Three proofs of quadratic reciprocity and their impact on twentieth century mathematics

Clemens Berger

Université Côte d'Azur

UGC Utrecht, January 16, 2024

Definition (Legendre symbol for odd prime p and coprime x)

$$\left(\frac{x}{p}\right) = \begin{cases} +1 & \text{if } x \text{ is a square in } \mathbb{F}_p^\times \\ -1 & \text{if } x \text{ is not a square in } \mathbb{F}_p^\times \end{cases}$$

Lemma (Euler's criterion)

$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ in $\mathbb{F}_p$ so that $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$ in $\mathbb{F}_p$.

Proof.

$X^{p-1} - 1 = (X^{\frac{p-1}{2}} + 1)(X^{\frac{p-1}{2}} - 1)$ in $\mathbb{F}_p[X]$. □

Definition (Legendre symbol for odd prime p and coprime x)

$$\left(\frac{x}{p}\right) = \begin{cases} +1 & \text{if } x \text{ is a square in } \mathbb{F}_p^\times \\ -1 & \text{if } x \text{ is not a square in } \mathbb{F}_p^\times \end{cases}$$

Lemma (Euler's criterion)

$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ in $\mathbb{F}_p$ so that $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$ in $\mathbb{F}_p$.

Proof.

$X^{p-1} - 1 = (X^{\frac{p-1}{2}} + 1)(X^{\frac{p-1}{2}} - 1)$ in $\mathbb{F}_p[X]$. □

Definition (Legendre symbol for odd prime p and coprime x)

$$\left(\frac{x}{p}\right) = \begin{cases} +1 & \text{if } x \text{ is a square in } \mathbb{F}_p^\times \\ -1 & \text{if } x \text{ is not a square in } \mathbb{F}_p^\times \end{cases}$$

Lemma (Euler's criterion)

$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ in $\mathbb{F}_p$ so that $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$ in $\mathbb{F}_p$.

Proof.

$X^{p-1} - 1 = (X^{\frac{p-1}{2}} + 1)(X^{\frac{p-1}{2}} - 1)$ in $\mathbb{F}_p[X]$. □

Definition (Legendre symbol for odd prime p and coprime x)

$$\left(\frac{x}{p}\right) = \begin{cases} +1 & \text{if } x \text{ is a square in } \mathbb{F}_p^\times \\ -1 & \text{if } x \text{ is not a square in } \mathbb{F}_p^\times \end{cases}$$

Lemma (Euler's criterion)

$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ in $\mathbb{F}_p$ so that $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$ in $\mathbb{F}_p$.

Proof.

$X^{p-1} - 1 = (X^{\frac{p-1}{2}} + 1)(X^{\frac{p-1}{2}} - 1)$ in $\mathbb{F}_p[X]$. $\square$

Theorem (Quadratic reciprocity law – Euler, Legendre, Gauss)

- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$

Example (Is 14 a square in $\mathbb{F}_{41}$?)

- $\left(\frac{2}{41}\right) = +1$
- $\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1$
- $\left(\frac{14}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -1$ so the answer is no !

Theorem (Quadratic reciprocity law – Euler, Legendre, Gauss)

- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$

Example (Is 14 a square in $\mathbb{F}_{41}$?)

- $\left(\frac{2}{41}\right) = +1$
- $\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1$
- $\left(\frac{14}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -1$ so the answer is no !

Theorem (Quadratic reciprocity law – Euler, Legendre, Gauss)

- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$

Example (Is 14 a square in $\mathbb{F}_{41}$?)

- $\left(\frac{2}{41}\right) = +1$
- $\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1$
- $\left(\frac{14}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -1$ so the answer is no !

Theorem (Quadratic reciprocity law – Euler, Legendre, Gauss)

- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$

Example (Is 14 a square in $\mathbb{F}_{41}$?)

- $\left(\frac{2}{41}\right) = +1$
- $\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1$
- $\left(\frac{14}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -1$ so the answer is no !

Theorem (Quadratic reciprocity law – Euler, Legendre, Gauss)

- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$

Example (Is 14 a square in $\mathbb{F}_{41}$?)

- $\left(\frac{2}{41}\right) = +1$
- $\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1$
- $\left(\frac{14}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -1$ so the answer is no !

Theorem (Quadratic reciprocity law – Euler, Legendre, Gauss)

- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$

Example (Is 14 a square in $\mathbb{F}_{41}$?)

- $\left(\frac{2}{41}\right) = +1$
- $\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1$
- $\left(\frac{14}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -1$ so the answer is no !

Theorem (Quadratic reciprocity law – Euler, Legendre, Gauss)

- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$

Example (Is 14 a square in $\mathbb{F}_{41}$?)

- $\left(\frac{2}{41}\right) = +1$
- $\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1$
- $\left(\frac{14}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -1$ so the answer is no !

Theorem (Quadratic reciprocity law – Euler, Legendre, Gauss)

- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$

Example (Is 14 a square in $\mathbb{F}_{41}$?)

- $\left(\frac{2}{41}\right) = +1$
- $\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1$
- $\left(\frac{14}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -1$ so the answer is no !

Theorem (Quadratic reciprocity law – Euler, Legendre, Gauss)

- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$

Example (Is 14 a square in $\mathbb{F}_{41}$?)

- $\left(\frac{2}{41}\right) = +1$
- $\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1$
- $\left(\frac{14}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -1$ so the answer is no !

Remark (Lemmermeyer 2000)

has referenced more than 300 proofs of the quadratic reciprocity law among which 8 by Gauss.
We outline three of them, a combinatorial, an algebraic, and a cyclotomic proof.

method	keyword1	keyword2	Gauss's proof	extended by
combinatorial	signature	Gauss's Lemma	3/5 (1808/18)	Eisenstein[a], Zolotarev[b], Frobenius[c]
algebraic	discriminant	Gauss reduction	2 (1801)	Stickelberger[d], Hensel[e,f], Artin[g]
cyclotomic	character	Gauss sum	4/6 (1811/18)	Eisenstein[h], Dirichlet[i,j], Dedekind[k],

[a] Eisenstein/L18: Neuer elementarer Beweis des Legendre'schen Reciprocitäts-Gesetzes, Crelle 27 (1844), 322-329.
[b] Zolotarev/L53: Nouvelle démonstration de la loi de réciprocité de Legendre, Nouv. Ann. Math. (1872), 354-362.
[c] Frobenius/L169: Über das quadratische Reziprozitätsgesetz I, Sitzungsberichte Berliner Akad. (1914), 335-349.
[d] Stickelberger: Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, Intern. Math. Kongr. Zürich 1897 (Leipzig 1898), 182-193.
[e] Hensel/L152: Über die zu einem algebraischen Körper gehörigen Invarianten, Crelle 129 (1905), 68-87.
[f] Swan/L225: Factorization of polynomials over finite fields, Pac. J. Math. 12 (1962), 1099-1106.
[g] Artin : Beweis des allgemeinen Reziprozitätsgesetzes. Abh. Math. Sem. Univ. Hamburg 5 (1927), 353-363.
[h] Eisenstein/L17: La loi de réciprocité tirée des formules de Gauss, sans signe du radical, Crelle 28 (1844), 41-43.
[i] Dirichlet: Vorlesungen über Zahlentheorie, Vieweg (1894).
[j] Motose/L300: On Gauss sums and Vandermonde matrices, Bull. Sci. Technol. Hirosaki Univ. 6 (2003), 19-23.
[k] Dedekind/L57: Sur la théorie des nombres entiers algébriques, Bull. Sci. Math. Astr. 11 (1877), 207-248.

[k] ... cette démonstration de la loi de réciprocité, par laquelle on détermine en même temps le caractère quadratique du nombre $-i$, coïncide, au fond, avec la célèbre sixième démonstration de Gauss, reproduite plus tard sous les formes les plus différentes par Jacobi, Eisenstein et autres, et je ferai remarquer expressément que c'est en méditant sur le nerf de cette démonstration et des démonstrations analogues de la loi de réciprocité cubique et biquadratique, que j'ai été conduit aux recherches générales que j'ai indiquées plus haut ...

Remark (Lemmermeyer 2000)

has referenced more than 300 proofs of the quadratic reciprocity law among which 8 by Gauss.
We outline three of them, a combinatorial, an algebraic, and a cyclotomic proof.

method	keyword1	keyword2	Gauss's proof	extended by
combinatorial	signature	Gauss's Lemma	3/5 (1808/18)	Eisenstein[a], Zolotarev[b], Frobenius[c]
algebraic	discriminant	Gauss reduction	2 (1801)	Stickelberger[d], Hensel[e,f], Artin[g]
cyclotomic	character	Gauss sum	4/6 (1811/18)	Eisenstein[h], Dirichlet[i,j], Dedekind[k],

[a] Eisenstein/L18: Neuer elementarer Beweis des Legendre'schen Reciprocitäts-Gesetzes, Crelle 27 (1844), 322-329.
[b] Zolotarev/L53: Nouvelle démonstration de la loi de réciprocité de Legendre, Nouv. Ann. Math. (1872), 354-362.
[c] Frobenius/L169: Über das quadratische Reziprozitätsgesetz I, Sitzungsberichte Berliner Akad. (1914), 335-349.
[d] Stickelberger: Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, Intern. Math. Kongr. Zürich 1897 (Leipzig 1898), 182-193.
[e] Hensel/L152: Über die zu einem algebraischen Körper gehörigen Invarianten, Crelle 129 (1905), 68-87.
[f] Swan/L225: Factorization of polynomials over finite fields, Pac. J. Math. 12 (1962), 1099-1106.
[g] Artin : Beweis des allgemeinen Reziprozitätsgesetzes. Abh. Math. Sem. Univ. Hamburg 5 (1927), 353-363.
[h] Eisenstein/L17: La loi de réciprocité tirée des formules de Gauss, sans signe du radical, Crelle 28 (1844), 41-43.
[i] Dirichlet: Vorlesungen über Zahlentheorie, Vieweg (1894).
[j] Motose/L300: On Gauss sums and Vandermonde matrices, Bull. Sci. Technol. Hirosaki Univ. 6 (2003), 19-23.
[k] Dedekind/L57: Sur la théorie des nombres entiers algébriques, Bull. Sci. Math. Astr. 11 (1877), 207-248.

[k] ... cette démonstration de la loi de réciprocité, par laquelle on détermine en même temps le caractère quadratique du nombre $-i$, coïncide, au fond, avec la célèbre sixième démonstration de Gauss, reproduite plus tard sous les formes les plus différentes par Jacobi, Eisenstein et autres, et je ferai remarquer expressément que c'est en méditant sur le nerf de cette démonstration et des démonstrations analogues de la loi de réciprocité cubique et biquadratique, que j'ai été conduit aux recherches générales que j'ai indiquées plus haut ...

Remark (Lemmermeyer 2000)

has referenced more than 300 proofs of the quadratic reciprocity law among which 8 by Gauss.
We outline three of them, a combinatorial, an algebraic, and a cyclotomic proof.

method	keyword1	keyword2	Gauss's proof	extended by
combinatorial	signature	Gauss's Lemma	3/5 (1808/18)	Eisenstein[a], Zolotarev[b], Frobenius[c]
algebraic	discriminant	Gauss reduction	2 (1801)	Stickelberger[d], Hensel[e,f], Artin[g]
cyclotomic	character	Gauss sum	4/6 (1811/18)	Eisenstein[h], Dirichlet[i,j], Dedekind[k],

[a] Eisenstein/L18: Neuer elementarer Beweis des Legendre'schen Reciprocitäts-Gesetzes, Crelle 27 (1844), 322-329.
[b] Zolotarev/L53: Nouvelle démonstration de la loi de réciprocité de Legendre, Nouv. Ann. Math. (1872), 354-362.
[c] Frobenius/L169: Über das quadratische Reziprozitätsgesetz I, Sitzungsberichte Berliner Akad. (1914), 335-349.
[d] Stickelberger: Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, Intern. Math. Kongr. Zürich 1897 (Leipzig 1898), 182-193.
[e] Hensel/L152: Über die zu einem algebraischen Körper gehörigen Invarianten, Crelle 129 (1905), 68-87.
[f] Swan/L225: Factorization of polynomials over finite fields, Pac. J. Math. 12 (1962), 1099-1106.
[g] Artin : Beweis des allgemeinen Reziprozitätsgesetzes. Abh. Math. Sem. Univ. Hamburg 5 (1927), 353-363.
[h] Eisenstein/L17: La loi de réciprocité tirée des formules de Gauss, sans signe du radical, Crelle 28 (1844), 41-43.
[i] Dirichlet: Vorlesungen über Zahlentheorie, Vieweg (1894).
[j] Motose/L300: On Gauss sums and Vandermonde matrices, Bull. Sci. Technol. Hirosaki Univ. 6 (2003), 19-23.
[k] Dedekind/L57: Sur la théorie des nombres entiers algébriques, Bull. Sci. Math. Astr. 11 (1877), 207-248.

[k] ... cette démonstration de la loi de réciprocité, par laquelle on détermine en même temps le caractère quadratique du nombre $-i$, coïncide, au fond, avec la célèbre sixième démonstration de Gauss, reproduite plus tard sous les formes les plus différentes par Jacobi, Eisenstein et autres, et je ferai remarquer expressément que c'est en méditant sur le nerf de cette démonstration et des démonstrations analogues de la loi de réciprocité cubique et biquadratique, que j'ai été conduit aux recherches générales que j'ai indiquées plus haut ...

Theorem (Zolotarev 1878)

$\left(\frac{x}{p}\right) = \operatorname{sgn}(m_x)$ where $m_x : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ is multiplication by x.

Proof.

m_x has even/odd number of orbits iff x is/is not square in $\mathbb{F}_p$. □

Corollary (complementary laws of quadratic reciprocity)

- m_{-1} is fixpoint-free involution of $\mathbb{F}_p^\times$ with $\frac{p-1}{2}$ orbits
- m_2 is a $\left(\frac{p-1}{2}, \frac{p-1}{2}\right)$-shuffle of $\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$ with $1 + 2 + \cdots + \frac{p-1}{2} = \frac{p^2-1}{8}$ inversions.

Definition (Gauss 1808)

$n_p(x) = \#\{y \in \mathbb{F}_p \,|\, 0 < y \le \frac{p-1}{2} \text{ and } \frac{p-1}{2} < xy \le p-1\}$

Theorem (Zolotarev 1878)

$\left(\frac{x}{p}\right) = \mathrm{sgn}(m_x)$ where $m_x : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ is multiplication by x.

Proof.

m_x has even/odd number of orbits iff x is/is not square in $\mathbb{F}_p$. □

Corollary (complementary laws of quadratic reciprocity)

- m_{-1} is fixpoint-free involution of $\mathbb{F}_p^\times$ with $\frac{p-1}{2}$ orbits
- m_2 is a $(\frac{p-1}{2}, \frac{p-1}{2})$-shuffle of $\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$ with $1 + 2 + \cdots + \frac{p-1}{2} = \frac{p^2-1}{8}$ inversions.

Definition (Gauss 1808)

$n_p(x) = \#\{y \in \mathbb{F}_p \,|\, 0 < y \leq \frac{p-1}{2} \text{ and } \frac{p-1}{2} < xy \leq p-1\}$

Theorem (Zolotarev 1878)

$\left(\frac{x}{p}\right) = \mathrm{sgn}(m_x)$ where $m_x : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ is multiplication by x.

Proof.

m_x has even/odd number of orbits iff x is/is not square in $\mathbb{F}_p$. □

Corollary (complementary laws of quadratic reciprocity)

- m_{-1} is fixpoint-free involution of $\mathbb{F}_p^\times$ with $\frac{p-1}{2}$ orbits
- m_2 is a $(\frac{p-1}{2}, \frac{p-1}{2})$-shuffle of $\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$ with $1 + 2 + \cdots + \frac{p-1}{2} = \frac{p^2-1}{8}$ inversions.

Definition (Gauss 1808)

$n_p(x) = \#\{y \in \mathbb{F}_p \,|\, 0 < y \leq \frac{p-1}{2} \text{ and } \frac{p-1}{2} < xy \leq p-1\}$

Theorem (Zolotarev 1878)

$\left(\frac{x}{p}\right) = \operatorname{sgn}(m_x)$ where $m_x : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ is multiplication by x.

Proof.

m_x has even/odd number of orbits iff x is/is not square in $\mathbb{F}_p$. □

Corollary (complementary laws of quadratic reciprocity)

- m_{-1} is fixpoint-free involution of $\mathbb{F}_p^\times$ with $\frac{p-1}{2}$ orbits
- m_2 is a $(\frac{p-1}{2}, \frac{p-1}{2})$-shuffle of $\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$ with $1 + 2 + \cdots + \frac{p-1}{2} = \frac{p^2-1}{8}$ inversions.

Definition (Gauss 1808)

$n_p(x) = \#\{y \in \mathbb{F}_p \,|\, 0 < y \leq \frac{p-1}{2} \text{ and } \frac{p-1}{2} < xy \leq p-1\}$

Theorem (Zolotarev 1878)

$\left(\frac{x}{p}\right) = \operatorname{sgn}(m_x)$ where $m_x : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ is multiplication by x.

Proof.

m_x has even/odd number of orbits iff x is/is not square in $\mathbb{F}_p$. □

Corollary (complementary laws of quadratic reciprocity)

- m_{-1} is fixpoint-free involution of $\mathbb{F}_p^\times$ with $\frac{p-1}{2}$ orbits
- m_2 is a $(\frac{p-1}{2}, \frac{p-1}{2})$-shuffle of $\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$ with $1 + 2 + \cdots + \frac{p-1}{2} = \frac{p^2-1}{8}$ inversions.

Definition (Gauss 1808)

$n_p(x) = \#\{y \in \mathbb{F}_p \,|\, 0 < y \leq \frac{p-1}{2} \text{ and } \frac{p-1}{2} < xy \leq p-1\}$

Theorem (Zolotarev 1878)

$\left(\frac{x}{p}\right) = \mathrm{sgn}(m_x)$ where $m_x : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ is multiplication by x.

Proof.

m_x has even/odd number of orbits iff x is/is not square in $\mathbb{F}_p$. □

Corollary (complementary laws of quadratic reciprocity)

- m_{-1} is fixpoint-free involution of $\mathbb{F}_p^\times$ with $\frac{p-1}{2}$ orbits
- m_2 is a $(\frac{p-1}{2}, \frac{p-1}{2})$-shuffle of $\mathbb{F}_p^\times = \{1, 2, \dots, p-1\}$ with $1 + 2 + \cdots + \frac{p-1}{2} = \frac{p^2-1}{8}$ inversions.

Definition (Gauss 1808)

$n_p(x) = \#\{y \in \mathbb{F}_p \,|\, 0 < y \leq \frac{p-1}{2} \text{ and } \frac{p-1}{2} < xy \leq p-1\}$

Theorem (Zolotarev 1878)

$\left(\frac{x}{p}\right) = \mathrm{sgn}(m_x)$ where $m_x : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ is multiplication by x.

Proof.

m_x has even/odd number of orbits iff x is/is not square in $\mathbb{F}_p$. □

Corollary (complementary laws of quadratic reciprocity)

- m_{-1} is fixpoint-free involution of $\mathbb{F}_p^\times$ with $\frac{p-1}{2}$ orbits
- m_2 is a $(\frac{p-1}{2}, \frac{p-1}{2})$-shuffle of $\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$ with $1 + 2 + \cdots + \frac{p-1}{2} = \frac{p^2-1}{8}$ inversions.

Definition (Gauss 1808)

$n_p(x) = \#\{y \in \mathbb{F}_p \,|\, 0 < y \leq \frac{p-1}{2} \text{ and } \frac{p-1}{2} < xy \leq p-1\}$

Lemma (Gauss 1808/1818)

$\left(\frac{x}{p}\right) = (-1)^{n_p(x)}$ so that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{n_q(p)+n_p(q)}$.

Proof.

If $i < j$ is inverted by m_x then so is $p-j < p-i$. □

Definition

- $X_{p,q} = \{1, 2, \ldots, \frac{p-1}{2}\} \times \{1, 2, \ldots, \frac{q-1}{2}\} \subset \mathbb{N} \times \mathbb{N}$
- $S_{p,q} = \{(x, y) \in X_{p,q} \mid -\frac{p}{2} < qx - py < \frac{q}{2}\}$

Proposition (Eisenstein 1844, Frobenius 1914)

$(-1)^{n_q(p)+n_p(q)} = (-1)^{\#S_{p,q}} = (-1)^{\#X_{p,q}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

$(x, y) \mapsto (\frac{p}{2} - x, \frac{q}{2} - y)$ is fixpoint free on $X_{p,q} - S_{p,q}$.

Lemma (Gauss 1808/1818)

$\left(\frac{x}{p}\right) = (-1)^{n_p(x)}$ so that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{n_q(p)+n_p(q)}$.

Proof.

If $i < j$ is inverted by m_x then so is $p - j < p - i$. □

Definition

- $X_{p,q} = \{1, 2, \ldots, \frac{p-1}{2}\} \times \{1, 2, \ldots, \frac{q-1}{2}\} \subset \mathbb{N} \times \mathbb{N}$
- $S_{p,q} = \{(x, y) \in X_{p,q} \mid -\frac{p}{2} < qx - py < \frac{q}{2}\}$

Proposition (Eisenstein 1844, Frobenius 1914)

$(-1)^{n_q(p)+n_p(q)} = (-1)^{\# S_{p,q}} = (-1)^{\# X_{p,q}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

$(x, y) \mapsto (\frac{p}{2} - x, \frac{q}{2} - y)$ is fixpoint free on $X_{p,q} - S_{p,q}$.

Lemma (Gauss 1808/1818)

$\left(\frac{x}{p}\right) = (-1)^{n_p(x)}$ so that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{n_q(p)+n_p(q)}$.

Proof.

If $i < j$ is inverted by m_x then so is $p - j < p - i$. □

Definition

- $X_{p,q} = \{1, 2, \ldots, \frac{p-1}{2}\} \times \{1, 2, \ldots, \frac{q-1}{2}\} \subset \mathbb{N} \times \mathbb{N}$
- $S_{p,q} = \{(x, y) \in X_{p,q} \mid -\frac{p}{2} < qx - py < \frac{q}{2}\}$

Proposition (Eisenstein 1844, Frobenius 1914)

$(-1)^{n_q(p)+n_p(q)} = (-1)^{\#S_{p,q}} = (-1)^{\#X_{p,q}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

$(x, y) \mapsto (\frac{p}{2} - x, \frac{q}{2} - y)$ is fixpoint free on $X_{p,q} - S_{p,q}$.

Lemma (Gauss 1808/1818)

$\left(\frac{x}{p}\right) = (-1)^{n_p(x)}$ so that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{n_q(p)+n_p(q)}$.

Proof.

If $i < j$ is inverted by m_x then so is $p - j < p - i$. □

Definition

- $X_{p,q} = \{1, 2, \ldots, \frac{p-1}{2}\} \times \{1, 2, \ldots, \frac{q-1}{2}\} \subset \mathbb{N} \times \mathbb{N}$
- $S_{p,q} = \{(x, y) \in X_{p,q} \mid -\frac{p}{2} < qx - py < \frac{q}{2}\}$

Proposition (Eisenstein 1844, Frobenius 1914)

$(-1)^{n_q(p)+n_p(q)} = (-1)^{\#S_{p,q}} = (-1)^{\#X_{p,q}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

$(x, y) \mapsto (\frac{p}{2} - x, \frac{q}{2} - y)$ is fixpoint free on $X_{p,q} - S_{p,q}$.

Lemma (Gauss 1808/1818)

$\left(\frac{x}{p}\right) = (-1)^{n_p(x)}$ so that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{n_q(p)+n_p(q)}$.

Proof.

If $i < j$ is inverted by m_x then so is $p - j < p - i$. □

Definition

- $X_{p,q} = \{1, 2, \ldots, \frac{p-1}{2}\} \times \{1, 2, \ldots, \frac{q-1}{2}\} \subset \mathbb{N} \times \mathbb{N}$
- $S_{p,q} = \{(x, y) \in X_{p,q} \mid -\frac{p}{2} < qx - py < \frac{q}{2}\}$

Proposition (Eisenstein 1844, Frobenius 1914)

$(-1)^{n_q(p)+n_p(q)} = (-1)^{\#S_{p,q}} = (-1)^{\#X_{p,q}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

$(x, y) \mapsto (\frac{p}{2} - x, \frac{q}{2} - y)$ is fixpoint free on $X_{p,q} - S_{p,q}$.

Lemma (Gauss 1808/1818)

$\left(\frac{x}{p}\right) = (-1)^{n_p(x)}$ so that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{n_q(p)+n_p(q)}$.

Proof.

If $i < j$ is inverted by m_x then so is $p - j < p - i$. □

Definition

- $X_{p,q} = \{1, 2, \ldots, \frac{p-1}{2}\} \times \{1, 2, \ldots, \frac{q-1}{2}\} \subset \mathbb{N} \times \mathbb{N}$
- $S_{p,q} = \{(x, y) \in X_{p,q} \mid -\frac{p}{2} < qx - py < \frac{q}{2}\}$

Proposition (Eisenstein 1844, Frobenius 1914)

$(-1)^{n_q(p)+n_p(q)} = (-1)^{\#S_{p,q}} = (-1)^{\#X_{p,q}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

$(x, y) \mapsto (\frac{p}{2} - x, \frac{q}{2} - y)$ is fixpoint free on $X_{p,q} - S_{p,q}$.

Lemma (Gauss 1808/1818)

$\left(\frac{x}{p}\right) = (-1)^{n_p(x)}$ so that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{n_q(p)+n_p(q)}$.

Proof.

If $i < j$ is inverted by m_x then so is $p - j < p - i$. □

Definition

- $X_{p,q} = \{1, 2, \ldots, \frac{p-1}{2}\} \times \{1, 2, \ldots, \frac{q-1}{2}\} \subset \mathbb{N} \times \mathbb{N}$
- $S_{p,q} = \{(x, y) \in X_{p,q} \mid -\frac{p}{2} < qx - py < \frac{q}{2}\}$

Proposition (Eisenstein 1844, Frobenius 1914)

$(-1)^{n_q(p)+n_p(q)} = (-1)^{\#S_{p,q}} = (-1)^{\#X_{p,q}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

$(x, y) \mapsto (\frac{p}{2} - x, \frac{q}{2} - y)$ is fixpoint free on $X_{p,q} - S_{p,q}$.

Lemma (Gauss 1808/1818)

$\left(\frac{x}{p}\right) = (-1)^{n_p(x)}$ so that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{n_q(p)+n_p(q)}$.

Proof.

If $i < j$ is inverted by m_x then so is $p - j < p - i$. □

Definition

- $X_{p,q} = \{1, 2, \ldots, \frac{p-1}{2}\} \times \{1, 2, \ldots, \frac{q-1}{2}\} \subset \mathbb{N} \times \mathbb{N}$
- $S_{p,q} = \{(x, y) \in X_{p,q} \mid -\frac{p}{2} < qx - py < \frac{q}{2}\}$

Proposition (Eisenstein 1844, Frobenius 1914)

$(-1)^{n_q(p)+n_p(q)} = (-1)^{\#S_{p,q}} = (-1)^{\#X_{p,q}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

$(x, y) \mapsto (\frac{p}{2} - x, \frac{q}{2} - y)$ is fixpoint free on $X_{p,q} - S_{p,q}$.

Definition (discriminant of a polynomial)

For $f(X) \in K[X]$ and $f(X) = (X-\alpha_1)\cdots(X-\alpha_n) \in L[X]$:

- $\Delta_f = \prod_{i<j}(\alpha_i - \alpha_j)^2 \in K$
- $\sqrt{\Delta_f} = \prod_{i<j}(\alpha_j - \alpha_i) = V(\alpha_1, \ldots, \alpha_n) \in L$
- $\left(\frac{\Delta_f}{K}\right) = \begin{cases} +1 & \text{if } \Delta_f \text{ is a square in } K\,(i.e. \sqrt{\Delta_f} \in K) \\ -1 & \text{if } \Delta_f \text{ is not a square in } K\,(i.e. \sqrt{\Delta_f} \notin K) \end{cases}$

Proposition (assume $\mathrm{Gal}(L/K)$ is cyclic with generator $\phi_{L/K}$)

$\left(\frac{\Delta_f}{K}\right) = \mathrm{sgn}(\phi_{L/K})$ where $\phi_{L/K}$ permutes the roots of f.

Proof.

$\phi_{L/K}(\sqrt{\Delta_f}) = \mathrm{sgn}(\phi_{L/K})\sqrt{\Delta_f}$. □

Definition (discriminant of a polynomial)

For $f(X) \in K[X]$ and $f(X) = (X - \alpha_1)\cdots(X - \alpha_n) \in L[X]$:

- $\Delta_f = \prod_{i<j}(\alpha_i - \alpha_j)^2 \in K$
- $\sqrt{\Delta_f} = \prod_{i<j}(\alpha_j - \alpha_i) = V(\alpha_1, \ldots, \alpha_n) \in L$
- $\left(\frac{\Delta_f}{K}\right) = \begin{cases} +1 & \text{if } \Delta_f \text{ is a square in } K\,(i.e. \sqrt{\Delta_f} \in K) \\ -1 & \text{if } \Delta_f \text{ is not a square in } K\,(i.e. \sqrt{\Delta_f} \notin K) \end{cases}$

Proposition (assume $\mathrm{Gal}(L/K)$ is cyclic with generator $\phi_{L/K}$)

$\left(\frac{\Delta_f}{K}\right) = \mathrm{sgn}(\phi_{L/K})$ where $\phi_{L/K}$ permutes the roots of f.

Proof.

$\phi_{L/K}(\sqrt{\Delta_f}) = \mathrm{sgn}(\phi_{L/K})\sqrt{\Delta_f}$. □

Definition (discriminant of a polynomial)

For $f(X) \in K[X]$ and $f(X) = (X - \alpha_1) \cdots (X - \alpha_n) \in L[X]$:

- $\Delta_f = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in K$
- $\sqrt{\Delta_f} = \prod_{i<j} (\alpha_j - \alpha_i) = V(\alpha_1, \ldots, \alpha_n) \in L$
- $\left(\frac{\Delta_f}{K}\right) = \begin{cases} +1 & \text{if } \Delta_f \text{ is a square in } K \, (i.e. \sqrt{\Delta_f} \in K) \\ -1 & \text{if } \Delta_f \text{ is not a square in } K \, (i.e. \sqrt{\Delta_f} \notin K) \end{cases}$

Proposition (assume $\mathrm{Gal}(L/K)$ is cyclic with generator $\phi_{L/K}$)

$\left(\frac{\Delta_f}{K}\right) = \mathrm{sgn}(\phi_{L/K})$ where $\phi_{L/K}$ permutes the roots of f.

Proof.

$\phi_{L/K}(\sqrt{\Delta_f}) = \mathrm{sgn}(\phi_{L/K}) \sqrt{\Delta_f}$. □

Definition (discriminant of a polynomial)

For $f(X) \in K[X]$ and $f(X) = (X - \alpha_1) \cdots (X - \alpha_n) \in L[X]$:

- $\Delta_f = \prod_{i<j}(\alpha_i - \alpha_j)^2 \in K$
- $\sqrt{\Delta_f} = \prod_{i<j}(\alpha_j - \alpha_i) = V(\alpha_1, \ldots, \alpha_n) \in L$
- $\left(\frac{\Delta_f}{K}\right) = \begin{cases} +1 & \text{if } \Delta_f \text{ is a square in } K \,(i.e. \sqrt{\Delta_f} \in K) \\ -1 & \text{if } \Delta_f \text{ is not a square in } K \,(i.e. \sqrt{\Delta_f} \notin K) \end{cases}$

Proposition (assume $\mathrm{Gal}(L/K)$ is cyclic with generator $\phi_{L/K}$)

$\left(\frac{\Delta_f}{K}\right) = \mathrm{sgn}(\phi_{L/K})$ where $\phi_{L/K}$ permutes the roots of f.

Proof.

$\phi_{L/K}(\sqrt{\Delta_f}) = \mathrm{sgn}(\phi_{L/K})\sqrt{\Delta_f}$. □

Definition (discriminant of a polynomial)

For $f(X) \in K[X]$ and $f(X) = (X - \alpha_1) \cdots (X - \alpha_n) \in L[X]$:

- $\Delta_f = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in K$
- $\sqrt{\Delta_f} = \prod_{i<j} (\alpha_j - \alpha_i) = V(\alpha_1, \ldots, \alpha_n) \in L$
- $\left(\frac{\Delta_f}{K}\right) = \begin{cases} +1 & \text{if } \Delta_f \text{ is a square in } K \ (i.e. \sqrt{\Delta_f} \in K) \\ -1 & \text{if } \Delta_f \text{ is not a square in } K \ (i.e. \sqrt{\Delta_f} \notin K) \end{cases}$

Proposition (assume $\mathrm{Gal}(L/K)$ is cyclic with generator $\phi_{L/K}$)

$\left(\frac{\Delta_f}{K}\right) = \mathrm{sgn}(\phi_{L/K})$ where $\phi_{L/K}$ permutes the roots of f.

Proof.

$\phi_{L/K}(\sqrt{\Delta_f}) = \mathrm{sgn}(\phi_{L/K})\sqrt{\Delta_f}$. □

Definition (discriminant of a polynomial)

For $f(X) \in K[X]$ and $f(X) = (X - \alpha_1)\cdots(X - \alpha_n) \in L[X]$:

- $\Delta_f = \prod_{i<j}(\alpha_i - \alpha_j)^2 \in K$
- $\sqrt{\Delta_f} = \prod_{i<j}(\alpha_j - \alpha_i) = V(\alpha_1, \ldots, \alpha_n) \in L$
- $\left(\frac{\Delta_f}{K}\right) = \begin{cases} +1 & \text{if } \Delta_f \text{ is a square in } K \, (i.e. \sqrt{\Delta_f} \in K) \\ -1 & \text{if } \Delta_f \text{ is not a square in } K \, (i.e. \sqrt{\Delta_f} \notin K) \end{cases}$

Proposition (assume $\mathrm{Gal}(L/K)$ is cyclic with generator $\phi_{L/K}$)

$\left(\frac{\Delta_f}{K}\right) = \mathrm{sgn}(\phi_{L/K})$ where $\phi_{L/K}$ permutes the roots of f.

Proof.

$\phi_{L/K}(\sqrt{\Delta_f}) = \mathrm{sgn}(\phi_{L/K})\sqrt{\Delta_f}$. □

Definition (discriminant of a polynomial)

For $f(X) \in K[X]$ and $f(X) = (X - \alpha_1) \cdots (X - \alpha_n) \in L[X]$:

- $\Delta_f = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in K$
- $\sqrt{\Delta_f} = \prod_{i<j} (\alpha_j - \alpha_i) = V(\alpha_1, \ldots, \alpha_n) \in L$
- $\left(\frac{\Delta_f}{K}\right) = \begin{cases} +1 & \text{if } \Delta_f \text{ is a square in } K \, (i.e. \sqrt{\Delta_f} \in K) \\ -1 & \text{if } \Delta_f \text{ is not a square in } K \, (i.e. \sqrt{\Delta_f} \notin K) \end{cases}$

Proposition (assume $\mathrm{Gal}(L/K)$ is cyclic with generator $\phi_{L/K}$)

$\left(\frac{\Delta_f}{K}\right) = \mathrm{sgn}(\phi_{L/K})$ where $\phi_{L/K}$ permutes the roots of f.

Proof.

$\phi_{L/K}(\sqrt{\Delta_f}) = \mathrm{sgn}(\phi_{L/K})\sqrt{\Delta_f}$. □

Lemma ($p^* = (-1)^{\frac{p-1}{2}} p$)

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ if and only if $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$

Theorem (Dedekind 1877)

$$\left(\frac{p^*}{q}\right) = \left(\frac{\Delta_{X^p-1}}{\mathbb{F}_q}\right) = \left(\frac{q}{p}\right)$$

Proof.

$\Delta_f = (-1)^{\binom{n}{2}} \prod_i f'(\alpha_i)$ so $\Delta_{X^p-1} = (-1)^{\binom{p}{2}} \prod_{i=1}^p p\alpha_i^{p-1} \equiv p^*$.
$X^p - 1$ splits in $\mathbb{F}_{q^r}$ if $p|q^r - 1$ and $\mathrm{sgn}(\phi_{\mathbb{F}_{q^r}/\mathbb{F}_q}) = \mathrm{sgn}(m_q)$. □

Theorem (Stickelberger 1898, Hensel 1905, Swan 1962)

For $f \in \mathbb{F}_q[X]$ sth. $\Delta_f \neq 0$ one has $\left(\frac{\Delta_f}{\mathbb{F}_q}\right) = (-1)^{\deg(f) - \#\mathrm{irrfact}(f)}$

Lemma ($p^* = (-1)^{\frac{p-1}{2}} p$)

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ if and only if $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$

Theorem (Dedekind 1877)

$\left(\frac{p^*}{q}\right) = \left(\frac{\Delta_{X^p-1}}{\mathbb{F}_q}\right) = \left(\frac{q}{p}\right)$

Proof.

$\Delta_f = (-1)^{\binom{n}{2}} \prod_i f'(\alpha_i)$ so $\Delta_{X^p-1} = (-1)^{\binom{p}{2}} \prod_{i=1}^p p\alpha_i^{p-1} = p^*$.
$X^p - 1$ splits in $\mathbb{F}_{q^r}$ if $p|q^r - 1$ and $\mathrm{sgn}(\phi_{\mathbb{F}_{q^r}/\mathbb{F}_q}) = \mathrm{sgn}(m_q)$. □

Theorem (Stickelberger 1898, Hensel 1905, Swan 1962)

For $f \in \mathbb{F}_q[X]$ sth. $\Delta_f \neq 0$ one has $\left(\frac{\Delta_f}{\mathbb{F}_q}\right) = (-1)^{\deg(f) - \#\mathrm{irrfact}(f)}$

Lemma ($p^* = (-1)^{\frac{p-1}{2}} p$)

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ if and only if $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$

Theorem (Dedekind 1877)

$$\left(\frac{p^*}{q}\right) = \left(\frac{\Delta_{X^p-1}}{\mathbb{F}_q}\right) = \left(\frac{q}{p}\right)$$

Proof.

$\Delta_f = (-1)^{\binom{n}{2}} \prod_i f'(\alpha_i)$ so $\Delta_{X^p-1} = (-1)^{\binom{p}{2}} \prod_{i=1}^p p\alpha_i^{p-1} = p^*$.
$X^p - 1$ splits in $\mathbb{F}_{q^r}$ if $p|q^r - 1$ and $\mathrm{sgn}(\phi_{\mathbb{F}_{q^r}/\mathbb{F}_q}) = \mathrm{sgn}(m_q)$. □

Theorem (Stickelberger 1898, Hensel 1905, Swan 1962)

For $f \in \mathbb{F}_q[X]$ sth. $\Delta_f \neq 0$ one has $\left(\frac{\Delta_f}{\mathbb{F}_q}\right) = (-1)^{\deg(f) - \#\mathrm{irrfact}(f)}$

Lemma ($p^* = (-1)^{\frac{p-1}{2}} p$)

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ if and only if $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$

Theorem (Dedekind 1877)

$$\left(\frac{p^*}{q}\right) = \left(\frac{\Delta_{X^p-1}}{\mathbb{F}_q}\right) = \left(\frac{q}{p}\right)$$

Proof.

$\Delta_f = (-1)^{\binom{n}{2}} \prod_i f'(\alpha_i)$ so $\Delta_{X^p-1} = (-1)^{\binom{p}{2}} \prod_{i=1}^p p\alpha_i^{p-1} \equiv p^*$.
$X^p - 1$ splits in $\mathbb{F}_{q^r}$ if $p | q^r - 1$ and $\mathrm{sgn}(\phi_{\mathbb{F}_{q^r}/\mathbb{F}_q}) = \mathrm{sgn}(m_q)$. □

Theorem (Stickelberger 1898, Hensel 1905, Swan 1962)

For $f \in \mathbb{F}_q[X]$ sth. $\Delta_f \neq 0$ one has $\left(\frac{\Delta_f}{\mathbb{F}_q}\right) = (-1)^{\deg(f) - \#\mathrm{irrfact}(f)}$

Lemma ($p^* = (-1)^{\frac{p-1}{2}} p$)

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ if and only if $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$

Theorem (Dedekind 1877)

$$\left(\frac{p^*}{q}\right) = \left(\frac{\Delta_{X^p-1}}{\mathbb{F}_q}\right) = \left(\frac{q}{p}\right)$$

Proof.

$\Delta_f = (-1)^{\binom{n}{2}} \prod_i f'(\alpha_i)$ so $\Delta_{X^p-1} = (-1)^{\binom{p}{2}} \prod_{i=1}^{p} p\alpha_i^{p-1} \equiv p^*$.
$X^p - 1$ splits in $\mathbb{F}_{q^r}$ if $p | q^r - 1$ and $\mathrm{sgn}(\phi_{\mathbb{F}_{q^r}/\mathbb{F}_q}) = \mathrm{sgn}(m_q)$. □

Theorem (Stickelberger 1898, Hensel 1905, Swan 1962)

For $f \in \mathbb{F}_q[X]$ sth. $\Delta_f \neq 0$ one has $\left(\frac{\Delta_f}{\mathbb{F}_q}\right) = (-1)^{\deg(f) - \#\mathrm{irrfact}(f)}$

Definition (Dirichlet character)

$\chi : \mathbb{F}_p^\times \to \mathbb{C}^*$ sth. $\chi(xy) = \chi(x)\chi(y)$ and $\chi(1) = 1$. For pointwise multiplication, Dirichlet characters mod p form a cyclic group.

Remark

The Legendre symbol is the only Dirichlet character of order 2.

Definition (Gauss sums for $\zeta = e^{2\pi i/p}$)

- $\tau_\chi = \sum_{k=1}^{p-1} \chi(k)\zeta^k$
- $\hat{\chi}(s) = \sum_{k=1}^{p-1} \chi(k)\zeta^{sk}$
- $\tau_p = \tau_{\left(\frac{\cdot}{p}\right)} = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$

Definition (Dirichlet character)

$\chi : \mathbb{F}_p^\times \to \mathbb{C}^*$ sth. $\chi(xy) = \chi(x)\chi(y)$ and $\chi(1) = 1$. For pointwise multiplication, Dirichlet characters mod p form a cyclic group.

Remark

The Legendre symbol is the only Dirichlet character of order 2.

Definition (Gauss sums for $\zeta = e^{2\pi i/p}$)

- $\tau_\chi = \sum_{k=1}^{p-1} \chi(k)\zeta^k$
- $\hat{\chi}(s) = \sum_{k=1}^{p-1} \chi(k)\zeta^{sk}$
- $\tau_p = \tau_{\left(\frac{\cdot}{p}\right)} = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$

Definition (Dirichlet character)

$\chi : \mathbb{F}_p^\times \to \mathbb{C}^*$ sth. $\chi(xy) = \chi(x)\chi(y)$ and $\chi(1) = 1$. For pointwise multiplication, Dirichlet characters mod p form a cyclic group.

Remark

The Legendre symbol is the only Dirichlet character of order 2.

Definition (Gauss sums for $\zeta = e^{2\pi i/p}$)

- $\tau_\chi = \sum_{k=1}^{p-1} \chi(k)\zeta^k$
- $\hat{\chi}(s) = \sum_{k=1}^{p-1} \chi(k)\zeta^{sk}$
- $\tau_p = \tau_{\left(\frac{\cdot}{p}\right)} = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\zeta^k.$

Definition (Dirichlet character)

$\chi : \mathbb{F}_p^\times \to \mathbb{C}^*$ sth. $\chi(xy) = \chi(x)\chi(y)$ and $\chi(1) = 1$. For pointwise multiplication, Dirichlet characters mod p form a cyclic group.

Remark

The Legendre symbol is the only Dirichlet character of order 2.

Definition (Gauss sums for $\zeta = e^{2\pi i/p}$)

- $\tau_\chi = \sum_{k=1}^{p-1} \chi(k)\zeta^k$
- $\hat{\chi}(s) = \sum_{k=1}^{p-1} \chi(k)\zeta^{sk}$
- $\tau_p = \tau_{\left(\frac{(-)}{p}\right)} = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$

Definition (Dirichlet character)

$\chi : \mathbb{F}_p^\times \to \mathbb{C}^*$ sth. $\chi(xy) = \chi(x)\chi(y)$ and $\chi(1) = 1$. For pointwise multiplication, Dirichlet characters mod p form a cyclic group.

Remark

The Legendre symbol is the only Dirichlet character of order 2.

Definition (Gauss sums for $\zeta = e^{2\pi i/p}$)

- $\tau_\chi = \sum_{k=1}^{p-1} \chi(k)\zeta^k$
- $\hat{\chi}(s) = \sum_{k=1}^{p-1} \chi(k)\zeta^{sk}$
- $\tau_p = \tau_{\left(\frac{(-)}{p}\right)} = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$

Definition (Dirichlet character)

$\chi : \mathbb{F}_p^\times \to \mathbb{C}^*$ sth. $\chi(xy) = \chi(x)\chi(y)$ and $\chi(1) = 1$. For pointwise multiplication, Dirichlet characters mod p form a cyclic group.

Remark

The Legendre symbol is the only Dirichlet character of order 2.

Definition (Gauss sums for $\zeta = e^{2\pi i/p}$)

- $\tau_\chi = \sum_{k=1}^{p-1} \chi(k)\zeta^k$
- $\hat{\chi}(s) = \sum_{k=1}^{p-1} \chi(k)\zeta^{sk}$
- $\tau_p = \tau_{\left(\frac{(-)}{p}\right)} = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$

Definition (Dirichlet character)

$\chi : \mathbb{F}_p^\times \to \mathbb{C}^*$ sth. $\chi(xy) = \chi(x)\chi(y)$ and $\chi(1) = 1$. For pointwise multiplication, Dirichlet characters mod p form a cyclic group.

Remark

The Legendre symbol is the only Dirichlet character of order 2.

Definition (Gauss sums for $\zeta = e^{2\pi i/p}$)

- $\tau_\chi = \sum_{k=1}^{p-1} \chi(k)\zeta^k$
- $\hat{\chi}(s) = \sum_{k=1}^{p-1} \chi(k)\zeta^{sk}$
- $\tau_p = \tau_{\left(\frac{(-)}{p}\right)} = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$

Proposition (Discrete Fourier Transform)

$\hat{\chi} = \tau_\chi \bar{\chi}$ and $\hat{\hat{\chi}} = \tau_\chi \tau_{\bar{\chi}} \chi$ and $\tau_\chi \tau_{\bar{\chi}} = p\chi(-1)$.

Proof.

$\chi(s)\hat{\chi}(s) = \chi(s)\sum_{k=1}^{p-1}\chi(k)\zeta^{sk} = \sum_{k=1}^{p-1}\chi(sk)\zeta^{sk} = \tau_\chi$.
Therefore, $\hat{\hat{\chi}} = \tau_\chi \hat{\bar{\chi}} = \tau_\chi \tau_{\bar{\chi}} \chi$
$\hat{\hat{\chi}} = V^2\chi = p\tilde{\chi}$ where V is defined below and $\tilde{\chi}(i) = \chi(p-i)$. □

Corollary (Eisenstein 1844)

$(\tau_p)^2 = p\left(\frac{-1}{p}\right) = p^*$ and $(\tau_p)^q \equiv \left(\frac{q}{p}\right)\tau_p \mod q\mathbb{Z}[\zeta]$

Proof.

$$(\tau_p)^q = \left(\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta^k\right)^q \overset{\text{mod } q\mathbb{Z}[\zeta]}{\equiv} \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta^{qk} = \left(\frac{q}{p}\right)\tau_p$$ □

Proposition (Discrete Fourier Transform)

$\hat{\chi} = \tau_\chi \bar{\chi}$ and $\hat{\hat{\chi}} = \tau_\chi \tau_{\bar{\chi}} \chi$ and $\tau_\chi \tau_{\bar{\chi}} = p\chi(-1)$.

Proof.

$\chi(s)\hat{\chi}(s) = \chi(s)\sum_{k=1}^{p-1} \chi(k)\zeta^{sk} = \sum_{k=1}^{p-1} \chi(sk)\zeta^{sk} = \tau_\chi$.
Therefore, $\hat{\hat{\chi}} = \tau_\chi \hat{\bar{\chi}} = \tau_\chi \tau_{\bar{\chi}} \chi$
$\hat{\hat{\chi}} = V^2\chi = p\tilde{\chi}$ where V is defined below and $\tilde{\chi}(i) = \chi(p-i)$. □

Corollary (Eisenstein 1844)

$(\tau_p)^2 = p\left(\frac{-1}{p}\right) = p^*$ and $(\tau_p)^q \equiv \left(\frac{q}{p}\right)\tau_p \mod q\mathbb{Z}[\zeta]$

Proof.

$(\tau_p)^q = \left(\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta^k\right)^q \stackrel{\text{mod } q\mathbb{Z}[\zeta]}{\equiv} \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta^{qk} = \left(\frac{q}{p}\right)\tau_p$ □

Proposition (Discrete Fourier Transform)

$\hat{\chi} = \tau_\chi \bar{\chi}$ and $\hat{\hat{\chi}} = \tau_\chi \tau_{\bar{\chi}} \chi$ and $\tau_\chi \tau_{\bar{\chi}} = p\chi(-1)$.

Proof.

$\chi(s)\hat{\chi}(s) = \chi(s) \sum_{k=1}^{p-1} \chi(k)\zeta^{sk} = \sum_{k=1}^{p-1} \chi(sk)\zeta^{sk} = \tau_\chi$.
Therefore, $\hat{\hat{\chi}} = \tau_\chi \hat{\bar{\chi}} = \tau_\chi \tau_{\bar{\chi}} \chi$
$\hat{\hat{\chi}} = V^2 \chi = p\tilde{\chi}$ where V is defined below and $\tilde{\chi}(i) = \chi(p-i)$. □

Corollary (Eisenstein 1844)

$(\tau_p)^2 = p\left(\frac{-1}{p}\right) = p^*$ and $(\tau_p)^q \equiv \left(\frac{q}{p}\right)\tau_p \mod q\mathbb{Z}[\zeta]$

Proof.

$(\tau_p)^q = \left(\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta^k\right)^q \overset{\mod q\mathbb{Z}[\zeta]}{\equiv} \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta^{qk} = \left(\frac{q}{p}\right)\tau_p$ □

Proposition (Discrete Fourier Transform)

$\hat{\chi} = \tau_\chi \bar{\chi}$ and $\hat{\hat{\chi}} = \tau_\chi \tau_{\bar{\chi}} \chi$ and $\tau_\chi \tau_{\bar{\chi}} = p\chi(-1)$.

Proof.

$\chi(s)\hat{\chi}(s) = \chi(s) \sum_{k=1}^{p-1} \chi(k)\zeta^{sk} = \sum_{k=1}^{p-1} \chi(sk)\zeta^{sk} = \tau_\chi$.
Therefore, $\hat{\hat{\chi}} = \tau_\chi \hat{\bar{\chi}} = \tau_\chi \tau_{\bar{\chi}} \chi$
$\hat{\hat{\chi}} = V^2 \chi = p\tilde{\chi}$ where V is defined below and $\tilde{\chi}(i) = \chi(p-i)$. □

Corollary (Eisenstein 1844)

$(\tau_p)^2 = p\left(\frac{-1}{p}\right) = p^*$ and $(\tau_p)^q \equiv \left(\frac{q}{p}\right)\tau_p \mod q\mathbb{Z}[\zeta]$

Proof.

$(\tau_p)^q = \left(\sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\zeta^k\right)^q \overset{\mod q\mathbb{Z}[\zeta]}{\equiv} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\zeta^{qk} = \left(\frac{q}{p}\right)\tau_p$ □

Proposition (Discrete Fourier Transform)

$\hat{\chi} = \tau_\chi \bar{\chi}$ and $\hat{\hat{\chi}} = \tau_\chi \tau_{\bar{\chi}} \chi$ and $\tau_\chi \tau_{\bar{\chi}} = p\chi(-1)$.

Proof.

$\chi(s)\hat{\chi}(s) = \chi(s) \sum_{k=1}^{p-1} \chi(k)\zeta^{sk} = \sum_{k=1}^{p-1} \chi(sk)\zeta^{sk} = \tau_\chi$.
Therefore, $\hat{\hat{\chi}} = \tau_\chi \hat{\bar{\chi}} = \tau_\chi \tau_{\bar{\chi}} \chi$
$\hat{\hat{\chi}} = V^2 \chi = p\tilde{\chi}$ where V is defined below and $\tilde{\chi}(i) = \chi(p-i)$. □

Corollary (Eisenstein 1844)

$(\tau_p)^2 = p\left(\frac{-1}{p}\right) = p^*$ and $(\tau_p)^q \equiv \left(\frac{q}{p}\right)\tau_p \mod q\mathbb{Z}[\zeta]$

Proof.

$$(\tau_p)^q = \left(\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k\right)^q \overset{\mod q\mathbb{Z}[\zeta]}{\equiv} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^{qk} = \left(\frac{q}{p}\right) \tau_p$$ □

Corollary (Quadratic reciprocity)

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

Theorem (Gauss 1818, proof by Motose 2003)

$$\tau_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \mod 4 \\ i\sqrt{p} & \text{if } p \equiv 3 \mod 4 \end{cases}$$

Definition (cyclotomic Vandermonde matrix)

For $V = \begin{pmatrix} \zeta & \zeta^2 & \cdots & \zeta^{p-1} \\ \zeta^2 & \zeta^4 & \cdots & \zeta^{2(p-1)} \\ \vdots & \vdots & \vdots & \vdots \\ \zeta^{p-1} & \zeta^{2(p-1)} & \cdots & \zeta^{(p-1)^2} \end{pmatrix}$ one has $V \begin{pmatrix} \chi(1) \\ \vdots \\ \vdots \\ \chi(p-1) \end{pmatrix} = \begin{pmatrix} \hat{\chi}(1) \\ \vdots \\ \vdots \\ \hat{\chi}(p-1) \end{pmatrix}$.

Remark (Variation on Wilson's Theorem)

$$\left(\frac{(\frac{p-1}{2})!}{p}\right) = (-1)^{\#\{\text{positive non-squares in } \mathbb{F}_p\}} = \left(\frac{-2}{p}\right) = (-1)^{\frac{(p-1)(p-3)}{8}}$$

Corollary (Quadratic reciprocity)

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

Theorem (Gauss 1818, proof by Motose 2003)

$$\tau_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \mod 4 \\ i\sqrt{p} & \text{if } p \equiv 3 \mod 4 \end{cases}$$

Definition (cyclotomic Vandermonde matrix)

For $V = \begin{pmatrix} \zeta & \zeta^2 & \cdots & \zeta^{p-1} \\ \zeta^2 & \zeta^4 & \cdots & \zeta^{2(p-1)} \\ \vdots & \vdots & \vdots & \vdots \\ \zeta^{p-1} & \zeta^{2(p-1)} & \cdots & \zeta^{(p-1)^2} \end{pmatrix}$ one has $V \begin{pmatrix} \chi(1) \\ \vdots \\ \vdots \\ \chi(p-1) \end{pmatrix} = \begin{pmatrix} \hat{\chi}(1) \\ \vdots \\ \vdots \\ \hat{\chi}(p-1) \end{pmatrix}$.

Remark (Variation on Wilson's Theorem)

$$\left(\frac{(\frac{p-1}{2})!}{p}\right) = (-1)^{\#\{\text{positive non-squares in } \mathbb{F}_p\}} = \left(\frac{-2}{p}\right) = (-1)^{\frac{(p-1)(p-3)}{8}}$$

Corollary (Quadratic reciprocity)

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

Theorem (Gauss 1818, proof by Motose 2003)

$$\tau_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \mod 4 \\ i\sqrt{p} & \text{if } p \equiv 3 \mod 4 \end{cases}$$

Definition (cyclotomic Vandermonde matrix)

For $V = \begin{pmatrix} \zeta & \zeta^2 & \cdots & \zeta^{p-1} \\ \zeta^2 & \zeta^4 & \cdots & \zeta^{2(p-1)} \\ \vdots & \vdots & \vdots & \vdots \\ \zeta^{p-1} & \zeta^{2(p-1)} & \cdots & \zeta^{(p-1)^2} \end{pmatrix}$ one has $V \begin{pmatrix} \chi(1) \\ \vdots \\ \vdots \\ \chi(p-1) \end{pmatrix} = \begin{pmatrix} \hat{\chi}(1) \\ \vdots \\ \vdots \\ \hat{\chi}(p-1) \end{pmatrix}$.

Remark (Variation on Wilson's Theorem)

$$\left(\frac{(\frac{p-1}{2})!}{p}\right) = (-1)^{\#\{\text{positive non-squares in } \mathbb{F}_p\}} = \left(\frac{-2}{p}\right) = (-1)^{\frac{(p-1)(p-3)}{8}}$$

Corollary (Quadratic reciprocity)

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

Theorem (Gauss 1818, proof by Motose 2003)

$$\tau_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \mod 4 \\ i\sqrt{p} & \text{if } p \equiv 3 \mod 4 \end{cases}$$

Definition (cyclotomic Vandermonde matrix)

For $V = \begin{pmatrix} \zeta & \zeta^2 & \cdots & \zeta^{p-1} \\ \zeta^2 & \zeta^4 & \cdots & \zeta^{2(p-1)} \\ \vdots & \vdots & \vdots & \vdots \\ \zeta^{p-1} & \zeta^{2(p-1)} & \cdots & \zeta^{(p-1)^2} \end{pmatrix}$ one has $V \begin{pmatrix} \chi(1) \\ \vdots \\ \vdots \\ \chi(p-1) \end{pmatrix} = \begin{pmatrix} \hat{\chi}(1) \\ \vdots \\ \vdots \\ \hat{\chi}(p-1) \end{pmatrix}$.

Remark (Variation on Wilson's Theorem)

$$\left(\frac{(\frac{p-1}{2})!}{p}\right) = (-1)^{\#\{\text{positive non-squares in } \mathbb{F}_p\}} = \left(\frac{-2}{p}\right) = (-1)^{\frac{(p-1)(p-3)}{8}}$$

Corollary (Quadratic reciprocity)

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

Theorem (Gauss 1818, proof by Motose 2003)

$$\tau_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \mod 4 \\ i\sqrt{p} & \text{if } p \equiv 3 \mod 4 \end{cases}$$

Definition (cyclotomic Vandermonde matrix)

For $V = \begin{pmatrix} \zeta & \zeta^2 & \cdots & \zeta^{p-1} \\ \zeta^2 & \zeta^4 & \cdots & \zeta^{2(p-1)} \\ \vdots & \vdots & \vdots & \vdots \\ \zeta^{p-1} & \zeta^{2(p-1)} & \cdots & \zeta^{(p-1)^2} \end{pmatrix}$ one has $V \begin{pmatrix} \chi(1) \\ \vdots \\ \vdots \\ \chi(p-1) \end{pmatrix} = \begin{pmatrix} \hat{\chi}(1) \\ \vdots \\ \vdots \\ \hat{\chi}(p-1) \end{pmatrix}$.

Remark (Variation on Wilson's Theorem)

$$\left(\frac{(\frac{p-1}{2})!}{p}\right) = (-1)^{\#\{\text{positive non-squares in } \mathbb{F}_p\}} = \left(\frac{-2}{p}\right) = (-1)^{\frac{(p-1)(p-3)}{8}}$$

Proof.

$$\det(V) = \zeta^{\binom{p-1}{2}} \prod_{j>i} (\zeta^j - \zeta^i) = \prod_{j=p-i} (\zeta^j - \zeta^i) \prod_{j\neq p-i} (\zeta^j - \zeta^i)$$
$$= (-1)^{\frac{p-1}{2}} i^{\frac{p-1}{2}} \sqrt{p} \cdot p^{\frac{p-3}{2}}$$

V is conjugate (choosing Dirichlet characters as basis) to a matrix decomposing into 2×2 principal block matrices thus yielding:

$$\det(V) = (-1)^{\frac{p-3}{2}} \prod_{\chi} \tau_\chi = (-1)^{\frac{p-1}{2}} \tau_p (p\chi_2(-1)) \cdots (p\chi_{\frac{p-1}{2}}(-1))$$
$$= (-1)^{\frac{p-1}{2}} \tau_p \cdot \left(\frac{(\frac{p-1}{2})!}{p} \right) \cdot p^{\frac{p-3}{2}}$$
$$= (-1)^{\frac{p-1}{2}} \tau_p \cdot (-1)^{\frac{(p-1)(p-3)}{8}} \cdot p^{\frac{p-3}{2}}$$

□

Proof.

$$\det(V) = \zeta^{\binom{p-1}{2}} \prod_{j>i} (\zeta^j - \zeta^i) = \prod_{j=p-i} (\zeta^j - \zeta^i) \prod_{j \neq p-i} (\zeta^j - \zeta^i)$$
$$= (-1)^{\frac{p-1}{2}} i^{\frac{p-1}{2}} \sqrt{p} \cdot p^{\frac{p-3}{2}}$$

V is conjugate (choosing Dirichlet characters as basis) to a matrix decomposing into 2×2 principal block matrices thus yielding:

$$\det(V) = (-1)^{\frac{p-3}{2}} \prod_{\chi} \tau_\chi = (-1)^{\frac{p-1}{2}} \tau_p (p\chi_2(-1)) \cdots (p\chi_{\frac{p-1}{2}}(-1))$$
$$= (-1)^{\frac{p-1}{2}} \tau_p \cdot \left(\frac{(\frac{p-1}{2})!}{p} \right) \cdot p^{\frac{p-3}{2}}$$
$$= (-1)^{\frac{p-1}{2}} \tau_p \cdot (-1)^{\frac{(p-1)(p-3)}{8}} \cdot p^{\frac{p-3}{2}}$$

□

Proof.

$$\det(V) = \zeta^{\binom{p-1}{2}} \prod_{j>i} (\zeta^j - \zeta^i) = \prod_{j=p-i} (\zeta^j - \zeta^i) \prod_{j \neq p-i} (\zeta^j - \zeta^i)$$
$$= (-1)^{\frac{p-1}{2}} i^{\frac{p-1}{2}} \sqrt{p} \cdot p^{\frac{p-3}{2}}$$

V is conjugate (choosing Dirichlet characters as basis) to a matrix decomposing into 2×2 principal block matrices thus yielding:

$$\det(V) = (-1)^{\frac{p-3}{2}} \prod_{\chi} \tau_\chi = (-1)^{\frac{p-1}{2}} \tau_p (p\chi_2(-1)) \cdots (p\chi_{\frac{p-1}{2}}(-1))$$
$$= (-1)^{\frac{p-1}{2}} \tau_p \cdot \left(\frac{(\frac{p-1}{2})!}{p} \right) \cdot p^{\frac{p-3}{2}}$$
$$= (-1)^{\frac{p-1}{2}} \tau_p \cdot (-1)^{\frac{(p-1)(p-3)}{8}} \cdot p^{\frac{p-3}{2}}$$

□