On Pure Gauss sums

by

Noboru AOKI

(Received September 30, 2012)
(Revised November 10, 2012)

1. Introduction

Throughout this paper $m$ will denote a positive integer greater than one. Let $\zeta_m$ be the $m$-th root of unity $e^{2\pi i/m}$ in the complex number field and $K = \mathbb{Q}(\zeta_m)$ the $m$-th cyclotomic field. Let $p$ be a prime number not dividing $m$. If $p$ is a prime ideal of $K$ lying above $p$ then the norm of $p$ is a power of $p$, say $q = p^f$. Then $f$ is the least positive integer such that $p^f \equiv 1 \pmod{m}$. Let $O_K$ denote the integer ring of $K$. Then the residue field $O_K/p$ is the finite field $\mathbb{F}_q$ of $q$ elements. Since $|\mathbb{F}_q^\times| = q - 1 \equiv 0 \pmod{m}$, $\mathbb{F}_q^\times$ contains a subgroup of order $m$. For any $x \in O_K \setminus p$, the $m$-th power residue symbol $\left(\frac{x}{p}\right)_m$ is by definition the $m$-th root of unity in the complex numbers uniquely determined by the congruence

$\left(\frac{x}{p}\right)_m \equiv x^{\frac{q-1}{m}} \pmod{p}$. 

We define the Gauss sum $g(m, p)$ by

$g(m, p) = \sum_{x \in \mathbb{F}_q^\times} \left(\frac{x}{p}\right)_m \zeta_p^{\text{Tr}(x)}$, \hspace{1cm} (1)

where $\text{Tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p$ denotes the trace map. (See [5] and [8] for more details on Gauss sums.)

Although Gauss sums appear in many important aspects in number theory, it is not easy in general to obtain their explicit expressions. If $m = 2$ then $K = \mathbb{Q}$ and $p = p\mathbb{Z}$, and the Gauss sum (1) is the quadratic Gauss sum

$g(2, p) = \sum_{x \in \mathbb{F}_q^\times} \left(\frac{x}{p}\right) \zeta_p^x$, 

where $\left(\frac{x}{p}\right)$ is the Legendre symbol. In this case, we know that

$g(2, p) = \sqrt{p^*}$, \hspace{1cm} (2)

where $p^* = p$ if $p \equiv 1 \pmod{4}$ and $p^* = -p$ if $p \equiv 3 \pmod{4}$. As is well known, this formula was proved by Gauss in an effort to prove the quadratic reciprocity law.
As for the case of \( m > 2 \), Stickelberger [11] proved that if \( f \) is even and \( p^{f/2} \equiv -1 \) (mod \( m \)) then

\[
g(m, p) = (-1)^{\frac{p^{f/2+1}}{m}} \sqrt{q}.
\]  

(3)

We say that \((m, p)\) is supersingular if

\[
p^v \equiv -1 \pmod{m}
\]

for some integer \( v \). 

(4)

This terminology may be justified by the fact that the Fermat varieties of degree \( m \) over \( \mathbb{F}_p \) is supersingular if Condition (4) holds (see [10]).

The Gauss sum \( g(m, p) \) is said to be pure if \( g(m, p)_k \) is a real number for some positive integer \( k \). It is known that \( g(m, p) \) is pure if and only if \( g(m, p) = \zeta \sqrt{q} \) for some root of unity \( \zeta \), whose proof will be recalled in Proposition 4.4. By abuse of terminology, we say that \((m, p)\) is pure if \( g(m, p) \) is pure. The formulas (2) and (3) then show that \((m, p)\) is pure whenever \((m, p)\) is supersingular. On the other hand, in [7] Evans found sufficient conditions under which \((m, p)\) is pure, and showed that there are infinitely many non-supersingular pure pairs \((m, p)\) (see Theorem 3.1).

The purpose of this paper is to determine all the pure pairs \((m, p)\) under the assumption that every prime factor of \( m \) is congruent to 3 modulo 4 (see Theorem 2.3). As a corollary, we show that there are infinitely many pure pairs \((m, p)\) which are neither supersingular nor of Evans type.

2. The main theorem

Let \( m = l^o_1 \cdots l^o_r \) be the prime power factorization of \( m \), where \( l_1, \ldots, l_r \) are distinct prime numbers. In this section, we assume that \( m \) satisfies the following condition:

\[
l_1 \equiv \cdots \equiv l_r \equiv 3 \pmod{4}.
\]  

(5)

For each \( i = 1, \ldots, r \), let \( m_i = l_i^o \). Then \((\mathbb{Z}/m_i\mathbb{Z})^x\) is a cyclic group of order \( \varphi(m_i) \).

Let \( f_i \) be the smallest positive integer such that \( p^{f_i} \equiv 1 \pmod{m_i} \).

**Proposition 2.1.** If \( f_i \) is even for any \( i = 1, \ldots, r \) then \((m, p)\) is supersingular.

**Proof.** If \( f_i \) is even for any \( i = 1, \ldots, r \) then \( p^{f_i/2} \equiv -1 \pmod{m_i} \). Moreover, since \( l_i \equiv 3 \pmod{4} \) for any \( i \), it follows that \( f/2 \) is an odd multiple of \( f_i/2 \), so \( p^{f/2} \equiv -1 \pmod{m} \). Therefore \((m, p)\) is a supersingular. \( \square \)

**Remark 2.2.** If \( m > 2 \) then one can easily verify that \((m, p)\) is supersingular if and only if \( f_i \) is even for any \( i = 1, \ldots, r \). On the contrary, if \( f_i \) is odd for any \( i = 1, \ldots, r \) then \( g(m, p) \) is never pure. We will prove this in Section 10.

Throughout this paper, we let

\[
A = \{1, 2, \ldots, r\}.
\]

For simplicity, we assume that \( f_i \) is odd for \( i = 1, \ldots, r_1 \) and \( f_i \) is even for \( i = r_1 + 1, \ldots, r \). Let

\[
A_1 = \{1, 2, \ldots, r_1\},
\]

\[
A_2 = \{r_1 + 1, r_1 + 2, \ldots, r\}.
\]
and put $r_2 = |A_2| = r - r_1$. For any subset $I$ of $A$, $I^c$ will denote the complement of $I$ in $A$, and $|I|$ will stand for the cardinality of $I$.

Let $D(m)$ denote the set of square-free positive divisors of $m$. If we put $m_0 = l_1 \cdots l_r$, the largest square-free divisor of $m$, then $D(m) = D(m_0)$. For any square-free odd integer $d > 1$, let $(\frac{d}{p})$ denote the Jacobi symbol modulo $d$. For convenience, we put $(\frac{a}{p}) = 1$ for any non-zero integer $a$. Define three subsets of $D(m)$ as follows:

$D^-(m) = \{ d \in D(m) \mid d \equiv 3 \pmod{4} \}$,

$D(m, p) = \{ d \in D(m) \mid (\frac{d}{p}) = 1 \}$,

$D^-(m, p) = D^-(m) \cap D(m, p)$.

Let $P(m)$ denote the set of prime divisor of $m$ and let

$E(m, p) = \{ d \in D^-(m, p) \mid (\frac{l}{d}) = -1 \text{ for any } l \in P(m_0/d) \}$.

Note that $m_0 \equiv (-1)^r \pmod{4}$, $(\frac{m_0}{p}) = (-1)^{r_2}$.

Therefore, $m_0 \in E(m, p)$ if and only if $r$ is odd and $r_2$ is even.

In order to state our main result, consider the following two conditions on $(m, p)$:

(C1) $r_1$ is even, $2f_i = \varphi(m_i)$ for any $i \in A_1$, and $(f_i, f_j) = 1$ for any $(i, j) \in A_1 \times A_1$ such that $i \neq j$.

(C2) $r_2$ is odd, $f_j = \varphi(m_j)$ for any $j \in A_2$, and $(f_i, f_j) \leq 2$ for any $(i, j) \in A \times A_2$ such that $i \neq j$.

Then the main theorem can be stated as follows.

**Theorem 2.3.** Let $m > 1$ be an integer satisfying Condition (5). Suppose $A_1 \neq \emptyset$ and $A_2 \neq \emptyset$. Then $(m, p)$ is pure if and only if the following two conditions hold.

(i) Either Condition (C1) or Condition (C2) holds.

(ii) $E(m, p) = \emptyset$.

**Remark 2.4.** If $A_1 = \emptyset$ then Condition (C1) is an empty condition. Moreover, as we will see in Proposition 10.1 (i), if $A_1 = \emptyset$ then $E(m, p) = \emptyset$. On the other hand, if $A_2 = \emptyset$ then $(m, p)$ is never pure (see Corollary 10.3).

**Remark 2.5.** Assume that $f_i$ equals either $\varphi(m_i)$ or $\varphi(m_i)/2$ for any $i \in A$ and that $(f_i, f_j) \leq 2$ for any $i \neq j$ then both (C1) and (C2) hold. In this special case, we showed in [4] that $g(m, p)$ belongs to the multi-quadratic field $\mathbb{Q}(\sqrt{-d}, d \in E(m, p))$.

Thus, if $E(m, p) = \emptyset$ then $g(m, p) \in \mathbb{Q}$, so $(m, p)$ is pure.
3. A theorem of Evans

In [7] Evans found three types of sufficient conditions under which \((m, p)\) is pure. In order to state them we introduce some notation. Let \(m > 1\) be an integer which is not necessarily odd, and let

\[ m = l_1^{e_1} \cdots l_r^{e_r} \]

be the prime power decomposition of \(m\), where \(l_1, \ldots, l_r\) are distinct prime numbers. For any subset \(I\) of \(\Lambda\), we let

\[ m_I = \prod_{i \in I} m_i \]

and let \(f_I\) denote the order of \(p\) in \((\mathbb{Z}/m_I\mathbb{Z})^\times\). In our notation, Evans’ theorem can be stated as follows.

**Theorem 3.1 (Evans).** Suppose \(m = m_I m_J\) for some \(I, J\) \(= Ic \subset \Lambda\) such that \((f_I, f_J) = 1\). Then \(g(m, p)\) is pure if any of the following three conditions is satisfied.

(i) \(f_I = \varphi(m_I)\) and \(l \equiv p^\nu \) \((\mod m_J)\) \((\exists \nu \in \mathbb{Z})\) for some \(l \in \mathcal{P}(m_I)\), and all of this holds with \(m_I\) and \(m_J\) interchanged.

(ii) \(p^k \not\equiv -1 \) \((\mod m_I)\) \((\forall k \in \mathbb{Z})\), \(2 f_I = \varphi(m_I)\), \(l \equiv p^\nu \) \((\mod m_J)\) \((\exists \nu \in \mathbb{Z})\) for some \(l \in \mathcal{P}(m_I)\), and all of this holds with \(m_I\) and \(m_J\) interchanged.

(iii) \(m\) is even, \(2 + m/2 \not\equiv p^k \) \((\mod m_I)\) \((\forall k \in \mathbb{Z})\), \(2 f_I = \varphi(m_I)\), \(-1\) or \(l\) is congruent to \(p^\nu \) \((\mod m_J)\) \((\exists \nu \in \mathbb{Z})\) for some \(l \in \mathcal{P}(m_I)\), and all of this holds with \(m_I\) and \(m_J\) interchanged.

In the following, we will show that, under Condition (5), Evans’ conditions imply our conditions in Theorem 2.3.

Suppose \(m\) satisfies Condition (5). Since the third condition of Theorem 3.1 is concerned with the case of even \(m\), we consider only the first and second conditions.

In the first condition (i), in order that \(f_I = \varphi(m_I)\) it is necessary that \(I = \{i\}\) for some \(i \in \Lambda_2\), say \(I = \{r\}\). Then \(g(m, p)\) is pure if any of the following three conditions is satisfied. Moreover, for any \(d \in \mathcal{D}(m)\), we have

\[ \left( \frac{p}{d} \right) = \begin{cases} -1 & \text{if } l_r \mid d, \\ 1 & \text{otherwise}. \end{cases} \]

It follows that \(\mathcal{D}(m, p) = \mathcal{D}(m_J)\). But, since \(l_r \equiv p^\nu \) \((\mod m_J)\) \((\exists \nu \in \mathbb{Z})\), we have

\[ \left( \frac{l_r}{f_I} \right) = \left( \frac{p}{l_r} \right)^\nu = 1 \]

for any \(d \in \mathcal{D}(m_J)\). Therefore \(\mathcal{E}(m, p) = \emptyset\).

We now consider the case where Condition (ii) of Theorem 3.1 holds. In this case, since \(2 f_I = \varphi(m_I)\) and \(2 f_J = \varphi(m_J)\), one can easily see that \(|I| \leq 2\) and \(|J| \leq 2\).

Firstly, suppose \(|I| = |J| = 1\), say \(I = \{1\}\) and \(J = \{2\}\). Then \(m = l_1^{e_1} l_2^{e_2}\) and both \(f_1\) and \(f_2\) are odd, so

\[ \left( \frac{p}{l_1} \right) = \left( \frac{p}{l_2} \right) = 1. \]
But, since $l_1 \equiv p^{v_1} \pmod{l_2}$ for some $v_1 \in \mathbb{Z}$ and $l_2 \equiv p^{v_2} \pmod{l_2}$ for some $v_2 \in \mathbb{Z}$, we have 
\[
\left(\frac{l_1}{l_2}\right) = \left(\frac{l_2}{l_1}\right) = 1,
\]
which is impossible since $l_1 \equiv l_2 \equiv 3 \pmod{4}$. Therefore, this case does not occur.

Secondly, suppose $|I| = |J| = 2$. In this case, both $f_I$ and $f_J$ are even. But this is impossible since $f_I$ and $f_J$ are assumed to be relatively prime. Therefore, this case also does not occur.

Lastly, suppose $|I| \neq |J|$. By symmetry in $I$ and $J$, we may assume that $|I| = 1$ and $|J| = 2$, say $I = \{1\}$ and $J = \{2, 3\}$. Then, as in the argument above, we see that $f_I$ is odd and $f_J$ is even. In particular, $J$ cannot be contained in $A_1$. If $J \subsetneq A_2$ then $p^{1/2} \equiv -1 \pmod{m_f}$, which is a contradiction. Hence $J \not\subset A_2$, so we may assume that $A_1 = \{1, 2\}$ and $A_2 = \{3\}$. The assumption that $(f_I, f_J) = 1$ then implies that $D$ is strictly $A_2$-disconnected, so Condition (C2) is satisfied. Moreover, we have $D^\sim(m, p) = \{l_1, l_2\}$ and $\mathcal{E}(m, p) \subset \{l_1, l_2\}$. But since $l_1 \equiv p^k \pmod{m_f}$ for some $k \in \mathbb{Z}$, we have $(\frac{l_1}{l_2}) = 1$. Hence $l_2 \not\in \mathcal{E}(m, p)$. Similarly, since $l_2$ or $l_3$ is congruent to a power of $p$ modulo $m_1$, we have 
\[
\left(\frac{l_2}{l_3}\right) = 1 \text{ or } \left(\frac{l_3}{l_2}\right) = 1.
\]
But the first case cannot occur since $(\frac{l_3}{l_2}) = 1$. Hence $(\frac{l_2}{l_3}) = 1$, so $l_3 \not\in \mathcal{E}(m, p)$. Consequently, we have $\mathcal{E}(m, p) = \emptyset$. Therefore, in this case, the conditions of Theorem 2.3 hold.

4. Some basic properties of Gauss sums

In this section, we collect some basic properties on Gauss sums and state a theorem of Stickelberger which plays a key role in the proof of Theorem 2.3. In this section, we do not assume that $m$ is odd.

Let $K$ denote the cyclotomic field $\mathbb{Q}(\zeta_m)$, and let $G = \text{Gal}(K/\mathbb{Q})$ denote the Galois group of $K/\mathbb{Q}$. We fix the standard isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \cong G$; for any integer $t$ prime to $m$, let $\sigma_t$ denote the element of the Galois group $G$ uniquely determined by the rule $\sigma_t(\zeta_m) = \zeta_m^t$. Then the map sending $t \pmod{m}$ to $\sigma_t$ gives rise to an isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \cong G$.

**Proposition 4.1.** Notation being as above, the following assertions hold.

(i) $|g(m, p)^\sigma| = \sqrt{m}$ for any $\sigma \in \text{Gal}(\mathbb{C}/\mathbb{Q})$.
(ii) Let $H$ be the cyclic subgroup of $G$ generated by $\sigma_p$. Then $g(m, p)^m \in K^H$.

**Proof.** (i) This is well-known and essentially proved in [8, Proposition 8.2.2].
(ii) See [8, Proposition 14.3.1 (c)] and the proof of [8, Chapter 14, Theorem 3]. \(\square\)

**Proposition 4.2.** If $g(m, p)$ is pure then $mf$ is even.

**Proof.** Suppose $g(m, p)$ is pure, and choose a positive integer $k$ such that $g(m, p)^k$ is real. Then $g(m, p)^k = \pm p^{k/2}$ since $|g(m, p)| = p^{k/2}$ by Proposition 4.1 (i). Therefore,
$pm^{f/2} = \pm g(m, p)^{nk}$ belongs to $K$ by Proposition 4.1 (ii). But, since $\sqrt{p}$ does not belong to $K$, $mf$ must be even. This proves the proposition.

Actually one can say more about ord$_2$($m$) when $g(m, p)$ is pure and $f$ is odd: If $g(m, p)$ is pure then ord$_2$($m$) = 1, and there exist infinitely many pair ($m$, $p$) for which ord$_2$($m$) = 1 and $g(m, p)$ is pure (see [2]).

**PROPOSITION 4.3.** If $p^v \equiv -1 \pmod{m}$ for some $v \in \mathbb{Z}$ then $g(m, p)$ is pure.

**Proof.** If $p^v \equiv -1 \pmod{m}$ for some $v \in \mathbb{Z}$ then $H$ contains $\sigma_{-1}$, which acts on $K$ by the complex conjugate. Hence $K^H$ is a real field. It then follows from Proposition 4.1 (ii) that $g(m, p)^m$ is real. Therefore $g(m, p)$ is pure.

**PROPOSITION 4.4.** The following three conditions are equivalent.

(i) $g(m, p)$ is pure.

(ii) $g(m, p) = \zeta^{p^{f/2}}$ for some root of unity $\zeta$.

(iii) We have $(g(m, p)^m) = (p^{mf/2})$, where $(g(m, p)^m)$ and $(p^{mf/2})$ denote the principal ideals of $K$ generated by $g(m, p)^m$ and $p^{mf/2}$, respectively.

**Proof.** (i) $\implies$ (ii): Suppose $g(m, p)$ is pure. Then $g(m, p)^k$ is real for some positive integer $k$. Since $|g(m, p)| = \sqrt{k}$ by Proposition 4.1 (i), it follows that $g(m, p)^k = \pm \sqrt{k}$. Hence $g(m, p) = \zeta \sqrt{k}$ for some $2k$-th root of unity.

(ii) $\implies$ (i): This is clear.

(iii) $\implies$ (ii): Suppose $(g(m, p)^m) = (p^{mf/2})$. Then $g(m, p)^m = u \sqrt{m}$ for some unit in $K$. Since $|g(m, p)^m| = \sqrt{m}$ for any $\sigma \in \text{Gal}(K/\mathbb{Q})$, it follows that $|u^\sigma| = 1$ for any $\sigma$. But this holds only when $u$ is a root of unity by Kronecker’s theorem.

Now, in order to state Stickelberger’s theorem, we let $\theta$ denote the Stickelberger element in the group ring $\mathbb{Q}[G]$:

$$\theta = \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \left\langle \frac{t}{m} \right\rangle \sigma_t^{-1} \in \mathbb{Q}[G],$$

where for any $x \in \mathbb{R}$, $\langle x \rangle$ denotes the fractional part of $x$, so $0 \leq \langle x \rangle < 1$ and $x - \langle x \rangle \in \mathbb{Z}$. It is then clear from the definition of $\theta$ that $m \theta \in \mathbb{Z}[G]$.

**LEMMA 4.5.** Let $v_G = \sum_{\sigma \in G} \sigma$ denote the norm element of $\mathbb{Z}[G]$ and let $\rho = \sigma_{-1}$.

Then

$$\rho - 1)\theta = v_G - 2 \theta.$$

**Proof.** Note that

$$\rho \theta = \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \left\langle \frac{t}{m} \right\rangle \sigma_{-1} \sigma_t^{-1} = \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \left\langle \frac{t}{m} \right\rangle \sigma_{-1} - \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \left\langle -\frac{t}{m} \right\rangle \sigma_t^{-1}.$$  

Here we have

$$\left\langle \frac{t}{m} \right\rangle + \left\langle -\frac{t}{m} \right\rangle = 1$$
for any \( t \in (\mathbb{Z}/m\mathbb{Z})^\times \). It follows that

\[
\rho \theta = \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \left( 1 - \frac{t}{m} \right) \sigma_t^{-1} = \nu_G - \theta .
\]

Therefore \( (\rho - 1)\theta = \nu_G - 2\theta \).

In the notation above, Stickelberger’s theorem can be stated as follows.

**Theorem 4.6** (Stickelberger). The prime ideal decomposition of the ideal \((g(m, p)^m)\) of \(K\) is given by

\[
(g(m, p)^m) = p^m \theta .
\]

**Proof.** See [8, Chapter 14, §3, Theorem 2].

**Corollary 4.7.** \(g(m, p)\) is pure if and only if

\[
p^{m(\rho - 1)\theta} = (1) . \tag{6}
\]

**Proof.** Suppose \(g(m, p)\) is pure. Then the principal ideal \((g(m, p)^m)\) in \(K\) is equal to \((p^{f/2})\) by Proposition 4.1. Let \(\rho = \sigma_{-1}\) denote the complex conjugate. Then

\[
(g(m, p)^m)^\rho = (g(m, p)^m) .
\]

Hence

\[
(g(m, p)^m(\rho - 1)\theta) = (1) .
\]

But this is equivalent to (6) by Theorem 4.6.

Conversely, if (6) holds then

\[
p^{m(\nu_G - 2\theta)} = (1) .
\]

by Lemma 4.5. Since \(p^\nu_H = (p^f)\), it follows that

\[
p^{m\theta} = (p^{mf/2}) .
\]

Hence \((g(m, p)^m) = (p^{mf/2})\), so \(g(m, p)\) is pure by Proposition 4.4.

**Lemma 4.8.** Let \(\alpha \in \mathbb{Z}[G]\). Then \(p^\alpha = (1)\) if and only if \(\alpha \nu_H = 0\), where

\[
\nu_H = 1 + \sigma_p + \sigma_p^2 + \cdots + \sigma_p^{f-1} \in \mathbb{Z}[G] .
\]

**Proof.** Recall that \(H\) is the cyclic subgroup of \(G\) generated \(\sigma_p\). Let \(T \subset G\) be a complete set of the representatives of the quotient group \(G/H\). Since \(p\) is fixed by \(H\), we can write

\[
p^\alpha = \prod_{t \in T} (p^{c_t})^{g_t}
\]

with some integers \(c_t\). Then the uniqueness of the prime ideal decomposition implies that \(p^\alpha = (1)\) if and only if \(c_t = 0\) for any \(t \in T\). Since

\[
\nu_H \alpha = \nu_H \sum_{t \in T} c_t \sigma_t = \sum_{t \in T} c_t \sigma_{ht} ,
\]

it follows that \(c_t = 0\) for any \(t \in T\) if and only if \(\alpha \nu_H = 0\). Therefore, \(p^\alpha = (1)\) if and only if \(\alpha \nu_H = 0\).
Thanks to Theorem 4.6, the purity problem of $g(m, p)$ can be reduced to analysis of $\theta$. To be more precise, we denote by $C(m)$ the character group of $(\mathbb{Z}/m\mathbb{Z})^\times$. For any $\chi \in C(m)$, we extend $\chi$ to a ring homomorphism from $\mathbb{Z}[G]$ to $\mathbb{Z}[\chi] := \{ \chi(a); a \in (\mathbb{Z}/m\mathbb{Z})^\times \}$ in a natural way. We obtain a ring homomorphism

$$
\mathbb{Z}[G] \rightarrow \bigoplus_{\chi \in C(m)} \mathbb{Z}[\chi], \quad \alpha \mapsto (\chi(\alpha))_\chi .
$$

Clearly this is an injection. Therefore, given an element $\alpha \in \mathbb{Z}[G]$, we have $\alpha = 0$ if and only if $\chi(\alpha) = 0$ for any $\chi \in C(m)$.

Now consider the following subsets of $C(m)$:

- $C^- (m) = \{ \chi \in C(m) \mid \chi(-1) = -1 \}$,
- $C^- (m, p) = \{ \chi \in C(m) \mid \chi(p) = 1 \}$,
- $C^- (m, p) = C^- (m) \cap C(m, p)$.

We say that a character $\chi \in C(m)$ is quasi-primitive if the conductor of $\chi$ is divisible by any prime factor of $m$. In particular, if $\chi \in C(m)$ is quasi-primitive then $\chi(l) = 0$ for any prime $l$ dividing $m$. We denote by $QC(m)$ the set of quasi-primitive characters of $(\mathbb{Z}/m\mathbb{Z})^\times$ and put

$$
QC^-(m, p) = QC(m) \cap C^-(m, p) .
$$

Let $m = l_1^{e_1} \cdots l_r^{e_r}$ be the prime power factorization of $m$. For any subset $I$ of $\Lambda := \{ 1, \ldots, r \}$, we set

$$
m_I = \prod_{i \in I} l_i^{e_i} .
$$

Note that $(m_I, m/m_I) = 1$ for any $I$.

**Proposition 4.9.** $g(m, p)$ is pure if and only if the following two conditions hold.

(i) $QC^- (m, p) = \emptyset$.

(ii) For any non-empty subset $I \subseteq \Lambda$ and any $\chi \in QC^- (m_I, p)$, there exists a prime $l$ dividing $m/m_I$ such that $\chi(l) = 1$.

**Proof.** By Corollary 4.7 and Lemma 4.8, $g(m, p)$ is pure if and only if $(\rho - 1)\nu_H = 0$. But this is equivalent to

$$
\chi((\rho - 1)\nu_H) = 0 \quad (\forall \chi \in C(m)) \quad (7)
$$

by the remark above. Note that, if $\chi$ is even, that is, $\chi(\rho) = 1$ then $(7)$ always holds. On the other hand, if $\chi$ is an odd character, that is $\chi(\rho) = -1$, then

$$
\chi((\rho - 1)\nu_H) = 2\chi(\theta)\chi(\nu_H) .
$$

If $\chi(p) \neq 1$ then $\chi(\nu_H) = 0$. If $\chi(p) = 1$ then $\chi(\nu_H) = p \neq 0$, so the condition $(7)$ boils down to the condition

$$
\chi(\theta) = 0 \quad (\forall \chi \in C^-(m, p)) .
$$

Here we recall that

$$
\chi(\theta) = \prod_{l \in \mathcal{P}(m/d)} (1 - \chi(l)) \cdot B_{1, \chi} ,
$$

where $\mathcal{P}(m/d)$ is the set of prime divisors of $m/d$. Therefore, $\chi(\theta) = 0$ if and only if $\chi(l) = 0$ for any prime $l$ dividing $m/d$. This is equivalent to $(7)$. Hence, we conclude that $\chi((\rho - 1)\nu_H) = 0$ if and only if $\chi(l) = 0$ for any prime $l$ dividing $m/m_I$.

For any subset $I$ of $\Lambda := \{ 1, \ldots, r \}$, we set

$$
m_I = \prod_{i \in I} l_i^{e_i} .
$$

Note that $(m_I, m/m_I) = 1$ for any $I$.
where $B_{1,\chi}$ is the generalized Bernoulli number. Since $B_{1,\chi} \neq 0$ for any primitive odd character $\chi$, (8) holds if and only if

$$\prod_{l\mid m/m_I} (1 - \chi(l)) = 0 \quad (\forall \chi \in QC^- (m_I, p))$$

(9)

for any non-empty subset $I \subset \Lambda$.

If $I = \Lambda$ then the left hand side of (9) is regarded as 1, and Condition (9) is equivalent to $QC^- (m, p) = \emptyset$. On the other hand, if $I \neq \Lambda$ then for an $\chi \in QC^- (m_I, p)$ we have

$$\prod_{l\mid m/m_I} (1 - \chi(l)) = 0$$

if and only if $\chi(l) = 1$ for some $l \in \mathcal{P}(m/m_I)$. This completes the proof of Proposition 4.9.

Proposition 4.9 shows that the purity problem of Gauss sums can be reduced to two arithmetic conditions. In the next section we will reduce the first condition to a certain linear Diophantine equation. The second condition will be studied on and after Section 9.

5. A linear Diophantine equation

In this section, we assume that $m$ is odd. Let $m = m_1 \cdots m_r \ (m_i = l_i^{n_i})$ be the prime power decomposition of $m$ as in Section 2 and put $n_i = \varphi(m_i)$ for each $i$. Note that $n_i$ are all even since we are assuming that $m_i > 2$. We consider a finite additive group $V(m) = \mathbb{Z}/n_1 \mathbb{Z} \times \cdots \times \mathbb{Z}/n_r \mathbb{Z}$.

Then $(\mathbb{Z}/m \mathbb{Z})^\times \cong V(m)$. We specify this isomorphism as follows. Recall that $f_i$ denotes the least positive integer such that

$$p^{f_i} \equiv 1 \pmod{m_i}.$$  

For each $i$, choose and fix a primitive root $g_i \mod m_i$ such that

$$p \equiv g_i^{n_i/f_i} \pmod{m_i}.$$  

(10)

For any $x \in (\mathbb{Z}/m \mathbb{Z})^\times$, we denote by $\text{Ind}_{g_i}(x) \in \mathbb{Z}/n_i \mathbb{Z}$ the index of $x$ with respect to the primitive root $g_i$. Thus, $a = \text{Ind}_{g_i}(x)$ if and only if

$$x \equiv g_i^a \pmod{m_i}.$$  

Then the map

$$\text{Ind}_{g_i} : (\mathbb{Z}/m_i \mathbb{Z})^\times \longrightarrow \mathbb{Z}/n_i \mathbb{Z}$$

is a group isomorphism. This can be naturally generalized to an isomorphism

$$\text{Ind} : (\mathbb{Z}/m \mathbb{Z})^\times \longrightarrow V(m)$$

by letting

$$\text{Ind}(x) = (\text{Ind}_{g_1}(x), \ldots, \text{Ind}_{g_r}(x))$$
for any \( x \in (\mathbb{Z}/m\mathbb{Z})^\times \). It is then clear from (10) that
\[
\text{Ind}(p) = \left( \frac{n_1}{f_1}, \ldots, \frac{n_r}{f_r} \right).
\]
Moreover, it is also clear from the definition of \( \text{Ind} \) that
\[
\text{Ind}(-1) = \left( \frac{n_1}{2}, \ldots, \frac{n_r}{2} \right).
\]

Let \( C(m_i) \) be the character group of \((\mathbb{Z}/m_i\mathbb{Z})^\times\), which is a cyclic group of order \( n_i \) since we are assuming that \( m_i \) is a power of an odd prime number. Choose a generator \( \chi_i \) of \( C(m_i) \) such that
\[
\chi_i(g_i) = \exp \left( \frac{2\pi \sqrt{-1}}{n_i} \right).
\]
For any \( a = (a_1, \ldots, a_r) \in V(m) \), we put
\[
\chi^a = \chi_1^{a_1} \cdots \chi_r^{a_r}.
\]
Then the map \( a \mapsto \chi^a \) defines an isomorphism
\[
V(m) \cong C(m).
\]

For any \( a \in \mathbb{Z}/n_i\mathbb{Z} \), we denote by \( \frac{a}{n_i} \in \mathbb{Q}/\mathbb{Z} \) the image of \( a \) under the natural isomorphism
\[
\mathbb{Z}/n_i\mathbb{Z} \cong \frac{1}{n_i}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}.
\]
In the notation above, for any \( a = (a_1, \ldots, a_r), \ b = (b_1, \ldots, b_r) \in V(m) \), we define an inner product on \( V(m) \) with values in \( \mathbb{Q}/\mathbb{Z} \) by
\[
\langle a, b \rangle_m = \sum_{i=1}^r \frac{a_ib_i}{n_i} \in \mathbb{Q}/\mathbb{Z}.
\]
Using this inner product, we can compute \( \chi^a \) as follows.

**Lemma 5.1.** For any \( a \in V(m) \) and any \( b \in (\mathbb{Z}/m\mathbb{Z})^\times \), we have
\[
\chi^a(b) = \exp \left( 2\pi \sqrt{-1} \langle a, \text{Ind}(b) \rangle_m \right).
\]

**Proof.** Let \( \text{Ind}(b) = (k_1, \ldots, k_r) \in V(m) \), that is, \( b \equiv g_i^{k_i} \pmod{m_i} \). Then
\[
\chi^a(b) = \prod_{i=1}^r \chi_i(g_i)^{a_i k_i} = \prod_{i=1}^r \exp \left( \frac{2\pi \sqrt{-1} a_i k_i}{n_i} \right) = \exp \left( 2\pi \sqrt{-1} \langle a, \text{Ind}(b) \rangle_m \right).
\]
This proves the lemma. \( \square \)

We now consider two functions \( \varepsilon \) and \( \omega_p \) on \( V(m) \) with values in \( \mathbb{Z}/2\mathbb{Z} \) and \( \mathbb{Q}/\mathbb{Z} \) respectively: For any \( a = (a_1, \ldots, a_r) \in V(m) \), let
\[
\varepsilon(a) = a_1 + \cdots + a_r \pmod{2} \in \mathbb{Z}/2\mathbb{Z},
\]
\[
\omega_p(a) = \sum_{i=1}^r \frac{a_i}{f_i} \in \mathbb{Q}/\mathbb{Z}.
\]
The next proposition gives a characterization of the set $QC^-(m, p)$ in terms of $\varepsilon$ and $\omega_p$.

**LEMMA 5.2.** Notation being as above, the following assertions hold.

(i) $\chi^a$ is odd if and only if $\varepsilon(a) \equiv 1 \pmod{2}$.

(ii) $\chi^a(p) = 1$ if and only if $\omega_p(a) \equiv 0 \pmod{1}$.

**Proof.** (i) Since $\text{Ind}(-1) = (\frac{n_1}{2}, \ldots, \frac{n_r}{2})$, it follows that $\chi^a(-1) = \exp\left(2\pi \sqrt{-1} \cdot \frac{a_1 + \cdots + a_r}{2}\right) = \exp\left(\pi \sqrt{-1} \varepsilon(a)\right)$.

Therefore, $\chi^a(-1) = -1$ if and only if $\varepsilon(a) \equiv 1 \pmod{2}$. This proves (i).

(ii) Note that $\text{Ind}(p) = (\frac{a_1}{p}, \ldots, \frac{a_r}{p})$, so $\omega_p(a) = \langle a, \text{Ind}(p) \rangle_m$. Therefore (ii) immediately follows from Lemma 5.1 □

Let

$$A(m) = \{(a_1, \ldots, a_r) \in V(m) \mid a_i \not\equiv 0 \pmod{n_i} \quad \forall i \in \Lambda\},$$

$$A^-(m) = \{a \in A(m) \mid \varepsilon(a) \equiv 1 \pmod{2}\},$$

$$A(m, p) = \{a \in A(m) \mid \omega_p(a) = 0\},$$

$$A^-(m, p) = A^-(m) \cap A(m, p).$$

It is then easy to see that

$$QC(m) = \{\chi^a \mid a \in A(m)\},$$

$$QC^-(m, p) = \{\chi^a \mid a \in A^-(m, p)\}.$$

**PROPOSITION 5.3.** $g(m, p)$ is pure if and only if the following two conditions hold.

(i) $A^-(m, p) = \emptyset$.

(ii) For any non-empty subset $I \subseteq \Lambda$ and any $a \in A^-(m_I, p)$, there exists a prime $l$ dividing $m/m_I$ such that $\langle a, \text{Ind}(l) \rangle_{m_I} = 0$.

**Proof.** In view of Lemma 5.1 and Lemma 5.2, this is just a restatement of Proposition 4.9. □

6. A theorem of Sun and Wang

In Proposition 5.3 we have shown that the purity problem for the Gauss sums $g(m, p)$ is reduced to solving a linear Diophantine problem

$$\frac{x_1}{f_1} + \cdots + \frac{x_r}{f_r} \equiv 0 \pmod{1} \quad (11)$$

in the range $0 < x_i < n_i$ (\forall i \in \Lambda) with a parity condition

$$x_1 + \cdots + x_r \equiv 1 \pmod{2} \quad (12)$$

In order to solve the Diophantine problem above, we first start with a slightly general setting without the parity condition. As in the previous section, let $r$ be a positive integer.
and let

\[ \Lambda = \{1, \ldots, r\}. \]

Let \( N = (n_1, \ldots, n_r) \) denote an \( r \)-tuple of positive even integers. (We do not assume that \( N \) is of the form \((\phi(m_1), \ldots, \phi(m_r))\) as in the previous section.) Let \( D = (d_1, \ldots, d_r) \) denote an \( r \)-tuple of positive integers such that \( d_i \mid n_i \) for any \( i \in \Lambda \). Let

\[ B_N = \{(a_1, \ldots, a_r) \in \mathbb{Z}^r \mid 0 < a_i \leq n_i (\forall i \in \Lambda)\}, \]

\[ A_N = \{(a_1, \ldots, a_r) \in \mathbb{Z}^r \mid 0 < a_i < n_i (\forall i \in \Lambda)\}. \]

Thus \( A_N \subset B_N \).

Generalizing the map \( \omega_p \) in the previous section, we define a homomorphism

\[ \omega_D : \mathbb{Z}^r \rightarrow \mathbb{Q}/\mathbb{Z} \]

by setting

\[ \omega_D(a) = \sum_{i=1}^{r} \frac{a_i}{d_i} \pmod{\mathbb{Z}} \]

for \( a = (a_1, \ldots, a_r) \in \mathbb{Z}^r \). It is then clear that

\[ \text{Im}(\omega_D) = \frac{\text{LCM}(D)}{\mathbb{Z}} \mathbb{Z}/\mathbb{Z}, \]

where \( \text{LCM}(D) \) denotes the least common multiple of \( d_1, \ldots, d_r \).

Consider the following sets:

\[ B_N(D) = \{a \in B_N \mid \omega_D(a) = 0\}, \]

\[ A_N(D) = A_N \cap B_N(D). \]

In particular, if \( N = (\phi(m_1), \ldots, \phi(m_r)) \) and \( D = (f_1, \ldots, f_r) \) then the set \( A_N(D) \) is the set of integral solutions of (11). Note that \( N \in B_N \) and \( \omega_D(N) = 0 \), so \( N \in B_N(D) \) and \( B_N(D) \) is always non-empty.

In this section we are going to study a necessary and sufficient condition for \( A_N(D) = \emptyset \). For this end, we begin with the special case \( D = N \). For simplicity, we write \( A(D) \) for \( A_N(D) \):

\[ A(D) = \{a \in A_D \mid \omega_D(a) = 0\}, \]

\[ = \left\{ (a_1, \ldots, a_r) \in A_D \mid \sum_{i=1}^{r} \frac{a_i}{d_i} \equiv 0 \pmod{1} \right\}. \]

If \( I = \{i_1, \ldots, i_t\} \) is a subset of \( \Lambda \) and \( a = (a_1, \ldots, a_r) \in \mathbb{Z}^r \), then we define the \( I \)-component of \( a \) to be

\[ a_I = (a_{i_1}, \ldots, a_{i_t}) \in \mathbb{N}^t. \]

Moreover, for any subset \( X \) of \( \mathbb{Z}^r \), we set

\[ X_I = \{a_I \mid a \in X\}. \]

We define a lowering operator \( a^\triangledown \) and a raising operator \( a^\sharp \) on \( \mathbb{N} \); for any \( a \in \mathbb{N} \), we set

\[ a^\triangledown = \begin{cases} a & \text{if } a \text{ is odd}, \\ a/2 & \text{if } a \text{ is even}, \end{cases} \quad a^\sharp = \begin{cases} 2a & \text{if } a \text{ is odd}, \\ a & \text{if } a \text{ is even}. \end{cases} \]
Moreover for $\mathbf{a} = (a_1, \ldots, a_r) \in \mathbb{N}^r$ we set
\[
\mathbf{a}^b = (a_1^b, \ldots, a_r^b), \quad \mathbf{a}^r = (a_1^r, \ldots, a_r^r).
\]

For a non-empty subset $I \subseteq \Lambda$, we say that $D$ is $I$-disconnected if there exists an index $i \in I$ such that $(d_i, d_j) = 1$ for any $j \in \Lambda \setminus \{i\}$. If $D$ is $\Lambda$-disconnected, we simply say that $D$ is disconnected. Moreover we say that $D$ is strictly $I$-disconnected if $D$ is $\{i\}$-disconnected for any $i \in I$. In particular, we say that $D$ is strictly disconnected if $D$ is $\Lambda$-disconnected. Let
\[
\Lambda_2 = \{ i \in \Lambda | d_i \text{ is even} \}.
\]

The following theorem is proved in [13]. We give a proof for the sake of completeness,

**Theorem 6.1** (Sun and Wang). \( A(D) = \emptyset \) if and only if one of the following two conditions holds.

(i) $D$ is disconnected.

(ii) $|\Lambda_2|$ is odd and $D^b$ is strictly $\Lambda_2$-disconnected.

Before proving the theorem, we prove two lemmas below.

**Lemma 6.2.** Let $I, J$ be subsets of $\Lambda$ such that $I \cup J = \Lambda$ and $I \cap J = \emptyset$. Suppose $(d_i, d_j) = 1$ for any $(i, j) \in I \times J$. Then
\[
A(D) = A(D_I) \times A(D_J).
\]
Thus, $A(D) = \emptyset$ if and only if either $A(D_I) = \emptyset$ or $A(D_J) = \emptyset$. In particular, if either $|I| = 1$ or $|J| = 1$, then $A(D) = \emptyset$.

**Proof.** For any $\mathbf{a} \in A(D)$, the assumption implies that the denominators of $\omega_{D_I}(\mathbf{a}_I)$ and $\omega_{D_J}(\mathbf{a}_J)$ are coprime. Hence $\omega_D(\mathbf{a}) = 0$ if and only if $\omega_{D_I}(\mathbf{a}_I) = \omega_{D_J}(\mathbf{a}_J) = 0$. Therefore $A(D) = A(D_I) \times A(D_J)$. The remaining part of the assertion of the lemma is clear. □

**Lemma 6.3.** Suppose $\Lambda_1 = \emptyset$ and $D^b$ is strictly disconnected. Then
\[
A(D) = \begin{cases} 
\{ D^b \} & \text{if } r \text{ is even,} \\
\emptyset & \text{if } r \text{ is odd.}
\end{cases}
\]

**Proof.** Let $\mathbf{a} \in A(D)$. Then $\mathbf{a} \pmod{D^b}$ belongs to $B(D^b)$. The argument of Lemma 6.2 shows that
\[
B(D^b) = B(d_i^1) \times \cdots \times B(d_i^r).
\]
Since $B(d) = [0, d]$ for any positive integer $d$, this implies that $A(D) \subseteq \{ D^b \}$. Here we have
\[
\omega_D(D^b) \equiv \frac{r}{2} \pmod{1}.
\]
Therefore, $D^b \in A(D)$ if and only if $r$ is even, which proves the lemma. □

**Proof of Theorem 6.1.** We first show that both of (i) and (ii) are sufficient conditions for $A(D) = \emptyset$. Suppose $D$ is disconnected, namely, there exists $i \in \Lambda$ such that $(d_i, d_j) = 1$ for any $j \in \Lambda \setminus \{i\}$. Then, applying lemma 6.2 to the case $I = \{i\}$ and $J = \Lambda \setminus \{i\}$, we have $A(D) = \emptyset$. 

Moreover for $\mathbf{a} = (a_1, \ldots, a_r) \in \mathbb{N}^r$ we set
\[
\mathbf{a}^b = (a_1^b, \ldots, a_r^b), \quad \mathbf{a}^r = (a_1^r, \ldots, a_r^r).
\]

For a non-empty subset $I \subseteq \Lambda$, we say that $D$ is $I$-disconnected if there exists an index $i \in I$ such that $(d_i, d_j) = 1$ for any $j \in \Lambda \setminus \{i\}$. If $D$ is $\Lambda$-disconnected, we simply say that $D$ is disconnected. Moreover we say that $D$ is strictly $I$-disconnected if $D$ is $\{i\}$-disconnected for any $i \in I$. In particular, we say that $D$ is strictly disconnected if $D$ is $\Lambda$-disconnected. Let
\[
\Lambda_2 = \{ i \in \Lambda | d_i \text{ is even} \}.
\]

The following theorem is proved in [13]. We give a proof for the sake of completeness,
On the other hand, if \(|A_2|\) is odd and \(D^\flat\) is strictly \(A_2\)-disconnected, then

\[
A(D) = A(D_{A_1}) \times A(D_{A_2})
\]

by Lemma 6.2. But \(A(D_{A_2}) = \emptyset\) by Lemma 6.3, so \(A(D) = \emptyset\).

We next show that if \(A(D) = \emptyset\) then one of the conditions of the theorem holds. For any prime \(l\), let

\[
\text{Supp}_l(D) = \{i \in A \mid d_i \equiv 0 \pmod{l}\},
\]

\[
\mathcal{L}(D) = \{l \mid |\text{Supp}_l(D)| \geq 2\}.
\]

Assume that \(D\) is not disconnected. Then, for any \(i \in A\), there exists \(j \in A \setminus \{i\}\) such that \([i, j] \subset \text{Supp}_l(D)\) for some prime \(l\).

If \(l > 2\), then one can choose an integer \(x_{i,l}\) for each \(i \in \text{Supp}_l(D)\) such that \(0 < x_{i,l} < l\) and

\[
\sum_{i \in \text{Supp}_l(D)} x_{i,l} \equiv 0 \pmod{l}.
\]

In case \(|A_2|\) is even, if we set \(x_{i,2} = 1\) for any \(i \in A_2\) then (13) is also satisfied.

If \(|A_2|\) is odd then we further assume that \(D^\flat\) is not strictly \(A_2\)-disconnected. This means that \(d := (d_{i_0}, d_{j_0}) > 2\) for some \((i_0, j_0) \in A_2 \times A\). If \(i_0 \in \text{Supp}_l(D)\) for an odd prime \(l\) then we set

\[
x_{i,2} = \begin{cases} 0 & (i = i_0), \\ 1 & (i \neq i_0). \end{cases}
\]

then (13) is satisfied. For each \(i \in A\), choose an integer \(x_i\) such that \(0 \leq x_i \leq d_i\) and

\[
x_i \equiv \sum_{l \in \mathcal{L}(D)} \frac{d_i x_{i,l}}{l} \pmod{d_i}.
\]

Since \(x_{i,l} \not\equiv 0 \pmod{l}\), we have

\[
\sum_{l \in \mathcal{L}(D)} \frac{x_{i,l}}{l} \not\equiv 0 \pmod{l},
\]

so \(0 < x_i < d_i\). Put \(x = (x_1, \ldots, x_r)\). Then we have

\[
\omega_D(x) = \sum_{i=1}^{r} x_i = \sum_{i \in A \setminus \{i_0\}} \sum_{l \in \mathcal{L}(D)} \frac{x_{i,l}}{l} = \sum_{l \in \mathcal{L}(D) \setminus \{2\}} \sum_{i \in \text{Supp}_l(D)} \frac{x_{i,l}}{l} \equiv 0 \pmod{1}.
\]

Therefore \(x \in A(D)\), so \(A(D) \neq \emptyset\).

If \(d\) is a power of 2 then \(j \in A_2\). In this case we choose \(x_{i,j}\) in the same way as above for any odd \(l \in \mathcal{L}(D)\). For each \(i \in A\), choose an integer \(x_i\) such that \(0 \leq x_i \leq d_i\) and

\[
x_i \equiv \sum_{l \in \mathcal{L}(D) \setminus \{2\}} \frac{d_i x_{i,l}}{l} + \begin{cases} \frac{d_i}{2} & (i = i_0, j_0), \\ \frac{d_i}{4} & (i \neq i_0, j_0). \end{cases} \pmod{d_i}.
\]

Then we have \(0 < x_i < d_i\) in this case as well. Moreover, similarly as above, we see that \(x := (x_1, \ldots, x_r) \in A(D)\), so \(A(D) \neq \emptyset\).

Thus, if \(A(D) = \emptyset\) then either \(D\) is disconnected or \(|A_2|\) is odd and \(D^\flat\) is strictly \(A_2\)-disconnected. This completes the proof of Theorem 6.1. \(\square\)
7. A formula for $|A_N(D)|$

In this section we prove the following theorem.

**Theorem 7.1.** $A_N(D) = \emptyset$ if and only if Condition (C2) holds.

In order to prove Theorem 7.1, we first prove a formula for $|A_N(D)|$.

**Proposition 7.2.** Notation being as above, we have

$$|A_N(D)| = \sum_{I \supseteq \delta(D, N)} |A(D_I)| \prod_{i \in I} \frac{n_i}{d_i} \prod_{i \in A \setminus I} \left( \frac{n_i}{d_i} - 1 \right),$$

where $\delta(D, N) = \{ i \in A \mid d_i = n_i \}$ and the sum is taken over the subsets $I$ of $A$ containing $\delta(D, N)$.

In order to prove Proposition 7.2 we need further notation. Given a positive integer $d$ and an integer $a$, we denote by $[a]_d$ the unique integer such that $0 < [a]_d \leq d$, $a \equiv [a]_d \pmod{d}$.

For $D \in N^r$ and $a = (a_1, \ldots, a_r) \in Z^r$, we let

$$[a]_D = ([a_1]_{d_1}, \ldots, [a_r]_{d_r}) \in B_D.$$

Moreover, writing $a_i = d_i k_i + [a_i]_{d_i}$, and $k = (k_1, \ldots, k_r)$, we define a map

$$\pi_D : Z^r \rightarrow B_D \times Z^r, \quad a \mapsto ([a]_D, k).$$

It is then clear from the definition that $\pi_D$ is an injection and

$$\omega_D(a) = \omega_D([a]_D)$$

for any $a \in Z^r$. Hence $\pi_D(B_N(D)) = B(D)$. But $\pi_D(A_N(D))$ is not necessarily equal to $A(D)$. In order to determine the image $\pi_D(A_N(D))$, for any $I \subseteq A$, let

$$B(D, I) = \left\{ (b_1, \ldots, b_r) \in B(D) \mid \begin{array}{l} b_i \neq d_i \quad (i \in I), \\ b_i = d_i \quad (i \in I') \end{array} \right\},$$

$$K(N/D, J) = \left\{ (k_1, \ldots, k_r) \in Z^r \mid \begin{array}{l} 0 \leq k_i \leq n_i/d_i \quad (i \in A), \\ k_i < n_i/d_i \quad (i \in J) \end{array} \right\}.$$

Then we have the following

**Lemma 7.3.** Notation being as above, we have

$$\pi_D(A_N(D)) = \coprod_{I \subseteq A} B(D, I) \times K(N/D, I'').$$

**Proof.** Note that $B(D)$ is a disjoint union of $B(D, I)$’s:

$$B(D) = \coprod_{I \subseteq A} B(D, I).$$
Therefore
\[ \pi_D(B_N(D)) \subseteq \prod_{I \subseteq \Lambda} \mathbb{Z}^r \times B(D, I). \]

For each \( b = (b_1, \ldots, b_r) \in B(D, I) \), take \( a = (a_1, \ldots, a_r) \in \pi_D^{-1}(b) \) and write
\[ a_i = d_i k_i + b_i, \]
where \( k_i \) is an integer. Note that \( 0 < a_i \leq n_i \) if and only if \( 0 \leq k_i \leq \frac{n_i}{d_i} - 1 \). Moreover we have
\[ 0 < a_i < n_i \iff \begin{cases} 0 \leq k_i \leq \frac{n_i}{d_i} - 2 & \text{(if } b_i = d_i) \text{),} \\ 0 \leq k_i \leq \frac{n_i}{d_i} - 1 & \text{(if } b_i \neq d_i). \end{cases} \]

If we put \( k = (k_1, \ldots, k_r) \) then this equivalence implies that
\[ a \in A_N(D) \iff k \in K(N/D, I^c). \]

This proves the lemma. \( \square \)

**Proof of Proposition 7.2.** Lemma 7.3 shows that
\[ |A_N(D)| = \sum_{I \subseteq \Lambda} |B(D, I)| \cdot |K(N/D, I^c)|. \]

Note that taking the \( I \)-component yields a bijection \( B(D, I) \rightarrow A(D_I) \), so \[ |B(D, I)| = |A(D_I)|. \] Moreover, it is clear from the definition of \( K(N/D, I^c) \) that
\[ |K(N/D, I^c)| = \prod_{i \in I^c} (n_i/d_i - 1) \cdot \prod_{i \in I} n_i/d_i. \]

In particular,
\[ K(N/D, I^c) \neq \emptyset \iff \prod_{i \in I^c} (n_i/d_i - 1) \neq 0 \iff I \supset \delta(D, N). \]

Then proposition immediately follows from this. \( \square \)

**Proof of Theorem 7.1.** First, suppose (C2) holds. This in particular implies that \( D_2^\circ \) and \( D^{\circ} \) is strictly \( \Lambda_2 \)-disconnected. Hence, if \( A_N(D) \neq \emptyset \), then any \( a \in A_N(D) \) is of the form \( a = (a_1, D_2^\circ) \). But we have
\[ \omega_D(a) = \omega_D(a_1) + \frac{n_2}{2} \neq 0 \pmod{1}, \]
which is a contradiction. This proves that if Condition (C2) holds, then \( A_N(D) = \emptyset \).

Conversely suppose \( A_N(D) = \emptyset \). If \( |A_2| \) is even then
\[ \omega_D(D^{\circ}) = \frac{|A_2|}{2} \equiv 0 \pmod{1}, \]
so \( D^{\circ} \in A_N(D) \), which is a contradiction. Therefore we may assume that \( |A_2| \) is odd.

By Proposition 7.2, \( A_N(D) = \emptyset \) if and only if \( A(D_I) = \emptyset \) for any \( I \supset \delta(D, N) \). On the other hand, Theorem 6.1 shows that \( A(D_I) = \emptyset \) if and only if either \( D_I \) is disconnected or \( |I_2| \) is odd and \( D_I^\circ \) is strictly \( I_2 \)-disconnected.
First, we consider the case where $D_2 \neq N_2$. Then there exists $I_2$ such that $\delta(D, N) \subset I_2 \subset \Lambda_2$ and $|I_2|$ is even. For such a $I_2$, $I_2 \subset \Lambda_2$ must be disconnected, which is possible only when $I_2 = \emptyset$. Hence $\delta(D, N) = \emptyset$. But, in this case, we have $D \in AN(D)$, so $AN(D) \neq \emptyset$.

Next, suppose $D_2 = N_2$. Then Proposition 7.2 and Theorem 6.1 shows that $AN(D) = \emptyset$ if and only if either $D_I$ is disconnected or $D^i$ is strictly $\Lambda_2$-disconnected for any $I \supset \Lambda_2$. In particular, either $D$ is disconnected or $D^i$ is strictly $\Lambda_2$-disconnected. If $|\Lambda_2| > 1$ then $D$ cannot be disconnected, so $D^i$ must be strictly $\Lambda_2$-disconnected. If $|\Lambda_2| = 1$ then $D_{\Lambda_2 \cup \{i\}}$ is disconnected or is strictly $\Lambda_2$-disconnected for any $i \in \Lambda_1$, so $D^i$ is strictly $\Lambda_2$-disconnected in this case as well. □

8. Parity condition

In this section, we study the integral solution of the Diophantine equation (11) with a parity condition (12). For this purpose, we define the $\pm$-part of $AN(D)$ by

$$A^+_N(D) = \{a \in AN(D) | \varepsilon(a) \equiv 0 \pmod{2}\},$$
$$A^-_N(D) = \{a \in AN(D) | \varepsilon(a) \equiv 1 \pmod{2}\}.$$

As in the case of $AN(D)$, we simply write $A^\pm(D)$ for $A^\pm N(D)$.

The purpose of this section is to prove the following

THEOREM 8.1. Suppose $\text{ord}_2(n_i) = 1$ for any $i \in \Lambda$. Then $AN(D) = \emptyset$ if and only if either (C1) or (C2) holds.

In order to prove Theorem 2.3, we need the following proposition, which is a refinement of Proposition 7.2. To state it, we let

$$J_1(D, N) = \{I \subset \Lambda | \delta(D, N) \subset I \not\subset \Lambda_2\},$$
$$J_2(D, N) = \{I \subset \Lambda | \delta(D, N) \subset I \subset \Lambda_2\}.$$

Moreover, we let

$$K^+(N/D, J) = \{k \in K(N/D, J) | \varepsilon(k_1) \equiv 0 \pmod{2}\},$$
$$K^-(N/D, J) = \{k \in K(N/D, J) | \varepsilon(k_1) \equiv 1 \pmod{2}\},$$

where $k_1 = k_{A_1}$.

PROPOSITION 8.2. Suppose $n_1, \ldots, n_r$ are all even. Let * denote $+$ or $-$. Then

$$|A^*_N(D)| = \frac{1}{2} \sum_{I \in J_1(D, N)} |A(D_I)| \cdot |K(N/D, I^*)|$$
$$+ \sum_{I \in J_2(D, N)} \left| (A^{(-1)^{\tau_1}*}(D_I)) \cdot |K^+(N/D, I^*)| \right|$$
$$+ \sum_{I \in J_2(D, N)} \left| (A^{(-1)^{\tau_1}*}(D_I)) \cdot |K^-(N/D, I^*)| \right|,$$

where $(-1)^{\tau_1}$ denotes $(-1)^{\tau_1}$ or $-(-1)^{\tau_1}$ according as $* = +$ or $* = -$.

Before proving the proposition we prove a lemma.
LEMMA 8.3. Let $M$ be an element of $\mathbb{N}^r$ and put $X = BM$. Then the following assertions hold.

(i) If $|X|$ is even then $|X^+| = |X^-| = \frac{1}{2}|X|$.
(ii) If $|X|$ is odd and $|X| > 1$ then neither $X^+$ nor $X^-$ is empty.
(iii) If $|X| = 1$ then $X^+ = \{0, \ldots, 0\}$ and $X^- = \emptyset$.

Proof. Let $M = (m_1, \ldots, m_r)$.

(i) If $|X|$ is even then $m_i$ is even for some $i$, say $i = 1$. Consider the map

$$\iota: X \rightarrow X$$

which sends $(x_1, x_2, \ldots, x_r)$ to $(m_1 + 1 - x_1, x_2, \ldots, x_r)$. Then $\iota$ is an involution. Moreover since $\varepsilon(\iota(x)) = 1 + \varepsilon(x)$ for any $x \in X$, we have $\iota(X^+) = X^-$ and $\iota(X^-) = X^+$. Therefore

$$|X^+| = |X^-| = \frac{1}{2}|X|.$$ 

(ii) Since $(0, \ldots, 0)$ always belongs to $X^+$, we have $X^+ \neq \emptyset$. If $|X| > 1$ then $m_i > 1$ for some $i$, say $i = 1$. Then $(1, 0, \ldots, 0) \in X^-$, so $X^- \neq \emptyset$.

(iii) This is clear. □

Proof of Proposition 8.2. For any $a = (a_1, \ldots, a_r) \in B_N$, let $b = [a]_D = (b_1, \ldots, b_r)$ and write

$$a_i = d_i k_i + b_i$$

with $k_i \in \mathbb{Z}$ as in Section 7. Then

$$\varepsilon(a) \equiv \sum_{i \in A_1} k_i + \varepsilon(b) \pmod{2}.$$ 

Therefore

$$\pi_D(A_{\mathbb{N}}(D)) = \bigsqcup_{I \supseteq \delta(D, N)} \left( (B^+(D, I) \times K^+(N/D, I^c)) \sqcup (B^-(D, I) \times K^-(N/D, I^c)) \right).$$

It follows that

$$|A_{\mathbb{N}}(D)| = \sum_{I \supseteq \delta(D, N)} \left[ |B^+(D, I)| \cdot |K^+(N/D, I^c)| + |B^-(D, I)| \cdot |K^-(N/D, I^c)| \right].$$

Here $|K(N_1/D_1, (I^c)_1)|$ is odd if and only if $I \subset A_2$. To see this, put $J = I^c$ and note that

$$|K(N_1/D_1, J_1)| = \prod_{i \in I_1} \left( \frac{n_i}{d_i} - 1 \right) \cdot \prod_{i \in I_1} \frac{n_i}{d_i};$$

where $I_1 = I \cap A_1$ and $J_1 = J \cap A_1$. Since $\frac{n_i}{d_i}$ is even for any $i \in A_1$, it follows that $|K(N_1/D_1, J_1)|$ is odd if and only if $J_1 = \emptyset$, which is equivalent to $I \subset A_2$.

Thus, if $I \in J_1(D, N)$ then

$$|K^+(N/D, I^c)| = |K^-(N/D, I^c)| = \frac{1}{2} |K(N/D, I^c)|$$
by Lemma 8.3. Hence

\[
\sum_{I \in J_1(D, N)} |B^+(D, I)| \cdot |K^+(N/D, I^c)| + |B^-(D, I)| \cdot |K^-(N/D, I^c)|
\]

\[
= \frac{1}{2} \sum_{I \in J_1(D, N)} \left( |B^+(D, I)| + |B^-(D, I)| \right) \cdot |K(N/D, I^c)|
\]

\[
= \frac{1}{2} \sum_{I \in J_1(D, N)} |B(D, I)| \cdot |K(N/D, I^c)|
\]

\[
= \frac{1}{2} \sum_{I \in J_1(D, N)} |A(D_I)| \cdot |K(N/D, I^c)|.
\]

On the other hand, if \( I \in J_2(D, N) \), then taking the \( I \)-component yields a bijection

\[
B^*(D, I) \longrightarrow A(-1)^{r_1}(D_I).
\]

Therefore, the formula (17) can be rewritten as

\[
|A_N^*(D)| = \frac{1}{2} \sum_{I \in J_1(D, N)} |A(D_I)| \cdot |K(N/D, I^c)|
\]

\[
+ \sum_{I \in J_2(D, N)} \left( |A(-1)^{r_1}(D_I)| \cdot |K^+(N/D, I^c)| + |A(-1)^{r_1}(D_I)| \cdot |K^-(N/D, I^c)| \right).
\]

This proves the proposition. □

**Proposition 8.4.** Let the notation and the assumption be as in Proposition 8.2. If \( D_1^2 \neq N_1 \) then \( A_N^*(D) = \emptyset \) if and only if Condition (C2) holds.

**Proof.** If \( D_1^2 \neq N_1 \) then \( |K(N/D, I^c)| > 1 \) for any \( I \subset \Lambda \), so Lemma 8.3 shows that \( K^\pm(N/D, I^c) \neq \emptyset \) for any \( I \subset \Lambda \) with \( I \supset \delta(D, N) \). Therefore, \( A_N^*(D) = \emptyset \) if and only if \( A(D_I) = \emptyset \) for any \( I \supset \delta(D, N) \). This is equivalent to \( A_N(D) = \emptyset \) by Proposition 7.2. Then by Theorem 7.1 this holds if and only if Condition (C2) holds. □

**Proposition 8.5.** Let the notation and the assumption be as in Proposition 8.2. If \( D_1^2 = N_1 \), then \( A_N^*(D) = \emptyset \) if and only if \( A(D_I) = \emptyset \) for any \( I \in J_1(D, N) \) and \( A(-1)^{r_1}(D_I) = \emptyset \) for any \( I \in J_2(D, N) \).

**Proof.** Suppose \( D_1^2 = N_1 \). Since

\[
K^*(D, J) = K^*(N_1/D_1, J_1) \times K(N_2/D_2, J_2).
\]

and \( K(N_2/D_2, J_2) \neq \emptyset \) such that \( I \supset \delta(D, N) \), we have

\[
K^-(D, J) = \emptyset \iff K^-(N_1/D_1, J_1) = \emptyset \iff |K(N_1/D_1, J_1)| = 1.
\]

Recall that

\[
|K(N_1/D_1, J_1)| = \prod_{i \in J_1} \left( \frac{n_i}{d_i} - 1 \right) \cdot \prod_{i \in J_2} \frac{n_i}{d_i}.
\]
Since \( n_i/d_i = 2 \) for any \( i \in A_1 \), we have \(|K(N_1/D_1, J_1)| = 1\) if and only if \( J_1 = A_1 \), or equivalently \( I \subset A_2 \). In this case, we have \( K^+(N/D, J) \neq \emptyset \) and \( K^-(N/D, J) = \emptyset \) by Lemma 8.3. Consequently \( A^+_N(D) = \emptyset \) if and only if \( A(D_I) = \emptyset \) for any \( I \in J_1(D, N) \) and \( A^{(1)}(D_I) = \emptyset \) for any \( I \in J_2(D, N) \). This completes the proof.

**Proposition 8.6.** Assume that \( D^+_1 = N_1 \). If \( A(D_I) = \emptyset \) for any \( I \in J_1(D, N) \) then either \( D \) is strictly \( A_1 \)-disconnected or \((C2)\) holds.

**Proof.** Suppose the following condition holds:

\[
A(D_I) = \emptyset \quad \text{for any} \quad I \in J_1(D, N). \tag{18}
\]

By Theorem 6.1 we have \( A(D_I) = \emptyset \) if and only if either \( D_I \) is disconnected or \(|I_2|\) is odd and \( D^\circ \) is strictly \( I_2 \)-disconnected.

If \( D_2 \neq N_2 \), there exists an index set \( I_2 \) such that \( \delta(D, N) \subset I_2 \subset A_2 \) and \(|I_2|\) is even. Hence by Condition (18) we have \( A(D_{I_2 \cup K}) = \emptyset \) for any non-empty subset \( K \subset A_1 \). Theorem 6.1 then implies that \( D_{I_2 \cup K} \) is disconnected. But, since \(|I_2|\) is even, this implies that \( D_{I_2 \cup K} \) is \( K \)-disconnected for any non-empty subset \( K \subset A_1 \). Thus \( D \) is strictly \( A_1 \)-disconnected.

On the other hand, suppose \( D_2 = N_2 \). If \(|A_2|\) is even then, repeating the same argument as above, we obtain the same consequence. Thus, we may assume that \(|A_2|\) is odd.

In this case, we conclude that either \( D_{A_2 \cup \{i\}} \) is disconnected or \( D^\circ_{A_2 \cup \{i\}} \) is strictly \( A_2 \)-disconnected for any non-empty \( K \subset A_1 \).

If \( D^\circ_{A_2} \) is not strictly \( A_2 \)-disconnected, then \( D^\circ_{A_2 \cup \{i\}} \) is strictly \( A_2 \)-disconnected, so \( D_{A_2 \cup \{i\}} \) is disconnected for any non-empty \( K \subset A_1 \). Hence \( D \) is strictly \( A_1 \)-disconnected.

On the other hand, if \( D^\circ_{A_2} \) is strictly \( A_2 \)-disconnected then Condition (18) implies that either \( D_{A_2 \cup \{i\}} \) is disconnected or \( D^\circ_{A_2 \cup \{i\}} \) is strictly \( A_2 \)-disconnected. Then \( D^\circ \) is strictly \( A_2 \)-disconnected. This proves that if Condition (18) holds then either \( D \) is strictly \( A_1 \)-disconnected or \((C2)\) holds.

**Proof of Theorem 8.1.** If \((C2)\) holds, then \( A_N(D) = \emptyset \) by Theorem 7.1, hence \( A^+_N(D) = \emptyset \). If \((C1)\) holds, then any element \( a \in A_N(D) \) is of the form

\[
a = (D_1, a_2)
\]

with \( a_2 \in A_{N_1}(D_2) \). But, under the assumption that \( \text{ord}_2(n_i) = 1 \) for any \( i \in A \), the denominator of \( \omega_{D_2}(a_2) \) is odd if and only if \( e(a_2) \equiv 0 \pmod{2} \). This shows that \( A^+_N(D_2) = \emptyset \), so \( A^+_N(D) = \emptyset \).

Conversely, suppose \( A^+_N(D) = \emptyset \). If \( r_1 \) is even, then Proposition 8.2 shows that \( A(D_I) = \emptyset \) for any \( I \in J_1(D, N) \) and \( A^+(D_I) = \emptyset \) for any \( I \in J_2(D, N) \). The first condition implies that either \((C1)\) or \((C2)\) holds by Proposition 8.6, and the second condition is always satisfied by Lemma 8.3. This proves the equivalence.

Next suppose \( r_1 \) is odd. In this case, Proposition 8.2 shows that \( A^-N(D) = \emptyset \) if and only if \( A(D_I) = \emptyset \) for any \( I \in J_1(D, N) \) and \( A^+(D_I) = \emptyset \) for any \( I \in J_2(D, N) \). The second condition is satisfied only when \((C2)\) holds. This proves the equivalence.
9. Proof of Theorem 2.3

In order to state the following proposition, let $A^{\perp}(m, p)$ be the perpendicular space of $A^{-}(m, p)$ with respect to the inner product $\langle \cdot, \cdot \rangle_m$:

$$A^{-}(m, p)^{\perp} = \{ x \in V(m) \mid \langle a, x \rangle_m = 0 \ (\forall a \in A^{-}(m, p)) \}.$$

**Proposition 9.1.** Assume that $(f_i, f_j) = 1$ for any $i \in A_1$ and any $j \in A_2$. Suppose $A^{-}(m, p) \neq \emptyset$ and let $x = (x_1, \ldots, x_r) \in A^{-}(m, p)^{\perp}$. Then

$$2x = \text{Ind}(p^{2\nu})$$

for some integer $\nu$.

We need an elementary lemma.

**Lemma 9.2.** Let $n \geq 2$ and let $k_1, \ldots, k_n$ be positive integers. Then for given integers $a_1, \ldots, a_n$, the following two conditions are equivalent.

(i) There exists an integer $x$ such that $x \equiv a_i \pmod{k_i}$ for any $i = 1, \ldots, n$.

(ii) $a_i \equiv a_j \pmod{(k_i, k_j)}$ for any $i, j$ with $i \neq j$.

**Proof.** We prove the lemma in the case of $n = 2$ since the general cases are deduced from this case. Since the implication (i) $\Rightarrow$ (ii) is clear, we prove the converse implication (ii) $\Rightarrow$ (i). Let $k_{12} = \text{GCD}(k_1, k_2)$ and suppose $a_1, a_2$ satisfy the congruence $a_1 \equiv a_2 \pmod{k_{12}}$. Then there exist integers $s, t$ such that $k_1s - k_2t = a_2 - a_1$. This implies that $k_1s + a_1 = k_2t + a_2$. Therefore, if we put $x = k_1s + a_1$, then $x = k_2t + a_2$, hence $x \equiv a_1 \pmod{k_1}$ and $x \equiv a_2 \pmod{k_2}$. This proves the lemma. \qed

**Proof of Proposition 9.1.** In the following, we let

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{Z}^r$$

for each $i \in A$. Recall that

$$\text{Ind}(p) = \left( \frac{n_1}{f_1}, \ldots, \frac{n_r}{f_r} \right).$$

Thus, in order to prove the proposition, we have to show first that $x_i \equiv 0 \pmod{n_i/f_i^{2\nu}}$ for any $i$. If $f_i^{2\nu} = n_i$ then there is nothing to prove. Suppose $f_i^{2\nu} < n_i$. Then $2f_i^{2\nu} < n_i$ since $\text{ord}_2(n_i) = 1$. Let $a = (a_1, \ldots, a_r) \in A^{-}(m, p)$. If $a_i \not\equiv -f_i^{2\nu} \pmod{n_i}$ then

$$a' := a + f_i^{2\nu} e_i \in A^{-}(m, p).$$

Then we have

$$\frac{x_i f_i^{2\nu}}{n_i} \equiv \langle a', x \rangle_m - \langle a, x \rangle_m = 0.$$

It follows that $x_i \equiv 0 \pmod{n_i/f_i^{2\nu}}$. If $a_i \equiv -f_i^{2\nu} \pmod{n_i}$ then

$$a' = a - f_i^{2\nu} e_i \in A^{-}(m, p).$$

Therefore, repeating the same argument as above, we get the same result. Thus we can write $2x_i = \frac{n_i y_i}{f_i^{2\nu}}$ for some $y_i \in \mathbb{Z}$. 


Let \( f_{ij} = (f_i, f_j) \). We next show that
\[
y_i \equiv y_j \pmod{f_{ij}}.
\] (19)
If this holds for any \( i \neq j \) then there exists an integer \( y \) such that \( y \equiv y_i \pmod{f_i} \) by Lemma 9.2. Hence we have
\[
2x_i \equiv \frac{n_i y}{f_i} \pmod{n_i}
\]
for any \( i \in A \). Since \( A_2 \neq \emptyset \), we have \( 2x_i \equiv \frac{n_i y}{f_i} \pmod{n_r} \). Since \( \frac{n_i}{f_i} \) is odd, this shows that \( y \) is even, say \( y = 2\nu \) (\( \nu \in \mathbb{Z} \)). Then
\[
2x = \text{Ind}(p^{2\nu}).
\]
Thus it suffices to show that (19) holds for any \( i, j \).

If \( i \in A_1 \) and \( j \in A_2 \) then the assumption implies that \( f_{ij} = 1 \), so there is nothing to prove. Thus we may assume that either \( \{i, j\} \subset A_1 \) or \( \{i, j\} \subset A_2 \). In these two cases, both \( \frac{f_i}{f_{ij}} \) and \( \frac{f_j}{f_{ij}} \) are odd. If
\[
a_i \not\equiv -\frac{f_i}{f_{ij}} \pmod{n_i}
\]
and
\[
a_j \not\equiv \frac{f_j}{f_{ij}} \pmod{n_j}
\]
then
\[
a' := a + \frac{f_i}{f_{ij}}e_i - \frac{f_j}{f_{ij}}e_j \in A^-(m, p).
\]
Therefore
\[
\frac{y_i}{f_{ij}} - \frac{y_j}{f_{ij}} \equiv (a', x) - (a, x) \equiv 0 \pmod{1}.
\]
It follows that \( y_i \equiv y_j \pmod{f_{ij}} \). Similarly, if \( a_i \not\equiv \frac{f_i}{f_{ij}} \pmod{n_i} \) and \( a_j \not\equiv -\frac{f_j}{f_{ij}} \pmod{n_j} \) then we get the same result.

If \( a_i \equiv \frac{f_i}{f_{ij}} \pmod{n_i} \) and \( a_j \equiv \frac{f_j}{f_{ij}} \pmod{n_j} \) then we consider the element
\[
a^* = a + \frac{2f_i}{f_{ij}}e_i - \frac{2f_j}{f_{ij}}e_j.
\]
If we write \( a^* = (a_1^*, \ldots, a_r^*) \) then \( a_i^* \equiv \frac{2f_i}{f_{ij}} \pmod{n_i} \). But, since \( f_i/f_{ij} \) is odd, \( 3f_i/f_{ij} \not\equiv 0 \pmod{n_i} \). Hence \( a_i^* \not\equiv 0 \pmod{n_i} \). Quite similarly we have \( a_j^* \not\equiv 0 \pmod{n_j} \), so \( a^* \in A^-(m, p) \). Therefore, repeating the same argument as above, we get the same result. \( \square \)

**Proposition 9.3.** Suppose \( QC^-(m', p) \neq \emptyset \). If \( \chi(l) = 1 \) for any \( \chi \in QC^-(m', p) \) then
\[
l \equiv up^v \pmod{m'}
\]
for some integers \( v, u \) such that \( u^2 \equiv 1 \pmod{m'} \).

**Proof.** Put \( x = \text{Ind}(l) \). Then \( x \in A(m', p)^\perp \). Therefore Lemma 9.2 implies that
\[
2x = \text{Ind}(p^v)
\]
for some even integer \( y \), say \( y = 2v \) (\( v \in \mathbb{Z} \)). Then \( l^2 \equiv p^{2v} \pmod{m'} \), so \( l \equiv up^v \pmod{m'} \) for some \( u \in \mathbb{Z} \) such that \( u^2 \equiv 1 \pmod{m'} \). \( \square \)
**Corollary 9.4.** Let \( l, m', p \) be as above. Then for any \( \chi \in C(m', p) \) there exists a square-free divisor \( d \) of \( m' \) such that \( \chi(l) = \left( \frac{d}{m} \right) \).

**Proof.** Proposition 9.3 implies that \( l \equiv u \nu \pmod{m'} \) for some \( u \) such that \( u^2 \equiv 1 \pmod{m'} \). Thus

\[
\chi(l) = \chi(u) \chi(p) \nu = \chi(u)
\]

for any \( \chi \in C(m', p) \). We now write \( \chi = \chi^a \) with \( a \in V(m') \). Now, for each \( i \), we have

\[
\chi_i(l)^a = \begin{cases} \left( \frac{li}{d} \right) & \text{if } a_i \text{ is odd,} \\ 1 & \text{if } a_i \text{ is even.} \end{cases}
\]

Therefore, letting \( d \) be the product of \( li \) such that \( a_i \) is odd, we have \( \chi(l) = \left( \frac{d}{m} \right) \). This proves the corollary. \( \square \)

We now prove Theorem 2.3.

**Proof of Theorem 2.3.** By Proposition 4.4 \( g(m, p) \) is pure if and only if (i) \( A = (m, p) = \emptyset \) and (ii) for any \( \emptyset \neq I \subseteq A \) there exists \( l \in P(m/m_I) \) such that \( \text{Ind}(l) \in A(m_I, p)^\perp \).

The first condition holds if and only if either (C1) or (C2) holds by Theorem 8.1.

On the other hand, the second condition is satisfied if and only if for any square-free divisor \( d > 1 \) of \( m \) there exists \( l \in P(m/d) \) such that \( \left( \frac{d}{p} \right) = 1 \). But this is equivalent to \( E(m, p) = \emptyset \). The proof is now complete. \( \square \)

10. Two extreme cases

In this section, we study the set \( E(m, p) \) in two extreme cases where \( A_1 = \emptyset \) or \( A_2 = \emptyset \).

**Proposition 10.1.** If \( m \) satisfies Condition (5) then the following two assertions hold.

(i) If \( A_1 = \emptyset \) then \( E(m, p) = \emptyset \).

(ii) If \( A_2 = \emptyset \) then \( E(m, p) \neq \emptyset \).

**Remark 10.2.** The first assertion of Proposition 10.1 is actually an easy consequence of Theorem 2.3. Indeed, if \( A_1 = \emptyset \) then \( p^{f_i/2} \equiv -1 \pmod{m_i} \) for any \( i \in A \). Since \( f_i/2 \) is odd, so \( f/2 \) is an odd multiple. Hence \( p^{f/2} \equiv -1 \pmod{m} \), and \( (m, p) \) is supersingular. This, in particular, implies that \( E(m, p) = \emptyset \) by Theorem 2.3. But we give a direct proof which does not use Stickelberger’s theorem.

As for the second assertion of Proposition 10.1, note that if \( A_2 = \emptyset \) then \( f \) is odd. But this implies that \( g(m, p) \) is not pure, so Theorem 2.3 implies that either both (C1) and (C2) do not hold, or \( E(m, p) \neq \emptyset \). Proposition 10.1 shows that the latter condition does hold.

**Proof of Proposition 10.1.** (i) If \( A_1 = \emptyset \) then \( \left( \frac{d}{m} \right) = -1 \) for any \( i \), so \( \left( \frac{d}{m} \right) = \left( \frac{-1}{d} \right) \) for any \( d \in D(m_0) \). Therefore, for any \( d \in D(m_0) \), the condition \( d \equiv 3 \pmod{4} \) cannot be consistent with the condition \( \left( \frac{d}{m} \right) = 1 \). Hence \( E(m, p) = \emptyset \) if \( A_1 = \emptyset \).
(ii) If $A_2 = \emptyset$ then $\left( \frac{d}{m} \right) = 1$ for any $d \in \mathcal{D}(m_0)$. Therefore,

$$\mathcal{E}(m, p) = \{ d \in \mathcal{D}^- (m_0) \mid \left( \frac{d}{m} \right) = 1 \text{ for any } l \in \mathcal{P}(m_0) \}.$$ 

It is clear that if $r$ is odd then $\mathcal{E}(m, p) \neq \emptyset$ since $m_0 \in \mathcal{E}(m, p)$. Thus, we have only to consider the case where $r$ is even. We will see in Proposition 12.2 that if $r = 2$ then $\mathcal{E}(m, p) = \emptyset$.

In the following, we suppose $r$ is even and $r \geq 4$. For each $i \in \{1, \ldots, r\}$, let $d_i = \frac{m_0}{l_i}$.

If $\left( \frac{d_i}{m} \right) = -1$ then $d_i \in \mathcal{E}(m, p)$. Therefore, we may assume that

$$\left( \frac{l_i}{d_i} \right) = 1 \text{ for any } i \in \{1, \ldots, r\}.$$ 

For any ordered subset $\{i_1, \ldots, i_n\} \subset \{1, \ldots, r\}$, we call the $n$-tuple $(l_{i_1}, \ldots, l_{i_n})$ an $n$-chain if $i_1, \ldots, i_n$ are all distinct and

$$\left( \frac{l_{i_1}}{l_{i_2}} \right) = \left( \frac{l_{i_2}}{l_{i_3}} \right) = \cdots = \left( \frac{l_{i_{n-1}}}{l_{i_n}} \right) = 1.$$ 

Moreover we call the $n$-tuple $(l_{i_1}, \ldots, l_{i_n})$ an $n$-cycle if it is an $n$-chain and $\left( \frac{d_{i_1}}{m} \right) = 1$.

First note that if $(l_i, l_j, l_k)$ is a 3-chain, then

$$d_{ijk} := \frac{m_0}{l_il_jl_k} \in \mathcal{E}(m, p).$$ 

Indeed, since we are assuming that $\left( \frac{d_i}{m} \right) = 1$ for any $i = 1, \ldots, r$, we have

$$\left( \frac{l_i}{d_{ijk}} \right) = \left( \frac{l_i}{l_il_j} \right) \left( \frac{l_i}{l_il_k} \right) = \left( \frac{l_i}{l_i} \right) \left( \frac{l_i}{l_i} \right) = -1.$$ 

Similarly, we have $\left( \frac{l_i}{d_{ijk}} \right) = \left( \frac{d_i}{m} \right) = -1$. Therefore $d_{ijk} \in \mathcal{E}(m, p)$.

Thus, in order to prove (ii), it suffices to show that $\{l_1, \ldots, l_r\}$ contains a 3-cycle. We first show that $\{l_1, \ldots, l_r\}$ contains a cycle. To see this, assume that $\{l_1, \ldots, l_r\}$ contains no cycle. Note that for any $i$ there exists $i$ such that $\left( \frac{l_i}{l_i} \right) = 1$. Indeed, if $\left( \frac{l_i}{l_i} \right) = -1$ for any $j$, then

$$\left( \frac{l_i}{d_i} \right) = \prod_{j \neq i} \left( \frac{l_i}{l_j} \right) = (-1)^{r-1} = -1,$$

which is a contradiction. This, in particular, implies that $\{l_1, \ldots, l_r\}$ contains a chain of length $\geq 3$. Let $(l_1, \ldots, l_n)$ be a chain. Since we are assuming that this contains no cycle, there exists $j \notin \{1, \ldots, n\}$ such that $\left( \frac{l_j}{l_j} \right) = 1$. Hence $(l_1, \ldots, l_n, l_j)$ is a chain.

Repeating the same argument and renumbering $l_1, \ldots, l_r$ if necessary, we may assume that $(l_1, \ldots, l_r)$ is a chain. Since $\left( \frac{l_1}{l_1} \right) = 1$ for some $i$, we obtain a cycle $(l_1, \ldots, l_r)$, which is a contradiction. Therefore $(l_1, \ldots, l_r)$ contains a cycle.

Let $(l_1, \ldots, l_n)$ be a cycle of the minimal length. If $\left( \frac{l_i}{l_i} \right) = 1$ for some $i \in \{3, \ldots, n - 1\}$, then $(l_1, \ldots, l_i)$ is a cycle of length $i < n$, which is a contradiction. Hence $\left( \frac{l_i}{l_i} \right) = 1$.
for any $i \in \{3, \ldots, n-1\}$. But in this case, $(l_1, l_{n-1}, l_n)$ is a 3-cycle, which proves that $(l_1, \ldots, l_n)$ contains a 3-cycle, as desired. \qed

**Corollary 10.3.** If $A_2 = \emptyset$ then $g(m, p)$ cannot be pure.

**Proof.** This is a direct consequence of Proposition 10.1 and Theorem 2.3. \qed

11. **Sufficient conditions for $E(m, p) = \emptyset$**

In order to give some examples of $(m, p)$ for which $A_1 \neq \emptyset$ and $E(m, p) = \emptyset$, we consider the following condition on an $s$-tuple of odd prime numbers $(p_1, \ldots, p_s)$:

\[
\left( \frac{p_i}{p_j} \right) = \begin{cases} 
1 & (i < j), \\
-1 & (i > j).
\end{cases}
\]

We say that $(p_1, \ldots, p_s)$ is a line if Condition (20) holds. On the other hand, recall that we say that $(p_1, \ldots, p_s)$ is a cycle if

\[
\left( \frac{p_1}{p_2} \right) = \cdots = \left( \frac{p_{s-1}}{p_s} \right) = \left( \frac{p_s}{p_1} \right) = 1.
\]

**Lemma 11.1.** For prime factors $l_1, \ldots, l_r$ of $m$, the following assertions hold.

(i) If $(l_1, \ldots, l_r)$ is a cycle, then none of $l_1, \ldots, l_r$ belongs to $E(m, p)$.

(ii) If $(l_1, \ldots, l_r)$ is a line, then none of $l_1, \ldots, l_r$ belongs to $E(m, p)$.

**Proof.** This is clear from the definition of $E(m, p)$. \qed

**Theorem 11.2.** Let $m$ be as in Theorem 2.3 and assume that $A_1 \neq \emptyset$ and $A_2 \neq \emptyset$. Then $E(m, p) = \emptyset$ if one of the following conditions holds.

(i) $r_2$ is odd, $(l_{r_1+1}, \ldots, l_r)$ is a line and

\[
\left( \frac{l_i}{l_j} \right) = (-1)^{j-i} (i \in A_1, \ j \in A_2).
\]

(ii) Both $r_1$ and $r_2$ are even, both $(l_1, \ldots, l_{r_1})$ and $(l_{r_1+1}, \ldots, l_r)$ are lines and

\[
\left( \frac{l_i}{l_j} \right) = \begin{cases} 
1 & (i < j - r_1), \\
-1 & (i \geq j - r_1) \quad (i \in A_1, \ j \in A_2).
\end{cases}
\]

**Proof.** (i) For any $d \in D(m_0)$, take $I_1 \subset A_1$ and $I_2 \subset A_2$ such that $d = d_1d_2$, where

\[
d_1 = \prod_{i \in I_1} l_i, \quad d_2 = \prod_{j \in I_2} l_j.
\]

Note that \((\frac{d}{d}) = 1\) if and only if $I_2$ is even, and $d \equiv 3 \pmod{4}$ if and only if $|I_1| = |I_2|$ is odd. Thus we may assume that $|I_1|$ is odd and $|I_2|$ is even. Then, in particular, $I_2 \neq A_2$ since $A_2$ is odd. Let $v = \min(A_2 \setminus I_2)$. Then

\[
\left( \frac{l_v}{d} \right) = \left( \frac{l_v}{d_1} \right) \left( \frac{l_v}{d_2} \right) = \prod_{i \in I_1} \left( \frac{l_v}{l_i} \right) \cdot \prod_{j \in I_2} \left( \frac{l_v}{l_j} \right) = \left( (-1)^{v-r_1} |I_1| \cdot (-1)^{v-r_1-1} \right) = 1.
\]

It follows that $d \not\in E(m, p)$, so $E(m, p) = \emptyset$. 

Pure Gauss sums 157
(ii) Since we are assuming that both \( r_1 \) and \( r_2 \) are even, one of the following two cases occurs.

(Case 1) : There exists \( \nu \in \Lambda_1 \) such that \( \{1, 2, \ldots, \nu \} \subset I_1 \), \( \nu \in A_1 \setminus I_1 \) and \( \{r_1 + 1, \ldots, r_1 + \nu - 1\} \in I_2 \).

(Case 2) : There exists \( \nu \in \Lambda_1 \) such that \( \{1, 2, \ldots, \nu \} \subset I_1 \) and \( \{r_1 + 1, \ldots, r_1 + \nu - 1\} \in I_2 \) and \( r_1 + \nu \in A_2 \setminus I_2 \).

In Case 1, since \((l_1, \ldots, l_{r_1})\) is a line, we have \( \left( \frac{l_\nu}{d_2} \right) = (-1)^{\nu-1} \). On the other hand, we have

\[
\left( \frac{l_\nu}{d_2} \right) = \prod_{j < \nu} \left( \frac{l_\nu}{l_j} \right) \cdot \prod_{j \geq \nu} \left( \frac{l_\nu}{l_j} \right) = (-1)^{|I_2|-(\nu-1)} = (-1)^{\nu-1}.
\]

Therefore \( \left( \frac{l_\nu}{d_2} \right) = 1 \), so \( \mathcal{E}(m, p) = \emptyset \).

In Case 2, since \((l_{r_1+1}, \ldots, l_{r})\) is a line, we have \( \left( \frac{l_{r_1+\nu}}{d_1} \right) = (-1)^{\nu-1} \). On the other hand, we have

\[
\left( \frac{l_{r_1+\nu}}{d_1} \right) = \prod_{i \in \Lambda_1} \left( \frac{l_{r_1+\nu}}{l_i} \right) \cdot \prod_{i \in \Lambda_2} \left( \frac{l_{r_1+\nu}}{l_i} \right) = (-1)^{\nu-1}.
\]

Therefore \( \left( \frac{l_\nu}{d_2} \right) = 1 \), so \( \mathcal{E}(m, p) = \emptyset \). \( \Box \)

The following tables illustrate the conditions of (i) and (ii), respectively.

**Table 1.** \( r_1 = 4, r_2 = 3 \)

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>+</td>
<td>−</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>−*</td>
<td>*</td>
<td>*</td>
<td>+</td>
<td>−</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>−*</td>
<td>−*</td>
<td>*</td>
<td>+</td>
<td>−</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>−*</td>
<td>−*</td>
<td>−*</td>
<td>+</td>
<td>−</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>−</td>
<td>−</td>
<td>−</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>−</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>−</td>
<td>−</td>
<td>−</td>
<td>−</td>
<td>−</td>
<td>−</td>
<td></td>
</tr>
</tbody>
</table>

In Table 1 we consider the case where \( \Lambda_1 = \{1, 2, 3, 4\} \) and \( \Lambda_2 = \{5, 6, 7\} \), and in Table 2 we consider the case where \( \Lambda_1 = \{1, 2, 3, 4\} \) and \( \Lambda_2 = \{5, 6, 7, 8\} \). The signs of in
the \((i, j)\) component of the tables mean the sign of the Legendre symbols \((\frac{i}{j})\). Moreover, \(*\) denotes arbitrary sign.

12. \(\mathcal{E}(m, p)\) in the case of \(r \leq 4\)

In this section we determine \(\mathcal{E}(m, p)\) for square-free positive integers \(m\) satisfying Condition (5) with \(r \leq 4\).

As we have seen in Proposition 10.1, if \(\Lambda_1 = \emptyset\) then \(\mathcal{D}^-(m, p) = \emptyset\), so \(\mathcal{E}(m, p) = \emptyset\). Therefore we only consider the case where \(\Lambda_1 \neq \emptyset\) in the following propositions.

**Proposition 12.1.** Suppose \(m = l_1\) and \(\Lambda_1 = \{1\}\). Then \(\mathcal{E}(m, p) = \{l_1\}\).

*Proof.* We have \(\mathcal{D}^-(m, p) = \{l_1\}\), and the proposition immediately follows. \(\square\)

**Proposition 12.2.** Suppose \(m = l_1l_2\).

(i) If \(\Lambda_1 = \{1\}\) and \(\Lambda_2 = \{2\}\) then

\[
\mathcal{E}(m, p) = \begin{cases} 
\{l_1\} & \text{if } \left(\frac{l_1}{l_2}\right) = 1, \\
\emptyset & \text{if } \left(\frac{l_1}{l_2}\right) = -1. 
\end{cases}
\]

(ii) If \(\Lambda_1 = \{1, 2\}\) and \(\Lambda_2 = \emptyset\) then, assuming that \(\left(\frac{1}{l_2}\right) = 1\), we have \(\mathcal{E}(m, p) = \{l_1\}\).
PROPOSITION 12.3. Suppose \( m = l_1 l_2 l_3 \).

(i) If \( A_1 = \{1\} \) and \( A_2 = \{2, 3\} \) then, assuming that \( \left( \frac{1}{n} \right) = 1 \), we have

\[
E(m, p) = \begin{cases} 
\{l_1, m\} & \text{if } \left( \frac{1}{n} \right) = 1, \\
\{m\} & \text{otherwise}.
\end{cases}
\]

(ii) If \( A_1 = \{1, 2\} \) and \( A_2 = \{3\} \) then, assuming that \( \left( \frac{1}{n} \right) = 1 \), we have

\[
E(m, p) = \begin{cases} 
\{l_1\} & \text{if } \left( \frac{1}{n} \right) = 1, \\
\emptyset & \text{if } \left( \frac{1}{n} \right) = -1.
\end{cases}
\]

(iii) If \( A_1 = \{1, 2, 3\} \) and \( A_2 = \emptyset \) then, assuming that \( \left( \frac{1}{n} \right) = 1 \), we have

\[
E(m, p) = \begin{cases} 
\{l_1, m\} & \text{if } \left( \frac{1}{n} \right) = 1, \\
\{m\} & \text{if } \left( \frac{1}{n} \right) = -1.
\end{cases}
\]

Proof. In the case of (i), we may assume that \( \left( \frac{1}{n} \right) = 1 \) without loss of generality. We then have \( D^-(m, p) = \{l_1, m\} \) and \( m \in E(m, p) \). Moreover, \( l_1 \) belongs to \( E(m, p) \) if and only if \( \left( \frac{1}{l_2} \right) = \left( \frac{1}{n} \right) = 1 \). This proves (i).

In the case of (ii), we may assume that \( \left( \frac{1}{n} \right) = 1 \) without loss of generality. We then have \( D^-(m, p) = \{l_1, l_2\} \). Since \( \left( \frac{1}{l_2} \right) = 1, l_2 \) cannot belong to \( E(m, p) \). Moreover, \( l_1 \) belongs to \( E(m, p) \) if and only if \( \left( \frac{1}{l_2} \right) = \left( \frac{1}{n} \right) = 1 \). This proves (ii).

In the case of (iii), we may assume that \( \left( \frac{1}{l_2} \right) = \left( \frac{1}{l_3} \right) = 1 \) without loss of generality. We then have \( D^-(m, p) = \{l_1, l_2, l_3, m\} \) and \( m \in E(m, p) \). This, in particular, implies that neither \( l_2 \) nor \( l_3 \) belongs to \( E(m, p) \). Moreover, \( l_1 \) belongs to \( E(m, p) \) if and only if \( \left( \frac{1}{l_2} \right) = \left( \frac{1}{l_3} \right) = 1 \). This proves (iii).

\[\square\]

REMARK 12.4. Note that the second case of (ii) in Proposition 12.3 is one of the cases studied by Evans mentioned in Section 2.

PROPOSITION 12.5. Suppose \( m = l_1 l_2 l_3 l_4 \) and put \( d_i = m / l_i \) for \( i = 1, 2, 3, 4 \).

(i) If \( A_1 = \{1\} \) and \( A_2 = \{2, 3, 4\} \) then, without loss of generality, we may assume that \( \left( \frac{1}{n} \right) = \left( \frac{1}{l_1} \right) = 1 \).
(i-1) If \(\left(\frac{l_4}{l_2}\right) = 1\) then \((l_2, l_3, l_4)\) is cycle and \(E(m, p)\) is given as follows.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>(E(m, p))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>({l_1})</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>({d_4})</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>({d_3, d_4})</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>({d_2, d_3, d_4})</td>
</tr>
</tbody>
</table>

(i-2) If \(\left(\frac{l_4}{l_2}\right) = -1\) then \((l_2, l_3, l_4)\) is a line and \(E(m, p)\) is given as follows.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>(E(m, p))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>({l_1, d_2, d_4})</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>({d_2})</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>({d_2, d_3, d_4})</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>({d_2, d_3})</td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>({d_4})</td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>({d_3, d_4})</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>({d_3})</td>
</tr>
</tbody>
</table>
(ii) If \( \Lambda_1 = \{1, 2\} \) and \( \Lambda_2 = \{3, 4\} \) then, without loss of generality, we may assume that \( \left( \frac{l_1}{l_2} \right) = \left( \frac{l_3}{l_4} \right) = 1 \). Then \( E(m, p) \) is given as follows.

<table>
<thead>
<tr>
<th>( \left( \frac{l_1}{l_2} \right) )</th>
<th>( \left( \frac{l_1}{l_2} \right) )</th>
<th>( \left( \frac{l_3}{l_4} \right) )</th>
<th>( E(m, p) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>{l_1, d_1, d_2}</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>{l_1, d_1}</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>{d_2}</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>\emptyset</td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>{d_2}</td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>\emptyset</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>{d_1, d_2}</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>\emptyset</td>
</tr>
</tbody>
</table>

(iii) If \( \Lambda_1 = \{1, 2, 3\} \) and \( \Lambda_2 = \{4\} \) then, without loss of generality, we may assume that \( \left( \frac{l_1}{l_2} \right) = \left( \frac{l_3}{l_4} \right) = 1 \).

(iii-1) If \( \left( \frac{l_1}{l_2} \right) = 1 \) then \( (l_1, l_2, l_3) \) is a cycle and \( E(m, p) \) is given as follows.

<table>
<thead>
<tr>
<th>( \left( \frac{l_1}{l_2} \right) )</th>
<th>( \left( \frac{l_1}{l_2} \right) )</th>
<th>( \left( \frac{l_3}{l_4} \right) )</th>
<th>( E(m, p) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>{d_4}</td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>\emptyset</td>
</tr>
</tbody>
</table>
(iii-2) If \( \left( \frac{a}{p} \right) = -1 \) then \( (l_1, l_2, l_3) \) is a line and \( \mathcal{E}(m, p) \) is given as follows.

<table>
<thead>
<tr>
<th>( \left( \frac{l_1}{l_2} \right) )</th>
<th>( \left( \frac{l_1 l_3}{l_4} \right) )</th>
<th>( \mathcal{E}(m, p) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>{l_1, d_4}</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>{l_1}</td>
</tr>
<tr>
<td>-1</td>
<td>1</td>
<td>\emptyset</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>{d_4}</td>
</tr>
</tbody>
</table>

(iv) Suppose \( \Lambda_1 = \{1, 2, 3, 4\} \) then \( l_1, l_2, l_3, l_4 \) are completely symmetric.

(iv-1) If \( \{l_1, l_2, l_3, l_4\} \) contains a 3-cycle, say \( (l_1, l_2, l_3) \), then \( \mathcal{E}(m, p) \) is given as follows.

<table>
<thead>
<tr>
<th>( \left( \frac{l_1}{l_2} \right) )</th>
<th>( \left( \frac{l_2}{l_3} \right) )</th>
<th>( \left( \frac{l_3}{l_4} \right) )</th>
<th>( \mathcal{E}(m, p) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>{d_1, d_2, d_3, d_4}</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>{d_1, d_2}</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>{d_1, d_4}</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>{d_4}</td>
</tr>
</tbody>
</table>

(iv-2) If \( \{l_1, l_2, l_3, l_4\} \) contains no 3-cycle then, after renumbering \( l_1, l_2, l_3, l_4 \) properly, we may assume that \( (l_1, l_2, l_3, l_4) \) is a line. In this case we have \( \mathcal{E}(m, p) = \{l_1, d_2, d_4\} \).

Proof. (i) If \( \Lambda_1 = \{1\} \) and \( \Lambda_2 = \{2, 3, 4\} \) then

\[
\mathcal{E}(m, p) \subset \mathcal{D}^- (m, p) = \{l_1, d_2, d_3, d_4\}.
\]

Moreover, if \( (l_2, l_3, l_4) \) is a cycle, then one can easily see that

\[
\left( \frac{l_i}{d_i} \right) = \left( \frac{l_1}{l_i} \right)
\]

for any \( i = 2, 3, 4 \). The assertion of (i-1) then immediately follows from this.

On the other hand, if \( (l_2, l_3, l_4) \) is a line, then one can easily see that

\[
\left( \frac{l_2}{d_2} \right) = -\left( \frac{l_1}{l_2} \right), \quad \left( \frac{l_3}{d_3} \right) = \left( \frac{l_1}{l_3} \right), \quad \left( \frac{l_4}{d_4} \right) = -\left( \frac{l_1}{l_4} \right).
\]

The assertion of (i-2) immediately follows from this.
(ii) If \( A_1 = \{1, 2\} \) and \( A_2 = \{3, 4\} \) then \( D^-(m, p) = \{l_1, l_2, d_1, d_2\} \). Since
\[
\left( \frac{l_1}{l_2} \right) = \left( \frac{l_1}{d_1} \right) = 1,
\]
l_2 does not belong to \( \mathcal{E}(m, p) \), so \( \mathcal{E}(m, p) \subset \{l_1, d_1, d_2\} \). Moreover, we have
\[
\left( \frac{l_1}{d_1} \right) = \left( \frac{l_1}{l_3} \right) \left( \frac{l_1}{l_4} \right), \quad \left( \frac{l_2}{d_2} \right) = -\left( \frac{l_2}{l_3d_4} \right).
\]
The assertion of (ii) then immediately follows from this.

(iii) If \( A_1 = \{1, 2, 3\} \) and \( A_2 = \{4\} \) then \( D^-(m, p) = \{l_1, l_2, l_3, d_4\} \). Moreover, if \( (l_1, l_2, l_3) \) is a cycle, then none of \( l_1, l_2, l_3 \) belongs to \( \mathcal{E}(m, p) \) by Lemma 11.1, so \( \mathcal{E}(m, p) \subset \{d_4\} \). Since
\[
\left( \frac{l_4}{d_4} \right) = -\left( \frac{l_1l_2l_3}{l_4} \right),
\]
the assertion of (iii-1) holds.

On the other hand, if \( (l_1, l_2, l_3) \) is a line, then neither \( l_2 \) nor \( l_3 \) belongs to \( \mathcal{E}(m, p) \) by Lemma 11.1, so \( \mathcal{E}(m, p) \subset \{l_1, d_4\} \). In this case, we have
\[
\left( \frac{l_4}{d_4} \right) = -\left( \frac{l_3}{l_4} \right),
\]
and the assertion of (iii-2) holds.

(iv) If \( A_1 = \{1, 2, 3, 4\} \) then \( D^-(m, p) = \{l_1, l_2, l_3, l_4, d_1, d_2, d_3, d_4\} \). Moreover, if \( (l_1, l_2, l_3) \) is a cycle, then \( \mathcal{E}(m, p) \subset \{l_4, d_1, d_2, d_3, d_4\} \). Since
\[
\left( \frac{l_1}{d_1} \right) = \left( \frac{l_1}{l_4} \right), \quad \left( \frac{l_2}{d_2} \right) = -\left( \frac{l_2}{l_4} \right), \quad \left( \frac{l_3}{d_3} \right) = -\left( \frac{l_1}{l_4} \right), \quad \left( \frac{l_4}{d_4} \right) = -\left( \frac{l_1l_2l_3}{l_4} \right),
\]
the assertion of (iv-1) holds.

On the other hand, if \( (l_1, l_2, l_3, l_4) \) is a line, then none of \( l_2, l_3, l_4 \) belong to \( \mathcal{E}(m, p) \) by Lemma 11.1, so \( \mathcal{E}(m, p) \subset \{l_1, d_1, d_2, d_3, d_4\} \). Moreover, we have
\[
\left( \frac{l_1}{d_1} \right) = 1, \quad \left( \frac{l_2}{d_2} \right) = -1, \quad \left( \frac{l_3}{d_3} \right) = 1, \quad \left( \frac{l_4}{d_4} \right) = -1,
\]
so \( \mathcal{E}(m, p) = \{l_1, d_2, d_4\} \), which proves (iv-2). This completes the proof. \( \square \)

References

[ 12 ] Sun, Q., Wan, D. Q. and Ma, D., On the Diophantine equation $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod{1}$, Chinese Ann. of Math. Ser. B **7**, No. 2 (1986), 232–236.