ACTA ARITHMETICA
XCVIII.1 (2001)

On an equation in cyclotomic numbers

by

Roberto Dvornicich (Pisa)

1. Introduction. Let K be a field of characteristic 0 and let a, b, c be non-zero elements of K. In connection with the problem of studying the possible degree of $(f(x), g(x))$, where $f(x) = x^n + Ax^m + B$ is a trinomial and $g(x) = x^Q - C$ is a binomial, A. Schinzel asked (oral communication) the following

Question. *Let ζ_1, ζ_2 be two complex roots of unity with least common order Q and suppose that m, n are integers such that $(m, n, Q) = 1$ and*

$$|\zeta_1^m - 1|^m |\zeta_1^{n-m} - 1|^{n-m} |\zeta_1^n - 1|^{-n} = |\zeta_2^m - 1|^m |\zeta_2^{n-m} - 1|^{n-m} |\zeta_2^n - 1|^{-n}, \tag{1}$$

where none of the six absolute values is 0. Is it true that then $\zeta_2 = \zeta_1^{\pm 1}$?

For the connection between these two problems, see Schinzel [4].

We remark that there is a symmetry among the numbers $m, n-m, -n$: in fact, $|\zeta^n - 1| = |\zeta^{-n} - 1|$ and we can rewrite equation (1) in the symmetric form

$$|\zeta_1^a - 1|^a |\zeta_1^b - 1|^b |\zeta_1^c - 1|^c = |\zeta_2^a - 1|^a |\zeta_2^b - 1|^b |\zeta_2^c - 1|^c, \tag{2}$$

where $\{a, b, c\} = \{m, n-m, -n\}$. Assuming again that none of the six absolute values is zero, the hypotheses in Schinzel's question can then be translated into $a + b + c = 0$ and $(a, b, c, Q) = 1$.

The aim of this paper is to prove that Schinzel's question has a positive answer with essentially one exception. More precisely, we shall prove

Theorem 1. *Let $\zeta_1, \zeta_2, Q, m, n$ be as above and assume that (1) holds. Then either $\zeta_2 = \zeta_1^{\pm 1}$ or $Q = 10$, $\{m, n-m, -n\} = \{x, 3x, -4x\}$ for some integer x with $(x, 10) = 1$, and ζ_1, ζ_2 are any two primitive tenth roots of unity.*

2000 *Mathematics Subject Classification*: 11R18, 11R27.

Let $\zeta = \zeta_Q$ be a primitive Qth root of unity. According to a definition given by Conrad [1], the multiplicative group generated by the numbers $\zeta^\nu - 1$ with $\nu \not\equiv 0 \pmod{Q}$ modulo roots of unity is the group $D^{(Q)}$ of *cyclotomic numbers*. This group and its subgroups, in particular the subgroup of *cyclotomic units*, have been studied by many authors (see for instance [3], [6]–[8]). A classification of short multiplicative relations among cyclotomic numbers, however, is not available in the literature, and even for a simple equation like (1) there is no automatic way to find all solutions.

The main tool for the proof of Theorem 1 will be a result by Ennola [3], which gives necessary and sufficient conditions for a relation among cyclotomic numbers to hold. In Section 2 we shall recall Ennola's result and we shall examine a few small values of Q. After some preliminary lemmas (Section 3), we shall split our analysis into a fairly large number of cases. The proof of Theorem 1 will result from the combination of Propositions 1–10 of Sections 4 and 5. As the proof is rather technical, we shall leave enough detail in the general arguments, but we shall omit completely the verifications when these concern a finite number of cases, which can very easily be checked by a computer search.

2. Ennola's result and a few small values of Q. We shall always denote by ζ a primitive Qth root of unity. We briefly recall the main result of Ennola [3].

For $x \in \mathbb{Z}/Q\mathbb{Z}$, let

$$A_x = \log|\zeta^x - 1|,$$

and consider a linear combination with integer coefficients of the A_x,

$$R = \sum_{x=1}^{Q-1} C_x A_x. \tag{3}$$

For an even character χ mod Q of conductor $f > 1$ and for each d such that $f \mid d \mid Q$, we define

$$T(\chi, d, R) = \sum_{\substack{x=1 \\ (x,d)=1}}^{d-1} \chi(x) C_{(Q/d)x} \tag{4}$$

and

$$Y(\chi, R) = \sum_{\substack{d \\ f \mid d \mid Q}} \frac{1}{\phi(d)} \prod_{p \mid d} (1 - \overline{\chi}(p)) T(\chi, d, R); \tag{5}$$

moreover, for all prime numbers $p \mid Q$ we define

$$Y_p(R) = \sum_{x=1}^{p^{\gamma_p}-1} (x, p^{\gamma_p}) C_{(Q/p^{\gamma_p})x}, \tag{6}$$

where $p^{\gamma_p} \,||\, Q$. Then we have the following

THEOREM 2 (Ennola). *We have $R = 0$ if and only if*

$$Y(\chi, R) = 0 \quad \textit{for every even character } \chi \neq \chi_1 \tag{7}$$

and

$$Y_p(R) = 0 \quad \textit{for every prime } p \textit{ dividing } m. \tag{8}$$

Throughout the paper we shall keep the notation of (1)–(6), which is borrowed from [3] with the only exception that in the present paper the common order of ζ_1 and ζ_2 is called Q. Moreover, for a positive integer d we shall denote by μ_d the group of complex dth roots of unity and by ζ_d (for $d > 2$) a primitive dth root of unity. The symbol ζ without a subscript will always stand for a primitive Qth root of unity.

Let $\zeta_1 = \zeta^l$, $\zeta_2 = \zeta^k$. In Ennola's notation, relation (1) reads as $R = 0$ where

$$\begin{aligned} R = {} & mA_{lm} + (n-m)A_{l(n-m)} - nA_{ln} \\ & - (mA_{km} + (n-m)A_{k(n-m)} - nA_{kn}). \end{aligned} \tag{9}$$

We shall derive most of our results as consequences of relations (7). For $Q \in \{1, 2, 3, 4, 6\}$, however, there is no even character $\chi \neq \chi_1$ modulo Q, so conditions (7) are empty. We leave it to the reader to verify that equations (8) are sufficient to prove Theorem 1 for these particular values of Q.

Therefore, we shall assume $Q \notin \{1, 2, 3, 4, 6\}$ from now on. Moreover, we shall deal separately with the case when $Q \equiv 2 \pmod 4$, since in this case there is no *primitive* character with modulus Q.

3. Preliminary results. We recall without proof the following

LEMMA 1. *Let C be the maximal conductor of an even primitive character modulo a divisor of Q. Then*

$$C = \begin{cases} Q' & \textit{if } Q = 2Q' \textit{ and } Q' \textit{ is odd}, \\ Q & \textit{otherwise.} \end{cases}$$

A primitive character mod C is also a Dirichlet character mod C. Let G be the group of all even Dirichlet characters mod C and let K be the subgroup of G generated by the set X of primitive even characters, i.e. of even Dirichlet characters of maximal conductor.

LEMMA 2. *$K = G$ unless $Q = 2^a \cdot 3$, $a \geq 3$, in which case $[G : K] = 2$.*

Proof. We split the proof in a number of cases.

CASE 1: *Q is odd or $Q = 2^a$.* This case is trivial if Q is a prime power, since the group of even Dirichlet characters is cyclic and any generator must clearly have maximal conductor. Let then $Q = q_1 \dots q_r = p_1^{a_1} \dots p_r^{a_r}$ be the factorization of Q into primes, $2 < p_1 < \dots < p_r$, $r \geq 2$ and let $\chi_1, \dots, \chi_r$ be Dirichlet characters induced by (odd) generators of the primitive characters mod $q_1, \dots, q_r$, respectively. Note that χ_i^2 also has conductor q_i unless $q_i = 3$, so in particular χ_i^2 has conductor q_i for $i \geq 2$. We have

$$(\chi_1\chi_2\chi_3^2 \dots \chi_r^2) \cdot (\chi_1\chi_2^{-1}\chi_3^{-2} \dots \chi_r^{-2}) = \chi_1^2 \in K$$

and, similarly, $\chi_i^2 \in K$ for all $i = 1, \dots, r$. Also,

$$(\chi_1\chi_2\chi_3^2 \dots \chi_r^2) \cdot (\chi_3^{-2} \dots \chi_r^{-2}) = \chi_1\chi_2 \in K$$

and, similarly, $\chi_1\chi_i \in K$ for all $i > 1$. Finally, if $1 < i < j$ we have $\chi_1^{-2} \cdot \chi_1\chi_i \cdot \chi_1\chi_j = \chi_i\chi_j \in K$.

The case follows since G is generated by the set $\{\chi_i\chi_j \mid 1 \leq i \leq j \leq r\}$.

CASE 2: *$Q = 2Q'$ and Q' odd.* By Lemma 1, we have to consider the characters mod Q', so Case 1 applies.

CASE 3: *$Q = 2^aQ'$, $a \geq 2$, Q' odd and $Q' > 3$.* Let $Q' = q_1 \dots q_r = p_1^{a_1} \dots p_r^{a_r}$. The assumption $Q' > 3$ implies that either $r \geq 2$ or $r = 1$ and $q_1 > 3$.

Let χ_0 be a generator of the even characters mod 2^a and let $\chi^{(4)}$ be the (odd) primitive character mod 4. As in Case 1, we see immediately that $\chi_i^2 \in K$ and $\chi_i\chi_j \in K$ for $0 \leq i \leq j \leq r$. Also, $\chi_0 \in K$, since for $a = 2$ we have $\chi_0 = 1$ and, for $a > 2$:

- if $r \geq 2$, then $\chi_0\chi_1\chi_2\chi_3^2 \dots \chi_r^2 \in K$ implies that $\chi_0 \in K$;
- if $r = 1$, then $\chi_0\chi_1^2 \in K$ implies that $\chi_0 \in K$.

Furthermore,

$$\chi^{(4)}\chi_0\chi_1\chi_2^2 \dots \chi_r^2 \in K \;\Rightarrow\; \chi^{(4)}\chi_1 \in K$$

and $\chi^{(4)}\chi_i = \chi^{(4)}\chi_1 \cdot \chi_1\chi_i \cdot \chi_1^{-2} \in K$ for all $i \geq 1$. Since all odd characters mod 2^a are of the form $\chi_0^b\chi^{(4)}$ and $\chi_0^b\chi^{(4)}\chi_i \in K$ for all $i \geq 1$, it follows that K is again the full group of even characters.

CASE 4: *$Q = 2^a \cdot 3$, $a \geq 2$.* If $a = 2$, then $\chi^{(4)}\chi_1 \in K$ and generates the group of even characters mod 12. If $a > 2$, all characters of maximal conductor are contained in the subgroup generated by $\chi^{(4)}\chi_0\chi_1$, which has order 2^{a-2}, while G has order 2^{a-1}. ∎

COROLLARY 1. *Let k be such that $\chi(k) = 1$ for all even primitive characters of maximal conductor C. Then*

(a) *$k \equiv \pm 1, \pm i \pmod{Q}$ if $Q = 2^a \cdot 3$, $a \geq 3$, where i is defined by the congruences $i \equiv 2^{a-1} + 1 \pmod{2^a}$, $i \equiv -1 \pmod{3}$,*

(b) $k \equiv \pm 1 \pmod{Q'}$ *if* $Q = 2Q'$, Q' *odd*;
(c) $k \equiv \pm 1 \pmod{Q}$ *otherwise.*

Proof. The case $Q = 2^a \cdot 3$ is established by looking at the kernel of $\chi^{(4)}\chi_0\chi_1$. The remaining cases are direct consequences of Cases 1–3 of Lemma 2. ∎

4. The case when at least one root is primitive. Throughout this section we shall assume that either ζ_1 or ζ_2 is a primitive Qth root of unity. Without loss of generality, we shall also assume that $\zeta_1 = \zeta$.

4.1. *The case* $Q \not\equiv 2 \pmod 4$. If Q is odd, we can improve on Lemma 2 as follows. Let $Q = q_1 \dots q_r = p_1^{a_1} \dots p_r^{a_r}$ be the prime factorization of Q, $3 \le p_1 < \dots < p_r$, $r \ge 2$. Let $\chi_1, \dots, \chi_r$ be as in Lemma 2. Any Dirichlet character mod Q can be written in the form $\chi = \chi_1^{i_1} \dots \chi_r^{i_r}$, and the subgroup G of even Dirichlet characters is defined by the equation $i_1 + \dots + i_r \equiv 0 \pmod 2$. The following lemma is very similar in spirit to the results of [5, Sect. 3].

LEMMA 3. *If* $Q > 3$ *is odd, the set* X *of Dirichlet characters of maximal conductor* Q *is not contained in the union of two maximal subgroups* H_0, K_0 *of* G *unless* Q *can be written as* $Q = 3Q_1Q_2$ *with* $Q_1, Q_2 > 1$, $(3, Q_1) = (3, Q_2) = (Q_1, Q_2) = 1$ *and the subgroups* H_0, K_0 *are defined by the equations*

$$\sum_{\substack{h \\ p_h \mid Q_1}} i_h \equiv 0 \pmod 2, \qquad \sum_{\substack{h \\ p_h \mid Q_2}} i_h \equiv 0 \pmod 2$$

respectively.

Proof. The conclusion is trivial if G is cyclic, since in this case any generator of G has maximal conductor and cannot be contained in any proper subgroup. Hence from now on we can suppose that the number r of distinct prime factors of Q is ≥ 2.

We recall that any maximal subgroup of a finite abelian group has prime index in the full group.

CASE 1: $[G : H_0] = \ell_1$, $[G : K_0] = \ell_2$, ℓ_1, ℓ_2 *primes* > 2. The equations defining H_0 and K_0 must be of the form

$$a_1 i_1 + \dots + a_r i_r \equiv 0 \pmod{\ell_1}, \tag{10}$$

$$b_1 i_1 + \dots + b_r i_r \equiv 0 \pmod{\ell_2}. \tag{11}$$

REMARK 1. If $a_i \not\equiv 0 \pmod{\ell_1}$ (resp. $b_i \not\equiv 0 \pmod{\ell_2}$) then necessarily $p_i = \ell_1$ and $q_i \ge \ell_1^2$ or $p_i \equiv 1 \pmod{\ell_1}$ (resp. $p_i = \ell_2$ and $q_i \ge \ell_2^2$ or $p_i \equiv 1 \pmod{\ell_2}$). In particular, $a_i \equiv 0 \pmod{\ell_1}$ and $b_i \equiv 0 \pmod{\ell_2}$ if $q_i = 3$ or $q_i = 5$.

If there exists a prime $p_h > 3$ such that $a_h \not\equiv 0 \pmod{\ell_1}$ and $b_h \not\equiv 0 \pmod{\ell_2}$, let $j = 1$ if $p_1 = 3$ and j be any index such that $j \neq h$ otherwise. Then one of the even r-tuples $(i_1, \dots, i_r)$ defined by

$$i_h = 1, -1, 3,\ i_j = 1,\ i_\lambda = 2 \text{ for } \lambda \neq h, j$$

does not satisfy either of equations (10) and (11). (In what follows, we say that an even r-tuple is *good* if it does not satisfy either of the equations defining the subgroups H_0 and K_0.)

If there exist two distinct primes $p_h, p_j > 3$ such that $a_h \not\equiv 0 \pmod{\ell_1}$ and $b_j \not\equiv 0 \pmod{\ell_2}$, suppose, by symmetry, that $p_h < p_j$. Then one of the r-tuples $(i_1, \dots, i_r)$ defined by

$$\begin{cases} i_h = \pm 1,\ i_j = \pm 1 \text{ and } i_\lambda = 2 \text{ for } \lambda \neq h, j & \text{if } p_1 > 3, \\ i_h = \pm 1,\ i_j = \pm 2,\ i_1 = 1,\ i_\lambda = 2 \text{ for } \lambda \neq 1, h, j & \text{otherwise,} \end{cases}$$

is good. So, since neither of equations (10) and (11) can be empty, we are left with the case (up to symmetry between ℓ_1 and ℓ_2) when $p_1 = 3$, $\ell_2 = 3$ and

$$a_1 i_1 + \ldots + a_r i_r \equiv 0 \pmod{\ell_1}, \qquad i_1 \equiv 0 \pmod{3}.$$

If $a_h \equiv 0 \pmod{\ell_1}$ for all $h > 1$, then the r-tuple defined by $i_1 = i_2 = 1$, $i_\lambda = 2$ for $\lambda > 2$ is good. If $a_h \not\equiv 0 \pmod{\ell_1}$ for some $h > 1$, then at least one of the r-tuples defined by $i_1 = 1, i_h = \pm 1, i_\lambda = 2$ for $\lambda \neq 1, h$ is good.

Case 2: $[G : H_0] = 2$ *and* $[G : K_0] = \ell > 2$. The group $G/2G$ has order 2^r if all p_i are congruent to 1 mod 4, and 2^{r-1} otherwise. In any case G has $2^{r-1} - 1$ subgroups of index 2 given by equations of type

$$\sum_{h \in S} i_h \equiv 0 \pmod{2}, \qquad S \neq \emptyset, \{1, \dots, r\}$$

(the interchange between S and its complementary set $\{1, \dots, r\} \setminus S$ gives the same subgroup). These are all subgroups of index 2 if there exists at least one prime p_h which is congruent to 3 mod 4. If $p_h \equiv 1 \pmod{4}$ for all i, then we also have the 2^{r-1} subgroups given by equations of type

$$\varepsilon_1 i_1 + \ldots + \varepsilon_r i_r \equiv 0 \pmod{4},$$

where $\varepsilon_h = \pm 1$ and changing all signs gives rise to the same subgroup. So this case splits into two subcases.

Subcase 2a: The relevant equations are:

$$\varepsilon_1 i_1 + \ldots + \varepsilon_r i_r \equiv 0 \pmod{4}, \qquad \varepsilon_h = \pm 1,$$
$$a_1 i_1 + \ldots + a_r i_r \equiv 0 \pmod{\ell},$$

and $p_h \equiv 1 \pmod{4}$ for all h.

Choose an index h such that $a_h \not\equiv 0 \pmod{\ell}$, and let $j \neq h$ be any other index. Then at least one of the r-tuples

$$i_h = \pm 1, \pm 3,\ i_j = 1,\ i_\lambda = 2 \text{ for } \lambda \neq h, j$$

is good. (Note that $\chi_h^{\pm 1} \neq \chi_h^{\mp 3}$ by Remark 1.)

Subcase 2b: The relevant equations are:

$$\sum_{h \in S} i_h \equiv 0 \pmod{2}, \qquad S \neq \emptyset, \{1, \ldots, r\},$$
$$a_1 i_1 + \ldots + a_r i_r \equiv 0 \pmod{\ell}.$$

Note that, by Remark 1, if $q_i = 3, 5$ then $a_i = 0$. Interchanging S with its complementary set if necessary, we may suppose that there exists an index $h \notin S$ such that $a_h \not\equiv 0 \pmod{\ell}$. Let $j = 1$ if $1 \in S$ and j be any index such that $j \in S$ otherwise. Then at least one of the two r-tuples

$$\begin{cases} i_1 = 1,\ i_h = \pm 1,\ i_\lambda = 2 \text{ for } \lambda \neq 1, h & \text{if } 1 \in S, \\ i_1 = 1,\ i_j = 1,\ i_h = \pm 2,\ i_\lambda = 2 \text{ for } \lambda \neq 1, h, j & \text{otherwise,} \end{cases}$$

is good.

Case 3: $[G : H_0] = 2$, $[G : K_0] = 2$. Also this case splits into subcases.

Subcase 3a: The equations are

$$\varepsilon_1 i_1 + \ldots + \varepsilon_r i_r \equiv 0 \pmod{4}, \qquad \varepsilon_h = \pm 1,$$
$$\delta_1 i_1 + \ldots + \delta_r i_r \equiv 0 \pmod{4}, \qquad \delta_h = \pm 1;$$

in this case all primes p_h are congruent to 1 mod 4.

The r-tuple $i_1 = 2$, $i_\lambda = 4$ for $\lambda > 1$ is good.

Subcase 3b: The equations are

$$\varepsilon_1 i_1 + \ldots + \varepsilon_r i_r \equiv 0 \pmod{4}, \qquad \varepsilon_h = \pm 1,$$
$$\sum_{h \in S} i_h \equiv 0 \pmod{2}, \qquad S \neq \emptyset, \{1, \ldots, r\};$$

in this case all primes p_h are congruent to 1 mod 4.

Let $h \in S$, $j \notin S$; at least one of the r-tuples

$$i_h = \pm 1,\ i_j = 1,\ i_\lambda = 2 \text{ for } \lambda \neq h, j$$

is good.

Subcase 3c: The equations are

$$\sum_{h \in S} i_h \equiv 0 \pmod{2}, \qquad S \neq \emptyset, \{1, \ldots, r\},$$
$$\sum_{h \in T} i_h \equiv 0 \pmod{2}, \qquad T \neq \emptyset, \{1, \ldots, r\}.$$

We may of course suppose that $S \neq T$ and, possibly interchanging the roles of S, T and their complementary sets, that $1 \notin S \cup T$.

If $S \cap T \neq \emptyset$, let h be an index such that $h \in S \cap T$. The r-tuple

$$i_1 = i_h = 1,\ i_\lambda = 2 \text{ for } \lambda \neq 1, h$$

is good.

Suppose then that $S \cap T = \emptyset$. If there exists $h > 1$ such that $h \notin S \cup T$, let $j_1 \in S$, $j_2 \in T$; the r-tuple

$$i_1 = i_h = i_{j_1} = i_{j_2} = 1,\ i_\lambda = 2 \text{ for } \lambda \neq 1, h, j_1, j_2$$

is good.

If $q_1 \neq 3$, we can get the same conclusion by looking at the r-tuple $i_{j_1} = i_{j_2} = 1$, $i_\lambda = 2$ for $\lambda \neq j_1, j_2$.

So we are left with the case when $q_1 = 3$, $S \cap T = \emptyset$, $S \cup T = \{2, \dots, r\}$, thereby proving Lemma 3. ∎

With the notation of Lemma 3, suppose next that $Q = 3Q_1Q_2$, and that H is a subgroup of G contained in H_0. We have the following

LEMMA 4. *Let Q be odd, $Q = 3Q_1Q_2$, with $Q_1, Q_2 > 1$ and $(3, Q_1) = (3, Q_2) = (Q_1, Q_2) = 1$. Then the set X of Dirichlet characters of maximal conductor Q is not contained in $H \cup K_0$ unless $Q_1 = 5$ and H coincides with the subgroup H_1 defined by the equation*

$$i_2 + 2i_3 + \dots + 2i_r \equiv 0 \pmod 4. \tag{12}$$

Proof. By Lemma 3, we have $X \not\subset H \cup K_0$ whenever H is contained in a maximal subgroup of G of odd index; hence we may only consider the case when H is contained in a maximal subgroup of H_0 of index 2.

The group $H_0/2H_0$ has order 2^{r-1} if all primes p_h with $h \in S$ are congruent to 1 mod 4 and order 2^{r-2} otherwise. In any case there are $2^{r-2} - 1$ subgroups of H_0 of index 2 given by the equations

$$\sum_{h \in U} i_h \equiv 0 \pmod 2,$$

where U is a subset of $\{1, \dots, r\}$ different from $\emptyset$, $\{1, \dots, r\}$, S, T, and two sets U and U' give rise to the same subgroup if and only if $U \cap S$, $U' \cap S$ and $U \cap T$, $U' \cap T$ are either equal or complementary in S and T respectively.

In the case when there exists $h \in S$ with $p_h \equiv 3 \pmod 4$, these are all possible equations of subgroups of H_0 of index 2. But since necessarily in an equation of this type we must have $U \neq S, T$, the argument of the proof of Lemma 3 shows that we are done in this case.

In the case when p_h is congruent to 1 mod 4 for all $h \in S$, renumber the indices $2, \dots, r$ so that $S = \{2, \dots, s\}$, $T = \{s+1, \dots, r\}$ and $p_2 < \dots < p_s$, $p_{s+1} < \dots < p_r$. Then the other 2^{r-2} subgroups of index 2 are given by the

equations

$$\varepsilon_2 i_2 + \ldots + \varepsilon_s i_s + \delta_{s+1} i_{s+1} + \ldots + \delta_r i_r \equiv 0 \pmod 4,$$

where $\varepsilon_h = \pm 1$, $\delta_h = 0, 2$, and two such equations give rise to the same subgroup if and only if they are equal or obtained from one another by changing all signs.

If $|S| \geq 2$, hence $s \geq 3$, then at least one of the r-tuples given by

$$i_1 = i_r = 1,\ i_2 = 2,\ i_3 = 2, 4,\ i_\lambda = 4 \text{ for } \lambda \neq 1, 2, 3, r$$

is good.

If $s = 2$ and $q_2 \neq 5$, then at least one of the r-tuples

$$i_1 = i_r = 1,\ i_2 = 2, 4,\ i_\lambda = 4 \text{ for } \lambda \neq 1, 2, r$$

is good.

Suppose now that $s = 2$ and $q_2 = 5$. If there exists $h > 2$ such that $\delta_h = 0$, then the r-tuple given by

$$i_1 = 1 = i_h = 1,\ i_\lambda = 2 \text{ for } \lambda \neq 1, h$$

is good.

Hence the only possibility is that $Q_1 = 5$ and that H_1 is the unique maximal subgroup of H_0 containing H.

If $H = H_1$, then in fact we have $X \subset H_1 \cup K_0$. If H is properly contained in H_1, then in fact it must be contained in a subgroup of H_1 of index 2. As before, we can check that $H_1/2H_1$ has order 2^{r-2} and that all its subgroups of index 2 are given by equations of type

$$\sum_{h \in V} i_h \equiv 0 \pmod 2,$$

where V is a non-empty subset of $\{3, \ldots, r\}$. Let $h \in V$. Then the r-tuple given by

$$i_1 = i_h = 1,\ i_\lambda = 2 \text{ for } \lambda \neq 1, h$$

is then good, and this concludes the proof of the lemma. ∎

Consider now the case when all $m, n-m, n$ are coprime to Q. Notice that Q must be odd in this case, since at least one of the three numbers $m, n-m, n$ is even.

Let z be the solution mod Q of the congruence $m \equiv zn \pmod Q$. Let H, K be the subgroups of G defined by the equations $\chi(z) = \chi(1-z) = 1$ and $\chi(k) = 1$, respectively. We have the following

LEMMA 5. *If $Q > 3$ is odd and $k \neq \pm 1$ then the set X of Dirichlet even characters of maximal conductor Q is not contained in $H \cup K$.*

Proof. By Lemma 2, the condition $k \neq \pm 1$ implies that $K \neq G$. Lemma 3 shows that we only have to take care of the case when $Q = 3Q_1Q_2$ with

$Q_1, Q_2 > 1$, $(3, Q_1) = (3, Q_2) = (Q_1, Q_2) = 1$ and the subgroups H, K are contained in maximal subgroups H_0, K_0 defined by the equations

$$\sum_{h \in S} i_h \equiv 0 \pmod 2, \qquad \sum_{h \in T} i_h \equiv 0 \pmod 2$$

respectively, where $S = \{h : p_h \mid Q_1\}$ and $T = \{h : p_h \mid Q_2\}$.

However, we note that H cannot coincide with the subgroup H_0: in fact, the set $\{x \in \mathbb{Z} \mid \chi(x) = 1 \ \forall \chi \in H_0\}$ is contained in the set $x \equiv \pm 1 \pmod{Q_1}$ in this case, and it is immediately seen that z and $1 - z$ cannot both lie in this set (note that $Q_1 > 3$). So it remains to consider the case when H is properly contained in H_0, and, by Lemma 4, only the case when $H = H_1$, i.e. the subgroup defined by the equation

$$i_2 + 2i_3 + \ldots + 2i_r \equiv 0 \pmod 4.$$

One easily sees that the set $\{x \in \mathbb{Z} \mid \chi(x) = 1 \ \forall \chi \in H_1\}$ is contained in the set $\{x \in \mathbb{Z} \mid x \equiv \pm 1 \pmod{Q_2}\}$, and again it is not possible that both z and $1 - z$ belong to this set. This concludes the proof of the lemma. ∎

Proposition 1. *Let $\zeta_1 = \zeta$ be a primitive Qth root of unity and $\zeta_2 = \zeta^k$. Assume that $(m, Q) = (n - m, Q) = (n, Q) = 1$, whence, in particular, that Q is odd. If* (1) *holds, then $k \equiv \pm 1 \pmod Q$.*

Proof. Consider all relations (7) relative to characters of maximal conductor. They have the form

$$(1 - \chi(k))(m\chi(m) + (n - m)\chi(n - m) - n\chi(n)) = 0.$$

We look when the term inside the second parentheses is zero, i.e. when

$$m\chi(m) + (n - m)\chi(n - m) - n\chi(n) = 0. \tag{13}$$

In our notation, this amounts to studying the vanishing of the quantity $m\chi(z) + (n - m)\chi(1 - z) - n$. Since $|\chi(z)| = |\chi(1 - z)| = 1$, this vanishes if and only if $\chi(z) = \chi(1 - z) = 1$. Since H is a proper subgroup of G, Lemma 5 implies that $K = G$ and, by Corollary 1(c), $k \equiv \pm 1 \pmod Q$. ∎

Proposition 2. *Let $\zeta_1 = \zeta$, $\zeta_2 = \zeta^k$. Suppose that $Q \not\equiv 2 \pmod 4$, and that exactly two of the numbers (m, Q), $(n - m, Q)$, (n, Q) are equal to* 1. *If* (1) *holds, then $k \equiv \pm 1 \pmod Q$.*

Proof. By symmetry, we may consider only the case when $(m, Q) = (n - m, Q) = 1$ and $(n, Q) > 1$. For an even character of maximal conductor χ, relations (7) take the form

$$(1 - \chi(k))(m\chi(m) + (n - m)\chi(n - m)) = 0.$$

Now $m\chi(m) + (n - m)\chi(n - m) = 0$ implies $|m| = |n - m|$, hence $n = 2m$ and $2m\chi(m) = 0$, a contradiction. This means that we must have $\chi(k) = 1$ for

all even characters of maximal order. By Corollary 1, the conclusion follows if Q is not of the form $Q = 2^a \cdot 3$, $a \geq 3$.

If $Q = 2^a \cdot 3$, $a \geq 3$, we need to exclude the case when $k = \pm i$ (with the notation of Corollary 1). Consider a generator χ_0 of the even characters mod 2^a; we have $\chi_0(\pm i) = -1$ and the relation $Y(\chi_0, R) = 0$ is

$$\frac{1}{\phi(2^a)} \sum_{\substack{x=1 \\ (x,2^a)=1}}^{2^a-1} \chi_0(x) C_{3x} + \frac{1}{\phi(2^a \cdot 3)} (1 - \overline{\chi}_0(3)) \sum_{\substack{x=1 \\ (x,2^a \cdot 3)=1}}^{2^a \cdot 3 - 1} \chi_0(x) C_x = 0. \tag{14}$$

Since $2 \,|\, n$ and $3 \nmid m(n-m)$ all the equations $3x = m, n-m, -n$, $3x = \mp im, \mp i(n-m), \pm in$ are unsolvable under the condition $(x, 2^a) = 1$; moreover, $\chi_0(n) = \chi_0(\pm in) = 0$. So equation (14) becomes

$$2(1 - \overline{\chi}_0(3))(m\chi(m) + (n-m)\chi(n-m)) = 0,$$

which is impossible since $\chi_0(3) \neq 1$. ∎

Proposition 3. *Let $\zeta_1 = \zeta$, $\zeta_2 = \zeta^k$. Suppose that $Q \not\equiv 2 \pmod 4$, and that exactly one of the numbers (m, Q), $(n-m, Q)$, (n, Q) is equal to 1. If (1) holds, then $k \equiv \pm 1 \pmod Q$.*

Proof. By symmetry, we may only consider the case when $(m, Q) = 1$, $(n-m, Q) > 1$ and $(n, Q) > 1$. For any even character of maximal conductor Q, relation (7) reads

$$(1 - \chi(k))\chi(m) = 0.$$

By Corollary 1, we need only exclude the case when $Q = 2^a \cdot 3$, $a \geq 3$, and $k = \pm i$. We consider again the character χ_0. Exactly one number between n and $n-m$ is divisible by 2, whereas the other one is divisible by 3. Again we deal only with the case when $2 \,|\, n$ and $3 \,|\, n-m$, the other case being similar. Equation (14) becomes

$$\frac{2}{\phi(2^a)}(n-m)\chi_0\left(\frac{n-m}{3}\right) + \frac{2}{\phi(2^a \cdot 3)}(1 - \overline{\chi}_0(3))m\chi_0(m) = 0,$$

or, equivalently,

$$2(n-m)\chi_0\left(\frac{n-m}{3}\right) + (1 - \overline{\chi}_0(3))m\chi_0(m) = 0.$$

This last equation implies that $|1 - \overline{\chi}_0(3)| = 2(n-m)/m$; but $1 - \chi_0(3)$ is an algebraic integer, so if its absolute value is rational then it must be an integer, and in fact it can only be 0, 1, 2. All possibilities are easily excluded under our hypotheses, so the proposition follows. ∎

Proposition 4. *Let $\zeta_1 = \zeta$, $\zeta_2 = \zeta^k$. Suppose that $Q \not\equiv 2 \pmod 4$, and that none of the numbers $m, n-m, n$ is coprime to Q. If (1) holds, then $k \equiv \pm 1 \pmod Q$.*

Proof. Let $(m,Q)=p_1^{\alpha_1}\dots p_r^{\alpha_r}$, $m=(m,Q)m^*$, $Q=(m,Q)f_m$, so that $(m^*,f_m)=1$, whereas $(n-m,f_m)>1$ and $(n,f_m)>1$. Define f_{n-m} and f_n similarly. All numbers f_m,f_{n-m},f_n are divisible by at least two prime factors and at least two of them, say f_m and f_n, are divisible by the same power of 2 as Q. Consider even characters χ of conductor $f=f_m$.

Let d be an integer such that $f_m \mid d \mid Q$, and write $d=p_1^{i_1}\dots p_r^{i_r}f$. The equations $(Q/d)x=n, kn$ are not solvable under the given conditions, since $(Q/d,n)=1$ and a possible solution would satisfy $x\equiv 0 \pmod n$, hence $(x,f_m)>1$ and a fortiori $(x,d)>1$; the same argument shows that the equations $(Q/d)x=n-m, k(n-m)$ are not solvable with $(x,d)=1$. The equation $(Q/d)x=p_1^{\alpha_1-i_1}\dots p_r^{\alpha_r-i_r}x=m$ has solution $x=p_1^{i_1}\dots p_r^{i_r}m^*$, but this solution is coprime to d only if $i_1=\dots=i_r=0$, i.e. if $d=f_m$. Hence relations (7) for such characters become

$$\frac{1}{\phi(f_m)}(1-\chi(k))m\chi(m^*)=0$$

and we can obtain a similar expression by considering the conductor f_n. Since at most one of f_m and f_n, say f_m, can be of the form $2^a\cdot 3$, $a\ge 3$, we get the system

$$\begin{cases} k\equiv \pm 1(\pm i) \pmod{f_m},\\ k\equiv \pm 1 \pmod{f_n}. \end{cases}$$

But the solutions of the single congruences must agree modulo $(f_m,f_n)>1$ and $[f_m,f_n]=Q$, hence we get $k\equiv\pm 1 \pmod Q$. ∎

4.2. *The case* $Q\equiv 2 \pmod 4$. Consider the case when $Q=2Q'$, Q' odd; then exactly one of $m, n-m, n$ is even, say $n=2n_1$. By this assumption we lose some of the symmetries among the numbers $m, n-m, -n$, hence throughout this subsection the number $-n$ will be given a distinguished role. As remarked above, we can suppose that $Q'>3$.

Proposition 5. *Let* $\zeta_1=\zeta$, $\zeta_2=\zeta^k$, k *odd, and* $Q=2Q'$, Q' *odd. Suppose moreover that* $(m,Q')=(n-m,Q')=(n,Q')=1$. *If* (1) *holds, then* $k\equiv\pm 1 \pmod Q$, *except for the case* $Q'=5$, $\{4m,4(n-m)\}=\{n,3n\}$, *where* k *can be any number coprime to* 10.

Proof. For even characters χ of modulus Q' relations (7) give

$$(1-\overline{\chi}(2))\sum_{\substack{x=1\\(x,Q)=1}}^{Q}\chi(x)C_x+\sum_{\substack{x=1\\(x,Q')=1}}^{Q'}\chi(x)C_{2x}=0.$$

If k is odd, this becomes

$$(15)\quad (1-\chi(k))[(1-\overline{\chi}(2))(m\chi(m)+(n-m)\chi(n-m))-n\chi(n_1)]=0.$$

We first examine the characters χ for which

$$(1-\overline{\chi}(2))(m\chi(m)+(n-m)\chi(n-m))-n\chi(n_1)=0. \tag{16}$$

LEMMA 6. *If equation* (16) *holds, then either*

$$\chi(2)=\chi(3)=-1 \quad \textit{and} \quad \{4m,4(n-m)\}=\{n,3n\} \tag{17}$$

or

$$\chi(2)=\zeta_6 \quad \textit{and} \quad \chi(n_1)=\zeta_6\chi(m)=\zeta_6\chi(n-m). \tag{18}$$

Proof. Let d be the order of such a χ, ζ_d be a primitive dth root of unity and consider the congruence mod $2\mathbb{Z}[\zeta_d]$; since m is odd, we obtain

$$(1-\overline{\chi}(2))(\chi(m)-\chi(n-m))\equiv 0 \pmod{2\mathbb{Z}[\zeta_d]}. \tag{19}$$

Let $(2)=(\mathcal{P}_1\dots\mathcal{P}_s)^e$ be the factorization of the ideal (2) into prime ideals (notice that e is a power of 2). We observe that if a number of the form $1-\zeta_d^a$ belongs to $\mathcal{P}_h^i$ for some h,i, then all its conjugates, being its multiples, belong to $\mathcal{P}_h^i$; consequently, $1-\zeta_d^a\in\mathcal{P}_j^i$ for all j, since the prime ideals $\mathcal{P}_j$ are all conjugate under the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$.

Hence at least one of the numbers $(1-\overline{\chi}(2))^2$ and $(\chi(m)-\chi(n-m))^2$ belongs to the ideal (2).

CASE 1: $1-(\overline{\chi}(2))^2\in(2)$. In this case we have $\chi(2)=\pm1,\pm i$, where $i^2=-1$. If $\chi(2)=1$ equation (16) is clearly impossible. If $\chi(2)=-1$, taking the squares of absolute values in (16) we get

$$4[m^2+(n-m)^2+m(n-m)\cdot 2\Re(\chi(m)\overline{\chi}(n-m))]=n^2.$$

It follows that the algebraic integer $\theta=2\Re(\chi(m)\overline{\chi}(n-m))$ is a rational number, hence $\theta\in\{-2,-1,0,1,2\}$. We get

$$(8-4\theta)m^2+(4\theta-8)mn+3n^2=0.$$

This equation can have integer solutions only if $\theta=-2,-1,2$. If $\theta=2$ then $n=0$, impossible. If $\theta=-1$, then $n=2m$, but in this case $n-m=m$, hence $\chi(m)=\chi(n-m)$, $\chi(m)\overline{\chi}(m-n)=1$ and $\theta=2$, a contradiction. If $\theta=-2$, then either $4m=n$ and $4(n-m)=3n$ or $4m=3n$ and $4(n-m)=n$, and therefore $\chi(3)=-1$.

If $\chi(2)=\pm i$, taking the squares of absolute values in (16) we get

$$2(m^2+(n-m)^2+\theta m(n-m))=n^2.$$

This last equation has rational solutions only if $\theta=0,2$. If $\theta=0$ we get $n=2m$, $n-m=m=n_1$ and

$$(1\pm i)n\chi(n_1)=n\chi(n_1),$$

a contradiction. If $\theta=2$ we get $n=0$, also a contradiction.

It follows that this case implies $\chi(2)=\chi(3)=-1$, $\{4m,4(n-m)\}=\{n,3n\}$.

Case 2: $(\chi(m))^2 - (\chi(n-m))^2 \in (2)$. This implies that either $\chi(m) = \pm\chi(n-m)$ or $\chi(m) = i\chi(n-m)$, where $i^2 = -1$. In the latter case the greatest common divisor of the ideals $((1 \pm i)\chi(m))$ and (2) is $(1 \pm i) = (\mathcal{P}_1 \dots \mathcal{P}_s)^{e/2}$, hence we fall again into Case 1.

If $\chi(m) = -\chi(n-m)$, then from (16) we have

$$(1 - \overline{\chi}(2))(2m - n)\chi(m) = n\chi(n_1).$$

This implies again that $|1 - \overline{\chi}(2)| \in \{0, 1, 2\}$. The case when $1 - \overline{\chi}(2) = 0$, hence $\chi(2) = 1$, is excluded trivially. If $|1 - \overline{\chi}(2)| = 1$, then we get $|2m - n| = |n|$, which implies either $n = m$ or $m = 0$, both cases being impossible. If $|1 - \overline{\chi}(2)| = 2$, hence $\chi(2) = -1$, we get $|4m - 2n| = |n|$, and considering both signs we get $\{4m, 4(n-m)\} = \{n, 3n\}$, and consequently $\chi(3) = -1$.

If $\chi(m) = \chi(n-m)$, we obtain

$$(1 - \overline{\chi}(2))n\chi(m) = n\chi(n_1),$$

whence $\chi(2) = 1 - \overline{\chi}(2) = \zeta_6$ and $\chi(n_1) = \zeta_6\chi(m) = \zeta_6\chi(n-m)$. ∎

Let X be the set of even Dirichlet characters of conductor Q' and let Z be the subset of even characters of conductor Q' having either property (17) or (18). Moreover, let H be the subgroup of even Dirichlet characters mod Q' generated by Z and let K be the subgroup of even Dirichlet characters mod Q' defined by the equation $\chi(k) = 1$. Equation (16) holds for all even characters of conductor Q' only if $X \subset Z \cup K$, whence clearly only if $X \subset H \cup K$.

Suppose that $K \neq G$, and consider first the case when H is the full group of even Dirichlet characters mod Q'. Since both equations (17) and (18) imply that $\chi(2)^6 = 1$, this can only happen if $2^6 \equiv \pm 1 \pmod{Q'}$, i.e. $Q' \mid 63$ or $Q' \mid 65$.

Lemma 7. *If $Q' \neq 3, 5$ and either $Q' \mid 63$ or $Q' \mid 65$, then there exists a subset Y of the set X of even primitive characters mod Q' such that*:

(i) *for all $\chi \in Y$ relation (16) does not hold*;

(ii) *Y generates the full group G of even Dirichlet characters mod Q'.*

Proof. Direct checking or computer search. ∎

By Lemma 7, we immediately conclude that $k \equiv \pm 1 \pmod{Q'}$ if $Q' \mid 64 \pm 1$ except for the case when $Q' = 5$ and $\{4m, 4(n-m)\} = \{n, 3n\}$.

Let Q' be such that $Q' \nmid 64 \pm 1$ and suppose that $K \neq G$. By Lemma 3, and with the notation of that lemma, $X \not\subset H \cup K$ unless $Q' = 3Q'_1Q'_2$, H is contained in the maximal subgroup H_0 given by those characters whose restriction mod Q'_1 is the full group of even characters mod Q'_1, and K is contained in the maximal subgroup K_0 given by those characters whose restriction mod Q'_2 is the full group of even characters mod Q'_2.

Lemma 8. *If $H = H_0$, then $X \not\subset Z \cup K$.*

Proof. By (17) and (18), $H = H_0$ implies that $64 \equiv \pm 1 \pmod{Q'_1}$. Since $(3, Q'_2) = 1$, we can have $3Q'_2 \mid 64 \pm 1$ only if $Q'_2 = 7$.

Case 1: $Q'_2 \neq 7$. By Lemma 2, the set of primitive even characters mod $3Q'_2$ generates the group of all even Dirichlet characters mod $3Q'_2$, hence there exists an even character χ of conductor $3Q'_2$ such that $\chi(2) \notin \mu_6$. Letting χ' be any even character of conductor Q'_1, we get $\chi'\chi(2) \notin \mu_6$, hence neither (17) nor (18) is satisfied; moreover, the restriction of $\chi'\chi$ mod Q'_2 is odd, so $\chi'\chi \notin K$.

Case 2: $Q'_2 = 7$. By direct checking, we get $Q'_1 \in \{5, 13, 65\}$. For all these cases, it is an exercise to find characters χ of conductor Q' for which $\chi(2) = \zeta_3$, whence $\chi \notin Z \cup K$. ∎

If H is strictly contained in H_0, then Lemma 4 shows again that $X \not\subset H \cup K$ unless $Q'_1 = 5$, $Q' = 3 \cdot 5 \cdot Q'_2$, $(15, Q'_2) = 1$, H coincides with the subgroup of the characters defined by equation (12) and K is contained in the subgroup of those characters whose restriction mod 15 is even. We claim that also in this case $X \not\subset Z \cup K$.

Definition 1. Here and in what follows, if $q > 2$ is a prime power we shall denote by χ_q an (odd) generator of the group of characters mod q.

Consider characters of type $\chi_3\chi_5^2\chi$, where χ is an odd primitive character mod Q'_2. Since $\chi_3\chi_5^2(2) = 1$, it is enough to show that there exists an odd primitive character χ mod Q'_2 such that $\chi(2) \neq -1, \zeta_6$. Clearly the odd primitive characters mod Q'_2 generate the full group $\widehat{G}$ of Dirichlet characters mod Q'_2 (remember that Q'_2 is odd), hence the existence of such a χ is guaranteed unless $Q'_2 \nmid 63 = 2^6 - 1$, which, in our situation, leaves only the case $Q'_2 = 7$. In this case we can take $\chi = \chi_3\chi_5^2\chi_7$, and the claim is proved.

It follows that, if $H \neq G$, then $X \subset H \cup K$ implies $K = G$, whence $k \equiv \pm 1 \pmod{Q'}$. Together with Lemma 7, this concludes the proof of Proposition 5. ∎

Remark 2. We make it explicit what happens in the case $Q' = 5$ and $\{4m, 4(n-m)\} = \{n, 3n\}$. The assumptions in Proposition 5 say that k is odd; moreover, in this case $k \not\equiv 5 \pmod{10}$, since otherwise we would have $\zeta^{kn} - 1 = 0$. The condition $\chi(2) = \chi(3) = -1$ is clearly satisfied for the only non-trivial even character χ mod 5. The condition $\{4m, 4(n-m)\} = \{n, 3n\}$ implies that $n = 4x$ for some integer x; moreover, x cannot be divisible by 5 (otherwise n would be divisible by 10 and $\zeta^{kn} - 1 = 0$) and x must be odd (otherwise $m, n-m, n$ would be all even). It follows that $\{m, n-m\} = \{x, 3x\}$ and $n = 4x$ for some x coprime to 10. In all these cases, it is easy to verify that the two terms in (1) coincide, their common value being $1/5^x$. Finally, by the symmetry among the numbers $m, n-m, -n$ remarked in the

introduction, equation (1) holds whenever $\{m, n-m, -n\} = \{x, 3x, -4x\}$ and $(x, 10) = (k, 10) = 1$.

PROPOSITION 6. *Let $\zeta_1 = \zeta$, $\zeta_2 = \zeta^k$, k even, and $Q = 2Q'$, Q' odd. Suppose that $(m, Q') = (n-m, Q') = (n_1, Q') = 1$. Then equation (1) does not hold.*

Proof. Let $k = 2k_1$. For even characters χ of modulus Q' Ennola's relations (7) give

$$[1 - \overline{\chi}(2) - \chi(k_1)](m\chi(m) + (n-m)\chi(n-m)) = (1 - \chi(k))n\chi(n_1). \tag{20}$$

Suppose first that $\chi(k_1) = 0$, whence $\chi(k) = 0$. Then equation (20) reduces to equation (16). Proposition 5 shows that this equation can be satisfied for all characters only if $Q' = 5$. But in this case $\chi(k)$ cannot be zero, since otherwise k would be divisible by 10. Hence in the rest of the proof we shall assume $\chi(k_1) \neq 0$.

LEMMA 9. *If equation (20) holds, then $\chi(2)$ belongs either to μ_6 or to μ_{10}. Moreover, if $\chi(2) = \pm 1$, then χ has order multiple of 6.*

Proof. Consider, as in Lemma 6, the congruence modulo the ideal (2) in $\mathbb{Z}[\zeta_d]$:

$$(1 - \overline{\chi}(2) - \chi(k_1))(\chi(m) - \chi(n-m)) \equiv 0 \pmod{(2)}. \tag{21}$$

The greatest common divisor between the ideals $(\chi(m) - \chi(n-m))$ and (2) is of the form $(\mathcal{P}_1 \dots \mathcal{P}_s)^{e'}$, hence we see again that either $(1 - \overline{\chi}(2) - \chi(k_1))^2$ or $(\chi(m) - \chi(n-m))^2$ must be divisible by 2.

CASE 1: $1 - (\overline{\chi}(2))^2 - (\chi(k_1))^2 \in (2)$. If we have $1 + \zeta_d^a + \zeta_d^b \in (2)$, then the same is true for its complex conjugate, hence $1 + \zeta_d^{b-a} + \zeta_d^b \in (2)$ and $\zeta_d^a + \zeta_d^{b-a} \in (2)$. This means that $\zeta_d^a = \pm\zeta_d^{b-a}$, $\zeta_d^b = \zeta_d^a\zeta_d^{b-a} = \pm\zeta^{2a}$ and $\zeta^{3a} = \pm 1$. Notice that however ζ^a cannot be itself equal to ± 1, hence $\zeta^a = \zeta_3$ or $\zeta^a = \zeta_6$.

It follows that $\chi(2)$ must be one of $\zeta_3, \zeta_6, \zeta_{12}$.

CASE 2: $(\chi(m))^2 - (\chi(n-m))^2 \in (2)$. As in Lemma 6, we can suppose that $\chi(m) = \pm\chi(n-m)$.

Suppose that $\chi(m) = \chi(n-m)$. Putting this into (20), we get

$$[1 - \overline{\chi}(2) - \chi(k_1)]\chi(m) = (1 - \chi(k))\chi(n_1), \tag{22}$$

giving a 5-term relation among roots of unity. Suppose first that such a relation is indecomposable. By a theorem of Conway and Jones [2], all the roots of unity involved (i.e. the ratios between two roots of unity occurring in the relation) must belong either to μ_6 or to μ_{10}. If the relation is decomposable, then necessarily it must split into two subrelations of lengths 2 and 3. We leave it as an exercise to the reader to check that all possible splittings give either a contradiction or the conclusion $\chi(2) \in \mu_6$.

Moreover, notice that substituting $\chi(2) = 1$ into (22) gives $\chi(k) = \chi(k_1) = \zeta_6$ and $\chi(m) = \zeta_6\chi(n_1)$; and substituting $\chi(2) = -1$ gives $\chi(k_1) = -\chi(k) = \zeta_6$ and again $\chi(m) = \zeta_6\chi(n_1)$, whence χ has order multiple of 6.

Suppose now that $\chi(m) = -\chi(n-m)$, and substitute this into (20). We get

$$[1 - \overline{\chi}(2) - \chi(k_1)](2m - n)\chi(m) = (1 - \chi(k))n\chi(n_1), \tag{23}$$

yielding a 5-term relation among roots of unity. If the relation is indecomposable, then all roots of unity involved belong either to μ_6 or to μ_{10}. If any of the roots of unity involved has order multiple of 5, then all coefficients must have the same absolute value, hence $|2m - n| = |n|$, impossible under our hypotheses. Hence necessarily all roots involved, and in particular $\chi(2)$, must belong to μ_6. Consider now the case when the relation is decomposable, whence necessarily it splits in one 2-term relation and one 3-term relation. Both relations must have coefficients of equal absolute value, whence the only possibility is that the two terms are $1, \chi(k)$ and the three terms are $1, \overline{\chi}(2), \chi(k_1)$. This again implies that $\chi(2) \in \mu_6$.

Moreover, note that if $\chi(2) = 1$ then $\chi(k) = \chi(k_1)$ and $1 - \chi(k)$ must be an integer. If $1 - \chi(k) = 0$ then $2m - n = 0$ and $\chi(m) = \chi(n - m)$, a contradiction. If $1 - \chi(k) = 1$ then $|2m - n| = |n|$, impossible under our hypotheses. If $1 - \chi(k) = 2$, hence $\chi(k) = -1$, we get $(2m - n)\chi(m) = 2n\chi(n_1)$; it follows that $|2m - n| = |2n|$, so either $2m = 3n$ and $2(n - m) = -n$ or $2m = -n$ and $2(n-m) = 3n$. In both cases we must have $\chi(3) = -1$ and, substituting into (23), we get a contradiction.

If $\chi(2) = -1$, hence $\chi(k) = -\chi(k_1)$, then taking absolute values we obtain

$$[5 - 2(\chi(k_1) + \overline{\chi}(k_1))](2m - n)^2 = [2 + (\chi(k_1) + \overline{\chi}(k_1))]n^2.$$

It follows that $\chi(k_1)+\overline{\chi}(k_1)$ must lie in the set $\{-2, -1, 0, 1, 2\}$; a direct check shows that the cases when $\chi(k_1)+\overline{\chi}(k_1) = 0, -1$ do not have integer solutions (m, n); the case $\chi(k_1) + \overline{\chi}(k_1) = -2$ gives $n = 2m$ and contradicts our hypotheses, the case $\chi(k_1)+\overline{\chi}(k_1) = 1$ gives $|2m-n| = |n|$, contradicting our hypotheses; finally, $\chi(k_1)+\overline{\chi}(k_1) = 2$ leads to the equation $(2m-n)\chi(m) = 2n\chi(n_1)$, already considered above and shown to be contradictory.

To conclude the proof of the lemma, it remains to exclude the case when $\chi(2) \in \mu_{12}$, which occurs in Case 1.

If $\chi(2) = \zeta_{12}$ and $1-(\overline{\chi}(2))^2-(\chi(k_1))^2 \in (2)$, then $\chi(k_1) \in \{\zeta_{12}, \zeta_{12}^4, \zeta_{12}^7, \zeta_{12}^{10}\}$. The factorization of the ideal (2) in $\mathbb{Z}[\zeta_{12}]$ is $(2) = \mathcal{P}^2 = (\zeta_{12}^2+\zeta_{12}+1)^2$ and it is easily checked that in all the above cases we have $(1-\overline{\chi}(2)-\chi(k_1)) = \mathcal{P}$. This means that Case 2 must hold as well. Since $\chi(m) = \pm\chi(n - m)$ imply that $\chi(2)$ belongs either to μ_6 or to μ_{10}, it remains to consider the

case when $\chi(m) = \pm i\chi(n-m)$, where $i^2 = -1$. For $j \in \{1,4,7,10\}$, let

$$A_j = |1 - \overline{\chi}(2) - \chi(k_1)|^2 = |1 - \zeta_{12}^{-1} - \zeta_{12}^{j}|^2,$$
$$B_j = |1 - \chi(k)|^2 = |1 - \zeta_{12}^{j+1}|^2.$$

Taking the squares of absolute values in (20) we obtain

$$A_j[m^2 + (n-m)^2] = B_j n^2 \quad \text{for } j \in \{1,4,7,10\}.$$

We leave it to the reader to check that the last equation has no integer solutions (m,n) for $j \in \{1,4,7,10\}$. ∎

By Lemma 9, if $Q' \nmid 2^{10} \pm 1$ and $Q' \nmid 2^6 \pm 1$ there exist even characters of maximal conductor for which (20) is not true, hence Proposition 6 follows for these values of Q'. The remaining cases can be settled by a computer search. ∎

PROPOSITION 7. *Let $\zeta_1 = \zeta$, $\zeta_2 = \zeta^k$, $Q = 2Q'$, Q' odd. Suppose that exactly two of the numbers $m, n-m, n_1$ are coprime to Q. If equation* (1) *holds, then $k \equiv \pm 1 \pmod{Q}$.*

Proof. The relevant equations depend on the parity of k and on which terms are coprime to Q. Consider first the case when k is odd. Then we must consider specializations of (15).

CASE 1: The relevant equation is

$$(1 - \chi(k))[(1 - \overline{\chi}(2))(m\chi(m) + (n-m)\chi(n-m))] = 0.$$

We examine when the term inside the square brackets is zero, i.e. when

$$(1 - \overline{\chi}(2))(m\chi(m) + (n-m)\chi(n-m)) = 0. \tag{24}$$

Equation (24) implies that $\chi(2) = 1$. The subgroup H of Dirichlet characters with this property is always proper. If $K \neq G$, we can have $X \subset H \cup K$ only if $Q' = 3Q_1'Q_2'$ and H is contained in the subgroup of those characters whose restriction mod Q_1' is even. It cannot coincide with this subgroup, since $Q_1' \neq 3$. If it is properly contained in this subgroup, then the only possibility is that $Q = 3 \cdot 5 \cdot Q_2'$ and H coincides with the subgroup defined by equation (12), while K is contained in the subgroup of those characters whose restriction mod 15 is even.

If this is the case, consider characters of the type $\chi_3\chi_5^2\chi$, where χ is an odd primitive character mod Q_2'. Since $\chi_3\chi_5^2(2) = 1$, it is enough to show that there exists a primitive character χ mod Q_2' such that $\chi(2) \neq 1$, and this is trivial.

CASE 2: The equation is

$$(1 - \chi(k))[(1 - \overline{\chi}(2))m\chi(m) - n\chi(n_1)] = 0.$$

We look again when the term inside the square brackets is zero, i.e. when

$$(1-\overline{\chi}(2))m\chi(m)-n\chi(n_1)=0. \tag{25}$$

Equation (25) can hold only if the congruence mod (2) is satisfied, i.e. if $\chi(2)=\pm 1$. The subgroup of characters with this property is not the full group G unless $Q'=5$. But Q' cannot be a prime number, otherwise we would have $Q' \mid n-m$, contrary to our assumptions. Hence the subgroup is proper, and we can use the argument above to show that we need only consider the case $Q=3Q'_1Q'_2$ and H is contained in the subgroup of those characters whose restriction mod Q' is even. Both when H coincides with this subgroup and when it is properly contained in it, we must have $Q'_1=5$. Remembering that $\chi_3\chi_5^2(2)=1$, this time it is enough to show that there exists an odd primitive character χ mod Q'_2 such that $\chi(2)\neq\pm 1$, and this is again trivial.

Let now $k=2k_1$ be even. Then we must look at specializations of (20).

Case 3: The equation is

$$(1-\overline{\chi}(2)-\chi(k_1))(m\chi(m)+(n-m)\chi(n-m))=0.$$

If $\chi(k_1)=0$, we reduce to equation (24) and the argument of Case 1 applies.

If $\chi(k_1)\neq 0$, then the only possibility is that $\chi(2)=\chi(k_1)=\zeta_6$. This leads again to the study of the cases when either $Q' \mid 63$ or $Q' \mid 65$, which can be dealt with directly.

Case 4: The equation is

$$(1-\overline{\chi}(2)-\chi(k_1))m\chi(m)=(1-\chi(k))n\chi(n_1). \tag{26}$$

If $\chi(k_1)=0$, then we reduce to (25), and the argument of Case 2 applies.

If $\chi(k_1)\neq 0$, then the congruence mod (2) implies that $\chi(2)=\zeta_3,\zeta_6$, hence $Q' \mid 63$ or $Q' \mid 65$. A direct check gives the conclusion. ∎

Proposition 8. *Let $\zeta_1=\zeta$, $\zeta_2=\zeta^k$, $Q=2Q'$, Q' odd. Suppose that exactly one of the numbers $m, n-m, n_1$ is coprime to Q. If equation* (1) *holds, then $k\equiv\pm 1 \pmod{Q}$.*

Proof. Consider first the case when k is odd, and hence specializations of (15).

Case 1: The equation is

$$(1-\chi(k))[(1-\overline{\chi}(2))m\chi(m)]=0.$$

Use the same argument as in Proposition 7, Case 1.

Case 2: The equation is

$$(1-\chi(k))n\chi(n_1)=0,$$

which gives immediately the conclusion.

Suppose now that $k=2k_1$ is even, and specialize (20) accordingly.

Case 3: The equation is

$$(1-\overline{\chi}(2)-\chi(k_1))m\chi(m)=0.$$

Use the same argument as in Proposition 7, Case 3.

Case 4: The equation is

$$(1-\chi(k))n\chi(n_1)=0.$$

This equation can be true for all primitive characters only if $k \equiv \pm 1 \pmod{Q'}$. If this is the case, let $(m,Q')=m_0$, $m=m_0m^*$, $Q'=m_0f_m$, so that $(m^*,f_m)=1$. Define $(n-m)^*$ and f_{n-m} similarly. Since $[f_m,f_{n-m}]=Q'$ and Q' has at least two distinct prime factors, at least one between f_m and f_{n-m}, say f_m, is greater than 3, hence we may consider non-trivial even characters χ of conductor $f=f_m$. Let d be such that $f \mid d \mid Q$. The equation $(Q/d)x=m$ has a solution with $(x,d)=1$ only in the case $d=2f$ and the solution is $x=m^*$; the equation $(Q/d)x=km$ has a solution with $(x,d)=1$ only if $d=f$ and the solution is $x=k_1m^*$; the equations $(Q/d)x=n-m,k(n-m)$ do not have solutions with $(x,d)=1$ since $(Q,n-m)=1$ and $(n-m,f)>1$; the equations $(Q/d)x=n,kn$ have solutions with $(x,d)=1$ only if $d=m_0f=Q'$ and the solutions are $x=n_1,kn_1$. The corresponding relations (7) give

$$\frac{1}{\phi(f)}(1-\overline{\chi}(2)-\chi(k_1))m\chi(m^*)=\frac{1}{\phi(Q')}\Big(\prod_{p\mid m_0}(1-\overline{\chi}(p))\Big)(1-\chi(k))\chi(n_1).$$

Now notice that $k\equiv\pm1 \pmod{Q'}$ implies $k\equiv\pm1 \pmod{f}$, hence $\chi(k)=1$ and the term on the right is zero. Also, since $k=2k_1$, $\chi(k_1)=\overline{\chi}(2)$, hence we obtain $2\overline{\chi}(2)=1$, a contradiction. ∎

Proposition 9. *Let $\zeta_1=\zeta$, $\zeta_2=\zeta^k$, $Q=2Q'$, Q' odd. Suppose that none of the numbers $m, n-m, n_1$ is coprime to Q. Then $k\equiv\pm1 \pmod{Q}$.*

Proof. Let $(m,Q')=p_1^{\alpha_1}\dots p_r^{\alpha_r}$, $m=(m,Q')m^*$, $Q'=(m,Q')f_m$, so that $(m^*,f_m)=1$, whereas $(n-m,f_m)>1$ and $(n,f_m)>1$. Define f_{n-m} and f_n similarly. All numbers f_m, f_{n-m}, f_n are divisible by at least two prime factors. Consider even characters χ of conductor $f=f_m$.

Let d be an integer such that $f_m \mid d \mid Q$, and write $d=p_1^{i_1}\dots p_r^{i_r}f$. The equations $(Q/d)x=n,kn$ are not solvable under the given conditions, since $(Q/d,n)=2$ and a possible solution would satisfy $x\equiv0 \pmod{n_1}$, hence $(x,f_m)>1$ and a fortiori $(x,d)>1$; the same argument shows that the equations $(Q/d)x=n-m,k(n-m)$ are not solvable with $(x,d)=1$. The equation $(Q/d)x=(2Q'/d)x=p_1^{\alpha_1-i_1}\dots p_r^{\alpha_r-i_r}x=m$ has a solution only if $2 \mid d$ and the solution is $x=p_1^{i_1}\dots p_r^{i_r}m^*$; this solution is coprime to d only if

$i_1 = \ldots = i_r = 0$, i.e. if $d = 2f_m$. As for the equation $(Q/d)x = (2Q'/d)x = km$, there is only one solution of the type required, namely $x = km^*$ for $d = 2f_m$ if k is odd, and $x = k_1 m^*$ for $d = f_m$ if $k = 2k_1$ is even.

Hence relations (7) for such characters become

$$\begin{cases} (1-\chi(k))(1-\overline{\chi}(2))m\chi(m^*) = 0 & \text{if } k \text{ is odd,} \\ (1-\overline{\chi}(2)-\chi(k_1))m\chi(m^*) = 0 & \text{if } k \text{ is even.} \end{cases}$$

By Proposition 8, we obtain $k \equiv \pm 1 \pmod{2f_m}$ and, similarly, $k \equiv \pm 1 \pmod{2f_{n-m}}$. But the solutions of the single congruences must agree modulo $(2f_m, 2f_{n-m}) > 2$ and $[2f_m, 2f_{n-m}] = Q$, hence we get $k \equiv \pm 1 \pmod{Q}$. ∎

REMARK 3. If $Q \not\equiv 2 \pmod 4$ and at least one of the numbers $m, n-m, n$ is coprime to Q, Propositions 1, 2 and 3 show that equation (13) cannot be true for all primitive characters mod Q. If $Q \equiv 2 \pmod 4$ and at least one of the numbers $m, n-m, n_1$ is coprime to Q', Propositions 5, 7 and 8 show that, apart from the exceptions given, equation (16) cannot be true for all primitive characters mod Q'.

We shall use this remark in the proof of Proposition 10.

5. The case when none of the roots is primitive

PROPOSITION 10. *If neither ζ_1 nor ζ_2 is a primitive Qth root of unity, then equation* (1) *does not hold.*

Proof. Let $\zeta_1 = \zeta^l$ and $\zeta_2 = \zeta^k$, $(l, Q) = D_l > 1$, $(k, Q) = D_k > 1$, $(D_l, D_k) = 1$.

Let also $l = D_l l^*$, $Q = D_l f_l$ so that $(l^*, f_l) = 1$ and $(k, f_l) > 1$. Define f_k similarly. Note that, since $(l, k, Q) = 1$, we have $[f_l, f_k] = Q$.

By using relations of type (8), one can easily exclude the finite number of cases when both f_l and f_k are contained in the set $\{2, 3, 4, 6\}$. By symmetry, we can suppose that $f_l \notin \{2, 3, 4, 6\}$. If both f_l and f_k do not belong to $\{2, 3, 4, 6\}$, one can of course suppose also that $f_l \neq 10$. If f_k does belong to the set $\{2, 3, 4, 6\}$, one further application of relations (8) leads us to exclude that $f_l = 10$ and $\{4m, 4(n-m)\} = \{n, 3n\}$.

Summarizing, we can assume, by symmetry, that f_l satisfies the following condition:

(27) $f_l \notin \{2, 3, 4, 6\}$ and, if $f_l = 10$, then $\{4m, 4(n-m)\} \neq \{n, 3n\}$.

The following lemma shows that we can also assume that $D_k \neq 2, 4$.

LEMMA 10. *If $D_k = 2, 4$ and f_l satisfies condition* (27), *then $D_l \neq 2, 4$ and we can assume that also f_k satisfies condition* (27).

Proof. Since $(k,l,Q)=1$, $D_k=2,4$ implies that D_l is odd. Now, as $Q=D_kf_k$, the lemma is reduced to the verification of a finite number of cases. ∎

Suppose now that $f_l \not\equiv 2 \pmod 4$ and at least one of the numbers m, $n-m, n$ is coprime to f_l. Consider even characters χ of conductor $f=f_l$ and let d be such that $f \mid d \mid Q$. The equations $(Q/d)x = km, k(n-m), kn$ are not solvable under the given conditions, since $(Q/d,k)=1$ and $(k,f_l)>1$. Similarly, the equations $(Q/d)x = lm, l(n-m), n$ can have a solution of the type required only if $d=f_l$ (the existence of a solution depending, respectively, on whether or not $(m,f_l)=1$, $(n-m,f_l)=1$, $(n,f_l)=1$). In any case we are left with the relations

$$\chi(l^*)(m\chi(m)+(n-m)\chi(n-m)-n\chi(n))=0.$$

Since $\chi(l^*)\neq 0$, these relations cannot hold for all even characters χ of conductor f_l by Remark 3.

Next, suppose that $f_l=2f_l' \equiv 2 \pmod 4$, $n=2n_1$ and that at least one of the numbers $m, n-m, n_1$ is coprime to f_l. Consider even characters χ of conductor $f=f_l'$ and let d be such that $f \mid d \mid Q$ as before.

The equations $(Q/d)x = km, k(n-m), kn$ are not solvable under the given conditions, since $(Q/d,k)\leq 2$ and $(k,f_l)>2$. The equations $(Q/d)x = lm, l(n-m)$ can have a solution of the type required only if $d=f_l'$, and in this case we have $x=l^*m, l^*(n-m)$. The equation $(Q/d)x=ln$ can have a solution of the type required only if $d=f_l$, the solution being $x=l^*n_1$. Hence relations (7) for these characters give

$$\chi(l^*)[(1-\overline{\chi}(2))(m\chi(m)+(n-m)\chi(n-m))-n\chi(n_1)]=0.$$

But $\chi(l^*)\neq 0$, and, taking into account that we have supposed $\{4m, 4(n-m)\} \neq \{n, 3n\}$ if $f_l=10$, these relations cannot hold for all even characters χ of conductor f_l' by Remark 3.

Assume now that none of the numbers $m, n-m, n$ is coprime to f_l, and let $D_m=(m,f_l)>1$, $D_{n-m}=(n-m,f_l)>1$, $D_n=(n,f_l)>1$. Clearly we have $(D_m,D_{n-m})=(D_m,D_n)=(D_{n-m},D_n)=1$. Notice that in this case f_l must be divisible by at least three distinct prime factors, and in particular there exists a prime $p_0\geq 5$ such that $p_0 \mid f_l$. If $D_k \mid 2D_m$, then $D_k \nmid 2D_{n-m}$ and $D_k \nmid 2D_n$, otherwise m and n would have a common factor which is a divisor of Q (remember that we have supposed $D_k \neq 2,4$).

Remark 4. In what follows we allow complete symmetry among the numbers $m, n-m, -n$, and in particular we do not suppose that $-n$ is the even number among the three.

Possibly interchanging the roles of $m, n-m, n$, we can then suppose that $D_k \nmid 2D_m$. Also, since at least two of $m, n-m, n$ have this property, the

choice can be made so that $p_0 \nmid D_m$. Let $f_l = D_m f^*$, $m = D_m m^*$, so that $(m^*, f^*) = 1$. Now f^* is divisible by at least two distinct prime factors, one of which is p_0. Finally, if any of the numbers D_m, D_{n-m}, D_n is equal to 2, we agree to choose m so that $D_m = 2$, while D_{n-m} and D_n are odd.

If $f^* \not\equiv 2 \pmod 4$, consider even primitive characters of conductor f^*. Letting again d be such that $f^* \mid d \mid Q$, the equations $(Q/d)x = km$, $k(n-m), kn$ have no solutions under the given conditions, since $(D_l, D_k) = 1$ and $D_k \nmid D_m$ ensure that a possible solution would be divisible by a prime dividing D_k, and hence would not be coprime to f^*. The equation $(Q/d)x = lm$ has a solution of the type required only if $d = f^*$, the solution being $x = l^* m^*$, a number coprime to f^*. The equations $(Q/d)x = l(n-m), ln$ do not have solutions of the type required; in fact, in order that a solution be coprime to df^* we must necessarily have $(d, l) = 1$ and, assuming this, the condition $(D_m, D_{n-m}) = (D_m, D_n) = 1$ implies that a possible solution would have a factor dividing D_{n-m}, D_n, respectively, and hence would not be coprime to df^*. It follows that relations (7) simply tell you that

$$m\chi(l^* m^*) = 0,$$

a contradiction.

If $f^* = 2f'^* \equiv 2 \pmod 4$, consider even primitive characters of conductor f'^*. Letting again d be such that $f^* \mid d \mid Q$, the equations $(Q/d)x = km$, $k(n-m), kn$ have no solutions under the given conditions, since $(D_l, D_k) = 1$ and $D_k \nmid 2D_m$ ensure that a possible solution would be divisible by a prime dividing D_k, and hence would not be coprime to f^*. The equation $(Q/d)x = lm$ has a solution of the type required only if either $d = f^*$ or $d = f'^*$, depending on whether m^* is odd or $m^* = 2m_1^*$ is even; the solution in this case is either $x = l^* m^*$ or $x = l^* m_1^*$, in any case a number coprime to f'^*. The equations $(Q/d)x = l(n-m), ln$ do not have solutions of the type required; in fact, in order that a solution be coprime to df^* we must necessarily have $(d, l) = 1$; assuming this, the conditions $(D_m, D_{n-m}) = (D_m, D_n) = 1$ and $D_{n-m} \neq 2$, $D_n \neq 2$ imply that $D_{n-m} \nmid 2D_m$, $D_n \nmid 2D_m$, hence a possible solution would have a factor dividing D_{n-m}, D_n, respectively, and therefore would not be coprime to df^*. It follows that relations (7) simply tell you that

$$\begin{cases} (1 - \overline{\chi}(2))m\chi(l^* m^*) = 0 & \text{if } m^* \text{ is odd,} \\ m\chi(l^* m_1^*) = 0 & \text{if } m^* \text{ is even,} \end{cases}$$

and this is impossible for all even characters mod f'^* since f'^* is divisible by $p_0 \geq 5$. ∎

Acknowledgements. I wish to thank Professor Andrzej Schinzel for suggesting the problem to me and for several helpful comments. Also, I acknowledge the hospitality of the Instytut Matematyczny Polskiej Akademii Nauk, where most of this research was done.

References

[1] M. Conrad, *On explicit relations between cyclotomic numbers*, Acta Arith. 93 (2000), 67–76.
[2] J. H. Conway and A. J. Jones, *Trigonometric diophantine equations* (*On vanishing sums of roots of unity*), ibid. 30 (1976), 229–240.
[3] V. Ennola, *On relations between cyclotomic units*, J. Number Theory 4 (1972), 236–247.
[4] A. Schinzel, *On the greatest common divisor of two univariate polynomials*, *II*, this issue, 95–106.
[5] A. Schinzel, J. Urbanowicz and P. Van Wamelen, *Class numbers and short sums of Kronecker symbols*, J. Number Theory 78 (1999), 62–84.
[6] C.-G. Schmidt, *Die Relationsfaktorgruppen von Stickelberger-Elementen und Kreiszahlen*, J. Reine Angew. Math. 315 (1980), 60–72.
[7] W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. 108 (1978), 107–134.
[8] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1997.

Dipartimento di Matematica
Via F. Buonarroti, 2
56127 Pisa, Italy
E-mail: dvornic@dm.unipi.it

Received on 1.2.2000
and in revised form on 23.5.2000 (3748)