NOM GUEDJ

Prénom Alexandre

Promo 2018

Date 23/03/16

2 0 ,

GUEDJ Alexandre
L3 - 2015

$\frac{22}{25}$

MATIÈRE Théorie des Graphes.

Exercice 1.

Dans $(\mathbb{Z}/48\mathbb{Z}, \oplus)$, l'ordre de $\overline{20}$ est un diviseur de 48.

Liste des diviseurs de 48 : $\{1, 2, 4, 6, 8, 12, 24, 48\}$.

Pour trouver l'ordre de $\overline{20}$, on trouve x tel que

$\overline{20}x = \overline{0}$.

Si 20 et 48 sont premiers entre eux, alors l'ordre est 48.

Or, leur PGCD est 4. On teste donc avec les diviseurs restant.

$\overline{20} \times 1 = \overline{20}$

(2)

$\overline{20} \times 2 = \overline{40}$

$\overline{20} \times 4 = \overline{32}$

$\overline{20} \times 8 \quad \overline{16}$

$\overline{20} \times 12 = \overline{0}$.

Ainsi, l'ordre de $\overline{20}$ est 12.

Exercice 2 -

a - Dans $(\mathbb{Z}/48\mathbb{Z}, \oplus, \odot)$, le nombre d'éléments inversibles est défini par $\varphi(48)$. $48 = 2^4 \times 3$, ainsi :

$$\varphi(48) = 2^4\left(1 - \frac{1}{2}\right)2$$
$$= 16.$$ Il y a 16 éléments inversibles. 2

Les éléments inversibles sont ceux qui sont premiers avec 48 et compris entre 0 et 47 :

$\{\bar{1}, \bar{5}, \bar{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, \overline{35}, \overline{37}, \overline{41}, \overline{43}, \overline{47}\}$

Nous obtenons bien 16 éléments inversibles.

b - L'inverse de $\bar{7}$ est $\bar{x}$ tel que $\bar{7}\bar{x} = \bar{1}$, ou encore

$7x - 1 \equiv 0[48]$. $48 \mid 7x - 1$, $7x - 48k = 1$.

On applique l'algorithme afin de trouver x : 2

K	x	r	q
1	0	48	
0	1	7	
1	-6	6	6
-1	7	1	1
—	—	0	6

Ainsi, l'inverse de $\bar{7}$ est $\bar{7}$.

e - $\bar{7}x + \overline{12} = \bar{5}$

donc $\bar{7}x + \overline{12} + \overline{36} = \bar{5} + \overline{36}$. $\overline{36}$ étant l'inverse de $\overline{12}$.

donc $\bar{7}x = \overline{41}$.

donc $\bar{7} \times \bar{7}x = \overline{41} \times \bar{7}$

donc $x = \overline{47}$

(2)

Exercice 3

a - R_{48} désigne les elements inversibles dans $\mathbb{Z}/48\mathbb{Z}$. Or, le PGCD de 26 et 48 est 2, 26 et 48 n'étant pas premiers entre eux, $\overline{26}$ n'est pas inclu dans R_{48}. (2)

b - Trouvons u tel que $\bar{x}^{13u} = \bar{x}$. D'après le théorème d'Euler, on sait que $\bar{x}^{\varphi(n)} = \bar{1}$ $\forall x \in R_n$.

Ainsi, trouvons u tel que $13u \equiv 1 [16]$, 16 étant $\varphi(48)$.

K	u	r	q
1	0	16	
0	1	13	
1	-1	3	1
-4	5	1	4
—	—	0	3

$u = 5$.

On a finalement $f^{-1}(x) = x^5$.

(2)

Exercice 4.

a. Si $P(X)$ réductible, alors il peut s'écrire sous la forme

$(X+a)(X^2+bX+c)$. Trouvons les valeurs a, b, c :

$= X^3 + bX^2 + cX + aX^2 + abX + ac$

$= X^3 + X^2(a+b) + X(ab+c) + ac$. Par identification, on a :

$a + b = 1$
$ab + c = 0$
$ac = 1$. Si $ac = 1$, alors $a = c = 1$.

2

Dans ce cas, $1 + b = 1$, $b = 0$.

Or, si $a = 1$, $b = 0$, $c = 1$, on a $ab + c = 1$, et non 0.
Ainsi, on démontre que $P(X) = X^3 + X^2 + 1$ est irréductible.

b. Il y a 8 éléments du corps $(K = \mathbb{F}_2[X]/P(X), \oplus, \odot)$.

2

NOM GCEDJ

Prénom Alexandre

Promo 2018

Date 23/03/16.

MATIÈRE Théorie des Groupes

d. On doit trouver x tel que $\theta x = \overline{1}$. Or, on sait que $\theta^3 + \theta^2 + 1 = 0$, ou encore $\theta^3 + \theta^2 = 1$, ou encore $\theta(\theta^2 + \theta) = 1$. Ainsi, on en déduit que l'inverse de θ est $\underline{\theta^2 + \theta}$.
On aurait pu également utiliser l'algorithme ~~afin~~ d'Euclide étendu afin de trouver x.

3

e. On sait que $\theta^3 = \theta^2 + 1$. On obtient le tableau suivant :

θ	θ
θ^2	θ^2
θ^3	$\theta^2 + 1$
θ^4	$\theta^2 + \theta + 1$
θ^5	$\theta + 1$
θ^6	$\theta^2 + \theta$
θ^7	1
θ^8	θ

3