Cryptographie : Fiche

Sommaire

---

1. Bases mathématiques

1.1. Congruences

On fixe un entier $n \geq 2$.

1.1.1. Définition

> Deux entiers (relatifs) x et y sont **congrus modulo** n si n divise $x - y$
>
> Autrement dit : si x et y sont égaux à un multiple de n près.

1.1.2. Notation

- $x \equiv y \bmod n$
- $x \equiv y \ \ [n]$

1.1.3. Remarque

$$x \equiv y \ \ [n] \Leftrightarrow (\exists k \in \mathbb{Z} | y = x + 2k)$$

1.1.4. Définition

> Pour x dans $\mathbb{Z}$, on appelle **classe de x modulo n** l'ensemble
>
> $$\overline{x} = \{y \in \mathbb{Z} \ | \ y \equiv x \ \ [n]\}$$

1.1.5. Exemple

Soit $n = 2$:

- $\overline{0} = \{$ entiers pairs $\}$
- $\overline{1} = \{$ entiers impairs $\}$

1.1.6 Propriété

> Pour $n \geq 2$ quelconque, il y aura exactement n classes (de $\overline{0}$ à $\overline{n-1}$)

1.1.7. Définition

> On note $\mathbb{Z}_{/n\mathbb{Z}}$ l'ensemble des classes modulo n. $\mathbb{Z}_{/n\mathbb{Z}}$ a exactement n éléments.
>
> $\mathbb{Z}_{/n\mathbb{Z}}$ est l'anneau des entiers modulo n et on le note parfois $\mathbb{Z}_n$

1.1.8. Propriété

> On peut définir une opération $+$ sur $\mathbb{Z}_{/n\mathbb{Z}}$, en posant :
>
> $$\overline{x} + \overline{y} := \overline{x+y}$$

- Cette opération vérifie les mêmes propriétés que l'addition de $\mathbb{Z}$:
    - $\forall \overline{x}, \overline{y} \in \mathbb{Z}_{/n\mathbb{Z}},\ \ \overline{x} + \overline{y} = \overline{y} + \overline{x}$
    - $\forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_{/n\mathbb{Z}},\ \ (\overline{x} + \overline{y}) + \overline{z} = \overline{x} + (\overline{y} + \overline{z})$
    - $\exists e = \overline{0} \mid \forall \overline{x},\ \ \overline{x} + e = \overline{x}$
    - $\forall \overline{x}, \exists \overline{y} \mid \overline{x} + \overline{y} = \overline{0}$

1.1.9. Démonstration

Hypothese :

- Si $\begin{cases} \overline{x'} = \overline{x} \\ \overline{y'} = \overline{y} \end{cases}$ alors $\overline{x'+y'} = \overline{x+y}$

Vérifions :

- $\overline{x'} = \overline{x} \Leftrightarrow \exists k \in \mathbb{Z} \mid x' = x + kn$
- $\overline{y'} = \overline{y} \Leftrightarrow \exists l \in \mathbb{Z} \mid y' = y + ln$
- Alors $x' + y' = (x+y) + (k+l)n \Rightarrow \overline{x'+y'} = \overline{x+y}$

1.1.10. Propriété

> On peut faire de même pour définir la multiplication dans $\mathbb{Z}_{/n\mathbb{Z}}$:
>
> $$\overline{x} \times \overline{y} := \overline{x \times y}$$

- Cette opération vérifie ces propriétés :
    - $\forall \overline{x}, \overline{y} \in \mathbb{Z}_{/n\mathbb{Z}},\ \ \overline{x} \times \overline{y} = \overline{y} \times \overline{x}$
    - $\forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_{/n\mathbb{Z}},\ \ (\overline{x} \times \overline{y}) \times \overline{z} = \overline{x} \times (\overline{y} \times \overline{z})$
    - $\exists e = \overline{1} \mid \forall \overline{x},\ \ \overline{x} \times e = \overline{x}$
    - Il n'est pas vrai en général que $\forall \overline{x}, \exists \overline{y} \mid \overline{x} \times \overline{y} = \overline{1}$

1.1.11. Propriété

> $$\forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_{/n\mathbb{Z}},\ \ \overline{x} \times (\overline{y} + \overline{z}) = \overline{x} \times \overline{y} + \overline{x} \times \overline{z}$$

1.2. Interprétation logique

> Cas particulier : $\mathbb{Z}_{/2\mathbb{Z}} = \{\overline{0}, \overline{1}\}$

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

1.2.1. Interprétation

- $\overline{0} \rightarrow$ Faux
- $\overline{1} \rightarrow$ Vrai

- Alors
  - $+ \to XOR$
  - $\times \to AND$

1.3. Permutations d'un ensemble à n éléments

Soient $n \geq 1$ et X un ensemble à n éléments, en pratique $X = \{1, 2, ..., n\}$

1.3.1. Définition

> Une **permutation** de X est une application $\sigma : X \to X$ bijective, c'est-à-dire $\forall y \in X, \exists! x \in X, \ \ \sigma(x) = y$

1.3.2. Notation

> $\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & ... & \sigma(n-1) & \sigma(n) \end{pmatrix}$

- On peut alors les composer. En particulier, on pose $\sigma^k := \sigma \circ \sigma \circ ... \circ \sigma (k$ fois $)$

1.3.4. Définition

> L'ordre de σ est le plus petit entier $k \geq 0$ tel que $\sigma^k = id_X$ $(\Rightarrow \sigma^{k-1} = \sigma^{-1})$
>
> Un élément i de X est un **point fixe** de σ si $\sigma(i) = i$

1.3.5. Exercice

Dans ces deux cas, déterminer les points fixes, l'ordre et la permutation inverse (= réciproque)

1. $n = 4, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$
2. $n = 10, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 10 & 3 & 1 & 8 & 4 & 9 & 5 & 2 & 7 \end{pmatrix}$

1.3.6. Correction

Question 1:

- Points fixes : 3
- Ordre : $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \\ 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} \Rightarrow \sigma_1^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \Rightarrow ordre = 3$
- Inverse : $\sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$

Question 2 :

- Point fixe : 3
- Ordre : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 10 & 3 & 1 & 8 & 4 & 9 & 5 & 2 & 7 \\ 4 & 7 & 3 & 6 & 5 & 1 & 2 & 8 & 10 & 9 \\ ... \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix} \Rightarrow ordre = 12$
- Inverse : $\sigma_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 9 & 3 & 6 & 8 & 1 & 10 & 5 & 7 & 2 \end{pmatrix}$

---

2. Système de chiffrement

2.1. Définition

> Un **système de chiffrement**, ou **cryptosystème**, ou **chiffrement**, est la donnée de $(\mathbf{P}, \mathbf{C}, \epsilon, \mathbf{E}, \mathbf{D})$

- $\mathbf{P}$: ensemble, ses éléments sont appelés **messages en clair** *(plaintext)*

- $\mathbf{C}$: ensemble, ses éléments sont appelés **messages chiffrés** *(cyphertext)*
- $\mathbf{K}$: ensemble, ses éléments sont appelés **clés** *(keys)*
- ϵ : $\{E_k, k \in K\}$: famille de fonctions E_k : $\mathbf{P} \to \mathbf{C}$, ses éléments sont appelés **fonctions de chiffrement** *(encryption functions)*
- $\mathbf{D}$: $\{D_k, k \in K\}$: famille de fonctions D_k : $\mathbf{C} \to \mathbf{P}$, ses éléments sont appelés **fonctions de déchiffrement** *(decryption functions)*

> A chaque clé $e \in \mathbf{K}$ on sait associer une clé $d \in \mathbf{K}$ telle que $D_d(E_e(p)) = p$ pour tout message p

2.3. Chiffrement symétrique (à clé secrète)

2.3.1. Système DES *(Data Encryption Standard)*

> **Chiffrement par blocs** : Mots clés de longueur n et les fonctions de chiffrement par bloc sont des permutations.

- On prend
    - $\mathbf{P} = \mathbf{C} = \{0,1\}^{64}$
    - $\mathbf{K} = \{(b_1, ..., b_{64}) \in \{0,1\}^{64} \mid \forall j = 0, ..., 7 \ \sum_{i=1}^{S} b_{Sj+1} \equiv 1[2]\}^*$

2.3.1.1. Fonctionnement

- Le coeur de DES consiste en 1- tours utilisant chacun une clé différente.
- Chaque tour est composé de 3 étapes :
    1. **Expansion** : on étend le message de 32 bits à 48 bits en ajoutant des bits de contrôle
    2. `XOR` : on fait un `XOR` avec la clé
    3. **Substitution** : on remplace chaque groupe de 6 bits par un groupe de 4 bits
- On répète ce processus 16 fois

---

3. Bases mathématiques 2 (AES)

3.1. Arithmétique des entiers, suite

3.1.1. Algorithme d'Euclide étendu

On cherche à déterminer le **pgcd** de deux entiers positifs a et b par des **divisions euclidiennes successives**. $d = \operatorname{pgcd}(a, b)$.

> $a = b \times q + r, \ 0 \leq r < b$ alors $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(b, r)$

- En effet, si k divise a et b, alors k divise $r = a - bq$, donc k divise b et r. La réciproque est vraie, ainsi les divisuers communs à a et b sont les mêmes que ceux de b et r.
- Le pgcd est le dernier reste non nul obtenu par cette méthode.
- On peut exprimer d en fonction de a, b.

3.1.2. Exemple

Calculer le pgcd de $a = 126$ et $b = 33$:

$$\begin{aligned}
126 &= 33 \times 3 + 27 \\
33 &= 27 \times 1 + 6 \\
27 &= 6 \times 4 + 3 \\
6 &= 3 \times 2 + 0
\end{aligned}$$

- Donc $d = \operatorname{pgcd}(126, 33) = \operatorname{pgcd}(6, 3) = 3$

Expression de d en fonction de a et b :

$$
\begin{aligned}
3 &= 27 - 6 \times 4 \\
&= 27 - (33 - 27 \times 1) \times 4 \\
&= 27 \times 5 - 33 \times 4 \\
&= (126 - 33 \times 3) \times (5 - 33 \times 4) + 33 \times 4 \\
&= 126 \times 5 - 33 \times 19 \\
&= a \times 5 - b \times 19
\end{aligned}
$$

3.1.3. Théorème de Bézout

> Soient a et b deux entiers relatifs. Alors il existe deux entiers u et v tels que $au + bv = \operatorname{pgcd}(a, b)$.

3.1.4. Exercice

Trouver u et v pour $a = 261$ et $b = 25$.

3.1.5. Correction

$$
\begin{aligned}
&261 = 25 \times 10 + 11 \\
&25 = 11 \times 2 + 3 \\
&11 = 3 \times 3 + 2 \\
&3 = 2 \times 1 + 1 \\
&2 = 1 \times 2 + 0
\end{aligned}
$$

- On a donc $d = \operatorname{pgcd}(261, 25) = \operatorname{pgcd}(2, 1) = 1$

Expression de d en fonction de a et b :

$$
\begin{aligned}
1 &= 3 - 2 \times 1 \\
&= 3 - (11 - 3 \times 3) \\
&= 3 \times 4 - 11 \\
&= (25 - 11 \times 2) \times 4 - 11 \\
&= 25 \times 4 - 11 \times 9 \\
&= 25 \times 4 - (261 - 25 \times 10) \times 9 \\
&= 25 \times 94 - 261 \times 9 \\
&= -9a + 94b
\end{aligned}
$$

- Par identification, $u = -9$ et $v = 94$

3.1.6. Conséquences

> **1. Soit n entier ≥ 2, alors $\overline{a}$ est inversible dans $(\mathbb{Z}_{/n\mathbb{Z}}, \times)$ ssi $\operatorname{pgcd}(a, n) = 1$.**

- En effet, si $\operatorname{pgcd}(a, n) = 1$, d'après le théorème : $\exists (u, v) \in \mathbb{Z}^2 | ua + vn = 1$. Alors dans $\mathbb{Z}_{/n\mathbb{Z}}$: $\overline{ua + vn} = \overline{1}$. Or $\overline{ua + vn} = \overline{ua} + \overline{vn} = \overline{u} \times \overline{a} + \overline{v} \times \overline{n} = 0$ dans $\mathbb{Z}_{/n\mathbb{Z}}$
- Ainsi, $\overline{u} = \overline{a} = \overline{1}$, c'est-à-dire que $\overline{u}$ est l'inverse de \overline a$ dans $(\mathbb{Z}_{/n\mathbb{Z}}, \times)$
- **Remarque :** l'algorithme d'Euclide étendu permet de calculer cet inverse (on admet la réciproque).

> **2. $\mathbb{Z}_{/n\mathbb{Z}}$ est un corps ssi n est premier.**

- **Rappel :** $\mathbb{Z}_{/n\mathbb{Z}}$ est muni de $+$ et $\times$. C'est un **corps** (commutatif) si tout élément non nul est inversible pour $\times$.
- Pour $\mathbb{Z}_{/n\mathbb{Z}} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$
  - Si n est premier, alors $a = 1, 2, ..., n-1$ vérifie $\operatorname{pgcd}(a, n) = 1$
  - Sinon, on peut écrire $n = pq$, p et q sont entiers, $2 \leq p < n$ et $2 \leq q < n$. Alors $\overline{n} = \overline{0} = \overline{p} \times \overline{q}$ avec $\overline{p}$ et $\overline{q} \neq \overline{0}$. Ainsi $\overline{p}$ est un élément non nul de $\mathbb{Z}_{/n\mathbb{Z}}$ qui n'a pas d'inverse : s'il existait $\overline{x}$ tel que $\overline{p} \times \overline{x} = 1$, on aurait alors $\overline{q} \times \overline{p} \times \overline{x} = \overline{q} \times (\overline{p} \times \overline{x}) = \overline{q} = (\overline{q} \times \overline{p}) \times \overline{x} = \overline{0} \times \overline{x} = \overline{0}$. D'où $\overline{q} = 0$, ce qui est faux puisque $2 \leq q < n$.
- Notation, si p est premier, on écrira $\mathbb{F}_p = \mathbb{Z}_{/p\mathbb{Z}}$ *(field)*.

3.2. Arithmétique des polynômes

> On fixe un **corps K commutatif** $(K = \mathbb{R}, \mathbb{C},\ \text{ou}\ \mathbb{Z}_{/p\mathbb{Z}}\ (p\ \text{premier}\ ))$

- On va calculer dans $K[X]$, ensemble des polynômes à coefficients dans K :

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + a_2 X^2 + a_1 X + a_0$$

- On peut les ajouter, les multiplier mais aussi faire la **division euclidienne**.

3.2.1. Division

> On divise le polynôme A par le polynôme B en écrivant : $A = B \times Q + R$ avec $Q \in K[X]$ et $R \in K[X]$

- Soit $R = 0$, soit $d^0 R < d^0 B$

3.2.2. Théorème

> $\forall A, B \neq 0 \;\; \exists!\, Q, R.$

3.2.3. Exercice

On prend $K = \mathbb{F}_2$. Soient

- $A = 1 + X^2 + X^3 + X^5 + X^6$
- $B = X + X^2 + X^3 + X^4$

1. Calculer $A + B$ et $A \times B$.
2. Trouver C tel que $A + C = 0$.
3. Faire la division euclidienne de A par B (où on a posé $1 = \overline{1}$ et $0 = \overline{0} \Rightarrow X^2 = \overline{1} \times X^2$).

3.2.4. Correction

Question 1 :

$$\begin{aligned} A + B &= 1 + X + 2X^2 + 2X^3 + X^4 + X^5 + X^6 \\ &= 1 + X + X^4 + X^5 + X^6 \end{aligned}$$

$$\begin{aligned} A \times B = X &+ X^3 + X^4 + X^6 + X^7 \\ &+ X^2 + X^4 + X^5 + X^7 + X^8 \\ &+ X^3 + X^5 + X^6 + X^8 + X^9 \\ &+ X^4 + X^6 + X^7 + X^9 + X^{10} \\ &= X + X^2 + X^4 + X^6 + X^7 + X^{10} \end{aligned}$$

Question 2 :

- Soit $K = \mathbb{F}_2$:

$$A + C = 0 \iff C = A$$

Question 3 :

$$\begin{aligned} &X^6 + X^5 + X^3 + X^2 + 1 + (X^4 + X^3 + X^2 + X + 1) \times X^2 = X^4 + X^2 + 1 \\ &X^4 + X^2 + 1 + (X^4 + X^3 + X^2 + X + 1) \times 1 = X^3 + X + 1 \end{aligned}$$

$$\begin{aligned} Q &= X^2 + 1 \\ R &= X^3 + X + 1 \end{aligned}$$

- Donc $A = (X^2 + 1) \times B + (X^3 + X + 1)$

> $d^0(X^3 + X + 1) = 3 < d^0 B$

3.2.5. Quotients

Retour à $\mathbb{Z}_{/n\mathbb{Z}} \equiv \{\overline{0}, \overline{1}, ..., \overline{n-1}\}[n]$. Avec :

- $\overline{0} = \{0, n, 2n, ..., -n, -2n, ...\} = 0 + n\mathbb{Z} = 0 + \{kn, k \in \mathbb{Z}\}$
- $\overline{1} = \{1, n+1, 2n+1, ..., -n+1, -2n+1, ...\} = 1 + n\mathbb{Z}$
- ...

- $\overline{n-1} = (n-1) + n\mathbb{Z}$

> $\mathbb{Z}_{/n\mathbb{Z}}$ c'est $\mathbb{Z}$ où on a **"tué" tous les multiples de** n.

Dans $K[X]$**, on peut faire de même**, on fixe un polynôme $f \neq 0$:

> On définit $K[X]_{/(f)}$ ou $K[X]_{/fK[X]}$ comme étant $K[X]$ où on a **"tué" tous les polynômes multiples de** f.

- Les objets de $K[X]_{/(f)}$ sont les objets de la forme $P(X) \in K[X], P(X) + fK[X] = \{P(X) + f(X)A(X) \mid A(X) \in K[X]\}$ qu'on notera $\overline{P(X)}$.
- On peut calculer dans $K[X]_{/(f)}$ avec les opérations suivantes ($\forall \overline{P}, \overline{Q} \in K[X]_{/(f)}$) :

$$\begin{aligned}&\text{Addition :}\\&\quad \overline{P(X)} + \overline{Q(X)} := \overline{P(X) + Q(X)}\\&\quad (\overline{P(X)} + fK[X]) + (\overline{Q(X)} + fK[X]) = (\overline{P(X) + Q(X)}) + fK[X]\\&\text{Multiplication :}\\&\quad \overline{P(X)} \times \overline{Q(X)} := \overline{P(X) \times Q(X)}\\&\quad (\overline{P(X)} + fK[X]) \times (\overline{Q(X)} + fK[X]) = (\overline{P(X) \times Q(X)}) + fK[X]\end{aligned}$$

- On a ainsi sur $K[X]_{/(f)}$ une sructure d'anneau (commutatif), mais pas de corps en général : un élément $\overline{P(X)}$ n'a pas forcément d'inverse pour x. Il n'existe pas forcément de $\overline{Q(X)}$ tel que $\overline{P(X)} \times \overline{Q(X)} = \overline{1}$.

3.2.6. Exercice

1. Qu'est-ce que $\mathbb{R}[X]_{/(X^2+1)}$?
2. Dans $\mathbb{F}_2[X]$, on prend $f(x) = X^2 + X + 1$. Faire la liste de éléments de $\mathbb{F}_2[X]_{/(f)}$ et les tables de $+$ et $\times$.

3.2.7. Correction

Question 1 :

$$\begin{aligned}\mathbb{R}[X]_{/(X^2+1)} &\Rightarrow \overline{X^2+1} = 0\\&\Rightarrow \overline{X^2} + \overline{1} = 0\\&\Rightarrow \overline{X^2} = -1\end{aligned}$$

$\Rightarrow g = a_0 + a_1X + a_2X^2 + a_3X^3 \rightarrow \overline{g} = a_0 + a_1\overline{X} - a_2 - a_3\overline{X}$

Opérations :

- $\overline{P} + \overline{Q} = \overline{P+Q}$
- $\overline{P} \times \overline{Q} = \overline{P \times Q}$

$$\begin{aligned}(a \times \overline{1} + b\overline{X}) + (c \times \overline{1} + d\overline{X}) &= (ac) \times \overline{1} + (bc + ad)\overline{X} + bd \times (-\overline{1})\\&= (ac - bd) \times \overline{1} + (bc + ad) \times \overline{X}\end{aligned}$$

> En fait, $\mathbb{R}[X]_{/(X^2+1)}$ est le corps des complexes $\mathbb{C}$.

Question 2 :

Posons B = $\mathbb{F}_2[X]_{/(f)}$.

$P(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + ... + a_nX^n$ avec $a_i \in \mathbb{F}_2 = \{0, 1\}$

$$\begin{aligned}\mathbb{F}_2[X]_{/(f)} &\Rightarrow \overline{X^2 + X + 1} = 0\\&\Rightarrow \overline{X^2} = -(\overline{X+1}) = 1 \times \overline{1} + 1 \times \overline{X}\\&\Rightarrow \overline{X^3} = \overline{X} \times \overline{X^2} = ... = 1\\&\Rightarrow \overline{X^4} = \overline{X} \times \overline{X^3} = ... = \overline{X}\end{aligned}$$

- Tout élément de B peut s'écrire :

$$\overline{P} = a \times \overline{1} + b \times \overline{X},\ \ a \text{ et } b \in \mathbb{F}_2$$

Donc a et b velent soit 0 soit 1.

- Ainsi :

$$
\begin{aligned}
B = \{0 &= 0 \times \overline{1} + 0 \times \overline{X}, \\
1 &= 1 \times \overline{1} + 0 \times \overline{X}, \\
\overline{X} &= 0 \times \overline{1} + 1 \times \overline{X}, \\
1 + \overline{X} &= 1 \times \overline{1} + 1 \times \overline{X}\}
\end{aligned}
$$

On a pour les opérations :

- Addition :

$$
\begin{array}{c|cccc}
+ & 0 & 1 & \overline{X} & 1+\overline{X} \\
\hline
0 & 0 & 1 & \overline{X} & 1+\overline{X} \\
1 & 1 & 0 & 1+\overline{X} & \overline{X} \\
\overline{X} & \overline{X} & 1+\overline{X} & 0 & 1 \\
1+\overline{X} & 1+\overline{X} & \overline{X} & 1 & 0
\end{array}
$$

- Multiplication :

$$
\begin{array}{c|ccc}
\times & 1 & \overline{X} & 1+\overline{X} \\
\hline
1 & 1 & \overline{X} & 1+\overline{X} \\
\overline{X} & \overline{X} & 1+\overline{X} & 1 \\
1+\overline{X} & 1+\overline{X} & 1 & \overline{X}
\end{array}
$$

> Remarque : pour tout élément $P(X)$ de B, il existe un unique élément $\overline{Q(X)}$ tel que $\overline{P(X)} \times \overline{Q(X)} = \overline{1}$. Ainsi, B est un corps commutatif. $\mathbb{F}_2[X]_{/(X^2+X+1)}$ est donc le corps à 4 éléments noté $\mathbb{F}_4$.

3.2.8. Théorème

> Pour tout nombre premier p et tout entier $k \geq 1$, il exitste un unique corps commutatif à p^k éléments. On le notera $\mathbb{F}_{p^k}$.

> Si $k = 1$, on a $\mathbb{F}_{p^1} = \mathbb{Z}_{/p\mathbb{Z}}$.

3.2.9. Exemples

- $p = 2$ et $k = 2$, on a $\mathbb{F}_{2^2} = \mathbb{F}_4 = \mathbb{F}_2[X]_{/(X^2+X+1)}$.

Exemple très important, à réviser :

> $p = 2$ et $k = 8$, on a $\mathbb{F}_{2^8} = \mathbb{F}_{256} = \mathbb{F}_2[X]_{/(X^8+X^4+X^3+X+1)}$.

3.2.10. Remarque

> **Désormais, on ne met plus les barres car c'est lourd**

3.2.11. Exercice

Dans F_{256}, calculer :

1. $(X^7 + X^4 + X^3 + X + 1) \times (X^7 + X^6 + X^3 + X^2 + 1)$
2. L'inverse de $(X^7 + X^4 + X^3 + X + 1)$ (Utiliser l'algorithme d'Euclide étendu)
3. En déduire l'image de a par **SubBytes**

Soit $C = a_3Y^3 + a_2Y^2 + a_1Y + a_0$, $a_i \in \mathbb{F}_{256}$. Par défintion, l'image de C par **MixColumns** est :

$$
m(C) = C(Y) + ((03)_{16}Y^3 + (01)_{16}Y^2 + (01)_{16}Y + (02)_{16}) \text{ réduit modulo } Y^4 + 1
$$

3.2.12. Correction

Question 1 :

$$
(X^7 + X^4 + X^3 + X + 1) \times (X^7 + X^6 + X^3 + X^2 + 1) \rightarrow (1001\ 1011)_2 \times (1100\ 1101)_2
$$

$$
\begin{aligned}
= & X^{14} + X^{13} + X^{10} + X^9 + X^7 \\
& + X^{11} + X^{10} + X^7 + X^6 + X^4 \\
& + X^{10} + X^9 + X^6 + X^5 + X^3 \\
& + X^8 + X^7 + X^4 + X^3 + X \\
& + X^7 + X^6 + X^3 + X^2 + 1 \\
= & X^{14} + X^{13} + X^{11} + X^{10} + X^8 + X^6 + X^5 + X^3 + X^2 + 1
\end{aligned}
$$

Question 2 :

On cherche l'inverse de $a = X^7 + X^4 + X^3 + X + 1$ dans $\mathbb{F}_{256}$.

- On fait la division euclidienne de f par a.
  - On obtient $f = X \times a + R_1$ avec $R1 = X^5 + X^3 + X^2 + 1,\ d^\circ R_1 < d^\circ a$
- On fait la division euclidienne de a par R_1.
  - On obtient $a = (X^2+1) \times R_1 + R_2$ avec $R_2 = X,\ d^\circ R_2 < d^\circ R_1$
- On fait la division euclidienne de R_1 par R_2.
  - On obtient $R_1 = (X^4 + X^2 + X) \times R_2 + R_3$ avec $R_3 = 1,\ d^\circ R_3 < d^\circ R_2$
- On fait la division euclidienne de R_2 par R_3.
  - On obtient $R_2 = R_2 \times 1$

Comme pour les entiers :

$$\begin{aligned}\operatorname{pgcd}(f, a) &= \operatorname{pgcd}(a, R_1)\\ &= \operatorname{pgcd}(R_1, R_2)\\ &= \operatorname{pgcd}(R_2, R_3)\\ &= 1\end{aligned}$$

En remontant :

$$\begin{aligned}1 &= R_1 - (X^4 + X^2 + X) \times R_2\\ &= R_1 + (X^4 + X^2 + X) \times (a - (X^2+1) \times R_1)\\ &= R_1(1 + (X^4 + X^2 + X) \times (X^2+1)) + (X^4 + X^2 + X) \times a\\ &= (f - Xa)(1 + X^6 + X^4 + X^3 + X^4 + X^2 + X) + (X^4 + X^2 + X)a\\ &= f(X^6 + X^3 + X^2 + X + 1) + a(X^7 + X^4 + X^3 + X^2 + X + X^4 + X^2 + X)\end{aligned}$$

Ainsi, $1 = Uf + Va,\ U, V \in \mathbb{F}_2[X]$ avec :

$$\begin{aligned}U &= X^6 + X^3 + X^2 + X + 1\\ V &= X^7 + X^3\end{aligned}$$

Alors, dans $\mathbb{F}_{256}$:

$$\begin{aligned}1 = 0 + Va \text{ où } V &= X^7 + X^3\\ &= (10001000)_2\\ &= (88)_{16}\end{aligned}$$

Question 3 :

$s(a) = inv(a) * A_1 + A_0$ avec :

- $inv(a) = (88)_{16}$
- $A_1 = (1F)_{16}$
- $A_0 = (63)_{16}$

On a :

$$s(a) = (X^7 + X^3) * (X^4 + X^3 + X^2 + X + 1) + (X^6 + X^5 + X + 1)$$

On prend $R = \mathbb{F}_2[X]_{/(g)}$; $g = X^8 + 1$

$$\begin{aligned}(X^7 + X^3) * (X^4 + X^3 + X^2 + X + 1) &= (X^7 + X^3)(X^4 + X^3 + X^2 + X + 1) \text{ réduit modulo } g\\ &= X^{11} + X^{10} + X^9 + X^8 + X^7 + X^7 + X^6 + X^5 + X^4 + X^3 \text{ modulo } g\\ &= X^{11} + X^{10} + X^9 + X^8 + X^6 + X^5 + X^4 + X^3 \text{ modulo } g\\ &= X^8(X^3 + X^2 + X + 1) + X^6 + X^5 + X^4 + X^3 \text{ modulo } g\\ &= X^3 + X^2 + X + 1 + X^6 + X^5 + X^4 + X^3\\ &= X^6 + X^5 + X^4 + X^2 + X + 1\end{aligned}$$

Finalement :

$$
\begin{aligned}
s(a) &= inv(a) * A_1 + A_0 \\
&= X^6 + X^5 + X^4 + X^2 + X + 1 + X^6 + X^5 + X + 1 \\
&= X^4 + X^2 \\
&= (00010100)_2 \\
&= (14)_{16}
\end{aligned}
$$

3.2.13 Exercice

1. Montrer que l'application $S \longrightarrow S$ utilisée pour **MixColumns** est celle qui, à l'octet (a_3, a_2, a_1, a_0) associe son produit par la matrice d'octets (chaque octet est ici écrit comme un couple de nombres hexadécimaux)

$$
M = \begin{pmatrix} 02 & 01 & 01 & 03 \\ 03 & 02 & 01 & 01 \\ 01 & 03 & 02 & 01 \\ 01 & 01 & 03 & 02 \end{pmatrix}
$$

2. Vérifier que, dans S, l'inverse du polynôme

$$
(00000011)_2 Y^3 + (00000001)_2 Y^2 + (00000001)_2 Y + (00000010)_2 = 03Y^3 + 01Y^2 + 01Y + 02
$$

est le polynôme :

$$
0BY^3 + 0DY^2 + 09Y + 0E = (00001011)_2 Y^3 + (00001101)_2 Y^2 + (00001001)_2 Y + (00001110)_2
$$

3.2.14 Correction

Question 1 :

- $S = \mathbb{F}_{256}[Y]_{/(Y^4+1)}$
- L'applicaion de **MixColumns** est :

> Pour $(a_3 \quad a_2 \quad a_1 \quad a_0) = a_3 Y^3 + a_2 Y^2 + a_1 Y + a_0$, l'image est $m(c) = (a_3 Y^3 + a_2 Y^2 + a_1 Y + a_0)(03Y^3 + 01Y^2 + 01Y + 02)$.
>
> Où par exemple $03 = (03)_{16}$ est un octet, élément de $\mathbb{F}_{256} = \mathbb{F}_f[X]_{/(f)}$.

$$
\begin{aligned}
m(C) =& (03 \times a_3) Y^6 + (01 \times a_3 + 03 \times a_2) Y^5 + (01 \times a_3 + 01 \times a_2 + 03 \times a_1) Y^4 \\
&+ (02 \times a_3 + 01 \times a_2 + 01 \times a_1 + 03 \times a_0) Y^3 + (02 \times a_2 + 01 \times a_1 + 01 \times a_0) Y^2 \\
&+ (02 \times a_1 + 01 \times a_0) Y + 02 \times a_0
\end{aligned}
$$

$$
\Rightarrow m(C) = 3a_3 Y^6 + (a_3 + 3a_2) Y^5 + (a_3 + a_2 + 3a_1) Y^4 + (2a_3 + a_2 + a_1 + 3a_0) Y^3 + (2a_2 + a_1 + a_0) Y^2 + (2a_1 + a_0) Y + 2a_0
$$

> A comparer avec :

$$
M = \begin{pmatrix} 02 & 01 & 01 & 03 \\ 03 & 02 & 01 & 01 \\ 01 & 03 & 02 & 01 \\ 01 & 01 & 03 & 02 \end{pmatrix}
$$

$$
MC = \begin{pmatrix} 2a_3 + a_2 + a_1 + 3a_0 \\ 3a_3 + 2a_2 + a_1 + a_0 \\ a_3 + 3a_2 + 2a_1 + a_0 \\ a_3 + a_2 + 3a_1 + 2a_0 \end{pmatrix} \begin{aligned} =& (2a_3 + a_2 + a_1 + 3a_0) Y^3 + (3a_3 + 2a_2 + a_1 + a_0) Y^2 \\ &+ (a_3 + 3a_2 + 2a_1 + a_0) Y + (a_3 + a_2 + 3a_1 + 2a_0) \end{aligned}
$$

> On réduit $m(C)$ modulo $Y^4 + 1$ (car $S = \mathbb{F}_{256}[Y]_{/(Y^4+1)}$) :

$$
\begin{aligned}
m(C) =& Y^4 (3a_3 Y^2 + (a_3 + 3a_2) Y + (a_3 + a_2 + 3a_1)) \\
&+ (2a_3 + a_2 + a_1 + 3a_0) Y^3 + (2a_2 + a_1 + a_0) Y^2 + (2a_1 + a_0) Y + 2a_0 \text{ modulo } Y^4 + 1
\end{aligned}
$$

$$
\Rightarrow m(c)(2a_3 + a_2 + a_1 + 3a_0) Y^3 + (3a_3 + 2a_2 + a_1 + a_0) Y^2 + (a_3 + 3a_2 + 2a_1 + a_0) Y + (a_3 + a_2 + 3a_1 + 2a_0)
$$

Question 2 :

> Il faut vérifier que $(03Y^3 + 01Y^2 + 01Y + 02)(0BY^3 + 0DY^2 + 09Y + 0E) \text{ modulo } = 1$.
>
> Etape par étape :

$$
\begin{aligned}
&03Y^3(0BY^3+0DY^2+09Y+0E)\\
&=(00000011)_2Y^3\times((00001011)_2Y^3+(00001101)_2Y^2+(00001001)_2Y+(00001110)_2)
\end{aligned}
$$

Soit $f = X^8 + X^4 + X^3 + X + 1$, Calculons $03 \times 0B$:

$$03 \times 0B = (00000011)_2 \times (00001011)_2$$

$$
\begin{aligned}
\rightarrow (X+1)(X^3+X+1) \text{ modulo } f &= X^4+X^2+X+X^3+X+1 \text{ modulo } f\\
&= X^4+X^3+X^2+1\\
&\Rightarrow (00011101)_2 = 1D
\end{aligned}
$$

Calculons la suite :

$$
\begin{aligned}
&03 \times 0D = (X+1)(X^3+X^2+1) = X^4+X^2+X+1 = 17\\
&03 \times 09 = (X+1)(X^3+1) = X^4+X^3+X+1 = 1B\\
&03 \times 0E = (X+1)(X^3+X^2+X) = X^4+X = 12
\end{aligned}
$$

Donc :

$$03Y^3(0BY^3+0DY^2+09Y+0E) = (1D)Y^6+(17)Y^5+(1B)Y^4+(12)Y^3$$

Suite :

$$
\begin{aligned}
&02 \times 0B = 16\\
&02 \times 0D = 1A\\
&02 \times 09 = 12\\
&02 \times 0E = 1C\\
&\ldots
\end{aligned}
$$

On a :

$$
\begin{aligned}
p =&(1D)Y^6+((OB)+(17))Y^5+((1B)+(OD)+(OB))Y^4\\
&+((12)+(09)+(0D)+(16))Y^3+((OE)+(09)+(1A))Y^2+((0E)+(12))Y+(1C)
\end{aligned}
$$

Somme bit à bit (XOR), par exemple :

$$
\begin{aligned}
(OB)+(17) &= (00001011)_2+(00010111)_2\\
&= (00011100)_2\\
&= 1C
\end{aligned}
$$

On obtient :

$$
\begin{aligned}
p &= (1D)Y^6+(1C)Y^5+(1D)Y^4+(00)Y^3++((OE)+(09)+(1A))Y^2+((0E)+(12))Y+(1C)\\
&= 1DY^2+1CY+1D+1DY^2+1CY+1C\\
&= 1D+1C = 01 = 1
\end{aligned}
$$

4. Bases mathématiques 3 (RSA)

Dans tout ce chapitre, lorsque nous parlerons de nombre, il s'agira de nombres entiers strictement supérieurs à 0.

4.1. Nombres premiers

4.1.1. Théorème d'Euclide *(~-300)*

Il existe une infinité de nombres premiers.

4.1.2. Démonstration

Supposons qu'il n'existe qu'un nombre fini de nombres premiers. Alors, on peut les énumérer : $p_1, p_2, \ldots, p_n$. Posons $A = p_1 \times p_2 \times \cdots \times p_n + 1$:

- Si A est premier, alors on a une contradiction car $A > p_i$ pour tout i.
- Sinon, A est divisible par un des p_i mais p_i divise $p_1 \times p_2 \times \cdots \times p_n$ donc ne peut diviser A.

4.2. Nombres premiers entre eux

> Soienta, b deux nombres.

4.2.1. Définition

> a et b sont dits premiers entre eux si leur plus grand diviseur commun est égal à 1.

4.2.2. Propriété

> a et b sont premiers entre eux si et seulement si il existe u, v dans $\mathbb{Z}$ tels que $ua + vb = 1$.

4.2.3. Remarque

L'**algorithme d'Euclide étendu** permet de trouver explicitement u et v vérifiant cette égalité, alors pour tout entier k, $(u + kb, v - ka)$ marchera aussi :

$$(u + kb)a + (v - ka)b = ua + vb = 1$$

4.3. Indicatrice d'Euler *(1707 - 1783)*

> Soit n un entier, $n \geq 2$.

4.3.1. Définition

> On note $\Phi(n)$ le nombre d'entiers m vérifiant : $\begin{cases} 1 \leq m \leq n-1 \\ m \text{ est premier avec } n \end{cases}$

4.3.2. Exemples

Calculer $\Phi(7)$ et $\Phi(8)$. On trouve :

- $\Phi(7) = 6$ car $1, 2, 3, 4, 5, 6$ sont premiers avec 7.
- $\Phi(8) = 4$ car $1, 3, 5, 7$ sont premiers avec 8.

4.3.3. Remarque générale

> Si n est premier, alors $\Phi(n) = n - 1$.

4.3.4. Propriété 1

> $\Phi(n)$ est le nombre d'éléments inversibles dans le groupe $(\mathbb{Z}_{/n\mathbb{Z}})^*$ des éléments inversibles de $\mathbb{Z}_{/n\mathbb{Z}}$ pour la multiplication.

4.3.5. Démonstration

Si $\overline{a}$ est inversible dans $(\mathbb{Z}_{/n\mathbb{Z}}, \times)$, cela veut dire qu'il existe $\overline{u}$ dans $(\mathbb{Z}_{/n\mathbb{Z}}, \times)$ tel que $\overline{a} \times \overline{u} = 1$. C'est-à-dire $\overline{a \times u} = \overline{1}$.

Ainsi au est congru à $1 \bmod n$. Donc il existe un entier k tel que $au = 1 + kn$.

Posant $v = -k$, on obtient $ua + vn = 1$. Par l'**identité de Bézout**, a et n sont premiers entre eux.

Réciproquement, si $\mathrm{pgcd(a,n)} = 1$, par Bézout : $\exists (u, v) \in \mathbb{Z}^2 | ua + vn = 1$, alors $\mod{\mathrm{n}}$: $\overline{ua} + \overline{0} = \overline{1}$. Donc $\overline{u} \times \overline{a} = \overline{1}$, donc $\overline{a}$ est inversible dans $(\mathbb{Z}_{/n\mathbb{Z}}, \times)$.

4.3.6. Propriété 2

> Soient $n \geq 2$ et x premier avec n. Alors $x^{\Phi(n)} \equiv 1 \bmod n$.

4.3.6.1. Cas particulier

> Si p est un nombre premier, alors pour x non multiple de p, $x^{p-1} \equiv 1 \bmod p$. C'est le **"petit théorème de Fermat"**.

(Le "grand théorème de Fermat" dit que l'équation $x^n + y^n = z^n$ n'a pas de solution entière pour $n \geq 3$. Démonstration par Wiles en 1993.)

4.3.7. Démonstration

Pour un tel x, considérons :

$$\begin{aligned} f : (\mathbb{Z}_{/n\mathbb{Z}})^* &\longrightarrow (\mathbb{Z}_{/n\mathbb{Z}})^* \\ \overline{t} &\longmapsto \overline{x}, \overline{t} \end{aligned}$$

- Par hypothèse $\operatorname{pgcd}(x, n) = 1$ donc $\overline{x}$ est inversible pour $\times$ *(propriété 1)*
- f est injective, en effet :

$$\begin{aligned} f(\overline{t}) = f(\overline{t'}) &\Rightarrow \overline{x}\overline{t} = \overline{x}\overline{t'} \\ &\Rightarrow (\overline{x})^{-1}\overline{x}\overline{t} = (\overline{x})^{-1}\overline{x}\overline{t'} \\ &\Rightarrow \overline{t} = \overline{t'} \end{aligned}$$

- Comme $(\mathbb{Z}_{/n\mathbb{Z}})^*$ est fini, f est surjective donc bijective.

Ainsi :

$$\prod_{\overline{t} \in (\mathbb{Z}_{/n\mathbb{Z}})^*} f(\overline{t}) = \prod_{\overline{t} \in (\mathbb{Z}_{/n\mathbb{Z}})^*} \overline{t}$$

Or :

$$\begin{aligned} \prod_{\overline{t} \in (\mathbb{Z}_{/n\mathbb{Z}})^*} \overline{t} &= \prod_{\overline{t} \in (\mathbb{Z}_{/n\mathbb{Z}})^*} \overline{x} \times \overline{t} \\ &= \prod_{\overline{t} \in (\mathbb{Z}_{/n\mathbb{Z}})^*} \overline{x} \times \prod_{\overline{t} \in (\mathbb{Z}_{/n\mathbb{Z}})^*} \overline{t} \\ &= \overline{x}^{\operatorname{card}((\mathbb{Z}_{/n\mathbb{Z}})^*)} \times \prod_{\overline{t} \in (\mathbb{Z}_{/n\mathbb{Z}})^*} \overline{t} \\ &= \overline{x}^{\Phi(n)} \times \prod_{\overline{t} \in (\mathbb{Z}_{/n\mathbb{Z}})^*} \overline{t} \end{aligned}$$

D'où, en simplifiant :

$$\overline{x}^{\Phi(n)} = \overline{1} \text{ dans } \mathbb{Z}_{/n\mathbb{Z}}$$

4.3.8. Propriété 3

> Si m et n sont deux nombres premiers entre eux, alors $\Phi(mn) = \Phi(m) \times \Phi(n)$.

4.3.8.1. Remarques

- L'hypothèse est nécessaire, voici un exemple : $\Phi(2) = 1$ et $\Phi(4) = 2 \neq 1 = \Phi(2) \times \Phi(2)$
- Si p et q sont premiers, on a donc $\Phi(pq) = (p-1)(q-1)$.
- Démonstration avec le **"théorème chinois des restes"**.

4.4. Exemple d'algorithme d'exponentiation rapide

Calcul rapide de $x^{37} = z$

- Algorithme de base :

```
z = 1
Pour i allant de 1 à 37 faire :
    z = z * x
```

> 37 produits.

- Idée : $x^{37} = x^{32+4+1}$
  - On calcule $x^2, x^4, (x^4)^2 = x^8, (x^8)^2 = x^{16}, (x^{16})^2 = x^{32}$

- Alors $z = x^{32} \times x^4 \times x \rightarrow 32 = (100101)_2$

> 7 produits.

4.5. Retour sur l'autre façon de calculer x^{-1} comme application de la propriété 2

En effet, dans $\mathbb{Z}_{/n\mathbb{Z}}$ cette congruence devient :

$$\overline{x}^{\Phi(n)} = \overline{1}$$

Donc $x \times x^{\Phi(n)-1} = 1$. C'est-à-dire que $x^{\Phi(n)-1}$ est l'inverse de x dans $\mathbb{Z}_{/n\mathbb{Z}}$.. or pour n premier, $\Phi(n) = n-1$ et si $n = pq$ avec p et q premiers, $\Phi(n) = (p-1)(q-1)$.

On sait donc calculer l'inverse de x au moins dans ces cas là.

4.6. Remarque sur le décryptage RSA

> Avec les notations du diaporama *(page 30)*, on a besoin de savoir que x est premier avec N pour pouvoir dire que $x^{\Phi(N)} = 1$.
>
> Si ce n'est pas le cas : $x \in [\![0, N-1]\!]$ et $N = pq$, p et q premiers, donc x est divisible par p ou q. On écarte les cas $x = 0$ ou $x = 1$.

En fait :

- On peut montrer que $x^{\Phi(N)} \equiv 1 \pmod{n}$ reste vrai.
- Ce cas est peu probable : le risque de "tirer" un message clair x divisible par p ou q parmi tous les messages en clair possibles est :

$$1 - \frac{\Phi(N)}{N}$$

Soit, avec n le nombre de bits de N à peu près :

$$\frac{p+q-1}{pq} \simeq \frac{2 \times 2^{\frac{n}{2}}}{2^n}$$

en considérant que p et q sont de même ordre de grandeur : $p \simeq q \simeq \sqrt{N} \simeq 2^{\frac{n}{2}}$. Donc ce risque est négligeable.

4.7. Théorème chinois des restes

Préliminaires : peut-on comparer $\mathbb{Z}_{/n\mathbb{Z}}$ et $\mathbb{Z}_{/m\mathbb{Z}}$ pour $n \neq m$?

On va noter :

$$\begin{aligned} f_{n,m} : \mathbb{Z}_{/n\mathbb{Z}} &\longrightarrow \mathbb{Z}_{/m\mathbb{Z}} \\ x \bmod n &\longmapsto x \pmod{m} \end{aligned}$$

4.7.1. Exercices

1. $f_{2,3}$ est-elle bien définie ? Si oui, est-il vrai que $\forall a, b \in \mathbb{Z}_{/n\mathbb{Z}}$:

$$f_{2,3}(a+b) = f_{2,3}(a) + f_{2,3}(b) \text{ et } f_{2,3}(ab) = f_{2,3}(a) \times f_{2,3}(b)$$

- Même question pour $f_{3,2}$.
- Même question pour $f_{6,3}$.

2. Trouver tous les entiers x vérifiant :

$$* \begin{cases} x \equiv 1 \pmod{3} & (1) \\ x \equiv 2 \pmod{4} & (2) \\ x \equiv 0 \pmod{5} & (3) \end{cases}$$

4.7.2. Correction

Question 1 :

> Pour $f_{2,3}$, on a :

$$\mathbb{Z}_{/2\mathbb{Z}} = \{\overline{0}, \overline{1}\}, \mathbb{Z}_{/3\mathbb{Z}} = \{\tilde{0}, \tilde{1}, \tilde{2}\}$$

$$\overline{x} \longmapsto \tilde{x}$$

$$\begin{aligned}\overline{0} &= \{0 + 2k, k \in \mathbb{Z}\}\\ \overline{1} &= \{1 + 2k, k \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}f_{2,3} : \overline{0} &\longmapsto \tilde{0} = \{0, 3, 6, 9, \dots, -3, \dots\}\\ = \overline{2} &\longmapsto \tilde{2} = \{2, 5, 8, 11, \dots, -1, \dots\}\end{aligned}$$

Donc $f_{2,3}$ n'est pas définie.

> Même réponse pour $f_{3,2}$.

> Pour $f_{6,3}$, on a :

$$\begin{aligned}f_{6,3} : \mathbb{Z}_{/6\mathbb{Z}} &\longrightarrow \mathbb{Z}_{/3\mathbb{Z}}\\ \overline{x} = \{x + 6k, k \in \mathbb{Z}\} &\longmapsto \tilde{x} = \{x + 3l, l \in \mathbb{Z}\}\end{aligned}$$

Si $\overline{x} = \overline{x'}$, on peut écrire $x' = x + 6k, k \in \mathbb{Z}$ alors $x' = 3 \times (2k)$, avec $2k \in \mathbb{Z}$ donc $\tilde{x'} = \tilde{x}$ dans $\mathbb{Z}_{/3\mathbb{Z}}$.

Bilan à ce stade : $f_{n,m}$ est bien définie si et seulement si n et multiple de m.

Opérations :

$$\begin{aligned}f_{6,3}(a + b) &= f_{6,3}(\overline{x} + \overline{y})\\ &= f_{6,3}(\overline{x + y})\\ &= \widetilde{x + y}\\ &= \tilde{x} + \tilde{y}\\ &= f_{6,3}(\overline{x}) + f_{6,3}(\overline{y})\\ &= f_{6,3}(a) + f_{6,3}(b)\end{aligned}$$

De même pour $\times$.

Question 2 :

Soit x dans $\mathbb{Z}$ vérifiant $*$.

- Par (3), x est multiple de 5.
- Par (2), x est pair donc x est multiple de 10.

Testons :

x	$x \pmod 3$	$x \pmod 4$	$x \pmod 5$
0	0	0	0
10	1	2	0
20	2	0	0
30	0	2	0
40	1	0	0
50	2	2	0
60	0	0	0
70	1	2	0
$\dots$	$\dots$	$\dots$	$\dots$

Ca marche donc pour $x = 10 + 60k$ avec $k \in \mathbb{Z}$.

4.7.3. Retour sur le théorème chinois des restes

> Soient n et m dans $\mathbb{Z}$ premier entre eux. ALors l'application

$$f : \mathbb{Z}_{/nm\mathbb{Z}} \longrightarrow \mathbb{Z}_{/n\mathbb{Z}} \times \mathbb{Z}_{/m\mathbb{Z}}$$
$$x \pmod{nm} \longmapsto (x \pmod n, x \pmod m)$$

> est bien définie, elle respecte les opérations $+$ et $\times$ et est bijective.

4.7.4. Démonstration

Il reste à montrer que f est bijective. On va construire sa réciproque.

Comme n et m sont premiers entre eux, par l'identité de Bezout, il existe u, v dans $\mathbb{Z}$ tels que $un + vm = 1$, alors :

$$\mathbb{Z}_{/n\mathbb{Z}} \times \mathbb{Z}_{/m\mathbb{Z}} \longrightarrow \mathbb{Z}_{/nm\mathbb{Z}}$$
$$(a, b) \longmapsto bum + avn$$

définit g qui satisfait $g = f^{-1}(\dots)$.

Conséquence déjà vue : sous la méme hypotèse :

$$\Phi(nm) = \Phi(n) \times \Phi(m)$$

En effet, $\Phi(n)$ est le nombre d'élements inversibles pour x dans $\mathbb{Z}_{/n\mathbb{Z}}$, c'est-à-dire $\text{card }((\mathbb Z_{/n \mathbb Z})^*) et par le théorème :

$$(\mathbb{Z}_{/nm\mathbb{Z}})^* \longrightarrow^{f}_{\text{bijective}} (\mathbb{Z}_{/n\mathbb{Z}})^* \times (\mathbb{Z}_{/m\mathbb{Z}})^*$$
$$\Phi(nm) \longmapsto \Phi(n) \times \Phi(m)$$

4.7.5. Exemple : Système bancaire allemand (2015)

> RSA avec $n = 1024$, chaque usager à un N différent, mais $e = 2^16 + 1$ est la même pour tous. (e est un nombre premier, donc il suffit de prendre, pour $N = pq, p, q \neq e$).
>
> Il est envisageable que le même message m soit envoyé à beaucoup d'utilisateurs différents, au moins e. On note $N_1, \dots, N_e$ les différents modules N utilisés. Pour chaque client i ($i = 1, \dots, e$), le message m est crypté par RSA avec la clé (N_i, e).
>
> Le message crypté est donc $c_i = m^e \pmod{N_i}$.

Quelqu'un intercepte ces messages cryptés.

Supposons de plus que les p_i, q_i définissant $N_i = p_i q_i$ soient tous distincts. On peut alors utiliser le théorème chinois des restes. On a alors X dans $\mathbb{Z}$ tel que $X \equiv c_1 \pmod{N_i}$ pour tout $i = 1, \dots, e$. On peut donc calculer $X^{\frac{1}{e}}$ dans $\mathbb{Z}$. Alors $m = X^{\frac{1}{e}} \pmod{u \cap N_i}$.

4.7.6. Contre-exemple au théorème chinois des restes

$$\mathbb{Z}_{/4\mathbb{Z}} \longrightarrow \mathbb{Z}_{/2\mathbb{Z}} \times \mathbb{Z}_{/2\mathbb{Z}}$$

> Rappel:
>
> $$\mathbb{Z}_{/n\mathbb{Z}} \longrightarrow \mathbb{Z}_{/m\mathbb{Z}}$$
> $$x \pmod n \longmapsto x \pmod m$$
>
> est bien définie si m divise n et respecte les opérations.

$$x \pmod 4 \longmapsto (x \pmod 2, x \pmod 2)$$

Table de $(\mathbb{Z}_{/4\mathbb{Z}}, +)$:

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Table de $(\mathbb{Z}_{/2\mathbb{Z}} \times \mathbb{Z}_{/2\mathbb{Z}}, +)$:

	$(\tilde{0},\tilde{0})$	$(\tilde{0},\tilde{1})$	$(\tilde{1},\tilde{0})$	$(\tilde{1},\tilde{1})$
$(\tilde{0},\tilde{0})$	$(\tilde{0},\tilde{0})$	$(\tilde{0},\tilde{1})$	$(\tilde{1},\tilde{0})$	$(\tilde{1},\tilde{1})$
$(\tilde{0},\tilde{1})$	$(\tilde{0},\tilde{1})$	$(\tilde{0},\tilde{0})$	$(\tilde{1},\tilde{1})$	$(\tilde{1},\tilde{0})$
$(\tilde{1},\tilde{0})$	$(\tilde{1},\tilde{0})$	$(\tilde{1},\tilde{1})$	$(\tilde{0},\tilde{0})$	$(\tilde{0},\tilde{1})$
$(\tilde{1},\tilde{1})$	$(\tilde{1},\tilde{1})$	$(\tilde{1},\tilde{0})$	$(\tilde{0},\tilde{1})$	$(\tilde{0},\tilde{0})$

> Nous regardons où nous retrouvons des $\overline{0}$ dans la table de $(\mathbb{Z}_{/4\mathbb{Z}},+)$, et nous regardons où nous retrouvons des $(\tilde{0},\tilde{0})$ dans la table de $(\mathbb{Z}_{/2\mathbb{Z}} \times \mathbb{Z}_{/2\mathbb{Z}},+)$.

- Nous voyons que $\mathbb{Z}_{/4\mathbb{Z}}$ est cyclique :

$$\begin{aligned}\overline{1} &= \overline{0} + \overline{1}\\ \overline{2} &= \overline{1} + \overline{1}\\ \overline{3} &= \overline{1} + \overline{1} + \overline{1}\end{aligned}$$

- Nous voyons que $\mathbb{Z}_{/2\mathbb{Z}} \times \mathbb{Z}_{/2\mathbb{Z}}$ ne l'est pas ($(\tilde{0},\tilde{0})$ dans la diagonale) :

$$(\tilde{1},\tilde{0}) \neq (\tilde{0},\tilde{1}) + (\tilde{0},\tilde{1})$$

> Donc ils ne sont pas **isomorphes**.

4.7.7. Remarque

> Soit :
>
> $$\begin{cases} x \equiv a_1 \pmod{N}_1 \\ x \equiv a_2 \pmod{N}_2 \end{cases}$$
>
> Résoudre ce système, c'est chercher x dans $\mathbb{Z}_{/N\mathbb{Z}}$ tel que :
>
> $$\begin{aligned}\mathbb{Z}_{/N\mathbb{Z}} &\longrightarrow \mathbb{Z}_{/N_1\mathbb{Z}} \times \mathbb{Z}_{/N_2\mathbb{Z}}\\ x &\longmapsto (a_1, a_2)\end{aligned}$$

4.7.8. Un peu d'histoire

Pourquoi le théorème **chinois** des restes ? (~ 1200)

Parce que les Chinois l'ont utilisé en **astronomie** pour déterminer :

$$\begin{cases} x \equiv a_1 \pmod{N}_1 \\ x \equiv a_2 \pmod{N}_2 \end{cases}$$

Avec :

$$N_1 = 28, N_2 = 365$$

- **28** : nombre de jours dans un mois lunaire
- **365** : nombre de jours dans une année

Afin de répondre à la question : *Dans combien de jours la pleine lune tombera-t-elle au solstice d'hiver ?*

5. Exercices

5.1. Exercice 1

Sujet :

On pose $x = [1,0,1,0,1,0,1,0]$

Calculer SubBytes(x).

Méthode :

1. Calculer $\text{inv}(x)$ dans $\mathbb{F}_{256} = \mathbb{F}_8[X]_{/(f)}$ par l'algorithme d'Euclide étendu.
2. Calculer $\text{SubBytes}(x) = \text{inv}(x) * A_1 + A_0$

- $+$: Somme bit à bit.
- $*$: Produit modulo $g = X^8 + 1$.