СУМИ НА ГАУС. КВАДРАТИЧЕН ЗАКОН ЗА РЕЦИПРОЧНОСТ.

1. Квадратични остатъци. Символ на Льожандър.

Дефиниция 1.1 (Квадратични остатъци)**.** Цялото число a се нарича квадратичен остатък (съотв. неостатък) по модул простото число p, когато сравнението $x^2 \equiv a \mod p$ има решение (съотв. няма решение).

Тъй като случаят $p = 2$ е тривиален, от тук нататък ще разглеждаме само нечетни прости числа.

Сравнението $x^2 \equiv a \mod p$ е еквивалентно на уравнението $x^2 = \overline{a}$ в крайното поле $\mathbb{Z}_p$, където $\overline{a}$ е образът на a при естествения хомоморфизъм $\mathbb{Z} \to \mathbb{Z}_p$. Ако a не се дели на p, то a е квадратичен остатък, точно когато $\overline{a} \neq 0$ е квадрат в мултипликативната група $\mathbb{Z}_p^*$ на полето $\mathbb{Z}_p$ (т. е. $\overline{a} = x^2$ за някой $x \in \mathbb{Z}_p^*$). Да забележим, че ядрото на хомоморфизмът $\mathbb{Z}_p^* \to \mathbb{Z}_p^*$, който е определен с $x \mapsto x^2$, е подгрупата $\{1, -1\}$, защото 1 и -1 са единствените решения на уравнението $x^2 = 1$ в полето $\mathbb{Z}_p$. Тъй като образът на този хомоморфизъм е подгрупата на всички квадрати в $\mathbb{Z}_p^*$, броят на класовете квадратични остатъци a, такива че $a \not\equiv 0 \mod p$, е равен на $(p-1)/2$.

За всяко число a, което не се дели на p, *символът на Льожандър*

$$\left(\frac{a}{p}\right) \in \{1, -1\}$$

се дефинира както следва:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{когато } a \text{ е квадратичен остатък по модул } p. \\ -1 & \text{когато } a \text{ е квадратичен неостатък по модул } p. \end{cases}$$

Когато a се дели на p, сравнението $x^2 \equiv a \mod p$ има решение, но в този случай правилното определение на символа на Льожандър е $\left(\frac{a}{p}\right) = 0$.

Твърдение 1.1 (Критерий на Ойлер)**.** $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$.

Доказателство. Твърдението е очевидно, когато $a \equiv 0 \mod p$. Когато $a \not\equiv 0 \mod p$, трябва да докажем, че ако a е квадратичен остатък (съотв. квадратичен неостатък), то $a^{(p-1)/2} \equiv 1 \mod p$ (съотв. $a^{(p-1)/2} \equiv -1 \mod p$). Ще докажем твърдението в следната еквивалентна форма: $x \in \mathbb{Z}_p^*$ е квадрат в $\mathbb{Z}_p^*$ точно когато $x^{(p-1)/2} = 1$.

Тъй като $x^{p-1} = 1$ за всеки $x \in \mathbb{Z}_p^*$, то

$$(x^{(p-1)/2})^2 = x^{p-1} = 1$$

за всеки $x \in \mathbb{Z}_p^*$. Следователно $x^{(p-1)/2} = \pm 1$ за всеки $x \in \mathbb{Z}_p^*$, защото 1 и -1 са единствените решения на уравнението $u^2 = 1$ в полето $\mathbb{Z}_p$. Ако $x = y^2$ е квадрат в $\mathbb{Z}_p^*$, то $x^{(p-1)/2} = (y^2)^{(p-1)/2} = y^{p-1} = 1$, което показва, че всеки квадрат в $\mathbb{Z}_p^*$ е решение на уравнението $x^{(p-1)/2} = 1$. Тъй като това уравнение има най-много $(p-1)/2$ решения в $\mathbb{Z}_p$, а броят на всички квадрати в $\mathbb{Z}_p^*$ е $(p-1)/2$, то решенията на това уравнение са точно всички квадрати в $\mathbb{Z}_p^*$. □

Твърдение 1.2 (Мултипликативност на символа на Льожандър)**.** *Ако a и b са цели числа, то*

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

Доказателство. От критерия на Ойлер следва, че

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

Тъй като двете страни на горното сравнение са равни на ± 1, те съвпадат, защото простото число p е нечетно. □

2. Адитивни характери на $\mathbb{Z}_p$

Дефиниция 2.1. Изображението $\psi : \mathbb{Z}_p \to \mathbb{C}^*$ се нарича *адитивен характер* на $\mathbb{Z}_p$, ако $\psi(x+y) = \psi(x)\psi(y)$ за всички $a, b \in \mathbb{Z}_p$.

Адитивните характери на $\mathbb{Z}_p$ са точно хомоморфизмите от адитивната група на $\mathbb{Z}_p$ в мултипликативната група на полето на комплексните числа. В частност, $\psi(0) = 1$ и $\psi(k \cdot x) = \psi(x)^k$, $x \in \mathbb{Z}_p$, $k \in \mathbb{Z}$.

За всеки $x \in \mathbb{Z}_p$, комплексното число $\psi(x)$ е корен на единицата от степен p, защото $\psi(x)^p = \psi(p \cdot x) = \psi(0) = 1$. Ако $x \in \mathbb{Z}_p$ и n е цяло число, такова че $\overline{n} = x$, то

$$\psi(x) = \psi(\overline{n}) = \psi(n \cdot 1) = \psi(1)^n.$$

Следователно всеки адитивен характер ψ на $\mathbb{Z}_p$ е напълно определен от комплексното число $\psi(1)$, което е корен на единицата от степен p. Тъй като корените на единицата от степен p са точно p на брой, съществуват p на брой различни адитивни характери на $\mathbb{Z}_p$.

Нека $\omega = \cos\dfrac{2\pi}{p} + i\sin\dfrac{2\pi}{p}$. Тогава степените ω^a, $a \in \mathbb{Z}$, изчерпват корените на единицата от степен p, като $\omega^a = \omega^b$ точно когато $a \equiv b \mod p$. Да означим с ψ_a единственият адитивен характер, такъв че $\psi_a(1) = \omega^{-a}$. В явен вид

$$\psi_a(\overline{n}) = \omega^{-an}, \qquad n \in \mathbb{Z}.$$

Ясно е, че $\psi_a = \psi_b$, когато $a \equiv b \mod p$. Това ни позволява да определим коректно ψ_x за всеки $x \in \mathbb{Z}_p$ по следния начин: $\psi_x = \psi_a$, където a е цяло число, такова че $\overline{a} = x$.

Ако ψ е характер на $\mathbb{Z}_p$, изображението $\overline{\psi} : \mathbb{Z}_p \to \mathbb{C}^*$, което е определено с $\overline{\psi}(x) = \overline{\psi(x)}$, $x \in \mathbb{Z}_p$, също е характер на $\mathbb{Z}_p$, който се нарича *спрегнат характер* на ψ. От $\overline{\omega} = \omega^{-1}$, следва че $\overline{\psi_a} = \psi_{-a}$, $n \in \mathbb{Z}$, и $\overline{\psi_x} = \psi_{-x}$, $x \in \mathbb{Z}_p$.

Характерът ψ_0 се нарича единичен характер:

$$\psi_0(x) = 1 \text{ за всеки } x \in \mathbb{Z}_p.$$

Когато няма опасност от недоразумение, ще означаваме характера ψ_0 с 1.

Ако ψ_1 и ψ_2 са адитивни характери на $\mathbb{Z}_p$, то изображението $\psi_1\psi_2 : \mathbb{Z}_p \to \mathbb{C}^*$, което е определено с $(\psi_1\psi_2)(x) = \psi_1(x)\psi_2(x)$, $x \in \mathbb{Z}_p$, също е характер на $\mathbb{Z}_p$, който се нарича *произведение* на характерите ψ_1 и ψ_2. Не е трудно да се види, че тази дефиниция превръща множеството на всички характери в абелева група, която се нарича *група на адитивните характери* на $\mathbb{Z}_p$.

Твърдение 2.1. *Групата на адитивните характери на $\mathbb{Z}_p$ е изоморфна на групата $\mathbb{Z}_p$.*

Доказателство. Тъждеството

$$\psi_a(\overline{n})\psi_b(\overline{n}) = \omega^{-an}\omega^{-bn} = \omega^{-(a+b)n} = \psi_{a+b}(\overline{n}), \qquad a, b, n \in \mathbb{Z},$$

показва, че $\psi_a\psi_b = \psi_{a+b}$, откъдето $\psi_x\psi_y = \psi_{x+y}$ за всички $x, y \in \mathbb{Z}_p$. Сега не е трудно да се провери, че изображението $x \mapsto \psi_x$ е изоморфизъм на $\mathbb{Z}_p$ и групата на адитивните характери на $\mathbb{Z}_p$. □

Лема 2.2. *Ако $\psi \neq 1$ е адитивен характер на $\mathbb{Z}_p$, то*

$$\sum_{t\in\mathbb{Z}_p} \psi(t) = 0.$$

Ако $\psi = 1$, то

$$\sum_{t\in\mathbb{Z}_p} \psi(t) = p.$$

Доказателство. Да забележим, че изображението $\mathbb{Z}_p \to \mathbb{Z}_p$, $t \mapsto t+1$, е биекция. Следователно

$$\sum_{t\in\mathbb{Z}_p} \psi(t) = \sum_{t\in\mathbb{Z}_p} \psi(t+1) = \sum_{t\in\mathbb{Z}_p} \psi(t)\psi(1) = \psi(1)\sum_{t\in\mathbb{Z}_p} \psi(t).$$

Ако $\psi \neq 1$, то $\psi(1) \neq 1$, откъдето следва първото тъждество. Второто тъждество е тривиално. □

Да означим с V_p множеството на всички изображения от $\mathbb{Z}_p$ в полето на комплексните числа. Множеството V_p има естествена структура на линейно пространство над полето на комплексните числа — ако $f : \mathbb{Z}_p \to \mathbb{C}$ и $g : \mathbb{Z}_p \to \mathbb{C}$ са две такива изображения, то

$$(f+g)(x) = f(x) + g(x) \qquad (\alpha f)(x) = \alpha f(x) \qquad \alpha \in \mathbb{C},\ x \in \mathbb{Z}_p.$$

Тъй като изображението $V_p \to \mathbb{C}_p$, зададено с $f \mapsto (f(\overline{1}), \ldots, f(\overline{p}))$, е изоморфизъм на линейни пространства над $\mathbb{C}$, линейното пространство V_p има размерност p над полето на комплексните числа.

В линейното пространство V_p се въвежда ермитово скаларно произведение по следния начин:

$$\langle f, g\rangle = \sum_{t\in\mathbb{Z}_p} f(t)\overline{g(t)}.$$

Лема 2.3 (Ортогоналност на характерите)**.** *Множеството от всички адитивни характери $\{\psi_x\}_{x\in\mathbb{Z}_p}$ на $\mathbb{Z}_p$ е ортогонален базис на V_p.*

Доказателство. От определението на ермитовото скаларно произведение във V_p и доказателството на Твърдение 2.1 следва, че

$$\langle \psi_x, \psi_y\rangle = \sum_{t\in\mathbb{Z}_p} \psi_x(t)\overline{\psi_y(t)} = \sum_{t\in\mathbb{Z}_p} \psi_x(t)\psi_{-y}(t) = \sum_{t\in\mathbb{Z}_p} \psi_{x-y}(t).$$

Сега твърдението следва от Лема 2.2. □

От Лема 2.2 също така следва, че $\|\chi_x\|^2 = \langle \psi_x, \psi_x\rangle = p$ за всеки $x \in \mathbb{Z}_p$.

От горната лема незабавно получаваме

Твърдение 2.4. *Ако $f \in V_p$ е изображение от $\mathbb{Z}_p$ в $\mathbb{C}$, то*

$$f = \sum_{x\in\mathbb{Z}_p} \frac{\langle f, \psi_x\rangle}{p}\,\psi_x \quad \textit{и} \quad p\|f\|^2 = \sum_{x\in\mathbb{Z}_p} |\langle f, \psi_x\rangle|^2.$$

Доказателство. Наистина, ако $f = \sum_{x \in \mathbb{Z}_p} \lambda_x \psi_x$, то $\langle f, \psi_x \rangle = \lambda_x \langle \psi_x, \psi_x \rangle$, откъдето

$$\lambda_x = \frac{\langle f, \psi_x \rangle}{\langle \psi_x, \psi_x \rangle} = \frac{\langle f, \psi_x \rangle}{p}.$$

От ортогоналността на системата от вектори $\{\psi_x\}_{x \in \mathbb{Z}_p}$ следва тъждеството

$$\|f\|^2 = \sum_{x \in \mathbb{Z}_p} |\lambda_x|^2 \|\psi_x\|^2,$$

което незабавно води до втората формула. □

3. Мултипликативни характери на $\mathbb{Z}_p$

Дефиниция 3.1. Изображението $\chi : \mathbb{Z}_p^* \to \mathbb{C}^*$ се нарича *мултипликативен характер* на $\mathbb{Z}_p$, когато $\chi(xy) = \chi(x)\chi(y)$ за всички $x, y \in \mathbb{Z}_p^*$.

Мултипликативните характери на $\mathbb{Z}_p$ са точно хомоморфизмите от мултипликативната група на полето $\mathbb{Z}_p$ в мултипликативната група на полето на комплексните числа. Целесъобразно е всеки мултипликативен характер χ на $\mathbb{Z}_p$ да се продължи до изображение от $\mathbb{Z}_p$ в $\mathbb{C}$, като се положи $\chi(0) = 0$. Тогава $\chi(xy) = \chi(x)\chi(y)$ за всички $x, y \in \mathbb{Z}_p$.

Ако $t \in \mathbb{Z}_p^*$, комплексното число $\psi(t)$ е корен на единицата от степен $p-1$, защото $\chi(t)^{p-1} = \chi(t^{p-1}) = \chi(1) = 1$. Следователно $|\chi(t)| = 1$ за всеки $t \in \mathbb{Z}_p^*$. Това наблюдение ни позволява да пресметнем лесно дължината на всеки мултипликативен характер в ермитовото пространство V_p.

Лема 3.1. *Ако χ е мултипликативен характер на $\mathbb{Z}_p$, то $\|\chi\|^2 = p - 1$.*

Доказателство. От определението на ермитовото скаларно произведение в линейното пространство V_p следва, че

$$\|\chi\|^2 = \langle \chi, \chi \rangle = \sum_{t \in \mathbb{Z}_p} \chi(t)\overline{\chi(t)} = \sum_{t \in \mathbb{Z}_p} |\chi(t)|^2 .$$

Остава да забележим, че $\chi(0) = 0$ и $|\chi(t)|^2 = 1$, когато $t \neq 0$. □

Най-важният за нас мултипликативен характер на $\mathbb{Z}_p$ е индуциран от символа на Льожандър. Тъй като от $a \equiv b \mod p$ следва, че

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

то можем да асоциираме със символа на Льожандър мултипликативен характер χ на $\mathbb{Z}_p$ по следния начин:

$$\chi(x) = \left(\frac{a}{p}\right), \text{ където } a \text{ е цяло число, такова че } \overline{a} = x.$$

Твърдение 3.2. *Ако χ е мултипликативен характер на $\mathbb{Z}_p$, такъв че $\chi(x) \neq 1$ за някой $x \in \mathbb{Z}_p^*$, то*

$$\sum_{t \in \mathbb{Z}_p} \chi(t) = 0.$$

Доказателство. Да забележим, че за всяко $x \in \mathbb{Z}_p^*$, изображението $\mathbb{Z}_p \to \mathbb{Z}_p$, $t \mapsto xt$, е биекция на $\mathbb{Z}_p$. От това наблюдение следва, че

$$\sum_{t \in \mathbb{Z}_p} \chi(t) = \sum_{t \in \mathbb{Z}_p} \chi(xt) = \chi(x) \sum_{t \in \mathbb{Z}_p} \chi(t),$$

за всяко $x \in \mathbb{Z}_p^*$. Ако сега $\chi(x) \neq 1$ за някой $x \in \mathbb{Z}_p^*$, то от горното тъждество получаваме незабавно, че $\sum_{t \in \mathbb{Z}_p} \chi(t) = 0$. □

Твърдение 3.2 показва, че $\sum_{a=0}^{p-1}\left(\frac{a}{p}\right)=0$. Последното тъждество също така следва директно от факта, че подгрупата на квадратите в $\mathbb{Z}_p^*$ има индекс 2.

4. Суми на Гаус

Нека χ е мултипликативен характер на $\mathbb{Z}_p$. За всяко цяло число $a\in\mathbb{Z}$ *сумата на Гаус* $\tau_a(\chi)$ се определя по следния начин:

$$\tau_a(\chi)=\sum_{t\in\mathbb{Z}_p}\chi(t)\omega^{at}=\langle\chi,\psi_a\rangle.$$

Ако $\chi=\sum_{x\in\mathbb{Z}_p}\lambda_x\psi_x$, то според Лема 2.4 $\lambda_{\overline{a}}=\dfrac{\tau_a(\chi)}{p}$ и $p\|\chi\|^2=\sum_{a=0}^{p-1}|\tau_a(\chi)|^2$. От последното равенство и от $\|\chi\|^2=p-1$ (вж. Лема 3.1) получаваме тъждеството

$$\sum_{a=0}^{p-1}|\tau_a(\chi)|^2=p(p-1).$$

Лема 4.1. *Ако χ е мултипликативен характер на $\mathbb{Z}_p$, такъв че $\chi(x)\neq 1$ за някой $x\in\mathbb{Z}_p^*$, то $\tau_0(\chi)=0$.*

Доказателство. Следва непосредствено от определението на сумата на Гаус и Твърдение 3.2. □

Лема 4.2. *Ако цялото число $a\in\mathbb{Z}$ не се дели на p, то $\chi(\overline{a})\tau_a(\chi)=\tau_1(\chi)$ и $|\tau_a(\chi)|=|\tau_1(\chi)|$.*

Доказателство. Тъй като $\overline{a}\neq 0$, изображението $\mathbb{Z}_p\to\mathbb{Z}_p$, $t\mapsto at$, е биекция, откъдето $\sum_{t\in\mathbb{Z}_p}\chi(t)\omega^t=\sum_{t\in\mathbb{Z}_p}\chi(at)\omega^{at}$. Следователно

$$\begin{aligned}\tau_1(\chi)&=\sum_{t\in\mathbb{Z}_p}\chi(t)\omega^t=\sum_{t\in\mathbb{Z}_p}\chi(at)\omega^{at}=\sum_{t\in\mathbb{Z}_p}\chi(\overline{a})\chi(t)\omega^{at}=\\&=\chi(\overline{a})\sum_{t\in\mathbb{Z}_p}\chi(t)\omega^{at}=\chi(\overline{a})\tau_a(\chi).\end{aligned}$$

За доказателството на второто равенство използваме, че $|\chi(\overline{a})|=1$. □

Твърдение 4.3. *Ако цялото число $a\in\mathbb{Z}$ не се дели на p, а χ е мултипликативен характер на групата $\mathbb{Z}_p^*$, такъв че $\chi(x)\neq 1$ за някой $x\in\mathbb{Z}_p^*$, то*

$$|\tau_a(\chi)|^2=p.$$

Доказателство. Предишната лема показва, че $|\tau_a(\chi)|=|\tau_b(\chi)|$, когато целите числа a и b не се делят на p. Сега от $\tau_0(\chi)=0$ и $\sum_{a=0}^{p-1}|\tau_a(\chi)|^2=p(p-1)$ следва, че $(p-1)\,|\tau_a(\chi)|^2=p(p-1)$, откъдето $|\tau_a(\chi)|^2=p$. □

За всеки мултипликативен характер χ на $\mathbb{Z}_p$ определяме *спрегнатия характер* $\overline{\chi}$ на χ с формулата

$$\overline{\chi}(x)=\overline{\chi(x)},\qquad x\in\mathbb{Z}_p.$$

Ако $\chi=\sum_{x\in\mathbb{Z}_p}\lambda_x\psi_x$, то

$$\overline{\chi}=\sum_{x\in\mathbb{Z}_p}\overline{\lambda_x}\,\overline{\psi_x}=\sum_{x\in\mathbb{Z}_p}\overline{\lambda_x}\,\psi_{-x}=\sum_{x\in\mathbb{Z}_p}\overline{\lambda_{-x}}\,\psi_x.$$

Тъй като за всяко цяло число a и всеки мултипликативен характер χ на $\mathbb{Z}_p$ е в сила $\lambda_{\overline{a}} = \dfrac{\tau_a(\chi)}{p}$, от последното представяне следва, че

$$\tau_a(\overline{\chi}) = p\,\overline{\lambda_{-\overline{a}}} = \overline{\tau_{-a}(\chi)}, \qquad a \in \mathbb{Z}_p.$$

Сега да забележим, че съгласно Лема 4.2

$$\chi(-\overline{a})\tau_{-a}(\chi) = \tau_1(\chi) = \chi(\overline{a})\tau_a(\chi)$$

когато a не се дели на p. Тъй като $\chi(-\overline{a}) = \chi(-1)\chi(\overline{a})$, то $\tau_{-a}(\chi) = \chi(-1)\tau_a(\chi)$ за всяко a, което не се дели на p. Да забележим също, че $\chi(-1) = \pm 1$, защото $\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1$. Окончателно получаваме

Твърдение 4.4. *Ако цялото число $a \in \mathbb{Z}$ не се дели на p, то*

$$\tau_a(\overline{\chi}) = \chi(-1)\,\overline{\tau_a(\chi)}.$$

Нека сега $\chi : \mathbb{Z}_p \to \mathbb{C}$ е мултипликативният характер на $\mathbb{Z}_p$, който е асоцииран със символа на Льожандър. Тогава $\overline{\chi} = \chi$, откъдето

$$\tau_a(\chi) = \chi(-1)\,\overline{\tau_a(\chi)} = \left(\frac{-1}{p}\right)\overline{\tau_a(\chi)}$$

за всяко цяло число a, което не се дели на p.

Теорема 4.5. *Ако цялото число $a \in \mathbb{Z}$ не се дели на p, а $\chi : \mathbb{Z}_p \to \mathbb{C}$ е мултипликативният характер на $\mathbb{Z}_p$, който е асоцииран със символа на Льожандър, то*

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

Доказателство. От тъждеството $\tau_a(\chi) = \left(\dfrac{-1}{p}\right)\overline{\tau_a(\chi)}$ следва, че

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

Тъй като $|\tau_a(\chi)|^2 = p$, съгласно Твърдение 4.3, доказателството е завършено. □

5. Квадратичен закон за реципрочност

В този параграф ще означаваме с χ мултипликативния характер на $\mathbb{Z}_p$, който е асоцииран със символа на Льожандър:

$$\chi(\overline{a}) = \left(\frac{a}{p}\right), \qquad a \in \mathbb{Z}.$$

Сумата на Гаус $\tau_1(\chi)$ ще бъде означавана с τ:

$$\tau = \sum_{t \in \mathbb{Z}_p} \chi(t)\omega^t = \sum_{t \in \mathbb{Z}_p} \left(\frac{t}{p}\right)\omega^t.$$

Тъй като ω е цяло алгебрично число, сумата на Гаус τ също е цяло алгебрично число. Ясно е, че τ принадлежи на пръстена $R = \mathbb{Z}[\omega]$, който се състои от цели алгебрични числа. В доказателството на квадратичния закон за реципрочност ще използваме следната лема.

Лема 5.1. *Нека $n \neq 0$ е цяло число и нека a, b са цели числа, такива че $a \equiv b \mod nR$. Тогава $a \equiv b \mod n\mathbb{Z}$.*

Доказателство. Сравнението $a \equiv b \mod nR$ означава, че $(b-a)/n \in R$. Следователно $(b-a)/n$ е цяло алгебрично число. Но $(b-a)/n$ е също така рационално число, откъдето следва, че $(b-a)/n \in \mathbb{Z}$, т. е. $a \equiv b \mod n\mathbb{Z}$. □

Нека $p^* = \left(\frac{-1}{p}\right) p = (-1)^{(p-1)/2} p$. Тогава $\tau^2 = p^*$ според Теорема 4.5.

Теорема 5.2 (Квадратичен закон за реципрочност)**.** *Ако p и q са различни нечетни прости числа, то*

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Доказателство. Според критерия на Ойлер

$$\left(\frac{p^*}{q}\right) \equiv (p^*)^{(q-1)/2} = (\tau^2)^{(q-1)/2} = \tau^{q-1} \mod q\mathbb{Z}.$$

Умножавайки горното сравнение с τ, получаваме ново сравнение, този път в пръстена R:

$$\tau \left(\frac{p^*}{q}\right) \equiv \tau^q \mod qR.$$

Тъй като q е просто число, то

$$\tau^q = \Big(\sum_{t\in\mathbb{Z}_p} \chi(t)\omega^t\Big)^q \equiv \sum_{t\in\mathbb{Z}_p} \chi(t)^q\, \omega^{qt} \mod qR.$$

Да забележим, че $\chi(t)^q = \chi(t)$ за всеки $t \in \mathbb{Z}_p$, защото $\chi(t) \in \{0, \pm 1\}$ и q е нечетно число. Следователно

$$\tau^q \equiv \sum_{t\in\mathbb{Z}_p} \chi(t)^q\, \omega^{qt} \equiv \sum_{t\in\mathbb{Z}_p} \chi(t)\, \omega^{qt} = \tau_q(\chi) \mod qR.$$

Сега $\tau_q(\chi) = \chi(\overline{q})\tau_1(\chi) = \left(\frac{q}{p}\right)\tau$ съгласно Лема 4.2, откъдето

$$\tau \left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right)\tau \mod qR.$$

Умножавайки горното сравнение по τ, получаваме

$$p^* \left(\frac{p^*}{q}\right) \equiv p^* \left(\frac{q}{p}\right) \mod qR,$$

а тъй като p^* е обратим елемент по модул идеала qR (защо?), то окончателно

$$\left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right) \mod qR.$$

От последното сравнение и Лема 5.1 следва, че

$$\left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right) \mod q\mathbb{Z},$$

което директно влече $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$. □

От $p^* = (-1)^{(p-1)/2} p$ и мултипликативността на символа на Льожандър следва, че

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

Това ни води до обичайната формулировка на квадратичния закон за реципрочност:

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