Linear Algebra and its Applications 438 (2013) 111–120

Contents lists available at SciVerse ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

Upper bounds on cyclotomic numbers

Koichi Betsumiya [a], Mitsugu Hirasaka [b,*,1], Takao Komatsu [a,2], Akihiro Munemasa [c]

[a] Graduate School of Science and Technology, Hirosaki University, Hirosaki 036-8561, Japan
[b] Department of Mathematics, Pusan National University, Jang-jeon dong, Busan 609-735, Republic of Korea
[c] Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan

ARTICLE INFO

Article history:
Received 3 October 2011
Accepted 29 June 2012
Available online 13 September 2012

Submitted by V. Nikiforov

AMS classification:
11T22
15A15

Keyword:
Cyclotomic numbers

ABSTRACT

In this article, we give upper bounds for cyclotomic numbers of order e over a finite field with q elements, where e is a positive divisor of $q-1$. In particular, we show that under certain assumptions, cyclotomic numbers are at most $\lceil \frac{k}{2} \rceil$, and the cyclotomic number $(0, 0)$ is at most $\lceil \frac{k}{2} \rceil - 1$, where $k = (q-1)/e$. These results are obtained by using a known formula for the determinant of a matrix whose entries are binomial coefficients.

1. Introduction

Cyclotomic numbers have been studied since the beginning of the last century. According to [4, p. 25] we define them as follows:

Definition 1.1. Let q be a power of a prime p. Let $GF(q)$ denote the Galois field with q elements and let α be a primitive element of $GF(q)$. For a positive divisor e of $q-1$ and integers a, b with $0 \leqslant a, b < e$ we define the *cyclotomic number* $(a, b)_e$, which we denoted by (a, b) for short, to be

* Corresponding author.
E-mail addresses: betsumi@cc.hirosaki-u.ac.jp (K. Betsumiya), hirasaka@pusan.ac.kr (M. Hirasaka), komatsu@cc.hirosaki-u.ac.jp (T. Komatsu), munemasa@math.is.tohoku.ac.jp (A. Munemasa).
1 The second author thanks the support from the grant represented by the third author when the second author stayed at Hirosaki University from April 22–27 in 2011.
2 The third author is supported in part by the Grant-in-Aid for Scientific Research (C) (No. 22540005), the Japan Society for the Promotion of Science.

http://dx.doi.org/10.1016/j.laa.2012.06.045

$$|C_b \cap (C_a + 1)|$$

where C_a denote the cyclotomic coset $\langle\alpha^e\rangle\alpha^a$.

For example, when $q = 17$ and $e = 2$,

$$C_0 = \{1, 2, 4, 8, 16, 15, 13, 9\}, \quad C_1 = \{3, 6, 12, 7, 14, 11, 5, 10\}$$

where the numbers are read modulo 17, and the cyclotomic numbers in this case are:

$$(0, 0) = |\{1, 9, 16\}| = 3, \quad (0, 1) = (1, 0) = (1, 1) = 4.$$

In fact, when $e = 2$ and $q \equiv 1 \pmod 4$, the general formulas (see [4, p. 30, Lemma 6]) give

$$(0, 0) = \frac{q-5}{4}, \quad (0, 1) = (1, 0) = (1, 1) = \frac{q-1}{4}.$$

It is known that cyclotomic numbers can be determined from the knowledge of Gauss sums. However, explicit evaluation of Gauss sums of large orders is difficult in general [1, pp. 98–99 and p. 152], so one cannot expect a general formula for cyclotomic numbers for large e.

On the other hand, a somewhat rough estimate for cyclotomic numbers can be obtained following the approach by Wilson [6]. He gave an inequality for higher cyclotomic numbers. This in particular gives upper and lower bounds for ordinary cyclotomic numbers. A more direct approach is exact evaluation of the variance of cyclotomic numbers [5] where we set k as $\frac{q-1}{e}$:

$$\sum_{a,b=0}^{e-1} \left((a, b) - \frac{q-2}{e^2}\right)^2 = (e-3)k + 1 + \frac{2k}{e} - \frac{1}{e^2} \leqslant q - 1. \tag{1}$$

For each fixed e, we see from (1) that the cyclotomic number (a, b) is close to $\frac{k}{e}$, that is,

$$(a, b) = \frac{k}{e} + O(\sqrt{k}) \quad \text{as } k \to \infty. \tag{2}$$

However, when $e \geqslant k$, the formula does not seem to give any reasonable bound for (a, b) beyond the trivial bound $(a, b) \leqslant k$. This is unavoidable since, when $k + 1$ is a power of p, $(0, 0) = k - 1$.

The purpose of this paper is to give upper bounds on cyclotomic numbers without assuming any relations among e and k, but instead, we need to assume that p is sufficiently large compared to k. In order to obtain such upper bounds we will show that the cyclotomic number (a, b) is equal to $k - \operatorname{rank} C^{(a,b)}$, where $C^{(a,b)}$ is a certain matrix with entries in $GF(q)$ (see Lemma 3.1). Thus, giving a lower bound for the rank of $C^{(a,b)}$ results in an upper bound for the cyclotomic number (a, b). This is a problem in linear algebra over $GF(q)$, but it turns out that the matrix $C^{(a,b)}$ contains a submatrix whose entries consist entirely of elements of the prime field. More explicitly, $C^{(a,b)}$ contains a submatrix which is the modulo p reduction of the following matrix given in [2] for suitable r and s:

$$\left(\binom{r+s}{r-i+j}\right)_{1\leqslant i,j\leqslant m}. \tag{3}$$

Therefore, we obtain a lower bound for the rank whenever the determinant of the matrix (3) does not vanish modulo p. The following is our main result and the first three statements are obtained by this method.

Theorem 1.1. *Let q be a power of an odd prime p and k a positive divisor of $q - 1$. Then we have the following:*