13. Calcul de $\varphi(n)$ l'indicatrice d'Euler

Soit $E_n = \{ \bar{a} \in \frac{\mathbb{Z}}{n\mathbb{Z}} \ / \ \bar{a}$ est inversible pour $(\cdot) \}$

$= \{ a : 1 \leq a < n \ / \ \Delta(a,n) = 1 \}$

on pose $\varphi(n) = |E_n|$.

Pour $n = p$ (premier), tout entier $a < p$ est premier avec p : $\Delta(a,p) = 1$

donc $\varphi(p) = p-1$. D'une façon générale on montre que

$\varphi(p^m) = p^m - p^{m-1}$ et pour tout entier $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ (p_i premiers)

$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)$.

ex : a) $\varphi(4) = \varphi(2^2) = 2^2 - 2^1 = 2$ et $E_4 = \{1, 3\}$.

b) pour $n = 12 = 2^2 \times 3$, $\varphi(n) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$ et

$E_{12} = \{1, 5, 7, 11\}$.

Petit théorème de Fermat :

Si a est un entier premier avec p (premier) : $\Delta(a,p) = 1$

alors $a^{p-1} \equiv 1 [p]$.

Théorème de Fermat (ou d'Euler)

$\Delta(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 [n]$

ex : soit $n = 12$ et $a = 5$, $\Delta(5, 12) = 1 \Rightarrow 5^4 \equiv 1 [12]$.

14. Cryptosystème RSA

Ce cryptosystème est basé sur la difficulté de la factorisation d'un entier en facteurs premiers.

1. Choisir deux nombres premiers distincts p et q assez grands et calculer $n = pq$.

2. prendre un entier e premier avec $\varphi(n)=(p-1)(q-1)$.

3. calculer d tel que $e.d \equiv 1\ [\varphi(n)]$.

(n, e) est la clé publique.

d est la clé privée.

4. Chiffrement : on transforme le message en un nombre $m<n$ et on calcule $m' = m^e\ [n]$.

5. Déchiffrement : on déchiffre m' par la clé privée d :

$D(m') \equiv m'^d\ [n]$.

Ex : on prend $p=3$, $q=11$ et $e=7$

$n=pq=33 \Rightarrow \varphi(n)=(p-1)(q-1) = 2\times 10 = 20$

$\Delta(7,20)=1 \Rightarrow \exists d$ tel que $7.d\equiv 1\ [20]$, $d=3$.

* chiffrer $m=2$ par $m'^e = 2^7\ [33]$ donc $m'=29$.
* Déchiffrer $m'=29$ par $m'^d = 29^3\ [33]$, d'où $D(m')=2$.

15. Les carrés dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Pour alléger l'écriture on peut écrire a au lieu de $\bar{a}$,

$a\in\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un carré s'il existe $x\in\frac{\mathbb{Z}}{n\mathbb{Z}}$ tel que $a=x^2\ [n]$,

on dit aussi que a est résidu quadratique.

Ex : Dans $\frac{\mathbb{Z}}{7\mathbb{Z}}$ les carrés (non nuls) sont $1, 4, 2=3^2$ et

les non carrés sont $3, 5, 6$.

* on montre d'une façon générale que dans $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, p premier, $p\neq 2$, il y a exactement $\frac{p-1}{2}$ carrés et $\frac{p-1}{2}$ non carrés.
* Pour l'étude des carrés dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ on fait appel au symbole de Legendre **ou** le critère d'Euler :

* Symbole de Legendre :

Soient p un nombre premier impair et a un entier, alors le Symbole de Legendre est défini par :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } \Delta(a,p)=1 \text{ et } a \text{ est un carré (dans } \frac{\mathbb{Z}}{p\mathbb{Z}}). \\ -1 & \text{si } \Delta(a,p)=1 \text{ et } a \text{ n'est pas un carré.} \\ 0 & \text{si } \Delta(a,p)\neq 1 \end{cases}$$

* Critère d'Euler :

Si p est un nombre premier impair et $a \in \mathbb{Z}$, alors :

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} [p].$$

ex : $\frac{\mathbb{Z}}{13\mathbb{Z}}$ admet $\frac{p-1}{2} = 6$ carrés : $1^2=1, 2^2=4, 3^2=9, 4^2=3, 5^2=12, 6^2=10$

et 6 non carrés : $2,5,6,7,8,11$.

pour $a=2$, $\left(\frac{2}{13}\right) \equiv 2^{\frac{13-1}{2}} [13] \equiv -1 [13]$, donc 2 est non carré.

$a=3$, $\left(\frac{3}{13}\right) = 3^6 [13] \equiv 1 [13]$; donc 3 est un carré.

16. construction des corps finis

$(\frac{\mathbb{Z}}{p\mathbb{Z}}, +, \cdot)$ est un corps si p est premier, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est appelé corps premier, $\frac{\mathbb{Z}}{2\mathbb{Z}} = \mathbb{F}_2 = \{0,1\}$ est le plus petit corps fini.

On montre que le cardinal d'un corps fini $\mathbb{F}_q$ est une puissance d'un nombre premier : $|\mathbb{F}_q| = q = p^m$.

$\mathbb{F}_q^* = (\mathbb{F}_q - \{0\}, \cdot)$ est un groupe cyclique :

$(*)$: $\mathbb{F}_q^* = \{\alpha, \alpha^2, \dots, \alpha^{q-1} = 1\} = \langle\alpha\rangle$, α est appelé élément primitif, le polynôme primitif de α est le polynôme unitaire f de degré minimum et vérifiant $f(\alpha)=0$.

ex: dans $\frac{\mathbb{Z}}{7\mathbb{Z}}$, l'élément 3 est primitif car $\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^* = \langle 3 \rangle$

$= \{3^2, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1\}$.

16.1 La représentation (*): $\mathbb{F}_q = \{\alpha, \alpha^2, \ldots, \alpha^{q-1} = 1, 0\}$ est dite description primitive de $\mathbb{F}_q$.

* un polynôme $g(x) \in \mathbb{F}_q(x)$ est irréductible si $g(x) = g_1(x) g_2(x) \Rightarrow g_1(x)$ ou $g_2(x)$ est une constante.

ex: dans $\mathbb{F}_7(x)$ x^2+3 n'est pas irréductible car on peut le factoriser: $x^2+3 = x^2-4 = (x-2)(x+2) = (x+5)(x+2)$.

$g(x) = x^2+4$ est irreductible car on ne peut pas le factoriser en produit de 2 polynômes de degré 1 et $g(x) \neq 0$ pour tout $x \in \mathbb{F}_7$.

16.2 Description polynomiale d'un corps fini

Soit $f(x) \in \mathbb{F}_p[x]$ un polynôme irreductible de degré m alors

$$\mathbb{F}_q = \frac{\mathbb{F}_p[x]}{\langle f(x) \rangle} = \{ b_0 + b_1 \bar{X} + \cdots + b_{m-1} \bar{X}^{m-1} \,/\, b_0, b_1, \ldots, b_{m-1} \in \mathbb{F}_p \}$$ est un corps

de cardinal $q = p^m$. Cettre représentation est appelée description polynomiale de $\mathbb{F}_q$

ex: a) soit $f(x) = x^2+x+1 \in \mathbb{F}_2[x]$, il n'a pas de racines dans $\mathbb{F}_2$: $f(0) \neq 0$, $f(1) \neq 0$ donc il est irreductible et

$\mathbb{F}_4 = \mathbb{F}_{2^2} = \{ b_0 + b_1 X \,/\, b_0, b_1 \in \mathbb{F}_2 \} = \{0, 1, x, 1+x\}$ est un corps de cardinal 4, la somme (+) est définie par:

$(a+bx) + (c+dx) = (a+c) + (b+d)x$ et le produit (.) est défini par $(a+bx)(c+dx) = ac + adx + cbx + bdx^2$, ($x^2+x+1=0 \Rightarrow x^2 = x$)

$= ac + bd(x+1) + (ad+cb)x$

$= (ac+bd) + (bd+ad+bc)x \in \mathbb{F}_4$.

b) construction de $\mathbb{F}_8$:

Soit $f(x) = x^3+x+1 \in \mathbb{F}_2(x)$, il est irreductible car il n'a pas de racines dans $\mathbb{F}_2$, $f(0)\neq 0$, $f(1)\neq 0$ et

$\mathbb{F}_8 = \frac{\mathbb{F}_2[x]}{<f(x)>} = \{ b_0+b_1x+b_2x^2 \mid b_n \in \mathbb{F}_2 \}$ est un corps formé de $2^3=8$ polynômes. la somme est définie par :

$(b_0+b_1x+b_2x^2)+(a_0+a_1x+a_2x^2) = (b_0+a_0)+(b_1+a_1)x+(b_2+a_2)x^2$

pour le calcul du produit x^3 est remplacé par $x+1$:

$x^3+x+1=0 \Rightarrow x^3=x+1$.

par exemple : $x(1+x+x^2) = x+x^2+x^3 = x+x^2+x+1 = x^2+1$.

17. <u>Applications</u> :

<u>Registre à décalage LFSR</u> (linear feedback shift register) :

est un procédé pour engendrer des suites de nombres pseudo-aléatoires.

Soit $\varphi(x) = x^r - q_{r-1}x^{r-1} \ldots - q_1x - q_0 \in \mathbb{F}_p(x)$.

considérons la suite $(u_n)_{n\geq 0}$ définie par les valeurs initiales

* $u_0, \ldots, u_{r-1}$ et

** la relation de recurrence : $u_n = u_{n-r}q_0 + u_{n-r+1}q_1 + \cdots + u_{n-1}q_{r-1}$

La suite (u_n) est périodique, elle est de periode maximale $T = p^r-1$ si le polynôme $\varphi(x)$ est primitif sur $\mathbb{F}_p$.

Examinons le cas binaire $p=2$:

<u>Ex</u>s a) soit $\varphi(x) = x^2+x+1 \in \mathbb{F}_2(x)$ et $(u_0,u_1)=(0,1)$.

Alors $\varphi(x) = x^2-1.x-1$ et $(q_1,q_0)=(1,1)$.

$u_n = u_{n-2}q_0 + u_{n-1}q_1 = u_{n-2}+u_{n-1}$

$u_2 = u_1 + u_0 = 1+0 = 1$, $u_3 = u_2 + u_1 = 1+1 = 0$ et on obtient la suite $\underbrace{011}\underbrace{011}\underbrace{011}\ldots$ périodique et sa période $T = 3 = 2^{deg(\varphi)} - 1 = 2^2 - 1 = 3$, elle est maximale car φ est primitif : $x^2 = x+1$

$$x^3 = x(x+1) = x^2 + x = x+1+x = 1$$

b) Soit $\varphi(x) = x^3 + x + 1 \in \mathbb{F}_2(x)$ et $(u_0, u_1, u_2) = (1,1,1)$.

Alors $\varphi(x) = x^3 - 0.x^2 - 1.x - 1$ et $(q_2, q_1, q_0) = (0,1,1)$.

$$u_n = u_{n-3}\,q_0 + u_{n-2}\,q_1 + u_{n-1}\,q_2 = u_{n-3} + u_{n-2}$$

d'où la suite $\underbrace{1110010}\underbrace{1110010}\ldots\ldots$ et

$T = 7 = 2^{deg\varphi} - 1 = 2^3 - 1$ elle est maximale car $\varphi(x)$ est primitif : $x^3 = x+1$, $x^4 = x^2 + x$, $x^5 = x^3 + x^2 = x^2 + x + 1$,

$x^6 = x^3 + x^2 + x = x+1+x^2+x = x^2+1$

$x^7 = x^3 + x = x+1+x = 1$.

c) Soit $\varphi(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2(x)$ et $(u_0 u_1 u_2 u_3) = 1001$.

Alors $\varphi(x) = x^4 - 1.x^3 - 1.x^2 - 1.x - 1$ et $(q_3, q_2, q_1, q_0) = (1111)$.

$u_n = u_{n-4} + u_{n-3} + u_{n-2} + u_{n-1} \Rightarrow (u_n) = \underbrace{10010}\underbrace{10010}\underbrace{10010}\ldots$

et $T = 5 \neq 2^4 - 1 = 15$, T n'est pas maximal car $\varphi(x)$ n'est pas primitif :

$x^4 = x^3 + x^2 + x + 1$

$x^5 = x^4 + x^3 + x^2 + x = (x^3 + x^2 + x + 1) + x^3 + x^2 + x = 1$.

Dans les suites obtenues on remarque que le nombre des 1 est presque égal au nombre des 0.