A METHOD OF STUDYING THE MULTIPLIER CONJECTURE AND SOME PARTIAL SOLUTIONS FOR IT*

Qiu Weisheng

Institute of Mathematics, Peking University
Beijing 100871, People's Republic of CHINA

Abstract

This paper sketch the method of studying the Multiplier Conjecture that we presented in [1], and add one lemma. Applying this method we obtain some partial solutions for it: in the case $n = 2n_1$, the Second Multiplier Theorem holds without the assumption " $n_1 > \lambda$ ", except that one case is yet undecided where n_1 is odd and $7||v$ and $t \equiv 3, 5$, or 6 $(mod \quad 7)$, and for every prime divisor $p(\neq 7)$ of v such that the order w of 2 mod p satisfies that $2|\frac{\phi(p)}{w}$; in the case $n = 3n_1$ and $(v, 3 \cdot 11) = 1$, then the Second Multiplier Theorem holds without the assumption " $n_1 > \lambda$ ", except that one case is yet undecided where n_1 can not divide by 3 and $13||v$ and the order of t mod 13 is 12, 4 or 6, 2, and for every prime divisor $p(\neq 13)$ of v such that the order w of 3 mod p satisfies that $2|\frac{\phi(p)}{w}$. These distinctly improve McFarland's corresponding results and Turyn's result.

§1. Introduction

Multiplier Theorem . *Let G be an abelian group with a (v, k, λ)-difference set D, and let p be a prime dividing n but not v. If $p > \lambda$, then $\mu_p : g \longmapsto g^p$ $(\forall g \in G)$ is a multiplier of D.*

The condition "$p > \lambda$" is crucial to all known proofs of the Multiplier Theorem. However, no examples are known showing that this

---

*The project supported by National Natural Science Foundation of China.

restriction is necessary. The following has been conjectured.

Multiplier Conjecture . *The Multiplier Theorem holds without the assumption that* $p > \lambda$.

Since then virtually all further multiplier theorem have arisen in an attempt to weaken the condition $p > \lambda$.

In 1955 Bruck([2]) proved the following theorem which is called Second Multiplier Theorem, where the assumption "$p > \lambda$" is replaced by "$n_1 > \lambda$".

Second Multiplier Theorem . *Let G be an abelian group with a (v, k, λ)-difference set D, and let v_0 be the exponent of G, let n_1 be a divisor of $n = k - \lambda$ such that $(n_1, v) = 1$, and $n_1 > \lambda$. Suppose that t is an integer such that for every prime divisor p of n_1, there exists a positive integer j such that $t \equiv p^j (mod \quad v_0)$. Then $\mu_t : g \longmapsto g^t$ $(\forall g \in G)$ is a multiplier of D.*

In 1963 Newman([3]) proved : If $n = 2p$ and G is a cyclic group, then the assumption "$p > \lambda$" can be replaced by "$(v, 7) = 1$ ".

In 1964 Turyn([4]) proved : If $n = 2p^r$, then the assumption "$p > \lambda$ " can be replaced by " r is odd ".

In 1970 McFarland([5], [6] or [7]) proved : If $n = 2n_1$, then the assumption "$n_1 > \lambda$" can be replaced by " v and $2 \cdot 7$ are coprime "; if $n = 3n_1$, then the assumption "$n_1 > \lambda$" can be replaced by "v and $2 \cdot 3 \cdot 11 \cdot 13$ are coprime"; if $n = 4n_1$, then the assumption "$n_1 > \lambda$" can be replaced by "v and $2 \cdot 3 \cdot 7 \cdot 31$ are coprime"; etc.

In 1987 Wu Xiao-hong ([8]) proved : If $n = n_1$ and G is a cyclic group with prime order, then the assumption "$n_1 > \lambda$" may be removed.

In 1992 we([1]) presented a character approach to the Multiplier Conjecture, and proved : if $n = 3n_1$ and $(v, 3 \cdot 13) = 1$, then in the majority of the cases the assumption "$n_1 > \lambda$" may be removed.

This paper sketch the method of studying the Multiplier Conjecture that we presented in [1], and add one lemma. Applying this method we prove :

(1) If $n = n_1$, then the assumption "$n_1 > \lambda$" may be removed;

(2) If $n = 2n_1$, then the assumption "$n_1 > \lambda$" may be removed, except that one case is yet undecided where n_1 is odd and $7||v$ and $t \equiv 3, 5$, or $6 \pmod{7}$, and for every prime divisor $p(\neq 7)$ of v such that the order w of 2 mod p satisfies that $2|\frac{\phi(p)}{w}$;

(3) If $n = 3n_1$ and $(v, 3 \cdot 11) = 1$, then the assumption " $n_1 > \lambda$ " may be removed, except that one case is yet undecided where n_1 can not divide by 3 and $13||v$ and the order of t mod 13 is 12, 4 or 6, 2, and for every prime divisor $p(\neq 13)$ of v such that the order w of 3 mod p satisfies that $2|\frac{\phi(p)}{w}$.

These distinctly improve McFarland's corresponding results, Newman's result and Turyn's result. Wu's result is merely a particular case of (1).

§2. A Method of Studying the Multiplier Conjecture

A method of studying the Multiplier Conjecture contains the following lemma 1, theorem 1, lemma 2, lemma 3, lemma 4, and lemma 5.

Lemma 1. *Let G be an abelian group with a (v, k, λ)- difference set D, and let v_0 be the exponent of G. Set $n = k - \lambda$. Let $n = dn_1$ (d is a positive integer), and $(n_1, v) = 1$. Suppose that t is an integer such that for every prime divisor p of n_1, there exists a positive integer j such that $t \equiv p^j \pmod{v_0}$. Set $\mu_t : g \longmapsto g^t, \forall g \in G$. If every prime divisor q of d satisfy $q|n_1$, then μ_t is a multiplier of D.*

Proof. See [1].

We denote the complex character group of an abelian group G by $\hat{G}$. Let $G = \{g_1, g_2, \cdots, g_v\}$, where $g_1 = 1$. Supposed that

$$G = < g_{l_1} > \times < g_{l_2} > \times \cdots \times < g_{l_s} > . \qquad (1)$$

Let the order of g_{l_i} be $p_i^{\alpha_i}$, $1 \leq i \leq s$. Let ω_i be a primitive $p_i^{\alpha_i}$-th root of 1, $1 \leq i \leq s$. Given $g = g_{l_1}^{t_1} \cdots g_{l_s}^{t_s}$, set

$$\chi_g\left(g_{l_1}^{r_1} \cdots g_{l_s}^{r_s}\right) = \omega_1^{r_1 t_1} \cdots \omega_s^{r_s t_s},$$

then $g \longmapsto \chi_g$ is an isomorphism of G onto $\hat{G}$. We rewrite χ_{g_i} as χ_i. Thus $g_i \longmapsto \chi_i$ $(1 \leq i \leq v)$ is an isomorphism of G onto $\hat{G}$, where χ_1 is the principal character of G. Clearly

$$\sum_{l=1}^{v} \chi_l(g_1) = v. \qquad (2)$$

By the second orthogonality relation of characters we have

$$\sum_{l=1}^{v} \chi_l(g_j) = 0, \qquad 2 \leq j \leq v. \qquad (3)$$

Let v_0 be the exponent of G, then $\chi_l(g_j)$ is a v_0-th root of 1, $1 \leq l \leq v$, $1 \leq j \leq v$.

Let $\overline{\chi_l}$ denote the character afforded by the contragredient representation of the representation χ_l. By [9] we have

$$\overline{\chi_l}(g_j) = \overline{\chi_l(g_j)}, \quad 1 \leq l, j \leq v. \qquad (4)$$

and

$$\overline{\chi_l} = \chi_l^{-1} \qquad 1 \leq l \leq v. \qquad (5)$$

Let $D = \{g_{r_1}, \cdots, g_{r_k}\}$ is a subset of G. Consider the group algebras QG and $Q\hat{G}$ over the rational field Q. Since $g_1, g_2, \cdots, g_v$ is a basis of QG, by the definition of difference set D is a (v, k, λ)-difference set if and only if

$$\begin{aligned} \sum_{i=1}^{k} g_{r_i} \cdot \sum_{j=1}^{k} g_{r_j}^{-1} &= k g_1 + \lambda \sum_{l=2}^{v} g_l \\ &= n g_1 + \lambda \sum_{l=1}^{v} g_l, \qquad (6) \end{aligned}$$

where $n = k - \lambda$. Since $G \cong \hat{G}$, we get $QG \cong Q\hat{G}$. Thus D is a (v, k, λ)-difference set if and only if

$$\sum_{i=1}^{k} \chi_{r_i} \cdot \sum_{j=1}^{k} \overline{\chi_{r_j}} = n\chi_1 + \lambda \sum_{l=1}^{v} \chi_l. \qquad (7)$$

We denote the character ring of G by char(G).

Let d be a positive integer. Consider the following equations :

$$\begin{cases} \sum_{l=1}^{v} c_l = d, & (8) \\ \sum_{l=1}^{v} {c_l}^2 = d^2, & (9) \\ \xi\bar{\xi} = d^2\chi_1, & (10) \end{cases}$$

where $\xi = \sum_{l=1}^{v} c_l\chi_l$, $\bar{\xi} := \sum_{l=1}^{v} c_l\overline{\chi_l}$, and $c_1, \cdots, c_v$ are integers. The equation (10) implies (9).

Clearly $\xi_1 = d\chi_s \quad \forall \chi_s \in \hat{G}$ are solutions of (8), (9) and (10). They are called trivial solutions.

Definition 1. Let d be a positive integer. A solution $\xi \in char(G)$ of (8), (9) and (10) is called nontrivial if $\xi \neq d\chi_s \quad \forall \chi_s \in \hat{G}$.

Theorem 1. *Let G be an abelian group with a (v, k, λ)-difference set $D = \{g_{r_1}, \cdots, g_{r_k}\}$. Let $g_i \longmapsto \chi_i$ $(1 \leq i \leq v)$ be an isomorphism of G onto its character group $\hat{G}$, where χ_1 is the principal character of G. Let $n = dn_1$ and $(n_1, v) = 1$. Let t be an integer meeting the conditions of the Second Multiplier Theorem . If there is a condition C so that no nontrivial solution ξ of (8) and (10) also satisfies*

$$\sum_{i=1}^{k} {\chi_{r_i}}^t \cdot \sum_{j=1}^{k} \overline{\chi_{r_j}} = n_1\xi + \lambda\sum_{l=1}^{v} \chi_l, \qquad (11)$$

then we can replace "$n_1 > \lambda$" by condition C in the Second Multiplier Theorem.

Proof. It follows immediately from the theorem 1 in [1].

Definition 2. If a nontrivial solution $\xi = \chi_{l_m}(\sum_{i=1}^{m-1} c_{l_i}\chi_{l_i} + c_{l_m}\chi_1)$ such that $\chi_{l_i}(1 \leq i \leq m-1)$ are in a cyclic group $< \chi_u >$, then ξ is called a cyclic solution and χ_u is called a generator of ξ. If $\chi_{l_i}(1 \leq i \leq m-1)$ are in a group with prime order p, then ξ is called a p-solution.

Let G be an abelian group of order v. Decompose G as a product of cyclic groups with prime power order. Given any prime divisor p of v, there are only four possible cases :

Case 1. There is at least one generator with order p^e, $e > 1$;

Case 2. No generator have order $p^e (e > 1)$, but there are at least two generators with order p;

Case 3. $p || v$ and $v \neq p$;

Case 4. $v = p$.

In the case 1 set $v_1 = p^e$. In the case 2 set $v_1 = p$. In the case 3 set $v_1 = pp_2$, where p_2 is another prime divisor of v. Let ς be a primitive v_1-th root of 1. $Q(\varsigma)$ denotes the v_1-th cyclotomic field. B denotes the ring of algebraic integers in $Q(\varsigma)$. For integer t meeting the conditions of the Second Multiplier Theorem we have $(t, v_0) = 1$. Thus $(t, v_1) = 1$. Hence there is a Q-automorphism σ_t of $Q(\varsigma)$ such that $\sigma_t(\varsigma) = \varsigma^t$. Let $(d) = D_1 D_2 \cdots D_r$, where (d) donotes the ideal generated by a positive integer d in B, and $D_i (i = 1, \cdots, r)$ are prime ideals in B.

Condition A. σ_t such that either

$$\sigma_t(D_{i_1}) \cdots \sigma_t(D_{i_h}) D_{i_{h+1}} \cdots D_{i_{2h}} = (d)$$

for any r_th permutation $i_1 \cdots i_h i_{h+1} \cdots i_r$, or

$$\sigma_t(D_{i_1}) \cdots \sigma_t(D_{i_h}) D_{i_{h+1}} \cdots D_{i_{2h}} \neq (d)$$

for any r_th permutation $i_1 \cdots i_h i_{h+1} \cdots i_r$, where $2h = r$.

Lemma 2. *Let G be an abelian group with a (v, k, λ)-difference set $D = \{g_{r_1}, \cdots, g_{r_k}\}$. Let $g_i \longmapsto \chi_i$ $(1 \leq i \leq v)$ be the isomorphism of G onto its character group $\hat{G}$, where χ_1 is the principal character of G. Let $n = dn_1$ and $(d, n_1) = 1$, and $(d, v) = 1$, and let t be an integer meeting the conditions of the Second Multiplier Theorem. Let $\xi_p = \chi_b(\sum_{i=1}^{m-1} c_{l_i} \chi_w{}^{s_i} + c_{l_m} \chi_1)$ be a p-solution of the equations (8), (9) and (10), where $0 < s_i < p$, $i = 1, \cdots, m-1$. Suppose that*

$v \neq p$. If $p > m$ and σ_t satisfying the condition A, then ξ_p do not satisfy the equation (11).

Proof. Since the order of χ_w is p, so is that of g_w. Let

$$G = < g_{l_1} > \times < g_{l_2} > \times \cdots \times < g_{l_s} >, \qquad (1)$$

where the order of g_{l_i} be $p_i^{\alpha_i}$, $1 \leq i \leq s$. We can assume that $p_1 = p$, and $g_w = {g_{l_1}}^{p^{e-1}}$, where $e = \alpha_1$. Let ω_i be a primitive $p_i^{\alpha_i}$*_th* root of 1, $1 \leq i \leq s$. Set $g_{l_2}{}' = {g_{l_2}}^{p_2^{\alpha_2 - 1}}$. Thus

$$\chi_w(g_{l_1}) = {\omega_1}^{1 \cdot p^{e-1}} {\omega_2}^{0 \cdot 0} \cdots {\omega_s}^{0 \cdot 0} = {\omega_1}^{p^{e-1}}, \qquad (12)$$

$$\chi_w(g_{l_2}{}') = {\omega_1}^{0 \cdot p^{e-1}} {\omega_2}^{p_2^{\alpha_2 - 1} \cdot 0} \cdots {\omega_s}^{0 \cdot 0} = 1, \quad if \quad s > 1 \qquad (13)$$

$$\chi_w(g_w) = {\omega_1}^{p^{e-1} \cdot p^{e-1}} {\omega_2}^{0 \cdot 0} \cdots {\omega_s}^{0 \cdot 0} = 1, \quad if \quad e > 1. \qquad (14)$$

Set $\varepsilon = {\omega_1}^{p^{e-1}}$, then ε is a primitive p_th root of 1. We have

$$\xi_p(g_{l_1}) = \chi_b(g_{l_1})(\sum_{i=1}^{m-1} c_{l_i} \varepsilon^{s_i} + c_{l_m}), \qquad (15)$$

$$\xi_p(g_{l_2}{}') = \chi_b(g_{l_2}{}')(\sum_{i=1}^{m-1} c_{l_i} + c_{l_m}) = d \cdot \chi_b(g_{l_2}{}'), \quad if \quad s > 1, \quad (16)$$

$$\xi_p(g_w) = \chi_b(g_w)(\sum_{i=1}^{m-1} c_{l_i} + c_{l_m}) = d \cdot \chi_b(g_w), \quad if \quad e > 1. \qquad (17)$$

If $e > 1$, then set $v_1 = p^e$. If $e = 1$ and $p_2 = p$, then set $v_1 = p$. If $p \| v$, then set $v_1 = pp_2$ because of $v \neq p$. Let ς be a primitive v_1-th root of 1. $Q(\varsigma)$ denotes the v_1-th cyclotomic field. B denotes the ring of algebraic integers in $Q(\varsigma)$. By [10] $B = Z[\varsigma]$. Clearly $\varepsilon = \varsigma^{\frac{v_1}{p}}$. Since $p > m$ and $\phi(v_1)$ consecutive powers of ς are linearly independent, we get

$$\sum_{i=1}^{m-1} c_{l_i} \varsigma^{s_i \frac{v_1}{p}} + c_{l_m} \neq d.$$

Since ξ_p is a nontrivial solution, $0 \neq |c_{l_m}| < d$. Thus for any unit γ in B we have

$$\sum_{i=1}^{m-1} c_{l_i} \varsigma^{s_i \frac{v_1}{p}} + c_{l_m} \neq d\gamma.$$

Hence

$$(\xi_p(g_{l_1})) \neq (d), \qquad (18)$$

and if $e > 1$ we have

$$(\xi_p(g_w)) = (d), \qquad (19)$$

and if $s > 1$ we have

$$(\xi_p(g_{l_2}')) = (d), \qquad (20)$$

By (7) and (3) for any $g_j \in G (2 \leq j \leq v)$ we have

$$\sum_{i=1}^{k} \chi_{r_i}(g_j) \cdot \sum_{i=1}^{k} \overline{\chi_{r_i}}(g_j) = n. \qquad (21)$$

Let q be any prime divisor of n_1. Since $(n_1, v_0) = 1$, we get $(q, v_1) = 1$. Thus by [11] (q) is unramified in $Q(\varsigma)$. Hence $(q) = Q_1 Q_2 \cdots Q_h$, where $Q_1, Q_2, \cdots Q_h$ are different prime ideals in B. Since $(q, v_1) = 1$, the Frobenius automorphism for (q) in $Q(\varsigma)$ is σ_q, where $\sigma_q(\varsigma) = \varsigma^q$ (See [10]). Thus $\sigma_q(Q_i) \subseteq Q_i, i = 1, \cdots, h$. Since $Gal(\mathbb{Q}(\varsigma)/\mathbb{Q})$ transitively acts on the set $\{Q_1, \cdots, Q_h\}$ (see [10]), we have $\sigma_q(Q_i) = Q_i, 1 \leq i \leq h$. Since for every prime divisor q of n_1 there exists a positive integer j such that $t \equiv q^j (mod \quad v_0)$, we have $(t, v_0) = 1$. Thus $(t, v_1) = 1$. Hence there is a Q-automorphism σ_t of $Q(\varsigma)$ such that $\sigma_t(\varsigma) = \varsigma^t$. Since $t \equiv q^j (mod \quad v_0)$ and $v_1 | v_0$, we get $t \equiv q^j (mod \quad v_1)$. Thus $\sigma_t = \sigma_q{}^j$. Hence $\sigma_t(Q_i) = Q_i, 1 \leq i \leq h$.

Let $(n_1) = Q_1 Q_2 \cdots Q_l$, where $Q_1, Q_2, \cdots Q_l$ are prime ideals in B. By the above argument we have $\sigma_t(Q_i) = Q_i \quad (1 \leq i \leq l)$.

Let $(d) = D_1 D_2 \cdots D_r$, where $D_1, D_2, \cdots, D_r$ are prime ideals in B. From (21) we get

$$(\sum_{i=1}^{k} \chi_{r_i}(g_j) \cdot \sum_{i=1}^{k} \overline{\chi_{r_i}}(g_j)) = (n)$$
$$=(d)(n_1) = D_1 \cdots D_r Q_1 \cdots Q_l, \quad 2 \le j \le v \tag{22}$$

If $e > 1$ we take $g_j \in < g_{l_1} >$, otherwise we take $g_j \in < g_{l_1} > \times < g_{l_2}{}' >$. Thus $\sum_{i=1}^{k} \chi_{r_i}(g_j) \in B$, and $\sum_{i=1}^{k} \overline{\chi_{r_i}}(g_j) \in B$. Since the factorization of an ideal in B as a product of prime ideals is unique and $(d, n_1) = 1$, we can suppose that

$$(\sum_{i=1}^{k} \chi_{r_i}(g_j)) = D_{j_1} \cdots D_{j_h} Q_{k_1} \cdots Q_{k_t}, \tag{23}$$

where $1 \le h < r$. Thus

$$(\sum_{i=1}^{k} \overline{\chi_{r_i}}(g_j)) = \overline{D}_{j_1} \cdots \overline{D}_{j_h} \overline{Q}_{k_1} \cdots \overline{Q}_{k_t}. \tag{24}$$

where $\overline{D}_i := \{\bar{z} | z \in D_i\}$, etc. Set $\sigma_t(S) := \{\sigma_t(s) | s \in S\}$ for any subset S of B. If $\sigma_t(D_i) \ne D_i \quad (1 \le i \le r)$, then one get

$$\{\overline{D}_{j_1}, \cdots, \overline{D}_{j_h}\} = \{D_{j_{h+1}}, \cdots, D_{j_r}\}, \tag{25}$$
$$\{\overline{Q}_{k_1}, \cdots, \overline{Q}_{k_t}\} = \{Q_{k_{t+1}}, \cdots, Q_{k_l}\}.$$

thus $r = 2h$. Clearly $\sigma_t|_B$ is an automorphism of B. Thus

$$(\sum_{i=1}^{k} \chi_{r_i}{}^t(g_j)) = \sigma_t(D_{j_1}) \cdots \sigma_t(D_{j_h}) Q_{k_1} \cdots Q_{k_t}, \tag{26}$$

From (26), (24), (23) and (22) one get

$$(\sum_{i=1}^{k} \chi_{r_i}{}^t(g_j) \cdot \sum_{i=1}^{k} \overline{\chi_{r_i}}(g_j))$$
$$=(n_1)\sigma_t(D_{j_1}) \cdots \sigma_t(D_{j_h}) D_{j_{h+1}} \cdots D_{j_r}. \tag{27}$$

Case 1. $e > 1$.

By the condition A there are only two cases :

Case 1.1) σ_t such that $\sigma_t(D_{j_1})\cdots\sigma_t(D_{j_h})D_{j_{h+1}}\cdots D_{j_r} = (d)$ for any r_th permutation $j_1\cdots j_h j_{h+1}\cdots j_r$.

In this case we have

$$(\sum_{i=1}^{k}\chi_{r_i}{}^t(g_j)\cdot\sum_{i=1}^{k}\overline{\chi_{r_i}}(g_j)) = (n_1)(d), \quad \forall g_j \in < g_{l_1} > . \tag{28}$$

If ξ_p satisfy (11), then

$$(\sum_{i=1}^{k}\chi_{r_i}{}^t(g_{l_1})\cdot\sum_{i=1}^{k}\overline{\chi_{r_i}}(g_{l_1})) = (n_1)(\xi_p(g_{l_1})). \tag{29}$$

From (28) and (29) we get $(\xi_p(g_{l_1})) = (d)$. This contradicts (18).

Case 1.2) σ_t such that $\sigma_t(D_{j_1})\cdots\sigma_t(D_{j_h})D_{j_{h+1}}\cdots D_{j_r} \neq (d)$ for any r_th permutation $j_1\cdots j_h j_{h+1}\cdots j_r$.

In this case we have

$$(\sum_{i=1}^{k}\chi_{r_i}{}^t(g_j)\cdot\sum_{i=1}^{k}\overline{\chi_{r_i}}(g_j)) \neq (n_1)(d), \quad \forall g_j \in < g_{l_1} > . \tag{30}$$

If ξ_p satisfy (11), then

$$(\sum_{i=1}^{k}\chi_{r_i}{}^t(g_w)\cdot\sum_{i=1}^{k}\overline{\chi_{r_i}}(g_w)) = (n_1)(\xi_p(g_w)) = (n_1)(d).$$

This contradicts (30).

Hence in the case 1 ξ_p dose not satisfy the equation (11).

Case 2. $e = 1$ and $p_2 = p$.

Case 2.1) σ_t such that $\sigma_t(D_{j_1})\cdots\sigma_t(D_{j_h})D_{j_{h+1}}\cdots D_{j_r} = (d)$ for any r_th permutation $j_1\cdots j_h j_{h+1}\cdots j_r$.

In this case we have (28) for $g_j \in < g_{l_1} > \times < g_{l_2}{}' >$. If ξ_p satisfy (11), then we have (29). Thus $(\xi_p(g_{l_1})) = (d)$. This contradicts (18).

Case 2.2) σ_t such that $\sigma_t(D_{j_1})\cdots\sigma_t(D_{j_h})D_{j_{h+1}}\cdots D_{j_r} \neq (d)$ for any r_th permutation $j_1\cdots j_h j_{h+1}\cdots j_r$.

In this case we have

$$(\sum_{i=1}^{k} \chi_{r_i}{}^t(g_j) \cdot \sum_{i=1}^{k} \overline{\chi_{r_i}}(g_j)) \neq (n_1)(d), \qquad (31)$$

where $g_j \in < g_{l_1} > \times < g_{l_2}' >$. If ξ_p satisfy (11), then

$$(\sum_{i=1}^{k} \chi_{r_i}{}^t(g_{l_2}') \cdot \sum_{i=1}^{k} \overline{\chi_{r_i}}(g_{l_2}')) = (n_1)(\xi_p(g_{l_2}')) = (n_1)(d).$$

This contradicts (31).

Hence in the case 2 ξ_p dose not satisfy the equation (11).

Case 3. $p||v$.

It is similar to the case 2 that ξ_p does not satisfy (11). ∎

The lemma 3 lemma 4 and lemma 5 see [1].

§3. Some Partial Solutions for the Multiplier Conjecture

Let G be an abelian group with a (v, k, λ)-difference set D, and let v_0 be the exponent of G. In this section we follow notations in the lemma 2.

Theorem 2. *If $n = n_1$, then the Second Multiplier Theorem holds without the assumption "$n_1 > \lambda$ ".*

Proof. In this case $d = 1$. Thus it immediately follows from the Lemma 1 or the theorem 1.

Theorem 3. *If $n = 2n_1$, then the Second Multiplier Theorem holds without the assumption "$n_1 > \lambda$ ", except that one case is yet undecided where n_1 is odd and $7||v$ and $t \equiv 3, 5,$ or $6 \pmod{7}$, and for every prime divisor $p(\neq 7)$ of v such that the order w of 2 mod p satisfies that $2|\frac{\phi(p)}{w}$.*

Proof. If $2|n_1$, then by the lemma 1 we obtain that μ_t is a multiplier of D.

Now we suppose that n_1 is odd. In this case n isn't a square. Thus v has to be odd.

By the theorem 1 it is sufficient to prove that no nontrivial solution ξ of the following equations

$$\begin{cases} \sum_{l=1}^{v} c_l = 2, & (32) \\ \xi\bar{\xi} = 4\chi_1. & (33) \end{cases}$$

also satisfies the equation (11).

By the theorem 2 in [1] if $(v, 2) = 1$, then all the nontrivial solutions of (32) and (33) are 7-solutions which have the form:

$$\xi = \chi_b(\chi_u + \chi_u^2 + \chi_u^4 - \chi_1), \qquad (34)$$

where χ_u is any element of order 7 in $\hat{G}$, and χ_b is any element of $\hat{G}$.

If $(v, 7) = 1$, then there is only trivial solution of (32) and (33), and the assumption "$n_1 > \lambda$" may be removed. Now suppose that $7|v$. If $v = 7$, then it is easy to see that there are only two cases satisfying $\lambda(v-1) = k(k-1)$: $k = 3, \lambda = 1, n = 2$, or $k = 4, \lambda = 2, n = 2$. In these cases we get $n = n_1$, this contradicts the assumption $n = 2n_1$. Hence $v \neq 7$. Let

$$G = < g_{l_1} > \times < g_{l_2} > \times \cdots \times < g_{l_s} >, \quad . \qquad (1)$$

where the order of g_{l_i} be $p_i^{\alpha_i}$, $1 \le i \le s$. We can assume that $p_1 = 7$, and $g_u = g_{l_1}{}^{7^{e-1}}$, where $e = \alpha_1$. Set $g_{l_2}{}' = g_{l_2}{}^{p_2^{\alpha_2 - 1}}$.

Case 1. $e > 1$.

In this case $v_1 = 7^e$. Since $(2, 7^e) = 1$, (2) is unramified in $Q(\varsigma)$. Let $(2) = D_1 D_2 \cdots D_r$, where D_i $(1 \le i \le r)$ are different prime ideals in B. We denote the residue class degree of D_i by f_i $(1 \le i \le r)$. Since $Gal(Q(\varsigma)/Q)$ transitively acts on the set $\{D_1, D_2, \cdots, D_r\}$, we have $f_1 = f_2 = \cdots = f_r =: f$. Since $\sum_{i=1}^{r} e_i f_i = \phi(7^e)$, where e_i is the ramification index of D_i (see [11]), $1 \cdot r \cdot f = \phi(7^e) = 6 \cdot 7^{e-1}$. It is not difficult to see that the order of 2 mod 7^e is $3 \cdot 7^{e-1}$. Since f is equal to the order of 2 mod 7^e, we get $r = 2$.

Hence $(2) = D_1 D_2$. Since $Gal(Q(\varsigma)/Q)$ transitively acts on the set $\{D_1, D_2\}$, $\sigma_t(D_i) = D_i\,(i = 1, 2)$, or $\sigma_t(D_1) = D_2$ and $\sigma_t(D_2) = D_1$. Hence σ_t such that either $\sigma_t(D_{i_1})D_{i_2} = (2)$ for any 2_th permutation $i_1 i_2$, or $\sigma_t(D_{i_1})D_{i_2} \neq (2)$ for any 2_th permutation $i_1 i_2$. Since $7 > 4$ and σ_t satisfy the condition A, by the lemma 2 ξ do not satisfy the equation (11).

Case 2. $e = 1$ and $p_2 = 7$.

In this case $v_1 = 7$. Similarly we can show that σ_t satisfy the condition A. Hence in the case 2 ξ does not satisfy (11).

Case 3. $7 \| v$.

Since v is odd, $p_2 \neq 2$. In the case 3 $v_1 = 7p_2$, and ς is a primitive $7p_2$-th root of 1. Set $\eta = \varsigma^7$, then η is a primitive p_2-th root of 1. We denote the p_2-th cyclotomic field by $Q(\eta)$. B_1 denotes the ring of algebraic integers in $Q(\eta)$. Since $(2, p_2) = 1$, (2) is unramified in $Q(\eta)$. Let $(2)_1 = H_1 \cdots H_r$, where $(2)_1$ denotes the ideal generated by 2 in B_1, and $H_1, \cdots, H_r$ are different prime ideals in B_1. From (21) we get

$$\left(\sum_{i=1}^{k} \chi_{r_i}(g_{l_2}') \cdot \sum_{i=1}^{k} \overline{\chi_{r_i}}(g_{l_2}')\right)_1 = (2)_1 (n_1)_1. \qquad (35)$$

It follows that $2|r$.

Let the order of 2 mod p_2 is w.

Case 3.1) Let $\frac{\phi(p_2)}{w}$ is odd.

Since the residue class degree f of H_i is equal to w, $r = \frac{\phi(p_2)}{w}$. This contradicts $2|r$. Hence the case 3.1) is impossible.

Case 3.2) Let $2|\frac{\phi(p_2)}{w}$.

Set $\varepsilon = \varsigma^{p_2}$, then ε is a primitive 7_th root of 1. We denote the ring of algebraic integers in $Q(\varepsilon)$ by B_0. Since $(2, 7) = 1$, (2) is unramified in $Q(\varepsilon)$. Let $(2)_0 = P_1 \cdots P_r$, where $(2)_0$ denotes the ideal generated by 2 in B_0, and $P_1, \cdots, P_r$ are different prime ideals in B_0. Since the order of 2 mod 7 is 3, $r = \phi(7)/3 = 2$. Hence $(2)_0 = P_1 P_2$.

Since $\sigma_t(\varepsilon) = \varsigma^{tp_2} = \varepsilon^t$, $\sigma_t|_{Q(\varepsilon)}$ is a Q-automorphism of $Q(\varepsilon)$. Since $Gal(Q(\varepsilon)/Q)$ permutes $\{P_1, P_2\}$ transitively, the homomorphic image of $Gal(Q(\varepsilon)/Q)$ is a group of order 2. We denote the image of $\sigma_t|_{Q(\varepsilon)}$ by $\tilde{\sigma}_t|_{Q(\varepsilon)}$.

Case 3.2.1) Let $t \equiv 1, 2$, or $4 \pmod 7$.

Since the order of $\sigma_t|_{Q(\varepsilon)}$ is equal to the order of $t \pmod 7$ in $(Z/(7))^*$, in the case 3.2.1) the order of $\sigma_t|_{Q(\varepsilon)}$ is 1 or 3. Thus $\tilde{\sigma}_t|_{Q(\varepsilon)} = 1$. Hence it is easy to see that

$$(\sum_{i=1}^{k} \chi_{r_i}{}^t(g_{l_1}) \cdot \sum_{i=1}^{k} \overline{\chi_{r_i}}(g_{l_1}))_0 = (n_1)_0(2)_0. \qquad (36)$$

If ξ satisfy (11), then

$$(\sum_{i=1}^{k} \chi_{r_i}{}^t(g_{l_1}) \cdot \sum_{i=1}^{k} \overline{\chi_{r_i}}(g_{l_1}))_0 = (n_1)_0(\xi(g_{l_1}))_0.$$

Thus $(\xi(g_{l_1}))_0 = (2)_0$. Since $7 > 4$, it is similar to the proof of the lemma 2 that $(\xi(g_{l_1}))_0 \neq (2)_0$. Hence ξ does not satisfy (11).

By the argument above we obtain that if $n = 2n_1$, then the Second Multiplier Theorem holds without the assumption "$n_1 > \lambda$", provided that one of the following conditions holds:

(i) $2|n_1$;

(ii) n_1 is odd, and v can not divide by 7;

(iii) n_1 is odd, and $7^2|v$;

(iv) n_1 is odd, and $7||v$, and t is a quadratic residue mod 7.

The remaining undecided case is : n_1 is odd, and $7||v$, and t is a quadratic nonresidue mod 7, and for every prime divisor $p(\neq 7)$ of v such that the order w of 2 mod p satisfies that $2|\frac{\phi(p)}{w}$.

The proof of the theorem 3 is completed now. ∎

Theorem 4. *If $n = 3n_1$ and $(v, 3 \cdot 11) = 1$, then the Second Multiplier Theorem holds without the assumption "$n_1 > \lambda$", except that one case is yet undecided where n_1 can not divide by 3 and $13||v$*

and the order of t mod 13 is 12, 4 or 6, 2, and for every prime divisor $p(\neq 13)$ *of v such that the order w of 3 mod p satisfies that* $2|\frac{\phi(p)}{w}$.

Proof. If $3|n_1$, then by the Lemma 1 we obtain that μ_t is a multiplier of D.

Now we suppose that n_1 can not divide by 3. In this case n isn't a square. Thus v has to be odd.

By the theorem 1 it is sufficient to prove that the condition '$(v, 3 \cdot 11) = 1$" such that no nontrivial solution of the following equations

$$\begin{cases} \sum_{l=1}^{v} c_l = 3, & (37) \\ \xi\bar{\xi} = 9\chi_1. & (38) \end{cases}$$

also satisfies (11).

By the theorem 2 in [1] if $(v, 2 \cdot 3 \cdot 11) = 1$, then all the nontrivial solutions of (37) and (38) are 13-solutions.

If $(v, 13) = 1$, then there is only trivial solution of (37) and (38), so that the assumption "$n_1 > \lambda$" may be removed. Now we consider the case $13|v$. If $v = 13$, it is easy to see that there are only two cases satisfying $\lambda(v-1) = k(k-1)$: $k = 4, \lambda = 1, n = 3$, or $k = 9, \lambda = 6, n = 3$. In these cases we get $n = n_1$, this contradicts the assumption $n = 3n_1$. Hence $v \neq 13$. Take any 13-solution ξ. In the decomposition (1) of G we can assume that $p_1 = 13$.

Case 1. $e > 1$.

In this case $v_1 = 13^e$. Since $(3, 13^e) = 1$, (3) is unramified in $Q(\varsigma)$. Let $(3) = D_1 D_2 \cdots D_r$, where D_i $(1 \leq i \leq r)$ are different prime ideals in B. Clearly the order of 3 mod 13 is 3. It is not difficult to see that the order of 3 mod 13^e is $3 \cdot 13^{e-1}$. Thus the residue class degree f of $D_i (1 \leq i \leq r)$ is equal to $3 \cdot 13^{e-1}$. Hence $r = \phi(13^e)/f = 4$, and $(3) = D_1 D_2 D_3 D_4$. Since $Gal(Q(\varsigma)/Q)$ permutes $\{D_1, D_2, D_3, D_4\}$ transitively, there is a homomorphism of $Gal(Q(\varsigma)/Q)$ into the symmetric group S_4. We denote the homomorphic image of $Gal(Q(\varsigma)/Q)$ by H. $\tilde{\sigma}_t$ denotes the homomorphic image of σ_t. Since there is a primitive root for 13^e, $(\mathbb{Z}/(13^e))^*$ is a cyclic group. Since $Gal(Q(\varsigma)/Q) \cong (\mathbb{Z}/(13^e))^*$, $Gal(Q(\varsigma)/Q)$ is a cyclic group of order $12 \cdot 13^{e-1}$. Let the order of H be s, then $s|12 \cdot 13^{e-1}$ and $s|24$. Thus $s|12$. Since H is transitive on $\{D_1, D_2, D_3, D_4\}$, $s = 4$ and $H =< (a_1a_2a_3a_4) >$, where $a_1a_2a_3a_4$ is a permutation of 1234. It is not difficult to see that if the order of t mod 13^e are $12 \cdot 13^\alpha$ and $4 \cdot 13^\alpha$, or $6 \cdot 13^\alpha$ and $2 \cdot 13^\alpha$, or $3 \cdot 13^\alpha$ and 13^α, then the order of $\tilde{\sigma}_t$ are 4, or 2, or 1, respectively.

Case 1.1) Let the order of t mod 13^e are $3 \cdot 13^\alpha$, or 13^α.

In this case $\tilde{\sigma}_t = 1$. Thus $\sigma_t(D_{i_1})\sigma_t(D_{i_2})D_{i_3}D_{i_4} = (3)$ for any 4_th permutation $i_1i_2i_3i_4$.

Case 1.2) Let the order of t mod 13^e are $6 \cdot 13^\alpha$, or $2 \cdot 13^\alpha$.

In this case the order of $\tilde{\sigma}_t$ is 2. We denote the complex conjugate by τ. Clearly the order of τ is 2, and $\tau \in Gal(Q(\varsigma)/Q)$. Thus $\tilde{\sigma}_t = \tilde{\tau}$. Hence

$$\sigma_t(D_{i_1})\sigma_t(D_{i_2})D_{i_3}D_{i_4} = D_{i_3}{}^2 D_{i_4}{}^2 \neq (3)$$

for any 4_th permutation $i_1i_2i_3i_4$.

Case 1.3) Let the order of t mod 13^e are $12 \cdot 13^\alpha$, or $4 \cdot 13^\alpha$.

In this case the order of $\tilde{\sigma}_t$ is 4. Thus $\sigma_t(D_{i_1})\sigma_t(D_{i_2})D_{i_3}D_{i_4} \neq (3)$ for any 4_th permutation $i_1i_2i_3i_4$.

Hence in the case 1 σ_t satisfy the condition A. Since $13 > 9$, by the lemma 2 ξ does not satisfy the equation (11).

Case 2. $e = 1$ and $p_2 = 13$.

In this case $v_1 = 13$. It is similar to the case 1 that σ_t satisfy the condition A. Hence ξ does not satisfy the equation (11).

Case 3. $13||v$.

In this case $v_1 = 13p_2$. Set $\eta = \varsigma^{13}$, then η is a primitive p_2_th root of 1. We denote the p_2_th cyclotomic field by $Q(\eta)$. B_1 denotes the ring of algebraic integers in $Q(\eta)$. Since $(v,3) = 1$, $(p_2, 3) = 1$. Thus (3) is unramified in $Q(\eta)$. Let $(3)_1 = H_1 \cdots H_r$, where $(3)_1$ denotes the ideal generated by 3 in B_1, and $H_1, \cdots, H_r$ are different prime ideals in B_1. From (21) we get

$$\left(\sum_{i=1}^{k}\chi_{r_i}(g_{l_2}')\cdot\sum_{i=1}^{k}\overline{\chi_{r_i}}(g_{l_2}')\right)_1 = (3)_1(n_1)_1.$$

It follows that $2|r$.

Let the order of 3 mod p_2 is w.

Case 3.1) Let $\frac{\phi(p_2)}{w}$ is odd.

Since the residue class degree f of H_i is equal to w, $r = \frac{\phi(p_2)}{w}$. This contradicts $2|r$. Hence the case 3.1) is impossible.

Case 3.2) Let $2|\frac{\phi(p_2)}{w}$.

Set $\varepsilon = \varsigma^{p_2}$, then ε is a primitive 13-th root of 1. We denote the ring of algebraic integers in $Q(\varepsilon)$ by B_0. Since $(3,13) = 1$, (3) is unramified in $Q(\varepsilon)$. Let $(3)_0 = P_1\cdots P_r$, where $(3)_0$ denotes the ideal generated by 3 in B_0, and $P_1,\cdots,P_r$ are different prime ideals in B_0. Since the order of 3 mod 13 is 3, $r = \phi(13)/3 = 4$. Hence $(3)_0 = P_1P_2P_3P_4$.

Since $\sigma_t(\varepsilon) = \varsigma^{tp_2} = \varepsilon^t$, $\sigma_t|_{Q(\varepsilon)}$ is a Q-automorphism of $Q(\varepsilon)$. Since $Gal(Q(\varepsilon)/Q)$ permutes $\{P_1,P_2,P_3,P_4\}$ transitively, the homomorphic image H of $Gal(Q(\varepsilon)/Q)$ is a cyclic group of order 4. We denote the image of $\sigma_t|_{Q(\varepsilon)}$ by $\tilde{\sigma_t}|_{Q(\varepsilon)}$.

Case 3.2.1) Let the order of t mod 13 is 3 or 1.

Since the order of $\sigma_t|_{Q(\varepsilon)}$ is equal to the order of $t(mod\ 13)$ in $(Z/(13))^*$, $\tilde{\sigma_t}|_{Q(\varepsilon)} = 1$. Hence it is easy to see that

$$\left(\sum_{i=1}^{k}\chi_{r_i}{}^t(g_{l_1})\cdot\sum_{i=1}^{k}\overline{\chi_{r_i}}(g_{l_1})\right)_0 = (n_1)_0(3)_0.$$

If ξ satisfy (11), then

$$\left(\sum_{i=1}^{k}\chi_{r_i}{}^t(g_{l_1})\cdot\sum_{i=1}^{k}\overline{\chi_{r_i}}(g_{l_1})\right)_0 = (n_1)_0(\xi(g_{l_1}))_0.$$

Thus $(\xi(g_{l_1}))_0 = (3)_0$. Since $13 > 9$, it is similar to the proof of the lemma 2 that $(\xi(g_{l_1}))_0 \neq (3)_0$. Hence ξ does not satisfy (11).

By the argument above we obtain that if $n = 3n_1$ and $(v, 3\cdot 11) = 1$, then the Second Multiplier Theorem holds without the assumption "$n_1 > \lambda$", provided that one of the following conditions holds:

(i) $3|n_1$;

(ii) n_1 can not divide by 3, and v can not divide by 13;

(iii) n_1 can not divide by 3, and $13^2|v$;

(iv) n_1 can not divide by 3, and $13||v$, and the order of t mod 13 is 3 or 1.

The remaining undecided case is : n_1 can not divide by 3, and $13||v$, and the order of t mod 13 is 12,4 or 6,2, and for every prime divisor $p(\neq 13)$ of v such that the order w of 3 mod p satisfies that $2|\frac{\phi(p)}{w}$.

The proof of the theorem 4 is completed now. ∎

Acknowledgement. The author is thankful to the referee for suggestions.

References

[1] Qiu Weisheng, *A Character Approach to the Multiplier Conjecture and a New Result on It*, submitted.

[2] R.H. Bruck, *Difference Sets in a Finite Group*, Trans. Amer. Math. Soc, **78**(1955), 464-481.

[3] M. Newman, *Multipliers of Difference Sets*, Canad. J. Math., **15**(1963), 121-124.

[4] R.J.Turyn, *The Multiplier Theorm for Difference Sets*, Canad. J. Math., **16**(1964), 386-388.

[5] R.L.McFarland, *On Multipliers of Abelian Difference Sets*, Ohio State University, Ph.D.dissertation, 1970.

[6] E.S.Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge University Press , Cambridge, 1983, 196-218.

[7] D.Jungnickel, *Design Theory : An Update*, ARS Combinatoria, **28**(1989), 129-199.

[8]Wu Xiao-Hong, *A Multiplier Theorem of Cyclic Difference Sets*, Kaxue Tongbao, 9(1987), 718-719.

[9] C. W. Curtis & I. Reiner, *Representation Theory of Finite Groups and Associated Algebras*, Wiley-Interscience, New York, 1962.

[10] R.L.Long, *Algebraic Number Theory*, Dekker, New York, 1977.