Chapitre 3

Congruences et théorème chinois

Dans ce chapitre, nous présentons les théorèmes d'Euler, de Fermat et des restes chinois. Ces théorèmes trouvent de nombreuses applications, notamment en cryptographie. Nous commencerons par un bref rappel sur l'ordre d'un éléments avant d'exposer les théorèmes d'Euler et de Fermat. Ensuite, nous traiterons le théorème chinois et son utilisation dans la résolution des systèmes de congruences.

3.1 Ordre d'un élément

Rappelons que pour deux entiers x et m avec $m > 0$, la suite

$$1 = x^0 \mod m,\ \ x \mod m,\ \ x^2 \mod m,\ \ x^3 \mod m,\ \ \cdots,\ \ x^m \mod m$$

comporte toujours une collision ; c'est à dire, il existe toujours $i, j \in \{0, \cdots, m\}$ tels que $i \neq j$ et $x^i = x^j \mod n$. En effet, on a $m+1$ entiers modulo m, puisque le nombre de classes d'équivalences modulo m est m, on a nécessairement au moins deux de ces entiers qui partagent la même classe d'équivalence. De cette observation, on déduit le résultat suivant.

Proposition 1. Soient a et $m > 0$ deux entiers. Si a et m sont *premiers entre eux*, alors il existe $t \in \{1, \cdots, m-1\}$ tel que $a^t = 1 \mod m$.

Preuve. Puisque a et m sont premiers entre eux, pour tout entier $s > 0$, $m \nmid a^s$. Ainsi, les classes de congruence des m entiers $1, a, a^2, \cdots, a^{m-1}$ sont toutes différentes de $\bar{0}$. Ainsi, deux de ces entiers sont nécessairement dans la même classe d'équivalence. Il existe donc $s \geqslant 0$ et $0 < t < m-1$ tels que $a^s = a^{s+t} \mod m$. Puisque a et m sont premiers entre eux, on obtient $a^t = 1 \mod m$. □

Remarque 1. On notera que, d'après la proposition ci–dessus, si $\bar{a}$ est inversible dans l'anneau $\mathbb{Z}/m\mathbb{Z}$, alors il existe $t \in \{1, \cdots, m-1\}$ tel que $\bar{a}^t = \bar{1}$.

Définition 1. Soient a et $m \geqslant 2$ deux entiers *premiers entre eux*. On définit *l'ordre de a modulo m* comme étant le plus petit entier positif t tel que $a^t = 1 \mod m$. En d'autres termes, c'est le plus petit positif t tel que $m \,|\, (a^t - 1)$.

Exemple 1. Pour $m = 7$,
- l'ordre de 1 est 1 ;
- l'ordre de 2 est 3 car $\bar{2}^1 = \bar{2} \neq \bar{1}$, $\bar{2}^2 = \bar{4} \neq \bar{1}$, $\bar{2}^3 = \bar{8} = \bar{1}$;
- l'ordre de 3 est 6 (la vérification est laissée au lecteur).

Remarque 2. L'ordre de a modulo m est l'ordre de $\bar{a}$ dans le groupe multiplicatif $(\mathbb{Z}/m\mathbb{Z} \setminus \{0\}, \cdot\,)$.

En utilisant la division euclidienne, on montre la proposition suivante dont la preuve est laissée en exercice.

Proposition 2. Soient a et $m \geqslant 2$ deux entiers premiers entre eux. Si t est l'ordre de a modulo m, pour tout entier s, si $a^s = 1 \mod m$ alors $t \mid s$.

Dans le précédent chapitre, nous avons vu l'algorithme d'Euclide qui permet de calculer de façon efficace le pgcd d'un ensemble fini d'entiers. Étant donné l'ordre de a modulo m, le résultat suivant permet de calculer de façon efficace l'ordre de a^d modulo m.

Proposition 3. Soient a et $m \geqslant 2$ deux entiers premiers entre eux et d un entier strictement positif. Si t est l'ordre de a modulo m et $g = \mathsf{pgcd}(d, t)$, alors l'ordre de a^d modulo m est $\dfrac{t}{g}$.

Preuve. Rappelons que

$$\mathsf{pgcd}(t, d) \cdot \mathsf{ppcm}(t, d) = td.$$

Soit $l = \mathsf{ppcm}(t, d)$. Puisque $t \mid l$, on a

$$a^l = 1 \mod m.$$

Ainsi,

$$\left(a^d\right)^{\frac{l}{d}} = 1 \mod m.$$

Ainsi, l'ordre modulo m de a^d divise $\dfrac{l}{d}$.
Soit $s > 0$ tel que $\left(a^d\right)^s = 1 \mod m$; on a alors $a^{ds} = 1 \mod m$. Ainsi, ds est un multiple de t, et donc un multiple commun de t et d. Donc de la définition de $l = \mathsf{ppcm}(t, d)$, on a ainsi nécessairement $ds \geqslant l$, ou encore $s \geqslant \dfrac{l}{d}$. Ainsi, l'ordre de a^d modulo m est $\dfrac{l}{d}$; puisque $\dfrac{l}{d} = \dfrac{t}{g}$, le résultat est démontré. □

3.2 Théorème de Fermat

Nous avons vu au chapitre 3 du *cours d'algèbre 1* que pour tout entier n, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. De ce résultat, on démontre le théorème suivant.

Théorème 1 (Fermat)**.** Si p un nombre premier et a un entier non divisible par p, alors

$$a^{p-1} = 1 \mod p.$$

Autrement dit, si $\bar{a}$, la classe de a dans $\mathbb{Z}/p\mathbb{Z}$, est non–nulle, alors

$$\bar{a}^{p-1} = \bar{1};$$

ou encore,

$$p \mid a^{p-1} - 1.$$

Preuve. Si a n'est pas divisible par p, alors la classe de a modulo p est distincte de $\bar{0}$; $\bar{a}$ est donc inversible dans $\mathbb{Z}/p\mathbb{Z}$. Soit $F = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$. L'application φ_a de F vers F qui a $\bar{x}$ associe $\bar{a}\bar{x}$ est bijective, car injective. On a donc

$$\prod_{\bar{x}\in F} \bar{a}\bar{x} \;=\; \prod_{\bar{x}\in F} \bar{x}.$$

Or,

$$\prod_{\bar{x}\in F} \bar{a}\bar{x} = \bar{a}^{p-1} \prod_{\bar{x}\in F} \bar{x};$$

on déduit

$$\bar{a}^{p-1} = \overline{a^{p-1}} = \bar{1},$$

ou encore $a^{p-1} = 1 \mod p$, ce qui démontre le résultat. □

Le corollaire suivant facilite la recherche de l'ordre d'un élément dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \cdot\,)$.

Corollaire 1. Pour tout $\bar{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, l'ordre de $\bar{a}$ dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \cdot\,)$ divise $p-1$.

Exemple 2. Déterminons l'ordre de $\bar{7}$ dans le groupe multiplicatif $\mathbb{Z}/11\mathbb{Z} \setminus \{0\}$.
D'après le corollaire ci–dessus, l'ordre de $\bar{7}$ divise 10. Les valeurs possible sont donc $1, 2, 5$ et 10. On peut écarter 1, du fait que $\bar{7}^1 = \bar{7} \neq \bar{1}$. On calcule, $\bar{7}^2 = \bar{49} = \bar{5} \neq \bar{1}$; la valeur 2 est écartée aussi. Vérifions pour 5, on a $\bar{7}^5 = \bar{7}^2 \cdot \bar{7}^2 \cdot \bar{7} = \bar{5} \cdot \bar{5} \cdot \bar{7} = \bar{3} \cdot \bar{7} = \bar{10} \neq \bar{1}$. On déduit que l'ordre de $\bar{7}$ est 10.

3.3 Théorème d'Euler

Nous avons vu dans les sections précédentes que si a et $m > 0$ sont des entiers premiers entre aux, alors il existe t tel que $a^t = 1 \mod m$. D'après le théorème de Fermat, dans le cas où m est premier, la valeur $t = m - 1$ convient. L'objet de cette section est de déterminer une valeur de t qui convient dans le cas où m est composite.

Définition 2. Pour tout entier m, on $\phi(m)$ le nombre d'inversibles (par rapport à la loi $\cdot$) dans $\mathbb{Z}/m\mathbb{Z}$. Autrement dit, $\phi(m)$ est le cardinal de l'ensemble des entiers r qui vérifient $0 \leqslant r \leqslant m$ et $\mathsf{pgcd}(m, r) = 1$. La fonction ϕ est dite fonction ϕ d'Euler.

Une adaptation simple du théorème de Fermat donne le résultat suivant dont la preuve est laissée en exercice.

Théorème 2 (Euler)**.** Soit $m \geqslant 2$ un entier naturel. Pour tout élément $\bar{a}$ de $\mathbb{Z}/m\mathbb{Z}$, si $\bar{a}$ est inversible dans $\mathbb{Z}/m\mathbb{Z}$, alors $\bar{a}^{\phi(m)} = \bar{1}$.

La proposition suivante permet de calculer $\phi(m)$ dans le cas où l'on dispose d'une factorisation de m.

Proposition 4.
(a) Pour tout premier p et pour tout entier $e > 0$, $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$;

(b) si a et b sont deux entiers premiers entre eux, alors $\phi(ab) = \phi(a)\phi(b)$.

Preuve. (a) Les entiers plus petits que p^e et qui ne lui sont pas premiers sont les multiples de p. Ainsi, l'ensemble de ces entiers est $T = \{p, 2p, 3p, \cdots, p^{e-1}p\}$, son cardinal est p^{e-1}. Tout entier strictement plus petit que p^e et n'appartenant pas à T est premier avec p^e. On déduit

$$\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1).$$

(b) On notera que ce point équivaut au fait de dire que les anneaux $\mathbb{Z}/(ab)\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ sont isomorphes. La démonstration de ce point est laissée en exercice. Chaque étudiant est invité à fournir au tuteur une démonstration.

□

3.4 Théorème chinois

Dans cette section, nous discutons des conditions dans lesquelles un système d'équations de la forme

$$\begin{cases} x &= a_1 \mod m_1 \\ \vdots & \vdots \\ x &= a_n \mod m_n \end{cases}$$

admet une solution, ainsi que du calcul effectif des solutions dans le cas où elles existent. Nous commencerons par la cas où le système contient uniquement deux équations, avant de proposer une généralisation.

Le résultat suivant permet, dans le cas où le système contient deux équations, de savoir s'il admet des solutions, et d'expliciter celles–ci (dans le cas où elles existent).

Théorème 3 (Restes chinois)**.** Soient m et n deux entiers strictement supérieurs à 1 et premiers entre eux. Pour tous entiers $a, b \in \mathbb{Z}$, le système

$$\begin{cases} x &= a \mod m \\ x &= b \mod n \end{cases} \tag{3.1}$$

admet une solution si et seulement si $\mathsf{pgcd}(m,n) \mid b-a$. De plus, si x_0 est une solution du système, pour tout $x_0' \in \mathbb{Z}$, x_0' est une solution si et seulement si

$$x_0 = x_0' \mod \mathsf{ppcm}(m,n).$$

Preuve. Supposons que x soit une solution du système (3.1). Il existe alors $s, t \in \mathbb{Z}$ tels que $x = a + sm$ et $x = b + tn$. Ainsi,

$$b - a = sm - tn.$$

De cette relation, on déduit :

– si $\mathsf{pgcd}(m,n) \nmid (b-a)$, le système n'admet pas de solution ;

– si $\mathsf{pgcd}(m,n) \mid (b-a)$, alors il existe $q \in \mathbb{Z}$ tel que $b-a = q\,\mathsf{pgcd}(m,n)$. En utilisant l'algorithme d'Euclide étendu, on calcule $u, v \in \mathbb{Z}$ tels que

$$mu + nv = \mathsf{pgcd}(m,n).$$

On obtient ainsi,

$$m(qu) + n(qv) = q\,\mathsf{pgcd}(m,n) = b-a.$$

On posant

$$x = a + (qu)m = b - (qv)n,$$

on obtient une solution de (3.1).

Ce qui démontre pa première partie du résultat.

Si x_0 et x_0' sont deux solutions de (3.1), $x_0 - x_0'$ est alors solution du système homogène

$$\begin{cases} x &= 0 \mod m \\ x &= 0 \mod n \end{cases} \tag{3.2}$$

Ainsi, $x_0 - x_0'$ est un multiple commun de m et n d'où la relation

$$x_0 = x_0' \mod \mathsf{ppcm}(m,n).$$

Réciproquement, si x_0 est une solution de (3.1) et x_0' est tel que

$$x_0 = x_0' \mod \mathsf{ppcm}(m,n),$$

alors x_0' vérifie (3.1) aussi. Le résultat est ainsi démontré. □

Exemple 3.

– Considérons le système de congruences

$$\begin{cases} x &= 11 \mod 74 \\ x &= 13 \mod 63. \end{cases} \tag{3.3}$$

Une exécution de l'algorithme d'Euclide étendu donne

$$23 \cdot 74 - 27 \cdot 63 = 1.$$

Ainsi, $\mathsf{pgcd}(74,63) = 1$ et le système admet une solution. De la relation

$$13 - 11 = 2 \cdot 1 = 2 \cdot (23 \cdot 74 - 27 \cdot 63) = (2 \cdot 23) \cdot 74 - (2 \cdot 27) \cdot 63,$$

on déduit

$$(2 \cdot 27) \cdot 63 + 13 = (2 \cdot 23) \cdot 74 + 11,$$

ou encore

$$54 \cdot 63 + 13 = 46 \cdot 74 + 11,$$

d'où l'on conclut que $x_0 = 3415$ est une solution du système (3.3). Puisque 74 et 63 sont premiers entre eux, $\mathsf{ppcm}(74, 63) = 74 \cdot 63 = 4662$, et l'ensemble des solutions du système est $3415 + 4662\,\mathbb{Z}$.

– Considérons à présent le système de congruences suivant

$$\begin{cases} x &= 5 \mod 20 \\ x &= 15 \mod 16. \end{cases} \tag{3.4}$$

On a $15 - 5 = 10$ et $\mathsf{pgcd}(20, 16) = 4$. Or $4 \nmid 10$, on conclut que le système n'admet pas de solution.

3.4.1 Système de congruences de trois équations ou plus

La méthode que nous venons de voir se généralise à un système comportant un nombre d'équations supérieur à trois. En exemple, considérons le système de congruences suivant

$$\begin{cases} x &= 2 \mod 12 \\ x &= 8 \mod 10 \\ x &= 9 \mod 13. \end{cases} \tag{3.5}$$

Si le sous–système

$$\begin{cases} x &= 2 \mod 12 \\ x &= 8 \mod 10, \end{cases} \tag{3.6}$$

constituée des deux premières équations de (3.5), n'admet pas de solutions, alors le système (3.5) n'en admet pas non plus. On a $\mathsf{pgcd}(10, 12) = 2$ et $2 \mid (8-6)$, on conclut que le système (3.6) est soluble. De l'algorithme d'Euclide étendu, on obtient

$$8 - 2 = 6 = 3 \cdot 2 = 3 \cdot (-1) \cdot 10 + 3 \cdot 1 \cdot 12.$$

D'où l'on déduit que 38 est une solution de (3.6) et que l'ensemble des solutions de ce système est $38 + 60\,\mathbb{Z}$. Ainsi, le système (3.6) est réduit à l'équation

$$x = 38 \mod 60,$$

le système (3.5) est donc équivalent au système suivant

$$\begin{cases} x &= 36 \mod 60 \\ x &= 9 \mod 10, \end{cases} \tag{3.7}$$

que nous savons résoudre.
La preuve du résultat suivant utilise un argumentaire similaire à celui que nous avons vu à travers cet exemple.

Théorème 4 (Restes chinois)**.** Si $m_1, \cdots, m_n$ des entiers positifs strictement supé-

rieurs à 1 et deux à deux premiers entre eux, alors le système de congruences

$$\begin{cases} x & = & a_1 & \mod m_1 \\ \vdots & \vdots & & \vdots \\ x_n & = & a_n & \mod m_n \end{cases} \tag{3.8}$$

admet une solution. De plus, si x_0 est une solution, alors l'ensemble des solutions est $x_0 + M\mathbb{Z}$ où $M = m_1 \cdots m_n$.

Preuve. Procédons par récurrence. Pour $n = 2$, puisque m_1 et m_2 sont premiers entre eux,

$$1 = \mathsf{pgcd}(m_1, m_2) \mid (a_2 - a_1)$$

et le système admet une solution, et si x_0 est une solution alors l'ensemble des solutions est donné par

$$x_0 + M\mathbb{Z} \text{ où } M = \mathsf{ppcm}(m_1, m_2) = m_1 m_2.$$

Supposons le résultat vrai pour tout système de $n-1$ congruences et montrons qu'il l'est alors pour tout système de n congruences. Soit

$$\begin{cases} x & = & a_1 & \mod m_1 \\ \vdots & \vdots & & \vdots \\ x_n & = & a_n & \mod m_n \end{cases} \tag{3.9}$$

un système de n congruences tel que pour tout i, j, si $i \neq j$, alors $\mathsf{pgcd}(m_i, m_j) = 1$. Puisque $\mathsf{pgcd}(m_1, m_2) = 1$, le sous–système

$$\begin{cases} x & = & a_1 & \mod m_1 \\ x_n & = & a_2 & \mod m_2 \end{cases} \tag{3.10}$$

équivaut à une équation de la forme

$$x = x_0 \mod m_1 m_2. \tag{3.11}$$

Ainsi, le système (3.10) équivaut au système

$$\begin{cases} x & = & x_0 & \mod m_1 m_2 \\ x & = & a_3 & \mod m_3 \\ \vdots & \vdots & & \vdots \\ x_n & = & a_n & \mod m_n \end{cases} \tag{3.12}$$

qui comporte $n-1$ équations. Puisque pour tout $j \in \{3, \cdots, n\}$, si $\mathsf{pgcd}(m_1, m_j) = 1$ et $\mathsf{pgcd}(m_2, m_j) = 1$, on déduit $\mathsf{pgcd}(m_1 m_2, m_j) = 1$. D'après l'hypothèse de récurrence, le système (3.12) admet une solution x_0.
Reste à montrer que l'ensemble des solutions est $x_0 + M\mathbb{Z}$ où $M = m_1 \cdots m_n$. Ce dernier point de la preuve est laissé en exercice. □