Periodica Mathematica Hungarica Vol. 47 (1–2), 2003, pp. 111–117

ON THE MAXIMAL DIFFERENCE BETWEEN AN ELEMENT AND ITS INVERSE MODULO n

Mizan R. Khan (Willimantic) and Igor E. Shparlinski (Sydney)

[Communicated by: András Sárközi]

Abstract

We derive a lower bound for the arithmetic function

$$M(n) = \max\{|a-b| : a, b \in \mathbb{Z}_n \text{ and } ab \equiv 1 \pmod{n}\}$$

which then gives the asymptotic $n - M(n) = o\left(n^{.75+\varepsilon}\right)$ for any $\varepsilon > 0$.

1. Introduction

Let $\mathbb{Z}_n$ denote the residues modulo an integer $n \geq 2$. Throughout the paper we assume these residues to consist of the elements $\{0, 1, \ldots, n-1\}$.

Some years ago the first co-author [6] considered the arithmetical function $M(n)$ defined by

$$M(n) := \max\{|a-b| : a, b \in \mathbb{Z}_n \text{ and } ab \equiv 1 \pmod{n}\},$$

and proved by elementary methods that

$$M(n) \leq \left\lfloor n - 2\sqrt{n-1} \right\rfloor \tag{1}$$

with equality for infinitely many n.

Indeed, suppose the pair $(a, b) \in \mathbb{N}^2$ satisfies the following conditions:

$$1 \leq a, b \leq n-1, \ ab \equiv 1 \pmod{n}, \text{ and } M(n) = b - a.$$

Now $a(n-b) = kn - 1$ for some positive integer k. By the arithmetic-geometric mean inequality,

$$\frac{a+n-b}{2} \geq \sqrt{a(n-b)} = \sqrt{kn-1} \geq \sqrt{n-1},$$

which implies (1). Some further calculations give the following two properties:

$$M(n) = \left\lfloor n - 2\sqrt{n-1} \right\rfloor \Longleftrightarrow a(n-b) = n-1,$$

Mathematics subject classification number: 11A07, 11L05, 11T23.
Key words and phrases: residues, exponential sums.

0031-5303/03/$20.00

Akadémiai Kiadó, Budapest
Kluwer Academic Publishers, Dordrecht

thus

$$\left\{n : n \in \mathbb{N},\ M(n) = \left\lfloor n - 2\sqrt{n-1} \right\rfloor\right\}$$
$$= \left\{n : n = m^2 + lm + 1,\ m \in \mathbb{N},\ l \in \mathbb{Z},\ 0 \le l < 2\sqrt{m} + 1\right\}.$$

In this paper we derive, via exponential sums, a lower bound for $M(n)$ from which we conclude

$$n - M(n) = o\left(n^{0.75+\varepsilon}\right) \tag{2}$$

for any $\varepsilon > 0$.

Apparently the first person to explicitly study the difference between an element and its inverse modulo n is Zhang [9, 10]. Around the same time Zheng [11] obtains similar results in a more general context. The results in [10] and [11] have been generalized in the recent papers [2, 4, 8]. However, none of these papers explicitly address the question of bounding $M(n)$. The bound which we prove is slightly more accurate and explicit than what follows from the above works.

We denote the group of units of $\mathbb{Z}_n$ by $\mathbb{Z}_n^*$, thus the cardinality of $\mathbb{Z}_n^*$ is given by the Euler function $\varphi(n)$. Three other arithmetical functions we use are the Mobius function, $\mu(n)$, the number and the sum of divisors functions

$$\tau(n) = \sum_{d|n,\, d>0} 1, \qquad \sigma(n) = \sum_{d|n,\, d>0} d = n \sum_{d|n,\, d>0} \frac{1}{d}.$$

As usual $\zeta(s)$ denotes the Riemann zeta function

$$\zeta(s) = \sum_{m=1}^{\infty} \frac{1}{m^s}.$$

Finally for an integer $m \ge 1$ we define

$$\mathbf{e}_m(z) = \exp\left(2\pi i z/m\right).$$

2. Exponential sums

Here we collect several, mainly known, results about exponential sums.

First of all we need the identity which follows from the formula for the sum of a geometric progression.

$$\sum_{\lambda=0}^{n-1} \mathbf{e}_n(\lambda w) = \begin{cases} 0, & \text{if } w \not\equiv 0 \pmod{n}, \\ n, & \text{if } w \equiv 0 \pmod{n}. \end{cases} \tag{3}$$

Let us define the sums

$$T(r;h) = \sum_{x=0}^{h-1} \mathbf{e}_n(rx) \quad \text{and} \quad W_d(h) = \sum_{\substack{r \in \mathbb{Z}_n \\ \gcd(r,n)=d}} |T(r;h)|^2.$$

The following statement is essentially Lemma 17.3 in [7].