Université de Strasbourg,
Département de Mathématiques

Septembre 2019
Agrégation Interne
Arithmétique

ARITHMETIQUE

Exercice 1 Trouver des entiers r et s tels que $547r + 632s = 1$. Est-ce qu'il existe des entiers r et s tels que $1841r + 3647s = 1$?

Exercice 2 Démontrer que l'équation en nombres entiers $x^2 + 1 = 3y^2$ n'admet pas de solution.

Exercice 3 Résoudre dans $\mathbb{Z}$ la congruence $x^2 + 3 = 0\, mod 7$.

Exercice 4 (Résidus quadratiques) Soit n un entier, ≥ 2 et p un nombre premier impair. On dit que x est un carré ou résidu quadratique (modulo n) s'il existe un $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $y^2 = x\,(mod\, n)$.

a) Déterminer les résidus quadratiques pour $n = 13$ et $n = 19$.

b) Montrer que si $n = p$ est un premier impair alors il y a exactement $(p+1)/2$ résidus quadratiques et que chaque résidu non-nul a exactement deux racines carrées.

c) Supposons maintenant que p soit un premier congru à 3 modulo 4. Montrer que si x est un carré modulo p alors ses racines carrées sont $x^{(p+1)/4}$ et $-x^{(p+1)/4}$.

d) Soit n de la forme $n = pq$ où p et q sont des nombres premiers distincts. Montrer que x est un carré modulo n si et seulement si ses réductions dans $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ sont des carrés. En déduire le nombre de résidus quadratiques. Discuter le nombre de racines carrées d'un élément donné.

Exercice 5 Résoudre les systèmes de congruence suivants

$$\left\{ \begin{array}{rcll} x & \equiv & 7 & (9) \\ x & \equiv & 13 & (23) \\ x & \equiv & 1 & (2) \end{array} \right\}$$

$$\left\{ \begin{array}{rcll} x & \equiv & 7 & (9) \\ x & \equiv & 5 & (6) \\ x & \equiv & 3 & (4) \end{array} \right\}$$

$$\left\{ \begin{array}{rcll} x & \equiv & 7 & (9) \\ x & \equiv & 4 & (6) \\ x & \equiv & 2 & (4) \end{array} \right\}$$

POLYNOMES

Exercice 6 Dans cet exercice le corps de coefficients est de caractéristique zéro (par exemple le corps des réels).

a) Calculer le pgcd de A(X) et de B(X) dans les cas suivants :

i) $A(X) = X^5 + X^3 + X^2 + 1$ et $B(X) = X^4 + X^3 + 2X^2 + X + 1$,

ii)$A(X) = X^4 + X^3 + 6X^2 + 4X + 8$ et $B(X) = X^5 + 3X^4 + 7X^3 + 13X^2 + 12X + 4$.

b) On reprend les exemples de la question a). L'équation

$$S(X)A(X) + T(X)B(X) = X^3 + X$$

admet-elle des solutions dans chacun des deux cas ? Si oui, les déterminer toutes.

c) Soient $A(X) = X^3 + 1$ et $B(X) = X^4 + 1$. Montrer que A(X) et B(X) sont premiers entre eux et déterminer deux polynômes U(X) et V (X) tels que $U(X)A(X)+V(X)B(X) = 1$ et $degU < degB, degV < degA$.

d) Déterminer tous les polynômes $P \in \mathbb{Q}[X]$ tels que $X^4 + 1$ divise P et $x^3 + 1$ divise $P - 2$.

Exercice 7 Soit K un corps fini de caractéristique $p > 3$ et $P(X) = X^2 - X + 1 \in K[X]$.

a) Soit a un élément de K. Montrer que a est racine de P si et seulement si a est d'ordre 6 dans K.

b) En déduire une condition nécessaire et suffisante pour que b dans K soit racine du polynôme $Q(X) = X^4 - X^2 + 1$.

c) Montrer que, ou bien Q n'a pas de racine dans K, ou bien Q possède quatre racines dans K.

d) Qu'en est-il pour $\mathbb{F}_{73}$? Et pour $\mathbb{F}_{89}$?

e) Donner un exemple d'un corps K dans lequel P possède deux racines distinctes, mais dans lequel Q n'a pas de racine.

Exercice 8 Compter le nombre de polynômes irréductibles unitaires de degré 2 à coefficients dans $\mathbb{F}_p$. Expliquer pourquoi un corps de caractéristique p où un de ces polynômes se scinde contient des racines de tous les autres polynômes.

(Même question en degré 3)

Exercice 9 Soient $f \in \mathbb{Z}[x]$ un polynôme unitaire et p un nombre premier. Démontrer que si f est irréductible modulo p il est aussi irréductible sur $\mathbb{Z}$. Expliquer pourquoi l'hypothèse d'être unitaire est nécessaire. Démontrer que $f = x^4 + 1$ est irréductible sur $\mathbb{Z}$ bien qu'il soit réductible modulo p pour tout p.

ANNEAUX ET CORPS

Exercice 10 a) Rappeler pourquoi les anneaux $\mathbb{Z}, K[X], \mathbb{Z}[i]$ sont principaux. Donner la liste des inversibles de chaque anneaux.

b) Soit p un nombre premier (dans $\mathbb{Z}$). Montrer que l'anneau $\mathbb{Z}[i]/p$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z}[X])/(X^2+1)$.

c) En déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

d) Montrer par ailleurs que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p = 2$ ou $p \equiv 1[4]$.

e) Montrer par ailleurs (en considérant la norme) que p est réductible dans $\mathbb{Z}[i]$ si et seulement si on peut l'exprimer comme somme de deux carrés dans $\mathbb{Z}$.

f) Mettre toutes les pièces ensemble et conclure qu'un nombre premier est somme de deux carrés si et seulement si $p = 2$ ou $p \equiv 1[4]$.

g) Utiliser la factorialité de $\mathbb{Z}[i]$ pour déterminer tous les entiers qui peuvent s'écrire comme somme de deux carrés (dans $\mathbb{Z}$).

Exercice 11 Déterminer le nombre d'idéaux des anneaux $\mathbb{R}[x]/(x^4+x^2+1)$.

(Même question pour $\mathbb{R}[x]/(x^6+x^4+x^2+1)$.)

Exercice 12 Considérons l'anneau $\mathbb{F}_2[x]/(x^3+x+1)$. Démontrer que c'est un corps à 8 éléments. Démontrer que x est un générateur du groupe multiplicatif. Déterminer $a, b, c \in \{0,1\}$ tels que ax^2+bx+c soit l'inverse de x.

Exercice 13 Supposons $p = 2$. Démontrer que tout $\alpha \in \mathbb{F}_{p^2} - \mathbb{F}_p$ est générateur du groupe $\mathbb{F}_{p^2}^*$. Inversement, démontrer que pour tout $p \neq 2$ il existe un $\alpha \in \mathbb{F}_{p^2} - \mathbb{F}_p$ qui n'est pas générateur du groupe $\mathbb{F}_{p^2}^*$.

Exercice 14 Considérons l'anneau de polynômes $\mathbb{Q}[x]$.

1. Rappeler pourquoi ses idéaux sont tous de la forme $(p(x))$ avec $p(x) \in \mathbb{Q}[x]$.
2. Démontrer que $(p(x)) \subset (q(x))$ si et seulement si $q(x)$ divise $p(x)$.
3. Justifier qu'il y a une bijection entre l'ensemble des idéaux de $\mathbb{Q}[x]$ qui contiennent l'idéal $(x^2(x-1))$ et l'ensemble des idéaux de l'anneau $\mathbb{Q}[x]/(x^2(x-1))$,
4. Déduire le nombre d'déaux de $\mathbb{Q}[x]/(x^2(x-1))$ et en donner la liste.
5. Parmi ceux là qui sont les maximaux ?
6. Et les premiers ?

Exercice 15 Considérons l'application

$$f : \mathbb{R}[x] \longrightarrow \mathbb{R}^3$$

définie par

$$p(x) \mapsto (p(0), p(1), p(2)).$$

1. Démontrer que f est un morphisme d'anneaux.
2. Déterminer son image
3. Déterminer son noyau.
4. En utilisant le Théorème de factorisation déduire un isomorphisme entre anneaux convenables.

Exercice 16 Donner un isomorphisme entre l'anneau $\mathbb{Q}[x]/(x^3-1)$ et l'anneau A des matrices 3×3 à coefficients rationnels de la forme

$$A = \left\{ \begin{pmatrix} a & c & b \\ b & a & c \\ c & b & a \end{pmatrix}, a,b,c \in \mathbb{Q} \right\}.$$

Exercice 17 Soient A un anneau et I et J deux idéaux de A. Rappeler que $I \cap J$ est un idéal. Donner un exemple où l'ensemble des produits $\{i \cdot j\}_{i\in I, j\in J}$ n'est pas un idéal. Définissons $I \cdot J$ comme l'idéal engendré. Démontrer l'inclusion $I \cdot J \subset I \cap J$. Donner un exemple où l'inclusion est stricte. Démontrer que si on a $I + J = A$ alors l'inclusion est une égalité.

Exercice 18 (Perrin, Chaptire V, §6 (4))
Déterminer tous les sous-anneaux de $\mathbb{Q}$.

Exercice 19 Déterminer tous les anneaux de cardinalité $2, 3, 4, 5$ et 6.

Exercice 20 Considérons l'anneau A des fonctions continues de $[0,1]$ dans $\mathbb{R}$. Pour chaque $x \in [0,1]$ définissons $P_x = \{f \in A, f(x) = 0.\}$ Démontrer que P_x est un idéal maximal. Démontrer que tous les idéaux maximaux de A sont de cette forme.

Exercice 21 Donner deux sous corps de $\mathbb{C}$ différents mais isomorphes comme corps. Donner deux extensions finies de $\mathbb{Q}$ de même degré et non isomorphes.

Exercice 22 Quand p est un nombre premier on note

$$\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p}, \text{ avec } a, b \in \mathbb{Q}\}.$$

1. Démontrer que $\mathbb{Q}(\sqrt{p})$ est un anneau.
2. Démontrer qu'il y a un isomorphisme entre $\mathbb{Q}(\sqrt{p})$ et $\mathbb{Q}[x]/(x^2-p)$.
3. Démontrer qu'aucun élément α de $\mathbb{Q}(\sqrt{5})$ vérifie $\alpha^2 = 7$.
4. En déduire que les anneaux $\mathbb{Q}[x]/(x^2-5)$ et $\mathbb{Q}[x]/(x^2-7)$ ne sont pas isomorphes.
5. Démontrer que les anneaux $\mathbb{R}[x]/(x^2-5)$ et $\mathbb{R}[x]/(x^2-7)$ sont isomorphes et en donner un isomorphisme explicite.

Exercice 23 En utilisant le fait que $\mathbb{C}$ est algébriquement clos, décrire toutes les extensions finies de $\mathbb{R}$.

Exercice 24 Déterminer tous les sous-corps de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.