NOTES ON CHARACTER SUMS

WEN WANG

Abstract. In this article, the properties of character sums, including Gauss sums and Jacobi sums are investigated.

1. Introduction–Historical Notes

The origin of the Gauss sum and Jacobi sum in the work of C.F. Gauss and C.G.J. Jacobi. Gauss introduced the Gauss sum in his *Disquisitione Arithmeticae*[Ga1] in July, 1801, and Jacobi introduced the Jacobi sum in a letter to Gauss[Ja1] dated February 8, 1827.

The sum introduced by Gauss in 1801 is

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

which is now called a quadratic Gauss sum. This sum is not easy to evaluate, even in the special case that $m = 1$ and k is an odd positive integer. In this case, Gauss was easily able to show that this sum has the value $\pm\sqrt{k}$ or $\pm i\sqrt{k}$, according as k is of the form $4u + 1$ or $4u + 3$, respectively. Specific examples convinced Gauss that the plus sign is always correct. On August 30, 1805, Gauss wrote in his diary he was able to prove his conjecture on the sign of these sums. A few years later, Gauss[Ga2] published an evaluation of his quadratic Gauss sum for all positive integer k.

In his study of primes in arithmetic progressions, G.L. Dirichlet [Di1] introduced the multiplicative character χ modulo k and the sum

$$G(\chi) = \sum_{n=0}^{k-1} e^{2\pi imn/k}.$$

This is also called a Gauss sum, as it coincides with the quadratic Gauss sum above in the case that χ has order 2 and k is a prime not dividing m.

The sum now called a Jacobi sum, which is in essence the one Jacobi introduced in 1827, is

Date: 2010-03-12.

Key words and phrases. Character sums, Finite fields.

The calculation in section 9 of this article is done by SAGE, an open source mathematical calculation software program directed by William Stein. See http://www.sagemath.org/.

$$J(\chi,\psi)=\sum_{n \mod p}\chi(n)\psi(1-n),$$

where χ and ψ are multiplicative characters modulo a prime p. Jacobi was already aware in 1827 that Gauss and Jacobi sums are related like gamma and beta functions, i.e., for $k=p$ and $m=1$.

$$J(\chi,\psi)=G(\chi)G(\psi)/G(\chi\psi)$$

when $\chi\psi$ is non-trivial.

After the initial work of Gauss, Dirichlet, and Jacobi, many well-known mathematicians made contributions to the theory of Gauss and Jacobi sums, including L. Carlitz, A. Cauchy, S. Chowla, H. Davenport, G. Eisenstein, B. Gross, H. Hasse, N.M. Katz, N. Koblitz, L. Kronecker, E.E. Kummer, D.H. and E. Lehmer, I.J. Mordell, S.J. Patterson, C.L. Siegel, L. Stickelbegger, and A. Weil.

In the following sections, Gauss and Jacobi sums are introduced via the language of characters over finite fields.

2. Characters of finite fields

Suppose F be a finite field with $q=p^d$ elements, where p is a prime number. It is obvious that $\mathbb{F}_p=\mathbb{Z}/\mathbb{Z}_p$ and therefore F is a dimension d vector space over $\mathbb{F}_p$. We say that χ is a character of F^*, or just of F if there is no ambiguity, if χ is a multiplicative group homomorphism of F into $\mathbb{C}^*$. χ is called *primitive* if it is injective. Note that F^* is a cyclic group with a generater, say, g. Then χ is determined by $\chi(g)\in\mathbb{C}^*$. If χ is primitive, one may choose g such that $\chi(g)=e^{\frac{2\pi i}{p-1}}$. Note that $\mathrm{Hom}(F^*,\mathbb{C}^*)$ has a natural abelian group structure, i.e., for $\chi,\psi\in\mathrm{Hom}(F^*,\mathbb{C}^*)$, $\chi\psi(a)=\chi(a)\psi(a)$, for any $a\in F^*$. It is not hard to verify that the identity for $\mathrm{Hom}(F^*,\mathbb{C}^*)$ is the character that maps every element of F^* to $1\in\mathbb{C}$, we shall call this character the identity character and denote it by $\mathbf{1}$.

For a given character, let m be the smallest positive integer such that $\chi^m=\mathbf{1}$. Hence m divides $q-1$. It follows that there is a primitive order m character of F if and only if m divides $q-1$. For example, if F is a prime field and $\mathrm{char}F>2$, then $2\mid p-1$, therefore there exist an order 2 character of F. Since F^* is cyclic, therefore this order 2 character is unique, which is the well-known the Legendre symbol: $\left(\frac{\cdot}{p}\right)$, which maps a quadratic residue to 1 and a non-residue to -1.

We say that τ is an *additive* character if τ is a group homomorphism from the additive group of F into the multiplicative group $\mathbb{C}^*$. Note that the trace map $\mathbf{tr}$ is an additive map, which will be used for the construction of the Gauss sum in the next section.

3. Gauss Sums

Let F be a finite field with q elements, and let $\mathbf{tr}$ be the trace map from F to the prime field $\mathbb{F}_p$. The Gauss sum of a character χ of F is defined as follows:

$$G(\chi) := \sum_{t\in F} \chi(t)\zeta_p^{\mathbf{tr}t}.$$

In general, according to an additive character τ, we can form the Gauss sum in the following way:

$$G_a(\chi;\tau) = \sum_{t\in F} \chi(t)\tau(at)$$

for some fixed $a \neq 0 \in F$.

Note that if we consider the case when F itself is the prime field $\mathbb{F}_p$, then the Gauss sum becomes:

$$G_a(\chi) := \sum_{t\in F} \chi(t)\zeta_p^{at}.$$

For now on and to the end of this section we will consider the case when F is the prime field. Note that $\chi(t)$ is a power of ζ_{p-1} for any χ and any $t \in F$, therefore the Gauss sum $G(\chi) \in \mathbb{Q}(\zeta_{p-1}, \zeta p)$. We also have the following basic property of the Gauss sums[Ir1, Co1]:

Proposition 3.1. *If $\chi \neq \varepsilon$, then $|G(\chi)| = \sqrt{p}$.*

Proof. The ideal is to evaluate the sum

$$\sum_a G_a(\chi)\overline{G_a(\chi)}$$

in two ways.

If $a \neq 0$, then $\overline{G_a(\chi)} = \chi(a)\overline{G(\chi)}$ and $G_a(\chi) = \chi(a)^{-1}G(\chi)$. Thus $G_a(\chi)\overline{G_a(\chi)} = |G(\chi)|^2$. Since $G_0 = 0$, the sum evaluates as $(p-1)|G(\chi)|^2$.

On the other hand,

$$G_a(\chi)\overline{G_a(\chi)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{ax-ay}.$$

Summing both sides over a yields,

$$sum_a G_a(\chi)\overline{G_a(\chi)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\delta(x,y)p = (p-1)p,$$

where $\delta(x,y) = 1$ if $x = y$ and zero otherwise.

Hence $|G(\chi)| = \sqrt{p}$. □

4. Jacobi Sums

The Jacobi sum was first introduced by Jacobi in a letter to Gauss, which is defined as following. For two multiplicative character on $\mathbb{F}_p^*$, we defined the Jacobi sum to be

$J(\chi, \psi) = \sum_t \chi(t)\psi(1-t)$

Here are some basic properties of the Jacobi sum:

Proposition 4.1. *Let ε be the trivial character. Then,*

(a) $J(\varepsilon, \varepsilon) = p$.
(b) $J(\varepsilon, \chi) = 0$.
(c) $J(\chi, \chi^{-1}) = -\chi(-1)$.
(d) *If $\chi\psi \neq \varepsilon$, then*

$$J(\chi, \psi) = \frac{G(\chi)G(\psi)}{G(\chi\psi)}.$$

Proof. Part (a) is immediate. Part (b) is a consequence of Lemma 7.3.

To prove (c), notice that

$$J(\chi, \chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{a+b=1, b\neq 0} \chi\left(\frac{a}{b}\right) = \sum_{a\neq 1} \chi\left(\frac{a}{1-a}\right).$$

Set $a/(1-a) = c$. If $c \neq 1$, then $a = c/(1+c)$. It follows that as a varies over $\mathbb{F}_p$, except the element 1, then c varies over $\mathbb{F}_p$, except for -1. Thus

$$J(\chi, \chi^{-1}) = \sum_{c\neq -1} \chi(c) = -\chi(-1).$$

To prove (d), notice that

$$\begin{aligned} G(\chi)G(\psi) &= \left(\sum_x \chi(x)\zeta^x\right)\left(\sum_y \psi(y)\zeta(y)\right) \\ &= \sum_{x,y} \chi(x)\psi(y)\zeta^{x+y} \\ &= \sum_t \left(\sum_{x+y=t} \chi(x)\psi(y)\right)\zeta^t. \end{aligned}$$

If $t = 0$, then

$$\sum_{x+y=0} \chi(x)\psi(y) = \sum_x \chi(x)\psi(-x) = \psi(-1)\sum_x \chi\psi(x) = 0,$$

since $\chi\psi \neq \varepsilon$ by assumption.

If $t \neq 0$, define x' and y' by $x = tx'$ and $y = ty'$. If $x + y = t$, then $x' + y' = 1$. It follows that

$$G(\chi)G(\psi) = \sum_t \chi\psi(t)J(\chi,\psi)\zeta^t = J(\chi,\psi)G(\chi\psi).$$

Substituting into Equation (7.1) yields

$$G(\chi)G(\psi) = J(\chi,\psi)G(\chi\psi).$$

□

We have the following consequence

Corollary 4.2. *If χ, ψ, $\chi\psi$ are all not equal to ε, then $|J(\chi,\psi)| = \sqrt{p}$.*

Proof. Clear from Proposition 4.1. □

5. The Analogy between Gauss and Jacobi sums and Gamma and Beta functions

Gross and Koblitz [Ko1, Ko2]noted that there is an analogy between the Gauss sums and Jacobi sums, to the Gamma and Beta functions respectively. In this section the analogy is stated briefly.

Recall the (real) gamma function on $x > 0$ is defined as:

$$\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt,$$

and the (real) beta function on $x > 0, y > 0$ is defined as:

$$B(x,y) = \int_0^1 t^{x-1}(1-t)^{x-1}dt.$$

Note that the relation between Beta and Gamma function could be written as:

$$B(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$$

Here comes the analogy: the integration $\int dt$ could be viewed as a sum on the domain $(0,1)$. Note that $t \mapsto t^{x-1}$ is a multiplicative character from the multiplicative group of $\mathbb{R}_{\geq 0}$ to itself, determined by x. Also note that e^{-t} is an additive character from $[0,+\infty)$ to $[0,1]$. The analogy is then visually clear.

6. Eisenstein Sums

Let $\mathbb{F}_p = k \subset K \subset F$ be a tower of extensions of finite fields. Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^n}$ and put $q = p^f$. Then F is a finite extension of K and k. Denote with $\mathbf{Tr}$ the trace from F to k, and $\mathbf{tr}$ the trace form K to k, and $\mathbf{T}$ the trace from F to K. Note that $\mathbf{Tr} = \mathbf{T} \circ \mathbf{tr}$.

For a character χ on F with order $m > 1$ and an element $\alpha \in K$, we could form the Eisenstein sum

$$E(\chi; \alpha) = \sum_{T(t)=\alpha} \chi(t).$$

It is clear that $E(\chi;\alpha) \in \mathbb{Z}[\zeta_m]$. If $\alpha = a \in F$, we put $E(\chi;\alpha) = E_a(\chi)$, $E(\chi) = E_1(\chi)$. Denote by χ_K be the restriction of χ on K^*. The following properties of Eisenstein sums follows immediately from definition[**?**]:

Proposition 6.1. *Let χ be a character defined on F^*, where F is the extension of degree n over $K = \mathbb{F}_q$.*

1. *$E(\chi;\alpha) = \chi(\alpha)E(\chi)$ for all $\alpha \in K^*$;*
2. *$E(\chi^p;\alpha) = E(\chi;\alpha^p)$;*
3. *$G_\alpha(\chi) = E(\chi)G_\alpha(\chi_K) + E_0(\chi)$ for all $\alpha \in K$;*
4. *The table below gives some useful relations between Gauss and Eisenstein sums depending on whether $\chi_K = \mathbf{1}_K$ or not:*

	$E_0(\chi)$	$G_\alpha(\chi)$	$E(\chi)E(\chi^{-1})$
$\chi_K \neq \mathbf{1}_K$	0	$E(\chi)G_\alpha(\chi)$	q^{n-1}
$\chi_K = \mathbf{1}_K$	$(1-q)E(\chi)$	$qE(\chi)$	q^{n-2}

7. Power Residue Characters of Small Primes

Recall that the definition of Jacobi sums gives rise to the following proposition[Le1]:

Proposition 7.1. *Let $p = mn+1$ be a prime, and let χ be a character of order m on $\mathbb{F}_p^*$. Then $\chi(2) = -J(\chi^n,\chi^n) \mod 2$. In particular, if m is odd then 2 is an m-th power residue modulo p if and only if $J(\chi,\chi) \equiv 1 \mod 2$.*

Proof. The key observation is that the summation over t in the Jacobi sum

$$-J(\chi^n,\chi^n) = \sum_{t=2}^{p-2} \chi^n(t)\chi^n(1-t)$$

is symmetric with respect to $\frac{p+1}{2}$: since the contributions from t and $p+t-1$ are equal and therefore cancel modulo 2, we find

$$-J(\chi^n,\chi^n) \equiv \chi^n(\frac{p+1}{2})\chi^n(1-\frac{p+1}{2}) = \chi^{-2n}(2) = \chi(2) \mod 2.$$

Since different m-th roots of unity differ modulo 2 when m is odd, this implies that $\chi(2) = 1$ if and only if $J(\chi^n, \chi^n) \equiv 1 \mod 2$. But $J(\chi^n, \chi^n) = \sigma_n J(\chi, \chi)$, where σ_n is the automorphism of $\mathbb{Q}(\zeta_m)$ that sends $\zeta_m \mapsto \zeta_m^n$, and our claim follows. □

We also have the following Proposition that characterizes the power residue modulo small primes ([Le1], Prop.4.28.).

Proposition 7.2. *Let $\mathfrak{p}$ be a prime ideal of degree 1 in $K = \mathbb{Q}(\zeta_m)$; its norm is then a prime $p \equiv 1 \mod m$. Let $\chi = \left(\frac{\cdot}{p}\right)_m$ be an m-th power character modulo $\mathfrak{p}$. Then $J(\chi^a, \chi^b) \equiv 0 \mod \mathfrak{p}$ for all integers $a, b \geq 1$ such that $a + b \leq m - 1$.*

Proof. We have $\chi(t) \equiv t^{(p-1)/m} \mod \mathfrak{p}$ for every integer t coprime to p by definition of the power residue symbol. Hence

$$J(\chi^a, \chi^b) = t^{a(p-1)/m}(1-t)^{b(p-1)/m} \mod p.$$

The lemma below shows that the right hand side is divisible by p whenever the degree $(a+b)(p-1)/m$ of the polynomial is strictly smaller than $p - 1$. Since $\mathfrak{p} \mid p$, our claim follows. □

Lemma 7.3. *Let p be a prime; then*

$$\sum_{a=1}^{p-1} a^k \equiv \begin{cases} 0 \mod p, & \textit{if } 0 < k < p-1; \\ -1 \mod p, & \textit{if } k = p-1. \end{cases}$$

Proof. □

Lemma 7.4. *Let χ be a character on $\mathbb{F}_q$, and let ρ be the quadratic character on $\mathbb{F}_q$, then $J(\chi, \rho) = \chi(4)J(\chi, \chi)$.*

8. Number of Points on Certain Elliptic Curves and Jacobi Sums

A good use of the Jacobi sum is to determine the number of points on diagonal surfaces. As an example, here we evaluate the number of points of the special elliptic curves

$$E : y^2 = x^3 + D$$

Let ρ be the character of $\mathbb{F}_p$ of order 2 and χ be the character of $\mathbb{F}_p$ with order 3. Then the number of points on E_1 could be written as

$$\begin{aligned} N(y^2 = x^3 + D) &= \sum_{u+v=D} N(y^2 = u)N(x^3 = -v) \\ &= \sum_{u+v=D} (1 + \rho(u))(1 + \chi(-v) + \chi(-v)^2) \\ &= p + \sum_{u+v=D} \rho(u)\chi(v) + \sum_{u+v=D} \rho(u)\chi^2(v) \\ &= p + 1 + \rho\chi(D) + \overline{\rho\chi(D)J(\rho,\chi)} \end{aligned}$$

By applying the fact $J(\rho, \chi) = \chi(4)J(\chi, \chi)$, one gets

$$N(y^2 = x^3 + D) = p + 1 + \rho\chi(4D)J(\chi, \chi) + \overline{\rho\chi(4D)J(\chi, \chi)}.$$

For example let us consider the curve $y^2 = x^3 + 5$ over $\mathbb{F}_{19}$. Note that $19 = (5 + 3\omega)(3 + 3\omega^2)$, where ω is a primitive third root of unity. Note that $5 + 3\omega \equiv 2 \mod 3$, then $J(\chi, \chi) = 5 + 3\omega$. Since $4 \cdot 5 = 1$ is sixth power in $\mathbb{F}_{19}$, therefore the number of points is given by $19 + 1 + 5 + 3\omega + 5 + 3\omega^2 = 27$.

References

Ch1. S. Chowla, B. Dwork, and R.J. Evans. On the mod p^2 determination of $\binom{(p-1)/2}{(p-1)/4}$. *J. Number Theory*24(1986), 188-196.

Co1. H. Cohen, *Number Theory: Volume I Tools and Diophantine Equations, 2ed.* Graduate Texts in Mathematics 239. Springer-Verlag, Newyork, 1997.

Di1. G.L. Dirichlet. Recherches sur diverses applications de l'analysis infinitésimale à la théorie des nobres, *J. Reine Angew. Math.*21(1840), 134-155.

Ga1. C.F. Gauss, *Disquisitiones Arithmeticae,* Fleischer, Leipzig, 1801.

Ga2. C.F. Gauss. Summatio quarumdam serieum singularium, *Comment. Soc. Reg. Sci. Gottingensis*1(1811), 18pp.

Go1. B.H. Gross, N. Koblitz. Gauss sums and the p-adic Γ-function. *Ann. Math.* 109(1979), 569-581.

Ir1. K.F. Ireland, M.I. Rosen. *A Classical Introduction to Modern Number Thoery, 2ed* . Graduate Texts in Mathematics 84. Springer-Verlag, New York, 1990.

Ja1. C.G.J. Jacobi, Brief an Gauss vom 8. Februar 1827. [CW: vol. 7, pp.393-400]

Ko1. N. Koblitz. *p-adic Numbers, p-adic Analysis, and zeta-Functions.* Graduate Texts in Mathematics 59. Springer-Verlag, New York, 1977.

Ko2. N. Koblitz. *p-adic Analysis, a short Course on Recent Work.* London Mathematical Society lecture notes series 46. Cambirge University Press, London-New York, 1980.

Le1. F. Lemmermeyer. *Reciprocity laws: from Euler to Eisenstein.*Springer-Verlag, Berlin-Heidelberg-New York, 2000.

Sc1. C.-G. Schmidt. Gause Sums and the Classical Gamma Function. *Bull. London Math. Soc.*12 (1980), 344-346.

E-mail address: `wenw@uw.edu`