PRÉPARATION À L'AGRÉGATION EXTERNE : LOI DE RÉCIPROCITÉ QUADRATIQUE

TONY LIMAGNE

Résumé. On sait que -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p = 1 \mod 4$. La loi de récriprocité quadratique fournit un résultat analogue pour les nombres premiers l impairs et distincts de p. En fait, cette loi permet aussi de répondre à des questions très concrètes du type : 219 est-il un carré modulo 383 ? Bien sûr, pour décrire correctement cette situation il faut au préalable introduire les objets adéquats : c'est la raison-d'être du symbole de Legendre qui détecte quels sont les entiers qui sont des carrés modulo p et lesquel n'en sont pas. La loi de réciprocité quadratique s'obtient traditionnellement en évaluant de deux manières différentes le cardinal d'un certain ensemble (qui dépend du symbole de Legendre). Ici nous adoptons une démarche originale puisque cette évaluation repose en partie sur la théorie des formes quadratiques sur les corps finis.

Le développement ci-dessous est adapté pour les leçons 123, 121, 101, 170 et 190.

1. Carrés dans un corps fini

On fixe p un nombre premier et $q = p^n$ une puissance de p (avec $n \in \mathbb{N}$). On note $\mathbb{F}_q$ le corps fini à q éléments. On sait que le groupe multiplicatif $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ est cyclique d'ordre $q-1$.

Définition 1. Un élément $x \in \mathbb{F}_q$ est un *carré* (de $\mathbb{F}_q$) lorsqu'il existe $y \in \mathbb{F}_q$ tel que $x = y^2$. Un entier m est un *résidu quadratique modulo* q (ou un *carré modulo* q) lorsque son image dans $\mathbb{F}_q$ est un carré. On note $\mathbb{F}_q^2$ l'ensemble des carrés de $\mathbb{F}_q$ et on précise par $\mathbb{F}_q^{*2}$ l'ensemble des carrés non nuls de $\mathbb{F}_q$.

Lorsque p est impair on a $-1 \neq +1$ dans $\mathbb{F}_q$ si bien que le morphisme de groupes $\mathbb{F}_q^* \to \mathbb{F}_q^*, x \mapsto x^2$ induit l'isomorphisme

$$\mathbb{F}_q^{*2} \cong \mathbb{F}_q^* / \{-1, +1\}.$$

En particulier on a $|\,\mathbb{F}_q^{*2}\,| = \frac{q-1}{2}$.

Théorème 2. (1) Si $p = 2$ alors $\mathbb{F}_q^2 = \mathbb{F}_q$.
(2) Si $p \neq 2$, les éléments de $\mathbb{F}_q^{*2}$ sont les racines du polynôme $X^{(q-1)/2} - 1$.

Démonstration. (1) Comme $\mathrm{car}(\mathbb{F}_q) = 2$ l'application $\mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^2$ est un morphisme de corps (c'est le morphisme de Frobénius de $\mathbb{F}_q$). Cette application est donc injective, donc bijective (car $\mathbb{F}_q$ est un ensemble fini).
(2) Notons R l'ensemble des racines dans $\mathbb{F}_q$ du polynôme $X^{\frac{q-1}{2}} - 1$. Un élément $x \in \mathbb{F}_q^{*2}$ qui s'écrit $x = y^2$ dans $\mathbb{F}_q$ vérifie

$$x^{\frac{q-1}{2}} = y^{q-1} = 1,$$

Date: Année 2024.

car $\mathbb{F}_q^*$ est un groupe d'ordre $q-1$. On a donc $\mathbb{F}_q^{*2} \subseteq R$. Or $\mathbb{F}_q$ est un corps de sorte que $\#R \leqslant \deg(X^{\frac{q-1}{2}} - 1) = \frac{q-1}{2}$. Et puisque $|\,\mathbb{F}_q^{*2}\,| = \frac{q-1}{2}$ on a alors $\mathbb{F}_q^{*2} = R$. □

Remarque 3. Lorsque $p \neq 2$, les non-carrés non nuls de $\mathbb{F}_q$ sont les racines du polynôme $X^{\frac{q-1}{2}} + 1$, et on possède une description des carrés de $\mathbb{F}_p$:

$$\mathbb{F}_p^{*2} = \left\{ 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \right\}.$$

Application 4. Soient $a, b \in \mathbb{F}_q^*$. L'équation $ax^2 + by^2 = 1$ possède au moins une solution dans $\mathbb{F}_q^*$.

Référence : pour l'essentiel voir [P, Chap. III, §2.d)] ; en ce qui concerne l'application 4 voir [P, Chap. V, §6, Lemme 6.10].

2. Symbole de Legendre et lois complémentaires

Dans la suite p est un nombre premier *impair*. Deux questions nous motivent :

Question 1. Étant donné $n \in \mathbb{Z}$, peut-on déterminer rapidement si n est un carré modulo p ?
Question 2. Quels sont les nombres premiers impairs et distincts de p qui sont des carrés modulo p et lesquels n'en sont pas ?

Soit $x \in \mathbb{F}_p^*$. On définit le *symbole de Legendre* de x par

$$\left(\frac{x}{p}\right) = x^{(p-1)/2} \in \{-1, +1\}. \tag{1}$$

On étend ce symbole sur $\mathbb{F}_p$ en posant $\left(\frac{0}{p}\right) = 0$. Lorsque $n \in \mathbb{Z}$ a pour image $x \in \mathbb{F}_p$ on pose aussi $\left(\frac{n}{p}\right) = \left(\frac{x}{p}\right)$.

Proposition 5. Soient $x, y \in \mathbb{F}_p^*$.

(1) On a $\left(\frac{x}{p}\right) = 1$ si et seulement si $x \in \mathbb{F}_p^{*2}$.
(2) On a $\left(\frac{x}{p}\right) = -1$ si et seulement si $x \notin \mathbb{F}_p^{*2}$.
(3) On a $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$.

La proposition 5.(3) est appelée la *règle du produit*. Les points (1) et (2) de la proposition 5 montre que le symbôle de Legendre permet de détecter les entiers qui sont des résidus quadratiques modulo p (et ceux qui n'en sont pas). Cette interprétation est souvent prise pour définition. Dans ce cas, l'égalité (1) constitue une proposition, appelée le *critère d'Euler* (voir [S, Chap.5, §5.5, Proposition 1]).

Les deux théorèmes suivants apportent une réponse partielle (mais on le verra fondamentale) à la question 1.

Théorème 6 (Première loi complémentaire)**.** On a la formule

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

Autrement dit, -1 est un carré de $\mathbb{F}_p$ si et seulement si $p \equiv 1 \mod 4$.

Démonstration. Par le théorème 2.(2) : $(-1) \in \mathbb{F}_p^{*2} \Leftrightarrow (-1)^{(p-1)/2} = 1 \Leftrightarrow p \equiv 1 \mod 4$. □

Remarque 7. Le résultat est plus général : $-1 \in \mathbb{F}_q^{*2} \Leftrightarrow q \equiv 1 \mod 4$.

Théorème 8 (Deuxième loi complémentaire)**.** On a la formule

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Autrement dit, 2 est un carré de $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \mod 8$.

Démonstration. Comme p est impair on a $p^2 - 1 \equiv 0 \mod 8$. Le groupe cyclique $\mathbb{F}_{p^2}^*$ possède donc un élément ζ d'ordre 8. On a

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2.$$

En effet on a $\zeta^8 = 1$ et $\zeta^4 \neq 1$ donc $\zeta^4 = -1$, soit encore $\zeta^2 + \zeta^{-2} = 0$. Ainsi on a $2 \in \mathbb{F}_p^{*2}$ si et seulement si $\zeta + \zeta^{-1} \in \mathbb{F}_p$. Il suffit alors de montrer que $\zeta + \zeta^{-1} \in \mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \mod 8$.

Notons σ le morphisme de Frobénius de $\mathbb{F}_{p^2}$. Si $p \equiv \pm 1 \mod 8$ alors $\sigma(\zeta+\zeta^{-1}) = \zeta + \zeta^{-1}$. Or l'extension $\mathbb{F}_{p^2} / \mathbb{F}_p$ est galoisienne donc $\zeta + \zeta^{-1} \in \mathbb{F}_p$. Par l'absurde si $p \equiv \pm 3 \mod 8$ et $\zeta + \zeta^{-1} \in \mathbb{F}_p$ alors on aurait $\sigma(\zeta + \zeta^{-1}) = \zeta + \zeta^{-1} = \zeta^3 + \zeta^{-3}$ et donc $\zeta^2 + \zeta^{-2} = \zeta^4 + \zeta^{-4}$ c'est-à-dire $\zeta^2 + \zeta^{-2} = -2$. Et puisque $p \neq 2$ on a alors $\zeta^2 + \zeta^{-2} \neq 0$. Absurde. □

Référence : [S, Chap. 1, §3].

3. Classification des formes quadratiques non dégénérées sur un corps fini

Le théorème de réduction suivant est basé sur l'application 4.

Théorème 9. Soient $\mathbb{F}_q$ un corps fini de caractéristique différente de 2 et E un $\mathbb{F}_q$-espace vectoriel de dimension finie $n \geqslant 2$. Fixons $\alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$. Il y a exactement deux classes d'équivalence de formes quadratiques non dégénérées sur E, de matrices

$$\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \\ 0 & \cdots & 0 & \alpha \end{pmatrix}.$$

Référence : [P, Chap. V, §6, Théorème 6.8].

Corollaire 10. Soient $\mathbb{F}_q$ un corps fini de caractéristique différente de 2 et E un $\mathbb{F}_q$-espace vectoriel de dimension finie $n \geqslant 2$. Fixons $\alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$. Deux formes quadratiques non dégénérées Q et Q' sur E sont équivalentes si et seulement si elles ont le même discriminant.

4. Développement

Lemme 11. Soit $a \in \mathbb{F}_p^*$. L'ensemble $\{x \in \mathbb{F}_p : ax^2 = 1\}$ est de cardinal $1 + \left(\frac{a}{p}\right)$.

Démonstration. Le polynôme $aX^2 - 1 \in \mathbb{F}_p[X]$ admet une racine dans $\mathbb{F}_p$ si et seulement si $a^{-1} \in \mathbb{F}_p^{*2}$, ce qui équivaut encore à $a \in \mathbb{F}_p^{*2}$. L'ensemble $\{x \in \mathbb{F}_p : ax^2 = 1\}$ est donc l'ensemble des racines de $aX^2 - 1$ dans $\mathbb{F}_p$. Son cardinal vaut donc $2 = 1 + \left(\frac{a}{p}\right)$ si $a \in \mathbb{F}_p^{*2}$ et $0 = 1 + \left(\frac{a}{p}\right)$ sinon. □

Théorème 12 (Loi de réciprocité quadratique)**.** Soit l un nombre premier impair et distinct de p. On a la formule

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

Démonstration. Un vecteur général $\mathbf{x}$ de $\mathbb{F}_l^p$ sera noté $\mathbf{x} = (x_1, \dots, x_p)$. On munit $\mathbb{F}_l^p$ de la forme quadratique

$$Q(\mathbf{x}) = \sum_{i=1}^{p} x_i^2,$$

et on note $S = \{\mathbf{x} \in \mathbb{F}_l^p : Q(\mathbf{x}) = 1\}$. On fait agir le groupe $(\mathbb{F}_p, +)$ sur S via l'action

$$(k \mod p).\mathbf{x} = (x_{1+k}, \dots, x_{p+k}).$$

Par le théorème de Lagrange on a : $\mathrm{Stab}(\mathbf{x}) = \{0\}$ ou $\mathbb{F}_p$. Un élément $\mathbf{x} \in S$ est un point fixe si et seulement si $x_1 = \cdots = x_p$ de sorte que

$$\begin{array}{ccc} \{\mathbf{x} \in S : \mathrm{Stab}(\mathbf{x}) = \mathbb{F}_p\} & \to & \{x \in \mathbb{F}_l : px^2 = 1\} \\ \mathbf{x} & \mapsto & x_1 \end{array},$$

est une bijection (de réciproque $x \mapsto (x, \dots, x)$). D'après le lemme 11 les points fixes sont donc au nombre de $1 + \left(\frac{p}{l}\right)$. Soit $\{\mathbf{x}_1, \dots, \mathbf{x}_r\}$ est un système de représentants des orbites non singletons. Par l'équation aux classes on a

$$\#S = 1 + \left(\frac{p}{l}\right) + \sum_{i=1}^{r} |\,\mathbb{F}_p\,| \equiv 1 + \left(\frac{p}{l}\right) \mod p.$$

Posons $d = \frac{p-1}{2}$, $a = (-1)^d$ et $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{M}_2(\mathbb{F}_l)$. La matrice symétrique

$$\begin{pmatrix} \boxed{\mathrm{J}} & & & 0 \\ & \ddots & & \vdots \\ & & \boxed{\mathrm{J}} & 0 \\ 0 & & 0 & a \end{pmatrix} \in \mathrm{M}_p(\mathbb{F}_l),$$

représente dans la base canonique de $\mathbb{F}_l^p$ une forme quadratrique Q' ayant pour discriminant

$$\mathrm{discr}(Q') = \det(J)^d \times a = 1 = \mathrm{discr}(Q).$$

(Cette égalité a lieu dans le quotient $\mathbb{F}_l^* / \mathbb{F}_l^{*2}$). Ainsi par le théorème 9 les formes quadratiques Q et Q' sont équivalentes. En particulier on a

$$\#S = \#S',$$

où $S' = \{\mathbf{x} \in \mathbb{F}_l^p : Q'(\mathbf{x}) = 1\}$. Explicitement on a

$$S' = \left\{ (a_1, z_1, \dots, a_d, z_d, t) \in \mathbb{F}_l^p : 2\sum_{i=1}^{d} a_i z_i + at^2 = 1 \right\}.$$

Pour $(a_1, z_1, \dots, a_d, z_d, t) \in S'$, on distingue deux cas :

(1) ou bien

$$a_1 = \cdots = a_d = 0, \tag{C1}$$

et alors $at^2 = 1$. Toujours d'après le lemme 11, les éléments de S' vérifiant (C1) sont donc au nombre de

$$1 \cdot l^d \cdot \left(1 + \left(\frac{a}{l}\right)\right).$$ [1]

(2) ou bien

$$\exists i \in [\![1, d]\!], \quad a_i \neq 0, \tag{C2}$$

et alors le vecteur $(z_1, \ldots, z_d)$ vérifie l'équation paramétrique d'un hyperplan (affine) de $\mathbb{F}_l^d$, à savoir

$$\sum_{i=1}^{d} (2a_i) z_i + (at^2 - 1) = 0. \tag{$\mathscr{H}$}$$

Un hyperplan de $\mathbb{F}_l^d$ contient l^{d-1} éléments (comme $\mathbb{F}_l$-sous-espace vectoriel de dimension $d-1$). Les éléments de S' vérifiant (C2) sont donc au nombre de

$$(l^d - 1) \cdot l \cdot l^{d-1} \equiv 1 - l^d \mod p.$$ [2]

En résumé on a $\#S' \equiv l^d \left(\frac{a}{l}\right) + 1 \mod p$. Et puisque $\#S = \#S'$ on peut conclure (toujours dans $\mathbb{F}_p$) :

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

(La dernière égalité est obtenue en appliquant (deux foix) le critère d'Euler.) □

Référence : [CG, Chap. V, §C, Corollaire C.3 et Théorème C.5].

Remarque 13. (1) Les théorèmes 6, 8 et 12 sont de nature très différentes. Moralement, la loi de réciprocité quadratique dit que la situation rencontrée dans les théorèmes 6 et 8 n'est pas générale. Par exemple, 5 est un carré de $\mathbb{F}_7$ tandis que 7 n'est pas un carré de $\mathbb{F}_5$.

(2) Il existe beaucoup de démonstrations de la loi de réciprocité quadratique. Toutes sont basées sur une double évaluation du cardinal d'un ensemble particulier. La plus "élémentaire" utilise des sommes particulières, appelées *sommes de Gauss* (voir [S, Chap. 5, §5.5, Théorème 1]).

5. Réponses aux questions 1 et 2

La loi de réciprocité quadratique permet de répondre clairement à la question 2. Couplée à la règle du produit et aux lois complémentaires elle permet aussi de répondre à la question 1.

Exemple 14. 219 est-il un résidu quadratique modulo 383 ?

---

1. Dans l'ordre : (nombre de choix pour $a_1, \ldots, a_d$)× (nombre de choix pour $z_1, \ldots, z_d$)×(nombre de choix pour t).

2. Dans l'ordre : (nombre de choix pour $a_1, \ldots, a_d$)×(nombre de choix pour t)×(nombre d'éléments dans l'hyperplan d'équation ($\mathscr{H}$)). Au passage, la congruence donnée ici est obtenue en appliquant le théorème de Fermat.

Détails de l'exemple. La réponse est oui. En effet, par la proposition 5.(3) on a

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\left(\frac{73}{383}\right).$$

On applique deux fois la loi de réciprocité quadratique :

$$\left(\frac{3}{383}\right) = -\left(\frac{383}{3}\right) = -\left(\frac{-1}{3}\right) \quad \text{et} \quad \left(\frac{73}{383}\right) = +\left(\frac{383}{73}\right) = \left(\frac{18}{73}\right).$$

Encore par la proposition 5.(3) on a

$$\left(\frac{18}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{3^2}{73}\right) = \left(\frac{2}{73}\right).$$

Enfin puisque $3 \not\equiv 1 \mod 4$ et $73 \equiv 1 \mod 8$ on applique les deux lois complémentaires :

$$\left(\frac{-1}{3}\right) = -1 \qquad \text{et} \qquad \left(\frac{2}{73}\right) = 1,$$

et donc $\left(\frac{219}{383}\right) = 1$. On conclut grâce à la proposition 5.(1). □

Référence : [Z, Chap. 2, Problème 6, Question 5.].

Exercice 15. Montrer que 23 n'est pas un résidu quadratique modulo 59.

Référence : [S, Chap. 5, §5.5, Exemple d'application (après la proposition 2)].

6. Quelques questions bêtes auxquelles il faut absolument savoir répondre rapidement

(1) Pourquoi dans la preuve du théorème 12 les formes quadratiques Q et Q' sont non dégénérées ?

(2) Soient K un corps fini, $a \in K \setminus \{0\}$ et $c \in K$. À quelle condition l'équation $ax^2 + bx + c = 0$ admet-elle au moins une racine dans K ?

(3) Identifier les endroits de la preuve du théorème 12 où on utilise vraiment les hypothèses $p \neq l$ et p, l impairs.

Références

[CG] Ph. Caldero et J. Germoni, *Nouvelles histoires hédonistes de groupes et géométries*, Vol. 1, Calvage & Mounet, 2017.

[S] J-P. Serre, *Cours d'arithmétique*, 3^e édition, Puf, 1988.

[P] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

[Z] M. Zavidovique, *Un Max de Math*, Calvage & Mounet, 2013.

[S] P. Samuel, *Théorie algébrique des nombres*, Méthodes, Hermann, 2003.