Serdica
Mathematical Journal
Сердика
Математическо списание

For further information on
Serdica Mathematical Journal
which is the new series of
Serdica Bulgaricae Mathematicae Publicationes
visit the website of the journal http://www.math.bas.bg/~serdica
or contact: Editorial Office
Serdica Mathematical Journal
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Telephone: (+359-2)9792818, FAX:(+359-2)971-36-49
e-mail: serdica@math.bas.bg

Serdica Math. J. **37** (2011), 251–260

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ZOLOTAREV'S PROOF OF GAUSS RECIPROCITY AND JACOBI SYMBOLS

Marek Szyjewski

Communicated by P. Pragacz

Abstract. We extend to the Jacobi symbol Zolotarev's idea that the Legendre symbol is the sign of a permutation, which leads to simple, stright-forward proofs of many results, the proof of the Gauss Reciprocity for Jacobi symbols including.

Introduction. The Quadratic Reciprocity Law was noticed by Legendre, who published in 1788 an incomplete proof. Nevertheless, the Quadratic Reciprocity is usually attributed to Gauss, who included it, with a couple of proofs, into his *Disquisitiones Arithmeticae*, and subsequently published several other proofs. The largest number of different published proofs belongs undoubtedly to Eisenstein; these proofs were published before Gauss's death.

According to `http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html` there are 233 published papers which supposedly contain a proof of the Quadratic Reciprocity Law. Some of them contain only "crucial steps", like a version of Step

2010 *Mathematics Subject Classification:* Primary 11A15.
Key words: Jacobi symbol, Gauss Reciprocity, permutations.

1 in the proof of Theorem 1 below, which is the starting point of the Zolotarev proof of the Quadratic Reciprocity Law (see [3].)

Zolotarev's idea was to represent the Legendre symbol as the sign of a permutation. G. Rousseau noticed that Zolotarev's proof works for the Jacobi symbol in place of the Legendre symbol (see [1].) Our goal is to show that Zolotarev's point of view is the most natural, and leads to the simplest proof of every theorem about quadratic residues on the level of the Jacobi symbol, including the Gauss lemma. The Gauss lemma for the Legendre symbol is the main argument in most proofs of the Quadratic Reciprocity. We prove the Gauss Lemma for the Jacobi symbol (Proposition 3 below,) although we do not need it for the Quadratic Reciprocity.

Apart from the Chinese Remainder Theorem and existence of a primitive root for a prime module, all we need here is elementary properties of permutations.

1. Regular representation and Jacobi symbol.

We denote

$$x \bmod n = x - n \left\lfloor \frac{x}{n} \right\rfloor ,$$

$\mathbb{Z}_n = \mathbb{Z}/\mathbb{Z}n$ the ring of residue classes $\bmod n$, and $x \mapsto x \bmod n$ the canonical map $\mathbb{Z} \to \mathbb{Z}_n$. For fixed integer a, if a is relatively prime to n, then $\lambda_a(x) = ax \bmod n$ is a permutation of the set $\mathbb{Z}_n$. Moreover,

$$\lambda_{ab} = \lambda_a \lambda_b .$$

Theorem 1. *If n is a positive odd integer, then for an integer a relatively prime to n the sign of the permutation λ_a equals the Jacobi symbol $\left(\frac{a}{n}\right)$:*

$$\operatorname{sgn}(\lambda_a) = \left(\frac{a}{n}\right) .$$

Proof. Case 1. If $n = p$ is an odd prime, then 0 is a fixed point of λ_a, $\mathbb{Z}_n \setminus \{0\} = \mathbb{Z}_n^*$ is a cyclic group of even order. If g is a primitive root $\bmod n$ (a generator of $\mathbb{Z}_n^*$), then λ_g is a cycle of even length:

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

Thus λ_g is an odd permutation, and $\lambda_{g^k} = \lambda_g^k$ is an even permutation iff k is even, i.e. iff g^k is a square $\bmod n$. It follows that in this case

$$\operatorname{sgn} \lambda_a = \left(\frac{a}{p}\right),$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol.

Case 2. If $n = p^l$ is a prime power with odd p, we slightly change the notation for this case only: for $k = 1, 2, \ldots$ let

$$\begin{aligned} \lambda_{a,k} &: \mathbb{Z}_{p^k} \to \mathbb{Z}_{p^k} \\ \lambda_{a,k}(x) &= ax \bmod p^k. \end{aligned}$$

Since $\mathbb{Z}_{p^l} = \mathbb{Z}_{p^l}^* \cup (p)$ is a sum of disjoint invariant subsets of $\lambda_a = \lambda_{a,l}$, the sign $\operatorname{sgn}(\lambda_a)$ is the product of signs of restrictions λ', λ'' of λ to those invariant subsets.

$$\operatorname{sgn}(\lambda_{a,l}) = \operatorname{sgn}(\lambda') \operatorname{sgn}(\lambda'').$$

$\mathbb{Z}_{p^l}^*$ is a cyclic group of even order, so the argument of Case 1 applies verbatim:

$$\operatorname{sgn}(\lambda') = \begin{cases} 1 & \text{iff } a \text{ is a square } \bmod p^l \\ -1 & \text{iff } a \text{ is not a square } \bmod p^l \end{cases}.$$

Now, a is a square $\bmod p^l$ iff a is a square $\bmod p$: if $a \equiv b^2 (\bmod p^l)$ then $a \equiv b^2 (\bmod p)$; conversely, if $a \equiv b^2 (\bmod p)$, then

$$a = b^2 (1 + pt),$$

and if

$$\sqrt{1+X} = \sum_{i=0}^{\infty} u_i X^i$$

is a Taylor expansion, then

$$a \equiv b^2 \left(\sum_{i=0}^{\infty} \left(u_i \cdot (tp)^i \right) \bmod p^l \right)^2$$

where all but finite number of terms are 0. Thus

$$\operatorname{sgn}(\lambda') = \left(\frac{a}{p}\right).$$

Now for $\lambda_{a,l-1} : \mathbb{Z}_{p^{l-1}} \to \mathbb{Z}_{p^{l-1}}$ and $\lambda'' : (p) \to (p)$ the map

$$\begin{aligned} f &: \mathbb{Z}_{p^{l-1}} \to (p) \\ f\left(x \bmod p^{l-1}\right) &= px \bmod p^l \end{aligned}$$

is an equivariant bijection, so

$$\operatorname{sgn}\left(\lambda''\right) = \operatorname{sgn}\left(\lambda_{a,l-1}\right).$$

Finally

$$\operatorname{sgn}\left(\lambda_{a,l}\right) = \left(\frac{a}{p}\right) \operatorname{sgn}\left(\lambda_{a,l-1}\right)$$

and, by obvious induction,

$$\operatorname{sgn}\left(\lambda_a\right) = \operatorname{sgn}\left(\lambda_{a,l}\right) = \left(\frac{a}{p}\right)^l = \left(\frac{a}{p^l}\right)$$

by the definition of the Jacobi symbol.

Case 3. (the general case) If

$$n = km$$

with coprime odd factors k, m, then by the Chinese Remainder Theorem

$$\mathbb{Z}_n \cong \mathbb{Z}_k \times \mathbb{Z}_m.$$

Let

$$\begin{aligned} \lambda'_a &: \mathbb{Z}_k \to \mathbb{Z}_k, \qquad \lambda'_a\left(x \bmod k\right) = ax \bmod k \\ \lambda''_a &: \mathbb{Z}_m \to \mathbb{Z}_m, \qquad \lambda''_a\left(x \bmod m\right) = ax \bmod m. \end{aligned}$$

Assume inductively that

$$\operatorname{sgn}\left(\lambda'_a\right) = \left(\frac{a}{k}\right) \text{ and } \operatorname{sgn}\left(\lambda''_a\right) = \left(\frac{a}{m}\right).$$

Let $b \bmod n$ correspond to $(a \bmod k, 1)$ and $c \bmod n$ correspond to $(1, a \bmod m)$ via the Chinese Remainder isomorphism:

$$\begin{aligned} b &\equiv a \,(\bmod k), \qquad c \equiv 1 \,(\bmod k), \\ b &\equiv 1 \,(\bmod m), \qquad c \equiv a \,(\bmod m), \end{aligned}$$

$$a \equiv bc \,(\bmod n),$$

$$\operatorname{sgn}(\lambda_a) = \operatorname{sgn}(\lambda_b)\operatorname{sgn}(\lambda_c).$$

Since

$$\begin{aligned}\lambda_b(x \bmod k, y \bmod m) &= (ax \bmod k, y \bmod m)\\ \lambda_c(x \bmod k, y \bmod m) &= (x \bmod k, ay \bmod m),\end{aligned}$$

we have

$$\begin{aligned}\operatorname{sgn}(\lambda_b) &= \left(\operatorname{sgn}\left(\lambda'_a\right)\right)^m = \operatorname{sgn}\left(\lambda'_a\right) = \left(\frac{a}{k}\right)\\ \operatorname{sgn}(\lambda_c) &= \left(\operatorname{sgn}\left(\lambda''_a\right)\right)^k = \operatorname{sgn}\left(\lambda''_a\right) = \left(\frac{a}{m}\right)\end{aligned}$$

$$\operatorname{sgn}(\lambda_a) = \operatorname{sgn}(\lambda_b)\operatorname{sgn}(\lambda_c) = \left(\frac{a}{k}\right)\left(\frac{a}{m}\right).$$

If

$$n = p_1^{l_1} p_2^{l_2} \cdot \dots \cdot p_s^{l_s}$$

is the prime decomposition of n with distinct odd primes $p_1, p_2, \dots, p_s$, then by induction

$$\operatorname{sgn}(\lambda_a) = \left(\frac{a}{p_1}\right)^{l_1} \cdot \dots \cdot \left(\frac{a}{p_s}\right)^{l_s} = \left(\frac{a}{n}\right)$$

by the definition of the Jacobi symbol. □

Remark 1. Case 1 – of a prime module – was discovered by Zolotarev [3, Th. 1 p. 354]. In [2] elementary properties of the Legendre symbol are derived from the Zolotarev theorem.

Remark 2. $\left(\frac{a}{p^l}\right) = 1$ iff a is a square in the Galois field of p^l elements.

Proposition 1. *If n is an odd integer, then*

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}, \qquad \left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}.$$

P r o o f. Since n is odd, the permutation

$$\lambda_{-1} = (1, n-1)(2, n-2)\cdots\left(\frac{n-1}{2}, \frac{n+1}{2}\right)$$

is a product of $\dfrac{n-1}{2}$ transpositions. The permutation

$$\lambda_2 = \begin{pmatrix} 1 & 2 & \cdots & \dfrac{n-1}{2} & \dfrac{n+1}{2} & n-\dfrac{n-3}{2} & \cdots & n-1 \\ 2 & 4 & \cdots & n-1 & 1 & 3 & \cdots & n-2 \end{pmatrix}$$

has

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

inversions. □

Proposition 2 (Gauss Lemma)**.** *If $n>1$ is an odd integer, and μ is the number of residues $i \le \dfrac{n-1}{2}$ such that $ai \bmod n > \dfrac{n-1}{2}$, then for a coprime to n*

$$\left(\frac{a}{n}\right) = (-1)^{\mu}.$$

P r o o f. In the right-hand side product

$$\operatorname{sgn}(\lambda_a) = \operatorname{sgn}\prod_{i<j}(aj \bmod n - ai \bmod n)$$

factors $(aj \bmod n - ai \bmod n)$ and $(a(n-i) \bmod n - a(n-j) \bmod n)$ for $i<j\le\dfrac{n-1}{2}$ are equal, so the product is a square times

$$\begin{aligned}\prod_{i\le\frac{n-1}{2}<j}(aj \bmod n - ai \bmod n) &= \prod_{i,k\le\frac{n-1}{2}}(a(n-k) \bmod n - ai \bmod n)\\ &= \prod_{i,k\le\frac{n-1}{2}}(n-a(k+i)) \bmod n\end{aligned}$$

In this product there are two equal factors for every pair of integers $u<v\le\dfrac{n-1}{2}$: one for $i=u$, $k=v$ and one for $i=v$, $k=u$. Thus the product is a square times

$$\prod_{i\le\frac{n-1}{2}}(n-2(ai \bmod n))$$

and $n-2(ai \bmod n)<0$ iff $ai \bmod n > \dfrac{n-1}{2}$. The number of such factors is μ. □

2. Main case of Quadratic Reciprocity.

Theorem 2. *If n, m are relatively prime odd integers, then*

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}.$$

P r o o f. We shall do some computations in the ring $\mathbb{Z}_{nm}$. The Chinese Remainder isomorphism $\mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$ shows that

$$\begin{aligned} n^{\varphi(m)} + m^{\varphi(n)} &\equiv 1 (\bmod\, nm), \\ n^{\varphi(m)-1} + m^{\varphi(n)-1} &\equiv (n+m)^{-1} (\bmod\, nm). \end{aligned}$$

The number $n^{\varphi(m)-1}$ differs from n by a square factor ($\varphi(m)$ is even for $m > 2$). Let

$$u = n^{\varphi(m)-1} + m.$$

For the permutation λ_u of the set $\mathbb{Z}_{nm}$

$$\begin{aligned} \operatorname{sgn}(\lambda_u) &= \left(\frac{u}{nm}\right) = \left(\frac{u}{n}\right)\left(\frac{u}{m}\right) \\ &= \left(\frac{n^{\varphi(m)-1}+m}{n}\right)\left(\frac{n^{\varphi(m)-1}+m}{m}\right) \\ &= \left(\frac{m}{n}\right)\left(\frac{n^{\varphi(m)-1}}{m}\right) = \left(\frac{m}{n}\right)\left(\frac{n}{m}\right) \end{aligned}$$

by Theorem 1.

Let

$$z = xn + y$$

be the result of division $z \in \mathbb{Z}_{nm}$ by n with quotient $x \in \mathbb{Z}_m$ and the remainder $y \in \mathbb{Z}_n$. We have

$$\begin{aligned} \lambda_u(xn+y) &= \left(n^{\varphi(m)-1} + m\right)(xn+y) \bmod nm \\ &= ym + xn^{\varphi(m)} + yn^{\varphi(m)-1} \bmod nm \\ &= ym + x - xm^{\varphi(n)} + yn^{\varphi(m)-1} \bmod nm. \end{aligned}$$

We define two new permutations of $\mathbb{Z}_{nm}$. For $w = \lambda_u(xn+y)$ one may express x and y as

$$x = \left\lfloor \frac{\lambda_u^{-1}(w)}{n} \right\rfloor, \qquad y = \lambda_u^{-1}(w) \bmod n.$$

To remove the unwanted term $yn^{\varphi(m)-1}$ in

$$\lambda_u(xn+y) = ym + xn^{\varphi(m)} + yn^{\varphi(m)-1} \bmod nm$$

let

$$\sigma(w) = w - \left(\lambda_u^{-1}(w) \bmod n\right) n^{\varphi(m)-1} \bmod mn.$$

If $w = \lambda_u(xn+y)$, then

$$\sigma \circ \lambda_u(xn+y) = ym + xn^{\varphi(m)} \bmod nm.$$

The correcting term $b = \left(\lambda_u^{-1}(w) \bmod n\right) n^{\varphi(m)-1}$ is constant on each coset $a + n\mathbb{Z}_{nm}$ and $\sigma(w) \equiv w \,(\bmod n)$. Thus each coset $a + n\mathbb{Z}_{nm}$ is an invariant subset of σ and in this subset each cycle

$$(w, w+b, w+2b, \ldots)$$

of σ has length equal to order of b in the additive group $n\mathbb{Z}_{nm} \cong \mathbb{Z}_m$, which divides m, hence is odd. Therefore σ is an even permutation.

Next to correct the term $xn^{\varphi(m)}$ in

$$\sigma \circ \lambda_u(xn+y) = ym + xn^{\varphi(m)} \bmod nm$$

to $x = \sigma \circ \lambda_u(xn+y) \bmod m$ let

$$\begin{aligned} \tau(w) &= w + (w \bmod m)\left(1 - n^{\varphi(m)}\right) \bmod nm \\ &= w + (w \bmod m)\, m^{\varphi(n)} \bmod nm. \end{aligned}$$

First

$$\tau \circ \sigma \circ \lambda_u(xn+y) = ym + x \bmod nm.$$

Second, the correcting term $d = (w \bmod m)\left(1 - n^{\varphi(m)}\right)$ is constant on each coset $c + m\mathbb{Z}_{nm}$ and $\tau(w) \equiv w \,(\bmod m)$. Thus each coset $c + m\mathbb{Z}_{nm}$ is an invariant subset of τ and in this subset each cycle

$$(w, w+d, w+2d, \ldots)$$

of τ has length equal to order of d in the additive group $m\mathbb{Z}_{nm} \cong \mathbb{Z}_n$, which divides n, hence is odd. Therefore τ is an even permutation.

Now

$$\operatorname{sgn}(\lambda_u) = \operatorname{sgn}(\tau \circ \sigma \circ \lambda_u).$$

The natural order in $\mathbb{Z}_{nm}$ corresponds to the lexicographic order of pairs (x, y): for $z_1 = x_1 n + y_1$, $z_2 = x_2 n + y_2$,

$$z_1 < z_2 \text{ iff } \begin{cases} x_1 < x_2 \text{ or} \\ x_1 = x_2 \text{ and } y_1 < y_2 \end{cases}.$$

The analogous statement holds for $v_i = y_i m + x_i$.

The permutation

$$\tau \circ \sigma \circ \lambda_u (xn + y) = ym + x$$

has an inversion in $z_1 < z_2$ iff

$$\begin{cases} x_1 < x_2 \text{ or} \\ x_1 = x_2 \text{ and } y_1 < y_2 \end{cases} \text{ and } \begin{cases} y_2 < y_1 \text{ or} \\ y_1 = y_2 \text{ and } x_2 < x_1 \end{cases}$$

i.e. iff

$$x_1 < x_2 \text{ and } y_2 < y_1,$$

which happens for

$$\frac{m(m-1)}{2} \frac{n(n-1)}{2}$$

pairs $z_1 < z_2$. Therefore

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \operatorname{sgn}(\lambda_u) = (-1)^{mn \frac{n-1}{2} \frac{m-1}{2}} = (-1)^{\frac{n-1}{2} \frac{m-1}{2}}. \qquad \square$$

Remark 3. Zolotarev in [3] restricted his proof to the case of n, m prime and the Legendre symbol. He started with our $\tau \circ \sigma \circ \lambda_u$, composed it with a permutation like σ to get product of Legendre symbols, and computed the sign directly.

Remark 4. G. Rousseau also proved the Quadratic Reciprocity for Jacobi symbols in [1], using a variant of Zolotarev's method.

REFERENCES

[1] G. Rousseau. On the Jacobi symbol. *J. Number Theory* **48**, *1* (1994), 109–111.

[2] M. Szyjewski. Algebraic proof of Gauss Quadratic Reciprocity. *Int. J. Pure Appl. Math.* **22**, *2* (2005) 233–238.

[3] E. I. Zolotarev. Nouvelle démonstration de la loi de réciprocité de Legendre. *Nouv. Ann. Math (2)*, **11** (1872), 354–362.

ul. Mieszka I 15/97
PL40-877 Katowice, Poland
e-mail: szyjewsk@ux2.math.us.edu.pl

Received October 19, 2011