357 Exercices utilisant le corps $\mathbb{Z}/n\mathbb{Z}$

Ex 1 Congruences et équations diophantiennes Francon TP1 et 1.9 p21

1) Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation $\bar{3}x+\bar{2}=-\bar{1}$

2) Résoudre le système suivant : $\begin{cases} 3x+2 \equiv -1 \ (5) \\ 3x-1 \equiv 3 \ (7) \end{cases}$

3) Résoudre le système suivant $\begin{cases} 5x+2y \equiv 3 \ (6) \\ 2x+4y \equiv 1 \ (5) \end{cases}$

Ex 2 . Codage RSA Francon ex 1.12 p 25

On se donne p, q deux nombres premiers distincts

1) Justifier que pour $a \in \mathbb{Z}$ non divisible par q et p, on a
$$a^{(p-1)(q-1)} \equiv 1 \ (pq)$$

2) Soit $d \in [\![1, (p-1)(q-1)]\!]$ premier avec $(p-1)(q-1)$. Justifier l'existence de $e \in [\![1, (p-1)(q-1)]\!]$ tel que $ed \equiv 1 \ ((p-1)(q-1))$

3) Montrer que $\forall a \in \mathbb{Z}$, $a^{de} \equiv a \ [pq]$

Ex 3 - Petit théorème de Fermat, Rombaldi p41

L'anneau $\mathbb{F}_p[X]$ est utilisé pour donner une démonstration du petit théorème de Fermat. Soient $p \geq 2$ un nombre premier et $P(X) = X^p - X$ dans $\mathbb{F}_p[X]$

1) Montrer que $P(X+\bar{1}) = P(X)$ dans $\mathbb{F}_p[X]$

2) En déduire que $\binom{p}{k} \equiv 0 \ (p)$ et $\binom{p-1}{k} \equiv (-1)^k \ (p)$

$\forall k \in [\![1, p-1]\!]$

3) En déduire le petit théorème de Fermat.

Exercice 4 : X-ENS Alg. 2 Les cailloux pts

1) Soit $A = (a_{ij}) \in M_n(\mathbb{R})$ avec $a_{ii} = 0$ $\forall i$ et $a_{ij} = \{\pm 1\}$ $i \neq j$
Si n est pair, montrer que A est inversible

2) On dispose de $2n+1$ cailloux, $n \geq 1$. On suppose que chaque sous-ensemble de $2n$ cailloux peut se partager en deux paquets de même masse totale. Montrer que tous les cailloux ont la même masse.

Exercice 5 Delaunay Pl ex 24 p57 Carré dans $\mathbb{Z}/p\mathbb{Z}$ (Sympl) avec Petito Thm 5

Soit p un nombre premier ≥ 3.

a) Quel est le nombre de carré dans $\mathbb{Z}/p\mathbb{Z}$.

b) On suppose que $p \equiv 1 (4)$. Justifier que $\overline{-1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ en calculant de 2 façons le choix de congruence de $(p-1)!$

c) On suppose que $p \equiv 3 (4)$, montrer que $\overline{(-1)}$ n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

$x = 4\ [5]$ $\qquad n = 5 \times 6 \times 7$

$x = 3\ [6]$ $\qquad = 210$

$x = 2\ [7]$ $\qquad A_1 = 42 \quad A_2 = 35 \quad A_3 = 30$

$A_1 u_1 + A_2 u_2 + A_3 u_3 = 1$

$1 = A_1 \wedge A_2 \wedge A_3$

~~$= 5\ 42 \wedge (35 \wedge$~~

$35 = 1 \times 30 + 5$

$30 =$

$A_2 \wedge A_3 = 35 \wedge 30 = 5$

$42 = 8 \times 5 + 2$

$5 = 2 \times 2 + 1$

$1 = A_1 \wedge 5 = 42 \wedge 5$

$1 = 5 - 2 \times 2$

$1 = 5 - 2 \times (42 - 8 \times 5)$

$1 = 17 \times 5 - 2 \times 42.$

$= 5 - 2 \times 42 + 16 \times 5$

$= 17 \times 5 - 2 \times 42.$

$= 17 \times (35 - 1 \times 30) - 2 \times 42.$

$= 17 \times 35 - 17 \times 30 - 2 \times 42$

$= -2 \times 42 + 17 \times 35 - 17 \times 30$

$\Leftrightarrow k_0 = -8 \times 42 + 3 \times 17 \times 35 - 2 \times 17 \times 30$

$= 429$

210

2.

$9 + 210\,\mathbb{Z}$

Rétlock si $n_1 \wedge n_2 \wedge n_3 = 1$ $\qquad n = n_1 \times n_2 \times n_3$

calcule $A_1 = \frac{n}{n_1} \quad A_2 = \frac{n}{n_2} \quad A_3 = \frac{n}{n_3}$

puis ...

$x = 2 \ (4)$
$x = 3 \ (5)$
$x = 1 \ (9)$

$A_1 = \frac{180}{4} = 45 \qquad A_2 = \frac{180}{5} = 36 \qquad A_3 = 20$

$180\ e_1 \quad A_1 u_1 + A_2 u_2 + A_3 u_3 = 1$

$A_2 \wedge A_3 = 4 = 2 \times 20 - 1 \times 36$

$1 = A_1 \wedge A_2 \wedge A_3 = A_1 \wedge (A_2 \wedge A_3)$

$= 45 \wedge 4.$

$= 1 \times 45 - 4 \times 11$

$45 = 11 \times 4 + 1$

$36 = 1 \times 20 + 16$
$20 = 1 \times 16 + 4$
$16 = 4$
$4 = 20 - 1 \times 16$
$4 = 20 - 1 \times (36 - 1 \times 20)$
$= 20 - 36 + 20$
$= 2 \times 20 - 1 \times 36$

$1 = 1 \times 45 - (2 \times 20 - 1 \times 36) \times 11$

$= 45 - 22 \times 20 + 11 \times 36$

$= 1 \times 45 - 22 \times 20 + 11 \times 36$

$= 1 \times 45 + 11 \times 36 - 22 \times 20$

$= 1 \times A_1 + 11 \times A_2 - 22 \times A_3$

$= 2 A_1 + 3 \times 11 \times A_2 - 22 \times A_3$

$= 2 \times 45 + 33 \times 36 - 22 \times 20$

$\beta = 838 + 180 k$

$= 118 + 180 k$

Rifle

L357 Exercices utilisant le corps $\mathbb{Z}/p\mathbb{Z}$

Ex1 Resolution de l'équation dans $\mathbb{Z}/p\mathbb{Z}$

1) Eq. de degré 1 Fermont

Resoudre dans $\mathbb{Z}/5\mathbb{Z}$, l'equation $\overline{3}x + \overline{2} = \overline{-1}$

2) Eq de degré 2 X ENS Alg 1

m.que pour tout nbre premier p, il existe un entier naturel n tel que.

$6n^2 + 5n + 1 \equiv 0 \ [p]$

Ex2: Demonstration du pti th de Fermat en utilisant $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ Rombaldi

Soient p un nbre premier $p \geq 2$. et $P(X) = X^p - X$ dans $\mathbb{F}_p[X]$

1) m.que $P(X+1) = P(X)$ ds $\mathbb{F}_p[X]$

2) En deduire que $\binom{p}{k} \equiv 0 \ [p]$ et $\binom{p-1}{k} \equiv (-1)^k \ [p]$ pour tout entier $k \in [\![1; p-1]\!]$

3) En déduire le petit th. de Fermat

ex3 (Cricket Ensisheim) X ENS Alg 1

1 a) On dit qu'un polynôme non nul de $\mathbb{Z}[X]$ est primitif si le pgcd de ses coefficients est egal à 1

m. que le produit de 2 polynômes primitifs de $\mathbb{Z}[X]$ est primitif

b) Pour $A \in \mathbb{Z}[X]$ non nul, on appelle contenu de A et on note $c(A)$ le pgcd des coefficients de A

Soit A et B deux polynômes non nuls de $\mathbb{Z}[X]$ mq $c(AB) = c(A)c(B)$

2) Soit $A = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \quad A \in \mathbb{Z}[X]$

p un nombre premier

on suppose que. $p \nmid a_n$

. pour tout $k \in [\![0, n-1]\!]$ $p \mid a_k$.

. $p^2 \nmid a_0$

m que A est irréductible dans $\mathbb{Q}[X]$

Ex4: Soit p un nombre premier. X ENS Alg 1

1) Soit q un nombre premier qui divise $p-1$

Etablir l'existence d'un el^t de $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ d'ordre q

2) Soit q un nbre premier et $\alpha \in \mathbb{N}^*$ tq q^α divise $p-1$

montrer l'existence d'un el^t de $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ d'ordre q^α

3) En déduire $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est cyclique.