

Pacific Journal of Mathematics

ZOLOTAREV'S THEOREM ON THE LEGENDRE SYMBOL

J. L. BRENNER

ZOLOTAREV'S THEOREM ON THE LEGENDRE SYMBOL

J. L. BRENNER

Dedicated to Professor D. H. Lehmer

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

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 $i \rightarrow i + 1 \pmod{n}$, i.e., $p_{i2} = p_{23} = \dots = p_{n-1,n} = p_{n1} = 1$; $p_{ij} = 0$ otherwise.

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

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

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

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

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 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]. $(a/p) = \text{sign of the permutation } i(\text{mod } p) \longrightarrow ia(\text{mod } p), \text{ where } p \text{ is a prime.}$

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

EDITORS

H. SAMELSON

Stanford University
Stanford, California 94305

J. DUGUNDJI

Department of Mathematics
University of Southern California
Los Angeles, California 90007

C. R. HOBBY

University of Washington
Seattle, Washington 98105

RICHARD ARENS

University of California
Los Angeles, California 90024

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY

UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY
NAVAL WEAPONS CENTER

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

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.

| | |
|--|-----|
| Kenneth Paul Baclawski and Kenneth Kapp, <i>Induced topologies for quasigroups and loops</i> | 393 |
| D. G. Bourgin, <i>Fixed point and min – max theorems</i> | 403 |
| J. L. Brenner, <i>Zolotarev's theorem on the Legendre symbol</i> | 413 |
| Joseph Atkins Childress, Jr., <i>Restricting isotopies of spheres</i> | 415 |
| John Edward Coury, <i>Some results on lacunary Walsh series</i> | 419 |
| James B. Derr and N. P. Mukherjee, <i>Generalized Sylow tower groups. II</i> | 427 |
| Paul Frazier Duvall, Jr., Peter Fletcher and Robert Allen McCoy, <i>Isotopy Galois spaces</i> | 435 |
| Mary Rodriguez Embry, <i>Strictly cyclic operator algebras on a Banach space</i> | 443 |
| Abi (Abiadbollah) Fattahi, <i>On generalizations of Sylow tower groups</i> | 453 |
| Burton I. Fein and Murray M. Schacher, <i>Maximal subfields of tensor products</i> | 479 |
| Ervin Fried and J. Sichler, <i>Homomorphisms of commutative rings with unit element</i> | 485 |
| Kenneth R. Goodearl, <i>Essential products of nonsingular rings</i> | 493 |
| George Grätzer, Bjarni Jónsson and H. Lakser, <i>The amalgamation property in equational classes of modular lattices</i> | 507 |
| H. Groemer, <i>On some mean values associated with a randomly selected simplex in a convex set</i> | 525 |
| Marcel Herzog, <i>Central 2-Sylow intersections</i> | 535 |
| Joel Saul Hillel, <i>On the number of type-k translation-invariant groups</i> | 539 |
| Ronald Brian Kirk, <i>A note on the Mackey topology for $(C^b(X))^*$, $C^b(X)$</i> | 543 |
| J. W. Lea, <i>The peripherality of irreducible elements of lattice</i> | 555 |
| John Stewart Locker, <i>Self-adjointness for multi-point differential operators</i> | 561 |
| Robert Patrick Martineau, <i>Splitting of group representations</i> | 571 |
| Robert Massagli, <i>On a new radical in a topological ring</i> | 577 |
| James Murdoch McPherson, <i>Wild arcs in three-space. I. Families of Fox-Artin arcs</i> | 585 |
| James Murdoch McPherson, <i>Wild arcs in three-space. III. An invariant of oriented local type for exceptional arcs</i> | 599 |
| Fred Richman, <i>The constructive theory of countable abelian p-groups</i> | 621 |
| Edward Barry Saff and J. L. Walsh, <i>On the convergence of rational functions which interpolate in the roots of unity</i> | 639 |
| Harold Eugene Schlais, <i>Non-aposyndesis and non-hereditary decomposability</i> | 643 |
| Mark Lawrence Teply, <i>A class of divisible modules</i> | 653 |
| Edward Joseph Tully, Jr., <i>\mathcal{H}-commutative semigroups in which each homomorphism is uniquely determined by its kernel</i> | 669 |
| Garth William Warner, Jr., <i>Zeta functions on the real general linear group</i> | 681 |
| Keith Yale, <i>Cocycles with range $\{\pm 1\}$</i> | 693 |
| Chi-Lin Yen, <i>On the rest points of a nonlinear nonexpansive semigroup</i> | 699 |