ÉNS de Lyon
M2 FEADEP

Cours d'algèbre
2018-2019

Symboles de Legendre, de Jacobi et résidus quadratiques

Leçons concernées (2019)

(120) Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

(121) Nombres premiers. Applications.

(126) Exemples d'équations en arithmétique.

Bibliographie

- À suivre...

A contrario des précédents cours, celui-ci constitue davantage des compléments sur des points non essentiels qui sont néanmoins source de nombreux développements, compléments dans un plan ou exercices classiques. Ce cours est entremêlé d'exercices qui sont repris et complétés dans la feuille d'exercice qui lui est associée.

1 Le symbole de Legendre

Soit $n \geqslant 3$ un entier. On définit un morphisme de groupes $\begin{array}{rccc} \varphi : & (\mathbb{Z}/n\mathbb{Z})^\times & \to & (\mathbb{Z}/n\mathbb{Z})^\times \\ & x & \mapsto & x^2 \end{array}$ d'élévation au carré. Son image est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$ qu'on pourra noter $(\mathbb{Z}/n\mathbb{Z})^{\times 2}$.

Exemple 1.1. Si $n = 36 = 2^2 \cdot 3^2$, le noyau de φ est $\{\overline{1}, \overline{17}, \overline{19}, \overline{35}\}$ et l'image est $(\mathbb{Z}/36\mathbb{Z})^{\times 2} = \{\overline{1}, \overline{13}, \overline{25}\}$

Si $n = p$ est un nombre premier, le noyau de φ est alors $\{\pm 1\}$ car ce sont les racines de $X^2 + 1$ dans le corps $\mathbb{F}_p$. Les carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ forment donc un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$ de cardinal $\frac{p-1}{2}$.

Exercice 1. 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 ?

Dans toute la suite p désigne un nombre premier **différent de** 2.

Définition 1.2 (Symbole de Legendre)**.**

Soit $a \in \mathbb{Z}$.

• Si a n'est pas divisible par p, le *symbole de Legendre de a modulo p*, noté $\left(\frac{a}{p}\right)$ est défini par

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

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 1.3 (Critère d'Euler)**.**

Pour tout $a \in \mathbb{F}_p^\times$, on a $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$.

En conséquence, le symbole de Legendre est un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z})^\times$ 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 $\mathbb{F}_p^*$, on a $a^{(p-1)/2} \neq 1$ mais son carré vaut encore 1. C'est donc -1, et ainsi

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

□

Proposition 1.4. *Pour tout p premier impair,*

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

Démonstration. Le critère d'Euler donne $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p$. Comme $p \geqslant 3$, on a $-1 \not\equiv 1 \mod p$. D'où la première égalité.

La seconde est une étude de la parité de $\dfrac{p-1}{2}$. □

Exercice 2. Pour $p = 3, 5, 7, 11, 13$, calculer $\left(\frac{a}{p}\right)$ pour tout $a \in [\![1, p-1]\!]$.

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 1.5. *Pour tout nombre p premier impair, on a*

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

Démonstration. La seconde égalité se déduit d'opérations arithmétiques élémentaires et est laissée en exercice au lecteur. On va montrer l'égalité entre le premier et le troisième terme de ces égalités.

Considérons le produit $A = \prod_{k=1}^{(p-1)/2} 2k$. D'une part, on a $A = 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$.

Raisonnons modulo p, de sorte que $A \equiv \left(\frac{p-1}{2}\right)! \left(\frac{2}{p}\right) \mod p$.

On observe une certaine symétrie du produit qu'il est tentant de « découper » en son milieu car, modulo p, on a $-(2k-p) = -2k \mod p$ et le terme $p-2k$ est un entier positif impair qu'on réécrit $p - 2k = 2\ell - 1$.

• cas où $p \equiv 1 \mod 4$:
Pour k parcourant $[\![\frac{p+3}{4}, \frac{p-1}{2}]\!]$, les ℓ correspondants parcourent $[\![1, \frac{p-1}{4}]\!]$. On a alors

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

Comme $\left(\frac{p-1}{2}\right)!$ est inversible modulo p, on en déduit dans ce cas que $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}$. Ainsi, par le critère d'Euler, on en déduit que 2 est carré modulo p si et seulement si $p \equiv 1 \mod 8$.

• cas où $p \equiv 3 \mod 4$:
Pour k parcourant $[\![\frac{p+1}{4}, \frac{p-1}{2}]\!]$, les ℓ correspondants parcourent $[\![1, \frac{p+1}{4}]\!]$. On a alors

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

Comme $\left(\frac{p-1}{2}\right)!$ est toujours inversible modulo p, on en déduit dans ce cas que $\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}$. Ainsi, par le critère d'Euler, on en déduit que 2 est carré modulo p si et seulement si $p \equiv -1 \mod 8$. □

On observe ici que le fait que 2 est 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.

2 Loi de réciprocité quadratique

Théorème 2.1 (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 2.2. *Pour un nombre premier fixé q, le fait que q soit un résidu quadratique ou non modulo p dépend seulement de la classe de congruence de p modulo $4q$.*

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

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 2.3 (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 2.4. 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 2.5. *On a les propriétés suivantes des sommes de Gauss :*

(a) $\forall a \in \mathbb{Z},\ G(a) = \left(\frac{a}{p}\right) G(1)$ *;*

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

(c) pour tout nombre premier impair q différent de p, la différence $G(1)^{q-1} - \left(\frac{q}{p}\right)$ est le produit d'un élément de $\mathbb{Z}[\zeta]$ (qui est en particulier un 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,

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

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 $j=k$, auquel cas 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 :

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

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.

Démonstration du théorème de réciprocité quadratique.

Soient p et q deux nombres premiers impairs distincts. On note encore $\zeta=e^{2i\pi/p}$ et $A=\mathbb{Z}[\zeta]$. Dans l'anneau quotient $B=A/qA$, on utilise la proposition précédente pour effectuer les identifications :

$$\begin{aligned}\left(\frac{q}{p}\right) &\equiv G(1)^{q-1} \mod q\mathbb{Z}[\zeta] && \text{par (c)} \\ &\equiv \left(G(1)^2\right)^{\frac{q-1}{2}} \mod q\mathbb{Z}[\zeta] \\ &\equiv \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} p^{\frac{q-1}{2}} \mod q\mathbb{Z}[\zeta] && \text{par (b)} \\ &\equiv \underbrace{\left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}}}_{\in\{\pm1\}}\underbrace{\left(\frac{p}{q}\right)}_{\in\{\pm1\}} \mod q\mathbb{Z}[\zeta] && \text{par le critère d'Euler}\end{aligned}$$

où les deux termes écrits sont vu dans $\{pm1\}$ comme produit de tels éléments.

Ainsi, la différence $\left(\frac{q}{p}\right)-(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)\in q\mathbb{Z}[\zeta]$ est aussi dans $\{-2,0,2\}$. Comme on a supposé q impair, on a $\pm2\notin q\mathbb{Z}[\zeta]$. Donc $\left(\frac{q}{p}\right)-(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)=0$. □

Exercice 4. 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 Le symbole de Jacobi

Définition 3.1 (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

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

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

Exercice 5.

(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.

Proposition 3.2. *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 :*

1. $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a'}{b}\right)$;
2. $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a}{b'}\right)$;
3. $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$;
4. $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$;
5. *si a est aussi impair positif, alors* $\left(\frac{a}{b}\right) = (-1)^{\frac{(a-1)(b-1)}{4}} \left(\frac{b}{a}\right)$.

Démonstration. Ceci est laissé en exercice au lecteur assidu. □

Grâce aux formules de cette proposition, on dispose d'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 $\varepsilon := 1$:

- 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.

Exercice 6. 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 $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, on définit deux morphismes de groupes de $(\mathbb{Z}/n\mathbb{Z})^\times$ dans lui-même :

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

le premier étant même à valeurs dans les classes de ± 1 modulo n.

Si n est premier, on a vu que $\chi_1 = \chi_2$ par le critère d'Euler.

S'il existe $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $\chi_1(a) \neq \chi_2(a)$, alors n est composé. Un tel a est appelé *témoin de Solovay-Strassen*.

Le résultat essentiel est le suivant.

Théorème 4.1 (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 $\chi_1 = \chi_2$ 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 $\alpha \geq 2$. Considérons le morphisme de surjection canonique $\pi : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/pm\mathbb{Z})^\times$ et le sous-groupe $H = \ker \pi$ de $(\mathbb{Z}/n\mathbb{Z})^\times$ constitué des éléments congrus à 1 modulo pm. On peut vérifier (exercice) que H est cyclique de cardinal $p^{\alpha-1}$ engendré par $\overline{1+pm}$. Comme H est cyclique d'ordre impair, tous ses éléments sont des carrés donc χ_1 est trivial sur H.

Par ailleurs, comme H est de cardinal $p^{\alpha-1}$, 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 $(n-1)$. En particulier, χ_2 est non trivial sur H.

• 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 $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ 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. □

Si n est composé, l'ensemble des « faux témoins de Solovay-Strassen » (c'est-à-dire des $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ pour lesquels on a quand même $\chi_1(a) = \chi_2(a)$) est donc un sous-groupe strict de $(\mathbb{Z}/n\mathbb{Z})^\times$, 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.

Remarque 4.2. Il existe un autre test de primalité : le test de Miller-Rabin qui s'avère a priori plus efficace car les témoins de Miller-Rabin sont en proportion 3/4 au lieu de 1/2 pour les témoins de Solovay-Strassen.

4.2 Nombre de racines carrés modulo n

Soit $n \in \mathbb{N}^*$ impair et $a \in \mathbb{Z}/n\mathbb{Z}$. On s'intéresse aux racines carrées de a modulo n, autrement dit aux solutions de l'équation diophantienne $x^2 = a$ dans $\mathbb{Z}/n\mathbb{Z}$.

Écrivons $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ une décomposition de n en produit de ses facteurs premiers. Par le théorème des restes chinois, trouver une racine carrée de a modulo n revient à trouver des racines carrées de a modulo $p_i^{\alpha_i}$ pour tout $i \in [\![1, r]\!]$. On se réduit donc au cas où $n = p^\alpha$ est une puissance d'un nombre premier impair.

Lemme 4.3. *Dans $\mathbb{Z}/p\mathbb{Z}$ avec p premier impair, si $a \in \mathbb{Z}/p\mathbb{Z}$, alors l'équation $x^2 = a$ a exactement $1 + \left(\frac{a}{p}\right)$ solutions.*

Démonstration. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc intègre. Si $a = 0$, nécessairement $x = 0$ par intégrité et $\left(\frac{a}{p}\right) = 0$, d'où le résultat.

Si a est un carré, alors il y a exactement deux racines carrées, racines du polynôme $X^2 - a$, et sinon il n'y a aucune solutions. D'où le résultat. □

Avant d'énoncer le théorème général, comparons les carrés modulo p et modulo p^α.

Lemme 4.4. *Soit p un nombre premier impair, $m \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ premier à p, alors a est un carré modulo p si, et seulement si, c'est un carré modulo p^m.*

Démonstration. On montre d'abord que si a est un carré modulo p^m, alors c'est un carré modulo p^{2m}. Soit $x \in \mathbb{Z}$ tel que $\overline{x}$ est une racine carrée de a modulo p^m et $z \in \mathbb{Z}$. Posons $y = x + zp^m$. On cherche une valeur de z pour que y soit une racine carrée de a modulo p^{2m}. On a $y^2 \equiv x^2 + 2xzp^m \mod p^{2m}$. Ainsi $y^2 \equiv a \mod p^{2m} \iff \frac{x^2-a}{p^m} \equiv 2xz \mod p^m$. Comme $2x$ est inversible modulo p^m, en prenant z tel que $z \equiv \frac{x^2-a}{p^m}(2x)^{-1} \mod p^m$, on fait de y une racine carrée de a modulo p^{2m}.

Il est clair que si a est un carré modulo p^m, c'en est un modulo p^s pour tout $s \leq m$ par réduction. Inversement, supposons que a est un carré modulo p. Par une récurrence immédiate, on observe que a est un carré modulo p^{2^k} pour tout $k \in \mathbb{N}$. En prenant k assez grand, on a $2^k \geq m$ et donc a est un carré modulo p^{2^k} donc aussi modulo p^m. □

Théorème 4.5. *Soit p un nombre premier impair et $\alpha \in \mathbb{N}^*$. Soit $a \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Alors l'équation $x^2 = a$ a exactement $1 + \left(\frac{a}{p}\right)$ solutions dans $\mathbb{Z}/p^\alpha\mathbb{Z}$.*

Démonstration. D'après le lemme si a n'est pas un carré modulo p^α, alors ce n'est pas un carré modulo p donc l'équation est sans solutions et $1 + \left(\frac{a}{p}\right) = 0$.

Supposons que a est un carré modulo p^α. Il suffit de montrer qu'il y a exactement deux racines carrées de a dans $\mathbb{Z}/p^\alpha\mathbb{Z}$. Soient x, y deux racines carrées de a modulo p^α. Alors $a \equiv x^2 \equiv y^2 \mod p^\alpha$ donc $(x-y)(x+y) \equiv 0 \mod p^\alpha$. Si $p|(x-y)$ et $p|(x+y)$ alors $p|2x$ donc $p|x$ car p est impair. Mais alors $p|x^2 = a$, ce qui est exclu. Donc $(x-y)$ ou $(x+y)$ est inversible modulo p^α et on a alors $y \equiv \pm x \mod p^\alpha$. Ce qui montre que a admet au plus deux racines carrées. On ne peut pas avoir $x \equiv -x \mod p^\alpha$ car p est impair. Donc a admet exactement deux racines carrées et alors l'équation $x^2 = a$ admet $1 + \left(\frac{a}{p}\right)$ solutions. □

Corollaire 4.6. *Si $n \in \mathbb{N}^*$ est impair et $a \in \mathbb{Z}$ est premier à n, alors le nombre de solutions de $x^2 = a$ dans $\mathbb{Z}/n\mathbb{Z}$ est*

$$\prod_{p|n} \left(1 + \left(\frac{a}{p}\right)\right) \in \left\{0, 2^{\text{Card}\{p \text{ premier impair divisant } n\}}\right\}.$$

Exercice 7. Résoudre l'équation $x^2 = 2$ dans $\mathbb{Z}/5831\mathbb{Z}$.

Exercice 8.

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 $\mathbb{Z}/n\mathbb{Z}$.