rcoRATTRAPAGE « Groupes »

Ni documents, ni machines, ni téléphones

(étudiants chinois : dictionnaires autorisés)

Tout résultat doit être justifié par un théorème du cours (qui sera énoncé), un raisonnement et/ou un calcul

Exercice 1. 2 pts environ

Déterminer le plus petit entier positif x tel que 7x≡1[41]

Solution. algorithme d'euclide étendu

u	v	r	
1	0	41	
0	1	7	
1	-5	6	5
-1	6	1	1
...	...	0	6

donc -1.41+(6)7=1

et l'ensemble des couples (u,v) est $\{(-1-7t, 6+41t)t\in\mathbb{Z}\}$ donc 6 est la plus petite solution positive.

Bien sûr on peut trouver 6 par calcul mental, et c'est le plus petit si on vérfie que 1,2,3,4,5 ne convienne pas

Exercice 2. On considère le groupe $(R_{21},.)$ 6 pts environ

1. Déterminer le nombre d'éléments de R_{21}.
2. On considère l'application $f\colon R_{21}\longrightarrow R_{21}$ définie comme suit: $\forall x\in R_{21}, f(x)=x^5$.

a. Déterminez l'application f^{-1}

b. Résoudre l'équation f(x)=$\bar{4}$.

Solution.

1. $\varphi(21)=\varphi(3)\varphi(7)=2\,6=12$.

2. a. méthode rsa on cherche u tel que 5u≡1[12]; soit par l'algo d'euclide soit par calcul 5.5≡1[12], donc $\forall x\in R_{21}$, $f^{-1}(x)=x^5$

b. f(x)=$\bar{4}$. $\Longleftrightarrow x=f^{-1}(\bar{4})=\bar{4}^5$.

$\bar{4}^2=\overline{16}, \bar{4}^3=\overline{64}=\bar{1}$,$\bar{4}^4=\bar{4}$,$\bar{4}^5=\overline{16}$

Exercice 3. On considère l'anneau de polynômes $F_2[X]$ 12 pts environ

1. Montrer que le polynôme X^3+X+1 est irréductible dans $F_2[X]$
2. On définit comme dans le cours K=$F_2[X]/X^3+X+1$

Déterminer le nombre de ses éléments

3. On désigne par θ la classe de X

a. Déterminer le plus petit entier k>0 tel que $\theta^k=1$

b. Calculer $\theta(\theta^2+1)$.

4. Déterminer le polynôme unitaire B(X) de plus bas degré tel que XB(X)≡1$[X^3+X+1]$

Solution.

1. supposons qu'il n'est pas irréductible alors X^3+X+1=(X+a)$(X^2+$bX$+c)$ (a,b,c dans F_2)

alors $\begin{cases} a+b=0 \\ \mathrm{ab}+c=1 \\ \mathrm{ac}=1 \end{cases}$ donc a=c=1 et b=1 d'où 1+=1, absurde.

2. ce corps représente les restes possibles dans la division par un polynôme de degré 3, donc tous les polynômes de degré inférieur ou égal à 2:2*2*2=8

3. d'après le cours θ est un générateur du groupe $F_2[X]/X^3+X+1\backslash\{0\}$, donc il est d'ordre 7

b. $\theta(\theta^2+1)$=$\theta^3+\theta=+1$ donc (θ^2+1) est l'inverse de θ

4. Dire que XB(X)≡1$[X^3+X+1]$ signifie que B(θ) est l'inverse de θ donc B(θ)=θ^2+1 d'où B(X)=X^2+1