National Research University Higher School of Economics

Faculty of mathematics

as a manuscript

Alexander Kalmynin

Values of arithmetic functions in short intervals and random multiplicative functions

Summary of the PhD thesis
for the purpose of obtaining academic degree
Philosophy Doctor in Mathematics

Academic supervisor
Doctor of Science in Physics and Mathematics
Korolev Maxim Aleksandrovich

Moscow – 2022

Abstract

This thesis is devoted to the study of statistical properties of certain sets and arithmetical functions connected to the set of squares of integers. In the first chapter, we study the intervals between numbers which are sums of two squares. Namely, we study the quantity

$$\sum_{s_{n+1}\le x}(s_{n+1}-s_n)^{\gamma},$$

where s_n is the n-th number representable as a sum of two squares. When $\gamma \le 2$, we prove an estimate for this sum that differs from the optimal one by a factor of $(\ln x)^{O(1)}$. Such sums were studied in papers of C. Hooley [6] and V. Plaksin [10]. We present an alternative approach to this problem. More precisely, we construct a function $S(N, M)$ which is close to zero at those points N that are far away from the nearest sum of two squares. This function has an expansion into the sum of oscillating Bessel functions, which allows us to prove the required result using the "almost orthogonality" relation. The main transformation formula for $S(N, M)$ turns out to be a type of automorphy. Series analogous to $S(N, M)$ were studied in works of N.V. Kuznetsov [8] and H. Cohen [2]. Further, in Chapter 1, the connection between the distribution of sums of two squares in short intervals and "small" quadratic residues $\bmod N$ is found. Under assumption of randomness of distribution for such quadratic residues, this observation allows one to improve the Euler's elementary estimate for gaps between sums of two squares.

In the second chapter, we show that there exist infinitely many primes p for which the set of quadratic residues in $\mathbb{Z}/p\mathbb{Z}$ does not have some properties of a random set. Namely, we were able to show that for any $A > 0$ there exist infinitely many primes p for which sums of Legendre symbols of length $(\ln p)^A$ do not admit any upper bound which is non-trivial in order. To prove that, we construct a non-negative weight w_p on primes $p \in (x, 2x]$ which causes a substantial positive bias in character sums. The computations of corresponding weighted sums rely on classical results on zeros of Dirichlet L-functions and smooth numbers. The obtained lower bound contradicts the properties of random subset of $\mathbb{Z}/p\mathbb{Z}$ which were proved in the work of S.V. Konyagin and I.D. Shkredov [7]. Thus, for such primes p the quadratic residues $\bmod p$ are not a typical realization of a random set in the sense of this model.

The third chapter is dedicated to the extreme case of non-randomness of quadratic residues. In this chapter, we study the set $\mathcal{L}^+$ of all primes p for which the sums of Legendre symbols over the intervals of the form $[0, N]$ are non-negative for all $N \ge 0$. In the thesis we present a proof of explicit upper bound for the relative density of $\mathcal{L}^+$ in the set of all prime numbers. R. Baker and H. Montgomery [1] showed that the relative density of $\mathcal{L}^+$ tends to 0, our result is an effective version of their theorem. Two main ingredients of the proof is the reduction of the density estimate to the estimate of probability of non-negativity of sums of random multiplicative functions and results of A. Harper [5] on large values of random zeta-function near the critical line. As a model of Legendre symbol modulo p we use the random completely multiplicative function such

that its values at primes are independent and have the Rademacher distribution. The probability of non-negativity of the first N partial sums in this model is also equal to the proportion of Dyck prefixes among all multiplicative paths.

Chapter 1

In Chapter 1, we study the properties of the series $S(N, M)$, given by the formula

$$S(N, M) = \sum_{n \geq 0} r_2(n) J_0(2\pi\sqrt{nN}) e^{-\pi n/M},$$

where $r_2(n) = \#\{(a, b) \in \mathbb{Z}^2 : a^2 + b^2 = n\}$ and $J_0(x)$ is the Bessel function of the first kind or order 0. Next, using the obtained properties we study the gaps $s_{n+1} - s_n$. In the first section of Chapter 1 we present three different proofs of the following transformation formula for $S(N, M)$:

Theorem 1. *For all $N, M > 0$ the identity*

$$S(N, M) = Me^{-\pi NM} \sum_{n \geq 0} r_2(n) I_0(2\pi M\sqrt{Nn}) e^{-\pi nM}$$

holds. Here I_0 is the modified Bessel function of the first kind of order 0.

For the first proof, we show that the function $S(N, M)/M$ is equal to the mean value of the product $\vartheta_M(x)\vartheta_M(y)$ over the circle $x^2 + y^2 = N$, where

$$\vartheta_M(z) = \sum_{n \in \mathbb{Z}} e^{2\pi i n z - \pi n^2/M}.$$

The statement of Theorem 1 then follows from the modular transformation formula for theta-function. The second way to establish the truth of Theorem 1 is to interpret $S(N, M)$ as the Kuznetsov-Cohen series for the modular form θ^2 and then use the general result of [8]. Finally, the third approach uses the functional equation for the Dirichlet series

$$Q(s) = \sum_{(a,b) \in \mathbb{Z}^2 \setminus (0,0)} \frac{1}{(a^2 + b^2)^s}$$

and Kummer's relation for the confluent hypergeometric function

$${}_1F_1(a, b; z) = e^z {}_1F_1(b - a, b; -z), \text{ where } {}_1F_1(a, b; z) = \sum_{n=0}^{+\infty} \frac{a^{(n)} z^n}{b^{(n)} n!}.$$

These relations turn out to be useful because the Mellin transform of the function $S(Nx, M/x) - 1$ is equal to

$$M^s \pi^{-s} Q(s) \Gamma(s) {}_1F_1(s, 1; -\pi MN).$$

Denote the distance from N to the closest sum of two squares by $R(N)$. In the second section we prove that for $R(N) \geq H \geq \sqrt{\ln N}$ and $M = \frac{N \ln N}{H^2}$ the estimate

$$S(N, M) \ll N \exp\left(-\frac{\pi M R(N)^2}{4N}\right)$$

holds. This implies, for instance, that the value $S(N, M)$ is close to zero for $R(N) \geq \sqrt{2 \ln N}$ and $M \geq \frac{2N \ln N}{R(N)^2}$. After that, we use the "almost orthogonality" relation for Bessel functions to show that the function $S(N, M)$ is close to 1 in quadratic mean. Namely, we consider the integral

$$J(N, M) = \int_0^N (S(x, M) - 1)^2 dx$$

and show that for $\frac{N}{2 \ln^2 N} \geq M \geq 2 \ln N$ the bound

$$J(N, M) \ll \sqrt{NM} \ln N$$

holds. From this we easily derive the inequality

$$\mu(\{X < t \leq 2X : R(t) > 2^k (\ln X)^{3/2}\}) \ll \frac{X}{2^k},$$

which leads to the following final result:

Theorem 2. *For any* $1 \leq \gamma \leq 2$ *the relation*

$$\sum_{s_{n+1} \leq x} (s_{n+1} - s_n)^\gamma \ll x (\ln x)^{\frac{3}{2}(\gamma - 1)} \delta(x, \gamma)$$

holds. Here

$$\delta(x, \gamma) = \begin{cases} 1 \ \text{for } \gamma < 2 \\ \ln x \ \text{for } \gamma = 2. \end{cases}$$

The remaining section of Chapter 1 is devoted to the study of connection between "small" quadratic residues $\bmod N$ and distribution of sums of two squares in short intervals. Namely, let N be a large number and $\sqrt{N} \leq R \leq N$ be a parameter. Consider the set $\mathcal{R}(N, R) = \{r^2 \mod N : r \leq R\}$. Let $g(N, R)$ be the largest interval in $\mathbb{Z}/N\mathbb{Z}$ between elements of $\mathcal{R}(N, R)$. We have the following

Theorem 3. *For any* R *the inequality*

$$R(x) \ll g(2[\sqrt{x}], R) + R^4 x^{-1}$$

is true.

It is natural to conjecture that $\mathcal{R}(N,R)$ has properties of a random subset of $\mathbb{Z}/N\mathbb{Z}$ with density

$$\frac{|\mathcal{R}(N,R)|}{N}=\frac{R}{N^{1+o(1)}}.$$

In this case from Borel-Cantelli lemma one can deduce that $g(N,R)\ll\frac{N^{1+o(1)}}{R}$. We conjecture that for our range of values of R this relation always holds.

Hypothesis 1. *For any $\varepsilon>0$ and all $\sqrt{N}\le R\le N$ the inequality*

$$g(N,R)\ll\frac{N^{1+\varepsilon}}{R}$$

is true.

In particular, Hypothesis 1 implies the estimate $R(x)\ll x^{1/5+o(1)}$, which improves the best known bound $R(x)\ll x^{1/4}$.

Chapter 2

The main result of Chapter 2 is the theorem on infinitude of primes for which the character sums of logarithmic length do not admit a non-trivial upper bound. More precisely, we prove the following statement

Theorem 4. *Let $A>0$ be a real number, $x\ge x_0(A)$. Then there is at least one prime $x<p\le 2x$ such that*

$$\sum_{n\le(\ln p)^A}\left(\frac{n}{p}\right)\gg_A(\ln p)^A.$$

The first section of this chapter is a discussion of certain analogies between hypotheses of number theory and limit theorems in probability theory. In particular, we discuss an analogy between the law of the iterated logarithm and the Riemann hypothesis as well as the Cramér model [3],[4], which establishes this connection more rigorously. We also formulate the following result of S.V. Konyagin and I.D. Shkredov [7], which plays a role of Cramér model for the set of quadratic residues

Theorem 5. *Let $\mathbf{G}$ be an abelian group of order $N\to+\infty$ and $w:\mathbb{N}\to\mathbb{R}$ be an arbitrary function tending to infinity for $N\to+\infty$. Define the random subset $A\subset\mathbf{G}$ of density $1/2$ as follows: for any $g\in\mathbf{G}$ the probability of the event $g\in A$ is equal to $1/2$ and these events are mutually independent for all g. Let $A:\mathbf{G}\to\{0,1\}$ be an indicator function of the set A. Then with probability $1-o(1)$ for any two subsets $X,Y\subset\mathbf{G}$ with*

$$|X|\ge w(N)\ln N(\ln\ln N)^2\ \text{и}\ |Y|\ge w(N)\ln N(\ln\ln N)^{10}$$

we have

$$\sum_{x\in X,y\in Y}A(x+y)=\frac{1}{2}|X||Y|+o(|X||Y|).$$

In this context, Theorem 4 is an analogue of Maier's theorem [9], i.e. it demonstrates a difference between a probabilistic model and a deterministic arithmetical set. In the second section we prove Theorem 4 using results on zeros of L-functions and smooth numbers. Namely, we define a weight on primes $x < p \le 2x$ by the formula

$$w_p = \prod_{q \le M} \left(1 + \left(\frac{q}{p}\right)\right),$$

where the product is taken over primes $q \le M = (\ln x)^{1/3}$. We then consider two sums

$$S_0(x) = \sum_{x<p\le 2x} w_p \ln p \text{ and } S_1(x) = \sum_{x<p\le 2x} w_p S(p,N) \ln p.$$

Here

$$S(p,N) = \sum_{n\le N} \left(\frac{n}{p}\right), N = (\ln x)^A.$$

Since the Dirichlet series that appear in the evaluation of $S_i(x)$ can have exceptional zeros, we are not able to find asymptotic formulas for $S_0(x)$ and $S_1(x)$. It turns out, however, that their ratio admits a lower bound

$$\frac{S_1(x)}{S_0(x)} \gg \Psi(N,M) \gg_A N,$$

which gives the desired result. This relation follows from an equality between coefficients in character expansions of S_0 and S_1, $\Psi(N,M)$ here is the number of M-smooth numbers below N. Let us remind that the number is called M-smooth, if all its prime factor do not exceed M. In the final section of the second chapter we generalize the result of Theorem 4 somewhat, obtaining the bound

Theorem 6. *For any $\varepsilon > 0$ there exists $x_0(\varepsilon) > 0$ such that for $x > x_0(\varepsilon)$ for any $N \le \exp\left(\left(\frac{1}{4} - \varepsilon\right) \frac{\ln\ln^2 x}{\ln\ln\ln x}\right)$ there is a prime $p \in (x, 2x]$ with*

$$S(p,N) \ge (1+o(1))\Psi(N, 0.2c_4\sqrt{\ln x}).$$

One can use Theorem 6 to deduce the following corollaries:

Corollary 1. *For $N = \exp\left(\left(\frac{1}{4} - \varepsilon\right) \frac{\ln\ln^2 x}{\ln\ln\ln x}\right)$ and large x, between x and $2x$ there is a prime p such that*

$$S(p,N) \gg \frac{N}{(\ln x)^{1/2-\varepsilon}}.$$

Corollary 2. *Let $C > 0$ be a constant. For $N = \exp\left(\frac{C}{2} \frac{\ln\ln x \ln\ln\ln x}{\ln\ln\ln\ln x}\right)$ and $x \to +\infty$ there is a prime $p \in (x, 2x]$ such that*

$$S(p,N) \gg \frac{N}{(\ln\ln x)^{C-o(1)}}.$$

Chapter 3

The last chapter of this thesis deals with the distribution of the set of primes $\mathcal{L}^+$ — the set of p such that for all natural N the inequality

$$\left(\frac{1}{p}\right) + \ldots + \left(\frac{N}{p}\right) \geq 0$$

holds. In the first section, we present a motivation for the study of the set $\mathcal{L}^+$. Namely, it is easy to show that for any $p \in \mathcal{L}^+$ the Fekete polynomial

$$f_p(t) = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) t^n$$

is positive on the interval $(0, 1)$. This implies, for instance, that for any such prime the corresponding L-function $L\left(s, \left(\frac{\cdot}{p}\right)\right)$ has no real zeros and also that the relative density of $\mathcal{L}$ is 0. The last statement is contained in the work [1]. More formally, it means the following

Theorem 7 (R. Baker, H. Montgomery)**.** *For $x \to +\infty$ the identity*

$$|\mathcal{L}^+ \cap [1, x]| = o(\pi(x))$$

holds.

Moreover, in view of recent solution of the Erdős discrepancy problem by T. Tao [11], the modifications $\widetilde{\chi_p}(n)$ of Legendre symbols turn out to be the most positively biased "almost counterexamples" to this problem.

The second section reduces the problem of estimating $\mathcal{L}^+$ to the estimation of certain probabilistic quantity $m(x)$. To do so, we introduce the notion of multiplicative Dyck prefix: a path $\{(1, \varepsilon_n)\}_{n \leq N}$ with $\varepsilon_{nm} = \varepsilon_n \varepsilon_m$ for $nm \leq N$ and $\varepsilon_1 + \ldots + \varepsilon_n \geq 0$ for all $n \leq N$. Let now $m(x)$ be a proportion of multiplicative Dyck prefixes among all $2^{\pi(x)}$ multiplicative paths of length $[x]$. The Brun-Tichmarsh inequality and quadratic reciprocity law allow one to prove the following relation

Theorem 8. *For all $x \geq 8$ the estimate*

$$|\mathcal{L}^+ \cap [1, x]| \ll \pi(x) m(0.5 \ln x)$$

holds.

Further, the quantity $m(x)$ can be defined in probabilistic terms. Let $f(n)$ be a random completely multiplicative function for which $f(p)$ are independent random variables that have the Rademacher distribution. We call the distribution of a random variable Rademacher if

$$\mathbb{P}(X = -1) = \mathbb{P}(X = 1) = \frac{1}{2}.$$

It is easy to see that $m(x)$ is the probability of the event

$$f(1) + \ldots + f(n) \geq 0 \text{ for all } n \leq x.$$

In the final section of Chapter 3 this event is studied in terms of the random zeta-function

$$\zeta_f(s) = \sum_{n=1}^{+\infty} \frac{f(n)}{n^s}$$

and its behavior near the critical line $\operatorname{Re} s = \frac{1}{2}$. It turns out that if the partial sums $f(1) + \ldots + f(n)$ are non-negative for $n \leq x$, then with high probability the inequality

$$\max_{|t| \leq \tau} |\zeta_f(\sigma + it)| \leq (\ln x)^{1/2+o(1)}$$

is true. Here

$$\tau = \frac{1}{2}(\ln \ln N)^3 - 1, \sigma = \frac{1}{2} + 3\frac{\ln \ln N}{\ln N}.$$

On the other hand, the results of A. Harper [5] on the behavior of the maximum in the left-hand side of the inequality above show that with high probability one has

$$\max_{|t| \leq \tau} |\zeta_f(\sigma + it)| \geq (\ln x)^{1-o(1)}.$$

Quantitative forms of these arguments lead to the following theorem

Theorem 9. *For $c = 2 + \sqrt{2} - \frac{\sqrt{23+16\sqrt{2}}}{2} \approx 0.0368$ the upper bound*

$$m(N) \ll \frac{1}{(\ln N)^{c-o(1)}}$$

is true. Consequently, we have an upper bound

$$|\mathcal{L}^+ \cap [1, x]| \ll \frac{\pi(x)}{(\ln \ln x)^{c-o(1)}}.$$

Approbation of the results of the dissertation research

The results of this PhD thesis were presented at the following seminars and conferences:

1. Talk “Positivity of character sums and random multiplicative functions”, Memorial Conference on Analytic Number Theory and Applications Dedicated to the 130th Anniversary of I. M. Vinogradov (Moscow, Russia), September 2021

2. Talk “Positivity of character sums and random multiplicative functions”, Conference of International Mathematical Centers of World Level, (Sirius, Russia), August 2021

3. Talk “Random multiplicative functions and zeros of Dirichlet L-functions”, A seminar on geometric structures on manifolds, (Moscow, Russia), May 2021

4. Talk “Quadratic characters with nonnegative partial sums”, XIX International Conference Algebra, Number Theory, Discrete Geometry And Multiscale Modeling Modern Problems, Applications And Problems Of History Dedicated To The Bicentennial Of Academician P. L. Chebyshev (Tula, Russia), May 2021
5. Talk “Quadratic characters with positive partial sums”, Seminar “Contemporary Problems in Number Theory”, (Moscow, Russia), April 2021
6. Talk “Cohen-Kuznetsov construction and arithmetical functions in short intervals”, Seminar “Automorphic forms and their applications”, (Moscow, Russia), March 2019
7. Talk “On the distribution of gaps between consecutive sums of two squares”, Number Theory Seminar, TU Graz (Graz, Austria), March 2019
8. Talk “Large values of short character sums”, Uniform Distribution Theory-2018, (Luminy, Marseille, France), November 2018
9. Talk “Large values of short character sums”, Alexei Zykin memorial conference, (Moscow, Russia), June 2018
10. Talk “Large values of short character sums”,International conference “Algebra, algebraic geometry and number theory”, dedicated to the memory of academician Igor Rostislavovich Shafarevich, (Moscow, Russia), June 2018
11. Talk “Intervals between numbers which can be expressed as a sum of two squares”, XV International Conference “Algebra, Number Theory and Discrete Geometry: modern problems and applications»” dedicated to the centenary of the birth of the Doctor of Physical and Mathematical Sciences, Professor of the Moscow State University Korobov Nikolai Mikhailovich, (Tula, Russia), May 2018
12. Talk “Cohen-Kuznetsov series and intervals between numbers that are sums of two squares”, School and research conference “Modular forms and beyond”, (Saint-Petersburg, Russia), May 2018
13. Talk “Large values of character sums”, seminar “Contemporary problems in number theory”, (Moscow, Russia), December 2017
14. Talk “Intervals between numbers that are sums of two squares and Jacobi-type forms”, “Workshop:Motives, Periods and L-functions”, (Moscow, Russia), April 2017

Publications

The main results of the thesis are presented in 2 papers:

1. A. Kalmynin, “Intervals between consecutive numbers which are sums of two squares”, Mathematika, 65(4), 1018-1032, 2019
2. A.B. Kalmynin, “Large values of short character sums”, Journal of Number Theory, Volume 198, 200-210, 2019

References

[1] R.C. Baker, H.L. Montgomery, Oscillations of Quadratic L-Functions, Analytic Number Theory. Progress in Mathematics (ed. B.C. Berndt et al.), vol 85. Birkhäuser Boston, 23-40, 1990.

[2] H. Cohen, Sums involving the values at negative integers of L-functions of quadratic characters, Math. Ann. 217, 271–285, 1975

[3] H. Cramér, On the order of magnitude of the difference between consecutive prime numbers, Acta Arith., 2: 23–46, 1936.

[4] H. Cramér, Prime numbers and probability, Skand. Math. Kongr. 8, 107–115, 1935.

[5] A.J. Harper, Bounds on the suprema of Gaussian processes, and omega results for the sum of a random multiplicative function, Ann. Appl. Probab. 23 (2) 584 - 616, 2013

[6] C. Hooley, On the intervals between numbers that are sums of two squares I, Acta Math., 127, 279-297, 1971

[7] S.V. Konyagin, I.D. Shkredov, On subgraphs of random Cayley sum graphs, Eur. J. Comb. 70, 61–74, 2017.

[8] N. V. Kuznetsov, New class of identities for Fourier coefficients of modular forms, Acta Arith. 27, 1975, 505-519

[9] H. Maier, Primes in short intervals, Mich. Math. J., 32 (2), 221–225, 1985

[10] V. A. Plaksin, The distribution of numbers representable as sum of two squares, Izv. Math.,31(1):171, 1988

[11] T. Tao, The Erdős discrepancy problem, Discrete Anal.: 1-29, 2016