Zeta functions of quadratic Artin-Schreier curves in characteristic two

Régis Blache, Timothé Pierre

ZETA FUNCTIONS OF QUADRATIC ARTIN-SCHREIER CURVES IN CHARACTERISTIC TWO

RÉGIS BLACHE AND TIMOTHÉ PIERRE

ABSTRACT. The aim of this paper is twofold: on one hand we study the invariants of traces of quadratic forms over a finite field of characteristic two. On the other hand, we give results about the zeta functions of certain curves studied by van der Geer and ven der Vlugt.

1. INTRODUCTION

We denote by $\mathbf{F}_{2^m}$ a finite field of characteristic 2, and by

$$R := \sum_{i=0}^{d} a_i x^{2^i} \in \mathbf{F}_{2^m}[x], a_d \neq 0$$

a 2-linearized (or additive) polynomial. We also set $f(x) = xR(x)$.

The family of (non singular, projective) Artin-Schreier curves having an affine equation of the form

$$C_R \ : \ y^2 + y = xR(x)$$

is our main object of study. It was introduced in [12]. These curves have beautiful properties, such as being supersingular, or having a large group of automorphisms. Moreover, many examples of maximal curves are of this form [2]. Finally, they also have been used in [13] to construct supersingular curves of any genus over a finite field of characteristic two. We call these curves *quadratic* Artin-Schreier curves.

Their study also has numerous applications to information theory: in coding theory their numbers of rational points give the weight enumerators of some Reed-Muler codes, and they can also be used to construct certain binary sequences.

Here we shall concentrate on their zeta functions. Recall that if $\#C_R(\mathbf{F}_{2^{mn}})$ denotes the number of rational points of the curve C_R over the degree n extension of the base field, its zeta function is defined by

$$Z(C_R, T) = \exp\left(\sum_{n\geq 1} \#C_R(\mathbf{F}_{2^{mn}})\frac{T^n}{n}\right)$$

This is a rational function from Weil(s proof of the Riemann hypothesis for curves; more precisely, its denominator is $(1-T)(1-2^mT)$, and its numerator $L(C_R, T)$, called the L-function of the curve, is a polynomial of degree $2g = 2^d$, where g denotes the genus of the curve C_R.

On the other hand, we consider for any $n \geq 1$ the sum and the L-function

$$S_n(f) := \sum_{x\in\mathbf{F}_{2^{mn}}} (-1)^{\mathrm{Tr}_{\mathbf{F}_{2^{mn}}/\mathbf{F}_2}\circ f(x)}, \ L(f,T) := \exp\left(\sum_{n\geq 1} S_n(f)\frac{T^n}{n}\right)$$

Date: December 3, 2021.

2010 *Mathematics Subject Classification.* 11G20, 14H05.

Key words and phrases. Zeta functions of curves, quadratic forms and exponential sums over finite fields.

It is well-known that we have $\#C(\mathbf{F}_{2^{mn}}) = 1+2^{mn}+S_n(f)$, which gives the equality

$$L(C_R, T) = L(f, T)$$

and the link between the two objects.

Since the function $x \mapsto \mathrm{Tr}_{\mathbf{F}_{2^{mn}}/\mathbf{F}_2} \circ f(x)$ is a quadratic form over the $\mathbf{F}_2$-vector space $\mathbf{F}_{2^{mn}}$, the exponential sum $S_n(f)$ is determined by the isometry class of this form, i.e. by the dimension of the radical of the associated bilinear form, and an invariant $\varepsilon_n(f)$. The radical depends on the solutions of the so-called kernel equation, and is in principle easy to compute once we know the decomposition field of this equation. The invariant $\varepsilon_n(f)$ is finer, and there have been many attempts to compute it in general (see for instance [5]) or in particular cases (see [3] for binomials in $\mathbf{F}_2[x]$ or [10] for forms with a big radical).

Here we show that all the invariants $\varepsilon_n(f)$ depend on the finite number of those $\varepsilon_d(f)$ for which d divides (twice) the degree of the decomposition field of the kernel polynomial.

As a consequence, we give a factorization of the L-function $L(f, T)$: the factors are almost cyclotomic polynomials, and we express their multiplicities from the above data, namely the dimensions of the radicals, and the invariants. This improves on [12, Theorems 10.1 and 10.2] where the zeta function is determined only over some particular base fields.

Let us describe our methods in a few words. Whereas the proofs in [12] are mostly geometric, we reason here in a much more arithmetic (and elementary) way.

The first observation, Proposition 3.6, is well-known (see [9] for instance). Since the curves are supersingular, the reciprocal roots of the L-function are almost roots of unity, and its factors are almost cyclotomic polynomials. If we define the period as the least common multiple of the orders of these roots of unity, then there must be some periodicity in the number of points from the very definition of the zeta function.

The second observation is Proposition 3.8. Since we have rather explicit evaluations of the exponential sums associated to quadratic functions, we can determine the period from the knowledge of at most two values of the invariant.

Once we have observed these two facts, the results follow in a completely elementary way from the properties of some well known arithmetic functions.

The paper is organized as follows. In section 2, we recall (and prove when necessary) some technical results that we use later in the paper. Then in Section 3, we determine the period from the degree of the decomposition field of the kernel polynomial and some invariants. In Section 4 and 5, we give the main results, respectively in the cases of even and odd m: we give the relations between the invariants, determine them in some cases, and express the multiplicities of the cyclotomic factors. Finally, we treat an example associated to the Suzuki curve in the last Section, in order to illustrate the preceding results.

2. Preliminaries

2.1. **Factorization of cyclotomic polynomials.** We first need to determine the factorization of cyclotomic polynomials over the field $\mathbf{Q}(\sqrt{2})$.

For any $n \geq 1$, we set $\zeta_n := e^{\frac{2i\pi}{n}}$.

Since we have $\sqrt{2} = \zeta_8 + \zeta_8^7$, the field $\mathbf{Q}(\sqrt{2})$ is the subfield of $\mathbf{Q}(\zeta_8)$ fixed by the Galois automorphism defined by $\zeta_8 \mapsto \zeta_8^7$. From this observation, we deduce that for $v_2(\ell) < 3$, the fields $\mathbf{Q}(\zeta_\ell)$ and $\mathbf{Q}(\sqrt{2})$ are linearly disjoint, and the polynomial $\Phi_\ell(T)$ remains irreducible over $\mathbf{Q}(\sqrt{2})$.

If we have $v_2(\ell) \geq 3$, then $\mathbf{Q}(\sqrt{2})$ is the subfield of $\mathbf{Q}(\zeta_\ell)$ fixed by the subgroup H of $\mathrm{Gal}(\mathbf{Q}(\zeta_\ell)/\mathbf{Q})$ corresponding to

$$\left\{k \in (\mathbf{Z}/\ell\mathbf{Z})^\times,\ k \equiv \pm 1 \mod 8\right\}$$

This is the kernel of the following character

Definition 2.1. We denote by χ the Dirichlet character of modulus 8 defined by $\chi(3) = \chi(5) = -1$.

The action of the group H on the set of primitive ℓ-th roots of unity has two orbits, namely

$$\mu_\ell^{\times +} = \{\zeta_\ell^i,\ 0 \leq i \leq \ell - 1,\ \chi(i) = 1\},\ \mu_\ell^{\times -} = \{\zeta_\ell^i,\ 0 \leq i \leq \ell - 1,\ \chi(i) = -1\}$$

As a consequence, the factorization of Φ_ℓ over $\mathbf{Q}(\sqrt{2})$ is

$$\Phi_\ell(T) = \Phi_\ell^+(T)\Phi_\ell^-(T),\ \Phi_\ell^\pm(T) := \prod_{i,\ \chi(i)=\pm 1} (1 - \zeta_\ell^i T) = \prod_{\zeta \in \mu_\ell^{\times \pm}} (1 - \zeta T)$$

2.2. **Evaluation of certains sums of roots of unity.** We introduce two families of sums of roots of unity

Definition 2.2. First, the *Ramanujan sums* [11]: for any $\ell, n \geq 1$

$$c_\ell(n) := \sum_{i \in (\mathbf{Z}/\ell\mathbf{Z})^\times} \zeta_\ell^{ni}$$

Second, for any ℓ multiple of 8 and n the sums

$$\sigma_\ell(n) := \sum_{i \in (\mathbf{Z}/\ell\mathbf{Z})^\times} \chi(i)\zeta_\ell^{ni}$$

If φ denotes Euler's totient, and μ the Möbius function, the Ramanujan sums have the following well known expression, called the von Sterneck arithmetic function

$$c_\ell(n) = \mu\left(\frac{\ell}{\gcd(\ell, n)}\right) \frac{\varphi(\ell)}{\varphi\left(\frac{\ell}{\gcd(\ell,n)}\right)} \tag{2.1}$$

For the second family of sums, we have the following

Lemma 2.3. *Write $\ell = 2^k\ell'$, $k = v_2(\ell) \geq 3$; then we have*

$$\sigma_\ell(n) = \begin{cases} \chi(\ell' n')2^{k-2}\sqrt{2}c_{\ell'}(n') & \text{if} \quad n = 2^{k-3}n',\ n' \text{odd} \\ 0 & \text{if} \quad v_2(n) \neq v_2(\ell) - 3 \end{cases}$$

Proof. We first write Bezout identity $2^k u + \ell' v = 1$; from the Chinese remainder theorem, we deduce that can rewrite the sum (recall that χ is defined modulo 8)

$$\begin{aligned} \sigma_\ell(n) &= \sum_{a \in (\mathbf{Z}/2^k\mathbf{Z})^\times} \sum_{b \in (\mathbf{Z}/\ell'\mathbf{Z})^\times} \chi(2^k ub + \ell' va)\zeta_\ell^{n(2^k ub + \ell' va)} \\ &= \chi(\ell') \sum_{a \in (\mathbf{Z}/2^k\mathbf{Z})^\times} \chi(va)\zeta_{2^k}^{nva} \sum_{b \in (\mathbf{Z}/\ell'\mathbf{Z})^\times} \zeta_{\ell'}^{nub} \\ &= \chi(\ell') \sum_{a \in (\mathbf{Z}/2^k\mathbf{Z})^\times} \chi(a)\zeta_{2^k}^{na} \sum_{b \in (\mathbf{Z}/\ell'\mathbf{Z})^\times} \zeta_{\ell'}^{nub} \end{aligned}$$

We recognize that the last sum is the Ramanujan sum $c_{\ell'}(nu) = c_{\ell'}(n)$.

If we write $n = 2^t n'$, with n odd, we get that the sum over $(\mathbf{Z}/2^k\mathbf{Z})^\times$ is equal to

(a) $\sum_{a \in (\mathbf{Z}/2^k\mathbf{Z})^\times} \chi(a) = 0$ if $t \geq k$;
(b) $-\sum_{a \in (\mathbf{Z}/2^k\mathbf{Z})^\times} \chi(a) = 0$ if $t = k - 1$;

(c) $\sum_{a\in(\mathbf{Z}/2^k\mathbf{Z})^\times}\chi(a)i^{n'a}=0$ if $t=k-2$.

If $t\leq k-3$, we set $a=a_0+8a_1$, $a_0\in(\mathbf{Z}/8\mathbf{Z})^\times$, $a_1\in\mathbf{Z}/2^{k-3}\mathbf{Z}$; then

$$\sum_{a\in(\mathbf{Z}/2^k\mathbf{Z})^\times}\chi(a)\zeta_{2^k}^{na}=\sum_{a_0}\chi(a_0)\zeta_{2^{k-t}}^{n'a_0}\sum_{a_1}\zeta_{2^{k-t-3}}^{n'a_1}$$

The last sum is zero, unless we have $t=k-3$ and then it is equal to 2^{k-3}. The sum over a_0 is equal to $\chi(n')2\sqrt{2}$, and this gives the result. □

2.3. **Some matrices whose entries are arithmetic functions.** We introduce here two sequences of matrices for future use

Definition 2.4. For any integer $n\geq 1$, we set

$$A(n):=(c_\ell(d))_{d,\ell|n},\ B(n):=(\sigma_\ell(d))_{d,\ell|n}$$

The matrix $A(n)$ is invertible: in order to see this, it is sufficient to slightly modify the argument in the proof of [1, Theorem 9] to verify that its determinant is the product of the divisors of n.

Set $n=2^an'$, with n' odd. Then we can write the matrix $A(n)$ in the following block form

$$A(n)=(A(n)_{ij})_{0\leq i,j\leq a},\ A(n)_{ij}:=(c_\ell(d))_{d,\ell|N,\ v_2(d)=i,\ v_2(\ell)=j}$$

Using von Sterneck arithmetic function, we have

$$A_{ij}(n)=\begin{cases}0 & \text{if} \quad i\leq j-2\\ -2^iA(n') & \text{if} \quad i=j-1\\ A(n') & \text{if} \quad j=0\\ 2^{j-1}A(n') & \text{if} \quad i\geq j\geq 1\end{cases}\tag{2.2}$$

We turn our attention to the matrix $B(n)$. We introduce a diagonal matrix

Definition 2.5. Let n' denote an odd integer. The matrix $\Delta(n')$ is the diagonal matrix whose coefficients are the $\chi(\ell)$, $\ell|n'$.

We can write it in block form as above, with blocks $B_{ij}(n)$. From the expression in Lemma 2.3, we see that all blocks are zero, except the blocks $B(n)_{ii+3}$ and that

$$B(n)_{ii+3}=2^{i-2}\sqrt{2}\Delta(n')A(n')\Delta(n')\tag{2.3}$$

2.4. **Quadratic forms over a finite field of characteristic two.** We recall the classification, up to isometry, of quadratic forms over a finite dimensional $\mathbf{F}_2$-vector space.

Let $q:V\to\mathbf{F}_2$ denote a quadratic form over a $\mathbf{F}_2$-vector space V of dimension k. We associate to q a bilinear form, its polarisation, defined by $b(x,y)=q(x+y)+q(x)+q(y)$; then b is alternate, and it does not depend on the diagonal part of q. We no longer have a one to one correspondance between the quadratic forms and the bilinear forms over V.

We denote by $\operatorname{rad}b:=V^\perp$ the radical of b, and by c its dimension (which has the same parity as k). Then there exists a basis $(e_1,\dots,e_r,e_{r+1},\dots,e_k)$ of V, such that $(e_{r+1},\dots,e_k)$ is a basis of $\operatorname{rad}b$ and q can be written in (the dual basis of) this basis in one of the following ways [8, Theorem 6.30]

(i) $q(x)=x_1x_2+\cdots+x_{r-1}x_r+x_{r+1}^2$
(ii) $q(x)=x_1x_2+\cdots+x_{r-1}x_r$
(iii) $q(x)=x_1^2+x_1x_2+x_2^2+\cdots+x_{r-1}x_r$

Remark 2.6. Remark that the first case corresponds to the quadratic forms that are not trivial on the radical of their polarisation, and the last two to the forms having trivial restriction.

We now define the invariants that we shall study.

Definition 2.7. To each isometry class, we associate an invariant which is respectively $0, 1, -1$ in each of the cases (i), (ii) or (iii) and that we denote by $\varepsilon(q)$.

We have the following [8, Theorem 6.32]

Proposition 2.8. *The exponential sum associated to the quadratic form q satisfies*

$$\sum_{x\in V}(-1)^{q(x)} = \varepsilon(q)2^{\frac{k+c}{2}}$$

3. General results on the zeta functions

We fix once and for all a 2-linear polynomial of degree 2^d, $R := \sum_{i=0}^{d} a_i x^{2^i}$ in $\mathbf{F}_{2^m}[x]$, and we set $f(x) := xR(x)$.

We consider the non singular projective curve C_R defined over $\mathbf{F}_{2^m}$ by the affine equation $y^2 + y = f(x)$. This is an hyperelliptic curve (equivalently, an Artin-Schreier covering of the projective line, since the characteristic is two) with genus $g = 2^{d-1}$. Moreover it is supersingular [12, Theorem 9.4].

Since the point at infinity of the projective line is totally ramified in the covering, the number of rational points of this curve over the field $\mathbf{F}_{2^{mn}}$ is

$$\#C_R(\mathbf{F}_{2^{mn}}) = 1 + 2^{mn} + \sum_{x\in\mathbf{F}_{2^{mn}}}(-1)^{\mathrm{Tr}_{\mathbf{F}_{2^{mn}}/\mathbf{F}_2}\circ f(x)} = 1 + 2^{mn} + S_n(f)$$

and the numerator of the zeta function $Z(C_R, T)$ is the L-function $L(f, T)$.

In the following, we focus on this last function.

3.1. First properties of the quadratic forms.

Let us first define our main objects of study

Definition 3.1. For each integer $n \geq 1$, we denote by q_n the quadratic form $q_n := \mathrm{Tr}_{\mathbf{F}_{2^{mn}}/\mathbf{F}_2}\circ f$ from $\mathbf{F}_{2^{mn}}$ to $\mathbf{F}_2$. We denote by b_n its polarisation, and by $\mathrm{rad}(b_n)$ its radical.

We denote respectively by $c_n(f)$ and $\varepsilon_n(f)$ the codimension of the radical of b_n, and its invariant.

From Proposition 2.8, we have

$$S_n(f) = \varepsilon_n(f)2^{\frac{mn+c_n(f)}{2}}$$

These forms, and the associated sums, have already been studied in many papers; let us just cite [3, 5]. We extract some results from [5], that we reprove for completeness.

First about the radical $\mathrm{rad}(b_n)$. To the additive polynomial R, we associate another additive polynomial

Definition 3.2. The *kernel polynomial* associated to the family of quadratic forms (q_n) is the polynomial

$$\widetilde{R} := (R + R^*)^{2^d} = \sum_{i=0}^{d} a_i^{2^d} x^{2^{d+i}} + a_i^{2^{d-i}} x^{2^{d-i}}$$

where R^* is the adjoint of the polynomial R.

We denote by $\mathbf{F}_{2^{mN}}$ the decomposition field of $\widetilde{R}$ over $\mathbf{F}_{2^m}$, and by $\mathrm{Ker}\,\widetilde{R} \subset \mathbf{F}_{2^{mN}}$ the set of roots of this polynomial.

In the following, we set $N = 2^a N'$, with N' odd.

Fix an $n \geq 1$; for any $x, y \in \mathbf{F}_{2^{mn}}$, we have

$$b_n(x,y) = \mathrm{Tr}_{\mathbf{F}_{2^{mn}}/\mathbf{F}_2}(xR(y) + R(x)y) = \mathrm{Tr}_{\mathbf{F}_{2^{mn}}/\mathbf{F}_2}(x^{2^d}\widetilde{R}(y))$$

As a consequence, since the bilinear form $(x,y) \mapsto \mathrm{Tr}_{\mathbf{F}_{2^{mn}}/\mathbf{F}_2}(xy)$ is non degenerate, we have

$$\mathrm{rad}(b_n) = \mathrm{Ker}\,\widetilde{R} \cap \mathbf{F}_{2^{mn}}$$

Since the degree 1 coefficient of $\widetilde{R}$ is $a_d \neq 0$, this polynomial is separable, all its roots are simple, and we have $2^{c_n(f)} = \deg \gcd(\widetilde{R}, x^{2^{mn}} + x)$.

Note that $\widetilde{R}$ divides $x^{2^{mN}} + x$ and we have $c_N(f) = 2d$.

We begin with

Lemma 3.3. [5, Propositions 3.1 and 3.3] *Notations are as above*

1. *for any $n \geq 1$, we have $c_n(f) = c_{\gcd(n,N)}(f)$;*
2. *if moreover $v_2(n) > v_2(N)$, then $\varepsilon_n(f) \neq 0$.*

Proof. Let $n \geq 1$; then we have

$$\begin{aligned}
\gcd(\widetilde{R}, x^{2^{mn}} + x) &= \gcd(\gcd(\widetilde{R}, x^{2^{mN}} + x), x^{2^{mn}} + x)) \\
&= \gcd(\widetilde{R}, \gcd(x^{2^{mN}} + x, x^{2^{mn}} + x)) \\
&= \gcd(\widetilde{R}, x^{2^{m\gcd(n,N)}} + x)
\end{aligned}$$

From the equality $2^{c_n(f)} = \deg \gcd(\widetilde{R}, x^{2^{mn}} + x)$, we deduce the first assertion.

Assume that $v_2(n) > v_2(N)$; then we have $n = d\gcd(n,N)$ for some even d. We have seen that $\mathrm{rad}(b_n) = \mathrm{rad}(b_{\gcd(n,N)})$; if x lies in this subspace, $f(x)$ is in $\mathbf{F}_{2^{m\gcd(n,N)}}$, and

$$\begin{aligned}
q_n(x) &= \mathrm{Tr}_{\mathbf{F}_{2^{mn}}/\mathbf{F}_2}(f(x)) \\
&= \mathrm{Tr}_{\mathbf{F}_{2^{m\gcd(n,N)}}/\mathbf{F}_2}\left(\mathrm{Tr}_{\mathbf{F}_{2^{mn}}/\mathbf{F}_{2^{m\gcd(n,N)}}}(f(x))\right) \\
&= \mathrm{Tr}_{\mathbf{F}_{2^{m\gcd(n,N)}}/\mathbf{F}_2}(df(x)) = 0
\end{aligned}$$

We deduce that the restriction of q_n to $\mathrm{rad}(b_n)$ is trivial, and the second assertion from Remark 2.6.

□

3.2. **First properties of the L-function.** We shall study a new function, close to the L-function, but with simpler arithmetical properties

Definition 3.4. The modified L-function is

$$L^*(f,T) := L\left(f, \frac{T}{\sqrt{2}^m}\right)$$

Remark 3.5. In the same way as the L-function comes from the sums $(S_n(f))_{n\geq 1}$, the modified L-function comes from the modified sums

$$S_n^*(f) = (\sqrt{2})^{-mn} S_n(f) = \varepsilon_n(f) 2^{\frac{c_n(f)}{2}} = \varepsilon_n(f) 2^{\frac{c_{\gcd(n,N)}(f)}{2}} \tag{3.1}$$

from the first part of Lemma 3.3.

We list the first properties of this new function in the following

Proposition 3.6. *The function $L^*(f,T)$ satisfies*

(i) *it is a polynomial of degree 2^d, with coefficients in $\mathbf{Z}[\sqrt{2}]$;*
(ii) *its reciprocal roots are roots of unity.*
(iii) *if m is even, then it has integer coefficients.*

Proof. We only show assertion (ii): the other assertions follow readily from the fact that the L function $L(f,T)$ is a polynomial of degree 2^d with integer coefficients.

The reciprocal roots of the modified L-function are the $\beta_i = \alpha_i/\sqrt{2}^m$, $1 \leq i \leq 2^d$, where the α_i are the reciprocal roots of the function $L(f,T)$. For any odd prime ℓ, these numbers are ℓ-adic units from Weil's proof of the Riemann hypothesis over finite fields.

We consider their 2-adic valuations. Since the curve is supersingular, we have $v_2(\alpha_i) = m/2$ for all i, and we deduce that the β_i are 2-adic units. Thus all the β_i are algebraic integers.

Finally, since all conjugates of the β_i have complex module 1, a classical theorem of Kronecker [6] ensures that they are roots of unity. □

We borrow the following definition to [9]

Definition 3.7. The *period* D of the function $L(f,T)$ is the least common multiple of the orders of the reciprocal roots of the modified L function.

The period has a simple expression in the degree of the decomposition field of the polynomial $\widetilde{R}$

Proposition 3.8. *Recall that* $\mathbf{F}_{2^{mN}}$ *is the decomposition field of* $\widetilde{R}$ *over* $\mathbf{F}_{2^m}$*. Then the period satisfies* $D \in \{N, 2N, 4N\}$.

Precisely, we have the following cases

(i) *if* $\varepsilon_N(f) = -1$*, then* $D = N$*;*

(ii) *if* $\varepsilon_N(f) = 1$*, then* $\varepsilon_{2N}(f) = -1$*,* $D = 2N$*, and all roots orders have dyadic valuation* $v_2(N) + 1$*;*

(iii) *if* $\varepsilon_N(f) = 0$*, we have the following alternative*

  (iiia) *if* $\varepsilon_{2N}(f) = -1$*, then* $D = 2N$*;*

  (iiib) *if* $\varepsilon_{2N}(f) = 1$*, then* $D = 4N$*, and all roots orders have dyadic valuation* $v_2(N) + 2$.

Proof. If we compare the logarithmic derivatives of both sides of the equality

$$L^*(f,T) = \prod_{i=1}^{2^d} (1 - \beta_i T)$$

we see that for any $n \geq 1$ the modified sum can be written from the reciprocal roots of the modified L-function as

$$S_n^*(f) = -\sum_{i=1}^{2^d} \beta_i^n \tag{3.2}$$

From the expression (3.1) of the sum $S_n^*(f)$, and since we have $c_N(f) = 2d$ by definition of the decomposition field, we deduce

$$-\sum_{i=1}^{2^d} \beta_i^N = \varepsilon_N(f) 2^d$$

In the case $\varepsilon_N(f) = -1$, the triangle inequality ensures that $\beta_i^N = 1$ for all i. Thus D divides N. Since N is the least integer with $c_N(f) = 2d$, we get assertion (i).

When $\varepsilon_N(f) = 1$, we get $\beta_i^N = -1$ and $\beta_i^{2N} = 1$ for all i. Thus D divides $2N$, and the root orders all have dyadic valuation equal to $v_2(N) + 1$. Here again, N is the least integer such that $\left|\sum_{i=1}^{2^d} \beta_i^N\right| = 2^d$, and we have $D = 2N$.

In the case $\varepsilon_N(f) = 0$, we have $\varepsilon_{2N}(f) = \pm 1$ from Lemma 3.3 (ii). Then we conclude as above from the value of $\varepsilon_{2N}(f)$ since we have $c_{2N}(f) = 2d$. □

4. The case of even m

In this section, m is even.

In this case, the $\mathbf{F}_2$-vector space $\mathbf{F}_{2^{mn}}$ has even dimension for all n, and the corank $c_n(f)$ is even. Thus the modified L-function has integer coefficients; it is a product of cyclotomic polynomials from Proposition 3.6 (2), and we write

$$L^*(f,T) = \prod_\ell \Phi_\ell(T)^{m_\ell(f)} \tag{4.1}$$

As a consequence, (3.2) gives the following expression for the modified sums, where $c_\ell(n)$ is the Ramanujan sum from Definition 2.2

$$-S_n^*(f) = \sum_\ell m_\ell(f) c_\ell(n). \tag{4.2}$$

From Proposition 3.8, we deduce

Proposition 4.1. *Assume m is even. The invariants $\varepsilon_n(f)$, $n \geq 1$, satisfy*

(i) *if $\varepsilon_N(f) = -1$, then $\varepsilon_n(f) = \varepsilon_{\gcd(n,N)}(f)$;*
(ii) *when $\varepsilon_N(f) = 1$, we have*
  - *if $v_2(n) \leq v_2(N) - 1$, then $\varepsilon_n(f) = 0$;*
  - *if $v_2(n) = v_2(N)$, then $\varepsilon_n(f) = \varepsilon_{\gcd(n,N)}(f)$;*
  - *if $v_2(n) \geq v_2(N) + 1$, then $\varepsilon_n(f) = -\varepsilon_{\gcd(n,N)}(f)$;*

(iii) *when $\varepsilon_N(f) = 0$, we have the following cases*
(iiia) *if $\varepsilon_{2N}(f) = -1$, then $\varepsilon_n(f) = \varepsilon_{\gcd(n,2N)}(f)$ for all $n \geq 1$.*
(iiib) *if $\varepsilon_{2N}(f) = 1$, then*
  - *if $v_2(n) \leq v_2(N)$, then $\varepsilon_n(f) = 0$;*
  - *if $v_2(n) = v_2(N) + 1$, then $\varepsilon_n(f) = \varepsilon_{\gcd(n,2N)}(f)$;*
  - *if $v_2(n) \geq v_2(N) + 2$, then $\varepsilon_n(f) = -\varepsilon_{\gcd(n,2N)}(f)$;*

Proof. This is a consequence of proposition 3.8, equation (4.2) and of the von Sterneck expression for Ramanujan sums (2.1).

First, when ℓ divides D, we have $c_\ell(n) = c_\ell(\gcd(D,n))$, that ensures $\varepsilon_n(f) = \varepsilon_{\gcd(n,D)}(f)$ for all $n \geq 1$. This proves assertions (i) and (iiia).

In case (ii), we have $v_2(\ell) = v_2(N) + 1$ for any ℓ such that $m_\ell(f) \neq 0$ from Proposition 3.8 (ii). This implies the following equalities

- $c_\ell(n) = 0$ if $v_2(n) \leq v_2(N) - 1$,
- $c_\ell(n) = c_\ell(\gcd(n, 2N)) = c_\ell(\gcd(n, N))$ if $v_2(n) = v_2(N)$, and
- $c_\ell(n) = c_\ell(\gcd(n, 2N)) = c_\ell(2\gcd(n, N)) = -c_\ell(\gcd(n, N))$ else.

Case (iiib) is treated as case (ii), noting that $v_2(\ell) = v_2(N) + 2$ for all ℓ such that $m_\ell(f) \neq 0$. □

Remark 4.2. Let us denote by σ the number of divisors function, and set $N = 2^a N'$, with N' odd.

We deduce from the preceding result that the knowledge of the family $(S_n(f))_{n\geq 1}$ can be reduced to the knowledge of $\sigma(N)$ of these sums in case (i), $\sigma(2N)$ of these sums in case (iiia) and $\sigma(N')$ in the remaining cases.

These results are in the spirit of [9, Theorem 1].

We end this section with an expression for the multiplicities $m_\ell(f)$ in (4.1).

Proposition 4.3. *Assume m is even; recall that we have set $N = 2^a N'$, N' odd. The multiplicities $m_\ell(f)$ satisfy the following systems, depending on the case from the above Proposition*

(i) $A(N)(m_\ell(f))_{\ell|N} = (-S_d^*(f))_{d|N}$;
(ii) $2^a A(N')(m_{2^{a+1}\ell}(f))_{\ell|N'} = (S_{2^a d}^*(f))_{d|N'}$;
(iiia) $A(2N)(m_\ell(f))_{\ell|2N} = (-S_d^*(f))_{d|2N}$;

(iiib) $2^{a+1}A(N')(m_{2^{a+2}\ell}(f))_{\ell|N'} = (S^*_{2^{a+1}d}(f))_{d|N'}$

Proof. We start with the system consisting of the equations (4.2) for $n \geq 1$.

In case (i) (*resp.* (iiia)) of the preceding proposition, this system is equivalent to the system consisting of the same equations, when n runs over the divisors of N (*resp.* $2N$). Now the corresponding assertions are just the matrix forms of this last system.

In case (ii), we first reduce to the system consisting of the same equations, when n runs over the divisors of N. Then we use the block form of the matrix A. Since the only non zero multiplicities are the ones with $v_2(\ell) = a+1$, and the only non zero sums $S^*_n(f)$ are those with $v_2(n) = a$, the block corresponding to the remaining part of the system is A_{aa+1}, and we get the result from its description (2.2).

Case (iiib) is proven the same way, replacing a by $a+1$. □

5. The case of odd m

We first remark that when m is odd, the equality $c_N(f) = 2d$, joint to the fact that the rank of a quadratic form is an even integer, force mN, and N to be even.

We thus write as above $N = 2^a N'$, with N' odd and $a \geq 1$.

If m is odd, the modified sums $S^*_n(f)$ are no longer integers, but algebraic integers in $\mathbf{Z}[\sqrt{2}]$. The same is true for the coefficients of the modified L-function; since its reciprocal roots are roots of unity, we get from 2.1 a factorization of the form

$$L^*(f,T) = \prod_{\ell,\ v_2(\ell)\leq 2} \Phi_\ell(T)^{m_\ell(f)} \prod_{\ell,\ v_2(\ell)\geq 3} \Phi^+_\ell(T)^{m^+_\ell(f)} \Phi^-_\ell(T)^{m^-_\ell(f)}$$

If we take logarithmic derivatives of both sides, we obtain the following expression for the modified sums

$$-S^*_n(f) := \sum_{\ell,\ v_2(\ell)\leq 2} m_\ell(f) c_\ell(n) + \sum_{\ell,\ v_2(\ell)\geq 3} \left(m^+_\ell(f) c^+_\ell(n) + m^-_\ell(f) c^-_\ell(n)\right)$$

where we have used the Ramanujan sums, and we have set

$$c^\pm_\ell(n) = \sum_{i,\ \chi(i)=\pm 1} \zeta^{ni}_\ell,$$

We now change the variables: we modify the multiplicities in order to make the sums from Definition 2.2 appear.

Definition 5.1. We define the *positive multiplicities* associated to f as

$$M^+_\ell(f) := \begin{cases} m_\ell(f) & \text{if} \quad v_2(\ell) \leq 2 \\ \frac{m^+_\ell(f)+m^-_\ell(f)}{2} & \text{if} \quad v_2(\ell) \geq 3 \end{cases}$$

and the *negative multiplicities* associated to f as

$$M^-_\ell(f) := \begin{cases} 0 & \text{if} \quad v_2(\ell) \leq 2 \\ \frac{m^+_\ell(f)-m^-_\ell(f)}{2} & \text{if} \quad v_2(\ell) \geq 3 \end{cases}$$

Since we have $c^+_\ell(n) + c^-_\ell(n) = c_\ell(n)$ and $\sigma_\ell(n) = c^+_\ell(n) - c^-_\ell(n)$ we rewrite the modified sums as

$$-S^*_n(f) := \sum_\ell M^+_\ell(f) c_\ell(n) + \sum_{\ell,\ v_2(\ell)\geq 3} M^-_\ell(f)\sigma_\ell(n) \tag{5.1}$$

The rank of a bilinear form is even, and we have $c_n(f) \equiv n \mod 2$. We deduce that the modified sum $S^*_n(f)$ is in $\mathbf{Z}$ if n is even, and in $\sqrt{2}\mathbf{Z}$ if n is odd. As a

consequence of the evaluations of the sums $c_\ell(n)$ and $\sigma_\ell(n)$ in 2.3, we deduce

$$\sum_\ell M_\ell^+(f)c_\ell(n) = \begin{cases} -S_n^*(f) & \text{if} \quad v_2(n) \geq 1 \\ 0 & \text{if} \quad v_2(n) = 0 \end{cases} \tag{5.2}$$

$$\sum_{\ell,\ v_2(\ell)\geq 3} M_\ell^-(f)\sigma_\ell(n) = \begin{cases} -S_n^*(f) & \text{if} \quad v_2(n) = 0 \\ 0 & \text{si} \quad v_2(n) \geq 1 \end{cases} \tag{5.3}$$

The first system is similar to the one given when m is even, and we deduce the following equivalent of Proposition 4.1

Proposition 5.2. *Assume m is odd. For any even $n \geq 2$, the invariant $\varepsilon_n(f)$ satisfies*

(i) *if $\varepsilon_N(f) = -1$, then $\varepsilon_n(f) = \varepsilon_{\gcd(n,N)}(f)$;*
(ii) *if $\varepsilon_N(f) = 1$, then*
- *if $1 \leq v_2(n) \leq v_2(N) - 1$, then $\varepsilon_n(f) = 0$;*
- *if $v_2(n) = v_2(N)$, then $\varepsilon_n(f) = \varepsilon_{\gcd(n,N)}(f)$;*
- *if $v_2(n) \geq v_2(N) + 1$, then $\varepsilon_n(f) = -\varepsilon_{\gcd(n,N)}(f)$;*

(iii) *if $\varepsilon_N(f) = 0$, then*
(iiia) *when $\varepsilon_{2N}(f) = -1$, we have $\varepsilon_n(f) = \varepsilon_{\gcd(n,2N)}(f)$;*
(iiib) *when $\varepsilon_{2N}(f) = 1$, we have*
- *if $1 \leq v_2(n) \leq v_2(N)$, then $\varepsilon_n(f) = 0$;*
- *if $v_2(n) = v_2(N) + 1$, then $\varepsilon_n(f) = \varepsilon_{\gcd(n,2N)}(f)$;*
- *if $v_2(n) \geq v_2(N) + 2$, then $\varepsilon_n(f) = -\varepsilon_{\gcd(n,2N)}(f)$.*

On the other hand, we also deduce expressions for the multiplicities as in Proposition 4.3

Proposition 5.3. *Assume m is odd; recall that we have set $N = 2^a N'$, N' odd. The multiplicities $M_\ell^+(f)$ satisfy the following systems, depending on the case from the above Proposition*

(i) $A(N)(M_\ell^+(f))_{\ell|N} = (-S_d^*(f))_{d|N}$;
(ii) $2^a A(N')(M_{2^{a+1}\ell}^+(f))_{\ell|N'} = (S_{2^a d}^*(f))_{d|N'}$;
(iiia) $A(2N)(M_\ell^+(f))_{\ell|2N} = (-S_d^*(f))_{d|2N}$;
(iiib) $2^{a+1} A(N')(M_{2^{a+2}\ell}^+(f))_{\ell|N'} = (S_{2^{a+1} d}^*(f))_{d|N'}$

We now exploit the second system (5.3).

We know from Proposition 3.8 that all roots orders ℓ divide the period D, and $D \in \{N, 2N, 4N\}$.

Since the sum $\sigma_\ell(n)$ is zero when $v_2(n) \neq v_2(\ell) - 3$, the system (5.3) boils down to the $v_2(D) - 2$ following systems

$$\sum_{\ell|D,\ v_2(\ell)=3} M_\ell^-(f)\sigma_\ell(n) = -S_n^*(f), \qquad v_2(n) = 0$$

$$\sum_{\ell|D,\ v_2(\ell)=i} M_\ell^-(f)\sigma_\ell(n) = 0, \qquad v_2(n) = i - 3,\ 4 \leq i \leq v_2(D)$$

Recall the expression of $\sigma_\ell(n)$ from Lemma 2.3.

First assume that $v_2(n) \neq v_2(\ell) - 3$. In this case, since $\ell|D$, we have $v_2(\ell) \neq v_2(D)$, and $v_2(\gcd(n, D)) = \min\{v_2(n), v_2(D)\} \neq v_2(\ell) - 3$. Thus we have

$$\sigma_\ell(\gcd(n, D)) = \sigma_\ell(n) = 0$$

When we have $v_2(n) = v_2(\ell) - 3$, we also have $v_2(\gcd(n, D)) = v_2(\ell) - 3$ since ℓ divides D. Moreover, we have $\gcd(n, D) = 2^{v_2(n)} \gcd(n, N')$, and we deduce from

Lemma 2.3 that

$$\sigma_\ell(\gcd(n,D)) = \chi(n\gcd(n,N'))\sigma_\ell(n)$$

When n is odd, we deduce the following relation for the $\varepsilon_n(f)$

Proposition 5.4. *Assume m is odd; recall that we have set $N = 2^aN'$, N' odd. For any odd integer n, we have the equality*

$$\varepsilon_n(f) = \chi(n\gcd(n,N'))\varepsilon_{\gcd(n,N')}(f)$$

On the other hand, if we set $\ell = 2^i\ell'$, $\ell'|N'$, we deduce the following rewriting for the $v_2(D)-2$ systems

$$\sum_{\ell'|N'} M^-_{8\ell'}(f)\sigma_{8\ell'}(n) = -S^*_n(f), \qquad n|N'$$

$$\sum_{\ell'|N'} M^-_{2^i\ell'}(f)\sigma_{2^i\ell'}(2^{i-3}n) = 0, \qquad n|N',\ 4\le i\le v_2(D)$$

The matrices associated to these systems are the $B(D)_{i-3,i}$ for $3\le i\le v_2(D)$ from (2.3), which are invertible.

This proves the following for the negative multiplicities

Proposition 5.5. *Recall that we have set $N = 2^aN'$. Notations are as above. Then we have*

(1) *for any ℓ such that $v_2(\ell)\neq 3$, we have $M^-_\ell(f) = 0$.*
(2) *the non zero multiplicities $M^-_{8\ell'}(f)$, $\ell'|N'$ satisfy the system*

$$2\sqrt{2}\Delta(N')A(N')\Delta(N')\left(M^-_{8\ell'}(f)\right)_{\ell'|N'} = \left(S^*_n(f)\right)_{n|N'}$$

When the period is not divisible by 8, or when the roots orders have dyadic valuation different from 3, we see that the negative multiplicities are all equal to zero, and we deduce the following cancellations

Corollary 5.6. *Assume m is odd. For any odd $n\ge 1$, the sums $S_n(f)$ are zero and the modified L-function has integer coefficients when*

(a) *we have $v_2(D)\le 2$;*
(b) *we are in case (ii) and $v_2(N) = v_2(D)-1\neq 2$;*
(c) *we are in case (iiib) and $v_2(N) = v_2(D)-2\neq 1$;*

where the cases are those of Proposition 3.8.

6. An example and an application around the Suzuki curve

In this section, we fix an integer $h\ge 1$, and we set $q_0 := 2^h$, $q := 2^{2h+1} = 2q_0^2$.

We consider the polynomial $f(x) = x^{q_0}(x^q+x)$ in the following, and we determine all sums $S_n(f)$, $n\ge 1$ from a finite number of them, in order to illustrate the results described above.

Note that the polynomial f comes from the well-known Suzuki curve, defined over $\mathbf{F}_q$ by the equation

$$S_h:\ y^q + y = x^{q_0}(x^q+x) \tag{6.1}$$

The number of rational points of this curve over any extension of $\mathbf{F}_q$ is given in [4, Proposition 4.3]. Actually this curve is defined over the base field $\mathbf{F}_2$, and as an application of the preceding results, we give the number of its rational points over any field $\mathbf{F}_{2^n}$.

In order to do this, we determine the sums

$$S_n(f) := \sum_{x\in\mathbf{F}_{2^n}} (-1)^{\mathrm{Tr}_{\mathbf{F}_{2^n}/\mathbf{F}_2}(f(x))}$$

for any $n \geq 1$.

First remark the following fact: since we have $x^{q_0+q} = (x^{1+2q_0})^{q_0}$, for any $x \in \mathbf{F}_{2^n}$, we have

$$\mathrm{Tr}_{\mathbf{F}_{2^n}/\mathbf{F}_2}(f(x)) = \mathrm{Tr}_{\mathbf{F}_{2^n}/\mathbf{F}_2}(x^{q_0+q}+x^{q_0+1}) = \mathrm{Tr}_{\mathbf{F}_{2^n}/\mathbf{F}_2}(x^{2q_0+1}+x^{q_0+1}) = \mathrm{Tr}_{\mathbf{F}_{2^n}/\mathbf{F}_2}(xR(x))$$

where we have set $R(x) := x^{2q_0} + x^{q_0}$. With this additive polynomial, we obtain

$$\widetilde{R}(x) = x^{2q} + x^q + x^2 + x = (x^q + x) \circ (x^2 + x)$$

The roots of this polynomial form a $\mathbf{F}_2$-vector space of dimension $2h + 2$ that contains $\mathbf{F}_q$ and $\mathbf{F}_4$. Since $2h + 1$ is odd, this is the sub-vector space of $\mathbf{F}_{q^2}$ generated by $\mathbf{F}_q \cup \mathbf{F}_4$. We deduce easily the following

Lemma 6.1. *Notations are as above. The decomposition field of $\widetilde{R}$ is $\mathbf{F}_{q^2}$, and we have for all $n \geq 1$*

$$c_n(f) = \begin{cases} \gcd(n, 2h+1) & \text{if } n \text{ is odd} \\ \gcd(n, 2h+1) + 1 & \text{if } n \text{ is odd} \end{cases}$$

We now evaluate some of the sums $S_n(f)$. First note than when n divides $2h+1$, the field $\mathbf{F}_{2^n}$ is contained in $\mathbf{F}_q$, and we have $f(x) = 0$ for all x in $\mathbf{F}_{2^n}$. We deduce immediately the first assertion of the following

Lemma 6.2. *Notations are as above. We have*

1. *if n divides $2h + 1$, then $S_n(f) = 2^n$;*
2. *if $n = 4d$, where d divides $2h + 1$, then $S_n(f) = \chi(d)\chi(2h + 1)2^{\frac{5d+1}{2}}$*

Proof. We first choose $\alpha \in \mathbf{F}_4$ and $\beta \in \mathbf{F}_{16}$ such that $\alpha^2 + \alpha = 1$ and $\beta^2 + \beta = \alpha$. Then $\{1, \alpha, \beta, \alpha\beta\}$ is a basis for the $\mathbf{F}_2$-vector space $\mathbf{F}_{16}$, and since d is odd, it remains a basis for the $\mathbf{F}_{2^d}$-vector space $\mathbf{F}_{2^n}$.

Thus, for any $x \in \mathbf{F}_{2^n}$, we can write $x = x_0 + \alpha x_1 + \beta x_2 + \alpha\beta x_3$ where $(x_0, x_1, x_2, x_3) \in \mathbf{F}_{2^d}^4$. After some calculations, we get

$$\mathrm{Tr}_{\mathbf{F}_{2^n}/\mathbf{F}_{2^d}}(f(x)) = x_1^{q_0}x_3 + x_1x_3^{q_0} + x_2^{q_0+1} + x_2x_3^{q_0} + \epsilon x_3^{q_0+1}$$

where $\epsilon = 0$ if $\chi(2h + 1) = 1$ and $\epsilon = 1$ if $\chi(2h + 1) = -1$. Putting this into the sum, we get

$$\begin{aligned} S_n(f) &= \sum_{(x_0,x_1,x_2,x_3)\in\mathbf{F}_{2^d}^4} \psi\left(\mathrm{Tr}_{\mathbf{F}_{2^d}/\mathbf{F}_2}(x_1^{q_0}x_3 + x_1x_3^{q_0} + x_2^{q_0+1} + x_2x_3^{q_0} + \epsilon x_3^{q_0+1})\right) \\ &= 2^d \sum_{(x_2,x_3)\in\mathbf{F}_{2^d}^2} \psi\left(\mathrm{Tr}_{\mathbf{F}_{2^d}/\mathbf{F}_2}(x_2^{q_0+1} + x_2x_3^{q_0} + \epsilon x_3^{q_0+1})\right) S(x_3) \end{aligned}$$

where we have set $S(x_3) = \sum_{x_1\in\mathbf{F}_{2^d}} \psi\left(\mathrm{Tr}_{\mathbf{F}_{2^d}/\mathbf{F}_2}(x_1^{q_0}x_3 + x_1x_3^{q_0})\right)$. Now since we have $\mathrm{Tr}_{\mathbf{F}_{2^d}/\mathbf{F}_2}(x_1^{q_0}x_3) = \mathrm{Tr}_{\mathbf{F}_{2^d}/\mathbf{F}_2}(x_1x_3^{2q_0})$, we deduce from an orthogonality relation that the sum $S(x_3)$ is zero, except when $x_3 \in \mathbf{F}_2$, and then $S(x_3) = 2^d$. We get

$$\begin{aligned} S_n(f) &= 2^{2d}\left(\sum_{x_2\in\mathbf{F}_{2^d}} \psi\left(\mathrm{Tr}_{\mathbf{F}_{2^d}/\mathbf{F}_2}(x_2^{q_0+1})\right) + \sum_{x_2\in\mathbf{F}_{2^d}} \psi\left(\mathrm{Tr}_{\mathbf{F}_{2^d}/\mathbf{F}_2}(x_2^{q_0+1} + x_2 + \epsilon)\right)\right) \\ &= 2^{2d}\left(\sum_{x_2\in\mathbf{F}_{2^d}} \psi\left(\mathrm{Tr}_{\mathbf{F}_{2^d}/\mathbf{F}_2}(x_2^{q_0+1})\right) + \chi(2h+1)\sum_{x_2\in\mathbf{F}_{2^d}} \psi\left(\mathrm{Tr}_{\mathbf{F}_{2^d}/\mathbf{F}_2}(x_2^{q_0+1} + x_2)\right)\right) \end{aligned}$$

The first sum is associated to the polynomial $xR_1(x)$, with $R_1(x) = x^{q_0}$. The roots of the polynomial $\widetilde{R}_1$ are the elements of the field $\mathbf{F}_{q_0^2}$, and since d divides $2h + 1$,

the only roots in $\mathbf{F}_{2^d}$ are the elements in $\mathbf{F}_2$. Now since d is odd the restriction of the quadratic form $\psi\left(\mathrm{Tr}_{\mathbf{F}_{2^d}/\mathbf{F}_2}(x_2^{q_0+1})\right)$ to $\mathbf{F}_2$ is non trivial, and the first sum is zero.

Finally, we apply [7, Corollary 3] to the second sum: it is equal to $\chi(d)2^{\frac{d+1}{2}}$, and this gives the desired result. □

With these results at hand, we are able to determine all sums $S_n(f)$. From Lemma 6.1, it is sufficient to give the invariants $\varepsilon_n(f)$

Proposition 6.3. *Recall that $f(x) = x^{q_0}(x^q + x)$. Then for all $n \geq 1$ we have*

(1) *if n is odd, then*

$$\varepsilon_n(f) = \chi\left(n \gcd(n, 2h+1)\right)$$

(2) *if n is even, then*

$$\varepsilon_n(f) = \begin{cases} 0 & \text{if } v_2(n) = 1 \\ \chi\left((2h+1)\gcd(n, 2h+1)\right) & \text{if } v_2(n) = 2 \\ -\chi\left((2h+1)\gcd(n, 2h+1)\right) & \text{if } v_2(n) \geq 3 \end{cases}$$

Proof. From Lemma 6.1, the degree of the decomposition field of $\widetilde{R}$ over $\mathbf{F}_2$ is $N = 4h+2$. From Lemma 6.2 (2), we have $\varepsilon_{2N}(f) = 1$, and we deduce from Proposition 3.8 that $D = 4N$.

Now assertion (1) comes readily from Proposition 5.4.

From Lemma 6.2, we have $\varepsilon_{4d}(f) = \chi\left((2h+1)d\right)$ for all divisors of $2h+1$. Now assertion (2) is a consequence of Proposition 5.2 since for all n such that $v_2(n) \geq 2$, we have $\gcd(n, 2N) = 4\gcd(n, 2h+1)$. □

We deduce some results on the factorization of the modified L-function below. They are an immediate consequence of the above result, and of Propositions 5.3 (iiib) and 5.5 (2).

Proposition 6.4. *For f as above, the only non zero multiplicities are among those $M_{8\ell}^{\pm}(f)$, $\ell | 2h+1$.*

Moreover, we have $M_{8\ell}^{-}(f) = \chi(\ell)\chi(2h+1)M_{8\ell}^{+}(f)$, and the $M_{8\ell}^{+}(f)$ are the solutions of the system

$$A(2h+1)\left(M_{8\ell}^{+}(f)\right)_{\ell | 2h+1} = \chi(2h+1)\left(\chi(d)2^{\frac{d-3}{2}}\right)_{d | 2h+1}$$

We end with the determination of the number of rational points of the curve S_h over any extension of $\mathbf{F}_2$

Proposition 6.5. *For any integer $n \geq 1$, we have*

$$\#S_h(\mathbf{F}_{2^n}) = 2^n + 1 + (2^{\gcd(n, 2h+1)} - 1)S_n(f)$$

Proof. First observe that the equation $y^q + y = t$ has $\sum_{z \in \mathbf{F}_{2^n} \cap \mathbf{F}_q} \psi \circ \mathrm{Tr}_{\mathbf{F}_{2^n}/\mathbf{F}_2}(tz)$ solutions for any $t \in \mathbf{F}_{2^n}$.

We deduce that the number of affine rational points over $\mathbf{F}_{2^n}$ of the curve S_h is

$$\sum_{z \in \mathbf{F}_{2^n} \cap \mathbf{F}_q} S_n(zf)$$

When $z = 0$, the sum is 2^n. When $z \neq 0$, we remark that for any $t \in \mathbf{F}_q$, we have $f(tx) = t^{q_0+1}f(x)$. Since $q_0 + 1$ is prime to $q - 1$, for any $z \in \mathbf{F}_q \cap \mathbf{F}_{2^n}$, there exists an unique $t \in \mathbf{F}_q \cap \mathbf{F}_{2^n}$ such that $t^{q_0+1} = z$. Thus we have $S_n(zf) = S_n(f)$, and this is the desired result □

REFERENCES

[1] Tom M. Apostol. Arithmetical properties of generalized Ramanujan sums. *Pacific J. Math.*, 41:281–293, 1972.

[2] Emrah Çakçak and Ferruh Özbudak. Some Artin-Schreier type function fields over finite fields with prescribed genus and number of rational places. *J. Pure Appl. Algebra*, 210(1):113–135, 2007.

[3] Robert W. Fitzgerald. Invariants of trace forms over finite fields of characteristic 2. *Finite Fields Appl.*, 15(2):261–275, 2009.

[4] Johan P. Hansen. Deligne-Lusztig varieties and group codes. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 63–81. Springer, Berlin, 1992.

[5] Xiang-Dong Hou. Explicit evaluation of certain exponential sums of binary quadratic functions. *Finite Fields Appl.*, 13(4):843–868, 2007.

[6] L. Kronecker. Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.*, 53:173–175, 1857.

[7] Jyrki Lahtonen, Gary McGuire, and Harold N. Ward. Gold and Kasami-Welch functions, quadratic forms, and bent functions. *Adv. Math. Commun.*, 1(2):243–250, 2007.

[8] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.

[9] Gary McGuire and Emrah Sercan Yılmaz. On the zeta functions of supersingular curves. *Finite Fields Appl.*, 54:65–79, 2018.

[10] Ferruh Özbudak, Elif Saygı, and Zülfükar Saygı. Quadratic forms of codimension 2 over finite fields containing $\mathbb{F}_4$ and Artin-Schreier type curves. *Finite Fields Appl.*, 18(2):396–433, 2012.

[11] S. Ramanujan. On certain trigonometrical sums and their applications in the theory of numbers. In *Collected papers of Srinivasa Ramanujan*, pages 179–199. AMS Chelsea Publ., Providence, RI, 2000.

[12] Gerard van der Geer and Marcel van der Vlugt. Reed-Muller codes and supersingular curves. I. *Compositio Math.*, 84(3):333–367, 1992.

[13] Gerard van der Geer and Marcel van der Vlugt. On the existence of supersingular curves of given genus. *J. Reine Angew. Math.*, 458:53–61, 1995.

LAMIA, UNIVERSITÉ DES ANTILLES
Email address: regis.blache@univ-antilles.fr

UNIVERSITÉ D'ÉTAT D'HAÏTI
Email address: pierretimothe1979@yahoo.fr