

Marko Rinta-aho

ON MONOMIAL
EXPONENTIAL SUMS IN
CERTAIN INDEX 2 CASES
AND THEIR CONNECTIONS
TO CODING THEORY

FACULTY OF SCIENCE,
DEPARTMENT OF MATHEMATICAL SCIENCES,
UNIVERSITY OF OULU

A

SCIENTIAE RERUM
NATURALIUM



ACTA UNIVERSITATIS OULUENSIS
A Scientiae Rerum Naturalium 503

MARKO RINTA-AHO

**ON MONOMIAL EXPONENTIAL
SUMS IN CERTAIN INDEX 2 CASES
AND THEIR CONNECTIONS
TO CODING THEORY**

OULUN YLIOPISTO, OULU 2008

Copyright © 2008
Acta Univ. Oul. A 503, 2008

ISBN 978-951-42-8736-7 (Paperback)
ISBN 978-951-42-8737-4 (PDF)
<http://herkules oulu.fi/isbn9789514287374/>
ISSN 0355-3191 (Printed)

ISSN 1796-220X (Online)
<http://herkules oulu.fi/issn03553191/>

Cover design
Raimo Ahonen

OULU UNIVERSITY PRESS
OULU 2008

Rinta-aho, Marko, On monomial exponential sums in certain index 2 cases and their connections to coding theory

Faculty of Science, Department of Mathematical Sciences, University of Oulu, P.O.Box 3000, FI-90014 University of Oulu, Finland

Acta Univ. Oul. A 503, 2008

Oulu, Finland

Abstract

In this paper monomial exponential sums over finite fields in certain index 2 cases are considered. A recursion is given to compute these sums for most values of the parameters. For the remaining values we should know certain Gauss sums exactly, which seems to be a hard problem in general. Examples illustrating the methods and the remaining difficulties are given. Also, computational data is given showing what happens for small values of the parameters.

Keywords: exponential sums, Gauss sums

1 Introduction

Let $N > 1$ be an odd integer satisfying the conditions $\text{ord}_N 2 = \phi(N)/2$ and $-1 \notin \langle 2 \rangle \subseteq \mathbb{Z}_N^*$. Then we say that index 2 case holds for N . In (10) it is shown that N can have at most 2 different prime factors, say p and q , and there are three possible cases for N , namely

I) $N = q^v, q \equiv 7 \pmod{8}, \text{ord}_{q^v} 2 = \phi(q^v)/2$;

II) $N = p^u q^v, p \equiv 5 \pmod{8}, q \equiv 3 \pmod{8}, 2$ is a primitive root modulo p^u and modulo q^v ;

III) $N = p^u q^v, p \equiv 3, 5 \pmod{8}, q \equiv 7 \pmod{8}, \text{ord}_{p^u} 2 = \phi(p^u)$, and $\text{ord}_{q^v} 2 = \phi(q^v)/2$ with $-1 \notin \langle 2 \rangle$ modulo q^v .

Throughout the paper we will use the following notations.

- $N = p^u q^v$ with p, q primes, $u \geq 0, v \geq 1, \text{ord}_N 2 = \phi(N)/2$, and $-1 \notin \langle 2 \rangle \subseteq \mathbb{Z}_N^*$;
- $D = p^s q^t$ with $D \mid N$;
- $r = 2^{\frac{m\phi(N)}{2}}$ with $m \in \mathbb{Z}_+$, and \mathbb{F} is the finite field with r elements and with a primitive element γ ;
- $n = (r-1)/N$.

Our aim is to obtain information in the index 2 case III on the monomial exponential sums

$$S(a, D) := \sum_{x \in \mathbb{F}^*} e(\gamma^a x^D)$$

where $e(x) = (-1)^{\text{tr}x}$ is the canonical additive character of \mathbb{F} and tr is the absolute trace of \mathbb{F} . In cases I and II the sums $S(a, D)$ were computed by Moisiso in (10) and in the special case III case $N = pq$ by van der Vlugt in (15). The sums $S(a, N)$ can be applied to computation of the weight distribution of irreducible cyclic codes and their duals in the following way. Let

$$C_N(n) := \{\mathbf{c} = (c_0, \dots, c_{n-1}) \in \mathbb{F}_2^n \mid c(\gamma^N) = 0\}, \quad (1)$$

where $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in \mathbb{F}_2[x]/\langle x^n - 1 \rangle$, be a cyclic code with a zero γ^N . The dual of $C_N(n)$ is an irreducible cyclic code

$$C_N(n)^\perp = \{\mathbf{c}(\alpha) = (\text{tr}(\alpha), \text{tr}(\alpha\gamma^N), \dots, \text{tr}(\alpha\gamma^{(n-1)N})) \mid \alpha \in \mathbb{F}\}.$$

The weight of a word $\mathbf{c}(\alpha) \in C_N(n)^\perp$ for $\alpha = \gamma^a$ is

$$\begin{aligned} w(\mathbf{c}(\alpha)) &= \frac{1}{2} \sum_{i=0}^{n-1} (1 - (-1)^{\text{tr}(\alpha \gamma^{iN})}) = \frac{1}{2} \left(n - \sum_{i=0}^{n-1} (-1)^{\text{tr}(\gamma^a \gamma^{iN})} \right) \\ &= \frac{1}{2} \left(n - \frac{1}{N} S(a, N) \right) \end{aligned} \quad (2)$$

since γ^N is an n th root of unity. The weight distributions of a code and its dual are connected via the Pless power moment identity, see (14). For $C_N(n)$, (11, Theorem 3) gives a nice recursion connecting $C_N(n)^\perp$ and the sums $S(a, N)$. This is quoted in Proposition 15 on page 31.

The dimension of $C_N(n)^\perp$ is the degree of the generator polynomial of $C_N(n)$, which is the size of the 2-cyclotomic coset modulo $r - 1$ containing N , as its only zero is γ^N . The dimension is thus $\text{ord}_n 2$. Letting

$$\Psi: (\mathbb{F}, +) \rightarrow C_N(n)^\perp, \alpha \mapsto \mathbf{c}(\alpha) \quad (3)$$

we see that each codeword in $C_N(n)^\perp$ occurs $|\ker \Psi| = 2^{m\phi(N)/2 - \text{ord}_n 2}$ times.

The rest of the paper is organized as follows: in section 2 we present the work done on $S(a, N)$ so far, some preliminaries on cyclotomic cosets and introduce notations; in section 3 we prove the recursive results in case III on $S(a, D)$ which we use in computing the value distribution of $S(a, N)$; section 4 deals with the Gauss sums involved in the sums $S(a, D)$. The main problem will be determining the signs of their imaginary parts. To that end we prove a congruence that enables us to compute the value distribution of $S(a, N)$ for most N ; in section 5 we present examples that classify numbers N according to which technique can be used to determine the value distribution. These examples also point to the difficulties that remain for those N to which our techniques do not apply; the last section gives experimental results from our computer calculations, showing how small N and m distribute into different classes.

2 Previous Work and Preliminaries

In this section we recall what is known about $S(a, N)$ in the cases I and II, and present the concepts and lemmas needed to handle case III. First, let us gather some useful arithmetical facts about the cases with which we are dealing. The proofs can be found in (10, II lemmas 2, 3 and 5).

Lemma 1. *If $\text{ord}_{q^v} 2 = \phi(q^v)$, resp. $\phi(q^v)/2$, then $\text{ord}_{q^j} 2 = \phi(q^j)$, resp. $\phi(q^j)/2$, for all $1 \leq j \leq v$.*

If $N = q^v$ then $-1 \notin \langle 2 \rangle \subseteq \mathbb{Z}_N^$ if and only if $q \equiv 7 \pmod{8}$.*

If $N = p^u q^v$, $\text{ord}_{p^u} 2 = \phi(p^u)$ and $\text{ord}_{q^v} 2 = \phi(q^v)/2$ then $\text{ord}_{p^i q^j} 2 = \phi(p^i q^j)/2$ for all $1 \leq i \leq u$ and $1 \leq j \leq v$.

Each value x^D is obtained D times as x runs through \mathbb{F}^* , so we have $D \mid S(a, D)$. Further, $S(a, D) = S(b, D)$ whenever $a \equiv b \pmod{D}$, especially if $D \mid a$ then $S(a, D) = S(0, D)$. From the basic properties of the trace map and the fact that $x \mapsto x^2$ is bijective in \mathbb{F}^* it follows that

$$S(2a, D) = \sum_{x \in \mathbb{F}^*} e(\gamma^{2a} x^D) = \sum_{x \in \mathbb{F}^*} e((\gamma^a x^D)^2) = \sum_{x \in \mathbb{F}^*} e(\gamma^a x^D) = S(a, D).$$

Thus it suffices to compute $S(a, D)$ when a runs through the representatives of the 2-cyclotomic cosets modulo D . Denote the coset of a modulo D by C_a^D . By the above, for a fixed a there are $\frac{r-1}{D} |C_a^D|$ values $b \in \{0, \dots, r-2\}$ such that $S(b, D) = S(a, D)$. The representatives and the sizes of C_a^D are given in (10, II Lemma 7). In case I the representatives and the sizes are

$$0, \pm q^j; \quad |C_{\pm q^j}^D| = \frac{\phi(q^{t-j})}{2}, \quad 0 \leq j < t. \quad (4)$$

In case II they are, for $D = p^s q^t$, $s, t \geq 1$,

$$0, \pm p^i q^j, \quad p^s q^j, \quad p^i q^t, \quad 0 \leq i < s, \quad 0 \leq j < t, \quad (5)$$

and

$$|C_{\pm p^i q^j}^D| = \frac{\phi(D/p^i q^j)}{2}, \quad |C_{p^s q^j}^D| = \phi(q^{t-j}), \quad |C_{p^i q^t}^D| = \phi(p^{s-i}).$$

In case III we give a proof for the convenience of the reader and present the result as the following lemma. We will use later only those $D \mid N$ for which $q \mid D$. If N satisfies case III then $D = q^t$, $1 \leq t \leq v$, satisfies case I by Lemma 1 and the representatives are in (4). Hence only $D = p^s q^t$ with $s, t \geq 1$ are listed below.

Lemma 2. In case III the representatives of C_a^D are for $D = p^s q^t$ with $s, t \geq 1$

$$0, \pm p^i q^j, \pm p^s q^j, p^i q^t, \quad 0 \leq i < s, \quad 0 \leq j < t,$$

and the sizes of the cosets are

$$|C_{\pm p^i q^j}^D| = \frac{\phi(D/p^i q^j)}{2}, \quad |C_{\pm p^s q^j}^D| = \frac{\phi(q^{t-j})}{2}, \quad |C_{p^i q^t}^D| = \phi(p^{s-i}).$$

Proof. If $|a| \neq |b|$ for non-zero claimed representatives a and b and $C_a^D = C_b^D$ then the largest powers of p and q dividing a and b differ (at least) for one prime, say q . After dividing the common factors from the congruence $a \equiv b2^l \pmod{D}$, possibly interchanging a and b and looking it modulo q , we find $j \geq 1$ and i such that $p^i q^j \equiv \pm 2^l \pmod{q}$ or $q^j \equiv \pm p^i 2^l \pmod{q}$. Both of the cases lead to a contradiction.

If $C_a^D = C_{-a}^D$ and $j < t$ then $-1 \equiv 2^l \pmod{q}$ for some l . By Lemma 1, $\text{ord}_q 2 = \phi(q)/2$ and $-1 \notin \langle 2 \rangle$ in \mathbb{Z}_q , making it impossible to find such l . Hence the given representatives define different cosets.

For $a = \pm p^i q^j$ and l , $|C_a^D| \mid l$ if and only if $1 \equiv 2^l \pmod{p^{s-i} q^{t-j}}$. Thus $|C_a^D| = \text{ord}_{|D/a|} 2$. By this and Lemma 1, $|C_{\pm p^i q^j}^D| = \phi(\frac{D}{p^i q^j})/2$, $|C_{\pm p^s q^j}^D| = \phi(q^{t-j})/2$ and $|C_{p^i q^t}^D| = \phi(p^{s-i})$ for $i < s$ and $j < t$.

If we take the sum $\sum |C_a^D|$ over all the given representatives, then the numbers $D/p^i q^j$, q^{t-j} and p^{s-i} run over all positive factors of D except 1. Thus these cosets contain $\sum_{d|D, d>1} \phi(d) = D - 1$ elements. Counting also 0 we have the lemma. \square

Let $\left(\frac{a}{b}\right)$ denote the Legendre symbol. Its i th power $\left(\frac{a}{b}\right)^i$ equals $\left(\frac{a^i}{b}\right)$ and the latter form will be used here to avoid confusing the Legendre symbol with a rational non-integer. The cosets C_a^D with $a \mid N$, $D \nmid a$ can be determined by the next lemma.

Lemma 3. Let case III hold for N and let $\varepsilon \in \{-1, 1\}$, $a = \varepsilon p^i q^j$ and $D \nmid a$. When $i \geq s$, let $\varepsilon' = \varepsilon \cdot \left(\frac{p^{i-s}}{q}\right)$. Then

$$C_a^D = \begin{cases} C_{\varepsilon' p^s q^j}^D & \text{if } i \geq s, \\ C_{p^i q^t}^D & \text{if } j \geq t, \end{cases}$$

and $C_a^D \subseteq C_a^{D'}$ for every $D' \mid D$.

Proof. If $i \geq s$, then $j < t$. Let $a \equiv c2^{l_1} \pmod{D}$, where $l_1 \in \mathbb{Z}_+$ and c is one of the representatives in Lemma 2. Since $p^s q^j \mid \gcd(a, D)$, $p^s q^j \mid c$. Since $q^{j+1} \mid D$ and $q^{j+1} \nmid a$, $q^{j+1} \nmid c$. Thus $c = \delta p^s q^j$ with $\delta = \pm 1$. Then $\varepsilon p^i q^j \equiv \delta p^s q^j 2^{l_1} \pmod{D}$, and $p^{i-s} \equiv \varepsilon \delta 2^{l_1} \pmod{q}$. By Lemma 1 $\text{ord}_q 2 = \phi(q)/2$, so 2 is the square of a primitive

root modulo q and $\langle 2 \rangle \subseteq \mathbb{Z}_q^*$ is the subgroup of squares. Further, $-1 \notin \langle 2 \rangle \pmod{q}$, hence $\left(\frac{p^{i-s}}{q}\right) = \varepsilon\delta$. The claim for $i \geq s$ now follows.

If $j \geq t$ we get $C_a^D = C_{\pm p^i q^t}^D$ similarly as above. Since $-1 \in \langle 2 \rangle \subseteq \mathbb{Z}_{p^{s-i}}^*$ by Lemma 1, we have $-1 \equiv 2^{l_2} \pmod{p^{s-i}}$ for some $l_2 \in \mathbb{Z}_+$. Thus $-p^i q^t \equiv p^i q^t 2^{l_2} \pmod{D}$, and $C_{-p^i q^t}^D = C_{p^i q^t}^D$.

Let $D' \mid D$ and $b \in C_a^{D'}$. Then $b \equiv a 2^j \pmod{D}$ with some $j \in \mathbb{Z}_+$, so $b \equiv a 2^j \pmod{D'}$, i.e. $b \in C_a^{D'}$. \square

Let us now shortly recall how $S(a, D)$ can be computed in cases I and II or when $-1 \in \langle 2 \rangle$ modulo D . For $-1 \in \langle 2 \rangle$ modulo D , i.e. when $s = 0$ or $t = 0$ in case II and when $t = 0$ in case III, we have by (10, II Theorem 1 and eq. (9))

$$S(a, D) = \begin{cases} (-1)^{m'-1} (D-1) \sqrt{r} - 1 & \text{if } D \mid a, \\ (-1)^{m'} \sqrt{r} - 1 & \text{if } D \nmid a, \end{cases} \quad (6)$$

where in case II $m' \equiv 0 \pmod{2}$ if $s = 0$, and $m' \equiv m \pmod{2}$ if $t = 0$. In case III we have, for $t = 0$, $m' \text{ord}_{p^s} 2 = m\phi(N)/2$ (see Theorem 1 and the beginning of section 2 in (10, II)). By Lemma 1 $\text{ord}_{p^s} 2 = \phi(p^s)$, so $m' = m\phi(q^v)/2 \equiv m \pmod{2}$.

For the rest of the paper we let $\varepsilon \in \{-1, 1\}$, denote $1 + \delta\sqrt{-q}$ by $c(\delta)$ and let χ be the multiplicative character of order N in \mathbb{F}^* with $\chi(\gamma) = e^{2\pi i/N}$ where e is the Napier's number and i is the imaginary unit. Let $G(\chi^j) = \sum_{x \in \mathbb{F}^*} \chi^j(x) e(x)$ denote the Gauss sum over \mathbb{F} defined by χ^j , $j = 1, \dots, N$. In case I, i.e. for $N = q^v$, we have by (10, II Theorem 2)

$$S(a, q^t) = \begin{cases} \phi(q^t) \text{Re}(G(\chi^{\frac{N}{q^t}})) + S(0, q^{t-1}) & \text{if } a = 0, \\ -q^{t-1} \text{Re}(G(\chi^{\frac{N}{q^t}}) c(\varepsilon)) + S(0, q^{t-1}) & \text{if } a \in C_{\varepsilon q^{t-1}}^{q^t}, \\ S(a, q^{t-1}) & \text{otherwise.} \end{cases} \quad (7)$$

In case II $\text{ord}_{p^s} 2 = \phi(p^s)$ and $\text{ord}_{q^t} 2 = \phi(q^t)$, so for $s = 0$ or $t = 0$ we get $S(a, D)$

from (6). For $s, t \geq 1$ we have by (10, II Theorem 3)

$$S(a, D) = \begin{cases} \phi(D) \operatorname{Re}(G(\chi^{\frac{N}{D}})) + S(0, \frac{D}{p}) + S(0, \frac{D}{q}) - S(0, \frac{D}{pq}), & a = 0, \\ \frac{\phi(D)}{1-p} \operatorname{Re}(G(\chi^{\frac{N}{D}})) + S(0, \frac{D}{p}) + S(\frac{D}{pq}, \frac{D}{q}) - S(0, \frac{D}{pq}), & a \in C_{D/p}^D, \\ \frac{\phi(D)}{1-q} \operatorname{Re}(G(\chi^{\frac{N}{D}})) + S(\frac{D}{pq}, \frac{D}{p}) + S(0, \frac{D}{q}) - S(0, \frac{D}{pq}), & a \in C_{D/q}^D, \\ \frac{\phi(D)}{\phi(pq)} \operatorname{Re}(G(\chi^{\frac{N}{D}})(1 + \varepsilon\sqrt{-pq})) \\ \quad + S(\frac{D}{pq}, \frac{D}{p}) + S(\frac{D}{pq}, \frac{D}{q}) - S(0, \frac{D}{pq}), & a \in C_{\varepsilon D/pq}^D, \\ S(a, \frac{D}{p}), & a \in C_{\varepsilon \frac{D}{p^i q^j}}^D, \\ S(a, \frac{D}{q}), & a \in C_{\varepsilon \frac{D}{p^j q^i}}^D, \end{cases} \quad (8)$$

where $i \geq 2$. The representatives of the cosets C_a^D can be seen in (4) and (5).

In case III for $s, t \geq 1$, we have by (10, II eq. (4)),

$$S(a, D) = g(a, D) + S(a, D/p) + S(a, D/q) - S(a, D/pq), \quad (9)$$

where

$$g(a, D) = 2 \operatorname{Re}(G(\chi^{N/D})_{s_D}(a)) \quad (10)$$

with

$$s_D(a) = \sum_{j \in \langle 2 \rangle \subseteq \mathbb{Z}_D^*} \chi^{-\frac{N}{D}j}(\gamma^a) = \sum_{j \in \langle 2 \rangle \subseteq \mathbb{Z}_D^*} \zeta_D^{-aj}$$

and $\zeta_D = e^{2\pi i/D}$. Since $\mathbb{Z}_D^* = \langle 2 \rangle \cup (-\langle 2 \rangle)$ and $\langle 2 \rangle \cap (-\langle 2 \rangle) = \emptyset$, we have

$$2 \operatorname{Re}(s_D(a)) = \overline{s_D(a)} + s_D(a) = \sum_{j \in \langle 2 \rangle} \zeta_D^{aj} + \sum_{j \in \langle 2 \rangle} \zeta_D^{-aj} = \sum_{j \in \mathbb{Z}_D^*} \zeta_D^{aj}$$

where \bar{z} denotes the complex conjugate of z . The last sum is the Ramanujan sum, so by (2, Theorem 272, p. 238)

$$2 \operatorname{Re}(s_D(a)) = \mu(D_0) \frac{\phi(D)}{\phi(D_0)}, \quad (11)$$

where $D_0 = D/\gcd(D, a)$ and μ is the Möbius function

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not square-free,} \\ (-1)^i & \text{if } n \text{ is the product of } i \geq 0 \text{ distinct primes.} \end{cases}$$

Let χ_D be the residue class character modulo D with

$$\chi_D(j) = \begin{cases} 1 & \text{if } j \in \langle 2 \rangle \subseteq \mathbb{Z}_D^*, \\ -1 & \text{if } j \notin \langle 2 \rangle \subseteq \mathbb{Z}_D^*. \end{cases}$$

Since $\chi_D(-1) = -1$,

$$\begin{aligned} -2i \operatorname{Im}(s_D(a)) &= \overline{s_D(a)} - s_D(a) = \sum_{j \in \langle 2 \rangle} \zeta_D^{aj} - \sum_{j \in \langle 2 \rangle} \zeta_D^{-aj} \\ &= \sum_{j \in \langle 2 \rangle} \zeta_D^{aj} + \sum_{j \in \langle 2 \rangle} \chi_D(-j) \zeta_D^{-aj} = \sum_{j \in \mathbb{Z}_D^*} \chi_D(j) \zeta_D^{aj}. \end{aligned}$$

Denoting $D_0 = D / \gcd(D, a)$ as above and $a_0 = a / \gcd(D, a)$, we get by the above, (4, p. 446 (I), p. 449 (IV), p. 471 (IX)) and (10, II Lemma 8) that

$$-2i \operatorname{Im}(s_D(a)) = \begin{cases} 0 & \text{if } q \nmid D_0, \\ \frac{\phi(D)}{\phi(D_0)} \mu\left(\frac{D_0}{q}\right) \chi_q\left(\frac{D_0}{q}\right) \chi_q(a_0) \sqrt{-q} & \text{if } q \mid D_0, \end{cases} \quad (12)$$

where $\chi_q(j)$ is defined to be 0 when $q \mid j$. Since 2 generates the squares modulo q , $\chi_q(j) = \left(\frac{j}{q}\right)$, the Legendre symbol. Noting that $\phi(D)/\phi(D_0) \in \mathbb{R}$ and $\mu(D_0/q) = -\mu(D_0)$ for square-free D_0 and $q \mid D_0$, the equation (10) gives after substituting (11) and (12) into it

$$\begin{aligned} g(a, D) &= \frac{\mu(D_0)\phi(D)}{\phi(D_0)} \operatorname{Re}(G(\chi^{N/D})(1 + \chi_q\left(\frac{D_0}{q}\right) \chi_q(a_0) \sqrt{-q})) \\ &= \frac{\mu(D_0)\phi(D)}{\phi(D_0)} \operatorname{Re}(G(\chi^{N/D})c(\chi_q\left(\frac{D_0}{q}\right) \chi_q(a_0))) \quad \text{for } q \mid D_0. \end{aligned} \quad (13)$$

Using these we are able to derive in case III recursions similar to those in (8) for case II. This will be done in the next section.

3 The Recursion

For the rest of the paper we let case III hold for N and let $\varepsilon \in \{-1, 1\}$ and $c(\delta) = 1 + \delta\sqrt{-q}$ as above. For $D = p^s$ we have $t = 0$ and $m' \equiv m \pmod{2}$ in (6), yielding

$$S(a, p^s) = \begin{cases} (-1)^{m-1}(p^s - 1)\sqrt{r} - 1 & \text{if } p^s \mid a, \\ (-1)^m\sqrt{r} - 1 & \text{if } p^s \nmid a. \end{cases} \quad (14)$$

By (10, II eq. (3)) $S(a, q^t) = \sum_{d|q^t} g(a, d)$. Using The Möbius inversion formula we get $S(a, q^t) = g(a, q^t) + S(a, q^{t-1})$ as in (10, II eq. (4)) and in case I. Here $g(a, q^t)$ is as in (10). Substituting (10) through (13) into this we get (cf. (7))

$$S(a, q^t) = \begin{cases} \phi(q^t) \operatorname{Re}(G(\chi^{\frac{N}{q^t}})) + S(0, q^{t-1}) & \text{if } a = 0, \\ -q^{t-1} \operatorname{Re}(G(\chi^{\frac{N}{q^t}})c(\varepsilon)) + S(0, q^{t-1}) & \text{if } a \in C_{\varepsilon q^{t-1}}^t, \\ S(a, q^{t-1}) & \text{otherwise.} \end{cases} \quad (15)$$

Using equations (9) through (13) we get for $s, t \geq 1$

$$S(a, D) = \begin{cases} \phi(D) \operatorname{Re}(G(\chi^{\frac{N}{D}})) + \Sigma(0, D) & \text{if } a = 0, \\ \frac{\phi(D)}{1-p} \operatorname{Re}(G(\chi^{\frac{N}{D}})) + \Sigma(a, D) & \text{if } a \in C_{D/p}^D, \\ \frac{\phi(D)}{1-q} \operatorname{Re}(G(\chi^{\frac{N}{D}})c(\varepsilon)) + \Sigma(a, D) & \text{if } a \in C_{\varepsilon D/q}^D, \\ \frac{\phi(D)}{\phi(pq)} \operatorname{Re}(G(\chi^{\frac{N}{D}})c(\varepsilon(\frac{D}{pq}))) + \Sigma(a, D) & \text{if } a \in C_{\varepsilon D/pq}^D, \\ \Sigma(a, D) & \text{otherwise,} \end{cases} \quad (16)$$

where $\Sigma(a, D) = S(a, D/p) + S(a, D/q) - S(a, D/pq)$. The $\Sigma(a, D)$ can be calculated by the following result.

Theorem 4. *In (16)*

$$\Sigma(a, D) = \begin{cases} S(0, \frac{D}{p}) + S(0, \frac{D}{q}) - S(0, \frac{D}{pq}) & \text{if } a = 0, \\ S(0, \frac{D}{p}) + S(\frac{D}{pq}, \frac{D}{q}) - S(0, \frac{D}{pq}) & \text{if } a \in C_{D/p}^D, \\ S(\varepsilon(\frac{D}{q}) \frac{D}{pq}, \frac{D}{p}) + S(0, \frac{D}{q}) - S(0, \frac{D}{pq}) & \text{if } a \in C_{\varepsilon D/q}^D, \\ S(a, \frac{D}{p}) + S(\frac{D}{pq}, \frac{D}{q}) - S(0, \frac{D}{pq}) & \text{if } a \in C_{\varepsilon \frac{D}{pq}}^D, \\ S(a, \frac{D}{p}) & \text{if } a \in C_{\varepsilon \frac{D}{p^j q^t}}^D, \\ S(a, \frac{D}{q}) & \text{if } a \in C_{\varepsilon \frac{D}{p^j q^t}}^D, \end{cases}$$

where $i \geq 2$.

Proof. Case $a = 0$ is clear. For $a = D/p$ the middle term follows from Lemma 3 and the others since D/p and D/pq divide a . Similarly, we get the cases $a = \varepsilon D/q$ and $a = \varepsilon D/pq$.

For $a = \varepsilon p^i q^j$ with $i \leq s-2$ we use induction on t . For $t = 1$, i.e. for $D = p^s q$, we have by (14) and by $p^{s-1} \nmid a$

$$\Sigma(a, D) = S(a, \frac{D}{p}) + S(a, p^s) - S(a, p^{s-1}) = S(a, \frac{D}{p}).$$

If $S(a, D') = S(a, D'/p)$ for $D' = p^s q^{t-1}$ then

$$\Sigma(a, D) = S(a, \frac{D}{p}) + S(a, \frac{D}{q}) - S(a, \frac{D}{pq}) = S(a, \frac{D}{p}) + S(a, D') - S(a, \frac{D'}{p}) = S(a, \frac{D}{p}).$$

For $a = \varepsilon p^j q^j$ with $j \leq t-2$ and $s = 1$ we get by (15)

$$\Sigma(a, D) = S(a, \frac{D}{q}) + S(a, q^t) - S(a, q^{t-1}) = S(a, \frac{D}{q})$$

and the induction step is similar as above. \square

For $a = D/p$ and $a = \varepsilon D/q$ we can use (16) and Theorem 4 to write $S(a, D)$ more explicitly.

Corollary 5. For $a = D/p$ and $a = \varepsilon D/q$ we have

$$\begin{aligned} S(\frac{D}{p}, D) &= \frac{1}{1-p} \sum_{i=0}^{t-1} \phi\left(\frac{D}{q^i}\right) \operatorname{Re}(G(\chi^{\frac{N}{D} q^i})) + S(0, \frac{D}{p}) + (-1)^m p^{s-1} \sqrt{r} \\ S(\varepsilon \frac{D}{q}, D) &= \frac{1}{1-q} \sum_{i=0}^s \phi\left(\frac{D}{p^i}\right) \operatorname{Re}(G(\chi^{\frac{N}{D} p^i}) c(\varepsilon(\frac{p^i}{q}))) + S(0, \frac{D}{q}). \end{aligned}$$

Proof. By (8) the cases $a = D/p$ and $a = 0$ have the same recursion as in the index 2 case II so (10, II Lemma 13) gives the formula for $S(D/p, D)$. For $a = \varepsilon D/q$ we have by equation (16) and Theorem 4

$$\begin{aligned} S(\varepsilon \frac{D}{q}, D) &= \frac{\phi(D)}{1-q} \operatorname{Re}(G(\chi^{\frac{N}{D}}) c(\varepsilon)) + S(\varepsilon(\frac{p}{q}) \frac{D}{pq}, \frac{D}{p}) + S(0, \frac{D}{q}) - S(0, \frac{D}{pq}) \\ &= \frac{\phi(D)}{1-q} \operatorname{Re}(G(\chi^{\frac{N}{D}}) c(\varepsilon)) + \frac{\phi(D/p)}{1-q} \operatorname{Re}(G(\chi^{\frac{N}{D} p}) c(\varepsilon(\frac{p}{q}))) \\ &\quad + S(\varepsilon(\frac{p^2}{q}) \frac{D}{p^2 q}, \frac{D}{p^2}) - S(0, \frac{D}{p^2 q}) + S(0, \frac{D}{q}). \end{aligned}$$

Continuing this process and recalling that $D/p^s = q^t$, we finally obtain by (15)

$$\begin{aligned} S(a, D) &= \frac{1}{1-q} \sum_{i=0}^{s-1} \phi\left(\frac{D}{p^i}\right) \operatorname{Re}(G(\chi^{\frac{N}{D} p^i}) c(\varepsilon(\frac{p^i}{q}))) \\ &\quad + S(\varepsilon(\frac{p^s}{q}) q^{t-1}, q^t) - S(0, q^{t-1}) + S(0, \frac{D}{q}) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{1-q} \sum_{i=0}^{s-1} \phi\left(\frac{D}{p^i}\right) \operatorname{Re}\left(G\left(\chi^{\frac{N}{D}p^i}\right)c\left(\varepsilon\left(\frac{p^i}{q}\right)\right)\right) \\
&\quad - q^{t-1} \operatorname{Re}\left(G\left(\chi^{\frac{N}{q^t}}\right)c\left(\varepsilon\left(\frac{p^s}{q}\right)\right)\right) + S(0, q^{t-1}) - S(0, q^{t-1}) + S\left(0, \frac{D}{q}\right) \\
&= \frac{1}{1-q} \sum_{i=0}^s \phi\left(\frac{D}{p^i}\right) \operatorname{Re}\left(G\left(\chi^{\frac{N}{D}p^i}\right)c\left(\varepsilon\left(\frac{p^i}{q}\right)\right)\right) + S\left(0, \frac{D}{q}\right).
\end{aligned}$$

□

4 Determination of the Gauss Sums

In this section we first recall what is known about the Gauss sums appearing in (16) and then study what can be said about the signs of the real and the imaginary part. From equations (14)–(16), Theorem 4 and Corollary 5 it follows that we need the sums $G(\chi^{\frac{N}{D}})$ for which $q \mid D$.

Mbobj (9) has also studied these Gauss sums. He has obtained an expression for them containing the class number of $\mathbb{Q}(\sqrt{-q})$ and a Diophantine equation related to a certain ellipse, see Propositions 3.2, 3.3 and 3.4, and Theorem 3.5 in (9). Our method is similar to that in (10, II), it does not use the class number and it yields a simpler Diophantine equation. Let

$$h_m = \min\left\{S_2\left(\frac{r-1}{D}\right), \frac{m\phi(N)}{2} - S_2\left(\frac{r-1}{D}\right)\right\} \quad (17)$$

with $S_2(x)$ denoting the digit sum of the binary expansion of x . Since

$$\frac{r-1}{D} = \frac{2^{m\phi(N)/2} - 1}{D} = \frac{2^{\phi(N)/2} - 1}{D} \sum_{i=0}^{m-1} 2^{i\phi(N)/2}$$

we see by denoting $r_1 = 2^{\phi(N)/2}$ that

$$h_m = \min\left\{mS_2\left(\frac{r_1-1}{D}\right), \frac{m\phi(N)}{2} - mS_2\left(\frac{r_1-1}{D}\right)\right\} = mh_1.$$

We know (see e.g. (10, II p. 8)) that $G(\chi^{\frac{N}{D}}) = 2^{h_m}(b + c\sqrt{-q})/2$, where $b, c \in \mathbb{Z}$ are odd if $h_m < m\phi(N)/4$ and $(b, c) = (\pm 2, 0)$ if $h_m = m\phi(N)/4$. Further, $|G(\chi^{\frac{N}{D}})| = \sqrt{r}$ and $(\pm b, \pm c)$ are the only solutions to the Diophantine equation

$$b^2 + qc^2 = 2^{m\phi(N)/2 - 2h_m + 2} = 2^{m(\phi(N)/2 - 2h_1) + 2}. \quad (18)$$

In (3) a fast algorithm for solving this equation is presented. Note that $G(\chi^{\frac{N}{D}}) \in \mathbb{R}$ if and only if $h_m = m\phi(N)/4$. Also, p cannot divide both b and c , and q cannot divide b , for otherwise $p \mid 2$ or $q \mid 2$.

To determine the sign of $\text{Re}(G(\chi^{\frac{N}{D}}))$ we use the following theorem which is a modification to the case III of the lemma on page 1245 of (12). That lemma gives similar simple congruences in cases I and II.

Theorem 6. For $D = q^t$,

$$\operatorname{Re} G(\chi^{\frac{N}{D}}) \equiv -1 \pmod{q},$$

and for $D = p^s q^t$, $s, t \geq 1$,

$$\operatorname{Re} G(\chi^{\frac{N}{D}}) \equiv (-1)^{m-1} \pmod{q}.$$

Proof. Denote $G(\chi^{\frac{N}{D}}) = 2^{h_m-1}(b + c\sqrt{-q})$ with h_m as in (17). If $D = q^t$ then we get as in (12)

$$\begin{aligned} 2^{(h_m-1)q^t}(b^{q^t} + (c\sqrt{-q})^{q^t}) &\equiv G(\chi^{\frac{N}{D}})^{q^t} \equiv \sum_{x \in \mathbb{F}^{q^t}} \chi^{\frac{N}{D}q^t}(x)e(q^t x) \\ &= \sum_{x \in \mathbb{F}^{q^t}} e(x) \equiv -1 \pmod{q}. \end{aligned}$$

Since $q \nmid b$, $\gcd(2^{h_m-1}b, q) = 1$ and the claim in this case follows from Fermat's little theorem.

For $D = p^s q^t$ with $s, t \geq 1$ we similarly obtain

$$2^{(h_m-1)q^t}(b^{q^t} + (c\sqrt{-q})^{q^t}) \equiv G(\chi^{\frac{N}{D}})^{q^t} \equiv \sum_{x \in \mathbb{F}^{q^t}} \chi^{\frac{N}{p^s}}(x)e(q^t x) = G(\chi^{\frac{N}{p^s}}) \pmod{q}$$

since $e(q^t x) = e(x)$ as q^t is odd. Here $\operatorname{ord} \chi^{\frac{N}{p^s}} = p^s$ and -1 is a power of 2 modulo p^s , so by a result of Stickelberger and by Davenport-Hasse theorem (see e.g. (10, II Lemma 1)),

$$G(\chi^{\frac{N}{p^s}}) = (-1)^{m-1} \sqrt{r} = (-1)^{m-1} 2^{\frac{m\phi(N)}{4}}.$$

Again, by Fermat's little theorem, $2^{h_m-1}b \equiv (-1)^{m-1} 2^{\frac{m\phi(N)}{4}} \equiv (-1)^{m-1} \pmod{q}$ and the claim follows. \square

The congruence in Theorem 6 is satisfied by $\operatorname{Re} G(\chi^{\frac{N}{D}})$ whose absolute value is known from (18). Both choices of the sign can not satisfy the congruence since then we could subtract the congruences and would get $q \mid 2^{h_m}b$ for a solution (b, c) of (18) leading to a contradiction. Hence exactly one of $\pm 2^{h_m-1}|b|$ satisfies Theorem 6 and we get $\operatorname{Re} G(\chi^{\frac{N}{D}})$ completely.

For some D and m we could also generalize the method from (15) in the following way: for $D = q^t$ and arbitrary m , let χ' be a multiplicative character of \mathbb{F}_{2^l} of order $\operatorname{ord} \chi' = \operatorname{ord} \chi^{\frac{N}{D}} = q^t$, where $l = (q-1)q^{t-1}/2 = \phi(q^t)/2$. This χ' exists since $q^t \mid$

$(2^l - 1)$ as $\text{ord}_q 2 = \phi(q^t)/2 = l$. If $G(\chi') = 2^{h'-1}(b' + c'\sqrt{-q})$ then the absolute values of b' and c' are determined by the equation $b'^2 + qc'^2 = 2^{l-2h'+2}$ where

$$h' = \min \left\{ S_2\left(\frac{2^l-1}{q^t}\right), l - S_2\left(\frac{2^l-1}{q^t}\right) \right\}.$$

The degree l' of the extension $\mathbb{F}_r/\mathbb{F}_{2^l}$ is $l' = m(p-1)p^{u-1}q^{v-t}$, so by the Davenport-Hasse identity (see e.g. (7, Theorem 5.14)) we have $G(\chi^{\frac{N}{D}}) = -(-G(\chi'))^{l'}$. For any complex number z and an even integer $k \geq 0$ the real part of z^k is given by $\text{Re} z^k = \sum_{i \text{ even}} \binom{k}{i} (\text{Re} z)^{k-i} (i \text{Im} z)^i$, so $\text{sgn} \text{Re} z^k$ is the same regardless of $\text{sgn} \text{Re} z$. Here

$$\text{sgn} x = \begin{cases} -1 & \text{if } x < 0, \\ 0 & \text{if } x = 0, \\ 1 & \text{if } x > 0, \end{cases}$$

denotes the signum function. Since the exponent l' is even, we find $\text{sgn} \text{Re} G(\chi^{\frac{N}{D}})$. When m is even we can use similarly the intermediate field \mathbb{F}_{2^l} with $l = \phi(p^s q^t)/2$ since now $l' = mp^{u-s}q^{v-t}$ is even regardless of D .

Knowing only the real part is enough to compute $S(0, D)$ and $S(D/p, D)$ for every $D \mid N$. For $S(\varepsilon D/q, D)$ and $S(\varepsilon D/pq, D)$ we get two choices for each term $G(\chi^{\frac{N}{D}})c(\varepsilon)$ or $G(\chi^{\frac{N}{D}})c(\varepsilon(\frac{2}{q}))$ appearing in the equation (16). By Corollary 5, equation (16) and Theorem 4 we need, for $S(\varepsilon D/q, D)$ and $S(\varepsilon D/pq, D)$, the imaginary parts $\text{Im} G(\chi^{\frac{N}{D} p^i}) = \text{Im} G(\chi^{p^{u-s+i} q^{v-t}})$ for $i = 0, \dots, s$. Since, for $\delta = \pm 1$,

$$\text{Re} (G(\chi^{\frac{N}{D} p^i})(1 + \delta\sqrt{-q})) = \text{Re} G(\chi^{\frac{N}{D} p^i}) - \delta\sqrt{q} \text{Im} G(\chi^{\frac{N}{D} p^i})$$

we see that if the signs of both δ and $\text{Im} G(\chi^{\frac{N}{D} p^i})$ are changed then this term remains the same.

Suppose that, for fixed D and $a \in \{\varepsilon D/q, \varepsilon D/pq\}$, we have computed $S(a, D)$ for every possible combination of $\text{sgn} \text{Im} G(\chi^{\frac{N}{D} p^i})$, $i = 0, \dots, s$ (we do not know which combination is the correct one). Then $S(-a, D)$ is obtained for a given sequence of the signs by changing every sign and computing $S(a, D)$ using these altered signs. Hence, if we are able to limit the possible combinations down to two we know that one gives $S(a, D)$ and the other $S(-a, D)$ and we get the value distribution. In other words, we can compute $S(a, D)$ and $S(-a, D)$ with a fixed combination and the distribution is the same with the other combination, too. We will illustrate these concepts in the next section.

Before that, let us show how the imaginary parts are related to each other modulo p . Note that, for each $S(a, D)$, in the needed $\text{Im} G(\chi^{\frac{N}{D} p^i})$ the power of q is fixed and only the power of p varies.

Theorem 7. For a fixed t , let $G(\chi^{\frac{N}{D}}) = G(\chi^{p^{u-s}q^{v-t}}) = b_s + c_s\sqrt{-q}$. Then, for $0 < s \leq u$,

$$c_s \equiv \left(\frac{p^s}{q}\right)(c_0 - c'_{s-1}) \pmod{p} \quad (19)$$

where $c'_0 = 0$ and for $0 < s < u$

$$c'_s = \frac{1}{p} \left(\left(\frac{p^s}{q}\right)c_s - (c_0 - c'_{s-1}) \right) \in \mathbb{Z}. \quad (20)$$

Proof. First we note that (19) is equivalent to finding $c'_s \in \mathbb{Z}$ satisfying (20). The real parts for $S(\varepsilon \frac{D}{q}, D)$ in Corollary 5 are

$$\operatorname{Re}(G(\chi^{p^{u-s+i}q^{v-t}})(1 + \varepsilon \left(\frac{p^i}{q}\right)\sqrt{-q})) = b_{s-i} - \varepsilon q \left(\frac{p^i}{q}\right)c_{s-i} \quad (21)$$

for $0 \leq i \leq s$. For $s = 1$ we have by (21) and Corollary 5

$$S(\varepsilon p q^{t-1}, p q^t) = \frac{\phi(q^t)}{1-q} (\phi(p)(b_1 - \varepsilon q c_1) + (b_0 - \varepsilon q \left(\frac{p}{q}\right)c_0)) + S(0, \frac{D}{q}).$$

Since $D \mid S(a, D)$,

$$0 \equiv S(p q^{t-1}, p q^t) - S(-p q^{t-1}, p q^t) = 2q^t ((p-1)c_1 + \left(\frac{p}{q}\right)c_0) \pmod{p q^t}$$

and we have $-c_1 + \left(\frac{p}{q}\right)c_0 \equiv 0 \pmod{p}$. Thus the claim holds with $s = 1$, and $c'_0 = 0$.

Assume now that $c_i \equiv \left(\frac{p^i}{q}\right)(c_0 - c'_{i-1}) \pmod{p}$ with $\left(\frac{p^i}{q}\right)c_i = c_0 - c'_{i-1} + p c'_i$ for all $1 \leq i < s$. By (21) and Corollary 5 we get again

$$\begin{aligned} 0 &\equiv S(p^s q^{t-1}, p^s q^t) - S(-p^s q^{t-1}, p^s q^t) \\ &= \frac{\phi(q^t)}{1-q} \sum_{i=0}^s \phi(p^{s-i}) (-q \left(\frac{p^i}{q}\right)c_{s-i} - q \left(\frac{p^i}{q}\right)c_{s-i}) \equiv 2q^t \sum_{i=0}^s \phi(p^i) \left(\frac{p^{s-i}}{q}\right)c_i \pmod{p^s q^t}. \end{aligned}$$

Thus

$$-\phi(p^s)c_s \equiv \sum_{i=0}^{s-1} \phi(p^i) \left(\frac{p^{s-i}}{q}\right)c_i \pmod{p^s}.$$

Here $-\phi(p^s) \equiv p^{s-1} \pmod{p^s}$ and $\left(\frac{p^{s-i}}{q}\right) = \left(\frac{p^{s+i}}{q}\right)$. Then we have by the inductive assumption

$$\begin{aligned} p^{s-1}c_s &\equiv \left(\frac{p^s}{q}\right)c_0 + \sum_{i=1}^{s-1} \phi(p^i) \left(\frac{p^s}{q}\right)(c_0 - c'_{i-1} + p c'_i) \\ &= \left(\frac{p^s}{q}\right) \left(c_0 \sum_{i=0}^{s-1} \phi(p^i) - \sum_{i=0}^{s-2} \phi(p^{i+1})c'_i + \sum_{i=1}^{s-1} \phi(p^i) p c'_i \right) \end{aligned}$$

$$= \binom{p^s}{q} (p^{s-1}c_0 + \phi(p^{s-1})pc'_{s-1}) \equiv \binom{p^s}{q} (p^{s-1}c_0 - p^{s-1}c'_{s-1}) \pmod{p^s}.$$

The claim now follows by cancelling p^{s-1} . \square

Remark 8. From Theorem 7 it clearly follows that $p \mid c_0$ if, and only if, $p \mid c_1$. Other similar equivalences or implications do not seem obvious since c'_s depends also on the quotient, not only on the remainder modulo p . For instance, $c_2 \equiv c_0 - c'_1 \pmod{p}$ with $c'_1 = \frac{\binom{p}{q}c_1 - c_0}{p}$. In order to tell how c_2 and c_0 are related modulo p we should know something about c'_1 modulo p and hence about c_0 and c_1 modulo p^2 . However, our computations indicate that either $p \mid c_s$ for every $0 \leq s \leq u$ or $p \nmid c_s$ for every $0 \leq s \leq u$, see sections 5 and 6.

Remark 9. Assume that $p \nmid c_s$ for every $s \geq 0$. Then c_0 determines, by Theorem 7, recursively the other c_s and we have only two possibilities for the signs. Hence by the discussion before Theorem 7 we can fix $\text{sgn}c_0$ e.g. to $+1$, compute $\text{sgn}c_s$, $s \geq 1$, with that and then compute the value distribution using these signs.

A Gauss sum G is said to be *pure* if $G^n \in \mathbb{R}$ for some $n \in \mathbb{Z}_+$. Evans (1) gives some sufficient conditions for Gauss sums to be pure. Setting $e = q^t$, $t \geq 1$ in his Theorem 2, we see that $G(\chi^{p^m q^{v-t}})$ can not be pure, especially this Gauss sum is not real, so $c_0 \neq 0$ in our Theorem 7. By (10, II Lemma 1), $G(\chi^{\frac{N}{p^s}}) = (-1)^{m-1} \sqrt{r} \in \mathbb{R}$. For $s, t \geq 1$, we are able to prove, using the results of (1, 9), that $G(\chi^{p^{m-s} q^{v-t}}) \in \mathbb{R}$ if, and only if, $\binom{p}{q} = 1$. The if part of the claim is also proved in (9, Theorem 3.5) with slightly different method. For completeness, we give a proof for that, too, but use a method based on (1). First, let us give one lemma.

Lemma 10. *Let $\alpha \notin \mathbb{R}$ be an element of a quadratic number field $\mathbb{Q}(\sqrt{-d})$, where $d \in \mathbb{Z}_+$, $d \notin \{1, 3\}$, is square-free. Assume that $\text{Re } \alpha \neq 0$. Then, for every $l \in \mathbb{Z}_+$, $\alpha^l \notin \mathbb{R}$.*

Proof. Assume the claim does not hold and let $l \in \mathbb{Z}_+$ be the smallest exponent such that $\alpha^l \in \mathbb{R}$. Obviously, $\alpha^l \in \mathbb{Q}$ and $l > 2$ since $\alpha \in \mathbb{Q}(\sqrt{-d})$ and $\text{Re } \alpha \neq 0$. We let $\alpha^l = a \in \mathbb{Q}$ and we will prove that $x^l - a$ is irreducible in $\mathbb{Q}[x]$. First, $4 \nmid l$, for otherwise $\alpha^{l/2} \in \mathbb{R}$ or $\text{Re } \alpha^{l/2} = 0$. The first contradicts the minimality of l and the latter would imply $\text{Re}(b + c\sqrt{-d})^2 = 0$, where $b + c\sqrt{-d} = \alpha^{l/4}$. Then $b^2 - dc^2 = 0$ giving $d = 1$.

Since $4 \nmid l$, (6, Theorem 16) tells that $x^l - a$ is irreducible in $\mathbb{Q}[x]$ if, and only if, a is not a λ th power in \mathbb{Q} for any prime λ dividing l . Suppose a is a λ th power in \mathbb{Q} for some prime $\lambda \mid l$. If $\lambda = 2$ then $\alpha^{l/2} \in \mathbb{Q}$, a contradiction. If λ is odd then $\alpha^{l/\lambda} = \zeta \sqrt[\lambda]{a}$

where $\sqrt[\lambda]{a} \in \mathbb{Q}$ and $\zeta \notin \mathbb{R}$ is a (primitive) λ th root of unity. Then ζ and $\alpha^{1/\lambda}$ determine the same number field. Since the degrees of $\mathbb{Q}(\zeta)$ and $\mathbb{Q}(\alpha^{1/\lambda}) = \mathbb{Q}(\sqrt{-d})$ over \mathbb{Q} are $\lambda - 1$ and 2 , this contradicts $d \notin \{1, 3\}$.

Thus $x^l - a$ is irreducible and $\mathbb{Q}(\alpha)$ has degree l over \mathbb{Q} . But this is not possible since $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-d})$ and $l \geq 3$. \square

Clearly the restrictions $d \notin \{1, 3\}$, $\operatorname{Re} \alpha \neq 0$, in the above lemma are necessary, as $(1+i)^4 = -4$, $(-1 + \sqrt{-3})^3 = 8$, and $(\sqrt{-d})^2 = -d$. Lemma 10 could also be proved using (13, Theorem 3.11), which gives the degree of $\tan(\frac{k\pi}{l})$ over \mathbb{Q} . The connection to the tangent function follows from the fact that if $(b + c\sqrt{-d})^l \in \mathbb{R}$ then $\tan(\frac{k\pi}{l}) = \frac{c\sqrt{-d}}{b}$ for some $k \in \mathbb{Z}$.

Theorem 11. *Let $s, t \geq 1$. Then $G(\chi^{p^{u-s}q^{v-t}}) \in \mathbb{R}$ if, and only if, $(\frac{p}{q}) = 1$. Moreover, if $(\frac{p}{q}) = -1$, then these Gauss sums can not be pure.*

Proof. Let first $(\frac{p}{q}) = 1$. This part of the claim is also proven in (9, Theorem 3.5) but we use here a method based on (1). Take $e = p^s q^t$ in the equation (22) of Theorem 3 in (1), which then says that $p \in \langle 2 \rangle \subseteq \mathbb{Z}_{q^t}$ implies that $G(\chi^{\frac{N}{D}})$ is pure.

As argued in the proof of Lemma 3, 2 is the square of a primitive root modulo q^t , hence $\langle 2 \rangle$ is the subgroup of squares in \mathbb{Z}_{q^t} and $p \in \langle 2 \rangle$ is equivalent to p being a square modulo q^t . This holds if, and only if, p is a square modulo q , which is seen as follows.

Let $m \geq 1$, and let $p \equiv a^2 \pmod{q^m}$ for some a . Then $a^2 = kq^m + p$, $k \in \mathbb{Z}$. As $\gcd(2a, q) = 1$, we find $l \in \mathbb{Z}$ such that $2al = -k$ in \mathbb{Z}_q . Then

$$(a + lq^m)^2 = a^2 + 2alq^m + l^2q^{2m} \equiv a^2 - kq^m = p \pmod{q^{m+1}},$$

hence p is a square modulo q^{m+1} . By induction p is a square modulo every q^t . The converse is clear.

By the above, if p is a square modulo q , i.e. if $(\frac{p}{q}) = 1$, then $G(\chi^{\frac{N}{D}})$ is pure for $D = p^s q^t$. As the characteristic is 2 the pureness and (1, Lemma 6) imply $G(\chi^{\frac{N}{D}})^2 = r > 0$, so $G(\chi^{\frac{N}{D}}) \in \mathbb{R}$. Hence we have the claim for $(\frac{p}{q}) = 1$.

If $(\frac{p}{q}) = -1$ then (9, Theorem 3.5 and Proposition 3.4) give

$$G(\chi^{\frac{N}{D}}) = 2^{\frac{\phi(N)}{4} - \frac{hN}{D}} (b + c\omega)^{\frac{2N}{D}},$$

where h is the class number of $\mathbb{Q}(\sqrt{-q})$, $\omega = (-1 + \sqrt{-q})/2$ and the integers b and c satisfy $2 \nmid c$, $c > 0$,

$$b^2 - bc + \frac{q+1}{4}c^2 = 2^h, \quad \text{and} \quad \frac{2b-c}{2} \equiv -2^{\frac{\phi(N)}{4} + \frac{h}{2}} \pmod{q}.$$

Here $b + c\omega = \frac{2b-c}{2} + \frac{c}{2}\sqrt{-q}$. Using $c > 0$ and the congruence for b and c we see that the real and imaginary parts of $b + c\omega$ are both non-zero. Lemma 10 and $\frac{\phi(N)}{4} - \frac{hN}{D} \in \mathbb{Z}$ now imply that neither $G(\chi^{\frac{N}{D}})$ nor any of its powers can be real. This completes the proof. \square

Viewing Theorem 11 in light of (17) and (18) (recall that $c = 0$ in (18) if, and only if, $h_m = m\phi(N)/4$) we see that if $\left(\frac{D}{q}\right) = 1$ then $S_2\left(\frac{2^{m\phi(N)/2}-1}{D}\right) = \frac{m\phi(N)}{4}$ for every $m \geq 1$ and $1 \leq s \leq u$, which is a nice arithmetic result.

5 Examples

In this section we give numerical examples illustrating the use of (16) and Theorems 4 and 7. Determining $\text{sgn Im } G(\chi^{\frac{N}{D}})$ for the needed Gauss sums will be crucial in our task to compute the value distribution of $S(a, D)$. Fortunately, Theorem 7 gives us enough information for most N .

In the index 2 cases I and II the only instances for which we need an imaginary part are, by (7), $S(\varepsilon q^{t-1}, q^t)$ in case I and, by (8), $S(\varepsilon D/pq, D)$ in case II. The other $S(a', D')$ needed to compute these $S(a, D)$ do not fall into the same category, so only one imaginary part is needed. Hence we have only two possibilities for each particular value $S(a, D)$ of which one equals $S(a, D)$ and the other $S(-a, D)$.

The case III is different since now we need several $\text{Im } G(\chi^j)$ for $S(\varepsilon D/q, D)$ and $S(\varepsilon D/pq, D)$. In accordance with the discussion preceding Theorem 7 the crucial step is to limit the possible combinations of $\text{sgn Im } G(\chi^{\frac{N}{D} p^i})$, $i = 0, \dots, s$, to two. We have found three different ways these Gauss sums can turn out:

- $c_s = 0$ for all $1 \leq s \leq u$ in Theorem 7, call this *the real case* (for N and t);
- $p \nmid c_s$ for all $0 \leq s \leq u$ in Theorem 7, call this *the irreducible case* (for N and t);
- $c_s \neq 0$ and $p \mid c_s$, for all $0 \leq s \leq u$ in Theorem 7, call this *the reducible case* (for N and t).

Except for some reducible cases, we are able to determine the value distribution completely. Let us start with the real case, which holds, by Theorem 11, if, and only if, $\left(\frac{p}{q}\right) = 1$. Then the Gauss sums are real for $s \geq 1$, they are known exactly and the only ambiguity is about $\text{sgn Im } G(\chi^{p^u q^{v-t}})$. Thus we have only two possibilities for the signs and the value distribution of $S(a, D)$ is known from the discussion preceding Theorem 7. This situation is illustrated in the following example.

Example 12. Let $N = 11 \cdot 7$ and $m = 1$. Then we have index 2 case III with $p = 11$ and $q = 7$, and $\left(\frac{11}{7}\right) = 1$. Now $\phi(N)/2 = 30$, $r = 2^{30} = 1073741824$, and $n = 13944699$. As noted at the beginning of section 4 we now need the Gauss sums $G(\chi^{\frac{N}{D}})$ with $D = 7$ and $D = N = 77$, i.e. $G(\chi^{11})$ and $G(\chi)$. With $D = 77$ (for $G(\chi)$) the equation (17) yields

$$h_1 = \min \left\{ S_2\left(\frac{2^{30}-1}{77}\right), 30 - S_2\left(\frac{2^{30}-1}{77}\right) \right\} = \min \left\{ S_2(n), 30 - S_2(n) \right\} = 15 = \frac{\phi(N)}{4}$$

giving $G(\chi) = \pm 2^{15} \in \mathbb{R}$. The latter congruence of Theorem 6 now gives $G(\chi) = 2^{15}$.

With $D = 7$ (for $G(\chi^{11})$) we similarly get

$$\begin{aligned} h_1 &= \min \left\{ S_2\left(\frac{2^{30}-1}{7}\right), 30 - S_2\left(\frac{2^{30}-1}{7}\right) \right\} \\ &= \min \left\{ S_2\left(\frac{(2^3)^{10}-1}{2^3-1}\right), 30 - S_2\left(\frac{(2^3)^{10}-1}{2^3-1}\right) \right\} = 10 \end{aligned}$$

and the equation (18) becomes $b^2 + 7c^2 = 2^{30-2 \cdot 10+2} = 2^{12}$, yielding $b = \pm 57$ and $c = \pm 11$. The former congruence in Theorem 6 now tells that $b = -57$ and Remark 9 that we may assume $c = 11$. Hence $G(\chi^{11}) = 2^9(-57 + 11\sqrt{-7})$.

Using the above results equation (15) gives

$$\begin{aligned} S(0, 7) &= 6\operatorname{Re}G(\chi^{11}) - 1 = -171 \cdot 2^{10} - 1, \\ S(\varepsilon, 7) &= -\operatorname{Re}(G(\chi^{11})(1 + \varepsilon\sqrt{-7})) - 1 = -2^9(-57 - 77\varepsilon) - 1 \\ &\in \{67, -10\} \cdot 2^{10} - 1, \end{aligned}$$

where the value for $\varepsilon = 1$ is presented first. We will use the same order in the following too. As $G(\chi) = 2^{15} \in \mathbb{R}$, $\operatorname{Re}(G(\chi)c(\pm\varepsilon)) = 2^{15}$ and the only ambiguity in $S(\varepsilon 11, 77)$ and $S(\varepsilon, 77)$ comes from $S(\pm 1, 7)$. Equations (16) and (14), Theorem 4 and the above formulae for $S(a, 7)$ now give

$$\begin{aligned} S(0, 77) &= \phi(77)\operatorname{Re}G(\chi) + S(0, 7) + S(0, 11) - S(0, 1) \\ &= 60 \cdot 2^{15} - 171 \cdot 2^{10} + 10 \cdot 2^{15} - 1 = 2069 \cdot 2^{10} - 1, \\ S(\varepsilon, 77) &= \operatorname{Re}(G(\chi)(1 + \varepsilon\sqrt{-7})) + S(\varepsilon, 7) + S(1, 11) - S(0, 1) = S(\varepsilon, 7), \\ S(\varepsilon 11, 77) &= -10\operatorname{Re}(G(\chi)(1 + \varepsilon\sqrt{-7})) + S(\varepsilon, 7) + S(0, 11) - S(0, 1) = S(\varepsilon, 7), \\ S(7, 77) &= -6\operatorname{Re}G(\chi) + S(0, 7) + S(1, 11) - S(0, 1) \\ &= -6 \cdot 2^{15} - 171 \cdot 2^{10} - 2^{15} - 1 = -395 \cdot 2^{10} - 1. \end{aligned}$$

Each value $S(a, N)$ appears $\frac{r-1}{N}|C_a^N| = n|C_a^N|$ times and Lemma 2 gives $|C_\varepsilon^{77}| = \phi(77)/2 = 30$, $|C_{\varepsilon 11}^{77}| = \phi(7)/2 = 3$ and $|C_7^{77}| = \phi(11) = 10$. The weights in $C_{77}(n)^\perp$ are then obtained from (2) and each $S(a, N)$ corresponds to $|\ker \Psi| = 1$ codeword with Ψ as in (3). The results are summarized in Table 1, where ‘‘F’’ denotes the frequency of the given value of $S(a, D)$ and the given weight. The sums $S(a, D)$ correspond to the non-zero words, so only they are listed ($\mathbf{0}$ corresponds to $\sum_{x \in \mathbb{F}^*} e(0 \cdot x^D)$).

Table 1. The value distribution of $S(a, 77)$ and the weight distribution of $C_{77}(n)^\perp$ for $N = 11 \cdot 7$ and $m = 1$.

| $S(a, 77)$ | $C_{77}(n)^\perp$ | F/n |
|-------------------------|--------------------------------------|---------------|
| $-395 \cdot 2^{10} - 1$ | $2^9 \cdot \frac{2^{20} + 395}{77}$ | 10 |
| $-10 \cdot 2^{10} - 1$ | $2^{10} \cdot \frac{2^{19} + 5}{77}$ | $30 + 3 = 33$ |
| $67 \cdot 2^{10} - 1$ | $2^9 \cdot \frac{2^{20} - 67}{77}$ | $30 + 3 = 33$ |
| $2069 \cdot 2^{10} - 1$ | $2^9 \cdot \frac{2^{20} - 2069}{77}$ | 1 |

In this example we saw that $S(\varepsilon, 77) = S(\varepsilon 11, 77) = S(\varepsilon, 7)$. This is no coincidence, for if $N = pq$ and $G(\chi) \in \mathbb{R}$ then

$$(-1)^{m-1} \equiv \operatorname{Re} G(\chi) = |G(\chi)| \operatorname{sgn} G(\chi) = 2^{\phi(N)/4} \operatorname{sgn} G(\chi) \equiv \operatorname{sgn} G(\chi) \pmod{q}$$

by Theorem 6 and since $\frac{q-1}{2} \mid \frac{\phi(N)}{4}$. Hence $G(\chi) = (-1)^{m-1} \sqrt{r}$. By (14), $S(0, p) = (p-1)G(\chi) - 1$ and $S(1, p) = -G(\chi) - 1$. Substituting these into (16) and Theorem 4 and remembering that $S(0, 1) = -1$ we see that from $S(\varepsilon, pq)$, resp. $S(\varepsilon p, pq)$, cancels out everything but $S(\varepsilon, q)$, resp. $S(\varepsilon \frac{p}{q}, q)$. Especially, if $\frac{p}{q} = 1$ then by the above and Theorem 11 $S(\varepsilon, pq) = S(\varepsilon p, pq) = S(\varepsilon, q)$.

Let us next consider the irreducible case. Now the congruences of Theorem 7, together with $\operatorname{sgn} \operatorname{Im} G(\chi^{p^u q^{v-t}})$, determine recursively $\operatorname{sgn} \operatorname{Im} G(\chi^{p^{u-i} q^{v-t}})$ for $1 \leq i \leq s$, as noted in Remark 9. Thus there are only two possible sequences of the signs and again the value distribution can be computed. If $m = 1$ gives the irreducible case for N and t then the Davenport-Hasse identity can be used to compute the Gauss sums for other m , too. Denote $\chi_m = \chi$ and $G_m(\chi_m^{N/D}) = G(\chi^{N/D})$ and let $\chi_m = \chi_1 \circ \operatorname{Norm}$ and $G_1(\chi_1^{N/D})$ be the corresponding character and Gauss sum over $\mathbb{F}_{2^{\phi(N)/2}}$, where Norm is the norm from \mathbb{F} onto $\mathbb{F}_{2^{\phi(N)/2}}$. Then the Davenport-Hasse identity tells that

$$G_m(\chi_m^{N/D}) = -(-G_1(\chi_1^{N/D}))^m \quad (22)$$

and we have the required Gauss sums over $\mathbb{F}_{2^{m\phi(N)/2}}$. The following example shows one case when $m = 1$ gives an irreducible case and illustrates the above method to compute the Gauss sums for $m = 2$.

Example 13. Let $N = 21 = 3 \cdot 7$ and $m = 1$, so that index 2 case III holds with $p = 3$ and $q = 7$. Now $\phi(N)/2 = 6$, $r = 2^6 = 64$, and $n = \frac{63}{21} = 3$. Although the code $C_N(n) =$

$C_{21}(3)$ that $S(a, N)$ is now connected to is not interesting (as the length n is 3) these parameters make a fine example of our techniques.

The computation proceeds as in the previous example. Now we need the Gauss sums $G(\chi)$ and $G(\chi^3)$. For $G(\chi)$, by (17),

$$h_1 = \min\{S_2(3), 6 - S_2(3)\} = 2.$$

Equation (18) becomes now $b^2 + 7c^2 = 2^{6-2 \cdot 2+2} = 2^4$ and gives $b = \pm 3$ and $c = \pm 1$, thus $G(\chi) = 2(\pm 3 \pm \sqrt{-7})$. Similarly, for $D = 7$, $h_1 = \min\{S_2(9), 6 - S_2(9)\} = 2$ yielding same equation as above. Thus $G(\chi^3) = 2(\pm 3 \pm \sqrt{-7})$.

Theorem 6 gives $\text{Re } G(\chi) = 2 \cdot (-3) = -6$ (the second congruence with $D = 3 \cdot 7$) and $\text{Re } G(\chi^3) = 6$ (the first congruence with $D = 7$). Now the irreducible case holds and we can use the congruences of Theorem 7. With those we get $c_1 \equiv (\frac{2}{7})c_0 \pmod{3}$, so $c_1 = -c_0$. By Remark 9, we may assume $\text{sgn } c_0 = +1$ and $G(\chi^3) = 2(3 + \sqrt{-7})$ and $G(\chi) = 2(-3 - \sqrt{-7})$.

From (15) we see that

$$\begin{aligned} S(0, 7) &= 6 \text{Re } G(\chi^3) + S(0, 1) = 6 \cdot 6 - 1 = 35, \\ S(\varepsilon, 7) &= -\text{Re}(G(\chi^3)(1 + \varepsilon\sqrt{-7})) - 1 = -2(3 - 7\varepsilon) - 1 \in \{7, -21\}, \end{aligned}$$

where the value for $\varepsilon = 1$ is again mentioned first. Continuing as in the previous example, and using equations (16) and (14), Theorem 4 and the $S(a, 7)$ above, we get

$$\begin{aligned} S(0, 21) &= \phi(21) \text{Re } G(\chi) + S(0, 7) + S(0, 3) - S(0, 1) \\ &= 12 \cdot (-6) + 35 + 2 \cdot 2^3 - 1 + 1 = -21, \\ S(\varepsilon, 21) &= \text{Re}(G(\chi)(1 - \varepsilon\sqrt{-7})) + S(\varepsilon, 7) + S(1, 3) - S(0, 1) \\ &\in \{2(-3 - 7) + 7, 2(-3 + 7) - 21\} - 2^3 = \{-21, -21\}, \\ S(\varepsilon 3, 21) &= -2 \text{Re}(G(\chi)(1 + \varepsilon\sqrt{-7})) + S(-\varepsilon, 7) + S(0, 3) - S(0, 1) \\ &\in \{-2 \cdot 2(-3 + 7) - 21, -2 \cdot 2(-3 - 7) + 7\} + 2 \cdot 2^3 - 1 + 1 \\ &= \{-21, 63\}, \\ S(7, 21) &= -6 \text{Re } G(\chi) + S(0, 7) + S(1, 3) - S(0, 1) \\ &= -6 \cdot (-6) + 35 - 2^3 - 1 + 1 = 63. \end{aligned}$$

Here $S(1, 21)$ and $S(-1, 21)$ happen to have the same value but this is not true in general. If we chose equal signs then we would have $S(\varepsilon, 21) \in \{7, -49\}$, and $S(\varepsilon 3, 21) \in \{35, 7\}$, which are not divisible by 21 and thus not applicable, as stated by Theorem 7.

Each $S(a, D)$ appears $\frac{r-1}{D}|C_a^D|$ times and by (4) and Lemma 2

$$\begin{aligned} |C_{\pm 1}^7| &= \frac{\phi(7)}{2} = 3, & |C_{\pm 1}^{21}| &= \frac{\phi(21)}{2} = 6, \\ |C_{\pm 3}^{21}| &= \frac{\phi(7)}{2} = 3, & |C_7^{21}| &= \phi(3) = 2. \end{aligned} \tag{23}$$

Thus $S(0, 7) = 35$ appears $\frac{2^6-1}{7} = 9$ times and $S(\varepsilon, 7) = 7$ or -21 each $9 \cdot 3 = 27$ times. Similarly for $S(a, 21)$, -21 appears $3 \cdot (1 + 2 \cdot 6 + 3) = 48$ times and 63 appears $3 \cdot (3 + 2) = 15$ times.

Using the notation of (22) we know from above that $G_1(\chi_1^3) = 2(3 + c_0\sqrt{-7}) = -G_1(\chi_1)$, where $c_0 = +1$ can be assumed for our purposes. By (22) then

$$G_m(\chi_m) = -(-G_1(\chi_1))^m = -G_1(\chi_1^3)^m = (-1)^m G_m(\chi_m^3).$$

Therefore $\text{Im } G_m(\chi_m)$ and $\text{Im } G_m(\chi_m^3)$ have the same signs if m is even and opposite signs if m is odd. For instance, with $m = 2$ we have $G_2(\chi_2^3) = 2^3(1 + 3c_0\sqrt{-7}) = G_2(\chi_2)$ where again $c_0 = +1$ can be assumed. The value distribution of $S(a, D)$ can now be computed as above. In Example 17 we will give details for this.

In the reducible case we have two or more unknown signs and Theorem 7 cannot rule out any of the combinations. If $m = 1$ leads to the irreducible case for N and t then we can use the Davenport-Hasse identity as discussed before Example 13. However, there are some pairs (p, q) such that $m = 1$ leads to the reducible case. By the next theorem then every m leads to the reducible case.

Theorem 14. *For given (N, t) , let $m_0 = m_0(N, t)$ be, if such exists, the smallest m such that we have the reducible case for N and t when we work in \mathbb{F}_r , $r = 2^{m\phi(N)/2}$. Then every multiple of m_0 gives the reducible case for N and t . For $m_0 \nmid m$ we have the irreducible case.*

Proof. Let $G_m(\chi_m^{N/D})$ and $G_1(\chi_1^{N/D})$ be as in (22). Further, for the rest of the proof let $\chi_j = \chi_1 \circ \text{Norm}$ be the lifted character to $\mathbb{F}_{2^{j\phi(N)/2}}$, where Norm is the norm from $\mathbb{F}_{2^{j\phi(N)/2}}$ onto $\mathbb{F}_{2^{\phi(N)/2}}$, and let $G_j(\chi_j^{N/D})$ be the corresponding Gauss sum over $\mathbb{F}_{2^{j\phi(N)/2}}$. Let (N, t) be given. If $m_0 \mid m$ and $G_{m_0}(\chi_{m_0}^{N/D}) = -b - c\sqrt{-q}$ with $p \mid c$ and $c \neq 0$ then by the Davenport-Hasse identity $G_m(\chi_m^{N/D}) = -(b + c\sqrt{-q})^{\frac{m}{m_0}}$ and

$$i \text{Im } G_m(\chi_m^{N/D}) = - \sum_{\substack{i=1 \\ i \text{ odd}}}^{m/m_0} \binom{m/m_0}{i} b^{\frac{m}{m_0}-i} (c\sqrt{-q})^i.$$

Hence $p \mid \text{Im} G_m(\chi_m^{N/D})/\sqrt{q}$. If $G_m(\chi_m^{N/D}) \in \mathbb{R}$ then (1, Lemma 6) yields $G_{m_0}(\chi_{m_0}^{N/D}) \in \mathbb{R}$ contradicting $c \neq 0$. Thus $\text{Im} G_m(\chi_m^{N/D}) \neq 0$, and we have another reducible case. If $m_0 \nmid m$ then $m = m_1 m_0 + m_2$ with $1 \leq m_2 < m_0$. By the above and the minimality of m_0

$$\begin{aligned} -(-G_1(\chi_1^{N/D}))^{m_1 m_0} &= G_{m_0 m_1}(\chi_{m_0 m_1}^{N/D}) = b_1 + c_1 \sqrt{-q} \quad \text{and} \\ (-G_1(\chi_1^{N/D}))^{m_2} &= -G_{m_2}(\chi_{m_2}^{N/D}) = b_2 + c_2 \sqrt{-q} \end{aligned}$$

for some b_i and c_i with $p \mid c_1$ and $p \nmid c_2$. Here p cannot divide both b_1 and c_1 (otherwise $p \mid 2$, see (18)). Now

$$\begin{aligned} G_m(\chi_m^{N/D}) &= -(-G_1(\chi_1^{N/D}))^{m_1 m_0} (-G_1(\chi_1^{N/D}))^{m_2} = (b_1 + c_1 \sqrt{-q})(b_2 + c_2 \sqrt{-q}) \\ &= b_1 b_2 - q c_1 c_2 + (b_1 c_2 + b_2 c_1) \sqrt{-q}, \end{aligned}$$

where $p \nmid (b_1 c_2 + b_2 c_1)$, and the last claim follows. \square

According to our computations (see section 6 for more details) 12 of the 1240 pairs with $p, q < 2000$ and $\phi(pq)/2 \leq 60000$ in case III have $m_0 = 1$ in the previous theorem. These pairs are

$$\begin{aligned} (5, q) \quad \text{with } q \in \{103, 487, 503, 607, 823, 967, 1543, 1607, 1823\}, \\ (13, 359), \quad (29, 1759) \quad \text{and} \quad (149, 311). \end{aligned} \tag{24}$$

In these cases the codes $C_N(n)$ may appear useful in determining the correct value distribution of $S(a, D)$. All of the above pairs give very large numbers to handle, so we will demonstrate the technique with $N = 21$ and $m = 2$. At the end of Example 13 we already computed the Gauss sums involved in $S(a, D)$, but in Example 17 we use the following method that avoids the Davenport-Hasse identity. We begin by quoting a result from (11) that connects the weight distribution of $C_N(n)$ to the power moments of Gaussian periods. Let

$$s_N(\alpha) := \sum_{i=0}^{n-1} e(\alpha \gamma^{iN})$$

denote the Gaussian periods and

$$M_j(N) := \sum_{i=0}^{N-1} (s_N(\gamma^i))^j, \quad j \geq 0, \tag{25}$$

their power moments. Note that since γ^N is an n th root of unity, $N s_N(\gamma^a) = S(a, N)$. Let also $\left\{ \begin{smallmatrix} a \\ b \end{smallmatrix} \right\} = \frac{1}{b!} \sum_{j=0}^b (-1)^{b-j} \binom{b}{j} j^a$ be the Stirling number of the second kind. It is

well known, see e.g. (5, p. 66), that $\left\{ \begin{smallmatrix} a \\ b \end{smallmatrix} \right\}$ reveals the number of ways a set of a elements can be partitioned into b disjoint nonempty subsets. By (11, Theorem 3) we have the following recursion.

Proposition 15. For $h \geq 0$ the number A_h of codewords of weight h in $C_N(n)$ can be calculated by the recursion $A_0 = 1$, and

$$h!A_h = \frac{1}{r} \sum_{j=0}^h (-1)^{h+j} \binom{h}{j} n^{h-j+1} M_j(N) - \sum_{j=0}^{h-1} (-1)^{h+j} A_j \sum_{i=j}^h i! \left\{ \begin{smallmatrix} h \\ i \end{smallmatrix} \right\} 2^{h-i} \binom{n-j}{n-i}.$$

Especially, the following corollary holds.

Corollary 16. $M_0(N) = N$, $M_1(N) = -1$, $M_2(N) = r - n$, and

$$A_3 = \frac{n}{6r} (M_3(N) + n^2). \quad (26)$$

Proof. Equation (26) is (11, Theorem 1). The formula for $M_0(N)$ is clear and

$$M_1(N) = \sum_{i=0}^{N-1} \sum_{k=0}^{n-1} e(\gamma^{i+kN}) = \sum_{x \in \mathbb{F}^*} e(x) = -1.$$

If there were a codeword with weight 1 or 2 in $C_N(n)$ then by the definition of $C_N(n)$ (see (1)) there would be $0 \leq i < j < n$ such that

$$\gamma^{iN} = 0 \quad \text{or} \quad \gamma^{iN} + \gamma^{jN} = 0.$$

Both contradict the fact that γ is a primitive element of \mathbb{F} . Hence substituting these $M_0(N)$, $M_1(N)$ and $A_1 = A_2 = 0$ into Proposition 15 gives with $h = 2$

$$\begin{aligned} 0 &= \frac{1}{r} (n^3 N - 2n^2 \cdot (-1) + nM_2(N)) - (\left\{ \begin{smallmatrix} 2 \\ 0 \end{smallmatrix} \right\} \cdot 2^2 + \left\{ \begin{smallmatrix} 2 \\ 1 \end{smallmatrix} \right\} \cdot 2 \cdot \binom{n}{n-1} + 2 \cdot \left\{ \begin{smallmatrix} 2 \\ 2 \end{smallmatrix} \right\} \cdot \binom{n}{n-2}) \\ &= \frac{n}{r} (n(r-1) + 2n + M_2(N)) - 2n - 2 \cdot \frac{n(n-1)}{2} \\ &= \frac{n}{r} (n(r+1) + M_2(N)) - n - n^2. \end{aligned}$$

Thus $\frac{1}{r} (n(r+1) + M_2(N)) = 1 + n$ yielding

$$M_2(N) = r + rn - nr - n = r - n$$

as claimed. □

The following example illustrates the use of Corollary 16.

Example 17. As in Example 13, let $N = 21 = 3 \cdot 7$, take $m = 2$, and proceed without the Davenport-Hasse identity. Now $\phi(N)/2 = 6$, $r = 2^{12} = 4096$, and $n = \frac{4095}{21} = 195$. Following the lines of Examples 13 and 12 we start by computing $G(\chi)$ and $G(\chi^3)$. In Example 13 we saw that $h_1 = 2$ for $D = 21$ and $D = 7$. Hence the Diophantine equation in (18) becomes $b^2 + 7c^2 = 2^{2(6-2 \cdot 2)+2} = 2^6$ for both $D = 21$ and $D = 7$. Now $m = 2$ is even and the congruences in Theorem 6 are the same. Hence $G(\chi)$ and $G(\chi^3)$ are $2^3(-1 \pm 3\sqrt{-7})$ but possibly with different signs of the imaginary parts.

Here $3 \mid \text{Im}G(\chi^{3^i})$ for $i = 0, 1$, so we have the reducible case and Theorem 7 becomes trivial. To apply Corollary 16 for the code $C_N(n) = C_{21}(195)$ we first compute the two possible distributions. From (15) we get

$$S(0,7) = 6\text{Re}G(\chi^3) - 1 = -49,$$

$$S(\varepsilon,7) = -\text{Re}(G(\chi^3)(1 + \varepsilon\sqrt{-7})) - 1 = \begin{cases} 11 \cdot 2^4 - 1 & \text{if } \text{sgn} \text{Im} G(\chi^3) = \varepsilon, \\ -10 \cdot 2^4 - 1 & \text{if } \text{sgn} \text{Im} G(\chi^3) \neq \varepsilon. \end{cases}$$

In the following the values of $S(1,21)$, respectively $S(3,21)$, are presented assuming the signs ($\text{sgn} \text{Im} G(\chi), \text{sgn} \text{Im} G(\chi^3)$) in the order $(+, +)$, $(+, -)$, $(-, +)$, $(-, -)$. By equations (16) and (14), Theorem 4, and $S(0,1) = -1$ we obtain

$$\begin{aligned} S(0,21) &= \phi(21) \text{Re} G(\chi) + S(0,7) + S(0,3) - S(0,1) \\ &= 12(-2^3) - 49 - 2 \cdot 2^6 = -273, \\ S(1,21) &= \text{Re}(G(\chi)(1 - \sqrt{-7})) + S(1,7) + S(1,3) - S(0,1) \\ &= \begin{cases} 2^3(-1 + 21) & \text{if } \text{sgn} \text{Im} G(\chi) = 1, \\ 2^3(-1 - 21) & \text{if } \text{sgn} \text{Im} G(\chi) = -1 \end{cases} \\ &\quad + \begin{cases} 11 \cdot 2^4 - 1 & \text{if } \text{sgn} \text{Im} G(\chi^3) = 1, \\ -10 \cdot 2^4 - 1 & \text{if } \text{sgn} \text{Im} G(\chi^3) = -1 \end{cases} + 2^6 \\ &\in \{21, 0, 0, -21\} \cdot 2^4 + 2^6 - 1 = \{399, 63, 63, -273\}, \\ S(3,21) &= -2\text{Re}(G(\chi)(1 + \sqrt{-7})) + S(-1,7) + S(0,3) - S(0,1) \\ &= -2 \cdot \begin{cases} 2^3(-1 - 21) & \text{if } \text{sgn} \text{Im} G(\chi) = 1, \\ 2^3(-1 + 21) & \text{if } \text{sgn} \text{Im} G(\chi) = -1 \end{cases} \\ &\quad + \begin{cases} -10 \cdot 2^4 - 1 & \text{if } \text{sgn} \text{Im} G(\chi^3) = 1, \\ 11 \cdot 2^4 - 1 & \text{if } \text{sgn} \text{Im} G(\chi^3) = -1 \end{cases} - 2 \cdot 2^6 \end{aligned}$$

$$\in \{192, 528, -480, -144\} - 2 \cdot 2^6 - 1 = \{63, 399, -609, -273\},$$

$$S(7, 21) = -6\text{Re}G(\chi) + S(0, 7) + S(1, 3) - S(0, 1) = -6(-2^3) - 49 + 2^6 = 63.$$

According to the discussion preceding Theorem 7 we obtain $S(-1, 21)$ with a given combination (\pm, \pm) by changing both signs and computing $S(1, 21)$ with those signs. Similarly, we get $S(-3, 21)$, hence

$$S(-1, 21) \in \{-273, 63, 63, 399\}, \quad S(-3, 21) \in \{-273, -609, 399, 63\},$$

assuming the same order as above for the pairs of signs.

Note that every possible value above for any $S(a, 21)$ is divisible by 21, as they should be, so this divisibility condition does not tell which sign combination is the correct one. In this case, however, we can make the required distinction by using the equation (26). For this we need the 3rd power moment of the Gaussian periods $s_{21}(\alpha) = \frac{1}{21}S(a, 21)$. The frequencies of the values of $S(a, 21)$ are $\frac{r-1}{N}|C_a^N| = n|C_a^N|$ with $|C_a^N|$ as in (23) since N is same as there. Table 2 shows the value distribution of $S(a, 21)$ assuming the same and opposite signs for $\text{Im}G(\chi)$ and $\text{Im}G(\chi^3)$. As in Table 1 the ‘‘F’’ denotes the frequency of the given value of $S(a, N)$.

Table 2. The possible value distributions of $S(a, N)$ for $N = 3 \cdot 7$ and $m = 2$.

| same signs | | opposite signs | |
|------------|----------------|----------------|----------------|
| $S(a, N)$ | F/n | $S(a, N)$ | F/n |
| -273 | 1 + 6 + 3 = 10 | -609 | 3 |
| 63 | 3 + 2 = 5 | -273 | 1 |
| 399 | 6 | 63 | 2 · 6 + 2 = 14 |
| | | 399 | 3 |

As $Ns_N(\gamma^a) = S(a, N)$ and for every $i = 0, \dots, N - 1$ we find n elements α such that $s_N(\alpha) = s_N(\gamma^i)$ in (25), we have

$$M_j(N) = \frac{1}{n} \sum_{a=0}^{r-1} \left(\frac{S(a, N)}{N} \right)^j. \quad (27)$$

Substituting the possible distributions for $S(a, N)$ from Table 2, $M_3(N)$ becomes for the

same signs

$$\begin{aligned} M_3(N) &= M_3(21) = 10 \cdot \left(\frac{-273}{21}\right)^3 + 5 \cdot \left(\frac{63}{21}\right)^3 + 6 \cdot \left(\frac{399}{21}\right)^3 \\ &= -10 \cdot 13^3 + 5 \cdot 3^3 + 6 \cdot 19^3 = 19319 \end{aligned}$$

and for opposite signs

$$\begin{aligned} M_3(N) &= 3 \cdot \left(\frac{-609}{21}\right)^3 + \left(\frac{-273}{21}\right)^3 + 14 \cdot \left(\frac{63}{21}\right)^3 + 3 \cdot \left(\frac{399}{21}\right)^3 \\ &= -3 \cdot 29^3 - 13^3 + 14 \cdot 3^3 + 3 \cdot 19^3 = -54409. \end{aligned}$$

Equation (26) now gives the number of words in $C_N(n) = C_{21}(195)$ having weight 3:

$$A_3 = \frac{195}{6 \cdot 2^{12}}(19319 + 195^2) = 455, \quad A_3 = \frac{195}{6 \cdot 2^{12}}(-54409 + 195^2) = -130$$

for the same and opposite signs, respectively. Opposite signs give a negative number, so we must have $\text{sgn Im } G(\chi) = \text{sgn Im } G(\chi^3)$. Equation (2) can now be used to compute the weight distribution of $C_{21}(195)^\perp$. The non-zero weights are

$$\frac{1}{2}(195 + \frac{273}{21}) = 104, \quad \frac{1}{2}(195 - \frac{63}{21}) = 96, \quad \frac{1}{2}(195 - \frac{399}{21}) = 88$$

with respective frequencies of $10n$, $5n$ and $6n$ ($|\ker \Psi| = 1$ for Ψ in (3)). These results are in accordance with the tables in (8).

We really need the codes $C_N(n)$, or some method other than the Davenport-Hasse identity, only for those N which have $m_0 = 1$ in Theorem 14. Unfortunately, among these there are cases when the code $C_N(n)$ does not help us. One such case is $N = 5 \cdot 103$, which corresponds to the smallest pair in (24). Then $m = 1$ leads to the reducible case, $r = 2^{204} \approx 2.6 \cdot 10^{61}$ and $n \approx 5.0 \cdot 10^{58}$. Now Corollary 16 gives positive integers for A_3 , whether the imaginary parts have the same or opposite signs. For both possibilities $A_3 \approx 8.1 \cdot 10^{113}$ with the first 26 digits coinciding and M_1 and M_2 agreeing with Corollary 16.

To conclude this section, let us illustrate our results when N is not square-free. In the next example N is of the form p^2q and, in the one after that, pq^2 .

Example 18. Let $N = 5^2 \cdot 7 = 175$ and $m = 1$. Then case III holds for N , $\phi(N)/2 = 60$, $r = 2^{60}$ and $n = (2^{60} - 1)/175 \approx 6.6 \cdot 10^{15}$. To determine the value distribution of $S(a, D)$ we now need $G(\chi^{\frac{N}{D}})$ for $D = 7, 35$ and 175 , i.e. $G(\chi^{25})$, $G(\chi^5)$ and $G(\chi)$. For $G(\chi^{25})$, i.e. $D = 7$, (17) gives

$$\begin{aligned} h_1 &= \min \left\{ S_2 \left(\frac{2^{60}-1}{7} \right), 60 - S_2 \left(\frac{2^{60}-1}{7} \right) \right\} \\ &= \min \left\{ S_2 \left(\frac{(2^3)^{20}-1}{2^3-1} \right), 60 - S_2 \left(\frac{(2^3)^{20}-1}{2^3-1} \right) \right\} = 20, \end{aligned}$$

then (18) and Theorem 6 yield $b^2 + 7c^2 = 2^{60-2 \cdot 20+2} = 2^{22}$ and $G(\chi^{25}) = 2^{19}(-1201 \pm 627\sqrt{-7})$. Similarly, for $D = 35$ we get

$$h_1 = \min \left\{ S_2\left(\frac{2^{60}-1}{35}\right), 60 - S_2\left(\frac{2^{60}-1}{35}\right) \right\} = 25,$$

$b^2 + 7c^2 = 2^{60-2 \cdot 25+2} = 2^{12}$, and $G(\chi^5) = 2^{24}(57 \pm 11\sqrt{-7})$. The same way for $D = N = 175$ we have

$$h_1 = \min \left\{ S_2\left(\frac{2^{60}-1}{175}\right), 60 - S_2\left(\frac{2^{60}-1}{175}\right) \right\} = 29,$$

$b^2 + 7c^2 = 2^{60-2 \cdot 29+2} = 2^4$, and $G(\chi) = 2^{28}(-3 \pm \sqrt{-7})$.

Now the irreducible case holds, so we can use Theorem 7 to limit the combinations for the signs of these imaginary parts to two. Using the notations of the theorem and assuming again $\text{sgn } c_0 = +1$ we have $c_0 = 2^{19} \cdot 627$ from $G(\chi^{25})$, $c_1 = \pm 2^{24} \cdot 11 \equiv \pm 1 \pmod{5}$ from $G(\chi^5)$, and $c_2 = \pm 2^{28} \equiv \pm 1 \pmod{5}$ from $G(\chi)$. By Theorem 7

$$c_1 \equiv \left(\frac{5}{7}\right) 2^{19} \cdot 627 \equiv -(3 \cdot 2) \equiv -1 \pmod{5},$$

so $\text{sgn } c_1 = -1$. Then

$$c'_1 = \frac{1}{5} \left(-\left(\frac{5}{7}\right) 2^{24} \cdot 11 - 2^{19} \cdot 627 \right) = -28835840 \equiv 0 \pmod{5}$$

and Theorem 7 gives that $c_2 \equiv \left(\frac{5^2}{7}\right) 2^{19} \cdot 627 \equiv 1 \pmod{5}$. Hence $\text{sgn } c_2 = \text{sgn } c_0 = 1$ and the signs $(+, -, +)$ can be assumed. As in the previous examples we get from (15)

$$S(0, 7) = 6 \text{Re } G(\chi^{25}) - 1 = -3603 \cdot 2^{20} - 1,$$

$$S(\varepsilon, 7) = -\text{Re}(G(\chi^{25})(1 + \varepsilon\sqrt{-7})) - 1 \in \{2795, -1594\} \cdot 2^{20} - 1,$$

where, as in Examples 13 and 12, the value for $\varepsilon = 1$ is written first. In the following we will use the same order. From equations (16) and (14) and Theorem 4 we get

$$\begin{aligned} S(0, 35) &= \phi(35) \text{Re } G(\chi^5) + S(0, 7) + S(0, 5) - S(0, 1) \\ &= 24 \cdot 2^{24} \cdot 57 - 3603 \cdot 2^{20} + 4 \cdot 2^{30} - 1 = 22381 \cdot 2^{20} - 1, \end{aligned}$$

$$\begin{aligned} S(\varepsilon, 35) &= \text{Re}(G(\chi^5)(1 - \varepsilon\sqrt{-7})) + S(\varepsilon, 7) + S(1, 5) - S(0, 1) \\ &\in 2^{24} \{57 - 77, 57 + 77\} + \{2795, -1594\} \cdot 2^{20} - 1 - 2^{30} \\ &= \{1451, -474\} \cdot 2^{20} - 1, \end{aligned}$$

$$\begin{aligned} S(\varepsilon 5, 35) &= -4 \text{Re}(G(\chi^5)(1 + \varepsilon\sqrt{-7})) + S(-\varepsilon, 7) + S(0, 5) - S(0, 1) \\ &\in -4 \cdot 2^{24} \{57 + 77, 57 - 77\} + \{-1594, 2795\} \cdot 2^{20} - 1 + 4 \cdot 2^{30} \end{aligned}$$

$$\begin{aligned}
&= \{-6074, 8171\} \cdot 2^{20} - 1, \\
S(7, 35) &= -6 \operatorname{Re}(G(\chi^5)) + S(0, 7) + S(1, 5) - S(0, 1) \\
&= -6 \cdot 2^{24} \cdot 57 - 3603 \cdot 2^{20} - 2^{30} - 1 = -10099 \cdot 2^{20} - 1.
\end{aligned}$$

Now we can proceed using again equations (16) and (14) and Theorem 4 to get $S(\varepsilon, 175) = S(\varepsilon, 35)$, $S(7, 175) = S(7, 35)$,

$$\begin{aligned}
S(0, 175) &= \phi(175) \operatorname{Re} G(\chi) + S(0, 35) + S(0, 25) - S(0, 5) \\
&= 120 \cdot 2^{28} \cdot (-3) + 22381 \cdot 2^{20} + 24 \cdot 2^{30} - 4 \cdot 2^{30} - 1 \\
&= -49299 \cdot 2^{20} - 1, \\
S(\varepsilon 5, 175) &= 5 \operatorname{Re}(G(\chi)(1 - \varepsilon\sqrt{-7})) + S(\varepsilon 5, 35) + S(5, 25) - S(0, 5) \\
&\in 5 \cdot 2^{28} \{-3 + 7, -3 - 7\} + \{-6074, 8171\} \cdot 2^{20} - 1 - 2^{30} - 4 \cdot 2^{30} \\
&= \{-6074, -9749\} \cdot 2^{20} - 1, \\
S(\varepsilon 25, 175) &= -20 \operatorname{Re}(G(\chi)(1 + \varepsilon\sqrt{-7})) + S(-\varepsilon 5, 35) + S(0, 25) - S(0, 5) \\
&\in -20 \cdot 2^{28} \{-3 - 7, -3 + 7\} \\
&\quad + \{8171, -6074\} \cdot 2^{20} - 1 + 24 \cdot 2^{30} - 4 \cdot 2^{30} \\
&= \{79851, -6074\} \cdot 2^{20} - 1, \\
S(35, 175) &= -30 \operatorname{Re}(G(\chi)) + S(0, 35) + S(5, 25) - S(0, 5) \\
&= -30 \cdot 2^{28} \cdot (-3) + 22381 \cdot 2^{20} - 2^{30} - 4 \cdot 2^{30} - 1 = 40301 \cdot 2^{20} - 1.
\end{aligned}$$

Equation (4) and Lemma 2 tell now the sizes of C_a^D , which are

$$\begin{aligned}
|C_{\pm 1}^7| &= \frac{\phi(7)}{2} = 3, & |C_{\pm 1}^{35}| &= \frac{\phi(35)}{2} = 12, & |C_{\pm 5}^{35}| &= \frac{\phi(7)}{2} = 3, \\
|C_7^{35}| &= \phi(5) = 4, & |C_{\pm 1}^{175}| &= \frac{\phi(175)}{2} = 60, & |C_{\pm 5}^{175}| &= \frac{\phi(35)}{2} = 12, \\
|C_7^{175}| &= \phi(25) = 20, & |C_{\pm 25}^{175}| &= \frac{\phi(7)}{2} = 3, & |C_{35}^{175}| &= \phi(5) = 4.
\end{aligned}$$

Combining these with the above values $S(a, D)$, we get the value distribution presented in Table 3, where $d = \frac{r-1}{D}$ for $D = 7$ and 35 .

Table 3. The value distributions of $S(a, D)$ for $N = 5^2 \cdot 7$ and $m = 1$.

| $S(a, 7)$ | F/d | $S(a, 35)$ | F/d | $S(a, 175)$ | F/n |
|--------------------------|-----|---------------------------|-----|---------------------------|---------------|
| $-3603 \cdot 2^{20} - 1$ | 1 | $-10099 \cdot 2^{20} - 1$ | 4 | $-49299 \cdot 2^{20} - 1$ | 1 |
| $-1594 \cdot 2^{20} - 1$ | 3 | $-6074 \cdot 2^{20} - 1$ | 3 | $-10099 \cdot 2^{20} - 1$ | 20 |
| $2795 \cdot 2^{20} - 1$ | 3 | $-474 \cdot 2^{20} - 1$ | 12 | $-9749 \cdot 2^{20} - 1$ | 12 |
| | | $1451 \cdot 2^{20} - 1$ | 12 | $-6074 \cdot 2^{20} - 1$ | $12 + 3 = 15$ |
| | | $8171 \cdot 2^{20} - 1$ | 3 | $-474 \cdot 2^{20} - 1$ | 60 |
| | | $22381 \cdot 2^{20} - 1$ | 1 | $1451 \cdot 2^{20} - 1$ | 60 |
| | | | | $40301 \cdot 2^{20} - 1$ | 4 |
| | | | | $79851 \cdot 2^{20} - 1$ | 3 |

Example 19. Let $N = 3 \cdot 7^2 = 147$ and $m = 1$, so that case III holds for N and $\phi(N)/2 = 42$, $r = 2^{42}$, and $n = (2^{42} - 1)/147 \approx 3.0 \cdot 10^{10}$. We now need $G(\chi^{\frac{N}{D}})$ for $D = 7, 21, 49$ and 147 , i.e. $G(\chi^{21})$, $G(\chi^7)$, $G(\chi^3)$ and $G(\chi)$. For $G(\chi^{21})$, (17) gives

$$\begin{aligned} h_1 &= \min \left\{ S_2 \left(\frac{2^{42}-1}{7} \right), 42 - S_2 \left(\frac{2^{42}-1}{7} \right) \right\} \\ &= \min \left\{ S_2 \left(\frac{(2^3)^{14}-1}{2^3-1} \right), 42 - S_2 \left(\frac{(2^3)^{14}-1}{2^3-1} \right) \right\} = 14, \end{aligned}$$

from which $G(\chi^{21}) = 2^{13}(87 \pm 91\sqrt{-7})$ by $b^2 + 7c^2 = 2^{42-2 \cdot 14+2} = 2^{16}$ and Theorem 6. For $G(\chi^7)$ we similarly get

$$h_1 = \min \left\{ S_2 \left(\frac{2^{42}-1}{21} \right), 42 - S_2 \left(\frac{2^{42}-1}{21} \right) \right\} = 14.$$

Therefore we have the same Diophantine equation as above but now Theorem 6 gives $G(\chi^7) = 2^{13}(-87 \pm 91\sqrt{-7})$. For $G(\chi^3)$ and $G(\chi)$ we have

$$h_1 = \min \left\{ S_2 \left(\frac{2^{42}-1}{49} \right), 42 - S_2 \left(\frac{2^{42}-1}{49} \right) \right\} = 20$$

and

$$h_1 = \min \left\{ S_2 \left(\frac{2^{42}-1}{147} \right), 42 - S_2 \left(\frac{2^{42}-1}{147} \right) \right\} = 20,$$

respectively. Again, the Diophantine equations are the same and $b^2 + 7c^2 = 2^{42-2 \cdot 20+2} = 2^4$ and Theorem 6 yield $G(\chi^3) = 2^{19}(3 \pm \sqrt{-7})$ and $G(\chi) = 2^{19}(-3 \pm \sqrt{-7})$.

Again, the irreducible case holds for N and t with both $t = 1, 2$, so Theorem 7 is useful. The theorem connects now $\text{sgn Im } G(\chi^{21})$ to $\text{sgn Im } G(\chi^7)$ and $\text{sgn Im } G(\chi^3)$ to $\text{sgn Im } G(\chi)$. For the first pair, $|c_0| = |c_1| = 2^{13} \cdot 91$ and Theorem 7 yields $c_1 \equiv (\frac{3}{7})c_0 = -c_0 \pmod{3}$. Hence the signs differ and, as in the previous example, we may assume by Remark 9 that $G(\chi^{21}) = 2^{13}(87 + 91\sqrt{-7})$ and $G(\chi^7) = 2^{13}(-87 - 91\sqrt{-7})$. Similarly, for $G(\chi^3)$ and $G(\chi)$, $|c_0| = |c_1| = 2^{19}$ and $c_1 \equiv (\frac{3}{7})c_0 = -c_0 \pmod{3}$. Again, the signs differ and we may assume $G(\chi^3) = 2^{19}(3 + \sqrt{-7})$ and $G(\chi) = 2^{19}(-3 - \sqrt{-7})$.

As before, (15) gives

$$\begin{aligned} S(0, 7) &= 6\text{Re } G(\chi^{21}) - 1 = 261 \cdot 2^{14} - 1, \\ S(\varepsilon, 7) &= -\text{Re } (G(\chi^{21})(1 + \varepsilon\sqrt{-7})) - 1 \in \{275, -362\} \cdot 2^{14} - 1, \\ S(0, 7^2) &= \phi(49)\text{Re } G(\chi^3) + S(0, 7) = 42 \cdot 2^{19} \cdot 3 + 261 \cdot 2^{14} - 1 = 4293 \cdot 2^{14} - 1, \\ S(\varepsilon, 7^2) &= S(\varepsilon, 7), \\ S(\varepsilon 7, 7^2) &= -7\text{Re } (G(\chi^3)(1 + \varepsilon\sqrt{-7})) + S(0, 7) \in \{1157, -1979\} \cdot 2^{14} - 1 \end{aligned}$$

with the values for $\varepsilon = 1$ shown first. The same order holds in the following. Again, equations (16) and (14) and Theorem 4 yield

$$\begin{aligned} S(0, 21) &= \phi(21)\text{Re } G(\chi^7) + S(0, 7) + S(0, 3) - S(0, 1) \\ &= 12 \cdot 2^{13} \cdot (-87) + 261 \cdot 2^{14} + 2 \cdot 2^{21} - 1 = -5 \cdot 2^{14} - 1, \\ S(\varepsilon, 21) &= \text{Re } (G(\chi^7)(1 - \varepsilon\sqrt{-7})) + S(\varepsilon, 7) + S(1, 3) - S(0, 1) \\ &\in 2^{13}\{-87 - 91 \cdot 7, -87 + 91 \cdot 7\} + \{275, -362\} \cdot 2^{14} - 2^{21} - 1 \\ &= \{-215, -215\} \cdot 2^{14} - 1, \\ S(\varepsilon 3, 21) &= -2\text{Re } (G(\chi^7)(1 + \varepsilon\sqrt{-7})) + S(-\varepsilon, 7) + S(0, 3) - S(0, 1) \\ &\in -2 \cdot 2^{13}\{-87 + 91 \cdot 7, -87 - 91 \cdot 7\} + \{-362, 275\} \cdot 2^{14} + 2 \cdot 2^{21} - 1 \\ &= \{-656, 1255\} \cdot 2^{14} - 1, \\ S(7, 21) &= -6\text{Re } (G(\chi^7)) + S(0, 7) + S(1, 3) - S(0, 1) \\ &= -6 \cdot 2^{13} \cdot (-87) + 261 \cdot 2^{14} - 2^{21} - 1 = 394 \cdot 2^{14} - 1. \end{aligned}$$

Similarly, we get $S(\varepsilon, 147) = S(\varepsilon, 21)$, $S(\varepsilon 3, 147) = S(\varepsilon 3, 21)$,

$$\begin{aligned} S(0, 147) &= \phi(147)\text{Re } G(\chi) + S(0, 49) + S(0, 21) - S(0, 7) \\ &= 84 \cdot 2^{19} \cdot (-3) + 4293 \cdot 2^{14} - 5 \cdot 2^{14} - 261 \cdot 2^{14} - 1 \\ &= -4037 \cdot 2^{14} - 1, \end{aligned}$$

$$\begin{aligned}
S(\varepsilon 7, 147) &= 7 \operatorname{Re}(G(\chi)(1 - \varepsilon\sqrt{-7})) + S(\varepsilon 7, 49) + S(7, 21) - S(0, 7) \\
&\in 7 \cdot 2^{19} \{-3 - 7, -3 + 7\} \\
&\quad + \{1157, -1979\} \cdot 2^{14} + 394 \cdot 2^{14} - 261 \cdot 2^{14} - 1 \\
&= \{-950, -950\} \cdot 2^{14} - 1,
\end{aligned}$$

$$\begin{aligned}
S(\varepsilon 21, 147) &= -14 \operatorname{Re}(G(\chi)(1 + \varepsilon\sqrt{-7})) + S(-\varepsilon 7, 49) + S(0, 21) - S(0, 7) \\
&\in -14 \cdot 2^{19} \{-3 + 7, -3 - 7\} \\
&\quad + \{-1979, 1157\} \cdot 2^{14} - 5 \cdot 2^{14} - 261 \cdot 2^{14} - 1 \\
&= \{-4037, 5371\} \cdot 2^{14} - 1,
\end{aligned}$$

$$\begin{aligned}
S(49, 147) &= -42 \operatorname{Re}(G(\chi)) + S(0, 49) + S(7, 21) - S(0, 7) \\
&= -42 \cdot 2^{19} \cdot (-3) + 4293 \cdot 2^{14} + 394 \cdot 2^{14} - 261 \cdot 2^{14} - 1 \\
&= 8458 \cdot 2^{14} - 1.
\end{aligned}$$

By (4) and Lemma 2 we have the following sizes for the cosets C_a^D :

$$\begin{aligned}
|C_{\pm 1}^7| &= \frac{\phi(7)}{2} = 3, & |C_{\pm 1}^{49}| &= \frac{\phi(49)}{2} = 21, & |C_{\pm 7}^{49}| &= \frac{\phi(7)}{2} = 3, \\
|C_{\pm 1}^{21}| &= \frac{\phi(21)}{2} = 6, & |C_{\pm 3}^{21}| &= \frac{\phi(7)}{2} = 3, & |C_7^{21}| &= \phi(3) = 2, \\
|C_{\pm 1}^{147}| &= \frac{\phi(147)}{2} = 42, & |C_{\pm 3}^{147}| &= \frac{\phi(49)}{2} = 21, & |C_{\pm 7}^{147}| &= \frac{\phi(21)}{2} = 6, \\
|C_{\pm 21}^{147}| &= \frac{\phi(7)}{2} = 3, & |C_{49}^{147}| &= \phi(3) = 2.
\end{aligned}$$

We are now able to compute the value distribution of $S(a, D)$ shown in Table 4. There $d = \frac{r-1}{D}$ for $D = 7, 49, 21$.

Table 4. The value distributions of $S(a, D)$ for $N = 3 \cdot 7^2$ and $m = 1$.

| $S(a, 7), S(a, 49)$ | F/d | $S(a, 21)$ | F/d | $S(a, 147)$ | F/n |
|--------------------------|-------|-------------------------|-------|--------------------------|-------------------|
| $-362 \cdot 2^{14} - 1$ | 3 | $-656 \cdot 2^{14} - 1$ | 3 | $-4037 \cdot 2^{14} - 1$ | 4 |
| $261 \cdot 2^{14} - 1$ | 1 | $-215 \cdot 2^{14} - 1$ | 12 | $-950 \cdot 2^{14} - 1$ | $2 \cdot 6 = 12$ |
| $275 \cdot 2^{14} - 1$ | 3 | $-5 \cdot 2^{14} - 1$ | 1 | $-656 \cdot 2^{14} - 1$ | 21 |
| $-1979 \cdot 2^{14} - 1$ | 3 | $394 \cdot 2^{14} - 1$ | 2 | $-215 \cdot 2^{14} - 1$ | $2 \cdot 42 = 84$ |
| $-362 \cdot 2^{14} - 1$ | 21 | $1255 \cdot 2^{14} - 1$ | 3 | $1255 \cdot 2^{14} - 1$ | 21 |
| $275 \cdot 2^{14} - 1$ | 21 | | | $5371 \cdot 2^{14} - 1$ | 3 |
| $1157 \cdot 2^{14} - 1$ | 3 | | | $8458 \cdot 2^{14} - 1$ | 2 |
| $4293 \cdot 2^{14} - 1$ | 1 | | | | |

6 Computer Runs

For the final part of this paper, let us present some results obtained from our computer runs in the index 2 case III. We executed the computations with Maple 9, running on a 2.66 GHz PC with 512 MB of RAM.

We checked every prime less than 2000 and found 117 primes p with $\text{ord}_p 2 = \phi(p) = p - 1$ and 61 primes q with $\text{ord}_q 2 = \phi(q)/2 = (q - 1)/2$ and $q \equiv 7 \pmod{8}$. Also, for those u and v that fit the ranges in our computations we have $\text{ord}_{p^u} 2 = \phi(p^u)$ and $\text{ord}_{q^v} 2 = \phi(q^v)/2$ with the above p and q . Since $\text{gcd}(p^u, q^v) = 1$, we have $\text{ord}_{p^u q^v} 2 = \text{lcm}(\text{ord}_{p^u} 2, \text{ord}_{q^v} 2)$. Hence, $N = p^u q^v$ is in case III if, and only if, $\text{gcd}(\phi(p^u), \phi(q^v)/2) = 1$. Among the above mentioned primes there are 5340 pairs such that pq satisfies case III, which is 75 % of all the pairs. In total there are 303 primes less than 2000.

We searched every N in case III and every m such that $m \leq 50$ and $m\phi(N)/2 \leq 60000$ with the prime factors of N less than 2000. For every such pair (m, N) we let D run through the divisors of N such that $q \mid D$, and checked whether $\text{Im}G(\chi^{\frac{N}{D}})$ is zero or not, or divisible by p . In other words, we checked whether the real or (ir)reducible case holds for N and t (recall that $D = p^s q^t$). We found that one of these cases does hold for every (m, N) . Also, the real case holds if, and only if, $\left(\frac{p}{q}\right) = 1$, as implied by Theorem 11. There are a total of 1689 numbers N in the above range and 1241 different pairs (p, q) are present in the prime factors of those N . The computation time was approximately 2 days (≈ 50 hours) in total.

For given N and t , let $m_0 = m_0(N, t)$ be 0 if the real case holds for N and t and otherwise, as in Theorem 14, the smallest m such that we have the reducible case for N and t when we work in \mathbb{F}_r , $r = 2^{m\phi(N)/2}$. By Theorem 11 $m_0 = 0$ if, and only if, $\left(\frac{p}{q}\right) = 1$. If $m_0 > 0$ then by Theorem 14 every m with $m_0 \mid m$, resp. $m_0 \nmid m$, gives the reducible, resp. the irreducible case. In addition, every N except $N = 83 \cdot 7^2$ in the checked range $m \leq 50$, $m\phi(N)/2 \leq 60000$, $p, q < 2000$, agrees with the following:

- m_0 exists for every N and $1 \leq t \leq u$,
- m_0 depends only on p and q (not on u , v or t),
- if $\left(\frac{p}{q}\right) = -1$, then $m_0 \mid \frac{p+1}{2}$ ($m_0 > 0$ by Theorem 11).

The $N = 83 \cdot 7^2$ (now $(p+1)/2 = 42$) agrees with all but the second property above. For this particular N we checked m up to m_0 and found that $m_0 = 6$ for N and $t = 1$ (i.e.

$D = 7$ or $83 \cdot 7$) and $m_0 = 42$ for N and $t = 2 = v$ (i.e. $D = 7^2$ or N).

Although they did not fit in our range, we checked $N = 83 \cdot 7^3$ and $N = 83 \cdot 7^4$. We found that, similarly for them, $m_0 = 42$ for N and $t = v$ (i.e. $D = N$ or $N/83$), and $m_0 = 6$ for N and $t < v$. Setting $v > 4$ yielded numbers and equations too big to compute. Also $N = 83 \cdot 7$ gives $m_0 = 42$ for N and $t = 1 = v$. As now $v = 1$, there are no cases $t < v$.

For the other 1240 pairs (p, q) giving index 2 case III in our range the m_0 distributes as in Table 5. There “other” means $1 < m_0 < \frac{p+1}{2}$ and “n/a” that all the computed m gave the irreducible case. In every such case our bounds for m and N did not allow m to be $\frac{p+1}{2}$, so these still agree with the existence of m_0 and the observation $m_0 \mid \frac{p+1}{2}$. Recall that $m_0 = 0$ in the real case. Also, the percentages for the different values are given.

Table 5. The distribution of m_0 .

| m_0 | 0 | 1 | $\frac{p+1}{2}$ | other | n/a |
|-------|------|-----|-----------------|-------|------|
| # | 604 | 12 | 102 | 34 | 488 |
| % | 48.7 | 1.0 | 8.2 | 2.7 | 39.3 |

We note that, even for moderate-sized p and q , the bound $m\phi(N)/2 \leq 60000$ restricts m heavily. For example, with $p = 53$, $q = 463$, and with $p \approx q \approx 160$ the largest m in this range is $m = 4$. In our range there are 1216, resp. 1236, numbers N in case III that do not allow m to be 10, resp. $(p+1)/2$. In total there are 1689 N fitting our range. Limiting ourselves to $\left(\frac{p}{q}\right) = -1$ we have 599, resp. 627, such N of 823 possible.

References

1. Evans RJ (1981) Pure gauss sums over finite fields. *Mathematika* 28: 239–248.
2. Hardy GH & Wright EM (1979) An introduction to the theory of numbers. Oxford Science Publication, 5th edition.
3. Hardy K, Muskat JB & Williams KS (1990) A deterministic algorithm for solving $n = fu^2 + gv^2$ in coprime integers u and v . *Math. Comp.* 55: 327–343.
4. Hasse H (1964) Vorlesungen über Zahlentheorie, volume 59 of *Grund. der Math. Wiss.*. Springer-Verlag, Berlin.
5. Knuth DE (1997) The art of computer programming I: fundamental algorithms. Addison-Wesley.
6. Lang S (1965) Algebra. Addison-Wesley Publishing Company, Inc.
7. Lidl R & Niederreiter H (1994) Introduction to finite fields and their applications. Cambridge Univ. Press, revised edition.
8. MacWilliams FJ & Seery J (1981) The weight distributions of some minimal cyclic codes. *IEEE Trans. Inform. Theory* 27: 796–806.
9. Mbodj OD (1998) Quadratic gauss sums. *Finite Fields Appl.* 4: 347–361.
10. Moisio M (1998) Exponential sums, gauss sums, and irreducible cyclic codes. *Acta Univ. Oulu A306* Available: <http://www.uwasa.fi/~mamo/>.
11. Moisio M, Ranto K, Rinta-aho M & Väänänen K (2006) On the weight distribution of the duals of irreducible cyclic codes, cyclic codes with two zeros and hyperkloosterman codes Submitted.
12. Moisio M & Väänänen K (1999) Two recursive algorithms for computing the weight distribution of certain irreducible cyclic codes. *IEEE Trans. Inform. Theory* 45: 1244–1249.
13. Niven I (1956) Irrational numbers. John Wiley and Sons, Inc.
14. Pless V (1963) Power moment identities on weight distributions in error correcting codes. *Inform. and Contr.* 6: 147–152.
15. van der Vlugt M (1995) Hasse-davenport curves, gauss sums, and weight distributions of irreducible cyclic codes. *J. Number Theory* 55: 145–159.

486. Halonen, Raija (2007) Challenges in an inter-organisational information system implementation. Participatory view
487. Välimäki, Panu (2007) Reproductive tactics in butterflies – the adaptive significance of monandry versus polyandry in *Pieris napi*
488. Oinas, Janne (2007) The degree theory and the index of a critical point for mappings of the type (S+)
489. Nuortila, Carolin (2007) Constraints on sexual reproduction and seed set in *Vaccinium* and *Campanula*
490. Peltoniemi, Mirva (2007) Mechanism of action of the glutaredoxins and their role in human lung diseases
491. Zheng, Xiaosong (2007) Reference modeling for high value added mobile services
492. Siira, Antti (2007) Mixed-stock exploitation of Atlantic salmon (*Salmo salar* L.) and seal-induced damage in the coastal trap-net fishery of the Gulf of Bothnia. Challenges and potential solutions
493. Donnini, Serena (2007) Computing free energies of protein-ligand association
494. Syrjänen, Anna-Liisa (2007) Lay participatory design: A way to develop information technology and activity together
495. Partanen, Sari (2007) Recent spatiotemporal changes and main determinants of aquatic macrophyte vegetation in large lakes in Finland
496. Vuoti, Sauli (2007) Syntheses and catalytic properties of palladium (II) complexes of various new aryl and aryl alkyl phosphane ligands
497. Alaviuhkola, Terhi (2007) Aromatic borate anions and thiophene derivatives for sensor applications
498. Törn, Anne (2007) Sustainability of nature-based tourism
499. Autio, Kaija (2007) Characterization of 3-hydroxyacyl-ACP dehydratase of mitochondrial fatty acid synthesis in yeast, humans and trypanosomes
500. Raunio, Janne (2008) The use of Chironomid Pupal Exuvial Technique (CPET) in freshwater biomonitoring: applications for boreal rivers and lakes
501. Paasivaara, Antti (2008) Space use, habitat selection and reproductive output of breeding common goldeneye (*Bucephala clangula*)
502. Asikkala, Janne (2008) Application of ionic liquids and microwave activation in selected organic reactions

Book orders:
OULU UNIVERSITY PRESS
P.O. Box 8200, FI-90014
University of Oulu, Finland

Distributed by
OULU UNIVERSITY LIBRARY
P.O. Box 7500, FI-90014
University of Oulu, Finland

S E R I E S E D I T O R S

A
SCIENTIAE RERUM NATURALIUM
Professor Mikko Siponen

B
HUMANIORA
Professor Harri Mantila

C
TECHNICA
Professor Hannu Heusala

D
MEDICA
Professor Olli Vuolteenaho

E
SCIENTIAE RERUM SOCIALIUM
Senior Researcher Eila Estola

E
SCRIPTA ACADEMICA
Information officer Tiina Pistokoski

G
OECONOMICA
Senior Lecturer Seppo Eriksson

EDITOR IN CHIEF
Professor Olli Vuolteenaho

EDITORIAL SECRETARY
Publications Editor Kirsti Nurkkala

ISBN 978-951-42-8736-7 (Paperback)

ISBN 978-951-42-8737-4 (PDF)

ISSN 0355-3191 (Print)

ISSN 1796-220X (Online)

