Problème n° 15 : Arithmétique

Problème 1 – Critères de primalité

Ce problème étudie des tests de primamité utilisés notamment dans l'étude des nombres de Fermat $F_n = 2^{2^n} + 1$, et des nombres de Mersenne $M_n = 2^n - 1$, $n \in \mathbb{N}^*$.

Les résultats suivants, vus en exercice, pourront être utilisés sans avoir à en redonner la preuve :

- *p étant un nombre premier impair, $\mathbb{F}_p^*$ contient autant de carrés que de non carrés. En d'autre termes, l'image par $x \mapsto x^2$ de $\mathbb{F}_p^*$ est de cardinal $\frac{p-1}{2}$.*
- *Sous les mêmes conditions, x est un carré dans $\mathbb{F}_p^*$ si et seulement si $x^{\frac{p-1}{2}} = 1$. Dans le cas contraire, $x^{\frac{p-1}{2}} = -1$.*
- *Pour tout corps fini K, le groupe $(K^*, \times)$ est cyclique. Il existe donc un élément $a \in K^*$ d'ordre (multiplicatif) $|K| - 1$.*

Soit p un nombre premier impair. On appelle résidu quadratique modulo p un entier a congru à un carré modulo p, c'est à dire tel que la classe $\overline{a}$ de a dans $\mathbb{F}_p$ soit un carré. En d'autres termes, il existe $x \in \mathbb{Z}$ tel que $a \equiv x^2$ $[p]$. Les autres éléments de $\mathbb{Z}$ sont appelés non-résidus quadratiques modulo p.

Question préliminaire

Montrer que si $n \in \mathbb{N}$ n'est pas un carré parfait (i.e. le carré d'un entier naturel), alors $\sqrt{n}$ est irrationnel.

Partie I – Anneaux $\mathbb{Z}[\xi]/(p)$

Dans cette partie, on considère le sous-anneau $\mathbb{Z}$ de l'anneau $(\mathbb{C}, +, \times)$ des nombres complexes, et $\xi \in \mathbb{C}$ un nombre complexe fixé. On définit $\mathbb{Z}[\xi]$ comme étant, s'il existe, le plus petit sous-anneau A de $\mathbb{C}$ tel que $\mathbb{Z} \subset A$ et $\xi \in A$. La minimalité se traduit par le fait que tout autre anneau B vérifiant ces deux conditions vérifie $\mathbb{Z}[\xi] \subset B$.

1. Justifier l'existence de $\mathbb{Z}[\xi]$ en l'exprimant sous forme d'une intersection.
2. Que dire de $\mathbb{Z}[\xi]$ lorsque $\xi \in \mathbb{Z}$?
3. Montrer que $\mathbb{Z}[\xi] = \{P(\xi) \mid P \in \mathbb{Z}[X]\}$, où $\mathbb{Z}[X]$ est l'ensemble de tous les polynômes à coefficients entiers. L'écriture d'un élément $a \in \mathbb{Z}[\xi]$ sous la forme $P(\xi)$ est-elle unique en général ? (on pourra par exemple considérer $\xi = \mathrm{i}$).

Dans la suite de cette partie, on se donne un nombre premier p.

4. On définit sur $\mathbb{Z}[\xi]$ le relation de congruence modulo p par :

$$\alpha \equiv \beta \ [p] \Longleftrightarrow \exists \gamma \in \mathbb{Z}[\xi],\ \alpha - \beta = p\gamma.$$

   Montrer qu'il s'agit d'une relation d'équivalence, et qu'elle est compatible avec le produit et l'addition de $\mathbb{Z}[\xi]$.
5. On note $\mathbb{Z}[\xi]/(p)$ l'ensemble quotient de $\mathbb{Z}[\xi]$ par la relation de congruence modulo p, donc l'ensemble des classes de congruence modulo p. Justifier que les lois de $\mathbb{Z}[\xi]$ passent au quotient et définissent une structure d'anneau sur $\mathbb{Z}[\xi]/(p)$.
6. Montrer que pour tout $(a, b) \in (\mathbb{Z}[\xi]/(p))^2$, on a $(a + b)^p = a^p + b^p$ (égalité dans $\mathbb{Z}[\xi]/(p)$).
7. A-t-on en général $a^p = a$, pour $a \in \mathbb{Z}[\xi]/(p)$?

On remarquera qu'en se restreignant aux classes des entiers, on peut considérer que $\mathbb{F}_p$ est un sous-anneau de $\mathbb{Z}[\xi]/(p)$.

Partie II – Adjonction d'une racine

On suppose dans cette partie que le nombre complexe ξ vérifie $\xi \notin \mathbb{Z}$ et $\xi^2 \in \mathbb{Z}$. On note $d = \xi^2$. L'anneau $\mathbb{Z}[\xi]$ construit dans la partie précédente est donc un anneau minimal dans lequel d admet une racine carrée. Il est parfois noté également formellement $\mathbb{Z}[\sqrt{d}]$. L'entier p est toujours supposé premier, et différent de 2. L'anneau $\mathbb{Z}[\xi]/(p)$ peut alors être assimilé à un anneau de calcul modulaire auquel on aurait adjoint une racine de d modulo p. Afin d'éviter des lourdeurs d'écriture (et une confusion possible des notations $\overline{a}$ pouvant désigner aussi bien la classe de a modulo p que le conjugué de a dans $\mathbb{C}$), on désignera par la même notation a un élément de $\mathbb{Z}[\xi]$ et sa classe modulo p dans $\mathbb{Z}[\xi]/(p)$.

1. Montrer que $\mathbb{Z}[\xi] = \{a\xi + b \mid a, b \in \mathbb{Z}\}$.
2. Montrer que la décomposition d'un élément x de $\mathbb{Z}[\xi]$ sous la forme $x = a\xi + b$ avec a, $b \in \mathbb{Z}$ est unique. On pourra distinguer deux cas, suivant que $d < 0$ ou $d > 0$.
3. On suppose toujours p premier impair, et on suppose que $d \wedge p = 1$. Montrer dans $\mathbb{Z}[\xi]/(p)$ l'implication $z^2 = 0 \Longrightarrow z = 0$.

Les deux dernières questions de cette partie ne sont pas indispensables à la suite du problème.

4. Pour tout $x \in \mathbb{Z}[\xi]$, si $x = a + \xi b$, on note $x^c = a - \xi b$, et $N(x) = x \times x^c$. Montrer que pour tout $x \in \mathbb{Z}[\xi]$, $N(x) \in \mathbb{Z}$, et x est inversible dans $\mathbb{Z}[\xi]/(p)$ si et seulement si p ne divise pas $N(x)$.
5. Montrer que si d n'est pas un résidu quadratique modulo p (donc d ne s'écrit pas sous forme d'un carré modulo p), alors $\mathbb{Z}[\xi]/(p)$ est un corps.

Partie III – Conditions pour que 2 et 3 soient résidus quadratiques

Le but de cette partie est d'établir certains résultats concernant les carrés dans $\mathbb{F}_p^*$. Nous cherchons notamment à savoir à quelle condition 2 et 3 sont des carrés modulo p, en discutant suivant la classe de congruence de p modulo 12 ou modulo 8. Les résultats obtenus dans cette partie sont des cas particuliers d'un théorème plus général (théorème de réciprocité quadratique), qui ne fait pas l'objet de ce problème.
Soit p un entier premier impair, et $n \in \mathbb{Z}$. On note $(\frac{n}{p})$ la quantité :

$$(\tfrac{n}{p}) = \begin{cases} 0 & \text{si } n \text{ est divisible par } p \\ 1 & \text{si } n \wedge p = 1 \text{ et } n \text{ est un résidu quadratique modulo } p \\ -1 & \text{si } n \wedge p = 1 \text{ et } n \text{ est un non-résidu quadratique modulo } p. \end{cases}$$

L'expression $(\frac{n}{p})$ est appelée symbole de Legendre.
On se fixe désormais un entier premier p différent de 2. Dans la suite du problème, on dira simplement que n est un résidu quadratique lorsque n est un résidu quadratique modulo p et qu'il n'y a pas d'ambiguïté sur l'entier premier p considéré.

1. Montrer que pour tout $n \in \mathbb{Z}$, $(\frac{n}{p}) \equiv n^{\frac{p-1}{2}}$ $[p]$.
2. À quelle condition sur p l'entier -1 est-il un résidu quadratique ?
3. Sans exprimer explicitement 2 sous forme d'un carré modulo p, déterminer si 2 est un résidu quadratique modulo p dans les cas suivants : $p = 11$, $p = 17$
4. 3 est-il un résidu quadratique modulo 11 ? modulo 17 ?
5. Montrer que pour tous entiers n et n' non divisibles par p :
   (i) si n et n' sont des résidus quadratiques, nn' aussi ;
   (ii) si n est un résidu quadratique et n' un non-résidu ou inversement, alors nn' est un non-résidu quadratique ;
   (iii) si n et n' sont des non-résidus quadratiques, nn' est un résidu quadratique (procéder par dénombrement).
6. En déduire que $(\frac{nn'}{p}) = (\frac{n}{p})(\frac{n'}{p})$.
7. Soit $j = \mathrm{e}^{\frac{2\,\mathrm{i}\,\pi}{3}}$. On suppose que $p > 3$.
   (a) Montrer que j est inversible dans $\mathbb{Z}[j]/(p)$. On pose $b = j - j^{-1}$, élément de $\mathbb{Z}[j]/(p)$.

(b) Calculer b^2, et en déduire que -3 est un résidu quadratique modulo p si et seulement si $b^p = b$.

(c) Exprimer b^p en fonction de j^p et j^{-p}, et en déduire une condition nécessaire et suffisante sur p pour que -3 soit un résidu quadratique modulo p.

(d) À l'aide de la question 5, en déduire que 3 est un résidu quadratique modulo p si et seulement si $p \equiv \pm 1$ [12].

8. Soit $\omega = \mathrm{e}^{\mathrm{i}\frac{\pi}{4}}$, vu comme élément de $\mathbb{Z}[\omega]/(p)$. En adaptant la preuve précédente, et en considérant $b = \omega + \omega^{-1}$, montrer que 2 est un résidu quadratique modulo p si et seulement si $p \equiv \pm 1$ [8], où p est un nombre premier supérieur ou égal à 3.

Partie IV – Critère de primalité de Lehmer et critère de Pépin

Soit $n > 1$ un entier impair

1. Soit $a \in \mathbb{Z}/n\mathbb{Z}$ un élément inversible. Montrer que l'ordre (multiplicatif) de a est égal $n-1$ si et seulement si $a^{n-1} \equiv 1$ [n] et pour tout diviseur *premier* q de $n-1$, $a^{\frac{n-1}{q}} \not\equiv 1$ [n].
2. Montrer que n est premier si et seulement s'il existe un entier a tel que $a^{n-1} \equiv 1$ [n] et pour tout diviseur premier q de $n-1$, $a^{\frac{n-1}{q}} \not\equiv 1$ [n] (critère de primalité de Lehmer)
3. En déduire que le nombre de Fermat F_n est premier si et seulement s'il existe a tel que $a^{\frac{F_n-1}{2}} \equiv -1$ [F_n].
4. Montrer que F_n est premier si et seulement si $3^{2^{2^n-1}} \equiv -1$ [F_n] (critère de Pépin).

Partie V – Suites de Lucas

Soit A un anneau, et $x \in A$ un élément inversible de A. On pose $a = x + x^{-1}$, et pour tout $n \in \mathbb{Z}$, $V_n = x^n + x^{-n}$. Par abus de notation, pour tout $n \in \mathbb{Z}$, on désignera simplement par n l'élément $n \cdot 1_A$ de A. On rappelle que par convention, $x^0 = 1_A$.

1. Montrer que $(V_n)_{n\in\mathbb{Z}}$ vérifie $V_0 = 2$, $V_1 = a$, pour tout $n \geqslant 1$, $V_{n+1} = aV_n - V_{n-1}$, et pour tout $n \in \mathbb{N}$, $V_{-n} = V_n$, et que ces relations déterminent entièrement (V_n) de façon unique.
2. Montrer que pour tout $(m,n) \in \mathbb{Z}^2$, $V_nV_m = V_{n+m} + V_{n-m}$ (on pourra commencer par justifier qu'on peut se contenter d'étudier le cas $(m,n) \in \mathbb{N}^2$).
3. En déduire une relation simple entre V_{2n} et V_n.

Partie VI – Critère de primalité de Lucas-Lehmer

1. *Soit p un nombre premier impair et $a \in \mathbb{F}_p$. On pose $\Delta = a^2 - 4$, qu'on suppose premier avec p, et ξ une racine de Δ dans $\mathbb{C}$.*

   (a) Montrer que dans $\mathbb{Z}[\xi]/(p)$, l'équation $x^2 - ax + 1 = 0$ admet au moins une solution. On se donne dans la suite une solution x de cette équation.

   (b) Justifier que x est inversible dans $\mathbb{Z}[\xi]/(p)$ et exprimer son inverse en fonction de a et de x.

   (c) Exprimer $(2x-a)^2$ en fonction de Δ, puis à l'aide de $(2x-a)^p$, montrer que si $\Delta^{\frac{p-1}{2}} \equiv 1$ [p] on a $x^{p-1} = 1$.

   (d) Montrer que si $\Delta^{\frac{p-1}{2}} \equiv -1$ [p], alors $x^{p+1} = 1$ dans $\mathbb{Z}[\xi]/(p)$.

   (e) Montrer que pour tout $m \in \mathbb{Z}$, $x^m = 1$ équivaut à $x^m + x^{-m} = 2$.

2. *Soit N un entier impair. On se donne a un entier tel que N et $a^2 - 4$ soient premiers entre eux. Soit $(V_i)_{i\in\mathbb{N}}$ la suite de Lucas initalisée par $V_0 = 2$, $V_1 = a$, et vérifiant donc la relation $V_{i+1} = aV_i - V_{i-1}$, $i \in \mathbb{N}^*$. On suppose que $V_{N+1} \equiv 2$ [N], et que $V_{\frac{N+1}{q}} - 2$ et N sont premiers entre eux pour tout facteur premier q de $N+1$. On considère p un facteur premier de N, et Δ, ξ et x tels que définis dans la question 1.*

   (a) Montrer que l'ordre (multiplicatif) de x dans $\mathbb{Z}[\xi]/(p)$ est égal à $N+1$.

   (b) Déduire de la question 1 que $N = p$, puis que N est premier (critère de primalité Lucas-Lehmer).

3. *Soit $s > 1$ et $M_s = 2^s - 1$ (nombre de Mersenne). Soit a un entier et $(L_i)_{i\geqslant 1}$ la suite définie par $L_1 = a$, $L_{i+1} = L_i^2 - 2$, pour tout $i > 0$.*
   (a) Montrer que si $a^2 - 4$ et M_s sont premiers entre eux, et si $L_{s-1} \equiv 0\ [M_s]$, alors M_s est premier (critère de Lucas)
   (b) Montrer que si $s > 1$ est impair le choix de $a = 4$ convient (on pourra commencer par montrer que $M_s \equiv 7\ [12]$). Que dire du cas s pair ?
4. *Dans cette question, on montre la réciproque. On suppose que M_s est premier et on définit la suite de Lucas (L_i) comme précédemment, définie avec la valeur $a = 4$. Soit ξ défini comme plus haut, à partir de la valeur $a = 4$, et $x \in \mathbb{Z}[\xi]/(M_s)$ tel que $x^2 - 4x + 1 = 0$. On pose $\beta = x - 2$.*
   (a) Montrer que $(1 + \beta)^2 = 2x$ et $(1 - \beta)^2 = 2x^{-1}$.
   (b) En déduire que dans l'anneau $\mathbb{Z}[\xi]/(M_s)$, on a l'égalité $2^{\frac{M_s+1}{2}} L_s = (1 + \beta)^{M_s+1} + (1 - \beta)^{M_s+1}$.
   *(c) En déduire que $L_{s-1} \equiv 0\ [M_s]$.

On a ainsi démontré le théorème de Lucas-Lehmer affirmant qu'avec les notations et les conditions de la question 3 et le choix de $a = 4$, M_s est premier si et seulement si $L_{s-1} \equiv 0\ [M_s]$.