REPORT ON THE DYNASTY FOUNDATION

ILYA VYUGIN

Results of the 2014 year

Results in additive combinatorics.

Let G be a subgroup of $\mathbb{F}_p^*$ (multiplicative group of $\mathbb{F}_p$), where p is a prime. We consider an equation

$$y = f(x) \tag{1}$$

where $f \in \mathbb{F}_p[x]$ is a polynomial, $x, y \in \mathbb{F}_p$. We obatain an estimate of the number of solutions (x, y) of (**??**) which are belonging to $G \times G$, or the product of cosets of G ($g_1G \times g_2G$).

Theorem *Let G be a subgroup of $\mathbb{F}_p^*$, $|G| = O(p^{3/4})$, $g_1, g_2 \in \mathbb{F}_p$ $f(x)$ be a polynomial of degree m, $f(0) \neq 0$, then the number of solutions (x, y) of equation*

$$y = f(x),$$

such that $(x, y) \in G \times G$, does not exceed $8(m + 2)|G|^{2/3}$.

The number of points of elliptic and hyperelliptic curves has the great interest for applications. Consider the curve

$$y^2 = P(x), \tag{2}$$

where $P(x)$ is a polynomial of degree m. It is easy to see that the number of solutions (x, y) of equation (**??**), such that $(x, y) \in g_1G \times g_2G$, does not exceed $16(m + 2)|G|^{2/3}$. Obviously, the number of pairs (x, y^2) does not exceed $8(m + 2)|G|^{2/3}$, consequently, the number of pairs (x, y) does not exceed $16(m+2)|G|^{2/3}$.

Let consider a subgroup $G \subset \mathbb{F}_p^*$, cosets $G_1, \dots, G_s$, $s = \frac{p-1}{t}$ and a map

$$f : x \longmapsto (f_1(x), \dots, f_n(x)) \in \mathbb{F}_p^n \tag{3}$$

with polynomials $f_1(x), \dots, f_n(x) \in \mathbb{F}_p[x]$. Let suppose that an each polynomial $f_i(x)$ has at least $l > 0$ (taking into account the multiplicity) unique roots, such roots that they do not roots of the other polynomials $f_j(x)$, $j \neq i$.

Polynomials $f_1(x), \dots, f_n(x)$ have degrees m_i ($\deg f_i(x) = m_i$, $i = 1, \dots, n$) for some collection m_i. We will estimate a cardinality of a set

$$L = \{x \mid f_i(x) \in G_{j_i},\ i = 1, \dots, n\}.$$

Theorem *Suppose that G is a subgroup of $\mathbb{F}_p^*$ (p is a prime), $|G| = t < \frac{p^{1-\frac{1}{2n+1}}}{(n+1)\prod_{i=1}^n m_i}$, $G_{j_1}, \dots, G_{j_n}$ are cosets, $f_1(x), \dots, f_n(x)$ are polynomials of degrees $m_1, \dots, m_n$. Then the cardinality of L does not exceed $C|G|^{1/2+1/(2n+1)}$, where C is an absolute constant.*

Theorem *Let $G_0, \dots, G_k \subseteq \mathbb{F}_p^*$ be subgroups of $\mathbb{F}_p^*$, $\mu_1, \dots, \mu_k$ be distinct nonzero residuals. Suppose that for all $k_1 = 1, \dots, k$ the following restrictions*

$$|G_0| \cdot \ldots \cdot |G_{k_1}| < (k_1 + 2)^{-\frac{2k_1+1}{2}} p^{k_1+\frac{1}{2}}$$

and for all $k_1 = 0, \dots, k$ *and for all* $j = 0, \dots, k_1$ *the following restrictions*

$$\frac{1}{2}\left(\prod_{i=0}^{k_1}|G_i|\right)^{\frac{1}{2k_1+1}} < |G_j| < \frac{1}{2(k_1+3)}\left(\prod_{i=0}^{k_1}|G_i|\right)^{\frac{2}{2k_1+1}}$$

imply. Then the following holds

$$|G_0 \cap (G_1+\mu_1) \cap \dots \cap (G_k+\mu_k)| \le 4k(k+2)(|G_0||G_1|\dots|G_k|)^{\frac{1}{2k+1}}.$$

Papers

[1] (With R.R. Gontsov) Solvability of linear differential systems in the Liouvillian sense
arXiv:1312.2518 , 2013, (submited to journal in 2014).

The paper concerns the solvability by quadratures of linear differential systems, which is one of the questions of differential Galois theory. We consider systems with regular singular points as well as those with (non-resonant) irregular ones and propose some criteria of solvability for systems whose (formal) exponents are sufficiently small.

[2] (With I.D. Shkredov, E.V. Solodkova) Intersections of multiplicative subgroups and Heilbronn's exponential sum
arXiv:1302.3839, 2014, (will be submited to journal).

The paper is devoted to some applications of Stepanov method. In the first part of the paper we obtain the estimate of the cardinality of the set, which is obtained as an intersection of additive shifts of some different subgroups of F_p^*. In the second part we prove a new upper bound for Heilbronn's exponential sum and obtain a series of applications of our result to distribution of Fermat quotients.

[3] On the number of solutions of discret algebraic curve
Proceedings of the young mathematician conference, 2014, p. 29-33 (an extended version will be submited to journal soon).

The number of solutions (x, y) of an equation

$$y = f(x), \qquad f(x) \in F_p[x]$$

such that $x, y \in G \times G$, where G is a subgroup of $\mathbb{F}_p^*$, was obtained in the paper.

Scientific conferences and seminar talks

[1] Workshop "Unlikely intersections", CIRM, Luminy, France, 3.02.2014-7.02.2014,
talk "On the intersection of additive shifts of subgroups of F_p^*".
[2] International conference on Differential and Functional Differential equations, Moscow, 22.08.2014-29.08.2014,
talk "On the Continous Limit for Systems of Diference Equations".
[3] The International Conference on Differential Equations and Dynamical Systems, Suzdal, Russia, 4.07.2014-9-07.2014,
Talk "Some estimates over finite fields and their continous analogs".
[4] Seminar "Analitic theory of differential equations" (D.V Anosov, V.P. Lexin), MIAN RAS

Talk “On the Continous limit for difference equations”.

[5] Seminar “Modern Problems of Number theory” (S.V. Konyagin, I.D. Shkredov), MIAN RAS

Talk “On the number of solutions of an equation over finite field”.

[6] Seminar of the group of complex analysis (B. Lamel, I. Kossovskiy, D. Dela Sala), University of Vienna

Talk “Linear differential equations and holomorphic vector bundles”.

Teaching

[1] Differential Geometry (lectures and seminars). Independent University of Moscow, II year students, Feburary-May 2013, 2+2 hours per week (joint with Yu. M. Burman).

Program

Rimannian Geometry

1. Curves. Ortogonal transformations classifications (Frenet formulas).
2. Surfacies. Bonne classification theorem.
3. An existence of Riemannian metric.
4. Levy-Civita connection.
5. Gauss-Bonne formula.
6. Euler–Lagrange equation.

Symplectic geometry

7. Darboux theorem.
8. Jacobi equality for invertible Poisson brackets.
9. Symplectic lies.
10. Moment map.

[2] Analitic theory of differential equations (lectures) Special course in HSE and IUM (joint with V.A. Poberezhny).

Program

Linear differential equations: asymptotics, geometry and Riemann–Hilbert problem

1. Fuchs conditions.
2. Riccati equation.
3. Linear differential equations: monodromy, singular points. Levelt decomposition.
4. Hypergeometric equation and hypergeometric functions.
5. Riemann–Hilbert problem