DM 24 :
Résidus quadratiques

Il s'agit d'un sujet supplémentaire pour votre travail personnel.
Il n'est pas à rendre.
Un corrigé sera fourni le vendredi 27 décembre.

Dans tout le problème, p désigne un nombre premier impair.
$\diamond$ Pour $a \in \mathbb{Z}$ tel que p ne divise pas a, on dit que a est un résidu quadratique modulo p (en abrégé : RQ mod p) si et seulement si il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv a$ modulo p.
Dans le cas contraire, on dit que a est non-résidu quadratique modulo p (en abrégé : NRQ mod p).
$\diamond$ Pour $\alpha \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, on dit que α est un résidu quadratique dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si il existe $\xi \in \mathbb{Z}/p\mathbb{Z}$ tel que $\xi^2 = \alpha$.

Partie I :

1°) **a)** Soit $a \in \mathbb{Z}$ tel que p ne divise pas a. Montrer que l'équation $\xi^2 = \overline{a}$, d'inconnue $\xi \in \mathbb{Z}/p\mathbb{Z}$, n'admet aucune solution ou bien en admet exactement deux.
b) En déduire qu'il y a dans $\{1, \ldots, p-1\}$ exactement $\dfrac{p-1}{2}$ résidus quadratiques modulo p, et $\dfrac{p-1}{2}$ non-résidus quadratiques modulo p.
c) Déterminer les RQ et les NRQ modulo 11 compris entre 1 et 10.

Pour $a \in \mathbb{Z}$ tel que p ne divise pas a, on définit le symbole de Legendre :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } a \text{ est RQ mod } p \\ -1 \text{ si } a \text{ est NRQ mod } p \end{cases}.$$

d) α) Pour tout $a \in \mathbb{Z}$ tel que p ne divise pas a, montrer que $\displaystyle\sum_{k=1}^{p-1} \left(\frac{ka}{p}\right) = 0$.

β)

1. Soit $k \in \{1, \ldots, p-2\}$ et $k' \in \{1, \ldots, p-1\}$ tels que $kk' \equiv 1$ modulo p.
   Montrer que $k' \neq p-1$ et que $\left(\dfrac{k(k+1)}{p}\right) = \left(\dfrac{k'+1}{p}\right)$.

2. En déduire que $\displaystyle\sum_{k=1}^{p-2}\left(\frac{k(k+1)}{p}\right) = -1$.

2°) a) Théorème d'Euler.

α) Montrer que pour tout $x \in \mathbb{Z}$ tel que p ne divise pas x, $x^{p-1} \equiv 1$ modulo p.

β) Lorsque $\left(\frac{a}{p}\right) = -1$, en utilisant l'application $\xi \longmapsto \xi^{-1}\overline{a}$ sur $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, montrer que $\overline{(p-1)!} = \overline{a}^{\frac{p-1}{2}}$.

δ) Montrer le théorème de Wilson, selon lequel $(p-1)! \equiv -1$ modulo p.

γ) Montrer que, pour tout $a \in \mathbb{Z}$ tel que p ne divise pas a, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ modulo p.

Montrer que $\left(\frac{10}{31}\right) = 1$.

b) En déduire que $\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ si } p \equiv 1 \text{ modulo } 4 \\ -1 \text{ si } p \equiv 3 \text{ modulo } 4 \end{cases}$.

c) α) Soit $n \in \mathbb{N}^*$ tel que $n \equiv 3$ modulo 4. Démontrer qu'il existe au moins un diviseur premier q de n tel que $q \equiv 3$ modulo 4.

β) En déduire que l'équation $x^2 + y^3 - 8(2z+1)^3 + 1 = 0$, d'inconnue $(x, y, z) \in \mathbb{Z}^3$ n'a pas de solution. *Indications :* en supposant que l'équation admet une solution (x, y, z), on pourra commencer par montrer que y est impair, puis que $x^2 + 1 = (2(2z+1) - y)A$, où $A \equiv 3$ modulo 4.

En déduire qu'en particulier, l'équation de Lebesgue $x^2 + y^3 = 7$ n'a pas de solution dans $\mathbb{Z}^2$.

3°) a) Soit $a, b \in \mathbb{Z}$ tels que p ne divise ni a ni b. Montrer :

1. $\left(\frac{1}{p}\right) = 1$;
2. $a \equiv b$ modulo $p \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
3. $\left(\frac{a^2}{p}\right) = 1$;
4. $\left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

b) Soit $a \in \mathbb{N}^*$ tel que p ne divise pas a. On note $a = \displaystyle\prod_{i=1}^{N} p_i^{r_i}$ la décomposition primaire de a et $I = \{i \in \{1, \ldots, N\} \ / \ r_i \text{ impair}\}$. On pose $a' = \displaystyle\prod_{i \in I} p_i$.

Montrer que $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$.

4°) Lemme de Gauss :
Soit $a \in \mathbb{Z}$ tels que p ne divise pas a. Pour tout $j \in \{1, \dots, \frac{p-1}{2}\}$, on note r_j le reste de la division euclidienne de ja par p.
a) Montrer que $r_1, \dots, r_{\frac{p-1}{2}}$ sont deux à deux distincts.

On note $u_1, \dots, u_s$ les éléments de $\{r_1, \dots, r_{\frac{p-1}{2}}\}$ qui sont inférieurs ou égaux à $\frac{p-1}{2}$, et $v_1, \dots, v_t$ les éléments de $\{r_1, \dots, r_{\frac{p-1}{2}}\}$ qui sont supérieurs ou égaux à $\frac{p+1}{2}$.
b) Etablir :

1. $u_1, \dots, u_s, v_1, \dots, v_t$ sont deux à deux distincts et forment $\{r_1, \dots, r_{\frac{p-1}{2}}\}$.
2. $u_1, \dots, u_s, p - v_1, \dots, p - v_t$ sont deux à deux distincts et forment $\{1, \dots, \frac{p-1}{2}\}$.

c) En déduire que $\left(\frac{a}{p}\right) = (-1)^t$: il s'agit du lemme de Gauss.

En déduire la valeur de $\left(\frac{8}{29}\right)$.

d) Montrer que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$: on pourra montrer que $\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8}$ modulo 2.

Montrer que $\left(\frac{8}{31}\right) = 1$.

e) Soit $n \in \mathbb{N}$. Montrer que si $8n + 7$ est premier, alors $8n + 7 \mid 2^{4n+3} - 1$ et que, si $n \geq 1$, $2^{4n+3} - 1$ est composé.

Partie II : loi de réciprocité quadratique de Gauss

1°) Soit p, q deux nombres premiers impairs distincts.
Dans le plan usuel, on note $A(\frac{p}{2}, 0), B(0, \frac{q}{2}), C(\frac{p}{2}, \frac{q}{2})$.
a) Montrer que le nombre de points de $(\mathbb{N}^*)^2$ situés strictement dans le rectangle $OACB$ est égal à $\frac{p-1}{2}\,\frac{q-1}{2}$.
b) Etablir qu'il n'y a aucun point de $(\mathbb{N}^*)^2$ sur le segment $[O, C]$.
c) Montrer que le nombre de points de $(\mathbb{N}^*)^2$ situés dans le triangle OAC est $\displaystyle\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$,

et que le nombre de points de $(\mathbb{N}^*)^2$ situés dans le triangle OBC est $\displaystyle\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor$.

d) On reprend les notations du lemme de Gauss (question I.4) en remplaçant a par q.
On pose $u = \displaystyle\sum_{i=1}^{s} u_i$ et $v = \sum_{k=1}^{t} v_k$.

Montrer que $t \equiv (u+v)+(u+pt-v)$ modulo 2. En déduire que $t \equiv \displaystyle\sum_{j=1}^{\frac{p-1}{2}} r_j + \frac{p^2-1}{8}$ modulo 2.

Montrer que $t \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$ modulo 2.

e) En déduire que $\left(\frac{p}{q}\right) \times \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\ \frac{q-1}{2}}$: il s'agit de la loi de réciprocité quadratique de Gauss.

2°) **a)** Déduire de la loi de réciprocité quadratique que, pour tous nombres premiers impairs distincts p et q, $\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) \text{ si } (p \equiv 1 \text{ modulo } 4) \vee (q \equiv 1 \text{ modulo } 4) \\ -\left(\frac{p}{q}\right) \text{ si } (p \equiv 3 \text{ modulo } 4) \wedge (q \equiv 3 \text{ modulo } 4) \end{cases}$.

b) Sachant que 6607 est premier, montrer que $\left(\frac{6417}{6607}\right) = 1$.

3°) **Test de Pépin.**

Pour tout $n \in \mathbb{N}^*$, on note $F_n = 2^{(2^n)} + 1$ (nombres de Fermat).

Démontrer que F_n est premier si et seulement si $3^{\frac{F_n-1}{2}} \equiv -1$ modulo F_n : pour la réciproque on pourra faire intervenir un diviseur premier quelconque p de F_n et le plus petit entier $\alpha \geq 1$ tel que $3^\alpha \equiv 1$ modulo p, et montrer que $\alpha \mid F_n - 1$ mais que α ne divise pas $\frac{F_n - 1}{2}$.

Par exemple, montrer que $F_5 = 2^{(2^5)} + 1$ est composé.

4°) On suppose que $p \geq 5$. Montrer :

a) $\left(\frac{3}{p}\right) = \begin{cases} 1 \text{ si } p \equiv \pm 1 \text{ modulo } 12 \\ -1 \text{ si } p \equiv \pm 5 \text{ modulo } 12 \end{cases}$;

b) $\left(\frac{-3}{p}\right) = \begin{cases} 1 \text{ si } p \equiv 1 \text{ modulo } 6 \\ -1 \text{ si } p \equiv -1 \text{ modulo } 6 \end{cases}$.