

СЕКЦИЯ

„АЛГЕБРА И ЛОГИКА”

Драги колеги,

На 7 юни 2024 г. (петък) от 12:30 часа в зала 503 на ИМИ-БАН ще се проведе присъствено заседание на семинара по Алгебра и логика.

Доклад на тема

Some Properties and Applications of Kloosterman Sums on Finite Fields

ще изнесе Любомир Борисов (ИМИ-БАН).

Поканват се всички желаещи да присъстват.

От секция „Алгебра и логика” на ИМИ – БАН

<http://www.math.bas.bg/algebra/seminarAiL/>

Some Properties and Applications of Kloosterman Sums on Finite Fields

Lyubomir Borissov

This project for Ph.D. thesis is devoted to some properties and applications of one-dimensional classical (or ordinary) Kloosterman sums on finite fields.

More specifically, let $\mathcal{K}_q(u) = \sum_{x \in \mathbb{F}_q^*} \exp(2\pi i \text{Tr}(x + u/x)/p)$ be the ordinary Kloosterman sum on finite field \mathbb{F}_q of order $q = p^m$, where $\text{Tr}(\cdot)$ is the absolute trace function from \mathbb{F}_q into \mathbb{F}_p . $\mathcal{K}_q(u)$ is a real number of absolute value at most $2\sqrt{q}$ by the Weil bound. The angle of $\mathcal{K}_q(u)$ is the unique real number θ_u with

$$\cos \theta_u = \frac{\mathcal{K}_q(u)}{2\sqrt{q}}, \quad 0 \leq \theta_u \leq \pi.$$

The main contributions of thesis are:

- It is proved that the angles of Kloosterman sums on arbitrary finite field are incommensurable with the constant π , i.e., θ_u is never a rational multiple of π . In particular, this implies that the Weil bound for Kloosterman sums on finite fields is never attained.
- It is shown that, for any $m > 1$, the so-called lifted Kloosterman sums $\mathcal{K}_{p^m}(u)$ with $u \in \mathbb{F}_p, p \geq 3$ are distinct. This result extends the corresponding Fischer's result for the simplest Kloosterman sums when m equals 1.
- Motivated by S.M. Dodunekov and H. Niederreiter's investigations concerning the binary finite field elements with related trace and co-trace, we address the problem of efficient enumeration of the elements of the field \mathbb{F}_q with prescribed absolute trace and co-trace for arbitrary characteristic p . It is shown that the problem can be converted to solving a system of $p-1$ linear equations with matrix of coefficients the left-circulant matrix constituted (up to some additive constants) by the simplest Kloosterman sums, and free-coefficient vector consisted of the corresponding lifted sums. The proposed approach is illustrated for characteristic $p = 2, 3$ and 5. Also, making use of the Weil bound, we study the asymptotic behavior of the quantities of interest and prove that it resembles q/p^2 .