Examen

17/12/2017. Durée : 3h

Aucun document, aucun appareil électronique autorisé. Le sujet contient une question de cours et 3 exercices indépendants. On rédigera **lisiblement** *et on justifiera les réponses avec soin.*

Question de cours. [Barême indicatif : 2 points]

1. Énoncer le théorème des restes chinois dans $\mathbb{Q}[X]$.
2. Quel est le problème mathématique algorithmiquement difficile à résoudre de manière efficace qui assure la sécurité du système de cryptage RSA ?

Exercice 1. [Barême indicatif : 7 points]

Soit $f\colon \mathbb{R} \to \mathbb{R}$ la fonction paire 2π-périodique vérifiant :

$$\forall x \in [0, \pi[\,,\ f(x) = x + \frac{\pi}{2}\,.$$

1. Tracer à main levée le graphe de f sur l'intervalle $[-2\pi, 2\pi]$.
2. Calculer les coefficients de Fourier $a_n(f)$ $(n \geq 0)$ et $b_n(f)$ $(n \geq 1)$.
3. Pour $N \geq 1$ un entier fixé, écrire la N-ème somme partielle $S_N(f)$ de la série de Fourier de f et expliquer avec soin pour quels $x \in \mathbb{R}$ on a

$$S_N(f)(x) \to f(x) \qquad (N \to \infty)\,.$$

4. Calculer la valeur de la somme $\displaystyle\sum_{k=0}^{\infty} \frac{1}{(2k+1)^2}$.
5. Calculer la valeur de la somme $\displaystyle\sum_{k=0}^{\infty} \frac{1}{(2k+1)^4}$.

Exercice 2. [Barême indicatif : 5 points]

1. Dans cette question, on traite des propriétés de divisibilité des entiers $M_n = 2^n - 1$, $n \geq 2$.
   (a) Montrer que s'il existe des entiers $a > 1$ et $b > 1$ tels que $n = ab$, alors M_n n'est pas un nombre premier.
   [On pourra considérer le quotient $(2^n - 1)/(2^a - 1)$.]

   Dans la suite de cette question on fixe un nombre premier *impair* p et l'on veut montrer que si $q \mid M_p$ alors $q \equiv 1 (\mathrm{mod}\ 2p)$.

   (b) Justifier qu'il suffit de traiter le cas où q est un diviseur *premier* de M_p.
   (c) Justifier que q est impair, puis déterminer l'ordre de 2 dans $(\mathbb{Z}/q\mathbb{Z})^\times$
   (d) En utilisant le petit théorème de Fermat, montrer que $p \mid (q-1)$.
   (e) Conclure.
2. Dans cette question, on traite des propriétés de divisibilité des entiers $F_n = 2^{2^n} + 1$, $n \geq 0$.
   (a) Combien d'opérations sur les chiffres sont-elles nécessaires (en fonction de n, et à une constante multiplicative près) à l'algorithme d'exponentiation rapide pour calculer F_n ? [On ne demande pas de refaire le calcul du coût de l'algorithme d'exponentiation rapide.]

Dans la suite de cette question on fixe un entier $n \geq 0$ et un diviseur *premier impair* q de F_n et on veut montrer que $q \equiv 1 (\text{mod } 2^{n+1})$.

(b) Montrer que $2^{2^{n+1}} \equiv 1 (\text{mod } q)$.

(c) Justifier que 2 est inversible modulo q et que son ordre dans $(\mathbb{Z}/q\mathbb{Z})^\times$ est une puissance de 2.

(d) Montrer que l'ordre de 2 dans $(\mathbb{Z}/q\mathbb{Z})^\times$ est 2^{n+1}. Conclure.

Exercice 3. [Barême indicatif : 6 points]

On dit qu'un polynôme $P \in \mathbb{C}[X]$ est *sans facteur carré* s'il n'est pas divisible par le carré d'un polynôme non constant $Q \in \mathbb{C}[X]$ (i.e. P ne peut pas être écrit $Q(X)^2 R(X)$ où Q et R sont des éléments de $\mathbb{C}[X]$).

1. Montrer que $P \in \mathbb{C}[X]$ est sans facteur carré si et seulement si P et son polynôme dérivé P' n'ont pas de racine commune.

On fixe désormais $P \in \mathbb{Q}[X]$. On suppose P **unitaire** et **sans facteur carré**. On appelle *suite de Sturm* associée à P la suite $(R_0, \ldots, R_n)$ de polynômes de $\mathbb{Q}[X]$ définie comme suit :

$$R_0 = P,\ R_1 = P'\,,\ R_{i+2} = -\text{reste}(R_i, R_{i+1})\,,$$

où $\text{reste}(R_i, R_{i+1})$ désigne le reste dans la division euclidienne de R_i par R_{i+1} et où n est le plus petit entier tel que $R_{n+1} = 0$.

2. Que vaut $|R_n|$? Expliquer.
3. Montrer que, pour tout $a \in \mathbb{R}$, la suite réelle $(R_0(a), R_1(a), \ldots, R_n(a))$ ne comporte pas deux coefficients nuls consécutifs.

   [On pourra utiliser le fait que, dans l'algorithme d'Euclide appliqué à un couple (a, b) quelconque de pgcd égal à d, si (r_j) est la suite des restes calculés par l'algorithme, on a $d = \text{pgcd}(r_{j-1}, r_j)$ pour tout $j \geq 0$.]
4. Soit $a \in \mathbb{R}$ et soit $1 \leqslant i \leqslant n-1$ tel que $R_i(a) = 0$. Montrer que $R_{i+1}(a) = -R_{i-1}(a)$ et que ce réel est non nul.
5. Écrivons $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0$. Montrer que si z est une racine complexe de P, on a
$$|z| \leqslant \max\left(1, \sum_{i=0}^{d-1} |a_i|\right).$$

Soit $(y_0, \ldots y_n)$ une suite réelle. On appelle *nombre de changements de signe* de cette suite le nombre d'indices $0 \leqslant i \leqslant n-1$ tels que

$$\text{soit } (y_i > 0 \text{ et } y_{i+1} \leqslant 0)\,, \qquad \text{soit } (y_i < 0 \text{ et } y_{i+1} \geqslant 0)\,.$$

On admet le résultat suivant :

Théorème de Sturm. *Soient $\alpha < \beta$ deux réels, le nombre de racines réelles de P dans l'intervalle $]\alpha, \beta]$ est égal à la différence entre le nombre de changements de signes de la suite $(R_0(\alpha), \ldots, R_n(\alpha))$ et de la suite $(R_0(\beta), \ldots, R_n(\beta))$.*

6. Écrire un pseudocode pour une procédure prenant en entrée un polynôme $P \in \mathbb{Q}[X]$ unitaire sans facteur carré et renvoyant le nombre de ses racines réelles.

FIN

Correction disponible sur `www.math.u-bordeaux.fr/~fjouve001` à partir de 18h environ le 17/12.