Trends in Mathematics
Information Center for Mathematical Sciences
Volume 1, Number 1, September 1998, Pages 52–57

Introduction to Exponential Sums

DAE SAN KIM

ABSTRACT. In this short survey paper, we show that exponential sums arise in various contexts of number theory and that they often give very interesting results. Also, we introduce the reader to the recent development on Gauss sums associated with representations of finite reductive groups over finite fields.

1. INTRODUCTION

The main purpose of this short survey article is to popularize the area of exponential sums within the Korean mathematical community.

After briefly introducing the necessary notations and definitions in Section 2, we will illustrate in Section 3 that the exponential sums arise in various contexts of number theory and that they often give very interesting results. In the final Section 4, we will introduce the reader to the recent development on "Gauss" sums associated with representations of finite reductive groups of finite fields.

As the space is limited, we have not been quite successful in explaining this new direction of research. We hope that in near future we will have an occasion to give a more full account of this new development.

References at the end is far from being complete. We recommend the reader to start with Chapter 6 of [17], which contains most of references up until 1985. In the other books in References, you can find various uses of classical exponential sums.

2. NOTATIONS AND DEFINITIONS

Let $\mathbb{F}_q$ be the finite field with q elements ($q = p^d$ is a power of a prime p), and let λ be an additive character of $\mathbb{F}_q$ (i.e., $\lambda \in \mathrm{Hom}(\mathbb{F}_q^+, \mathbb{C}^\times)$). Then $\lambda = \lambda_a$ for a unique $a \in \mathbb{F}_q$, where

$$\lambda_a(\alpha) = \exp\left\{\frac{2\pi i}{p}(a\alpha + (a\alpha)^p + \cdots + (a\alpha)^{p^{d-1}})\right\}.$$

Note that λ_a is trivial for $a = 0$, and λ_1 is called the canonical additive character of $\mathbb{F}_q$.

For any multiplicative character χ of $\mathbb{F}_q$ (i.e., $\chi \in \mathrm{Hom}(\mathbb{F}_q^\times, \mathbb{C}^\times)$), the (classical) Gauss sum $G(\chi, \lambda)$ is defined as:

$$G(\chi, \lambda) = \sum_{\alpha \in \mathbb{F}_q^\times} \chi(\alpha)\lambda(\alpha).$$

1991 *Mathematics Subject Classification.* 11L05, 11L10, 11T23, 11T24, 20G40, 20H30.

Key words and phrases. Gauss sum, Kloosterman sum, Jacobi sum, Jacobsthal sum, additive character, multiplicative character, representation, reductive group, symplectic group.

Also, for λ nontrivial and $a, b \in \mathbb{F}_q^\times$, the Kloosterman sum $K(\lambda; a, b)$ is given by:

$$K(\lambda; a, b) = \sum_{\alpha \in \mathbb{F}_q^\times} \lambda(a\alpha + b\alpha^{-1}).$$

Given any multiplicative characters χ_1 and χ_2 of $\mathbb{F}_q$, the Jacobi sum $J(\chi_1, \chi_2)$ is defined as:

$$J(\chi_1, \chi_2) = \sum_{\substack{\alpha, \beta \in \mathbb{F}_q \\ \alpha + \beta = 1}} \chi_1(\alpha)\chi_2(\beta).$$

Finally, for η the (multiplicative) quadratic character of $\mathbb{F}_q$ (q odd) and $a \in \mathbb{F}_q^\times$, the Jacobsthal sum $H_n(a)$ is defined to be:

$$H_n(a) = \sum_{\alpha \in \mathbb{F}_q} \eta(\alpha)\eta(\alpha^n + a).$$

So it is a special case of Weil sum for the multiplicative characters.

Finally, a more general type of classical Gauss sums appears in Section 3 whose definition will be given there.

3. Various Uses of Exponential Sums

1. Euler showed that every prime $p \equiv 1 (\mathrm{mod}\ 4)$ can be written as $p = a^2 + b^2$ for some integers a and b. One can give a very short proof for this by using Jacobi sum. We assume the following elementary estimation on the absolute value of Jacobi sum. Namely, $|J(\chi, \psi)| = \sqrt{p}$, provided that $\chi, \psi, \chi\psi$ are all nontrivial multiplicative characters of $\mathbb{F}_p$.

As $p \equiv 1 (\mathrm{mod}\ 4)$, there is a multiplicative character χ of $\mathbb{F}_p$ of order 4. Then $\eta = \chi^2 = \left(\frac{\cdot}{p}\right)$ is the quadratic character of $\mathbb{F}_p$. χ takes values in $\{\pm 1, \pm i\}$, and hence $J(\chi, \eta) \in \mathbb{Z}[i]$. So $J(\chi, \eta) = a + bi$ for some integers a and b. Thus we have $a^2 + b^2 = (\mathrm{Re} J(\chi, \eta))^2 + (\mathrm{Im} J(\chi, \eta))^2 = p$.

Using Jacobsthal sum, further informations on a and b can be obtained. We may assume that $a \equiv -1 (\mathrm{mod}\ 4)$. Then a is uniquely determined and b is determined up to sign. In fact, we have:

$$\begin{aligned} H_2(1) &= \sum_{\alpha \in \mathbb{F}_p} \eta(\alpha)\eta(\alpha^2 + 1) \\ &= \chi(-1)(J(\chi, \eta) + J(\chi^3, \eta)) \\ &= \chi(-1)(J(\chi, \eta) + \overline{J(\chi, \eta)}) \\ &= 2\chi(-1)\mathrm{Re} J(\chi, \eta). \end{aligned}$$

So $\mathrm{Re} J(\chi, \eta) = \pm\frac{1}{2} H_2(1)$. It is rather difficult to show that $\frac{1}{2} H_2(1) \equiv -1 (\mathrm{mod}\ 4)$. Thus $a = \frac{1}{2} H_2(1)$. As for b, we may choose it as $b = \frac{1}{2} H_2(\epsilon)$, for any $\epsilon \in \mathbb{F}_p$ with $\eta(\epsilon) = -1$.

One amusing observation is the following determination of a modulo p in terms of binomial coefficient. Regarding everything of the following as elements in $\mathbb{F}_p$, the classical Euler's criterion on the value of Legendre symbol modulo p yields:

$$\begin{aligned} 2a = H_2(1) &= \sum_{\alpha\in\mathbb{F}_p} \alpha^{p-1/2}(\alpha^2+1)^{p-1/2} \\ &= \sum_{j=0}^{p-1/2} \binom{p-1/2}{j} \sum_{\alpha\in\mathbb{F}_p} (\alpha^2+1)^{(p-1)/2+2j}. \end{aligned}$$

Noting that $\sum_{\alpha\in\mathbb{F}_p} \alpha^n = -1$, for $p-1$ dividing n, $=0$, for $p-1$ not dividing n, we have:

$$2a = -\binom{p-1/2}{p-1/4}, \text{ i.e., } a \equiv -\frac{1}{2}\binom{p-1/2}{p-1/4} (\text{mod } p).$$

For example, if $p=29$, then $29 = (-5)^2 + 2^2$ and $-\frac{1}{2}\binom{14}{7} = -11\cdot 12 \cdot 13 = -1716 \equiv -5(\text{mod } 29)$.

2. There are so many different ways of showing Quadratic Reciprocity Law. Here we reproduce a simple proof of it using classical quadratic Gauss sum. Let p be an odd prime, $\eta = \left(\frac{\cdot}{p}\right)$ the quadratic character of $\mathbb{F}_p$, and let $\lambda = \lambda_1$ be the canonical additive character of $\mathbb{F}_p$. Then it is easy to determine the square of the Gauss sum $G = G(\eta, \lambda_1)$. Indeed,

$$\begin{aligned} G^2 &= \sum_{\alpha,\beta} \eta(\beta)\lambda_1(\alpha(1+\beta)) = \sum_{\alpha} \eta(-1) + \sum_{\alpha,\beta\neq -1} \eta(\beta)\lambda_1(\alpha(1+\beta)) \\ &= (p-1)\eta(-1) + \left(\sum_{\alpha} \lambda_1(\alpha)\right)\left(\sum_{\beta\neq-1} \eta(\beta)\right) \\ &= (p-1)\eta(-1) + (-1)(-\eta(-1)) = \eta(-1)p = (-1)^{\frac{p-1}{2}}p. \end{aligned}$$

This means that $G(\eta,\lambda_1) = \pm\sqrt{p}$ for $p \equiv 1(\text{mod } 4)$, $= \pm i\sqrt{p}$ for $p \equiv 3(\text{mod } 4)$.

Determination of the correct sign is very hard. However, it can be shown that the plus sign is correct in either case. Let p, q be odd primes. On the one hand,

$$G^q \equiv \sum_{\alpha\in\mathbb{F}_p} \eta(\alpha)\lambda_1(q\alpha) \equiv \eta(q) \sum_{\alpha\in\mathbb{F}_p} \eta(q\alpha)\lambda_1(q\alpha) \equiv \left(\frac{q}{p}\right) G(\text{mod } q).$$

On the other hand,

$$G^q \equiv G(G^2)^{\frac{q-1}{2}} \equiv G(-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} \equiv G(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) (\text{mod } q).$$

From these, we get the celebrated Quadratic Reciprocity Law:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

3. Gauss sums appear also in functional equations of Dirichlet L-function. In below, we will briefly indicate how they arise in this context.

Let χ be a character of the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^{\times}$. Then, as usual, we extend this to a function on $\mathbb{Z}$ by defining $\chi(n) = \chi(n \bmod N)$ if $(n, N) = 1$, $= 0$ if $(n, N) \neq 1$. Now, the Dirichlet L-function attached to χ is defined to be

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad (\mathrm{Re}(s) > 1).$$

It is absolutely and locally uniformly convergent on the domain $\{s \in \mathbb{C} | \mathrm{Re}(s) > 1\}$, so that it represents an analytic function there. Also, if χ is "primitive" with $N > 1$, then it admits an analytic continuation to an entire function on $\mathbb{C}$ and satisfies the functional equation:

$$L(s, \chi) = \begin{cases} \frac{G(\chi)\left(\frac{2\pi}{N}\right)^s L(1-s, \chi^{-1})}{2\Gamma(s)\cos(\pi s/2)}, & \text{if } \chi(-1) = 1 (\text{i.e., } \chi \text{ even}), \\ \\ \frac{G(\chi)\left(\frac{2\pi}{N}\right)^s L(1-s, \chi^{-1})}{2\sqrt{-1}\Gamma(s)\sin(\pi s/2)}, & \text{if } \chi(-1) = -1 (\text{i.e., } \chi \text{ odd}). \end{cases}$$

Here $G(\chi)$ denotes Gauss sum $\sum\limits_{a=1}^{N} \chi(a) e^{2\pi i a/N}$. All of these can be derived from the following identity: Put $\delta = 0$ for χ even, $\delta = 1$ for χ odd. Also, define, for $t > 0$, the theta series $\theta(t, \chi)$ by $\theta(t, \chi) = \sum\limits_{n \in \mathbb{Z}} \chi(n) e^{-\pi n^2 t}$, for χ even, and by $\theta(t, \chi) = \sum\limits_{n \in \mathbb{Z}} \chi(n) n t^{1/2} e^{-\pi n^2 t}$, for χ odd. With $\xi(s, \chi) = N^{s/2} \pi^{-(s+\delta)/2}$, $((s+\delta)/2) L(s, \chi)$, $W(\chi) = (-i)^{\delta} N^{-1/2} G(\chi)$, we have the identity, which is valid for all $s \in \mathbb{C}$ by analytic continuation:

$$\xi(s, \chi) = \frac{1}{2} \left\{ \int_1^{\infty} \theta(t/N, \chi) t^{s/2} dt/t + W(\chi) \int_1^{\infty} \theta(t/N, \chi^{-1}) t^{(1-s)/2} dt/t \right\}.$$

4. Recent Development on Gauss Sums Associated with Representations of Finite Reductive Groups over Finite Fields

In this section, we introduce the reader to the definition of Gauss sums associated with representations of finite reductive groups over finite fields, and present one sample of results and mention some possible applications of it.

Let χ, λ be respectively a multiplicative and a nontrivial additive character of the finite field $\mathbb{F}_q$. For a finite reductive group G defined over $\mathbb{F}_q$ and its finite dimensional (rational) representation ϕ over $\mathbb{F}_q$, we define the Gauss sum $G(\phi, \chi, \lambda)$ as:

$$(*) \qquad G(\phi, \chi, \lambda) = \sum_{g \in G} \chi(\det\phi(g)) \lambda(\mathrm{tr}\phi(g)),$$

where $\det \phi(g)$ is the determinant of $\phi(g)$ and $\mathrm{tr}\phi(g)$ is the trace of $\phi(g)$.

Among other things, we were interested in finding explicit expressions for these Gauss sums. When G is one of the finite classical groups and ϕ is its natural representation, this has been done in the papers [6-11,14,15]. Also, when G is $G_2(q)$ and ϕ is its 7-dimensional faithful representation, and G is $GL(n,q)$ and ϕ is its adjoint representation, explicit expressions for $(*)$ were found [16,18].

After seeing all these evidences, and restricting only to finite groups of Lie type and their finite dimensional representations, K. Park was able to give conjectures [see the introduction, and Chap. 3, 18] about the general nature of the explicit expressions of $(*)$. Roughly speaking, it says the following. Let $G = G_l$ be a finite group of Lie type of rank l, and let $T = T_l$ be a maximal torus of G. Then the conjecture predicts that $(*)$ is a polynomial in q with coefficients involving the Gauss sum restricted to $T = T_l$ and its analogous sums associated with its subtori of lower ranks T_m $(m < l)$.

To give a feeling about the sum $(*)$ to the reader, we state the result in the case that $G = Sp(2n,q)$ and ϕ is its natural representation. Here $Sp(2n,q)$ is the symplectic group defined by $\{g \in GL(2n,q) | {}^t g J_{2n} g = J_{2n}\}$, where J_{2n} is the $2n \times 2n$ matrix given by

$$J_{2n} = \begin{bmatrix} 0 & 1_n \\ -1_n & 0 \end{bmatrix}.$$

The sum $\sum_{g \in Sp(2n,q)} \chi(\det g)\lambda(\mathrm{tr} g)$ is given by

$$\sum_{g \in Sp(2n,q)} \chi(\det g)\lambda(\mathrm{tr} g)$$
$$= q^{\binom{n+1}{2}} \sum_{\substack{0 \le r \le n \\ r \text{ even}}} q^{rn - \frac{1}{4}r^2} \begin{bmatrix} n \\ r \end{bmatrix}_a \prod_{j=1}^{r/2} (q^{2j-1} - 1) K_{GL(n-r,q)}(\lambda; 1, 1).$$

Here $\begin{bmatrix} n \\ r \end{bmatrix}_a = \prod_{j=0}^{r-1} (q^{n-j} - 1)/(q^{r-j} - 1)$, for integers n, r with $0 \le r \le n$, and

$$K_{GL(m,q)}(\lambda; a, b) = \sum_{g \in GL(m,q)} \lambda(a\mathrm{tr} g + b\mathrm{tr} g^{-1}), \text{ for } a, b \in \mathbb{F}_q.$$

Morever,

$$K_{GL(m,q)}(\lambda; 1, 1) = q^{\frac{1}{2}(m-2)(m+1)} \sum_{l=1}^{[(m+2)/2]} q^l K(\lambda; 1, 1)^{m+2-2l} \sum \prod_{k=1}^{l-1} (q^{j_k - 2k} - 1),$$

where the inner sum is over all integers $j_1, j_2, \cdots, j_{l-1}$ satisfying $2l - 1 \le j_{l-1} \le j_{l-2} \le \cdots \le j_1 \le m + 1$. Note here that the powers of Kloosterman sum $K(\lambda; 1, 1)$ are the sums relevant to the natural representation of $G = Sp(2n,q)$ restricted to various subtori of a maximal torus of $Sp(2n,q)$. So our conjecture is true in this case.

It would have been nice to have some applications of our result. Here we will be content with just mentioning that one can find a formula expressing the number of elements in $Sp(2n,q)$ with a given trace [12] and that certain "generalized Kloosterman sum over nonsingular matrices" can be determined even for certain cases that both of the arguments are not zero [3,7].

References

[1] B. C. Berndt, R. J. Evances and K. S. Williams, *Gauss and Jacobi sums*, The Canadian Math. Soc. Series of Monographs and Advanced Texts, Wiley, 1998.

[2] S. Chowla, *The Riemann Hypothesis and Hilbert's Tenth Problem*, Gordon and Breach, New York, 1987.

[3] H. Hodges, *Weighted partitions for skew matrices over a finite field*, Arch. Math. **8** (1957), 16–22.

[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., G. T. M. 84, Springer-Verlag, New York, 1990.

[5] Iwaniec, *Topics in Classical Automorphic Forms*, Graduate Studies in Math. 17, Amer. math. Soc., Providence, 1997.

[6] D. S. Kim, *Gauss sums for general and special linear groups over a finite field*, Arch. Math. (Basel) **69** (1997), 297–304.

[7] D. S. Kim, *Gauss sums for symplectic groups over a finite field*, Monatsh. Math. **126** (1998), 55–71.

[8] D. S. Kim, *Gauss sums for* $O^{-}(2n, q)$, Acta Arith. **80** (1997), 343–365.

[9] D. S. Kim, *Gauss sums for* $O(2n+1, q)$, Finite Fields and Their Applications **4** (1998), 62–86.

[10] D. S. Kim, *Gauss sums for* $U(2n, q^2)$, Glasgow Math. J. **40** (1998), 79–95.

[11] D. S. Kim, *Gauss sums for* $U(2n+1, q^2)$, J. Korean Math. Soc. **34** (1997), 871–894.

[12] D. S. Kim, *Exponential sums for symplectic groups and their applications*, Preprint.

[13] D. S. Kim, *Exponential sums for* $O^{+}(2n, q)$ *and their applications*, Preprint.

[14] D. S. Kim and I.-S. Lee, *Gauss sums for* $O^{+}(2n, q)$, Acta Arith. **78** (1996), 75–89.

[15] D. S. Kim and Y. H. Park, *Gauss sums for orthogonal groups over a finite field of characteristic two*, Acta Arith. **82** (1997), 331–357.

[16] I.-S. Lee and K. H. Park, *Gauss sums for* $G_2(q)$, Bull. Korean Math. Soc. **34** (1997), 305–315.

[17] R. Lidi and H. Niederreiter, *Finite fields*, Encyclopedia of Math. Appl. 20, Cambridge University Press , Cambridge, 1987.

[18] K. H. Park, *Gauss sums for representations of* $GL_n(q)$ *and* $SL_n(q)$, Ph. D. Thesis, Seoul National University, 1998.

Department of Mathematics Sogang University Seoul 121-742 Korea
dskim@ccs.sogang.ac.kr