Le 07.12.19

Devoir surveillé n°4

Durée de l'épreuve : 4 heures
La calculatrice est interdite

Le devoir est composé d'un exercice et d'un problème.
Lorsqu'une question est jugée, a priori, plus difficile, elle est précédée du symbole $(*)$ voire $(**)$.
La notation tiendra particulièrement compte de **la qualité de la rédaction, la précision des raisonnements et l'énoncé des formules utilisées**.

BON COURAGE

Exercice : Suite /6

On note $I = [\frac{-4}{3}, +\infty[$ et $f : x \mapsto \sqrt{3x+4}$.

1. Etudier les variations de f. Montrer que $f(I) \subset I$.

On considère la suite (u_n) définie par récurrence par $u_0 \in I$ et pour tout $n \in \mathbb{N}$, $u_{n+1} = f(u_n)$.

2. Montrer que si (u_n) converge vers ℓ, alors $\ell \in \{-1, 4\}$.
3. Etudier les variations de (u_n) (en fonction de $u_0 \leqslant 4$ ou $u_0 \geqslant 4$).
4. En déduire que (u_n) converge. Quelle est sa limite ?

Problème. « Theorema aureum » de Gauss

Notations :

- Dans ce problème, la lettre p designera toujours un nombre premier impair. Alors que la lettre m sera réservée pour un entier naturel strictement supérieur à 2 (sans autre condition).
- Soient $a \in \mathbb{Z}$.
  On dit que a **est un résidu quadratique modulo** m s'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv a[m]$.
- Selon la notation `Python`, on notera $a\%m$, le reste de la division euclidienne de a par m.
  On admet que dans l'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}}$, les classes $\overline{a}$ et $\overline{a'}$ son égales si et seulement si $a\%m = a'\%m$.
  Puis, nous prendrons le nombre $r = a\%m$ comme représentant principal de cette classe, classe notée alors $\dot{r}$ (voire r directement à partir de la partie D).

Objectifs

Dans ce problème, on cherche les nombres entiers qui sont des carrés modulo un entier m ou p (premier). On démontre pour terminer le « théorème d'or » de Gauss, appelé aussi théorème de réciprocité quadratique qui fait le lien entre les questions : p est-il un carré modulo q et q est-il un carré modulo p ?
Dans les *difficiles* préliminaires, on généralise sur le corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$, le premier résultat vu en début d'année sur la factorisation des polynômes. Dans la partie A, on se concentre sur un cas numérique particulier $p = 17$. Les résultats numériques trouvés dans cette partie peut être mobilisés par la suite...
Dans la partie B, on étudie des fonctions arithmétiques, pseudo-indicatrices, qui étudie si -1, 2 sont des résidus quadratiques modulo p, ainsi qu'une application θ particulière. Les résultats de cette partie sont exploitée en partie E (et D).
Dans la partie C, on met en place le symbole de Legendre assez pratique pour répondre à nos questions. On démontre aussi un résultat important x est un carré modulo p si et seulement si $x^{\frac{p-1}{2}} \equiv 1[p]$, à l'aide du petit théorème de Fermat.
Dans la partie D, on démontre le théorème de réciprocité quadratique pour des nombres premiers, que l'on généralise dans la partie E avec le symbole de Jacobi.

Préliminaires /6

Soit $p \in \mathbb{Z}$, nombre premier.

1. Soit $t_n : x \mapsto \sum_{k=0}^{n} a_k x^k$, polynomiale à coefficients entiers ($\forall\, i \in [\![0,n]\!]$, $a_i \in \mathbb{Z}$) de degré n.
   On suppose qu'il existe $\alpha \in \mathbb{Z}$ tel que $t_n(\alpha) \equiv 0[p]$.
   Montrer qu'il existe t_{n-1}, polynomiale à coefficients entiers et de degré au plus $n-1$ telle que

$$\forall\, x \in \mathbb{Z}, \quad t_n(x) \equiv (x-a)t_{n-1}(x)[p]$$

2. Soit $t_n : x \mapsto \sum_{k=0}^{n} a_k x^k$, une fonction polynôme à coefficients entiers de degré n.
   Montrer qu'il existe au plus n nombres distincts $\alpha_1, \dots \alpha_n$ de $[\![0, p-1]\!]$ tels que :
   pour tout $k \in \mathbb{N}_n$, $t_n(\alpha_k) \equiv 0[p]$

On a donc démontré :

> Si p est une fonction polynomiale de degré n dans un corps $\mathbb{K}$ (=$\mathbb{R}$, $\mathbb{C}$ ou $\frac{\mathbb{Z}}{p\mathbb{Z}}$)
> Alors p admet au plus n racines distinctes dans ce corps : $a_1, a_2 \dots a_r$ $(r \geqslant n)$
> et il existe un polynôme q à coefficients dans $\mathbb{K}$ tel que $\forall\, x \in \mathbb{K}$, $p(x) = q(x) \times \prod_{i=1}^{r}(x - a_i)$

A. Cas $p = 17$ /7

1. Montrer que, pour tout $a \in \mathbb{Z}$, $a^2 \equiv (17-a)^2[17]$.
2. Ecrire la table de tous les nombres a^2, pour a de 1 à 16, modulo 17.
   On attend, donc ici la liste $(a^2 \,\%17)_{a \in [\![1,16]\!]}$
3. Montrer alors qu'il existe exactement 8 résidus quadratiques modulo 17. Donner les racines de chacun de ces nombres
4. Pour tout $a \in [\![1,16]\!]$, que vaut $a^{16} \,\%17$?
5. Donner l'ensemble des nombres a tel que $a^8 \equiv 1[17]$.
   Quelle relation entre cet ensemble, et l'ensemble des résidus quadratiques modulo 17 ?

B. Applications pseudo-indicatrices /12

On considère de nouvelles applications définies sur $\mathbb{Z}$ ou $\mathbb{Z}^2$:

$$\epsilon : a \mapsto \begin{cases} 0 & \text{si } 2|a \\ 1 & \text{si } a \equiv 1[4] \\ -1 & \text{si } a \equiv 3[4] \end{cases}, \quad \omega : a \mapsto \begin{cases} 0 & \text{si } 2|a \\ 1 & \text{si } a \equiv 1[8] \text{ ou } a \equiv 7[8] \\ -1 & \text{si } a \equiv 3[8] \text{ ou } a \equiv 5[8] \end{cases}, \quad \theta : (a,a') \mapsto \begin{cases} 0 & \text{si } 2|a \text{ ou } 2|a' \\ -1 & \text{si } a \equiv 3[4] \text{ et } a' \equiv 3[4] \\ 1 & \text{sinon} \end{cases}$$

1. Etude de ϵ et ω.
   (a) Montrer que pour tout entier $\underline{a \text{ impair}}$, $\epsilon(a) = (-1)^{\frac{a-1}{2}}$ et $\omega(a) = (-1)^{\frac{a^2-1}{8}}$.
   (b) En déduire que pour tout $a, a' \in \mathbb{Z}$, $\epsilon(aa') = \epsilon(a)\epsilon(a')$ et $\omega(aa') = \omega(a)\omega(a')$
2. Etude de la fonction θ.
   (a) Calculer $\theta(1,3)$, $\theta(5,9)$, $\theta(1,2)$.
   (b) Montrer que $\forall\, a, a' \in \mathbb{Z}$, $\theta(a,a') = \theta(a',a)$
   (c) Dans le cas où a et a' sont des entiers impairs, montrer que $\theta(a,a') = (-1)^{\frac{(a-1)(a'-1)}{4}}$.
   (d) Montrer que pour tout $a, b, a' \in \mathbb{Z}$: $\theta(ab,a') = \theta(a,a') \times \theta(b,a')$

C. Symbole de Legendre /26

On considère m, un nombre entier strictement supérieur à 2. On note $\left(\frac{Z}{m\mathbb{Z}}\right)^*$ l'ensemble des nombres inversibles de $\frac{\mathbb{Z}}{m\mathbb{Z}}$.
On rappelle la convention de l'énoncé, ces éléments (qui sont des classes d'équivalence) sont notées $\dot{r}$ où $r \in [\![0, m-1]\!]$

1. Montrer que pour tout $a, b \in \frac{\mathbb{Z}}{m\mathbb{Z}}$, $\dot{ab} = \dot{a}\dot{\times}\dot{b}$.
2. Montrer que $\dot{r} \in \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$ si et seulement si $r \wedge m = 1$.
3. Dans le cas où $m = p$ est un nombre premier, que pensez-vous de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$?

Pour la suite de cette partie, on suppose que $m = p$ est un nombre premier et on note $\mathbb{F}_p = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, qui est un groupe (associé à la multiplication $\dot{\times}$ simplifiée en $\times$).

4. Deux morphismes de groupes multiplicatifs

On note alors $\varphi_p : \mathbb{F}_p \to \mathbb{F}_p$, $\dot{x} \mapsto \dot{x^{\frac{p-1}{2}}}$ et $\psi_p : \mathbb{F}_p \to \mathbb{F}_p$, $\dot{x} \mapsto \dot{x^2}$

Pour ces questions 4.(a) à 4.(f), on fera bien attention à différencier le nombre x de sa classe $\dot{x}$, « *nombre* » de $\mathbb{F}_p$.
Pour les questions suivantes, on pourra faire la confusion.

(a) A l'aide de 1., montrer que ψ_p est un morphisme de groupes multiplicatifs.
On admet que φ_p est également un morphisme de groupes multiplicatifs.

(b) En exploitant le (petit) théorème de Fermat montrer que $\psi_p \circ \varphi_p = \mathbf{1}_{\mathbb{F}_p}$.
(où $\mathbf{1}_{\mathbb{F}_p} : \dot{x} \mapsto \dot{1}$)

(c) Montrer que Ker $\psi_p = \{\dot{1}, \dot{p-1}\}$

(d) En déduire que Im $\varphi_p \subset \{\dot{1}, \dot{p-1}\}$

(e) En exploitant les fonctions polynomiales $t_1 : x \mapsto x^{\frac{p-1}{2}} - 1$ et $t_2 : x \mapsto x^{\frac{p-1}{2}} + 1$ *et le résultat démontré dans le préliminaire*, montrer que Im $\varphi_p = \{\dot{1}, \dot{p-1}\}$ et plus précisément

$$\text{card}\left(\varphi_p^{-1}(\{\dot{1}\})\right) = \text{card}\left(\varphi_p^{-1}(\{\dot{p-1}\})\right) = \frac{p-1}{2}$$

(f) Donner une condition nécessaire et suffisante sur $p\%4$ pour que $\varphi_p(\dot{-1}) = \dot{1}$.

5. Symbole de Legendre.

On note pour tout $a \in \mathbb{Z}$ (et p premier) :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p|a \\ -1 & \text{si } a \text{ n'est pas un résidu quadratique modulo } p \\ 1 & \text{sinon} \end{cases}$$

(a) Montrer que si $a \equiv a'[p]$, alors $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$

(b) En exploitant la partie A, donner la liste des valeurs de $\left(\frac{a}{17}\right)$ pour $a \in [\![30, 40]\!]$.

(c) Montrer également que $\left(\frac{a}{3}\right) \equiv a[3]$.

(d) Montrer que :

$$\forall\, a \in \mathbb{Z}, \quad \left(\frac{a}{p}\right) = \varphi_p(\dot{a\%p})$$

On complétera la définition de φ_p par : $\varphi_p(0) = 0^{\frac{p-1}{2}} = 0$. On rappelle que $\dot{-1} = \dot{p-1}$.

(e) En déduire la propriété de morphisme :

$$\forall\, a, a' \in \mathbb{Z}, \quad \left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right)$$

(f) Supposons que $a \wedge p = 1$. Comment se simplifie $\left(\frac{a^2a'}{p}\right)$?

(g) Montrer que $\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$.

D. Somme de Gauss et réciprocité quadratique /17

1. Somme de Gauss.

   On fixe un nombre premier $p > 2$ et considère $\xi = e^{2i\pi/p}$ et $\tau = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \xi^k$.

   (a) Calculer $\sum_{k=0}^{p-1} \xi^k$.

   (b) Montrer que pour tout $k \in \mathbb{N}_p$, $h_k : \mathbb{F}_p \to \mathbb{F}_p$, $s \mapsto ks$ est bijectif.

   En déduire que : $\tau^2 = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \xi^k \times \sum_{h=1}^{p-1} \left(\frac{h}{p}\right) \xi^h = \epsilon(p)p$

   On fera le changement de variable : $h \to s$ donné par la relation $h = ks$.

   (c) Soit q un nombre premier impair (différent de p).
   Montrer que : $\forall\ k \in [\![1, q-1]\!]$, $q \big| \binom{q}{k}$ puis par récurrence sur s

$$\forall\ a_1, \dots a_s \in \mathbb{Z}, \qquad \left(\sum_{k=1}^{s} a_k\right)^q \equiv \sum_{k=1}^{s} a_k^q\ [q]$$

   (d) Montrer que, pour $q(\neq p)$ premier impair : $\left(\frac{q}{p}\right) \tau^q \equiv \tau\ [q]$ avec q.

   (e) Montrer, par ailleurs, que $\tau^{q-1} \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)\ [q]$

2. Réciprocité quadratique.

   (a) Soient p et q deux nombres premiers impairs distincts. Montrer en exploitant 1.(d) et 1.(e) :

$$\left(\frac{p}{q}\right) = \theta(p,q) \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right)$$

   (b) Application : Est-ce que 17 est un carré de $\dfrac{\mathbb{Z}}{41\mathbb{Z}}$?

E. Symbole de Jacobi et réciprocité quadratique généralisée /10

1. Symbole de Jacobi.

On note pour tout $a \in \mathbb{Z}$ et $n \geqslant 3$ <u>impair</u> tels que $n = \prod_{i=1}^{s} p_i^{\alpha_i}$, décomposition en facteurs premiers de n :

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{s} \left(\frac{a}{p_i}\right)^{\alpha_i}$$

où $\left(\frac{a}{p_i}\right)$ est le symbole de Legendre

(a) Montrer que pour tout $a, a' \in \mathbb{Z}$, $m, m' \geqslant 3$, impairs tels que $m \wedge m' = 1$:

$$\left(\frac{aa'}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{a'}{m}\right) \qquad \text{et} \qquad \left(\frac{a}{mm'}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{m'}\right)$$

(b) Calculer $\left(\frac{14}{51}\right)$

2. Loi de réciprocité.
   Soient $n, m \in \mathbb{Z}$, impairs, positifs et premiers entre eux. Montrer que

$$\left(\frac{m}{n}\right) = \theta(m,n) \left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} \left(\frac{n}{m}\right)$$

3. Lois complémentaires.
   Montrer que pour tout n entier impair positif :

$$\left(\frac{-1}{n}\right) = \epsilon(n) = (-1)^{\frac{n-1}{2}} \qquad \text{et} \qquad \left(\frac{2}{n}\right) = \omega(n) = (-1)^{\frac{n^2-1}{8}}$$