Remarque 3.8 (Méthode de résolution d'un système de congruence)**.** *Pour résoudre*

$$\begin{cases} x \equiv b_1[a_1] \\ \vdots \\ x \equiv b_n[a_n] \end{cases}$$

avec $a_1, \dots, a_n$ *deux à deux premiers entre eux, on combine les solutions de*

$$\begin{cases} x \equiv \delta_{1,k}[a_1] \\ \vdots \\ x \equiv \delta_{n,k}[a_n] \end{cases}$$

Pour ces dernières, par exemple pour $k = 1$*, le système équivaut à*

$$\{x \equiv 1[a_1]\ x \equiv 0[a_2 \dots a_n]\}$$

Ce système se résout en écrivant une relation de Bézout entre a_1 *et* $a_2 \dots a_n$*.*

Exemple 3.9. *Résoudre le système suivant :*

$$\begin{cases} x \equiv 2[5] \\ x \equiv 2[8] \\ x \equiv -2[11] \end{cases}$$

Exemple 3.10. *Résoudre les deux systèmes suivants :*

$$\begin{cases} x \equiv 3[42] \\ x \equiv 10[49] \end{cases} \quad \textit{et} \quad \begin{cases} x \equiv 3[42] \\ x \equiv 9[49] \end{cases}$$

3.3 L'indicatrice d'Euler

Définition 3.11 (Indicatrice d'Euler φ)**.** *Soit* $n \in \mathbb{N}^*$*. L'indicatrice d'Euler est définie par*

$$\varphi(n) = \textit{Card}(\{k \in [1, n] \mid k \wedge n = 1\}).$$

Lemme 3.12 (Ordre du groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$)**.** *Soit* $n \in \mathbb{N}^*$*. Alors* $\textit{Card}((\mathbb{Z}/n\mathbb{Z})^\times) = \varphi(n)$*.*

Théorème 3.13 (Théorème d'Euler)**.** *Soit* $(k, n) \in \mathbb{Z} \times \mathbb{N}^*$ *tels que* $n \wedge k = 1$*. Alors* $k^{\varphi(n)} \equiv 1[n]$*.*

Éléments de preuve. C'est le théorème de Lagrange dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Remarque 3.14 (Lien avec le petit théorème de Fermat)**.** *Pour* $n = p \in \mathbb{P}$*,* $\varphi(p) = p - 1$*, et on retrouve, pour* $k \notin p\mathbb{Z}$*,* $k^{p-1} \equiv 1[p]$*. Ainsi, le théorème d'Euler est une généralisation du petit théorème de Fermat.*

Proposition 3.15 (Multiplicativité arithmétique de φ)**.** *Soit* $(m, n) \in (\mathbb{N}^*)^2$ *tel que* $m \wedge n = 1$*. Alors* $\varphi(mn) = \varphi(m)\varphi(n)$*.*

Éléments de preuve. En passant aux inversibles dans le théorème chinois, sachant qu'un isomorphisme préserve l'inversibilité. □

Lemme 3.16 ($\varphi(p^k)$). *Soit $p \in \mathbb{P}$ et $k \in \mathbb{N}^*$. Alors $\varphi(p^k) = p^{k-1}(p-1)$.*

Éléments de preuve. Dénombrement direct, sachant que k n'est pas premier avec $p \in \mathbb{P}$ si et seulement s'il est multiple de p. □

Théorème 3.17 (Expression de $\varphi(n)$). *Soit $n \in \mathbb{N}^*$, et $n = p_1^{a_1} \cdots p_r^{a_r}$ sa décomposition en facteurs premiers, avec $a_i > 0$. Alors*

$$\varphi(n) = \prod_{\ell=1}^{r} p_\ell^{a_\ell - 1}(p_\ell - 1) = n \prod_{\ell=1}^{r} \left(1 - \frac{1}{p_\ell}\right).$$

4. Arithmétique dans l'anneau $\mathbb{K}[X]$

Conformément au programme, soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$ (mais tous les résultats de cette section restent valides si $\mathbb{K}$ est un corps quelconque).

4.1 Idéaux de $\mathbb{K}[X]$

Théorème 4.1 (Description des idéaux de $\mathbb{K}[X]$.] *Soit $\mathbb{K}$ un corps. Alors :*

(i) *$\mathbb{K}[X]$ est un anneau principal.*

(ii) *De plus, deux polynômes P et Q engendrent le même idéal si et seulement s'il existe un $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.*

(iii) *En particulier, tout idéal non nul I de $\mathbb{K}[X]$ s'écrit de manière unique sous la forme $I = P \cdot \mathbb{K}[X]$, où P est un polynôme unitaire.*

Éléments de preuve. S'aider de la division euclidienne, comme pour montrer que $\mathbb{Z}$ est principal. C'est une propriété générale de tout anneau muni d'une division euclidienne (anneau euclidien). La deuxième partie provient de la description des inversibles de $\mathbb{K}[X]$. □

Définition 4.2 (Divisibilité dans $\mathbb{K}[X]$.] *Soit A et B deux polynômes de $\mathbb{K}[X]$. On dit que B divise A s'il existe un polynôme Q tel que $A = BQ$. Inversement, on dit que A est un multiple de B.*

Exercise 4.3. *Déterminer les polynômes $P \in \mathbb{C}[X]$ tels que P' divise P.*

Proposition 4.4 (Caractérisation en termes d'idéaux). *Soit A et B deux polynômes de $\mathbb{K}[X]$. Alors A divise B si et seulement si $B \in (A)$, ou encore si et seulement si $(B) \subset (A)$.*

Définition 4.5 ((Re)définition du PGCD de n polynômes). *Soit $n \geq 2$ et $P_1, \ldots, P_n$ des polynômes non tous nuls de $\mathbb{K}[X]$. Le PGCD Q de $P_1, \ldots, P_n$, noté $Q = P_1 \wedge P_2 \wedge \cdots \wedge P_n$, est l'unique polynôme unitaire tel que*

$$Q \cdot \mathbb{K}[X] = P_1 \cdot \mathbb{K}[X] + \cdots + P_n \cdot \mathbb{K}[X].$$