Gauss sums of the cubic character over GF(2m) : an elementary derivation

Schipani, D ; Elia, M

DOI: https://doi.org/10.4064/ba59-1-02

Gauss Sums of Cubic Characters over $GF(p^r)$, p odd

Michele Elia [*], Davide Schipani[†]

January 18, 2011

Abstract

An elementary approach is shown which derives the values of the Gauss sums over $\mathbb{F}_{p^r}$, p odd, of a cubic character without using Davenport-Hasse's theorem. New links between Gauss sums over different field extensions are shown in terms of factorizations of the Gauss sums themselves, which are then rivisited in terms of prime ideal decompositions. Interestingly, one of these results gives a representation of primes p of the form $6k+1$ by a binary quadratic form in integers of a subfield of the cyclotomic field of the p-th roots of unity.

Keywords: Gauss sum, character, finite fields, algebraic number fields.

Mathematics Subject Classification (2010): 12Y05, 12E30

1 Introduction

Let $\mathbb{F}_{p^r}$ be a Galois field of order p^r, with $\mathrm{Tr}_r(x) = \sum_{j=0}^{r-1} x^{p^j}$ being the trace function over $\mathbb{F}_{p^r}$, and $\mathrm{Tr}_{r/d}(x) = \sum_{j=0}^{r/d-1} x^{p^{dj}}$ the relative trace function over $\mathbb{F}_{p^r}$ relatively to $\mathbb{F}_{p^d}$, with $d|r$ [10].
Further let χ_m be a character of order m defined over $\mathbb{F}_{p^r}$ and taking values in the cyclotomic field $\mathbb{Q}(\zeta_m)$, where ζ_m denotes a primitive m-th root of unity.
The Gauss sum of χ_m over $\mathbb{F}_{p^r}$ is defined as ([3, 7])

$$G_r(\beta, \chi_m) = \sum_{y \in \mathbb{F}_{p^r}} \chi_m(y) \zeta_p^{\mathrm{Tr}_r(\beta y)} = \bar{\chi}_m(\beta) G_r(1, \chi_m) \ .$$

We will focus our interest on a cubic character χ_3 for an odd prime p (the case $p = 2$ is dealt with in [12]), namely χ_3 in this case is a mapping from $\mathbb{F}_{p^r}^*$ into the complex numbers defined as

$$\chi_3(\alpha^{h+3j}) = \zeta_3^h \quad h = 0, 1, 2 \ , \ j \in \mathbb{N}$$

where α is a generator of $\mathbb{F}_{p^r}^*$; in addition, $\chi_3(0) = 0$ by definition.
By the above assumptions, the values of the Gauss sums of a cubic character over $\mathbb{F}_{p^r}$ are in general algebraic integers in the field $\mathbb{Q}(\zeta_3, \zeta_p) = \mathbb{Q}(\zeta_{3p})$, $p \neq 3$ and $\mathbb{Q}(\zeta_3)$, if $p = 3$. Our aim is to derive more precise statements about these values with elementary techniques.

[*]Politecnico di Torino, Italy
[†]University of Zurich, Switzerland

2 Lemmas

For the considerations below, let

$$A_\ell(\alpha) = \sum_{y \in \mathbb{F}_{p^\ell}} \chi_m(y+\alpha) \ ,$$

where α may be in an extension of $\mathbb{F}_{p^\ell}$, and χ_m defined in the same extension.

Lemma 1 *Let χ_m be a nontrivial character of order m over $\mathbb{F}_{p^{2s}}$, p odd, whose restriction to $\mathbb{F}_{p^s}$ is also nontrivial; then*

$$G_{2s}(1,\chi_m) = \chi_m(\alpha) G_s(1,\chi_m) A_s(\frac{1}{2\alpha})$$

where α is a root of an irreducible polynomial $X^2-\beta$ (thus with relative trace $\mathrm{Tr}_{2s/s}(\alpha)=0$), for a suitable $\beta \in \mathbb{F}_{p^s}$ (that is $\chi_2(\beta)=-1$ for a quadratic character over $\mathbb{F}_{p^s}$).

PROOF. Since $\mathbb{F}_{p^{2s}}$ is a quadratic extension of $\mathbb{F}_{p^s}$, its elements can be written in the form $x+\alpha y$ with $x, y, \in \mathbb{F}_{p^s}$. We thus have

$$G_{2s}(1,\chi_m) = \sum_{z \in \mathbb{F}_{p^{2s}}} \chi_m(z) \zeta_p^{\mathrm{Tr}_{2s}(z)} = \sum_{x,y \in \mathbb{F}_{p^s}} \chi_m(x+\alpha y) \zeta_p^{\mathrm{Tr}_{2s}(x+\alpha y)} = \sum_{x,y \in \mathbb{F}_{p^s}} \chi_m(x+\alpha y) \zeta_p^{\mathrm{Tr}_s(2x)} \ ,$$

since

$$\mathrm{Tr}_{2s}(x+\alpha y) = \mathrm{Tr}_{2s}(x) + \mathrm{Tr}_{2s}(\alpha y) = 2\mathrm{Tr}_s(x) + \mathrm{Tr}_s(\alpha y) + \mathrm{Tr}_s(\alpha^{p^s} y) = 2\mathrm{Tr}_s(x) + \mathrm{Tr}_s(\alpha y) + \mathrm{Tr}_s(-\alpha y) \ ,$$

as the Frobenius map $x \to x^{p^s}$ permutes the roots of $X^2-\beta$. We thus have $\mathrm{Tr}_{2s}(x+\alpha y) = 2\mathrm{Tr}_s(x) = \mathrm{Tr}_s(2x)$. Multiplying the last sum by $\bar{\chi}_m(2)\chi_m(2)=1$, we can write

$$G_{2s}(1,\chi_m) = \bar{\chi}_m(2) \sum_{x',y \in \mathbb{F}_{p^s}} \chi_m(x'+2\alpha y) \zeta_p^{\mathrm{Tr}_s(x')} \ ,$$

and split the summation into three sums

$$\bar{\chi}_m(2) \sum_{y \in \mathbb{F}_{p^s}} \chi_m(2\alpha y) \ , \ \bar{\chi}_m(2) \sum_{x' \in \mathbb{F}^*_{p^s}} \chi_m(x') \zeta_p^{\mathrm{Tr}_s(x')} \ , \ \bar{\chi}_m(2) \sum_{x',y \in \mathbb{F}^*_{p^s}} \chi_m(x'+2\alpha y) \zeta_p^{\mathrm{Tr}_s(x')} \ .$$

The first summation is 0, the second summation is $\bar{\chi}_m(2) G_s(1,\chi_m)$; the third summation can be written as follows: the substitution $y = zx'$ yields

$$\bar{\chi}_m(2) \sum_{x',z \in \mathbb{F}^*_{p^s}} \chi_m(x'+2\alpha z x') \zeta_p^{\mathrm{Tr}_s(x')} = \bar{\chi}_m(2) \sum_{x' \in \mathbb{F}^*_{p^s}} \chi_m(x') \zeta_p^{\mathrm{Tr}_s(x')} \sum_{z \in \mathbb{F}^*_{p^s}} \chi_m(1+2\alpha z) =$$

$$\bar{\chi}_m(2) G_s(1,\chi_m) \chi_m(2\alpha) \sum_{z \in \mathbb{F}^*_{p^s}} \chi_m(z+\frac{1}{2\alpha}) = \bar{\chi}_m(2) G_s(1,\chi_m) \chi_m(2\alpha) [A_s(\frac{1}{2\alpha}) - \chi_m(\frac{1}{2\alpha})] \ .$$

In conclusion, by combining the above summations, we have $G_{2s}(1,\chi_m) = \chi_m(\alpha) G_s(1,\chi_m) A_s(\frac{1}{2\alpha})$.

□

Corollary 1 *Suppose p is odd and $t = 2^k s$, with $k \geq 1$, and let χ_m be a nontrivial character over $\mathbb{F}_{p^t}$, whose restriction to $\mathbb{F}_{p^s}$ is also nontrivial. Then*

$$G_t(1, \chi_m) = G_s(1, \chi_m) \prod_{i=1}^{k} \chi_m(\alpha_i) A_{2^{i-1}s}(\frac{1}{2\alpha_i}),$$

where α_i is a root of an irreducible polynomial $X^2 - \beta_i$ over $\mathbb{F}_{p^{2^{i-1}s}}$, $i = 1, \ldots, k$.

Lemma 2 *Let χ_m be a character over $\mathbb{F}_{p^s}$, $p \equiv -1$ mod m and m odd. Then $G_s(1, \chi_m)$ is real.*

PROOF.
We can write

$$G_s(1, \chi_m) = G_0 + \zeta_m G_1 + \zeta_m^2 G_2 + \cdots + \zeta_m^{m-1} G_{m-1} \ ,$$

where ζ_m is a primitive m-th root of unity and, for $0 \leq j \leq m-1$,

$$G_j = \sum_{\chi_m(x) = \zeta_m^j} \zeta_p^{\mathrm{Tr}_s(x)} \ .$$

These terms are real numbers, since $\chi_m(x) = \chi_m(-x)$, as $-1 = (-1)^m$ is an m-th power, thus in each sum the exponentials occur in complex conjugated pairs. Furthermore, $G_j = G_{m-j}$ as proved by the following argument:

$$G_j = \sum_{\chi_m(x) = \zeta_m^j} \zeta_p^{\mathrm{Tr}_s(x)} = \sum_{\chi_m(x) = \zeta_m^j} \zeta_p^{\mathrm{Tr}_s(x^p)} = \sum_{\chi_m(x^p) = \zeta_m^{pj}} \zeta_p^{\mathrm{Tr}_s(x^p)} = \sum_{\chi_m(y) = \zeta_m^{m-j}} \zeta_p^{\mathrm{Tr}_s(y)} = G_{m-j} \ ,$$

because raising the trace argument to the power p leaves the trace invariant, $\zeta_m^{pj} = \zeta_m^{-j}$ as p is congruent to -1 modulo m, and the automorphism $\sigma(x) = x^p$ simply permutes the elements of the field. Then for any j, $\zeta_m^j G_j$ and $\zeta_m^{m-j} G_{m-j}$ sum to give a real number, hence $G_s(1, \chi_m)$ is also real.

□

Corollary 2 *Let χ_3 be a nontrivial cubic character, $p \equiv 2$ modulo 3 ($p = 2$ or $p = 6k+5$). Then $G_s(1, \chi_3)$ is real.*

Remark 1. For the case $p = 2$, see an alternative proof in [12].

3 Results

Case p=3. If $p = 3$, then, for any r, $3^r - 1$ is not divisible by 3 and only the trivial character exists. Every β in $\mathbb{F}_{3^r}$ is a cube, as

$$\beta \cdot 1 = \beta \cdot (\beta^{3^r - 1}) = (\beta^{3^{r-1}})^3 \ ,$$

since $\beta^{3^r-1}=1$.
In this case, since $\mathbb{F}_{3^r}$ has only the trivial cubic character $\chi_3(x)=1$, $x\neq 0$, we have

$$G_1(1,\chi_3)=\sum_{y\in\mathbb{F}_3^*}\zeta_3^y=\sum_{y\in\mathbb{F}_3}\zeta_3^y-1=-1\ ,$$

as $\sum_{a\in\mathbb{F}_3}\zeta_3^a=0$. This same property holds for every $r>1$; in general we have

$$G_r(1,\chi_3)=\sum_{y\in\mathbb{F}_{3^r}}\chi_3(y)\zeta_3^{\mathrm{Tr}_r(y)}=\sum_{y\in\mathbb{F}_{3^r}}\zeta_3^{\mathrm{Tr}_r(y)}-1=3^{r-1}\sum_{a\in\mathbb{F}_3}\zeta_3^a-1=-1\ ,$$

as the character χ_3 is trivial and the number of elements with the same trace $a\in\mathbb{F}_3$ (0 included) is equal to 3^{r-1}, i.e. the number of roots in $\mathbb{F}_{3^r}$ of the equation $\mathrm{Tr}_r(x)=a$.

Case p=6k+5. If $p=6k+5$ and r is odd, a cubic character is trivial since every element β in $\mathbb{F}_{p^r}$ is a cube, as the following chain of equalities shows

$$\beta\cdot 1=\beta\cdot(\beta^{p^r-1})^2=\beta\beta^{2p^r-2}=\beta^{2p^r-1}=(\beta^{\frac{2p^r-1}{3}})^3\ ,$$

since $\beta^{p^r-1}=1$, and $p=-1 \bmod 3$, so that $2p^r-1$ is divisible by 3. The value of the Gauss sum is -1 as in the case $p=3$.
If $p=6k+5$ and r is even, a nontrivial cubic character exists and it will be shown, without recurring to Davenport-Hasse's theorem, that $G_r(1,\chi_3)=-(-p)^{r/2}$.

Theorem 1 *If $p=6k+5$ and s is odd, then $G_{2s}(1,\chi_3)=p^s$.*

PROOF. Let α be defined, as in Lemma 1, as a root of an irreducible polynomial $X^2-\beta$, with a suitable $\beta\in\mathbb{F}_{p^s}$, then the Gauss sum $G_{2s}(1,\chi_3)$ can be written as

$$G_{2s}(1,\chi_3)=\sum_{z\in\mathbb{F}_{p^{2s}}}\chi_3(z)\zeta_p^{\mathrm{Tr}_{2s}(z)}=\sum_{x,y\in\mathbb{F}_{p^s}}\chi_3(x+\alpha y)\zeta_p^{\mathrm{Tr}_{2s}(x+\alpha y)}=\sum_{x,y\in\mathbb{F}_{p^s}}\chi_3(x+\alpha y)\zeta_p^{\mathrm{Tr}_s(2x)}\ .$$

We split the summation into three

$$S_1=\bar\chi_3(2)\sum_{y\in\mathbb{F}_{p^s}}\chi_3(2\alpha y)\ ,\ S_2=\bar\chi_3(2)\sum_{x'\in\mathbb{F}_{p^s}^*}\chi_3(x')\zeta_p^{\mathrm{Tr}_s(x')}\ ,\ S_3=\bar\chi_3(2)\sum_{x',y\in\mathbb{F}_{p^s}^*}\chi_3(x'+2\alpha y)\zeta_p^{\mathrm{Tr}_s(x')}\ .$$

The first summation is $S_1=\chi(\alpha)(p^s-1)$, since the character is trivial over $\mathbb{F}_{p^s}$, the second summation is $S_2=-\bar\chi_3(2)$, and the third summation, after the substitution $y=zx'$, gives

$$S_3=\bar\chi_3(2)\sum_{x'\in\mathbb{F}_{p^s}^*}\chi_3(x')\zeta_p^{\mathrm{Tr}_s(x')}\sum_{z\in\mathbb{F}_{p^s}^*}\chi_3(1+2\alpha z)=-\bar\chi_3(2)[\chi_3(2\alpha)\sum_{z\in\mathbb{F}_{p^s}}\chi_3(\frac{1}{2\alpha}+z)-1]\ .$$

In order to evaluate $A_s(\frac{1}{2\alpha})=\sum_{z\in\mathbb{F}_{p^s}}\chi_3(\frac{1}{2\alpha}+z)$, we consider the sum of $A_s(\beta)$, for every $\beta\in\mathbb{F}_{p^{2s}}$, and observe that $A_s(\beta)=p^s-1$ if $\beta\in\mathbb{F}_{p^s}$, since all elements in this field are cubes, while, if $\beta\notin\mathbb{F}_{p^s}$ all sums assume the same value $A_s(\alpha)$, which is shown as follows: set $\beta=u+\alpha v$ with $v\neq 0$, then

$$\sum_{z\in\mathbb{F}_{p^s}}\chi_3(z+u+\alpha v)=\sum_{z\in\mathbb{F}_{p^s}}\chi_3(v)\chi_3((z+u)v^{-1}+\alpha)=\sum_{z'\in\mathbb{F}_{p^s}}\chi_3(z'+\alpha)=A_s(\alpha)\ .$$

Therefore, the sum $\sum_{\beta\in\mathbb{F}_{p^{2s}}} A(\beta) = \sum_{\beta\in\mathbb{F}_{p^{2s}}}\sum_{z\in\mathbb{F}_{p^s}} \chi_3(z+\beta) = \sum_{z\in\mathbb{F}_{p^s}}\sum_{\beta\in\mathbb{F}_{p^{2s}}} \chi_3(z+\beta) = 0$ yields

$$p^s(p^s-1) + (p^{2s}-p^s)A(\alpha) = 0$$

which implies $A(\alpha) = -1 = A(\frac{1}{2\alpha})$ (clearly $\frac{1}{2\alpha}$ is not in $\mathbb{F}_{p^s}$, otherwise $\alpha = \frac{1}{2\alpha}2\alpha^2 = 2\beta\frac{1}{2\alpha}$ would also be in $\mathbb{F}_{p^s}$). Finally, by combining the above,

$$G_{2s}(1,\chi_3) = \chi_3(\alpha)(p^s-1) + \chi_3(\alpha) = \chi_3(\alpha)p^s = p^s \ ,$$

since α, a root of $X^2-\beta$, is a cube, since every $\beta\in\mathbb{F}_{p^s}$ is a cube.

□

Remark 2. The above theorem can also be proved using a theorem by Stickelberger ([10, Theorem 5.16] or [13]).

Theorem 2 *If $p = 6k+5$ and s is even, then $G_{2s}(1,\chi_3) = (-p)^{s/2}G_s(1,\chi_3)$.*

PROOF.

Let $\alpha\in\mathbb{F}_{p^{2s}}$ be a cube and root of an irreducible polynomial $X^2-\beta$ over $\mathbb{F}_{p^s}$ (clearly such an α exists, since if γ is a root of $X^2-\beta$, with $\chi_2(\beta) = -1$, then γ^3, a cube, is a root of $X^2-\beta^3$ and $\chi_2(\beta^3) = \chi_2(\beta)^3 = -1$). Then by Lemma 1

$$G_{2s}(1,\chi_3) = G_s(1,\chi_3)A_s(\frac{1}{2\alpha}) \ ,$$

where $A_s(\frac{1}{2\alpha}) = \sum_{z\in\mathbb{F}_{p^s}}\chi_3(\frac{1}{2\alpha}+z)$ is an algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta_3)$ which can be written as $A_0+\zeta_3A_1+\zeta_3^2A_2$, where A_0, A_1, and A_2 are the number of characters $\chi_3(\frac{1}{2\alpha}+z)$ that are 1, ζ_3 or ζ_3^2, respectively, and $A_0+A_1+A_2 = p^s$.

Now, by Lemma 2, both $G_{2s}(1,\chi_3)$ and $G_s(1,\chi_3)$ are real, which implies that $A_s(\frac{1}{2\alpha})$ is also real, so that $A_1 = A_2$. We also know that $A_0+A_1+A_2 = A_0+2A_1 = p^s$, so we consider two equations for A_0 and A_1:

$$\begin{cases} A_0+2A_1 = p^s \\ A_0-A_1 = \pm p^{s/2} \end{cases}$$

obtained from the fact that we know the absolute values of $G_s(1,\chi_3)$ and $G_{2s}(1,\chi_3)$ ([3, Theorem 1.1.4, p.10],[12]).

Solving for A_1 we have $A_1 = \frac{1}{3}(p^s \mp p^{s/2})$. As A_1 must be an integer, we have

$$\begin{cases} A_0-A_1 = p^{s/2} & \text{if } s/2 \text{ is even} \\ A_0-A_1 = -p^{s/2} & \text{if } s/2 \text{ is odd.} \end{cases}$$

□

Corollary 3 *If $p = 6k+5$ and s is even, then $G_{2s}(1,\chi_3) = -p^s$.*

Case p=6k+1. If $p = 6k + 1$, $p^r - 1$ is divisible by 3, so there exists a nontrivial cubic character in $\mathbb{F}_{p^r}$ for every $r \geq 1$: we know that the Gauss sum over $\mathbb{F}_p$ of a nontrivial cubic character is an algebraic integer in $\mathbb{Q}(\zeta_{3p})$ of absolute value $\sqrt{p}$. Specifically we have

Theorem 3 *If $p = 6k+1$, then $G_1(1, \chi_3)$ is an element of $\mathbb{Q}(\zeta_3, \eta)$, a subfield of $\mathbb{Q}(\zeta_{3p})$ with degree 6 over $\mathbb{Q}$, where η is a root of a cubic polynomial with rational integer coefficients and cyclic Galois group over $\mathbb{Q}$.*

PROOF.
As in the proof of Lemma 2, for a cubic character we can write

$$G_1(1, \chi_3) = G_0 + \zeta_3 G_1 + \zeta_3^2 G_2 \ ,$$

where ζ_3 is a primitive cube root of unity and, for $0 \leq j \leq 2$,

$$G_j = \sum_{\chi_3(x)=\zeta_3^j} \zeta_p^x \ ,$$

which are real numbers since $\chi_3(x) = \chi_3(-x)$, as -1 is a cubic power. Let a be any positive integer less than p and $\sigma_a \in \mathfrak{G}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ be the element of the Galois group of $\mathbb{Q}(\zeta_p)$, whose action on ζ_p is defined as $\sigma_a(\zeta_p) = \zeta_p^a$ ([14]), then

$$\sigma(G_j) = \sum_{\chi_3(x)=\zeta_3^j} \zeta_p^{ax} = \sum_{\chi_3(x'a^{-1})=\zeta_3^j} \zeta_p^{x'} = \sum_{\chi_3(x')=\zeta_3^j \chi_3(a)} \zeta_p^{x'} \ .$$

This implies that any of these automorphisms induces a permutation of G_0, G_1, and G_2, and therefore leaves their symmetric functions invariant, which thus belong to $\mathbb{Q}$. In particular, the three elementary symmetric functions

$$s_1 = G_0 + G_1 + G_2 \ , \ \ s_2 = G_0G_1 + G_1G_2 + G_2G_1 \ , \ \ s_3 = G_0G_1G_2 \ ,$$

are rational integers; it follows that G_0, G_1, and G_2 are roots of a cubic polynomial with rational coefficients $p(x) = x^3 - s_1x^2 + s_2x - s_3$, which has a cyclic Galois group of order 3 (since $\frac{p-1}{3}$ values of a give the same permutation of its roots). Thus $p(x)$ is irreducible over $\mathbb{Q}$, and denoting one root with η, the other roots can be expressed as polynomials with integer coefficients $r_1(\eta)$ and $r_2(\eta)$ of degree 2 in η.

□

It is immediately seen that $s_1 = -1$, as $\sum_{x=0}^{p-1} \zeta_p^x = 0$, and it is natural to ask whether s_2 and s_3 can also be easily computed given p. We will show that $s_2 = -\frac{p-1}{3}$, while s_3 has not an equally simple expression, since it depends on the structure constants of the integral algebra generated by G_0, G_1, and G_2, as explained below.
Let σ be a generator of the cyclic Galois group of $\mathbb{Q}(\eta)$ (σ is also a generator of the Galois group of $p(x)$), then $G_0 = \eta$, $G_1 = \sigma(\eta)$, and $G_2 = \sigma^2(\eta)$ are linearly independent [2] and generate an integral algebra ([11, Lemma 2.2]), so that G_0G_1, G_1G_2, and G_2G_0 are linear combinations of G_0, G_1, and G_2 with integer coefficients ([11, Remark 2.3]). Furthermore, since these are cyclically permuted by the action of σ, we can write

$$\begin{cases} G_0G_1 = aG_0 + bG_1 + cG_2 \\ G_1G_2 = aG_1 + bG_2 + cG_0 \\ G_2G_0 = aG_2 + bG_0 + cG_1 \end{cases}$$

where a, b, c are integers whose sum is $\frac{p-1}{3}$, since each G_j contains $\frac{p-1}{3}$ powers of ζ_p and each G_iG_j expands into $\frac{(p-1)^2}{9}$ terms. Then, summing the three equations, we get

$$s_2 = (a+b+c)(G_0+G_1+G_2) = -\frac{p-1}{3} \ .$$

Evaluation of s_3 requires explicit knowledge of c: by summing the three equations, multiplied by G_2, G_0, and G_1 respectively, we obtain the relation

$$3G_0G_1G_2 = (a+b)s_2 + c(G_0^2+G_1^2+G_2^2) = (\frac{p-1}{3} - c)s_2 + c(1-2s_2) \ ,$$

which yields $s_3 = \frac{1}{3}[cp - \frac{(p-1)^2}{9}]$.

Remark 3. Since $\zeta_3^2 = -1-\zeta_3$, we can write

$$G_1(1,\chi_3) = G_0 - G_2 + \zeta_3(G_1 - G_2) \ ,$$

thus the relation $G_1(1,\chi_3)\bar{G}_1(1,\chi_3) = p$ yields

$$p = (G_0-G_2)^2 - (G_0-G_2)(G_1-G_2) + (G_1-G_2)^2$$

which shows that the equation $x^2 - xy + y^2 = p$ has further solutions in the order of $\mathbb{Q}(\zeta_p)$ besides the solutions in rational integers, for example $x = r_1(\eta) - \eta$ and $y = r_2(\eta) - \eta$.

Example Consider $p = 7$, then the Gauss sum has the form

$$G_1(1,\chi) = (\zeta_7 + \zeta_7^6) + \zeta_3(\zeta_7^2 + \zeta_7^5) + \zeta_3^2(\zeta_7^3 + \zeta_7^4) \ ,$$

the coefficients G_j of the powers of ζ_3 are real, and are roots of the cubic polynomial z^3+z^2-2z-1, which has a cyclic Galois group of order 3 over $\mathbb{Q}$. Let η_7 be a root of this polynomial. The other roots are $-2+\eta_7^2$, and $1-\eta_7-\eta_7^2$, thus it is direct to check that $x = -2+\eta_7^2-\eta_7$ and $y = 1-\eta_7-\eta_7^2-\eta_7$ give a representation of 7 through the quadratic form x^2-xy+y^2 in integers of $\mathbb{Q}(\eta_7)$, which may be of interest besides the 12 representations in rational integers (see e.g. [7, Proposition 8.3.1],[**?**]), namely $x = 2$ and $y = -1$ and those obtained through associates and conjugates of $2-\zeta_3$ in $\mathbb{Q}(\zeta_3)$.

A Gauss sum over $\mathbb{F}_{p^r}$ is in general also not rational, as can be seen using Davenport-Hasse's theorem ([3, 8]) by lifting the case over $\mathbb{F}_p$. Elementary proofs for every $r > 1$ appear to require special tricks that depend on r itself. However, an interesting expression is readily obtained by means of Lemma 1 considering the extension for $r = 2$, as proved in the following theorem.

Theorem 4 *If $p = 6k+1$, then $G_2(1,\chi_3)$ is again an element of the subfield $\mathbb{Q}(\zeta_3,\eta)$ of degree 6 of $\mathbb{Q}(\zeta_{3p})$, and in particular it can be written in the form*

$$G_2(1,\chi_3) = G_1(1,\chi_3)A_1(\frac{1}{2\alpha}) \ ,$$

where α is a root of $x^2-\beta$ and $\beta \in \mathbb{F}_p$ is a cube and quadratic non-residue.

PROOF.
As in Theorem 2, we can find such an α and then use Lemma 1 to deduce

$$G_2(1,\chi_3) = G_1(1,\chi_3)\sum_{z\in\mathbb{F}_p}\chi_3(\frac{1}{2\alpha}+z) = G_1(1,\chi_3)A_1(\frac{1}{2\alpha}) \ ,$$

where $A_1(\frac{1}{2\alpha})$ is an element of $\mathbb{Q}(\zeta_3)$ with absolute value $\sqrt{p}$ and $\chi_3(\alpha)=1$.
In conclusion $G_2(1,\chi_3) = G_1(1,\chi_3)A_1(\frac{1}{2\alpha})$ shows that $G_2(1,\chi_3)$ belongs to $\mathbb{Q}(\eta,\zeta_3)$.

□

Remark 4. Theorem 4 states that the Gauss sum $G_2(1,\chi_3)$ is the product of $G_1(1,\chi_3)$ and $A_1(\frac{1}{2\alpha})$, a result that is slightly different from that obtained using the Davenport-Hasse theorem, which states that $G_2(1,\chi_3') = -G_1(1,\chi_3)^2$, where χ_3' is defined by extending the nontrivial character over $\mathbb{F}_p$ to a character over $\mathbb{F}_{p^m}$, using the extension rule [7]

$$\chi_3'(x) = \chi_3(N_{F_{p^m}}(x)),$$

where $N_{F_{p^m}}(x) \doteq x\cdot x^p\cdots x^{p^{m-1}}$ is the norm of x. In our case we have $\chi_3'(x) = \chi_3(N_{F_{p^2}}(x))$, and whenever χ_3' is restricted to $\mathbb{F}_p$, we specifically have

$$\chi_3'(x) = \chi_3(N_{F_{p^2}}(x)) = \chi_3(x^2) = \bar{\chi}_3(x) \ \ \forall x\in\mathbb{F}_p \ .$$

Therefore, since $G_2(1,\bar{\chi}_3') = \chi_3'(-1)\bar{G}_2(1,\chi_3') = \bar{G}_2(1,\chi_3')$, the equation given by Davenport-Hasse can be read as

$$G_2(1,\chi_3') = -\bar{G}_1(1,\chi_3')^2 \ ,$$

where χ_3' is a cubic character defined in $\mathbb{F}_{p^2}$, and $\bar{G}_1(1,\chi_3')$ is evaluated on the subset $\mathbb{F}_p$.
In the following Proposition we show how this relation may also be derived elementarily. First we need a lemma (see also [7, Proposition 8.3.3] or [1]):

Lemma 3 *If $p=6k+1$, then $G_1(1,\chi_3)^3 = p\sum_{x\in\mathbb{F}_p}\chi_3(x(x-1))$.*

PROOF. The proof is straigthforward from the computation of the cube

$$G_1(1,\chi_3)^3 = \sum_{x,y,z\in\mathbb{F}_p}\chi_3(xyz)\zeta_p^{x+y+z} = \sum_{x,y,u\in\mathbb{F}_p}\chi_3(xy(u-x-y))\zeta_p^u \ ,$$

in which the substitution $u=x+y+z$ has been performed. The summation over x can be splitted into two summations S_1 and S_2, depending on whether $y=u$ or $y\neq u$. The first summation turns out to be 0, since

$$S_1 = \sum_{y\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_p}\chi_3(xy(x))\zeta_p^y = \sum_{y\in\mathbb{F}_p}\chi_3(y)\zeta_p^y\sum_{x\in\mathbb{F}_p}\chi_3(x^2) = \sum_{y\in\mathbb{F}_p}\chi_3(y)\zeta_p^y\sum_{x\in\mathbb{F}_p}\chi_3^2(x) = 0 \ .$$

The second summation, with the substitution $x=x'(u-y)$, becomes

$$S_2 = \sum_{\substack{y,u\in\mathbb{F}_p\\ y\neq u}}\zeta_p^u\sum_{x\in\mathbb{F}_p}\chi_3(xy(u-x-y)) = \sum_{\substack{y,u\in\mathbb{F}_p\\ y\neq u}}\chi_3(y)\zeta_p^u\sum_{x'\in\mathbb{F}_p}\bar{\chi}_3(u-y)\chi_3(x'(1-x')) \ .$$

Defining $A = \sum_{x' \in \mathbb{F}_p} \chi_3(x'(1-x'))$, a constant that does not depend on u and y, we may write

$$S_2 = A \sum_{u \in \mathbb{F}_p} \zeta_p^u \sum_{y \neq u} \chi_3(y)\bar{\chi}_3(u-y) = A[\sum_{y \in \mathbb{F}_p} \chi_3(y)\bar{\chi}_3(0-y) + \sum_{u \neq 0} \zeta_p^u \sum_{y \in \mathbb{F}_p} \chi_3(y)\bar{\chi}_3(u-y)] \ .$$

In conclusion, we have $S_2 = Ap$, since the first summation over y is $p-1$, the second summation over y is -1 independently of u ([12, 15]); finally, the summation over u is -1, so that $p-1+(-1)(-1) = p$.

□

Since $G_1(1,\chi_3)\bar{G}_1(1,\chi_3) = p$, the above result gives

$$G_1(1,\chi_3)^3 = G_1(1,\chi_3)\bar{G}_1(1,\chi_3)A$$

which implies that $G_1(1,\chi_3)^2 = \bar{G}_1(1,\chi_3)A$. On the other hand, Theorem 4 gives

$$G_2(1,\chi_3) = G_1(1,\chi_3)A_1(\frac{1}{2\alpha}) \ ,$$

thus we can prove the identity $G_2(1,\chi_3) = -\bar{G}_1(1,\chi_3)^2$, implied by the Davenport-Hasse theorem, if we can prove that $A = -\bar{A}_1(\frac{1}{2\alpha})$. It is in fact immediately seen that both A and $A_1(\frac{1}{2\alpha})$ are primes of the form $a + b\zeta_3$ and field norm p in $\mathbb{Z}(\zeta_3)$. Less direct is the exact relation between them, which we establish in the following proposition making use of the function defined as

$$F(d,i) \doteq \sum_{\substack{y \in \mathbb{F}_p^* \\ \chi_3(y)=1}} \left(\frac{\theta^i y + d}{p}\right) \ ,$$

where θ is a primitive element in $\mathbb{F}_p$.

Proposition 1

$$A = -\bar{A}_1(\frac{1}{2\alpha}) \ .$$

PROOF. We can write A in the following form

$$A = \sum_{x \in \mathbb{F}_p} \chi_3(x(x-1)) = \sum_{z \in \mathbb{F}_p} \chi_3(z^2 - \frac{1}{4}) \ , \tag{1}$$

where the last expression was obtained by making the substitution $x = z + \frac{1}{2}$. Furthermore, $A_1(\frac{1}{2\alpha})$ can be written in a similar form, arguing as follows:

$$\bar{A}_1(\frac{1}{2\alpha}) = \sum_{x \in \mathbb{F}_p} \bar{\chi}_3(x + \frac{1}{2\alpha}) = \sum_{x \in \mathbb{F}_p} \chi_3(x + \frac{1}{2\alpha})^2 \ ,$$

as the conjugate of ζ_3 is ζ_3^2. Furthermore, the identity $\chi_3(y) = \chi_3(y)^p = \chi_3(y^p)$, which is true since p is congruent to 1 modulo 3 and χ_3 is a multiplicative character, implies

$$\chi_3(x + \frac{1}{2\alpha}) = \chi_3(x + \frac{1}{2\alpha})^p = \chi_3(x^p + \frac{1}{(2\alpha)^p}) = \chi_3(x - \frac{1}{(2\alpha)}) \ ,$$

as x and 2 belong to $\mathbb{F}_p$, α is a root of $x^2-\beta$ and the Frobenius automorphism exchanges the roots. Then

$$\bar{A}_1(\frac{1}{2\alpha}) = \sum_{x\in\mathbb{F}_p} \chi_3(x+\frac{1}{2\alpha})\chi_3(x+\frac{1}{2\alpha}) = \sum_{x\in\mathbb{F}_p} \chi_3(x^2-\frac{1}{4\beta}) \ . \tag{2}$$

We notice now that, by definiton, the value of any summation $\sum_{z\in\mathbb{F}_p}\chi_3(z^2-d)$ can be written in the form $a_0+a_1\zeta_3+a_2\zeta_3^2$, where a_0, a_1 and a_2 are the numbers of $z\in\mathbb{F}_p$ such that the value of $\chi_3(z^2-d)$ is either 1, or ζ_3, or ζ_3^2. Therefore, writing $z^2-d=\theta^i y$, with $\chi_3(y)=1$, we have

$$a_i = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} [1+\left(\frac{\theta^i y+d}{p}\right)] = \frac{p-1}{3}+F(d,i) \quad i=0,1,2 \ ,$$

since $[1+\left(\frac{\theta^i y+d}{p}\right)]$ is equal to 0, if $\theta^i y+d$ is not a square; it is equal to 1 if $\theta^i y+d=0$; and it is equal to 2 if $\theta^i y+d$ is a square.
Then, setting $A=b_0+b_1\zeta_3+b_2\zeta_3^2$ and $\bar{A}_1(\frac{1}{2\alpha})=c_0+c_1\zeta_3+c_2\zeta_3^2$, and using the expressions for A and $\bar{A}_1(\frac{1}{2\alpha})$ given in (1) and (2), we obtain

$$b_i = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} [1+\left(\frac{\theta^i y+\frac{1}{4}}{p}\right)] \text{ and } c_i = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} [1+\left(\frac{\theta^i y+\frac{1}{4\beta}}{p}\right)] \quad i=0,1,2 \ .$$

The numbers c_i can be written as follows

$$c_i = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} [1+\left(\frac{\theta^i y+\frac{1}{4\beta}}{p}\right)] = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} [1-\left(\frac{\beta}{p}\right)\left(\frac{\theta^i y+\frac{1}{4\beta}}{p}\right)] = \sum_{\substack{y\in\mathbb{F}_p^* \\ \chi_3(y)=1}} [1-\left(\frac{\theta^i \beta y+\frac{1}{4}}{p}\right)]$$

because β is a quadratic nonresidue; furthermore, since β is a cube, setting $w=y\beta$, we deduce that

$$c_i = \sum_{\substack{w\in\mathbb{F}_p^* \\ \chi_3(w)=1}} [1-\left(\frac{\theta^i w+\frac{1}{4}}{p}\right)] = \frac{p-1}{3}-F(\frac{1}{4},i) \ .$$

which only differs in sign from $b_i=\frac{p-1}{3}+F(\frac{1}{4},i)$. The proposition follows from the fact that

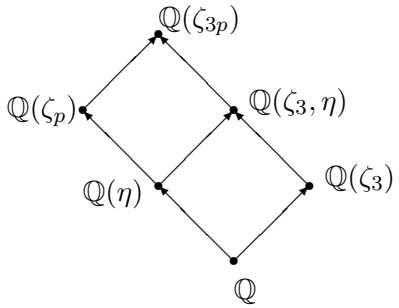
$$A = b_0+b_1\zeta_3+b_2\zeta_3^2 = (b_0-b_2)+(b_1-b_2)\zeta_3$$

and

$$\bar{A}_1(\frac{1}{2\alpha}) = (c_0-c_2)+(c_1-c_2)\zeta_3 = (b_2-b_0)+(b_2-b_1)\zeta_3 \ .$$

□

Remark 5. As has been said, Gauss sums are algebraic integers that belong to a subfield of a cyclotomic field, and in the above Theorems we found some factorizations of Gauss sums into elements that may belong to different subfields. For example Theorem 4 shows that $G_2(1,\chi_3) \in \mathbb{Q}(\zeta_3,\eta)$ can be expressed as a product of $G_1(1,\chi_3) \in \mathbb{Q}(\zeta_3,\eta)$ and $A_1(\frac{1}{2\alpha}) \in \mathbb{Q}(\zeta_3)$. The general picture of the fields involved in these factorizations is shown in the following figure



Every extension is Galois, in particular $\mathbb{Q}(\eta)$, $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_3,\eta)$ have Galois groups $\mathfrak{G}(\mathbb{Q}(\eta)/\mathbb{Q})$, $\mathfrak{G}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$, and $\mathfrak{G}(\mathbb{Q}(\zeta_3,\eta)/\mathbb{Q})$, which are cyclic groups of order 3, 2, and 6, respectively; moreover, the third group $\mathfrak{G}(\mathbb{Q}(\zeta_3,\eta)/\mathbb{Q}) = \mathfrak{G}(\mathbb{Q}(\zeta_3)/\mathbb{Q}) \times \mathfrak{G}(\mathbb{Q}(\eta)/\mathbb{Q})$ is a direct product of the other two (see also [14]). In these fields, every rational prime p of the form $6k+1$ splits into prime ideals as follows:

$(p) = \mathfrak{p}^3$ in $\mathbb{Q}(\eta)$, i.e. the ideal (p) fully ramifies;

$(p) = (\pi_1)(\pi_2)$ in $\mathbb{Q}(\zeta_3)$, i.e. the ideal (p) fully splits into principal ideals;

$(p) = \mathfrak{P}_1^3\mathfrak{P}_2^3$ in $\mathbb{Q}(\zeta_3,\eta)$, i.e. the ideal (p) fully splits into ramified ideals;

$(\pi_1) = \mathfrak{P}_1^3$ and $(\pi_2) = \mathfrak{P}_2^3$, i.e. the principal ideals of $\mathbb{Q}(\zeta_3)$ fully ramify in $\mathbb{Q}(\zeta_3,\eta)$;

$\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2$ in $\mathbb{Q}(\zeta_3,\eta)$.

These factorizations can be established by the properties given in [4, p.137-138], that is Dedekind's formulation in terms of ideals of a theorem of Kummer's, or in [14, p.15].
Let τ_2 denote the automorphism of order 2 in $\mathfrak{G}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$, which leaves the elements of $\mathbb{Q}(\eta)$ invariant when considered as elements of $\mathfrak{G}(\mathbb{Q}(\zeta_3,\eta)/\mathbb{Q})$, then $\tau_2(\mathfrak{P}_1) = \mathfrak{P}_2$.
Now, the Gauss sum $G_1(1,\chi_3)$ is an element of $\mathbb{Q}(\zeta_3,\eta)$ that divides p, as $G_1(1,\chi_3)\bar{G}_1(1,\chi_3) = p$ ([3]), so that $(G_1(1,\chi_3))(\tau_2(G_1(1,\chi_3))) = (G_1(1,\chi_3))(\bar{G}_1(1,\chi_3)) = (p)$.Therefore the principal ideal $(G_1(1,\chi_3))$ will be a product of powers of the two primes $\mathfrak{P}_1$ and $\mathfrak{P}_2$, i.e $(G_1(1,\chi_3)) = \mathfrak{P}_1^a\mathfrak{P}_2^b$, where $a+b=3$ by the unique factorization in prime ideals, since the previous relation gives $(p) = \mathfrak{P}_1^a\mathfrak{P}_2^b\tau_2(\mathfrak{P}_1^a\mathfrak{P}_2^b) = \mathfrak{P}_1^a\mathfrak{P}_2^b\mathfrak{P}_2^a\mathfrak{P}_1^b = \mathfrak{P}_1^{a+b}\mathfrak{P}_2^{a+b}$.
Thus, we may assume that $(G_1(1,\chi_3)) = \mathfrak{P}_1\mathfrak{P}_2^2$, as $G_1(1,\chi_3)$ belongs properly to $\mathbb{Q}(\zeta_3,\eta)$, whence Theorem 4 and Proposition 1 show that $(G_2(1,\chi_3)) = \mathfrak{P}_1^4\mathfrak{P}_2^2 = (\pi_1)\mathfrak{P}_1\mathfrak{P}_2^2$.
In this framework, if the character χ_3' is used, the role of the two prime ideals is simply exchanged, i.e. $(G_2(1,\chi_3')) = \mathfrak{P}_2^4\mathfrak{P}_1^2 = (\pi_2)\mathfrak{P}_2\mathfrak{P}_1^2$, which is the expression defined by the Davenport-Hasse theorem written in terms of ideals.

In general, the Gauss sums $G_s(1,\chi_3)$ for any s can be expressed in terms of ideals as follows: $(G_s(1,\chi_3)) = \mathfrak{P}_2^s\mathfrak{P}_1^{2s}$.
However, these formulations in terms of ideals (see also [5, 9, 13]) conceal the information about which units are involved. In this sense, the elementary direct approach can be more informative, although it may require various approaches for different situations. Considering for example the Gauss sum mentioned above, $G_1(1,\chi)$ for $p = 7$ (see also [6]), setting $\eta_7 = \zeta_7 + \zeta_7^6$, we can explicitly write

$$G_1(1,\chi) = \eta_7 + \zeta_3(-2 + \eta_7^2) + \zeta_3^2(1 - \eta_7 - \eta_7^2) \ ,$$

whereas, choosing the ideals $\mathfrak{P}_1 = (\zeta_3 - \eta_7)$, $\mathfrak{P}_2 = (\zeta_3^2 - \eta_7)$, we must find a unit in order to obtain complete factorization: $G_1(1,\chi) = (4 - \eta_7 - 2\eta_7^2)(\zeta_3 - \eta_7)(\zeta_3^2 - \eta_7)^2$, where $4 - \eta_7 - 2\eta_7^2$ is a unit.

Acknowledgment

The Research was supported in part by the Swiss National Science Foundation under grant No. 132256.

References

[1] S.D. Adhikari, The early reciprocity laws: from Gauss to Eisenstein, *Cyclotomic fields and related topics*, p.55-74, Bhaskaracharya Pratishthana, Pune 2000.

[2] E. Artin, *Galois Theory*, Second Edition, Notre Dame University, 1959.

[3] B. Berndt, R.J. Evans, H. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

[4] R. Dedekind, *Theory of Algebraic Numbers*, Cambridge, London, 1996.

[5] R. Denomme, A History of Stickelberger's Theorem, *Senior Honors Thesis*, The Ohio State University, 2009.

[6] P. Garrett, Kummer, Eisenstein, computing Gauss sums as Lagrange resolvents, *http://www.math.umn.edu/∼garrett*, 2010.

[7] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1990.

[8] D. Jungnickel, *Finite Fields, Structure and Arithmetics*, Wissenshaftsverlag, Mannheim, 1993.

[9] S.A. Katre, Gauss-Jacobi sums and Stickelberger's theorem, *Cyclotomic fields and related topics*, p.75-92, Bhaskaracharya Pratishthana, Pune 2000.

[10] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, 1986.

R. A. Mollin, *Advanced Number Theory with Applications*, CRC Press, Boca Raton (FL), 2010.

[11] C. Monico, M. Elia, An Additive Characterization of Fibers of Characters on $\mathbb{F}_p^*$ *International Journal of Algebra*, Vol. 1-4, n.3, 2010, p.109-117.

[12] D. Schipani, M. Elia, Gauss sums of the cubic character over $GF(2^m)$: an elementary derivation, *www.arxiv.org*, 2010.

[13] L. Stickelberger, Ueber eine Verallgemeinerung der Kreistheilung, Mathematische Annalen, XXXVII Band, 3 Heft, 1890, p.321-367.

[14] L.C. Washington, *Introduction to Cyclotomic Fields*, 2^{nd} edition, Springer, New York, 1997.

[15] A. Winterhof, On the Distribution of Powers in Finite Fields, *Finite Fields and Their applications*, 4, (1998), p.43-54.