Polynomial Equations over Subgroups

Ilya Vyugin

Department of Mathematics of HSE and IITP

Mathematics, Computer and Information Technologies Seminar

12.12.2017

Background

Let $\mathbb{F}_p^*$ is a field of residues modulo prime p,

$$P(x, y) = 0 \tag{1}$$

is an algebraic curve. Then the number N_p of pairs (x, y) such that $x, y \in \mathbb{F}_p$ lying on the curve (1) is approximately p.

$$|N_p - (p + 1)| \leqslant 2g\sqrt{p}$$

(Hasse, Weil, Delighne).

Equations in subgroups

Let G be a subgroup of $\mathbb{F}_p^*$, p is a prime.
The bound of the number of solutions of equation

$$P(x,y) = 0, \qquad P \in \mathbb{F}_p[x,y],$$

such that $x \in g_1G$, $y \in g_2G$, where g_1G, g_2G are costes by subgroup G, was obtained by Corvaja and Zannier.

P. Corvaja, U. Zannier, Gratest Common Divisor $u-1, v-1$ in positiv characteristic and rational points on curves over finite fields, J. of Eur. Math. Soc., V. 15, I. 5, pp. 1927-1942, 2013.

The case of linear equations

Theorem (Garcia, Voloch)

Let $G \subset \mathbb{F}_p^*$ be a subgroup, such that $|G| < (p-1)/((p-1)^{1/4}+1)$. Then the number of solutions of the equation

$$y = x + q, \quad q \neq 0,$$

such that $x, y \in G$ does not exceed $4|G|^{2/3}$ or in other words

$$|G \cap (G+q)| \leqslant 4|G|^{2/3}.$$

Heath-Brown and Konyagin reproved this result by Stepanov method.

The bound in average

Theorem (Konyagin)

In conditions of previous theorem the following bound holds. The the number of solutions of the union of equations

$$y = x + q_i, \quad i = 1, \ldots, h,$$

where q_i belong to different cosets by subgroup G, such that $x, y \in G$ does not exceed $Ch^{2/3}|G|^{2/3}$.

Case of many shifts

Theorem (Shkredov, I.V.)

Let G be a subgroup of $\mathbb{F}_p^*$, such that $|G| > 32n2^{20n\log(n+1)}$, $p > 4n|G|(|G|^{\frac{1}{2n+1}} + 1)$, $q_1, \ldots, q_n$ be different residues. Then the number of such $x \in \mathbb{F}_p$ that

$$|G \cap \ldots \cap (G + q_n)| \leqslant 4n(n+1)(|G|^{\frac{1}{2n+1}} + 1)^{n+1}.$$

Asymptotic form of the previous theorem

Theorem

If $C_1(n) < |G| < C_2(n)p^{1-\alpha_n}$*, then*

$$|G \cap \ldots \cap (G + q_n)| < C_3(n)|G|^{1/2+\beta_n}$$

where $\alpha_n, \beta_n \to 0$*,* $n \to \infty$*,* $C_1(n), C_2(n), C_3(n)$ *are some constants.*

One cryptography problem

Let p be a large prime;
$\mathbb{F}_p$ be a field of residues modulo prime p;
t is a divisor of $(p-1)$;

Oracle give us the number $(x+s)^t$ by x in $\mathbb{F}_p$.

Problem: Find the unknown number s by minimum arithmetic operations (complexity) and questions to Oracle.

One cryptography application

Theorem (Bourgain, Konyagin, Shparlinsky)

Let $q \in \mathbb{F}_p$ *be some prime number and at least one non-residue of the order* q *is known. Then for any* $\varepsilon > 0$ *there exists an algorithm, that find* s *such that the number of questions to Oracle does not exceed* $O_\varepsilon\left(\frac{\log p}{\log(p/t)}\right)$ *and complexity does not exceed*

$$t^{1+\varepsilon}(\log p)^{O(1)}.$$

Application to decomposition of subgroups

Let G be a subgroup of F_p^*.

Suppose that $G = A + B$, where A and B are some subsets of F_p. Then $|A|$ and $|B|$ are around of $\sqrt{G}$.

Ilya Shkredov has proved that a subgroup G can not be represented as a sum of two sets $G \neq A + B$ (in some restriction on the size of subgroup).

Additive energy

Let A be a subset of $\mathbb{F}_p$
Additive energy

$$E_k(A) = \#\{(x_1, \ldots, x_{2n}) \mid x_1 + x_2 = \cdots = x_{2n-1} + x_{2n},$$

$$x_i \in A,\ i = 1, \ldots, 2n\}$$

Theorem (Konyagin)

Let G be a subgroup of F_p^*, and $|G| \leqslant p^{3/4}$. Then

$$E_2(G) < C|G|^{5/2}.$$

Idea of the proof

$$\Omega = G \cap \ldots \cap (G + q_n)$$

To estimate $|\Omega|$ let us construct the polynomial $\Psi(x)$ such that:
1) $\Psi(x) \not\equiv 0$;
2) the elements of Ω are roots of $\Psi(x)$ of order at least D.
Then

$$|\Omega| \leqslant \frac{\deg \Psi}{D}.$$

Idea of the proof

$$\Psi(x) = \sum_{a,b} \lambda_{a,b} x^a x^{b_0 t} (x-q_1)^{b_1 t} \dots (x-q_n)^{b_n t},$$

where $a < A$, $b_i < B_i$, $t = |G|$.

$$\forall x \in \Omega \quad \Psi(x) = \Psi'(x) = \dots = \Psi^{(D-1)}(x) = 0.$$

$$[x(x-q_1)\dots(x-q_n)]^k \sum_{a,b} \frac{d^k}{dx^k} \lambda_{a,b} x^a x^{b_0 t} (x-q_1)^{b_1 t} \dots (x-q_n)^{b_n t} =$$

$$= \lambda_{a,b} P_{k,a,b}(x) x^a x^{b_0 t} (x-q_1)^{b_1 t} \dots (x-q_n)^{b_n t} = P_{k,a,b}(x), \qquad x \in \Omega.$$

1) $\deg P_{k,a,b}(x) \leqslant nk$;
2) coefficients of $P_{k,a,b}(x)$ are linear forms on λ_a.
If $\#\lambda_{a,b} > \#(\text{coefficients of } P_{k,a,b}(x))$ then there exists $\Psi(x)$ which satisfy the conditions.

Corvaja and Zannier's bound

Theorem (Corvaja-Zannier) *Let X be a smooth projective absolutely irreducible curve over a field κ of characteristic p. Let $u, v \in \kappa(X)$ be rational functions, multiplicatively independent modulo κ^*, and with non-zero differentials; let S be the set of their zeros and poles; and let $\chi = |S| + 2g - 2$ be the Euler characteristic of $X \setminus S$. Then*

$$\sum_{\nu \in X(\overline{\kappa}) \setminus S} \min\{\nu(1-u), \nu(1-v)\} \leqslant \left(3\sqrt[3]{2}(\deg u \deg v)^{1/3}, 12\frac{\deg u \deg v}{p}\right),$$

where $\nu(f)$ denotes the multiplicity of vanishing of f at the point ν.

$$\Omega = \{(x, y) \mid x \in g_1 G,\ y \in g_2 G,\ P(x, y) = 0\}$$

We obtain by Stepanov method the upper bound

$$\#\Omega < 12mn^2(m+n)|G|^{2/3}.$$

Bound in average

Let us suppose that $P(x, y)$ is a homogeneous of degree n, $l_1, \dots, l_h$ belongs to different cosets by subgroup G of $\mathbb{F}_p^*$.

Theorem (Makarychev, I.V.)

Let us consider a homogeneous polynomial $P(x, y)$ of degree n, such that $\deg P(x, 0) \geqslant 1$. Then the set of equations

$$P(x, y) = l_i, \quad i = 1, \dots, h,$$

$h < \min(\frac{1}{81}|G|^{4/3}, \frac{1}{3}pt^{-4/3})$ *the sum N_h of numbers of solutions of the set of equations does not exceed*

$$N_h \leqslant 32h^{2/3}n^5|G|^{2/3}.$$

Let A be a subset of F_p, $P(x,y)$ be a polynomial. Polynomial energy

$$E_k^P(A) = \#\{(x_1, \dots, x_{2n}) \mid P(x_1, x_2) = \dots = P(x_{2n-1}, x_{2n}),$$

$x_i \in A,\ i = 1, \dots, 2n\}.$

Theorem (Makarychev, I.V.)

Let G be a subgroup of F_p^*, $P \in \mathbb{F}_p[x,y]$ is a homogeneous and $100(mn)^{3/2} < |G| < \left(\frac{p}{3}\right)^{\frac{12}{17}}$. Then the following holds: if $q \leqslant 3$ then

$$E_P^q(G) \leqslant C(n,q)|G|^{\frac{7q+16}{12}};$$

if $q = 4$ then

$$E_P^4 \leqslant C(n,q)|G|^{1+\frac{2q}{3}} \ln |G|;$$

if $q \geqslant 5$ then

$$E_P^q(G) \leqslant C(n,q)|G|^{1+\frac{2q}{3}},$$

where $C(n,q)$ depends only on n and q.

Markoff's equation

Markoff's equation

$$x^2 + y^2 + z^2 = 3xyz$$

Any solution of this equation in $\mathbb{Z}$ can be obtained from two basic solutions $(0,0,0)$ and $(1,1,1)$ by combination following transforms

a) permutations of components;
b) $(x,y,z) \to (-x,-y,z)$;
c) $(x,y,z) \to (x,y,z-3xy)$

Solutions of Markoff's equation in $\mathbb{Z}$ generate a tree.

Markoff's equation in $\mathbb{F}_p$

$$x^2 + y^2 + z^2 = 3xyz, \qquad x, y, z \in \mathbb{F}_p.$$

Conjecture: Any solution of this equation in $\mathbb{F}_p$ can be obtained from two basic solutions $(0, 0, 0)$ and $(1, 1, 1)$ by combination transforms a), b) and c).

Main problem: prove the conjecture.

Structure of Markoff's graph

Theorem (Bourgain, Gamburd and Sarnak, 2016)

For any fixed $\varepsilon > 0$ and sufficiently large p there exists the orbit $C(p)$ in the solutions space $X^*(p)$ such that

$$|X^*(p) \setminus C(p)| \leqslant p^{\varepsilon}$$

and for any nonzero orbit

$$|D(p)| > (\log p)^{1/3}.$$

Structure of Markoff's graph

Theorem (Konyagin, Makarychev, Shparlinski and Vyugin, 2017)

There exists the orbit $C(p)$ in the solutions space $X^*(p)$ such that

$$|X^*(p) \setminus C(p)| \leqslant \exp((\log p)^{1/2+o(1)}), \quad p \to \infty$$

and for any nonzero orbit

$$|D(p)| > c(\log p)^{7/9},$$

where c is an absolute constant.

Approach to solving the problem

Consider the following chain of Markoff triples

$$(a, u_{i-1}, u_i) \to (a, u_i, u_{i+1})$$

where $u_{i+1} = 3au_i - u_{i-1}$.

These triples (a, u_{i-1}, u_i) generate a linear recurrence with characteristic equation $\lambda^2 - 3a\lambda + 1 = 0$

$$u_k = \alpha\lambda^k + \beta\lambda^{-k}, \qquad \lambda = \frac{3a + \sqrt{9a^2 - 4}}{2}.$$

Thank you for your attention!!!