ON THE NUMBER OF $N$-FREE ELEMENTS WITH PRESCRIBED TRACE

ALEKSANDR TUXANIDY AND QIANG WANG

ABSTRACT. Contrary to the case of the irreducible polynomials of degree $m$ over a finite field, say $F_q$, up to present there are no known (to the knowledge of the authors) explicit formulas for the number of primitive polynomials of degree $m$ over $F_q$ with a prescribed coefficient. For instance, whereas the number of irreducible polynomials with a prescribed trace coefficient (the coefficient of $x^{m-1}$) can be described by a simple beautiful formula due to Carlitz, no analogue is known in the case of primitives, even in any specific non-trivial case. In this paper we derive an explicit formula for the number of primitive elements, in quartic extensions of Mersenne prime fields, having absolute trace zero. We also give a simple formula in the case when $Q = (q^m - 1)/(q - 1)$ is prime. More generally, in the former case, for a positive integer $N$ whose prime factors divide $Q$ and satisfy the so called semi-primitive condition, we give an explicit formula for the number of $N$-free elements with trace zero. In addition we show that if all the prime factors of $q - 1$ divide $m$, then the number of primitive elements in $F_{q^m}$, with prescribed non-zero trace, is uniformly distributed. Finally we explore the related number, $P_{q^m}(N, c)$, of elements in $F_{q^m}$ with multiplicative order $N$ and having trace $c \in F_q$. By showing a connection between $N$-free and order in the special case when $L_Q | N$, where $L_Q$ is the largest divisor of $q^m - 1$ with the same radical as that of $Q$, we are able to derive the number of elements in $F_{p^4}$, $p$ being a Mersenne prime, with absolute trace zero and having the corresponding large order $L_Q$.

1. INTRODUCTION

Let $q$ be the power of a prime number $p$ and let $F_q$ be a finite field with $q$ elements. In 1992, Hansen and Mullen [10] conjectured that, except for very few exceptions, there exist both irreducible and primitive polynomials of degree $m$ over $F_q$ with any prescribed coefficient. This led to a great deal of work in the area, and both of these conjectures have since been resolved in the affirmative (see [18, 9] for irreducibles, as well as see the survey in [5] and [7] for primitives).

Particular interest has also been placed in deriving explicit formulas for the exact number of irreducible polynomials of degree $m$ over $F_q$ with one or more prescribed coefficients (see for example [3, 11, 12, 13, 19] and the survey [5] or Section 3.5 by S. D. Cohen in the Handbook of finite fields [16]). Here it is worth mentioning the following beautiful formula due to Carlitz [3] describing the number of irreducible polynomials of degree $m$ with a prescribed trace coefficient (the coefficient of $x^{m-1}$). Let $N_{q,m}(c)$ denote the number of irreducible polynomials of degree $m$ over $F_q$ with trace $c$. Let $\mu$ be the Möbius function.

Key words and phrases. $N$-free, character, Gaussian sum, Gaussian period, semi-primitive, primitive, irreducible polynomial, trace, Mersenne prime, uniform, prescribed coefficient, finite fields.

The research of Aleksandr Tuxanidy and Qiang Wang is partially supported by OGS and NSERC, respectively, of Canada.
Theorem 1.1 (Carlitz (1952)). Let $q$ be a power of a prime $p$ and let $m \in \mathbb{N}$. Then for any non-zero element $c \in \mathbb{F}_q \setminus \{0\}$, the number of irreducible polynomials of degree $m$ over $\mathbb{F}_q$ and with trace $c$ is given by

$$N_{q,m}(c \neq 0) = \frac{1}{qm} \sum_{d|m \atop p \nmid d} \mu(d)q^{m/d} = \frac{I(q,m) - N_{q,m}(0)}{q-1},$$

where

$$I(q,m) = \frac{1}{m} \sum_{d|m} \mu(d)q^{m/d}$$

is the number of irreducible polynomials of degree $m$ over $\mathbb{F}_q$.

Note that $N_{q,m}(c)$ is a constant for any $c \in \mathbb{F}_q^*$, and so $N_{q,m}(c)$ is said to be uniformly distributed for $c \in \mathbb{F}_q^*$. We will return to this concept later.

In the case of the primitive polynomials of degree $m$, or equivalently of primitive elements in $\mathbb{F}_{q^m}$, things are more complicated. Most of work on primitive polynomials with prescribed coefficients focus on the asymptotic analysis for their number and existence. One can see Section 4.2 by S. D. Cohen and the references therein, in the Handbook of Finite Fields [16]. In fact, except for the trivial cases and those when all the primitive polynomials of degree $m$ are all the irreducibles of degree $m$ (i.e., when $q = 2$ and $m = \ell$ with $2^\ell - 1$ a (Mersenne) prime) no explicit formulas are known to date. In particular an analogue, for primitives, to the formula above due to Carlitz is unknown, including in any specific non-trivial case of $q, m$.

In attacking the trace problem for primitives one should first note that, as Cohen [4] showed in the following theorem (see also [6] for a more self-contained proof) existence of such primitives is guaranteed except for the trivial cases corresponding to trace zero. Denote with $\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ the trace function from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$.

Theorem 1.2 (Cohen (1990)). Let $q$ be a power of a prime, let $r = q^m$ with $m > 1$, and let $c$ be an arbitrary element in $\mathbb{F}_r$. If $m = 2$ or $(q,m) = (4,3)$, further assume that $c \neq 0$. Then there exists a primitive element $\xi$ of $\mathbb{F}_r$ with $\text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(\xi) = c$.

It is a simple matter to show that in the case of quadratic extensions ($m = 2$) no primitive element of $\mathbb{F}_{q^2}$ with trace zero, in $\mathbb{F}_{q^2}$, exists. But in fact, as it turns out, this case falls under the more general category below of Proposition 1.3, for which we are able to, in this note, obtain the corresponding formula for the zero trace. First, for an integer $n \neq 0$, let us denote with $\text{Rad}(n)$ the product of all the distinct prime factors of $n$.

Proposition 1.3. Let $q = p^s$ be a power of a prime number $p$ and let $m > 1$ be an integer. Then there exists a positive integer $j$ such that

$$p^j \equiv -1 \pmod{\text{Rad}\left(\frac{q^m - 1}{q - 1}\right)}$$

if and only if $m = 2$, or, $q = p$ is a Mersenne prime and $m = 4$. The latter case only holds for $j = 2$.

Recall that a Mersenne prime $M_{\ell}$ is of the form $M_{\ell} = 2^\ell - 1$ for some prime $\ell$. Usually the world’s record of the largest prime is broken by a Mersenne prime, and, although only 48 such primes have been discovered thus far (see the Great Internet Mersenne Prime Search (GIMPS)
available online) it is a well-known conjecture that there exist infinitely many of them. They appear in various areas of number theory and finite fields, including in the Great Trinomial Hunt [2], an ongoing project for the search of primitive trinomials (i.e., primitive polynomials with exactly three non-zero terms) over $\mathbb{F}_2$ with degree the “exponent” $\ell$ of a Mersenne prime $M_\ell$.

We obtain the following simple formula for the number of primitive elements, with absolute trace zero, in quartic extensions of Mersenne prime fields. Let $\phi$ be the Euler’s totient function. In general, there are $\phi(q - 1)$ primitive elements in a finite field $\mathbb{F}_q$.

**Theorem 1.4.** Let $p$ be a Mersenne prime. Then the amount of primitive elements $\xi$ in $\mathbb{F}_p^\ast$, satisfying $\text{Tr}_{\mathbb{F}_p^4/\mathbb{F}_p}(\xi) = 0$ is given by

$$\frac{1}{p} \left( \phi(p^4 - 1) - \phi\left(\frac{p^4 - 1}{p + 1}\right) \right).$$

Although the formula above corresponds to primitive elements and hence primitive polynomials, we will however consider, in the sections that follow, the more general concept of an element of $\mathbb{F}_q^\ast$ being $N$-free, for a positive divisor $N$ of $q^m - 1$. But let us first fix the following notations and definitions.

**Notations:** In what follows we let $q = p^s$ be a power of a prime number $p$, let $r = q^m$, let $Q = (r - 1)/(q - 1)$, and let $\alpha$ be a primitive element of $\mathbb{F}_r$. For a positive divisor $N$ of $r - 1$, we say that a non-zero element $\xi \in \mathbb{F}_r^\ast$ is $N$-free if, for any $d \mid N$, $\xi = \gamma^d$, $\gamma \in \mathbb{F}_r$, implies $d = 1$. Equivalently, $\xi$ is $N$-free if and only if $\xi = \alpha^k$ for some integer $k$ that is coprime to $N$. Note that the definition of $N$-free is independent of the choice of the primitive element $\alpha$. Furthermore, for an element $c \in \mathbb{F}_q$, we denote with $Z_{q,r}(N,c)$ the number of $N$-free elements $\xi$ in $\mathbb{F}_r^\ast$ such that $\text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(\xi) = c$. Moreover we let $P_{q,r}(N,c)$ be the number of non-zero elements $\xi$ in $\mathbb{F}_r^\ast$ with multiplicative order $N$ and satisfying $\text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(\xi) = c$. In particular $Z_{q,r}(r - 1, c) = P_{q,r}(r - 1, c)$ is the number of primitive elements $\xi$ in $\mathbb{F}_r$ such that $\text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(\xi) = c$. For an integer $k$ and $N \mid r - 1$, denote

$$\Delta_k(N) := \sum_{d \mid N} \mu(d)\eta_k^{(d,r)},$$

where in the sum $\eta_k^{(d,r)}$ is the $k$-th Gaussian period of type $(d,r)$ (we refer the reader to Section 2 for its definition). Note that the value of $\Delta_k(N)$ depends only on the square-free part of $N$. As we shall see later on, there is a special reason behind the choice of the notation $\Delta$.

**Theorem 1.4** is a consequence of the following more general result. It is obtained thanks in part to well-known explicit expressions for the Gaussian periods in the so called semi-primitive case (see Lemma 2.6).

**Theorem 1.5.** Let $sm$ be even with $m > 1$, let $q = p^s$ be a power of a prime $p$, let $r = q^m$, and let $Q = (r - 1)/(q - 1)$. Suppose that $N \mid r - 1$ is such that $n := \gcd(Q,N) > 1$ is not a power of 2 and that $p^j \equiv -1 \pmod{\text{Rad}(n)}$ for some positive integer $j$. Assume that $j$ is the least such and define $\gamma = sm/2j$. Let $K_Q$ be the part of $N$ that is coprime to $Q$. Then the number of $N$-free elements $\xi \in \mathbb{F}_r$ with $\text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(\xi) = 0$ is given by

$$Z_{q,r}(N,0) = \frac{(q - 1)\phi(K_Q)}{qK_Q} \left( \frac{Q}{n} \phi(n) + \Delta_0(n) \right),$$
where the value of $\Delta_0(n)$ is given in what follows. First let $\eta_0^{2,r}$ be as in Lemma 2.4.

(a) If $\gamma$ and $p$ are odd, $n$ is even and 2 has multiplicity 1 in the factorization of $p^j + 1$, then

$$\Delta_0(n) = -\eta_0^{2,r} - \left(1 + \sqrt{r}\right) \left(\frac{1}{2} + \frac{\phi(n)}{n}\right).$$

(b) In all other cases,

$$\Delta_0(n) = -\epsilon_2 \left(\left(-1\right)^\gamma \sqrt{r} + 1 \right) + \eta_0^{2,r} \left(1 - \frac{1}{n}\right)\phi(n),$$

where

$$\epsilon_2 = \begin{cases} 1 & \text{if } n \text{ is even;} \\ 0 & \text{otherwise.} \end{cases}$$

Previously Cohen and Prešern [6] derived a formula for $Z_{q,r}(N,c)$ in terms of Gaussian sums (see Lemma 2.2 there). From this they were able to, through various assisting sieving inequalities, obtain improved lower bounds and estimates thus proving Theorem 1.2 in a more self-contained fashion than previously done in [1]. However as it was perhaps beyond the scope of their work, and except for their Corollary 2.3 where they give an explicit formula for $Z_{q,r}(N,c)$ in a few special cases of Theorem 1.5 above and Corollary 1.10 below, their results were mainly constrained to lower bounds and existence results. It is interesting to note that in the case of trace zero, as they showed in their Lemma 2.1, there is the connection between primitives with trace zero and $Q$-free elements with trace zero: $Z_{q,r}(r - 1,0) = \Theta(K)Z_{q,r}(Q,0)$. Here $K$ is the part of $r - 1$ that is coprime to $Q$, and $\Theta(K) = \phi(K)/K$ is the proportion of primitive $K$-th roots of unity among the $K$-th roots. But more generally, as we show here thorough our calculations, a lemma due to Ding and Yang [8] (see Lemma 2.1 there) implies that something similar holds in general for any divisor $N$ of $r - 1$: $Z_{q,r}(N,0) = \Theta(K)Z_{q,r}(\gcd(Q,N),0)$, where $K$ is now the part of $N$ that is coprime to $Q$. See the following lemma, proved later in Section 4.1.

**Lemma 1.6.** Let $q$ be a power of a prime, let $r$ be a power of $q$, let $N \mid r - 1$, let $K_Q$ be the largest divisor of $N$ that is coprime to $Q = (r - 1)/(q - 1)$, and let $g(N) = \gcd(Q,N)$. Then

$$Z_{q,r}(N,0) = \frac{(q - 1)\phi(K_Q)}{qK_Q} \left(\frac{Q}{g(N)}\phi(g(N)) + \Delta_0(g(N))\right).$$

Note that obtaining the value of $Z_{q,r}(N,0)$ boils down to computing $\Delta_0(\gcd(Q,N))$. Since Gaussian sums and hence periods are known in only very few cases, obtaining images of $\Delta_0$ may be quite hard in general. But by using known results on periods we can clearly obtain some explicit expressions. For instance we obtain the following two direct consequences.

**Theorem 1.7.** Let $q$ be a power of a prime, let $m \in \mathbb{N}$ and let $N \mid q - 1$ such that $N$ is coprime to $(q^m - 1)/(q - 1)$. Then the number of $N$-free elements $\xi \in \mathbb{F}_{q^m}$ with $\Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\xi) = 0$ is given by

$$Z_{q,q^m}(N,0) = \frac{\phi(N)}{N} (q^{m-1} - 1).$$

Setting $N = 1$ above one obtains the well-known number, $q^{m-1} - 1$, of non-zero elements lying in the kernel of the trace map.
Theorem 1.8. Let \( q \) be a power of a prime \( p \) and assume that \( Q = (q^\ell - 1)/(q - 1) \) is prime for some prime \( \ell \). Then the number of primitive elements \( \xi \in \mathbb{F}_q^* \) satisfying \( \text{Tr}_{\mathbb{F}_q}/\mathbb{F}_q(\xi) = 0 \) is given by

\[
Z_{q,q^\ell}(q^\ell - 1, 0) = \begin{cases} 
\phi(q^\ell - 1)/q & \text{if } \ell \neq p; \\
\phi(q^p - 1)/q - \phi(q - 1) & \text{otherwise}.
\end{cases}
\]

Since quadratic and cubic Gaussian periods are known as well, we also immediately obtain Theorems 4.4 and 4.5. These two correspond to the cases when \( \gcd(Q, N) \) is a power of 2 and 3, respectively.

In Section 5 we finally return to the concept of uniformity, already met in Theorem 1.1, now for \( N \)-free elements; in particular, for primitive elements. Although it is easy to find examples of \( q, m, N \) for which \( Z_{q,r}(N, c) \) does not behave uniformly for \( c \in \mathbb{F}_q^* \) (and indeed, when \( N = q^m - 1 \) is fixed as well), it is of special interest to find and classify instances of \( q, m, N \) for which \( Z_{q,r}(N, c \neq 0) \) does. One of the obvious reasons being that, in this case, in order to obtain the number of \( N \)-free elements with a prescribed non-zero trace, it would be enough to find the corresponding amount for the zero trace. The following theorem gives a sufficient criteria for this to happen, but we ask the interested reader to characterize all such instances of \( q, m, N \).

Theorem 1.9. Let \( q \) be a power of a prime \( q \), and let \( r \) be a power of \( q \), and let \( N \) be a positive divisor of \( r - 1 \). If every prime divisor of \( N \) divides \( Q = (r - 1)/(q - 1) \), then, for every element \( c \in \mathbb{F}_q \setminus \{0\} \), the amount of \( N \)-free elements \( \xi \in \mathbb{F}_r \) satisfying \( \text{Tr}_{\mathbb{F}_r}/\mathbb{F}_q(\xi) = c \) is given by

\[
Z_{q,r}(N, c \neq 0) = \frac{r^{-1} \phi(N) - Z_{q,r}(N, 0)}{q - 1}.
\]

In particular, setting \( N = r - 1 \), we obtain that \( Z_{q,r}(r - 1, c) \) is a constant for any \( c \in \mathbb{F}_q^* \) whenever the radical (the product of all the distinct prime divisors) of \( Q \) is the same as that of \( r - 1 \). This occurs whenever all the prime factors of \( q - 1 \) divide \( m \), where \( r = q^m \). See Corollary 5.3 for this. Thus we obtain the following immediate consequence to Theorems 1.9 and 1.5.

Corollary 1.10. Assume that \( q, r, N \), satisfy the assumptions of Theorem 1.9 and further assume that \( \text{Rad}(N) | Q \). Then for any non-zero \( c \in \mathbb{F}_q^* \), the number of \( N \)-free elements \( \xi \in \mathbb{F}_r \) with \( \text{Tr}_{\mathbb{F}_r}/\mathbb{F}_q(\xi) = c \) is given in what follows. First let \( \eta^{(2,r)}_0 \) be as in Lemma 2.4.

(a) If \( \gamma \) and \( p \) are odd, \( N \) is even and 2 has multiplicity 1 in the factorization of \( p^j + 1 \), then

\[
Z_{q,r}(N, c \neq 0) = \frac{1}{q} \left( \eta^{(2,r)}_0 + (1 + \sqrt{r}) \left( \frac{1}{2} + \frac{\phi(N)}{N} \right) + \phi(N) \left( \frac{qQ}{N} - 1 \right) \right).
\]

(b) In all other cases,

\[
Z_{q,r}(N, c \neq 0) = \frac{\phi(N)}{qN} \left( r + (-1)^{j+1} \sqrt{r} + qQ - N + \epsilon_2 \cdot \left( \frac{(-1)^j \sqrt{r} + 1}{2} + \eta^{(2,r)}_0 \right) \right),
\]

where

\[
\epsilon_2 = \begin{cases} 
1 & \text{if } N \text{ is even}; \\
0 & \text{otherwise}.
\end{cases}
\]
As a consequence of Theorem 1.9 one obtains the following interesting property of the sum \( \Delta_0(N) \) for \( N \mid r-1 \) such that \( \text{Rad}(N) \mid Q = (r-1)/(q-1) \). It is the constant difference between the amount of \( N \)-free elements with zero and non-zero traces in \( \mathbb{F}_t \), for any subfield \( \mathbb{F}_t \) of \( \mathbb{F}_q \).

**Corollary 1.11.** Let \( N \mid r-1 \) such that every prime divisor of \( N \) divides \((r-1)/(q-1)\). Then for every subfield \( \mathbb{F}_t \) of \( \mathbb{F}_q \) and every \( c_t \in \mathbb{F}_t \), we have
\[
\Delta_0(N) = Z_{t,r}(N,0) - Z_{t,r}(N, c_t \neq 0).
\]
Furthermore, if \( t \neq q \), then
\[
\Delta_0(N) = \frac{qZ_{q,r}(N,0) - tZ_{t,r}(N,0)}{q-t}.
\]

Although the paper is primarily concerned with the amount \( Z_{q,r}(N,c) \), we briefly consider in Section 6 the seemingly closely related number, \( P_{q,r}(N,c) \), of elements with order \( N \) having a prescribed trace \( c \). There we derive a general formula for \( P_{q,r}(N,c) \) (see Lemma 6.3) and show its relation to \( Z_{q,r}(N,c) \) as well as Hamming weights of specific codewords in irreducible cyclic codes. Let \( L_Q \) be the largest divisor of \( r-1 \) with the same radical as that of \( Q \). We also show, in Lemma [6.3] that if \( N \mid r-1 \) is such that \( L_Q \mid N \), then the following simple relation holds:
\[
Z_{q,r}(N,0) = \frac{1}{r} P_{q,r}(N,0).
\]
We believe it should not be too difficult to generalize this even further for arbitrary \( N \), but we leave this to the interested reader. As a consequence of this and of Theorem 1.4 we obtain in Theorem 6.4 the number of elements of order \( 2(p+1)(p^2+1) \), in quartic extensions of Mersenne prime fields \( \mathbb{F}_{p^r} \), with absolute trace zero.

The rest of the paper goes as follows. In Section 2 we go over some preliminary concepts which will be of use in further sections. In Section 3 we derive a formula for \( Z_{q,r}(N,c) \) in terms of Gaussian periods (see Lemma 3.4). In Section 4 we specifically consider the case of the zero trace and simplify our formula, in Subsection 4.1, with the use of a lemma due to Ding and Yang [8]. Then in Subsection 4.2 we prove Theorems 1.5 and 1.4. In Section 5 we give a sufficient criteria for uniformity to occur (see Theorem 1.9), as well as some other related results. Then in Section 6 we focus our attention to the number \( P_{q,r}(N,c) \) and give some other related results (see above). Finally in the Appendix we include a table of data corresponding to Theorem 1.4, giving the number of primitive elements in quartic extensions of Mersenne prime fields, with absolute trace zero, for the first ten Mersenne primes.

## 2. Preliminaries

In this section we go over some preliminary concepts which will be of use in further sections. As before, we let \( q = p^s \) be a power of a prime number \( p \), let \( \mathbb{F}_q \) be a finite field with \( q \) elements, let \( r = q^m \) and let \( \mathbb{F}_r \) be the degree-\( m \) extension of \( \mathbb{F}_q \). The following concepts and definitions are well-known and may be found for example in Chapter 5 of [14] and in [8]. Now let \( \chi_q, \chi_r \), be the canonical additive characters of \( \mathbb{F}_q, \mathbb{F}_r \), respectively, defined by \( \chi_q(x) = e^{2\pi i \text{Tr}(x)/p} \) for \( x \in \mathbb{F}_q \) and \( \chi_r = \chi_q \circ \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q} \). By the transitivity of the trace function, \( \chi_r(z) = e^{2\pi i \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(z)/p} \) for \( z \in \mathbb{F}_r \). Denote with \( \chi_{a}^{(r)} \) the additive character of \( \mathbb{F}_r \) corresponding to \( a \in \mathbb{F}_r \), that is \( \chi_{a}^{(r)}(z) = \chi_r(az) \) for any \( z \in \mathbb{F}_r \). Clearly \( \chi_1^{(r)} = \chi_r \). The following orthogonality relation will be of
use.

\[
\sum_{a \in \mathbb{F}_q} \chi_q(ax) = \begin{cases} 
q & \text{if } x = 0; \\
0 & \text{if } x \in \mathbb{F}_q^*. 
\end{cases}
\]

Let \( \alpha \) be a primitive element of \( \mathbb{F}_r \). For a divisor \( N \) of \( r-1 \), let \( \psi_N \) be a multiplicative character of \( \mathbb{F}_r \) of order \( N \). That is, \( \psi_N \) is defined by \( \psi_N(\alpha^j) = e^{2\pi \sqrt{-1} x/jN} \) for some integer \( j \) that is coprime to \( N \).

The Gaussian sums of order \( N \) are given by

\[
G_r(\psi_N, \chi_r(a)) = \sum_{\beta \in \mathbb{F}_r^*} \psi_N(\beta) \chi_r(a\beta).
\]

We denote \( G_r(\psi_N) := G_r(\psi_N, \chi_r) \). Note that if \( a \neq 0 \), then \( G_r(\psi_N, \chi_r^{(r)}) = \psi_N(a)G_r(\psi_N) \) (Theorem 5.12 (i), [14]).

For \( N \mid r-1 \), the cyclotomic classes of \( \mathbb{F}_r^* \) of type \( (N, r) \) are defined by \( C_{k,r} = \alpha^k \langle \alpha^N \rangle \), where \( k \in \mathbb{Z} \). Clearly \( C_{k,r} = C_{0,r} \) whenever \( k \equiv 0 \pmod{N} \). Then the Gaussian periods of type \( (N, r) \) are given by

\[
\eta_{k,r} = \sum_{x \in C_{k,r}} \chi_r(x).
\]

The Gaussian sums are the discrete Fourier transforms of the Gaussian periods and hence the two are related by the equation

\[
\eta_{k,r} = \frac{1}{N} \sum_{j=0}^{N-1} \sum_{x \in \mathbb{F}_r^*} \chi_r(\alpha^k x) \psi_N^j(x) = \frac{1}{N} \sum_{j=0}^{N-1} \psi_N^j(\alpha^k) G_r(\psi_N^j)
\]

\[
= \frac{1}{N} \left( -1 + \sum_{j=1}^{N-1} \psi_N^j(\alpha^k) G_r(\psi_N^j) \right),
\]

where \( \psi_N \) is a multiplicative character of \( \mathbb{F}_r \) with order \( N \) (see equation (9) in [8]).

In their study of Hamming weights of irreducible cyclic codes, Ding and Yang [8] recently obtained the following fact regarding cyclotomic classes.

**Lemma 2.1** (Lemma 5, [8]). Let \( N \) be a positive divisor \( r-1 \) and let \( k \in \mathbb{Z} \). We have the following multiset equality:

\[
\left\{ax : a \in \mathbb{F}_q^*, x \in C_{k,r} \right\} = \frac{(q-1) \gcd(Q,N)}{N} \cdot C_{k,\gcd(Q,N),r},
\]

where the right hand side denotes the multiset in which each element in the set \( C_{k,\gcd(Q,N),r} \) appears in the multiset with multiplicity \( \frac{(q-1) \gcd(Q,N)}{N} \).

A consequence to the above is the following.

**Lemma 2.2.** Let \( N \mid r-1 \) and let \( k \in \mathbb{Z} \). Then

\[
\sum_{i=0}^{q-2} \eta_{Q_i+k}^{(N,r)} = \frac{(q-1) \gcd(Q,N)}{N} \eta_k^{(\gcd(Q,N),r)}.
\]
Proof. For the sake of brevity denote \( g(N) := \gcd(Q, N) \). Now, by definition and by Lemma 2.1,

\[
\sum_{i=0}^{q-2} \eta_{Q^i+k}^{(N,r)} = \sum_{i=0}^{q-2} \sum_{x \in C_k^{(N,r)}} \chi_r(\alpha^{Q^i+k}x) = \sum_{i=0}^{q-2} \sum_{x \in C_k^{(N,r)}} \chi_r(\alpha^{Q^i}x)
\]

\[
= \sum_{a \in \mathbb{F}_q^*} \sum_{x \in C_k^{(N,r)}} \chi_r(ax) = \frac{(q-1)g(N)}{N} \sum_{x \in C_k^{(g(N),r)}} \chi_r(x)
\]

\[
= \frac{(q-1)g(N)}{N} \eta_k^{(g(N),r)}.
\]

\[\Box\]

Remark 2.3. It is known that \( \eta_k^{(N,r)} \in \mathbb{Z} \) whenever \( N \mid Q \) (see Theorem 13 (i) in [8]).

The following results about Gaussian periods are well known and may be found for example in [8]. We only give the 0-th Gaussian periods as these will be of greater interest to us in the sections that follow. For the other cases we refer the interested reader to [8]. First it is easy to show that \( \eta_k^{(1,r)} = -1 \) for any \( k \in \mathbb{Z} \) and hence \( \Delta_k(1) = -1 \).

Lemma 2.4. When \( N = 2 \), the 0-th Gaussian periods are given by the following:

\[
\eta_0^{(2,r)} = \begin{cases} 
-1 + \left(\frac{r_{1/2}}{2}\right)^{1/2} & \text{if } p \equiv 1 \pmod{4}; \\
-1 + \left(\frac{p^{1/2} - 1}{2}\right)^{1/2} & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]

In the case when \( N = 3 \) we only give a particular instance although the results in other cases are also known.

Lemma 2.5. Let \( N = 3 \), let \( sm \equiv 0 \pmod{3} \), let \( p \equiv 1 \pmod{3} \), and let \( c, d, \) be the unique (up to sign) solutions to the equation \( 4p^{s^m/3} = c^2 + 27d^2 \) with \( c \equiv 1 \pmod{3} \) and \( p \nmid c \). Then

\[
\eta_0^{(3,r)} = \frac{-1 + cr^{1/3}}{3}.
\]

The Gaussian periods in the so called semi-primitive case are known as well and are given in the following lemma. See [8].

Lemma 2.6. Assume that \( N > 2 \) and there exists a positive integer \( j \) such that \( p^j \equiv -1 \pmod{N} \) and that \( j \) is the least such. Let \( r = p^{2j\gamma} \) for some integer \( \gamma \).

(a) If \( \gamma, p \) and \((p^j + 1)/N\) are all odd, then

\[
\eta_0^{(N,r)} = -\frac{r^{1/2} + 1}{N}.
\]

(b) In all other cases,

\[
\eta_0^{(N,r)} = \frac{(-1)^{\gamma+1}(N-1)r^{1/2} - 1}{N}.
\]

The following fact will be useful as well.
Lemma 2.7. Let $q$ be a power of a prime $p$, let $r = q^m$, and let $Q = (r - 1)/(q - 1)$. Then

$$\eta_0^{(Q,r)} = \begin{cases} -1 & \text{if } p \nmid m; \\ q - 1 & \text{otherwise.} \end{cases}$$

Proof. By definition,

$$\eta_0^{(Q,r)} = \sum_{x \in (\alpha^Q)} \chi_r(x) = \sum_{x \in \mathbb{F}_q^*} \chi_r(x) = \sum_{x \in \mathbb{F}_q^*} \chi_q(\text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(x)) = \sum_{x \in \mathbb{F}_q^*} \chi_q(mx).$$

Now the result follows by (1). \qed

3. A FORMULA FOR $Z_{q,r}$

In this section we derive, in terms of Gaussian periods, a formula for the number of $N$-free elements with prescribed trace (see Lemma 3.4). Note that Cohen and Prešern [6] already did so in terms of Gaussian sums (see their Lemma 2.2). However by the means of Gaussian periods we will be able to apply the Ding-Yang lemma (Lemma 2.1 and 2.2) thus obtaining, for the case of the zero trace, the simplified version of Lemma 1.6 and the fact that $Z_{q,r}(N,0) = \Theta(K)Z_{q,r}(\gcd(Q,N),0)$ already mentioned in the Introduction. Recall that here $K$ is the part of $N$ that is coprime to $Q$, and $\Theta(K) = \phi(K)/K$.

The following characteristic function for $N$-free elements, due to Vinogradov, is typically used in works on the topic. See for instance [4, 5, 6, 7] and the references therein.

Proposition 3.1 (Vinogradov). Let $N$ be a positive divisor of $r - 1$ and let $\xi \in \mathbb{F}_r^*$. Then

$$\frac{\phi(N)}{N} \sum_{d \mid N} \frac{\mu(d)}{\phi(d)} \sum_{\psi: \text{ord}(\psi) = d} \psi(\xi) = \begin{cases} 1 & \text{if } \xi \text{ is } N\text{-free;} \\ 0 & \text{otherwise}, \end{cases}$$

where in the inner sum $\psi$ runs through all the multiplicative characters of $\mathbb{F}_r$ with order $d$.

We will however consider the following apparently simpler form of the function.

Lemma 3.2. Let $N$ be a positive divisor of $r - 1$ and let $\xi \in \mathbb{F}_r^*$. For each positive divisor $d$ of $N$, fix a multiplicative character $\psi_d$ of $\mathbb{F}_r$ with order $d$. Then

$$\sum_{d \mid N} \frac{\mu(d)}{d} \sum_{j=0}^{d-1} \psi_d^j(\xi) = \begin{cases} 1 & \text{if } \xi \text{ is } N\text{-free;} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $\alpha$ be primitive in $\mathbb{F}_r$. Then $\xi = \alpha^k$ for some integer $k$. Note that

$$\frac{1}{d} \sum_{j=0}^{d-1} e^{2\pi \sqrt{-1} jk/d} = \begin{cases} 1 & \text{if } d \mid k; \\ 0 & \text{otherwise.} \end{cases}$$

Hence

$$\sum_{d \mid N} \frac{\mu(d)}{d} \sum_{j=0}^{d-1} \psi_d^j(\alpha^k) = \sum_{d \mid N} \frac{\mu(d)}{d} \sum_{j=0}^{d-1} e^{2\pi \sqrt{-1} jk/d} = \sum_{d \mid \gcd(N,k)} \mu(d) = \begin{cases} 1 & \text{if } \gcd(N,k) = 1; \\ 0 & \text{otherwise.} \end{cases} \qed$$
Recall that for a positive divisor $N$ of $r - 1$, an integer $k$, and $c \in \mathbb{F}_q$, we denote
\[
\Delta_k(N) = \sum_{d|N} \mu(d) \eta_k^{(d,r)}.
\]

The following proposition highlights some of the basic properties of $\Delta_k$.

**Proposition 3.3.** Let $N | r - 1$ and let $k \in \mathbb{Z}$. Then we have the following three identities:
\[
\Delta_{Nk}(N) = \Delta_0(N);
\]
\[
\sum_{i=0}^{N-1} \Delta_i(N) = -\phi(N);
\]
and
\[
\Delta_k(N) = \sum_{\gcd(N,i-k)=1} \chi_r(x^i).
\]

**Proof.** The first identity follows from the fact that the sequence of periods of type $(N, r)$ has period $N$, i.e., $\eta_k^{(N,r)} = \eta_0^{(N,r)}$ whenever $k \equiv 0 \pmod{N}$. To prove the second identity, note that for each positive divisor $d$ of $N$,
\[
\sum_{i=0}^{N-1} \eta_i^{(d,r)} = \frac{N}{d} \sum_{i=0}^{d-1} \eta_i^{(d,r)} = \frac{N}{d} \sum_{x \in \mathbb{F}_r^*} \chi_r(x) = -\frac{N}{d}.
\]

Hence
\[
\sum_{i=0}^{N-1} \Delta_i(N) = \sum_{d|N} \mu(d) \sum_{i=0}^{N-1} \eta_i^{(d,r)} = -\sum_{d|N} \mu(d) \frac{N}{d} = -\phi(N).
\]

For the last identity, by (2) and Lemma 3.2, we have
\[
\Delta_k(N) = \sum_{d|N} \mu(d) \eta_k^{(d,r)} = \sum_{d|N} \frac{\mu(d)}{d} \sum_{j=0}^{d-1} \psi^j_d(\alpha^k) G_r(\psi^j_d)
\]
\[
= \sum_{d|N} \frac{\mu(d)}{d} \sum_{j=0}^{d-1} \psi^j_d(\alpha^k) \sum_{i=1}^{r-1} \chi_r(\alpha^i) \psi^j_d(\alpha^i)
\]
\[
= \sum_{i=1}^{r-1} \chi_r(\alpha^i) \sum_{d|N} \frac{\mu(d)}{d} \sum_{j=0}^{d-1} \psi^j_d(\alpha^{i-k})
\]
\[
= \sum_{\gcd(N,i-k)=1} \chi_r(\alpha^i).
\]

\[\square\]
For the sake of brevity let us also fix the following notation for the remaining of the paper.

\[ f_k(N, c, \Delta) := \sum_{i=0}^{q-2} \chi_q(\alpha Q_i c) \Delta_{Q_i+k}(N). \]

Now we give the general formula for \( Z_{q,r}(N, c) \).

**Lemma 3.4.** Let \( N \) be a positive divisor of \( r - 1 \) and let \( c \) be an arbitrary element of \( \mathbb{F}_q \). Then

\[ Z_{q,r}(N, c) = \frac{1}{q} \left( \frac{r - 1}{N} \phi(N) + f_0(N, c, \Delta) \right). \]

**Proof.** By the orthogonality relation in (1) and by the transitivity of the trace function, note that

\[ \frac{1}{q} \sum_{a \in \mathbb{F}_q} \chi_q(ac) \chi_r(a\alpha^k) = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \chi_q(a) \left( \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(\alpha^k) - c \right) = \begin{cases} 1 & \text{if } \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(\alpha^k) = c; \\ 0 & \text{otherwise}. \end{cases} \]

Thus if we multiply the characteristic function above with that of Lemma 3.2 and then sum over all the elements in \( \mathbb{F}_r^* \), we get

\[ Z_{q,r}(N, c) = \frac{1}{q} \sum_{d|N} \mu(d) \sum_{a \in \mathbb{F}_q} \chi_q(ac) \sum_{j=0}^{d-1} \sum_{k=1}^{r-1} \chi_r(a\alpha^k) \psi_d^j(\alpha^k) \]

\[ = \frac{1}{q} \left( \sum_{k=1}^{r-1} \sum_{d|N} \mu(d) \sum_{j=0}^{d-1} \psi_d^j(\alpha^k) + \sum_{i=0}^{q-2} \chi_q(\alpha Q_i c) \sum_{d|N} \mu(d) \sum_{j=0}^{r-1} \chi_r(\alpha^{Q_i x}) \psi_d^j(x) \right) \]

\[ = \frac{1}{q} \left( \frac{r - 1}{N} \phi(N) + \sum_{i=0}^{q-2} \chi_q(\alpha^{Q_i c}) \sum_{d|N} \mu(d) \eta_{Q_i}^{(d,r)} \right) \]

\[ = \frac{1}{q} \left( \frac{r - 1}{N} \phi(N) + f_0(N, c, \Delta) \right). \]

\[ \square \]

4. THE CASE OF THE ZERO TRACE

In this section we consider the special case of the zero trace and prove some of the corresponding results already mentioned in the Introduction, as well as give some other related results. We start off in Subsection 4.1 by deriving Lemma 1.6 and giving some immediate consequences. See Theorem 1.7 and 1.8 of the Introduction, as well as see Theorem 4.4 and 4.5. Then in Subsection 4.2 we prove Theorems 1.5 and 1.4 as well as prove the “semi-primitive” characterization in Proposition 1.3.

4.1. Simplification of \( Z_{q,r}(N, 0) \) and direct consequences. First, in the case of the zero trace, apply the Ding-Yang lemma (Lemma 2.1 and 2.2) to simplify the expression for \( f(N, 0, \Delta) \).
Lemma 4.1. Let $N \mid r - 1$, let $k \in \mathbb{Z}$ and let $K_Q$ be the largest divisor of $N$ that is coprime to $Q$. Then

$$f_k(N, 0, \Delta) = (q - 1) \frac{\phi(K_Q)}{K_Q} \Delta_k(g\gcd(Q, N)).$$

Proof. For a positive divisor $d$ of $r - 1$, let us denote, for the sake of brevity, $g(d) = \gcd(Q, d)$. Now, by Lemma 2.2,

$$f_k(N, 0, \Delta) = \sum_{d \mid N} \mu(d) \sum_{i=0}^{q-2} \eta^{(d, r)}_{Q_i + k} \left( q - 1 \right) \sum_{d \mid N} \mu(d) \frac{g(d)}{d} \eta_k^{(g(d), r)}.$$

Note Rad($N$) = Rad($K_Q$) Rad($g(N)$) is the product of the two coprime numbers Rad($K_Q$) and Rad($g(N)$). Then we can write any positive divisor $d$ of Rad($N$) uniquely as $d = yz$, where $y \mid \text{Rad}(K_Q)$ and $z \mid \text{Rad}(g(N))$. Moreover $g(yz) = z$ for any such $y, z$. Hence

$$f_k(N, 0, \Delta) = (q - 1) \sum_{y \mid K_Q \mid g(N)} \mu(y) \frac{g(yz)}{y} \frac{g(yz)}{y} \eta_k^{(g(yz), r)} = (q - 1) \sum_{y \mid K_Q} \mu(y) \sum_{z \mid g(N)} \mu(z) \eta_k^{(z, r)} = \left( q - 1 \right) \frac{\phi(K_Q)}{K_Q} \Delta_k(g(N)).$$

Proof of Lemma 1.6. By Euler’s product formula for $\phi$, and using the fact that $K_Q$ is coprime to $g(N)$ with Rad($N$) = Rad($K_Q$) Rad($g(N)$), we have

$$\frac{\phi(N)}{N} = \prod_{\ell \mid N} \left( 1 - \frac{1}{\ell} \right) = \left( \prod_{\ell \mid K_Q} \left( 1 - \frac{1}{\ell} \right) \right) \left( \prod_{\ell \mid g(N)} \left( 1 - \frac{1}{\ell} \right) \right) = \frac{\phi(K_Q)}{K_Q} \frac{\phi(g(N))}{g(N)},$$

where in the three products $\ell$ runs through all the distinct prime divisors of $N, K_Q$ and $g(N)$, respectively. Hence by Lemma 3.4 and 4.1

$$Z_{q, r}(N, 0) = \frac{1}{q} \left( (r - 1) \frac{\phi(N)}{N} + (q - 1) \frac{\phi(K_Q)}{K_Q} \Delta_0(g(N)) \right) = \frac{\phi(K_Q)}{q K_Q} \left( (r - 1) \frac{\phi(g(N))}{g(N)} + (q - 1) \Delta_0(g(N)) \right) = \frac{\phi(K_Q)}{q K_Q} \left( \frac{Q}{g(N)} \phi(g(N)) + \Delta_0(g(N)) \right).$$

In particular one obtains in Lemma 4.2 the number of primitives with zero trace. The second equality (on the right) gives Lemma 2.1 in [6].
Lemma 4.2. Let $D$ be the smallest positive divisor of $q - 1$ such that $(q - 1)/D$ is coprime to $Q$. Then the number of primitive elements $\xi$ in $\mathbb{F}_q$ with $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_Q}(\xi) = 0$ is given by

$$Z_{q,r}(r - 1, 0) = D\phi \left(\frac{q - 1}{D}\right) \frac{\phi(Q) + \Delta_0(Q)}{q} = D\phi \left(\frac{q - 1}{D}\right) \frac{Z_{q,r}(Q,0)}{q - 1}.$$ 

Some other immediate consequences to Lemma 1.6 are the following.

Proof of Theorem 4.4. Follows directly from Lemma 1.6 and 2.4.

Lemma 4.3. Let $q$ be a power of a prime $p$ and assume that $Q = (q^{\ell} - 1)/(q - 1)$ is prime for some prime $\ell$. Then

$$\Delta_0(Q) = \begin{cases} 0 & \text{if } \ell \neq p; \\ -q & \text{otherwise.} \end{cases}$$

Proof. Since $Q$ is prime, then $\Delta_0(Q) = -1 - \eta_0(Q^{p^\ell})$. Now the result follows from Lemma 2.7.

Proof of Theorem 1.8. Note that $\gcd(q - 1, Q) = 1$ since otherwise $Q \mid q - 1$ contradicting $Q > q - 1$ for $\ell \geq 2$. Now the result follows directly from Lemma 4.3 and 4.2.

Theorem 4.4. Let $q = p^s$, let $r = q^m$, let $Q = (r - 1)/(q - 1)$, let $N \mid r - 1$ such that $\gcd(Q,N) = 2^n$ for some $n \geq 1$, and let $K_Q$ be the largest odd divisor of $N$. Then

$$\frac{2qK_Q}{(q - 1)\phi(K_Q)}Z_{q,r}(N,0) = \begin{cases} Q - 1 + (-1)^{sm}r^{1/2} & \text{if } p \equiv 1 \pmod{4}; \\ Q - 1 + (-\sqrt{-1})^{sm}r^{1/2} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Proof. Follows directly from Lemma 1.6 and 2.4.

Theorem 4.5. Let $p \equiv 1 \pmod{3}$, let $q = p^s$, let $r = q^m$, let $Q = (r - 1)/(q - 1)$, let $N \mid r - 1$ such that $\gcd(N,Q) = 3^n$ for some $n \geq 1$, and let $K_Q$ be the largest odd divisor of $N$ with $3 \nmid K_Q$. Let $c \in \mathbb{Z}$ with $c \equiv 1 \pmod{3}$ and $p \nmid c$ be a solution to the equation $4r^{1/3} = c^2 + 27d^2$ with $d \in \mathbb{Z}$. Then

$$Z_{q,r}(N,0) = \frac{(q - 1)\phi(K_Q)qK_Q}{3} \left(\frac{2Q - 2 - cr^{1/3}}{3}\right).$$

Proof. Note that since $\gcd(Q,N) = 3$, then $Q \equiv m \equiv 0 \pmod{3}$. The result now follows from Lemma 2.5 and 1.6.

As a result of Theorem 1.2 one obtains the following interesting inequality for the sum $\Delta_0(Q)$. As we shall see later on, for any subfield $\mathbb{F}_t$ of $\mathbb{F}_q$ and every non-zero element $c_t \in \mathbb{F}_t^*$, we have $\Delta_0(Q) = Z_{t,r}(Q,0) - Z_{t,r}(Q,c_t \neq 0)$, where, as before, $Q = (r - 1)/(q - 1)$.

Proposition 4.6. Let $q$ be a power of a prime, let $r = q^m$, and let $Q = (r - 1)/(q - 1)$. Then we have the following inequality:

$$\Delta_0(Q) + \phi(Q) \geq 0$$

with equality holding if and only if $m = 1, 2$, or $(q, m) = (4, 3)$.

Proof. This is a direct consequence of Theorem 1.2 and the fact that $\Delta_0(1) = -1$ for the case of $m = 1$. 

□
4.2. Proof of Theorems 1.4 and 1.5. In this subsection we prove Theorems 1.5 and 1.4 stated in the Introduction, corresponding to the case of the zero trace. We employ the known explicit formulas for the Gaussian periods in the semi-primitive case (see Lemma 2.6) to first derive, in the following lemma, the value of the sum $\Delta_0(N)$ for $N$ falling under the category of Lemma 2.6. Then by Lemma 1.6 we get the result of Theorem 1.5. One of course can then naturally consider whether this result applies to primitives, but unfortunately, as Proposition 1.3 shows, it only extends to primitives in quartic extensions of Mersenne prime fields. However given the apparent absence of results in literature regarding the number of primitives with prescribed trace, then, in the opinion of the authors, the result of Theorem 1.4 stands on its own. Interestingly, Mersenne primes also appear in the trivial case for which a formula is known. This is the case when all the irreducibles are also the primitives, that is, when $q = 2$ and $m = \ell$ with $2^{\ell} - 1$ being a Mersenne prime. See the comments under Theorem 1.1 in the Introduction.

Lemma 4.7. Let $sm$ be even with $m > 1$, let $q = p^s$ be a power of a prime $p$, let $r = q^m$, and suppose that $n > 1$ is not a power of 2 and satisfies $n \mid r - 1$. Further assume that $p^j \equiv -1 \pmod{\text{Rad}(n)}$ for some positive integer $j$ and that $j$ is the least such. Define $\gamma = sm/2j$ and let $\eta_{0}^{(2,r)}$ be as in Lemma 2.4.

(a) If $\gamma$ and $p$ are odd, $n$ is even and $2$ has multiplicity 1 in the factorization of $p^j + 1$, then

$$
\Delta_0(n) = -\eta_{0}^{(2,r)} - \left(1 + \sqrt{r}\right)\left(\frac{1}{2} + \frac{\phi(n)}{n}\right).
$$

(b) In all other cases,

$$
\Delta_0(n) = \epsilon_2 \cdot \left(\frac{(-1)^{\gamma+1}\sqrt{r} - 1}{2} - \eta_{0}^{(2,r)}\right) + \frac{(-1)^{\gamma}\sqrt{r} - 1}{n} \phi(n),
$$

where

$$
\epsilon_2 = \begin{cases} 1 & \text{if } n \text{ is even;} \\ 0 & \text{otherwise.} \end{cases}
$$

Proof. First assume that $d \mid n$ with $d \geq 3$ and $\mu(d) \neq 0$. Clearly $p^j \equiv -1 \pmod{d}$. We claim that $j$ is the least such. Indeed, suppose on the contrary that $p^t \equiv -1 \pmod{d}$ for some $t < d$. Then for some integers $a, b$, with $a \neq b$, we have $ad = p^t + 1$ and $bd = p^t + 1$; hence $(a - b)d = p^t(p^{j-t} - 1)$. Since $p$ is a prime and $p \nmid d$, then $d \mid p^{j-t} - 1$ from which it follows that $d$ is a power of 2 (because $d \mid p^j + 1$ and $j \neq t$). But $d \geq 3$ with $\mu(d) \neq 0$. Contradiction. The claim follows.

(a) Consider any such $d$ as above. If $d$ is odd, then $(p^j + 1)/d$ is even and so $\eta_{0}^{(d,r)}$ belongs to case (b) of Lemma 2.6. Moreover since 2 has multiplicity 1 in the factorization of $p^j + 1$, then $(p^j + 1)/2d$ is odd if so is $d$; in this case $\eta_{0}^{(2d,r)}$ belongs to case (a) in Lemma 2.6. Now let $V_2$ be
the largest power of 2 dividing \( n \). We then have

\[
\sum_{3 \leq d | n} \mu(d) \eta_0^{(d,r)} = \sum_{3 \leq d | n \atop d \text{ odd}} \left( \mu(d) \eta_0^{(d,r)} + \mu(2d) \eta_0^{(2d,r)} \right) = \sum_{3 \leq d | n \atop d \text{ odd}} \mu(d) \left( \eta_0^{(d,r)} - \eta_0^{(2d,r)} \right)
\]

\[
= \sum_{3 \leq d | n \atop d \text{ odd}} \mu(d) \left( \frac{(d-1) \sqrt{r} - 1}{d} + \frac{\sqrt{r} + 1}{2d} \right)
\]

\[
= \sum_{3 \leq d | n \atop d \text{ odd}} \mu(d) \left( \sqrt{r} - \frac{\sqrt{r} + 1}{2d} \right)
\]

\[
= \frac{1 - \sqrt{r}}{2} + \sum_{d | n \atop d \text{ odd}} \mu(d) \left( \sqrt{r} - \frac{\sqrt{r} + 1}{2d} \right)
\]

\[
= \frac{1 - \sqrt{r}}{2} + \sum_{d | n/V_2} \mu(d) \left( \sqrt{r} - \frac{\sqrt{r} + 1}{2d} \right)
\]

\[
= \frac{1 - \sqrt{r}}{2} - \frac{\sqrt{r} + 1}{2} \sum_{d | n/V_2} \frac{\mu(d)}{d}
\]

\[
= \frac{1 - \sqrt{r}}{2} - \frac{(1 + \sqrt{r}) V_2}{2n} \phi \left( \frac{n}{V_2} \right)
\]

\[
= \frac{1 - \sqrt{r}}{2} - \frac{1 + \sqrt{r}}{n} \phi(n)
\]

since \( V_2 \) is coprime to \( n/V_2 \) and \( \phi(V_2) = V_2/2 \). Then we have

\[
\Delta_0(n) = -1 - \eta_0^{(2,r)} + \sum_{3 \leq d | n} \mu(d) \eta_0^{(d,r)} = -1 - \eta_0^{(2,r)} + \frac{1 - \sqrt{r}}{2} - \frac{1 + \sqrt{r}}{n} \phi(n).
\]

Result follows.

(b) As before assume \( d \mid n \) with \( d \geq 3 \) and \( \mu(d) \neq 0 \). We claim that \( \eta_0^{(d,r)} \) belongs to case (b) in Lemma 2.6. Indeed, if \( p \) or \( \gamma \) is even, then \( \eta_0^{(d,r)} \) belongs to (b). If \( d \) is odd, necessarily \( (p^j + 1)/d \) is even unless \( p \) is even; hence (b). This also takes care of the case when \( n \) is odd. Finally if \( n \) is even and 2 has multiplicity greater than 1 in the factorization of \( p^j + 1 \), then \( (p^j + 1)/2d \) is even.
for any such $d$ odd. The claim follows. Hence by Lemma [2.6](b) we have
\[
\sum_{3 \leq d | n} \mu(d) \eta^{(d,r)} = \sum_{3 \leq d | n} \mu(d) \left( \frac{(-1)^{\gamma+1}d\sqrt{r} + (-1)^{\gamma}\sqrt{r} - 1}{d} \right)
\]
\[
= 1 + \epsilon_2 \cdot \left( \frac{(-1)^{\gamma+1}\sqrt{r} - 1}{2} \right) + \sum_{d | n} \mu(d) \left( \frac{(-1)^{\gamma+1}\sqrt{r} + (-1)^{\gamma}\sqrt{r} - 1}{d} \right)
\]
\[
= 1 + \epsilon_2 \cdot \left( \frac{(-1)^{\gamma+1}\sqrt{r} - 1}{2} \right) + \sum_{d | n} \mu(d) \left( \frac{(-1)^{\gamma}\sqrt{r} - 1}{d} \right)
\]
\[
= 1 + \epsilon_2 \cdot \left( \frac{(-1)^{\gamma+1}\sqrt{r} - 1}{2} \right) + \frac{(-1)^{\gamma}\sqrt{r} - 1}{n} \sum_{d | n} \mu(d) \frac{n}{d}
\]
\[
= 1 + \epsilon_2 \cdot \left( \frac{(-1)^{\gamma+1}\sqrt{r} - 1}{2} \right) + \frac{(-1)^{\gamma}\sqrt{r} - 1}{n} \phi(n).
\]
Result follows. \[\square\]

**Proof of Theorem 1.5.** Follows directly from Lemma 4.7 and 1.6. \[\square\]

In order to prove Proposition 1.3 we make use of Mihăilescu’s result [15], also known as Catalan’s conjecture. Although like Wiles’ Theorem (Fermat’s Last Theorem) it is easily stated, it took 160 years for the conjecture to be finally solved, by Mihăilescu [15].

**Proposition 4.8 (Mihăilescu (2004)).** Let $x, y, a, b \in \mathbb{N}$ with $a, b > 1$. If $x^a - y^b = 1$, then $x = b = 3$ and $y = a = 2$.

**Proof of Proposition 1.3.** The case when $m = 2$ is clear as $(q^2 - 1)/(q - 1) = q + 1$ and so we can let $j = s$. Now write $m = 2^nk$ for some $n \geq 0$ and odd $k$. Note that $(q^k - 1)/(q - 1)$ is odd and
\[
\frac{q^m - 1}{q - 1} = \left( \frac{q^k - 1}{q - 1} \right) \prod_{i=0}^{n-1} \left( q^{2^i} + 1 \right).
\]
If $k > 1$ and $l$ is a (necessarily odd) prime divisor of $(q^k - 1)/(q - 1)$ and hence of $q^k - 1$, then $l \nmid (p^j + 1)$ since otherwise $l = 2$. Thus if the congruence above holds, then $k = 1$ and $m = 2^n$. Hence
\[
\frac{q^m - 1}{q - 1} = \prod_{i=0}^{n-1} \left( q^{2^i} + 1 \right).
\]
Let $t$ be a positive integer. We claim that Rad$(p^t + 1)$ | $(p^j + 1)$ if and only if $t = j$, or, $t = 1$ and $p$ is a Mersenne prime. Indeed, suppose a prime divisor $l$ of $p^t + 1$ divides $p^j + 1$. Then $al = p^t + 1$ and $bl = p^j + 1$ for some integers $a, b$. Without loss of generality we may assume that $j \geq t$. Then $(b - a)l = p^t(p^{j-t} - 1)$. If $a \neq b$, then, since $l$ is a prime, it follows that either $l = p$ or $l \nmid (p^{j-t} - 1)$. Only the latter case is possible which occurs if and only if $t = j$ or $l = 2$ (since $l \nmid (p^j + 1)$). Then if $t \neq j$, necessarily Rad$(p^t + 1)$ | $(p^j + 1)$ if and only if $p^t = 2^v - 1$ for some positive integer $v$; i.e., if and only if $2^v - p^t = 1$. In this case it is clear that $v > 1$; then we can not have $t > 1$ since otherwise Proposition 4.8 is contradicted. Hence $t = 1$ and $p = 2^v - 1$ is a Mersenne prime.
The claim follows. As a result, only one of the values $\text{Rad}(q^2 + 1), \text{Rad}(q^2 + 1), \ldots$, can divide $p^i + 1$. But, if $i > 1$ and $q^2 + 1$ divides $(q^m - 1)/(q - 1)$, then $q^2 + 1$ divides $(q^m - 1)/(q - 1)$. Hence if the congruence is satisfied for $m > 2$, then only the case of $m = 4$ is possible, whence $(q^m - 1)/(q - 1) = (q + 1)(q^2 + 1)$. If $\text{Rad}(q^2 + 1) \mid (p^j + 1)$, the claim above implies that $j = 2s$. But then $\text{Rad}(q + 1) \mid (p^{2s} + 1)$ if and only if $q = p$ is a Mersenne prime, whence $s = 1$ and $j = 2$. Now conversely, since $\text{Rad}((q + 1)(q^2 + 1)) = \text{Rad}(q^2 + 1)$ if $q = p$ is a Mersenne prime, then $j = 2$ is the unique solution to the congruence.

**Proof of Theorem 1.4.** Theorem 1.5 applies with $j = 2$. In particular, in the case of primitives, i.e., $F_q$, prove Theorem 1.9. As a consequence of this and of Theorem 1.5, Corollary 1.10 is straightforward. In particular, in the case of primitives, i.e., $N = r - 1$, we give sufficient conditions for $Z_{q,r}(r - 1, c)$ to behave uniformly for $c \in F_q$. See Corollary 5.3 for this.

5. Uniformity in the case of the non-zero trace

In this section we explore the concept of uniformity, already discussed in the Introduction. That is, the main concern here is as follows: what triples $(q, r, N)$, with $r = q^m$ and $N \mid r - 1$, are such that $Z_{q,r}(N, c)$ is a constant for every non-zero $c \in F_q$? Accordingly, in this section we prove Theorem 1.9. As a consequence of this and of Theorem 1.5, Corollary 1.10 is straightforward. In particular, in the case of primitives, i.e., $N = r - 1$, we give sufficient conditions for $Z_{q,r}(r - 1, c)$ to behave uniformly for $c \in F_q$. See Corollary 5.3 for this.

**Lemma 5.1.** Let $N \mid r - 1$, let $c \in F_q$, be arbitrary, let $K_Q$ be the largest divisor of $N$ that is coprime to $Q$, and let $g(N) = \gcd(Q, N)$. Then

$$Z_{q,r}(N, c \neq 0) = \frac{1}{q} \left( \frac{r - 1}{N} \phi(N) + K_Q \frac{r - 1}{N} \phi(N) - qZ_{q,r}(N, 0) \right) + f_0(N, c, \Delta) - f_0(g(N), c, \Delta).$$
Proof. By Proposition 3.3 and using the fact that \( \sum_{a \in \mathbb{F}_q} \chi_q(ac) = -1 \) for \( c \neq 0 \), we get

\[
f_0(g(N), c, \Delta) = \sum_{i=0}^{q-2} \chi_q(\alpha Q_i \Delta) \Delta_{Q_i}(g(N)) = \sum_{i=0}^{q-2} \chi_q(\alpha Q_i \Delta) \Delta_0(g(N))
\]

Hence

\[
f_0(N, c, \Delta) = -\Delta_0(g(N)) + f_0(N, c, \Delta) - f_0(g(N), c, \Delta).
\]

By Lemma 1.6 we can write \( \Delta_0(g(N)) \) in terms of \( Z_{q,r}(N, 0) \). Now the expression for \( Z_{q,r}(N, c) \neq 0 \) follows from Lemma 3.4.

Proof of Theorem 1.9. If every prime divisor of \( N \) divides \( Q \), then \( \text{Rad}(N) = \text{Rad}(q(N)) \) and \( K_Q = 1 \). Now the result follows from Lemma 5.1 together with the fact that \( f_0(d, c, \Delta) = f_0(\text{Rad}(d), c, \Delta) \) for every \( d \mid r - 1 \).

Lemma 5.2. Let \( b, m \in \mathbb{N} \). Then \( \text{Rad}(b^m - 1) = \text{Rad}(\frac{b^m - 1}{b-1}) \) if and only if every prime factor of \( b - 1 \) divides \( m \).

Proof. First note that \( \text{Rad}(b^m - 1) = \text{Rad}(\frac{b^m - 1}{b-1}) \) if and only if \( \text{Rad}(b - 1) \mid \text{Rad}(\frac{b^m - 1}{b-1}) \). Now

\[
\frac{b^m - 1}{b-1} = 1 + b + b^2 + \cdots + b^{m-1}
\]

\[
= (1 - b) + (b - 1) + (b^2 - 1) + \cdots + (b^{m-1} - 1) + b + m - 1.
\]

It follows that \( \text{Rad}(b - 1) \mid \text{Rad}(\frac{b^m - 1}{b-1}) \) if and only if \( \text{Rad}(b - 1) \) divides \( m \).

As a result of Lemma 5.2, we obtain the following immediate result.

Corollary 5.3. Let \( q \) be a power of a prime, let \( m \in \mathbb{N} \) and let \( r = q^m \). If every prime factor of \( q - 1 \) divides \( m \), then, for every element \( c \in \mathbb{F}_q \setminus \{0\} \), the amount, \( Z_{q,r}(r-1, c) \), of primitive elements \( \xi \in \mathbb{F}_r \) with \( \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(\xi) = c \), is given by

\[
Z_{q,r}(r-1, c \neq 0) = \frac{\phi(r-1) - Z_{q,r}(r-1, 0)}{q - 1}.
\]

Some other consequences to Theorem 1.9 are the following.

Corollary 5.4. Let \( N \mid r - 1 \) such that \( \text{Rad}(N) \mid Q \) and let \( \mathbb{F}_t \) be any subfield of \( \mathbb{F}_q \). Then, for all \( c_t \in \mathbb{F}_t^* \) and \( c_q \in \mathbb{F}_q^* \), we have

\[
Z_{t,r}(N, c_t \neq 0) = \frac{\phi(N) - Z_{t,r}(N, 0)}{t - 1} = q^\frac{t}{t-1}Z_{q,r}(N, c_q).
\]

Proof. Follows from Theorem 1.9 together with the fact that, since \( N \mid (r - 1)/(q - 1) \) and \( (r - 1)/(q - 1) \mid (r - 1)/(t - 1) \), then \( N \mid (r - 1)/(t - 1) \).
**Proof of Corollary** [1,11]. The first equality follows directly from Lemma [1,6] and Theorem [1,9] together with the fact mentioned in the proof of Corollary [5,4]. The second equality follows from the first together with Corollary [5,4]. Indeed,

\[ qZ_{q,r}(N,0) - tZ_{t,r}(N,0) = q(\Delta_0(N) + Z_{q,r}(N,c_q)) - t(\Delta_0(N) + Z_{t,r}(N,c_t)) \]

\[ = (q-t)\Delta_0(N) + qZ_{q,r}(N,c_q) - tZ_{t,r}(N,c_t) \]

\[ = (q-t)\Delta_0(N). \]

**Corollary 5.5.** Let \( N \mid r-1 \) such that \( \text{Rad}(N) \mid Q \). Then \( Z_{t,r}(N,0) \) is related to \( Z_{q,r}(N,0) \) by the equation

\[ (q-1)Z_{t,r}(N,0) = \left(q - \frac{q}{t}\right)Z_{q,r}(N,0) + \left(\frac{q}{t} - 1\right)\frac{r-1}{N}\phi(N). \]

**Proof.** By Corollary [1,11] we have

\[ Z_{t,r}(N,0) - Z_{t,r}(N,c_t) = Z_{q,r}(N,0) - Z_{q,r}(N,c_q). \]

Hence, by Corollary [5,4]

\[ Z_{t,r}(N,0) = Z_{q,r}(N,0) + \left(\frac{q}{t} - 1\right)Z_{q,r}(N,c_q) \]

\[ = Z_{q,r}(N,0) + \left(\frac{q}{t} - 1\right)\left(\frac{r-1}{N}\phi(N) - Z_{q,r}(N,0)\right) \]

\[ = \left(q - \frac{q}{t}\right)Z_{q,r}(N,0) + \left(\frac{q}{t} - 1\right)\frac{r-1}{N}\phi(N). \]

\[ \square \]

### 6. Connection to \( P_{q,r}(N, c) \)

In this section we briefly explore the seemingly related number, \( P_{q,r}(N, c) \), of elements in \( \mathbb{F}_r^* \) with order \( N \) and with prescribed trace \( c \). We start off by deriving a formula for the number of elements with order \( N \) in an arbitrary subset \( A \) of \( \mathbb{F}_r^* \) and apply this to obtain a formula for \( P_{q,r}(N, c) \) (see Lemma [6,1]). Let \( L_Q \) be the largest divisor of \( r-1 \) with the same radical as that of \( Q \). In the special case of the zero trace and the case when \( L_Q \mid N \), we show in Lemma [6,3] the simple relation \( Z_{q,r}(N,0) = \frac{r-1}{N}P_{q,r}(N,0) \). Then from this and Theorem [1,4] we give in Theorem [6,4] the number of elements of order \( 2(p+1)(p^2+1) \) with absolute trace zero in quartic extensions of Mersenne prime fields \( \mathbb{F}_p \).

For a subset \( A \subseteq \mathbb{F}_r^* \) and a divisor \( N \) of \( r-1 \), denote with \( M_r(N,A) \) the number of non-zero elements in \( A \) having multiplicative order \( N \) in \( \mathbb{F}_r^* \). In particular, \( M_r(r-1,A) \) denotes the number of primitive elements of \( \mathbb{F}_r^* \) that are contained in \( A \).

**Lemma 6.1.** Let \( q \) be a prime power, let \( r \) be a power of \( q \), let \( A \) be a subset of \( \mathbb{F}_r^* \), and let \( N \) be a positive divisor of \( r-1 \). Then the number of elements in \( A \) that have multiplicative order \( N \) is given by

\[ M_r(N,A) = \frac{1}{r-1} \sum_{d|N} \mu(d) \frac{N}{d} \left| \left\{ x \in \mathbb{F}_r^* : x^{\frac{r-1}{d}} \in A \right\} \right|. \]
In particular, for \( c \in \mathbb{F}_q \), the number of elements \( \beta \in \mathbb{F}_r^* \) with order \( N \) and satisfying \( \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(\beta) = c \), is given by

\[
P_{q,r}(N, c) = \frac{N}{q(r-1)} \sum_{d|N} \frac{\mu(d)}{d} \sum_{a \in \mathbb{F}_q} \chi_q(ac) \sum_{x \in \mathbb{F}_r^*} \chi_r \left( ax \frac{r-1}{d} \right).
\]

\[
= \frac{1}{q} \left( \phi(N) + \sum_{i=0}^{q-2} \chi_q(\alpha^{Qi}) \sum_{d|N} \mu(d) \eta_{Qi} \left( \frac{r-1}{d} \right) \right).
\]

**Proof.** If we define the arithmetic function \( f(n) := \sum_{d|n} M_r(d, A) \), then by the Moebius Inversion Formula,

\[
M_r(N, A) = \sum_{d|N} \mu(d) f(N/d) = \sum_{d|N} \mu(d) \sum_{b|N/d} M_r(b, A).
\]

Since \( f(N/d) \) represents the amount of elements in \( A \) with orders that are divisors of \( N/d \), and each such element can be written uniquely as \( \alpha \frac{r-1}{d} \) for \( 0 \leq i < N/d \), then

\[
\sum_{b|N/d} M_r(b, A) = \left| \left\{ 0 \leq i < N/d : \alpha \frac{r-1}{d} \in A \right\} \right|
\]

\[
= \frac{N}{d(r-1)} \left| \left\{ x \in \mathbb{F}_r^* : x \frac{r-1}{N} \in A \right\} \right|.
\]

With regards to \( P_{q,r}(N, c) \), observe that if we let \( A_c := \{ x \in \mathbb{F}_r^* : \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(x) = c \} \), then \( P_{q,r}(N, c) = M_r(N, A_c) \). Now it remains to obtain the expression for \( |\{ x \in \mathbb{F}_r^* : \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(x \frac{r-1}{N}) = c \}| \) \( = |\{ x \in \mathbb{F}_r^* : \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(x \frac{r-1}{N}) = c \}| \), which can be done by applying (1). Indeed, by (1) and by the transitivity of the trace function,

\[
\left| \left\{ x \in \mathbb{F}_r^* : \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(x \frac{r-1}{N}) = c \right\} \right| = \sum_{x \in \mathbb{F}_r^*} \frac{1}{q} \sum_{a \in \mathbb{F}_q} \chi_q \left( \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(a x \frac{r-1}{N}) - c \right)
\]

\[
= \frac{1}{q} \sum_{a \in \mathbb{F}_q} \chi_q(ac) \sum_{x \in \mathbb{F}_r^*} \chi_r \left( \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(a x \frac{r-1}{N}) \right)
\]

\[
= \frac{1}{q} \sum_{a \in \mathbb{F}_q} \chi_q(ac) \sum_{x \in \mathbb{F}_r^*} \chi_r \left( ax \frac{r-1}{N} \right).
\]

Result follows. \( \square \)

For \( k \in \mathbb{Z} \) and \( N | r - 1 \), denote

\[
\Gamma_k(N) = \sum_{d|N} \mu(d) \eta_k \left( \frac{r-1}{d} \right).
\]

For \( \beta \in \mathbb{F}_r \), let \( W_H(N, \beta) \) denote the Hamming weight of the \( n \)-tuple, where \( n = (r - 1)/N \), given by

\[
c(N, \beta) := (\text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(\beta), \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(\beta \alpha^N), \ldots, \text{Tr}_{\mathbb{F}_r/\mathbb{F}_q}(\beta \alpha^{(n-1)N}))
\]

For an integer \( t \neq 0 \), let \( \omega(t) \) be the number of distinct prime divisors of \( t \).
The following proposition gives some general identities relating $Z_{q,r}(N, c)$, $P_{q,r}(N, c)$, through the Moebius inversion formula, as well as shows their connection to Hamming weights.

**Proposition 6.2.** Let $r$ be a power of a prime, let $N \mid r - 1$ and let $k \in \mathbb{Z}$. Then the following identities hold:

$$
\sum_{d \mid \text{Rad}(N)} \mu(d) \Delta_k \left( \frac{\text{Rad}(N)}{d} \right) = (-1)^{\omega(N)} \eta_k^{(\text{Rad}(N), r)}; \\
\sum_{d \mid N} \Gamma_k(d) = \eta_k^{(\frac{r - 1}{N}, r)}; \\
\sum_{d \mid \text{Rad}(N)} \mu(d) \Delta_k \left( \frac{\text{Rad}(N)}{d} \right) = (-1)^{\omega(N)} \sum_{d \mid \text{Rad}(N)} \Gamma_k(d); \\
(-1)^{\omega(N)} \sum_{d \mid \text{Rad}(N)} \mu(d) f_0 \left( \frac{\text{Rad}(N)}{d}, \Delta, c \right) = q \sum_{d \mid \text{Rad}(N)} P_{q,r}(d, c) - \frac{r - 1}{\text{Rad}(N)}; \\
f_0(N, \Delta, c) = q \sum_{d \mid N} \mu(d) \sum_{b \mid \left( \frac{r - 1}{d} \right)} P_{q,r}(b, c) - \frac{r - 1}{N} \phi(N); \\
Z_{q,r}(N, c) = \sum_{d \mid N} \mu(d) \sum_{b \mid \left( \frac{r - 1}{d} \right)} P_{q,r}(b, c) \\
Z_{q,r}(N, 0) = \frac{r - 1}{N} \phi(N) - \sum_{d \mid N} \mu(d) W_H(d, 1).
$$

**Proof.** The first six identities use the Moebius inversion formula together with Lemma 3.4 and Lemma 6.1. The last identity follows from the one before it. Indeed, noting that

$$
W_H(d, 1) = \sum_{c \in \mathbb{F}_q^* b \left( \frac{r - 1}{d} \right)} P_{q,r}(b, c),
$$

we get

$$
\frac{r - 1}{N} \phi(N) - Z_{q,r}(N, 0) = \sum_{c \in \mathbb{F}_q^*} Z_{q,r}(N, c) = \sum_{d \mid N} \mu(d) \sum_{c \in \mathbb{F}_q^* b \left( \frac{r - 1}{d} \right)} P_{q,r}(b, c) \\
= \sum_{d \mid N} \mu(d) W_H(d, 1).
$$

□

But as the following shows, we can obtain a much simpler relation among $Z_{q,r}(N, 0)$ and $P_{q,r}(N, 0)$ in the special case when $L_Q \mid N$. 
Lemma 6.3. Let $D$ be the smallest positive divisor of $q - 1$ such that $(q - 1)/D$ is coprime to $Q$, and let $N | r - 1$ such that $DQ | N$. Then $Z_{q,r}(N,0)$ is related to $P_{q,r}(N,0)$ by the equation

$$Z_{q,r}(N,0) = \frac{r - 1}{N} P_{q,r}(N,0).$$

In particular we have the following relation:

$$P_{q,r}(r - 1, 0) = \frac{\phi(r - 1)}{\phi(DQ)} P_{q,r}(DQ, 0).$$

Proof. First note that since $N$ is a multiple of $DQ$, then $(r - 1)/N$ divides $(q - 1)/D$ and hence is coprime to $Q$. Let $g(N) = \gcd(Q, N)$ and let $K$ be the largest divisor of $N$ that is coprime to $Q$. Then similarly as done in the proof of Lemma 4.1, we have, by Lemma 2.2,

$$
\sum_{d|N} \mu(d) \sum_{i=0}^{q-2} \eta_{qi}^{(q-1)/d,r} = \sum_{b|K} \mu(b) \sum_{d|g(N)} \mu(d) \frac{(q - 1)d}{r - 1} \sum_{i=0}^{q-2} \eta_{qi}^{(q-1)/bd,r} = \sum_{b|K} \mu(b) \sum_{d|g(N)} \mu(d) \frac{(q - 1)d}{r - 1} \eta_0^{(q-1)/bd,r}
$$

$$= \frac{N}{Q} \sum_{b|K} \mu(b) \Delta_0(g(N)) = \frac{N\phi(K)}{QK} \Delta_0(g(N)).$$

Then by Lemma 6.1 and using the fact that $\frac{\phi(N)}{N} = \frac{\phi(K)}{K} \frac{\phi(g(N))}{g(N)}$, we get

$$P_{q,r}(N, 0) = \frac{N}{qQ} \left( Q \frac{\phi(N)}{N} \phi(g(N)) + \frac{\phi(K)}{K} \Delta_0(g(N)) \right)
$$

$$= \frac{N\phi(K)}{qQK} \left( \frac{Q}{g(N)} \phi(g(N)) + \Delta_0(g(N)) \right).$$

Now the first identity follows from Lemma 1.6.

For the second, Lemma 4.2 and the first identity gives

$$\frac{(q - 1)/D}{\phi((q - 1)/D)} P_{q,r}(r - 1, 0) = Z_{q,r}(Q, 0) = Z_{q,r}(DQ, 0) = \frac{q - 1}{D} P_{q,r}(DQ, 0).$$

Hence we obtain

$$P_{q,r}(r - 1, 0) = \phi \left( \frac{q - 1}{D} \right) P_{q,r}(DQ, 0).$$

Now the result follows by noticing that, since $DQ$ is coprime to $(q - 1)/D$, then

$$\phi(r - 1) = \phi \left( DQ \frac{q - 1}{D} \right) = \phi(DQ) \phi \left( \frac{q - 1}{D} \right).$$

Note that $L_Q := DQ$ is the largest divisor of $r - 1$ with the same radical as that of $Q$. Moreover whenever $P_{q,r}(r - 1, 0) \neq 0$, the ratio, of the number primitive elements with zero trace, to the number of elements of order $L_Q$ with trace zero, is the same as that of the number of primitive elements to the number of elements of order $L_Q$.

We apply Lemma 6.3 together with Theorem 1.4 to obtain the following consequence.
Theorem 6.4. Let $p$ be a Mersenne prime and let $Q = (p^4 - 1)/(p - 1) = (p + 1)(p^2 + 1)$. Then the number of non-zero elements in $\mathbb{F}_p^*$ with order $2Q$ and absolute trace zero is $\phi(2Q)/(p+1) = 2\phi(p^2+1)$.

Proof. In this case $Q = (p + 1)(p^2 + 1)$ and so the only prime diving both $p - 1$ and $Q$ is 2. Since 2 has multiplicity 1 in the factorization of $p - 1$, it follows that $D = 2$, where $D$ is as defined in Lemma 6.3. Then by Lemma 6.3 and Theorem 1.4 we get

$$P_{q,r}(2Q, 0) = \frac{\phi(2Q) \left( \phi(p^4 - 1) - \phi \left( \frac{p^4 - 1}{p+1} \right) \right)}{p\phi(p^4 - 1)} = \frac{\phi(2Q)}{p} \phi \left( \frac{p^4 - 1}{p+1} \right).$$

By Euler’s product formula for $\phi$ and using the fact that $2 \mid p - 1$ while $p + 1$ is a power of 2, note that

$$(p + 1)\phi ((p - 1)(p^2 + 1)) = (p + 1)(p - 1)(p^2 + 1) \prod_{l \mid (p - 1)(p^2 + 1)} \left( 1 - \frac{1}{l} \right)$$

$$= (p + 1)(p - 1)(p^2 + 1) \prod_{l \mid (p + 1)(p - 1)(p^2 + 1)} \left( 1 - \frac{1}{l} \right)$$

$$= \phi(p^4 - 1).$$

Now from the fact that $(p^4 - 1)/(p + 1) = (p - 1)(p^2 + 1)$, the above yields

$$P_{q,r}(2Q, 0) = \frac{\phi(2Q)}{p} - \frac{\phi(2Q)}{p(p + 1)} = \frac{\phi(2Q)}{p + 1}.$$ 

Remains to note that, since $p$ is a Mersenne prime,

$$\frac{\phi(2Q)}{p + 1} = 2(p^2 + 1) \prod_{l \mid p^2 + 1} \left( 1 - \frac{1}{l} \right) = 2\phi(p^2 + 1).$$

\[\square\]

7. Conclusion

In this paper we gave a very simple formula for the number of primitive elements in quartic extensions of Mersenne prime fields, having absolute trace zero. In contrast to the case of the irreducible polynomials, no such formulas were known, up to now, in any specific non-trivial case of the primitives. In addition, using the known explicit expressions for Gaussian periods in the semi-primitive case as well as the results on uniformity in Section 5, we obtained in Theorem 1.5 and 1.10 an explicit formula for the number of $N$-free elements with prescribed trace. We also derived in Section 6 an expression, in terms of Gaussian periods, for the number of elements with order $N$ having a prescribed trace. Here we managed to derive an explicit
formula, in Theorem 6.4, for the number of elements in $\mathbb{F}_{p^4}$ with absolute trace zero and high order $2(p + 1)(p^2 + 1)$, where $p$ is a Mersenne prime.

Previously Cohen [4] proved that, except for a small number of trivial exceptions, there exists a primitive element with any prescribed trace. That is, he showed that for all $c \in \mathbb{F}_q^*$, $P_{q,q^m}(q^m - 1, c) > 0$, while, if $m \neq 2$ and $(q, m) \neq (4, 3)$, then $P_{q,q^m}(q^m - 1, 0) > 0$. One can see this as a classification of all the pairs $(q, m)$ such that there exists an element of order $q^m - 1$ in $\mathbb{F}_{q^m}$ with any prescribed trace. One could also consider the following more general problem:

1. Classify all the triples $(q, m, N)$ such that there exists an element with order $q^m - 1$ in $\mathbb{F}_{q^m}$ having any prescribed trace.

Additionally, the reader might be interested in the following related problems:

2. Find more classes of triples $(q, m, c)$ for which explicit formulas may be obtained for $Z_{q,q^m}(q^m - 1, c)$, say in the style of Theorem 1.4.

3. Classify all triples $(q, m, N)$ such that $P_{q,q^m}(N, c \neq 0)$ behaves uniformly. One could also consider specifically the case when $N = q^m - 1$.

4. Classify all triples $(q, m, N)$ such that $Z_{q,q^m}(N, c \neq 0)$ behaves uniformly as in Theorem 1.9.

5. Find tight bounds for $Z_{q,r}(N, c)$ and $P_{q,r}(N, c)$. In particular, in the case of $c = 0$, find tight bounds for the sum $\Delta_0(n)$, where $n$ divides $Q$.

APPENDIX A.

The following table gives the amounts of primitive elements in the quartic extensions of Mersenne prime fields having absolute trace zero, for the first ten Mersenne primes. See Theorem 1.4. SAGE software was used for the computations.

| Mersenne prime, $p$ | $Z_{p,p^4}(p^4 - 1, 0)$ |
|---------------------|-------------------------|
| $2^2 - 1$           | 8                       |
| $2^3 - 1$           | 80                      |
| $2^5 - 1$           | 6,912                   |
| $2^7 - 1$           | 464,256                 |
| $2^{13} - 1$        | 111,974,400,000         |
| $2^{17} - 1$        | 519,390,596,431,872     |
| $2^{19} - 1$        | 30,572,599,504,748,544  |
| $2^{31} - 1$        | 1,968,482,608,781,191,263,129,600,000 |
| $2^{61} - 1$        | 2,159,465,982,279,294,537,199,679,191,374,585,254,935,265,280,000,000,000 |
| $2^{89} - 1$        | 51,505,739,520,752,637,174,787,391,794,396,705,748,179,291,647,742,969,497,437,393,928,825,245,616,046,080 |
ON THE NUMBER OF N-FREE ELEMENTS WITH PRESCRIBED TRACE

REFERENCES

[1] E. Bach, J. Shallit, Algorithmic number theory, Vol. 1. Foundations of Computing Series. MIT Press, Cambridge, MA, 1996. Efficient algorithms.

[2] R.P. Brent, P. Zimmermann, The great trinomial hunt, Notices Amer. Math. Soc. 58 (2011), no. 2, 233–239.

[3] L. Carlitz, A theorem of Dickson on irreducible polynomials, Proc. Amer. Math. Soc. 3 (1952), 693–700.

[4] S.D. Cohen, Primitive elements and polynomials with arbitrary trace, Discrete Math. 83 (1990), no. 1, 1–7.

[5] S.D. Cohen, Explicit theorems on generator polynomials, Finite Fields Appl. 11, no. 3 (2005), 337–357.

[6] S.D. Cohen, M. Prešern, Primitive finite field elements with prescribed trace, Southeast Asian Bull. Math. 29 (2005), no. 2, 283–300.

[7] S.D. Cohen, M. Prešern, The Hansen-Mullen primitive conjecture: completion of proof, Number theory and polynomials, 89–120, London Math. Soc. Lecture Note Ser., 352, Cambridge Univ. Press, Cambridge, 2008.

[8] C. Ding, J. Yang, Hamming weights in irreducible cyclic codes, Discrete Math. 313 (2013), no. 4, 434–446.

[9] K.H. Ham, G.L. Mullen, Distribution of irreducible polynomials of small degrees over finite fields, Math. Comp. 67 (221) (1998) 337341.

[10] T. Hansen, G.L. Mullen, Primitive polynomials over finite fields, Math. Comput. 59 (1992) 639–643, S47S50.

[11] B. Koma, D. Panario, Q. Wang, The number of irreducible polynomials of degree n over $\mathbb{F}_q$ with given trace and constant terms, Discrete Mathematics, 310 (2010), 1282–1292.

[12] E. N. Kuzmin, On irreducible polynomials over a finite field (Russian) Sibirsk. Mat. Zh. 30 (1989), no. 6, 98–109; translation in Siberian Math. J.

[13] E. N. Kuzmin, A class of irreducible polynomials over a finite field, (Russian) Dokl. Akad. Nauk SSSR 313 (1990), no. 3, 552555; translation in Soviet Math. Dokl. 42 (1991), no. 1, 45–48.

[14] R. Lidl, H. Niederreiter, Finite fields, Cambridge University Press, Cambridge, (1997).

[15] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan’s conjecture, J. Reine Angew. Math. 572 (2004), 167–195.

[16] G.L. Mullen and D. Panario, Handbook of finite fields, CRC Press, 2013.

[17] P. Ribenboim, The New Book of Prime Number Records, 3rd ed., Springer-Verlag, New York, 1995.

[18] D. Wan, Generators and irreducible polynomials over finite fields, Math. Comp. 66 (219) (1997) 1195–1212.

[19] J.L. Yucas, Irreducible polynomials over finite fields with prescribed trace/prescribed constant term, Finite Fields Appl. 12 (2006), no. 2, 21–221.

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6, Canada.

E-mail address: AleksandrTuxanidyTor@mail.carleton.ca, wang@math.carleton.ca