# 2 Corps finis

**Exercice 2.1** — Algorithme d'Euclide

1. Soit $a$ et $b$ deux entiers strictement positifs tels que $a > b$. On pose $r_0 = a$ et $r_1 = b$ et on fait des divisions euclidiennes successives :

$$\begin{array}{rcll} r_0 & = & r_1 q_1 + r_2, & 0 < r_2 < r_1 \\ r_1 & = & r_2 q_2 + r_3, & 0 \leq r_3 < r_2 \\ & \vdots & & \vdots \\ r_{n-2} & = & r_{n-1} q_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} & = & r_n q_n + 0 & \end{array}$$

   Montrer que si $d \mid a$ et $d \mid b$ alors pour $0 \leq i \leq n$ : $d \mid r_i$.
2. Calculer les $r_i$ et $q_i$ pour $a = 1016$ et $b = 317$. Que peut-on en déduire sur ces deux nombres ?
3. Les nombres $q_i$ étant construit comme ci-dessus, on définit $u_i$ et $v_i$ par :

$$\begin{array}{l} u_0 = 1,\ u_1 = 0, \text{ et pour } i \geq 1 : u_{i+1} = u_{i-1} - u_i q_i \\ v_0 = 0,\ v_1 = 1, \text{ et pour } i \geq 1 : v_{i+1} = v_{i-1} - v_i q_i \end{array}$$

   Montrer qu'on a pour $0 \leq i \leq n$ : $r_i = a u_i + b v_i$
4. Calculer les $u_i$ et $v_i$ pour $a = 1016$ et $b = 317$, et en déduire $u$ et $v$ tels que $au + bv = 1$.
5. Autre exemple : $a = 571$ et $b = 258$.

**Définition 2.2** — définition « rapide » de $\mathbb{Z}/n\mathbb{Z}$, suffisante pour faire des calculs :
- $\mathbb{Z}/n\mathbb{Z}$ est un ensemble de $n$ éléments notés $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$,
- si $a \notin \{0, 1, 2, \ldots n-1\}$ alors $\overline{a} = \overline{r}$ où $r$ est le reste de la division euclidienne de $a$ par $n$,
- en particulier : $\overline{n} = \overline{0}$,
- si $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ et $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ on pose $\overline{a} + \overline{b} = \overline{a+b}$ et $\overline{a} \times \overline{b} = \overline{ab}$

**Exercice 2.3**

1. Écrire les tables d'addition et de multiplication de $\mathbb{Z}/6\mathbb{Z}$ et de $\mathbb{Z}/7\mathbb{Z}$.
2. Vérifier que tout élément non nul de $\mathbb{Z}/7\mathbb{Z}$ est inversible.
3. Quels sont les éléments inversibles de $\mathbb{Z}/6\mathbb{Z}$ ?

**Exercice 2.4**

1. Pour tout élément $\overline{a}$ de $\mathbb{Z}/7\mathbb{Z}$, calculer $\overline{a}^2$, $\overline{a}^3$, $\overline{a}^4$, $\overline{a}^5$, $\overline{a}^6$.
2. Déterminer le reste de la division euclidienne de $123^{456}$ par 7.
3. Dans $\mathbb{Z}/19\mathbb{Z}$ calculer $\overline{a} = \overline{2}^2$, $\overline{b} = \overline{2}^4 = \overline{a}^2$, $\overline{c} = \overline{2}^8 = \overline{b}^2$, $\overline{d} = \overline{2}^{16} = \overline{c}^2$ et en déduire $\overline{2}^{18}$. Faire de même pour les puissances de $\overline{3}$.
4. Montrer que $2^{345} + 6^{789}$ est divisible par 19.

**Exercice 2.5** Calcul rapide de puissances

1. Calculer modulo 71 : $a = 3^2$, $b = 3^4 = a^2$, $c = 3^8 = b^2$, $d = 3^{16} = c^2$ et $e = 3^{32} = d^2$.
2. En déduire $3^{35} \pmod{71}$.
3. Quel est l'ordre multiplicatif de 3 dans $\mathbb{F}_{71}^*$ ?
4. Donner un générateur $\mathbb{F}_{71}^*$.

**Exercice 2.6** Montrer que le polynôme $P = X^4 + 2X^3 + 2X + 1$ admet une racine dans $\mathbb{F}_3[X]$. Factoriser $P$ dans $\mathbb{F}_3[X]$.

**Exercice 2.7** Factoriser le polynôme $P = 3X^3 + 4X^2 + 2X - 4$ dans $\mathbb{F}_5[X]$ et dans $\mathbb{F}_7[X]$.

**Exercice 2.8** Quels sont les polynômes unitaires irréductibles de degré inférieur ou égal à 4 dans $\mathbb{F}_2[X]$ ? Dans $\mathbb{F}_3[X]$ ?

**Exercice 2.9**

1. Effectuer la division euclidienne de $X^3 + X^2 + 1$ par $X^2 + X + 1$ dans $\mathbb{F}_2[X]$
2. Trouver une relation de Bézout entre ces deux polynômes.

**Exercice 2.10** Soit $\mathbf{k}$ un corps et $P \in \mathbf{k}[X]$ un polynôme unitaire. Donner une définition « rapide » de $\mathbf{k}[X]/P\mathbf{k}[X]$, suffisante pour faire des calculs.

**Exercice 2.11** Soit $P = X^2 + X + 1 \in \mathbb{F}_5$, $K = \mathbb{F}_5[X]/P\mathbb{F}_5[X]$ et $x$ la classe de $X$ dans $K$.

1. Quel est le cardinal de $K$ ?
2. Soit $f = ax + b \in K$ et $g = cx + d \in K$ où $a, b, c, d \in \mathbb{F}_5$. Exprimer le produit $f \times g$ sous la forme $\alpha x + \beta$ où $\alpha, \beta \in \mathbb{F}_5$.
3. Montrer que $P$ n'a pas de racine dans $\mathbb{F}_5$.
4. Montrer que $K$ est un corps.
5. Déterminer l'inverse de $x$ dans $K$.
6. Soit $a \in \mathbb{F}_5$ ; faire la division euclidienne de $P$ par $X+a$ et en déduire l'inverse de $x+a$ dans $K$.
7. Déterminer le plus petit entier $n > 0$ tel que $x^n = 1$ (càd l'ordre multiplicatif de $x$ dans $K^*$).
8. Déterminer le plus petit entier $m > 0$ tel que $(x + 1)^m = 1$ (l'ordre multiplicatif de $x + 1$).
9. Montrer que $x + 2$ est un générateur de $K^*$ (càd : $x + 2$ est d'ordre le cardinal de $K^*$).