

Les différentes parties constituant ce problème sont totalement indépendantes. Il s'agit, plutôt que de faire un problème suivi, de balayer une bonne partie du programme d'algèbre en abordant des choses classiques que vous pourriez être amenés à rencontrer.

I. Irrationalité de π (3/2)

On suppose l'existence de deux entiers positifs et premiers entre eux a et b tels que $\pi = \frac{a}{b}$.

Pour n entier naturel et x réel, on pose :

$$P_n(x) = \frac{x^n(a-bx)^n}{n!} \quad \text{et} \quad I_n = \int_0^\pi P_n(x) \sin x \, dx.$$

1.
 - a. Calculer $\sup_{0 \leq x \leq \pi} |P_n(x)|$ en fonction de a , b et n .
 - b. Prouver que I_n est strictement positif pour tout n , et déterminer la limite de la suite (I_n) .
2. Pour tout entier k , la dérivée d'ordre k du polynôme P_n sera notée $P_n^{(k)}$. Par convention, $P_n^{(0)} = P_n$. Calculer en fonction de a , b , n et k les valeurs de $P_n^{(k)}(0)$ et de $P_n^{(k)}\left(\frac{a}{b}\right)$ dans les trois cas suivants :
 - i. $0 \leq k \leq n-1$ (lorsque $n \geq 1$) ;
 - ii. $n \leq k \leq 2n$;
 - iii. $k \geq 2n+1$.

Montrer que dans tous les cas considérés, $P_n^{(k)}(0)$ et $P_n^{(k)}\left(\frac{a}{b}\right)$ sont des entiers relatifs.

3.
 - a. Montrer que I_n est un entier relatif pour tout entier n .
 - b. Prouver que π est irrationnel.

I. Carrés de $\mathbb{Z} / p\mathbb{Z}$ (5/2)

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 , \bar{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 \bar{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 $(x + 2)((x - 1)^2 + 3) = y^2 + 1$ (faites-moi confiance, ça marche !).

Prouver que l'entier $(x - 1)^2 + 3$ se doit de posséder un diviseur premier de la forme $4n + 3$.

II. Codage RSA

1. Le petit théorème de Fermat

L'objectif de cette question est de donner une preuve du petit théorème de Fermat plus élémentaire que celle donnée dans le cours.

a. Soit p un nombre premier. Prouver que pour tout entier k compris entre 1 et $p - 1$, le coefficient binomial $\binom{p}{k}$ est divisible par p .

b. En déduire que pour tout élément x de $\mathbb{Z}/p\mathbb{Z}$, on a $(x + 1)^p = x^p + 1$, puis que $x^p = x$.

c. Soit M un entier. En envisageant deux cas, suivant que la classe de M est nulle ou non modulo p , prouver en utilisant la question précédente que $M^{k(p-1)+1} - M$ est un multiple de p pour tout entier k .

2. Soient p et q deux nombres premiers distincts, et $N = pq$. Soit e un nombre premier avec le produit $S = (p - 1)(q - 1)$, et d son inverse modulo S .

a. Comment, en pratique, détermine-t-on le nombre d connaissant e ?

b. Soit M un entier, et $C = M^e$.

Montrer, en utilisant la question 3.c., que $C^d - M$ est multiple de p .

c. Calculer C^d modulo N .

Intérêt de ce résultat : Alice désire que Bernard lui envoie un message codé. Elle publie dans la presse les nombres N et e , qui constituent sa clef publique. Cependant, elle garde secrets les nombres S et d , qui constituent sa clef secrète de déchiffrement (tout le principe de ce codage repose sur le fait que si p et q sont très grands, la connaissance de $N = pq$ ne permet pas de retrouver p et q ; Alice, qui connaît p et q puisque c'est elle qui a publié N , est donc la seule à connaître S et d).

Bernard, s'il veut coder un message M pour Alice, lui envoie $C = M^e [N]$. Alice n'a alors plus qu'à calculer C^d modulo N pour retrouver M ... joli, non ? À noter que Bernard, une fois qu'il a codé son message pour Alice, est totalement incapable de décoder son propre message puisqu'il ne connaît pas d ! C'est le principe du codage asymétrique, où le processus de décodage n'est pas simplement l'inverse du processus de codage.

III. Polynômes réels scindés simples

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 $P = X^n + a_{n-1}X^{n-1} \dots + a_1X + a_0 \in \mathbb{R}[X]$. On pose $Y = X + \frac{a_{n-1}}{n}$.
 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 $P = X^n + a_{n-1}X^{n-1} \dots + a_1X + a_0 \in \mathbb{R}[X]$ supposé être scindé simple. On notera r_1, r_2, \dots, 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 $\frac{P'}{P}$.
- b. En déduire que le polynôme $PP'' - P'^2$ est à valeurs négatives.
- c. Prouver l'inégalité : $a_0 a_2 \leq a_1^2$.
- d. Prouver que les coefficients de P encadrant un éventuel coefficient nul sont de signes contraires.