INSTITUT JOSEPH FOURIER

UNIVERSITÉ GRENOBLE ALPES

TRAVAIL D'ÉTUDE ET DE RECHERCHE

ANNÉE 2021

La loi de réciprocité biquadratique

ROMAIN MÉNABÉ

Encadrante : ODILE GAROTTA

Introduction

La loi de réciprocité quadratique est un résultat remarquable qui a trait à la propriété, pour p premier et a premier distinct de p, que a soit, ou non, un carré modulo p. Elle relie les propriétés, pour deux nombres premiers impairs distincts, que l'un soit, ou non, un carré modulo l'autre.

Elle fut conjecturée d'abord par Euler, puis reformulée par Legendre, et enfin démontrée pour la première fois par Gauss en 1801 dans *Disquisitiones arithmeticae*. Cette loi de réciprocité, qui a reçu de nombreuses preuves, a, par la suite, été largement généralisée.

Le but de ce mémoire est de traiter une de ces généralisations, nommée la loi de réciprocité biquadratique, qui relie les propriétés, pour deux irréductibles distincts de $\mathbb{Z}[i]$, que l'un soit, ou non, une puissance quatrième modulo l'autre.

Pour ce faire, nous introduisons de nouveaux objets tels que les caractères multiplicatifs, des applications analogues au symbole de Legendre à valeurs dans $\mathbb{C}^*$, et grâce à eux, les sommes de Gauss, qui en sont des transformées de Fourier discrètes, et les sommes de Jacobi, qui prennent en argument un nombre fini de caractères multiplicatifs, et renvoient un produit de convolution de ces caractères. Ces outils permettent d'exprimer et donc, suivant André Weil, d'approximer le nombre de solutions de certaines équations sur $\mathbb{F}_\mathrm{p}$. Ils nous fournissent au passage une autre preuve de la loi de réciprocité quadratique, puis une preuve de la loi de réciprocité biquadratique. Nous finissons par deux compléments autour de cette loi. D'abord, nous relions, pour deux premiers distincts congrus à 1 modulo 4, les propriétés d'être, ou non, une puissance $4^{ème}$ modulo l'autre, puis nous donnons une condition nécessaire et suffisante sur p, premier positif congru à 1 modulo 4, pour que 2 soit une puissance quatrième modulo p.

Table des matières

1 Préliminaires

1.1 Le symbole de Legendre

Définition 1.1.1. Soit p un nombre premier et a un entier.
Alors le *symbole de Legendre* $(\frac{a}{p})$ vaut :
0 si a est divisible par p.
1 si a est un résidu quadratique modulo p (c'est à dire qu'il existe $k \in \mathbb{Z}$ tel que $a \equiv k^2\ mod(p)$) mais n'est pas divisible par p.
-1 si a n'est pas un résidu quadratique modulo p.

Proposition 1.1.2. *(Critère d'Euler) :*
Soit p un nombre premier impair. On a, pour tout entier a :

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

Démonstration. Soit a un entier.
Si a est divisible par p, $a^{\frac{p-1}{2}}$ l'est aussi donc $a^{\frac{p-1}{2}} \equiv 0\ mod(p)$.
Si a n'est pas divisible par p, $a^{p-1} \equiv 1\ mod(p)$, donc, en raisonnant dans le corps $\mathbb{F}_p$, $a^{\frac{p-1}{2}} \equiv \pm 1\ mod(p)$.
Si a est un résidu quadratique modulo p, alors il existe $k \in \mathbb{Z}$ tel que $a \equiv k^2\ mod(p)$.
Donc $a^{\frac{p-1}{2}} \equiv (k^2)^{\frac{p-1}{2}}\ mod(p) \equiv k^{p-1}\ mod(p) \equiv 1\ mod(p)$.
Réciproquement, supposons que $a^{\frac{p-1}{2}} \equiv 1\ mod(p)$.
Soit g un élément de $\mathbb{Z}$ tel que la classe de g est un générateur de $\mathbb{F}_p^*$ cyclique. Alors la classe de a dans $\mathbb{F}_p^*$ est une puissance, que l'on note l, de la classe de g. Or, $g^{\frac{l(p-1)}{2}} = 1$ par hypothèse. Donc, $\frac{l(p-1)}{2}$ divise $p-1$, et donc 2 divise l.
En posant $g' = g^{\frac{l}{2}}$, on a $g'^2 \equiv a\ mod(p)$. □

Corollaire 1.1.3. *Soient p un nombre premier, et $a, b \in \mathbb{Z}$.*
Alors :
a) $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$.
b) Si $a \equiv b\ mod(p)$, *alors* $(\frac{a}{p}) = (\frac{b}{p})$.
c) Si p impair, $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

Démonstration. :
a) C'est une conséquence directe du critère d'Euler.
b) Cela vient directement avec la définition du symbole de Legendre.
c) On applique le critère d'Euler à $a = -1$ pour obtenir $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}}\ mod(p)$. Donc il existe $k \in \mathbb{Z}$ tel que $(\frac{-1}{p}) - (-1)^{\frac{p-1}{2}} = kp$. Puisque $p \geq 3$, en appliquant la valeur absolue de chaque côté de l'égalité, on a forcément $k = 0$, donc $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$. □

Définition 1.1.4. (*Symbole de Jacobi*)
Soit b un entier impair positif et a un entier. On décompose $b = p_1 ... p_n$ en produit d'entiers premiers positifs.
Le *symbole de Jacobi* est défini par

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) ... \left(\frac{a}{p_n}\right)$$

Lemme 1.1.5. *Soient $n \geq 2$, et $r_1, ..., r_n$ des entiers impairs. Alors,*

$$\sum_{i=1}^{n} \frac{(r_i - 1)}{2} \equiv \frac{(r_1 ... r_n - 1)}{2}\ mod(2)$$

Démonstration. Par récurrence sur n :
$n = 2$: Soient r et s deux entiers impairs.
Puisque $(r-1)(s-1) \equiv 0\ mod(4)$, $rs - 1 \equiv (r-1) + (s-1)\ mod(4)$.
En divisant par 2 de chaque côté, on obtient $\frac{rs-1}{2} \equiv \frac{(r-1)}{2} + \frac{(s-1)}{2}\ mod(2)$.
Donc la propriété est vraie au rang 2.

Soit $n \geq 2$. Supposons que la propriété est vraie pour n entiers impairs.
Montrons qu'elle le reste pour $n+1$ entiers impairs.
Soient $r_1, ..., r_{n+1}$ des entiers impairs.
On note $r' = r_1...r_n$. r' est impair comme produit d'entiers impairs.
Et par le cas $n = 2$, $\frac{r'r_{n+1}-1}{2} \equiv \frac{(r'-1)}{2} + \frac{(r_{n+1}-1)}{2}\ mod(2)$.
Or, par hypothèse de récurrence, $\frac{(r'-1)}{2} \equiv \sum_{i=1}^{n} \frac{(r_i-1)}{2}\ mod(2)$.

Donc, $\frac{r_1...r_{n+1}-1}{2} \equiv \sum_{i=1}^{n+1} \frac{(r_i-1)}{2}\ mod(2)$. □

Proposition 1.1.6. *Soit b entier positif impair.*
a) $(\frac{-1}{b}) = (-1)^{\frac{b-1}{2}}$.
b) Si a est un entier positif impair, alors

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

Démonstration. a) On décompose b en produit de nombres premiers positifs (impairs), $b = p_1...p_n$.
Alors, par définition, $(\frac{-1}{b}) = (\frac{-1}{p_1})...(\frac{-1}{p_1})$.
Par le Corollaire 1.1.3, pour tout $1 \leq i \leq n$, $(\frac{-1}{p_i}) = (-1)^{\frac{p_i-1}{2}}$.
Donc $(\frac{-1}{b}) = (-1)^{\sum_i \frac{p_i-1}{2}}$.
Par le Lemme 1.1.5, $\frac{p_i-1}{2} \equiv \frac{b-1}{2}\ mod(2)$.
Ainsi, $(\frac{-1}{b}) = (-1)^{\frac{b-1}{2}}$.

b) Soit a entier positif impair. On décompose a et b en produits d'élements premiers impairs positifs, $a = \prod_i q_i$ et $b = \prod_j p_j$.
Alors, $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \prod_i \prod_j (\frac{q_i}{p_j})(\frac{p_j}{q_i}) = (-1)^{\sum_{i,j} \frac{q_i-1}{2}\frac{p_j-1}{2}}$ d'après la loi de réciprocité quadratique (on l'admet pour l'instant, elle est démontrée plus loin).
Or, par le Lemme 1.1.5, $\sum_{i,j} \frac{q_i-1}{2}\frac{p_j-1}{2} \equiv \frac{a-1}{2}\frac{b-1}{2}\ mod(2)$. □

1.2 Puissances dans $\mathbb{F}_p$

Proposition 1.2.1. *Soient a, n et p des entiers.*
La congruence $nb \equiv a\ mod(p-1)$ a des solutions si, et seulement si, $d = pgcd(n, p-1)$ divise a. Si d divise a, alors il y a exactement d solutions modulo $p-1$.

Démonstration. On écrit pour la suite $n = n'd$ et $p - 1 = ld$ Si b_0 est solution, on écrit $nb_0 - a = (p-1)y_0, y_0 \in \mathbb{Z}$.
Donc $nb_0 - (p-1)y_0 = a$, et puisque d divise n et $p-1$, d divise a.

Réciproquement, supposons que d divise a.
Par Bézout, il existe x et y entiers tels que $nx + (p-1)y = d$. On pose $a' = \frac{a}{d} \in \mathbb{Z}$ et on multiplie les

deux côtés de l'égalité précédente par a'.
Alors, $a'nx - (p-1)ya' = a$. En posant $b_0 = a'x$, on obtient $nb_0 \equiv a\ mod(p-1)$, donc on a trouvé une solution à la congruence.
Soient maintenant b_0 et b_1 deux solutions de la congruence. Cela implique que $p-1$ divise $n(b_0 - b_1)$, donc l divise $n'(b_0 - b_1)$. Or, l et n' sont premiers entre eux, donc l divise $b_0 - b_1$, ou encore $b_1 = b_0 + kl, k \in \mathbb{Z}$. On vérifie alors que chaque $b_0 + kl, k \in \mathbb{Z}$ est une solution et que $b_0, b_0 + l, ..., b_0 + (d-1)l$ sont des solutions de la congruence, et qu'elles sont distinctes deux à deux.
Soit $b_1 = b_0 + kl$ une solution distincte des précédentes. Alors, il existe r et s des entiers tels que $0 \leq r < d$ et $k = sd + r$. Donc $b_1 = b_0 + rl + s(p-1)$, donc congru à $b_0 + rl$ modulo $p-1$.

□

Proposition 1.2.2. *Soit $a \in \mathbb{F}_p^*$, n entier et on pose $d = pgcd(p-1, n)$.*
Alors, $x^n = \alpha$ a des solutions si, et seulement si, $\alpha^{\frac{p-1}{d}} = 1$. De plus, s'il y a une solution, il y en a excatement d.

Démonstration. Soit g un générateur du groupe cyclique $\mathbb{F}_p^*$, et on écrit $\alpha = g^a$, et si $x \in \mathbb{F}_p^*$, on écrit $x = g^b$. Alors, résoudre $x^n = \alpha$ est équivalent à résoudre la congruence $nb \equiv a\ mod(p-1)$.
D'après la Proposition 1.2.1, on obtient que $x^n = \alpha$ admet d solutions si, et seulement si d divise a, et 0 sinon.
Si $\alpha^{\frac{p-1}{d}} = 1$, $g^{\frac{a(p-1)}{d}} = 1$, donc d divise a.
Si d divise $a, \alpha^{\frac{p-1}{d}} = g^{\frac{a}{d}(p-1)} = 1$.

□

1.3 Les entiers algébriques

Définition 1.3.1. Soit $\alpha \in \mathbb{C}$.
On dit que α est un *entier algébrique* s'il existe $P \in \mathbb{Z}[X]$, $P \neq 0$, et unitaire tel que $P(\alpha) = 0$.

Notation. *On note Ω l'ensemble des entiers algébriques. On admet dans la suite (cf. cours de M1) que Ω est un anneau.*

Proposition 1.3.2. *On a $\Omega \cap \mathbb{Q} = \mathbb{Z}$*

Démonstration. Si $\alpha \in \mathbb{Z}$, alors c'est une racine du polynôme $X - \alpha$, qui est non nul, unitaire et dans $\mathbb{Z}[X]$.
Donc $\alpha \in \Omega$.
Réciproquement, soit $\alpha \in \Omega \cap \mathbb{Q}$.
Puisque $\alpha \in \mathbb{Q}$, il existe p et q entiers premiers entre eux tels que $\alpha = \frac{p}{q}$.
Et puisque $\alpha \in \Omega$, il existe $P \neq 0$ unitaire à coefficients dans $\mathbb{Z}$ tel que $P(\alpha) = 0$. On écrit $P = \sum_{i=1}^{n-1} a_i X^i + X^n$ avec, pour tout $1 \leq i \leq n, a_i \in \mathbb{Z}$.
Alors, $\sum_{i=1}^{n-1} a_i (\frac{p}{q})^i + (\frac{p}{q})^n = 0$
En multipliant des deux côtés par q^n, on obtient $\sum_{i=1}^{n-1} a_i p^i q^{n-i} = -p^n$.
Or, q divise le terme de gauche dans l'égalité, donc il divise p^n. Mais p et q sont premiers entre eux, donc $q = \pm 1$.

□

Théorème 1.3.3. *(Frobenius)*
Soient ω_1 et $\omega_2 \in \Omega$ et $p \in \mathbb{Z}$ un nombre premier.
Alors :

$$(\omega_1 + \omega_2)^p \equiv \omega_1^p + \omega_2^p\ mod(p)$$

Démonstration. $(\omega_1+\omega_2)^p = \sum_{k=0}^{p} \binom{p}{k}\omega_1^k\omega_2^{p-k}$.
Or, si $1 \leq k \leq p-1$, p divise $\binom{p}{k}$.
Donc $(\omega_1+\omega_2)^p \equiv \omega_1^p + \omega_2^p \ mod(p)$. □

2 Le symbole de Legendre de 2

Posons $\xi = e^{\frac{2i\pi}{8}}$.
Alors, ξ est une racine primitive 8^{eme} de l'unité.
Donc $\xi^8 - 1 = 0$.
Or, $\xi^8 - 1 = (\xi^4-1)(\xi^4+1)$
Puisque $\xi^4 \neq 1$ (sinon ξ n'est pas primitive), et puisque $\mathbb{C}$ est intègre, on a $\xi^4 = -1$.
En multipliant par ξ^{-2} de chaque côté, on a $\xi^2 + \xi^{-2} = 0$.
Le caractère quadratique de 2 va maintenant venir de la relation $(\xi+\xi^{-1})^2 = \xi^2 + 2 + \xi^{-2} = 2$.
Posons $\tau = \xi + \xi^{-1}$ et notons que ξ et τ sont des entiers algébriques.
En effet, d'après ce qu'on vient de voir, si on pose $P = X^8 - 1$ et $Q = X^2 - 2$, on a P et Q non nuls unitaires, dans $\mathbb{Z}[X]$, et on a $P(\xi) = 0$ et $Q(\tau) = 0$.
On va donc travailler avec les congruences sur l'anneau des entiers algébriques.
Soit $p \in \mathbb{Z}$ un premier impair. On a alors :
$\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} \equiv (\frac{2}{p}) \ mod(p)$
On en déduit que $\tau^p = \tau^{p-1}\tau = (\frac{2}{p})\tau \ mod(p)$.
D'après le Théorème 1.3.3, $\tau^p = (\xi+\xi^{-1})^p \equiv \xi^p + \xi^{-p} mod(p)$.
En se rappelant que $\xi^8 = 1$, on a si $p \equiv \pm 1 \ mod(8)$, il existe $k \in \mathbb{Z}$, tel que $p = \pm 1 + 8k$.
Alors, $\xi^p + \xi^{-p} = \xi^{\pm 1+8k} + \xi^{-(\pm 1+8k)} = \xi + \xi^{-1}$ et de la même façon, si $p \equiv \pm 3 \ mod(p)$, $\xi^p + \xi^{-p} = \xi^3 + \xi^{-3}$.
Et en remarquant que $\xi^4 = -1$, on obtient que $\xi^3 = -\xi^{-1}$.
Donc si $p \equiv \pm 3 \ mod(p)$, $\xi^p + \xi^{-p} = -(\xi+\xi^{-1})$.
On a ainsi traité tous les cas possibles pour p.
Pour résumer, $\xi^p + \xi^{-p} = \begin{cases} \tau \text{ si } p \equiv \pm 1 \ mod(p) \\ -\tau \text{ si } p \equiv \pm 3 \ mod(p) \end{cases}$
En substituant ce résultat dans la relation $\tau^p \equiv (\frac{2}{p})\tau \ mod(p)$ cela donne :
$(-1)^\varepsilon \tau \equiv (\frac{2}{p})\tau \ mod(p)$ où $\varepsilon \equiv \frac{p^2-1}{8} \ mod(2)$.
En effet :
Si $p \equiv \pm 1 \ mod(8)$:
Il existe $k \in \mathbb{Z}$ tel que $p = \pm 1 + 8k$.
Donc : $p^2 = 1 \pm 16k + 64k^2$.
$p^2 - 1 = \pm 16k + 64k^2$.
$\frac{p^2-1}{8} = \pm 2k + 8k^2 = 2\underbrace{(\pm k + 4k^2)}_{\in\mathbb{Z}}$.
Donc $\frac{p^2-1}{8} \equiv 0 \ mod(2)$.
De même :
Si $p \equiv \pm 3 \ mod(8)$:
Il existe $k \in \mathbb{Z}$ tel que $p = \pm 3 + 8k$.
Donc : $p^2 = 9 \pm 48k + 64k^2$.
$p^2 - 1 = 8 \pm 48k + 64k^2$.
$\frac{p^2-1}{8} = 1 \pm 6k + 8k^2 = 1 + 2\underbrace{(\pm 3k + 4k^2)}_{\in\mathbb{Z}}$.
Donc $\frac{p^2-1}{8} \equiv 1 mod(2)$.
$(-1)^\epsilon$ a donc bien la valeur souhaitée.
Et donc on a : $(-1)^\varepsilon \tau \equiv (\frac{2}{p})\tau \ mod(p)$.
En multipliant par τ, on obtient $(-1)^\varepsilon 2 \equiv (\frac{2}{p})2 \ mod(p)$.

Or, la classe de 2 est inversible dans $\mathbb{F}_p \subset \Omega/_{(p)}$ car $p \geq 3$ impair.
On simplifie par 2 pour obtenir : $(-1)^\varepsilon \equiv (\frac{2}{p})\ mod(p)$.
Donc il existe $\omega \in \Omega$ tel que $(-1)^\varepsilon = (\frac{2}{p}) + \omega p$.
Puisque $p \neq 0$, on a : $\omega = \underbrace{\frac{(-1)^\varepsilon - (\frac{2}{p})}{p}}_{\in\mathbb{Q}}$.
Donc $\omega \in \Omega \cap \mathbb{Q}$.
D'après la Proposition 1.3.2, on a donc $\omega \in \mathbb{Z}$.
Et puisque $p \geq 3$, on a forcément $\omega = 0$.
On conclut que $(-1)^\varepsilon = (\frac{2}{p})$ où $\varepsilon \equiv \frac{p^2-1}{8}\ mod(2)$.

3 Sommes quadratiques de Gauss et loi de réciprocité quadratique

En rappelant la relation $(\xi + \xi^{-1})^2 = 2$ de la partie précédente, on peut se demander si on a une relation similaire pour p premier impair. La réponse est oui, et, de plus, la loi de réciprocité quadratique entière découle de cette nouvelle relation en utilisant la méthode vue dans la partie précédente.
Pour toute cette partie, on pose p un nombre premier positif impair et $\xi = e^{\frac{2i\pi}{p}}$ une racine $p^{ème}$ primitive de l'unité.

Lemme 3.0.1. $\sum_{k=0}^{p-1} \xi^{ak} = \begin{cases} p \ si\ a \equiv 0\ mod(p) \\ 0\ sinon \end{cases}$

Démonstration. Si $a \equiv 0\ mod(p)$, il existe $k \in \mathbb{Z}$ tel que $a = pk$.
Alors, ξ^a=1, et donc $\sum_{k=0}^{p-1} \xi^{ak} = \sum_{k=0}^{p-1} 1 = p$.
Sinon, $\xi^a \neq 1$, et donc on peut écrire $\sum_{k=0}^{p-1} \xi^{ak} = \frac{\xi^{ap}-1}{\xi^a-1} = 0$ car ξ^{ap}=1.

□

Corollaire 3.0.2. $\frac{1}{p} \sum_{k=0}^{p-1} \xi^{k(x-y)} = \delta(x,y)$ *où* $\delta(x,y) = \begin{cases} 1\ si\ x \equiv y\ mod(p) \\ 0\ sinon \end{cases}$

Lemme 3.0.3. *Soit p un nombre premier impair.*
Alors, il y a $\frac{p-1}{2}$ *carrés dans* $\mathbb{F}_p^*$.

Démonstration. On considère la fonction $f : \begin{array}{ccc} \mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ x & \longmapsto & x^2 \end{array}$ C'est un morphisme de $\mathbb{F}_p^*$, on va donc chercher son noyau et quotienter pour trouver le cardinal de son image.
Identifier son noyau revient à chercher les racines du polynôme $P = X^2 - 1$ dans $\mathbb{F}_p$.
Or, $\mathbb{F}_p$ est un corps et P est de degré 2, donc il admet au plus deux racines dans $\mathbb{F}_p$.
De plus, les classes de 1 et de -1 sont distinctes (et distinctes de celle de 0) puisque $p \geq 3$ et annulent ce polynôme. On a ainsi trouvé toutes les racines de P, elles sont dans $\mathbb{F}_p^*$, et au nombre de 2.
Le premier théorème d'isomorphisme donne alors que $Im(f)$ est de cardinal $\frac{p-1}{2}$.

□

Corollaire 3.0.4. *Il y a autant de résidus quadratiques non nuls que de résidus non quadratiques modulo p.*

C'est une conséquence immédiate du Lemme précédent.

Lemme 3.0.5. $\sum_{k=0}^{p-1} \left(\frac{k}{p}\right) = 0$, *avec* $\left(\frac{k}{p}\right)$ *le symbole de Legendre.*

Démonstration.
Par définition, $\left(\frac{0}{p}\right)$ =0.
Pour les $p-1$ autres termes de la somme , la moitié sont $+1$ et l'autre moitié -1, puisque d'après le Corollaire 3.0.4, il y a autant de résidus quadratiques non nuls que de résidus non quadratiques modulo p.
Cela donne le résultat attendu. □

On va maintenant introduire la notion de somme de Gauss.

Définition 3.0.6. On appelle *somme quadratique de Gauss* $g_a = \sum_{k=0}^{p-1} (\frac{k}{p})\xi^{ak}$.

Proposition 3.0.7. *On a* $g_a = (\frac{a}{p})g_1$.

Démonstration. Si a $\equiv 0$ $mod(p)$, alors $\xi^{ak} = 1$ pour tout k, et $g_a = \sum_{k=0}^{p-1} (\frac{k}{p}) = 0$ d'après le Lemme 3.0.5.
Sinon, $(\frac{a}{p}) = \pm 1$, donc son inverse aussi.
Et $(\frac{a}{p})g_a = (\frac{a}{p})\sum_{k=0}^{p-1} (\frac{k}{p})\xi^{ak} = \sum_{k=0}^{p-1} (\frac{ak}{p})\xi^{ak}$.
Or, p est premier donc l'application qui à k associe ak dans $\mathbb{F}_p$ est bijective, et donc, par le changement de variable $k' = ak$, on trouve :
$(\frac{a}{p})g_a = \sum_{k'=0}^{p-1} (\frac{k'}{p})\xi^{k'} = g_1$ donc $g_a = (\frac{a}{p})g_1$ en remarquant que $(\frac{a}{p})^{-1} = (\frac{a}{p})$.

□

A partir de maintenant, on va noter g à la place de g_1.
D'après ce qu'on vient de faire, $g_a^2 = g^2$.
Dans la suite, on va chercher cette valeur commune.

Proposition 3.0.8. *On a* $g^2 = (-1)^{\frac{p-1}{2}} p$.

Démonstration. :
L'idée de la preuve est d'évaluer la somme $\sum_{k=0}^{p-1} g_k g_{-k}$ de deux manières différentes.
Si k n'est pas divisible par p, alors $g_k g_{-k} = (\frac{k}{p})(\frac{-k}{p})g^2 = (\frac{-1}{p})g^2$ (indépendant de k).
Donc $\sum_{k=0}^{p-1} g_k g_{-k} = (p-1)(\frac{-1}{p})g^2$.
Maintenant, notons que $g_k g_{-k} = \sum_{n=0}^{p-1}\sum_{m=0}^{p-1} (\frac{n}{p})(\frac{m}{p})\xi^{k(n-m)}$.

Et donc on a :

$$\begin{aligned}
\sum_{k=0}^{p-1} g_k g_{-k} &= \sum_{k=0}^{p-1}\sum_{n=0}^{p-1}\sum_{m=0}^{p-1}\left(\frac{n}{p}\right)\left(\frac{m}{p}\right)\xi^{k(n-m)} \\
&= \sum_{n=0}^{p-1}\sum_{m=0}^{p-1}\left(\frac{n}{p}\right)\left(\frac{m}{p}\right)\sum_{k=0}^{p-1}\xi^{k(n-m)} \quad \text{car les sommes sont finies} \\
&= \sum_{n=0}^{p-1}\sum_{m=0}^{p-1}\left(\frac{n}{p}\right)\left(\frac{m}{p}\right)p\delta(n,m) \text{ par le Corollaire 3.0.2} \\
&= p\sum_{m=0}^{p-1}\left(\frac{m}{p}\right)^2
\end{aligned}$$

Si $m \equiv 0\ mod(p)$, $(\frac{0}{p}) = 0$, et sinon, $(\frac{m}{p}) \in \{\pm 1\}$, donc $(\frac{m}{p})^2 = 1$.
Donc $\sum_{k=0}^{p-1} g_k g_{-k} = p(p-1)$.
Avec nos deux calculs, on obtient $p(p-1) = (\frac{-1}{p})(p-1)g^2$.
De plus, par le critère d'Euler, $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}}\ mod(p)$, et c'est une congruence dans $\mathbb{Z}$, et $p \geq 3$, donc $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.
Ainsi, $g^2 = p(-1)^{\frac{p-1}{2}}$. □

Proposition 3.0.9. *(Loi de réciprocité quadratique)*
Soient p et q deux entiers premiers positifs impairs distincts.
Alors $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Démonstration. Posons $p^* = p(-1)^{\frac{p-1}{2}}$.
L'équation $g^2 = p^*$ obtenue dans la Proposition précédente est l'analogue désirée de l'équation $\tau^2 = 2$.
Soit $q \neq p$ un entier premier impair.
Pour prouver la loi de réciprocité quadratique, nous utiliserons des congruences modulo q dans l'anneau Ω. Puisque $\mathbb{Z} \subset \Omega$, toutes les congruences dans $\mathbb{Z}$ sont aussi des congruences dans Ω, et donc les Propriétés commme le critère d'Euler restent valables .
$g^{q-1} = (g^2)^{\frac{q-1}{2}} = {p^*}^{\frac{q-1}{2}} \equiv (\frac{p^*}{q})\ mod(q)$
Donc, puisque $g \in \Omega$ comme somme et produits d'éléments de Ω, $g^q \equiv g(\frac{p^*}{q})\ mod(q)$.
Or, on a $g^q = (\sum_{k=0}^{p-1}(\frac{k}{p})\xi^k)^q \equiv \sum_{k=0}^{p-1}(\frac{k}{p})^q\xi^{qk} mod(q)$ en utilisant le Théorème de Frobenius.
Puisque q est impair, $(\frac{k}{p})^q = (\frac{k}{p})$, donc $\sum_{k=0}^{p-1}(\frac{k}{p})^q\xi^{qk} = \sum_{k=0}^{p-1}(\frac{k}{p})\xi^{qk} = g_q$ par définition.
Ainsi, $g^q \equiv g_q\ mod(q)$. Or, d'après la Proposition 3.0.7, $g_q = (\frac{q}{p})g$.
Donc $g^q \equiv (\frac{q}{p})g\ mod(q)$. On en déduit que $(\frac{q}{p})g \equiv (\frac{p^*}{q})g\ mod(q)$.
En multipliant les deux côtés de la congruence par g, on obtient $(\frac{q}{p})p^* \equiv (\frac{p^*}{q})p^*\ mod(q)$.
Et puisque p et q sont premiers distincts, on peut simplifier par p^* et on a alors $(\frac{q}{p}) \equiv (\frac{p^*}{q})\ mod(q)$
En écrivant $(\frac{q}{p}) - (\frac{p^*}{q}) = \omega q$, $\omega \in \Omega$, on remarque que $\omega \in \mathbb{Q}$, donc $\omega \in \mathbb{Z}$ par la Proposition 1.3.2. Et puisque $q \geq 3$, on a forcément $\omega = 0$ en passant à la valeur absolue de chaque côté de l'égalité.
Donc $(\frac{q}{p}) = (\frac{p^*}{q})$.

$$\text{On a, } \left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right)$$
$$= \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \text{ par multiplicativité du symbole de Legendre}$$
$$= ((-1)^{\frac{q-1}{2}})^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \text{ par le point c) du Corollaire 1.1.3}$$
$$= (-1)^{\frac{(q-1)}{2}\frac{(p-1)}{2}} \left(\frac{p}{q}\right).$$

Finalement,

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

$\square$

La notion de somme de Gauss qu'on a utilisée sera généralisée par la suite. Une de ses généralisations, nommée somme biquadratique de Gauss, nous sera utile pour prouver la loi de réciprocité biquadratique.

4 Sommes de Gauss et de Jacobi

4.1 Caractères multiplicatifs

Un *caractère multiplicatif* sur $\mathbb{F}_p$ est une fonction de $\mathbb{F}_p^*$ dans $\mathbb{C}^*$ qui vérifie $\forall a, b \in \mathbb{F}_p^*$, $\chi(ab)=\chi(a)\chi(b)$

Remarque. *Le symbole de Legendre $(\frac{a}{p})$ est un exemple d'un tel caractère s'il est regardé comme une fonction des classes à gauche de a modulo p.*
Le caractère multiplicatif trivial est défini par : $\forall a \in \mathbb{F}_p^*, \epsilon(a) = 1$.
C'est souvent utile d'étendre le domaine de définition des caractères multiplicatifs à tout $\mathbb{F}_p$.
Pour $\chi = \epsilon$, on prend $\epsilon(0)$ =1.
Sinon, on prend $\chi(0) = 0$.

Dans la suite, pour les indices des sommes, on assimilera l'ensemble des entiers $\{1, ..., p\}$ (ou $\{0, ..., p-1\}$) à $\mathbb{Z}/p\mathbb{Z}$.

Proposition 4.1.1.
Soit χ un caractère multiplicatif et $a \in \mathbb{F}_p^*$. Alors :
a) $\chi(1_{\mathbb{F}_p}) = 1_{\mathbb{C}}$.
b) $\chi(a)$ est une racine $(p-1)^{ème}$ de l'unité.
c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Démonstration.
a) $\chi(1) = \chi(1.1) = \chi(1)\chi(1)$
Donc $\chi(1)(1 - \chi(1))$=0, et puisque χ est à valeurs dans $\mathbb{C}^*$ et par intégrité de $\mathbb{C}$, on a $\chi(1) = 1$.

b) On sait que $a^{p-1} = 1$ car $a \in \mathbb{F}_p$.
Donc $\chi(a^{p-1}) = \chi(1) = 1$ d'après a).
Mais par définition des caractères multiplicatifs, on a $\chi(a^{p-1}) = \chi(a)^{p-1}$.
Donc $\chi(a)^{p-1} = 1$ et $\chi(a)$ est une racine $(p-1)^{ème}$ de l'unité.

c)$\chi(aa^{-1}) = \chi(a)\chi(a^{-1})$ par définition et $\chi(aa^{-1}) = \chi(1) = 1$ d'après a).
Donc $\chi(a)\chi(a^{-1}) = 1$ et $\chi(a^{-1}) = \chi(a)^{-1}$.
D'après b), $\chi(a)$ est une racine $(p-1)^{ème}$ de l'unité, donc $|\chi(a)|$=1.
Or, $|\chi(a)| = \chi(a)\overline{\chi(a)}$.
Donc $\chi(a)\overline{\chi(a)} = 1$, ce qui donne $\overline{\chi(a)} = \chi(a)^{-1}$.

□

Dans la suite, par souci de simplification, on nommera simplement "caractère" les caractères multiplicatifs.

Proposition 4.1.2. *Soit χ un caractère multiplicatif.*
a) Si χ n'est pas le caractère trivial, $\sum_{k=1}^{p} \chi(k) = 0$.
b) Si χ est trivial, $\sum_{k=1}^{p} \chi(k) = p$.

Démonstration.
a)Supposons χ non trivial.
Dans ce cas, il existe $a \in \mathbb{F}_p^*$ tel que $\chi(a) \neq 1$. Soit a un tel élément.
On pose $T = \sum_{k=1}^{p} \chi(k)$.
Alors $\chi(a)T = \chi(a)\sum_{k=1}^{p} \chi(k) = \sum_{k=1}^{p} \chi(a)\chi(k) = \sum_{k=1}^{p} \chi(ak)$.
La fonction de $\mathbb{F}_p$ dans $\mathbb{F}_p$ qui à k associe ak étant une bijection, on effectue le changement de variable $k' = ak$ et on trouve :
$\chi(a)T = T$, donc $T(\chi(a) - 1)$=0.
Or, $\mathbb{C}$ est intègre, et, par hypothèse, $\chi(a) \neq 1$.
Donc $T = 0$.

b) Si χ est le caractère trivial, chaque terme de la somme vaut 1, et il y a p termes dans cette somme.
Donc $\sum_{k=1}^{p} \chi(k)$=p. □

On pose les définitions suivantes :
(1) : Si χ et λ sont des caractères, alors $\chi\lambda$ est une fonction qui, à a, associe $\chi(a)\lambda(a)$.
(2) : Si χ est un caractère, χ^{-1} est une fonction qui, à $a \in \mathbb{F}_p^*$, associe $\chi(a)^{-1}$.

Avec ces définitions, on a :

Proposition 4.1.3. *L'ensemble des caractères forme un groupe pour la multiplication.*

Démonstration.
Soient χ et λ deux caractères.
Vérifions que $\chi\lambda$ est un caractère sur $\mathbb{F}_p^*$.
$\chi\lambda$ est défini sur $\mathbb{F}_p^*$ et à valeurs dans $\mathbb{C}^*$ car χ et λ le sont.
De plus, soient $a, b \in \mathbb{F}_p^*$.

$$\begin{aligned}\chi\lambda(ab) &= \chi(ab)\lambda(ab) \text{ par la définition (1)}\\ &= \chi(a)\chi(b)\lambda(a)\lambda(b) \text{ car } \chi \text{ et } \lambda \text{ sont des caractères}\\ &= \chi(a)\lambda(a)\chi(b)\lambda(b) \text{ car } \mathbb{C}^* \text{ est commutatif.}\\ &= \chi\lambda(a)\chi\lambda(b) \text{ par la définition (1).}\end{aligned}$$

Donc $\chi\lambda$ est une caractère multiplicatif.
Associativité :
Soit $a \in \mathbb{F}_p^*$ et χ, λ et μ des caractères

$$\begin{aligned}(\chi(\lambda\mu))(a) &= \chi(a)\lambda\mu(a) \text{ par la définition (1)}\\ &= \chi(a)(\lambda(a)\mu(a)) \text{ par la définition (1)}\\ &= (\chi(a)\lambda(a))\mu(a) \text{ par associativité de la multiplication dans } \mathbb{C}\\ &= \chi\lambda(a)\mu(a) \text{ par la définition (1)}\\ &= ((\chi\lambda)\mu)(a) \text{ par la définition (1).}\end{aligned}$$

Donc $\chi(\lambda\mu) = (\chi\lambda)\mu$.

L'élément neutre est le caractère trivial.

Élément symétrique :
Soit $a \in \mathbb{F}_p^*$.
On rappelle que, d'après la définition (2), $\chi^{-1}(a)$=$\chi(a)^{-1}$.
Donc :
$\chi\chi^{-1}(a) = \chi(a)\chi(a)^{-1} = 1$.
Ceci étant valable pour tout a dans $\mathbb{F}_p^*$, on en conclut que $\chi\chi^{-1} = \epsilon$.

□

Dans la suite, on notera $\mathcal{X}_p$ le groupe des caractères sur $\mathbb{F}_p$.

Proposition 4.1.4. *$\mathcal{X}_p$ est un groupe cyclique d'ordre $p-1$.*
Si $a \in \mathbb{F}_p^*$, $a \neq 1$, alors il existe un caractère χ tel que $\chi(a) \neq 1$.

Démonstration. : $\mathbb{F}_p^*$ est cyclique, donc on pose g un de ses générateurs.
On voit que si χ est un caractère sur $\mathbb{F}_p$, χ est entièrement déterminé par son image en g.
Donc il y a au plus $p-1$ caractères dans $\mathcal{X}_p$.
On définit une fonction λ sur $\mathbb{F}_p$ par $\lambda(0) = 0$ et pour tout k dans $\mathbb{F}_p^*$, $\lambda(g^k) = e^{\frac{2i\pi k}{p-1}}$.
On a que, par des calculs simples, λ est un caractère non trivial. On note n son ordre.
Pour commencer, $\lambda^{p-1}(g) = \lambda(g^{p-1}) = \lambda(1) = 1$, donc $\lambda^{p-1} = \epsilon$.
On a donc que n divise $p-1$.
Et, $\lambda^n(g) = \lambda(g^n) = e^{\frac{2i\pi n}{p-1}}$. Or, par hypothèse, $\lambda^n(g) = 1$, donc $e^{\frac{2i\pi n}{p-1}} = 1$.
On obtient ainsi $p-1$ divise n.
On conclut que $n = p-1$.
Et donc, puisqu'il y a au plus $p-1$ caractères dans $\mathcal{X}_p$, et qu'on vient d'en exhiber un d'ordre $p-1$, on conclut que $\mathcal{X}_p$ est cyclique d'ordre $p-1$.

Soit $a \in \mathbb{F}_p^*$, $a \neq 1$.
Alors, $a = g^l$, avec l qui n'est pas divisible par $p-1$.

De plus, $\lambda(a)=\lambda(g)^l=e^{\frac{2i\pi n}{p-1}} \neq 1$.

□

Corollaire 4.1.5. *Soit $a \in \mathbb{F}_p^*$, $a \neq 1$.*
Alors, $\sum_{\chi \in \mathcal{X}_p} \chi(a) = 0$.

Démonstration. Posons $S= \sum_{\chi \in \mathcal{X}_p} \chi(a)$.
Puisque $a \neq 1$, il existe $\lambda \in \mathcal{X}_p$ tel que $\lambda(a) \neq 1$ d'après la Proposition précédente.
Ainsi, $\lambda(a)S = \sum_{\chi \in \mathcal{X}_p} \lambda(a)\chi(a) = \sum_{\chi \in \mathcal{X}_p} \lambda\chi(a)$.
En effectuant le changement de variable bijectif $\chi' = \lambda\chi$, on trouve :
$\lambda(a)S = \sum_{\chi' \in \mathcal{X}_p} \chi'(a) = S$.
Donc $(\lambda(a) - 1)S = 0$, avec $\lambda(a) \neq 1$ et $\mathbb{C}$ intègre.
On en déduit que $S = 0$.

□

Les caractères sont utiles dans l'étude des équations sur $\mathbb{F}_p$.
En effet, considérons l'équation $x^n=a$ avec $a \in \mathbb{F}_p^*$. Par la Proposition 1.2.2, on sait qu'il existe une solution à cette équation si, et seulement si $a^{\frac{p-1}{d}}=1$, où $d=\text{pgcd}(n,p-1)$, et que s'il y a existence d'au moins une solution, il y en a en fait exactement d.
Pour simplifier, on va supposer que n divise $p-1$.
Dans ce cas, $d=n$.
On donne maintenant un critère d'existence de ces solutions qui utilise les caractères.

Proposition 4.1.6. *Si $a \in \mathbb{F}_p^*$, n divise $p-1$ et l'équation $x^n=a$ n'est pas résoluble, alors il existe un caractère χ tel que :*
a) $\chi^n= \epsilon$.
b) $\chi(a) \neq 1$.

Démonstration. Soient λ et g définis comme dans la Proposition 4.1.4, et posons $\chi = \lambda^{\frac{p-1}{n}}$.
Alors, $\chi(g)=\lambda^{\frac{p-1}{n}}(g)=\lambda(g)^{\frac{p-1}{n}}=e^{\frac{2i\pi}{n}}$.
Or, on sait qu'il existe l dans $\mathbb{Z}$ tel que $a = g^l$.
Puisque l'équation $x^n=a$ n'est pas résoluble par hypothèse, on a que n ne divise pas l.
Alors, $\chi(a)=\chi(g)^l=e^{\frac{2il\pi}{n}} \neq 1$ car n ne divise pas l.
Pour finir, $\chi^n=\lambda^{p-1}=\epsilon$.

□

Pour $a \in \mathbb{F}_p^*$, on note $N(x^n=a)$ le nombre de solutions de l'équation $x^n=a$.

Proposition 4.1.7. *Si n divise $p-1$, alors $N(x^n = a) = \sum_{\chi^n=\epsilon} \chi(a)$*

Démonstration. D'après la Proposition 4.1.4, $\mathcal{X}_p$ est un groupe cyclique d'ordre $p-1$.
Puisqu'on a supposé que n divise $p-1$, on sait qu'il existe un unique sous-groupe d'ordre n dans $\mathcal{X}_p$.
Dans la proposition 4.1.6, on a trouvé un caractère tel que $\chi(g)=e^{\frac{2i\pi}{n}}$.
Il suit que $\epsilon,\chi,...,\chi^{n-1}$ sont n caractères distincts dont l'ordre divise n.

Pour prouver la formule, notons que l'équation $x^n=0$ a une seule solution, à savoir $x=0$.

Maintenant, $\sum_{\chi^n=\epsilon} \chi(0)=1$ puisque $\epsilon(0)=1$ et $\forall \chi \neq \epsilon, \chi(0) = 0$.
On suppose maintenant que $a \neq 0$ et que $x^n=a$ est résoluble, c'est-à-dire qu'il existe b tel que $b^n=a$.
Si $\chi^n=\epsilon$, alors $\chi(a) = \chi(b^n) = \chi(b)^n = \chi^n(b) = \epsilon(b) = 1$.
Ainsi, $\sum_{\chi^n=\epsilon} \chi(a)=n$, qui est $N(x^n = a)$ dans ce cas.

Pour finir, on suppose que $a \neq 0$ et que $x^n=a$ n'a pas de solution.
On doit montrer que $\sum_{\chi^n=\epsilon} \chi(a)=0$.
Notons $T = \sum_{\chi^n=\epsilon} \chi(a)$.
Par la proposition 4.1.6, il existe un caractère ρ tel que $\rho(a) \neq 1$ et $\rho^n = \epsilon$.
En utilisant le fait que les caractères dont l'ordre divise n forment un groupe, un calcul simple montre que $\rho(a)T=T$.
Puisque $\rho(a) \neq 1$ par hypothèse, et que $\mathbb{C}$ est intègre, on en conclut que $T = 0$.

□

On va regarder un cas particulier : supposons p impair et $n=2$.
Alors, la proposition précédente donne $N(x^2 = a) = 1 + (\frac{a}{p})$.

4.2 Les sommes de Gauss

On avait déjà défini les sommes quadratiques de Gauss plus tôt.
La définition qui suit en est une généralisation.

Définition 4.2.1. Soit χ dans $\mathcal{X}_\mathrm{p}$ et $a \in \mathbb{F}_\mathrm{p}$.
Posons $g_a(\chi) = \sum_{k=0}^{p-1} \chi(k)\xi^{ak}$ où $\xi = \mathrm{e}^{\frac{2i\pi}{p}}$.
$g_a(\chi)$ est appelée *somme de Gauss associée au caractère* χ.

Proposition 4.2.2.
Si $a \neq 0$ et $\chi \neq \epsilon$, on a $g_a(\chi)=\chi(a^{-1})g_1(x)$.
Si $a \neq 0$ et $\chi=\epsilon$, $g_a(\epsilon)=0$.
Si $a=0$ et $\chi \neq \epsilon$, $g_0(\chi)= 0$.
Si $a=0$ et $\chi=\epsilon$, $g_0(\epsilon)= p$.

Démonstration. Si $a \neq 0$ et $\chi \neq \epsilon$:
$\chi(a)g_a(\chi)=\chi(a)\sum_{k=0}^{p-1} \chi(k)\xi^{ak}=\sum_{k=0}^{p-1} \chi(ak)\xi^{ak}$.
On effectue ensuite le changement de variable bijectif $k' = ak$.
On a alors $\chi(a)g_a(\chi)=\sum_{k'=0}^{p-1} \chi(k')\xi^{k'}=g_1(\chi)$.
Puisque $\chi(a)^{-1}=\chi(a^{-1})$, on a prouvé le premier point.

Si $a \neq 0$, $g_a(\epsilon) = \sum_{k=0}^{p-1} \epsilon(k)\xi^{ak} = \sum_{k=0}^{p-1} \xi^{ak}=0$ (somme géométrique).
Si $a = 0$: $g_0(\chi) = \sum_{k=0}^{p-1} \chi(k)\xi^{0\times k} = \sum_{k=0}^{p-1} \chi(k)$.
Si $\chi =\epsilon$, on trouve p.
Si $\chi \neq \epsilon$, d'après la Proposition 4.1.2, on trouve 0.

□

A partir de maintenant, on notera $g(\chi)$ à la place de $g_1(\chi)$.
On souhaite déterminer le module de $g(\chi)$. Cela peut être fait facilement en imitant la preuve de la Proposition 3.0.8.

Proposition 4.2.3. *Si $\chi \neq \epsilon$, alors $|g(\chi)| = \sqrt{p}$.*

Démonstration. L'idée est d'évaluer la somme $\sum_{a=0}^{p-1} g_a(\chi)\overline{g_a(\chi)}$ de deux manières.
Si $a \neq 0$, on a, par la Proposition 4.2.2, $\overline{g_a(\chi)}=\overline{\chi(a^{-1})g(\chi)}=\chi(a)\overline{g(\chi)}$.
De plus, $g_a(\chi)=\chi(a^{-1})g(\chi)$, et $g_0(\chi)=0$.
Ainsi, $g_a(\chi)\overline{g_a(\chi)}=g(\chi)\overline{g(\chi)}= |g(\chi)|^2$.
Donc, $\sum_{a=0}^{p-1} g_a(\chi)\overline{g_a(\chi)}=\sum_{a=1}^{p-1} g_a(\chi)\overline{g_a(\chi)}=(p-1)|g(\chi)|^2$.
D'un autre côté, $g_a(\chi)\overline{g_a(\chi)}=\sum_x\sum_y \chi(x)\overline{\chi(y)}\xi^{ax-ay}$.

En sommant sur a des deux côtés et en utilisant le Corollaire 3.0.2 qui dit que $\frac{1}{p}\times\sum_{a=0}^{p-1}\xi^{a(x-y)} =\delta(x,y)$, on a :

$$\begin{aligned}\sum_a\sum_x\sum_y \chi(x)\overline{\chi(y)}\xi^{ax-ay} &= \sum_x\sum_y\sum_a \chi(x)\overline{\chi(y)}\xi^{ax-ay} \text{ car sommes finies}\\ &= p\sum_x\sum_y \delta(x,y)\chi(x)\overline{\chi(y)}\xi^{ax-ay}\\ &= p(p-1).\end{aligned}$$

Ainsi, $(p-1)\ |g(\chi)|^2= (p-1)p$.
Donc $|g(\chi)|^2= p$, et $|g(\chi)| =\sqrt{p}$.

□

Avant de continuer, on peut se demander quelle est la relation entre $\overline{g(\chi)}$ et $g(\overline{\chi})$
($\overline{\chi}$ est le caractère qui à a associe $\overline{\chi(a)}$)
$\overline{g(\chi)}=\sum_t \overline{\chi(t)}\xi^{-t}=\chi(-1)\sum_t \overline{\chi(-t)}\xi^{-t}=\chi(-1)g(\overline{\chi})$
En effet, puisque $\chi(-1)^2=\chi((-1)^2)=1$, on a $\chi(-1)=\pm 1$, et donc $\overline{\chi(-1)}=\chi(-1)$
Ainsi, $|g(\chi)|^2= p$ peut s'écrire $g(\chi)g(\overline{\chi})=\chi(-1)\ p$.
Si χ est le symbole de Legendre, on obtient le résultat de la Proposition 3.0.8.

4.3 Sommes de Jacobi

Considérons l'équation $x^2 + y^2 = 1$ sur le corps $\mathbb{F}_\mathrm{p}$. Puisque $\mathbb{F}_\mathrm{p}$ est un corps fini, l'équation n'a qu'un nombre fini de solutions.
On pose $N(x^2 + y^2 = 1)$ le nombre de ses solutions.
On va chercher à déterminer sa valeur explicite.
Notons que $N(x^2 + y^2 = 1) = \sum_{a+b=1} N(x^2 = a)N(y^2 = b)$
D'après le complément à la fin de la Proposition 4.1.7, on a $N(x^2 = a) = 1 + (\frac{a}{p})$.
On obtient donc en remplaçant dans la somme précédente :
$N(x^2 + y^2 = 1) = p + \sum_a(\frac{a}{p}) + \sum_b(\frac{b}{p}) + \sum_{a+b=1}(\frac{a}{p})(\frac{b}{p})$
D'après la Proposition 4.1.2, $\sum_a(\frac{a}{p})$ et $\sum_b(\frac{b}{p})$ sont nulles.

Nous obtiendrons ci-dessous en 4.3.2b) que la dernière somme vaut $-(-1)^{\frac{p-1}{2}}$

Il vient donc :

$$N(x^2+y^2=1)=\begin{cases} p-1 \text{ si } p\equiv 1 mod(4) \\ p+1 \text{ si } p\equiv 3 mod(4)\end{cases}$$

Définition 4.3.1. Soient χ et λ des caractères dans $\mathbb{F}_p$ et posons $J(\chi,\lambda)=\sum_{a+b=1}\chi(a)\lambda(b)$.
$J(\chi,\lambda)$ est une *somme de Jacobi.*

Théorème 4.3.2. *Soient χ et λ des caractères non triviaux. Alors :*
a) $J(\epsilon,\epsilon)=p$.
b) $J(\epsilon,\chi)=0$.
c) $J(\chi,\chi^{-1})=-\chi(-1)$.
d) Si $\chi\lambda\neq\epsilon$, alors $J(\chi,\lambda)=\frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.

Démonstration. a) Il suffit de voir combien il y a de termes dans la somme.
Le choix de b est entièrement déterminé par celui de a, et on a p choix pour a.
Donc il y a p termes dans cette somme, et on a le résultat attendu.

b) Conséquence immédiate de la Proposition 4.1.2.

c) $J(\chi,\chi^{-1})=\sum\limits_{a+b=1}\chi(a)\chi^{-1}(b)=\sum\limits_{\substack{b\neq 0\\ a+b=1}}\chi(ab^{-1})=\sum\limits_{a\neq 1}\chi(a(1-a)^{-1})$.
On effectue le changement de variable bijectif $c=a(1-a)^{-1}$ (Si $c\neq -1$, $a=c(1+c)^{-1}$).
Ainsi, $J(\chi,\chi^{-1})=\sum_{c\neq -1}\chi(c)=\sum_c\chi(c)-\chi(-1)=-\chi(-1)$.

d) On a :

$$\begin{aligned} g(\chi)g(\lambda)&=(\sum_a\chi(a)\xi^a)(\sum_y\lambda(y)\xi^y)\\ &=\sum_{a,y}\chi(a)\lambda(y)\xi^{a+y}\\ &=\sum_t(\sum_{a+y=t}\chi(a)\lambda(y))\xi^t \qquad (1)\end{aligned}$$

Si $t=0$, alors :

$$\begin{aligned}\sum_{a+y=0}\chi(a)\lambda(y)&=\sum_a\chi(a)\lambda(-a)\\ &=\lambda(-1)\sum_a\chi\lambda(a)\\ &=0 \text{ d'après la Proposition 4.1.2 puisque par hypothèse }, \chi\lambda\neq\epsilon.\end{aligned}$$

Si $t\neq 0$, on effectue les changements de variables bijectifs $a'=\frac{a}{t}$ et $y'=\frac{y}{t}$.
Si $a+y=t$, alors $a'+y'=1$.
On en déduit que :

$$\begin{aligned}\sum_{a+y=t}\chi(a)\lambda(y)&=\sum_{a'+y'=1}\chi(ta')\lambda(ty')\\ &=\chi(t)\lambda(t)\sum_{a'+y'=1}\chi(a')\lambda(y')\\ &=\chi\lambda(t)J(\chi,\lambda) \qquad \text{par définition des sommes de Jacobi.}\end{aligned}$$

En remplaçant dans l'équation (1), on trouve :

$$\begin{aligned} g(\chi)g(\lambda) &= \sum_t \chi\lambda(t)J(\chi,\lambda)\xi^t \\ &= J(\chi,\lambda)\sum_t \chi\lambda(t)\xi^t \\ &= J(\chi,\lambda)g(\chi\lambda) \text{ par définition d'une somme de Gauss.} \end{aligned}$$

De plus, puisque $\chi\lambda$ est non trivial, on a, par la Proposition 4.2.3, $g(\chi\lambda) \neq 0$.
On en conclut que $J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.

□

Corollaire 4.3.3. *Si χ, λ et $\chi\lambda$ sont différents de ϵ, alors $|J(\chi,\lambda)| = \sqrt{p}$.*

Démonstration.

$$\begin{aligned} |J(\chi,\lambda)| &= \left|\frac{g(\chi)g(\lambda)}{g(\chi\lambda)}\right| \qquad \text{d'après le théorème 4.3.2} \\ &= \frac{|g(\chi)||g(\lambda)|}{|g(\chi\lambda)|} \\ &= \frac{\sqrt{p}^2}{\sqrt{p}} \text{ d'après la Proposition 4.2.3} \\ &= \sqrt{p}. \end{aligned}$$

□

Proposition 4.3.4. *Si $p \equiv 1\ mod(4)$, il existe des entiers a et b tels que $p = a^2 + b^2$.*

Démonstration. On se place dans le groupe $\mathcal{X}_\mathrm{p}$. Il est cyclique d'ordre $p-1$ par la Proposition 4.1.4.
Et 4 est un diviseur de $p-1$ par hypothèse, donc en particulier, $\mathcal{X}_\mathrm{p}$ admet un sous-groupe cyclique d'ordre 4. Soit χ un de ses générateurs. Puisque χ est d'ordre 4, il est à valeurs dans $\{1,-1,i,-i\}$
Donc $J(\chi,\chi) = \sum_{s+t=1} \chi(s)\chi(t)$ est un élément de D.
On écrit alors $J(\chi,\chi) = a + ib, a, b \in \mathbb{Z}$. On a donc $|J(\chi,\chi)|^2 = a^2 + b^2$.
Or, par le Corollaire 4.3.3, $|J(\chi,\chi)|^2 = p$.
On a donc $p = a^2 + b^2$. □

Proposition 4.3.5. *Supposons que $p \equiv 1\ mod(n)$ et que χ est un caractère d'ordre $n > 2$.*
Alors $g(\chi)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)...J(\chi,\chi^{n-2})$.

Démonstration. Le fait de prendre $p \equiv 1\ mod(n)$ garantit l'existence d'un caractère d'ordre n.
Puisque χ est un caractère d'ordre $n > 2$, χ^2 est non trivial.
En utilisant le point d) du Théorème 4.3.2, on a $g(\chi)^2 = J(\chi,\chi)g(\chi^2)$.
En multipliant de chaque côté par $g(\chi)$, on obtient $g(\chi)^3 = J(\chi,\chi)g(\chi^2)g(\chi)$.
Si $n = 3, g(\chi^2) = g(\chi^{-1}) = g(\overline{\chi})$ et $g(\overline{\chi})g(\chi) = \chi(-1)p$.
Cela conclut pour le cas $n = 3$.
Sinon, on utilise encore une fois le point d) du Théorème 4.3.2, et on obtient $g(\chi)g(\chi^2) = g(\chi^3)J(\chi,\chi^2)$.
D'où $g(\chi)^3 = J(\chi,\chi)J(\chi,\chi^2)g(\chi^3)$.
En continuant de la même manière, on a en $n-1$ étapes $g(\chi)^{n-1} = J(\chi,\chi)...J(\chi,\chi^{n-2})g(\chi^{n-1})$.
Puisque χ est d'ordre n, $\chi^{n-1} = \chi^{-1} = \overline{\chi}$, donc $g(\chi)g(\chi^{n-1}) = g(\chi)g(\overline{\chi}) = \chi(-1)p$.
Ainsi, en multipliant par $g(\chi)$ de chaque côté dans l'expression de $g(\chi)^{n-1}$, on obtient $g(\chi)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)...J(\chi,\chi^{n-2})$.

□

4.4 L'équation $x^n + y^n$=1 dans $\mathbb{F}_p$

On suppose $p \equiv 1\ mod(n)$ et on va exprimer le nombre de solutions de l'équation $x^n + y^n = 1$ sur le corps $\mathbb{F}_p$.
On a $N(x^n + y^n = 1) = \sum_{a+b=1} N(x^n = a)N(y^n = b)$.
Soit χ un caractère d'ordre n.
D'après les Propositions 4.1.4 et 4.1.7, $N(x^n = a) = \sum_{i=0}^{n-1} \chi^i(a)$.
On obtient donc :

$$\begin{aligned} N(x^n + y^n = 1) &= \sum_{a+b=1} (\sum_{i=0}^{n-1} \chi^i(a))(\sum_{j=0}^{n-1} \chi^j(b)) \\ &= \sum_{a+b=1} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \chi^i(a)\chi^j(b) \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \sum_{a+b=1} \chi^i(a)\chi^j(b) \text{ car toutes les sommes sont finies} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} J(\chi^i, \chi^j) \text{ par définition.} \end{aligned}$$

D'après le théorème 4.3.2, on a :
Quand $i = j = 0$, on a $J(\chi^0, \chi^0) = J(\epsilon, \epsilon) = p$.
Quand $j + i = n$, $\chi^i = (\chi^j)^{-1}$, et donc par le Théorème 4.3.2, $J(\chi^i, \chi^j) = -\chi^i(-1)$.
On note $S = -\sum_{j=0}^{n-1} \chi^j(-1)$.
On va poser un Lemme avant de continuer :

Lemme 4.4.1. *Les éléments du noyau de χ sont les puissances $n^{èmes}$ dans $\mathbb{F}_p^*$.*

Démonstration. Puisque χ est d'ordre n, si un élément est une puissance $n^{ème}$ dans $\mathbb{F}_p^*$, il est dans le noyau.
Soient l un élément du noyau et g un générateur de $\mathbb{F}_p^*$.
χ est non trivial donc $\chi(g) \neq 1$. On écrit $\chi(g) = e^{\frac{2i\pi\alpha}{n}}$, $\alpha \in \mathbb{Z}$ avec $pgcd(n, \alpha) = 1$ (sinon, χ n'est pas d'ordre n).
On écrit aussi $l = g^k$, $k \in \mathbb{Z}$. Alors, $1 = \chi(l) = \chi(g)^k = e^{\frac{2i\pi\alpha k}{n}}$.
Or, $pgcd(\alpha, n) = 1$, donc n divise k, et l est une puissance $n^{ème}$ dans $\mathbb{F}_p^*$.

□

On remarque avec ce Lemme que $\sum_{j=1}^{n-1} \chi^j(-1)(=-S+1)$ vaut $n-1$ quand -1 est une puissance $n^{ème}$ dans $\mathbb{F}_p$ et 0 sinon.
Ainsi, on a $S = 1 - n\delta_n(-1)$ où

$$\delta_n(-1) = \begin{cases} 1 \text{ si } -1 \text{ est une puissance } n^{ème} \text{ dans } \mathbb{F}_p \\ 0 \text{ sinon.} \end{cases}$$

Enfin, si i=0 et $j \neq 0$ (ou inversement), $J(\chi^i, \chi^j) = 0$.

Ainsi, $N(x^n + y^n = 1) = p + 1 - n\delta_n(-1) + \sum_{\substack{i,j \\ 1 \leq i,j \leq n-1 \\ i+j \neq n}} J(\chi^i, \chi^j)$.

On va compter le nombre de termes dans la somme :
On a $(n-1)^2$ choix pour i et j tels que $1 \leq i, j \leq n$ auxquels il faut enlever les $n-1$ i (à j fixé) tels que $i+j=n$.
Il y a donc $(n-1)^2-(n-1)(=(n-1)(n-2))$ termes dans cette somme, et tous ces termes sont, d'après le Corollaire 4.3.3, de module égal à $\sqrt{p}$.

Proposition 4.4.2. *On a* $|N(x^n+y^n=1)+n\delta_n(-1)-(p+1)| \leq (n-1)(n-2)\sqrt{p}$.

Cette Proposition résulte de ce qu'on a écrit ci-dessus et en utilisant l'inégalité triangulaire. Pour p grand, l'estimation ci-dessus montre l'existence de nombreuses solutions non triviales.

4.5 Généralisation des sommes de Jacobi

Définition 4.5.1. Soient χ_1,...,χ_l des éléments de $\mathcal{X}_\mathrm{p}$.
La *somme de Jacobi associée à* χ_1,...,χ_l est définie par la formule :
$J(\chi_1,...,\chi_l)=\sum_{t_1+...+t_l=1}\chi_1(t_1)...\chi_l(t_l)$.
Quand $l=2$, on retrouve notre ancienne définition.
On pose aussi $J_0(\chi_1,...,\chi_l)=\sum_{t_1+...+t_l=0}\chi_1(t_1)...\chi_l(t_l)$.

Proposition 4.5.2.
a) $J_0(\epsilon,...,\epsilon)=J(\epsilon,...,\epsilon)=p^{l-1}$.

b) Si l'un des $\chi_i(1 \leq i \leq l)$ *est trivial, mais pas tous, alors* $J_0(\chi_1,...,\chi_l)=J(\chi_1,...,\chi_l)=0$.

c) Supposons $\chi_l \neq \epsilon$.
Alors : $J_0(\chi_1,...,\chi_l)=\begin{cases} 0 \text{ si } \chi_1...\chi_l \neq \epsilon \\ \chi_l(-1)(p-1)J(\chi_1,...,\chi_{l-1}) \text{ sinon.} \end{cases}$

Démonstration.
a) $J_0(\epsilon,...,\epsilon)=\sum_{t_1+...+t_l=0}1$.
Or, si on choisit arbitrairement $t_1,...,t_{l-1}$ dans $\mathbb{F}_\mathrm{p}$, t_l sera entièrement déterminé par l'équation $t_1+...+t_l=0$.
Il y a donc p^{l-1} termes dans cette somme.
On effectue le même raisonnement pour $J(\epsilon,...,\epsilon)$.

b) On peut supposer, sans perte de généralité, que $\chi_1,...,\chi_s$ sont non triviaux et $\chi_{s+1}=...=\chi_l=\epsilon$ où $1 \leq s \leq l-1$.
Alors :

$$\begin{aligned} J_0(\chi_1,...,\chi_l) &= \sum_{t_1+...+t_l=0}\chi_1(t_1)...\chi_l(t_l) \\ &= \sum_{t_1,...,t_{l-1}}\chi_1(t_1)...\chi_s(t_s) \\ &= \left(\sum_{t_1}\chi_1(t_1)\right)...\left(\sum_{t_s}\chi_s(t_s)\right)\left(\sum_{t_{s+1},...,t_{l-1}}1\right) \\ &= p^{l-s-1}\left(\sum_{t_1}\chi_1(t_1)\right)...\left(\sum_{t_s}\chi_s(t_s)\right) \\ &= 0 \text{ d'après la Proposition 4.1.2 puisque } \chi_1,...,\chi_s \text{ sont non triviaux.} \end{aligned}$$

On effectue le même raisonnement sur $J(\chi_1, ..., \chi_l)$ pour trouver le même résultat.

c) $J_0(\chi_1, ..., \chi_l) = \sum_s \left(\sum_{t_1+...+t_{l-1}=-s} \chi_1(t_1)...\chi_{l-1}(t_{l-1}) \right) \chi_l(s)$
Puisque $\chi_l \neq \epsilon$, $\chi_l(0) = 0$, donc on suppose dans la suite que $s \neq 0$
On effectue alors le changement de variable bijectif $t'_i = \frac{-t_i}{s}$. Alors :

$$\begin{aligned}\sum_{t_1+...+t_{l-1}=-s} \chi_1(t_1)...\chi_{l-1}(t_{l-1}) &= \chi_1...\chi_{l-1}(-s) \sum_{t'_1+...+t'_{l-1}=1} \chi_1(t'_1)...\chi_{l-1}(t'_{l-1}) \\ &= \chi_1...\chi_{l-1}(-s) J(\chi_1, ..., \chi_{l-1}).\end{aligned}$$

En rassemblant ces égalités, on obtient :
$J_0(\chi_1, ..., \chi_l) = \chi_1...\chi_{l-1}(-1) J(\chi_1, ..., \chi_{l-1}) \sum_{s\neq 0} \chi_1...\chi_l(s)$.
De plus, la Proposition 4.1.2 donne :
$\sum_{s\neq 0} \chi_1...\chi_l(s) = \begin{cases} 0 \text{ si } \chi_1...\chi_l \neq \epsilon \\ p-1 \text{ sinon} \end{cases}$
De plus, dans le deuxième cas, puisque $\chi_1...\chi_l = \epsilon$ et $\forall \chi \in \mathcal{X}_p, \chi(-1) = \pm 1$, on a $\chi_l(-1) = \chi_1...\chi_{l-1}(-1)$.
On obtient donc le résultat attendu.

□

Théorème 4.5.3. *Supposons que $\chi_1, ..., \chi_r$ sont non triviaux et que $\chi_1...\chi_r$ est non trivial. Alors $g(\chi_1)...g(\chi_r) = J(\chi_1, ..., \chi_r) g(\chi_1...\chi_r)$.*

Démonstration. Par définition : $g(\chi) = \sum_t \chi(t)\xi^t$.
Donc :

$$\begin{aligned}g(\chi_1)...g(\chi_r) &= \left(\sum_{t_1} \chi_1(t_1)\xi^{t_1} \right) ... \left(\sum_{t_r} \chi_r(t_r)\xi^{t_r} \right) \\ &= \sum_s \left(\sum_{t_1+...+t_r=s} \chi_1(t_1)...\chi_r(t_r) \right) \xi^s.\end{aligned}$$

Si $s = 0$, on reconnaît $J_0(\chi_1, ..., \chi_r)$, et puisque $\chi_1...\chi_r$ est non trivial, on a d'après le point c) de la Proposition 4.5.2, $\sum_{t_1+...+t_r=0} \chi_1(t_1)...\chi_r(t_r) = 0$.

Si $s \neq 0$, on effectue le changement de variables bijectif $t'_i = s^{-1}t_i$.
Alors : $\sum_{t_1+...+t_r=s} \chi_1(t_1)...\chi_r(t_r) = \chi_1...\chi_r(s) J(\chi_1, ..., \chi_r)$.
En réunissant ces égalités, on trouve :

$$\begin{aligned}g(\chi_1)...g(\chi_r) &= J(\chi_1, ..., \chi_r) \sum_{s\neq 0} \chi_1...\chi_r(s)\xi^s \\ &= J(\chi_1, ..., \chi_r) \sum_s \chi_1...\chi_r(s)\xi^s \text{ car } \chi_1...\chi_r \text{ est non trivial donc } \chi_1...\chi_r(0) = 0 \\ &= J(\chi_1, ..., \chi_r) g(\chi_1...\chi_r).\end{aligned}$$

□

Corollaire 4.5.4. *Supposons que $\chi_1, ..., \chi_r$ sont non triviaux et que $\chi_1...\chi_r = \epsilon$.*
Alors $g(\chi_1)...g(\chi_r) = \chi_r(-1)pJ(\chi_1, ..., \chi_{r-1})$.

Démonstration. Puisque $\chi_1, ..., \chi_r$ sont non triviaux et $\chi_1...\chi_r = \epsilon$, on a $\chi_1...\chi_{r-1} \neq \epsilon$.
Donc on peut appliquer le théorème précédent à $\chi_1, ..., \chi_{r-1}$:
$g(\chi_1)...g(\chi_{r-1}) = J(\chi_1, ..., \chi_{r-1})g(\chi_1...\chi_{r-1})$.
En multipliant de chaque côté par $g(\chi_r)$, on obtient :

$$\begin{aligned} g(\chi_1)...g(\chi_r) &= J(\chi_1, ..., \chi_{r-1})g(\chi_1...\chi_{r-1})g(\chi_r) \\ &= J(\chi_1, ..., \chi_{r-1})g(\chi_r^{-1})g(\chi_r) \\ &= \chi_r(-1)pJ(\chi_1, ..., \chi_{r-1}) \text{ d'après la remarque qui suit la Proposition 4.2.3.} \end{aligned}$$

□

Corollaire 4.5.5. *Supposons que $\chi_1, ..., \chi_r$ sont non triviaux et que $\chi_1...\chi_r = \epsilon$.*
Alors, $J(\chi_1, ..., \chi_r) = -\chi_r(-1)J(\chi_1, ..., \chi_{r-1})$.
(où on pose la convention : si $r = 2$, on prend $J(\chi_1) = 1$).

Démonstration. Si $r = 2$, il s'agit du point c) du Théorème 4.3.2.
Supposons r>2.

$$\begin{aligned} g(\chi_1)...g(\chi_r) &= \sum_s \left(\sum_{t_1+...+t_r=s} \chi_1(t_1)...\chi_r(t_r) \right) \xi^s \\ &= \sum_{t_1+...+t_r=0} \chi_1(t_1)...\chi_r(t_r) + \sum_{s\neq 0} \left(\sum_{t_1+...+t_r=s} \chi_1(t_1)...\chi_r(t_r) \right) \xi^s \\ &= J_0(\chi_1, ..., \chi_r) + J(\chi_1, ..., \chi_r) \sum_{s\neq 0} \xi^s. \end{aligned}$$

Puisque $\sum_{s=0}^{p-1} \xi^s = 0$ (somme géométrique), $\sum_{s=1}^{p-1} \xi^s = -1$.
Par le point c) de la Proposition 4.5.2, puisque $\chi_1...\chi_r = \epsilon$, on a $J_0(\chi_1, ..., \chi_r) = \chi_r(-1)(p-1)J(\chi_1, ..., \chi_{r-1})$.
De plus, par le Corollaire 4.5.4, $g(\chi_1)...g(\chi_r) = \chi_r(-1)pJ(\chi_1, ..., \chi_{r-1})$.
En réunissant toutes ces égalités, on trouve :

$$\begin{aligned} \chi_r(-1)pJ(\chi_1, ..., \chi_{r-1}) &= J_0(\chi_1, ..., \chi_r) - J(\chi_1, ..., \chi_r) \\ -J(\chi_1, ..., \chi_r) &= \chi_r(-1)pJ(\chi_1, ..., \chi_{r-1}) - \chi_r(-1)(p-1)J(\chi_1, ..., \chi_{r-1}) \\ J(\chi_1, ..., \chi_r) &= -J(\chi_1, ..., \chi_{r-1})\chi_r(-1)(p-(p-1)) \\ J(\chi_1, ..., \chi_r) &= -\chi_r(-1)J(\chi_1, ..., \chi_{r-1}). \end{aligned}$$

□

Théorème 4.5.6. *Supposons que $\chi_1, ..., \chi_r$ sont non triviaux.*
a) Si $\chi_1...\chi_r \neq \epsilon$, alors $|J(\chi_1, ..., \chi_r)| = p^{\frac{r-1}{2}}$.
b) Si $\chi_1...\chi_r = \epsilon$, alors

$$|J_0(\chi_1, ..., \chi_r)| = (p-1)p^{\frac{r}{2}-1}$$
$$\text{et } |J(\chi_1, ..., \chi_r)| = p^{\frac{r}{2}-1}.$$

Démonstration. On rappelle que d'après la Proposition 4.2.3, si $\chi \neq \epsilon$, alors $|g(\chi)| = \sqrt{p}$.
a) D'après le Théorème 4.5.3, puisque $\chi_1, ..., \chi_r$ sont non triviaux et $\chi_1...\chi_r \neq \epsilon$, $g(\chi_1)...g(\chi_r) = J(\chi_1, ..., \chi_r)g(\chi_1...\chi_r)$.
Et donc, d'après le rappel qu'on vient de faire, on obtient directement que $|J(\chi_1, ..., \chi_r)| = p^{\frac{r-1}{2}}$

b) D'après le point c) de la Proposition 4.5.2, puisque $\chi_1...\chi_r = \epsilon$, on a $J_0(\chi_1, ..., \chi_r) = \chi_r(-1)(p-1)J(\chi_1, ..., \chi_{r-1})$.
Or, $\chi(-1)^2 = \chi((-1)^2) = 1$, donc $|\chi(-1)| = 1$.
De plus, $\chi_1, ..., \chi_r$ sont non triviaux et $\chi_1...\chi_r = \epsilon$, donc $\chi_1...\chi_{r-1} \neq \epsilon$.
On applique donc le point a) à $\chi_1, ..., \chi_{r-1}$.
On trouve alors $|J(\chi_1, ..., \chi_{r-1})| = p^{\frac{(r-1)-1}{2}} = p^{\frac{r}{2}-1}$.
Finalement, $|J_0(\chi_1, ..., \chi_r)| = (p-1)p^{\frac{r}{2}-1}$.

D'après le corollaire 4.5.5, $J(\chi_1, ..., \chi_r) = -\chi_r(-1)J(\chi_1, ..., \chi_{r-1})$.
On a vu précédemment que $|\chi_r(-1)| = 1$.
Et, $\chi_1, ..., \chi_r$ sont non triviaux et $\chi_1...\chi_r = \epsilon$, donc $\chi_1...\chi_{r-1} \neq \epsilon$.
On applique le point a) à $\chi_1, ..., \chi_{r-1}$.
On trouve $|J(\chi_1, ..., \chi_r)| = p^{\frac{(r-1)-1}{2}} = p^{\frac{r}{2}-1}$.

□

Nous terminons cette section par 2 applications des sommes de Gauss et de Jacobi.

4.6 Nombre de points sur la sphère de $\mathbb{F}_p{}^r$

En 4.4, on avait cherché le nombre de solutions de l'équation $x^n + y^n = 1$ dans le corps $\mathbb{F}_p$. Il est naturel de se poser la même question à propos de l'équation $x_1^2 + ... + x_r^2 = 1$ sur $\mathbb{F}_p{}^r$.

Proposition 4.6.1.
Si r est impair, alors $N(x_1^2 + ... + x_r^2 = 1) = p^{r-1} + (-1)^{(\frac{r-1}{2})(\frac{p-1}{2})}p^{\frac{r-1}{2}}$.
Si r est pair, alors $N(x_1^2 + ... + x_r^2 = 1) = p^{r-1} - (-1)^{\frac{r}{2}\frac{p-1}{2}}p^{\frac{r}{2}-1}$.

Démonstration. On sait que $N(x_1^2 + ... + x_r^2 = 1) = \sum_{a_1+...+a_r=1} N(x_1^2 = a_1)...N(x_r^2 = a_r)$.
Soit χ le caractère d'ordre 2 (le symbole de Legendre).
Alors, par définition de χ, on a, dans le corps $\mathbb{F}_p$, $N(x^2 = a) = 1 + \chi(a)$.
Donc, $N(x_1^2 + ... + x_r^2 = 1) = \sum_{a_1+...+a_r=1} (1 + \chi(a_1))...(1 + \chi(a_r))$.
En développant et en utilisant la Proposition 4.5.2, tous les produits qui n'ont pas soit que les 1, soit que les $\chi(a_i)$ sont nuls, et on trouve :
$N(x_1^2 + ... + x_r^2 = 1) = p^{r-1} + J(\underbrace{\chi, ..., \chi}_{r \text{ termes}})$.
Puisque χ est le caractère d'ordre 2, si r est impair, $\chi^r = \chi$, et si r est pair, $\chi^r = \epsilon$.

Supposons tout d'abord que r est impair.
Alors, on applique le Théorème 4.5.3, qui donne :
$g(\chi)^r = J(\chi, ..., \chi)g(\chi)$.
D'après la Proposition 4.2.3, puisque $\chi \neq \epsilon$, $g(\chi) \neq 0$, donc $g(\chi)^{r-1} = J(\chi, ..., \chi)$.
Or, d'après le Corollaire 4.5.4, $g(\chi)^2 = \chi(-1)p$.
Et puisque r est impair, $r-1$ est pair.
On peut donc écrire : $J(\chi, ..., \chi) = \chi(-1)^{\frac{r-1}{2}}p^{\frac{r-1}{2}}$. (*)

Supposons maintenant que r est pair.

On applique le Corollaire 4.5.5, et on trouve $J(\underset{r \text{ termes}}{\chi,...,\chi}) = -\chi(-1)J(\underset{r-1 \text{ termes}}{\chi,...,\chi})$.
Puisque $r-1$ est impair, on peut appliquer ce qu'on a fait avant au termes de droite, et on trouve :

$$\begin{aligned} J(\underset{r \text{ termes}}{\chi,...,\chi}) &= -\chi(-1)\chi(-1)^{\frac{r-2}{2}}p^{\frac{r-2}{2}} \\ &= -\chi(-1)^{\frac{r}{2}}p^{\frac{r-2}{2}}. \end{aligned}$$

Pour finir, on avait vu dans le Corollaire 1.1.3 que $\chi(-1) = (-1)^{\frac{p-1}{2}}$.

□

Les équations les plus générales qui peuvent être traitées avec la même méthode sont de la forme $a_1x^{l_1} + a_2x^{l_2} + ... + a_rx^{l_r} = b$, où $a_1, ..., a_r$ et b sont dans $\mathbb{F}_p$, et $l_1, ..., l_r$ sont des entiers positifs.

Nous allons maintenant utiliser les sommes de Jacobi pour donner une nouvelle preuve de la loi de réciprocité quadratique.

4.7 Seconde preuve de la loi de réciprocité quadratique

Soit q un nombre premier impair distinct de p, et χ le caractère d'ordre 2 sur $\mathbb{F}_p^*$ (symbole de Legendre).
Par le Corollaire 4.5.4, $g(\chi)^{q+1} = (-1)^{\frac{p-1}{2}}pJ(\underset{q \text{ termes}}{\chi,...,\chi})$. (∗)
Puisque $q+1$ est pair,

$$\begin{aligned} g(\chi)^{q+1} &= (g(\chi)^2)^{\frac{q+1}{2}} \\ &= ((-1)^{\frac{p-1}{2}\frac{q+1}{2}})p^{\frac{q+1}{2}} \text{ par la Proposition 4.6.1} \end{aligned}$$

Par la formule (*), on trouve :
$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}} = J(\chi,...,\chi)$
Maintenant, $J(\chi,...,\chi) = \sum_{t_1+...+t_q=1} \chi(t_1)...\chi(t_q)$.
Si $t = t_1 = ... = t_q$, alors $t = q^{-1}$ et ce terme de la somme vaut $\chi(q^{-1})^q = \chi(q)^{-q} = \chi(q)$ car χ d'ordre 2 et q est impair.
On remarque que les termes de la somme sont invariants par permutation par un q-cycle. Donc si les t_i ne sont pas tous égaux, on sait qu'on va obtenir q q-uplets différents $(t_1, ..., t_q)$ tels que leurs termes correspondant dans la somme soient identiques.
Ainsi, on a la congruence $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}} \equiv \chi(q)\ mod(q)$.
Puisque $\chi(q) = (\frac{q}{p})$ et $p^{\frac{q-1}{2}} \equiv (\frac{p}{q})\ mod(q)$ par le critère d'Euler, on a :
$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}(\frac{p}{q}) \equiv (\frac{q}{p})\ mod(q)$.
Et puisque c'est une congruence dans $\mathbb{Z}$ entre nombres valant ± 1 et que $q \geq 3$, on trouve :
$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}(\frac{p}{q}) = (\frac{q}{p})$.

5 La loi de réciprocité biquadratique

5.1 Préliminaires

Dans toute la suite, D désignera l'anneau $\mathbb{Z}[i]$ des entiers de Gauss.
On rappelle que D est un anneau euclidien.
Donc, si, dans D, π est irréductible et π divise $\alpha\beta$, alors π divise α ou π divise β.
En particulier, on peut définir un pgcd sur cet anneau, que l'on notera *pgcd* dans la suite.

On a aussi que D est factoriel, donc on a l'existence et l'unicité (à inversible près) de la décomposition de tout élément non nul de D en produit d'irréductibles.

On définit une fonction N sur D à valeurs dans $\mathbb{N}$, qui à π dans D associe $N(\pi) = \pi\overline{\pi}$. On remarque que N peut être définie sur $\mathbb{C}$, mais alors elle est à valeurs dans $\mathbb{R}^+$.
On va surtout s'intéresser à la fonction N restreinte à D. Elle possède plusieurs propriétés intéressantes :
Elle est multiplicative :
pour tous λ, π dans D, $N(\lambda\pi) = N(\lambda)N(\pi)$.
Si $\pi \in D, N(\pi) = 1$ si, et seulement si, π est inversible. En particulier, les inversibles de D sont 1, -1, i et $-i$.
$N(\pi) = 2$ si, et seulement si, $(\pi) = (1 + i)$.

5.2 Les irréductibles de $\mathbb{Z}[i]$

Lemme 5.2.1. *Si π est irréductible dans D, alors il existe p entier premier positif tel que π divise p. De plus, si $(\pi) \neq (p)$, alors N(π)=$\pi\overline{\pi}$=p et $p = 2$ ou $p \equiv 1$ mod(4).*

Démonstration. On a $N(\pi) = \pi\overline{\pi}$ par définition.
Mais N est à valeurs dans $\mathbb{N}$, donc on peut écrire $N(\pi) \neq 0$ et 1 car π n'est pas inversible. comme un produits de facteurs premiers.
Ainsi, il existe $(p_i)_i$ des entiers premiers de $\mathbb{N}$ tels que $N(\pi) = p_1...p_r$.
Alors, $\pi\overline{\pi} = p_1...p_r$.
Et puisque D est euclidien, on en déduit qu'il existe $1 \leq i \leq r$ tel que π divise p_i.
Si π divise p, $N(\pi)$ divise p^2. Or, si $(\pi) \neq (p)$, $N(\pi) \neq N(p) = p^2$. Puisque π est non inversible, on a forcément $N(\pi) = p$.
Ecrivons $\pi = a + ib, a, b \in \mathbb{Z}$. On réécrit $N(\pi) = a^2 + b^2 = p$.
Donc forcément $p = 2$ ou $p \equiv 1$ $mod(4)$. □

Lemme 5.2.2. *Si $\alpha \in D$ et $N(\alpha)$ est premier, alors α est irréductible.*

Démonstration. Comme $N(\alpha) \neq 1$, α n'est pas inversible dans D Si $\alpha = \mu\lambda$, alors par multiplicativité de N, $N(\alpha) = N(\mu)N(\lambda)$.
Puisque $N(\alpha)$ est premier, on a alors $N(\mu) = 1$ ou $N(\lambda) = 1$.
Et donc soit λ, soit μ est inversible.
On conclut que α est irréductible. □

Lemme 5.2.3. *$1+i$ est irréductible, associé à $1-i$, et $2 = -i(1+i)^2$ est la factorisation en irréductibles de 2 dans D.*

Démonstration. $(1 + i) \in D$ et $N(1 + i) = 2$, donc par le lemme précédent, $1 + i$ est irréductible, et $-i(1 + i) = 1 - i$.
Et par un calcul rapide, $-i(1+i)^2 = 2$, $-i$ est inversible et $1+i$ est irréductible d'après ce qu'on vient de faire.

□

Lemme 5.2.4. *Soit q un entier premier positif dans $\mathbb{Z}$.*
Si $q \equiv 3$ mod(4) alors q est un irréductible de D.

Démonstration. Supposons que q n'est pas irréductible.
Alors, $q = \alpha\beta$ avec $N(\alpha) > 1$ et $N(\beta) > 1$.
En passant à la norme des deux côtés de l'égalité, on trouve $N(q) = N(\alpha)N(\beta)$, donc $q^2 = N(\alpha)N(\beta)$.
Puisque q est premier, $N(\alpha) > 1$ et $N(\beta) > 1$, on a $N(\alpha) = q$ et $N(\beta) = q$.
On écrit $\alpha = a + ib$, avec $a, b \in \mathbb{Z}$.
Alors, $q = a^2 + b^2$.

C'est une contradiction puisque la somme de deux carrés dans $\mathbb{Z}$ est toujours congrue à 0, 1 ou 2 modulo 4.
On conclut par l'absurde que q est irréductible dans D.

□

Lemme 5.2.5. *Soit p un premier positif dans $\mathbb{Z}$.*
Si $p \equiv 1\ mod(4)$, alors il existe un irréductible π de D tel que $p = \pi\overline{\pi}$.
De plus, $(\pi) \neq (\overline{\pi})$.

Démonstration. Par la Proposition 4.3.4, puisque $p \equiv 1\ mod(4)$, il existe des entiers a et b tels que $p = a^2 + b^2$. On pose alors $\pi = a + ib$, et on obtient $\pi\overline{\pi} = p$.
Supposons que $(\pi) = (\overline{\pi})$.
Alors, π et $\overline{\pi}$ sont associés, c'est-à-dire qu'il existe u inversible de D tel que $\pi = u\overline{\pi}$.
u vaut donc $1, -1, i$ ou $-i$.
Si $u = 1$ (respectivement -1), alors π est un réel (respectivement un imaginaire pur), ce qui contredit p=$\pi\overline{\pi}$.
Et si u vaut i ou $-i$, on trouve alors $|a| = |b|$.
L'irréductibilité de π force $|a| = |b| = 1$.
Mais dans ce cas, p=2, ce qui est absurde puisque $p \equiv 1\ mod(4)$. □

Théorème 5.2.6. *Les irréductibles de D.*
Les irréductibles de D sont :
les 4 éléments de norme 2, $\pm 1 \pm i$, tous associés.
si $p \equiv 1\ mod(4)$ est entier premier positif, les 8 éléments de D de norme p, formant 2 classes d'association.
si $p \equiv 3\ mod(4)$ est entier premier positif, $\pm p$ et $\pm ip$.

Démonstration. Les éléments de norme 2 sont exactement $\pm 1 \pm i$, donc par le Lemme 5.2.2, ce sont des éléments irréductibles de D.
Soit $p \equiv 1\ mod(4)$ un entier premier positif.
Par le Lemme 5.2.5, il existe un irréductible π tel que $p = \pi\overline{\pi}$, $\overline{\pi}$ est irréductible et π et $\overline{\pi}$ ne sont pas associés. En multipliant π et $\overline{\pi}$ par les 4 inversibles de D, on trouve 8 éléments distincts et irréductibles. Le fait que ce soient les 8 seuls vient du fait que D est factoriel.
Soit $p \equiv 3\ mod(4)$ un entier premier positif.
Par le Lemme 5.2.4, p est irréductible et donc $-p, ip$ et $-ip$ le sont.

Soit maintenant π irréductible dans D.
Par le Lemme 5.2.1, il existe un entier premier positif p tel que π divise p. Soit un tel p.
Si $(\pi) \neq (p)$, on a par le Lemme 5.2.1, $N(\pi) = p$ et $p = 2$ ou $p \equiv 1\ mod(4)$.
Si $p = 2$, on retrouve $\pm 1 \pm i$ et si $p \equiv 1\ mod(4)$, on retrouve un élément du deuxième point du Théorème.
Et, si $(\pi) = (p)$, π vaut p, $-p$, ip ou $-ip$.
Alors, on a forcément $p \neq 2$ car 2 n'est pas irréductible et p n'est pas congru à 1 modulo 4 car, par le Lemme 5.2.5, un tel élément n'est pas irréductible.
Puisque p est premier positif, il ne reste plus que $p \equiv 3\ mod(4)$.
On retrouve alors un élément du troisième point du Théorème. □

Définition 5.2.7. Soit $\alpha \in D$, non inversible.
On dit que α est **primaire** si $\alpha \equiv 1\ mod((1+i)^3)$.

Lemme 5.2.8. *Soit $\alpha = a + ib$ un élément non inversible de D, $a, b \in \mathbb{Z}$.*
α est primaire si, et seulement si, ($a \equiv 1\ mod(4)$ et $b \equiv 0\ mod(4)$), ou ($a \equiv 3\ mod(4)$ et $b \equiv 2\ mod(4)$).

Démonstration. Puisque $(1+i)^3 = -2+2i$, montrer que α est primaire est équivalent à montrer que $\frac{\alpha-1}{-2+2i}$ est dans D.
Or :

$$\begin{aligned}\frac{\alpha-1}{-2+2i} &= \frac{a+ib-1}{-2+2i} \\ &= \frac{(a-1+bi)(-2-2i)}{(-2+2i)(-2-2i)} \\ &= \frac{-2a+2-2ib-2ia+2i+2b}{8} \\ &= \frac{-a+b+1}{4} + \frac{-b-a+1}{4}i\end{aligned}$$

Ainsi, α est primaire si, et seulement si , $\frac{-a+b+1}{4}$ et $\frac{-b-a+1}{4}$ sont dans $\mathbb{Z}$.
si, et seulement si, $a-b \equiv 1\ mod(4)$ et $a+b \equiv 1\ mod(4)$;
si, et seulement si, $2a \equiv 2\ mod(4)$ et $a-b \equiv 1\ mod(4)$;
si, et seulement si, $a \equiv 1\ mod(4)$ et $b \equiv 0\ mod(4)$, ou $a \equiv 3\ mod(4)$ et $b \equiv 2\ mod(4)$.

□

Lemme 5.2.9. *Soit $\alpha = a+ib$ un élément de D, $a, b \in \mathbb{Z}$.*
$1+i$ divise α dans D si, et seulement si, a et b ont même parité.

Démonstration. Supposons que $1+i$ divise α dans D.
Alors, par multiplicativité de N, puisque $N(1+i)=2$ et N à valeurs dans $\mathbb{N}$, $N(\alpha)$ est pair.
Or, $N(\alpha) = a^2+b^2$, donc on a forcément a^2 et b^2 de même parité.
Mais un nombre et son carré ont même parité.
On conclut donc que a et b ont même parité.

Supposons que a et b ont même parité.
On a alors que $a+b$ et $a-b$ sont pairs.
On écrit alors :

$$\begin{aligned}\frac{a+ib}{1+i} &= \frac{(a+ib)(1-i)}{(1+i)(1-i)} \\ &= \frac{a-ia+ib+b}{2} \\ &= \frac{a+b}{2} + i\frac{b-a}{2}\end{aligned}$$

Et puisque $a+b$ et $b-a$ sont pairs, on obtient que $\frac{a+ib}{1+i} \in D$, donc $1+i$ divise α. □

Lemme 5.2.10.
a) Tout non inversible $\alpha \equiv 1\ mod(4)$ dans D est primaire.
b) Si α est primaire, alors $1+i$ ne divise pas α dans D.
c) Si q est un entier premier positif tel que $q \equiv 3\ mod(4)$, alors $-q$ est primaire irréductible.

Démonstration.
a) Soit α non inversible dans D tel que $\alpha \equiv 1 mod(4)$ dans D.
Alors, il existe d dans D tel que $\alpha = 1+4d$. Soit un tel élément d.
On a $4 = -(1+i)^4$. On pose $d' = -(1+i)d$.
$d' \in D$ car $d \in D$, $-(1+i) \in D$ et D est un anneau.

De plus, $\alpha = 1 + d'(1+i)^3$, donc $\alpha \equiv 1 mod((1+i)^3)$, et, par hypothèse, α est non inversible.
On en conclut que α est primaire.

b) Soit $\alpha = a + ib$ un élément primaire de D, $a, b \in \mathbb{Z}$.
D'après les congruences du Lemme 5.2.8, a et b n'ont pas la même parité, donc par une contraposée du Lemme 5.2.9, $1 + i$ ne divise pas α.

c) Soit q entier premier positif tel que $q \equiv 3\ mod(4)$.
Par le Lemme 5.2.4, q est un élément irréductible de D donc $-q$ aussi.
Puisque $q \equiv 3\ mod(4)$, $-q \equiv 1 mod(4)$. De plus, $-q$ est dans D et $-q$, comme q, est non inversible, donc, par le point a), $-q$ est primaire.
On conclut donc que $-q$ est primaire irréductible dans D.

□

Lemme 5.2.11.
Soit α un élément non inversible de D, tel que $1 + i$ ne divise pas α.
Alors, il existe un unique inversible u de D tel que $u\alpha$ est primaire.

Démonstration.
Existence :
On écrit $\alpha = a + ib$ où $a, b \in \mathbb{Z}$. D'après le Lemme 5.2.8, a et b n'ont pas la même parité. Et donc, il existe v inversible de D tel que $v\alpha = a' + ib'$ avec a' impair et b' pair.
Et, en multipliant si nécessaire par -1 pour obtenir les congruences du Lemme 5.2.8, on conclut qu'il existe u dans D tel que $u\alpha$ est primaire.

Unicité :
Soient u_1 et u_2 deux inversibles de D tels que $u_1\alpha$ et $u_2\alpha$ sont primaires.
Puisque $1 + i$ ne divise pas α, et D est euclidien donc factoriel, $u_1 \equiv u_2 mod((1+i)^3)$ ou encore $u_1 - u_2 \equiv 0 mod((1+i)^3)$.
On écrit $u_1 - u_2 = d(1+i)^3$, avec $d \in D$. En appliquant la norme de chaque côté de cette égalité, on trouve $N(u_1 - u_2) = 8N(d)$.
Or, $N(u_1 - u_2) \leq 4$ car u_1 et u_2 sont des éléments de $\{1, -1, i, -i\}$.
De plus, $N(d) \in \mathbb{N}$, donc on a forcément $N(d) = 0$, et donc $d = 0$.
On conclut ainsi que $u_1 = u_2$.

□

Lemme 5.2.12.
Tout élément primaire peut s'écrire comme le produit d'éléments primaires irréductibles.

Démonstration.
Soit $\alpha \in D$ primaire.
D est euclidien donc $\alpha \neq 0$ non inversible admet une décomposition en irréductibles et inversible dans D.
On écrit donc $\alpha = u\pi_1 ... \pi_r$ avec u inversible et $\pi_1, ..., \pi_r$ irréductibles non inversibles.
Or, les π_i sont irréductibles non inversibles et $1 + i$ ne divise pas α, donc il ne divise pas les π_i.
Donc d'après le Lemme 5.2.11, pour tout $1 \leq i \leq r$, il existe un inversible u_i tel que $u_i\pi_i$ est primaire.
Soient de tels éléments, et notons pour tout $1 \leq i \leq r, \pi'_i = u_i\pi_i$.
Alors, les π'_i sont tous irréductibles primaires et $\alpha = v\pi'_1 ... \pi'_r$, avec $v = uu_1^{-1} ... u_r^{-1}$ inversible de D.
Il ne reste plus qu'à montrer que $v = 1$ pour conclure.
En passant à la congruence modulo $(1+i)^3$ dans la dernière égalité obtenue, et on obtient $1 \equiv v\ mod((1+i)^3)$.

Par le même raisonnement avec la norme qu'à la fin du Lemme précédent, on conclut que $v = 1$.
On conclut que tout élément primaire de D s'écrit comme le produit de primaires irréductibles.

□

5.3 Le symbole résidu biquadratique

Soit π un irréductible de D. On se donne α et β des éléments de D.

Proposition 5.3.1.
L'anneau quotient $D/_{\pi D}$ est un corps fini avec $N(\pi)$ éléments.

Démonstration.
Pour commencer, puisque π est irréductible et D est principal, $D/_{\pi D}$ est un corps. Nous allons donc maintenant différencier deux cas, donnés par le Théorème 5.2.6.
a) Si $p = 2$ ou $p \equiv 1\ mod(4)$ est un entier premier positif tel que $p = \pi\overline{\pi}$:
Ecrivons $\pi = a + ib$, $a, b \in \mathbb{Z}$, a et $b \neq 0$.
Soit $\mu = m + in$ un élément de D, $m, n \in \mathbb{Z}$. Puisque $p = a^2 + b^2$, on a que p ne divise pas b. Donc il existe un entier c tel que $cb \equiv n\ mod(p)$.
Alors, $\mu - c\pi = m + in - ca - cib \equiv m - ca\ mod(p)$.
Donc $\mu \equiv m - ca\ mod(\pi)$.
On a donc que la classe de tout élément de D dans $D/_{\pi D}$ est celle d'un entier.
Autrement dit, on vient d'établir que le morphisme d'anneaux naturel f de $\mathbb{Z}$ dans $D/_{\pi D}$ qui à un k entier naturel associe la classe de k dans $D/_{\pi D}$ est surjectif.
Or, π divise p donc $f(p) = 0$ et $p\mathbb{Z} \subset ker(f)$. De plus, $p\mathbb{Z}$ est un idéal maximal et $f(1) = 1$, donc $p\mathbb{Z} = ker(f)$. Par le premier théorème d'isomorphisme, on obtient qu'il y a un isomorphime entre $\mathbb{F}_p$
On conclut que $D/_{\pi D}$ est un corps à $N(\pi) = p$ éléments.

b) Si $|\pi| = p$, où p entier premier positif congru à 3 modulo 4.
On pose, $L = \{a + ib$ tel que $0 \leq a < q$ et $0 \leq b < q\}$.
On va montrer que c'est un ensemble complet des représentants des classes de $D/_{\pi D}$.
On écrit $\mu = m + in, m, n \in \mathbb{Z}$ un élément de D.
On réalise les divisions euclidiennes de m et n par q dans $\mathbb{Z}$:
Il existe s_1, s_2, r_1 et r_2 dans $\mathbb{Z}$ tels que $0 \leq r_1 < q$, $0 \leq r_2 < q$, $m = s_1 + r_1$ et $n = s_2 + r_2$.
On a alors $\mu \equiv r_1 + ir_2\ mod(q)$. Ainsi, toute classe d'un élément de D est celle d'un élément de L.
Soient deux éléments de L, $a_1 + ib_1$ et $a_2 + ib_2$ avec $0 \leq a_1, a_2, b_1, b_2 < q$ tels que $a_1 + ib_1 \equiv a_2 + ib_2$ $mod(q)$.
Alors, $(a_1 - a_2) + i(b_1 - b_2) \equiv 0\ mod(q)$, donc q divise $a_1 - a_2$ et $b_1 - b_2$.
Or, $-q < a_1 - a_2 < q$, donc $a_1 - a_2 = 0$, et ainsi $a_1 = a_2$. De même, $b_1 = b_2$. Et L contient q^2 éléments.
On conclut que $D/_{\pi D}$ est un corps à $N(\pi) = q^2$ éléments.

□

Corollaire 5.3.2.
Soit $\alpha \in D$.
Si π ne divise pas α, alors $\alpha^{N(\pi)-1} \equiv 1\ mod(\pi)$.

Démonstration. Le groupe multiplicatif d'un corps à n éléments est constitué de $n - 1$ éléments.
Donc le groupe multiplicatif de $D/_{\pi D}$ contient $N(\pi) - 1$ éléments. De plus, par hypothèse, π ne divise pas α, donc la classe de α dans $D/_{\pi D}$ est dans le groupe multiplicatif de $D/_{\pi D}$.
Par Lagrange, on a donc que la classe de $\alpha^{N(\pi)-1}$ dans $D/_{\pi D}$ est celle de 1.

□

Lemme 5.3.3.
Si $(\pi) \neq (1 + i)$, on a $N(\pi) \equiv 1\ mod(4)$, et les classes de $1, -1, i$ et $-i$ sont distinctes dans $D/_{\pi D}$. Elles y forment le sous-groupe multiplicatif d'ordre 4.

Démonstration. :
Supposons $(\pi) \neq (1+i)$, c'est-à-dire $N(\pi) \neq 2$
Comme π non inversible, il vient $N(\pi) > 2$.
De plus, puisque π est irréductible et $N(\pi) \neq 2$, par le Théorème 5.2.6, on a soit $\pi = uq$ avec q entier premier positif, $q \equiv 3\ mod(4)$ et u inversible, donc $N(\pi) = q^2 \equiv 1\ mod(4)$, soit $N(\pi) = p$ avec p entier premier positif, $p \equiv 1\ mod(4)$.
Dans tous les cas, $N(\pi) \equiv 1\ mod(4)$, et donc $N(\pi) \geq 5$. Si on suppose maintenant que deux éléments u_1 et u_2 parmi $1, -1, i$ et $-i$ sont congrus modulo π, on a :
$u_1 - u_2 = d\pi$ avec $d \in D$. En appliquant la norme de chaque côté de l'égalité, puisque $N(u_1 - u_2) \leq 4$, on trouve $d = 0$ et donc $u_1 = u_2$.
Donc les classes de $1, -1, i$ et $-i$ dans $D/\pi D$ sont distinctes.

□

Proposition 5.3.4. *Si π ne divise pas α, et $(\pi) \neq (1+i)$, alors il existe un unique entier $0 \leq j \leq 3$ tel que $\alpha^{\frac{N(\pi)-1}{4}} \equiv i^j\ mod(\pi)$.*

Démonstration. Pour commencer, par le Lemme 5.3.3, on a $N(\pi) \equiv 1\ mod(4)$, donc $\frac{N(\pi)-1}{4}$ est un entier.
D'après le Corollaire 5.3.2, la classe de $\alpha^{\frac{N(\pi)-1}{4}}$ est racine du polynôme $X^4 - 1$ dans le corps $D/\pi D$.
Or, les seules racines de ce polynôme dans le corps $D/\pi D$ sont les 4 classes distinctes de $1, -1, i$ et $-i$, par le Lemme 5.3.3. □

Définition 5.3.5.
Soit π un irréductible de D, tel que $N(\pi) \neq 2$.
Si π ne divise pas α, on définit

$$\chi_\pi(\alpha) = i^j \text{ où } j \text{ est déterminé par la Proposition 5.3.4.}$$

C'est le *caractère biquadratique* de α.
Si π divise α, on prend $\chi_\pi(\alpha) = 0$.

Dans la suite, on suppose que $(\pi) \neq (1+i)$, c'est-à-dire $N(\pi) \neq 2$.

Proposition 5.3.6.
a) Il existe $\alpha \in D$ tel que π ne divise pas α et $\chi_\pi(\alpha) = i$.
b) Si π ne divise pas α, alors $\chi_\pi(\alpha) = 1$ si, et seulement si, $x^4 \equiv \alpha\ mod(\pi)$ a une solution dans D.
c) $\overline{\chi_\pi(\alpha\beta)} = \chi_\pi(\alpha)\chi_\pi(\beta)$.
d) $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$.
e) Si $\pi = a + ib$ $(a, b \in \mathbb{Z})$ est primaire irréductible, alors $\chi_\pi(-1) = (-1)^{\frac{a-1}{2}}$.
f) Si on a $\alpha \equiv \beta\ mod(\pi)$, alors $\chi_\pi(\alpha) = \chi_\pi(\beta)$.
g) Si $(\pi) = (\lambda)$, alors, $\chi_\pi(\alpha) = \chi_\lambda(\alpha)$.

Démonstration.
a) Puisque $(\pi) \neq (1+i)$, $N(\pi) \neq 2$ et donc $N(\pi) \equiv 1\ mod(4)$.
D'après la Proposition 5.3.1, $D/\pi D$ est un corps fini à $N(\pi)$ éléments, donc $(D/\pi D)^*$ est cyclique d'ordre $N(\pi) - 1$.
Soit g un de ses générateurs. On pose $g' = g^{\frac{N(\pi)-1}{4}}$ (possible car $N(\pi) - 1$ divisible par 4).
On rappelle que $(D/\pi D)^*$ est cyclique et 4 est un diviseur de $N(\pi) - 1$, donc il admet un unique sous-groupe d'ordre 4, et donc il contient tous les éléments d'ordre 4, les seuls étant ainsi les classes de i et $-i$.

Or, g' est d'ordre 4, donc, quitte à considérer g'^{-1}, on peut supposer que g' est la classe de i.
On prend donc $\alpha = g$, π ne divise pas α car g dans $(D/_{\pi D})^*$ et $\chi_\pi(\alpha) = i$.

b) Ce résultat suit de la Proposition 1.2.2.

c) Si π divise α ou β, alors il divise le produit $\alpha\beta$, donc $\chi_\pi(\alpha\beta) = \chi_\pi(\alpha)\chi_\pi(\beta) = 0$.
Si π ne divise ni α, ni β, alors le résultat vient de la multiplicativité des congruences.

d) $\chi_\pi(\alpha) = i^j$ avec j déterminé de manière unique par $\alpha^{\frac{N(\pi)-1}{4}} \equiv i^j mod(\pi)$.
$\overline{\chi_\pi(\alpha)} = (-i)^j = i^{3j}$.
Et puisque $\alpha^{\frac{N(\pi)-1}{4}} \equiv i^j mod(\pi), \overline{\alpha^{\frac{N(\pi)-1}{4}}} \equiv \overline{i^j} mod(\overline{\pi})$.
On obtient donc $\overline{\alpha}^{\frac{N(\pi)-1}{4}} \equiv i^{3j} mod(\overline{\pi})$.
Ainsi, $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$.

e) On écrit $\pi = a + ib$, donc $N(\pi) = a^2 + b^2$ et on va traiter les deux cas donnés par le Lemme 5.2.8.
Si $a \equiv 1\ mod(4)$ et $b \equiv 0\ mod(4)$, alors on écrit $a = 1 + 4k$, $k \in \mathbb{Z}$ et $b = 4k'$, $k' \in \mathbb{Z}$.
On a : $a^2 = (1+4k)^2 = 1 + 8k + 16k^2, b^2 = 16k'^2$.
Cela donne $a^2 - 1 \equiv 0\ mod(8)$ et $b^2 \equiv 0\ mod(8)$, donc $(-1)^{\frac{N(\pi)-1}{4}} = 1$. Et $(-1)^{\frac{a-1}{2}} = (-1)^{\frac{1+4k-1}{2}} = (-1)^{2k} = 1$.

Si $a \equiv 3\ mod(4)$ et $b \equiv 2\ mod(4)$, alors on écrit $a = 3 + 4k, k \in \mathbb{Z}$ et $b = 2 + 4k', k' \in \mathbb{Z}$.
On a : $a^2 = (3+4k)^2 = 9 + 24k + 16k^2, b^2 = (2+4k')^2 = 4 + 16k' + 16k'^2$
Cela donne $a^2 - 1 \equiv 0\ mod(8)$ et $b^2 \equiv 4\ mod(8)$, donc $(-1)^{\frac{N(\pi)-1}{4}} = -1$. Et $(-1)^{\frac{a-1}{2}} = (-1)^{\frac{3+4k-1}{2}} = (-1)^{1+2k} = -1$.

On a vérifié l'égalité dans les deux cas, on peut donc conclure que $\chi_\pi(-1) = (-1)^{\frac{a-1}{2}}$.

f) Clair par la définition de χ_π.

g) Supposons que $(\pi) = (\lambda)$.
Soit $\alpha \in D$.
Alors λ divise α et $\chi_\pi(\alpha) = \chi_\lambda(\alpha) = 0$.
Si π ne divise pas α :
Soit j tel que $\alpha^{\frac{N(\pi)-1}{4}} \equiv i^j\ mod(\pi)$.
Puisque $(\pi) = (\lambda)$, $\alpha^{\frac{N(\pi)-1}{4}} \equiv i^j\ mod(\lambda)$.
Donc $\chi_\pi(\alpha) = \chi_\lambda(\alpha)$.

□

Proposition 5.3.7.
Soit q un entier premier, $q \equiv 3\ mod(4)$.
Alors, pour tout a dans $\mathbb{Z}$ tel que q ne divise pas a, $\chi_q(a) = 1$.

Démonstration.
Soit a dans $\mathbb{Z}$ tel que q ne divise pas a. On a $N(q) = q^2$. Donc :

$$\begin{aligned}
\chi_q(a) &\equiv a^{\frac{q^2-1}{4}} mod(q) \text{ par définition} \\
&\equiv (a^{q-1})^{\frac{q+1}{4}} mod(q) \text{ car } q \equiv 3\ mod(4) \\
&\equiv 1^{\frac{q+1}{4}} mod(q) \text{ par le théorème de Fermat} \\
&\equiv 1\ mod(q).
\end{aligned}$$

□

On va maintenant généraliser le caractère biquadratique.

Définition 5.3.8.
Soit $\alpha \in D$ tel que $\alpha \neq 0$ et $1+i$ ne divise pas α et $\beta \in D$.
On écrit $\alpha = \prod_k \lambda_k$, avec λ_k irréductible pour tout k.
Si α et β sont premiers entre eux, on définit $\chi_\alpha(\beta)$ par

$$\chi_\alpha(\beta) = \prod_k \chi_{\lambda_k}(\beta).$$

Quelques justifications sont nécessaires :
Comme α et β sont premiers entre eux, on a, pour tout k, λ_k ne divise pas β. Et on a aussi, puisque $1+i$ ne divise pas α, $(\lambda_k) \neq (1+i)$.
La décomposition de α en produit d'irréductibles n'est unique qu'à inversibles près.
On sait que si on a deux décompositions en irréductibles de α, $\alpha = \prod_k \lambda_k = \prod_j \mu_j$, alors les deux familles (λ_k) et (μ_j) ont le même nombre d'éléments, et pour tout k, il existe un j tel que λ_k et μ_j sont associés.
Et donc, par le point g) de la Proposition 5.3.6, $\chi_{\lambda_k}(\beta) = \chi_{\mu_j}(\beta)$.
Donc la définition est bien posée.
Et on remarque, avec le point f) de la Proposition 5.3.6, si $\beta \equiv \alpha \ mod(\pi), \chi_\pi(\alpha) = \chi_\pi(\beta)$.

Proposition 5.3.9.
Soit $a \in \mathbb{Z}, a \neq 0$ et $b \in \mathbb{Z}$ impair non inversible.
Si $pgcd(a,b) = 1$, alors $\chi_b(a) = 1$.

Démonstration.
On peut supposer, sans perte de généralité, que $b > 0$.
On écrit $b = \prod_j p_j \prod_k q_k$, avec tous les p_j premiers positifs congrus 1 modulo 4 et tous les q_k premiers positifs congrus à 3 modulo 4.
2 ne peut pas être dans cette décomposition car, par hypothèse, b est impair.
Par la Proposition 5.3.7, il suffit de montrer que pour tout i, $\chi_{p_j}(a) = 1$.
Par le Lemme 5.2.5, pour tout j, il existe π_j irréductible tel que $p_j = \pi_j \overline{\pi_j}$.
Alors, pour tout j,

$$\begin{aligned}
\chi_{p_j}(a) &= \chi_{\pi_j}(a)\chi_{\overline{\pi_j}}(a) \text{ par définition} \\
&= \chi_{\pi_j}(a)\overline{\chi_{\pi_j}(a)} \text{ par le point d) de la Proposition5.3.6} \\
&= \chi_{\pi_j}(a)\chi_{\pi_j}(a)^{-1} \\
&= 1.
\end{aligned}$$

□

Lemme 5.3.10.
Pour tout $r \in \mathbb{N}^*$, pour tout $s_1, ..., s_r$ entiers tels que pour tout $1 \leq i \leq r$, $s_i \equiv 1 \ mod(4)$, on a $\frac{s_1 ... s_r - 1}{4} \equiv \sum_{i=1}^{r} \frac{s_i - 1}{4} mod(4)$.

Démonstration.
Par récurrence sur r :
L'hypothèse de récurrence à r fixé est : "pour tout $s_1, ..., s_r$ entiers tels que pour tout $1 \leq j \leq r$, $s_i \equiv 1 mod(4)$, on a $\frac{s_1...s_r-1}{4} \equiv \sum_{i=1}^{r} \frac{s_i-1}{4} mod(4)$".
Initialisation :
r=1 clair
r=2 : Soient s_1 et s_2 entiers tels que pour tout $1 \leq i \leq 2$, $s_i \equiv 1\ mod(4)$.
Alors, il existe k_1 et k_2 entiers tels que $s_1 = 1 + 4k_1$ et $s_2 = 1 + 4k_2$.
Alors $s_1 s_2 = (1 + 4k_1)(1 + 4k_2) = 1 + 4k_1 + 4k_2 + 16k_1k_2$.
Donc $\frac{s_1s_2-1}{4} = \frac{1+4k_1+4k_2+16k_1k_2-1}{4} = \frac{4k_1+4k_2}{4} + 4k_1k_2 = \frac{s_1-1+s_2-1}{4} + 4k_1k_2$.
Donc $\frac{s_1s_2-1}{4} \equiv \sum_{j=1}^{2} \frac{s_j-1}{4} mod(4)$.
Donc la proposition est vraie aux rangs 1 et 2.

Hérédité :
Soit $r \geq 2$. Supposons que l'hypothèse de récurrence est vérifiée jusqu'au rang r.
Soient $s_1, ..., s_{r+1}$ entiers tels que pour tout $1 \leq j \leq r+1$, $s_j \equiv 1\ mod(4)$
On pose $s' = s_1...s_r$. On a donc $s' \equiv 1\ mod(4)$.
Or, $s_1...s_{r+1} = s's_{r+1}$. Donc, par le cas r=2, on trouve $\frac{s's_{r+1}-1}{4} \equiv \frac{s'-1}{4} + \frac{s_{r+1}-1}{4}\ mod(4)$.
De plus, par hypothèse de récurrence, $\frac{s'-1}{4} \equiv \sum_{j=1}^{r} \frac{s_j-1}{4}\ mod(4)$.
On obtient donc $\frac{s_1...s_{r+1}-1}{4} \equiv \sum_{j=1}^{r+1} \frac{s_i-1}{4}\ mod(4)$.
Donc la proposition est vraie au rang $r+1$.

□

Proposition 5.3.11.
Soit $n \in \mathbb{Z}$, $n \neq 1$, tel que $n \equiv 1\ mod(4)$.
Alors, $\chi_n(i) = (-1)^{\frac{n-1}{4}}$.

Démonstration.
Comme n est impair, $1 + i$ ne divise pas n, donc $\chi_n(i)$ est bien défini. Si n est premier positif, alors on écrit grâce au Lemme 5.2.5, $n = \pi\overline{\pi}$.
On a alors :

$$\begin{aligned}\chi_p(i) &= \chi_\pi(i)\chi_{\overline{\pi}}(i) \text{ par définition} \\ &= (i^{\frac{p-1}{4}})^2 \\ &= (i^2)^{\frac{p-1}{4}} \\ &= (-1)^{\frac{p-1}{4}}.\end{aligned}$$

Si n est premier négatif, $n = -q$ avec $q \equiv 3\ mod(4)$ premier, irréductible par le Lemme 5.2.4, alors :

$$\begin{aligned}\chi_{-q}(i) &= i^{\frac{q^2-1}{4}} \text{ par définition} \\ &= (i^{q-1})^{\frac{q+1}{4}} \text{ car } q \equiv 3\ mod(4) \\ &= (-1)^{\frac{q+1}{4}} \text{ car } q - 1 \equiv 2\ mod(4) \\ &= (-1)^{\frac{-q-1}{4}} \\ &= (-1)^{\frac{n-1}{4}}.\end{aligned}$$

Si maintenant $n \equiv 1\ mod(4)$ est arbitraire, puisque $n \neq 1$, on peut décomposer n en produit de facteurs premiers. Puisque $n \equiv 1\ mod(4)$, n n'est pas pair donc 2 n'apparaît pas dans cette décomposition.
On peut donc écrire $n = p_1...p_t(-q_1)...(-q_r)$, avec pour tout j, $p_j \equiv 1\ mod(4)$ et $q_j \equiv 3\ mod(4)$ et tous les p_j et les q_j sont positifs.
Par ce qu'on vient de faire, on a pour tout j, $\chi_{p_j}(i) = (-1)^{\frac{p_j-1}{4}}$ et $\chi_{-q_j}(i) = (-1)^{\frac{-q_j-1}{4}}$.
Donc $\chi_n(i) = (-1)^{\sum_{j=1}^{r+t} \frac{s_j-1}{4}}$ avec $s_j = p_j$ si $j \leq t$ et $s_j = -q_{j-s}$ sinon.
Or, par le Lemme 5.3.10, $\sum_{j=1}^{r+t} \frac{s_j-1}{4} \equiv \frac{s_1...s_{r+t}-1}{4} mod(4)$.
Donc $(-1)^{\sum_{j=1}^{r+t} \frac{s_j-1}{4}} = (-1)^{\frac{s_1...s_{r+t}-1}{4}} = (-1)^{\frac{n-1}{4}}$.
On conclut que $\chi_n(i) = (-1)^{\frac{n-1}{4}}$.

□

Proposition 5.3.12. *Si $\pi = a + ib$ $(a, b \in \mathbb{Z})$ est primaire, alors $\chi_\pi(-1) = (-1)^{\frac{a-1}{2}}$.*
C'est une généralisation du point d) de la Proposition 5.3.6 *à tous les primaires.*

Démonstration. Si π est primaire irréductible, le point d) de la Proposition 5.3.6 donne le résultat.
On suppose dans la suite que π n'est pas irréductible.
Par le Lemme 5.2.12, π peut s'écrire comme produit de primaires irréductibles.
Soit $\pi = \prod_{j=1}^{n} \pi_j$, $n \geq 2$ une telle décomposition.
On écrit, pour tout $j \in \{1, ..., n\}$, $\pi_j = a_j + ib_j$.
On a, par définition de χ_π et par le point d) de la Proposition 5.3.6, $\chi_\pi(-1) = \prod_{j=1}^{n} (-1)^{\frac{a_j-1}{2}}$.
On aimerait montrer que ce produit est égal à $(-1)^{\frac{a-1}{2}}$.
On commence par écrire $\pi = (a_1 + ib_1)...(a_n + ib_n)$, où $a_j, b_j \in \mathbb{Z}$. On remarque que la partie réelle de π, c'est-à-dire a, est une somme de produits de n termes, chaque produit contenant un nombre pair de b_j. Or, puisque les π_j sont primaires, les congruences du Lemme 5.2.8 donnent que pour tout $j \neq k, b_j b_k \equiv 0\ mod(4)$.
Donc dans l'expression de a, seul le terme produit de tous les a_j n'est pas congru à 0 modulo 4, c'est lui qui détermine la congruence de a modulo 4.
On a ainsi, par opérations sur les congruences, que $a \equiv 1\ mod(4)$ si, et seulement si, il y a un nombre pair de a_j congrus à 3 modulo 4.
On écrit $\prod_{j=1}^{n} (-1)^{\frac{a_j-1}{2}} = \prod_{a_j \equiv 3\ mod(4)} (-1)^{\frac{a_j-1}{2}} \prod_{a_j \equiv 1\ mod(4)} (-1)^{\frac{a_j-1}{2}} = \prod_{a_j \equiv 3\ mod(4)} (-1)^{\frac{a_j-1}{2}}$
Si $a \equiv 1\ mod(4)$, il y a un nombre pair de a_j congrus à 3 modulo 4, donc $\prod_{a_j \equiv 3 mod(4)} (-1)^{\frac{a_j-1}{2}} = 1 = (-1)^{\frac{a-1}{2}}$.
Si $a \equiv 3\ mod(4)$, il y a un nombre impair de a_j congrus à 3 modulo 4, donc $\prod_{a_j \equiv 3 mod(4)} (-1)^{\frac{a_j-1}{2}} = -1 = (-1)^{\frac{a-1}{2}}$.

□

5.4 La loi de réciprocité biquadratique

La loi de réciprocité biquadratique peut être énoncée comme suit :

Théorème 5.4.1.
Soient λ et π deux éléments primaires de D premiers entre eux.

Alors, $\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{(\frac{N(\lambda)-1}{4})(\frac{N(\pi)-1}{4})}$.

Si $\pi = a + ib$ et $\lambda = c + id$ sont primaires où $a, b, c, d \in \mathbb{Z}$, on peut voir avec des calculs que $(\frac{N(\lambda)-1}{4})(\frac{N(\pi)-1}{4})$ et $(\frac{a-1}{2})(\frac{c-1}{2})$ ont la même parité, donc on peut réécrire l'égalité du Théorème :

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{(\frac{a-1}{2})(\frac{c-1}{2})}$$

On peut alors, avec le Lemme 5.2.8, différencier deux cas :
Si λ ou π est congru à 1 modulo 4, alors π et λ ont le même caractère biquadratique, $\chi_\pi(\lambda) = \chi_\lambda(\pi)$.
Si λ et π sont congrus à $3 + 2i$ modulo 4, alors π et λ ont des caractères "opposés", dans le sens $\chi_\pi(\lambda) = -\chi_\lambda(\pi)$.

On se donne dans ce qui suit π un primaire irréductible, avec $N(\pi) = p \equiv 1 mod(4)$ où p est premier, et soit χ_π son caractère biquadratique.
Alors, χ_π peut être vu comme un caractère multiplicatif sur le corps fini $D/\pi D$. On rappelle que ce corps est fini isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Définition 5.4.2.
Si $\xi = e^{\frac{2i\pi}{p}}$, on pose $g(\chi_\pi) = \sum_{j \in D/\pi D} \chi_\pi(j)\xi^j$, la somme de Gauss de χ_π.

Si $\Psi = \chi_\pi^2$, alors Ψ est le caractère non trivial, d'après le point a) de la Proposition 5.3.6, d'ordre 2 sur $D/\pi D \simeq \mathbb{Z}/p\mathbb{Z}$ c'est-à-dire le symbole de Legendre.

Proposition 5.4.3.
On a $J(\chi_\pi, \chi_\pi) = \chi_\pi(-1)J(\chi_\pi, \Psi)$.

Démonstration. Par le Théorème 4.3.2, puisque $\chi_\pi^2 = \Psi$ est non trivial, on a $J(\chi_\pi, \chi_\pi) = \frac{g(\chi_\pi)^2}{g(\Psi)} (\neq 0)$. Ainsi,

$$\begin{aligned} J(\chi_\pi)^2 &= \frac{g(\chi_\pi)^4}{g(\Psi)^2} \\ &= \frac{\chi_\pi(-1)pJ(\chi_\pi, \chi_\pi)J(\chi_\pi, {\chi_\pi}^2)}{g(\Psi)^2} \text{ par la Proposition 4.3.5} \\ &= \frac{\chi_\pi(-1)pJ(\chi_\pi, \chi_\pi)J(\chi_\pi, {\chi_\pi}^2)}{(-1)^{\frac{p-1}{2}}p} \text{ par la Proposition 3.0.8} \\ &= \chi_\pi(-1)J(\chi_\pi, \chi_\pi)J(\chi_\pi, \Psi) \text{ car } p \equiv 1 \ mod(4) \text{ et } {\chi_\pi}^2 = \Psi. \end{aligned}$$

Et, puisque χ_π et ${\chi_\pi}^2$ ne sont pas triviaux, $J(\chi_\pi, \chi_\pi) \neq 0$, et donc, en divisant des deux côtés de l'égalité par $J(\chi_\pi, \chi_\pi)$, on trouve :
$J(\chi_\pi, \chi_\pi) = \chi_\pi(-1)J(\chi_\pi, \Psi)$.

□

Proposition 5.4.4.
On a $g(\chi_\pi)^4 = pJ(\chi_\pi, \chi_\pi)^2$.

Démonstration.

$$\begin{aligned} g(\chi_\pi)^4 &= \chi_\pi(-1)pJ(\chi_\pi, \chi_\pi)J(\chi_\pi, {\chi_\pi}^2) \text{ par la Proposition 4.3.5} \\ &= J(\chi_\pi, \chi_\pi)^2 \text{ par la Proposition 5.4.3.} \end{aligned}$$

□

Lemme 5.4.5.
Tout inversible de D est congru à 1 modulo $1+i$.

Démonstration.
On a $-1 = 1 + (1-i)(1+i), i = 1 + i(1+i)$ et $-i = 1 - (1+i)$. □

Proposition 5.4.6. $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi)$ *est primaire.*

Démonstration.

$$\begin{aligned} J(\chi_\pi, \chi_\pi) &= \sum_{\substack{t+s=1 \\ t,s \in D/\pi D}} \chi_\pi(t)\,\chi_\pi(s) \text{ par définition} \\ &= \sum_{t=1}^{p} \chi_\pi(t)\,\chi_\pi(1-t) \\ &= 2\sum_{t=2}^{\frac{p-1}{2}} \chi_\pi(t)\,\chi_\pi(1-t) + \chi_\pi\left(\frac{p+1}{2}\right)^2 \text{ en regroupant les termes par symétrie.} \end{aligned}$$

Puisque $p \equiv 1\ mod(4)$, $p \equiv 1\ mod(2+2i)$.
De plus,

$$\begin{aligned} \chi_\pi\left(\frac{p+1}{2}\right)^2 &= \chi_\pi(2^{-1})^2 \\ &= \chi_\pi(2)^{-2} \\ &= \chi_\pi(2)^2 \text{ car } \chi_\pi \text{ d'ordre 4} \\ &= \chi_\pi(-i(1+i)^2)^2 \text{ car } 2 = -i(1+i)^2 \\ &= \chi_\pi(-i)^2\,\chi_\pi(1+i)^4 \text{ par multiplicativité} \\ &= \chi_\pi(-i)^2 \text{ car } \chi_\pi \text{ d'ordre 4} \\ &= \chi_\pi((-i)^2) \text{ par multiplicativité} \\ &= \chi_\pi(-1). \end{aligned}$$

De plus, chacun des termes de la somme est un produit d'inversibles donc est inversible, et par le Lemme 5.4.6, est congru à 1 modulo $1+i$. Donc la somme est congrue à son nombre de termes $(\frac{p-3}{2})$ modulo $1+i$, et en la multipliant par 2, elle est congrue à 2 fois son nombre de termes modulo $2+2i$. On obtient donc :

$$\begin{aligned} J(\chi_\pi, \chi_\pi) &\equiv 2\frac{p-3}{2} + \chi_\pi(-1)\ mod(2+2i) \\ &\equiv p - 3 + \chi_\pi(-1)\ mod(2+2i) \\ &\equiv -2 + \chi_\pi(-1)\ mod(2+2i) \text{ car } p \equiv 1\ mod(2+2i) \end{aligned}$$

$$\begin{aligned} \text{Et donc, } -\chi_\pi(-1)J(\chi_\pi, \chi_\pi) &\equiv 2\,\chi_\pi(-1) - \chi_\pi(-1)^2\ mod(2+2i) \\ &\equiv 2 - 1\ mod(2+2i) \text{ car } \chi_\pi(-1) \equiv 1\ mod(1+i) \text{ et } \chi_\pi(-1)^2 = \chi_\pi(1) = 1 \\ &\equiv 1\ mod(2+2i). \end{aligned}$$

Or, $2+2i = -(1+i)^3$, donc $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi) \equiv 1\ mod((1+i)^3)$.

□

Lemme 5.4.7.
Soient $k \in \mathbb{N}$ et p premier positif.
Si $p-1$ ne divise pas k, alors $1^k + ... + (p-1)^k \equiv 0\ mod(p)$.

Démonstration.
$\mathbb{F}_p^*$ est cyclique, on pose donc g un de ses générateurs. On remarque que $p \geq 3$, donc $g \neq 1$.
La classe dans $\mathbb{F}_p$ de $1^k + ... + (p-1)^k$ est $\sum_{i=0}^{p-2} g^{ik}$.
Et, $\sum_{i=0}^{p-2} g^{ik} = \frac{1-g^{k(p-1)}}{1-g}$ comme somme géométrique puisque $g \neq 1$.
Or, par Lagrange, $g^{k(p-1)} = 1$, donc $\sum_{i=0}^{p-2} g^{ik} = 0$.

□

Proposition 5.4.8. *On a $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi) = \pi$.*

Démonstration. D'après le Lemme 5.2.11, si on a un élément α de D qui n'est pas divisible par $1+i$, alors il existe un unique inversible u de D tel que $u\alpha$ est inversible.
π est irréductible par hypothèse donc en particulier, il n'est pas divisible par $1+i$. De plus, il est primaire par hypothèse et $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi)$ est primaire d'après la Proposition 5.4.6.
Il suffit donc de montrer que $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi)$ et π diffèrent multiplicativement d'un inversible.
$J(\chi_\pi, \chi_\pi) = \sum_{t=1}^{p-1} \chi_\pi(t)\,\chi_\pi(1-t)$
Donc $J(\chi_\pi, \chi_\pi) = \sum_{t=1}^{p-1} t^{\frac{p-1}{4}}(1-t)^{\frac{p-1}{4}} mod(\pi)$ car $N(\pi) = p$
Par le Lemme 5.4.7, on a donc $J(\chi_\pi, \chi_\pi) \equiv 0\ mod(\pi)$
Donc il existe v dans D tel que $J(\chi_\pi, \chi_\pi) = v\pi$. Soit un tel élément.
De plus, par le Corollaire 4.3.3, puisque χ_π et ${\chi_\pi}^2$ ne sont pas triviaux, $|J(\chi_\pi, \chi_\pi)| = \sqrt{p}$
Donc $N(J(\chi_\pi, \chi_\pi)) = |J(\chi_\pi, \chi_\pi)|^2 = p$ premier.
Donc par le Lemme 5.2.2, $J(\chi_\pi, \chi_\pi)$ est irréductible.
Et ce résultat donne que v est inversible.
On a donc $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi) = -\chi_\pi(-1)v\pi$. Et $-\chi_\pi(-1)v$ est inversible puisque c'est un produit d'éléments inversibles.

□

Proposition 5.4.9. *On a $g(\chi_\pi)^4 = \pi^3\overline{\pi}$.*

Démonstration.

$$\begin{aligned} g(\chi_\pi)^4 &= pJ(\chi_\pi, \chi_\pi)^2 \text{ par la Proposition 5.5.4} \\ &= p(-\chi_\pi(-1)\pi)^2 \text{ par la Proposition 5.4.8 et } \chi_\pi(-1)^{-1} = \chi_\pi(-1) \\ &= p\pi^2 \text{ car } \chi_\pi(-1)^2 = 1 \\ &= \pi^3\overline{\pi} \text{ car } p = \pi\overline{\pi}. \end{aligned}$$

□

Lemme 5.4.10.
Soit π dans D et $q \equiv 3 mod(4)$ un entier premier positif.
Alors, $\pi^q \equiv \overline{\pi}\ mod(q)$.

Démonstration.
Ecrivons $\pi = a + ib$, où $a, b \in \mathbb{Z}$

$$\begin{aligned}
\text{On a } \pi^q &= (a+ib)^q \\
&\equiv a^q + (ib)^q \ mod(q) \text{ par Frobenius} \\
&\equiv a^q - ib^q \ mod(q) \text{ car } q \equiv 3 \ mod(4) \\
&\equiv a - ib \ mod(q) \text{ par le théorème de Fermat} \\
&\equiv \overline{\pi} \ mod(q).
\end{aligned}$$

□

Nous allons maintenant prouver deux cas particuliers de la loi de réciprocité biquadratique qui nous serviront pour montrer le cas général.

Proposition 5.4.11.
Soit q un entier positif irréductible dans D.
Alors, $\chi_\pi(-q) = \chi_q(\pi)$.

Démonstration.
Puisque q est irréductible dans D, il l'est dans $\mathbb{Z}$ et est donc premier.
Donc, en utilisant les Lemmes 5.2.5, on a forcément $q \equiv 3 \ mod(4)$.
On a donc :

$$\begin{aligned}
g(\chi_\pi)^q &= (\sum_{j=1}^{p-1} \chi_\pi(j)\xi^j)^q \text{ par définition} \\
&\equiv \sum_{j=1}^{p-1} \chi_\pi(j)^q \xi^{qj} \ mod(q) \text{ par Frobenius dans } \mathbb{Z}[\xi, i] \\
&\equiv \sum_{j=1}^{p-1} \chi_\pi(j)^{-1} \xi^{qj} \ mod(q) \text{ car } \chi_\pi \text{ est d'ordre 4 et } q \equiv 3 \ mod(4) \\
&\equiv \sum_{j=1}^{p-1} \chi_\pi(q)\, \chi_\pi(q)^{-1}\, \chi_\pi(j)^{-1} \xi^{qj} \ mod(q) \\
&\equiv \chi_\pi(q) \sum_{j=1}^{p-1} \chi_\pi(qj)^{-1} \xi^{qj} \ mod(q) \\
&\equiv \chi_\pi(q) \sum_{j'=1}^{p-1} \chi_\pi(j')^{-1} \xi^{j'} \ mod(q) \text{ via le changement (car } q \text{ et } p \text{ premiers distincts) } j' = qj \\
&\equiv \chi_\pi(q) \sum_{j'=1}^{p-1} \overline{\chi_\pi(j')} \xi^{j'} \ mod(q) \text{ car } \chi_\pi(j')^{-1} = \overline{\chi_\pi(j')} \\
&\equiv \chi_\pi(q) g(\overline{\chi_\pi}) \ mod(q) \text{ par définition} \\
\text{Ainsi, } (g(\chi_\pi)^4)^{\frac{q+1}{4}} &= g(\chi_\pi)^{q+1} \\
&= g(\chi_\pi)^q g(\chi_\pi) \\
&\equiv \chi_\pi(q) g(\chi_\pi) g(\overline{\chi_\pi}) \ mod(q).
\end{aligned}$$

On a maintenant :

$$\begin{aligned}
\pi^{\frac{(q+3)(q+1)}{4}} &= \pi^{\frac{q(q+1)}{4}}\pi^{\frac{3(q+1)}{4}} \\
&= (\pi^q)^{\frac{(q+1)}{4}}(\pi^3)^{\frac{q+1}{4}} \\
&\equiv (\pi)^{\frac{(q+1)}{4}}(\pi^3)^{\frac{q+1}{4}}\ mod(q) \text{ par le Lemme 5.4.10} \\
&\equiv (\pi\pi^3)^{\frac{q+1}{4}}\ mod(q) \\
&\equiv (g(\chi_\pi)^4)^{\frac{q+1}{4}}\ mod(q) \text{ par la Proposition 5.4.9} \\
&\equiv \chi_\pi(q)g(\chi_\pi)g(\overline{\chi_\pi})\ mod(q) \text{ d'après ce qu'on a fait précédemment} \\
&\equiv \chi_\pi(q)\,\chi_\pi(-1)\overline{g(\chi_\pi)}g(\chi_\pi)\ mod(q) \text{ d'après la remarque qui suit la Proposition 4.2.3} \\
&\equiv \chi_\pi(q)\,\chi_\pi(-1)|g(\chi_\pi)|^2\ mod(q) \\
&\equiv \chi_\pi(-q)p\ mod(q) \text{ par la Proposition 4.2.3} \\
&\equiv \chi_\pi(-q)\pi\overline{\pi}\ mod(q) \\
&\equiv \chi_\pi(-q)\pi^{q+1}\ mod(q) \text{ par le Lemme 5.4.10.}
\end{aligned}$$

Et puisque q est irréductible, D/qD est un corps fini, donc en particulier intègre.
Puisque $\pi^{\frac{(q+3)(q+1)}{4}} = \pi^{\frac{q^2-1}{4}}\pi^{q+1}$, on a d'après ce qu'on vient de faire :
$\pi^{q+1}(\pi^{\frac{q^2-1}{4}} - \chi_\pi(-q)) = 0$ dans D/qD

Puisque q et π sont irréductibles, et $q \neq \pi$, on a $\pi^{q+1} \neq 0$ dans D/qD, donc par intégrité, $\pi^{\frac{q^2-1}{4}} - \chi_\pi(-q) = 0$ dans D/qD.
Donc $\pi^{\frac{q^2-1}{4}} \equiv \chi_\pi(-q)\ mod(q)$
Mais, par définition, $\pi^{\frac{q^2-1}{4}} \equiv \chi_q(\pi)\ mod(q)$
On a donc $\chi_\pi(-q) \equiv \chi_q(\pi)\ mod(q)$. Donc $\chi_\pi(-q) - \chi_q(\pi) = dq$, avec $d \in D$.
Et en passant à la norme de chaque côté, puisque $\chi_\pi(-q)$ et $\chi_q(\pi)$ sont inversibles, $N(\chi_\pi(-q) - \chi_q(\pi)) \leq 4$ et $q \geq 3$, donc $N(q) \geq 9$, on trouve $d = 0$, donc $\chi_\pi(-q) = \chi_q(\pi)$.

□

Notons que $-q$ est primaire irréductible et $\frac{N(q)-1}{4} = \frac{q^2-1}{4}$. Ainsi, la Proposition précédente est un cas particulier de la loi de réciprocité biquadratique.

Proposition 5.4.12.
Soit q premier positif tel que $q \equiv 1\ mod(4)$ et $q \neq p$.
Alors $\chi_\pi(q) = \chi_q(\pi)$.

Démonstration. $p \neq q$, donc $pgcd(\pi, q) = 1$, et $\chi_q(\pi)$ a un sens.

$$\begin{aligned}
g(\chi_\pi)^q &\equiv \sum_{j=1}^{p-1}\chi_\pi(j)^q\xi^{qj}\ mod(q) \text{ par Frobenius} \\
&\equiv \sum_{j=1}^{p-1}\chi_\pi(j)\xi^{qj}\ mod(q) \text{ car } q \equiv 1\ mod(4) \\
&\equiv \overline{\chi_\pi(q)}\sum_{j=1}^{p-1}\chi_\pi(qj)\xi^{qj}\ mod(q) \text{ en multipliant par } 1 = \overline{\chi_\pi(q)}\,\chi_\pi(q) \\
&\equiv \overline{\chi_\pi(q)}g(\chi_\pi)\ mod(q).
\end{aligned}$$

Donc $g(\chi_\pi)^{q+3} \equiv \overline{\chi_\pi(q)} g(\chi_\pi)^4 \ mod(q)$.
Puisque $q \equiv 1 \ mod(4)$, la Proposition 5.4.9 donne $(\pi^3\overline{\pi})^{\frac{q+3}{4}} \equiv \overline{\chi_\pi(q)}\pi^3\overline{\pi} \ mod(q)$.
Puisque les deux membres de cette congruence sont dans D et que $pgcd(q,\pi) = pgcd(q,\overline{\pi}) = 1$, on peut diviser par $\pi^3\overline{\pi}$ des deux côtés, et on trouve :
$(\pi^3\overline{\pi})^{\frac{q-1}{4}} \equiv \overline{\chi_\pi(q)} \ mod(q)$.
q est premier positif, $q \equiv 1 \ mod(4)$, donc, par le Lemme 5.2.5, $q = \lambda\overline{\lambda}$, avec λ irréductible.
On a donc $\chi_\lambda(\pi^3)\chi_\lambda(\overline{\pi}) \equiv \overline{\chi_\pi(q)} \ mod(\lambda)$ par définition de χ_λ.
Comme dans la Proposition précédente, en passant à la norme, on conclut que $\chi_\lambda(\pi^3)\chi_\lambda(\overline{\pi}) = \overline{\chi_\pi(q)}$.
Or, $\chi_\lambda(\pi^3) = \chi_\lambda(\pi)^3 = \chi_\lambda(\pi)^{-1} = \overline{\chi_\lambda(\pi)}$.
Donc

$$\begin{aligned}\chi_\lambda(\pi^3)\chi_\lambda(\overline{\pi}) &= \overline{\chi_\lambda(\pi)}\chi_\lambda(\overline{\pi}) \\ &= \chi_{\overline{\lambda}}(\overline{\pi})\chi_\lambda(\overline{\pi}) \text{ par le point d) de la Proposition 5.3.6} \\ &= \chi_q(\overline{\pi}) \text{ par définition.}\end{aligned}$$

On obtient $\overline{\chi_\pi(q)} = \chi_q(\overline{\pi})$, donc en passant au conjugué de chaque côté de l'égalité, on conclut que $\chi_\pi(q) = \chi_q(\pi)$.

□

Proposition 5.4.13.
Soit $a \neq 1$ un entier tel que $a \equiv 1 \ mod(4)$ et λ primaire tel que $pgcd(a,\lambda) = 1$.
Alors, $\chi_a(\lambda) = \chi_\lambda(a)$.

Démonstration.
λ est primaire (donc non inversible et $1+i$ ne divise pas λ) et $pgcd(\lambda, a) = 1$, donc $\chi_\lambda(a)$ existe.
De plus, λ est primaire donc, par le Lemme 5.2.12, il existe une famille $(\lambda_j)_j$ d'éléments primaires irréductibles telle que $\lambda = \prod_j \lambda_j$.
Et, en utilisant le même raisonnement que la Proposition 5.3.11, on a $a = p_1...p_t(-q_1)...(-q_r)$, avec pour tout $1 \leq k \leq t$, p_k premier positif et $p_k \equiv 1 \ mod(4)$ et, pour tout $1 \leq l \leq s$, q_l premier positif et $q_l \equiv 3 \ mod(4)$.
Donc,

$$\begin{aligned}\chi_\lambda(a) &= \prod_j \chi_{\lambda_j}(a) \\ &= \prod_j \chi_{\lambda_j}(p_1...p_t(-q_1)...(-q_r)) \\ &= \prod_j \chi_{\lambda_j}(p_1)...\chi_{\lambda_j}(p_t)\chi_{\lambda_j}(-q_1)...\chi_{\lambda_j}(-q_r) \text{ où } \forall j,k, pgcd(\lambda_j, p_k) = 1 \\ &= \prod_j \chi_{p_1}(\lambda_j)...\chi_{p_t}(\lambda_j)\chi_{q_1}(\lambda_j)...\chi_{q_r}(\lambda_j) \text{ par les Propositions 5.4.11 et 5.4.12} \\ &= \prod_j \chi_{p_1...p_tq_1...q_r}(\lambda_j) \\ &= \chi_{p_1...p_tq_1...q_r}(\lambda)\end{aligned}$$

Mais $p_1...p_tq_1...q_r$ et a ne différent multiplicativement que d'un signe, donc $(p_1...p_tq_1...q_r) = (a)$ et donc $\chi_{p_1...p_tq_1...q_r}(\lambda) = \chi_a(\lambda)$.
On conclut que $\chi_\lambda(a) = \chi_a(\lambda)$.

□

Proposition 5.4.14.
Soient $\pi = a + ib$ et $\lambda = c + id$, avec $a, b, c, d \in \mathbb{Z}$ deux éléments primaires et premiers entre eux.
Si $pgcd(a,b) = 1$ et $pgcd(c,d) = 1$, alors $\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{(\frac{a-1}{2})(\frac{c-1}{2})}$.

Démonstration.
Comme $pgcd(a,b)=1$, il existe u et v dans $\mathbb{Z}$ tels que $au+bv=1$. Soient deux tels entiers.
Alors, $(vi+u)a-iv\pi = via+ua-via+vb = au+bv = 1$.
Donc $pgcd(a,\pi)=1$. De la même façon, on a $pgcd(b,\pi)=pgcd(c,\lambda)=pgcd(d,\lambda)=1$.
On a aussi $c\pi - ib\lambda = ac+bd$, donc $c\pi \equiv ac+bd\ mod(\lambda)$, et, de la même manière, $a\lambda \equiv ac+bd\ mod(\pi)$.
Soit δ un diviseur commun à λ et $ac+bd$. Alors, d'après ce qu'on vient de faire, δ divise $c\pi$.
Or, $pgcd(\pi,\lambda)=1$ et $pgcd(c,\lambda)=1$, donc, $pgcd(\lambda,c\pi)=1$.
Or, par hypothèse, δ divise λ et δ divise $c\pi$, donc δ inversible.
Ainsi, $pgcd(ac+bd,\lambda)=1$, et de la même manière, $pgcd(ac+bd,\pi)=1$.
Ces égalités justifient l'existence des éléments qui vont suivre.
On a $\chi_\lambda(c\pi)=\chi_\lambda(ac+bd)$ d'après la congruence donnée plus tôt, donc $\chi_\lambda(c)\chi_\lambda(\pi)=\chi_\lambda(ac+bd)$.
De même, $\chi_\pi(a)\,\chi_\pi(\lambda)=\chi_\pi(ac+bd)$.
En multipliant la première égalité par le conjugué de la seconde, et en utilisant le point d) de la Proposition 5.3.6, on obtient la relation :
$\chi_\lambda(c)\chi_{\overline{\pi}}(a)\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)}=\chi_{\lambda\overline{\pi}}(ac+bd)$.
Et, en utilisant que l'inverse de ces éléments est en fait leur conjugué, et en appliquant encore une fois le point d) de la Proposition 5.3.6, on a :
$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)}=\chi_{\overline{\lambda}}(c)\,\chi_\pi(a)\chi_{\lambda\overline{\pi}}(ac+bd)$.

Supposons que ni c, ni a, ni $ac+bd$ n'est inversible.
On pose, pour tout entier n impair, $\epsilon(n)=(-1)^{\frac{(n-1)}{2}}$.
On remarque que que si $n\equiv 3 mod(4)$, $\epsilon(n)=-1$ et si $n\equiv 1 mod(4)$, $\epsilon(n)=1$, donc, pour tout n impair, $\epsilon(n)n\equiv 1 mod(4)$.
Et puisque λ et π sont primaires, on a par le 5.2.8 que b et d sont congrus à 0 ou 2 modulo 4, donc bd est congru à 0 modulo 4.
De plus, toujours par le Lemme 5.2.8, a et c sont impairs et donc $ac+bd$ est impair.
Ainsi, $\epsilon(ac+bd)=(-1)^{\frac{ac+bd-1}{2}}=(-1)^{\frac{ac-1}{2}}(-1)^{\frac{bd}{2}}=(-1)^{\frac{ac-1}{2}}$ car $bd\equiv 0 mod(4)$.
Et, par un calcul facile, on a que $ac-1\equiv(a-1)+(c-1) mod(4)$.
Donc $(ac+bd)=\epsilon(a)\epsilon(c)$. Et $\epsilon(n)^2=1$ pour tout n impair.
On écrit donc :

$$\begin{aligned}\chi_\lambda(c) &= \chi_\lambda(\epsilon(c)^2 c)\\ &= \chi_\lambda(\epsilon(c))\chi_\lambda(c\epsilon(c)) \text{ par multiplicativité}\\ &= \chi_\lambda(\epsilon(c))\chi_{c\epsilon(c)}(\lambda) \text{ d'après la Proposition 5.4.13 puisque } c\epsilon(c)\equiv 1\ mod(4)\\ &= \chi_\lambda(\epsilon(c))\chi_c(\lambda) \text{ car } (c)=(c\epsilon(c)).\end{aligned}$$

Donc $\chi_{\overline{\lambda}}(c)=\overline{\chi_\lambda(c)}=\chi_{\overline{\lambda}}(\epsilon(c))\chi_c(\overline{\lambda})$. De même, $\chi_\pi(a)=\chi_\pi(\epsilon(a))\chi_a(\pi)$ et $\chi_{\lambda\overline{\pi}}(ac+bd)=\chi_{\lambda\overline{\pi}}(\epsilon(a)\epsilon(c))\chi_{ac+bd}(\lambda\overline{\pi})$.
On remarque que $\chi_{\overline{\lambda}}(\epsilon(c))$ vaut 1 ou -1 au vu de la définition de ϵ, donc $\overline{\chi_{\overline{\lambda}}(\epsilon(c))}=\chi_{\overline{\lambda}}(\epsilon(c))$.
Donc $\chi_\lambda(\epsilon(c))=\chi_{\overline{\lambda}}(\epsilon(c))$.
De même, $\chi_\pi(\epsilon(a))=\chi_{\overline{\pi}}(\epsilon(a))$.
Par la Proposition 5.3.12, $\chi_\pi(\epsilon(c))=\chi_\lambda(\epsilon(a))$, donc $\chi_\pi(\epsilon(c))\,\chi_\lambda(\epsilon(a))=1$.
Et donc, $\chi_{\overline{\lambda}}(\epsilon(c))\,\chi_\pi(\epsilon(a))\chi_{\lambda\overline{\pi}}(\epsilon(a)\epsilon(c))=\chi_{\lambda\overline{\pi}}((\epsilon(a)\epsilon(c))^2)=1$.
Ainsi, $\chi_{\overline{\lambda}}(c)\,\chi_\pi(a)\chi_{\lambda\overline{\pi}}(ac+bd)=\chi_c(\overline{\lambda})\chi_a(\pi)\chi_{ac+bd}(\lambda\overline{\pi})$.

$$\begin{aligned}\chi_c(\overline{\lambda}) &= \chi_c(c-di)\\ &= \chi_c(-di) \text{ en appliquant le point g) de la Prop 5.3.6 aux caractères biquadratiques généralisés}\\ &= \chi_c(-d)\chi_c(i)\\ &= \chi_c(i) \text{ en appliquant la Proposition 5.3.9 puisque } pgcd(c,-d)=1 \text{ par hypothèse, et } c \text{ impair.}\end{aligned}$$

De même, $\chi_{\underline{a}}(\pi) = \chi_a(i)$ et $\chi_{ac+bd}(\lambda\overline{\pi}) = \chi_{ac+bd}(i)$.
Donc, $\chi_\lambda(\pi)\chi_\pi(\lambda) = \chi_c(i)\chi_a(i)\chi_{ac+bd}(i) = \chi_{ac(ac+bd)}(i)$.
Or, d'après les congruences données par le Lemme 5.2.8, on a $a^2 \equiv 1\ mod(4), c^2 \equiv 1\ mod(4)$ et $bd \equiv 0\ mod(4)$.
Puisque $ac(ac+bd) = a^2c^2 + acbd$, on a $ac(ac+bd) \equiv 1\ mod(4)$.
Donc, on peut appliquer la Proposition 5.3.11, et on trouve $\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = (-1)^{\frac{((ac+bd)ac-1)}{4}}$.
Et en utilisant les congruences données par le Lemme 5.2.8, par une démonstration similaire à celle du Lemme 5.3.10, on trouve :
$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = (-1)^{(\frac{a-1}{2})(\frac{c-1}{2})}$.
Puis en utilisant que $\overline{\chi_\pi(\lambda)} = \chi_\pi(\lambda)^{-1}$, on conclut que $\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{(\frac{a-1}{2})(\frac{c-1}{2})}$.

Supposons maintenant que a ou c ou $ac+bd$ est inversible.
En distinguant les valeurs 1, -1 et non inversible, au premier abord, il semble qu'il y ait 26 cas à traiter (3^3-1). Mais on remarque que les rôles de a et c sont symétriques. De cette manière, on réduit le nombre de cas à traiter à 17. De plus, le fait que, quelle que soit la situation, $bd \equiv 0\ mod(4)$ rend certains cas impossibles. Par exemple, si $a = c = 1$, on ne peut pas avoir $(1 + bd =)ac + bd = -1$. Et, par exemple, pour le cas $a = c = ac + bd = 1$, on remarque que cela implique $b = 0$ ou $d = 0$, donc π ou λ inversible ce qui est absurde par définition d'un élément primaire. De cette manière, on enlève les 6 cas où les trois sont inversibles, et cela nous ramène à 11 cas à traiter.
On rappelle qu'on a la formule

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_{\overline{\lambda}}(c)\,\chi_\pi(a)\chi_{\lambda\overline{\pi}}(ac+bd). \quad (*)$$

Et, on peut réutiliser le travail effectué précédemment dans la preuve dans le cas où un élément n'est pas inversible.

Cas 1 : $a = c = 1$, $ac + bd$ non inversible
On a $\chi_{\overline{\lambda}}(1) = \chi_\pi(1) = 1$
$\chi_{\overline{\pi}\lambda}(ac+bd) = \chi_{1+bd}(i) = (-1)^{\frac{1+bd-1}{4}}$ puisque $1 + bd$ non inversible et primaire
Or, par les hypothèses $a = c = 1$, on a $b \equiv d \equiv 0\ mod(4)$, donc $\frac{bd}{4}$ est pair, et $\chi_{\overline{\pi}\lambda}(ac+bd) = 1$.
On obtient donc par la formule (*) $\chi_\lambda(\pi) = \chi_\pi(\lambda)$.
Et $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = 1$.
Donc l'égalité reste vraie.

Cas 2 : $a = 1, c = -1, ac + bd$ non inversible
On a $\chi_\pi(1) = 1$. Puisque $\overline{\lambda}$ est primaire, on a, par la Proposition 5.3.12, $\chi_{\overline{\lambda}}(-1) = (-1)^{\frac{c-1}{2}} = -1$.

$$\begin{aligned}
\chi_{\overline{\pi}\lambda}(-1+bd) &= \chi_{\overline{\pi}\lambda}(-1)\,\chi_{\overline{\pi}\lambda}(1-bd) \\
&= (-1)^{\frac{a-1}{2}}(-1)^{\frac{a-1}{2}}\chi_{1-bd}(i) \quad \text{puisque } 1-bd \text{ non inversible et } 1-bd \equiv 1\ mod(4) \\
&= (-1)(-1)^{\frac{1-bd-1}{4}} \\
&= -1 \text{ car } b \equiv 0\ mod(4) \text{ et } d \text{ pair.}
\end{aligned}$$

On obtient avec la formule (*) $\chi_\lambda(\pi) = \chi_\pi(\lambda)$.
Et $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = 1$.
Donc l'égalité reste vraie.

Cas 3 : $a = c = -1$, $ac + bd$ non inversible
$\chi_\pi(-1) = (-1)^{\frac{a-1}{2}} = -1$ et $\chi_{\overline{\lambda}}(-1) = (-1)^{\frac{c-1}{2}} = -1$.
Et $\chi_{\overline{\pi}\lambda}(1+bd) = \chi_{1+bd}(i) = (-1)^{\frac{1+bd-1}{4}}$ car $1 + bd \equiv 1 mod(4)$.

Or $b \equiv d \equiv 2\ mod(4)$, donc $bd \equiv 4\ mod(8)$, et $(-1)^{\frac{1+bd-1}{4}} = -1$.
Donc $\chi_{\overline{\pi}\lambda}(1+bd) = -1 = \chi_\pi(-1)\,\chi_{\overline{\lambda}}(-1)\,\chi_{\overline{\pi}\lambda}(1+bd)$, et par la formule (*), $\chi_\lambda(\pi) = -\chi_\pi(\lambda)$.
De plus, $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = -1$.
Donc l'égalité reste vraie.

Cas 4 : $a = ac + bd = 1$, c non inversible
$c = 1 - bd$ par hypothèse, donc $c \equiv 1\ mod(4)$.
$\chi_\pi(1) = \chi_{\overline{\pi}\lambda}(1) = 1$ et $\chi_{\overline{\lambda}}(c) = \chi_c(i) = (-1)^{\frac{c-1}{4}}$.
Or, $\frac{c-1}{4} = \frac{-bd}{4}$, et puisque $a \equiv c \equiv 1\ mod(4)$, $b \equiv d \equiv 0\ mod(4)$, et donc $\frac{bd}{4}$ est pair et $\chi_{\overline{\lambda}}(c) = 1$.
On a donc avec la formule (*) $\chi_\lambda(\pi) = \chi_\pi(\lambda)$.
Et $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = 1$.
Donc l'égalité reste vraie.

Cas 5 : $a = 1$, c non inversible, $ac + bd = -1$
$c = -1 - bd$ par hypothèse, donc $c \equiv 3\ mod(4)$.
$\chi_\pi(1) = 1$ et $\chi_{\overline{\pi}\lambda}(-1) = (-1)^{\frac{c-1}{2}}(-1)^{\frac{a-1}{2}} = -1$

$$\begin{aligned}\chi_{\overline{\lambda}}(c) &= \chi_{\overline{\lambda}}(-1)\,\chi_{\overline{\lambda}}(-c)\\ &= (-1)^{\frac{c-1}{2}}\chi_{-c}(i) \quad \text{par la Proposition 5.3.12}\\ &= -(-1)^{\frac{-c-1}{4}}.\end{aligned}$$

Or, $-c = 1 + bd$, donc $\frac{-c-1}{4} = \frac{bd}{4}$ et puisque $b \equiv 0\ mod(4)$ et d pair, on a $(-1)^{\frac{-c-1}{4}} = 1$, donc $\chi_{\overline{\lambda}}(c) = -1$.
Le produit des trois résultats obtenus et la formule (*) donnent $\chi_\lambda(\pi) = \chi_\pi(\lambda)$.
Et $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = 1$.
Donc l'égalité reste vraie.

Cas 6 : $a = 1$, c et $ac + bd$ non inversibles
Pour commencer, $\chi_\pi(1) = 1$.
Pour le reste, $\chi_{\overline{\lambda}}(c)\,\chi_{\overline{\pi}\lambda}(ac+bd) = \chi_{\overline{\lambda}}(\epsilon(c))\,\chi_{\overline{\pi}\lambda}(\epsilon(c))\,\chi_{\overline{\lambda}}(c\epsilon(c))\,\chi_{\overline{\pi}\lambda}(\epsilon(c)(c+bd))$.
Or, $\chi_{\overline{\pi}\lambda}(\epsilon(c)) = \chi_\lambda(\epsilon(c))\,\chi_{\overline{\pi}}(\epsilon(c))$ et $\chi_\lambda(\epsilon(c)) = \chi_{\overline{\lambda}}(\epsilon(c))$ donc $\chi_{\overline{\lambda}}(\epsilon(c))\,\chi_{\overline{\pi}\lambda}(\epsilon(c)) = \chi_\lambda(\epsilon(c))^2\,\chi_{\overline{\pi}}(\epsilon(c)) = \chi_{\overline{\pi}}(\epsilon(c))$.
Si $\epsilon(c) = 1$, on obtient $\chi_{\overline{\lambda}}(\epsilon(c))\,\chi_{\overline{\pi}\lambda}(\epsilon(c)) = 1$, et si $\epsilon(c) = -1$, on a par la Proposition 5.3.12 $\chi_{\overline{\pi}}(\epsilon(c)) = (-1)^{\frac{a-1}{2}} = 1$, donc $\chi_{\overline{\lambda}}(\epsilon(c))\,\chi_{\overline{\pi}\lambda}(\epsilon(c)) = 1$.
Dans les deux cas, $\chi_{\overline{\lambda}}(c)\,\chi_{\overline{\pi}\lambda}(ac+bd) = \chi_{\overline{\lambda}}(c\epsilon(c))\,\chi_{\overline{\pi}\lambda}(\epsilon(c)(c+bd))$.
En utilisant les manipulations faites dans la première partie de la preuve, on trouve $\chi_{\overline{\lambda}}(c\epsilon(c))\,\chi_{\overline{\pi}\lambda}(\epsilon(c)(c+bd)) = \chi_{c(c+bd)}(i) = (-1)^{\frac{c(c+bd)-1}{4}}$ car $c(c+bd) \equiv 1\ mod(4)$.
Or, $b \equiv 0\ mod(4)$ et d impair, donc $bd \equiv 0\ mod(8)$ et ainsi, $cbd \equiv 0\ mod(8)$.
Et, quelle que soit la congruence de c modulo 4, (1 ou 3), on remarque par des calculs simples que $c^2 \equiv 1\ mod(8)$.
En rassemblant ces résultats, on obtient $(-1)^{\frac{c(c+bd)-1}{4}} = 1$, donc $\chi_{\overline{\lambda}}(c)\,\chi_{\overline{\pi}\lambda}(ac+bd) = 1$ et par la formule (*), $\chi_\lambda(\pi) = \chi_\pi(\lambda)$.
Et $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = 1$.
Donc l'égalité reste vraie.

Cas 7 : $a = -1$, c non inversible, $ac + bd = 1$
Par les hypothèses, $c = -1 + bd$, donc $c \equiv 3 mod(4)$.
Ainsi, $b \equiv d \equiv 2\ mod(4)$ et $bd \equiv 4\ mod(8)$.

$\chi_\pi(-1) = (-1)^{\frac{a-1}{2}} = -1$ et $\chi_{\overline{\pi}\lambda}(1) = 1$.

$$\begin{aligned}
\chi_{\overline{\lambda}}(c) &= \chi_{\overline{\lambda}}(-1)\,\chi_{\overline{\lambda}}(-c) \\
&= (-1)^{\frac{c-1}{2}}\chi_{-c}(i) \text{ par la Proposition 5.3.12} \\
&= -(-1)^{\frac{-c-1}{4}} \text{ car } c \equiv 3\ mod(4) \\
&= -(-1)^{\frac{-bd}{4}} \\
&= 1 \quad \text{car } bd \equiv 4\ mod(8).
\end{aligned}$$

Donc, par la formule (*), $\chi_\lambda(\pi) = -\chi_\pi(\lambda)$.
De plus, $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = -1$ car a et c sont congrus à 3 modulo 4.

Donc l'égalité reste vraie.

Cas 8 : $a = ac + bd = -1$, c non inversible
Par les hypothèses, $c = 1 + bd$ donc $c \equiv 1\ mod(4)$.
Ainsi, $b \equiv 2\ mod(4)$ et $d \equiv 0\ mod(4)$, donc $bd \equiv 0\ mod(8)$.
$\chi_\pi(-1) = (-1)^{\frac{a-1}{2}} = -1$ et $\chi_{\overline{\pi}\lambda}(-1) = (-1)^{\frac{c-1}{2}}(-1)^{\frac{a-1}{2}} = -1$.
$\chi_{\overline{\lambda}}(c) = \chi_c(i) = (-1)^{\frac{c-1}{4}}$ car $c \equiv 1\ mod(4)$.
Or, $c - 1 = bd \equiv 0\ mod(8)$, donc $\chi_{\overline{\lambda}}(c) = 1$.
La formule (*) donne donc $\chi_\lambda(\pi) = \chi_\pi(\lambda)$.
Et puisque $c \equiv 1\ mod(4)$, $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = 1$.
Donc l'égalité reste vraie.

Cas 9 : $a = -1$, c et $ac + bd$ non inversibles
$\chi_\pi(-1) = (-1)^{\frac{a-1}{2}} = -1$.
On rappelle que $c^2 \equiv 1\ mod(8)$.
Si $c \equiv 1\ mod(4)$:
On a $b \equiv 2\ mod(4)$ et $d \equiv 0\ mod(4)$, donc $bd \equiv 0\ mod(8)$ et $cbd \equiv 0\ mod(8)$.

$$\begin{aligned}
\chi_{\overline{\lambda}}(c)\,\chi_{\overline{\pi}\lambda}(-c + bd) &= \chi_c(i)\,\chi_{\overline{\pi}\lambda}(-1)\chi_{c-bd}(i) \qquad \text{par le travail effectué en première partie de preuve} \\
&= \chi_{c(c+bd)}(i)(-1)^{\frac{c-1}{2}+\frac{a-1}{2}} \\
&= -(-1)^{\frac{c(c+bd)-1}{4}} \qquad \text{car } c \equiv 1\ mod(4) \text{ et } c(c+bd) \equiv 1\ mod(4) \\
&= -1 \qquad \text{car } c^2 \equiv 1\ mod(8) \text{ et } cbd \equiv 0\ mod(8).
\end{aligned}$$

Donc la formule (*) donne $\chi_\lambda(\pi) = \chi_\pi(\lambda)$
Et puisque $c \equiv 1\ mod(4)$, $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = 1$.
Donc l'égalité reste vraie.

Si $c \equiv 3\ mod(4)$:
On a $b \equiv d \equiv 2\ mod(4)$, donc $cb \equiv 2\ mod(4)$ et $-cbd \equiv 4\ mod(8)$.

$$\begin{aligned}
\chi_{\overline{\lambda}}(c)\,\chi_{\overline{\pi}\lambda}(-c + bd) &= \chi_{-c}(i)\,\chi_{\overline{\lambda}}(-1)\chi_{-c+bd}(i) \qquad \text{par le travail effectué en première partie de preuve} \\
&= \chi_{-c(-c+bd)}(i)(-1)^{\frac{c-1}{2}} \\
&= -(-1)^{\frac{-c(-c+bd)-1}{4}} \qquad \text{car } c \equiv 3 mod(4) \text{ et } -c(-c+bd) \equiv 1\ mod(4) \\
&= 1 \qquad \text{car} c^2 \equiv 1 mod(8) \text{ et } cbd \equiv 0\ mod(8).
\end{aligned}$$

Donc la formule (*) donne $\chi_\lambda(\pi) = -\chi_\pi(\lambda)$, et puisque $c \equiv 3\ mod(4)$, $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = -1$.
Donc l'égalité reste vraie.

Cas 10 : a et c non inversible, $ac + bd = 1$
Puisque $ac + bd = 1$, $ac \equiv 1\ mod(4)$ on remarque par calculs simples que $a \equiv c\ mod(4)$.
Et donc, $b \equiv d\ mod(4)$.
$\chi_{\overline{\pi}\lambda}(1) = 1$ et $\chi_{\overline{\lambda}}(c)\,\chi_\pi(a) = \chi_\pi(\epsilon(a))\,\chi_{\overline{\lambda}}(\epsilon(c))\chi_{ac}(i) = \chi_{ac}(i)$ car a et c ont la même congruence modulo 4.
Or, $ac \equiv 1\ mod(4)$, donc $\chi_{ac}(i) = (-1)^{\frac{ac-1}{4}} = (-1)^{\frac{bd}{4}}$.
Si a et c sont congrus à 1 modulo 4, b et d sont congrus à 0 modulo 4 donc $\frac{bd}{4}$ est pair, et donc $\chi_{\overline{\lambda}}(c)\,\chi_\pi(a) = 1$.
La formule (*) donne alors $\chi_\lambda(\pi) = \chi_\pi(\lambda)$, et puisque $c \equiv a \equiv 1\ mod(4)$, $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = 1$.
Donc l'égalité reste vraie.
Si a et c sont congrus à 3 modulo 4, b et d sont congrus à 2 modulo 4 donc $bd \equiv 4\ mod(8)$, et $\frac{bd}{4}$ est impair.
Donc, $\chi_{\overline{\lambda}}(c)\,\chi_\pi(a) = -1$.
La formule (*) donne alors $\chi_\lambda(\pi) = -\chi_\pi(\lambda)$, et puisque $c \equiv a \equiv 3\ mod(4)$, $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = -1$.
Donc l'égalité reste vraie.

Cas 11 : a et c non inversibles, $ac + bd = -1$
Cette fois, $ac \equiv 3\ mod(4)$ donc a et c sont de congruences opposées modulo 4.
On va supposer, sans perte de généralité, que $a \equiv 1\ mod(4)$ et $c \equiv 3\ mod(4)$.
Donc $b \equiv 0\ mod(4)$ et $d \equiv 2\ mod(4)$, donc $bd \equiv 0\ mod(8)$.
$\chi_{\overline{\pi}\lambda}(-1) = (-1)^{\frac{a-1}{2}}(-1)^{\frac{c-1}{2}} = -1$, $\chi_\pi(a) = \chi_a(i)$ et $\chi_{\overline{\lambda}}(c) = \chi_{\overline{\lambda}}(-1)\chi_{-c}(i) = (-1)^{\frac{c-1}{2}}\chi_{-c}(i) = -\chi_{-c}(i)$.
Donc $\chi_{\overline{\pi}\lambda}(-1)\,\chi_\pi(a)\,\chi_{\overline{\lambda}}(c) = \chi_a(i)\chi_{-c}(i) = (-1)^{\frac{-ac-1}{4}}$ car $-ac \equiv 1\ mod(4)$. Or, $\frac{-ac-1}{4} = \frac{bd}{4}$, qui est pair car $bd \equiv 0\ mod(8)$.
Donc $\chi_{\overline{\pi}\lambda}(-1)\,\chi_\pi(a)\,\chi_{\overline{\lambda}}(c) = 1$, et la formule (*) donne $\chi_\lambda(\pi) = \chi_\pi(\lambda)$.
Et puisque $a \equiv 1\ mod(4)$, $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = 1$
Donc l'égalité reste vraie.

□

La loi générale de réciprocité biquadratique suit de cette Proposition.
Soient π et λ deux éléments primaires premiers entre eux. On suppose qu'aucun des deux n'est entier (ce cas a déjà été traité dans la Proposition 5.4.13, car par le Lemme 5.2.8, tout entier primaire est congru à 1 modulo 4)
On écrit $\pi = m(a + ib)$, $\lambda = n(c + id)$ avec $n \equiv m \equiv 1\ mod(4)$, $pgcd(a, b) = pgcd(c, d) = 1$. On peut faire une telle décomposition car si $\pi = a' + ib'$, avec $a', b' \in \mathbb{Z}$, $pgcd(a', b')$ est impair puisque a' et b' ne sont pas de même parité par le Lemme 5.2.8.
Donc $pgcd(a', b')$ est congru à 1 ou 3 modulo 4. On obtient le résultat voulu en factorisant π par $pgcd(a', b')$ ou $-pgcd(a', b')$.
On va supposer dans la suite que m et $n \neq 1$.
Par la Proposition 5.4.13, puisque n et m sont congrus à 1 modulo 4, λ et π primaires et $pgcd(n, \pi) = pgcd(\lambda, \pi) = pgcd(\lambda, m) = 1$, on a $\chi_\pi(n) = \chi_n(\pi)$ et $\chi_\lambda(m) = \chi_m(\lambda)$
Et puisque $a + bi \equiv 1\ mod((1 + i)^3)$, $c + di \equiv 1\ mod((1 + i)^3)$ et aucun des deux n'est inversible (puisque ni π ni λ n'est entier), ils sont primaires.

On a donc

$$\begin{aligned}\chi_\lambda(\pi) &= \chi_\lambda(m)\chi_\lambda(a+ib)\\ &= \chi_m(\lambda)\chi_n(a+ib)\chi_{c+id}(a+ib)\\ &= \chi_m(\lambda)\chi_{a+ib}(n)\chi_{a+ib}(c+id)(-1)^{(\frac{a-1}{2})(\frac{c-1}{2})} \text{ par la Proposition 5.4.14}\\ &= \chi_m(\lambda)\chi_{a+ib}(\lambda)(-1)^{(\frac{a-1}{2})(\frac{c-1}{2})} \text{ par multiplicativité}\\ &= \chi_\pi(\lambda)(-1)^{(\frac{a-1}{2})(\frac{c-1}{2})}.\end{aligned}$$

$N(\pi) = m^2(a^2+b^2)$ et $m \equiv 1\ mod(4)$, donc $m^2 \equiv 1\ mod(8)$ et $\frac{N(\pi)-1}{4}$ et $\frac{a^2+b^2-1}{4}$ ont la même parité.
Or, on l'avait déjà dit au début de la section sur la loi de réciprocité biquadratique, en utilisant que $a+ib$ est primaire, on a $\frac{a^2+b^2-1}{4}$ et $\frac{a-1}{2}$ de même parité.
Donc $\frac{N(\pi)-1}{4}$ et $\frac{a-1}{2}$ ont même parité.
De même, puisque $n \equiv 1\ mod(4)$, $\frac{N(\lambda)-1}{4}$ et $\frac{c-1}{2}$ ont même parité.
On conclut que $\chi_\lambda(\pi) = \chi_\pi(\lambda)(-1)^{(\frac{N(\pi)-1}{4})(\frac{N(\lambda)-1}{4})}$.
Il reste à traiter le cas où soit m soit n vaut 1. Par symétrie, il suffit de traiter le cas $m \neq 1$ et $n = 1$.
Alors, les calculs effectués précédemment restent les mêmes, en enlevant certains termes.
Dans les lignes 2 et 3 du dernier calcul, il suffit d'enlever les termes $\chi_n(a+ib)$ et $\chi_{a+ib}(n)$ puisque $n = 1$, et on retrouve les valeurs voulues et les résultats annoncés.

6 Pour aller plus loin...

6.1 Réciprocité biquadratique rationnelle

On utilise ici le caractère biquadratique pour relier les propriétés, pour p et q premiers distincts congrus à 1 modulo 4, que l'un soit, ou non, une puissance $4^{ème}$ modulo l'autre.
Tout au long de cette section, p et q désigneront des entiers premiers positifs distincts congrus à 1 modulo 4. Le groupe $\mathbb{F}_p^*$ est cyclique d'ordre $p-1$ et 4 divise $p-1$ par hypothèse donc $\mathbb{F}_p^*$ a un unique sous-groupe d'ordre $\frac{p-1}{4}$ qui consiste en les puissances quatrièmes des classes d'entiers.
On considère le caractère biquadratique χ_π où π irréductible qui divise p.
Soit n un entier premier à p.
Par le point b) de la Proposition 5.3.6, $\chi_\pi(n) = 1$ si, et seulement si, $x^4 \equiv n\ mod(\pi)$ a une solution dans D.

Lemme 6.1.1.
Soit n un entier premier à p.
$\chi_\pi(n) = 1$ si, et seulement si, $x^4 \equiv n\ mod(p)$ a une solution dans $\mathbb{Z}$.

Démonstration. Par la Proposition 5.3.1, le corps $D/\pi D$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
La classe de n est une puissance quatrième dans $D/\pi D$ si, et seulement si, c'en est une dans $\mathbb{Z}/p\mathbb{Z}$. □

Soit Ψ_p le symbole de Legendre modulo p.

Lemme 6.1.2. *Soit n un entier premier à p.*
Si $\Psi_p(n) = 1$, alors $\chi_\pi(n) = \pm 1$.

Démonstration. Puisque, par hypothèse, $n^{\frac{p-1}{2}} \equiv 1\ mod(p)$, il vient que $\chi_\pi(n)^2 \equiv (n^{\frac{p-1}{4}})^2 \equiv n^{\frac{p-1}{2}} \equiv 1\ mod(\pi)$.
Ainsi, $\chi_\pi(n)^2 = 1$, donc $\chi_\pi(n) = \pm 1$. □

Supposons que q est un carré modulo p. Alors, $\Psi_p(q) = 1$ et, par la loi de réciprocité quadratique, $\Psi_p(q) = 1$, donc, par le Lemme précédent, $\chi_\pi(q)$ vaut 1 ou -1. Plus précisément, $\chi_\pi(q)$ vaut 1 si q est une puissance quatrième modulo p et -1 sinon. Par la loi de réciprocité quadratique, puisque p et q sont congrus à 1 modulo 4 et $\chi_\pi(q) = 1$, on a $\Psi_q(p) = 1$.
On note que $\chi_\pi(q)$ ne dépend que de p et q, pas du choix de l'irréductible π qui divise p.
Contrairement à ce qu'on pourrait croire, la relation entre $\chi_\pi(q)$ et $\chi_\lambda(p)$ (où λ irréductible divise q) n'est pas une simple conséquence de la loi de réciprocité biquadratique.
Pour la suite, puisque p et q sont congrus à 1 modulo 4, on écrit $p = a^2 + b^2$ et $q = c^2 + d^2$ avec a et c impairs et b et d pairs.

On admet le Théorème suivant, démontré par Gauss en 1805 qui précise la Proposition 3.0.8 (voir la preuve dans [1], pp 74-75).

Théorème 6.1.3. *Soit q un entier premier impair.*
On note Ψ_q le symbole de Legendre modulo q.
La valeur de la somme de Gauss $g(\Psi_q)$ est donnée par :

$$g(\Psi_q) = \begin{cases} \sqrt{q} \text{ si } q \equiv 1 \ mod(4) \\ i\sqrt{q} \text{ si } q \equiv 3 \ mod(4) \end{cases}$$

Proposition 6.1.4. *Soit π primaire irréductible divisant p.*
Alors $g(\chi_\pi)^2 = -(-1)^{\frac{p-1}{4}}\sqrt{p}\pi$.

Démonstration. $p \equiv 1 \ mod(4)$ donc p est primaire, et donc par le Lemme 5.2.12, p se décompose en produit de primaires irréductibles, d'où l'existence de π.

$$\begin{aligned} \text{On a } J(\chi_\pi, \chi_\pi) &= -\chi_\pi(-1)\pi \text{ par la Proposition 5.4.8} \\ &= \frac{g(\chi_\pi)^2}{g(\Psi_p)} \text{ par le Théorème 4.3.2 et } \Psi_p \text{ non trivial.} \end{aligned}$$

Or, par définition, $\chi_\pi(-1) = (-1)^{\frac{p-1}{4}}$ et on a aussi $g(\Psi_p) = \sqrt{p}$ par le Théorème 6.1.3. □

Proposition 6.1.5. *Si π est primaire irréductible divisant p, alors $\chi_\pi(q)\,\chi_\lambda(p) \equiv \pi^{\frac{q-1}{2}} \ mod(q)$.*

Démonstration.

$$\begin{aligned} \text{On a dans l'anneau } \mathbb{Z}[\xi, i] \supset \mathbb{Z}[i],\ g(\chi_\pi)^q &= (\sum_j \chi_\pi(j)\xi^j)^q \\ &\equiv \sum_j \chi_\pi(j)\xi^{jq} \ mod(q) \text{ par Frobenius} \\ &\equiv \chi_\pi(q)^{-1} \sum_j \chi_\pi(qj)\xi^{jq} \ mod(q) \\ &\equiv \chi_\pi(q)^{-1} \sum_{j'} \chi_\pi(j')\xi^{j'} \ mod(q) \text{ (avec } j' = jq \text{)} \\ &\equiv \chi_\pi(q)^{-1} g(\chi_\pi) \ mod(q) \\ &\equiv \chi_\pi(q) g(\chi_\pi) \ mod(q) \text{ car } \chi_\pi(q)^2 = 1 \\ \text{En multipliant par } g(\chi_\pi)^3 \text{ , on obtient } g(\chi_\pi)^4 g(\chi_\pi)^{q-1} &\equiv \chi_\pi(q) g(\chi_\pi)^4 \quad \text{mod } (q) \\ \text{Donc } g(\chi_\pi)^4 (g(\chi_\pi)^{q-1} - \chi_\pi(q)) &\equiv 0 \ mod(q). \end{aligned}$$

Or, par la Proposition 4.3.5, le terme à gauche de la congruence est dans $\mathbb{Z}[i]$ et par la Proposition 4.2.3, $N(g(\chi_\pi)^4) = p^4$.
Puisque q et p sont premiers distincts, on peut donc simplifier la congruence pour obtenir $g(\chi_\pi)^{q-1} \equiv \chi_\pi(q)\ mod(q)$.
De plus, la Proposition 6.1.4 donne $(g(\chi_\pi)^2)^{\frac{q-1}{2}} = \sqrt{p}^{\frac{q-1}{2}}\pi^{\frac{q-1}{2}} = p^{\frac{q-1}{4}}\pi^{\frac{q-1}{2}}$.
Et, par définition, $p^{\frac{q-1}{4}} \equiv \chi_\lambda(p)\ mod(\lambda)$, et puisque les deux côtés de cette congruence sont des réels et que $pgcd(\lambda, \overline{\lambda}) = 1$, on obtient $p^{\frac{q-1}{4}} \equiv \chi_\lambda(p)\ mod(q)$.
En réunissant tous les calculs effectués, on trouve $\chi_\lambda(p)\pi^{\frac{q-1}{2}} \equiv \chi_\pi(q)\ mod(q)$.
Le fait que $\chi_\lambda(p)^2 = 1$ permet de conclure.

□

Lemme 6.1.6. *On a $\Psi_q(ad - bc) = \Psi_q(ad + bc)$.*

Démonstration. $c^2 + d^2 = q$ donc $c^2 \equiv -d^2 mod(q)$.

$$\begin{aligned}
\text{On a } \Psi_q(ad-bc)\Psi_q(ad+bc) &= \Psi_q(a^2d^2 - b^2c^2) \\
&= \Psi_q(d^2(a^2+b^2)) \\
&= \Psi_q(d^2p) \\
&= \Psi_q(d^2)\Psi_q(p) \\
&= \Psi_q(p) \text{ car } \Psi_q(d^2) = 1 \ (\Psi_q \text{ d'ordre 2}) \\
&= 1 \text{ par hypothèse.}
\end{aligned}$$

□

Dans la Proposition suivante, π n'est pas supposé primaire.

Proposition 6.1.7. *On a $\pi^{\frac{q-1}{2}} \equiv \Psi_q(d)\Psi_q(ad - bc)\ mod(q)$.*

Démonstration. $d\pi = da + idb \equiv da + idb - b\lambda \equiv ad - bc\ mod(\lambda)$.
Donc $(d\pi)^{\frac{q-1}{2}} \equiv (ad - bc)^{\frac{q-1}{2}}\ mod(\lambda)$.
Et donc, $\Psi_q(d)\pi^{\frac{q-1}{2}} \equiv \Psi_q(ad - bc)\ mod(\lambda)$.
De la même manière, $d\pi \equiv ad + bc\ mod(\overline{\lambda})$, donc $\Psi_q(d)\pi^{\frac{q-1}{2}} \equiv \Psi_q(ad + bc)\ mod(\overline{\lambda})$.
En utilisant le Lemme précédent et le fait que $pgcd(\lambda, \overline{\lambda}) = 1$ (par le Lemme 5.2.5), on peut conclure.

□

Lemme 6.1.8. *Si $q = c^2 + d^2$, $c > 0$, $c \equiv 1 mod(2)$, $\Psi_q(d) = (-1)^{\frac{q-1}{4}}$.*

Démonstration. Posons Ψ_c le symbole de Jacobi.
Par la Proposition 1.1.6, on a $\Psi_q(c) = \Psi_c(q) = \Psi_c(d^2) = 1$ car $q \equiv 1 mod(4)$ et avec la loi de réciprocité quadratique.
Mais $c^2 \equiv -d^2\ mod(q)$, donc $c^{\frac{q-1}{2}} \equiv (-1)^{\frac{q-1}{4}} d^{\frac{q-1}{2}}\ mod(q)$.
Ainsi, $\Psi_q(c) = 1 = (-1)^{\frac{q-1}{4}}\Psi_q(d)$.

□

Le Théorème suivant permet de relier les propriétés que p et q, qui sont des carrés l'un modulo l'autre, soient chacun, ou non, une puissance quatrième modulo l'autre.
Dans un premier temps, on n'y suppose pas π primaire.

Théorème 6.1.9. *On a $\chi_\pi(q)\,\chi_\lambda(p) = (-1)^{\frac{q-1}{4}}\Psi_q(ad - bc)$.*

Démonstration. On commence par remarquer que, puisque $\Psi_q(-1) = 1$, le Lemme 6.1.6 donne $\Psi_q(ad-bc) = \Psi_q(ad+bc) = \Psi_q(-ad+bc) = \Psi_q(-ad-bc)$.
Donc, on peut supposer, sans perte de généralité, que π est primaire.
Alors, par la Proposition 6.1.5, $\chi_\pi(q)\,\chi_\lambda(p) \equiv \pi^{\frac{q-1}{2}}\ mod(q)$ et par la Proposition 6.1.7, $\pi^{\frac{q-1}{2}} \equiv \Psi_q(d)\Psi_q(ad-bc)\ mod(q)$. Et, par le Lemme 6.1.8, en prenant c comme désiré pour appliquer la formule, on a $\Psi_q(d) = (-1)^{\frac{q-1}{4}}$.
En rassemblant ces égalités et ces congruences, et en utilisant le module et le fait que $q \geq 3$, on conclut que $\chi_\pi(q)\,\chi_\lambda(p) = (-1)^{\frac{q-1}{4}}\Psi_q(ad-bc)$. □

Exemple :
On étudie le cas $p = 13$ et $q = 17$:
Alors $a = 3, b = 2, c = 1$ et $d = 4$. Donc $ad-bc = 10$ et $(\frac{10}{17}) = (\frac{2}{17})(\frac{5}{17}) = 1 \times (\frac{5}{17}) = (\frac{17}{5}) = (\frac{2}{5}) = -1$.
On a donc que $\Psi_q(ad-bc) = -1$.De plus, $(-1)^{\frac{q-1}{4}} = (-1)^4 = 1$.
Et, $13^{\frac{17-1}{4}} \equiv (-4)^4 \equiv (-1)^2 \equiv 1\ mod(17)$ donc 13 est une puissance quatrième modulo 17, et donc $\chi_{c+id}(p) = 1$.
D'autre part, $17^{\frac{13-1}{4}} \equiv 4^3 \equiv 12 \equiv -1\ mod(13)$, donc 17 n'est pas une puissance quatrième modulo 13, et donc $\chi_{a+ib}(q) = -1$.
On retrouve la formule du Théorème 6.1.9.

6.2 Le caractère biquadratique de 2

Soit p un entier premier positif, $p \equiv 1\ mod(4)$, et π primaire irréductible avec $p = \pi\overline{\pi}$, $\pi = a + ib$, a impair et b pair.
On va étudier sous quelle condition 2 est une puissance quatrième modulo p.
On commence par remarquer que puisque p est premier, a et b sont tous les deux non nuls, et donc $pgcd(a, b) = 1$ (car π irréductible).

Lemme 6.2.1. *On a* $\chi_p(1+i) = i^{\frac{p-1}{4}}$.

Démonstration. $\overline{\chi_p(1+i)} = \chi_\pi(1+i)\,\chi_{\overline{\pi}}(1+i)$.
Or, $\chi_{\overline{\pi}}(1+i) = \overline{\chi_\pi(1-i)} = \chi_\pi(1-i)^3$ car χ_π est à valeurs dans le sous-groupe engendré par la classe de i (d'ordre 4) dans $D/\pi D$.
Ainsi, $\chi_p(1+i) = \chi_\pi((1+i)(1-i)^3) = \chi_\pi(2(-2i)) = \chi_\pi(-4)\,\chi_\pi(i)$.
Or, $-4 = (1+i)^4$ donc $\chi_\pi(-4) = 1$ et $\chi_\pi(i) = i^{\frac{p-1}{4}}$ par définition. □

Lemme 6.2.2. *Soit q un entier positif premier, $q \equiv 3\ mod(4)$.*
Alors $\chi_q(1+i) = (-i)^{\frac{q+1}{4}} = i^{\frac{-q-1}{4}}$.

Démonstration. D'après le Lemme 5.2.4, q est irréductible, donc $\chi_q(1+i) \equiv (1+i)^{\frac{q^2-1}{4}} \equiv ((1+i)^{q-1})^{\frac{q+1}{4}}\ mod(4)$.
De plus, $(1+i)^q \equiv 1 + i^q\ mod(q)$ par Frobenius, et $q \equiv 3\ mod(4)$, donc $(1+i)^q \equiv 1 - i\ mod(q)$, donc $(1+i)((1+i)^{q-1} + i) \equiv 0 mod(q)$.
Et puisque $1+i$ est un irréductible qui ne divise pas q, on obtient $(1+i)^{q-1} \equiv -i\ mod(q)$.
Et donc $(1+i)^{\frac{q^2-1}{4}} \equiv (-i)^{\frac{q+1}{4}}\ mod(q)$.
La dernière égalité du Lemme s'obtient en remarquant que $-i = i^{-1}$. □

Lemme 6.2.3. *Si $n \neq 1$, $n \equiv 1\ mod(4)$, alors* $\chi_n(1+i) = i^{\frac{n-1}{4}}$.

Démonstration. On écrit $n = p_1...p_r(-q_1)...(-q_s)$, où les p_i sont premiers positifs congrus à 1 modulo 4 et les q_j sont premiers positifs congrus à 3 modulo 4 (nombre pair de q_j si, et seulement si, a positif).
On a $\chi_a(1+i) = \chi_{p_1}(1+i)...\chi_{p_r}(1+i)\chi_{-q_1}(1+i)...\chi_{-q_s}(1+i)$.
Par le Lemme 6.2.1, pour tout j, $\chi_{p_j}(1+i) = i^{\frac{p_j-1}{4}}$.

De plus, pour tout k, $\chi_{-q_k}(1+i) = \chi_{q_k}(1+i) = i^{\frac{-q_k-1}{4}}$ par le Lemme 6.2.2.
Donc $\chi_n(1+i) = i^{\frac{p_1-1}{4}+...+\frac{p_r-1}{4}+\frac{-q_1-1}{4}+...+\frac{-q_s-1}{4}}$.
Et, par le Lemme 5.3.10, $\frac{p_1-1}{4} + ... + \frac{p_r-1}{4} + \frac{-q_1-1}{4} + ... + \frac{-q_s-1}{4} \equiv \frac{p_1...p_r(-q_1)...(-q_s)-1}{4} \equiv \frac{n-1}{4}$.

□

Lemme 6.2.4.
a) Si $\pi \equiv 1\ mod(4)$, alors $\chi_\pi(a) = i^{\frac{a-1}{2}}$.
b) Si $\pi \equiv 3+2i\ mod(4)$, alors $\chi_\pi(a) = -i^{\frac{-a-1}{2}}$.

Démonstration.
a) Si $\pi \equiv 1\ mod(4)$, $a \equiv 1\ mod(4)$ et $b \equiv 0\ mod(4)$.
On commence par remarquer que si $a = 1$, l'égalité est vraie.
Si $a \neq 1$:

$$\begin{aligned}\text{Donc, on a } \chi_\pi(a) &= \chi_a(p) \text{ par la Proposition 5.4.13}\\ &= \chi_a(ib)\\ &= \chi_a(i)\chi_a(b)\\ &= \chi_a(i) \text{ d'après la Proposition 5.3.9}\\ &= i^{\frac{a-1}{2}} \text{ d'après la Proposition 5.3.11}\end{aligned}$$

b) Si $\pi \equiv 3+2i\ mod(4), a \equiv 3\ mod(4)$ et $b \equiv 2\ mod(4)$.
Si $a \neq -1$:
$\chi_\pi(a) = \chi_\pi(-1)\,\chi_\pi(-a) = (-1)^{\frac{a-1}{2}} i^{\frac{-a-1}{2}}$ par le point d) de la Proposition 5.3.6 et le même raisonnement qu'au calcul précédent puisque $-a \equiv 1\ mod(4)$.
Or, $a \equiv 3\ mod(4)$, donc $(-1)^{\frac{a-1}{2}} = -1$, et donc $\chi_\pi(a) = -i^{\frac{1-1}{2}}$.

Si $a = -1$:
Par le point d) de la Proposition 5.3.6, $\chi_\pi(-1) = -1 = -i^{\frac{-a-1}{2}}$. □

Lemme 6.2.5. *On a $\chi_\pi(a)\,\chi_\pi(1+i) = i^{\frac{3(a+b-1)}{4}}$.*

Démonstration. Si $a + b \neq 1$:

$$\begin{aligned}\chi_\pi(a)\,\chi_\pi(1+i) &= \chi_\pi(a(1+i))\\ &= \chi_\pi(a+b+i\pi)\\ &= \chi_\pi(a+b)\\ &= \chi_{a+b}(\pi) \text{ par la Proposition 5.4.13 car } a+b \equiv 1\ mod(4)\\ &= \chi_{a+b}(a+ib)\\ &= \chi_{a+b}(i^3 a(1+i))\\ &= \chi_{a+b}(i)^3\chi_{a+b}(a)\chi_{a+b}(1+i)\\ &= \chi_{a+b}(i)^3\chi_{a+b}(1+i) \text{ par la Proposition 5.3.9 car } pgcd(a+b,b) = 1 \text{ et } a+b \text{ impair}\\ &= i^{3\frac{a+b-1}{2}} i^{\frac{a+b-1}{4}} \text{ en utilisant la Prop 5.3.11 et le Lemme 6.2.3}\\ &= i^{a+b-1+3\frac{a+b-1}{4}}\\ &= i^{\frac{3(a+b-1)}{4}} \text{ car } a+b-1 \equiv 0\ mod(4).\end{aligned}$$

Si $a + b = 1$, les 3 premières égalités restent vraies, et on trouve $\chi_\pi(a)\,\chi_\pi(1+i) = 1 = i^{3\frac{a+b-1}{4}}$. □

Lemme 6.2.6. *On a* $\chi_\pi(1+i) = i^{\frac{a-b-b^2-1}{4}}$.

Démonstration. Par le Lemme 6.2.5, $\chi_\pi(1+i)\,\chi_\pi(a) = i^{3\frac{a+b-1}{4}}$.
Si $\pi \equiv 1\ mod(4)$:
D'après le Lemme 6.2.4, $\chi_\pi(a) = i^{\frac{a-1}{2}}$, donc

$$\begin{aligned}\chi_\pi(1+i) &= i^{3\frac{a+b-1}{4} - \frac{a-1}{2}} \\ &= i^{\frac{3b+a-1}{4}} \\ &= i^{\frac{4b+b^2}{4}} i^{\frac{a-b^2-b-1}{4}} \\ &= i^{\frac{a-b^2-b-1}{4}} \text{ car } b \equiv 0\ mod(4) \text{ donc } b^2 \equiv 0\ mod(16).\end{aligned}$$

Si $\pi \equiv 3+2i\ mod(4)$:
D'après le Lemme 6.2.4, $\chi_\pi(a) = -i^{\frac{-a-1}{2}}$, donc

$$\begin{aligned}\chi_\pi(1+i) &= -i^{3\frac{a+b-1}{4} - \frac{-a-1}{2}} \\ &= -i^{a+\frac{4b+b^2}{4}} i^{\frac{a-b^2-b-1}{4}}.\end{aligned}$$

Or, $a \equiv 3\ mod(4), b \equiv 2\ mod(4)$, donc $4b \equiv 8\ mod(16)$ et $b^2 \equiv 4\ mod(16)$, donc $-i^{a+\frac{4b+b^2}{4}} = 1$.
Donc $\chi_\pi(1+i) = i^{\frac{a-b^2-b-1}{4}}$. □

Théorème 6.2.7. *Soit p premier positif tel que* $p \equiv 1\ mod(4)$
2 est un résidu biquadratique modulo p si, et seulement si, p s'écrit sous la forme $p = X^2 + 64Y^2, X, Y \in \mathbb{Z}$.

Démonstration. Par le Lemme 6.1.1, 2 est un résidu biquadratique modulo p si, et seulement si, $\chi_\pi(2) = 1$. Or, $2 = i^3(1+i)^2$, donc $\chi_\pi(2) = \chi_\pi(i)^3\,\chi_\pi(1+i)^2 = i^{\frac{2-2a-b-b^2}{2}} (= i^{1-a-\frac{b(b+1)}{2}})$ en utilisant le Lemme 6.2.6.
Pour conclure, il nous reste à montrer que $1 - a - \frac{b(b+1)}{2} \equiv 0\ mod(4)$ si, et seulement si, 8 divise b.
Supposons que 8 divise b.
En reprenant les étapes de la congruence du Lemme 5.2.8, on a qu'il existe x et y entiers tels que $a+b = 1+4x$ et $a-b = 1-4y$. Alors, par des calculs sur ces deux équations, on obtient $a-1 = 2(x-y)$ et $b = 2(x+y)$. Alors, puisque 8 divise b, on a forcément que 4 divise $x+y$. De plus, $x-y = x+y-2y$, donc $a-1 = 2(x+y) - 4y \equiv 0\ mod(4)$ car $x-y$ pair et $x+y$ et $x-y$ ont même parité.
Et puisque $b \equiv 0\ mod(8)$ par hypothèse, $\frac{b}{2} \equiv 0\ mod(4)$, et donc $1 - a - \frac{b(b+1)}{2} \equiv 0\ mod(4)$.
Supposons maintenant que $1 - a - \frac{b(b+1)}{2} \equiv 0\ mod(4)$.
On remarque par des calculs simples que, quelles que soient les congruences de a et b modulo 4 données par le Lemme 5.2.8, $1 - a - \frac{b^2}{2} \equiv 0\ mod(4)$.
Donc, par hypothèse, $-\frac{b}{2} \equiv 0\ mod(4)$, et donc 8 divise b.

□

7 Bibliographie

[1] K. Ireland- M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1990

[2] C.F. Gauss *Untersuchungen über höhere Arithmetik*

[3] G. Eisenstein, *Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste* . Crelle's J. 28 (1844) 223-245.

[4] A. Weil. *Number of solutions of equations in a finite field.* Bull. Am. Math. Soc., 55 (1949), 497-508.

[5] K. Burde. *Ein rationales biquadratisches Reciprozitatsgesetz.* J . Reine und Angew. Math .. 235 (1969),175-184 .

[6] P. Boyer *Petit compagnon des nombres et de leurs applications* , Calvage et Mounet, 2019