On Some Applications of Differential Equations to Problems in Additive Number Theory

Ilya Vyugin

Department of Mathematics of HSE and IITP RAS

Dynamics in Siberia – 2021

5.03.2021

Additive Number Theory

Sum and product of sets

Let $R = R(+;\cdot)$ be a ring and $A, B \subset R$ be any finite sets.

- $A + B := \{a + b \,:\, a \in A,\ b \in B\}$ (sumset)
- $A \cdot B := \{a \cdot b \,:\, a \in A,\ b \in B\}$ (product set)

We study both operations simultaneously (= Arithmetic Combinatorics).

Additive shift

- $A + q := \{a + q \,:\, a \in A\}$ (additive shift)

Sum-product problem

Conjecture (Erdos–Szemerédi, 1983)

Let $A \subset \mathbb{Z}$, $|A| < \infty$. Then

$$\max(|A + A|, |A \cdot A|) \geq C|A|^{2-\varepsilon}$$

for sum constant C and any arbitrary $\varepsilon > 0$.

The Conjecture is proved for $\varepsilon = 2/3$ (Solymosi, Konyagin, Shkredov, Rudnev, Stevens).

Sum-product problem over $\mathbb{F}_p$

Conjecture (Erdos–Szemerédi in $\mathbb{F}_p$)

Let $A \subset \mathbb{F}_p$, $|A| < p^{1/3}$. Then

$$\max(|A + A|, |A \cdot A|) \geq C|A|^{2-\varepsilon}$$

for sum constant C and any arbitrary $\varepsilon > 0$.

Theorem (Askoy-Yazici-Murphy-Rudnev-Shkredov, 2017)

Let $A \subset \mathbb{F}_p$, $|A| < p^{5/8}$. Then

$$\max(|A + A|, |A \cdot A|) > C|A|^{6/5}$$

for sum constant C.

Definitions

Simple finite field

- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$, p — is a prime number;
- $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ is the multiplicative group of $\mathbb{F}_p$;
- G is a subgroup of $\mathbb{F}_p^*$, $|G| = t$ ($|\cdot|$ — the number of elements.)

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*

$$|G \cap (G+q)| \leqslant 4|G|^{2/3}, \quad q \neq 0.$$

Heath-Brown and Konyagin reproved this result by Stepanov's method and obtained its average version.

The bound in average

Theorem (Konyagin)

In conditions of previous theorem we have the following bound

$$\bigcup_{i=1}^{h} |G \cap (G + q_i)| \leqslant Ch^{2/3}|G|^{2/3},$$

where q_i, $i = 1, \ldots, h$ *belong to different cosets by subgroup* G.

Sum-product problem for subgroup

Theorem (Shkredov, I.V.)

Let $G \subset \mathbb{F}_p^*$ be subgroup and $|G| < C_1 p^{1/2}$. Then

$$|G \pm G| > C_2 \frac{|G|^{5/3}}{\log^{1/2} |G|}$$

for some constants C_1, C_2.

Case of many shifts

Theorem (Shkredov, I.V., 2013)

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

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

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.*

On the sum-set hypothesis for subgroups

Let G be a subgroup of $\mathbb{F}_p^*$.

Suppose that $G = A + B$, where A and B are some subsets of $\mathbb{F}_p$. 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).

Application to cryptography

Let p be a large prime number;
$\mathbb{F}_p$ 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 the minimal number of arithmetic operations (complexity) and questions to Oracle.

Application to cryptography

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

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

The case of polynomial map

Definition

The set $f_1(x), \ldots, f_n(x)$ of polynomials is called admissible if there exist such $x_1, \ldots, x_n$ that

$$f_i(x_i) = 0, \quad f_i(x_j) \neq 0, \quad i \neq j.$$

Let us define the set

$$M = \{x \mid f_i(x) \in G_i,\ i = 1, \ldots, n\}.$$

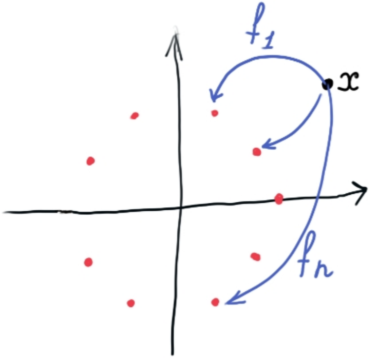

Figure: $M = \{x \in \mathbb{C} \mid f_i^t(x) = 1,\, i = 1, \dots, n\}$

Theorem (I.V., 2019)

Let G be subgroup of $\mathbb{F}_p^*$ (p is prime), and let $G_1, \dots, G_n$ be cosets by G, $n \geqslant 2$, $f_1(x), \dots, f_n(x)$ — admissible set of polynomials $\deg f_i(x) = m_i$ ($i = 1, \dots, n$):

$$C_1(\boldsymbol{m}, n) < |G| < C_2(\boldsymbol{m}, n) p^{1-\frac{1}{2n+1}},$$

where $C_1(\boldsymbol{m}, n), C_2(\boldsymbol{m}, n)$ depend only on n and $\boldsymbol{m} = (m_1, \dots, m_n)$. Then

$$|M| = |\{x \mid f_i(x) \in G_i,\ i = 1, \dots, n\}| \leqslant C_3(\boldsymbol{m}, n)|G|^{\frac{1}{2}+\frac{1}{2n}},$$

where $C_3(\boldsymbol{m}, n)$ depends only on n ¸ $\boldsymbol{m}$.

$$C_1(\mathbf{m},n) = 2^{2n} m_n^{4n}, \qquad C_2(\mathbf{m},n) = (n+1)^{-\frac{2n}{2n+1}} (m_1 \ldots m_n)^{-\frac{2}{2n+1}},$$

$$C_3(\mathbf{m},n) = 4(n+1)(m_1 \ldots m_n)^{\frac{1}{n}} \sum_{i=1}^{n} m_i.$$

Stepanov's method

If we construct the polynomial $\Psi(x)$ such that:

1) $\Psi(x) \not\equiv 0$;

2) $\deg \Psi(x) < p$;

3) all $x \in M$ be roots of $\Psi(x)$ of orders at least D:

$$\Psi(x) = \Psi'(x) = \ldots = \Psi^{(D-1)}(x) = 0, \quad x \in M.$$

Then

$$|M| \leqslant \frac{\deg \Psi}{D}, \quad M = G \cap (G + q_1) \cap \ldots \cap (G + q_n).$$

Stepanov's polynomial

Consider the polynomial

$$\Psi(x) = \sum_{a,b} \lambda_{a,b}\, x^a f_1^{b_0 t}(x) \dots f_n^{b_n t}(x),$$

with variable coefficients $\lambda_{a,b}$ ($a < A$, $b_i < B_i$, $t = |G|$).

If $x \in M$ then

$$\Psi(x) = \sum_{a,b} \lambda_{a,b}\, x^a,$$

because $f_1^t(x) = \ldots = f_n^t(x) = 1$.

If $\sum_b \lambda_{a,b} = 0$ for any a, then

$$\Psi(x) = 0, \qquad x \in M.$$

Vanishing conditions

Conditions

$$0 = \Psi(x) = \Psi'(x) = \ldots = \Psi^{(D-1)}(x), \quad x \in M$$

is equivalent to a system of linear homogeneous equations.

Step of induction

Let us suppose that functions:

$$x^a f_1^{b_1 t}(x) \dots f_{n-1}^{b_{n-1} t}(x)$$

are linear independent. If

$$0 = \sum_{a,b} C_{a,b} x^a f_1^{b_1 t}(x) \dots f_n^{b_n t}(x) =$$

$$\left(\sum_{a,b,b_n \geq 1} C_{a,b} x^a f_1^{b_1 t}(x) \dots f_n^{(b_n - 1) t}(x) \right) f_n^t(x) + \sum_{a,b,b_n = 0} C_{a,b} x^a f_1^{b_1 t}(x) \dots f_{n-1}^{b_{n-1} t}(x)$$

Step of induction

then

$$\sum_{a,b,b_n=0} C_{a,b} x^a f_1^{b_1 t}(x) \dots f_{n-1}^{b_{n-1} t}(x) \vdots f_n^t(x)$$

and

$$\sum_{a,b,b_n=0} C_{a,b} x^a f_1^{b_1 t}(x) \dots f_{n-1}^{b_{n-1} t}(x) \vdots (x - x_n)^t.$$

On the differential equations

Fuchsian equation

Let $a_1, \ldots, a_n$ be Fuchsian points of the equation

$$u^{(m)} + b_1(z)u^{(m-1)} + \ldots + b_m(z)u(z) = 0. \tag{1}$$

($z = a_i$ – Fuchsian point of (1) $\Longleftrightarrow b_j(z)$ has a pole of order $\leqslant j$ in $z = a_i$.)

Fuchs relation

Let $u_1, \ldots, u_m$ be the basis of solutions space of equations (1) and β_i^j be power exponents of solutions $u_j(z)$ in points a_i.
Then we have Fuchs inequality:

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \beta_i^j \leqslant \frac{(n-2)m(m-1)}{2}.$$

Corvaja and Zannier's bound

Theorem (Corvaja, Zannier,2013)

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.

Equations in subgroups

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

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

such that $x\in G_1$, $y\in G_2$, where G_1, G_2 are costes by subgroup G is

$$N\leqslant\left(3\sqrt[3]{2}|G|^{2/3},12\frac{|G|^2}{p}\right).$$

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.

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 (I.V., 2019)

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

$$P(x, y) = l_i, \quad i = 1, \dots, h, \tag{2}$$

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

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

On some generalization of sum-product problem

Let $P(x, y)$ be a polynomial, then let us define

$$P(A, B) = \{P(a, b) \mid a \in A,\ b \in B\}.$$

Theorem (Aleshina, I.V.)

For any n there exists $C > 0$ such that for any prime number p, (n, p)-admitted subgroup $G \in \mathbb{F}_p^*$ and a good polynomial $P(x, y)$ of degree n we have the bound

$$|P(G, G)| > C|G|^{3/2}.$$

Markoff equation

Markoff 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) $(x, y, z) \mapsto (-x, -y, z)$;
c) $(x, y, z) \mapsto (x, y, 3xy - z)$

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

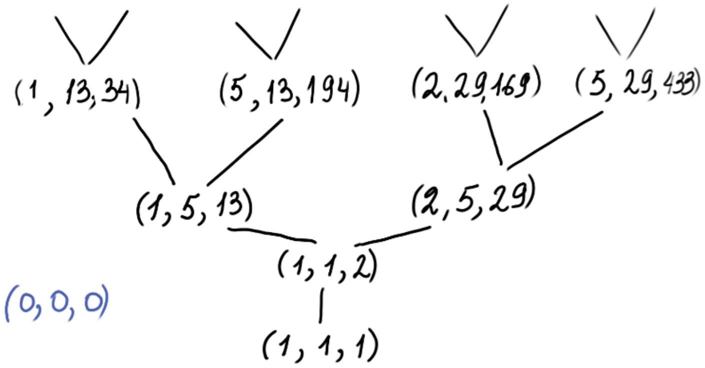

Figure: Markoff graph

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).

The 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 $D(p)$

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

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 $D(p)$

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

where c is an absolute constant.

Idea of the proof

Consider the following chain of Markoff triples

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

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

These triples (a, u_i, u_{i+1}) generate a linear recurrent chain

$$u_1, u_2, \dots \quad (u_{i+1} = 3au_i - u_{i-1})$$

with characteristic equation $\lambda^2 - 3a\lambda + 1 = 0$,

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

λ belongs to a subgroup $G \subset \mathbb{F}_{p^2}$.

Let us consider two different sequences: $u_1, u_2, \ldots, u_t$ and $u'_1, u'_2, \ldots, u'_t$, where

$$u_k = \alpha\lambda^k + \beta\lambda^{-k}, \quad u'_k = \gamma\lambda^k + \delta\lambda^{-k}.$$

The intersection of these two sequences is defined by:

$$u_k = u'_l \Longleftrightarrow \alpha\lambda^k + \beta\lambda^{-k} = \gamma\lambda^l + \delta\lambda^{-l}.$$

It is equivalent to the equation:

$$\alpha x + \frac{\beta}{x} = \gamma y + \frac{\delta}{y},$$

where $x = \lambda^k \in G$, $y = \lambda^l \in G$.

The number of solutions $(x, y) \in G \times G$ of equation

$$\alpha x^2 y - \gamma x y^2 + \beta x - \delta y = 0$$

does not exceed $C|G|^{2/3}$.

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

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

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

Theorem (W. Chen, 2020)

Every nonzero connection component of Markoff's graph $X^*(p)$ has size congruent to $0 \mod p$.

Bourgain, Gamburd, Sarnak:

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

William Chen, Strong approximation for the Markoff equation, arXiv:2011.12940 (Nov 26, 2020).

Bibliography

- S. V. Konyagin, I. E. Shparlinski, I. V. Vyugin, *Polynomial Equations in Subgroups and Applications* // arXiv:2005.05315.
- S. V. Konyagin, S. V. Makarychev, I. E. Shparlinski, I. V. Vyugin, *On the structure of graphs of Markoff triples* // Quart. Journal Math., 72:2 (2020), 637-648.
- I. V. V'yugin, *A Bound for the Number of Preimages of a Polynomial Mapping.* // Math Notes 106, 203-211 (2019).
- S. Makarychev, I. Vyugin, *Solutions of Polynomial Equations in Subgroups of* $\mathbb{F}_p$ // Arnold Math J. 5, 105-121 (2019).
- I. V. Vyugin, I. D. Shkredov, *On additive shifts of multiplicative subgroups* // Sbornik: Mathematics, 2012, 203:6, 844-863.

Thank you for your attention!!!