AMERICAN MATHEMATICAL SOCIETY
MathSciNet Mathematical Reviews on the Web

Previous | Up | Next Article

Citations
From References: 97
From Reviews: 18

MR1625181 (99d:11092) 11L05 (11A15 11L10 11T22 11T24)

Berndt, Bruce C. (1-IL); **Evans, Ronald J.** (1-UCSD); **Williams, Kenneth S.** (3-CARL)

★**Gauss and Jacobi sums.**

Canadian Mathematical Society Series of Monographs and Advanced Texts.
A Wiley-Interscience Publication.
John Wiley & Sons, Inc., *New York*, 1998. *xii*+583 *pp*. $69.95. *ISBN* 0-471-12807-4

FEATURED REVIEW.

Gauss and Jacobi sums have been a subject of high interest in number theory ever since Gauss used the former in his *Disquisitiones arithmeticae* (1801) and Jacobi used the latter in his paper "Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie" (1837). In both cases, the notions had been introduced earlier: for Gauss sums, by Lagrange in 1771 under the name of "resolvents"; for Jacobi sums, by Gauss in his unpublished manuscripts, by Jacobi himself in a letter of 1827 to Gauss and, independently, by Cauchy in 1829. In the nineteenth century, among the most notable contributors to the development and applications—to "cyclotomy", quadratic partitions of primes and reciprocity laws—of these sums were Gauss, Jacobi, Cauchy, Eisenstein, Kummer and Stickelberger. In the present century, there has been a great extension of the investigations and applications of these subjects. Among the topics of research involving Gauss and Jacobi sums are the study of cyclotomic fields, the derivation of reciprocity laws, the counting of the solutions of equations over finite fields and the study of the corresponding zeta functions, the construction of Hecke characters and the determination of their conductors, the explicit evaluation and the estimates of various related exponential sums, the relations and congruences among these sums and between them and the binomial coefficients or the p-adic gamma functions, the study of quadratic forms and that of power residue distributions. Further applications are concerned with combinatorial designs, coding theory and primality testing. The literature concerning these topics is immense and scattered in a great many papers, by numerous contributors. Some of the most cited references are by Hasse, Davenport, Weil, Mordell, Carlitz, Gross, Koblitz, Katz, Patterson, Chowla, Lehmer, and others. Until recently, the main source book for Gauss sums was H. Hasse's book [*Vorlesungen über Zahlentheorie*, Zweite neubearbeitete Auflage. Die Grundlehren der Mathematischen Wissenschaften, Springer, Berlin, 1964; MR0188128 (32 #5569)], which has a chapter dealing with the subject. Then a few more books treated in some detail Gauss and Jacobi sums, such as those of K. F. Ireland and M. I. Rosen [*A classical introduction to modern number theory*, Second edition, Springer, New York, 1990; MR1070716 (92e:11001)], S. Lang [*Cyclotomic fields*, Springer, New York, 1978; MR0485768 (58 #5578); *Vol. II*, 1980; MR0566952 (81i:12004)], L. C. Washington [*Introduction to cyclotomic fields*, Springer, New York, 1982; MR0718674 (85g:11001)], and R. Lidl and H. Niederreiter [*Finite fields*, Addison-Wesley, Reading, MA, 1983; MR0746963 (86c:11106)]. Also, a different approach to the study of Gauss and Kloosterman sums, via sheaf-theoretic methods, was presented by N. M. Katz [*Gauss sums, Kloosterman sums, and monodromy groups*, Princeton Univ. Press, Princeton, NJ, 1988; MR0955052 (91a:11028)]. However, the present book is exclusively concerned with Gauss, Jacobi and closely related sums, and gives the most extensive and systematic treatment of the subject, by a relatively elementary approach.

The basic theory of Gauss and Jacobi sums, over finite fields, is presented in a simple and efficient way in Chapters 1 and 2. There is in particular a reciprocity relation for generalized quadratic Gauss sums, proved using Cauchy's residue theorem, then applied to evaluate the classical quadratic Gauss sum. The latter is also obtained by two more elementary methods. One section deals with character sums over finite residue rings of integers. The cyclotomic numbers, which are linear combinations of Jacobi sums, are considered over a prime field $\mathbf{F}_p$ in Chapter 2 and over any finite field $\mathbf{F}_{p^r}$ in Chapter 11. A main theme of the book is the evaluation of various character sums of certain orders. A Gauss sum is (to within a well-determined root of unity factor) of the form $G_r(\chi) = \sum_{t\in\mathbf{F}_q} \chi(t)\zeta_p^{\mathrm{tr}(t)}$, where χ is a multiplicative character on the finite field $\mathbf{F}_q$, with $q = p^r$, p a prime number, $\zeta_p = e^{2\pi i/p}$ in $\mathbf{C}$ and tr is the trace map in $\mathbf{F}_q|\mathbf{F}_p$. A Jacobi sum can be written $J_r(\chi^m, \chi^n) = \sum_{t\in\mathbf{F}_q} \chi^m(t)\chi^n(1-t)$. The order k of these sums is that of the character χ. Another type of Gauss sum of order (a positive integer) k is $g_r(k) = \sum_{t\in\mathbf{F}_q} \zeta_p^{\mathrm{tr}(t^k)}$. It is related to the previous one by $g_r(k) = \sum_{j=1}^{k-1} G_r(\chi^j)$, provided that k divides $q-1$, with χ any character of order k on $\mathbf{F}_q$. In Chapter 3, the Jacobi sums over $\mathbf{F}_p$ of orders $k \leq 12$, $k \neq 9, 11$, and $k = 16, 20, 24$ are determined in terms of corresponding quadratic partitions of p. In Chapter 4, expressions of $g_1(k)$ for $k = 3, 4, 6$ are stated in terms of a Weierstrass $\wp$-function, and for $k = 8, 12$, they are given with a sign ambiguity. In Chapter 6, the Jacobsthal sums, which are related to Jacobi sums, are studied and similarly evaluated for some orders of characters. In Chapter 12, the Eisenstein sums, related to Gauss sums, are studied, and those of various orders over $\mathbf{F}_q$ are evaluated, which in turn allows the evaluation of $g_r(3)$ and $g_r(4)$. Another type of sum related to the Jacobsthal and Eisenstein sums, the Brewer sum, is studied and evaluated in Chapter 13. The Gaussian (f-nomial) periods over $\mathbf{F}_p$, closely related to the Gauss sums, are considered and applied in Chapter 5, which deals with "difference sets", and they are studied further in Chapter 10, while the periods over $\mathbf{F}_q$ are introduced in Chapter 12. The properties of Gauss sums are used, in Chapters 7 and 8, to derive various power residuacity criteria of small primes modulo a fixed prime p, in terms of quadratic partitions of p, and to obtain the cubic, biquadratic and some rational reciprocity laws. In Chapter 9, congruences $(\bmod\, p)$ for binomial coefficients, in terms of quadratic partitions of p, are established, using Jacobi sums; some of them are extended to congruences $(\bmod\, p^2)$ using the Gross-Koblitz formula, which relates the p-adic gamma function to Gauss sums. In Chapter 10, the number of solutions of diagonal equations over $\mathbf{F}_q$ is obtained in terms of generalized Jacobi sums (depending on more than two characters); the latter are first studied and some of the properties of the previously considered Jacobi sums are extended to them; upper bounds for the number of solutions are also deduced from those expressions. Chapter 11 contains the deepest results, namely the classical Stickelberger congruence for Gauss sums—yielding the prime ideal factorizations of Gauss and Jacobi sums—the Davenport-Hasse product formula for Gauss sums and the Davenport-Hasse theorem for lifted Gauss sums; the chapter concludes with an application to irreducible cyclic codes. Finally, Chapter 14 presents an extension of the classical Eisenstein reciprocity law to the p^nth power residue symbol, using the properties of Gauss and Jacobi sums, namely their prime ideal factorization, and based on work by A. E. Western (1907–1908).

Every chapter ends with a set of problems that complement and extend the results in the text.

These are followed by invaluable notes giving references to the vast literature, outlining the history of the results, and indicating links to related subjects and some current research directions. In this respect, the book ends with an interesting list of 28 open problems. The bibliography, which covers 66 pages, is fairly complete. Relatively few errors were found, most of which are easy to correct by the reader. On page 11, formula (1.1.4) is valid provided k divides $q-1$. On page 271, in Theorem 9.2.6, t is to be replaced by a_7. On page 362, before formula (11.6.1), the reference should be to Theorem 2.1.3(a) instead of Theorem 1.1.4(a). On page 365, after (11.6.4), one should read: let γ be a generator of $\mathbf{F}_q^*$ (instead of $\mathbf{F}_q$). On page 444, in formula (13.2.6), the second of the three terms in the equality ought to be $\Omega_d(a^{n/d})$. On page 468, after (14.1.1), where the domain of Φ_a is extended "to all nonzero ideals of O_K" and where $\Phi_a(\alpha)$ is defined, one should add the condition that these ideals and elements α of O_K be relatively prime to k. On page 470, the definition of a primary element as stated is not equivalent to (14.2.2) (which is the only condition used in the sequel), since if $l > 2$, one may have M odd and $\varepsilon_c(\nu) = (-1)^M = -1$; to correct this, one may either adopt (14.2.2) as the definition or set in the existing definition $\varepsilon_c(\nu) = (-1)^{M(k-1)}$.

The book is carefully written, in a clear and fluent style, which makes it accessible to a broad audience. It undoubtedly reaches its goal of being a "user-friendly" introduction to the subject, focused on "examining basic properties of Gauss and Jacobi sums, providing systematic and explicit evaluations of these sums, and providing applications". Even though it does not exhaust the immense subject of exponential sums, it should prove to be a standard reference.

Reviewed by *Charles Helou*