Upper bounds for cyclotomic numbers

Duc, Tai Do; Leung, Ka Hin; Schmidt, Bernhard

2020

Duc, T. D., Leung, K. H., & Schmidt, B. (2020). Upper bounds for cyclotomic numbers.
Algebraic Combinatorics, 3(1), 39-53. doi:10.5802/alco.86

https://hdl.handle.net/10356/145013

https://doi.org/10.5802/alco.86

ALGEBRAIC
COMBINATORICS

Tai Do Duc, Ka Hin Leung & Bernhard Schmidt

Upper Bounds for Cyclotomic Numbers

Volume 3, issue 1 (2020), p. 39-53.

<http://alco.centre-mersenne.org/item/ALCO_2020__3_1_39_0>

Algebraic Combinatorics
Volume 3, issue 1 (2020), p. 39–53
https://doi.org/10.5802/alco.86

Upper Bounds for Cyclotomic Numbers

Tai Do Duc, Ka Hin Leung & Bernhard Schmidt

Abstract Let q be a power of a prime p, let k be a nontrivial divisor of $q-1$ and write $e=(q-1)/k$. We study upper bounds for cyclotomic numbers (a,b) of order e over the finite field $\mathbb{F}_q$. A general result of our study is that $(a,b) \leqslant 3$ for all $a,b \in \mathbb{Z}$ if $p > (\sqrt{14})^{k/\mathrm{ord}_k(p)}$. More conclusive results will be obtained through separate investigation of the five types of cyclotomic numbers: $(0,0),(0,a),(a,0),(a,a)$ and (a,b), where $a \neq b$ and $a,b \in \{1,\dots,e-1\}$. The main idea we use is to transform equations over $\mathbb{F}_q$ into equations over the field of complex numbers on which we have more information. A major tool for the improvements we obtain over known results is new upper bounds on the norm of cyclotomic integers.

1. Introduction and Definitions

First, we fix some notation and definitions. By q we denote a power of a prime p. Let e and k be nontrivial divisors of $q-1$ such that $q=ek+1$. Let g denote a primitive element of the finite field $\mathbb{F}_q$. For each $a \in \mathbb{Z}$, write

$$C_a = \{g^a, g^{a+e}, \dots, g^{a+(k-1)e}\}. \tag{1}$$

As $C_a = C_{a+e}$, we only need to consider the sets C_a with $a \in \{0,1,\dots,e-1\}$.

Definition 1.1. *For $a,b \in \{0,1,\dots,e-1\}$, define (a,b) as the number of solutions to the equation*

$$1+x=y,\ x \in C_a,\ y \in C_b.$$

Equivalently, this is the number of pairs (r,s) with $0 \leqslant r,s \leqslant k-1$ such that

$$1+g^{a+re} = g^{b+se}. \tag{2}$$

The number (a,b) is called a cyclotomic number *of order e.*

Cyclotomic numbers have been studied for decades by many authors, as they have applications in various areas. These numbers can be used to compute Jacobi sums, and vice versa, see [12]. Vandiver [10, 15, 16, 17, 18] related cyclotomic numbers to Fermat's Last Theorem and proved the theorem for exponents $\leqslant 2000$. Cyclotomic classes C_a were used by Paley [11] in 1993 to construct difference sets. This approach was later employed by many other authors. Storer's book [14] summarizes the results in this direction up to 1967. In the 1960s to 1980s, Baumert [1], Evans [6], Lehmer [9],

Manuscript received 5th February 2019, revised 26th April 2019, accepted 8th May 2019.

Keywords. Finite fields, Cylotomic Fields, Norm Bounds.

Acknowledgements. Research is supported by grants R-146-000-276-114 and RG27/18 (S), Ministry of Education, Singapore.

ISSN: 2589-5486 http://algebraic-combinatorics.org/

Whiteman [19, 20, 21], et al. explicitly determined all numbers (a,b) of orders $e \leqslant 12$ and $e = 14, 15, 16, 18, 20, 24$. See [2, p. 152] for more details.

Under asymptotic conditions, cyclotomic numbers exhibit an interesting uniform behaviour. Katre [7] proved that, for fixed e and $q \to \infty$, we have $(a,b) \approx q/e^2$ for all $a, b \in \mathbb{Z}$. On the other hand, fixing k, it was proved by Betsumiya et al. [3] that $(0,0) \leqslant 2$ if p is sufficiently large compared to k. In [3], the condition "sufficiently large" is not explicitly specified and, in fact, the lower bound on p required for their method is difficult to write down explicitly. The goal of our paper is to find a simple and improved lower bound on p which guarantees that all numbers (a,b) are small. The following is our main result.

Theorem 1.2. *Let q be a power of a prime p. Let e and k be nontrivial divisors of $q-1$ such that $q = ek+1$. If*

$$p > \left(\sqrt{14}\right)^{k/\operatorname{ord}_k(p)},$$

then $(a,b) \leqslant 3$ for all $a, b \in \mathbb{Z}$.

If k is a prime, we obtain a better bound as follows.

Theorem 1.3. *Let q be a power of a prime p. Let e and k be nontrivial divisors of $q-1$ such that k is a prime and $q = ek+1$. If*

$$p > (3^{k-1}k)^{1/\operatorname{ord}_k(p)},$$

then

$$(a,b) \leqslant 2 \quad \textit{for all} \quad a, b \in \mathbb{Z}.$$

We continue with introducing some notation and results we need later. For a positive integer k, let ζ_k denote a complex primitive kth root of unity. A square matrix is called *circulant* if each of its rows (except the first) is obtained from the previous row by shifting the entries one position to the right and moving the last entry to the front. Moreover, given a matrix H, we denote the conjugate transpose of H by H^*. The following result about eigenvalues and eigenvectors of a circulant matrix is well known, see [5], for example.

Remark 1.4. Let k be a positive integer and let M be a circulant matrix with the first row $(a_0, \dots, a_{k-1})$ where $a_0, \dots, a_{k-1} \in \mathbb{C}$. Then the eigenvalues and eigenvectors of M are

$$\lambda_i = \sum_{j=0}^{k-1} a_j \zeta_k^{ij}, \ X_i = (1, \zeta_k^i, \dots, \zeta_k^{i(k-1)})^T \text{ for } 0 \leqslant i \leqslant k-1.$$

In the next section, we review some results on vanishing sums of roots of unity which will be needed for our study. The following terminology was used in [4]. Let T be a finite set of complex roots of unity and let c_α, $\alpha \in T$, be nonzero rational numbers. The sum

$$S = \sum_{\alpha \in T} c_\alpha \alpha, \ c_\alpha \in \mathbb{Q} \smallsetminus \{0\},$$

is called a *vanishing sum* of roots of unity if $S = 0$. We say that S is *nonempty* if $T \neq \varnothing$. The *length* $l(S)$ is the cardinality of T. The *exponent* $e(S)$ denotes the least common multiple of all orders of the roots of unity $\alpha \in T$. We say that S is *similar* to any sum of the form $k \cdot \beta S'$, where $k \in \mathbb{Q} \smallsetminus \{0\}$ and β is a root of unity and S' has the form

$$S' = \sum_{\alpha \in T} (\varepsilon_\alpha c_\alpha)(\varepsilon_\alpha \alpha), \text{ where } \varepsilon_\alpha \in \{1, -1\}.$$

We call the vanishing sum S *minimal* if S contains no vanishing subsum. The sum S is a *reduced sum* if $\alpha = 1$ for some $\alpha \in T$.

2. Vanishing Sums of Roots of Unity

The following result states that a minimal vanishing sum of roots of unity is similar to a vanishing sum whose order is squarefree, see [8, Corollary 3.2] or [4, Theorem 1] for a proof.

Remark 2.1. If $S=\alpha_1+\cdots+\alpha_n$ is a minimal vanishing sum of mth roots of unity, then after multiplying S by a suitable mth root of unity, we may assume that all α_i's are m_0th roots of unity, where m_0 is the largest square-free divisor of m.

The next result is part of [4, Theorem 6] and will be useful for our study.

Remark 2.2. Let S be a nonempty vanishing sum of length at most 6 that does not contain subsums similar to $1+(-1)$ or $1+\zeta_3+\zeta_3^2$. Then S is similar to one of the sums

$$\begin{gathered}1+\zeta_5+\zeta_5^2+\zeta_5^3+\zeta_5^4,\\ -\zeta_3-\zeta_3^2+\zeta_5+\zeta_5^2+\zeta_5^3+\zeta_5^4.\end{gathered}$$

3. Bounds on Norms of Cyclotomic Integers

A *cyclotomic integer* (not to be confused with a cyclotomic number) is an algebraic integer in a cyclotomic field. Every cyclotomic integer can be written as a sum of complex roots of unity. The improvements over the previously known results we obtain arise from new bounds on absolute norms of cyclotomic integers. First, we discuss a general norm bound.

Note that every cyclotomic integer in $\mathbb{Q}(\zeta_k)$ can be written as $f(\zeta_k)$, where $f(x)=\sum_{i=0}^{k-1}a_ix^i$ is a polynomial with integer coefficients. Since $|f(\zeta_k^j)|\leqslant\sum_{i=0}^{k-1}|a_i|$, an obvious bound for the absolute norm of $f(\zeta_k)$ is

$$|N(f(\zeta_k))|=\left|\prod_{j:\gcd(j,k)=1}f(\zeta_k^j)\right|\leqslant\left(\sum_{i=0}^{k-1}|a_i|\right)^{\varphi(k)}. \tag{3}$$

In this section, we provide some stronger bounds that are suitable for the applications to cyclotomic numbers we are interested in.

Theorem 3.1. *Let k be a positive integer, let $f(x)=\sum_{i=0}^{k-1}a_ix^i\in\mathbb{Z}[x]$ and let N denote the absolute norm of $\mathbb{Q}(\zeta_k)$. Then*

$$|N(f(\zeta_k))|\leqslant\left(\frac{k}{\varphi(k)}\sum_{i=0}^{k-1}a_i^2\right)^{\varphi(k)/2}. \tag{4}$$

In particular, if $\sum_{i=0}^{k-1}a_i^2\geqslant 3$, then

$$|N(f(\zeta_k))|\leqslant\left(\sum_{i=0}^{k-1}a_i^2\right)^{k/2}. \tag{5}$$

Proof. We have

$$\sum_{h=0}^{k-1}|f(\zeta_k^h)|^2=\sum_{i,j,h=0}^{k-1}a_ia_j\zeta_k^{(i-j)h}=k\sum_{i=0}^{k-1}a_i^2.$$

By the inequality between arithmetic and geometric means, we have

$$|N(f(\zeta_k))|=|\prod_{(h,k)=1}f(\zeta_k^h)|\leqslant\left(\frac{\sum_{(h,k)=1}|f(\zeta_k^h)|^2}{\varphi(k)}\right)^{\varphi(k)/2}\leqslant\left(\frac{k}{\varphi(k)}\sum_{i=0}^{k-1}a_i^2\right)^{\varphi(k)/2},$$

which proves (4).

Now assume that $S=\sum_{i=0}^{k-1} a_i^2 \geqslant 3$. Consider function $g(x)=(kS/x)^{x/2}$ on interval $[1,k]$. We have $g'(x)=(kS/x)^{x/2}\left(\ln(kS/x)/2-1/2\right)>0$ for $x\in[1,k]$, so $g(x)$ is increasing on $[1,k]$. We obtain

$$|N(f(\zeta_k))| \leqslant g(\varphi(k)) \leqslant g(k)=S^{k/2}. \qquad \square$$

In the case k is a prime, we obtain a different bound on the norm of $f(\zeta_k)$ in the next theorem. This bound is better than (4) in certain situations.

For the rest of this section, we assume that k is a prime. For $f(x)=\sum_{i=0}^{k-1} a_i x^i$, let M denote the circulant matrix with first row $(a_0,\dots,a_{k-1})$ and let N denote the $(k-1)\times(k-1)$ matrix obtained from M by deleting its first row and its first column. To find an upper bound for $|N(f(\zeta_k))|$, we first find a relation between $N(f(\zeta_k))$ and $\det(M)$ or $\det(N)$. Then an upper bound for $|\det(M)|$ or $|\det(N)|$ will give us an upper bound for $|N(f(\zeta_k))|$.

Bounds for the determinant of a matrix are abundant in the literature. We only need the following result by Schinzel [13].

Remark 3.2. Let $N=(a_{ij})_{i,j=0}^{n-1}$ be an $n\times n$ matrix with real entries. For $i=0,1,\dots,n-1$, write $N_i^+=\sum_{j=0}^{n-1}\max\{0,a_{ij}\}$ and $N_i^-=\sum_{j=0}^{n-1}\max\{0,-a_{ij}\}$. We have

$$|\det(N)| \leqslant \prod_{i=0}^{n-1}\max\{N_i^+,N_i^-\}. \tag{6}$$

Proposition 3.3. *Using the notation introduced above, we have the following*

(a) *If* $\sum_{i=0}^{k-1} a_i \neq 0$, *then*

$$N(f(\zeta_k))=\frac{\det(M)}{\sum_{i=0}^{k-1} a_i}. \tag{7}$$

(b) *If* $\sum_{i=0}^{k-1} a_i = 0$, *then*

$$N(f(\zeta_k))=k\det(N). \tag{8}$$

Proof. For each $0\leqslant i\leqslant k-1$, define a column vector

$$X_i=\frac{1}{\sqrt{k}}(1,\zeta_k^i,\zeta_k^{2i},\dots,\zeta_k^{(k-1)i})^T.$$

By Result 1.4, the eigenvalues of M are $\lambda_i=f(\zeta_k^i)$ and the corresponding eigenvectors are X_i, $0\leqslant i\leqslant k-1$. Since k is a prime, we have

$$N(f(\zeta_k))=\prod_{i=1}^{k-1} f(\zeta_k^i)=\prod_{i=1}^{k-1}\lambda_i. \tag{9}$$

Note that $\det(M)=\prod_{i=0}^{k-1}\lambda_i$. If $\lambda_0=\sum_{i=0}^{k-1} a_i\neq 0$, then (7) is clear.

Suppose that $\lambda_0=0$. Note that $X_i^*X_j=1$ if $i=j$ and $X_i^*X_j=0$ if $i\neq j$. Let Q be the $k\times k$ matrix with columns $X_0,\dots,X_{k-1}$, then Q^{-1} is the $k\times k$ matrix with rows $X_0^*,\dots,X_{k-1}^*$. We have

$$M=Q\begin{pmatrix}\lambda_0 & & & \\ & \lambda_1 & & \\ & & \ddots & \\ & & & \lambda_{k-1}\end{pmatrix}Q^{-1}.$$

By the definition of N, we have

$$N = Q_1 \begin{pmatrix} \lambda_0 & & & \\ & \lambda_1 & & \\ & & \ddots & \\ & & & \lambda_{k-1} \end{pmatrix} Q_1^{'},$$

where Q_1 is the $(k-1) \times k$ matrix formed by the last $k-1$ rows of Q and $Q_1^{'}$ is the $k \times (k-1)$ matrix formed by the last $k-1$ columns of Q^{-1}. Since $\lambda_0 = 0$, we have

$$N = Q_2 \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_{k-1} \end{pmatrix} Q_2^{'},$$

where Q_2 is the $(k-1) \times (k-1)$ matrix formed by the last $k-1$ columns of Q_1 and ${Q_2}'$ is the matrix formed by the last $k-1$ rows of Q_1'. We obtain

$$\det(N) = \det(Q_2 Q_2^{'}) \prod_{i=1}^{k-1} \lambda_i.$$

By (9), the equation (8) is equivalent to $\det(Q_2 Q_2^{'}) = 1/k$. Note that $(Q_2^{'})_{ij} = \overline{(Q_2)}_{ij}$ for any i, j, as Q_2 and $Q_2^{'}$ are submatrices of Q and Q^{-1}, respectively. More precisely, we have

$$Q_2 = \frac{1}{\sqrt{k}} \begin{pmatrix} \zeta_k & \zeta_k^2 & \cdots & \zeta_k^{k-1} \\ \zeta_k^2 & \zeta_k^4 & \cdots & \zeta_k^{2(k-1)} \\ & & \ddots & \\ \zeta_k^{k-1} & \zeta_k^{2(k-1)} & \cdots & \zeta_k^{(k-1)(k-1)} \end{pmatrix}.$$

The (i, j)th entry of $Q_2 Q_2^{'}$ is

$$\frac{1}{k} \sum_{t=1}^{k-1} \zeta_k^{(i-j)t} = \begin{cases} (k-1)/k & \text{if } i = j, \\ -1/k & \text{if } i \neq j. \end{cases}$$

Hence $Q_2 Q_2^{'}$ is a circulant matrix of size $(k-1) \times (k-1)$ with the first row is $((k-1)/k, -1/k, \ldots, -1/k)$. By Result 1.4, the eigenvalues of $Q_2 Q_2^{'}$ are

$$\beta_j = \frac{1}{k} \left(k - 1 - \sum_{i=1}^{k-2} \zeta_{k-1}^{ij} \right) = \begin{cases} 1/k & \text{if } \ j = 0, \\ 1 & \text{if } \ 1 \leqslant j \leqslant k-2. \end{cases}$$

We obtain

$$\det(Q_2 Q_2^{'}) = \prod_{j=0}^{k-2} \beta_j = 1/k. \qquad \square$$

Combining Result 3.2 and Proposition 3.3, we get the following norm bound, which in numerous cases is stronger than Theorem 3.1.

Corollary 3.4. *Let k be a prime and let $f(x) = \sum_{i=0}^{k-1} a_i x^i \in \mathbb{Z}[x]$. Write $A^+ = \sum_{j=0}^{n-1} \max\{0, a_j\}$, $A^- = \sum_{j=0}^{n-1} \max\{0, a_j\}$, and $A = \max\{A^+, A^-\}$.*

(a) *If $\sum_{i=0}^{k-1} a_i \neq 0$, then*

$$|N(f(\zeta_k))| \leqslant \frac{A^k}{|\sum_{i=0}^{k-1} a_i|}.$$

(b) *If* $\sum_{i=0}^{k-1} a_i = 0$, *then*

$$|N(f(\zeta_k))| \leqslant kA^{k-1}.$$

4. Equations over $\mathbb{F}_q$ and $\mathbb{C}$

The following theorem shows that under some condition on the characteristic of the finite field $\mathbb{F}_q$, we can transform certain equations over $\mathbb{F}_q$ to equations over the field of complex numbers $\mathbb{C}$, and vice versa.

Theorem 4.1. *Let q be a power of a prime p and let e, k be nontrivial divisors of $q-1$ such that $q = ek+1$. Let g be a primitive element of $\mathbb{F}_q$ and let $f(x) = \sum_{i=0}^{k-1} a_i x^i \in \mathbb{Z}[x]$. Suppose that*

$$p > \left(\frac{k}{\varphi(k)} \sum_{i=0}^{k-1} a_i^2\right)^{\frac{\varphi(k)}{2\mathrm{ord}_k(p)}}, \tag{10}$$

then $f(g^e) = 0$ over $\mathbb{F}_q$ if and only if $f(\zeta_k) = 0$ over $\mathbb{C}$.

In particular, the same conclusion holds if $\sum_{i=0}^{k-1} a_i^2 \geqslant 3$ and

$$p > \left(\sum_{i=0}^{k-1} a_i^2\right)^{\frac{k}{2\,\mathrm{ord}_k(p)}}. \tag{11}$$

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\zeta_k]$ that contains p. Write $q = p^n$ and $b = \mathrm{ord}_k(p)$. Note that b divides n because $q = p^n \equiv 1 \pmod{k}$. Since $\mathbb{Z}[\zeta_k]/\mathfrak{p}$ is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$ of order b, we have $\mathbb{Z}[\zeta_k]/\mathfrak{p} \cong \mathbb{F}_{p^b}$. Let $\phi : \mathbb{F}_{p^b} \to \mathbb{Z}[\zeta_k]/\mathfrak{p}$ be an isomorphism. Note that g^e is a primitive kth root of unity in $\mathbb{F}_{p^b}$, so $\phi(g^e)$ is also a primitive kth root of unity in $\mathbb{Z}[\zeta_k]/\mathfrak{p}$, which implies $\phi(g^e) = \zeta_k^j + \mathfrak{p}$ for some integer j coprime to k. We have

$$f(g^e) = 0 \text{ over } \mathbb{F}_q \Leftrightarrow \phi(f(g^e)) = f(\zeta_k^j) + \mathfrak{p} = 0 \text{ in } \mathbb{Z}[\zeta_k]/\mathfrak{p} \Leftrightarrow f(\zeta_k^j) \in \mathfrak{p}. \tag{12}$$

Suppose that $f(\zeta_k) = 0$ over $\mathbb{C}$. We have $f(\zeta_k^j) = 0$, as j is coprime to k. By (12), $f(g^e) = 0$ over $\mathbb{F}_q$. Now assume that $f(g^e) = 0$ over $\mathbb{F}_q$. Note that $N(\mathfrak{p}) = p^b$, where by $N(\mathfrak{p})$ we mean the norm of the ideal $\mathfrak{p}$ in $\mathbb{Z}[\zeta_k]$. By (12), we have $N(f(\zeta_k^j)) \equiv 0 \pmod{p^b}$. As j is coprime to k, we have $N(f(\zeta_k^j)) = N(f(\zeta_k))$. Thus

$$N(f(\zeta_k)) \equiv 0 \pmod{p^b}. \tag{13}$$

On the other hand, by Theorem 3.1 we have

$$|N(f(\zeta_k))| \leqslant \left(\frac{k}{\varphi(k)} \sum_{i=0}^{k-1} a_i^2\right)^{\varphi(k)/2}. \tag{14}$$

If $f(\zeta_k) \neq 0$, then $N(f(\zeta_k)) \neq 0$ and (13), (14) imply

$$p^b \leqslant \left(\frac{k}{\varphi(k)} \sum_{i=0}^{k-1} a_i^2\right)^{\varphi(k)/2},$$

contradicting (10). Therefore, $f(\zeta_k) = 0$.

Lastly, the conclusion for the case $\sum_{i=0}^{k-1} a_i^2 \geqslant 3$ follows from (5). □

The next theorem follows from Corollary 3.4 in the same way as Theorem 4.1 follows from Theorem 3.1, so we skip the proof.

Theorem 4.2. *Let q be a power of a prime p and let e, k be nontrivial divisors of $q-1$ such that $q = ek+1$ and k is a prime. Let g be a primitive element of $\mathbb{F}_q$ and let $f(x) = \sum_{i=0}^{k-1} a_i x^i \in \mathbb{Z}[x]$. Write $A^+ = \sum_{j=0}^{n-1} \max\{0, a_j\}$, $A^- = \sum_{j=0}^{n-1} \max\{0, a_j\}$, and $A = \max\{A^+, A^-\}$. Suppose that one of the following conditions holds.*

(a) $\sum_{i=0}^{k-1} a_i \neq 0$ *and*

$$p^{\operatorname{ord}_k(p)} > \frac{A^k}{|\sum_{i=0}^{k-1} a_i|}. \tag{15}$$

(b) $\sum_{i=0}^{k-1} a_i = 0$ *and*

$$p^{\operatorname{ord}_k(p)} > kA^{k-1}. \tag{16}$$

Then we have $f(g^e) = 0$ over $\mathbb{F}_q$ if and only if $f(\zeta_k) = 0$ over $\mathbb{C}$.

5. Upper Bounds for Cyclotomic Numbers

In this section, we apply Theorem 4.1 to derive upper bounds for cyclotomic numbers (a, b). In Theorem 3.1, the upper bound $(k/\varphi(k) \sum a_i^2)^{\varphi(k)/2}$ is largest when $\varphi(k)$ is approximately k. Thus, in this case, and in particular when k is a prime, an improved bound is desirable. Theorem 4.2 will come into play in this situation and we will discuss this case separately in the last section.

Note that $(a, b) = (a', b')$ whenever $a \equiv a' \pmod{e}$ and $b \equiv b' \pmod{e}$. From now on, we always assume that $a, b \in \{0, 1, \ldots, e-1\}$. We are now going to prove Theorem 1.2. Our proof is divided into five cases: We separately investigate cyclotomic numbers $(0,0), (0,a), (a,0), (a,a)$ and (a,b) where $a \neq b$ and $a, b \in \{1, \ldots, e-1\}$. In fact, in each case, we obtain a stronger result than Theorem 1.2, which is just a simplified consequence of the analysis of the different cases.

Theorem 5.1. *If*

$$p > \left(\frac{3k}{\varphi(k)}\right)^{\frac{\varphi(k)}{2\operatorname{ord}_k(p)}}, \tag{17}$$

then

$$(0,0) = \begin{cases} 0 \text{ if } k \not\equiv 0 \pmod{6} \text{ and } 2 \notin C_0, \\ 1 \text{ if } k \not\equiv 0 \pmod{6} \text{ and } 2 \in C_0, \\ 2 \text{ if } k \equiv 0 \pmod{6} \text{ and } 2 \notin C_0, \\ 3 \text{ if } k \equiv 0 \pmod{6} \text{ and } 2 \in C_0. \end{cases} \tag{18}$$

Proof. Suppose that there are $0 \leqslant a, b \leqslant k-1$ with $1 + g^{ae} = g^{be}$. Then $2 \in C_0$ if $a = 0$. Thus in the case $2 \in C_0$, there is one solution to $1 + g^{ae} = g^{be}$ in which $a = 0$.

From now on, suppose that $a \neq 0$ and $1 + g^{ae} = g^{be}$. We have $b \notin \{0, a\}$ and $f(x) = 1 + x^a - x^b$ is a polynomial of degree at most $k-1$ with two coefficients 1, one coefficient -1 and all other coefficients 0. Write $f(x) = \sum_{i=0}^{k-1} a_i x^i$, then $\sum_{i=0}^{k-1} a_i^2 = 3$ and $f(g^e) = 0$. By (17) and Theorem 4.1, we have

$$f(\zeta_k) = 1 + \zeta_k^a - \zeta_k^b = 0.$$

By Result 2.2, we obtain $1 + \zeta_k^a - \zeta_k^b = 1 + \zeta_3 + \zeta_3^2$, which happens only when $6 \mid k$ and $(a,b) \in \{(k/3, k/6), (2k/3, 5k/6)\}$, proving (18). □

Note that by (11), Theorem 5.1 still holds when (17) is replaced by $p > 3^{k/(2\operatorname{ord}_k(p))}$. This shows that Theorem 1.2 holds in the case $(a,b) = (0,0)$.

We mentioned in the introduction that Vandiver has used cyclotomic numbers to obtain results on Fermat's Last Theorem. The next Corollary gives an example for this kind of argument. Considering the Diophantine equation $x^e + y^e = z^e$ modulo p, Theorem 5.1 implies the following.

Corollary 5.2. *If p is a prime with $p = ek + 1 > 3^{k/2}$, then $x^e + y^e = z^e$ with $x, y, z \in \mathbb{Z}$, implies either 2 is an eth power modulo p or $xyz \equiv 0 \pmod{p}$.*

For example, let $p = 1301 = 100 \cdot 13 + 1$ and let $e = 100, k = 13$. Note that 2 is not a 100th power modulo 1301. Therefore, if $x^{100} + y^{100} \equiv z^{100} \pmod{1301}$, then $xyz \equiv 0 \pmod{1301}$.

Theorem 5.3. *Let $a \in \{1, \dots, e-1\}$. If*

$$p > \left(\frac{4k}{\varphi(k)}\right)^{\frac{\varphi(k)}{2\operatorname{ord}_k(p)}}, \tag{19}$$

then

$$(0, a) \leqslant \begin{cases} 3 \text{ if } 2 \in C_a, \\ 2 \text{ if } 2 \notin C_a. \end{cases} \tag{20}$$

Proof. Note that $1 + g^{ie} = g^{je+a}$ implies $1 + g^{-ie} = g^{(j-i)e+a}$, so each solution (i, j) to $1 + g^{ie} = g^{je+a}$ induces a solution $(-i, j - i)$ (calculation is modulo k) to the same equation, two of which are different if and only if $i \neq 0$. Moreover if $i = 0$, then $2 = g^{je+a} \in C_a$ and there is one solution to $1 + g^{ie} = g^{je+a}$ in which $i = 0$.

Suppose that $2 \in C_a$ and $(0, a) \geqslant 4$. There are two different pairs $(i_1, j_1), (i_2, j_2)$ with

$$i_1 \neq 0,\ i_2 \neq 0,\ (i_2, j_2) \neq (-i_1, j_1 - i_1) \text{ and } (i_1, j_1) \neq (-i_2, j_2 - i_2) \tag{21}$$

such that $1 + g^{i_1 e} = g^{j_1 e+a}$ and $1 + g^{i_2 e} = g^{j_2 e+a}$. We obtain

$$1 + g^{i_1 e} - g^{(j_1 - j_2)e} - g^{(j_1 - j_2 + i_2)e} = 0. \tag{22}$$

In (22), the numbers $0, i_1, j_1 - j_2$ and $j_1 - j_2 + i_2$ are pairwise different. Indeed, by (21), we need only to show that $i_1 \neq j_1 - j_2 + i_2$. If $i_1 - i_2 = j_1 - j_2$, then by subtracting two equations $1 + g^{i_1 e} = g^{j_1 e+a}$ and $1 + g^{i_2 e} = g^{j_2 e+a}$, we obtain $g^{i_2 e} = g^{j_2 e+a}$, a contradiction as $C_0 \cap C_a = \varnothing$.

By (19) and Theorem 4.1, the equation (22) implies

$$1 + \zeta_k^{i_1} - \zeta_k^{j_1 - j_2} - \zeta_k^{j_1 - j_2 + i_2} = 0.$$

By Result 2.2, this is possible only when the sum on left-hand side cancels in pairs. This happens only when "$2 \mid k$ and $i_1 = i_2 = k/2$" or "$j_1 = j_2$ and $i_1 = i_2$", both of which are not possible. Therefore, we obtain $(0, a) \leqslant 3$ if $2 \in C_a$.

Next, suppose that $2 \notin C_a$ and $(0, a) \geqslant 3$. Note that for any $0 \leqslant i, j \leqslant k - 1$ with $1 + g^{ie} = g^{je+a}$, we have $i \neq 0$. There exist two pairs (i_1, j_1) and (i_2, j_2) with

$$i_1 \neq 0,\ i_2 \neq 0,\ (i_2, j_2) \neq (-i_1, j_1 - i_1) \text{ and } (i_1, j_1) \neq (-i_2, j_2 - i_2)$$

such that $1 + g^{i_1 e} = g^{j_1 e+a}$ and $1 + g^{i_2 e} = g^{j_2 e+a}$. We obtain a contradiction by the same argument as in the previous case. □

Theorem 5.4. *Let $a \in \{1, \dots, e-1\}$. If*

$$p > \left(\frac{4k}{\varphi(k)}\right)^{\frac{\varphi(k)}{2\operatorname{ord}_k(p)}}, \tag{23}$$

then

$$(a, 0) \leqslant \begin{cases} 3 \text{ if } 2 \in C_a \text{ and } 2 \mid k, \\ 2 \text{ if } 2 \notin C_a \text{ and } 2 \mid k, \\ 2 \text{ if } 2 \nmid k. \end{cases} \tag{24}$$

Proof. First, assume that k is even. If $1+g^{ie+a}=g^{je}$, then $1+g^{(k/2+j)e}=g^{(k/2+i)e+a}$, as $g^{ek/2}=-1$. This implies $(a,0)=(0,a)$ and the conclusion follows from Theorem 5.3.

From now on, we assume that k is odd and $(a,0)\geqslant 3$. For $t=1,2,3$, let (i_t,j_t) be three different pairs with $0\leqslant i_t,j_t\leqslant k-1$ and $1+g^{i_te+a}=g^{j_te}$ for $t=1,2,3$. First, note that $j_t\neq 0$ for all t because $0\notin C_a$. Moreover, we obtain the following two equations which result from $1+g^{i_te+a}=g^{j_te}$ for $t=1,2,3$

$$1-g^{j_1e}-g^{(i_1-i_2)e}+g^{(i_1-i_2+j_2)e}=0,\ \text{and} \tag{25}$$

$$1-g^{j_1e}-g^{(i_1-i_3)e}+g^{(i_1-i_3+j_3)e}=0. \tag{26}$$

Suppose that there are four distinct terms in one of the equations above, assume that is (25). By (23) and Theorem 4.1, we have

$$1-\zeta_k^{j_1}-\zeta_k^{i_1-i_2}+\zeta_k^{i_1-i_2+j_2}=0.$$

By Result 2.2, the left-hand-side sum cancels in pairs, which is impossible because k is odd and all terms in the sum are distinct. Thus, we cannot have all four terms different in both (25) and (26). In (25), we have either $i_1-i_2=j_1$ or $i_1-i_2+j_2=0$. In (26), we have either $i_1-i_3=j_1$ or $i_1-i_3+j_3=0$. Due to the difference between three pairs (i_t,j_t), $t=1,2,3$, we can only have two cases: $i_1-i_2=j_1$ and $i_1-i_3+j_3=0$, or $i_1-i_2+j_2=0$ and $i_1-i_3=0$. The following argument works the same for both cases. Assuming that the first case happens, we have, by (25) and (26),

$$1-2g^{j_1e}+g^{(j_1+j_2)e}=0 \text{ and } 2-g^{j_1e}-g^{-j_3e}=0,$$

or equivalently

$$2-g^{-j_1e}-g^{j_2e}=0 \text{ and } 2-g^{j_1e}-g^{-j_3e}=0. \tag{27}$$

Hence $g^{-j_1e}+g^{j_2e}-g^{j_1e}-g^{-j_3e}=0$, which implies

$$1+g^{(j_1+j_2)e}-g^{2j_1e}-g^{(j_1-j_3)e}=0. \tag{28}$$

We claim that the numbers $0,j_1+j_2,2j_1,j_1-j_3$ are pairwise different. As j_1,j_2,j_3 are pairwise different, the claim is equivalent to $2j_1\neq 0$, $j_1+j_2\neq 0, j_2+j_3\neq 0$ and $j_1+j_3\neq 0$. Firstly, k odd and $j_1\neq 0$ implies $2j_1\neq 0$. Secondly, if $j_1+j_2=0$, then the first equation in (27) implies $2-2g^{-j_1e}=0$, so $j_1=0$ (note that $p>2$ by (23)), impossible. Thirdly, if $j_2+j_3=0$, then (28) implies $1-g^{2j_1e}=0$, so $j_1=0$. Lastly, if $j_1+j_3=0$, then the second equation in (27) implies $2-2g^{j_1e}=0$, so $j_1=0$, a contradiction. Now by (23) and Theorem 4.1, the equation (28) implies

$$1+\zeta_k^{(j_1-j_2)e}-\zeta_k^{2j_1}-\zeta_k^{(j_1-j_3)e}=0.$$

By Result 2.2, the left-hand-side sum cancels in pairs, impossible as k is odd and the terms $0,j_1-j_2,2j_1,j_1-j_3$ are pairwise different. □

Theorem 5.5. *Let $a\in\{1,\dots,e-1\}$. If*

$$p>\left(\frac{4k}{\varphi(k)}\right)^{\frac{\varphi(k)}{2\operatorname{ord}_k(p)}}, \tag{29}$$

then

$$(a,a)\leqslant\begin{cases}3 \text{ if } 2\in C_a \text{ and } 2\mid k,\\ 2 \text{ if } 2\notin C_a \text{ and } 2\mid k,\\ 2 \text{ if } 2\nmid k.\end{cases} \tag{30}$$

Proof. For each $0\leqslant i,j\leqslant k-1$ with $1+g^{ie+a}=g^{je+a}$, we have $1+g^{-ie-a}=g^{(j-i)e}$. Thus $(a,a)=(-a,0)$ and the conclusion follows directly from Theorem 5.4. □

Theorem 5.6. *Let $a \neq b \in \{1, \dots, e-1\}$. If*

$$p > \left(\frac{14k}{\varphi(k)}\right)^{\frac{\varphi(k)}{2\operatorname{ord}_k(p)}}, \tag{31}$$

then

$$(a, b) \leqslant 2.$$

This theorem is proved by contradiction. Let $(i_1, j_1), (i_2, j_2), (i_3, j_3)$ be three different pairs with $0 \leqslant i_t, j_t \leqslant k-1$ and $1 + g^{i_t e + a} = g^{j_t e + b}$ for $t = 1, 2, 3$. The following lemma states a simple relation between i_t's and j_t's which will be used repeatedly later.

Lemma 5.7. *Let $i_t, j_t, t = 1, 2, 3$, be defined as above, then the numbers $i_1 - j_1, i_2 - j_2, i_3 - j_3$ are pairwise different.*

Proof. Suppose that $i_1 - j_1 = i_2 - j_2$. We have $i_1 - i_2 = j_1 - j_2$. Subtracting two equations $1 + g^{i_1 e + a} = g^{j_1 e + b}$ and $1 + g^{i_2 e + a} = g^{j_2 e + b}$, we obtain

$$g^{i_2 e + a} = g^{j_2 e + b},$$

a contradiction as $C_a \cap C_b = \varnothing$. □

A major part in the proof of Theorem 5.6 is proving that the sum $\zeta_k^{i_1+j_2} + \zeta_k^{i_2+j_3} + \zeta_k^{i_3+j_1} - \zeta_k^{i_1+j_3} - \zeta_k^{i_2+j_1} - \zeta_k^{i_3+j_2}$, is nonzero, where $i_t, j_t, t = 1, 2, 3$, are given as above. We prove this result in the following proposition.

Proposition 5.8. *Let $i_t, j_t, t = 1, 2, 3$, be integers such that the i_t's are pairwise different modulo k, the j_t's are pairwise different modulo k and the $i_t - j_t$'s are pairwise different modulo k. Then the following sum is nonzero*

$$T = \zeta_k^{i_1+j_2} + \zeta_k^{i_2+j_3} + \zeta_k^{i_3+j_1} - \zeta_k^{i_1+j_3} - \zeta_k^{i_2+j_1} - \zeta_k^{i_3+j_2}.$$

Proof. Suppose that $T = 0$. Since T is a vanishing sum of roots of unity of length at most 6, Result 2.2 implies that T contains a subsum similar to $1 + (-1)$, or T contains two subsums each of which is similar to $1 + \zeta_3 + \zeta_3^2$, or T itself is similar to either $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4$ or $-\zeta_3 - \zeta_3^2 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4$.

Case 1. T contains a subsum similar to $1 + (-1)$.
Discarding the empty sum, the new T is a vanishing sum of 4 roots of unity. By Result 2.2 again, T cancels in pairs. Thus, the original sum T cancels in pairs. Note that none of the first three terms in T is canceled by any of the last three terms. Otherwise, let's say $\zeta_k^{i_1+j_2}$ is canceled by one of the last three terms. By the difference between the i_t's and j_t's, we can only have $i_1 + j_2 = i_2 + j_1$, which implies $i_1 - j_1 = i_2 - j_2$, contradicting Lemma 5.7. Thus, the first three terms of T cancel in pairs, impossible.

Case 2. T is similar to $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4$.
Note that by Case 1, the sets $\{i_1 + j_2, i_2 + j_3, i_3 + j_1\}$ and $\{i_1 + j_3, i_2 + j_1, i_3 + j_2\}$ are disjoint. As T has length 5, we can assume that the first two terms in T are the same, say $T = 2\zeta_k^{i_1+j_2} + \zeta_k^{i_3+j_1} - \zeta_k^{i_1+j_3} - \zeta_k^{i_2+j_1} - \zeta_k^{i_3+j_2}$. Hence, T is similar to the sum $2 + \zeta_k^{i_3+j_1-i_1-j_2} - \zeta_k^{j_3-j_2} - \zeta_k^{i_2+j_1-i_1-j_2} - \zeta_k^{i_3-i_1}$. It is impossible that this sum has the form $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4$.

Case 3. T contains two subsums each of which is similar to $1 + \zeta_3 + \zeta_3^2$.
Due to symmetry, we can consider two possibilities for these two subsums.

Subcase 1. The subsums are $\zeta_k^{i_1+j_2}+\zeta_k^{i_2+j_3}+\zeta_k^{i_3+j_1}$ and $\zeta_k^{i_1+j_3}+\zeta_k^{i_2+j_1}+\zeta_k^{i_3+j_2}$. We obtain $1+\zeta_k^{i_2+j_3-i_1-j_2}+\zeta_k^{i_3+j_1-i_1-j_2}=1+\zeta_k^{i_2+j_1-i_1-j_3}+\zeta_k^{i_3+j_2-i_1-j_3}$ and both sums have the form $1+\zeta_3+\zeta_3^2$. Thus $3\mid k$,

$$\{i_2+j_3-i_1-j_2, i_3+j_1-i_1-j_2\}=\{k/3,2k/3\}, \text{ and} \tag{32}$$

$$\{i_2+j_1-i_1-j_3, i_3+j_2-i_1-j_3\}=\{k/3,2k/3\}. \tag{33}$$

Since $k/3+2k/3=0$, we have $(i_2+j_3-i_1-j_2)+(i_3+j_1-i_1-j_2)=0$ and $(i_2+j_1-i_1-j_3)+(i_3+j_2-i_1-j_3)=0$, which implies

$$2(i_1+j_2)=(i_2+j_3)+(i_3+j_1) \tag{34}$$

and

$$2(i_1+j_3)=(i_2+j_1)+(i_3+j_2). \tag{35}$$

Subtracting (34) and (35), we obtain $j_2-j_3=k/3$. Now, the equation (32) gives $i_2-i_1=2k/3$ and the equation (33) gives $i_3-i_1=k/3$. We obtain $i_2-i_3=j_2-j_3=k/3$, so $i_2-j_2=i_3-j_3$, contradicting Lemma 5.7.

Subcase 2. The subsums are $\zeta_k^{i_1+j_2}+\zeta_k^{i_2+j_3}-\zeta_k^{i_2+j_1}$ and $\zeta_k^{i_3+j_1}-\zeta_k^{i_1+j_3}-\zeta_k^{i_3+j_2}$. We obtain $1+\zeta_k^{i_2+j_3-i_1-j_2}-\zeta_k^{i_2+j_1-i_1-j_2}=1+\zeta_k^{i_3+j_2-i_1-j_3}-\zeta_k^{i_3+j_1-i_1-j_3}$ and both sums are equal to $1+\zeta_3+\zeta_3^2$. Thus $6\mid k$ and the two sums $1+\zeta_k^{i_2+j_3-i_1-j_2}-\zeta_k^{i_2+j_1-i_1-j_2}$ and $1+\zeta_k^{i_3+j_2-i_1-j_3}-\zeta_k^{i_3+j_1-i_1-j_3}$ have form $1+\zeta_k^{k/3}-\zeta_k^{k/6}$ or $1+\zeta_k^{2k/3}-\zeta_k^{5k/6}$. If these two sums have the same form, then $i_2+j_1-i_1-j_2=i_3+j_1-i_1-j_3$, so $i_2-j_2=i_3-j_3$, contradicting Lemma 5.7. Thus, the two sums have different forms. Noting that $k/6+2k/3=5k/6$ and $5k/6+k/3=k/6$, we have

$$(i_2+j_1-i_1-j_2)+(i_3+j_2-i_1-j_3)=(i_3+j_1-i_1-j_3),$$

so $i_2=i_1$, a contradiction.

Case 4. T is similar to $-\zeta_3-\zeta_3^2+\zeta_5+\zeta_5^2+\zeta_5^3+\zeta_5^4$.
A reduced sum of this sum is

$$S'=1+\zeta_5+\zeta_5^2+\zeta_5^3-\zeta_3\zeta_5^{-1}-\zeta_3^2\zeta_5^{-1}.$$

Let S be the reduced sum obtained from T as follows

$$S=1+\zeta_k^{i_2+j_3-i_1-j_2}+\zeta_k^{i_3+j_1-i_1-j_2}-\zeta_k^{j_3-j_2}-\zeta_k^{i_2+j_1-i_1-j_2}-\zeta_k^{i_3-i_1}.$$

Dividing by a common divisor if necessary, we can assume that the greatest common divisor between k and all the exponents of ζ_k occurring in S is 1. This implies $e(S)=k$. In view of Result 2.1, we can assume that k is square-free. Since S and S' are similar reduced sums, we have $S=S'\zeta_{30}^t$ with $t\in\{0,1,11,12,18,24\}$ (the possible values of t are obtained from the fact that 1 appears in S). The 6 possibilities are

(i) $S'=1+\zeta_5+\zeta_5^2+\zeta_5^3-\zeta_{15}^2-\zeta_{15}^7$.
(ii) $S'\zeta_{30}=1+\zeta_3^2-\zeta_{15}^8-\zeta_{15}^{11}-\zeta_{15}^{14}-\zeta_{15}^2$.
(iii) $S'\zeta_{30}^{11}=1+\zeta_3-\zeta_{15}^{13}-\zeta_{15}-\zeta_{15}^4-\zeta_{15}^7$
(iv) $S'\zeta_{30}^{12}=1+\zeta_5^2+\zeta_5^3+\zeta_5^4-\zeta_{15}^8-\zeta_{15}^{13}$.
(v) $S'\zeta_{30}^{18}=1+\zeta_5+\zeta_5^3+\zeta_5^4-\zeta_{15}^{11}-\zeta_{15}$.
(vi) $S'\zeta_{30}^{24}=1+\zeta_5+\zeta_5^2+\zeta_5^4-\zeta_{15}^{14}-\zeta_{15}^4$.

Suppose that k is odd. We obtain $k=15$ and the sum S has the exact form as one of the 6 possibilities above, impossible as the sum of the coefficients in any of these possibilities is nonzero. Therefore, k is even. Note that $e(S'\zeta_{30}^t)=15$ in any case and we can write $\zeta_{30}=-\zeta_{15}^8$. So $k=30$. Multiplying all the terms in both sides of the equation $S=S'\zeta_{30}^t$, we obtain

$$\zeta_{30}^{2(i_2+i_3+j_1+j_3)-4(i_1+j_2)+15}=\zeta_{30}^{24+6t},$$

which implies $2(i_2+j_3+j_1+j_3)-4(i_1+j_2)-6t\equiv 9 \pmod{30}$, impossible. □

Proof of Theorem 5.6. Let $(i_1,j_1),(i_2,j_2),(i_3,j_3)$ be three different pairs so that $0\leqslant i_t,j_t\leqslant k-1$ and $1+g^{i_te+a}=g^{j_te+b}$ for $t=1,2,3$. We have

$$g^a(g^{i_1e}-g^{i_2e})=g^b(g^{j_1e}-g^{j_2e}),$$
$$g^b(g^{j_1e}-g^{j_3e})=g^a(g^{i_1e}-g^{i_3e}).$$

Multiplying these two equations, we obtain

$$g^{(i_1+j_2)e}+g^{(i_2+j_3)e}+g^{(i_3+j_1)e}-g^{(i_1+j_3)e}-g^{(j_2+j_1)e}-g^{(i_3+j_2)e}=0. \tag{36}$$

Write $f(x)=\sum_{i=0}^{k-1}a_ix^i$, where $f(g^e)$ is equal to the left-hand-side of (36). Each a_i is an integer in $[-3,3]$ and $\sum_{i=0}^{k-1}a_i=0$ and $\sum_{i=0}^{k-1}|a_i|\leqslant 6$. We claim that $\sum_{i=0}^{k-1}a_i^2\leqslant 14$. Note that $\sum_{i=0}^{k-1}a_i^2$ is largest when one term a_i^2 is largest possible and other terms a_j^2 are smallest possible. First, there are no $i\neq j$ with $|a_i|=|a_j|=3$. Otherwise, we have $g^{(i_1+j_2)e}=g^{(i_2+j_3)e}=g^{(i_3+j_1)e}$ and $g^{(i_1+j_3)e}=g^{(i_2+j_1)e}=g^{(i_3+j_2)e}$, and (36) implies $3(g^{(i_1+j_2)e}-g^{(i_1+j_3)e})=0$. Since $j_2\neq j_3$, we have $p=3$, contradicting (31) because $p>\sqrt{14}>3$. Therefore, the sum $\sum_{i=0}^{k-1}a_i^2$ is largest when there are three nonzero terms, one equal to $(\pm 3)^2$, one equal to $(\pm 2)^2$ and one equal to $(\pm 1)^2$, that is

$$\sum_{i=0}^{k-1}a_i^2\leqslant 9+4+1=14.$$

Now combining (36), (31) and Theorem 4.1, we obtain

$$f(\zeta_k)=\zeta_k^{i_1+j_2}+\zeta_k^{i_2+j_3}+\zeta_k^{i_3+j_1}-\zeta_k^{i_1+j_3}-\zeta_k^{i_2+j_1}-\zeta_k^{i_3+j_2}=0, \tag{37}$$

which is impossible by Lemma 5.7 and Proposition 5.8. □

Remark 5.9. Summarizing the results of Theorem 5.1, Theorem 5.3, Theorem 5.4, Theorem 5.5 and Theorem 5.6, we obtain $(a,b)\leqslant 3$ if $p>(14k/\varphi(k))^{\varphi(k)/(2\operatorname{ord}_k(p))}$. The inequality $p>\left(\sqrt{14}\right)^{k/\operatorname{ord}_k(p)}$ is sufficient for $p>(14k/\varphi(k))^{\varphi(k)/(2\operatorname{ord}_k(p))}$, due to (11). Thus, Theorem 1.2 is proved.

6. The Case where k is Prime

In this section, we will prove Theorem 1.3. We always assume that k is a prime and $a\neq b\in\{1,\dots,e-1\}$.

Similar to the proof of Theorem 1.2, the proof of Theorem 1.3 is divided into the cases $(0,0)$, $(0,a)$, $(a,0)$, (a,a) and (a,b) and Theorem 1.3 is just a simplified consequence of the results for the different cases. We remark that only in the cases $(0,a)$ and (a,b), we obtain better upper bounds for these numbers than the bounds obtained in the last section. We restate the results for $(0,0)$, $(a,0)$ and (a,a) here for the completeness of the proof.

Corollary 6.1. *If*

$$p>\left(\frac{3k}{k-1}\right)^{\frac{k-1}{2\operatorname{ord}_k(p)}},$$

then

$$(0,0)=\begin{cases}0 & \text{if } 2\notin C_0,\\ 1 & \text{if } 2\in C_0.\end{cases}$$

Proof. This theorem is a direct consequence of Theorem 5.1. Note that the case $6\mid k$ cannot occur because k is a prime. □

Corollary 6.2. *If*

$$p > \left(\frac{4k}{k-1}\right)^{\frac{k-1}{2\operatorname{ord}_k(p)}},$$

then

$$(a,0) \leqslant 2 \quad \textit{and} \quad (a,a) \leqslant 2.$$

Proof. If k is even, then $k=2$ and it is trivial that $(a,0) \leqslant 2$. If k is odd, then $(a,0) \leqslant 2$ by Theorem 5.4 (the case k is odd). Lastly, note that $(a,a) = (-a,0) \leqslant 2$. □

Theorem 6.3. *If*

$$p > \left(2^{k-1}k\right)^{1/\operatorname{ord}_k(p)}, \tag{38}$$

then

$$(0,a) \leqslant 2. \tag{39}$$

Proof. Each equation $1 + g^{ie} = g^{je+a}$ induces another equation $1 + g^{-ie} = g^{(j-i)e+a}$, and these equations are different only if $i \neq 0$. Moreover, if $i = 0$, then $2 = g^{je+a} \in C_a$.

First, suppose that $2 \in C_a$ and $(0,a) \geqslant 3$. We have $g^{le+a} = 2$ for some $0 \leqslant l \leqslant k-1$. There exist $0 \leqslant i,j \leqslant k-1$ with $i \neq 0$ and $j \neq l$ such that $1 + g^{ie} = g^{je+a}$. Writing $t = j - l$, we obtain

$$1 + g^{ie} - 2g^{te} = 0.$$

Note that the numbers $0, i, t$ are pairwise different. Write $1+x^i-2x^t$ in the polynomial form $f(x) = \sum_{i=0}^{k-1} a_i x^i$. Note that, using the notation of Theorem 4.2 (a), we have $A = 2$. Thus, by Theorem 4.2 (a) and (38), we have $f(\zeta_k) = 0$, as $f(g^e) = 0$. Hence

$$f(\zeta_k) = 1 + \zeta_k^i - 2\zeta_k^t = 0.$$

By Result 2.2, this happens only when the terms in $f(\zeta_k)$ cancel in pairs or $f(\zeta_k)$ is similar to $1 + \zeta_3 + \zeta_3^2$, both of which are not possible.

Next, suppose that $2 \notin C_a$ and $(0,a) \geqslant 3$. Similar to the proof of Theorem 5.3, we obtain the equation

$$1 + g^{i_1 e} - g^{(j_1-j_2)e} - g^{(j_1-j_2+i_2)e} = 0,$$

where the two pairs (i_1,j_1) and (i_2,j_2) are different and satisfy

$$i_1 \neq 0,\ i_2 \neq 0,\ (i_2,j_2) \neq (-i_1, j_1 - i_1)\} \text{ and } (i_1,j_1) \neq (-i_2, j_2 - i_2).$$

Write $f(x) = 1 + x^{i_1} - x^{j_1-j_2} - x^{j_1-j_2+i_2}$. Note that $f(x)$ is a polynomial with exactly 4 nonzero coefficients, as the numbers $0, i_1, j_1-j_2$ and $j_1-j_2+i_2$ are pairwise different (follows from the proof of Theorem 5.3). Thus, by Theorem 4.2 (a) and (38), we have

$$f(\zeta_k) = 1 + \zeta_k^{i_1} - \zeta_k^{j_1-j_2} - \zeta_k^{j_1-j_2+i_2} = 0.$$

By Result 2.2, the terms in $f(\zeta_k)$ cancel in pairs. This implies in $2 \mid k$ and $i_1 = i_2 = k/2$, or $j_1 = j_2$ and $i_1 = i_2$, both of which are not possible. □

Remark 6.4. The bound (38) is not better than the previous bound in (19) (in fact, they are very close). However, the conclusion (39) is better than the conclusion (20).

Theorem 6.5. *If*

$$p > (3^{k-1}k)^{1/\operatorname{ord}_k(p)}, \tag{40}$$

then

$$(a,b) \leqslant 2.$$

Proof. Similar to the proof of Theorem 5.6, we obtain the equation

$$g^{(i_1+j_2)e}+g^{(i_2+j_3)e}+g^{(i_3+j_1)e}-g^{(i_1+j_3)e}-g^{(j_2+j_1)e}-g^{(i_3+j_2)e}=0, \tag{41}$$

where (i_t,j_t), $t=1,2,3$, are pairwise different pairs each of which satisfy $1+g^{i_te+a}=g^{j_te+b}$. Write the left-hand-side of (41) as $\sum_{i=0}^{k-1}a_ig^{ie}$ and set $f(x)=\sum_{i=0}^{k-1}a_ix^i$. We have $\sum_{i=0}^{k-1}a_i=0$ and, using the notation of Theorem 4.2 (a), we have $A\geqslant 3$. Hence Theorem 4.2 (a) and (40) imply

$$f(\zeta_k)=\zeta_k^{i_1+j_2}+\zeta_k^{i_2+j_3}+\zeta_k^{i_3+j_1}-\zeta_k^{i_1+j_3}-\zeta_k^{i_2+j_1}-\zeta_k^{i_3+j_2}=0.$$

This is impossible by the proof of Theorem 5.6. □

Remark 6.6. Therem 6.5 is an improved version of Theorem 5.6, as the bound (40) is better than the one in (31). Furthermore, Theorem 6.1, Theorem 6.3, Theorem 6.2 and Theorem 6.5 prove Theorem 1.3.

References

[1] Leonard D. Baumert and Harold Fredricksen, *The cyclotomic numbers of order eighteen with applications to difference sets*, Math. Comp. **21** (1967), 204–219.

[2] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998, A Wiley-Interscience Publication.

[3] Koichi Betsumiya, Mitsugu Hirasaka, Takao Komatsu, and Akihiro Munemasa, *Upper bounds on cyclotomic numbers*, Linear Algebra Appl. **438** (2013), no. 1, 111–120.

[4] John Conway and Antony J. Jones, *Trigonometric diophantine equations (on vanishing sums of roots of unity)*, Acta Arith. **30** (1976), no. 3, 229–240.

[5] Philip J. Davis, *Circulant matrices*, Pure and Applied Mathematics, John Wiley & Sons, New York-Chichester-Brisbane, 1979, A Wiley-Interscience Publication.

[6] Ronald J. Evans and Jay R. Hill, *The cyclotomic numbers of order sixteen*, Math. Comp. **33** (1979), no. 146, 827–835.

[7] Shashikant A. Katre, *Cyclotomic numbers and a conjecture of Snapper*, Indian J. Pure Appl. Math. **20** (1989), no. 2, 99–103.

[8] Tsit Yuen Lam and Ka Hin Leung, *On vanishing sums of roots of unity*, J. Algebra **224** (2000), no. 1, 91–109.

[9] Emma Lehmer, *On cyclotomic numbers of order sixteen*, Canadian J. Math. **6** (1954), 449–454.

[10] Emma Lehmer and Harry S. Vandiver, *On the computation of the number of solutions of certain trinomial congruences*, J. Assoc. Comput. Mach. **4** (1957), no. 4, 505–510.

[11] Raymond E. A. C. Paley, *On orthogonal matrices*, Journal Math. Phys. **12** (1933), no. 1-4, 311–320.

[12] J. C. Parnami, M. K. Agrawal, and A. R. Rajwade, *Jacobi sums and cyclotomic numbers for a finite field*, Acta Arith. **41** (1982), no. 1, 1–13.

[13] Andrzej Schinzel, *An inequality for determinants with real entries*, Colloquium Mathematicum **38** (1978), no. 2, 319–321.

[14] Thomas Storer, *Cyclotomy and difference sets*, Lectures in Advanced Mathematics, vol. 2, Markham Publishing Co., Chicago, Ill., 1967.

[15] Harry S. Vandiver, *New types of trinomial congruence criteria applying to Fermat's last theorem*, Proc. Natl. Acad. Sci. USA **40** (1954), 248–252.

[16] ———, *On trinomial equations in a finite field*, Proc. Natl. Acad. Sci. USA **40** (1954), 1008–1010.

[17] ———, *Relation of the theory of certain trinomial equations in a finite field to Fermat's last theorem*, Proc. Natl. Acad. Sci. USA **41** (1955), 770–775.

[18] ———, *On distribution problems involving the numbers of solutions of certain trinomial congruences*, Proc. Natl. Acad. Sci. USA **45** (1959), 1635–1641.

[19] Albert L. Whiteman, *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc. **86** (1957), 401–413.

[20] ———, *The cyclotomic numbers of order ten*, in Combinatorial Analysis, Proc. Sympos. Appl. Math., vol. 10, American Mathematical Society, Providence, R.I., 1960, pp. 95–111.

[21] ———, *The cyclotomic numbers of order twelve*, Acta Arith. **6** (1960), 53–76.

Tai Do Duc, Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore
E-mail : `doductai001@e.ntu.edu.sg`

Ka Hin Leung, Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260, Republic of Singapore
E-mail : `matlkh@nus.edu.sg`

Bernhard Schmidt, Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore
E-mail : `bernhard@ntu.edu.sg`