Chapitre 1

Congruences

L'objectif de ce chapitre est de rappeler quelques notions et résultats élémentaires de théorie des congruences. Cette théorie conduit naturellement à introduire l'anneau $\mathbb{Z}/n\mathbb{Z}$ ainsi que le groupe de ses éléments inversibles (pour la multiplication), noté $(\mathbb{Z}/n\mathbb{Z})^*$. Nous rappelons la construction de ces objets et précisons leurs principales propriétés.

1.1 Quelques rappels sur les groupes finis

Soient G un groupe fini (noté multiplicativement) et H un sous-groupe de G. Un théorème de Lagrange affirme que le cardinal de H divise le cardinal de G. Maintenant, si g est un élément de G, alors il existe un plus petit entier $\omega \geq 1$ tel que $g^\omega = e$. Les éléments $e, g, g^2, \ldots, g^{\omega-1}$ sont alors tous distincts et l'ensemble

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{\omega-1}\}$$

est le plus petit sous-groupe de G contenant g. L'entier ω est appelé **l'ordre** de g. On vérifie facilement (en utilisant le théorème de la division euclidienne) que

$$g^m = e \Longleftrightarrow \omega | m.$$

En appliquant le théorème de Lagrange, on obtient immédiatement que ω divise le cardinal de G. En particulier, si G est un groupe de cardinal n, alors $g^n = e$ pour tout $g \in G$.

On rappelle qu'un groupe G est **cyclique** s'il existe $g \in G$ tel que le sous-groupe engendré par g est G tout entier. On dit dans ce cas que g est un **générateur** de G. Un élément g de G est un générateur de G si et seulement si l'ordre de g est maximal, c'est-à-dire exactement le cardinal de G.

Théorème 1.1.1 *Soit g un élément d'ordre n d'un groupe G. Pour tout entier naturel m, l'ordre de g^m est $n/(n,m)$, où (m,n) est le pgcd de m et n. En particulier, si G est un groupe cyclique d'ordre n et g un générateur de G, alors l'ensemble des générateurs de G est*

$$\{g^t : (t,n) = 1\}.$$

Preuve : Soit $d = (n,m)$ le pgcd de m et n, et écrivons $n = n'd$ et $m = m'd$. L'ordre de g^m est le plus petit entier naturel non nul k tel que

$$n|km \text{ ou encore } n'|km'.$$

Comme n' et m' sont premiers entre eux, la condition $n'|km'$ est satisfaite si et seulement si k est un multiple de $n' = n/d = n/(n,m)$. Ceci prouve le premier point.

L'élément g^t est générateur si et seulement si son ordre est n. Or d'après ce qui précède, l'ordre de g^t est $n/(n,t)$. On obtient donc que g^t est générateur si et seulement si $(t,n) = 1$.

□

Un autre résultat sur les groupes finis sera aussi utilisé.

Lemme 1.1.2 *Soient G un groupe fini commutatif et g, h deux éléments de G d'ordre respectif n et m. Si n et m sont premiers entre eux, alors l'élément gh est d'ordre mn.*

Preuve : Considérons l'intersection $M = \langle g \rangle \cap \langle h \rangle$. C'est un sous-groupe de $\langle g \rangle$ et $\langle h \rangle$. Le théorème de Lagrange implique alors que le cardinal de M divise n et m. Comme $(n,m) = 1$, on en déduit que nécessairement $M = \{e\}$. Vérifions maintenant que gh est d'ordre mn. Tout d'abord comme $gh = hg$, on a $(gh)^{mn} = g^{mn}h^{mn} = e$. Donc l'ordre de gh divise mn. Réciproquement si $(gh)^k = e$ alors $g^k = h^{-k} \in M$. Donc $g^k = h^k = e$. Ainsi $n|k$ et $m|k$. Une application du théorème 5.5.3 implique alors que le produit nm divise k. Finalement on conclut que l'ordre de gh est mn.

□

1.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Soient $n \geq 2$ un entier fixé. On dit que les entiers a et b sont **congrus modulo** n, et on écrit

$$a \equiv b \,(\mathrm{mod}\, n),$$

si $a - b$ est un multiple de n. On vérifie que la relation $\equiv$ est une relation d'équivalence sur $\mathbb{Z}$ compatible avec l'addition et la multiplication, c'est-à-dire que si $a \equiv a' \pmod{n}$ et si $b \equiv b' \pmod{n}$, alors

$$a + b \equiv a' + b' \pmod{n} \quad \text{et} \quad ab \equiv a'b' \pmod{n}.$$

Pour tout entier a, on note $a \bmod n$ la **classe de congruence** de a modulo n, et s'il n'y a pas d'ambiguité, on utilisera aussi la notation $\bar{a}$. Autrement dit,

$$a \bmod n = \bar{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}.$$

On note $\mathbb{Z}/n\mathbb{Z}$ le quotient de $\mathbb{Z}$ avec cette relation d'équivalence.

Pour $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$, on pose

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{et} \quad \bar{a}.\bar{b} = \overline{ab}.$$

On vérifie alors que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif unitaire. De plus, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est l'unique groupe cyclique à n éléments (à isomorphisme près) : il est engendré par $\bar{1}$, à savoir

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \ldots, \overline{n-1}\}.$$

1.3 Congruences linéaires et théorème des restes chinois

Le théorème suivant, bien qu'élémentaire, est très utile pour résoudre des congruences linéaires.

Théorème 1.3.1 *Soient $a, b \in \mathbb{Z}$, $n \geq 2$. Soit $d = (a, n)$ le pgcd de a et n. L'équation*

$$ax \equiv b \pmod{n} \tag{1.1}$$

a (au moins) une solution si et seulement si d divise b. Si d divise b, alors l'équation (1.1) a exactement d solutions entières modulo n.

Preuve : L'équation (1.1) possède une solution si et seulement s'il existe $x, y \in \mathbb{Z}$ tels que

$$ax - b = ny,$$

ou de manière équivalente

$$b = ax - ny.$$

Comme $(a, n) = d$, la dernière équation admet des solutions si et seulement si d divise b (voir appendice, théorème 5.4.1).

Maintenant si x et x_1 sont solutions de (1.1), on a

$$a(x_1 - x) = ax_1 - ax \equiv 0 \pmod{n},$$

d'où

$$a(x_1 - x) = nz$$

pour un certain entier z. On a alors $\frac{a}{d}(x_1 - x) = \frac{n}{d}z$. Comme $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, le lemme de Gauss implique alors que $\frac{n}{d}$ divise $x_1 - x$. D'où $x_1 = x + k\frac{n}{d}$ pour un certain $k \in \mathbb{Z}$. Autrement dit

$$x_1 \equiv x \left(\mathrm{mod}\, \frac{n}{d}\right).$$

De plus, chaque entier x_1 de cette forme est une solution de (1.1). Remarquons maintenant que les d entiers

$$x + i\frac{n}{d}, \qquad 0 \leq i \leq d-1,$$

sont deux à deux incongrus modulo n. En conséquence, l'équation (1.1) possède d solutions entières modulo n.

□

On en déduit immédiatement le corollaire suivant :

Corollaire 1.3.2 *Soient $a, b \in \mathbb{Z}$, $n \geq 2$ et supposons que $(a, n) = 1$. L'équation $ax \equiv b \pmod{n}$ a une unique solution modulo n.*

Dans la suite, nous allons nous intéresser au système de congruences suivant :

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \qquad \vdots \\ x \equiv a_k \pmod{m_k}, \end{cases}$$

où $k \geq 2$, $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ et $m_1, m_2, \ldots, m_k$ sont des entiers ≥ 2.

Commençons par le cas $k = 2$.

Théorème 1.3.3 (des restes chinois) *Soient $a, b \in \mathbb{Z}$ et $m, n \geq 2$. Le système*

$$(S) \begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

admet une solution x si et seulement si

$$a \equiv b \pmod{(m, n)}.$$

De plus, dans ce cas, si x est une solution du système (S), alors y est une solution de (S) si et seulement

$$y \equiv x \pmod{[m, n]}\ [1].$$

1. Dans tout le cours, $[m, n]$ désigne le ppcm de m et n et (m, n) désigne le pgcd de m et n.

Preuve : Si x est solution du système (S), alors il existe deux entiers u, v tels que $x = a + mu = b + nv$. D'où

$$a - b = nv - mu \equiv 0 \,(\mathrm{mod}(m, n)).$$

Réciproquement, si $a \equiv b \,(\mathrm{mod}(m, n))$, alors par la relation de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $a - b = nv - mu$. D'où $x := a + mu = b + nv$ est une solution du système (S). Cela conclut la première partie du théorème. Maintenant si x est une solution de (S), alors un entier y est solution de (S) si et seulement si

$$\begin{cases} y \equiv a \equiv x \,(\mathrm{mod}\, m) \\ y \equiv b \equiv x \,(\mathrm{mod}\, n) \end{cases}.$$

Par conséquent, $y - x$ est un multiple de m et n, donc de $[m, n]$. Autrement dit, $y \equiv x \,(\mathrm{mod}[m, n])$. Réciproquement, si $y \equiv x \,(\mathrm{mod}[m, n])$, alors $y \equiv x \,(\mathrm{mod}\, m)$ et $y \equiv x \,(\mathrm{mod}\, n)$. Donc y est solution de (S).

□

Remarque 1.3.4 On voit d'après la preuve du théorème 1.3.3 que si $a \equiv b \,(\mathrm{mod}(m, n))$, alors on construit une solution particulière du système (S) de la façon suivante. En utilisant l'algorithme d'Euclide, on commence par chercher une solution au système de Bezout suivant $d = mu + nv$ où $d = (m, n)$. Ensuite comme $a \equiv b \,(\mathrm{mod}\, d)$, il existe $k \in \mathbb{Z}$ tel que $a = b + dk$. Il suffit alors de considérer $x_0 = b + nkv$. L'ensemble des solutions du système (S) est alors donné par $x_0 \,\mathrm{mod}([m, n])$.

Théorème 1.3.5 (des restes chinois) *Soient k un entier ≥ 2, $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ et $m_1, m_2, \ldots, m_k$ des entiers ≥ 2. Supposons que les entiers $m_1, m_2, \ldots, m_k$ soient deux à deux premiers entre eux. Notons $m = m_1 m_2 \ldots m_k$. Alors le système*

$$(S) \begin{cases} x \equiv a_1 \,(\mathrm{mod}\, m_1) \\ x \equiv a_2 \,(\mathrm{mod}\, m_2) \\ \vdots \\ x \equiv a_k \,(\mathrm{mod}\, m_k), \end{cases}$$

possède une solution. De plus, si x est une solution du système (S), un entier y est aussi solution de (S) si et seulement si $y \equiv x \,(\mathrm{mod}\, m)$.

Preuve : On raisonne par récurrence sur l'entier k. Le cas $k = 2$ provient du lemme car $(m_1, m_2) = 1$ et $[m_1, m_2] = m_1 m_2$. Soit $k \geq 3$ et supposons que le résultat soit vrai pour $k - 1$ congruences. Alors il existe un entier z tel que $z \equiv a_i \,(\mathrm{mod}\, m_i)$, $1 \leq i \leq k - 1$. Comme $m_1, m_2, \ldots, m_k$ sont des entiers deux à deux premiers entre eux, on a $(m_1 m_2 \ldots m_{k-1}, m_k) = 1$. Donc le cas $k = 2$ permet de dire qu'il existe un entier x tel que

$$\begin{cases} x \equiv z \,(\mathrm{mod}\, m_1 m_2 \ldots m_{k-1}) \\ x \equiv a_k \,(\mathrm{mod}\, m_k). \end{cases}$$

D'où $x \equiv a_i \pmod{m_i}$, pour tout $1 \leq i \leq k$. Ainsi x est solution de (S). Ceci prouve la première partie du théorème. Maintenant, si y est une solution du système, alors $x - y$ est divisible par m_i, $1 \leq i \leq k$. Comme $m_1, m_2, \ldots, m_k$ sont deux à deux premiers entre eux, l'entier $x - y$ est divisible par $m_1 m_2 \ldots m_k$. Cela complète la preuve du résultat.

□

Remarque 1.3.6 Pour résoudre le système (S), on peut procéder de la façon suivante : pour chaque entier i, les entiers m_i et $\hat{m}_i = \frac{m}{m_i} = m_1 \ldots m_{i-1} m_{i+1} \ldots m_k$ sont premiers entre eux et donc d'après le théorème de Bezout, on peut trouver (en utilisant par exemple l'algorithme d'Euclide) des entiers u_i et v_i tels que $u_i m_i + v_i \hat{m}_i = 1$. Si on pose $e_i = v_i \hat{m}_i$, alors on a

$$e_i \equiv 1 \pmod{m_i}$$

et

$$e_i \equiv 0 \pmod{m_j} \text{ pour } j \neq i.$$

Une solution particulière de (S) est alors donnée par $x_0 = \sum_{i=1}^{k} a_i e_i$. Les autres solutions sont congrues à ce x_0 modulo m.

On peut donner une formulation plus abstraite du théorème des restes chinois.

Corollaire 1.3.7 *Soient $m_1, m_2, \ldots, m_k \geq 2$ des entiers deux à deux premiers entre eux et notons $m = m_1 m_2 \ldots m_k$. Alors l'application*

$$\begin{array}{rccc} \psi : & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \\ & x \bmod m & \longmapsto & (x \bmod m_1, \ldots, x \bmod m_k) \end{array}$$

définit un isomorphisme d'anneaux unitaires.

Preuve : Remarquons tout d'abord que si $x \bmod m = y \bmod m$, alors $x \bmod m_i = y \bmod m_i$ pour tout $1 \leq i \leq k$, donc l'application ψ est bien définie. On vérifie que

$$\psi(x \bmod m + y \bmod m) = \psi(x \bmod m) + \psi(y \bmod m),$$

$$\psi((x \bmod m)(y \bmod m)) = \psi(x \bmod m)\psi(y \bmod m),$$

et $\psi(1_{\mathbb{Z}/m\mathbb{Z}}) = 1_{\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}}$. Donc ψ est un morphisme d'anneaux unitaires. De plus, étant donné $(a_1 \bmod m_1, a_2 \bmod m_2, \ldots, a_k \bmod m_k) \in \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$, il existe d'après le théorème des restes chinois un élement $x \in \mathbb{Z}$ tel que

$$x \equiv a_i \pmod{m_i} \qquad 1 \leq i \leq k.$$

D'où $x \bmod m_i = a_i \bmod m_i$, $1 \leq i \leq k$, c'est-à-dire

$$\psi(x \bmod m) = (a_1 \bmod m_1, a_2 \bmod m_2, \ldots, a_k \bmod m_k).$$

De plus, le théorème des restes chinois implique également que la solution x est unique modulo m. Ainsi ψ est un isomorphisme d'anneaux unitaires.

□

1.4 Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ et l'indicatrice d'Euler

L'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ muni de la multiplication est un groupe. On le note $(\mathbb{Z}/n\mathbb{Z})^*$. Le résultat suivant caractérise ses éléments inversibles.

Proposition 1.4.1 *Pour que l'élément $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ soit inversible il faut et il suffit que $(a, n) = 1$. Dans ce cas, le calcul de l'inverse de $\bar{a}$ se fait à l'aide de l'algorithme d'Euclide étendu appliqué au couple (a, n).*

Preuve : Si $\bar{a}$ est inversible, il existe $\bar{b}$ tel que $\bar{a}\bar{b} = \bar{1}$. Il existe donc $v \in \mathbb{Z}$ tel que $ab - 1 = vn$, ou $ba - vn = 1$. Par le théorème de Bezout, a et n sont premiers entre eux. Réciproquement, si a et n sont premiers entre eux, il existe u et v entiers tels que $au + nv = 1$. Cela donne dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{au} = \overline{1 - nv} = \bar{1}$. Donc $\bar{a}$ est inversible, d'inverse $\bar{u}$.

□

On obtient immédiatement le corollaire suivant.

Corollaire 1.4.2 *Pour que l'anneau $\mathbb{Z}/p\mathbb{Z}$ soit un corps il faut et il suffit que p soit un nombre premier. On note parfois $\mathbf{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ lorsque p est premier.*

La fonction **indicatrice d'Euler** φ associe à un entier $n \geq 2$ l'entier $\varphi(n)$ défini par

$$\varphi(n) = \operatorname{card}\left((\mathbb{Z}/n\mathbb{Z})^*\right).$$

Autrement dit, d'après la proposition 1.4.1, on a

$$\varphi(n) = \operatorname{card}\{a : 0 \leq a \leq n - 1 \,\&\, (a, n) = 1\}. \tag{1.2}$$

Proposition 1.4.3 *Soit p un nombre premier et $\alpha \in \mathbb{N}^*$. On a*

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

En particulier, $\varphi(p) = p - 1$.

Preuve : On a d'après (1.2)

$$\varphi(p^\alpha) = \text{card}\{a : 0 \leq a \leq p^\alpha - 1 \,\&\, (a, p^\alpha) = 1\}.$$

On vérifie facilement que si $0 \leq a \leq p^\alpha - 1$, alors $(a, p^\alpha) > 1$ si et seulement si $p|a$. Or les multiples de p dans l'intervalle $[\![0, p^\alpha - 1]\!]$ sont

$$0, p, 2p, \ldots, p(p^{\alpha-1} - 1).$$

Il y en a donc $p^{\alpha-1}$. D'où $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

□

Lemme 1.4.4 *Soient $m, n \geq 2$. Si $(m, n) = 1$, alors $\varphi(mn) = \varphi(n)\varphi(m)$.*

Preuve : Remarquons que si A_1, A_2, A_3 sont trois anneaux unitaires tel qu'il existe un isomorphisme $\psi : A_1 \longrightarrow A_2 \times A_3$, alors $\psi(A_1^*) = A_2^* \times A_3^*$, où A_i^* désigne le groupe des éléments inversibles de A_i, $i = 1, 2, 3$. En particulier, A_1^* est isomorphe à $A_2^* \times A_3^*$. Il suffit de combiner ce résultat et le corollaire 1.3.7 pour obtenir que les groupes $(\mathbb{Z}/mn\mathbb{Z})^*$ et $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ sont isomorphes. Ils ont donc même cardinal, ce qui donne le résultat.

□

Théorème 1.4.5 *Soit $n \geq 2$. On a*

$$\varphi(n) = n \prod_{\substack{p \in \mathbb{P} \\ p|n}} \left(1 - \frac{1}{p}\right),$$

où $\mathbb{P}$ désigne l'ensemble des nombres premiers.

Preuve : Soit $n = p_1^{r_1} \ldots p_k^{r_k}$ la décomposition canonique de n en produits de facteurs premiers. D'après le lemme 1.4.4, on a

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{r_i}).$$

Or, avec la proposition 1.4.3, $\varphi(p_i^{r_i}) = p^{r_i} - p_i^{r_i - 1} = p_i^{r_i}(1 - \frac{1}{p_i})$, ce qui donne

$$\varphi(n) = \prod_{i=1}^{k} p_i^{r_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

□

1.5 Un théorème d'Euler et de Fermat

Théorème 1.5.1 (Euler) *Soient $n \geq 2$ et $a \in \mathbb{Z}$ tel que $(a, n) = 1$. Alors*

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

Preuve : On sait que l'ordre du sous-groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est $\varphi(n)$. D'autre part, comme $(a, n) = 1$, la proposition 1.4.1 implique que $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et donc est un élément de $(\mathbb{Z}/n\mathbb{Z})^*$. Le théorème de Lagrange affirme alors que l'ordre de $\bar{a}$ divise l'ordre de $(\mathbb{Z}/n\mathbb{Z})^*$, ce qui implique en particulier que

$$\overline{a^{\varphi(n)}} = \bar{a}^{\varphi(n)} = \bar{1}.$$

Le résultat suit immédiatement.

□

On en déduit alors ce qu'on appelle le "petit théorème de Fermat".

Théorème 1.5.2 (Fermat) *Soient p un nombre premier et $a \in \mathbb{Z}$. On a*

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

De plus, si p ne divise pas a, alors

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

Preuve : Si p est premier et ne divise pas a, alors on a $(a, p) = 1$ et $\varphi(p) = p - 1$. Le théorème d'Euler implique alors que

$$a^{p-1} = a^{\varphi(p)} \equiv 1 \pmod{p}.$$

En multipliant cet congruence par a, on obtient que $a^p \equiv a \pmod{p}$. Si p divise a, alors on a clairement

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

□

1.6 Sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$

La description des sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ est assez simple. Comme ici le groupe est additif, il faut prendre garde au fait que l'ordre d'un élément $x \bmod n$ est défini comme le plus petit entier $d \geq 1$ tel que $dx \equiv 0 \pmod{n}$. De plus, dans ce cas, les éléments $\bar{0}, \bar{x}, \overline{2x}, \ldots, \overline{(d-1)x}$ sont tous distincts et

$$\langle x \rangle = \{\bar{0}, \bar{x}, \overline{2x}, \ldots, \overline{(d-1)x}\}$$

est le plus petit sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$ contenant $\bar{x}$. De plus, si $k \geq 1$, on a

$$k\bar{x} = \bar{0} \Longleftrightarrow k|d.$$

Lemme 1.6.1 *Soient x un entier et $n \geq 2$. L'élément $x \bmod n$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z},+)$ si et seulement si $x \bmod n$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

Preuve : Supposons que $x \bmod n$ soit un générateur du groupe $(\mathbb{Z}/n\mathbb{Z},+)$. Alors

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{x}, \overline{2x}, \ldots, \overline{(n-1)x}\}$$

et donc il existe un entier $0 \leq k \leq n-1$ tel que $k\bar{x} = \bar{k}\bar{x} = \bar{1}$. D'où $x \bmod n$ est inversible d'inverse $k \bmod n$. Réciproquement, supposons que $x \bmod n$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et notons d l'ordre de $x \bmod n$ dans le groupe $(\mathbb{Z}/n\mathbb{Z},+)$. Alors $dx \equiv 0 \,(\bmod n)$. Autrement dit, n divise dx. Comme $x \bmod n$ est inversible, on a d'après la proposition 1.4.1, $(x,n) = 1$. Le lemme de Gauss implique alors que n divise d. Mais d'autre part, d'après le théorème de Lagrange, d divise n et donc $d = n$. Finalement on obtient que $x \bmod n$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z},+)$.

□

On déduit en particulier du lemme 1.6.1 que

$$\varphi(n) = \text{card}\{g : g \text{ générateur de } (\mathbb{Z}/n\mathbb{Z},+)\}. \tag{1.3}$$

Proposition 1.6.2 *Soit $n \geq 2$. Pour chaque entier $d \geq 1$ divisant n, il existe un unique sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$ d'ordre d, c'est le sous-groupe cyclique engendré par la classe de $\frac{n}{d}$ dans $\mathbb{Z}/n\mathbb{Z}$.*

Preuve : Supposons que $n = kd$. Alors l'élément $x = \bar{k}$ est d'ordre d. En effet, d'une part, on a

$$dx = d\bar{k} = \overline{dk} = \bar{n} = \bar{0}.$$

D'autre part, si $cx = 0$, alors $\overline{ck} = \bar{0}$. Autrement dit, n divise ck. Ceci implique que d divise c. Par conséquent, x est bien d'ordre d. Ainsi, le sous-groupe $\langle x \rangle$ est d'ordre d. Montrons que c'est le seul. Soit donc H un sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$ d'ordre d. Notons $s : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ la surjection canonique. On sait que $s^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$. Donc il existe un entier $m \in \mathbb{N}$ tel que $s^{-1}(H) = m\mathbb{Z}$. Par conséquent, s étant surjective, on a $H = s(s^{-1}(H)) = s(m\mathbb{Z}) = \langle \bar{m} \rangle$. Comme l'ordre de H est d, on a $d\bar{m} = \bar{0}$. Donc $n|dm$, c'est-à-dire $k|m$. Ceci implique que $H = \langle \bar{m} \rangle \subset \langle \bar{k} \rangle$. Or l'ordre du sous-groupe engendré par $\bar{k}$ est d'ordre d, ce qui implique que

$$H = \langle \bar{k} \rangle.$$

□

Corollaire 1.6.3 *Soit $n \geq 2$. On a*

$$n = \sum_{d|n} \varphi(d).$$

Preuve : On écrit

$$\mathbb{Z}/n\mathbb{Z} = \bigcup_{d|n} E_d,$$

où $E_d = \{x \bmod n : x \bmod dn \text{ est d'ordre } d\}$ et la réunion est disjointe. D'où

$$n = \sum_{d|n} \text{card}(E_d).$$

Or $x \bmod n \in E_d$ si et seulement si $x \bmod n$ est générateur d'un sous-groupe d'ordre d et d'après la proposition 1.6.2, ce sous-groupe d'ordre d est unique et isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Ainsi avec (1.3), on obtient que

$$\text{card}(E_d) = \text{card}\{g : g \text{ générateur de } (\mathbb{Z}/n\mathbb{Z}, +)\} = \varphi(d),$$

ce qui donne le résultat.

□

1.7 Exercices

Exercice 1.7.1 Calculer l'inverse de 13 modulo 100.

Exercice 1.7.2 Résoudre les équations

$$19x \equiv 2 \pmod{140} \qquad \text{et} \qquad 57x \equiv 87 \pmod{105}.$$

Exercice 1.7.3 Résoudre $42x + 150y = 18$.

Exercice 1.7.4

1. Résoudre $6u + 5z = 10$.
2. Résoudre $4x + 5y = u$.
3. En déduire les solutions de $24x + 30y + 5z = 10$.

Exercice 1.7.5 Soit p un nombre premier. Montrer que

$$x^2 \equiv 1 \,(\text{mod}\, p)$$

si et seulement si

$$x \equiv \pm 1 \,(\text{mod}\, p).$$

Exercice 1.7.6 (Théorème de Wilson) Soit p un nombre premier. Montrer que

$$(p-1)! \equiv -1 \,(\mathrm{mod}\, p).$$

Indication : vérifier d'abord le résultat pour $p = 2, 3$. On suppose alors que $p \geq 5$. Montrer que pour tout $a \in \{1, 2, \ldots, p-1\}$, il existe $a^\sharp \in \{1, 2, \ldots, p-1\}$ tel que $aa^\sharp \equiv 1 \,(\mathrm{mod}\, p)$. Remarquer alors que $a = a^\sharp$ si et seulement si $a = 1$ ou $a = p-1$ (voir exercice 1.7.5). Partitionner alors l'ensemble $\{2, \ldots, p-2\}$ en $(p-3)/2$ pairs d'entiers $(a_i, a_i^\sharp)$ tels que $a_i a_i^\sharp \equiv 1 \,(\mathrm{mod}\, p)$ pour $1 \leq i \leq (p-3)/2$. Conclure.

Exercice 1.7.7 Le produit de trois entiers consécutifs peut–il être un carré ?

Exercice 1.7.8

1. Montrer que, pour tout $n \in \mathbb{N}$, $n^{13} - n$ est multiple de 455.
2. Montrer qu'on peut améliorer ce résultat, c'est-à-dire qu'il existe un multiple non trivial de 455 qui divise tous les $n^{13} - n$.
3. En admettant que si p est un nombre premier, il existe un élément d'ordre $p-1$ dans $\mathbf{F}_p$, quel est le plus grand entier m qui divise tous les $n^{13} - n$?

Exercice 1.7.9 On définit la suite des nombres de Fermat par $F_n = 2^{2^n} + 1$.

1. Montrer que les F_n sont deux à deux premiers entre eux.

   Indication : si $m < n$ alors F_m divise $F_n - 2$.
2. En déduire qu'il existe une infinité de nombres premiers.

Exercice 1.7.10 Prouver qu'il existe une infinité de premiers de la forme $4k - 1$. Prouver de la même façon qu'il existe une infinité de nombres premiers de la forme $6k - 1$.

Exercice 1.7.11 Expliciter un n tel que $n, n+1, n+2, \ldots, n+9$ soient tous non premiers.

Indication : on pourra traduire le problème comme un système de congruences et utiliser le théorème des restes chinois.

Exercice 1.7.12 a et b sont premiers entre eux et $N \in \mathbb{N}$. On considère l'équation

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

1. Montrer que si N est assez grand l'équation (E) a une solution en entiers naturels.
2. Montrer que si $N = (a-1)(b-1) - 1$ l'équation (E) n'a pas de solutions en entiers naturels.

3. Montrer que si $N \geq (a-1)(b-1)$ l'équation (E) a une solution en entiers naturels.

Exercice 1.7.13 Soient $x_1, x_2, \ldots, x_n$ des entiers relatifs. Montrer qu'il existe i, j entiers, $1 \leq i < j \leq n$ tels que $x_i + x_{i+1} + \cdots + x_j \equiv 0 \pmod{n}$.

Indication : on pourra introduire

$$S_j = \sum_{0<i\leq j} x_j \bmod n$$

et appliquer le principe des tiroirs de Dirichlet.

Exercice 1.7.14 Vérifier que les 4 derniers chiffres (en base 10) de 9376^2 sont 9376. Déterminer tous les entiers x, $0 \leq x < 10000$ tels que $x^2 \equiv x \pmod{10000}$?

Indication : on pourra remarquer que x est solution de $X^2 - X \equiv 0 \pmod{N}$ si et seulement si $1 - x$ est solution.

Exercice 1.7.15 Résoudre le système de congruences

$$\begin{cases} 2x & \equiv & 3 & \pmod 5 \\ 4x & \equiv & 3 & \pmod 7 \\ 3x & \equiv & 5 & \pmod 8 \end{cases}$$

Exercice 1.7.16 Trouver les deux derniers chiffres de $39^{39^{39}}$. Même question avec $17^{17^{17}}$.

Exercice 1.7.17 Montrer que si n est impair alors $n \mid 2^{n!} - 1$.

Exercice 1.7.18 Pour un nombre réel x, on désigne par $\lfloor x \rfloor$ la partie entière de x, c'est-à-dire le plus petit entier k satisfaisant

$$k \leq x < k + 1.$$

Si $a \in \mathbb{Z}^*$ et p est un nombre premier, on appelle **valuation p-adique de a** le plus grand entier $\alpha \in \mathbb{N}$ tel que a est divisible par p^α mais pas par $p^{\alpha+1}$.

Soit n un entier positif ou nul.

1. Démontrer la formule de Legendre :

$$v_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots \lfloor \frac{n}{p^k} \rfloor + \cdots$$

2. Prouver que chacun des termes de la suite $\left(\lfloor \frac{n}{p^k} \rfloor \right)$ est le quotient de la division euclidienne du précédent par p.

Exercice 1.7.19 Soit $n \geq 2$ un entier et $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ sa décomposition en produit de facteurs premiers, où $p_1 < p_2 < \dots < p_k$.

1. Montrer que $k \leq \dfrac{\log n}{\log 2}$.
2. Pour $1 \leq i \leq k$, montrer que $p_i \geq i + 1$.
3. En déduire que
$$\varphi(n) \geq \frac{\log 2}{2} \frac{n}{\log n}.$$

Exercice 1.7.20 Un nombre entier m est appelé un **nombre de Carmichael** s'il vérifie les deux propriétés suivantes :

(i) m n'est pas premier ;

(ii) pour tout entier a premier avec m, on a
$$a^{m-1} \equiv 1 \pmod{m}.$$

Démontrer que $m = 561$ est un nombre de Carmichael (c'est en fait le plus petit nombre de Carmichael).

Indication : on pourra utiliser le théorème des restes chinois.

Exercice 1.7.21 Soit m entier tel que $6m + 1$, $12m + 1$, $18m + 1$ soient premiers. Démontrer que $n = (6m + 1)(12m + 1)(18m + 1)$ est un nombre de Carmichael.

Exercice 1.7.22 Soit n un entier non premier tel que

1. n est impair, sans facteurs carrés.
2. Pour tout diviseur premier p de n, $p - 1$ divise $n - 1$.

Démontrer que n est un nombre de Carmichael.

Exercice 1.7.23 Le but de cet exercice est de démontrer que la condition suffisante, obtenue dans l'exercice précédent pour qu'un entier soit un nombre de Carmichael, est aussi nécessaire. Considérons donc n un entier dont la factorisation (canonique) s'écrit
$$n = \prod_{i=1}^{r} p_i^{\alpha_i},$$
et supposons que n est un nombre de Carmichael.

1. Soit a un entier premier avec n. Prouver que son ordre dans $(\mathbb{Z}/n\mathbb{Z})^*$ est un diviseur de $n - 1$.
2. Soit p un diviseur premier impair de n et $\alpha = v_p(n)$ la valuation p-adique de n.

(a) Prouver qu'il existe un entier a, premier avec n, dont l'ordre dans $(\mathbb{Z}/n\mathbb{Z})^*$ est $p^{\alpha-1}(p-1)$.

Indication : utiliser le fait que si p est un nombre premier impair, alors $(\mathbb{Z}/p^\alpha Z)^*$ est cyclique et utiliser le théorème des restes chinois.

(b) En déduire que $\alpha = 1$, que $p-1$ est un diviseur de $n-1$ et enfin que n est impair.

3. Démontrer qu'une puissance de 2 n'est jamais un nombre de Carmichael.

4. Déduire des questions précédentes que

(a) n est impair, sans facteurs carrés.

(b) Pour tout diviseur premier p de n, $p-1$ divise $n-1$.