$, on a :

$$0^p \equiv 0 \pmod{p}.$$

**Hérédité** On suppose que $a^p \equiv a \pmod p$ pour un certain $a$ dans $\mathbf{N}$. On démontre que la proprété est vraie à l'ordre suivant. On a, par le binôme de Newton,

$$(a+1)^p = a^p + \mathrm{C}_p^1 a^{p-1} + \cdots + 1.$$

Compte tenu du lemme I.48,

$$(a^p + 1) \equiv a^p + 1 \pmod{p}.$$

On dmontre que $\mathrm{PGCD}(p, k!) = 1$ pour $1 \leq k \leq p-1$. D'après le lemme de Gauss, $p \mid \mathrm{C}_p^k$. Comme $p$ est premier, pour tout $1 \leq n \leq p-1$, $\mathrm{PGCD}(p, n) = 1$. Donc, $\mathrm{PGCD}(p, k!) = 1$, pour tout $1 \leq k \leq p-1$. D'où

$$(a+1)^p \equiv a^p + 1 \pmod{p}.$$

D'où, pour tout $a \in \mathbf{N}$, $a^p \equiv a \pmod{p}$. Mais il faut montrer la propriété pour $a \leq -1$. On a : $-a \geq 1$. On suppose, pour l'instant $p > 2$ (donc $p$ est impair). On a $(-a)^p = (-1)^p a^p = -(a^p)$. D'où, d'après le premier cas,

$$-a^p \equiv -a \pmod{p} \Rightarrow a^p \equiv a \pmod{p}.$$

On suppose maintenant $p = 2$, $a^2 \equiv a \pmod{2}$. Si $a$ est pair alors $a^2$ est pair et si $a$ est impair alors $a^2$ est impair. D'où : $a^2 \equiv a \pmod{2}$. □

**Théorème I.49** (Théorème de Fermat, seconde version)**.** *Soient $p$ un nombre premier et $a \in \mathbf{Z}$ tels que $p$ ne divise pas $a$. Alors :*

$$a^{p-1} \equiv 1 \pmod{p}.$$

On peut remarquer que le théorème I.46 est équivalent au théorème I.49. Avant de démontrer la seconde version du petit théorème de Fermat, on a besoin du lemme suivant :

**Lemme I.50.** *Soient $p$ un nombre premier et $a$ un entier. Si $p \nmid a$ alors* $\mathrm{PGCD}(p, a) = 1$.

*Démonstration du lemme I.50.* Comme $p$ est un nombre premier, le plus grand commun diviseur de $a$ et de $p$ est soit 1 ou $p$ mais comme $p$ ne divise pas $a$, on a bien $\mathrm{PGCD}(a, p) = 1$. □

*Preuve de la seconde version du petit théorème de Fermat.* D'après la première version du petit théorème de Fermat,

$$a^p \equiv a \pmod{p} \Leftrightarrow a(a^{p-1} - 1) \equiv 0 \pmod{p},$$

ainsi $p \mid a^{p-1} - 1$. Comme $p$ ne divise pas $a$, $\mathrm{PGCD}(a, p) = 1$ d'après le lemme I.50. Donc, d'après le lemme de Gauss, $p \mid a^{p-1} - 1$. Ainsi,

$$a^{p-1} - 1 \equiv 0 \pmod{p} \Leftrightarrow a^{p-1} \equiv p \pmod{0}.$$

□

**Exemple I.51.** 7 est un nombre premier et 7 ne divise pas $10^{10^{10}}$ puisque $10^{10^{10}}$ s'écrit sous la forme $2^\alpha \cdot 5^\beta$ avec $\alpha, \beta \in \mathbf{N}^*$. Donc, d'après la seconde version du petit théorème de Fermat, $\left(10^{10^{10}}\right)^6 \equiv 1 \pmod{7}$.

**Lemme I.52.** *Soit $(G, *)$ un groupe d'ordre $n$, on note $e$ l'élément neutre de $G$. Alors, pour tout $x \in G$,*

$$\underbrace{x * x * \cdots * x}_{n \text{ fois}} = e.$$

On propose maintenant une démonstration de la seconde version du petit théorème de Fermat en passant par le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$.

*Autre preuve de la seconde version du petit théorème de Fermat.* On doit montrer que

$$a^{p-1} \equiv 1 \pmod{p}.$$

Comme $\mathrm{PGCD}(a,p) = 1$, $\overline{a} \in \mathbf{Z}/p\mathbf{Z}$. Le problème revient à montrer que $\overline{a^{p-1}} = \overline{1}$, c'est-à-dire :

$$\underbrace{\overline{a} \otimes \overline{a} \otimes \cdots \otimes \overline{a}}_{p-1 \text{ fois}} = \overline{1}.$$

On considère le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$, comme il est d'ordre $p-1$, on peut poser :

$$(\mathbf{Z}/p\mathbf{Z})^\times = \left\{\overline{x_1}, \overline{x_2}, \ldots, \overline{x_{p-1}}\right\}.$$

Soit $a \in \mathbf{Z}$ tel que $\mathrm{PGCD}(a,p) = 1$. On montre que :

$$(\mathbf{Z}/p\mathbf{Z})^\times = \left\{\overline{a \cdot x_1}, \overline{a \cdot x_2}, \cdots, \overline{a \cdot x_{p-1}}\right\}.$$

On a $\mathrm{PGCD}(p, x_i) = 1$, pour tout $1 \leq i \leq p-1$ et $\mathrm{PGCD}(p,a) = 1$, ainsi $\mathrm{PGCD}(p, a \cdot x_i) = 1$. On montre, par l'absurde, que pour $1 \leq i < j \leq p-1$, on obtient $\overline{a \cdot x_i} \neq \overline{a \cdot x_j}$. On suppose donc que $\overline{ax_i} = \overline{ax_j}$, c'est-à-dire :

$$a \cdot x_i \equiv a \cdot x_j \pmod{p} \Leftrightarrow a(x_i - x_j) \equiv 0 \pmod{p} \Leftrightarrow p \mid a(x_i - x_j).$$

Comm $\mathrm{PGCD}(p,a) = 1$, d'après le lemme de Gauss, $p \mid x_i - x_j$ donc $x_i \equiv x_j \pmod{p}$, ce qui est absurde puisque $\overline{x_i} \neq \overline{x_j}$ pour tout $i \neq j$. Par conséquent, on a :

$$(\mathbf{Z}/p\mathbf{Z})^\times = \left\{\overline{x_1}, \ldots, \overline{x_{p-1}}\right\} = \left\{\overline{a \cdot x_1}, \ldots, \overline{a \cdot x_{p-1}}\right\}.$$

Donc :

$$\overline{x_1} \otimes \cdots \otimes \overline{x_{p-1}} = \overline{a \cdot x_1} \otimes \cdots \otimes \overline{a \cdot x_{p-1}} \Leftrightarrow \overline{x_1 \cdot \cdots \cdot x_{p-1}} = \overline{a^{p-1}} \otimes \overline{x_1 \cdot \cdots \cdot x_{p-1}}. \tag{I.9}$$

Comme $\overline{x_1 \cdot x_2 \cdot \cdots \cdot x_{p-1}}$ est inversible pour la multiplication, en multipliant par son inverse, les deux membres de l'égalité (I.9), on obtient :

$$\overline{a^{p-1}} = \overline{1} \Leftrightarrow a^{p-1} \equiv 1 \pmod{p}.$$

□

On va maintenant étudier une généralisation du petit théorème de Fermat.

**Théorème I.53** (Théorème d'Euler)**.** *Soient $m$ et $n$ deux entiers tels que* $\mathrm{PGCD}(m,n) = 1$. *Alors,*

$$m^{\varphi(n)} \equiv 1 \pmod{n}$$

*où $\varphi(n)$ est la fonction indicatrice d'Euler pour la valeur $n$.*

*Démonstration.* On considère le groupe $(\mathbf{Z}/m\mathbf{Z})^\times$. L'ordre de ce groupe est $\varphi(m)$. Donc, on peut poser :

$$(\mathbf{Z}/m\mathbf{Z})^\times = \left\{\overline{x_1}, \ldots, \overline{x_{\varphi(m)}}\right\}.$$

Soit $n \in \mathbf{Z}$ tel que $\mathrm{PGCD}(n, m)$. On peut démontrer, par l'absurde, que :

$$(\mathbf{Z}/m\mathbf{Z})^\times = \left\{\overline{n \cdot x_1}, \ldots, \overline{n \cdot x_{\varphi(m)}}\right\}.$$

Donc, on obtient :

$$\overline{x_1 \cdot x_2 \cdot \cdots \cdot x_{\varphi(m)}} = \overline{n \cdot x_1 \cdot n \cdot x_2 \cdot \cdots n \cdot x_{\varphi(m)}} \Leftrightarrow \overline{x_1 \cdot x_2 \cdot x_{\varphi(m)}} = \overline{n^{\varphi(m)}} \otimes \overline{x_1 \cdot \cdots \cdot x_{\varphi(m)}}.$$

En multipliant par l'inverse de $\overline{x_1 \cdot x_2 \cdot \cdots \cdot x_{\varphi(m)}}$, on obtient : $\overline{n^{\varphi(m)}} = \overline{1}$. □

Il y a une autre démonstration en utilisant le lemme I.52.

*Autre démonstration du théorème I.53.* On prend $G = (\mathbf{Z}/m\mathbf{Z})^\times$. L'ordre de $G$ est $\varphi(m)$. Soit $\overline{n} \in (\mathbf{Z}/m\mathbf{Z})^\times$ tel que $n \in \mathbf{Z}$ et $\mathrm{PGCD}(n, m) = 1$. D'après le lemme I.50 :

$$\underbrace{\overline{n} \otimes \overline{n} \otimes \cdots \otimes \overline{n}}_{\varphi(m) \text{ fois}} = \overline{1},$$

c'est-à-dire $\overline{n^{\varphi(m)}} = \overline{1}$. □

## I.3 Résolution de congruences

**Proposition I.54.** *Soient $a, b$ deux entiers tels que $\mathrm{PGCD}(a, b) = 1$ et $n \in \mathbf{Z}$. Si $n \equiv 0 \pmod{ab}$ alors $n \equiv 0 \pmod{a}$ et $n \equiv 0 \pmod{b}$.*

**Définition I.55** (Équation diophantienne)**.** *Une* équation diophantienne *linéaire à deux variables est une équation du type*

$$ax + by = c \qquad (E)$$

*où $a, b$ et $c$ sont des entiers donnés et $x$ et $y$ sont des inconnus entières.*

**Théorème I.56.** *On pose $d = \mathrm{PGCD}(a, b)$. L'équation (E) admet des solutions si et seulement si $d \mid c$. Si $d \mid c$ alors les solutions de (E) s'écrivent :*

$$\begin{cases} x = x_0 + \frac{b}{d} \cdot k \\ y = y_0 + \frac{a}{d} \cdot k \end{cases}, \quad k \in \mathbf{Z}.$$

*où $(x_0, y_0)$ est une solution de (E).*

Pour trouver une solution particulière $(x_0, y_0)$, on cherche deux entiers $u$ et $v$ tels que $au + bv = d$. En posant $c = c' \cdot \mathrm{PGCD}(a, b)$, on a alors :

$$a(uc') + b(vc') = c' \cdot \mathrm{PGCD}(a, b) = c.$$

**Définition I.57** (Équation de congruences)**.** *Soient $n \geq 1$, $a$ et $b$ des entiers. Une* équation de congruences *est une équation du type :*

$$ax \equiv b \pmod{n}. \tag{I.10}$$

*avec $x$ une inconnue entière.*

On a :

$$ax \equiv b \pmod{n} \Rightarrow ax = b - nk \Rightarrow ax - nk = b \text{ avec } k \in \mathbf{Z}.$$

Les solutions sont donc donnés à un multiple de $n$ près.

**Théorème I.58.** *Soient $n \geq 1$, $a$ et $b$ des entiers. On pose $d = \mathrm{PGCD}(a, n)$ et on considère l'équation* (I.10)*. Alors :*

*(i)* (I.10) *admet des solutions si et seulement si $d \mid b$.*

*(ii) Si $d \mid p$ alors* (I.10) *admet $d$ solutions modulo $n$.*

*Démonstration.* (i) On suppose que (I.10) admet une solution, c'est-à-dire :

$$\exists x \in \mathbf{Z},\ ax \equiv b \pmod{n} \Leftrightarrow \exists x \in \mathbf{Z},\ \exists k \in \mathbf{Z},\ ax = b + nk \tag{I.11}$$
$$\Leftrightarrow \exists x \in \mathbf{Z},\ \exists k \in \mathbf{Z},\ ax - nk = b. \tag{I.12}$$

(I.12) est une équation diophantienne donc :

$$\exists x \in \mathbf{Z},\ \exists k \in \mathbf{Z},\ ax - nk = b \Leftrightarrow d \mid b,$$

où $d = \mathrm{PGCD}(a, n)$.

(ii) On suppose que $d \mid p$. D'après le théorème I.56, les solutions de (I.11) s'écrivent :

$$\begin{cases} x = x_0 + \frac{n}{d} \cdot t \\ k = k_0 + \frac{n}{d} \cdot t \end{cases}, \quad t \in \mathbf{Z},$$

où $(x_0, k_0)$ est une solution de (I.11). Les solutions de (I.10) s'écrivent donc :

$$x = x_0 + \frac{n}{d} \cdot t, \quad t \in \mathbf{Z}$$

où $x_0$ est une solution de (I.10). On montre que (I.10) admet $d$ solutions modulo $n$. Pour cela, on fait une division euclidienne de $t$ par $d$ :

$$t = dq + r, \quad 0 \leq r \leq d - 1.$$

D'où :

$$x = x_0 + \frac{n}{d} \cdot (dq + r) \Rightarrow x = x_0 + \frac{n}{d} r + nq \Rightarrow x \equiv x_0 + \frac{n}{d} \cdot r \pmod{n}.$$

□

**Théorème I.59** (Théorème chinois)**.** *Soient $n_1, \dots, n_k$ des éléments de $\mathbf{N}^*$ premiers entre eux deux à deux et $a_1, \dots, a_k$ des entiers. On note $p = \prod_{i=1}^{k} n_i$. Alors le système d'équations :*

$$\begin{cases} x \equiv a_1 \pmod{n_1}, \\ x \equiv a_2 \pmod{n_2}, \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases} \tag{I.13}$$

*admet une unique solution modulo $p$.*

Avant de démontrer l'unicité de la solution, on montre ce lemme :

**Lemme I.60.** *Soient $a, b$ et $c$ des entiers tels que $a \mid b$ et $c \mid b$. Alors* $\mathrm{PPCM}(a, c) \mid b$.

*Démonstration du lemme I.60.* Si $a \mid b$ et $c \mid b$ alors il existe $k, k' \in \mathbf{Z}$ tels que

$$b = ak = ck'. \tag{I.14}$$

On pose $d = \mathrm{PGCD}(a, c)$, $a = da'$ et $c' = dc'$ avec $\mathrm{PGCD}(a', c') = 1$. Alors :

$$(\text{I.14}) \Leftrightarrow da'k = db'k \Leftrightarrow a'k = c'k \Leftrightarrow a' \mid c'k'.$$

Comme $\mathrm{PGCD}(a', c') = 1$ alors $a' \mid k'$. Donc, il existe $k'' \in \mathbf{Z}$ tel que $k' = a'k''$ et $b = ck' = ca'k'' = \pm\,\mathrm{PPCM}(a, c)k''$. D'où le résultat. □

*Unicité de la solution de l'équation* (I.13). On suppose qu'on a :

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases} \quad \text{et} \quad \begin{cases} y \equiv a_1 \pmod{n_1} \\ \quad \vdots \\ y \equiv a_k \pmod{n_k} \end{cases},$$

on peut montrer alors que :

$$\begin{cases} x \equiv y \pmod{n_1} \\ \quad \vdots \\ x \equiv y \pmod{n_k} \end{cases},$$

d'où :

$$\begin{cases} n_1 \mid x - y \\ n_2 \mid x - y \\ \quad \vdots \\ n_k \mid x - y \end{cases}.$$

D'après le lemme I.60, $\mathrm{PPCM}(n_1, n_2, \dots, n_k) \mid x - y$. Or les $n_i$ sont premiers entreux deux à deux donc,

$$\mathrm{PPCM}(n_1, \dots, n_k) = n_1 \cdot n_2 \cdot \dots \cdot n_k,$$

d'où $n_1 n_2 \cdots n_k \mid x - y$, c'est-à-dire :

$$x \equiv y \pmod{n_1 n_2 \cdots n_k}.$$

□

Pour montrer l'existence des solutions, on décompose notre démarche en trois cas :

*Cas d'un système à deux équations.* **Première façon** On pose $x = a_1 + nk = a_2 + nk$. Cette équation est équivalente à :

$$n_1 k - n_2 k' = a_2 - a_1.$$

Comme $\mathrm{PGCD}(n_1, n_2) = 1$ et $1 \mid a_2 - a_1$, l'équation (I.13) admet des solutions et ces solutions s'écrivent

$$\begin{cases} k = k_0 + n_2 t \\ k = k'_0 + n_1 t \end{cases}, \quad t \in \mathbf{Z}$$

avec $k_0$ et $k'_0$ des solutions de (I.13). Par conséquent :

$$\begin{aligned} x = a_1 n_1 (k_0 + n_2 t) &\Rightarrow x = a_1 + a_1 k_0 + n_1 n_2 t \\ &\Rightarrow x \equiv a_1 \pmod{n_1 k_0) n_1 n_2}. \end{aligned}$$

**Seconde méthode** On pose $x = x_1 n_1 + x_2 n_2$, où :

$$x_1 n_2 \equiv a_1 \pmod{n_1}, \tag{I.15}$$
$$x_2 n_1 \equiv a_2 \pmod{n_2}. \tag{I.16}$$

Or, $\mathrm{PGCD}(n_2, n_1) = 1$ et 1 divise $a_1$ et $a_2$. Donc $x_1$ et $x_2$ existent, (I.15) et (I.16) admettent des solutions puisque $\mathrm{PGCD}(n_1, n_2) = 1$.

□

*Cas d'un système à trois équations.* Soit à résoudre :

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ x \equiv a_3 \pmod{n_3} \end{cases} \tag{I.17}$$

Le système (I.17) a pour solution

$$x = x_1 n_2 n_3 + x_2 n_1 n_3 + x_3 n_1 n_2$$

où

$$\begin{cases} x_1 n_2 n_3 \equiv a_1 \pmod{n_1} \\ x_2 n_1 n_3 \equiv a_2 \pmod{n_2} \\ x_3 n_2 n_1 \equiv a_3 \pmod{n_3} \end{cases}.$$

□

*Cas général.* Soit à résoudre :

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad \vdots x \equiv a_k \pmod{n_k} \end{cases} \tag{I.18}$$

On pose $n = n_1 n_2 \cdots n_k$. Le système (I.19) a pour solution

$$x = \frac{n}{n_1} x_1 + \frac{n}{n_2} x_2 + \cdots + \frac{n}{n_k} a_k$$

où

$$\begin{cases} \frac{n}{n_1} x_1 \equiv a_1 \pmod{n_1} \\ \frac{n}{n_2} x_2 \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ \frac{n}{n_k} x_k \equiv a_k \pmod{n_k}. \end{cases} .$$

□

**Exemple I.61.** Soit à résoudre le système :

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 20 \pmod 4 \\ x \equiv 27 \pmod 5 \end{cases} \tag{I.19}$$

qui est équivalent au système :

$$\begin{cases} x \equiv -1 \pmod 3 \\ x \equiv 0 \pmod 4 \\ x \equiv 2 \pmod 5 \end{cases}$$

Le système (I.19) est un système chinois puisque $3, 4$ et $5$ sont premiers entre eux. Elle admet une unique solution modulo 60. Pour trouver la solution, on pose

$$x = 20x_1 + 15x_2 + 12x_3$$

où

$$\begin{cases} 4 \times 5 \times x_1 \equiv -1 \pmod 3 \\ 3 \times 5 \times x_2 \equiv 0 \pmod 4 \\ 3 \times 4 \times x_3 \equiv 2 \pmod 3 \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 1 \pmod 3 \\ x_2 \equiv 0 \pmod 4 \\ x_3 \equiv 1 \pmod 5 \end{cases} \Leftrightarrow \begin{cases} x_1 = 1 \\ x_2 = 0 \\ x_3 = 1 \end{cases} .$$

D'où :

$$x = 5 \times 4 \times 1 + 3 \times 5 \times 0 + 3 \times 4 \times 1 = 20 + 12 \equiv 32 \pmod{60}.$$

**Exercice I.62** (Problème du panier à œufs)**.** Trouver le plus petit nombre d'oeufs, sachant que lorsqu'on retire à chaque fois les œufs par $2, 3, 4, 5$, ou $6$, un œuf reeste dans le panier et lorsqu'on retire les œufs par $7$, aucun œuf ne reste.

**Proposition I.63.** *Soient $m$ et $n$ deux entiers $\geq 1$ tels que* $\mathrm{PGCD}(m,n) = 1$. *Alors :*

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

*Démonstration.* Soit $a \in \mathbf{Z}$, on note $[a]_n$ la classe de $a$ modulo $n$. On considère l'application :

$$\begin{array}{rccc} f & : & (\mathbf{Z}/mn\mathbf{Z})^\times & \to & (\mathbf{Z}/m\mathbf{Z})^\times \times (\mathbf{Z}/n\mathbf{Z})^\times \\ & & [a]_{mn} & \mapsto & ([a]_m, [a]_n) \end{array}.$$

Cette application est bien définie, en effet, si $[a]_{mn} \in (\mathbf{Z}/mn\mathbf{Z})^\times$ alors $\mathrm{PGCD}(a, mn) = 1$. Donc $\mathrm{PGCD}(a,n) = 1$ et $\mathrm{PGCD}(a,m) = 1$. Par conséquent,

$$[a]_m \in (\mathbf{Z}/m\mathbf{Z})^\times \quad \text{et} \quad [a]_n \in (\mathbf{Z}/n\mathbf{Z})^\times.$$

On montre que $f$ est bijective. Soit $([\alpha]_m, [\beta]_n) \in (\mathbf{Z}/n\mathbf{Z})^\times \times (\mathbf{Z}/m\mathbf{Z})^\times$. On montre qu'il existe une unique classe $[a]_{mn}$ telle que

$$f([a]_{mn}) = ([\alpha]_n, [\beta]_m \Leftrightarrow ([a]_n, [a]_m) = ([\alpha]_n, [\beta]_m.$$

Ceci est équivalent à résoudre le système suivant :

$$\begin{cases} [a]_n = [\alpha]_n \\ [a]_m = [\beta]_m \end{cases} \Leftrightarrow \begin{cases} a \equiv \alpha \pmod{n} \\ a \equiv \beta \pmod{m} \end{cases} \qquad (\mathscr{S})$$

($P$) est un système chinois donc il existe un unique $a$ modulo $mn$ qui vérifie ($P$). Donc, il existe une unique $[a]_{mn}$ tel que $f([a]_{mn}) = ([\alpha]_n, [\beta]_m)$, c'est-à-dire $f$ est bijective. Par conséquent :

$$\mathrm{card}((\mathbf{Z}/mn\mathbf{Z})^\times) = \mathrm{card}((\mathbf{Z}/n\mathbf{Z})^\times) \times \mathrm{card}((\mathbf{Z}/m\mathbf{Z})^\times) \Rightarrow \varphi(mn) = \varphi(m)\varphi(n).$$

□

## I.4 Applications

### 1 Codage des messages secrets

La méthode de codage qu'on va étudier a été découverte en 1976, elle est basée sur le problème suivant : « *Étant donné un entier $n$, il existe des algorithmes qui permettent de dire si $m$ est premier* ». Par contre, il n'existe pas d'algorithmes qui permet de donner la factoriser d'un entier en nombre premier [1]. On note $X$ l'emetteur du message et $Y$, le destinataire. Supposons que $X$ veut envoyer le message

$$M : \text{« Déclancher l'opération rouge »}.$$

1. C'est un problème ouvert !

$X$ transforme $M$ en chiffres selon les conventions suivantes :

$$\begin{cases} \text{A} \to 01 \\ \text{B} \to 02 \\ \text{C} \to 03 \\ \vdots \\ \text{Z} \to 26 \\ \sqcup \to 27 \end{cases}$$

où $\sqcup$ représente l'espace entre deux caractères. $Y$ choisit deux nombres premiers $p$ et $q$ assez long, il calcule $n = pq$ et :

$$\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1).$$

$Y$ choisit un entier $a$ compris entre 1 et $\varphi(n)$ et $a$ premier avec $\varphi(n)$. Il calcule ensuite $1 < x < \varphi(n)$ tel que $ax \equiv 1 \pmod{\varphi(n)}$. Les valeurs de $n$ et $a$ sont publiques, tandis que les valeurs de $p$, $q$ et $x$ sont privées. On code ainsi $M$ par :

$$M = 040503 \dots 05.$$

$X$ « casse » le message $M$ en paquet : $M_1$, $M_2, \dots, M_k$ tels que, pour tout $1 \leq i \leq n$, $\text{PGCD}(M_i, n) = 1$ et $1 \leq M_i \leq n$. Il calcule ensuite $(M_i)^a$ ($a$ étant publique) et il considère le reste de la division euclidienne de $(M_i)^a$ par $n$ qu'on note $(\tilde{M}_i)^a$, c'est-à-dire :

$$(\tilde{M}_i)^a \equiv (M_i)^a \pmod{n}, \quad 1 \leq M_i^a \leq n.$$

$X$ envoie donc le message $M = \tilde{M}_1^a \tilde{M}_2^a \dots \tilde{M}_k^a$.

Pour décoder le message, $Y$ calcule pour chaque $1 \leq i \leq k$, $(\tilde{M}_i^a)^x$ et tombe sur $M_i$. On montre que

$$(\tilde{M}_i^a)^x \equiv M_i^{ax} \pmod{n}.$$

Or, $ax \equiv 1 \pmod{\varphi(n)}$, c'est-à-dire il existe $k \in \mathbf{N}$, $ax = 1 + k\varphi(n)$. Donc :

$$M_i^{ax} = M_i^{1+k\varphi(n)} = M_i \times (M_I^k)^{\varphi(n)}.$$

Comme $\text{PGCD}(M_i, n) = 1$, $M_i^{\varphi(n)} \equiv 1 \pmod{n}$. Donc :

$$(\tilde{M}_i^a)^x \equiv M_i^{ax} \pmod{n}.$$

## 2 Période d'un développement décimal

**Définition I.64** (Développement décimal périodique)**.** *Soit $\alpha \in \mathbf{R}$. On dit que le développement décimal de $\alpha$ est* périodique *si $\alpha$ s'écrit :*

$$\alpha = \text{E}(\alpha) + 0, a_1 a_2 \dots a_k a_{k+1} \dots a_{k+h}$$

*où $\text{E}(\alpha)$ est la partie entière de $\alpha$ et $0 \leq a_i \leq 9$.*

**Définition I.65** (Cycle et période du développement décimal)**.** *Soit $\alpha \in \mathbf{R}$ tel que*

$$\alpha = \mathrm{E}(\alpha) + 0, a_1 a_2 \dots a_k a_{k+1} \dots a_{k+h}.$$

*On appelle la partie $a_{k+1} \dots a_{k+h}$, le* cycle *du développement décimal. Le plus petit entier $h \geq 1$ vérifiant cette propriété est appelée la* période *du développement décimal.*

Si $\alpha$ admet un développement décimal périodique de période $h$, on note :

$$\alpha = \mathrm{E}(\alpha) + 0{,}a_1 \dots a_k \overline{a_{k+1} \dots a_{k+h}}.$$

**Exemples I.66.**
1. $\alpha = \frac{1}{3} = 0{,}3333\dots = 0{,}\overline{3}$. La période du développement décimal de $\alpha$ est 1.
2. $\alpha = 0 = 0{,}\overline{0}$. La période du développement décimal de $\alpha$ est 1.
3. $\alpha = \frac{1}{7} = 0{,}\overline{142857}$. La période du développement décimal de $\alpha$ est 6.

**Théorème I.67.** *Soit $\alpha \in \mathbf{R}$. Le développement décimal de $\alpha$ est périodique si et seulement si $\alpha \in \mathbf{Q}$.*

*Démonstration.* ($\Rightarrow$) On suppose que $\alpha$ s'écrit :

$$\alpha = \mathrm{E}(\alpha) + 0{,}a_1 \dots a_k \overline{a_{k+} \dots a_{k+h}}$$

et on pose $\beta$ la partie décimale de $\alpha$. $\alpha$ appartient à $\mathbf{Q}$ si et seulement si $\beta \in \mathbf{Q}$. On pose :

$$10^k \cdot \beta = a_1 \dots a_k + 0{,}\overline{a_{k+1} \dots a_{k+h}} = a_1 \dots a_k + \gamma.$$

Ainsi :

$$10^h \gamma = a_{k+1} \dots a_{k+h} + 0{,}\overline{a_{k+1} \dots a_{k+h}} \Rightarrow 10^h \gamma = a_{k+1} \dots a_{k+h} + \gamma,$$

c'est-à-dire $(10^h - 1)\gamma = a_{k+1} \cdots a_{k+h}$. On a bien que $\gamma$ appartient à $\mathbf{Q}$ car $\gamma$ s'écrit comme :

$$\gamma = \frac{a_{k+1} \dots a_{k+h}}{10^h - 1}$$

avec $10^h - 1 \in \mathbf{N}^*$ car $h \geq 1$ et $a_{k+1} \dots a_{k+h} \in \mathbf{Z}$.

($\Leftarrow$) Soit $\alpha \in \mathbf{Q}^*$. On pose $\alpha := \mathrm{E}(\alpha) + \frac{m}{n}$ avec $m, n \in \mathbf{Z}$ tels que $0 < m < n$. On pose :

$$\begin{aligned} 10m &= na_1 + r_1 \quad \text{avec } 0 \leq r_1 < n,\ 0 \leq a_1 \leq 9, \\ 10r_1 &= na_2 + r_2 \quad \text{avec } 0 \leq r_2 < n,\ 0 \leq a_2 \leq 9. \end{aligned}$$

Ainsi de suite pour obtenir une suite d'enttiers $(r_1, r_2, \dots, r_k)$ tels que $0 \leq r_i < n$. Comme entre 0 et $n$, il y a un nombre d'entiers finis, il existe $h$ tels que $r_k = r_{k+h}$.

On a :

$$\begin{aligned}\frac{m}{n} &= 0{,}a_1 + 10^{-1}\frac{r_1}{n}\\ &= 0{,}a_1 + 10^{-1}\left(0{,}a_2 + 10^{-1}\frac{r_2}{n}\right)\\ &= 0{,}a_1 + 0{,}0a_2 + 10^{-2}\frac{r_2}{n}\\ &= \cdots\\ &= 0{,}a_1a_2\ldots a_k + 10^{-k}\left(\frac{r_k}{n}\right)\\ &= 0{,}a_1a_2\ldots a_ka_{k+1}\ldots a_{k+h} + 10^{-(k+h)}\frac{r_{k+h}}{n}.\end{aligned}$$

Comme $r_k = r_{k+h}$ :

$$\frac{m}{n} = 0{,}a_1a_2\ldots a_k\overline{a_{k+1}\ldots a_{k+h}}.$$

□

**Proposition I.68.** *Soient $m, n$ des entiers supérieurs à 1 tels que* $\mathrm{PGCD}(m,n) = 1$ *et* $\mathrm{PGCD}(n,10) = 1$. *Soit $h$ le plus petit entier $\geq 1$ tel que* $10^h \equiv 1 \pmod{n}$ *alord :*

$$\frac{m}{n} = \mathrm{E}\left(\frac{m}{n}\right) + 0{,}\overline{a_1\ldots a_h}.$$

**Remarque I.69.** Comme $\mathrm{PGCD}(n,10)$, d'après le théorème I.53 d'Euler, $10^{\varphi(n)} \equiv 1 \pmod{n}$. Donc un tel entier $h$ existe.

*Démonstration.* Soit

$$\frac{m}{n} = \mathrm{E}\left(\frac{m}{n}\right) + 0{,}a_1\ldots a_k\overline{a_{k+1}\ldots a_{k+h}}. \tag{I.20}$$

On montre que :

$$\begin{cases} a_1 = a_{k+1}\\ a_2 = a_{k+2}\\ \ldots\ldots \end{cases}. \tag{I.21}$$

Si on multiplie par $10^h$ dans les deux membres de (I.20), on obtient :

$$10^h\cdot\frac{m}{n} = 10^h\cdot\mathrm{E}\left(\frac{m}{n}\right) + a_1\ldots a_k + 0{,}a_{k+1}\ldots a_{k+h}. \tag{I.22}$$

Si on pose $10^h = 1 + kn$ avec $k \in \mathbf{N}$, on obtient dans l'équation (I.22) :

$$\begin{aligned}(1+kn)\cdot\frac{m}{n} &= (1+kn)\cdot\mathrm{E}\left(\frac{m}{n}\right) + a_1\ldots a_k + 0{,}\overline{a_{k+1}\ldots a_{k+h}}\\ \frac{m}{n} + km &= (1+kn)\cdot\mathrm{E}\left(\frac{m}{n}\right) + a_1\ldots a_k + 0{,}\overline{a_{k+1}\ldots a_{k+h}}\\ \frac{m}{n} &= -km + (1+kn)\cdot\mathrm{E}\left(\frac{m}{n}\right) + a_1\ldots a_k + 0{,}\overline{a_{k+1}\ldots a_{k+h}}.\end{aligned} \tag{I.23}$$

D'après l'unicité du développement décimal et les égalités (I.20) et (I.23), on obtient :

$$\begin{aligned} \mathrm{E}\left(\frac{m}{n}\right) &= -km + (1+kn)\cdot \mathrm{E}\left(\frac{m}{n}\right) + a_1 \dots a_k \\ \mathrm{E}\left(\frac{m}{n}\right) - (1+kn)\cdot \mathrm{E}\left(\frac{m}{n}\right) &= -km + a_1 \dots a_k \\ kn \cdot \mathrm{E}\left(\frac{m}{n}\right) &= -km + a_1 \dots a_k \\ k\left(n \cdot \mathrm{E}\left(\frac{m}{n}\right) + m\right) &= a_1 \dots a_k. \end{aligned}$$

et $0{,}a_1 \dots a_k = 0{,}a_{k+1}a_{k+2}\dots a_{k+h}$. D'où, on obtient (I.21) et

$$\frac{m}{n} = \mathrm{E}\left(\frac{m}{n}\right) + 0{,}\overline{a_1 \dots a_h}.$$

Réciproquement, on suppose que

$$\frac{m}{n} = \mathrm{E}\left(\frac{m}{n}\right) + 0{,}\overline{a_1 \dots a_h} \tag{I.24}$$

et on montre que $10^h \equiv 1 \pmod{n}$. On multiplie par $10^h$ les deux membres de (I.24) :

$$10^h \cdot \left(\frac{m}{n}\right) = 10^h \cdot \mathrm{E}\left(\frac{m}{n}\right) + a_1 \dots a_h + \left(\frac{m}{n} - \mathrm{E}\left(\frac{m}{n}\right)\right). \tag{I.25}$$

Si on multiplie par $n$, les deux membres de (I.25), on obtient :

$$10^h m = 10^h \cdot n \cdot \mathrm{E}\left(\frac{m}{n}\right) + n \cdot a_1 \dots a_h + \left(m - n\mathrm{E}\left(\frac{m}{n}\right)\right).$$

Ainsi, $n \mid 10^h m - m$, c'est-à-dire $n \mid (10^h - 1)m$. Or $\mathrm{PGCD}(m,n) = 1$ et d'après le lemme de Gauss, $n \mid 10^k - 1$. □

.

**Exemple I.70.** On cherche la période du développement décimal de $\alpha = \frac{10}{3}$. On a, tout d'abord $\mathrm{PGCD}(10,3) = 1$ (et donc $\mathrm{PGCD}(3,10) = 1$). Soit $h$ la période c'est-à-dire $h$ est le plus petit entier $\geq 1$ tel que $10^h \equiv 1 \pmod{3}$. Comme $10 \equiv 1 \pmod{3}$, on obtient $h = 1$ et donc :

$$\frac{10}{3} = \mathrm{E}\left(\frac{10}{3}\right) + 0{,}\overline{a}, \qquad \text{où } a \in \mathbf{Z}.$$

**Remarque I.71.** Soit $m$ et $n$ deux entiers tels que $\mathrm{PGCD}(m,n) = 1$ et $\mathrm{PGCD}(n,10) \neq 1$. On pose $m = 2^u 5^v n'$ avec $u \geq 0$, $v \geq 0$, $(u,v) \neq (0,0)$ et $\mathrm{PGCD}(n',10) = 1$. On a :

$$\frac{m}{n} = \frac{m}{2^u 5^v n'}.$$

Supposons que $u \geq v$, alors on écrit :

$$\frac{m}{n} = \frac{1}{10^k} \times \frac{5^{u-v}m}{n'}.$$

Comme $\mathrm{PGCD}(m,n) = 1$ et $n = 2^u 5^v n'$, on a : $\mathrm{PGCD}(m,n') = 1$ et comme $\mathrm{PGCD}(n',10) = 1$, on obtient $\mathrm{PGCD}(n',5^{u-v}) = 1$, d'où $\mathrm{PGCD}(5^{u-v}m,n') = 1$. D'après la proposition I.68,

$$\frac{5^{u-v}m}{n'} = \mathrm{E}\left(\frac{5^{u-v}m}{n'}\right) + 0,\overline{a_1 \dots a_k}.$$

On pose :

$$\mathrm{E}\left(\frac{5^{u-v}m}{n}\right) = b_1 \dots b_t,$$

d'où :

$$\frac{m}{n} = \frac{b_1 \dots b_t + 0,\overline{a_1 \dots a_k}}{10^k}.$$

De même, si $u \leq v$, on fait un raisonnement analogue.

## I.5 Exercices

**Exercice I.1.** Soit $n \in \mathbf{Z}$. Montrer que 3 (resp. 9) divise $n$ si et seulment si 3 (resp. 9) divise la somme des chiffres de $n$. Trouver un critère de divsibilité par 11.

**Exercice I.2.** Montrer que :

1. $3 \cdot 2^{101} + 9 \equiv 0 \pmod 7$,
2. $5^{6614} - 12^{857} \equiv 1 \pmod 7$.

**Exercice I.3.** Trouver le dernier chiffre (le chiffre des unités) de

1. $7^{139}$,
2. $13^{2002}$,
3. $4^n$, $n \in \mathbf{N}$ (discuter selon $n$).

**Exercice I.4.** Dans $\mathbf{R}$, on définit la relation $\mathscr{R}$ par

$$x \mathscr{R} y \Leftrightarrow x^2 = y^2$$

1. Montrer que $\mathscr{R}$ est une relation d'équivalence.
2. Soit $x \in \mathbf{R}$, que représente $\overline{x}$ ? Décrire les éléments de $\overline{x}$.

**Exercice I.5.** Soit $E$ un ensemble non vide. On considère $\mathscr{P}(E)$, l'ensemble des parties de $E$. On définit la relation dans $\mathscr{P}(E)$ par :

$$A \mathscr{R} B \Leftrightarrow A = B \quad \text{et} \quad A = B^{\mathrm{c}}.$$

1. Montre que $\mathscr{R}$ est une relation d'équivalence.
2. Soit $A \in \mathscr{P}(E)$. Décrire $\overline{A}$.
3. Application : $E = \{0, 1, 2\}$. Décrire $\{\overline{0}\}$, $\{\overline{1}\}$, $\{\overline{0}, \overline{1}\}$.

**Exercice I.6.** Écrire la table d'addition de $\mathbf{Z}/6\mathbf{Z}$.

**Exercice I.7.** Écrire la table de multiplication de $\mathbf{Z}/6\mathbf{Z}$.

**Exercice I.8.** Écrire la table de multiplication de $(\mathbf{Z}/4\mathbf{Z})^\times$.

**Exercice I.9.** Soit $\{\overline{x_1}, \ldots, \overline{x_n}\}$ un système complet de représentants de $\mathbf{Z}/N\mathbf{Z}$. Montrer que si $n$ est un entier impair $\geq 2$ alors $x_1 + \cdots + x_n \equiv 0 \pmod{n}$.

**Exercice I.10.** Soit $\left\{\overline{x_1}, \ldots, \overline{x_{\varphi(n)}}\right\}$ un système complet de représentants de classes de $(\mathbf{Z}/n\mathbf{Z})^\times$. Montre que si $n$ est un entier $> 2$ alors $x_1 + \cdots + x_{\varphi(n)} \equiv 0 \pmod{n}$.

**Exercice I.11.** Soit $n > 1$ un entier. Monter que $(n-1)! \equiv -1 \pmod{n}$ si et seulement si $n$ est premier.

**Exercice I.12.** Soit $n > 1$ un entier. Monter que $(n-2)! \equiv 1 \pmod{n}$ si et seulement si $n$ est premier.

**Exercice I.13.** Soit $p$ un nombre premier, montrer que

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}.$$

**Exercice I.14.** Montrer que, pour tout $n \in \mathbf{N}$,

$$\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} \in \mathbf{N}.$$

Plus généralement, montrer que si $p$ et $q$ sont deux nombres premiers,

$$\frac{n^p}{p} + \frac{n^q}{q} + \frac{(pq - p - q)n}{pq} \in \mathbf{N}, \quad \text{pour tout } n \in \mathbf{N}.$$

**Exercice I.15.** Soient $p$ et $q$ deux nombres premiers distincts, a-t-on $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ ?

**Exercice I.16.** Montrer que, pour tout $n \in \mathbf{N}$ tel que $\mathrm{PGCD}(n, 561) = 1$, $n^{560} \equiv 1 \pmod{561}$ (on pourra remarquer que $561 = 3 \cdot 11 \cdot 17$).

**Exercice I.17.** Soit $p$ un nombre premier, montrer que $p \mid a^p + a(p-1)!$, pour tout $a \in \mathbf{N}$.

**Exercice I.18.** Résoudre les équations à inconnues entières suivantes :

1. $3x \equiv 5 \pmod{6}$,
2. $13x \equiv 1 \pmod{7}$,

3. $120x \equiv 24 \pmod{132}$.

**Exercice I.19.** Résoudre les systèmes d'équations :

1. $\begin{cases} 2x \equiv 1 \pmod 3 \\ 13x \equiv 2 \pmod{11} \\ 21x \equiv 11 \pmod{13} \end{cases}$,
2. $\begin{cases} 6x \equiv 2 \pmod 4 \\ x \equiv 4 \pmod 6 \\ x \equiv 27 \pmod{25} \end{cases}$,
3. $\begin{cases} 20x \equiv 1 \pmod 3 \\ 20x \equiv 1 \pmod 6 \\ 46x \equiv 2 \pmod{25} \end{cases}$.

**Exercice I.20.** Déterminer la période et le cycle des fractions suivantes :

1. $\frac{1}{3^2}$,
2. $\frac{101}{7}$,
3. $\frac{1}{7^2}$,
4. $\frac{110}{17}$,
5. $\frac{133}{30}$,
6. $\frac{174}{35}$.

**Exercice I.21.** Soient $m, n \in \mathbf{N}^*$ tels que $lm < n$ et $\mathrm{PGCD}(m, n) = 1$. On suppose que

$$\frac{m}{n} = 0, \overline{a_1 \dots a_h}.$$

Montrer que $m$ divise $a_1 \dots a_h$.

# CHAPITRE II

# FRACTIONS CONTINUES

## II.1 Introduction

**Définition II.1** (Suite de Fibonacci)**.** *Soit* $(\mathscr{F}_n)_{n\in\mathbf{N}}$ *une suite numérique. On dit que la suite est de Fibonacci si* $\mathscr{F}_0$ *et* $\mathscr{F}_1$ *sont des réels quelconques et pour tout* $n \in \mathbf{N}$*, on a :*

$$\mathscr{F}_{n+2} = \mathscr{F}_{n+1} + \mathscr{F}_n.$$

On considère $(\mathscr{F}_n)_{n\in\mathbf{N}}$ une suite de Fibonacci avec $\mathscr{F}_0, \mathscr{F}_1 \in \mathbf{R}^*$. Comme $\mathscr{F}_1 \neq 0$, on peut noter $p$ le rapport entre $\mathscr{F}_0$ et $\mathscr{F}_1$. On a donc :

$$\mathscr{F}_2 = \mathscr{F}_1 + \mathscr{F}_0. \tag{II.1}$$

Comme $\mathscr{F}_1 \neq 0$, on peut diviser (II.1) par $\mathscr{F}_1$, on obtient :

$$\frac{\mathscr{F}_2}{\mathscr{F}_1} = 1 + \frac{\mathscr{F}_0}{\mathscr{F}_1} = 1 + \frac{1}{\frac{\mathscr{F}_1}{\mathscr{F}_0}} = 1 + \frac{1}{p}. \tag{II.2}$$

On fait de même pour le terme $\mathscr{F}_3$ :

$$\mathscr{F}_3 = \mathscr{F}_2 + \mathscr{F}_1. \tag{II.3}$$

On suppose que $\mathscr{F}_2$ est non nul, on peut donc diviser (II.3) par $\mathscr{F}_2$, on obtient alors :

$$\frac{\mathscr{F}_3}{\mathscr{F}_2} = 1 + \frac{\mathscr{F}_1}{\mathscr{F}_2} = 1 + \frac{1}{\frac{\mathscr{F}_2}{\mathscr{F}_1}},$$

mais, d'après (II.2), on a :

$$\frac{\mathscr{F}_3}{\mathscr{F}_2} = 1 + \frac{\mathscr{F}_1}{\mathscr{F}_2} = 1 + \frac{1}{\frac{\mathscr{F}_2}{\mathscr{F}_1}} = 1 + \frac{1}{1 + \frac{1}{p}}. \tag{II.4}$$

Si on contine avec :

$$\begin{aligned}
\mathscr{F}_4 &= \mathscr{F}_3 + \mathscr{F}_2,\\
\mathscr{F}_5 &= \mathscr{F}_4 + \mathscr{F}_3,\\
\mathscr{F}_6 &= \mathscr{F}_5 + \mathscr{F}_4,
\end{aligned}$$

on obtiendra toujours quelque chose en fonction de $p$, c'est-à-dire :

$$\frac{\mathscr{F}_4}{\mathscr{F}_3} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{p}}}, \quad \frac{\mathscr{F}_5}{\mathscr{F}_4} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{p}}}},$$

$$\frac{\mathscr{F}_6}{\mathscr{F}_5} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{p}}}}}},$$

et ainsi de suite. L'opération faite dans cette brève introduction s'appelle un *développement en fraction continue* (DFC) d'un nombre réel. Avant de dévoiler la définition d'une fraction continue, on peut regarder un exemple sur le nombre $\pi$.

**Exemple II.2.** Le but est de trouver des nombres entiers $n_0, n_1, n_2, \ldots$ tels que :

$$\pi = n_0 + \cfrac{1}{n_1 + \cfrac{1}{n_2 + \cfrac{1}{\ddots}}}.$$

On sait, tout d'abord, que $\pi = 3,141592$. La partie entière de $\pi$ est donc $\mathrm{E}(\pi) = 3$, d'où $n_0 = 3$. Pour trouver $n_1$, on remarque que $\frac{1}{\pi - 3} \simeq 7,04$, d'où $n_1 7$. En exercice, le lecteur pourra trouver les entiers $n_2$ et $n_3$. On obtient donc :

$$\pi \simeq 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}}.$$

On peut maintenant définir une fraction continue.

## II.2 Définitions et propriétés

**Définition II.3** (Fraction continue généralisée)**.** *Soit $n$ un entier naturel et soient $(a_k)_{0 \leq k \leq n}$ et $(b_k)_{0 \leq k \leq n}$ deux suites réels. Alors on appelle* fraction continue généralisée *une fraction de*

*la forme :*

$$a_0 + \cfrac{b_0}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_2}{a_3 + \cfrac{b_3}{\ddots\, a_{n-1} + \frac{b_n}{a_n}}}}}.$$

**Définition II.4** (Fraction cotninue finie)**.** *Dans la définition II.3, si la suite* $(b_k)_{0\leq k\leq n}$ *est constante et égale à* 1 *alors on dit que*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_{n-1} + \frac{1}{a_n}}}$$

*est une* fraction continue finie.

**Définition II.5** (Fraction continue finie simple)**.** *On dit qu'une fraction continue finie est* simple *si la suite* $(a_k)_{1\leq k\leq n}$ *est une suite d'entiers.*

Soit :

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_{n-1} + \frac{1}{a_n}}},$$

le développement en fraction continue simple finie (DFCSF) de $x$. On note alors :

$$x = a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_{n-1}+}\frac{1}{a_n}$$

ou

$$x = [a_0, a_1, \ldots, a_{n-1}, a_n].$$

**Remarque II.6.** Soit $[a_0, a_1, \ldots, a_n]$ une fraction continue simple. On peut obtenir une relation de récurrence :

$$[a_0, a_1, \ldots, a_n] = a_0 + \frac{1}{[a_1, \ldots, a_n]} = \left[a_0, a_1, \ldots, a_{n-1} + \frac{1}{a_n}\right].$$

**Théorème II.7.** *Un nombre est rationnel si et seulement s'il admet un DFCSF.*

*Démonstration.* Il est évident que si $x$ possède un développement fini en fraction continue alors il est rationnel (voir l'exercice II.2). On montre que si $x$ est rationnel alors il possède un développement en fraction continue. Comme $x$ est un rationnel alors il existe $p$ et $q$ deux entiers tels que $x = \frac{p}{q}$. On démontre, par récurrence, que $x$ admet un DFCSF.

**Initialisation** Si $q = 1$ alors on peut prendre $x = p$ et ainsi $x = [p]$.

**Hérédité** On suppose que la propriété est vérifiée pour toutes les fractions admettenant un dénominateur strictement plus petit que $q$. En faisant la division euclidienne de $p$ et $q$, on obtient l'existence de deux entiers $d$ et $r$ tels que :

$$p = d \cdot q + r \quad \text{avec } r < q.$$

D'où :

$$\frac{p}{q} = d + \frac{r}{q} = d + \frac{1}{\frac{q}{r}}.$$

Mais d'après l'hypothèse de récurrence, la fraction $\frac{q}{r}$ admet un DFCSF.

□

**Exemples II.8** (DFCSC d'un nombre rationnel)**.** 1. On veut trouver le développement en fraction continue finie simple du nombre rationnel $\frac{17}{49}$. On a :

$$\frac{17}{49} = \frac{49-32}{49} = \frac{49}{49} - \frac{32}{49} = 1 - \frac{32}{49}, \tag{II.5}$$

$$-\frac{49}{32} = \frac{(-64)+15}{32} = -\frac{64}{32} + \frac{15}{32} = -2 + \frac{15}{32}, \tag{II.6}$$

$$\frac{32}{15} = \frac{30}{15} + \frac{2}{15} = 2 + \frac{2}{15}, \tag{II.7}$$

$$\frac{15}{2} = 7 + \frac{1}{2}, \tag{II.8}$$

$$\frac{2}{1} = 2. \tag{II.9}$$

En combinant les égalités (II.5), (II.6), (II.7), (II.8), (II.9), on obtient la fraction continue simple de $\frac{17}{49}$ :

$$\frac{17}{49} = 1 + \cfrac{1}{-2 + \cfrac{1}{2 + \cfrac{1}{7 + \frac{1}{2}}}}.$$

2. On veut trouver le DFCSF du nombre rationnel $-\frac{225}{40}$. On utilise l'algorithme d'Euclide pour trouver les $a_i$ (ils sont encadrés ci-dessous) :

$$\begin{aligned} -225 &= 40 \times \boxed{-6} + 15, \\ 40 &= 15 \times \boxed{2} + 10, \\ 15 &= 10 \times \boxed{1} + 5, \\ 10 &= 5 \times \boxed{2}. \end{aligned}$$

D'où :

$$-\frac{225}{40} = [-6, 2, 1, 2].$$

**Remarque II.9.** Soit $x \in \mathbf{Q}$ tel que $x = [a_0, a_1, \ldots, a_n]$. Alors $a_0$ représente la partie entière de $x$, c'est-à-dire $a_0 = \mathrm{E}(x)$.

**Définition II.10** (Réduite d'une fraction cotninue)**.** *Soit $x = [a_0, a_1, \ldots, a_n]$. Alors*

$$r_k = \frac{p_k}{q_k} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_{k-1} + \frac{1}{a_k}}}$$

*est appelée la $k^{\mathrm{e}}$* réduite *de la fraction continue de $x$.*

**Théorème II.11.** *Soient $[a_0, a_1, \ldots, a_n]$ une fraction continue simple et $(r_k)_{0\leq k\leq n}$ la suite de ses réduites tels que $r_k = \frac{p_k}{q_k}$, pour tout $0 \leq k \leq n$. Alors*

$$p_0 = 1,\ q_0 = 0,\ p_1 = a_1,\ q_1 = 1$$

*et pour tout $k \geq 2$ :*

$$\begin{aligned} p_k &= a_k p_{k-1} + p_{k-2}, \\ q_k &= a_k q_{k-1} + q_{k-2}. \end{aligned}$$

*Démonstration, [11].* Pour démontrer le théorème, il faut utiliser le principe de récurrence d'ordre 2 sur $n$.

**Initialisation** Pour $n = 0$, on a $\frac{p_0}{q_0} = \frac{a_0}{1} = a_0$ et pour $n = 1$, on obtient $\frac{p_1}{q_1} = \frac{a_1 a_0 + 1}{a_1} = a_0 + \frac{1}{a_1}$. Les deux cas initiaux sont donc vérifiés.

**Hérédité** On suppose que $n \geq 2$ et qu'on a

$$\frac{p_{n-2}}{q_{n-2}} = [a_0, \ldots, a_{n-2}], \quad \frac{p_{n-1}}{q_{n-1}} = [a_0, \ldots, a_{n-2}, a_{n-1}]$$

quelque soit les valeurs $a_0, \ldots, a_{n-1}$. Or la fraction continue

$$[a_0, a_1, \ldots, a_{n-1}, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_{n-1} + \frac{1}{a_n}}}$$

s'obtient en prenant

$$[a_0, \ldots, a_{n-2}, a_{n-1}] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_{n-1}}}$$

et en remplaçant $a_{n-1}$ par $a_{n-1}+\frac{1}{a_n}$ (voir la remarque II.6). C'est-à-dire, on a :

$$\begin{aligned}
[a_0,\dots,a_{n-2},a_{n-1},a_n] &= [a_0,\dots,a_{n-2},a_{n-1},a_{n-1}+\frac{1}{a_n}] \\
&= \frac{p_{n-1}(a_0,\dots,a_{n-2},a_{n-1}+\frac{1}{a_n})}{q_{n-1}(a_0,\dots,a_{n-2},a_{n-1}+\frac{1}{a_n})} \\
&= \frac{(a_{n-1}+\frac{1}{a_n})p_{n-2}+p_{n-3}}{(a_{n-1}+\frac{1}{a_n})q_{n-2}+q_{n-3}} \\
&= \frac{a_{n-2}p_{n-2}+p_{n-3}+\frac{1}{a_n}p_{n-2}}{a_{n-1}q_{n-2}+q_{n-3}+\frac{1}{a_n}q_{n-2}} \\
&= \frac{p_{n-1}+\frac{1}{a_n}p_{n-2}}{q_{n-1}+\frac{1}{a_n}q_{n-2}} \\
&= \frac{a_np_{n-1}+p_{n-2}}{a_nq_{n-1}+q_{n-2}} = \frac{p_n}{q_n}.
\end{aligned}$$

□

**Théorème II.12.** *Soient $[a_0,\dots,a_n]$ une fraction continue simple et finie et $(r_k)_{0\le k\le n}$ la suite de ses réduites tels que $r_k=\frac{p_k}{q_k}$, pour tout $0\le k\le n$. Alors, on a, pour tout $n\ge 0$, $p_nq_{n-1}-p_{n-1}q_n=(-1)^n$.*

*Démonstration, [11].* On fait une preuve par récurrence sur $n$.

**Initialisation** Pour $n=0$, on a :

$$p_1q_0-q_1p_0=a_0\times 0-1\times 1=-1.$$

**Hérédité** Pour $n\ge 1$, on suppose par récurrence qu'on a :

$$p_{n-1}q_{n-2}-p_{n-2}q_{n-1}=(-1)^{n-2},$$

et on trouve

$$\begin{aligned}
p_nq_{n-1}-p_{n-1}q_n &= (a_np_{n-1}+p_{n-2})q_{n-1}-p_{n-1}(a_nq_{n-1}+a_{n-2} \\
&= p_{n-2}q_{n-1}-p_{n-1}q_{n-2}=-(-1)^{n-2}=(-1)^{n-1}.
\end{aligned}$$

□

## II.3 Fractions continues et équations diophantiennes

Grâce aux fractions continues, on peut résoudre les équations diophantiennes. Cela est dû au théorème suivant :

**Théorème II.13.** *Si* $\frac{a}{b} = [a_0, a_1, \ldots, a_n]$ *et* $\mathrm{PGCD}(a, b) = 1$ *alors* $x = q_{n-1}$ *et* $y = -p_{n-1}$ *est une solution de l'équation diophantienne* $ax + by = (-1)^n$.

*Démonstration.* La démonstration de ce théorème est laissée en exercice. □

**Exemple II.14.** On veut résoudre l'équation $457x - 53y = 1$. On a bien $\mathrm{PGCD}(457, 53) = 1$. Le DFCSF de $\frac{457}{53}$ est $[8, 1, 1, 1, 1, 1, 6]$. L'avant-dernière réduite de $\frac{457}{53}$ vaut :

$$[8,1,1,1,1,1] = 8 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}} = 8 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{2}}}}$$
$$= 8 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{2}{3}}} = 8 + \frac{1}{1 + \frac{3}{5}} = 8 + \frac{5}{8} = \frac{69}{8}.$$

La parité du développement étant impaire, on a bien :

$$457 \times 8 - 53 \times 69 = -1. \tag{II.10}$$

Mais on veut résoudre l'équation $457x - 53y = 1$. Pour cela, il faut changer la partié du développement en effectuant une expansion à droite, c'est-à-dire :

$$\frac{457}{53} = [8, 1, 1, 1, 1, 1, 5, 1].$$

L'avant-dernière réduite vaut maintenant $\frac{388}{45}$ et la parité du développement est, cette fois-ci, paire. On a donc :

$$457 \times 45 - 53 \times 388 = 1. \tag{II.11}$$

On a donc une famillie infinie de solutions qui est, dans le cas (II.10),

$$\begin{cases} x = 8 + 53k \\ y = 69 + 457k \end{cases}, \quad k \in \mathbf{Z},$$

et, dans le cas (II.11) :

$$\begin{cases} x = 45 + 53k \\ y = 388 + 457k \end{cases}, \quad k \in \mathbf{Z}.$$

**Proposition II.15.** *Le théorème II.13 est une méthode pour résoudre* toutes *les équations diophantiennes.*

*Démonstration.* Soient $a, b, c$ trois entiers tels que $\mathrm{PGCD}(a, b) = 1$. On veut résoudre l'équation diophantienne suivante :

$$ax + by = c \tag{II.12}$$

L'algorithme proposé ci-dessus fournit $x_0$ et $y_0$ tels que $ax_0 - by_0 = \pm 1$. Les couples $(cx_0 + kb, cy_0 + ka)$ sont les solutions de (II.12). En effet,

$$a(cx_0 + kb) - b(cy_0 + bk) = c(ax_0 - by_0) = \pm c.$$

□

**Exemple II.16.** On veut résoudre dans $\mathbf{Z}$, l'équation :

$$12x + 5y = 13. \tag{II.13}$$

Notons tout d'abord que $\mathrm{PGCD}(12, 5) = 1$. On transforme l'équation (II.13) en :

$$12x - (-5)y = 13.$$

On cherche donc le DFCSF de $-\frac{12}{5}$ :

$$-\frac{12}{5} = -3 + \frac{3}{5} = -3 + \frac{1}{1 + \frac{2}{3}} = -3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}.$$

D'où : $-\frac{12}{5} = [-3, 1, 1, 2]$. On cherche l'avant-dernière réduite de $-\frac{12}{5}$ :

$$[-3, 1, 1] = -3 + \frac{1}{1 + \frac{1}{1}} = -3 + \frac{1}{2} = -\frac{5}{2}.$$

On a une période impaire car $-5$ est impaire donc on a :

$$2 \times 12 - 5 \times 5 = -1.$$

On a alors une solution particulière de (II.13) :

$$(x_0, y_0) = (2 \times -13, -5 \times -13) = (-26, 65).$$

Donc les solutions dans $\mathbf{Z}$ sont :

$$x = -26 + 5k \quad \text{et} \quad y = 65 + 12k.$$

## II.4 Approximation des nombres irrationnels

**Théorème II.17** (Convergence des suites des réduites vers un réel)**.** *Soient $(a_k)_{k\geq 1}$ une suite d'entiers positifs et $r_k = [a_1, \ldots, a_k]$. Alors la suite $(r_k)_{k\geq 1}$ converge vers un réel.*

**Définition II.18** (Fractions continues infinie simples)**.** *La limite*

$$\lim_{n\to+\infty} [a_0, a_1, \ldots, a_n]$$

*est appelée* fraction continue infinie simple*.*

**Théorème II.19.** *Tout irrationnel $x$ admet un unique développement en fraction continue infinie.*

*Démonstration.* Soient $\alpha = [a_0, a_1, \ldots]$ et $\alpha_1 = [a_1, a_2, \ldots]$. D'après la remarque II.9, $\mathrm{E}(\alpha) = a_0$ et on a :

$$\alpha = a_0 + \underbrace{\cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}}_{\alpha_1} = a_0 + \frac{1}{\alpha_1}. =$$

En exercice, on peut montrer que, par récurrence, que si $\alpha = [a_0, a_1, \ldots] = [b_0, b_1, \ldots]$ alors $a_n = b_n$, pour tout $n \geq 1$. □

**Définition II.20** (Irrationnel quadratique)**.** *Un* irrationnel quadratique *est un nombre réel de la forme $a + b\sqrt{D}$ avecf $D \geq 2$ un entier non carré (c'est-à-dire il n'existe pas un entier $d$ tel que $D^2 = d$) et $a$, $b \neq 0$ des rationnels.*

**Définition II.21** (Fraction continue périodique)**.** *On note la* fraction continue périodique $[a_0, \ldots, a_k, \overline{a_{k+1}, \ldots, a_{k+h}}]$*, la fraction continue suivante :*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_k + \cfrac{1}{a_{k+1} + \cfrac{1}{\ddots\, a_{k+h} + \cfrac{1}{a_{k+1} + \cfrac{1}{\ddots}}}}}}.$$

**Théorème II.22.** *La fraction continue d'un réel est ultimement périodique si et seulement si $x$ est un irrationnel quadratique.*

**Exemples II.23.** 1. On veut trouver la valeur de $\alpha = [\overline{1}]$. Trouver la valeur de $\alpha = [\overline{1}]$ est équivalent à résoudre l'équation

$$x = 1 + \frac{1}{x}. \tag{II.14}$$

Si on multiplie par $x$ les deux membres de l'équation (II.14), on obtient $x^2 - x - 1 = 0$. La résolution de l'équation nous donne $x = \frac{1+\sqrt{5}}{2}$ et $x = \frac{1-\sqrt{5}}{2}$. Comme $\mathrm{E}(x) = 1$, la valeur de $x$ convenable est $\frac{1+\sqrt{5}}{2} \geq 0$.

2. On cherche la valeur de $\alpha = [2, \overline{1, 8}]$. On pose $\alpha = [2, y]$ avec $y = [\overline{1, 8}]$. On résoud donc l'équation suivante :

$$\begin{aligned} y = 1 + \frac{1}{8 + \frac{1}{y}} &\Leftrightarrow y = 1 + \frac{y}{8y+1} \\ &\Leftrightarrow \frac{9y+1}{8y+1} = y \\ &\Leftrightarrow y(8y+1) = 9y + 1 \Leftrightarrow 8y^2 - 8y - 1 = 0. \end{aligned}$$

Cette équation a pour solutions :

$$y_1 = \frac{1}{2} + \frac{\sqrt{6}}{4} \quad \text{et} \quad y_2 = \frac{1}{2} - \frac{\sqrt{6}}{2}$$

. Mais comme $\mathrm{E}(y) = 1$, la solution convenable est $y_1 = \frac{1}{2} + \frac{\sqrt{6}}{4}$. Or $\alpha = [2, y]$, donc :

$$\begin{aligned} \alpha &= 2 + \frac{1}{\frac{2+\sqrt{6}}{4}} = 2 + \frac{4}{2+\sqrt{6}} = \frac{2(2+\sqrt{6})+4}{2+\sqrt{6}} \\ &= \frac{8+2\sqrt{6}}{2+\sqrt{6}} = \frac{(8+2\sqrt{6})(2-\sqrt{6})}{4+6} = \frac{4-4\sqrt{6}}{10}. \end{aligned}$$

On propose maintenant un algorithme ([11]) pour calculer le développement en fraction continue simple infinie d'une racine carré.

**Initialisation** On pose $R_0 = \sqrt{D}$, on calcule $a_0 = \mathrm{E}\left(\sqrt{D}\right)$ en trouvant un encadrement de la racine. Pour la prochaine étape, on définit :

$$R_1 := \frac{1}{R_0 - a_0}$$

**Hérédité** Supposons qu'on a calculé les $a_k$ pour $0 \leq k \leq n$, on pose $R_n =:= \frac{1}{R_{n-1} - a_{n-1}}$ et $a_n = \mathrm{E}(R_n)$ (qu'on peut trouver en faisant un encadrement).

**Arrêt de l'algorithme** En vertu du théorème II.22, il y a des valeurs qui se répètent. Quand on trouve une répétition $R_i = R_{i+n}$, on sait qu'on aura ensuite :

$$\begin{aligned} a_i &= \mathrm{E}(R_i) = \mathrm{E}(R_{i+n}) = a_{i+n}, \\ R_{i+1} &= \frac{1}{R_i - a_i} = \frac{1}{R_{i+n} - a_{i+n}} = R_{i+n+1} \\ a_{i+1} &= \mathrm{E}(R_{i+1}) = \mathrm{E}(R_{i+n+1}) = a_{i+n+1} \\ &\cdots\cdots \end{aligned}$$

Donc on aura $a_k = a_{k+n}$ pour tout $k \geq i$ et la fraction continue est :

$$R = [a_0, a_1, \ldots, a_{i-1}, \overline{a_i, \ldots a_{i+n-1}}].$$

**Exemple II.24** ([11])**.** Soit $R = \sqrt{7}$, on veut trouver son développement en fraction continue simple infinie. On a :

$$R_0 = \sqrt{7}, \quad a_0 = \mathrm{E}\left(\sqrt{7}\right) = 2,$$

On a l'encadrement $4 < 7 < 9$, d'où $\mathrm{E}\left(\sqrt{7}\right) = 2$.

$$\begin{aligned}
R_1 &= \frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3}, \quad a_1 = \mathrm{E}\left(\frac{\sqrt{7}+2}{3}\right) = 1,\\
R_2 &= \frac{1}{\frac{\sqrt{7}-1}{3}} = \frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2}, \quad a_2 = \mathrm{E}\left(\frac{\sqrt{7}+1}{2}\right) = 1,\\
R_3 &= \frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3}, \quad a_3 = \mathrm{E}\left(\frac{\sqrt{7}+1}{3}\right) = 1,\\
R_4 &= \frac{3}{\sqrt{7}-2} = \sqrt{7}+2, \quad a_4 = \mathrm{E}\left(\sqrt{7}+2\right) = 4,\\
R_5 &= \frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3} = R_1.
\end{aligned}$$

D'où $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$.

On va maintenant développer les résultats d'approximation des nombres irrationnels.

**Théorème II.25.** *Soient $\alpha$ un irrationnel et $(r_k)_{k\in\mathbf{N}^*}$ tels que, pour tout $k \in \mathbf{N}^*$, $r_k = \frac{p_k}{q_k}$ la suite de ses réduites. Si une fraction irréductible $r = \frac{p}{q}$ avec $p \in \mathbf{N}$, $q \in \mathbf{N}^*$ vérifie $|\alpha - r| \leq |\alpha - r_n|$ pour un entier $n$ donné alors on a les inégalités $p \geq p_n$ et $q \geq q_n$.*

*Démonstration.* On distingue plusieurs cas :

1. Si $n = 0$ alors $\alpha - \frac{p}{q} \leq \alpha - \mathrm{E}(\alpha)$, on tire $p \geq \frac{p}{q} \geq \mathrm{E}(\alpha) = p_0$ et on a aussi $q \geq 1 = q_0$.
2. Si $n \geq 1$, on remarque tout d'abord que la suite $(p_n)_{n\in\mathbf{N}}$ est positive et croissante.
   (a) Si $r \in [r_n, r_{n+1}]$, le résultat est clair.
   (b) Si $r_n < r < r_{n+1}$ alors on peut montrer que $p \geq p_{n+1}$ et $q \geq q_{n+1}$. On a :

$$0 < \left|\frac{p}{q} - \frac{p_n}{q_n}\right| \leq |r_{n+1} - r_n| = \frac{1}{|q_n q_{n+1}|}$$
$$\Rightarrow 0 < |pq_n - qp_n|\, q_{n+1} \leq q \Rightarrow q \geq q_{n+1} \geq q_n$$

– Si $n$ est pair, on a : $r_{n+1} < r < r_n$, puis :

$$pq_n > qp_n \Rightarrow pq_n \geq qp_{n+1} \geq q_{n+1}p_{n+1} \Rightarrow p \geq p_{n+1} \geq p_n.$$

– Si $n$ est impair, on a $r_n < r < r_{n+1}$ puis $pq_{n+1} > qp_{n+1} \geq q_{n+1}p_{n+1}$ et donc $p \geq p_{n+1} \geq p_n$.

(c) Si $r$ est hors du segment d'extrémités $r_n$ et $r_{n+1}$, on peut vérifier que $r$ est strictement compris entre $r_{n-1}$ et $r_n$ et le cas précédent permet de conclure.

– Si $n$ est pair, de $r_n < \alpha < r_{n+1}$ et de l'hypothèse, on en tire que $r > r_n$ puis

$$r - \alpha \leq \alpha - r_n \Rightarrow r \leq 2\alpha - r_n 2r_{n+1} - r_n \leq r_{n-1}$$

– Si $n$ est impair alors de $r_{n+1} < x < r_n$ et de l'hypothèse, on en tire $r < r_n$ puis :

$$x - \alpha \leq r_n - x \Rightarrow r \geq 2x - r_n > 2r_{n+1} - r_n > r_{n-1}.$$

□

**Théorème II.26.** *Si $\alpha$ est un irrationnel et $\frac{p_n}{q_n}$ une réduite de $\alpha$ alors*

$$\left|\frac{p_n}{q_n} - \alpha\right| < \frac{1}{q_n^2}$$

**Exercice II.27.** Démontrer que :

$$\frac{p_n}{q_n} - \alpha = \frac{(-1)^n}{q_n(q_n r_{n+1} + q_{n+1})} \tag{II.15}$$

*Démonstration.* On utilise (II.15),

$$\frac{p_n}{q_n} - \alpha = \frac{(-1)^n}{q_n(q_n r_{n+1} + q_{n+1})}$$

où $(r_n)_{n\in\mathbf{N}^*}$ est la suite des réduites de $\alpha$. D'où

$$\left|\frac{p_n}{q_n} - \alpha\right| = \frac{1}{q_n(r_{n+1}q_n + q_{n-1})}.$$

Mais on a, $r_{n+1} \geq q_{n+1}$, $q_n > 0$ et $q_{n-1} > 0$ et $a_{n+1} \geq 1$, d'où :

$$r_{n+1}q_n + q_{n+1} \geq a_{n+1}q_n + q_{n-1} = q_{n+} > a_{n+1}q_n > q_n.$$

En multipliant ces inégalités par $q_n$ et en prenant les réciproques, on trouve le résultat du théorème. □

**Exemples II.28.**

1. Trouver un irrationnel $\frac{a}{b}$ tel que $\left|\sqrt{5} - \frac{a}{b}\right| < 10^{-4}$.
2. Sachant que $\pi = [3, 7, 15, 1, 192, 1, 1, 1, 2, \ldots]$, trouver un rationnel $\frac{a}{b}$ tel que $\left|\pi - \frac{a}{b}\right| < 10^{-4}$.

## II.5 Exercices

**Exercice II.1.** Calculer :

$$x_1 = 3 + \frac{1}{7},\ x_2 = 3 + \frac{1}{7 + \frac{1}{15}},\ x_3 = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1}}}.$$

Que remarque-t-on ?

**Exercice II.2.** Montrer que tout nombre rationnel peut s'écrire comem fraction continue simplie finie. Pour cela, on pourra utiliser l'algorithme d'Euclide.

**Exercice II.3.** Calculer les réduites du DFCSC de $\frac{117}{38}$.

**Exercice II.4.** Soient $[a_0, a_1, \ldots, a_n]$ une fraction continue simple et finie et $(r_k)_{0 \leq k \leq n}$ la sutie de ses réduites tels que $r_k = \frac{p_k}{q_k}$ pour tout $0 \leq k \leq n$. Montrer que

1. $q_0 < q_1 \leq q_2 < q_3 \leq \cdots$,
2. $r_1 < r_3 < r_5 < \cdots < r_6 < r_4 < r_2$.

**Exercice II.5.** Avec le même algorithme, trouver le développement en fraction simple infinie de $\sqrt{2}$, $\sqrt{5}$ et $3 + \sqrt{18}$.

.

# CHAPITRE A

# THÈMES DE RECHERCHE

## A.1 Nombres pythagoriciens et grand théorème de Fermat

### 1 Nombres pythagoriciens

Dans cette première partie du mémoire, on veut donner une description des triangles rectangles à côtés entiers. Ce problème se ramène à paramétrer l'ensemble des solutions de l'équation :

$$x^2 + y^2 = z^2, \quad (x, y, z) \in (\mathbf{N}^*)^3. \tag{E}$$

Dans toute cette partie, on va déterminer une paramétrisation de ($E$). On montrera que, quitte à permuter $x$ et $y$, avec $x, y, z > 0$), les solutions s'écrivent :

$$\begin{cases} x = d(v^2 - u^2) \\ y = 2duv \\ z = d(u^2 + v^2) \end{cases}, \quad d, u, v \in \mathbf{N}^*, \ v > u. \tag{P}$$

**Preuve arithmétique**

1. Soit $(x, y, z)$ une solution de ($E$) tel que $\mathrm{PGCD}(x, y, z) = 1$. Montrer que
   (a) $x, y$ et $z$ sont premiers entre eux deux à deux.
   (b) $z$ est impair et $x$ et $y$ sont de parités différentes.
   (c) Quitte à permuter $x$ et $y$, il existe deux entiers $u, v > 0$ tels que $z - x = 2u^2$, $z + x = 2v^2$ et $\mathrm{PGCD}(u, v) = 1$.
   (d) Conclure sur la paramétrisation de ($E$)
2. Soit $(x, y, z)$ solutions de ($E$) tels que $\mathrm{PGCD}(x, y, z) = d$ avec $d \geq 2$ (on dit que les triplets ne sont pas primitives). Montrer qu'on a la paramétrisation de ($E$) suivante :
$$\begin{cases} x = d(v^2 - u^2) \\ y = 2duv \\ z = d(u^2 + v^2) \end{cases}$$
avec $u, v \in \mathbf{N}^*$ et $\mathrm{PGCD}(u, v) = 1$.

**Paramétrisation du cercle** Soit $(x, y, z)$ un triplet pythagoricien. On pose :

$$x = z\cos\theta,\ y = z\sin\theta \quad \text{avec } \theta \in \left]0\,,\,\tfrac{\pi}{2}\right[.$$

1. En posant $t = \tan\left(\frac{\theta}{2}\right)$, montrer que $x$ et $y$ s'écrivent :
$$x = z \cdot \frac{1-t^2}{1+t^2}, \quad y = z \cdot \frac{2t}{1+t^2}.$$
2. (a) Montrer que $t$ est un rationnel strictement positif.
   (b) On pose $t = \frac{u}{v}$ avec $u, v \in \mathbf{N}^*$. En déduire que :
$$x = z \cdot \frac{v^2-u^2}{u^2+v^2}, \quad y = z \cdot \frac{2uv}{u^2+v^2}.$$
3. Montrer que $\mathrm{PGCD}(u^2+v^2, v^2-u^2) = 1$ ou $2$.
4. Démontrer que si $\mathrm{PGCD}(u^2+v^2, v^2-u^2) = 1$, $x$, $y$ et $z$ s'écrivent sous la forme donnée par ($P$).
5. On suppose que $\mathrm{PGCD}(u^2+v^2, v^2-u^2) = 2$. On pose $u' = \frac{v-u}{2}$ et $v' = \frac{u+v}{2}$. Justifier que $u'$ et $v'$ sont des entiers. Exprimer $x$, $y$ et $z$ en fonction de $u'$ et $v'$.
6. Conclure sur la paramétrisation de ($E$).

## 2 Grand théorème de Fermat

Dans cette seconde partie du mémoire, nous allons étudier l'équation

$$x^n + y^n = z^n, \quad (x, y, z) \in (\mathbf{N}^*)^*.$$

Pierre de Fermat avait énoncé ce théorème en ajoutant : *« J'ai trouvé une merveilleuse démonstration de cette proposition, mais la marge est trop étroite pour la contenir »*

1. Donner un bref historique du grand théorème de Fermat. Qui était Marin Marsenne ? Pierre de Fermat ? Sophie Germain ? Johann Peter Gustav Lejeune Dirichlet ?
2. Qu'est ce que « la méthode de la descente infinie » ?
3. On s'intéresse à l'équation $x^4 + y^4 = z^2$.
   (a) Démontrer que si l'on prouve que $x^4 + y^4 = z^2$ n'a pas de solutions en nombres entiers différents de zéro, alors on aura prouvé que l'équation $x^4 + y^4 = z^4$ n'a pas de solutions en nombres entiers différents de zéro.
   (b) Soient $(x, y, z)$ une solution de l'équation $x^4 + y^4 = z^2$ et $d = \mathrm{PGCD}(x, y)$. Montrer que $d^2$ divise $z$. Donner une paramétrisation comme dans la première partie (c'est-à-dire exprimer $x^2, y^2, z$ en fonction de $a$ et $b$ des nombres entiers).
   (c) Prouver que le triplet $(b, y, a)$ est encore un triplet pythagoricien primtif (c'est-à-dire trouver $m, n$ deux nombre entiers tels qu'on peut écrire $b, y, a$ en fonction de $m, n$ (comme dans la paramétrisation ($E$))).

(d) Prouver que les entiers $a, m, n$ sont tous les trois des carrés.

(e) On peut alors écrire $a = z'^2$, $m = x'^2$, $n = y'^2$, où $x', y', z'$ sont des nombres entiers. Prouver que le triplet d'entier $(x', y', z')$ est encore solution de l'équation $x^4 + y^4 = z^2$.

(f) Prouver que $0 < z' < z$.

(g) Conclure.

## A.2 Construction des nombres naturels

Dans ce mémoire, nous allons prouver des propriétés importantes relatives à la construction des nombres naturels. On commence par l'axiome de l'existence.

### 1 Définition, propriétés

**Axiome A.1.** *Il existe un ensemble* $\mathbf{N}$ *(dont les éléments sont dits* entiers naturels*) vérifiant les propriétés suivantes :*

*(i)* $\emptyset \in \mathbf{N}$,

*(ii) L'inclusion est un bon ordre sur* $\mathbf{N}$ *(c'est-à-dire tout sous-ensemble non vide de* $\mathbf{N}$ *admet un plus petit élément).*

*(iii) En notant* $\mathbf{N}^* = \mathbf{N} \setminus \{\emptyset\}$ *:*

$$n \in \mathbf{N}^* \Leftrightarrow \exists m \in \mathbf{N},\ n = m \cup \{m\}\,.$$

**Remarques A.2.** 1. Pour tout $n \in \mathbf{N}$, $n \cup \{n\} \in \mathbf{N}^*$.

2. Pour tout $n \in \mathbf{N}$, $n \in n \cup \{n\}$ et $n \subset n \cup \{n\}$.

On note $\emptyset = 0$, $0 \cup \{0\} = 1$, $1 \cup \{1\} = 2\ldots$ La relation d'ordre $\subset$ sur $\mathbf{N}$ est notée $\leq$ ; on définit sur $\mathbf{N}$ la relation $\prec$ par :

$$n \prec m \Leftrightarrow (n \leq m \text{ et } n \neq m).$$

**Questions :**

1. Montrer que $\leq$ est un bon ordre.
2. Montrer que la relation $\leq$ vérifie :

$$a \leq x \leq a \cup \{a\} \Leftrightarrow [x = a \text{ ou } x = a \cup \{a\}].$$

3. On définit l'application $\varphi\colon \mathbf{N} \to \mathbf{N}^*$ qui à un entier $n$ associe l'entier $\varphi(n) = n \cup \{n\}$. Montrer que $\varphi$ est une bijection de $\mathbf{N}$ sur $\mathbf{N}^*$.
4. Montrer que $\mathbf{N}$ est un ensemble infini.

## 2 Récurrence

**Théorème A.3** (Principe de récurrence)**.** *Soit $A \subset \mathbf{N}$ tel que $0 \in A$ et pour tout $n \in \mathbf{N}$, $n \in A \Rightarrow \varphi(n) \in A$. Alors $A = \mathbf{N}$.*

**Remarque A.4** (Principe de récurrence finie)**.** Soient $b \in \mathbf{N}$ et $B = \{n \in \mathbf{N},\ n \leq b\}$. Soit $A \subset B$ tel que $0 \in A$ et pour tout $n \in B \setminus \{b\}$, $n \in A \Rightarrow \varphi(n) \in A$. Alors $A = B$.

Le principe de la démonstration par récurrence est donc le suivant. Pour prouver une propriété $P_n$ (propriété dépendant de $n$) pour tout $n \in \mathbf{N}$, il suffit de prouver que $P_0$ est vraie et que pour tout $n \in \mathbf{N}$, $P_n \Rightarrow P_{\varphi(n)}$. On applique ensuite le principe de récurrence à l'ensemble $A = \{n \in \mathbf{N},\ P_n\}$.

**Théorème A.5.** *Pour tout entier $n$, on a :*

$$n = \{m \in \mathbf{N},\ m \prec n\}\,.$$

**Questions :**

1. Montrer le théorème A.3.
2. De la même façon que pour le principe de récurrence, montrer le principe de récurrence finie.
3. Montrer le théorème A.5.

**Remarque A.6.** On a :

$$m \in n \Leftrightarrow m \prec n \Leftrightarrow m \leq \varphi^{-1}(n).$$

On note donc $n = \{0, 1, \ldots, \varphi^{-1}(n)\}$.

## 3 Addition dans N

Pour tout $a \in \mathbf{N}$, on définit la fonction $f_a \colon \mathbf{N} \to \mathbf{N}$ de la façon suivante :

$$\begin{cases} f_a(0) = a \\ f_a(\varphi(n)) = \varphi(f_a(n)), \quad \forall n \in \mathbf{N} \end{cases}.$$

On note $f_a(n) = a + n$. On a ainsi défini une *addition* sur $\mathbf{N}$. Les deux propriétés définissant $f_a$ se traduisent par :

$$\begin{cases} a + 0 = a, & \forall a \in \mathbf{N}, \\ a + \varphi(n) = \varphi(a + n), & \forall a \in \mathbf{N},\ \forall n \in \mathbf{N}. \end{cases}$$

**Remarque A.7.** Pour $n = 0$, dans cette égalité, on obtient $a + 1 = \varphi(a)$ donc :

$$\forall a \in \mathbf{N},\ \forall n \in \mathbf{N}, \quad a + (n + 1) = (a + n) + 1.$$

**Questions :**

1. Montrer que l'opération + est associative, c'est-à-dire :

$$\forall a, b, c \in \mathbf{N}, \quad (a + b) + c = a + (b + c).$$

(on pourra faire une récurrence sur $c$).

2. Démontrer que 0 est un élément neutre de +.
3. Montrer que l'opération + est commutative, c'est-à-dire :

$$\forall a, b \in \mathbf{N},\ a + b = b + a.$$

(on pourra faire une récurrence sur $b$).

4. Montrer que pour tout $a, b, c \in \mathbf{N}$ :

$$(a + b = a + c \Rightarrow b = c).$$

(on pourra montrer cette propriété en faisant une récurrence sur $a$.

## 4 Addition et relation $\leq$

**Théorème A.8.** *Pour tous entiers $a$ et $n$, on a*

$$a + n \geq a.$$

**Théorème A.9.** *Soient $a$ et $b$ deux entiers. Alors on a l'équivalence :*

$$a \leq b \Leftrightarrow (\exists c \in \mathbf{N},\ b = a + c).$$

**Remarque A.10.** Si $a \leq b$, l'entier $c$ tel que $b = a + c$ est unique. En effet, l'égalité $a + c = a + c_1$ implique $c = c_1$ puisque $a$ est régulier. Cet entier est appelé différence de $a$ et $b$, et est noté $b - a$.

**Théorème A.11.** *L'addition et la relation d'ordre $\leq$ sont compatibles :*

$$(a \leq b \text{ et } c \leq d) \Rightarrow a + c \leq b + d$$

**Questions :**

1. Montrer le théorème .
2. Montrer le théorème .
3. Montrer le théorème .

## 5 Multiplication dans N

Pour tout $a \in \mathbf{N}$, on définit une fonction $g_a \colon \mathbf{N} \to \mathbf{N}$ par :

$$\begin{cases} g_a(0) = 0 \\ g_a(n+1) = g_a(n) + a, \quad \forall n \in \mathbf{N} \end{cases}.$$

On note $a \times n = g_a(n)$ (on note encore $a \cdot n$ ou $an$) ; on définit ainsi une *multiplication* sur $\mathbf{N}$. Les deux propriétés ci-dessus se traduisent par :

$$\begin{cases} a \times 0 = 0, & \forall a \in \mathbf{N}, \\ a(n+1) = an + a, & \forall a \in \mathbf{N},\ \forall n \in \mathbf{N}. \end{cases}$$

**Remarque A.12.** $a \times 1 = a \times 0 + a$ donc $a \times 1 = a$.

**Questions :**

1. Montrer que la multiplication est distributive sur l'addition, c'est-à-dire :

$$\forall a, b, c \in \mathbf{N}, \quad a(b+c) = ab + ac.$$

2. Montrer que la multiplication est associative, c'est-à-dire,

$$\forall a, b, c \in \mathbf{N}, \quad (ab)c = a(bc).$$

3. Montrer que 1 est élément neutre.
4. Montrer que 0 est un élément absorbant.
5. Montrer que la multiplication est commutative, c'est-à-dire :

$$\forall a, b \in \mathbf{N}, \quad ab = ba.$$

6. Montrer l'équivalence suivante :

$$\forall a, b \in \mathbf{N},\ ab = 0 \Leftrightarrow (a = 0 \text{ ou } b = 0).$$

7. Montrer que tout entier non nul est régulier pour la multiplication, c'est-à-dire :

$$\forall a \in \mathbf{N}^*,\ \forall b, c \in \mathbf{N}, \quad (ab = ac \Rightarrow b = c).$$

8. Montrer que $\leq$ et $\times$ sont compatibles, c'est-à-dire :

$$(a \leq b \text{ et } c \leq d) \Rightarrow ac \leq bd.$$

### 6 Division euclidienne dans N

**Lemme A.13** (Lemme d'Archimède)**.** *Soient $a$ et $b$ deux entiers avec $b \neq 0$. Alors*

$$\exists k \in \mathbf{N},\ a \prec bk.$$

**Théorème A.14** (Division euclidienne dans $\mathbf{N}$)**.** *Soient $a$ et $b$ deux entiers tels que $b \neq 0$. Alors il existe un unique couple $(q, r) \in \mathbf{N} \times \mathbf{N}$, $a = bq + r$ et $r \prec b$.*

**Questions :**

1. Montrer le lemme d'Archimède.
2. Montre le théorème A.14.

## A.3 Approximation du nombre $\pi$

### 1 Sur le nombre $\pi$

**Questions :**

1. Que représente le nombre $\pi$ ?
2. Donner un historique du nombre $\pi$.
3. Montrer que $\pi$ est un nombre irrationnel.
4. Est-ce que $\pi$ est un nombre aléatoire ?

### 2 Approximation du nombre $\pi$

**Questions :**
Donner :

1. Formule d'approximation d'Archimède.
2. Formule de Gregory-Leibniz.
3. Formule de Leohnard Euler.
4. Approximation étrange de Ramanujan.
5. Somme infinie de Ramanujan.
6. Formule de Simon Plouffe.
7. 100 premières décimales de $\pi$.

## A.4 Tables de logarithme

**Questions :**

1. Donner un bref historique sur les tables de logarithmes.
2. Un extrait d'une table de logarithme est donnée en table A.1. En remarquant que $\log(10^n) = n$, trouver la valeur de

(a) $\log(2,745)$,

(b) $\log(2745)$,

(c) $\log(2572)$,

(d) $\log(2,572 \times 10^{12})$.

| $N.$ | $L.$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **250** | 39 | 794 | 811 | 826 | 846 | 863 | 881 | 898 | 915 | 933 | 950 |
| 251 | | 967 | 985 | ∗002 | ∗019 | ∗037 | ∗054 | ∗071 | ∗088 | ∗106 | ∗123 |
| 252 | 40 | 140 | 157 | 175 | 192 | 209 | 226 | 243 | 261 | 278 | 295 |
| 253 | | 312 | 329 | 346 | 364 | 381 | 398 | 415 | 432 | 449 | 466 |
| 254 | | 483 | 500 | 518 | 535 | 552 | 569 | 586 | 603 | 620 | 637 |
| 255 | | 654 | 671 | 688 | 705 | 722 | 739 | 756 | 773 | 790 | 807 |
| 256 | | 824 | 841 | 858 | 875 | 892 | 909 | 926 | 943 | 960 | 976 |
| 257 | | 993 | ∗010 | ∗027 | ∗044 | ∗061 | ∗078 | ∗095 | ∗111 | ∗128 | ∗145 |
| 258 | 41 | 162 | 179 | 196 | 212 | 229 | 246 | 263 | 280 | 296 | 313 |
| 259 | | 330 | 347 | 363 | 380 | 397 | 414 | 430 | 447 | 464 | 481 |
| **260** | | 497 | 514 | 531 | 547 | 564 | 581 | 597 | 614 | 631 | 647 |
| 261 | | 664 | 681 | 697 | 714 | 731 | 747 | 764 | 780 | 797 | 814 |
| 262 | | 830 | 847 | 863 | 880 | 896 | 913 | 929 | 946 | 963 | 979 |
| 263 | | 996 | ∗012 | ∗029 | ∗045 | ∗062 | ∗078 | ∗095 | ∗111 | ∗127 | ∗144 |
| 264 | 42 | 160 | 177 | 193 | 210 | 226 | 243 | 259 | 275 | 292 | 308 |
| 265 | | 325 | 341 | 357 | 374 | 390 | 406 | 423 | 439 | 455 | 472 |
| 266 | | 488 | 504 | 521 | 537 | 553 | 570 | 586 | 602 | 619 | 635 |
| 267 | | 651 | 667 | 684 | 700 | 716 | 732 | 749 | 765 | 781 | 797 |
| 268 | | 813 | 830 | 846 | 862 | 878 | 894 | 911 | 927 | 943 | 959 |
| 269 | | 975 | 991 | ∗008 | ∗024 | ∗040 | ∗056 | ∗072 | ∗088 | ∗104 | ∗120 |
| **270** | 43 | 136 | 152 | 169 | 185 | 201 | 217 | 233 | 249 | 265 | 281 |
| 271 | | 297 | 313 | 329 | 345 | 361 | 377 | 393 | 409 | 425 | 441 |
| 272 | | 457 | 473 | 489 | 505 | 521 | 537 | 553 | 569 | 584 | 600 |
| 273 | | 616 | 632 | 648 | 664 | 680 | 696 | 712 | 727 | 743 | 759 |
| 274 | | 775 | 791 | 807 | 823 | 838 | 854 | 870 | 886 | 902 | 917 |
| 275 | | 933 | 949 | 965 | 981 | 996 | ∗012 | ∗028 | ∗044 | ∗059 | ∗075 |

TABLE A.1 – Extrait d'une table de logarithme

3. Quelle est la valeur de $x$ telle que :

(a) $\ln(x) = 0,43854$ ?

(b) $\ln(x) = 0,42226$ ?

(c) $\ln(x) = 43993$ ?

(d) $\ln(x) = 4216$ ?

4. On admet que :
$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} \dots .$$
Donner une valeur approchée de $\ln(2)$, $\ln(4)$, $\ln(9)$.
5. Construire la table de logarithmes $\log_b(n)$ pour $2 \leq n \leq 10$ et $2 \leq b \leq 10$.
6. Construire la table de logarithmes de $\log_{10} n$ et $\ln(n)$ pour $2 \leq n \leq 100$.

## A.5 Nombres transcendants

### 1 Généralités sur les nombres transcendants

**Définition A.15** (Nombre transcendant)**.** *Un* nombre transcendant *sur les rationnels est un nombre réel ou complexe qui n'est racine d'aucune équation polynômiale.*

**Théorème A.16.** *Soit A l'ensemble des nombres algébriques réels. Alors :*

*(i) A est un sous corps de* $\mathbf{R}$*,*

*(ii) A est dénombrable,*

*(iii) A est différent de* $\mathbf{R}$*.*

**Questions :**

1. Montrer le théorème A.16.

### 2 Théorème de Hermite-Lindermann

**Définition A.17** (Nombre algébrique)**.** *On appelle* nombre algébrique*, tout nombre qui est solution d'une équation algébrique (c'est-à-dire un polynôme non nul) à coefficients entiers (ou rationnels).*

**Théorème A.18** (Hermite-Lindemann)**.** *Si a est un nombre algébrique alors le nombre* $\mathrm{e}^a$ *est transcendant.*

**Questions :**

1. Montrer que $\mathrm{e}^1$ est un nombre transcendant.
2. Plus généralement, montrer que $\mathrm{e}^a$ pour tout $a$, nombre algébrique non nul.
3. Montrer que $\sin(1)$ est un nombre transcendant.
4. Plus généralement, montrer que $\cos(a)$ et $\sin(a)$ sont des nombres transcendants pour tout $a$, nombre algébrique non nul.
5. Montrer que $\pi$ est un nombre transcendant.
6. Montrer que $\log(a)$ est un nombre transcendant pour tout $a$ réel algébrique strictement positif et différent de 1.

### 3 Théorème de Gelfond-Schenider

**Théorème A.19.** *Si $\alpha$ est un nombre algébrique différent de 0 et de 1 et si $\beta$ est un nombre algébrique irrationnel alors $\alpha^\beta$ est un nombre transcendant.*

**Questions :**

1. Montrer que le nombre $2^{\sqrt{2}}$ (qu'on appelle *constante de Gelfond-Schneider*) est un nombre transcendant.
2. Montrer que le nombre $(-1)^{-\mathrm{i}}$ (qu'on appelle *constante de Gelfond*) est un nombre transcendant.
3. En remarquant que $\mathrm{i}^{\mathrm{i}}$ est la racine carrée de l'inverse de la constante de Gelfond, montrer que $\mathrm{i}^{\mathrm{i}}$ est un nombre transcendant.
4. Montrer que le nombre $\frac{\log(3)}{\log(2)}$ est un nombre transcendant.

### 4 Un exemple de nombres transcendants : le nombre de Champernowne

**Définition A.20** (Nombre normal)**.** *On dit qu'un nombre réel $x$ est* normal *en base $b$ si, toutes les séquences de chiffres possibles apparaissent avec la même probabilité dans son écriture en base $b$.*

On définit le nombre de Chapernowne en base 10 par :

$$C_{10} = 0,123456789101112\ldots$$

**Questions :**

1. Donner le nombre de Chapernowne en base 2 et 3.
2. Donner le développement en fraction continue de $C_{10}$.
3. Montrer que $C_{10}$ est un nombre transcendant.

### 5 Transendance des nombres e et $\pi$

**Théorème A.21.** *Les nombres* e *et $\pi$ sont transcendants.*

**Questions :**

1. Sans utiliser le théorème de Hermite-Lindermann, montrer le théorème A.21.

## A.6 Cryptographie à clef publique

Ce mémoire est un complément de la première partie du cours sur les Congruences. On va expliciter la crytographie développée par Rivest Shamir et Adleman (RSA).

## 1 Introduction et rappels du cours sur les Congruences

**Questions :**

1. Donner la liste des attaques de cet algorithme crytographique.
2. 1829 est-il premier ? 7919 est-il composé ?
3. Montrer le théorème d'Euler.
4. Résoudre le problème de Qiu JiuShao : « *Combien l'armée de Han XIng a-t-elle de soldats, si rangés en* 3 *colonnes, il en reste* 2*, par* 5 *colonnes, il en reste* 3 *et par* 7 *colonnes, il en reste* 2 *?* ».

## 2 Symbole de Legendre

Soit $p > 2$ premier et $a$ un entier. On veut savoir s'il existe $x \in \mathbf{Z}_p^*$ tel que $x^2 \equiv a \pmod{p}$. Pour cela, on note $\left(\frac{a}{p}\right)$ pour $p$ premier :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a \\ +1 & \text{si } a \text{ est un carré .} \\ -1 & \text{sinon} \end{cases}$$

**Questions :**

1. Montrer que $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$, pour $p$ premier.
2. Montrer les propriétés suivantes sur le symbole de Legendre :
   (a) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
   (b) $\left(\frac{(-1)}{p}\right) = (-1)^{(p-1)/2}$, autrement dit, $-1$ est un carré modulo $p$ si $p \equiv 1 \pmod{4}$ et n'est pas un carré modulo $p$ si $p \equiv 3 \pmod{4}$.
   (c) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, autrement dit, 2 est un carré modulo $p$ si $p \equiv \pm 1 \pmod{8}$ et n'est pas un carré modulo $p$ si $p \equiv \pm 3 \pmod{8}$.
   (d) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ si $b$ et $p$ sont premiers entre eux.
   (e)

$$\left(\frac{p}{q}\right) = (-1)^{((p-1)(q-1))/4}\left(\frac{p}{q}\right)$$
$$= \begin{cases} -\left(\frac{p}{q}\right) & \text{si } p \equiv 3 \pmod{4} \text{ et } q \equiv 3 \pmod{4} \\ \left(\frac{p}{q}\right) & \text{sinon.} \end{cases}$$

3. 7411 est-il un carré modulo 9283 ?

## 3 Chiffrement RSA

Le chiffrement RSA consiste à

1. choisir $p$ et $q$ premiers assez grands (de l'ordre de $10^{100}$),
2. fixer $n = pq$ et publier $n$,
3. calculer $\varphi(n) = (p-1)(q-1)$,
4. choisir et publier $e$ tel que $\text{PGCD}(e, \varphi(n)) = 1$,
5. calculer $d$ tel que $d \cdot e \equiv 1 \pmod{\varphi(n)}$.

**Questions :**

1. Démontrer le chiffrement RSA.
2. Si $A$ et $B$ utilisent le chiffrement RSA avec $n = 133$. La clé publique de $A$ est 37.
   (a) Quelle est sa clé privée ?
   (b) Si le cryptographe reçu par $A$ est 17, retrouver le clair. (Les messages sont compris entre 0 et $n-1$).

# Bibliographie


[1] *Groupe* $\mathbf{Z}/n\mathbf{Z}$, URL : http://pagesperso-orange.fr/cyd60000/cours/Congruence.pdf.

[2] *Congruences dans* $\mathbf{Z}$*, Anneaux* $\mathbf{Z}/n\mathbf{Z}$*, Applications*, URL : http://epsilon2000.free.fr/Csup/congruences.pdf.

[3] L. Merel, *Étude des groupes* $\mathbf{Z}/n\mathbf{Z}$, Université Paris VII, Année 2000-2001, DEUG 2ème année, Groupes et arithmétiques (MT282), URL : http://www.math.jussieu.fr/~merel/mt282-00-feuille5.pdf.

[4] C. Boulonne, *Notes de cours M101 : Fondements de l'algèbre*, Licence de Mathématiques, Semestre 1.

[5] *Petit théorème de Fermat et codage RSA*, URL : http://pagesperso-orange.fr/divers/rsa/rsa.fr.

[6] *Petit théorème de Fermat*, URL : http://www.anemath.net/ame_mathematique2/cours_ts/tifermat.pdf.

[7] M. Van Caneghem, *Congruences et théorème chinois des restes*, Férivier 2003, Département d'Informatique de la Faculté des Sciences de Luminy.

[8] G. Constatini, *Théorème chinois. Applications* URL : http://pagesperso-orange.Fr/gilles.constantini.

[9] M. Couchouron, *Développement d'un réel en fractions continues*, Université de Rennes 1, Préparation à l'agrégation de mathématiques.

[10] S. Caruso, *Fractions continues*, 7 mars 2009.

[11] C. Walter, *Chapitre 2 : Fractions continues*, URL : http://math.unice.fr/~walter/L1_Arith.

[12] F. Loret, *Activités autour du Dernier Théorème de Fermat*, Academie d'Aix-Marseille.

# Index