PRODUSE TRIGONOMETRICE ŞI LEGEA RECIPROCITĂŢII PĂTRATICE

Marcel Ţena[1)]

Abstract. This article presents a modified variant of the trigonometric Eisenstein's proof for quadratic reciprocity law.

Keywords: quadratic reciprocity law, Legendre symbol, Euler's criterion, Gauss's lemma, Eisenstein's proof.

MSC: 11A15

Legea reciprocităţii pătratice este unul dintre cele mai frumoase şi importante rezultate din teoria numerelor. A fost formulată de *Euler* şi *Legendre*, ultimul dându-i şi o demonstraţie parţială. Primul care a demonstrat-o complet, reuşind să-i dea nu mai puţin de şase demonstraţii, a fost *Gauss*, care o numeşte „teorema fundamentală" sau „teorema de aur". Au urmat multe alte demonstraţii sau extinderi (generalizări) date de *Eisenstein, Jacobi, Cauchy, Kummer, Dirichlet, Kronecker, Dedekind, Zolotarev, Hilbert, Artin, Hasse, Barbilian* ş.a. Conform cu [6] există până acum 246 de demonstraţii ale legii reciprocităţii pătratice, iar numărul lucrărilor dedicate diverselor legi de reciprocitate este 1099. Prezentăm în acest articol o demonstraţie inspirată din ideile lui *Eisenstein* ([1],[3]), bazată pe calculul unor produse trigonometrice şi legătura acestora cu simbolul lui *Legendre*. Mai întâi vom defini simbolul lui *Legendre* şi vom enunţa legea reciprocităţii pătratice.

[1)] Prof. dr., Colegiul Naţional „Sf. Sava", Bucureşti.

Definiţie. Dacă p este un număr prim şi $a \in \mathbb{Z}$, $(a,p)=1$, definim *simbolul lui Legendre* prin

$$\left(\frac{a}{p}\right) = \begin{cases} 1\text{ , dacă există } b \in \mathbb{Z} \text{ cu } a \equiv b^2 (\mathrm{mod} p) \text{ (i.e. } \widehat{a} \text{ este pătrat în } \mathbb{Z}_p) \\ -1, \text{în caz contrar.} \end{cases}$$

Când $a \equiv b^2(\text{mod } p)$ spunem că a este *rest pătratic mod* p, iar în caz contrar spunem că a este *nerest pătratic mod* p.

Teorema 1 (legea reciprocităţii pătratice). *Dacă p şi q sunt numere prime impare distincte, are loc egalitatea*:

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

Pentru a demonstra această teoremă, vom parcurge câţiva paşi preliminari.

Teorema 2 (Criteriul lui Euler). *Fie p un număr prim impar şi $a \in \mathbb{Z}$, $(a,p)=1$. Atunci*:

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

Demonstraţie. Este cunoscut că grupul $(\mathbb{Z}_p^*, \cdot)$ este ciclic cu $p-1=2s$ elemente; fie $\widehat{x}$ un generator al său. Avem $\widehat{x}^{2s} = \widehat{1}$ şi $\widehat{x}^s \neq \widehat{1}$, prin urmare $\widehat{x}^s = -\widehat{1}$. Atunci, clasele $\widehat{1}, \widehat{x}^2, \widehat{x}^4, \ldots, \widehat{x}^{2s-2}$ (pătratele perfecte din $\mathbb{Z}_p^*$) au puterea $s = \dfrac{p-1}{2}$ egală cu $\widehat{1}$, în timp ce clasele $\widehat{x}, \widehat{x}^3, \widehat{x}^5, \ldots, \widehat{x}^{2s-1}$ (nepătratele din $\mathbb{Z}_p^*$) au puterea s egală cu $-\widehat{1}$. $\square$

Teorema 3 (Lema lui Gauss). *Fie $p = 2s+1$ un număr prim impar şi $a \in \mathbb{Z}$, $(a,p)=1$. Fiecare dintre numerele $a, 2a, 3a, \ldots, sa$ este congruent* mod p *cu exact unul dintre numerele $\pm 1, \pm 2, \ldots, \pm s$ şi să notăm cu ν numărul acelora dintre $a, 2a, 3a, \ldots, sa$ congruente cu unul dintre numerele $-1, -2, \ldots, -s$. Atunci*:

$$\left(\frac{a}{p}\right) = (-1)^\nu.$$

Demonstraţie. Avem $ak \equiv \pm\sigma(k)(mod\ p)$, $k = \overline{1,s}$, unde σ este o permutare a mulţimii $\{1,2,3,\ldots,s\}$. Înmulţind aceste s congruenţe, obţinem

$$a^s \cdot s! \equiv (-1)^\nu s! \text{ (mod } p)$$

şi simplificând prin $s! \not\equiv 0$ (mod p) rezultă

$$a^s \equiv (-1)^\nu \text{ (mod } p).$$

Dar $a^s = a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$(mod p), conform criteriului lui *Euler*. Aşadar $\left(\frac{a}{p}\right) \equiv (-1)^\nu$(mod p) şi, cum $p > 2$, această congruenţă este o egalitate. $\square$

Teorema 4. *Există egalităţile*:

1° $\displaystyle\prod_{k=1}^{n-1} \sin\frac{k\pi}{n} = \frac{n}{2^{n-1}}$, *pentru* $n \in \mathbb{N}, n \geq 2$.

2° $\displaystyle\prod_{k=1}^{n-1} \cos\frac{k\pi}{n} = \frac{(-1)^{\frac{n-1}{2}}}{2^{n-1}}$, *pentru* $n \in \mathbb{N}, n$ *impar* ≥ 3.

Demonstraţie. Polinomul $X^{n-1} + X^{n-2} + \ldots + X + 1$ are rădăcinile $x_k = \cos\dfrac{2k\pi}{n} + \mathrm{i}\sin\dfrac{2k\pi}{n}$, $k = \overline{1, n-1}$, prin urmare

$$X^{n-1} + X^{n-2} + \ldots + X + 1 = \prod_{k=1}^{n-1}\left(X - \cos\frac{2k\pi}{n} - \mathrm{i}\sin\frac{2k\pi}{n}\right). \tag{1}$$

1° Luăm în (1) $X = 1$ şi obţinem

$$n = \prod_{k=1}^{n-1}\left(1 - \cos\frac{2k\pi}{n} - \mathrm{i}\sin\frac{2k\pi}{n}\right) = \prod_{k=1}^{n-1}\left(2\sin\frac{k\pi}{n}\left(\sin\frac{k\pi}{n} - \mathrm{i}\cos\frac{k\pi}{n}\right)\right) =$$
$$= 2^{n-1} \cdot \prod_{k=1}^{n-1} \sin\frac{k\pi}{n} \cdot \prod_{k=1}^{n-1}\left(\sin\frac{k\pi}{n} - \mathrm{i}\cos\frac{k\pi}{n}\right).$$

Trecând la module, rezultă $n = 2^{n-1}\displaystyle\prod_{k=1}^{n-1}\sin\frac{k\pi}{n}$, adică egalitatea din enunţ.

2° Luăm în (1) $X = -1$ şi avem

$$\begin{aligned}
1 &= \prod_{k=1}^{n-1}\left(-1 - \cos\frac{2k\pi}{n} - \mathrm{i}\sin\frac{2k\pi}{n}\right) = \\
&= (-1)^{n-1}\prod_{k=1}^{n-1}\left(2\cos\frac{k\pi}{n}\left(\cos\frac{k\pi}{n} + \mathrm{i}\sin\frac{k\pi}{n}\right)\right) = \\
&= 2^{n-1}\prod_{k=1}^{n-1}\cos\frac{k\pi}{n} \cdot \left(\cos\frac{(n-1)n\pi}{2n} + \mathrm{i}\sin\frac{(n-1)n\pi}{2n}\right) = \\
&= 2^{n-1}\prod_{k=1}^{n-1}\cos\frac{k\pi}{n} \cdot (\cos\pi + \mathrm{i}\sin\pi)^{\frac{n-1}{2}} = (-1)^{\frac{n-1}{2}} \cdot 2^{n-1}\prod_{k=1}^{n-1}\cos\frac{k\pi}{n},
\end{aligned}$$

de unde $\displaystyle\prod_{k=1}^{n-1}\cos\frac{k\pi}{n} = \frac{(-1)^{\frac{n-1}{2}}}{2^{n-1}}$. □

Teorema 5. *Dacă n este un număr impar ≥ 3, există egalitatea*:

$$n = \prod_{k=1}^{\frac{n-1}{2}}\left(4\sin^2\frac{2k\pi}{n}\right).$$

Demonstraţie. Conform teoremei 4 avem

$$n = 2^{n-1}\prod_{k=1}^{n-1}\sin\frac{k\pi}{n} = 2^{n-1}\prod_{k=1}^{n-1}\frac{\sin\dfrac{2k\pi}{n}}{2\cos\dfrac{k\pi}{n}} = \frac{\displaystyle\prod_{k=1}^{\frac{n-1}{2}}\sin\frac{2k\pi}{n}\cdot\prod_{k=\frac{n+1}{2}}^{n-1}\sin\frac{2k\pi}{n}}{\dfrac{(-1)^{\frac{n-1}{2}}}{2^{n-1}}} =$$

$$= (-1)^{\frac{n-1}{2}}\cdot 2^{n-1}\cdot\prod_{k=1}^{\frac{n-1}{2}}\sin\frac{2k\pi}{n}\cdot\prod_{k=\frac{n+1}{2}}^{n-1}\sin\frac{2k\pi}{n}.$$

În al doilea produs notăm $k = n - l$, cu $l \in \left\{1, 2, \dots, \dfrac{n-1}{2}\right\}$ şi, ţinând seama că $\sin\dfrac{2(n-l)\pi}{n} = -\sin\dfrac{2l\pi}{n}$, acest al doilea produs este egal cu $(-1)^{\frac{n-1}{2}}\cdot\displaystyle\prod_{k=1}^{\frac{n-1}{2}}\sin\frac{2k\pi}{n}$.

Continuând, obţinem $n = (-1)^{\frac{n-1}{2}}\cdot 2^{n-1}\cdot(-1)^{\frac{n-1}{2}}\cdot\left(\displaystyle\prod_{k=1}^{\frac{n-1}{2}}\sin\frac{2k\pi}{n}\right)^2 =$

$$= 4^{\frac{n-1}{2}}\cdot\left(\prod_{k=1}^{\frac{n-1}{2}}\sin\frac{2k\pi}{n}\right)^2 = \prod_{k=1}^{\frac{n-1}{2}}\left(4\sin^2\frac{2k\pi}{n}\right). \qquad \square$$

Teorema 6 (Eisenstein). *Fie p şi q numere prime impare distincte. Atunci:*

$$\left(\frac{q}{p}\right) = \frac{\displaystyle\prod_{k=1}^{\frac{p-1}{2}}\sin\frac{2kq\pi}{p}}{\displaystyle\prod_{k=1}^{\frac{p-1}{2}}\sin\frac{2k\pi}{p}}.$$

Demonstraţie. Dintre numerele $q, 2q, 3q, \dots, \dfrac{p-1}{2}\cdot q$ unele sunt congruente mod p cu unul din numerele $-1, -2, \dots, -\dfrac{p-1}{2}$ şi fie ν numărul acestora; cele rămase sunt congruente cu unul dintre numerele $1, 2, \dots, \dfrac{p-1}{2}$. Conform lemei lui *Gauss* avem $\left(\dfrac{q}{p}\right) = (-1)^\nu$.

Dacă $a \equiv b (\mathrm{mod}\ p)$ avem $\sin\dfrac{2a\pi}{p} = \sin\dfrac{2b\pi}{p}$ şi, deoarece $\sin(-\alpha) = -\sin\alpha$, rezultă

$$\prod_{k=1}^{\frac{p-1}{2}} \sin\frac{2kq\pi}{p} = (-1)^{\nu} \cdot \prod_{k=1}^{\frac{p-1}{2}} \sin\frac{2k\pi}{p} = \left(\frac{q}{p}\right) \cdot \prod_{k=1}^{\frac{p-1}{2}} \sin\frac{2k\pi}{p},$$

de unde egalitatea din enunţ. □

Teorema 7. *Dacă p şi q sunt numere prime impare distincte, atunci*:

$$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot p^{\frac{q-1}{2}} (\text{mod } q).$$

Demonstraţie. Considerăm rădăcina primitivă de ordin p a unităţii $\zeta = \cos\frac{2\pi}{p} + \mathrm{i}\sin\frac{2\pi}{p}$. Pentru orice k întreg avem $\zeta^k - \zeta^{-k} = 2\mathrm{i}\sin\frac{2k\pi}{p}$, prin urmare

$$(\zeta^k - \zeta^{-k})^2 = -4\sin^2\frac{2k\pi}{p}.$$

Notăm cu $\mathbb{Z}[\zeta]$ inelul format din toate expresiile polinomiale în ζ, cu coeficienţi întregi, adică $\mathbb{Z}[\zeta] = \{f(\zeta) | \ f \in \mathbb{Z}[X]\}$. Evident $\zeta \in \mathbb{Z}[\zeta]$, dar şi $\zeta^{-1} = \zeta^{p-1} \in \mathbb{Z}[\zeta]$. Deoarece $C_q^k \equiv 0(\text{mod } q)$, $k = \overline{1, q-1}$, în inelul $\mathbb{Z}[\zeta]$ există congruenţa $(A-B)^q \equiv A^q - B^q(\text{mod } q)$, pentru orice $A, B \in \mathbb{Z}[\zeta]$.

Să mai observăm că $\prod_{k=1}^{\frac{p-1}{2}} (\zeta^k - \zeta^{-k}) \not\equiv 0(\text{ mod } q)$, căci dacă am presupune contrariul, ridicând la pătrat, ar rezulta $\prod_{k=1}^{\frac{p-1}{2}} (\zeta^k - \zeta^{-k})^2 \equiv 0(\text{mod } q)$, adică $\prod_{k=1}^{\frac{p-1}{2}} \left(-4\sin^2\frac{2k\pi}{p}\right) \equiv 0(\text{mod } q)$ sau $(-1)^{\frac{p-1}{2}} \cdot p \equiv 0(\text{mod } q)$, absurd (am ţinut seama de teorema 5 şi de faptul că pentru $a, b \in \mathbb{Z}$ avem $a \equiv b(\text{mod } q)$ în $\mathbb{Z}[\zeta] \Leftrightarrow \ a \equiv b(\text{mod } q)$ în $\mathbb{Z}$).

Având în vedere că $\frac{\zeta^{kq} - \zeta^{-kq}}{\zeta^k - \zeta^{-k}} \in \mathbb{Z}[\zeta]$, aplicând teorema 6, avem succesiv:

$$\left(\frac{q}{p}\right) = \frac{\prod_{k=1}^{\frac{p-1}{2}} \sin\frac{2kq\pi}{p}}{\prod_{k=1}^{\frac{p-1}{2}} \sin\frac{2k\pi}{p}} = \frac{\prod_{k=1}^{\frac{p-1}{2}} \left(2\mathrm{i}\sin\frac{2kq\pi}{p}\right)}{\prod_{k=1}^{\frac{p-1}{2}} \left(2i\sin\frac{2k\pi}{p}\right)} = \frac{\prod_{k=1}^{\frac{p-1}{2}} \left(\zeta^{kq} - \zeta^{-kq}\right)}{\prod_{k=1}^{\frac{p-1}{2}} \left(\zeta^k - \zeta^{-k}\right)} \overset{\text{mod } q}{\equiv}$$

$$\overset{\bmod q}{\equiv} \frac{\prod\limits_{k=1}^{\frac{p-1}{2}} \left(\zeta^k - \zeta^{-k}\right)^q}{\prod\limits_{k=1}^{\frac{p-1}{2}} \left(\zeta^k - \zeta^{-k}\right)} = \prod_{k=1}^{\frac{p-1}{2}} \left(\zeta^k - \zeta^{-k}\right)^{q-1} = \prod_{k=1}^{\frac{p-1}{2}} \left(\left(\zeta^k - \zeta^{-k}\right)^2\right)^{\frac{q-1}{2}} =$$

$$= \prod_{k=1}^{\frac{p-1}{2}} \left(-4\sin^2 \frac{2k\pi}{p}\right)^{\frac{q-1}{2}} = \prod_{k=1}^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} \cdot \left(\prod_{k=1}^{\frac{p-1}{2}} \left(4\sin^2 \frac{2k\pi}{p}\right)\right)^{\frac{q-1}{2}} =$$

$$= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot p^{\frac{q-1}{2}},$$

unde pentru ultima egalitate am aplicat teorema 5. $\square$

Deomonstraţia teoremei 1. Conform criteriului lui *Euler* avem $p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod q$ şi, folosind teorema 7, obţinem

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

Dar $\left(\frac{q}{p}\right)$, $\left(\frac{p}{q}\right) \in \{-1,\ 1\}$, iar $q > 2$, prin urmare congruenţa obţinută este o egalitate, adică

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

Înmulţind cu $\left(\frac{p}{q}\right)$ şi ţinând seama că $\left(\frac{p}{q}\right)^2 = 1$, obţinem

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

Observaţie. Demonstraţia originală a lui *Eisenstein* foloseşte faptul că, pentru q impar, $\sin q\alpha = \sin\alpha \cdot P(\sin^2\alpha)$, unde P este un polinom din $\mathbb{Z}[X]$, de grad $\frac{q-1}{2}$.

Bibliografie

[1] G. Eisenstein: *Applications de l'algèbre à l'arithmétique transcendante*, J. Reine Angew.Math. 29, 1845, 177-184

[2] C. F. Gauss: *Cercetări aritmetice*, Ed. Amarcord, Timişoara, 1999 (traducere de Const. I. Giurescu; prima ediţie: *Disquisitiones Arithmeticae*, Braunschweig, 1801)

[3] F. Lemmermeyer: *Reciprocity Laws from Euler to Eisenstein*, Springer, Berlin, 2000

[4] L. Panaitopol, A. Gica: *O introducere în aritmetică şi teoria numerelor,* Ed. Univ. Bucureşti, 2001

[5] M. Ţena: *Rădăcinile unităţii*, SSMR, Bucureşti, 2005

[6] *Proofs of the Quadratic Reciprocity Law,* `www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`