BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 5, Number 2, September 1981

THE DETERMINATION OF GAUSS SUMS

BY BRUCE C. BERNDT[1] AND RONALD J. EVANS[2]

1. Introduction. Almost every student with a modicum of knowledge about geometric series can show that

$$\sum_{n=0}^{p-1} e^{2\pi in/p} = 0,$$

where p is any integer exceeding one. Suppose that we replace n by n^k in the sum, where k is an integer *greater* than one. The task of determining the sum then becomes considerably more difficult. In fact, for $k = 2$, it took Gauss several years to accomplish this. Define the Gauss sums $\mathcal{G}(k, p) = \mathcal{G}(k)$ by

$$\mathcal{G}(k) = \sum_n e^{2\pi in^k/p},$$

where k is a positive integer, p is a prime with $p \equiv 1 \pmod k$, and Σ_n indicates that the sum on n is over an arbitrary complete residue system $(\operatorname{mod} p)$. Closely connected with $\mathcal{G}(k)$ is the sum

$$G(\chi) = \sum_n \chi(n) e^{2\pi in/p},$$

where χ is a character $(\operatorname{mod} p)$ of order k. Both $\mathcal{G}(k)$ and $G(\chi)$ are called Gauss sums of order k and are intimately linked by the equalities

$$\mathcal{G}(k) = \sum_n e^{2\pi in/p}\{1 + \chi(n) + \cdots + \chi^{k-1}(n)\} = \sum_{j=1}^{k-1} G(\chi^j). \tag{1.1}$$

The first equality in (1.1) is a simple consequence of the fact that the sequence $\{n^k\}$, $1 \leqslant n \leqslant p - 1$, runs through the set of kth power residues $(\operatorname{mod} p)$ exactly k times.

The primary purpose of this paper is to survey the present knowledge on the values of the Gauss sums $\mathcal{G}(k)$ and $G(\chi)$, and to convey some of the principal ideas used in their determinations. We also briefly discuss more general Gauss sums.

We begin by making some elementary remarks about the values of Gauss sums. It is easily verified by direct multiplication that, for nonprincipal χ,

$$G(\chi)G(\bar{\chi}) = \chi(-1)p; \tag{1.2}$$

Received by the editors September 15, 1980.

1980 *Mathematics Subject Classification.* Primary 10G05.

Key words and phrases. Gauss sums, Jacobi sums, characters on finite fields, period equation, Kummer conjecture.

[1] Research partially supported by National Science Foundation grant no. MCS-7903359.

[2] Author supported by National Foundation Grant MCS-8101860.

see, e.g. [**80**, p. 91]. It follows that for such χ,

$$|G(\chi)| = \sqrt{p}. \tag{1.3}$$

Hence, (1.1) implies that

$$|\mathcal{G}(k)| \leqslant (k-1)\sqrt{p}. \tag{1.4}$$

1.1. Quadratic Gauss sums. Let us now look at the case $k = 2$ considered by Gauss. By (1.1),

$$\mathcal{G}(2) = \sum_n \left(\frac{n}{p}\right) e^{2\pi i n/p} = G(\chi), \tag{1.5}$$

where here $\chi(n) = (n/p)$ denotes the Legendre symbol. Replacing n by $-n$ in (1.5), we see that $\mathcal{G}(2)$ is real or purely imaginary according as $p \equiv 1$ or $3 \pmod 4$. Therefore, from (1.3) and (1.5),

$$\mathcal{G}(2) = \begin{cases} \pm\sqrt{p}, & \text{if } p \equiv 1 \pmod 4, \\ \pm i\sqrt{p}, & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{1.6}$$

In late May of 1801, Gauss conjectured that, in fact,

$$\mathcal{G}(2) = \begin{cases} \sqrt{p}, & \text{if } p \equiv 1 \pmod 4, \\ i\sqrt{p}, & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{1.7}$$

On August 30, 1805, Gauss wrote in his diary [**63**, pp. 37, 57], "Demonstratio theorematis venustissimi supra 1801 Mai commemorati, quam per 4 annos et ultra omni contentione quaesiveramus, tandem perfecimus." (At length we achieved a demonstration of the very elegant theorem mentioned before in May, 1801, which we had sought for more than four years with all efforts.) Gauss's proof, which is elementary, was published in 1811 [**64**], [**66**, pp. 9–45, 155–158]. In §2, we discuss this proof and a variety of other proofs of (1.7).

1.2. Jacobi sums. Jacobi sums play a central role in the determination of $\mathcal{G}(k)$ and $G(\chi)$ for $k > 2$. For characters χ and ψ (mod p), the Jacobi sum $J(\chi, \psi)$ is defined by

$$J(\chi, \psi) = \sum_n \chi(n)\psi(1-n). \tag{1.8}$$

For brevity, set $J(\chi) = J(\chi, \chi)$. Jacobi sums are related to Gauss sums by the basic formula [**80**, p. 92]

$$J(\chi, \psi) = G(\chi)G(\psi)/G(\chi\psi), \tag{1.9}$$

where $\chi\psi$ is nonprincipal. By the definition (1.8), $J(\chi)$ lies in $\mathbf{Q}(e^{2\pi i/k})$. Not surprisingly then, it is considerably easier, in general, to determine the algebraic shape of $J(\chi)$ than of $G(\chi)$. From (1.3) and (1.9), $|J(\chi)|^2 = p$ for characters χ of order $k > 2$. This leads to a representation of p as a quadratic form. For example, if $p \equiv 1 \pmod 4$ and χ has order 4, then by (1.8), $J(\chi) = a + bi$, where a and b are certain rational integers; thus, $p = |a + bi|^2 = a^2 + b^2$, a well-known result of Fermat. As we shall see later, the determinations of $\mathcal{G}(k)$ and $G(\chi)$ for $k > 2$ are effected in terms of parameters of quadratic forms corresponding to Jacobi sums $J(\psi)$ for characters ψ whose orders divide k.

1.3. The central problem. It follows directly from (1.2) and (1.9) that

$$G(\chi)^k = \omega(\chi), \tag{1.10}$$

where

$$\omega(\chi) = \chi(-1)p \prod_{j=1}^{k-2} J(\chi, \chi^j) \in \mathbf{Q}(e^{2\pi i/k}).$$

The central problem in evaluating $G(\chi)$ is to find a simple criterion for determining which kth root of $\omega(\chi)$ equals $G(\chi)$. We have noted that it took Gauss over four years to find such a criterion (1.7) in the case $k = 2$. (Observe that (1.6) and (1.10) are equivalent when $k = 2$.) The problem is considerably deeper for $k > 2$, and it is unsolved for $k > 4$. The evaluations of $G(\chi)$ and $\mathcal{G}(k)$ that are known are generally ambiguous in the sense that they involve undetermined kth roots of unity. In some cases, e.g., $k = 5$, the irreducible polynomial $P(z)$ of $\mathcal{G}(k)$ over $\mathbf{Q}$ can be explicitly given, but no procedure is known to identify the root of $P(z) = 0$ that is equal to $\mathcal{G}(k)$. (The equation $P(z) = 0$ is called the period equation, and its k distinct roots, called periods, are given by $\sum_n e^{2\pi i g^r n^k/p}$, $0 \leqslant r \leqslant k - 1$, where g is any primitive root (mod p).)

The interesting and important Gauss sums of orders 3 and 4 are investigated in §§3 and 4, respectively. The sums of orders 5, 6, 8, 12, 16, and 24 are briefly discussed in §§5–9. At present, little is known about the evaluations of Gauss sums of other orders. However, a famous conjecture on the uniform distribution of the arguments of Gauss sums (of any order) has now been settled; see §10.

2. Quadratic Gauss sums.

2.1. Proof of (1.7). We begin by presenting, in essence, Gauss's proof of (1.7). For each integer $n \geqslant 0$, define

$$(q)_n = (1-q)(1-q^2)\cdots(1-q^n),$$

where if $n = 0$, the empty product is understood to equal 1. For $0 \leqslant m \leqslant n$, the Gaussian coefficient $\left[{n \atop m}\right]$ is defined by

$$\left[{n \atop m}\right] = \frac{(q)_n}{(q)_m (q)_{n-m}}.$$

The Gaussian coefficient $\left[{n \atop m}\right]$ approaches the binomial coefficient $\binom{n}{m}$ as q tends to 1. It can be easily shown that $\left[{n \atop m}\right]$ is a polynomial in q, with the use of the following analogue of Pascal's formula

$$\begin{bmatrix} n \\ m \end{bmatrix} = \begin{bmatrix} n-1 \\ m-1 \end{bmatrix} + q^m \begin{bmatrix} n-1 \\ m \end{bmatrix}, \qquad 1 \leqslant m < n. \tag{2.1}$$

See, for example, Andrews' book [2, §3.3].

Gauss defined the polynomials

$$f_n(q) = \sum_{j=0}^{n} (-1)^j \begin{bmatrix} n \\ j \end{bmatrix}, \qquad n \geqslant 0, \tag{2.2}$$

which are related to $\mathcal{G}(2)$ by the formula

$$\mathcal{G}(2) = (-1)^{(p-1)(p-3)/8}\beta^{(p^2-1)/8}f_{p-1}(\beta), \tag{2.3}$$

where $\beta = \exp(2\pi i/p)$. To prove (2.3), first note that, from the definition of f_n,

$$f_{p-1}(\beta) = \sum_j \beta^{-j(j+1)/2}.$$

Setting $\alpha = (p-1)/2$, we find that

$$\begin{aligned} f_{p-1}(\beta) &= \sum_j \beta^{\alpha(j^2+j)} = \sum_j \beta^{\alpha(j-\alpha)^2-\alpha^3} \\ &= \beta^{-\alpha^3}\sum_j \beta^{\alpha j^2} = \beta^{-(p^2-1)/8}\sum_j \beta^{\alpha j^2} \\ &= \beta^{-(p^2-1)/8}\left(\frac{\alpha}{p}\right)\mathcal{G}(2), \end{aligned}$$

where the last equality follows easily from (1.5). Since $(\alpha/p) = (-2/p) = (-1)^{(p-1)(p-3)/8}$, formula (2.3) follows.

Using (2.1), Gauss established the recursion formula $f_n(q) = (1-q^{n-1})f_{n-2}(q)$, $n \geqslant 2$, which immediately implies the product formula

$$f_{2n}(q) = \prod_{j=1}^{n}(1-q^{2j-1}). \tag{2.4}$$

Putting $n = (p-1)/2$ and $q = \beta$ in (2.4), we find that

$$f_{p-1}(\beta) = \prod_{j=1}^{(p-1)/2}(1-\beta^{2j-1}) = \prod_{r=1}^{(p-1)/2}(1-\beta^{-2r}),$$

where j was replaced by $(p+1)/2 - r$. Thus,

$$\begin{aligned} f_{p-1}(\beta) &= \prod_{r=1}^{(p-1)/2}\beta^{-r}(\beta^{r}-\beta^{-r}) \\ &= \beta^{(1-p^2)/8}(2i)^{(p-1)/2}\prod_{r=1}^{(p-1)/2}\sin(2\pi r/p). \end{aligned} \tag{2.5}$$

Combining (2.3) and (2.5), we deduce that

$$\mathcal{G}(2) = (-1)^{(p-1)(p-3)/8}(2i)^{(p-1)/2}\prod_{r=1}^{(p-1)/2}\sin(2\pi r/p). \tag{2.6}$$

Since the product of sine functions in (2.6) is positive, (1.7) follows from (1.6).

2.2. Extensions of (1.7) to composite moduli. By further use of (2.4), Gauss proved the following generalization of (1.7)

$$\sum_{n=0}^{M-1} e^{2\pi i n^2/M} = \begin{cases} \sqrt{M}, & \text{if } M \equiv 1 \pmod 4, \\ 0, & \text{if } M \equiv 2 \pmod 4, \\ i\sqrt{M}, & \text{if } M \equiv 3 \pmod 4, \\ (1+i)\sqrt{M}, & \text{if } M \equiv 0 \pmod 4, \end{cases} \tag{2.7}$$

where M is any natural number. For complete details of his proof, consult the book of Nagell [**133**].

The left side of (2.7) can be viewed as the trace of an $M \times M$ finite Fourier transform matrix. An interesting discussion of the equivalence of (2.7) with the solution of the problem on multiplicity of eigenvalues of finite Fourier transforms is given by Auslander and Tolimieri [**4**, p. 856].

Let χ be a real, primitive character (mod M). Then

$$\sum_{n=0}^{M-1} \chi(n) e^{2\pi i n/M} = \begin{cases} \sqrt{M}, & \text{if } \chi(-1) = 1, \\ i\sqrt{M}, & \text{if } \chi(-1) = -1, \end{cases}$$

which is another generalization of (1.7). A proof of this result may be found, for example, in the books of Ayoub [**5**, pp. 317–319], Hasse [**73**, p. 471], Narkiewicz [**134**, pp. 256–260], and Borevich and Shafarevich [**16**, pp. 349–353].

Since Gauss's initial determination of $\mathcal{G}(2)$, many others have been found. We shall now briefly indicate some of these, beginning with the more analytic ones.

2.3. Analytic proofs of (1.7) and generalizations. The first proof given after that of Gauss was discovered in 1835 by Dirichlet [**43**]–[**45**], [**46**, pp. 239–256, 259–270, 473–496], [**47**, pp. 287–292]. Dirichlet employed a version of the Poisson summation formula,

$$\sum_{a \le n \le b}{}' f(n) = \int_a^b f(x)\,dx + 2 \sum_{n=1}^{\infty} \int_a^b f(x) \cos(2\pi n x)\,dx,$$

where f is continuous and of bounded variation on $[a, b]$, and where the prime on the summation sign at the left indicates that if a or b is an integer, then only $\frac{1}{2} f(a)$ or $\frac{1}{2} f(b)$, respectively, is counted. As one would suspect, Dirichlet applied this formula with $a = 0$, $b = p$, and $f(x) = \exp(2\pi i x^2/p)$. Dirichlet's method was also later discussed by Kronecker [**70**]. The books of Lang [**99**, pp. 88–90], Landau [**98**, pp. 197–199], and Davenport [**37**, pp. 14–17] contain nice presentations of Dirichlet's proof.

In a series of three papers [**146**]–[**148**] circa 1850, Schaar used the Poisson summation formula to prove and generalize Gauss's result (1.7). In [**146**], Schaar proved (1.7). In [**147**], he established a reciprocity formula for quadratic Gauss sums which generalizes (2.7). This reciprocity formula is now known as "Schaar's identity" and is the case $b = 0$ in (2.8). In [**148**], another generalization of (2.7) is given, but the formulation appears to be incorrect. In 1852, Genocchi [**69**] claimed to have given a proof and generalization of Schaar's identity, but in Lindelöf's book [**112**, p. 75], it is pointed out that Genocchi's proof is not rigorous.

Prior to Dirichlet's papers, an alleged proof of Gauss's result (1.7) was published by Libri [**109**]. However, it was pointed out by Liouville [**112**] that Libri's arguments were deficient. This evidently led to a bitter dispute which the two men waged in a series of letters [**113**], [**110**]. (See Smith's Report [**165**, article 20].)

In 1840, Cauchy [**28**], [**29**], [**30**, pp. 152–156] gave a proof based on the transformation formula $\theta(1/z) = \sqrt{z}\,\theta(z)$ for the classical theta-function

$$\theta(z) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 z}, \qquad \operatorname{Re} z > 0,$$

which can be thought of as an "infinite analogue" of the quadratic Gauss sum $\mathcal{G}(2)$. Later proofs and generalizations which use the same idea can be found in Kronecker's paper [**85**] and the books of Krazer [**83**, pp. 183–193], Bellman [**10**, pp. 38–39], and Eichler [**48**, pp. 46–48]. In 1919, Hecke [**75**], [**76**], [**77**, Chapter 8] generalized Cauchy's method by using multi-variable theta-functions to establish a reciprocity formula for quadratic Gauss sums over an arbitrary algebraic number field. Consult a paper of Barner [**8**] for references to further proofs and generalizations of Hecke's formula.

Another analytic tool used to determine $\mathcal{G}(2)$ is contour integration. The first proof by this technique is due to Kronecker [**86**] and can be found in the books of Landau [**98**, pp. 203–206] and Ayoub [**5**, pp. 315–317]. An especially elegant and simple use of the residue theorem to evaluate $\mathcal{G}(2)$ has been given by Mordell [**127**], [**128**]. A similar approach has been given by Siegel [**160**], [**163**, vol. III, pp. 334–349], and is presented in the books of Apostol [**3**, pp. 195–200] and Chandrasekharan [**34**, pp. 34–39]. In fact, these books contain special cases of the following reciprocity formula [**160**] for generalized quadratic Gauss sums

$$\sum_{n=0}^{|c|-1} e^{\pi i(an^2+bn)/c} = |c/a|^{1/2} e^{\pi i(|ac|-b^2)/(4ac)} \sum_{n=0}^{|a|-1} e^{-\pi i(cn^2+bn)/a}, \qquad (2.8)$$

where a, b, and c are integers with $ac \neq 0$ and $ac + b$ even. Observe that (2.8) yields (2.7) when $a = 2$, $b = 0$, and $c = M$. As we previously indicated, the case $b = 0$ of (2.8) is Schaar's formula.

The last analytic proofs that we mention are those of Genocchi [**68**] and Weber [**176**] which utilize the Abel-Plana summation formula, **79**, p. 274]

$$\sum_{n=0}^{\infty} f(n) = \frac{1}{2}f(0) + \int_0^{\infty} f(x)\,dx + i\int_0^{\infty} \frac{f(iy) - f(-iy)}{e^{2\pi y} - 1}\,dy,$$

where f is suitably restricted. An account of Weber's proof appears in Lindelöf's book [**111**, pp. 73–75].

2.4. Trigonometric proofs of (1.7). We turn to a class of determinations of $\mathcal{G}(2)$ that depends upon properties of trigonometric functions and sums. Most of the proofs are fairly elementary in nature. The principal idea in these proofs is to deduce (1.7) from (1.6) by using trigonometric inequalities to show that the real and imaginary parts of $\mathcal{G}(2)$ exceed $-\sqrt{p}$ in, respectively, the cases $p \equiv 1$ and 3 (mod 4). The first proof of this type was given in 1896 by Mertens [**125**] and can be found in Landau's book [**98**, pp. 213–218]. Landau himself [**97**] gave a very short, but less elementary proof based upon trigonometric sums. By approximating $\mathcal{G}(2)$ by an integral, van der Corput [**36**] offered a fairly elementary determination. Bambah and Chowla [**7**] simplified van der Corput's work. An elegant proof by trigonometric methods was found by Estermann [**51**]; an account of this proof appears in Chowla's book [**35**].

2.5. Algebraic proofs of (1.7) and generalizations. We now indicate some elementary algebraic proofs. One was given in 1840 by Cauchy in the same paper [**28**] that contains his analytic proof. Cauchy's idea is to show that

$$\mathcal{G}(2) \equiv i^{m^2}\sqrt{p} \quad (\mathrm{mod}(1-\beta)\sqrt{p}\,),$$

where $\beta = \exp(2\pi i/p)$ and $m = (p-1)/2$, by using (1.5) together with Euler's criterion, the binomial theorem, and elementary product formulas such as

$$\prod_{j=1}^{m} \{(\beta^j - \bar{\beta}^j)/i\} = \sqrt{p}\,.$$

It is interesting to note that both of Cauchy's proofs in [**28**] have inspired far-reaching generalizations of considerable significance. We have already pointed out that Cauchy's analytic proof led to Hecke's reciprocity law for Gauss sums over algebraic number fields. Cauchy's algebraic proof has led to the evaluation of the cubic Gauss sum (discussed in the next section).

An algebraic proof in the same spirit as Cauchy's was given in 1856 by Kronecker [**84**]. A remark of Dedekind [**39**] produced a slight simplification. The Cauchy-Kronecker proof can be found in the books of Bachmann [**6**, pp. 107–111], Weber [**177**, pp. 622–626], and Hasse [**73**, pp. 473–477]. Proofs along the same lines are given in papers of Mordell [**129**] and Carlitz [**23**].

Schur [**150**], [**151**, pp. 327–333] obtained an elementary proof using determinants of matrices whose elements are roots of unity. This proof is also in Landau's text [**98**, pp. 207–212]. Waterhouse [**175**], [**134**, pp. 256–258] substantially simplified Schur's work. Carlitz [**22**] gave another proof that employs determinants.

Shanks [**153**] has given a very short, elementary determination of $\mathcal{G}(2)$. His proof is based on the ingenious identity

$$\sum_{j=1}^{2n} x^{j(j-1)/2} = \sum_{j=0}^{n-1} \frac{P_n}{P_j} x^{j(2n+1)},$$

where $P_n = \prod_{s=1}^{n}((1-x^{2s})/(1-x^{2s-1}))$.

Finally, we mention the recent work of Bressoud [**18**], [**19**] in the area of basic hypergeometric series, which takes us full circle back to Gauss's original proof. Bressoud [**18**, Corollary 2.1] has found a multiple sum analogue of (2.4) for which (2.4) is a special case. He has also found a formula [**18**, Corollary 1.1] which equates a certain j-fold sum with a finite product; the case $j = 1$ leads [**19**] to another evaluation of $\mathcal{G}(2)$ by an argument similar to that of Gauss.

3. Cubic Gauss sums.

3.1. Irreducible polynomial of $\mathcal{G}(3)$. In his monumental *Disquisitiones Arithmeticae* [**67**, article 358], Gauss exhibited the irreducible cubic polynomial of $\mathcal{G}(3)$ over the rational numbers. He obtained this polynomial by studying the cubic periods. We now indicate a simpler approach based on Jacobi sums.

Throughout this section, let χ be a character (mod p) of order 3, where $p \equiv 1 \pmod 3$. It can be shown that (see, e.g., [**13**, Theorem 3.4])

$$2J(\chi) = r + 3ti\sqrt{3}\,, \tag{3.1}$$

where r and $|t|$ are integers uniquely determined by

$$4p = r^2 + 27t^2, \qquad r \equiv 1 \pmod 3). \tag{3.2}$$

We will show that the irreducible polynomial of $\mathcal{G}(3)$ is

$$x^3 - 3px - pr, \tag{3.3}$$

where r is defined by (3.2).

From (1.1),

$$\mathcal{G}(3) = G(\chi) + \overline{G(\chi)}\,. \tag{3.4}$$

Thus, by (1.2),

$$\mathcal{G}^3(3) = G^3(\chi) + \overline{G^3(\chi)} + 3p\mathcal{G}(3). \tag{3.5}$$

From (1.10),

$$G^3(\chi) = pJ(\chi), \tag{3.6}$$

and so by (3.1) and (3.5),

$$\mathcal{G}^3(3) = pr + 3p\mathcal{G}(3).$$

Therefore, (3.3) is the irreducible polynomial of $\mathcal{G}(3)$.

This derivation of (3.3) is similar to that given in Hasse's book [**73**, p. 488]. Other derivations are presented in the papers of Lebesgue [**102**], Cayley [**31**], Sylvester [**168**], Pellet [**145**], and Carey [**21**], and in the books of Legendre [**105**, pp. 196–198], Bachmann [**6**, pp. 209–213], Mathews [**118**, pp. 219–228], Weber [**177**, pp. 628–631], and Fricke [**60**, pp. 438–440].

From (3.4) and (1.4), we see that $\mathcal{G}(3)$ lies in the interval $[-2\sqrt{p}\,, 2\sqrt{p}\,]$, and it can be similarly shown that the other two zeros of $x^3 - 3px - pr$ also lie in this interval. In fact, it is not difficult to see that each of the intervals $(-2\sqrt{p}\,, -\sqrt{p}\,)$, $(-\sqrt{p}\,, \sqrt{p}\,)$, and $(\sqrt{p}\,, 2\sqrt{p}\,)$ contains exactly one zero of $x^3 - 3px - pr$. In the early 1840's, Lebesgue [**103**, p. 70] and Kummer [**93**] raised the following question: Which of these three intervals contains $\mathcal{G}(3)$? An equivalent question, in view of (3.4) and (3.6) is: Which of the three cube roots of $pJ(\chi)$ equals $G(\chi)$? While criteria have been put forth [**118**, pp. 224–228], [**24**] to resolve the ambiguity, none have yet been found which are comparable in elegance or simplicity to Gauss's criterion (1.7) for $\mathcal{G}(2)$. Nevertheless, in the last decade, some remarkable progress, which we next describe, has been made.

3.2. Location of cubic Gauss sums via elliptic functions. Let $\wp(z)$ be a Weierstrass $\wp$-function with $\wp'(z)^2 = 4\wp(z)^3 - 1$. Thus,

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq u \in U} \left(\frac{1}{(z-u)^2} - \frac{1}{u^2} \right),$$

where $U = \{\theta m + \theta n e^{2\pi i/3} \colon m, n \in \mathbf{Z}\}$ is the lattice of periods of $\wp$, with θ

equal to the least positive period. Let R be any "third-set" of residues (mod p) chosen such that $\Pi_{r\in R} r \equiv -1 \pmod{p}$. (A third-set S (mod p) is a set of $(p-1)/3$ residues (mod p) such that $S \cup S\omega \cup S\omega^2$ is a reduced residue system (mod p), where ω is a primitive cube root of 1 (mod p).) Cassels [25] constructed the product

$$H(\chi) = -\prod_{r\in R} \wp(r\theta/J(\chi)),$$

which does not depend upon the choice of R. He observed that $H^3(\chi) = J^{-2}(\chi)$. Thus, in view of (3.6), $G^3(\chi) = (p^{1/3}J(\chi)H(\chi))^3$. Cassels [25, equation (4.2)] conjectured that, indeed,

$$G(\chi) = p^{1/3}J(\chi)H(\chi), \tag{3.7}$$

where $p^{1/3} > 0$. Equivalent conjectures are discussed in [27]. Using some ideas of Cassels, Matthews [119], [120] proved Cassels' conjectures in 1978. The proof combines a variety of ingredients such as Stickelberger's computation of the first term in the local expansion of $G(\chi)$, the theory of elliptic curves and complex multiplication, Weil pairings, and Lubin-Tate theory. Note that Gauss connected the quadratic Gauss sum with a product of $(p-1)/2$ values of a trigonometric function in (2.6), while in (3.7), Cassels and Matthews connected the cubic Gauss sum with a product of $(p-1)/3$ values of an elliptic function $\wp(z)$.

A completely elementary algorithm for computing the right side of (3.7) has been devised by McGettrick [123], [25, §4]. This algorithm involves little more than the counting of lattice points within a triangle whose vertices are quite simply determined from the value of $J(\chi)$.

Formula (3.7) does not appear to shed any light on the famous statistical question of how the arguments of $G(\chi)$ are distributed. We next turn to this problem.

3.3. Distribution of cubic Gauss sums: Kummer's conjecture. The first mathematician to extensively examine the values of Arg $G(\chi)$ was Kummer [93], [94], [96, pp. 143–163]. He found that the 45 values of $|\text{Arg}\, G(\chi)|$ corresponding to the 45 primes $p < 500$ with $p \equiv 1 \pmod 3$ fall in the intervals $I_1 = (2\pi/3, \pi)$, $I_2 = (\pi/3, 2\pi/3)$, and $I_3 = (0, \pi/3)$, respectively, 7, 14, and 24 times. Kummer described his findings as follows [94, p. 353], [96, p. 157]. "Omnes numeri primi, formae $6n+1$, talimodo in tres classes dividunter, atque ex 45 numeris primis infra 500 ad classem primam pertinent 7, ad classem secundam 14, ed ad classem tertiam 24, quorum numerorum ratio proxime exprimitur per 1:2:3; nec improbabile est, eandem rationem etiam pro majore numero semper servatum iri." (All prime numbers of the form $6n+1$ are divided into three classes such that of 45 prime numbers below 500, seven belong to the first class, 14 to the second class, and 24 to the third class. The ratios of these numbers are expressed approximately as 1:2:3, and it is not improbable that the same ratios will always hold with respect to a larger number as well.) Kummer's tenuous speculation has been elevated to what is now called "Kummer's conjecture". Because of the prominence of this conjecture, the cubic Gauss sum is often referred to as Kummer's sum.

3.4. Resolution of Kummer's conjecture. Von Neumann and Goldstine [**135**] extended Kummer's investigations by considering primes p with $p < 10{,}000$ and $p \equiv 1 \pmod 3$. Their calculations showed that the ratios of the number of occurrences of $|\operatorname{Arg} G(\chi)|$ in the intervals I_1, I_2, and I_3, respectively, are nearly 2:3:4 in contrast to 1:2:3. Still further calculations of Beyer [**15**], E. Lehmer [**107**], Cassels [**24**], Fröberg [**61**], and Tabakova [**169**] suggest that perhaps the values of $G(\chi)p^{-1/2}$ are uniformly distributed on the unit circle, despite the apparent tendency of the initial values to lie in the right half-plane. (Shanks [**154**] and Cassels [**26**] have written interesting reviews of, respectively, the calculations of Fröberg and Tabakova.) An unsuccessful attempt to prove the uniform distribution of $\operatorname{Arg} G(\chi)$ was made by Vinogradov [**174**] in 1967. In 1974, using Hecke's theory of Grössencharaktere and L-functions, Moreno [**130**] proved the weaker result that the values of $G^3(\chi)p^{-3/2}$ are uniformly distributed on the unit circle. In [**140**]–[**142**], Patterson developed the pioneering work of Kubota [**90**]–[**92**] and established a cubic analogue of the classical theta-function. This enabled Patterson [**143**] to prove that the arguments of more general cubic Gauss sums $(\operatorname{mod} \alpha)$ are uniformly distributed, where α runs through the squarefree algebraic integers in $\mathbf{Q}(e^{2\pi i/3})$ that are congruent to $1 \pmod 3$. (These sums are defined by (10.1) with $K = \mathbf{Q}(e^{2\pi i/3})$, $I = O_K\alpha$, $a = \alpha^{-1}$, and ψ equal to the cubic residue symbol $(\operatorname{mod} \alpha)$ in K.) By combining the techniques of Patterson with a powerful new method of Vaughan [**173**] for estimating certain trigonometric sums, Heath-Brown and Patterson [**74**] proved in 1979 that the values of $G(\chi)p^{-1/2}$ are, indeed, uniformly distributed on the unit circle. Thus, Kummer's conjecture has finally been disproved after more than 130 years.

Despite the equidistribution of the values of $G(\chi)p^{-1/2}$ on the unit circle, it is likely that the average value of $\operatorname{Re}\{G(\chi)p^{-1/2}\}$ for $p < x$ is positive for large x. Indeed, a conjecture of Patterson [**143**, p. 127] supported by numerical evidence implies that

$$\sum_{p<x} \operatorname{Re}\{G(\chi)p^{-1/2}\} \sim \frac{(2\pi)^{2/3}x^{5/6}}{5\Gamma(2/3)\log x},$$

as x tends to ∞. It is then perhaps not surprising that the calculations of Kummer and later mathematicians showed a tendency for $G(\chi)p^{-1/2}$ to lie in the right half-plane.

4. Quartic Gauss sums.

4.1. Irreducible polynomial of $\mathcal{G}(4)$. The irreducible polynomial for $\mathcal{G}(4)$ over the rational numbers was essentially determined in 1828 by Gauss [**65**, articles 15–22], [**66**, pp. 65–92], although the polynomial was not explicitly exhibited. This polynomial can, however, be found in Legendre's textbook [**105**, pp. 199–205], published just two years later. The polynomial also appears in later papers of Lebesgue [**102**], [**104**], Cayley [**31**], Sylvester [**168**], Scott [**152**], Pellet [**145**], and Carey [**21**].

We now show how Jacobi sums can be used to determine $\mathcal{G}(4)$ up to one sign ambiguity. Throughout this section, let χ denote a character $(\operatorname{mod} p)$ of order 4, where $p \equiv 1 \pmod 4$. The quartic Jacobi sum $J(\chi)$ has the value (see, e.g., [**13**, Theorem 3.9])

$$J(\chi) = a + bi, \tag{4.1}$$

where a and $|b|$ are integers completely determined by

$$p = a^2 + b^2, \qquad a \equiv -1 \pmod 4. \tag{4.2}$$

By (1.1) and (1.7),

$$\mathcal{G}(4) = \sqrt{p} + G(\chi) + G(\bar{\chi}). \tag{4.3}$$

By (1.9),

$$G^2(\chi) = \sqrt{p}\, J(\chi). \tag{4.4}$$

Using (1.2), (4.4), and (4.1), we find that

$$\{G(\chi) + G(\bar{\chi})\}^2 = 2a\sqrt{p} + 2\chi(-1)p. \tag{4.5}$$

Since -1 is a quartic residue (mod p) if and only if $p \equiv 1 \pmod 8$, $\chi(-1) = (2/p)$. Thus, by (4.3) and (4.5),

$$\begin{aligned} \mathcal{G}(4) &= \sqrt{p} \pm \sqrt{2(2/p)p + 2a\sqrt{p}} \\ &= \begin{cases} \sqrt{p} \pm \sqrt{2p + 2a\sqrt{p}}\,, & \text{if } p \equiv 1 \pmod 8, \\ \sqrt{p} \pm i\sqrt{2p - 2a\sqrt{p}}\,, & \text{if } p \equiv 5 \pmod 8. \end{cases} \end{aligned} \tag{4.6}$$

Note that $\mathcal{G}(4)$ is real or nonreal, according as $p \equiv 1$ or $5 \pmod 8$. This derivation of (4.6) is similar to that found in Hasse's book [**73**, pp. 489–494]. Special cases of (4.6) have been simply derived in [**108**] and in [**12**].

Mathematicians have attempted for over a century to discover a simple criterion for determining the ambiguous sign in (4.6), or equivalently, by (4.3) and (4.4), for determining which square root of $p^{1/2}J(\chi)$ equals $G(\chi)$. The past few years have witnessed spectacular progress leading to a complete solution of this problem.

4.2. Location of quartic Gauss sums via elliptic functions. Let $\wp(z)$ be a Weierstrass $\wp$-function with $\wp'(z)^2 = 4\wp(z)^3 - \wp(z)$, with period lattice $\{\theta(m + ni)\colon m, n \in \mathbf{Z}\}$, where θ is the least positive period. Matthews [**121**] constructed the product

$$h(\chi) = \prod_{r=1}^{(p-1)/2} \wp'(r\theta/J(\chi))$$

and observed that $h^2(\chi) = -J^{-3}(\chi)$. Thus, from (4.4),

$$G^2(\chi) = \{i^{(p-5-2b)/4}p^{1/4}h(\chi)J^2(\chi)\}^2,$$

since it is easily deduced from (4.2) that $(p - 5 - 2b)/4$ is odd. Matthews [**121**] proved that, in fact,

$$G(\chi) = Bi^{(p-5-2b)/4}p^{1/4}h(\chi)J^2(\chi), \tag{4.7}$$

where $p^{1/4} > 0$ and $B = B(\chi)$ is defined by

$$B = \pm 1, \qquad B \equiv \frac{a}{b}\left(\frac{p-1}{2}\right)! \pmod{p}.$$

Note that (4.7) is the quartic analogue of (3.7). An equivalent version of (4.7), expressed in terms of the elliptic sn function instead of the $\wp$-function, was conjectured by McGettrick [124] in 1972.

4.3. Explicit elementary formulae for quartic Gauss sums. Loxton [114], [115, §§3C, 4B], [116] has formulated conjectures relating cubic and quartic Gauss sums to elementary products of sums of roots of unity. Such products are analogous to the one in (2.5) connected with $\mathcal{G}(2)$.

In 1977, Loxton [115, §4A], [116] conjectured the following explicit formula for the quartic Gauss sum $G(\chi)$ (in a slightly different form):

$$G(\chi) = C\left(\frac{|b|}{|a|}\right)(-1)^{(b^2+2b)/8}p^{1/4}J^{1/2}(\chi), \tag{4.8}$$

where $p^{1/4} > 0$, $\operatorname{Re} J^{1/2}(\chi) > 0$, $(|b|/|a|)$ denotes the Legendre-Jacobi symbol, and C is defined by

$$C = \pm 1, \qquad C \equiv \frac{|b|}{a}\left(\frac{p-1}{2}\right)! \pmod{p}. \tag{4.9}$$

Since $i\{-J(\chi)\}^{1/2} = (\operatorname{sgn} b)J^{1/2}(\chi)$, where both square roots have positive real parts, it follows from (4.3) and (4.6) that (4.8) is equivalent to the remarkably elegant formula

$$\mathcal{G}(4) = \begin{cases} \sqrt{p} + C\left(\frac{|b|}{|a|}\right)(-1)^{(b^2+2|b|)/8}\sqrt{2p + 2a\sqrt{p}}\,, & \text{if } p \equiv 1 \pmod{8}, \\ \sqrt{p} + C\left(\frac{|b|}{|a|}\right)(-1)^{(b^2+2|b|)/8}i\sqrt{2p - 2a\sqrt{p}}\,, & \text{if } p \equiv 5 \pmod{8}, \end{cases} \tag{4.10}$$

where C is defined by (4.9). (We are grateful to E. Bender for simplifying our original version of (4.10).) Using the theory of modular forms, Matthews [121] proved Loxton's conjecture (4.8) by deriving it from (4.7). Thus, almost 175 years after Gauss's determination of $\mathcal{G}(2)$, there has at last been found a formula for a nonquadratic Gauss sum which compares with Gauss's formula in simplicity and elegance.

Those interested in computing numerical values of $\mathcal{G}(4)$ for large primes p may be disappointed with (4.10), since it requires $O(p)$ operations to compute C from (4.9), whereas it requires $O(p)$ operations to evaluate the sum $\mathcal{G}(4)$ directly.

4.4. Distribution of quartic Gauss sums. Calculations of E. Lehmer [107] in 1956 tended to support the conjecture that the values of $G(\chi)p^{-1/2}$ are uniformly distributed on the unit circle. (See also Hasse's book [73, article 20, §6].) This conjecture has recently been proved, as we indicate in §10.

Some conjectures of Yamamoto [182, p. 212] on the distribution of $G(\chi)p^{-1/2}$ appear to be still open. However, Heath-Brown and Patterson (personal communication) have pointed out that most of them amount to assertions of the type "Re $L(1, \chi) > 0$ for all quartic characters $\chi \pmod{p}$" and are hence false.

5. Quintic Gauss sums. In this section, we exhibit the irreducible quintic polynomial $P(z)$ of $\mathcal{G}(5)$ over the rational number field.

Let χ be a character $(\operatorname{mod} p)$ of order 5, where $p \equiv 1 \pmod{5}$. It was essentially known to Dickson [**41**, p. 402] that

$$4J(\chi) = x + 5w\sqrt{5} + vi\sqrt{50 - 10\sqrt{5}} + ui\sqrt{50 + 10\sqrt{5}},$$

where x, w, u, and v are integers such that

$$16p = x^2 + 125w^2 + 50v^2 + 50u^2, \qquad xw = v^2 - u^2 - 4uv, \tag{5.1}$$

and $x \equiv 1 \pmod{5}$. For a fixed prime p, a solution (x, w, v, u) to (5.1) is "essentially unique" in that there is a simple prescription for obtaining the other solutions from it. Thus, there are eight solutions altogether, given by $\pm(x, w, v, u)$, $\pm(x, w, -v, -u)$, $\pm(x, -w, u, -v)$, and $\pm(x, -w, -u, v)$. Given any solution (x, w, v, u) to (5.1) with $x \equiv 1 \pmod{5}$, the irreducible polynomial of $\mathcal{G}(5)$ is

$$\begin{aligned} P(z) = z^5 - 10pz^3 - 5pxz^2 + \frac{5}{4}p(4p - x^2 + 125w^2)z \\ + \frac{p}{8}\{8px - x^3 + 625w(v^2 - u^2)\}. \end{aligned} \tag{5.2}$$

This formula for $P(z)$ can be established by using cyclotomy, as Gauss did in the cubic case. Various forms of (5.2), associated with different parameterizations, appear in the literature. The form given here was given by Lehmer [**106**, equation (10)] (where a factor p was inadvertently omitted).

Legendre [**105**, pp. 205–213] and Cayley [**32**], [**33**] initially made progress in determining $P(z)$. In 1886, Scott [**152**] found all of the coefficients of $P(z)$ except the constant term. In 1887, Tanner [**170**] calculated the constant term, and therefore $P(z)$ was finally determined. Carey [**21**], Glashan [**70**], and Burnside [**20**] also derived various forms of $P(z)$.

With the aid of (1.10) and the formulae for quintic Jacobi sums found in [**53**], $G^5(\chi)$ can be evaluated in terms of the parameters in (5.1). Ishimura [**81**] evaluated $G^5(\chi)$ in terms of parameters in a partition of p that is more complicated than that in (5.1).

6. Sextic Gauss sums. The irreducible polynomial of $\mathcal{G}(6)$ over the rational numbers was first exhibited by Smith [**164**] in 1880 with no proof. A proof was given somewhat later by Carey [**21**]. A short discussion of sextic Gauss sums appears in Hasse's text [**73**, pp. 489–490]. We now describe an explicit evaluation of $\mathcal{G}(6)$ given in [**13**, Theorem 3.8] by means of Jacobi sums.

Let χ denote a character $(\operatorname{mod} p)$ of order 3, where $p \equiv 1 \pmod{6}$. Then [**13**, Theorem 3.3]

$$\bar{\chi}(2)J(\chi) = X + iY\sqrt{3},$$

where X and $|Y|$ are integers uniquely determined by the conditions

$X \equiv -1 \pmod 3$ and $p = X^2 + 3Y^2$. If $3 \nmid Y$, define $\varepsilon, \delta \in \{\pm 1\}$ by

$$\varepsilon \equiv |Y| \pmod 3 \quad \text{and} \quad \delta = \operatorname{sgn}\{(\mathcal{G}^2(3) - p)(X + \varepsilon |Y|)\}.$$

Then

$$\mathcal{G}(6) = \begin{cases} \mathcal{G}(3) + \dfrac{\mathcal{G}(2)}{p}\{\mathcal{G}^2(3) - p\}, & \text{if } 3 | Y, \\ \mathcal{G}(3) + \dfrac{\mathcal{G}(2)}{2p}\{4p - \mathcal{G}^2(3) + \delta \mathcal{G}(3)\sqrt{12p - 3\mathcal{G}^2(3)}\}, & \text{if } 3 \nmid Y. \end{cases}$$

We remark that $3 | Y$ if and only if 2 is a cubic residue $(\operatorname{mod} p)$. This is a result of Gauss.

7. Octavic Gauss sums. We describe next an explicit evaluation of $\mathcal{G}(8)$ given by the authors [**13**, Theorem 3.18].

Let χ be a character $(\operatorname{mod} p)$ of order 8, where $p = 8f + 1$. From [**13**, Theorem 3.12],

$$\chi(4)J(\chi) = c + id\sqrt{2},$$

where c and $|d|$ are integers uniquely determined by the conditions $c \equiv -1$ (mod 4) and $p = c^2 + 2d^2$. Then

$$\mathcal{G}(8) = \mathcal{G}(4) \pm \{2(-1)^f(\sqrt{p} + c)(2\sqrt{p} + (-1)^{d/2}\{\mathcal{G}(4) - \sqrt{p}\}))\}^{1/2}. \tag{7.1}$$

Note that $\mathcal{G}(8)$ is real for $p \equiv 1 \pmod{16}$ and nonreal for $p \equiv 9 \pmod{16}$. No simple criterion for computing the ambiguous sign in (7.1) is known. Note, however, that $\mathcal{G}(4)$ can be determined unambiguously by (4.10).

8. Duodecimic Gauss sums. The sum $\mathcal{G}(12)$ has been determined in [**13**, Theorem 3.20]. Let $p \equiv 1 \pmod{12}$. Let $a^* = a$ if $3 \nmid a$ and $a^* = -a$ if $3 | a$, where a is defined by (4.1). Then

$$\mathcal{G}(12) = \mathcal{G}(6) + \mathcal{G}(4) - \sqrt{p} \pm p^{-1/2}\mathcal{G}(3)\{2(2/p)p + 2a^*\sqrt{p}\}^{1/2}. \tag{8.1}$$

No simple criterion for resolving the ambiguous sign in (8.1) is known.

9. Bioctavic and biduodecimic Gauss sums. The sums $\mathcal{G}(16)$ and $\mathcal{G}(24)$ have been explicitly evaluated up to several sign ambiguities. The formulae are too complicated to present here. Evaluations of $\mathcal{G}(16)$ and $\mathcal{G}(24)$ were accomplished by Evans [**55**] and Berndt and Evans [**13**, Theorem 3.32], respectively.

10. General remarks. Formulas (3.7) and (4.7) give unambiguous evaluations of the cubic and quartic Gauss sums $G(\chi)$ in terms of elliptic functions. At the end of [**121**], Matthews remarks that a paper of Kubota [**89**] gives a hint that similar evaluations for Gauss sums of higher orders might arise from the theory of complex multiplication of abelian varieties.

We indicated in §3 how Heath-Brown and Patterson [**74**] disproved the Kummer conjecture by showing that the values of $G(\chi)p^{-1/2}$ are uniformly distributed on the unit circle, where $G(\chi)$ is the cubic Gauss sum. These authors [**74**, §1] state that the theory of Eisenstein series on metaplectic groups has, in fact, led to a proof of the uniform distribution of $G(\chi)p^{-1/2}$ for Gauss sums $G(\chi)$ of any higher order. See [**144**] for further details.

It is well known that the general Gauss sum $\Sigma_{n \,(\mathrm{mod}\, m)}\psi(n)e^{2\pi in/m}$ for a character ψ (mod m) can be expressed, by certain reduction formulas [**73**, §20], [**37**, pp. 67–69, 148], in terms of the Gauss sums $G(\chi) = \Sigma_{n \,(\mathrm{mod}\, q)}\chi(n)e^{2\pi in/q}$, where q is a prime power dividing m and χ is a primitive character (mod q). The problem of evaluating the Gauss sum $G(\chi)$ is extremely deep only when q is a prime. In fact, for composite prime powers q, Odoni [**139**] has given an elementary, unambiguous evaluation of $G(\chi)$. For example, he has shown that $G(\chi) = pe^{2\pi i/p^2}$ when $q = p^2$ and p is prime.

The Gauss sums in the preceding paragraph are special cases of the Gauss sums in algebraic number fields K, defined by

$$\sum_{x \,(\mathrm{mod}\, I)} \psi(x)\exp(2\pi i \,\mathrm{Tr}_{K/Q}(ax)), \tag{10.1}$$

where I is an ideal of the ring O_K of integers of K, ψ is a character on the group of reduced residue classes in O_K (mod I) extended so that $\psi(x) = 0$ if x is not prime to I, and $a \in I^{-1}D^{-1}$, where D^{-1} is the inverse different of K over $\mathbf{Q}$, i.e.,

$$D^{-1} = \{y \in K: \mathrm{Tr}_{K/Q}(yO_K) \subset \mathbf{Z}\}.$$

Some properties of these sums are given in the book of Narkiewicz [**134**, p. 252].

Let $q = p^r$, where p is prime and $r \geqslant 1$, and let χ be a character on the finite field $GF(q)$. The Gauss sum $G_r(\chi)$ over $GF(q)$ is defined by

$$G_r(\chi) = \sum_{\alpha \in GF(q)} \chi(\alpha)e^{2\pi i(\alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^r})/p}.$$

Of course, $G_1(\chi)$ is the Gauss sum $G(\chi)$ (mod p). Stickelberger [**167**] investigated $G_r(\chi)$ in 1890, and he gave its prime ideal factorization. See also Lang's texts [**99**], [**100**]. Jacobi sums over $GF(q)$ had already been factored into prime ideals in 1856 by Kummer [**95**], [**96**, pp. 583–629].

Let $K = \mathbf{Q}(e^{2\pi i/k})$ for a prime $k > 2$, and let P be a prime ideal prime to k in the ring of integers O_K. Eisenstein in essence discovered in 1850 that the kth power of a Gauss sum of order k (cf. (1.10)) over the finite field O_K/P, by virtue of its prime ideal factorization, could be extended to act as (in modern language) a Hecke character on K. This was the basis for the beautiful Eisenstein reciprocity law (see papers of Eisenstein [**49**], [**50**, pp. 712–721] and Weil [**180**, p. 260]). Weil later showed how to extend general Jacobi sums over finite fields to act as Hecke characters on arbitrary abelian extensions of $\mathbf{Q}$ [**179**], [**181**]. See also Deligne's notes [**40**, p. 168]. The interpretation of Jacobi sums as Hecke characters provides an important link between Gauss and Jacobi sums and the modern theory of L-functions and zeta functions [**179**]–[**181**].

The number of solutions of certain equations in finite fields (and hence also the zeta functions of the corresponding varieties) can be explicitly computed with the use of Gauss sums. Elementary expositions may be found in the papers of Weil [**178**] and Joly [**82**, Chapters 6, 9], in the books of Ireland and Rosen [**80**, Chapters 10, 11], Schmidt [**149**, Chapter 4], and more briefly in the books of Lang [**100**, Chapter 1] and Borevich and Shafarevich [**16**, Chapter 1].

We now turn to the question of evaluating the Gauss sums $G_r(\chi)$ over $GF(q)$, where, as before, $q = p^r$. Let k be a positive divisor of $p - 1$ and let ψ denote a character on $GF(q)$ of order $q - 1$. Then $\psi^{(p-1)/k}$ can be viewed as a character $(\operatorname{mod} p)$ of order k, by restriction to $GF(p)$. A famous theorem of Davenport and Hasse [**38**, (0.8)], [**80**, p. 147] states that

$$G_r(\psi^{(q-1)/k}) = (-1)^{r-1} G^r(\psi^{(p-1)/k}). \tag{10.2}$$

(The counterpart of (10.2) for Jacobi sums over $GF(q)$ had already been discovered in 1915 by Mitchell [**126**, p. 176].) Thus, an evaluation of the Gauss sum $(\operatorname{mod} p)$ of order k yields an evaluation of the Gauss sum over $GF(q)$ of order k. For example, if χ has order 2, then by (10.2) and (1.7),

$$G_r(\chi) = \begin{cases} (-1)^{r-1}\sqrt{q}\,, & \text{if } p \equiv 1 \pmod 4, \\ -(-i)^r\sqrt{q}\,, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

If χ has order k and it happens that $k|r$, then in view of (1.10) and (10.2), the value of the Gauss sum $G_r(\chi)$ can be found in terms of the values of Jacobi sums $(\operatorname{mod} p)$. Examples are given in [**132**] and [**122**].

Suppose now that χ has order m, where $m \nmid (p - 1)$. Then (10.2) cannot, in general, be used to evaluate $G_r(\chi)$. Nevertheless, it is possible to determine $G_r(\chi)$ in some special circumstances. For example, assume that $p^t \equiv -1 \pmod m$ for some positive integer t, which we assume is minimal. Then p has order $2t \pmod m$, and so $r = 2ts$ for some integer s. Stickelberger [**167**, §§3.6 and 3.10] showed that

$$G_r(\chi) = \begin{cases} -\sqrt{q}\,, & \text{if } 2|m, 2\nmid(p^t + 1)/m, \\ (-1)^{s-1}\sqrt{q}\,, & \text{otherwise.} \end{cases} \tag{10.3}$$

See also [**9**]. Evaluations of $G_r(\chi)$ in other special cases may be found in [**122**, equation G10], [**14**, §7], [**58**], and [**52**, Theorem 4]. These evaluations, unlike those in (10.3), generally contain ambiguities.

Another beautiful formula of Davenport and Hasse is their product formula for Gauss sums [**38**, (0.9)]

$$G_r(\chi^m) = \chi^m(m) G_r(\chi) \prod_{j=1}^{m-1} \frac{G_r(\chi\psi^j)}{G_r(\psi^j)},$$

where χ and ψ are characters of $GF(p^r)$ such that ψ has order m. This formula has proved useful in many contexts, e.g., in the theory of cyclotomic numbers [**131**, p. 189]. No elementary proof is known (but see [**14**, §8] for an elementary proof in the case that m is a power of 2). Further formulae involving products of Gauss sums may be found in the papers of Boyarsky [**17**, p. 368], Evans [**59**], and Helversen-Pasotto [**78**]. (On the last line of p. 368 of [**17**], there should be no exponent l; in fact, the misprint $(\text{Teich } l)^l a(q - 1)$ should be corrected to $(\text{Teich } l)^{a(q-1)}$.)

Two combinatorial applications of the evaluations of Gauss sums will be mentioned. First, Gauss sums over finite fields are useful in computing weight distributions of cyclic codes [**122**], [**137**]. Secondly, Gauss sums (mod p) have been used to study power residue difference sets (mod p) [**13**, §5], [**55**], [**56**].

We now list a few additional topics in number theory in which Gauss sums have played an important part: functional equations for Dirichlet series [**155**, pp. 90–95]; Waring's problem [**5**, Chapter 4]; evaluation of Gauss sums in terms of the p-adic gamma function [**17**], [**72**], [**101**]; cubic and quartic reciprocity laws [**165**, pp. 76–92], [**80**, Chapter 9]; rational reciprocity laws [**57**]; and criteria for residuacity [**54**]. See also the lists of references in [**54**], [**57**].

Some interesting generalizations of Gauss sums can be found in the papers of Berndt [**11**], Stark [**166**], An [**1**], Siegel [**156**]–[**162**], [**163**, vol. I, pp. 326–405, 469–548, vol. III, pp. 85–91, 239–248, 373–435, 443–458] (Gauss sums associated with forms of degree $\geqslant 2$); Niederreiter [**136**], [**138**, §8] (Gauss sums for linear recurring sequences); Tsao [**171**], [**172**, §10] (Gauss sums over finite algebras); Martinet [**117**, pp. 38, 48], Fröhlich [**62**] (Galois Gauss sums); and Kubert and Lang [**88**] (Gauss sums over Cartan groups).

A nice exposition detailing advances up to 1977 in the determination of cubic and quartic Gauss sums has been presented by Loxton [**115**]. See [**42**, p. 38] for several classical references on Gauss sums of orders 3–6. Of all the textbooks on number theory, Hasse's [**73**] perhaps contains the most information on Gauss sums. A thorough treatment of theorems of Stickelberger and Hasse-Davenport for Gauss sums over finite fields is presented in Gras's exposition [**71**]. Gauss sums and their generalizations are pervasive in number theory, and we have mentioned here only a small fraction of the instances where they appear. Further references can be found in the book of Narkiewicz [**134**, p. 291].

We are very grateful for several helpful comments supplied by S. J. Patterson.

Note added in proof. In connection with the paragraph following (2.7), it may be remarked that eigenvector decompositions for the finite Fourier transform (Schur's matrix) have been given by McClellan and Parks [**188**] and by Morton [**189**]. Regarding §2.3, note that in Eichler's book [**184**, p. 137], a reciprocity formula for Gauss sums attached to quadratic forms is proved from the transformation formula for the theta-function. In connection with the paragraph preceding (10.1), note that Joris [**186**] has shown how the functional equation for Dirichlet L-series can be used to evaluate imprimitive Gauss sums in terms of primitive ones. Regarding the two paragraphs following (10.1), note that conductors of Gauss sums as Hecke characters have been investigated by Schmidt [**190**]. To the list of papers near the end of §10 giving interesting generalizations of Gauss sums, one should add the papers of O'Meara [**187**] and Jacobowitz [**185**], which use Gauss sums over lattices to classify local integral quadratic (respectively, hermitian) forms. Also, Carlitz [**183**] has evaluated a character sum which generalizes a cubic Gauss sum over $GF(2^n)$.

Using an estimate for generalized Kloosterman sums due to De Ligne

[**40**, p. 219], one can easily show that

$$\sum_{\chi} G(\chi)^k = O(p^{(k+1)/2}),$$

as p tends to ∞, where k is an arbitrary, fixed natural number and where the sum is over all characters $\chi(\text{mod } p)$. In particular, it follows that the arguments of the Gauss sums $G(\chi)$ are asymptotically uniformly distributed as p tends to ∞ [**191**].

References

1. C. An, *On values of exponential sums*, Proc. Amer. Math. Soc. **52** (1975), 131–135.

2. G. E. Andrews, *The theory of partitions*, Addison-Wesley, Reading, Mass., 1976.

3. T. M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976.

4. L. Auslander and R. Tolimieri, *Is computing with the finite Fourier transform pure or applied mathematics*?, Bull. Amer. Math. Soc. (N. S.) **1** (1979), 847–897.

5. R. Ayoub, *An introduction to the analytic theory of numbers*, Math. Surveys, no. 10, Amer. Math. Soc., Providence, R. I., 1963.

6. P. Bachmann, *Die Lehre von der Kreistheilung*, Teubner, Leipzig, 1872.

7. R. P. Bambah and S. Chowla, *On the sign of the Gaussian sum*, Proc. Nat. Acad. Sci. India Sect. A **13** (1947), 175–176.

8. K. Barner, *Zur Reziprozität quadratischer Charaktersummen in algebraischen Zahlkörpern*, Monatsh. Math. **71** (1967), 369–384.

9. L. D. Baumert and R. J. McEliece, *Weights of irreducible cyclic codes*, Inform. and Control **20** (1972), 158–172.

10. R. Bellman, *A brief introduction to theta functions*, Holt, Rinehart, and Winston, New York, 1961.

11. B. C. Berndt, *On Gaussian sums and other exponential sums with periodic coefficients*, Duke Math. J. **40** (1973), 145–156.

12. B. C. Berndt and S. Chowla, *The reckoning of certain quartic and octic Gauss sums*, Glasgow Math. J. **18** (1977), 153–155.

13. B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory **11** (1979), 349–398.

14. ______, *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer*, Illinois J. Math. **23** (1979), 374–437.

15. G. Beyer, *Über eine Klasseneinteilung aller kubischen Restcharaktere*, Abh. Math. Sem. Univ. Hamburg **19** (1954), 115–116.

16. Z. Borevich and I. Shafarevich, *Number theory*, Academic Press, New York, 1966.

17. M. Boyarsky, *p-adic gamma functions and Dwork cohomology*, Trans. Amer. Math. Soc. **257** (1980), 359–369.

18. D. M. Bressoud, *Applications of Andrews' basic Lauricella transformation*, Proc. Amer. Math. Soc. **72** (1978), 89–94.

19. ______, *On the value of Gaussian sums*, J. Number Theory **13** (1981), 88–94.

20. W. Burnside, *On cyclotomic quinquisection*, Proc. London Math. Soc. **14** (1915), 251–259.

21. F. S. Carey, *Notes on the division of the circle*, Quart. J. Math. **26** (1893), 322–371.

22. L. Carlitz, *A note on Gauss' sum*, Proc. Amer. Math. Soc. **7** (1956), 910–911.

23. ______, *A note on Gauss's sum*, Mathematiche (Catania) **23** (1968), 147–150.

24. J. W. S. Cassels, *On the determination of generalized Gauss sums*, Arch. Math. (Brno) **5** (1969), 79–84.

25. ______, *On Kummer sums*, Proc. London Math. Soc. (3) **21** (1970), 19–27.

26. ______, *Review of E. D. Tabakova, "A numerical investigation of Kummer cubic sums"* (Inst. Appl. Math. USSR Acad. Sci., Moscow, preprint No. 98 (1973), 22 pages), Math. Comp. **29** (1975), 665–666.

27. ______, *Trigonometric sums and elliptic functions*, Algebraic Number Theory (S. Iyanaga, ed.), Japan Society for the Promotion of Science, Tokyo, 1977, pp. 1–7.

28. A. Cauchy, *Méthode simple et nouvelle pour la détermination complète des sommes alternées formées avec les racines primitives des équationes binomes*, C. R. Acad. Sci. Paris **10** (1840), 560–572.

29. ______, *Méthode simple et nouvelle pour la détermination complète des sommes alternées formées avec les racines primitives des équationes binomes*, J. de Math. **5** (1840), 154–168. (Same article as in reference 28.)

30. ______, *Oeuvres*, I^{re} Série, t.v, Gauthier Villars, Paris, 1885.

31. A. Cayley, *On the binomial equation $x^p - 1 = 0$; trisection and quartisection*, Proc. London Math. Soc. **11** (1879), 4–17.

32. ______, *The binomial equation $x^p - 1 = 0$; quinquisection*, Proc. London Math. Soc. **12** (1880), 15–16.

33. ______, *The binomial equation $x^p - 1 = 0$; quinquisection, second note*, Proc. London Math. Soc. **16** (1885), 61–63.

34. K. Chandrasekharan, *Introduction to analytic number theory*, Springer-Verlag, New York, 1968.

35. S. Chowla, *The Riemann hypothesis and Hilbert's tenth problem*, Gordon and Breach, New York, 1965.

36. J. G. van der Corput, *Zahlentheoretische Abschätzungen*, Math. Ann. **84** (1921), 53–79.

37. H. Davenport, *Multiplicative number theory*, Markham, Chicago, Ill., 1967.

38. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1934), 151–182.

39. R. Dedekind, *Review of P. Bachmann, "Die Lehre von der Kreistheilung"*, Z. Math. Phys. **18** (1873), 14–24 (in Literaturzeitung).

40. P. De Ligne, *Cohomologie étale*, Lecture Notes in Math., vol. 569, Springer-Verlag, Berlin and New York, 1977.

41. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. **57** (1935), 391–424.

42. L. E. Dickson, H. H. Mitchell, H. S. Vandiver, and G. E. Wahlin, *Algebraic numbers*, Chelsea, New York, 1967.

43. P. G. L. Dirichlet, *Ueber eine neue Anwendung bestimmter Integrale auf die Summation endlicher oder unendlicher Reihen*, Abh. K. Preussischen Akad. Wiss., 1835, 391–407.

44. ______, *Sur l'usage des intégrales définies dans la sommation des séries finies ou infinies*, J. Reine Angew. Math. **17** (1837), 57–67.

45. ______, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*, J. Reine Angew. Math. **21** (1840), 134–155.

46. ______, *Werke*, Erster Band, Georg Reimer, Berlin, 1889.

47. ______, *Vorlesungen über Zahlentheorie*, 4th. ed., Friedrich Vieweg und Sohn, Braunschweig, 1894.

48. M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Academic Press, New York, 1966.

49. G. Eisenstein, *Beweis der allgemeinsten Reziprozitätsgesetze zwischen reellen und complexen Zahlen*, Monatsber. Preuss. Akad. Wiss. Berlin, 1850, 189–198.

50. ______, *Mathematische Werke*, vol. II, Chelsea, New York, 1975.

51. T. Estermann, *On the sign of the Gaussian sum*, J. London Math. Soc. **20** (1945), 66–67.

52. R. J. Evans, *Generalizations of a theorem of Chowla on Gaussian sums*, Houston J. Math. **3** (1977), 343–349.

53. ______, *Unambiguous evaluations of bidecic Jacobi and Jacobsthal sums*, J. Austral. Math. Soc. **28** (1979), 235–240.

54. ______, *The 2^rth power character of* 2, J. Reine Angew. Math. **315** (1980), 174–189.

55. ______, *Bioctic Gauss sums and sixteenth power residue difference sets*, Acta Arith. **38** (1980), 37–46.

56. ______, *Twenty-fourth power residue difference sets* (to appear).

57. ______, *Rational reciprocity laws*, Acta Arith. 39 (1980), 281–294.

58. ______, *Pure Gauss sums over finite fields* (to appear).

59. ______, *Identities for products of Gauss sums over finite fields*, L'Enseign. Math. (to appear).

60. R. Fricke, *Lehrbuch der Algebra*, Band I, Friedrich Vieweg und Sohn, Braunschweig, 1924.

61. C.-E. Fröberg, *New results on the Kummer conjecture*, BIT **14** (1974), 117–119.

62. A. Fröhlich, *Non-abelian Jacobi sums*, Number Theory and Algebra (H. Zassenhaus, ed.), Academic Press, New York, 1977, pp. 71–75.

63. C. F. Gauss, *Mathematisches Tagebuch* 1796–1814, Ostwalds Klassiker der exakten Wissenschaften, Bd. 256, Akad. Verlagsgesell., Geest & Portig K.-G., Leipzig, 1976. (Published also in Math. Annalen **57** (1903), 6–34.)

64. ______, *Summatio quarumdam serierum singularium*, Comm. soc. reg. sci. Gottingensis rec. **1** (1811).

65. ______, *Theoria residuorum biquadraticorum, Comment.* I, Comm. soc. reg. sci. Gottingensis rec. **6** (1828).

66. ______, *Werke*, K. Gesell. Wiss., Göttingen, 1876.

67. ______, *Disquisitiones arithmeticae* (translated by A. A. Clarke), Yale Univ. Press, New Haven, 1966.

68. A. Genocchi, *Sulla formula sommatoria di Eulero, e sulla teorica de' residui quadratici*, Ann. Sci. Mat. Fis. (Roma) **3** (1852), 406–436.

69. ______, *Note sur la théorie des résidus quadratiques*, Mem. Cour. Savants Etrangers, Acad. Roy. Sci. Lettres Beaux Arts Belgique **25** (1851/53), 54 pp.

70. J. C. Glashan, *Quinquisection of the cyclotomic equation*, Amer. J. Math. **21** (1899), 270–275.

71. G. Gras, *Sommes de Gauss sur les corps finis*, Publ. Math. Besancon, 1977–78, 71 pp.

72. B. H. Gross and N. Koblitz, *Gauss sums and the p-adic Γ-function*, Ann. of Math. (2) **109** (1979), 569–581.

73. H. Hasse, *Vorlesungen über Zahlentheorie*, zweite Auf., Springer-Verlag, Berlin, 1964.

74. D. R. Heath-Brown and S. J. Patterson, *The distribution of Kummer sums at prime arguments*, J. Reine Angew. Math. **310** (1979), 111–130.

75. E. Hecke, *Reziprozitätsgesetz und Gausssche Summen in quadratischen Zahlkörpern*, Nachr. Gesell. Wiss. Göttingen, Math.-Phys. Kl. 1919, 265–278.

76. ______, *Mathematische Werke*, zweite Auf., Vandenhoeck & Ruprecht, Göttingen, 1970.

77. ______, *Vorlesungen über die Theorie der algebraischen Zahlen*, Chelsea, New York, 1948.

78. A. Helversen-Pasotto, *L'identité de Barnes pour les corps finis*, C. R. Acad. Sci. Paris **286** (1978), A297–A300.

79. P. Henrici, *Applied and computational complex analysis*, vol. 1, Wiley, New York, 1974.

80. K. Ireland and M. I. Rosen, *Elements of number theory*, Bogden & Quigley, Tarrytown-on-Hudson, 1972.

81. S. Ishimura, *On Gaussian sums associated with a character of order* 5 *and a rational prime number* $p \equiv 1 \pmod{5}$, J. Tsuda College **8** (1976), 27–35.

82. J.-R. Joly, *Équations et variétés algébriques sur un corps fini*, Enseign. Math. **19** (1973), 1–117.

83. A. Krazer, *Lehrbuch der Thetafunktionen*, Teubner, Leipzig, 1903.

84. L. Kronecker, *Sur une formule de Gauss*, J. de Math. **21** (1856), 392–395.

85. ______, *Über den vierten Gauss'schen Beweis des Reziprozitätsgesetzes für die quadratischen Reste*, Monatsber, K. Preuss. Akad. Wiss. Berlin, (1880), 686–698, 854–860.

86. ______, *Summirung der Gaussschen Reihen* $\sum_{h=0}^{h=n-1} e^{2h^2\pi i/n}$, J. Reine Angew. Math. **105** (1889), 267–268.

87. ______, *Über die Dirichletsche Methode der Wertbestimmung der Gaussschen Reihen*, Mitth. Math. Gesell. Hamburg **2** (1890), 32–36.

88. D. S. Kubert and S. Lang, *Independence of modular units on Tate curves*, Math. Ann. **240** (1979), 191–201.

89. T. Kubota, *An application of the power residue theory to some abelian functions*, Nagoya Math. J. **27** (1966), 51–54.

90. ______, *On a special kind of Dirichlet series*, J. Math. Soc. Japan **20** (1968), 193–207.

91. ______, *Some results concerning reciprocity and functional analysis*, Actes, Congrès Intern. Math. 1970, vol. I, Gauthier-Villars, Paris, 1971, pp. 395–399.

92. ______, *Some results concerning reciprocity law and real analytic automorphic functions*, Proc. Sympos. Pure Math. vol. 20, Amer. Math. Soc., Providence, R. I., 1971, pp. 382–395.

93. E. E. Kummer, *Eine Aufgabe, betreffend die Theorie der kubischen Reste*, J. Reine Angew. Math. **23** (1842), 285–286.

94. ______, *De residuis cubicis disquisitiones nonnullae analyticae*, J. Reine Angew. Math. **32** (1846), 341–359.

95. ______, *Theorie der idealen Primfaktoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist*, Math. Abh. K. Akad. Wiss. Berlin (1856), 1–47.

96. ______, *Collected papers*, vol. I, A. Weil, ed., Springer-Verlag, Berlin, 1975.

97. E. Landau, *Über das Vorzeichen der Gaussschen Summe*, Nachr. Gesell. Wiss. Göttingen, Math.-Phys. Kl. 1928, 19–20.

98. ______, *Elementary number theory*, second ed., Chelsea, New York, 1958.

99. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, 1970.

100. ______, *Cyclotomic fields*, Springer-Verlag, Berlin, 1978.

101. ______, *Cyclotomic fields*, vol. II, Springer-Verlag, Berlin, 1980.

102. V.-A. Lebesgue, *Recherches sur les nombres*, J. de Math. **3** (1838), 113–144.

103. ______, *Sommation de quelques séries*, J. de Math. **5** (1840), 42–71.

104. ______, *Note sur les congruences*, C. R. Acad. Sci. (Paris) **51** (1860), 9–13.

105. A.-M. Legendre, *Théorie des nombres*, t. II, 4th. ed., Firmin Didot Frères, Paris, 1830.

106. E. Lehmer, *The quintic character of* 2 *and* 3, Duke Math. J. **18** (1951), 11–18.

107. ______, *On the location of Gauss sums*, Math. Tables Aids Comput. **10** (1956), 194–202.

108. ______, *Problem* 4636 *with solution by L. Carlitz*, Amer. Math. Monthly **63** (1956), 584–587.

109. G. Libri, *Mémoire sur la théorie des nombres*, J. Reine Angew. Math. **9** (1832), 169–188.

110. ______, *Résponse de M. Libri aux observations de M. Liouville*, C. R. Acad. Sci. (Paris) **10** (1840), 345–347.

111. E. Lindelöf, *Le calcul des résidus*, Chelsea, New York, 1947.

112. J. Liouville, *Sur les deux derniers cahiers du Journal de M. Crelle*, J. de Math. **3** (1838), 3–5.

113. ______, *Observations sur une Note de M. Libri*, C. R. Acad. Sci. (Paris) **10** (1840), 343–345.

114. J. H. Loxton, *Products related to Gauss sums*, J. Reine Angew. Math. **268/269** (1974), 53–67.

115. ______, *On the determination of Gauss sums*, Sem. Delange-Pisot-Poitou **18** (1976/77), 12 pp.

116. ______, *Some conjectures concerning Gauss sums*, J. Reine Angew. Math. **297** (1978), 153–158.

117. J. Martinet, *Character theory and Artin L-functions*, *Algebraic number fields*, A. Fröhlich, ed., Academic Press, New York, 1977, pp. 1–87.

118. G. B. Mathews, *Theory of numbers*, second ed., Chelsea, New York.

119. C. R. Matthews, *Gauss sums and elliptic functions*, Ph. D. thesis, Cambridge, 1978.

120. ______, *Gauss sums and elliptic functions*. I. *The Kummer sum*, Invent. Math. **52** (1979), 163–185.

121. ______, *Gauss sums and elliptic functions*. II. *The quartic sum*, Invent. Math. **54** (1979), 23–52.

122. R. J. McEliece, *Irreducible cyclic codes and Gauss sums*, Combinatorics (M. Hall Jr. and J. H. van Lint, eds.), Reidel, Dordrecht, Holland, 1975, pp. 185–202.

123. A. D. McGettrick, *A result in the theory of Weierstrass elliptic functions*, Proc. London Math. Soc. **25** (1972), 41–54.

124. ______, *On the biquadratic Gauss sum*, Proc. Cambridge Philos. Soc. **71** (1972), 79–83.

125. F. Mertens, *Ueber die Gaussischen Summen*, Sitz. Berliner Akad., 1896, 217–219.

126. H. Mitchell, *On the generalized Jacobi-Kummer cyclotomic function*, Trans. Amer. Math. Soc. **17** (1916), 165–177.

127. L. J. Mordell, *On a simple summation of the series* $\sum_{s=0}^{n-1} e^{2s^2\pi i/n}$, Messenger of Math. **48** (1918), 54–56.

128. ______, *The definite integral* $\int_{-\infty}^{\infty} e^{ax^2+bx}/(e^{cx}+d)\,dx$ *and the analytic theory of numbers*, Acta Math. **61** (1933), 323–360.

129. ______, *The sign of the Gaussian sum*, Illinois J. Math. **6** (1962), 177–180.

130. C. J. Moreno, *Sur le problème de Kummer*, L'Enseign. Math. **20** (1974), 45–51.

131. J. B. Muskat and A. L. Whiteman, *The cyclotomic numbers of order twenty*, Acta Arith. **17** (1970), 185–216.

132. G. Myerson, *Period polynomials and Gauss sums for finite fields*, Acta Arith. (to appear).

133. T. Nagell, *Introduction to number theory*, second ed., Chelsea, New York, 1964.

134. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, PWN, Warsaw, 1974.

135. J. von Neumann and H. H. Goldstine, *A numerical study of a conjecture of Kummer*, Math. Tables Aids Comput. 7 (1953), 133–134.

136. H. Niederreiter, *On the cycle structure of linear recurring sequences*, Math. Scand. **38** (1976), 53–77.

137. ______, *Weights of cyclic codes*, Inform. and Control **34** (1977), 130–140.

138. ______, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), 957–1041.

139. R. Odoni, *On Gauss sums* (mod p^n), $n \geqslant 2$, Bull. London Math. Soc. **5** (1973), 325–327.

140. S. J. Patterson, *A cubic analogue of the theta series*, J. Reine Angew. Math. **296** (1977), 125–161.

141. ______, *A cubic analogue of the theta series*. II, J. Reine Angew. Math. **296** (1977), 217–220.

142. ______, *On Dirichlet series associated with cubic Gauss sums*, J. Reine Angew. Math. **303/304** (1978), 102–125.

143. ______, *On the distribution of Kummer sums*, J. Reine Angew. Math. **303/304** (1978), 126–143.

144. ______, *The distribution of general Gauss sums at prime arguments*, Progress in Analytic Number Theory, vol. 2 (H. Halberstam and C. Hooley, eds.) Academic Press, New York, 1981, pp. 171–182.

145. A.-E. Pellet, *Mémoire sur la théorie algébrique des équations*, Bull. Soc. Math. France **15** (1887), 61–103.

146. M. Schaar, *Mémoire sur une formule d'analyse*, Mem. Cour. Savants Etrangers, Acad. Roy. Sci. Lettres Beaux Arts Belgique **23** (1848/50), 17 pp.

147. ______, *Mémoire sur la théorie des résidus quadratiques*, Acad. Roy. Sci. Lettres Beaux Arts Belgique **24** (1850), 14 pp.

148. ______, *Recherches sur la théorie des résidus quadratiques*, Acad. Roy. Sci. Lettres Beaux Arts Belgique **25** (1850), 20 pp.

149. W. Schmidt, *Equations over finite fields*, Lecture Notes in Math., vol. 536, Springer-Verlag, Berlin, 1976.

150. I. Schur, *Über die Gaussschen Summen*, Nachr. K. Gesell. Wiss. Göttingen, Math.-Phys. Kl., 1921, pp. 147–153.

151. ______, *Gesammelte Abhandlungen*, Band II, Springer-Verlag, Berlin, 1973.

152. C. A. Scott, *The binomial equation* $x^p - 1 = 0$, Amer. J. Math. **8** (1886), 261–264.

153. D. Shanks, *Two theorems of Gauss*, Pacific J. Math. **8** (1958), 609–612.

154. ______, *Review of C.-E. Fröberg, "Kummer's Förmodan"* (Lund University, 1973), Math. Comp. **29** (1975), 331–333.

155. G. Shimura, *Arithmetic theory of automorphic functions*, Princeton Univ. Press, Princeton, N. J., 1971.

156. C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. (2) **36** (1935), 527–606.

157. ______, *Über die analytische Theorie der quadratischen Formen*. III, Ann. of Math. (2) **38** (1937), 212–291.

158. ______, *Indefinite quadratische Formen und Modulfunktionen*, Studies and essays presented to R. Courant on his 60th birthday, January 8, 1948, Interscience, New York, 1948, pp. 395–406.

159. ______, *A generalization of the Epstein zeta function*,J. Indian Math. Soc. **20** (1956), 1–10.

160. ______, *Über das quadratische Reziprozitätsgesetz algebraischen Zahlkörpern*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl., No. 1, 1960, 1–16.

161. ______, *Moduln abelscher Funktionen*, Nachr. Akad. Wiss. Göttingen. Math. Phys. Kl., 1960, 51–57.

162. ______, *Über die Fourierschen Koeffizienten der Eisensteinschen Reihen*, Danske Vid. Selskab. Mat.-fys. Meddelelser **34** (1964), 18 pp.

163. ______, *Gesammelte Abhandlungen*, 3 vols., Springer-Verlag, Berlin, 1966.

164. H. J. S. Smith, *Sur l'équation a six périodes*, C. R. Assoc. Franc., Reims, 1880, pp. 190–191.

165. ______, *Report on the theory of numbers*, Chelsea, New York, 1965.

166. H. M. Stark, *L-functions and character sums for quadratic forms*. I, Acta Arith. **14** (1968), 35–50.

167. L. Stickelberger, *Ueber eine Verallgemeinerung der Kreistheilung*, Math. Ann. **37** (1890), 321–367.

168. J. J. Sylvester, *Sur les équations à 3 et à 4 périodes des racines de l'unité*, C. R. Assoc. Franc., Reims, 1880, pp. 96–98.

169. E. D. Tabakova, *A numerical investigation of Kummer cubic sums*, Inst. Appl. Math. USSR Acad. Sci., Moscow, preprint no. 98, 1973, 22 pp. (Russian)

170. H. W. L. Tanner, *On the binomial equation $x^p - 1 = 0$: quinquisection*, Proc. London Math. Soc. **18** (1887), 214–235.

171. L. Tsao, *Exponential sums over finite simple Jordan algebras and finite simple associative algebras*, Duke Math. J. **42** (1975), 333–345.

172. ______, *The rationality of the Fourier coefficients of certain Eisenstein series on tube domains*. I, Compositio Math. **32** (1976), 225–291.

173. R. C. Vaughan, *Sommes trigonométriques sur les nombres premiers*, C. R. Acad. Sci. (Paris) **285** (1977), 981–983.

174. A. I. Vinogradov, *On the cubic Gaussian sum*, Izv. Akad. Nauk SSSR Ser. Math. **31** (1967), 123–148; **33** (1969), 455. (Russian)

175. W. C. Waterhouse, *The sign of the Gaussian sum*, J. Number Theory **2** (1970), 363.

176. H. Weber, *Über Abel's Summation endlicher Differenzenreihen*, Acta Math. **27** (1903), 225–233.

177. ______, *Lehrbuch der Algebra*, Erster Band, zweite Auf., Friedrich Vieweg und Sohn, Braunschweig, 1898.

178. A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.

179. ______, *Jacobi sums as "Grössencharaktere"*, Trans. Amer. Math. Soc. **78** (1952), 487–495.

180. ______, *La cyclotomie jadis et naguère*, L'Enseign. Math. **20** (1974), 247–263.

181. ______, *Sommes de Jacobi et charactères de Hecke*, Nachr. Akad. Wiss. Göttingen. Math. Phys. Kl., 1974, 1–14.

182. K. Yamamoto, *On Gaussian sums with biquadratic residue characters*, J. Reine Angew. Math. **219** (1965), 200–213.

References added in proof.

183. L. Carlitz, *Explicit evaluation of certain exponential sums*, Math. Scand. **44** (1979), 5–16.

184. M. Eichler, *Quadratische Formen und Orthogonale Gruppen*, Springer-Verlag, Berlin, 1952.

185. R. Jacobowitz, *Gauss sums and the local classification of Hermitian forms*, Amer. J. Math. **90** (1968), 528–551.

186. H. Joris, *On the evaluation of Gaussian sums for non-primitive Dirichlet characters*, L'Enseign. Math. **23** (1977), 13–18.

187. O. T. O'Meara, *Local characterization of integral quadratic forms by Gauss sums*, Amer. J. Math. **79** (1957), 687–709.

188. J. H. McClellan and T. W. Parks, *Eigenvalue and eigenvector decomposition of the discrete Fourier transform*, IEEE Trans. on Audio and Electroacoustics **20** (1972), 66–74.

189. P. Morton, *On the eigenvectors of Schur's matrix*, J. Number Theory **12** (1980), 122–127.

190. C.-G. Schmidt, *Über die Führer von Gausschen Summen als Grössencharaktere*, J. Number Theory **12** (1980), 283–310.

191. R. A. Smith, *On n-dimensional Kloosterman sums*, C. R. Math. Rep. Acad. Sci. Canada **1** (1979), 173–176.

Department of Mathematics, University of Illinois, Urbana, Illinois 61801

Department of Mathematics, University of California, San Diego, La Jolla, California 92093