Sujet 1

Exercice 1 : Question de cours

Structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$.

Exercice 2

Résoudre dans $\mathbb{Z}$ l'équation diophantienne $x^2 + 2y^2 = 5z^2$

Exercice 3

1. Un polynôme non nul de $\mathbb{Z}[X]$ est dit primitif si les PGCD de ses coefficients vaut 1. Montrer que le produit de deux polynômes primitifs est un polynôme primitif.
2. Pour $A \neq 0 \in \mathbb{Z}[X]$, on note $c(A)$ le pgcd des coefficients de A.
   Montrer que $c(AB) = c(A)c(B)$.
3. Soit $A = a_n X^n + \cdots + a_1 X + a_0 \in Z[X]$ et p un nombre premier.

   On suppose que :

   — p ne divise pas a_n
   — p divise $a_0, \ldots, a_{n-1}$
   — p^2 ne divise pas a_0

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

Sujet 2

Exercice 1 : Question de cours

Idéaux de $\mathbb{K}[X]$.

Exercice 2

Soient $a, b \in \mathbb{N}^*$ et $m, n \in \mathbb{N}^*$ tels que :

$$m \wedge n = 1 \quad \text{et} \quad a^m = b^n$$

Montrer qu'il existe $c \in \mathbb{N}^*$ tel que : $a = c^n$ et $b = c^m$

Exercice 3

Soient A et B non nuls dans $\mathbb{K}[X]$.

Montrer que A et B sont premiers entre eux si et seulement si $A + B$ et AB le sont.

Exercice 4

Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$, $a \in \mathbb{K}$ et p un nombre premier.

On pose $Q = X^p - a$.

Montrer que Q est irréductible sur $\mathbb{K}$ si et seulement s'il n'a pas de racine dans $\mathbb{K}$.

Sujet 3

Exercice 1 : Question de cours

Soit $\mathbb{K}$ un sous-corps de C et $A, B \in \mathbb{K}[X]$

Énoncer une CNS portant sur les racines complexes de A et B pour qu'ils soient premiers entre eux.

Démontrer ce résultat.

Exercice 2

Soient p et q deux nombres premiers distincts. Montrer que :

$$p^{q-1} + q^{p-1} \equiv 1 \quad [pq].$$

Exercice 3

Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

Exercice 4

Soient $a_1, \ldots, a_n$ des entiers distincts.

Montrer que $(X - a_1) \ldots (X - a_n) - 1$ est irréductible dans $\mathbb{Z}[X]$.