EXPONENTIAL SUMS OVER MULTIPLICATIVE GROUPS IN FIELDS OF PRIME ORDER AND RELATED COMBINATORIAL PROBLEMS

Sergei Konyagin

Let p be a prime, and $\mathbb{Z}_p$ be the set of the residues classes modulo p. Then $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ is the multiplicative group of the field $\mathbb{Z}_p$. We take an arbitrary subgroup G of the group $\mathbb{Z}_p^*$.

For $u \in \mathbb{R}$ we denote $e(u) = \exp(2\pi i u)$. Observe that $e(x/p) = e(y/p)$ if $x \equiv y (\mathrm{mod} p)$. Thus, $e(a/p)$ is correctly defined for $a \in \mathbb{Z}_p$.

The main subject of my talks is the estimation of exponential sums over G:

$$S(a,G) = \sum_{x \in G} e(ax/p), \quad a \in \mathbb{Z}_p.$$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

These sums have numerous applications in additive problems modulo p, pseudo-random generators, coding theory, theory of algebraic curves and other problems.

Trivially,

$$|S(a,G)| \le |G|.$$

We are interested in obtaining nontrivial estimates for $S(a,G)$:

$$S(a,G) = o(|G|) \quad (p \to \infty, a \in \mathbb{Z}_p^*)$$

or, for some $\delta > 0$,

$$S(a,G) \le C(\delta)|G|p^{-\delta} \quad (a \in \mathbb{Z}_p^*).$$

Also, related combinatorial problems including the sums-products problem in $\mathbb{Z}_p$ and additive properties of groups G will be discussed.

The first lecture will be introductory. In the second lecture I suppose to talk about the using of Stepanov's method for study additive properties of groups G and exponential sums over G and also about the sums- products problem modulo p. In the concluding lecture some recent results related to exponential sums and additive properties of subsets of $\mathbb{Z}_p$ will be discussed.