La congruence $-J(\chi_3,\chi_3)\equiv 1 \bmod 3$ dans $\mathbb{Z}[j]$

On rappelle que la somme de Jacobi $J(\chi,\chi')$ de deux caractères multiplicatifs $\chi,\chi' : \mathbf{k}^* \to \mathbb{U}_3$ est définie par :

$$J(\chi,\chi') = \sum_{x+y=1} \chi(x)\chi'(y) = \sum_{x+y=1} \chi(x)\chi'(1-x)$$

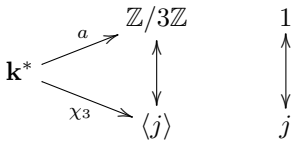
avec les conventions (que l'on connaît) de prolongement des caractères en 0.

La preuve qui suit est dûe à Weil, point 10, page 254, de "La cyclotomie jadis et naguère", exposé au séminaire Bourbaki, Paris, Juin 1974.

Lemme 1.
Soit $\mathbf{k}$ *un corps fini de cardinal* $q\equiv 1 \bmod 3$ *et* $\chi_3 : \mathbf{k}^* \to \mathbb{U}_3 = \langle j\rangle$ *un caractère d'ordre 3. Alors :*

$$\boxed{-J(\chi_3,\chi_3)\equiv 1 \bmod 3 \text{ dans } \mathbb{Z}[j]}$$

Preuve.
A l'arrivée, tout se passe dans $\mathbb{Z}[j]$.
On écrit $\chi_3(x) = j^{a(x)}$ avec $a(x)\in\mathbb{Z}$ déterminé modulo 3



On pose $\rho = j-1$ qui vérifie, puisque $(j-1)(j^2-1)=3$, l'égalité $-\rho^2 j^2 = 3$, donc

$$\rho^2 \equiv 0 \bmod 3$$

Alors, puisque $\rho^2\equiv 0 \bmod 3$:

$$j^a = (1+\rho)^a \equiv 1 + a\rho \bmod 3$$

En conséquence :

$$\chi_3(x)\equiv 1+\rho a(x) \bmod 3, \qquad \chi_3(1-x)\equiv 1+\rho a(1-x) \bmod 3$$

Et donc, en faisant le produit et en utilisant encore $\rho^2\equiv 0 \bmod 3$:

$$\chi_3(x)\chi_3(1-x)\equiv 1+\rho a(x)+\rho a(1-x) \bmod 3$$

En sommant :

$$(\star) \qquad J(\chi_3,\chi_3) \overset{\text{def.}}{=} \sum_{\substack{x\in\mathbf{k}\\ x\neq 0,1}} \chi_3(x)\chi_3(1-x) = (q-2) + \rho \sum_{\substack{x\in\mathbf{k}\\ x\neq 0,1}} a(x) + \rho \sum_{\substack{x\in\mathbf{k}\\ x\neq 0,1}} a(1-x)$$

Le $q-2$, c'est 1 que l'on sommé sur $\mathbf{k}\setminus\{0,1\}$.
Je dis que :

$$\sum_{\substack{x\in\mathbf{k}\\ x\neq 0,1}} a(x) \equiv 0 \bmod 3$$

Pour le voir, on regroupe x et x^{-1} ; pour $x\neq -1$, on utilise $a(x)+a(x^{-1})\equiv 0 \bmod 3$, dûe à l'égalité $\chi_3(x)\chi_3(x^{-1})=1$. Et pour $x=-1$, seule valeur pour laquelle on a $x=x^{-1}$, on a $a(-1)=0$ puisque -1 est un cube.
De la même manière :

$$\sum_{\substack{x\in\mathbf{k}\\ x\neq 0,1}} a(1-x) \equiv 0 \bmod 3$$

La somme $J(\chi_3,\chi_3)$ de $(\star)$ vérifie donc la conguence :

$$\sum_{\substack{x\in\mathbf{k}\\ x\neq 0,1}} \chi_3(x)\chi_3(1-x) \equiv q-2 \mod 3$$

Mais $q\equiv 1 \bmod 3$, donc $q-2\equiv -1 \bmod 3$. Bilan :

$$J(\chi_3,\chi_3)\equiv -1 \mod 3$$

ce qu'il fallait démontrer. □