International Journal of Pure and Applied Mathematics

Volume 22 No. 2 2005, 231-236

ALGEBRAIC PROOF OF GAUSS QUADRATIC RECIPROCITY

Marek Szyjewski

Institute of Mathematics
Silesian University
Bankowa 14 Str., Katowice, 40007, POLAND
e-mail: szyjewsk@gate.math.us.edu.pl

Abstract: Zolotareff expression of Legendre symbol by sign of permutation of regular representation of multiplicative group of a finite field applied to the Galois group of an extension of a finite field yields the Quadratic Reciprocity Law.

AMS Subject Classification: 11A15, 11T99, 12F10
Key Words: Legendre symbol, quadratic reciprocity, permutation, Frobenius automorphism

1. Introduction

There exist at least 214 published proofs (see [1]) of Gauss Theorema Fundamentalis, which nowadays reads as

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{1.1}$$

(p, q - odd primes) with two supplementary laws

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \tag{1.2}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{1.3}$$

Received: June 6, 2005

We prove (1.1) avoiding Gauss Lemma by three classical arguments: the Zolotarev Lemma 2.1, a Galois field $\mathbb{F}_{p^{q-1}}$ computation and a cyclotomic computation.

The proof we present here is intended to be included into an university abstract algebra course as an application. Therefore we name explicitely obvious and standard arguments, which enlarges volume of the paper.

2. The Proof

Let $\mathbb{F}_\rho$ be the Galois field of ρ elements. We shall study squares in this field. The Cayley Representation Theorem yields a homomorphism

$$\lambda : \mathbb{F}_\rho{}^* \to S_\rho$$

into a symmetric group S_ρ of the set $\mathbb{F}_\rho$ such that for $a \in \mathbb{F}_\rho{}^*$ the value λ_a is a permutation

$$\lambda_a(x) = ax.$$

Following lemma is due to Zolotarev ([2]):

Lemma 2.1. *For $a \in \mathbb{F}_\rho{}^*$, a is a square in $\mathbb{F}_\rho$ iff* $\operatorname{sgn}(\lambda_a) = 1$.

Proof. The group $\mathbb{F}_\rho{}^*$, like any finite subgroup of the multiplicative group of a field, is a cyclic group. Let g be a generator of $\mathbb{F}_\rho{}^*$ (a primitive root mod$p$ if $\rho = p$). The permutation λ_g is a cycle

$$\lambda_g = \left(1, g, g^2, \ldots, g^{\rho-2}\right)$$

of length $\rho - 1$.

For $\rho = 2^n$ everything is a square, since in

$$g^k = g^{k+(2^n-1)}$$

one of exponents is even; moreover the length $\rho - 1$ of the cycle λ_g is odd, so λ_g is an even permutation, $\operatorname{sgn}(\lambda_g) = 1$ and therefore $\operatorname{sgn}(\lambda_a) = 1$ for every $a \in \mathbb{F}_\rho{}^*$.

For odd ρ the length of cycle λ_g is even, so λ_g is an odd permutation, $\operatorname{sgn}(\lambda_g) = -1$ and

$$\operatorname{sgn}(\lambda_{g^k}) = (-1)^k. \qquad \square$$

In the particular case $\rho = p$ we obtain the Zolotarev formula

$$\left(\frac{a}{p}\right) = \operatorname{sgn}(\lambda_a). \tag{2.1}$$

From now on we assume that ρ is an odd number.

Corollary 2.2. *The element -1 is a square in $\mathbb{F}_\rho$ iff $\rho \equiv 1(\mathrm{mod}4)$.*

In fact, the permutation λ_{-1} is a product of $(\rho-1)/2$ transpositions $(x,-x)$, so λ_{-1} is an even permutation iff $(\rho-1)/2$ is an even number. The particular case $\rho = p$ of the corollary is the supplementary law (1.2).

Another corollary is (1.3): for $\rho = p$ the exponent

$$\frac{p^2-1}{8} = \frac{p-1}{2} + \frac{p-3}{2} + \cdots + 2 + 1$$

in (1.3) is exactly the number of inversions in

$$\lambda_2 = \begin{pmatrix} 1 & 2 & \cdots & \frac{p-1}{2} & \frac{p+1}{2} & \frac{p+3}{2} & \cdots & p-1 \\ 2 & 4 & \cdots & p-1 & 1 & 3 & \cdots & p-2 \end{pmatrix}.$$

Corollary 2.3. (Euler's Criterion)

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

In fact, there is an explicit formula for the sign of permutation:

$$\left(\frac{a}{p}\right) = \mathrm{sgn}\,(\lambda_a) = \prod_{0\le i<j<p} \frac{\lambda_a(j)-\lambda_a(i)}{j-i} \equiv \prod_{0\le i<j<p} \frac{aj-ai}{j-i},$$

$$\prod_{0\le i<j<p} \frac{aj-ai}{j-i} = a^{p\frac{p-1}{2}} \prod_{i<j} \frac{j-i}{j-i} = a^{p\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p)$$

since $a^p \equiv a(\mathrm{mod}p)$.

Remark 2.1. One may restrict λ_a to the set ${\mathbb{F}_p}^*$ since 0 is a fixed point of λ_a. Comparing signs of λ_a and its restriction yields Fermat's Theorem $a^{p-1} \equiv 1(\mathrm{mod}p)$.

For a closer study of cycle decomposition of the permutation λ_a let $\langle a\rangle$ be a subgroup of ${\mathbb{F}_\rho}^*$ generated by a.

Lemma 2.4. *The element $a \in {\mathbb{F}_\rho}^*$ **is not** a square iff the index $\left[{\mathbb{F}_\rho}^* : \langle a\rangle\right]$ is odd.*

Proof. Let $r(a) = |\langle a\rangle|$ be the order of a in the group ${\mathbb{F}_\rho}^*$. Every element $b \in {\mathbb{F}_\rho}^*$ is a member of the cycle

$$(b, ba, ba^2, \ldots, ba^{r(a)-1}) \tag{2.2}$$

of length $r(a)$ and λ_a is a product of such a cycles for all b from any fixed set of representatives of cosets ${\mathbb{F}_\rho}^*/\langle a\rangle$. So

$$\operatorname{sgn}(\lambda_a) = \left((-1)^{r(a)+1}\right)^{\left[{\mathbb{F}_\rho}^*:\langle a\rangle\right]},$$

where $r(a)$ is the length of cycle (2.2) and $\left[{\mathbb{F}_\rho}^* : \langle a\rangle\right]$ is a number of cycles (2.2). Note that by Lagrange Theorem $r(a)\left[{\mathbb{F}_\rho}^* : \langle a\rangle\right] = \rho - 1$, which is even, so

$$\operatorname{sgn}(\lambda_a) = (-1)^{\left[{\mathbb{F}_\rho}^*:\langle a\rangle\right]}. \qquad \square$$

Again there is a useful formula for Legendre symbol in the case $\rho = p$:

$$\left(\frac{a}{p}\right) = (-1)^{\left[{\mathbb{F}_p}^*:\langle a\rangle\right]}.$$

Let p, q be distinct odd primes and let $\rho = q^{p-1}$. By Fermat's Theorem $q^{p-1} \equiv 1(\mathrm{mod}p)$, so p divides the order of the cyclic group ${\mathbb{F}_\rho}^*$. Let $\omega \in {\mathbb{F}_\rho}^*$ be an element of order p. In formulas $\omega^i\omega^j = \omega^{i+j}$ and $\left(\omega^i\right)^j = \omega^{ij}$ exponents are mod$p$. The powers of ω: $\omega^1, \omega^2, \ldots, \omega^{p-1}$ have order p in the group ${\mathbb{F}_\rho}^*$, so these powers are all roots of the polynomial $X^p - 1$ distinct from 1:

$$f(X) = (X-1)(X-\omega)\left(X-\omega^2\right)\cdot\cdots\cdot\left(X-\omega^{p-1}\right) = X^p - 1.$$

Note that

$$pX^{p-1} = f'(X) = \sum_{i=0}^{p-1}\prod_{j\neq i}\left(X-\omega^j\right) \text{ and } p\omega^{i(p-1)} = \prod_{j\neq i}\left(X-\omega^j\right).$$

The Galois group $\mathrm{Gal}(\mathbb{F}_\rho/\mathbb{F}_q)$ is cyclic of order $p-1$ generated by the Frobenius automorphism $\varphi(x) = x^q$. For $x \in \mathbb{F}_\rho$ the conditions $x \in \mathbb{F}_q$ and $x^q = x$ are equivalent.

The set

$$\Omega = \{\omega^0, \omega^1, \omega^2, \ldots, \omega^{p-1}\}$$

is closed with respect to action of $\mathrm{Gal}(\mathbb{F}_\rho/\mathbb{F}_q)$ and the restriction $\varphi|_\Omega$ of the Frobenius authomorphism φ to Ω is essentially the permutation λ_q of the set $\{0, 1, 2, \ldots, p-1\}$. It follows that

$$\left(\frac{q}{p}\right) = \operatorname{sgn}(\varphi|_\Omega).$$

To compute

$$\operatorname{sgn}(\varphi|_\Omega) = \frac{\prod\limits_{0\le i<j<p}\left(\omega^{qj}-\omega^{qi}\right)}{\prod\limits_{0\le i<j<p}\left(\omega^{j}-\omega^{i}\right)}$$

denote $\delta = \prod\limits_{0\le i<j<p}\left(\omega^j-\omega^i\right)$; so $\operatorname{sgn}(\varphi|_\Omega) = \frac{\delta^q}{\delta}$. Since

$$\prod_{0\le j<i<p}\left(\omega^j-\omega^i\right) = (-1)^{\frac{p(p-1)}{2}}\delta = (-1)^{\frac{p-1}{2}}\delta,$$

we have

$$(-1)^{\frac{p-1}{2}}\delta^2 = \prod_{0\le j<i<p}\left(\omega^j-\omega^i\right)\cdot\prod_{0\le i<j<p}\left(\omega^j-\omega^i\right) = \prod_{k=0}^{p-1}\prod_{l\ne k}\left(\omega^k-\omega^l\right)$$
$$= \prod_{k=0}^{p-1} f'(\omega^k) = \prod_{k=0}^{p-1} p\omega^{k(p-1)} = p^p\cdot\left(\prod_{k=0}^{p-1}\omega^k\right)^{p-1} = p^p\cdot(-f(0))^{p-1} = p^p.$$

It follows that $(-1)^{\frac{p-1}{2}}p$ has a square root $\delta/p^{\frac{p-1}{2}}$ in $\mathbb{F}_\rho$:

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

Now $\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = 1$ iff the root $\delta/p^{\frac{p-1}{2}}$ is in $\mathbb{F}_q$ iff δ is in $\mathbb{F}_q$ iff $\delta^q = \delta$ iff $\operatorname{sgn}(\varphi|_\Omega) = 1$ iff $\left(\frac{q}{p}\right) = 1$. Hence

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

by Euler criterion. Finally the quadratic reciprocity law $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$ is proved. □

References

[1] F. Lemmermeyer, http://www.rzuser.uni-heidelberg.de/˜hb3/fchrono.html

[2] E. Zolotarev, Nouvelle démonstration de la loi de réciprocité de Legendre, *Nouv. Ann. Math*, **11**, No. 2 (1872), 354-362