UNIVERSITÉ DE RENNES 1

Théorie des nombres

Devoir à la maison (à rendre la semaine du 20 octobre)

Exercice 1

On considère l'anneau quotient

$$K = \mathbb{F}_3[X]/\langle X^2 + X + 2\rangle.$$

On note α l'image de X dans K.

1 Montrer que K est un corps et déterminer sa caractéristique. Donner la dimension de K comme $\mathbb{F}_3$-espace vectoriel, la base canonique de K ainsi que le nombre d'éléments de K.

2 Quel est l'ordre possible d'un élément de $K^\times$? Montrer que α est primitif.

3 Déterminer le nombre d'éléments primitifs de $K^\times$. Déterminer l'expression de ces derniers dans la base canonique.

4 Le polynôme $X^4 + X^3 + X^2 + X + 1$ a-t-il une racine dans K ?

Exercice 2

Soit p un nombre premier. Pour tout entier m non multiple de p, on note $m^\vee$ un entier tel que $mm^\vee \equiv 1 \mod p^2$.

1 Montrer que si $p > 2$, alors $1^\vee + 2^\vee + \cdots + (p-1)^\vee = 0 \mod p$.

2 On suppose $p > 3$.

a En développant le polynôme unitaire $P = \prod_{i=1}^{p-1}(X - i)$ on obtient dans $\mathbb{Z}[X]$

$$\prod_{i=1}^{p-1}(X - i) = X^{p-1} + a_{p-2}X^{p-2} + \cdots + a_1 X + (p-1)!.$$

Montrer que

$$a_1 \equiv (1^\vee + 2^\vee + \cdots + (p-1)^\vee)(p-1)! \mod p^2.$$

b Montrer que la réduction de P modulo p est égal à $X^{p-1} - 1$ puis que les entiers $a_{p-2}, \ldots, a_2$ sont divisibles par p.

c Montrer que $1^\vee + 2^\vee + \cdots + (p-1)^\vee = 0 \mod p^2$.

Exercice 3

1 Soient $a, b \geqslant 1$ des entiers. Montrer que si il existe une infinité de nombres premiers congrus à b modulo a, alors a et b sont premiers entre eux.

En 1838, J. P. G. Lejeune Dirichlet a montré que la réciproque était vraie, un résultat connu sous le nom de théorème de la progression arithmétique :

Théorème (J. P. G. Lejeune Dirichlet 1838)**.** *Soient a, b des entiers $\geqslant 1$ premiers entre eux. Alors il existe une infinité de nombres premiers congrus à b modulo a.*

Le but de cet exercice est de démontrer le cas particulier $b = 1$ du théorème de ce théorème. Dans la suite on supposera $b = 1$ et $a \geqslant 2$.

2 Soit $P \in \mathbb{Z}[X]$ un polynôme non constant.

a Montrer que la suite $(P(n))_{n\in\mathbb{N}}$ prend une infinité de valeurs qui ne sont pas des nombres premiers.

b Montrer que l'ensemble des nombres premiers p tel qu'il existe $n \in \mathbb{N}$ tel que $p|P(n)$ est un ensemble infini.

3 On note $\Phi_a \in \mathbb{Z}[X]$ le a-ème polynôme cyclotomique et on pose $P = \prod_{d|a,d\neq a} \Phi_d(X)$. On se propose de montrer dans cette question qu'il existe un nombre premier p et un entier n tels que p divise $\Phi_a(n)$ mais p ne divise pas $P(n)$.

a Justifier l'existence d'un entier $N > 1$ et de polynômes $A, B \in \mathbb{Z}[X]$ tel que

$$A\Phi_a + BP = N.$$

b Montrer que l'on peut trouver un entier n et un nombre premier p divisant $\Phi_a(n)$ mais ne divisant pas N.

c Conclure.

4 Montrer que n est d'ordre a dans $\mathbb{F}_p^\times$.

5 Montrer que p est congru à 1 modulo a puis qu'il existe une infinité de nombres premiers congrus à 1 modulo a.