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 $A$ 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). $Z(h,k) = (A/A:)$, 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, $\text{Sym}(X)$ denotes the symmetric group on the finite set $X$. We also write $\text{sgn} \pi = 1$ or $-1$ according as $\pi$ is an even or odd permutation of $X$, so that $\text{sgn}: \text{Sym}(X) \to \{1,-1\}$ 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 $(y,n)$, $y \in x$. $|X|$ denotes the cardinality of $X$.

We make use of the following elementary facts:

(1) Let $a_i \in \text{Sym}(X)$, $i = 1, \ldots, n$. Let $a = a_1 \times a_2 \times \cdots \times a_n$ be the permutation of $X = x_1 \times \cdots \times x_n$ obtained by applying each $a_i$ to $x_i$. If $y_i = |X| / |x_i|$, then

$$\text{sgn}(a) = \prod_{i=1}^{n} \text{sgn}(a_i)^{y_i}.$$ 

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

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

(3) Let $N$ be a normal subgroup of odd order in $G$. Then $\text{sgn}(xN) = 1$ if and only if $x$ is a square in $G/N$.

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

Received by the editors April 30, 1975.


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 \(\mathbb{Z}\)-modules,

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

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

\[
Z(h, k) = \prod_i \text{sgn}(\pi_i)^{y_i} = \prod_i \text{sgn} \pi_i \quad \text{(since \(y_i\) is odd)}
\]

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

If \(X = \mathbb{Z} / (k)\), set \(D_m = \{x \in X | (x, k) = m^m\}\). We have

\[
(5) \quad X = D_0 + D_1 + \cdots + D_a,
\]

where \(|D_i| = (p - 1)p^{a-i-1}\) for \(i \leq a - 1\) and \(D_a = \{0\}\). Then \(\tilde{h} = h + (k) \in D_0 = U(k)\) and the group \(D_0\) acts on \(X\) with (5) being a decomposition into \(D_0\)-orbits. Thus \(\pi = \tau_0 \cdots \tau_{a-1}\), 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 \(\tau_a = 1\) it remains only to determine \(\text{sgn} \tau_i\) for \(i \leq a - 1\).

By (4) \(D_0\) is a cyclic group acting transitively on each \(D_i\) and so \(D_0 \not\sim K_i\) is a cyclic regular group of permutations of \(D_i\), where \(K_i = \ker[D_0 \to \text{Sym}(D_i)]\), \(i = 1, \ldots, a - 1\). Thus \(|K_i| = p^l\) is odd, \(i \leq a - 1\), so by (3) \(\tilde{h}\) is a square mod \(K_i\) if and only if \(\tilde{h}\) is a square in \(D_0\). Thus \(\text{sgn}(\tau_0) = \text{sgn}(\tau_1) = \cdots = \text{sgn}(\tau_{a-1})\), whence

\[
(6) \quad Z(h, k) = \text{sgn}(\tau_{a-1})^a.
\]

Now \(\text{sgn}(\tau_{a-1}) = \text{sgn}(\tau_{a-1})^a\) where \(\tau_{a-1}\) 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 \(\mathbb{Z}\)-modules and so by (2), \(\text{sgn}(\tau_{a-1}) = 1\) if and only if \(h + (p)\) is a square in \(U(p)\) (that is to say, \(h\) is a quadratic residue modulo \(p\)). Thus \(\text{sgn}(\tau_{a-1}) = (h/p)\), the Legendre symbol. Hence by (6)

\[
Z(h, k) = (h/p)^a.
\]

This completes the proof.

**References**