TP7 14 mars 2025

## Section 7.6

**Exercice 16:** Montrer que les exposants $\frac{b^2-1}{8}$ et $\frac{(a-1)(b-1)}{4}$ dans la formule (7.5) donnant $J(a,b)$ sont toujours des entiers pour $a,b$ impairs.

**Sol:** Comme $a$ et $b$ sont impairs, on a que

$\exists k, \ell \in \mathbb{Z}_{\geq 0}$ tels que $a = 2k+1$ et $b = 2\ell+1$.
↳ car $a,b \in \mathbb{N}$

Ainsi, on a

$$\frac{b^2-1}{8} = \frac{(2\ell+1)^2-1}{8} = \frac{4\ell^2+4\ell+1-1}{8}$$

$$= \frac{4\ell(\ell+1)}{8}$$

$$= \frac{\ell(\ell+1)}{2}$$

Comme $\ell$ ou $\ell+1$ est pair, $2 \mid \ell$ ou $2 \mid \ell+1$

$$\Rightarrow \frac{b^2-1}{8} = \frac{\ell(\ell+1)}{2} \in \mathbb{Z}$$

Pour $\frac{(a-1)(b-1)}{4}$, on a

$$\frac{(a-1)(b-1)}{4} = \frac{(2k+1-1)(2\ell+1-1)}{4} = \frac{4k\ell}{4} = k\ell \in \mathbb{Z}$$

Exercice 17 : Soit $E_n = \{1, \dots, n-1\}$

(a) Soit $n=13$. Vérifier en calculant explicitement $J(a,n)$ et $a^{\frac{n-1}{2}} \pmod n$ que tout $a \in E_n$ satisfait à (7.4)

(b) Soit maintenant $n=15$. Combien de $a \in E_n$ ne satisfont pas au test ?

Sol : Rappel :

Si $n$ est un nombre premier et $a \in E_n$, alors

$$\begin{cases} (a,n) = 1 \\ J(a,n) \equiv a^{\frac{n-1}{2}} \pmod n \end{cases} \qquad (7.4)$$

Si $n$ n'est pas premier, alors au moins la moitié des nombres de $E$ ne satisfont pas à (7.4). Dès qu'un nombre $a \in E_n$ échoue au test (7.4), on sait que $n$ n'est pas premier.

Si on choisit $a \in E_n$ au hasard, on a donc Prob(a réussit le test | n est non premier) $\leq 1/2$

Définition du symbole de Jacobi :

Pour $a, b \in \mathbb{N}$ relativement premiers, si $b$ est premier, on a

$$J(a,b) = \begin{cases} 1 & \text{si } \exists x \in \mathbb{N} \text{ tel que } x^2 \equiv a \pmod{b} \\ -1 & \text{sinon} \end{cases}$$

Si $b$ n'est pas premier, on peut écrire $b = p_1 \cdots p_r$ (où les $p_i$ ne sont pas nécessairement tous disjoints), et on a

$$J(a,b) = \prod_{i=1}^{r} J(a, p_i)$$

Théorème 7.14 : Comment calculer le symbole de Jacobi.

Si $(a,b) = 1$, pour $a \leq b$ et $b$ impair, alors

$$J(a,b) = \begin{cases} 1 & , \text{ si } a = 1 \\ J\left(\frac{a}{2}, b\right)(-1)^{\frac{b^2-1}{8}} & , \text{ si } a \text{ pair} \\ J(b \pmod a, a)(-1)^{\frac{(a-1)(b-1)}{4}} & , \text{ si } a > 1 \text{ et impair} \end{cases}$$

Fin du rappel

(a) On a $E_n = E_{13} = \{1,2,3,4,5,6,7,8,9,10,11,12\}$

et $\frac{b^2-1}{8} = \frac{169-1}{8} = 21$

$$J(12,13) = J(6,13)(-1)^{\frac{13^2-1}{8}}$$

$$= J(6,13)(-1), \text{ car } \frac{13^2-1}{8} = 21$$

$$= J(3,13)$$

$$= J(1,3)(-1)^{\frac{(3-1)(13-1)}{4}}$$

$$= J(1,3), \text{ car } \frac{(3-1)(13-1)}{4} = 6$$

$$= 1$$

$$J(11,13) = J(2,11)(-1)^{\frac{(11-1)(13-1)}{4}}$$

$$= J(2,11), \text{ car } \frac{(11-1)(13-1)}{4} = 30$$

$$= J(1,11)(-1)^{\frac{11^2-1}{8}}$$

$$= J(1,11)(-1), \text{ car } \frac{11^2-1}{8} = 15$$

$$= -1$$

$$J(10,13) = -J(5,13)$$

$$= -J(3,5)(-1)^{\frac{(5-1)(13-1)}{4}}$$

$$= -J(3,5), \text{ car } \frac{(5-1)(13-1)}{4} = 12$$

$$= -J(2,3)(-1)^{\frac{(3-1)(5-1)}{4}}$$

$$= -J(2,3), \text{ car } \frac{(3-1)(5-1)}{4} = 2$$

$$= -J(1,3)(-1)^{3^2-1/8}$$

$$= 1 \text{, car } \frac{3^2-1}{8} = 1$$

$$J(9,13) = J(4,9)(-1)^{\frac{(9-1)(13-1)}{4}}$$

$$= J(4,9) \text{, car } \frac{(9-1)(13-1)}{4} = 24$$

$$= J(2,9)(-1)^{\frac{9^2-1}{8}}$$

$$= J(2,9) \text{, car } \frac{9^2-1}{8} = 10$$

$$= J(1,9)$$

$$= 1$$

$$J(8,13) = -J(4,13)$$

$$= J(2,13)$$

$$= -J(1,13)$$

$$= -1$$

$$J(7,13) = J(6,7)(-1)^{\frac{(7-1)(13-1)}{4}}$$

$$= J(6,7) \text{, car } \frac{(7-1)(13-1)}{4} = 18$$

$$= J(3,7)(-1)^{\frac{7^2-1}{8}}$$

$$= J(3,7) \text{, car } \frac{7^2-1}{8} = 6$$

$= J(1,3)(-1)^{\frac{(3-1)(7-1)}{4}}$

$= -J(1,3)$ , car $\frac{(3-1)(7-1)}{4} = 3$

$= -1$

$J(6,13) = -1$ , voir $J(12,13)$

$J(5,13) = -1$ , voir $J(10,13)$

$J(4,13) = -J(2,13)$

$= J(1,13)$

$= 1$

$J(3,13) = J(1,3)(-1)^{\frac{(3-1)(13-1)}{4}}$

$= J(1,3)$ , car $\frac{(3-1)(13-1)}{4} = 6$

$= 1$

$J(2,13) = -J(1,13)$

$= -1$

$J(1,13) = 1$

On a donc $J(12,13) = 1$ et $12^{\frac{13-1}{2}} = 2985984$

$\equiv 1 \pmod{13}$

$\Rightarrow J(12,13) \equiv 12^{\frac{13-1}{2}} \pmod{13}$

$J(11,13) = -1$ et $11^{\frac{13-1}{2}} = 161051$

$\equiv -1 \pmod{13}$

$\Rightarrow J(11,13) \equiv 11^{\frac{13-1}{2}} \pmod{13}$

$J(10,13) = 1$ et $10^{\frac{13-1}{2}} = 1000000$

$\equiv 1 \pmod{13}$

$\Rightarrow J(10,13) \equiv 10^{\frac{13-1}{2}} \pmod{13}$

$J(9,13) = 1$ et $9^{\frac{13-1}{2}} = 531441$

$\equiv 1 \pmod{13}$

$\Rightarrow J(9,13) \equiv 9^{\frac{13-1}{2}} \pmod{13}$

$J(8,13) = -1$ et $8^{\frac{13-1}{2}} = 262144$

$\equiv -1 \pmod{13}$

$\Rightarrow J(8,13) \equiv 8^{\frac{13-1}{2}} \pmod{13}$

$J(7,13) = -1$ et $7^{\frac{13-1}{2}} = 117649$

$\equiv -1 \pmod{13}$

$\Rightarrow J(7,13) \equiv 7^{\frac{13-1}{2}} \pmod{13}$

$J(6,13) = -1$ et $6^{\frac{13-1}{2}} = 46656$

$\equiv -1 \pmod{13}$

$$\Rightarrow J(6,13) \equiv 6^{\frac{13-1}{2}} \pmod{13}$$

$J(5,13) = -1$ et $5^{\frac{13-1}{2}} = 15625$

$$\equiv -1 \pmod{13}$$

$$\Rightarrow J(5,13) \equiv 5^{\frac{13-1}{2}} \pmod{13}$$

$J(4,13) = 1$ et $4^{\frac{13-1}{2}} = 4096$

$$\equiv 1 \pmod{13}$$

$$\Rightarrow J(4,13) \equiv 4^{\frac{13-1}{2}} \pmod{13}$$

$J(3,13) = 1$ et $3^{\frac{13-1}{2}} = 729$

$$\equiv 1 \pmod{13}$$

$$\Rightarrow J(3,13) \equiv 3^{\frac{13-1}{2}} \pmod{13}$$

$J(2,13) = -1$ et $2^{\frac{13-1}{2}} = 64$

$$\equiv -1 \pmod{13}$$

$$\Rightarrow J(2,13) \equiv 2^{\frac{13-1}{2}} \pmod{13}$$

$J(1,13) = 1$ et $1^{\frac{13-1}{2}} = 1 \equiv 1 \pmod{13}$

$$\Rightarrow J(1,13) \equiv 1^{\frac{13-1}{2}} \pmod{13}$$

(b) On a $E_{15} = \{1,2,3,4,5,6,7,8,9,10,11,12,13,14\}$.

et $\frac{15^2-1}{8} = 28$. Calculons

$$J(14,15) = J(7,15)$$

$$= J(1,7)\,(-1)^{\frac{(7-1)(15-1)}{4}}$$

$$= -J(1,7)$$

$$= -1$$

$$J(13,15) = J(2,13)\,(-1)^{\frac{(13-1)(15-1)}{4}}$$

$$= J(2,13)$$

$$= -1$$

$J(12,15)$ n'est pas défini car $(12,15) \neq 1$

$$J(11,15) = J(4,11)\,(-1)^{\frac{(11-1)(15-1)}{4}}$$

$$= -J(4,11)$$

$$= -J(2,11)\,(-1)^{\frac{11^2-1}{8}}$$

$$= J(2,11)$$

$$= -J(1,11)$$

$$= -1$$

$J(10,15)$ n'est pas défini car $(10,15) \neq 1$

$J(9,15) = 0$ n'est pas défini car $(9,15) \neq 1$

$$J(8,15) = J(4,15)$$

$= J(4,15)$

$= J(2,15)$

$= J(1,15)$

$= 1$

$J(7,15) = -1$, voir $J(14,15)$

$J(6,15)$ n'est pas défini car $(6,15) \neq 1$

$J(5,15)$ n'est pas défini car $(5,15) \neq 1$

$J(4,15) = 1$

$J(3,15)$ n'est pas défini car $(3,15) \neq 1$.

$J(2,15) = 1$

$J(1,15) = 1$

On sait déjà que 3, 5, 6, 9, 10, 12 échouent le test 7.4.

Pour les autres, on a

$$14^{\frac{15-1}{2}} = 14^7 \equiv (-1)^7 \pmod{15}$$

$$\equiv -1 \pmod{15}$$

$\Rightarrow$ 14 n'échoue pas le test

$13^{\frac{15-1}{2}} = 13^7 \equiv (-2)^7 \pmod{15}$

$\equiv -128 \pmod{15}$

$\equiv 7$

=> 13 échoue le test

$11^{\frac{15-1}{2}} = 11^7 \equiv (-4)^7 \pmod{15}$

$\equiv -16384 \pmod{15}$

$\equiv 11 \pmod{15}$

=> 11 échoue le test

$8^{\frac{15-1}{2}} = 8^7 = 2097152 \equiv 2 \pmod{15}$

=> 8 échoue le test

$7^{\frac{15-1}{2}} = 7^7 = 823543 \equiv 13 \pmod{15}$

=> 7 échoue le test

$4^{\frac{15-1}{2}} = 4^7 = 16384 \equiv 4 \pmod{15}$

=> 4 échoue le test

$2^{\frac{15-1}{2}} \equiv 2^7 = 128 \equiv 8 \pmod{15}$

=> 2 échoue le test

=> Ils échouent tous le test sauf 1 et 14

Exercice A: Alain, Béatrice et Catherine sont associés dans une compagnie. Pour communiquer entre eux ils utilisent des codes RSA. Pour simplifier, ils ont tous pris la même clé $n$. Béatrice demande d'utiliser une clé d'encryption $e_B$ et Catherine une clé d'encryption $e_C$. Il se trouve que $(e_B, e_C) = 1$. Alain doit envoyer une information confidentielle $m$ telle que $(m,n) = 1$ à Béatrice et à Catherine. Alain encode donc l'information pour Béatrice dans le message $m_B$ et pour Catherine dans le message $m_C$. Un espion capte les deux messages encodés $m_B$ et $m_C$. Expliquer comment il peut facilement retrouver le message $m$ confidentiel. Ceci signifie qu'une telle pratique n'est pas sécuritaire.

Sol: L'espion connait $m_B, m_C, n, e_B, e_C$. En effet, $n, e_B$ et $e_C$ sont publics.

On a que $m^{e_B} \equiv m_B \pmod{n}$ ①

et $m^{e_C} \equiv m_C \pmod{n}$ ②

De plus, on a $(e_B, e_C) = 1 \Rightarrow \exists\, s, t \in \mathbb{Z}$ tels que $s \cdot e_B + t \cdot e_C = 1$. Ce processus se fait rapidement pour un ordinateur (application de l'algo. d'Euclide).

Par l'équation ①, on a

$$(m^{e_B})^s \equiv m_B^s \pmod{n}$$

Par l'équation ②, on a

$$(m^{e_C})^t \equiv m_C^t \pmod{n}$$

Donc on a

$$(m^{e_B})^s (m^{e_C})^t \equiv m_B^s \cdot m_C^t \pmod{n}$$

$$\Leftrightarrow \quad m^{s \cdot e_B} m^{t \cdot e_C} \equiv m_B^s \cdot m_C^t \pmod{n}$$

$$\Leftrightarrow \quad m^{s \cdot e_B + t \cdot e_C} \equiv m_B^s \cdot m_C^t \pmod{n}$$

$$\Leftrightarrow \quad m \equiv m_B^s \cdot m_C^t \pmod{n}$$

L'espion doit donc trouver $s$ et $t$ en utilisant l'algorithme d'Euclide et calculer le restant de la division de $m_B^s \cdot m_C^t$ par $n$, et il retrouve $m$.

Exercice B : On représente les caractères A, B, ... comme dans le tableau de la question 7 (p.240).

On code un mot comme suit :

1. On remplace les caractères par leur nombre associé
2. Pour chaque caractère, on calcule le reste de la division de $3^n$ par 29, où n est le nombre associé au caractère
3. On trouve les caractères correspondant aux nombres obtenus : ceci donne le mot clé

(a) Coder le mot << JET >>.

(b) Expliquer pourquoi le code est inversible.

(c) Décoder le mot << XMF >>.

Sol : (a) 1. J : 10 ; E : 5 ; T : 20

2. $3^{10} \equiv (3^4)^2 3^2 \pmod{29}$ ; $3^5 \equiv 3^4 3 \pmod{29}$ ; $3^{20} \equiv (3^{10})^2 \pmod{29}$

$\equiv 23^2 3^2 \pmod{29}$ ; $\equiv 23 \cdot 3 \pmod{29}$ ; $\equiv 5^2 \pmod{29}$

$\equiv (23 \cdot 3)^2 \pmod{29}$ ; $\equiv 11 \pmod{29}$ ; $\equiv 25 \pmod{29}$

$\equiv 11^2 \pmod{29}$

$\equiv 5 \pmod{29}$

3. 5 : E | 11 : K | 25 : Y

=> <<JET>> devient <<EKY>>

(b) Comme 29 est premier, $(\mathbb{Z}/29\mathbb{Z})^\times$ est cyclique.

Comme on ne considère pas le caractère □,

on a $3^1 \equiv 3 \pmod{29}$

$3^2 \equiv 9 \pmod{29}$

$3^3 \equiv 27 \pmod{29}$

$3^4 \equiv 23 \pmod{29}$

$3^5 \equiv 11 \pmod{29}$

$3^6 \equiv 4 \pmod{29}$

$3^7 \equiv 12 \pmod{29}$

$3^8 \equiv 7 \pmod{29}$

$3^9 \equiv 21 \pmod{29}$

$3^{10} \equiv 5 \pmod{29}$

$3^{11} \equiv 15 \pmod{29}$

$3^{12} \equiv 16 \pmod{29}$

$3^{13} \equiv 19 \pmod{29}$

$3^{14} \equiv 28 \pmod{29}$

$3^{15} \equiv 26 \pmod{29}$

$3^{16} \equiv 20 \pmod{29}$

$3^{17} \equiv 2 \pmod{29}$

$3^{18} \equiv 6 \pmod{29}$

$3^{19} \equiv 18 \pmod{29}$

$3^{20} \equiv 25 \pmod{29}$

$3^{21} \equiv 17 \pmod{29}$

$3^{22} \equiv 22 \pmod{29}$

$3^{23} \equiv 8 \pmod{29}$

$3^{24} \equiv 24 \pmod{29}$

$3^{25} \equiv 14 \pmod{29}$

$3^{26} \equiv 13 \pmod{29}$

$$3^{27} \equiv 10 \pmod{29}$$

$$3^{28} \equiv 1 \pmod{29}$$

On voit donc que $\langle 3 \rangle = (\mathbb{Z}/28\mathbb{Z})^{\times}$, alors $3^n$ est associé à un unique caractère $\forall n \in \{1, 2, \ldots, 27\}$, le code est donc inversible.

(c) Pour X, on cherche $n \in \{1, 2, \ldots, 27\}$ tel que $3^n \equiv 24 \pmod{29}$. Par le (b), on a que $n = 24$

$\Rightarrow$ X devient X

Pour M, on cherche $n \in \{1, 2, \ldots, 27\}$ tel que $3^n \equiv 13$. Par le (b), on a que $n = 26$

$\Rightarrow$ M devient Z

Pour F, on cherche $n \in \{1, 2, \ldots, 27\}$ tel que $3^n \equiv 6$. Par le (b), on a que $n = 18$

$\Rightarrow$ F devient R

$\Rightarrow$ << XMF >> devient << XZR >>