(ii) *il existe* u *et* v *dans* $\mathbb{Z}$ *tels que* $uk + vn = 1$*;*

(iii) $k \wedge n = 1$.

Éléments de preuve. Immédiat par traduction des congruences, et par le théorème de Bézout. □

Remarque 3.2. *Le point (ii) nous dit comment trouver un inverse de* k *modulo* n *: il suffit de déterminer une relation de Bézout, et de la réduire modulo* n*.*

Corollaire 3.3 (Le corps $\mathbb{F}_p$)**.** *En particulier, pour* $p \in \mathbb{N}^*$*,* $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ *est un corps si et seulement si* p *est premier. Ce corps est noté* $\mathbb{F}_p$*.*

Éléments de preuve. Si $p \in \mathbb{P}$, tout élément de $[1, p-1]$ est premier avec p. Réciproquement, si $p \notin \mathbb{P}$, un diviseur strict de p n'est pas premier avec p et sa classe n'est pas inversible dans $\mathbb{Z}/p\mathbb{Z}$. □

Exemple 3.4. *Le corps* $\mathbb{F}_2$ *a seulement deux éléments. Le corps* $\mathbb{F}_3$ *en a 3. Décrire leurs lois.*

3.2 Théorème chinois, et systèmes de congruences

Théorème 3.5 (Théorème chinois)**.** *Soit* m *et* n *dans* $\mathbb{N}^*$*, tels que* $m \wedge n = 1$*. Pour* $k \in \mathbb{Z}$*, on note :*

- $\hat{k}$ *la classe de* k *dans* $\mathbb{Z}/mn\mathbb{Z}$*;*
- $\check{k}$ *la classe de* k *dans* $\mathbb{Z}/m\mathbb{Z}$*;*
- $\tilde{k}$ *la classe de* k *dans* $\mathbb{Z}/n\mathbb{Z}$*;*

L'application $\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *définie par*

$$\varphi(\hat{k}) = (\check{k}, \tilde{k})$$

est bien définie, et est un isomorphisme d'anneaux. Ceci s'étend sans difficulté au cas d'un plus grand nombre d'entiers 2 à 2 premiers entre eux.

Éléments de preuve. Pour montrer que c'est un isomorphisme, étudier le noyau en se ramenant à des propriétés arithmétiques. □

Corollaire 3.6 (Unicité modulo $a_1 \cdots a_n$ de la solution d'un système)**.** *Soit* $a_1, \ldots, a_n$ *des entiers deux à deux premiers entre eux, et* $b_1, \ldots, b_n$ *des entiers. Alors le système*

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

admet une solution, unique modulo $a_1 \cdots a_n$*.*

Corollaire 3.7 (Cas d'un second membre commun)**.** *En particulier, si* $b_1 = \cdots = b_n = b$*, la seule solution modulo* $a_1 \cdots a_n$ *est* b*.*

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