СЕМИНАР

„АЛГЕБРА И ЛОГИКА”

Драги колеги,
Следващото заседание на семинара ще се проведе
на 31 май 2019 г. (петък) от 12:30 часа
в зала 578 на ИМИ – БАН.
Доклад на тема

Върху различието на сумите на Клостерман над GF($\boldsymbol{p}$)

ще изнесе Любомир Борисов.

Покават се всички желаещи.

От секция „Алгебра и логика” на ИМИ – БАН

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

==

Резюме

Нека $\mathbb{F}_q$ е крайното поле с нечетна характеристика q от ред $q = p^m$, $m \in \mathbb{N}$; $\mathbb{F}_q^* = \mathbb{F}_q \ \{0\}$, Tr е функцията абсолютна следа над $\mathbb{F}_q$ и $a \in \mathbb{F}_q$. Сума на Клостерман $K_q(a)$ се дефинира, както следва:

Дефиниция 1:

$$K_q(a) = \sum_{x \in \mathbb{F}_q^*} \omega^{Tr(x + \frac{a}{x})},$$

където $\omega = e^{\frac{2\pi i}{p}}$ е комплексен примитивен p-ти корен на 1.

При сумите на Клостерман $K_q(a)$ има тенденция да са различни за достатъчно голямо p (с точност до действието на групата на Галоа $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, породена от автоморфизма на Фробениус), т.е. $K_q(a) = K_q(b)$ точно когато $b = a^{p^s}$ за някое s. Например в [1] е доказано, че това е вярно винаги за $p > (2.4^m + 1)^2$. Обаче не са известни резултати за различие на тези суми, когато p е малко спрямо m и a пробягва някое подполе. Тази работа дава частичен прогрес за прости подполета и $m = 2^n$, $n \in \mathbb{N}$. Основният резултат е формулиран в следната Теорема:

Теорема 2: За всяко $n \geq 0$, $(p-1)$-те суми на Клостерман $K_{p^{2^n}}(a)$, $a \in \mathbb{F}_p^*$ са различни.

Накрая на базата на известния факт, че $K_q(0) = -1$ за всяко q и на несъществуването на нули на Клостерман, когато $p > 3$ [2], получаваме следното следствие.

Следствие 3: За всяко $n \geq 0$, p-те суми на Клостерман $K_{p^{2^n}}(a)$, получени когато a пробягва простото поле $\mathbb{F}_p$, $p > 3$, са различни.

Литература

[1] B. Fischer, "Distinctness of Kloosterman sums", in Contemporary Mathematics: p-adic Methods in Number Theory and Algebraic Geometry, American Mathematical Society, 81-102, 1992.

[2] K.P. Kononen, M. Rinta-aho, K. Väänänen, "On integer values of Kloosterman sums", IEEE Transactions on Inform. Theory, vol. 57(3): 4011-4013, 2010.