Using (33) to eliminate r, we get

$$\sum_{c\in C}\lambda(c)\leqslant\frac{a}{2u}(2k-1+2u-w-q)(2k-2+2u-w+q)$$
$$\leqslant\frac{a}{2u}(2k-1+2u-w)(2k-2+2u-w).$$

Hence

$$\sum_{c\in C}\lambda(c)\leqslant\begin{cases}\dfrac{a}{w+2}(2k+1)(2k) & \text{if} \quad w \text{ is even,}\\ \dfrac{a}{w+1}(2k)(2k-1) & \text{if} \quad w \text{ is odd.}\end{cases}$$

Since $w\leqslant 2k-2$, $\dfrac{2k+1}{w+2}<\dfrac{2k}{w+1}$, hence

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

On the other hand $\sum_{c\in C}\lambda(c)\geqslant k^2$, exactly as in Case 1, so $a>\frac{1}{4}(w+1)$. Hence $a\geqslant\frac{1}{4}(w+2)$ and the lemma is proved.

References

[1] P. Erdös and H. Heilbronn, *On the addition of residue classes* mod p, Acta Arith. 9 (1964), pp. 149–159.
[2] J. H. B. Kemperman, *On complexes in a semigroup*, Indag. Math. 18 (1956), pp. 247–254.
[3] J. E. Olson, *An addition theorem modulo p*, J. Combinatorial Theory 5 (1968), pp. 45–52.
[4] E. Szemerédi, *On a conjecture of Erdös and Heilbronn*, Acta Arith. 17 (1970), pp. 227–229.

DEPARTMENT OF MATHEMATICS
PENNSYLVANIA STATE UNIVERSITY
University Park, Pennsylvania

Received on 29. 3. 1974 (548)

ACTA ARITHMETICA
XXVIII (1975)

A note on a cyclotomic diophantine equation

by

VEIKKO ENNOLA (Turku)

1. Introduction. Let $m\geqslant 3$ be a natural number, $\zeta_m=\exp(2\pi i/m)$, and let $K_m=Q(\zeta_m)$ denote the cyclotomic field over the rationals Q. We shall prove the following result:

THEOREM A. *If $q\geqslant 3$, β is a unit in K_m, and the equation*

$$\alpha^q=\beta+1 \tag{1}$$

has a solution $\alpha\in K_m$, then $\alpha=0$ or α is a root of unity.

In the special case when m is a prime >3 and α 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 $\geqslant 4$, $2\leqslant g\leqslant m-2$, and $q\geqslant 2$, then the only solution $\alpha\in K_m$ of the equation*

$$1+\zeta_m+\zeta_m^2+\ldots+\zeta_m^{g-1}=\alpha^q \tag{2}$$

is given by $q=2$, $m=12$, $g=7$, $\alpha=\pm\zeta_m^5(1-\zeta_m)^{-1}$.

In particular, if m is prime, then (2) does not have solutions with $q\geqslant 2$. 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 $\eta^n-\zeta$ 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 leaning 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 α 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 $q|m$. We use the following well-known fact: If γ is any unit in K_m, then there exists a root of unity $\varrho \in K_m$ such that $\bar{\gamma} = \varrho\gamma$. The basic idea, due to Newman, is to write (1) as $\alpha^q - 1 = \beta$, and then apply this fact to $\alpha - \zeta_q^k$ ($k = 0, 1, \ldots, q-1$), which are all units in K_m.

Consider first the possibility $q = 4$. We have

$$\bar{\alpha} - i^{-k} = \xi_k(\alpha - i^k) \quad (k = 0, 1, 2, 3), \tag{3}$$

for some roots of unity $\xi_k \in K_m$. Eliminating $\bar{\alpha}$ we obtain

$$(\xi_2 - \xi_0)\alpha = 2 - \xi_2 - \xi_0.$$

If $\xi_2 = \xi_0$, then $\xi_0 = 1$, whence α is real. Applying (3) for $k = 1$, we obtain $\alpha - i = 2i/(\xi_1 - 1)$. Since $\alpha - i$ is a unit, this is possible only for $\xi_1 = -1$. But then $\alpha = 0$, a contradiction. If $\xi_2 \neq \xi_0$, then $\alpha - 1 = 2(1-\xi_2)/(\xi_2 - \xi_0)$. Again, this is possible only for $\xi_2 = -\xi_0$, which implies $\alpha = -\xi_0^{-1}$, contradicting the assumption.

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

$$\bar{\alpha} - \zeta_q^{-k} = \xi_k(\alpha - \zeta_q^k) \quad (k = 0, 1, \ldots, q-1)$$

for some roots of unity $\xi_k \in K_m$. Assuming that $\xi_k \neq \xi_0$, we find, eliminating $\bar{\alpha}$,

$$\alpha = (1 - \zeta_q^{-k} + \xi_k\zeta_q^k - \xi_0)/(\xi_k - \xi_0) \quad (k = 1, 2, \ldots, q-1;\ \xi_k \neq \xi_0). \tag{4}$$

Therefore

$$(\xi_k - \xi_0)^q\beta \equiv (1 - \zeta_q^{-k} + \xi_k\zeta_q^k - \xi_0)^q - (\xi_k - \xi_0)^q \equiv 0 \bmod q.$$

This is possible only if $\xi_k\xi_0^{-1} = \zeta_q^{t_k}$ for some $t_k \not\equiv 0 \bmod q$. Then (4) implies

$$\alpha\xi_0(\zeta_q^{t_k} - 1) = 1 - \zeta_q^{-k} + \xi_0(\zeta_q^{k+t_k} - 1) \quad (k = 1, 2, \ldots, q-1;\ \xi_k \neq \xi_0). \tag{5}$$

Divide (5) by $1 - \zeta_q$ and consider the resulting equation mod $1 - \zeta_q$. We conclude that $\alpha\xi_0 t_k \equiv k + \xi_0(k + t_k) \bmod 1 - \zeta_q$ or

$$t_k \equiv (1 + \xi_0^{-1})(\alpha - 1)^{-1}k \bmod 1 - \zeta_q. \tag{6}$$

Since $\xi_k = \xi_0$ for at most one k with $1 \leqslant k \leqslant q-1$, the congruence (6) holds for some k, whence $(1 + \xi_0^{-1})(\alpha - 1)^{-1} \equiv d \bmod 1 - \zeta_q$ for some rational integer d ($1 \leqslant d \leqslant q-1$). Thus

$$t_k \equiv dk \bmod q. \tag{7}$$

We can now also see that $\xi_k = \xi_0$ cannot, in fact, hold for $k \neq 0$, because in this case $\xi_0 = -\zeta_q^{-k}$, and we would have $d \equiv 0 \bmod 1 - \zeta_q$.

Consider the polynomial

$$P(x) = \xi_0 x^{d+2} - \alpha\xi_0 x^{d+1} + (\alpha\xi_0 - \xi_0 + 1)x - 1.$$

It follows from (5) and (7) that $x - \zeta_q^k \mid P(x)$ for $k = 1, 2, \ldots, q-1$. Clearly also $x - 1 \mid P(x)$. Hence $x^q - 1 \mid P(x)$. However, it is easily seen that this is not possible, because $\alpha \neq 0$ and α is not a root of unity. This concludes the proof.

References

[1] V. Ennola, *Proof of a conjecture of Morris Newman*, J. Reine Angew. Math. 264 (1973), pp. 203–206.

[2] — *Solution of a cyclotomic diophantine equation*, J. Reine Angew. Math. 272 (1975), pp. 73–91.

[3] J. H. Loxton, *On a cyclotomic diophantine equation*, J. Reine Angew. Math. 270 (1974), pp. 164–168.

[4] M. Newman, *Units in cyclotomic number fields*, J. Reine Angew. Math. 250 (1971), pp. 3–11.

[5] — *Diophantine equations in cyclotomic fields*, J. Reine Angew. Math. 265 (1974), pp. 84–89.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TURKU
Finland

Received on 28.3.1974 (549)