BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 59, No. 1, 2011

FIELD THEORY AND POLYNOMIALS

Gauss Sums of the Cubic Character over GF(2^m): an Elementary Derivation

by

Davide SCHIPANI and Michele ELIA

Presented by Jerzy KACZOROWSKI

Summary. By an elementary approach, we derive the value of the Gauss sum of a cubic character over a finite field $\mathbb{F}_{2^s}$ without using Davenport–Hasse's theorem (namely, if s is odd the Gauss sum is -1, and if s is even its value is $-(-2)^{s/2}$).

1. Introduction. Let $\mathbb{F}_{2^s}$ be a Galois field over $\mathbb{F}_2$, with $\mathrm{Tr}_s(x) = \sum_{j=0}^{s-1} x^{2^j}$ being the trace function over $\mathbb{F}_{2^s}$, and $\mathrm{Tr}_{s/r}(x) = \sum_{j=0}^{s/r-1} x^{2^{rj}}$ the relative trace function over $\mathbb{F}_{2^s}$ relative to $\mathbb{F}_{2^r}$, with $r \mid s$ [3].

Further let χ_m be a character of order m defined over $\mathbb{F}_{2^s}$ and taking values in $\mathbb{Q}(\zeta_m)$, where ζ_m denotes a primitive mth root of unity and $\mathbb{Q}(\zeta_m)$ the corresponding cyclotomic field.

A Gauss sum of a character χ_m over $\mathbb{F}_{2^s}$ is defined as [1]

$$G_s(\beta, \chi_m) = \sum_{y \in \mathbb{F}_{2^s}} \chi_m(y) e^{\pi i \,\mathrm{Tr}_s(\beta y)} = \bar{\chi}_m(\beta) G_s(1, \chi_m) \quad \forall \beta \in \mathbb{F}_{2^s}.$$

A cubic character χ_3 is a mapping from $\mathbb{F}_{2^s}^*$ into the complex numbers defined as

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

where ζ_3 is a cubic root of unity, and α a primitive element in $\mathbb{F}_{2^s}^*$; furthermore we set by definition $\chi_3(0) = 0$.

The values of the Gauss sums of a cubic character over $\mathbb{F}_{2^s}$ can be found by computing the Gauss sum over $\mathbb{F}_4$ and applying Davenport–Hasse's theorem on the lifting of characters ([1, 2, 3]) for s even (and by computing

2010 *Mathematics Subject Classification*: Primary 12Y05; Secondary 12E30.
Key words and phrases: Gauss sum, character, binary finite fields.

DOI: 10.4064/ba59-1-2

the Gauss sum over $\mathbb{F}_2$ and then trivially lifting for s odd). However a more elementary approach is possible, and this is the subject of the present work.

If s is odd then the cubic character is trivial because every element β in $\mathbb{F}_{2^s}$ is a cube, as the following chain of equalities shows:

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

since $\beta^{2^s-1} = 1$, and $s+1$ is even, so that $2^{s+1}-1$ is divisible by 3. In this case we have

$$G_s(1, \chi_3) = \sum_{y\in\mathbb{F}_{2^s}} \chi_3(y) e^{\pi i \operatorname{Tr}_s(y)} = \sum_{y\in\mathbb{F}^*_{2^s}} e^{\pi i \operatorname{Tr}_s(y)} = -1,$$

since the number of elements with trace 1 is equal to the number of elements with trace 0, ($\operatorname{Tr}_s(x) \in \mathbb{F}_2$; moreover $\operatorname{Tr}_s(x) = 1$ and $\operatorname{Tr}_s(x) = 0$ are two equations of degree 2^{s-1}), and $e^{\pi i\cdot 0} = 1$ while $e^{\pi i \cdot 1} = -1$.

If s is even, the cubic character is nontrivial, and the computation of the Gauss sums requires some more effort; before we show how they can be computed with an elementary approach, we need some preparatory lemmas.

2. Preliminary facts. First of all we recall that, for any nontrivial character χ_m over $\mathbb{F}_q$, $\sum_{x\in\mathbb{F}_q} \chi_m(x) = 0$. This is used to prove a property of a sum of characters, already known to Kummer (see [4]), which can be formulated as follows

LEMMA 2.1. *Let χ_m be a nontrivial character and β any element of $\mathbb{F}_q$. Then*

$$\sum_{x\in\mathbb{F}_q} \chi_m(x)\bar{\chi}_m(x+\beta) = \begin{cases} q-1 & \text{if } \beta = 0, \\ -1 & \text{if } \beta \neq 0. \end{cases}$$

Proof. If $\beta = 0$, the summand is $\chi_m(x)\bar{\chi}_m(x) = 1$, unless $x = 0$ in which case it is 0, so the conclusion is immediate.

When $\beta \neq 0$, we can exclude again the term with $x = 0$, as $\chi_m(x) = 0$, so that x is invertible, and the summand can be written as

$$\chi_m(x)\bar{\chi}_m(x+\beta) = \chi_m(x)\bar{\chi}_m(x)\bar{\chi}_m(1+\beta x^{-1}) = \bar{\chi}_m(1+\beta x^{-1}).$$

With the substitution $y = 1 + \beta x^{-1}$, the summation becomes

$$\sum_{\substack{y\in\mathbb{F}_{2^{2m}} \\ y\neq 1}} \chi_m(y) = -1 + \sum_{y\in\mathbb{F}_{2^{2m}}} \chi_m(y) = -1,$$

as $\chi_m(y) = 1$ for $y = 1$. ∎

We are now interested in the sum $\sum_{x\in\mathbb{F}_q} \chi_m(x)\chi_m(x+1)$. Note that for the Gauss sums over $\mathbb{F}_{2^s}$ we have

$$G_s(1,\chi_m) = \sum_{\substack{y\in\mathbb{F}_{2^s}\\ \mathrm{Tr}_s(y)=0}} \chi_m(y) - \sum_{\substack{y\in\mathbb{F}_{2^s}\\ \mathrm{Tr}_s(y)=1}} \chi_m(y). \tag{2.1}$$

It follows that, if χ_m is a nontrivial character, then

$$G_s(1,\chi_m) = 2\sum_{\substack{y\in\mathbb{F}_{2^s}\\ \mathrm{Tr}_s(y)=0}} \chi_m(y).$$

In fact half of the field elements have trace 0 and the other half 1, so that

$$\sum_{\substack{y\in\mathbb{F}_{2^s}\\ \mathrm{Tr}_s(y)=0}} \chi_m(y) = -\sum_{\substack{y\in\mathbb{F}_{2^s}\\ \mathrm{Tr}_s(y)=1}} \chi_m(y)$$

as the sum over all field elements is zero, since χ_m is nontrivial.

LEMMA 2.2. *If χ_m is a nontrivial character over $\mathbb{F}_{2^s}$, then*

$$\sum_{x\in\mathbb{F}_{2^s}} \chi_m(x)\chi_m(x+1) = G_s(1,\chi_m).$$

Proof. We write the above sum as $\sum_{x\in\mathbb{F}_{2^s}} \chi_m(x(x+1))$, since the character is multiplicative. Now the function $f(x) = x(x+1)$ maps $\mathbb{F}_{2^s}$ onto its subset of 0-trace elements, as $\mathrm{Tr}_s(x) = \mathrm{Tr}_s(x^2)$ for any s, and each image comes from exactly two elements, x and $x+1$. It follows that

$$\sum_{x\in\mathbb{F}_{2^s}} \chi_m(x)\chi_m(x+1) = 2\sum_{\substack{y\in\mathbb{F}_{2^s}\\ \mathrm{Tr}_s(y)=0}} \chi_m(y) = G_s(1,\chi_m). \ \blacksquare \tag{2.2}$$

LEMMA 2.3. *Let χ_m be a nontrivial character of order $m = 2^r+1$. Then the Gauss sum $G_s(1,\chi_m)$ is a real number.*

Proof. Using (2.2) we have

$$\begin{aligned}\bar{G}_s(1,\chi_m) &= \sum_{x\in\mathbb{F}_{2^s}} \bar{\chi}_m(x)\bar{\chi}_m(x+1)\\ &= \sum_{x\in\mathbb{F}_{2^s}} \chi_m(x^{2^r})\chi_m(x^{2^r}+1)\\ &= \sum_{x\in\mathbb{F}_{2^s}} \chi_m(x)\chi_m(x+1) = G_s(1,\chi_m),\end{aligned}$$

as $\bar{\chi}_m(x) = \chi_m(x)^{2^r} = \chi_m(x^{2^r})$ and $x \mapsto x^{2^r}$ is a field automorphism, so it just permutes the elements of the field. $\blacksquare$

3. Main results. The absolute value of $G_s(1,\chi_m)$ can be evaluated using elementary standard techniques going back to Gauss (see e.g. [1]), while its argument requires a more subtle analysis. Our main theorems in this section yield in an elementary way the exact value of the Gauss sum for a cubic character χ_3 over $\mathbb{F}_{2^s}$, s even (the case of s odd is trivial, as shown above). Before we proceed, we show in a standard way what is its absolute value.

Since $G_s(\beta,\chi_3)=\bar{\chi}_3(\beta)G_s(1,\chi_3)$, on one hand, we have

$$\begin{aligned}\sum_{\beta\in\mathbb{F}_{2^s}} G_s(\beta,\chi_3)\bar{G}_s(\beta,\chi_3) &= \sum_{\beta\in\mathbb{F}_{2^s}} \bar{\chi}_3(\beta)\chi_3(\beta)G_s(1,\chi_3)\bar{G}_s(1,\chi_3)\\ &= \sum_{\beta\in\mathbb{F}^*_{2^s}} G_s(1,\chi_3)\bar{G}_s(1,\chi_3)\\ &= (2^s-1)G_s(1,\chi_3)\bar{G}_s(1,\chi_3).\end{aligned}\tag{3.1}$$

On the other hand, by the definition of Gauss sum, we have

$$\begin{aligned}&\sum_{\beta\in\mathbb{F}_{2^s}} G_s(\beta,\chi_3)\bar{G}_s(\beta,\chi_3)\\ &\qquad= \sum_{\beta\in\mathbb{F}_{2^s}}\sum_{\alpha\in\mathbb{F}_{2^s}}\sum_{\gamma\in\mathbb{F}_{2^s}} \bar{\chi}_3(\alpha)e^{\pi i\,\mathrm{Tr}_s(\beta\alpha)}\chi_3(\gamma)e^{-\pi i\,\mathrm{Tr}_s(\gamma\beta)},\end{aligned}$$

and substituting $\alpha=\gamma+\theta$ in the last sum, we have

$$\begin{aligned}\sum_{\beta\in\mathbb{F}_{2^s}} G_s(\beta,\chi_3)\bar{G}_s(\beta,\chi_3) &= \sum_{\gamma\in\mathbb{F}_{2^s}}\sum_{\theta\in\mathbb{F}_{2^s}} \bar{\chi}_3(\gamma+\theta)\chi_3(\gamma)\sum_{\beta\in\mathbb{F}_{2^s}} e^{\pi i\,\mathrm{Tr}_{2s}(\beta\theta)}\\ &= 2^s(2^s-1),\end{aligned}\tag{3.2}$$

as the sum on β is 2^s if $\theta=0$ and is 0 otherwise, since the values of the trace are equally distributed, as said above; consequently, the sum over γ is 2^s-1 times 2^s, as $\chi_3(0)=0$. From the comparison of (3.1) with (3.2) we get $G_s(1,\chi_3)\bar{G}_s(1,\chi_3)=2^s$, so $|G_s(1,\chi_3)|=2^{s/2}$.

Few initial values are $G_2(1,\chi_3)=2$, $G_4(1,\chi_3)=-4$, $G_6(1,\chi_3)=8$, $G_8(1,\chi_3)=-16$, and $G_{10}(1,\chi_3)=32$, so a reasonable guess is $G_s(1,\chi_3)=-(-2)^{s/2}$. This guess is correct as proved by the following theorems.

THEOREM 3.1. *If ℓ is odd, the value of the Gauss sum $G_{2\ell}(1,\chi_3)$ is 2^ℓ.*

Proof. Let α be a primitive cubic root of unity in $\mathbb{F}_{2^{2\ell}}$. Then it is a root of x^2+x+1. In other words, a root α of x^2+x+1, which does not belong to $\mathbb{F}_{2^\ell}$, as ℓ is odd, can be used to define a quadratic extension of this field, i.e. $\mathbb{F}_{2^{2\ell}}$, and the elements of this extension can be represented in the form $x+\alpha y$ with $x,y\in\mathbb{F}_{2^\ell}$. Furthermore, the two roots α and $1+\alpha$ of x^2+x+1 are either fixed or exchanged by any Frobenius automorphism; in particular the automorphism $\sigma^\ell(x)=x^{2^\ell}$ necessarily exchanges the two roots as it fixes precisely all the elements of $\mathbb{F}_{2^\ell}$, while α does not belong to this field, so that $\sigma^\ell(\alpha) \neq \alpha$. Now, a Gauss sum $G_{2\ell}(1,\chi_3)$ can be written as

$$G_{2\ell}(1,\chi_3) = 2\sum_{\substack{z\in\mathbb{F}_{2^{2\ell}}\\ \mathrm{Tr}_{2\ell}(z)=0}} \chi_3(z) = 2\sum_{\substack{x,y\in\mathbb{F}_{2^\ell}\\ \mathrm{Tr}_{2\ell}(x+\alpha y)=0}} \chi_3(x+\alpha y) \tag{3.3}$$
$$= 2\sum_{\substack{x,y\in\mathbb{F}_{2^\ell}\\ \mathrm{Tr}_\ell(y)=0}} \chi_3(x+\alpha y),$$

where we have used the trace property

$$\mathrm{Tr}_{2\ell}(x+\alpha y) = \mathrm{Tr}_{2\ell}(x)+\mathrm{Tr}_{2\ell}(\alpha y) = \mathrm{Tr}_\ell(x)+\mathrm{Tr}_\ell(x^{2^\ell})+\mathrm{Tr}_{2\ell}(\alpha y) = \mathrm{Tr}_{2\ell}(\alpha y),$$

and the fact that

$$\begin{aligned}\mathrm{Tr}_{2\ell}(\alpha y) &= \mathrm{Tr}_\ell(\alpha y) + \mathrm{Tr}_\ell(\alpha y)^{2^\ell} = \mathrm{Tr}_\ell(\alpha y) + \mathrm{Tr}_\ell((\alpha y)^{2^\ell})\\ &= \mathrm{Tr}_\ell(\alpha y) + \mathrm{Tr}_\ell(\alpha^{2^\ell} y) = \mathrm{Tr}_\ell(\alpha y) + \mathrm{Tr}_\ell((\alpha+1)y) = \mathrm{Tr}_\ell(y),\end{aligned}$$

since $\alpha^{2^\ell} = \alpha+1$ as shown previously. The last sum in (3.3) can be split into three sums by separating the cases $x=0$ and $y=0$:

$$\begin{aligned}2\sum_{\substack{x,y\in\mathbb{F}_{2^\ell}\\ \mathrm{Tr}_\ell(y)=0}} \chi_3(x+\alpha y) &= 2\sum_{\substack{y\in\mathbb{F}_{2^\ell}\\ \mathrm{Tr}_\ell(y)=0}} \chi_3(\alpha y) + 2\sum_{x\in\mathbb{F}_{2^\ell}} \chi_3(x)\\ &\quad + 2\sum_{\substack{x,y\in\mathbb{F}^*_{2^\ell}\\ \mathrm{Tr}_\ell(y)=0}} \chi_3(x+\alpha y).\end{aligned}$$

Considering the three sums separately, we have:

$$\sum_{x\in\mathbb{F}_{2^\ell}} \chi_3(x) = 2^\ell - 1,$$

as $\chi_3(x) = 1$ unless $x = 0$ since ℓ is odd;

$$\sum_{y\in\mathbb{F}_{2^\ell}\,\mathrm{Tr}_\ell(y)=0} \chi_3(\alpha y) = \chi_3(\alpha)(2^{\ell-1}-1),$$

as the character is multiplicative, $\chi_3(y) = 1$ unless $y = 0$, and only the 0-trace elements (which are $2^{\ell-1}-1$) should be counted; and

$$\begin{aligned}\sum_{\substack{x,y\in\mathbb{F}^*_{2^\ell}\\ \mathrm{Tr}_\ell(y)=0}} \chi_3(x+\alpha y) &= \sum_{\substack{x,y\in\mathbb{F}^*_{2^\ell}\\ \mathrm{Tr}_\ell(y)=0}} \chi_3(y)\chi_3(xy^{-1}+\alpha) = \sum_{\substack{z,y\in\mathbb{F}^*_{2^\ell}\\ \mathrm{Tr}_\ell(y)=0}} \chi_3(z+\alpha)\\ &= (2^{\ell-1}-1)\sum_{z\in\mathbb{F}^*_{2^\ell}} \chi_3(z+\alpha),\end{aligned}$$

as y is invertible, $\chi_3(y) = 1$ since ℓ is odd, z has been substituted for xy^{-1}, and the sum we get in the end, being independent of y, is simply multiplied by the number of values assumed by y. Altogether we have

$$G_{2\ell}(1,\chi_3) = 2^{\ell+1} - 2 + \chi_3(\alpha)(2^\ell - 2) + (2^\ell - 2) \sum_{z \in \mathbb{F}_{2^\ell}^*} \chi_3(z+\alpha)$$
$$= 2^{\ell+1} - 2 + (2^\ell - 2) \sum_{z \in \mathbb{F}_{2^\ell}} \chi_3(z+\alpha),$$

and, for later use, we define $A(\alpha) = \sum_{z\in\mathbb{F}_{2^\ell}} \chi_3(z+\alpha)$. In order to evaluate $A(\alpha)$, we consider the sum of $A(\beta)$ over $\beta \in \mathbb{F}_{2^{2\ell}}$, and observe that $A(\beta) = 2^\ell - 1$ if $\beta \in \mathbb{F}_{2^\ell}$, while if $\beta \notin \mathbb{F}_{2^\ell}$ all sums assume the same value $A(\alpha)$, which is shown as follows. Set $\beta = u + \alpha v$ with $v \neq 0$. Then

$$\sum_{z\in\mathbb{F}_{2^\ell}} \chi_3(z+u+\alpha v) = \sum_{z\in\mathbb{F}_{2^\ell}} \chi_3(v)\chi_3((z+u)v^{-1}+\alpha) = \sum_{z'\in\mathbb{F}_{2^\ell}} \chi_3(z'+\alpha).$$

Therefore, the sum

$$\sum_{\beta\in\mathbb{F}_{2^{2\ell}}} A(\beta) = \sum_{\beta\in\mathbb{F}_{2^{2\ell}}} \sum_{z\in\mathbb{F}_{2^\ell}} \chi_3(z+\beta) = \sum_{z\in\mathbb{F}_{2^\ell}} \sum_{\beta\in\mathbb{F}_{2^{2\ell}}} \chi_3(z+\beta) = 0$$

yields

$$2^\ell(2^\ell - 1) + (2^{2\ell} - 2^\ell)A(\alpha) = 0,$$

which implies $A(\alpha) = -1$, and finally

$$G_{2\ell}(1,\chi_3) = 2^{\ell+1} - 2 - (2^\ell - 2) = 2^\ell. \blacksquare$$

Remark. The above theorem can also be proved using a theorem by Stickelberger ([3, Theorem 5.16]).

Theorem 3.2. *If ℓ is even, then the Gauss sum $G_{2\ell}(1,\chi_3)$ is equal to $(-2)^{\ell/2}G_\ell(1,\chi_3)$.*

Proof. The relative trace of the elements of $\mathbb{F}_{2^{2\ell}}$ over $\mathbb{F}_{2^\ell}$, which is

$$\mathrm{Tr}_{2\ell/\ell}(x) = x + x^{2^\ell},$$

introduces the polynomial $x + x^{2^\ell}$ which defines a mapping from $\mathbb{F}_{2^{2\ell}}$ onto $\mathbb{F}_{2^\ell}$ with kernel $\mathbb{F}_{2^\ell}$ ([3]). The equation $x^{2^\ell} + x = y$ has in fact exactly 2^ℓ roots in $\mathbb{F}_{2^{2\ell}}$ for every $y \in \mathbb{F}_{2^\ell}$.

By definition we have

$$G_{2\ell}(1,\chi_3) = 2 \sum_{\substack{z\in\mathbb{F}_{2^{2\ell}} \\ \mathrm{Tr}_{2\ell}(z)=0}} \chi_3(z) = 2 \sum_{\substack{x,y\in\mathbb{F}_{2^\ell} \\ \mathrm{Tr}_{2\ell}(x+\alpha y)=0}} \chi_3(x+\alpha y),$$

where α is a root of an irreducible quadratic polynomial x^2+x+b over $\mathbb{F}_{2^\ell}$, i.e. $\mathrm{Tr}_\ell(b) = 1$ ([3, Corollary 3.79]) and $\mathrm{Tr}_{2\ell/\ell}(\alpha) = 1$, which can be seen from the coefficient of x of the polynomial. Now

$$\mathrm{Tr}_{2\ell}(x+\alpha y) = \mathrm{Tr}_{2\ell}(x) + \mathrm{Tr}_{2\ell}(\alpha y) = \mathrm{Tr}_{2\ell}(\alpha y) = \mathrm{Tr}_\ell(\alpha y) + \mathrm{Tr}_\ell(\alpha^{2^\ell} y),$$

but $\alpha^{2^\ell} = 1 + \alpha$, so that $\mathrm{Tr}_{2\ell}(x + \alpha y) = \mathrm{Tr}_\ell(y)$, and we have

$$\begin{aligned}
G_{2\ell}(1, \chi_3) &= 2 \sum_{\substack{x,y \in \mathbb{F}_{2^\ell} \\ \mathrm{Tr}_\ell(y)=0}} \chi_3(x + \alpha y) \\
&= 2 \sum_{x \in \mathbb{F}_{2^\ell}} \chi_3(x) + 2 \sum_{\substack{y \in \mathbb{F}^*_{2^\ell} \\ \mathrm{Tr}_\ell(y)=0}} \chi_3(\alpha y) + 2 \sum_{\substack{x,y \in \mathbb{F}^*_{2^\ell} \\ \mathrm{Tr}_\ell(y)=0}} \chi_3(x + \alpha y),
\end{aligned}$$

where the summation has been split into three sums, by separating the cases $y = 0$ and $x = 0$. We observe that, since the character over $\mathbb{F}_{2^\ell}$ is not trivial, the first sum is 0 and the second is $\chi_3(\alpha) G_\ell(1, \chi_3)$, while the third can be written as follows:

$$\begin{aligned}
2 \sum_{\substack{x,y \in \mathbb{F}^*_{2^\ell} \\ \mathrm{Tr}_\ell(y)=0}} \chi_3(x + \alpha y) &= 2 \sum_{\substack{x,y \in \mathbb{F}^*_{2^\ell} \\ \mathrm{Tr}_\ell(y)=0}} \chi_3(y)\chi_3(xy^{-1} + \alpha) \\
&= 2 \sum_{\substack{y \in \mathbb{F}^*_{2^\ell} \\ \mathrm{Tr}_\ell(y)=0}} \chi_3(y) \sum_{z \in \mathbb{F}^*_{2^\ell}} \chi_3(z + \alpha).
\end{aligned}$$

Putting all together, we obtain

$$G_{2\ell}(1, \chi_3) = G_\ell(1, \chi_3) \sum_{z \in \mathbb{F}_{2^\ell}} \chi_3(z + \alpha) = G_\ell(1, \chi_3) A_\ell(\alpha),$$

which shows that $|A_\ell(\alpha)| = 2^{\ell/2}$ and that $A_\ell(\alpha)$ is real, as both $G_{2\ell}(1, \chi_3)$ and $G_\ell(1, \chi_3)$ are real. Note that this holds for any α with $\mathrm{Tr}_{2\ell/\ell}(\alpha) = 1$. We will show now that $A_\ell(\alpha) = (-2)^{\ell/2}$. Consider the sum of $A_\ell(\gamma)$ over all γ with relative trace equal to 1, which is on one hand $2^\ell A_\ell(\alpha)$, as the polynomial $x^{2^\ell} + x = 1$ has exactly 2^ℓ roots in $\mathbb{F}_{2^{2\ell}}$, and on the other hand, explicitly we have

$$\begin{aligned}
\sum_{\substack{\gamma \in \mathbb{F}^*_{2^{2\ell}} \\ \mathrm{Tr}_{2\ell/\ell}(\gamma)=1}} A_\ell(\gamma) &= \sum_{z \in \mathbb{F}_{2^\ell}} \sum_{\substack{\gamma \in \mathbb{F}^*_{2^{2\ell}} \\ \mathrm{Tr}_{2\ell/\ell}(\gamma)=1}} \chi_3(z + \gamma) = \sum_{z \in \mathbb{F}_{2^\ell}} \sum_{\substack{\gamma' \in \mathbb{F}^*_{2^{2\ell}} \\ \mathrm{Tr}_{2\ell/\ell}(\gamma')=1}} \chi_3(\gamma') \\
&= 2^\ell \sum_{\substack{\gamma' \in \mathbb{F}^*_{2^{2\ell}} \\ \mathrm{Tr}_{2\ell/\ell}(\gamma')=1}} \chi_3(\gamma'),
\end{aligned}$$

where the summation order has been reversed, and $\mathrm{Tr}_{2\ell/\ell}(\gamma) = \mathrm{Tr}_{2\ell/\ell}(\gamma')$ as $\mathrm{Tr}_{2\ell/\ell}(z) = 0$ for any $z \in \mathbb{F}_{2^\ell}$. Comparing the two results, we have

$$A_\ell(\alpha) = \sum_{\substack{\gamma' \in \mathbb{F}^*_{2^{2\ell}} \\ \mathrm{Tr}_{2\ell/\ell}(\gamma')=1}} \chi_3(\gamma') = M_0 + M_1\zeta_3 + M_2\zeta_3^2,$$

where M_0 is the number of γ' with $\mathrm{Tr}_{2\ell/\ell}(\gamma') = 1$ that are cubic residues, i.e. they have character $\chi_3(\gamma')$ equal to 1, M_1 is the number of γ' with $\mathrm{Tr}_{2\ell/\ell}(\gamma') = 1$ that have character ζ_3, and M_2 is the number of γ' with $\mathrm{Tr}_{2\ell/\ell}(\gamma') = 1$ that have character ζ_3^2. Then $M_0 + M_1 + M_2 = 2^\ell$, and $M_1 = M_2$ since $A_\ell(\alpha)$ is real. Therefore, $A_\ell(\alpha) = M_0 - M_1$, and so we consider two equations for M_0 and M_1,

$$\begin{cases} M_0 + 2M_1 = 2^\ell, \\ M_0 - M_1 = \pm 2^{\ell/2}. \end{cases}$$

Solving for M_1 we have $M_1 = \frac{1}{3}(2^\ell \mp 2^{\ell/2})$. Since M_1 must be an integer, we obtain

$$\begin{cases} M_0 - M_1 = 2^{\ell/2} & \text{if } \ell/2 \text{ is even,} \\ M_0 - M_1 = -2^{\ell/2} & \text{if } \ell/2 \text{ is odd.} \end{cases} \blacksquare$$

COROLLARY 3.3. *For ℓ even, the value of the Gauss sum $G_{2\ell}(1, \chi_3)$ is -2^ℓ.*

Proof. This is a direct consequence of the two theorems above. ■

Acknowledgements. This research was partly supported by the Swiss National Science Foundation (grants No. 126948 and No. 132256).

References

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

[2] D. Jungnickel, *Finite Fields, Structure and Arithmetics*, Wissenschaftsverlag, Mannheim, 1993.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, Cambridge, 1986.

[4] A. Winterhof, *On the distribution of powers in finite fields*, Finite Fields Appl. 4 (1998), 43–54.

Davide Schipani
Institute of Mathematics
University of Zurich
8057 Zürich, Switzerland
E-mail: davide.schipani@math.uzh.ch

Michele Elia
Department of Electronics
Politecnico di Torino
10129 Torino, Italy
E-mail: michele.elia@polito.it

Received March 31, 2011 (7823)