Résidus quadratiques et symbole de Legendre

Ceci est une tentative de polycopié sous la forme de cours entrecoupé d'exercices, à propos du symbole de Legendre.

Pour commencer, on note ci-dessous p un nombre premier impair. On notera parfois $\mathbb{F}_p$ le corps de cardinal p au lieu de $\mathbb{Z}/p\mathbb{Z}$ quand ce sera pour insister sur ses propriétés de corps.

1 Le symbole de Legendre

L'application $x \mapsto x^2$ est un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z})^*$ dans lui-même, dont le noyau est $\{\pm 1\}$ car ce sont les racines de X^2+1 dans $\mathbb{F}_p$. Les carrés de $(\mathbb{Z}/p\mathbb{Z})^*$ forment donc un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ de cardinal $(p-1)/2$.

Exercice 1. Que se passerait-il pour $p = 2$ ou $p = n$ non premier avec ce morphisme ? Trouver des contre-exemples.

Exercice 2. Déduire de l'argument précédent que toute équation $ax^2 + by^2 = 1$ avec a et b non nuls dans $\mathbb{F}_p$ admet une solution $(x, y) \in {\mathbb{F}_p}^2$. Que dire si on considère un autre corps fini ?

Définition (Symbole de Legendre)**.**

• Pour tout $a \in \mathbb{Z}$ non divisible par p, le *symbole de Legendre de a modulo p*, noté $\left(\frac{a}{p}\right)$ est défini par

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si} \quad a \text{ est carré modulo } p, \\ -1 & \text{sinon.} \end{cases}$$

On le définit de la même manière sur $\mathbb{F}_p$ comme il ne dépend que de la classe de congruence modulo p.

• Si p divise a, on pose $\left(\frac{a}{p}\right) = 0$.

Les éléments de $\mathbb{Z}$ qui sont des carrés dans $(\mathbb{Z}/p\mathbb{Z})$ sont appelés *résidus quadratiques modulo p*.

Lemme (Critère d'Euler)**.** *Pour tout $a \in {\mathbb{F}_p}^*$,*

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p.$$

En conséquence, le symbole de Legendre est un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z})^*$ dans $\{\pm 1\}$, autrement dit

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

Démonstration. Si $a = b^2$ dans ${\mathbb{F}_p}^*$, comme $b^{p-1} = 1$ par le théorème de Lagrange, on a donc $a^{(p-1)/2} = 1$. Réciproquement, le polynôme $X^{(p-1)/2} - 1$, de degré $(p-1)/2$, a pour racines les $(p-1)/2$ carrés de ${\mathbb{F}_p}^*$ donc ce sont les seules, de sorte que pour tout a non carré dans ${\mathbb{F}_p}^*$, $a^{(p-1)/2} \neq 1$ mais son carré vaut encore 1. C'est donc -1, et ainsi

$$a^{(p-1)/2} \equiv -1 \equiv \left(\frac{a}{p}\right) \bmod p.$$

□

Proposition 1. *Pour tout p premier impair,*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{si} \quad p \equiv 1 \bmod 4, \\ -1 & \text{si} \quad p \equiv 3 \bmod 4 \end{cases}$$

Exercice 3. Prouver cette proposition.

Exercice 4. Pour $p = 3, 5, 7, 11, 13$, calculer $\left(\frac{a}{p}\right)$ pour tout $a \in \{1, \cdots, p-1\}$.

Il ne semble à première vue pas y avoir de comportement « régulier » d'un entier modulo p : est-il un carré modulo p lorsqu'on fait varier p ou non ?

En fait, la suite va prouver qu'il y a bien une régularité dans ce comportement. Commençons par regarder si 2 est carré modulo p ou non.

Proposition 2. *Pour tout p premier impair,*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{si} \quad p \equiv \pm 1 \bmod 8, \\ -1 & \text{si} \quad p \equiv \pm 3 \bmod 8. \end{cases}$$

Démonstration. Considérons le produit $A = \prod_{k=1}^{(p-1)/2} 2k$. D'un côté, on a $A = 2^{(p-1)/2}((p-1)/2)!$.

Pour tout $k \in \{1, \cdots, (p-1)/2\}$, on a

$$p - 2k = 2\ell + 1.$$

Plus précisément : si $p \equiv 1 \bmod 4$, si k parcourt $\{(p-1)/4+1, \cdots, (p-1)/2\}$, les ℓ correspondants parcourent $\{1, \cdots, (p-1)/4 - 1\}$. Alors, dans ce cas,

$$A = \prod_{k=1}^{(p-1)/4} 2k \prod_{k=(p+3)/4}^{(p-1)/2} 2k \equiv \left(\prod_{k=1}^{(p-1)/4} 2k\right) (-1)^{(p-1)/4} \prod_{\ell=1}^{(p-1)/4-1} (2\ell+1) \equiv (-1)^{(p-1)/4} \left(\frac{p-1}{2}\right)! \bmod p.$$

Par le critère d'Euler, comme $(p-1)/2!$ est inversible modulo p, on en déduit dans ce cas que 2 est carré modulo p si et seulement si $p \equiv 1 \bmod 8$. □

Exercice 5. Adapter la preuve pour le cas où $p \equiv 3 \bmod 4$.

On constate ici que le fait que 2 soit carré modulo p se lit directement par rapport à une classe de congruence de p modulo un certain entier (en l'occurrence, 8), ce qui n'est pas évident à partir de la définition de départ.

Ceci se formule en fait pour tout nombre premier, et c'est la *loi de réciprocité quadratique*, énoncée ci-dessous.

Théorème 1 (Loi de réciprocité quadratique)**.**

Pour tous nombres premiers impairs p et q distincts,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Ce produit vaut donc 1 si p ou q est congru à 1 modulo 4, et -1 sinon.

Corollaire 3. *Pour un nombre premier fixé q, le fait q soit un résidu quadratique ou non modulo p dépend seulement de la classe de congruence de p modulo $4q$.*

Exercice 6. Pour $q = 3, 11, 17$, établir pour n'importe quel nombre premier p quand est-ce que q est carré modulo p.

2 Preuve de la loi de réciprocité quadratique

Il existe de nombreuses preuves différentes de la loi de réciprocité quadratique (dont beaucoup font des développements intéressants), nous allons ici nous concentrer sur une des plus classiques, utilisant les sommes dites de Gauss.

Définition (Sommes de Gauss)**.**
On fixe p un nombre premier impair et $\zeta = e^{2i\pi/p}$.
Pour tout entier $a \in \mathbb{Z}$, on définit la *somme de Gauss* $G(a)$ par

$$G(a) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \zeta^{ak}.$$

Remarque. Les termes dans la somme définissant $G(a)$ ne dépendent que de k modulo p, on peut donc la réécrire

$$G(a) = \sum_{k \in (\mathbb{Z}/p\mathbb{Z})} \left(\frac{k}{p}\right) \zeta^{ak}.$$

Proposition 4.
(*a*) *Pour tout* $a \in \mathbb{Z}$,

$$G(a) = \left(\frac{a}{p}\right) G(1).$$

(*b*) *On a*

$$G(1)^2 = \left(\frac{-1}{p}\right) p.$$

(*c*) *Pour tout nombre premier impair* q *différent de* p,

$$G(1)^{q-1} \equiv \left(\frac{q}{p}\right) \bmod q,$$

au sens où $G(1)^{q-1} - \left(\frac{q}{p}\right)$ *est un multiple d'entier algébrique par* q.

Démonstration.
(*a*) Tout d'abord, si p divise a,

$$G(a) = \sum_{k \in (\mathbb{Z}/p\mathbb{Z})} \left(\frac{k}{p}\right) = 0$$

car il y a autant de carrés que de non-carrés modulo p et $\left(\frac{0}{p}\right) = 0$.

On peut donc supposer que p ne divise pas a. Alors, la multiplication par a est un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$. On note a^* l'inverse de a modulo p et on réindexe donc la somme sous la forme

$$G(a) = \sum_{k' \in (\mathbb{Z}/p\mathbb{Z})} \left(\frac{a^* k'}{p}\right) \zeta^{k'} = \left(\frac{a^*}{p}\right) G(1) = \left(\frac{a}{p}\right) G(1)$$

car $\left(\frac{a^*}{p}\right) = \left(\frac{a}{p}\right)^{-1} = \left(\frac{a}{p}\right)$ comme le symbole de Legendre est à valeurs dans $\{\pm 1\}$.
(*b*) Grâce à la formule précédente,

$$\sum_{a=0}^{p-1} G(a)G(-a) = \left(\frac{-1}{p}\right)(p-1)G(1)^2.$$

D'un autre côté,

$$\begin{aligned} \sum_{a=0}^{p-1} G(a)G(-a) &= \sum_{a=0}^{p-1} \sum_{j,k=0}^{p-1} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right) \zeta^{aj-ak} \\ &= \sum_{j,k=0}^{p-1} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right) \sum_{a=0}^{p-1} \zeta^{a(j-k)}, \end{aligned}$$

et la somme sur a est nulle à moins que $j = k$, alors elle vaut p. On a donc

$$\sum_{a=0}^{p-1} G(a)G(-a) = p(p-1),$$

d'où on déduit la formule sur $G(1)^2$.

(c) Considérons l'anneau $A = \mathbb{Z}[\zeta]$, constitué d'entiers algébriques et le quotient $B = A/qA$. Comme B est de caractéristique q, on a dans l'anneau B :

$$\begin{aligned} G(1)^q &\equiv \sum_{k=0}^{p-1} \left(\frac{k}{p}\right)^q \zeta^{kq} \bmod qA \\ &\equiv \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \zeta^{kq} \bmod qA \\ &\equiv G(q) \bmod qA \\ &\equiv \left(\frac{q}{p}\right) G(1) \bmod qA. \end{aligned}$$

Mais $G(1)^2 = \pm p$ et est donc inversible dans B car p et q sont premiers entre eux. On peut donc simplifier la congruence ci-dessus par $G(1)$, ce qui donne le résultat. □

Tous ces résultats intermédiaires permettent finalement de prouver le théorème de réciprocité quadratique.

Preuve du théorème de réciprocité quadratique.

Soient p et q premiers impairs distincts. On raisonne encore dans l'anneau $B = \mathbb{Z}[e^{2i\pi/p}]/q\mathbb{Z}[e^{2i\pi/p}]$. Grâce à la proposition précédente, dans B :

$$\left(\frac{q}{p}\right) \equiv G(1)^{q-1} \equiv \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} p^{\frac{q-1}{2}} \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right),$$

grâce au critère d'Euler, car on travaille dans le sous-anneau $\mathbb{Z}/p\mathbb{Z}$ de B pour la dernière égalité.

Cette égalité de nombres entiers modulo $q\mathbb{Z}[e^{2i\pi/p}]$ est une égalité de nombres dans $\mathbb{Z}$ car les deux côtés sont égaux à ± 1 et qu'on a supposé q impair, de sorte que 2 est non nul modulo $q\mathbb{Z}[e^{2i\pi/p}]$. □

Exercice 7. 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 l'exercice sont gérables à la main, mais ne le seraient pas pour les grands nombres : pourquoi ?

C'est une des motivations pour la définition du symbole de Jacobi.

3 Symbole de Jacobi

Définition (Symbole de Jacobi)**.**

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

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_r}\right)^{e_r}$$

si la décomposition en facteurs premiers de b est $b = p_1^{e_1} \cdots p_r^{e_r}$.

Exercice 8.
(a) Montrer qu'on peut avoir $\left(\frac{a}{b}\right) = 1$ même si a n'est pas un carré modulo b.

(b) Montrer également que $\left(\frac{a}{b}\right) = 0$ si et seulement si a et b ne sont pas premiers entre eux.

(c) Montrer que le symbole de Jacobi $\left(\frac{a}{b}\right)$ ne dépend que de la classe de congruence de a modulo b.

Exercice 9. Montrer que le symbole de Jacobi (sous les hypothèses de bonne définition) vérifie les mêmes formules que le symbole de Legendre et est multiplicatif en b, à savoir :

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

où a est supposé impair positif dans la dernière formule.

Grâce aux formules montrées dans l'exercice suivant, on a un algorithme de calcul du symbole de Legendre (et même de Jacobi) bien plus efficace que les méthodes précédentes :
Partant de a et b avec b impair positif, on utilise ε la variable de stockage, initialisée à 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.

Exercice 10. Quelle est la complexité de cet algorithme ?
Calculer ainsi les symboles de Jacobi

$$\left(\frac{57}{189}\right), \left(\frac{314}{701}\right), \left(\frac{111}{533}\right).$$

4 Applications des résidus quadratiques

4.1 Critère de primalité de Solovay-Strassen

Soit $n \geq 1$ impair. Le but est de donner un critère de primalité de n.
Pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^*$, on définit

$$\chi_1(a) = \left(\frac{a}{n}\right), \quad \chi_2(a) = a^{\frac{n-1}{2}}$$

deux morphismes de groupes de $(\mathbb{Z}/n\mathbb{Z})^*$ dans lui-même (le premier étant même à valeurs dans les classes de ± 1 modulo n).

Si n est premier, on a bien $\chi_1 = \chi_2$ comme montré plus haut. S'il existe $a \in (\mathbb{Z}/n\mathbb{Z})^*$ tel que $\chi_1(a) \neq \chi_2(a)$, on l'appelle *témoin de Solovay-Strassen*

Le résultat essentiel est le suivant.

Théorème 2 (Solovay-Strassen)**.**

Soit $n \geq 1$ un entier impair.

Si n est composé, il existe bien un témoin de Solovay-Strassen, autrement dit l'égalité $\chi_1 \equiv \chi_2$ est un critère de primalité.

Démonstration. Commençons par le cas où n a un facteur carré. On peut donc l'écrire $n = p^\alpha m$ avec $p \geq 3$ premier ne divisant pas m et $\alpha \geq 2$.

Alors, considérons le sous-groupe H de $(\mathbb{Z}/n\mathbb{Z})^*$ constitué des éléments congrus à 1 modulo pm. Ce sont des carrés modulo m, et modulo p^α également (exercice plus bas). En particulier, χ_1 est trivial sur H. Par ailleurs, H est de cardinal $p^{\alpha-1}$ et donc tous ses éléments sont d'ordre une puissance de p. Ses éléments non triviaux ne vérifient donc pas $x^{(n-1)/2} = 1$ car p ne divise pas $(n-1)$.

Supposons maintenant que n est composé et sans facteur carré, on l'écrit $n = pm$ avec p premier impair ne divisant pas m et $m \geq 3$. Par le théorème des restes chinois, on peut prendre $x \in (\mathbb{Z}/n\mathbb{Z})^*$ qui n'est pas un carré modulo p et congru à 1 modulo m. On a donc $\chi_2(x) \neq -1$ (simplement en utilisant la congruence modulo m), mais $\chi_1(x) = -1$ par construction. □

Exercice 11. Soit $a \in \mathbb{Z}$ et b impair.

Montrer que a est un carré modulo b si et seulement si c'est un carré modulo tout diviseur premier de b.

Comment étendre ce critère pour b pair ?

Si n est composé, l'ensemble des « faux témoins de Solovay-Strassen » (c'est-à-dire des $a \in (\mathbb{Z}/n\mathbb{Z})^*$ pour lesquels on a quand même $\chi_1(n) = \chi_2(n)$) est donc un sous-groupe strict de $(\mathbb{Z}/n\mathbb{Z})^*$, donc d'indice au moins deux. La probabilité en prenant un élément de $(\mathbb{Z}/n\mathbb{Z})^*$ au hasard que ce soit un témoin de Solovay-Strassen est donc au moins 1/2. Ceci fournit donc un bon test probabiliste de primalité.

4.2 Exercices divers

Exercice 12. 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 13. [Polya-Vinogradov]

(a) Pour tout $k \in \mathbb{Z}$, montrer que

$$\left(\frac{k}{p}\right) = \frac{1}{p} \sum_{a,b=0}^{p-1} \left(\frac{b}{p}\right) e^{\frac{2i\pi a(b-k)}{p}}.$$

(b) En déduire (avec la notation de somme de Gauss $G(a)$ comme plus haut) que pour tout ensemble I d'entiers fini, on a

$$\sum_{k \in I} \left(\frac{k}{p}\right) = \frac{1}{p} \sum_{a=0}^{p-1} G(a) \sum_{k \in I} e^{-\frac{2i\pi ak}{p}}.$$

(c) En déduire que si I est un intervalle fini d'entiers, on a l'inégalité de Polya-Vinogradov

$$\left| \sum_{k \in I} \left(\frac{k}{p}\right) \right| \leq \sqrt{p} \log p.$$

En conclure que pour tout nombre premier impair p, le premier entier naturel qui n'est pas un carré modulo p est inférieur à $\sqrt{p} \log p$.