Pacific Journal of Mathematics

ZOLOTAREV'S THEOREM ON THE LEGENDRE SYMBOL

J. L. Brenner

Vol. 45, No. 2 October 1973

PACIFIC JOURNAL OF MATHEMATICS
Vol. 45, No. 2, 1973

ZOLOTAREV'S THEOREM ON THE LEGENDRE SYMBOL

J. L. BRENNER

Dedicated to Professor D. H. Lehmer

Matrix-theoretic proof that $(a/p) =$ sign of the permutation $i(\text{mod } p) \rightarrow ia(\text{mod } p)$ of the residue classes $\text{mod } p$.

In [5], Zolotarev proved the quadratic reciprocity law on the basis of the above-stated result. Here is a short proof of that result; it uses matrix theory, together with a well-known result in number theory.

DEFINITION 1. An a-circulant is an $n \times n$ matrix such that each row (except the first) is obtained from the preceding by shifting each element a positions to the right.

DEFINITION 2. $P = (p_{ij})$ denotes the $n \times n$ permutation matrix that corresponds to the permutation $i \rightarrow i + 1$ (mod n), i.e., $p_{12} = p_{23} = \cdots = p_{n-1,n} = p_{n1} = 1$; $p_{ij} = 0$ otherwise.

Note that P^a, the ath power of P, is an a-circulant.

DEFINITION 3. $A(a)$ denotes the a-circulant, the first row of which has 1 in the ath column and zeros elsewhere.

Note that $PA(a) = A(a)P^a$.

THEOREM 4. Det $A(a) =$ *sign of the permutation* $i(\text{mod } n) \rightarrow ia(\text{mod } n)$.

This follows from one of the usual definitions of the determinant function.

LEMMA 5. *If the first row of* $A(a_1)$ *is multiplied by the matrix* $A(a_2)$, *the product is: the row that has all zeros except for* 1 *in the position* $a_1a_2(\text{mod } n)$. [Obvious.]

THEOREM 6. *The product of an* a_1-*circulant by an* a_2-*circulant is an* a_1a_2-*circulant.*

Proof. $PA(a_1)A(a_2) = A(a_1)A(a_2)P^e$, $e = a_1a_2$.

COROLLARY 7. $A(a_1)A(a_2) = A(a_1a_2)$;

$$\det A(a_1) \det A(a_2) = \det A(a_1a_2) .$$

COROLLARY 8. *For* $(a, n) = 1$, *the determinant of the set* $\{A(a)\}$ *is a character* $\text{mod } n$.

LEMMA 9. *If $a = g$ is a primitive root of the odd prime number $p = n$, then* $\det A(g) = -1$.

Proof. The corresponding permutation is an $(n-1)$-cycle; its sign is -1.

THEOREM 10. *If n is an odd prime p, then* $\det A(a) = (a/p)$, *the Legendre symbol.*

Proof. The Legendre symbol is the only real character modulo a prime that actually assumes the value -1.

COROLLARY 11. [Zolotarev]. $(a/p) =$ *sign of the permutation*

$$i(\mathrm{mod}\ p) \longrightarrow ia(\mathrm{mod}\ p), \text{ where } p \text{ is a prime.}$$

REMARK. The result $\det A(a) = (a/n)$ does hold in general [4]. When n is an odd prime power, this is obvious since n has a primitive root. For other odd n, it seems less obvious. See [2, 3] for proof.

Concluding remark. As Zolotarev showed, the argument of this article furnishes yet another proof, and the first matrix-theoretic one, of the quadratic reciprocity law.

Acknowledgment. I thank Professor D. H. Lehmer for asking whether the methods developed in [1] could be used to prove that $\det A(a) = (a/p)$.

REFERENCES

1. C. M. Ablow and J. L. Brenner, *Roots and canonical forms of circulant matrices*, Trans. Amer. Math. Soc., **107** (1963), 360-376.
2. J. L. Brenner, *A new property of the Jacobi symbol*, Duke Math. J., **29** (1962), 29-32.
3. D. H. Lehmer, *Mahler's matrices*, Notices of the Amer. Math. Soc., **1**, 365. abstract 569-50; Australian J. Math., I (1959/60), 385-395.
4. M. Riesz, *Sur le lemme de Zolotareff et sur la loi de réciprocité des restes quadratiques*, Math. Scand., **1** (1953), 159-169.
5. G. Zolotareff, *Nouvelle démonstration de la loi de réciprocité de Legendre*, Nouvelles Annales de Math. (ser. 2) **11** (1872), 354-362.

Received February 2, 1972. Supported by NSF Grant GP-32527.

UNIVERSITY OF VICTORIA, CANADA
AND
COLLEGE OF NOTRE DAME, BELMONT, CALIFORNIA

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. The editorial "we" must not be used in the synopsis, and items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. Index to Vol. **39**. All other communications to the editors should be addressed to the managing editor, Richard Arens, University of California, Los Angeles, California, 90024.

50 reprints are provided free for each article; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is issued monthly as of January 1966. Regular subscription rate: $48.00 a year (6 Vols., 12 issues). Special rate: $24.00 a year to individual members of supporting institutions.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 270, 3-chome Totsuka-cho, Shinjuku-ku, Tokyo 160, Japan.

Pacific Journal of Mathematics

Vol. 45, No. 2 October, 1973