Devoir à la maison n°2

Pour ce second devoir, vous devez choisir entre l'un des deux problèmes (et pas deux !), et rendre une solution en binôme.

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**.

Problème 1 : Somme de deux carrés

Dans ce problème, nous nous intéressons à un problème résolu par Fermat :

« *Quels sont les nombres premiers (en partie C) ou les nombres entiers (en partie D) qui peuvent s'écrire comme la somme de deux carrés ?* »

Pour résoudre ce problème, nous suivons la démarche proposée par Gauss. Il faut faire un détour dans $\mathbb{C}$ (!) et définir les entiers de Gauss. En partie A, nous voyons une image géométrique du produit dans $\mathbb{Z}[i]$, et dans la partie B, nous étudions nous étudions les propriétés arithmétiques de ces nombres particuliers...

Dans tout le problème, on note $\mathbb{Z}[i] = \{a + ib; a, b \in \mathbb{Z}\}$. On appelle cet ensemble, l'anneau des entiers de Gauss.
On peut donc écrire :

$$z \in \mathbb{Z}[i] \iff \exists\ (a, b) \in \mathbb{Z}^2 \text{ tels que } z = a + ib$$

A. L'anneau des entiers de Gauss

Dans cette partie, nous montrons que l'ensemble des entiers de Gauss a de nombreuses propriétés arithmétiques, comparables à celles dans $\mathbb{Z}$. Cela est une conséquence de l'existence d'une division euclidienne.

1. Montrer que si $z, z' \in \mathbb{Z}[i]$, alors $\overline{z}$, $z + z'$ et $z \times z' \in \mathbb{Z}[i]$.
   La stabilité de $\mathbb{Z}[i]$ assuré par ces deux dernières opérations explique ce nom d'anneau.
2. On note $N : \mathbb{Z}[i] \to \mathbb{N}, z \mapsto z\overline{z}$.
   Justifier que $N(\mathbb{Z}[i]) \subset \mathbb{N}$.
3. Montrer que $N(zz') = N(z)N(z')$
4. On note $\mathbb{Z}[i]^*$, l'ensemble des éléments inversibles de $\mathbb{Z}[i]$ et dont l'inverse est dans $\mathbb{Z}[i]$.
   Autrement écrit : $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid \exists\ z' \in \mathbb{Z}[i], z \times z' = 1\}$.
   (a) Montrer que $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\}$
   (b) En déduire les quatre éléments de $\mathbb{Z}[i]^*$.
5. Dans cette question, nous allons montrer que $\mathbb{Z}[i]$ est un anneau euclidien.
   Autrement écrit, il existe « une »(sorte de) division euclidienne sur $\mathbb{Z}[i]$.
   (a) Soit $s \in \mathbb{C}$ (non forcément entier de Gauss).
   Montrer qu'il existe $z \in \mathbb{Z}[i]$ tel que $|z - s| \leqslant \dfrac{\sqrt{2}}{2}$.
   On pourra s'aider d'un dessin pour faire la démonstration
   (b) En déduire, en choisissant bien s, :

$$\forall\ x, y \in \mathbb{Z}[i], \exists\ (q, r) \in \mathbb{Z}[i] \text{ tel que } x = qy + r \text{ avec } 0 \leqslant N(r) < N(y)$$

   On dit que $\mathbb{Z}[i]$ est muni d'une division euclidienne, ou que $\mathbb{Z}[i]$ est un anneau euclidien.
   On notera que le couple (q, r) n'est pas unique
   (c) Faire la division euclidienne de $3 + 2i$ par $1 - i$.

6. On dit que $p \in \mathbb{Z}[i]$ est i-premier si
   — p n'est pas inversible
   — si, pour tout $a, b \in \mathbb{Z}[i]$, $p = ab$, alors a est inversible ou b est inversible

   (a) Cette définition généralise-t-elle celle des nombres premiers sur $\mathbb{N}$?

   (b) Montrer que si $N(p)$ est premier alors p est nécessairement i-premier.
   Donner un nombre i-premier.

   (c) En considérant $3 \in \mathbb{Z}[i]$, montrer que la réciproque de la proposition précédente est fausse.

   (d) Soit p un nombre i-premier .
   Montrer que, pour tout $a, b \in \mathbb{Z}[i]$, $p|a \times b \Longrightarrow p|a$ ou $p|b$ *(Lemme de Gauss)*

   (e) (*) Démontrer l'extension du théorème fondamentale de l'arithmétique :
   Tout entier de $\mathbb{Z}[i]$ est soit une unité, soit divisible par un nombre i-premier
   Puis :
   Tout nombre entier de $\mathbb{Z}[i]$ non inversible s'écrit comme un produit unique de nombres i-premiers.
   (sans tenir compte des inversibles, des nombres associés et de l'ordre du produit).

B. Un nombre premier comme somme de 2 carrés

Dans cette partie nous montrons que :

$$p \in \mathbb{N} \text{ premier et } p \neq 2 \text{ s'écrit sous la forme } a^2 + b^2 \text{ si et seulement si } p \equiv 1[4].$$

Dans les questions 1. et 2., nous démontrons le sens direct de la proposition (condition nécessaire).
Dans la question 3., nous faisons un détour pour démontrer le théorème de Wilson.
Nous exploitons ce résultat dans la question 4., pour démontrer constructivement le sens indirect de la proposition (condition suffisante).

1. Montrer que si $p = 2$, il existe un seul couple $(a, b) \in \mathbb{N}$ tel que $p = a^2 + b^2$.
2. Soit p un nombre premier, différent de 2.
   Montrer que s'il existe $a, b \in \mathbb{N}$ tels que $p = a^2 + b^2$, alors $p \equiv 1[4]$
3. Soit q un entier premier.
   (a) Rappeler le petit théorème de Fermat avec comme hypothèse : q premier et $n \wedge q = 1$
   (b) On considère le polynôme $P(X) = (X^{q-1} - 1) - (X - 1)(X - 2) \cdots (X - (q - 1))$.
   Montrer que le degré de P est strictement inférieur à $q - 1$.
   On rappelle que le degré d'un polynôme est le plus grand coefficient k de X^k dans la combinaison linéaire définissant P.
   (c) Montrer que pour tout $k \in [\![1, q - 1]\!]$, $P(k) \equiv 0[q]$
   (d) En déduire le théorème de Wilson : $(q - 1)! \equiv -1[q]$.
   On admet le résultat suivant :
   Soit P de degré d à coefficients entiers, $P(X) = \sum_{k=0}^{d} a_k X^k$
   Si il existe $d + 1$ valeurs entiers, $0 < a_0, \cdots < a_d \leqslant p - 1$ tel que : $\forall\ i \leqslant d$, $P(a_i) \equiv 0[p]$, alors pour tout $k \in \{0, 1, \ldots d\}$, $a_k \equiv 0[p]$.
4. Nous allons démontrer l'application réciproque. Considérons p premier, tel que $p \equiv 1[4]$.
   (a) En exploitant le théorème de Wilson, montrer que

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1[p]$$

   (b) En déduire qu'il existe $x \in \mathbb{N}$ tel que $p|(x + i)(x - i)$.
   (c) Par l'absurde montrer que p ne peut pas être i-premier.
   On exploitera le Lemme de Gauss dans $\mathbb{Z}[i]$
   (d) Conclure.
   (e) Application : Trouver $a, b \in \mathbb{N}$ tel que $a^2 + b^2 = 13$

C. Somme de deux carrés

Dans cette partie, nous généralisons le résultat de la partie précédente à tout entier n.
Nous démontrons en particulier :

$$n \in \mathbb{N} \text{ s'écrit sous la forme } a^2+b^2 \text{ si et seulement si}$$
$$\text{chacun de ses facteurs premiers de la forme } 4k+3 \text{ intervient à une puissance paire}$$

Nous terminons cette partie en dénombrant le nombre de telle décomposition, selon la factorisation de n.

1. Soit $n = a^2+b^2 \in \mathbb{N}$, avec $a, b \in \mathbb{N}$.
   On note $\delta = a \wedge b$ et a' et b' tels que $a = a'\delta$ et $b = b'\delta$.
   (a) Soit p diviseur premier impair de $(a')^2+(b')^2$.
   Montrer que si p était i-premier (dans $\mathbb{Z}[i]$), alors p diviserait $2a'$ et $2b'$.
   En déduire une contradiction.
   On pourra utiliser le lemme de Gauss
   (b) Montrer alors que $p = z_1 z_2$, avec z_1 et z_2 non inversible.
   En déduire que $p = N(z_1)$ puis est la somme de deux carrés.
   (c) Conclure
2. Réciproquement, soit $n = 2^a \left(p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right)^2 q_1^{\beta_1} \cdots q_m^{\beta_m}$, avec $p_i \equiv 3[4]$ et $q_j \equiv 1[4]$
   (a) Montrer l'identité de Lagrange :
   $$\forall\ a,b,c,d \in \mathbb{Z} \qquad (a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2$$
   (b) Montrer alors que :
   $$\exists\ A, B \in \mathbb{N} \qquad \text{tels que} \qquad 2^a q_1^{\beta_1} \cdots q_m^{\beta_m} = A^2+B^2$$
   (c) En déduire que n peut s'écrire comme la somme de deux carrés.
3. Pour quel entier p, premier, a-t-on un triplet pythagoriciens $(a,b,p) \in \mathbb{N}$
   c'est-à-dire tel que $a^2+b^2 = p^2$?
4. En reexploitant l'identité de Lagrange, trouver les 6 représentations distinctes comme somme de carrés de $2925 = 3^2 \times 5^2 \times 13$.
   On compte comme représentations disctinctes, les deux représentations A^2+B^2 et B^2+A^2 (si $A \neq B$). On considère $A, B \geqslant 0$.
5. (**) On note $r_2(n)$ le nombre de représentation distinctes sous la forme $n = a^2+b^2$.
   Démontrer le théorème suivant :
   $$r_2(n) = \prod_{p \in \mathcal{P}_1} (v_p(n)+1) \times \prod_{p \in \mathcal{P}_3} \left(\frac{1+(-1)^{v_p(n)}}{2}\right)$$
   où $\mathcal{P}_1 = \{p \in \mathcal{P} \mid p \equiv 1[4]\}$ et $\mathcal{P}_3 = \{p \in \mathcal{P} \mid p \equiv 3[4]\}$.

Problème 2 : « 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.

A. Préliminaires

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 $\forall\, x \in \mathbb{K}$, $p(x) = q(x) \times \prod_{i=1}^{r}(x - a_i)$

B. Cas $p = 17$

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 ?

C. Applications pseudo-indicatrices

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

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

1. (a) Montrer que pour tout entier a 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. (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 $a, b, a' \in \mathbb{Z}$: $\theta(ab,a') = \theta(a,a') \times \theta(b,a')$

D. Symbole de Legendre

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 $a, b \in \frac{\mathbb{Z}}{m\mathbb{Z}}$, $\dot{\overbrace{ab}} = \dot{a} \dot{\times} \dot{b}$.
   Dans le cas où $m = p$ est un nombre premier, que pensez-vous de $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$?

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

2. On note alors $\varphi_p : \mathbb{F}_p \to \mathbb{F}_p$, $\dot{x} \mapsto \dot{\overbrace{x^{\frac{p-1}{2}}}}$ et $\psi_p : \mathbb{F}_p \to \mathbb{F}_p$, $\dot{x} \mapsto \dot{\overbrace{x^2}}$
   Pour les premières questions, 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 $\psi_p = \{\dot{1}, \dot{\overbrace{p-1}}\}$
   (d) En déduire que Im $\varphi_p \subset \{\dot{1}, \dot{\overbrace{p-1}}\}$
   (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 $\varphi_p = \{\dot{1}, \dot{\overbrace{p-1}}\}$ et plus précisément

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

   (f) Donner une condition nécessaire et suffisante sur $p\%4$ pour que $\varphi_p(\dot{-1}) = \dot{1}$.
3. 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 :

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

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

(e) En déduire la propriété de morphisme :

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

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

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

E. Somme de Gauss et réciprocité quadratique

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

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

(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 : $\tau^2 = \displaystyle\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\xi^k \times \sum_{h=1}^{p-1}\left(\frac{h}{p}\right)\xi^h = \epsilon(p)p$
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. (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 $\dfrac{\mathbb{Z}}{41\mathbb{Z}}$?

F. Symbole de Jacobi et réciprocité quadratique généralisée

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

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

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

1. (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. 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. Montrer que pour tout n entier impair positif :

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