Problème n° 1

Arithmétique : Autour du théorème de Dirichlet

Le théorème de Dirichlet en arithmétique dit que si a et b sont deux entiers naturels premiers entre eux, alors il existe une infinité de nombres premiers de la forme $a \times n + b$ (avec $n \in \mathbb{N}$). Dans cette exercice, nous montrons ce théorème pour quelques valeurs particulières de a et de b.

1) Soit p un nombre premier impair, et $r = \frac{p-1}{2}$ (on a remarquera que $r \in \mathbb{N}$).

a) Montrer que :

i) p est congru à soit 1 , soit 3 modulo 4 .

ii) p est congru à soit 1 , soit 3 , soit 5 , soit 7 modulo 8 .

b) On suppose qu'il existe un entier a tel que $-1 \equiv a^2[p]$.

i) Montrer que p ne divise pas a.

ii) En déduire que $a^{p-1} \equiv 1[p]$.

iii) Montrer que $(-1)^r \equiv 1[p]$.

iv) En déduire que $p \equiv 1[4]$.

On vient de montrer que si-1 est un carré modulo p, alors $p \equiv 1[4]$.

2) *Nombres premiers de la forme* $4n+3$. On suppose qu'il n'y a qu'un nombre fini de nombres premiers de la forme $4n+3$ avec $n \in \mathbb{N}$, on les note dans l'ordre croissant : $q_1, \ldots, q_r$ ($q_1 = 3, q_2 = 7, \ldots$). On pose $\mathrm{N} = 4 \times q_1 \times \cdots \times q_r - 1$, et on considère p un nombre premier qui divise N .

a) Vérifier que $\mathrm{N} \geqslant 2$.

b) Montrer que p est forcément impair.

c) Montrer que $p \notin \{q_1, \ldots, q_r\}$, en déduire que $p \equiv 1[4]$.

d) À l'aide de la décomposition en facteurs premiers, montrer que $N \equiv 1[4]$ et que ceci est absurde. Conclure.

3) *Nombres premiers de la forme* $8n+5$. On suppose qu'il n'y a qu'un nombre fini de nombres premiers de la forme $8n + 5$, on les note dans l'ordre croissant : $q_1, \ldots, q_r$ ($q_1 = 5, q_2 = 13, \ldots$). On pose $\mathrm{N} = 4 \times q_1^2 \times \cdots \times q_r^2 + 1$, et on considère p un nombre premier qui divise N (p est forcément impair).

a) Soit $a = 2 \times q_1 \times \cdots \times q_r$.

i) Montrer que $-1 \equiv a^2[p]$.

ii) En déduire que $p \equiv 1[4]$.

b) En déduire que $p \equiv 1[8]$ **OU** $p \equiv 5[8]$.

c) Montrer que $\mathrm{N} \equiv 5[8]$. En déduire que N a au moins un diviseur premier congru à 5 modulo 8. Indication : raisonner par l'absurde.

d) Montrer que ceci est contradictoire. Conclure.

e) L'existence d'une infinité de nombres premiers de la forme $8n + 5$ entraîne l'existence d'une infinité de nombre premiers de la forme $4n + 1$: pourquoi ?

Problème n° 2

Arithmétique : Triplets pythagoriciens

On dit que $(x,y,z) \in (\mathbb{N}^*)^3$ est un triplet pythagoricien si et seulement si $x^2+y^2=z^2$. L'objectif de cet exercice est de déterminer tous les triplets pythagoriciens. On note dans tout cet exercice $x \wedge y = \text{pgcd}(x,y)$. Les diviseurs considérés dans ce problème sont des entiers naturels. Enfin, on dira que $a \in \mathbb{N}$ est un carré si et seulement si il existe $b \in \mathbb{N}$ tel que $a = b^2$.

1) Soit $d \in \mathbb{N}^*$ un diviseur commun à x, y et z, en factorisant par d montrer qu'il suffit de déterminer les triplets pythagoriciens qui n'ont pas d'autres diviseurs communs que 1. On dit alors que x, y et z sont premiers entre eux et on parle dans ce cas de triplet pythagoricien primitif. Dans toute la suite, on s'intéresse à un triplet pythagoricien primitif (x,y,z).

2) Montrer que $x \wedge y = x \wedge z = y \wedge z = 1$. En déduire que x et y ne sont pas tous les deux pairs.

3) A l'aide de congruences modulo 4, montrer que x et y ne sont pas tous les deux impairs.
Les entiers naturels x et y sont de parités distinctes, sans perte de généralité on suppose dans toute la suite que x est pair et y impair.

4) Justifier qu'il existe $(u,v,w) \in (\mathbb{N}^*)^3$ tels que $x = 2u, z+y = 2v$ et $z-y = 2w$.

5) Montrer que $v \wedge w = 1$.

6) Montrer que vw est un carré, en déduire que v et w sont des carrés. On pose $v = n^2$ et $w = m^2$ où $(n,m) \in \mathbb{N}^2$.

7) Montrer que $n > m$ et que $n \wedge m = 1$. Exprimer u en fonction de n et m.

8) En déduire que (x,y,z) est un triplet pythagoricien primitif si et seulement si il existe deux entiers n et m premiers entre eux et de parités distinctes avec $n > m > 0$ tels que $x = 2nm, y = n^2-m^2$ et $z = n^2+m^2$ ou $x = n^2-m^2, y = 2nm$ et $z = n^2+m^2$.

Problème n° 3

Polynômes d'interpolations de Lagrange

Le but de cet exercice est de prouver le théorème suivant :

Théorème :

Soit $n \in \mathbb{N}, (x_1, \cdots, x_{n+1}) \in \mathbb{K}^{n+1}$ distincts et $(y_1, \cdots, y_{n+1}) \in \mathbb{K}^{n+1}$.
Alors il existe un unique polynôme P de $\mathbb{K}_n[X]$ (attention, pas $K_{n+1}[X]$) vérifiant :

$$\forall i \in [\![1, n+1]\!] \ , \ P(x_i) = y_i \ (\bigstar)$$

Dans la suite de cet énoncé on suppose fixé $n \in \mathbb{N}, (x_1, \cdots, x_{n+1}) \in R^{n+1}$ distincts et $(y_1, \cdots, y_{n+1}) \in \mathbb{K}^{n+1}$.

Partie 1 : Unicité

1) Montrer que si P et Q sont 2 polynômes de $K_n[X]$ vérifiant $(\bigstar)$ alors ils sont égaux.

Partie 2 : Existence

Dans cette partie nous allons explicitement déterminer un polynôme vérifiant $(\bigstar)$.

1) Soit $i \in [\![1, n+1]\!]$ et $L_i \in \mathbb{K}_n[X]$ vérifiant $\forall j \neq i L_i(x_j) = 0$. Par quel autre polynôme A de degré n le polynôme L_i est alors divisible ? En déduire une écriture de L_i sous la forme AQ, $Q \in \mathbb{K}[X]$.

2) Que peut-on dire sur le degré de Q ? On suppose en plus que $L_i(x_i) = 1$. En déduire l'expression de Q puis celle de L_i.

3) Montrer que $P = \sum_{i=1}^{n+1} y_i L_i$ vérifie $(\bigstar)$.

On vient de donner une expression explicite de l'unique polynôme de $\mathbb{K}_n[x]$ vérifiant $(\bigstar)$. On appelle ce polynôme polynôme interpolateur de Lagrange aux points $(x_1, \cdots, x_{n+1})$ pour les valeurs $(y_1, \cdots, y_{n+1})$

Partie 3 : Application

1) Donner l'expression de l'unique polynôme P de $R_2[X]$ vérifiant $P(0) = 1, P(1) = 2, P(2) = 3$ (on calculera bien chacun des coefficients).

2) Soit P_0 le polynôme interpolateur de Lagrange aux points $(x_1, \cdots, x_{n+1})$ pour les valeurs $(y_1, \cdots, y_{n+1})$. Soit $P \in K[x]$ vérifiant ★, montrer qu'il existe $Q \in \mathbb{K}[X]$ tel que $P = P_0 + (X - x_1)...(X - x_{n+1})Q$. Déterminer le degré de Q.

3) (Bonus : plus difficile) Montrer que pour tout $n \in \mathbb{N}$ il existe $(\lambda_0, \ldots, \lambda_n) \in \mathbb{R}^{n+1}$ tel que :

$$\forall P \in \mathbb{R}_n[X], \int_0^1 P(t)dt = \sum_{k=0}^{n} \lambda_k P\left(\frac{k}{n}\right).$$