UNIVERSITÉ DE RENNES 1

Théorie des nombres

Feuille n° 2 : Réciprocité quadratique

Carrés dans les corps finis

Test de compréhension

Test 1.

a. Est-ce que 94 est un carré modulo 131 ?

b. Calculer $\left(\frac{58}{77}\right)$, $\left(\frac{19}{41}\right)$, $\left(\frac{77}{91}\right)$, $\left(\frac{28}{59}\right)$.

Reponses : oui, 1,-1,0,1.

Exercices

Exercice 2.

Résoudre l'équation aux congruences $x^2 \equiv 39 \pmod{105}$.

Exercice 3.

Soit x un entier relatif, soit $n = x^2 - x + 1$ et soit p un diviseur premier de n.

1. Quel est le discriminant du polynôme $X^2 - X + 1$?
2. Montrer que -3 est un carré modulo p.
3. En déduire que $p = 3$ ou $p \equiv 1 \pmod{3}$.

Exercice 4.

1. Déterminer les nombres premiers p tels que 5 soit un carré modulo p, (montrer que ce sont $2, 5$ et les $p = \pm 1 \pmod{5}$).
2. Déterminer les nombres premiers p tels que 7 soit un carré modulo p (on explicitera cela en fonction de la classe de p modulo 28, en distingant les cas $p = 2$ et $p = 7$),
3. Déterminer les nombres premiers p tels que 6 soit un carré modulo p (on explicitera cela en fonction de la classe de p modulo un certain entier N)

Exercice 5.

a. Soit n un entier non multiple de 3. Montrer que $4n^2 + 3$ possède un facteur premier congru à 7 modulo 12.

b. Montrer qu'il existe un nombre infini de nombres premiers congrus à 7 modulo 12

Exercice 6.

Soit p un nombre premier tel que $p = 4l + 1$ pour un certain nombre premier l. Montrer que 2 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exercice 7. Carrés modulo n.

Le problème consiste a déterminer à quelle condition un nombre a est un carré modulo n lorsque n n'est pas premier, sous l'hypothèse $a \wedge n = 1$.

1. Soit $n \geq 1$ un entier et $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ sa décomposition en facteurs premiers. Montrer que a est un carré modulo n ssi a est un carré modulo $p_i^{\alpha_i}$ pour tout i.
2. Supposons maintenant $n = p^\alpha$, pour un certain nombre premier impair p. Supposons $a \in \mathbb{Z}$ premier à p. Montrer que a est un carré modulo p^α ssi a est un carré modulo p.
   Indication : montrer que si $a \equiv x^2 \pmod{p^k}$, il existe $u \in \mathbb{Z}$ tel que $(x + p^k u)^2 \equiv a \pmod{p^{k+1}}$.
3. Montrer de même que si a est un entier impair et si $\alpha \geqslant 3$, alors a est un carré modulo 2^α si et seulement si $a \equiv 1 \pmod 8$.
   Indication : on pourra chercher u tel que $(x + 2^{k-1}u)^2 \equiv a \pmod{2^{k+1}}$.
4. Est-ce que $125, 131$ sont des carres modulo 456 ?
5. Soit $n = 2^{\alpha_0} p_1^{\alpha_1} \dots p_r^{\alpha_r}$ (avec $\alpha_0 = 0$ si n est impair), et a premier avec n. Montrer que a est un carré modulo n si et seulement si
   a. pour tout $i \geq 1$, $\left(\frac{a}{p_i}\right) = 1$
   b. $a \equiv 1 \pmod 8$ si $\alpha_0 \geq 3$, et $a \equiv 1 \pmod 4$ si $\alpha_0 = 2$ (pas de condition si $\alpha_0 \leq 1$).

Exercice 8.

Soit $\mathbb{F}_q$ un corps fini à $q = p^\alpha$ éléments, de caractéristique p. Étant donné $a \in \mathbb{F}_q$, on définit la *norme* de a (vis à vis de l'extension $\mathbb{F}_p \subset \mathbb{F}_q$) ainsi : $N(a) \in \mathbb{F}_q$ est le déterminant de l'application F_p-linéaire $\mu_a : F_q \to F_q$ définie par $\mu_a : x \mapsto ax$.

Soit $\phi : F_q \to F_q$ le morphisme de Frobenius. On admet dans un premier temps que $N(a) = \prod_{i=0}^{\alpha-1} \phi^i(a)$.

a. Montrer que $N(a) = a^{\frac{q-1}{p-1}}$.

b. Montrer que a est un carré dans $\mathbb{F}_q$ si et seulement si $N(a)$ est un carré dans $\mathbb{F}_p$.

On veut maintenant démontrer que $N(a) = \prod_{i=0}^{\alpha-1} \phi^i(a)$.

c. Supposons le résultat connu si $a \in \mathbb{F}_q$ est un générateur du groupe cyclique $\mathbb{F}_q^\times$. Montrer qu'on peut en déduire le résultat pour tout $a \in \mathbb{F}_q$.

d. Supposons donc à partir de maintenant que a est un générateur du groupe cyclique $\mathbb{F}_q^\times$, et soit P le polynôme minimal de a. Montrer que $\deg P = \alpha$ et que $1, a, a^2, \dots a^{\alpha-1}$ est une $\mathbb{F}_p$-base de F_q.

e. Quelle est la matrice de μ_a dans cette base ? Vérifier que son déterminant est égal, au signe près, au coefficient constant de P.

f. Montrer les racines de P sont les $\phi^i(a)$ pour $i = 0, \dots, \alpha - 1$.

g. Conclure que $N(a) = \prod_{i=0}^{\alpha-1} a^{p^i}$.

Exercices supplémentaires

Exercice 9.

On fixe p un nombre premier, et n un entier tel que $n \wedge p = 1$.

Le but de l'exercice est de montrer que le polynome cyclotomique Φ_n est irreductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ ssi la classe de p dans $\mathbb{Z}/n\mathbb{Z}^*$ engendre le groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}^*$.

Soit Ψ_n l'image du polynôme cyclotomique Φ_n dans $\mathbb{Z}/p\mathbb{Z}[X]$, et K une extension finie de $\mathbb{Z}/p\mathbb{Z}$ dans laquelle Ψ_n est scindé. On note $U \subset K^\times$ le sous-groupe des racines n-ièmes de l'unité, et $U^* \subset U$ le sous-ensemble des racines primitives n-ièmes de l'unité dans K. On note $\phi : K \to K$ l'automorphisme de Frobénius défini par $\phi : x \mapsto x^p$.

a. Soit $f \in \mathbb{Z}/p\mathbb{Z}[X]$ un polynôme unitaire, scindé dans K. Montrer que si $\alpha \in K$ est une racine de f alors α^p aussi.

   Étant donné $\alpha \in K$, on définit $\Lambda_\alpha = \{\alpha^{p^k} | k \in \mathbb{Z}\}$.

b. Soit $\alpha \in K$ une racine de Ψ_n. Montrer que pour tout entier $k \wedge n = 1$, α^k est encore une racine de Ψ_n et que $\{\alpha^k | k \wedge n = 1\} = U^*$.

c. Supposons que la classe de p dans $\mathbb{Z}/n\mathbb{Z}^*$ engendre le groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}^*$. On veut démontrer que Ψ_n est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.

   (i) Soit $F \in \mathbb{Z}/p\mathbb{Z}[X]$ un diviseur irréductible de Ψ_n, et $\alpha \in K$ une racine de F. Montrer que $\Lambda_\alpha = U^*$.

   (ii) En déduire que Ψ_n est irréductible.

   On va maintenant démontrer la réciproque. Dans toute la suite, on fixe α une racine de Ψ_n.

d. Soit $P \in K[X]$ le polynôme défini par $P = \prod_{\lambda \in \Lambda_\alpha} (X - \lambda)$. Montrer que P est un diviseur de Ψ_n dans $K[X]$.

e. Montrer que les coefficients de P sont fixes par l'action de l'automorphisme de Frobenius de K. En déduire que P appartient à $\mathbb{Z}/p\mathbb{Z}[X]$, et que P est aussi un diviseur de Ψ_n dans $\mathbb{Z}/p\mathbb{Z}[X]$.

f. En déduire que si $\Lambda_\alpha \subsetneq U^*$, Ψ_n n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.

g. Considérons le cas particulier où $n = 12$ et $p = 5$, utiliser la question précédente pour montrer que Φ_{12} n'est pas irréductible modulo 5.

h. Montrer en général que si la classe de p dans $\mathbb{Z}/n\mathbb{Z}^*$ n'engendre pas le groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}^*$, alors Φ_n n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.