PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 54, January 1975

# A SIMPLE PROOF OF THE ZOLOTAREFF-FROBENIUS THEOREM

ROBERT E. DRESSLER AND ERNEST E. SHULT

ABSTRACT. We give a noncomputational, elementary group-theoretic proof of the Zolotareff-Frobenius Theorem. We use no results from the theory of quadratic residues.

Let $h$ and $k$ be coprime positive integers with $k$ odd and greater than 1. By the symbol $Z(h,k)$ we mean the sign of the permutation $\pi$ induced on the residue classes modulo $k$ obtained by multiplication by $h$.

THEOREM (ZOLOTAREFF-FROBENIUS). *$Z(h,k) = (h/k)$, the usual Jacobi symbol.*

Zolotareff [5] first proved this theorem for prime $k$. Frobenius, cf. [1], then found the general result and Lerch [2], Riesz [4] and Meyer [3] gave subsequent proofs. All these proofs of the general result are, to varying degrees, computational and it is our aim to give a noncomputational, elementary group-theoretic proof in the spirit of Zolotareff's original work.

In the following, $\mathrm{Sym}(X)$ denotes the symmetric group on the finite set $X$. We also write $\operatorname{sgn} \pi = 1$ or $-1$ according as $\pi$ is an even or odd permutation of $X$, so that sgn: $\mathrm{Sym}(X) \to \{1,-1\}$ is the usual group homomorphism. Finally, if $\bar{x}$ is a residue class modulo $n$, then we write $(\bar{x}, n)$ for the common value of $(y,n)$, $y \in \bar{x}$. $|X|$ denotes the cardinality of $X$.

We make use of the following elementary facts:

(1) Let $\sigma_i \in \mathrm{Sym}(X_i)$, $i = 1, \ldots, n$. Let $\sigma = \sigma_1 \times \sigma_2 \times \cdots \times \sigma_n$ be the permutation of $X = X_1 \times \cdots \times X_n$ obtained by applying each $\sigma_i$ to $X_i$. If $y_i = |X| \,/\, |X_i|$, then

$$\operatorname{sgn}(\sigma) = \prod_{i=1}^{n} \operatorname{sgn}(\sigma_i)^{y_i}.$$

PROOF. Let $\hat{\sigma}_i \in \mathrm{Sym}(X)$ be obtained by applying $\sigma_i$ to the $i$th coordinate, and the identity at all other coordinates. Then $\hat{\sigma}_i$ consists of $y_i$ copies of the permutation $\sigma_i$ so $\operatorname{sgn}(\hat{\sigma}_i) = \operatorname{sgn}(\sigma_i)^{y_i}$. Since $\sigma = \hat{\sigma}_1 \cdot \hat{\sigma}_2 \cdots \hat{\sigma}_n$, the result follows.

(2) Let $G$ be a transitive cyclic subgroup of $\mathrm{Sym}(X)$. Then $|G| = |X|$ and for each $x \in G$, $\operatorname{sgn}(x) = 1$ if and only if $x$ is a square in $G$.

(3) Let $N$ be a normal subgroup of odd order in $G$. Then $xN$ is a square in $G/N$ if and only if $x$ is a square in $G$.

(4) If $p$ is an odd prime, then $U(p^k)$, the group of units (mod $p^k$), is cyclic

Received by the editors April 30, 1975.
*AMS (MOS) subject classifications* (1970). Primary 10A15, 20B05.
*Key words and phrases*. Zolotareff's Theorem, permutation, Jacobi symbol.

of order $(p-1)p^{k-1}$. (This is an elementary application of the binomial theorem.)

We now proceed with the proof. From the primary decomposition of $Z$-modules,

$$Z\ /\ (k) = Z\ /\ (p_1^{a_1}) \oplus \cdots \oplus Z\ /\ (p_n^{a_n}),$$

we see that if $\pi_i$ is the permutation of $X_i = Z\ /\ (p_i^{a_i})$ induced by multiplication by $h$ and $y_i = k\ /\ p_i^{a_i}$, then (1) implies

$$\begin{aligned} Z(h,k) &= \prod_i \operatorname{sgn}(\pi_i)^{y_i} = \prod \operatorname{sgn}\pi_i \quad (\text{since } y_i \text{ is odd}) \\ &= \prod_i Z(h, p_i^{a_i}). \end{aligned}$$

Thus it suffices to take $k = p^a$, an odd prime power.

If $X = Z\ /\ (k)$, set $D_m = \{\bar{x} \in X \mid (\bar{x}, k) = p^m\}$. We have

(5) $X = D_0 + D_1 + \cdots + D_a$,

where $|D_i| = (p-1)p^{a-i-1}$ for $i \leqslant a-1$ and $D_a = \{\bar{0}\}$. Then $\bar{h} = h + (k) \in D_0 = U(k)$ and the group $D_0$ acts on $X$ with (5) being a decomposition into $D_0$-orbits. Thus $\pi = \tau_0 \cdots \tau_a$, where $\tau_i$ is the permutation of $X$ induced by applying multiplication by $h$ to the elements of $D_i$ only and applying the identity permutation elsewhere. Since $\tau_a = 1_X$ it remains only to determine $\operatorname{sgn}\tau_i$ for $i \leqslant a-1$.

By (4) $D_0$ is a cyclic group acting transitively on each $D_i$ and so $D_0\ /\ K_i$ is a cyclic regular group of permutations of $D_i$, where $K_i = \ker[D_0 \to \operatorname{Sym}(D_i)]$, $i = 1, \ldots, a-1$. Thus $|K_i| = p^i$ is odd, $i \leqslant a-1$, so by (3) $\bar{h}$ is a square mod $K_i$ if and only if $\bar{h}$ is a square in $D_0$. Thus $\operatorname{sgn}(\tau_0) = \operatorname{sgn}(\tau_1) = \cdots = \operatorname{sgn}(\tau_{a-1})$, whence

(6) $Z(h,k) = \operatorname{sgn}(\tau_{a-1})^a$.

Now $\operatorname{sgn}(\tau_{a-1}) = \operatorname{sgn}(\bar{\tau}_{a-1})$ where $\bar{\tau}_{a-1}$ is the restriction of $\tau_{a-1}$ to $D_{a-1}$. Since $M = D_{a-1} \cup D_a$ is a submodule of $X$ with annihilator $(p)$ we see that $M$ and $Z\ /\ (p)$ are isomorphic $Z$-modules and so by (2), $\operatorname{sgn}(\bar{\tau}_{a-1}) = 1$ if and only if $h + (p)$ is a square in $U(p)$ (that is to say, $h$ is a quadratic residue modulo $p$). Thus $\operatorname{sgn}(\tau_{a-1}) = (h/p)$, the Legendre symbol. Hence by (6)

$$Z(h,k) = (h/p)^a.$$

This completes the proof.

## References

1. G. Frobenius, *Über das quadratische Reziprozitätsgesetz*. I, S.-B. Preuss. Akad. Wiss. Berlin **1914**, 335—349.

2. M. Lerch, *Sur un Théorème arithmétique de Zolotarev*, Bull. Intern. **3**, Prague, 1896.

3. C. Meyer, *Über einige Andwendungen Dedkindscher Summen*, J. Reine Angew. Math. **198** (1957), 143—203. MR **21** #3396.

4. M. Riesz, *Sur le lemme de Zolotareff et sur la loi de réciprocité des restes quadratiques*, Math. Scand. **1** (1955), 159—169. MR **15**, 200.

5. E. Zolotareff, *Nouvelle démonstration de la loi de réciprocité de Legendre*, Novelles Ann. Math. (2) **11** (1872), 355—362.

Department of Mathematics, Kansas State University, Manhattan, Kansas 66506