ÉNS de Lyon
M2 FEADéP

Cours d'algèbre
2019–2020

Feuille d'exercices n°21 : Symbole de Legendre et résidus quadratiques.

Dans toute cette feuille p est un nombre premier différent de 2.

Symboles de Legendre et réciprocité quadratique

Exercice 1. Pour $p = 3, 5, 7, 11, 13$, calculer $\left(\frac{a}{p}\right)$ pour tout $a \in [\![1, p-1]\!]$.

Exercice 2. Pour $q = 3, 11, 17$, établir pour n'importe quel nombre premier p quand est-ce que q est carré modulo p.

Exercice 3. Grâce à la loi de réciprocité quadratique, calculer $\left(\frac{13}{37}\right), \left(\frac{45}{109}\right), \left(\frac{11}{199}\right)$.

Les calculs faits dans cet exercice sont faisable à la main, mais ne le seraient pas pour les grands nombres : pourquoi ?

Exercice 4. Soit p un nombre premier impair. Soit q une puissance de p et $\alpha \in \mathbb{F}_q^*$. On pose $\theta = \alpha + \alpha^{-1}$ et on note Φ_8 le 8-ième polynôme cyclotomique.

1. Montrer que $\theta^2 = 2 \iff \alpha$ est une racine de Φ_8.
2. On suppose que $\mathbb{F}_q$ est un corps de décomposition de Φ_8 sur $\mathbb{F}_p$ et que α est une racine de Φ_8. Montrer que $2^{\frac{p-1}{2}} = \frac{\theta^p}{\theta}$ et que $\alpha^p \in \{\pm \alpha^{\pm 1}\}$.
3. En déduire que $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \mod 8 \\ -1 & \text{si } p \equiv \pm 3 \mod 8 \end{cases}$.

Symboles de Jacobi

On rappelle que pour $a, b \in \mathbb{Z}$ avec b impair positif, on définit le *symbole de Jacobi* $\left(\frac{a}{b}\right)$ par

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{m_1} \cdots \left(\frac{a}{p_r}\right)^{m_r}$$

où la décomposition en facteurs premiers de b est $b = p_1^{m_1} \cdots p_r^{m_r}$.

Exercice 5. Soient $b \in \mathbb{N}^*$ impair et $a \in \mathbb{Z}$.

1. Montrer qu'on peut avoir $\left(\frac{a}{b}\right) = 1$ même si a n'est pas un carré modulo b.
2. Montrer également que $\left(\frac{a}{b}\right) = 0$ si et seulement si a et b ne sont pas premiers entre eux.
3. Montrer que le symbole de Jacobi $\left(\frac{a}{b}\right)$ ne dépend que de la classe de congruence de a modulo b.

Exercice 6. Soient $b \in \mathbb{N}^*$ impair et $a \in \mathbb{Z}$. Montrer que le symbole de Jacobi $\left(\frac{a}{b}\right)$ vérifie les mêmes formules que le symbole de Legendre et est multiplicatif en b, autrement dit que :

$$\begin{aligned}
\left(\frac{aa'}{b}\right) &= \left(\frac{a}{b}\right) \cdot \left(\frac{a'}{b}\right) \\
\left(\frac{a}{bb'}\right) &= \left(\frac{a}{b}\right) \cdot \left(\frac{a}{b'}\right) \\
\left(\frac{-1}{b}\right) &= (-1)^{\frac{b-1}{2}} \\
\left(\frac{2}{b}\right) &= (-1)^{\frac{b^2-1}{8}} \\
\left(\frac{a}{b}\right) &= (-1)^{\frac{(a-1)(b-1)}{4}} \left(\frac{b}{a}\right)
\end{aligned}$$

où a est supposé impair positif dans la dernière formule.

Exercice 7.

1. Quelle est la complexité de l'algorithme suivant calculant le symbole de Jacobi $\left(\frac{a}{b}\right)$?

   Partant de a et b avec b impair positif, on utilise ε la variable de stockage, initialisée à $\varepsilon := 1$:
   - Si $b = 1$, on renvoie ε.
   - Réduction 1 : si $a = bq + r$ est la division euclidienne de a par b, on a simplement à calculer $\left(\frac{r}{b}\right)$ (si $r = 0$, on termine l'algorithme en renvoyant 0), donc on remplace a par r, de sorte que $a < b$.
   - Réduction 2 : Si $a = 2^k a'$ avec a' impair, on multiplie ε par $(-1)^{\frac{b^2-1}{8}}$ à la puissance k puis on remplace a par a', de sorte que a est impair.
   - On multiplie ε par $(-1)^{(a-1)(b-1)/4}$ (autrement dit 1 sauf si a et b sont congrus à 3 modulo 4), et on échange les variables a et b, autrement dit on calcule $\left(\frac{b}{a}\right)$. On recommence à la première étape.
2. Calculer ainsi les symboles de Jacobi
$$\left(\frac{57}{189}\right), \left(\frac{314}{701}\right), \left(\frac{111}{533}\right).$$

Racines carrées modulo n

Exercice 8. Résoudre l'équation $x^2 = 2$ dans $\mathbb{Z}/5831\mathbb{Z}$.

Exercice 9.

1. Soit $\alpha \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ impair. Montrer que le nombre de solutions de l'équation $x^2 = a$ dans $\mathbb{Z}/2^\alpha\mathbb{Z}$ est égal à :
   - 1 si $\alpha = 1$
   - 2 si $\alpha = 2$ et $a \equiv 1 \mod 4$
   - 4 si $\alpha \geq 3$ et $a \equiv 1 \mod 8$
   - 0 dans tous les autres cas.
2. Soit $n \in \mathbb{N}^*$ et $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Déterminer en fonction de a et n, le nombre de solutions de $x^2 = a$ dans $\mathbb{Z}/n\mathbb{Z}$.

Exercices divers

Exercice 10. Montrer que pour tout premier impair p, au moins un entier parmi $-1, 2$ et -2 est un carré modulo p. En déduire que le polynôme $X^4 + 1$ est réductible modulo tout premier p.

Exercice 11. ***(Polya-Vinogradov)***

1. Pour tout $k \in \mathbb{Z}$, montrer que
$$\left(\frac{k}{p}\right) = \frac{1}{p}\sum_{a,b=0}^{p-1}\left(\frac{b}{p}\right)e^{\frac{2i\pi a(b-k)}{p}}.$$
2. En déduire (avec la notation de somme de Gauss $G(a)$ comme plus haut) que pour tout ensemble I d'entiers fini, on a
$$\sum_{k\in I}\left(\frac{k}{p}\right) = \frac{1}{p}\sum_{a=0}^{p-1}G(a)\sum_{k\in I}e^{-\frac{2i\pi ak}{p}}.$$
3. En déduire que si I est un intervalle fini d'entiers, on a l'inégalité de Polya-Vinogradov
$$\left|\sum_{k\in I}\left(\frac{k}{p}\right)\right| \leq \sqrt{p}\log p.$$
4. Conclure que pour tout nombre premier impair p, le premier entier naturel qui n'est pas un carré modulo p est inférieur à $\sqrt{p}\log p$.