Using (33) to eliminate \( r \), we get

\[
\sum_{c \in C} \lambda(c) \leq \frac{a}{2w} (2k-1+2w-w-g)(2k-2+2w-w+g) = \frac{a}{2w} (2k-1+2w-w)(2k-2+2w-w).
\]

Hence

\[
\sum_{c \in C} \lambda(c) \leq \begin{cases} 
\frac{a}{w+1} (2k+1)(2k) & \text{if } w \text{ is even,} \\
\frac{a}{w+1} (2k)(2k-1) & \text{if } w \text{ is odd.}
\end{cases}
\]

Since \( w \leq 2k-2 \), \( \frac{2k+1}{w+2} < \frac{2k}{w+1} \), hence

\[
\sum_{c \in C} \lambda(c) < \frac{4k^2a}{w+1}.
\]

On the other hand \( \sum_{c \in C} \lambda(c) \geq k^2 \), exactly as in Case 1, so \( a \geq \frac{1}{2}(w+1) \).

Hence \( a \geq \frac{1}{2}(w+2) \) and the lemma is proved.

References


A note on a cyclotomic diophantine equation

by

VeiKko ENNOLA (Turku)

1. Introduction. Let \( m \geq 3 \) be a natural number, \( \zeta_m = \exp(2\pi i / m) \),

and let \( K_m = \mathbb{Q} (\zeta_m) \) denote the cyclotomic field over the rationals \( \mathbb{Q} \).

We shall prove the following result:

**Theorem A.** Let \( q \geq 3 \), \( \beta \) is a unit in \( K_m \), and the equation

\[
a^q = \beta + 1
\]

has a solution \( a \in K_m \), then \( a = 0 \) or \( a \) is a root of unity.

In the special case when \( m \) is a prime \( \geq 3 \) and \( a \) is required to be a unit in \( K_m \), this result has been recently proved by Newman [5]. His proof depends on the following theorem (for prime values of \( m \)):

**Theorem B.** If \( m \) is any integer \( \geq 4 \), \( 2 \leq g \leq m-2 \), and \( q \geq 2 \), then

the only solution \( a \in K_m \) of the equation

\[
1 + \zeta_m + \zeta_m^2 + \cdots + \zeta_m^{g-1} = a^q
\]

is given by \( q = 2 \), \( m = 12 \), \( g = 7 \), \( a = \pm \zeta_m (1 - \zeta_m)^{-1} \).

In particular, if \( m \) is prime, then (2) does not have solutions with \( q \geq 2 \). This fact was stated as a conjecture by Newman [4] and was first proved by the author [1]. A very elegant proof of a more general result was given by Loxton [3]. The proof given by Newman [5] is incorrect. (The formula for \( \eta^q - \zeta \) on p. 87 is wrong.) In the general case Theorem B has been proved by the author [2].

Using the ideas of Newman we shall prove Theorem A directly without relying on Theorem B. It is possible that the new method will cause a simplification in the proof of Theorem B which is extremely complicated.

2. Proof of Theorem A. We assume that (1) has a solution, where \( a \) is nonzero and not a root of unity, and deduce a contradiction. Without loss of generality, we may assume that \( q = 4 \) or that \( q \) is an odd prime. By extending the field \( K_m \) if necessary, we may also assume that \( q \mid m \).

We use the following well-known fact: If \( \gamma \) is any unit in \( K_m \), then there
exists a root of unity \( \xi \in K \) such that \( \bar{y} = \eta y \). The basic idea, due to Newman, is to write (1) as \( \alpha^2 - 1 = \beta \), and then apply this fact to \( \alpha = \xi_k \) \((k = 0, 1, \ldots, q - 1)\), which are all units in \( K \).

Consider first the possibility \( q = 4 \). We have

\[
\xi - \xi^{-k} = \xi_k (\alpha - \xi_k^k) \quad (k = 0, 1, 2, 3),
\]

for some roots of unity \( \xi_k \in K \). Eliminating \( \alpha \) we obtain

\[
(\xi_k - \xi_k^k) \alpha = 2 - \xi_k - \xi_k^{-k}.
\]

If \( \xi_k = \xi_k \), then \( \xi_k = 1 \), whence \( \alpha \) is real. Applying (3) for \( k = 1 \), we obtain \( \alpha - 1 = 2(\xi_k - \xi_k^k) \). Since \( \alpha - 1 \) is a unit, this is possible only for \( \xi_k = -1 \). But then \( \alpha = 0 \), a contradiction. If \( \xi_k \neq \xi_k \), then \( \alpha - 1 = 2(1 - \xi_k^k) \). Again, this is possible only for \( \xi_k = -1 \), which implies \( \alpha = -\xi_k^k \), contradicting the assumption.

Consider now the case when \( q \) is an odd prime. We have

\[
\xi - \xi^{-k} = \xi_k (\alpha - \xi_k^k) \quad (k = 0, 1, \ldots, q - 1),
\]

for some roots of unity \( \xi_k \in K \). Assuming that \( \xi_k \neq \xi_k \), we find, eliminating \( \alpha \),

\[
a = (1 - \xi_k^k + \xi_k (\xi_k^k - \xi_k^k)/(\xi_k - \xi_k^k) \quad (k = 1, 2, \ldots, q - 1; \xi_k \neq \xi_k).\]

Therefore

\[
(\xi_k - \xi_k^k) \beta = (1 - \xi_k^k + \xi_k (\xi_k^k - \xi_k^k)^2 - (\xi_k - \xi_k^k)^2 = 0 \mod q.
\]

This is possible only if \( \xi_k \xi_k^{-1} = \xi_k^k \) for some \( t_k \neq 0 \mod 2 \). Then (4) implies

\[
a \xi_k (\xi_k^k - 1) = 1 - \xi_k^k + \xi_k (\xi_k^k - 1) \quad (k = 1, 2, \ldots, q - 1; \xi_k \neq \xi_k).
\]

Divide (5) by \( 1 - \xi_k^k \) and consider the resulting equation \( 1 - \xi_k^k \). We conclude that

\[
a \xi_k t_k = \xi_k (t_k + 1) \mod 1 - \xi_k^k.
\]

(6)

\[
t_k = (1 - \xi_k^k)(\alpha - 1)^{-k} \mod 1 - \xi_k.
\]

Since \( \xi_k = \xi_k \) for at most one \( k \) with \( 1 \leq k \leq q - 1 \), the congruence (8) holds for some \( k \), whence \( (1 - \xi_k^k)(\alpha - 1)^{-k} = \xi_k \) for some rational integer \( d \). (1 \leq d \leq q - 1). Thus

\[
t_k = d \xi_k \mod q.
\]

(7)

We now see also that \( \xi_k = \xi_k \) cannot, in fact, hold for \( k \neq 0 \), because in this case \( \xi_k = -\xi_k^k \), and we would have \( d = 0 \mod 1 - \xi_k^k \).

Consider the polynomial

\[
P(x) = \xi_k^k x^2 + a \xi_k^k x^{d+1} + (a \xi_k^k - \xi_k^k + 1) x - 1.
\]

It follows from (5) and (7) that \( x - \xi_k^k P(x) = 1 \) for \( k = 1, 2, \ldots, q - 1 \). Clearly also \( x - 1 | P(x) \). Hence \( x^k - 1 | P(x) \). However, it is easily seen that this

References


DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TURKU
Finland

Received on 28.3.1974

(549)