EXERCICE 1

Soit p un nombre premier supérieur ou égal à 3. On donne dans cet exercice une caractérisation des classes qui sont des carrés dans $\mathbb{Z}/p\mathbb{Z}$. Les questions **3.** et **4.** sont des applications de ce résultat.

1. **a.** Prouver que $(p-1)! \equiv -1[p]$.

b. En regroupant chaque terme avec son opposé dans $(p-1)!$, prouver que si p est de la forme $4n+1$ alors -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

c. Prouver que si p est de la forme $4n+3$, -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$ (on pourra utiliser le petit théorème de Fermat).

2. Soit a un entier non multiple de p.

a. Prouver que si la classe de a, $\overline{a}$, est un carré dans $\mathbb{Z}/p\mathbb{Z}$, alors $a^{\frac{p-1}{2}} \equiv 1[p]$.

b. Combien y a-t-il de carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$?

c. En écrivant $X^{p-1}-1 = (X^{\frac{p-1}{2}}-1)(X^{\frac{p-1}{2}}+1)$, prouver que si $\overline{a}$ n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, alors $a^{\frac{p-1}{2}} \equiv -1[p]$.

3. On suppose qu'il n'existe qu'un nombre fini de nombres premiers de la forme $4n+1$, notés $p_1, p_2, \dots, p_N$. On pose alors $A = 4p_1^2 \dots p_N^2 + 1$. Prouver que A ne saurait avoir de diviseur de la forme $4n+3$ et conclure.

4. On considère ici une hypothétique solution (x,y) de l'équation en nombres entiers : $x^3 = y^2 - 7$.

a. Prouver que x est impair.

b. On réécrit cette équation sous la forme $(x+2)\left((x-1)^2+3\right) = y^2+1$ (faites-moi confiance, ça marche !). Prouver que l'entier $(x-1)^2+3$ se doit de posséder un diviseur premier de la forme $4n+3$.

c. Conclure.

EXERCICE 2

Tous les polynômes envisagés dans ce problème seront supposés être à coefficients *réels.* Un polynôme non nul $P \in \mathbb{R}[X]$ sera dit « scindé-simple » (sous-entendu « dans $\mathbb{R}$ ») si ses racines sont toutes réelles et simples. Comme on s'intéresse ici essentiellement à leurs racines, les polynômes envisagés seront supposés *unitaires* (c'est-à-dire de coefficient dominant égal à 1), quitte pour cela à les diviser par leur coefficient dominant.

Le sous ensemble de $\mathbb{R}[X]$ (resp. de $\mathbb{R}_n[X]$) constitué des polynômes scindés simples sera noté $SS[X]$ (resp. $SS_n[X]$).

1. Généralités

1. **a.** Le produit de deux éléments de $SS[X]$ est-il dans $SS[X]$?

b. La somme de deux éléments de $SS[X]$ est-elle dans $SS[X]$?

2. Soit $P = X^2 + aX + b \in \mathbb{R}_2[X]$. Donner une condition nécessaire et suffisante pour que P soit scindé-simple.

3. **a.** Soit $P = X^n + a_{n-1}X^{n-1} \ldots + a_1X + a_0 \in \mathbb{R}[X]$. On pose $Y = X + \dfrac{a_{n-1}}{n}$.

Quelle particularité possède le polynôme $Q(Y) = P(X)$?

b. Prouver que $P \in SS[X] \Leftrightarrow Q \in SS[Y]$.

2. Le cas $n = 3$

On fixe un polynôme $P = X^3 + pX + q \in \mathbb{R}[X]$, et l'on cherche une condition nécessaire et suffisante pour que P soit dans $SS_3[X]$.

4. Justifier le choix d'une telle particularité pour P.

5. **a.** Étudier les variations de P (on distinguera, cela va de soi, les cas $p \geq 0$ et $p < 0$).

b. Que dire dans le cas $p \geq 0$?

6. On suppose dans toute cette question que p est strictement négatif : $p < 0$.

a. Donner une expression très simple du produit $P(-\sqrt{-\frac{p}{3}}) \times P(\sqrt{-\frac{p}{3}})$.

b. En déduire que $P \in SS_3(X) \Leftrightarrow 4p^3 + 27q^2 < 0$.

7. Prouver qu'en toute généralité (sans donc rien supposer sur le signe de p), $P \in SS_3(X) \Leftrightarrow 4p^3 + 27q^2 < 0$.

3. Coefficients d'un élément de $SS[X]$

On fixe dans cette partie un élément $P = X^n + a_{n-1}X^{n-1} \ldots + a_1X + a_0 \in \mathbb{R}[X]$ supposé être scindé simple. On notera $r_1, r_2, \ldots, r_n$ ses racines, que l'on pourra, au besoin, supposer être rangées dans l'ordre croissant.

8. Prouver que le polynôme dérivé P' de P est lui-aussi scindé simple, puis qu'il en va de même des polynômes dérivés successifs de P jusqu'à l'ordre $n - 1$.

9. En déduire que P ne saurait avoir deux coefficients nuls successifs.

10. **a.** Expliciter la décomposition en éléments simples de la fraction rationnelle $\dfrac{P'}{P}$.

b. En déduire que le polynôme $PP'' - P'^2$ est à valeurs négatives.

c. Prouver l'inégalité : $a_0a_2 \leq a_1^2$.

d. Prouver que les coefficients de P encadrant un éventuel coefficient nul sont de signes contraires.