Российская Академиия наук

Математический институт имени В. А. Стеклова

На правах рукописи
УДК 511.321+ 511.218

Штейников Юрий Николаевич

Тригонометрические суммы по подгруппам и задачи делимости частных Ферма.

01.01.06 – математическая логика,
алгебра и теория чисел

А В Т О Р Е Ф Е Р А Т
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2015

Работа выполнена в отделе алгебры и теории чисел Федерального государственного бюджетного учреждения науки Математический институт имени В.А. Стеклова Российской академии наук

Научный руководитель:
Конягин Сергей Владимирович, член-корреспондент РАН, доктор физико-математических наук, главный научный сотрудник отдела теории функций ФГБУН Математический институт имени В.А. Стеклова Российской академии наук (специальность 01.01.01).

Официальные оппоненты:
Бояринов Роман Николаевич, доктор физико-математических наук, доцент кафедры математического анализа механико-математического факультета МГУ имени М.В. Ломоносова (специальность 01.01.06);

Вьюгин Илья Владимирович, кандидат физико-математических наук, старший научный сотрудник Лаборатории № 4 ФГБУН Институт проблем передачи информации им. А.А. Харкевича РАН (специальность 01.01.02)

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тульский государственный педагогический университет имени Л.Н. Толстого».

Защита диссертации состоится 24 декабря 2015 г. в 15 часов на заседании диссертационного совета Д 002.022.03 при Математическом институте им. В. А. Стеклова Российской академии наук по адресу 119991, Москва, ул. Губкина, д.8

С диссертацией можно ознакомиться в библиотеке Математического института им. В. А. Стеклова и на сайте
http://www.mi.ras.ru/dis/ref15/shteinikov/shteinikov_dis.pdf

Автореферат разослан "_____" ноября 2015 г.

Ученый секретарь
диссертационного совета
Д 002.022.03 при МИАН,
д. ф.-м. н. профессор

И. Д. Шкредов

Актуальность темы

Настоящая диссертация посвящена исследованию оценок тригонометрических сумм по подгруппам, их приложениям к задачам делимости частных Ферма и свойствам распределения элементов полугрупп натуральных чисел. Постановки задач, связанных с оценками тригонометрических сумм по подгруппам берут начало из работ К. Гаусса, Г.Г. Харди, Дж.Е. Литтлвуда. Впоследствии этой задачей занимались такие известные математики как А.А. Карацуба, И.Е. Шпарлинский, Д.Р. Хиф-Браун, С.В. Конягин, Ж. Бургейн, И.Д. Шкредов и другие специалисты. Этой и сходным задачам посвящен ряд работ как в России, так и за рубежом.

Тригонометрические суммы по подгруппам могут быть выражены через так называемые суммы Гаусса. Их происхождение связано с классическим результатом К. Гаусса о точном значении величин $\sum_{0\le x\le q-1} e^{2\pi i\frac{x^2}{q}}$. В работе Г.Г. Харди и Дж. Е. Литллвуда[1], были установлены нетривиальные по порядку оценки таких сумм для подгрупп меньшего размера. Оценка модуля тригонометрической суммы по подгруппе может быть получена с использованием оценок количества решений специальных сравнений. В совместной работе Д. Р. Хиф-Брауна и С.В. Конягина[2] была получена нетривиальная оценка на число решений определенного сравнения с использованием метода С.А. Степанова. Позже в работах С.В. Конягина[3], Ю.В. Малыхина[4], Б. Жоу[5], И.Д. Шкредова[6][7][8] было получено существенное развитие этого метода для задачи об оценке модуля тригонометрической суммы и других приложений.

Используя подход И. Д. Шкредова в его последних работах, в первой главе получена новая оценка количества решений специального сравнения. Это – основной результат первой главы, из которого получаются новые верхние оценки тригонометрических сумм по подгруппам в поле вычетов простого порядка, когда размер подгруппы есть p^α и α лежит в окрестности $1/3$.

В диссертации также исследуются задачи о делимости частных Ферма на простое и квадрат простого числа. Данное свойство имеет некоторые теоретико-числовые приложения[9] [10]. Первые результаты в задаче делимости частного Ферма на простое число появились в работах Х. Ленстры[9], Э. Грэнвиля [11]. С использованием тригонометриче-

---

[1] Hardy G.H., Littlewood J.E. Some problems of "Partitio Numerorum": IV The singular series in Waring's problem, Math. Z. 12 (1922), 161-188.

[2] Heath-Brown D. R., Konyagin S. V. New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum, Q. J. Math., 51:2 (2000), 221–235.

[3] Конягин С. В. Оценки тригонометрических сумм по подгруппам и сумм Гаусса, IV Международная конференция – Современные проблемы теории чисел и ее приложения, посвященная 180-летию П. Л. Чебышева и 110-летию И. М. Виноградова: Актуальные проблемы ч. III, МГУ, мехмат 2002, стр. 86–114.

[4] Малыхин Ю.В. Оценки тригонометрических сумм по модулю p^2, Фундамент. и прикл. матем., 11:6 (2005),с. 81–94.

[5] Zhou B. A note on exponential sums over subgroups of $\mathbb{Z}^*_{p^2}$ and their applications, J. Number Theory, 130:11 2010, p. 2467–2479.

[6] Shkredov I.D. On Heilbronn's exponential sum, Q. J. Math., 64:4, 2013, p. 1221–1230.

[7] Shkredov I.D. Some new inequalities in additive combinatorics, Moscow journal of combinatorics and number theory 3, 2013 p. 189–239.

[8] Shkredov I.D. On exponential sums over multiplicative subgroups of medium size, Finite fields and applications, 30, 2014, p. 72–87.

[9] Lenstra H.W. Miller's primality test, Inform. Process. Lett. 8 (1979), 86–88.

[10] Granville A. Some conjectures related to Fermat's last theorem, Number theory (Banff, 1988)pp.177–192, de Gruyter, New York, 1990

[11] Granville A. On pairs of coprime integers with no large prime factors, Expos. Math., 9(1991), p.

ских сумм и комбинаторных идей в работе Ж. Бургейна, С.В. Конягина, К. Форда, И.Е. Шпарлинского[12] были получены существенные продвижения в этой задаче. В диссертации будет усилена одна из теорем этой работы[12].

Цель работы:

– получение оценок тригонометрических сумм по подгруппам и связанных с ними некоторых величин;

– получение новых оценок наименьшего числа, не обладающего свойством делимости частного Ферма на простое число, за исключением множества простых относительной нулевой плотности;

– получение оценок количества чисел, не превосходящих заданного, вычеты по двум модулям которых принадлежат двум фиксированным множествам;

– изучение распределения на коротких интервалах элементов множеств натуральных чисел, замкнутых относительно опрерации умножения.

Методы исследования

В работе используются результаты, полученные методом С.А. Степанова, линейная алгебра, результаты о распределении гладких чисел, некоторые комбинаторные идеи.

Теоретическая и практическая ценность

Диссертация носит теоретический характер. Ее результаты могут быть использованы при исследовании распределения конечных множеств.

Научная новизна

Доказанные результаты являются новыми, полученными автором самостоятельно. Основными результатами данной работы можно считать следующие:

- Получены новые оценки тригонометрических сумм по подгруппам в поле вычетов простого порядка, размер которых есть приблизительно кубический корень из простого числа. (теоремы 4, 5);

- Получена новая верхняя оценка на первое число, не обладающего свойством делимости частного Ферма на простое число, за исключением множества простых относительной нулевой плотности. (теорема 15);

- Получены оценки количества элементов полугрупп натуральных чисел на коротких отрезках с заданным степенным распределением на больших интервалах. (теорема 10).

335–350.

[12] Bourgain J., Ford K., Konyagin S. , Shparlinskii I. On the divisibility of Fermat Quotients, Michigan J. Math. 59, 2010 p. 313–328.

Достоверность результатов

Обоснованность и достоверность результатов и выводов подтвеждена:

– обсуждением результатов исследования на российских и международных научных конференциях;

– обсуждением результатов исследования на различных научных семинарах;

– публикациями результатов исследования в рецензируемых научных изданиях, рекомендованных ВАК РФ.

Апробация работы

Результаты настоящей диссертации докладывались автором на следующих семинарах и международных конференциях.

- Современные проблемы теории чисел – под руководством С.В. Конягина и И.Д. Шкредова в Математическом институте имени В.А. Стеклова;
- Ортогональные ряды – под руководством Б.С. Кашина, С.В. Конягина на механико-математическом факультете Московского государственного университета имени М.В. Ломоносова;
- международная конференция "Компьютерная алгебра и информационные технологии", Одесса, 20–26 августа 2012 года;
- 13-ая Всероссийская молодежная школа-конференция "Лобачевские чтения – 2014", Казань, 24-29 октября 2014 года;
- международная конференция "Воронежская зимняя математическая школа. Современные методы теории функций и смежные проблемы", Воронеж, 27 января – 2 февраля 2015 года;
- международная конференция "Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения", Тула, 25–30 мая 2015 года;
- XII Международная Казанская летняя школа-конференция – "Теория функций, ее приложения и смежные вопросы Казань", 27 июня – 4 июля 2015 г.

Публикации

По теме диссертации опубликовано девять работ, в том числе три [1,3,4] - в изданиях из списка, рекомендованного ВАК РФ. Список публикаций приведен в конце автореферата.

Структура и объем работы

Диссертация изложена на 60 страницах и состоит из введения, четырех глав и списка использованных источников, включающего 37 наименований.

Краткое содержание работы

Содержание главы 1.

Основной результат первой главы – получение новых оценок тригонометрических сумм по подгруппам мультипликативным группы простого поля (теоремы 4,5).

Для натурального q мы будем обозначать через $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$, а через $\mathbb{Z}_q^*$ условимся обозначать множество обратимых элементов кольца $\mathbb{Z}_q$, p – достаточно большое простое число, если не оговорено обратное. Для целого x обозначим $e_q(x) := e^{2\pi ix/q}$. Пусть $\Gamma \subseteq \mathbb{Z}_q^*$ - некоторая подгруппа по умножению и $t := |\Gamma|$.

Определение 1. *Тригонометрическими суммами по подгруппе* Γ *будут называться величины* $S(a,\Gamma)$

$$S(a,\Gamma) := \sum_{x\in\Gamma} e_q(ax), \quad \text{где} \quad a \in \mathbb{Z}. \tag{1}$$

Важной задачей является установление нетривиальных по порядку верхних оценок для $S(\Gamma) := \max_{a\in\mathbb{Z}_q^*} |S(a,\Gamma)|$:

$$S(\Gamma) = o(|\Gamma|), q \to \infty.$$

Определение 2. *Для натурального* k *обозначим через* $T_k(\Gamma)$ *величину*

$$|\{(x_1,\dots,x_{2k}) \in \Gamma^{(2k)} : x_1+\dots+x_k = x_{k+1}+\dots+x_{2k}\}|. \tag{2}$$

Верхние оценки для $S(\Gamma)$ могут быть получены с использованием оценок для $T_k(\Gamma)$. Известна следующая теорема.

Теорема 1. *Для произвольных натуральных* k,l *справедливо неравенство:*

$$S(\Gamma) \le (qT_k(\Gamma)T_l(\Gamma))^{\frac{1}{2kl}} t^{1-1/k-1/l}.$$

Оценки такого вида установлены И.М. Виноградовым для тригонометрических сумм Вейля. Доказательство теоремы 1 можно найти в книге[13]. Приведем краткий обзор предшествующих результатов.

Пусть $\Gamma \subseteq \mathbb{Z}_p^*$ - подгруппа мультипликативной группы поля простого порядка p и $t := |\Gamma|$. На основании метода С.А. Степанова Д.Р. Хиф-Браун и С.В. Конягин установили[2], что при $t < p^{2/3}$ справедлива оценка $T_2(\Gamma) \ll t^{5/2}$. Затем С.В. Конягин[3] получил нетривиальные оценки для $T_k(\Gamma)$ для всех натуральных $k > 1$.

Теорема 2. *Для любого натурального* m *существует такое* $C(m)$*, что для любых* p,Γ *таких, что* $t < p^{2/3}$ *при* $m = 2$ *и* $t < p^{1/2}$ *при* $m > 2$*, имеет место оценка:*

$$T_m(\Gamma) \le C(m) t^{2m-2+1/2^{m-1}}.$$

И.Д. Шкредов[7] усилил этот результат для $m = 2$. Его результат формулируется так.

Теорема 3. *При* $t < p^{2/3}$ *справедлива оценка:*

$$T_2(\Gamma) \ll \min(t^{\frac{32}{13}}(\log t)^{\frac{41}{65}}, t^3 p^{-\frac{1}{3}} \log t + p^{\frac{1}{26}} t^{\frac{31}{13}} (\log t)^{\frac{8}{13}}).$$

[13] Konyagin S., Shparlinskii I. Character sums with exponential functions, Cambridge University Press, Cambridge, 1999.

В первой главе диссертации получена новая оценка для величины $T_3(\Gamma)$. Это – основной результат первой главы. Теорема формулируется так.

Теорема 4. *При $t < p^{1/2}$ справедлива следующая оценка:*

$$T_3(\Gamma) \ll t^{4\frac{3}{14}} (\log t)^{12/7}.$$

Доказательство теоремы 4 использует идеи из работ И.Д. Шкредова[7] и С.В. Конягина[3]. Из этого утверждения по теореме 1 получаются новые верхние оценки тригонометрических сумм по подгруппам в поле вычетов простого порядка в случае когда t принадлежит определенному диапазону.

Теорема 5. *Справедливы неравенства:*

$$\begin{cases} p^{\frac{182}{515}} < t < p^{\frac{182}{487}} \Rightarrow S(\Gamma) \ll p^{\frac{1}{12}} t^{\frac{1579}{2184}} (\log t)^{\frac{1067}{5460}}; \\ p^{\frac{56}{185}} < t < p^{\frac{182}{515}} \Rightarrow S(\Gamma) \ll p^{\frac{1}{18}} t^{\frac{101}{126}} (\log t)^{\frac{4}{21}}; \\ p^{\frac{28}{95}} < t < p^{\frac{56}{185}} \Rightarrow S(\Gamma) \ll p^{\frac{1}{24}} t^{\frac{1139}{1344}} (\log t)^{\frac{1}{14}} \end{cases}$$

Далее в этой главе будет получена с использованием тригонометрических сумм и других величин новая оценка для наибольшего расстояния между соседними элементами подгруппы Γ, $|\Gamma| \geq p^{\frac{1}{2}}$. Для подгруппы Γ определим

$$H_p(\Gamma) = max\{H : \exists a \in \mathbb{Z}_p^*, \exists u \in \mathbb{Z}_p : u + j \in \mathbb{Z}_p \setminus a\Gamma\}$$

Теорема формулируется так.

Теорема 6. *Для $t \geq p^{1/2}$ имеет место оценка:*

$$H_p(\Gamma) \leq p^{\frac{5977}{6552}+o(1)}, p \to \infty.$$

Отметим, что для любого натурального $g > 1$ и для почти всех простых чисел p элемент g порождает в $\mathbb{Z}_p^*$ подгруппу мощности не меньше $p^{\frac{1}{2}}$. Распределение элементов такой подгруппы в $\mathbb{Z}_p$, в частности оценки наибольших расстояний между соседними элементами, связано с разложением числа $\frac{1}{p}$ в $g-$ичной системе счисления. Теорема 6 дает результат о некотором свойстве такого разложении числа $\frac{1}{p}$. Мы отмечаем, что предыдущие результаты такого типа были установлены например в книге[13], а также в статье[14].

Также будет получена оценка тригонометрических сумм по специальной подгруппе в кольце вычетов по модулю p^3, и этот результат будет использован в четвертой главе для задачи делимости частных Ферма на квадрат простого числа.

М.З. Гараев и Х. Силлеруело[15] получили оценки количества решений сравнения $ux \equiv y \pmod p, x, y \in I, u \in U$, включающего интервал натуральных чисел I и множества с малым мультипликативным удвоением U. В четвертой главе доказывается аналогичный результат для сравнения по произвольному модулю m. Ниже сформулирована эта теорема.

---

[14] Bourgain J., Konyagin S.V., ShparlinskiI.E. Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm International Math Research Notices 2008, p. 1–29.

[15] Cilleruelo J., Garaev M. Z. Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications, http://arxiv.org/abs/1404.5070.

Теорема 7. *Пусть* $U \subseteq \mathbb{Z}_m^*$ *и* n, H *- натуральные числа, что*

$$|U| < m^{n/(2n+1)}; |U * U| < |U|^{1+o(1)}; |U|H^n < m.$$

Тогда число решений J *сравнения*

$$ux \equiv y \pmod m; 1 \le x, y \le H; u \in U$$

удовлетворяет неравенству $J \le Hm^{o(1)}$.

При доказательстве теоремы 7 используются те же идеи, что и в работе [15].

Содержание главы 2.

Во второй главе рассматривается задача о количестве натуральных чисел, не превосходящих заданного, вычеты которых по двум модулям принадлежат двум фиксированным множествам. Основным результатом второй главы является теоремы 8, 9.

Введем некоторые обозначения. Пусть даны два произвольных множества G_1 и G_2, причем $G_1 \subseteq \mathbb{Z}_{q_1}, G_2 \subseteq \mathbb{Z}_{q_2}$, q_1 и q_2 – различные натуральные числа, $q_1 < q_2, A := q_2/q_1$. Для заданного z требуется оценить сверху размер такого множества $\{n \le q_1 z, \quad n \in G_1 \pmod{q_1}, \quad n \in G_2 \pmod{q_2}\}$.

Подобная величина, когда $q_1 = p_1^2, q_2 = p_2^2$ и p_1, p_2 являются простыми числами, а G_1, G_2 являются мультипликативными подгруппами групп $\mathbb{Z}_{q_1}^*$ и $\mathbb{Z}_{q_2}^*$ размеров $p_1 - 1$ и $p_2 - 1$ соответственно, была оценена в работе[12] с использованием комбинаторных рассуждений и там же использовалась для исследования свойств делимости частных Ферма. Во второй главе рассматривается эта задача в несколько более общей формулировке.

Нам понадобятся такие величины. Для целого k обозначим через $f_1(k)$ - число решений сравнения относительно $x_1, x_2 \in G_1$

$$x_1 - x_2 \equiv kq_2 \pmod{q_1}.$$

Введем по определению

$$N_1 := \sum_{0 \le k \le \frac{z}{A}} f_1(k).$$

Аналогично, через $f_2(k)$ обозначим число решений сравнения относительно $x_1, x_2 \in G_2$

$$x_1 - x_2 \equiv kq_1 \pmod{q_2}.$$

И

$$N_2 := \sum_{0 \le k \le z} f_2(k).$$

Теперь сформулируем основной результат второй главы.

Теорема 8. *Предположим даны числа* q_1, q_2, A, z, $q_1 < q_2$, *множества* G_1, G_2 *и соответственно заданы величины* N_1, N_2. *Тогда справедлива оценка*

$$|\{n \le q_1 z, \quad n \in G_1 \pmod{q_1}, \quad n \in G_2 \pmod{q_2}\}| \ll (N_1 N_2)^{1/2}.$$

Отметим, что оценка, полученная в этой теореме, является правильной по порядку. Ниже приводится соответствующая теорема, относящаяся ко второй главе диссетрации.

Теорема 9. *Пусть целые числа* $q, m_1, m_2, z, l \to \infty$, *причем*

$$zm_1 < q/10, zm_2 < ql/10, \sqrt{\frac{\max\{m_1, m_2\}}{\min\{m_1, m_2\}}} = o(z)$$

Тогда существуют подмножества

$$G_1 \subseteq \mathbb{Z}_q, G_2 \subseteq \mathbb{Z}_{q+1}$$

такие, что выполнены следующие условия:

1) $|G_1| \asymp m_1, |G_2| \asymp m_2$,

2) число решений сравнения относительно x_1, x_2, n

$$x_1 - x_2 \equiv n \pmod{q}, 0 \le n \le z; x_1, x_2 \in G_1$$

есть $O(m_1)$.

3) число решений сравнения относительно x_1, x_2, n

$$x_1 - x_2 \equiv n \pmod{q+1}, 0 \le n \le z; x_1, x_2 \in G_2$$

есть $O(lm_2)$.

4) величина

$$|[1, qz] \bigcap \overline{G_1} \bigcap \overline{G_2}|$$

не может быть оценена величиной $O(m_1 m_2)^{1/2}$.

Мы отмечаем, что результат теоремы 8 используется далее в четвертой главе.

Содержание главы 3.

Третья глава диссертации затрагивает вопрос о распределении элементов натуральных чисел, принадлежащие множеству, замкнутому относительно операции умножения. Основной результат приведен в теореме 10

Рассматривается такая задача. Пусть q – некоторое натуральное число. Также пусть $A \subseteq \mathbb{N} \cap [1, q]$ – множество, замкнутое относительно опрерации умножения, то есть если $a_1, a_2 \in A$ и $a_1 a_2 \le q$ то $a_1 a_2 \in A$. Можно считать, что элементы A это те целые числа из отрезка $[1, q]$, которые принадлежат некоторой полугруппе натуральных чисел.

Пусть для некоторого $0 < \nu < 1$ справедливо неравенство:

$$|A| < q^{\nu} \tag{4}$$

Требуется оценить количество элементов множества A на интервале $[1, n]$, когда n растет медленнее чем любая степень q. В третьей главе диссертации получены верхние оценки для такой величины.

Например, в качестве множества A можно взять все натуральные числа, у которых вычеты по модулю q принадлежат мультипликативной подгруппе $\Gamma \subset \mathbb{Z}_q^*$. Отметим, что в работе[16] получены оценки на количество чисел не превосходящих n, которые принадлежат подгруппе порядка t группы $\mathbb{Z}_p^*$. Эти оценки содержательны, когда t мало по сравнению с p. Из результата третьей главы вытекают оценки в случае, когда t растет как степень p, а n мало. Сформулируем основной результат.

[16] Bourgain J., Konyagin S., Shparlinski I. Distribution of elements of cosets of small subgroups and applications, International Math Research Notices, 2012:9 (2012), 1968–2009.

Теорема 10. *Пусть A – множество, замкнутое относительно операции умножения, удовлетворяет условию (4) и $x = (\log q)^u$.*

1) если $\log\log x = o(\log\log q)$, то

$$\frac{f(x)}{x} \leq exp\{-(C + o(1))u(1-\nu)^2 \log(u(1-\nu)^2)\}$$

где C - некоторая абсолютная константа.

2) если $\gamma = \frac{\log\log x}{\log\log q}$ и $\log x = o(\log q)$, то

$$f(x) \leq x^{1-max\{L_\gamma, C_\gamma\}+o(1)}, q \to \infty,$$

где $L_\gamma = \gamma(\frac{1-\nu}{1-\gamma+\sqrt{(1-\gamma)^2+\gamma(1-\nu)}})^2$ и $C_\gamma = \frac{(1-\nu)^2\gamma}{4(1-\gamma)}$, если $\gamma \leq \frac{2}{3-\nu}$ и $C_\gamma = 2 - \nu - \frac{1}{\gamma}$, если $\gamma > \frac{2}{3-\nu}$.

Доказательство теоремы 10 основано на комбинаторной идее и некторых свойствах делимости и распределения гладких чисел.

Содержание главы 4.

В четвертой главе изучается свойство делимости частных Ферма на простое и квадрат простого числа. Главным результатом является оценка на первое число, не обладающего свойством делимости частного Ферма на простое число, за исключением множества простых относительной нулевой плотности (теорема 15).

Для простого p и целого a, $(a, p) = 1$, определяется частное Ферма:

$$q_p(a) := \frac{a^{p-1} - 1}{p}.$$

В четвертой главе исследуются задачи о делимости $q_p(a)$ на p и p^2. Нас будет интересовать наименьшее a, для которого не выполнено сравнение $q_p(a) \equiv 0 \pmod p$. Для простого p обозначим это число l_p.Приведем краткий обзор предшествующих результатов.

Х. Ленстра[9] доказал следующие неравенства.

Теорема 11.

$$p > 3 \Rightarrow l_p \leq 4(\log p)^2$$
$$p \to \infty \Rightarrow l_p \leq (4e^{-2} + o(1))(\log p)^2.$$

Э. Грэнвиль[11] установил такое неравенство

Теорема 12.

$$l_p \leq (\log p)^2$$

Можно, однако, ожидать гораздо более сильную оценку на l_p. Например, Ленстра предположил, что $l_p \leq 3$. В работе[12] были расмотрены три задачи о верхней оценке l_p :

1)для всех простых p,

2) для всех простых на заданном интервале, возможно, кроме одного,

3)для большинства простых на заданном интервале.

Например для задачи 2) и 3) в статье[12] были доказаны следующие теоремы.

Теорема 13. *Для каждого $\varepsilon > 0$ существует $\delta > 0$, что для всех, кроме, быть может, одного простого $p \in [Q^{1-\delta}; Q]$ выполнено неравенство :*

$$l_p \leq (\log p)^{\frac{59}{35}+\varepsilon}$$

Теорема 14. *Для каждого $\varepsilon > 0$ существует такое $\delta > 0$, что для достаточно больших Q неравенство*

$$l_p \leq (\log p)^{\frac{5}{3}+\varepsilon}$$

выполнено для всех простых $p < Q$, за исключением $O(Q^{1-\delta})$ простых.

Основной результат четвертой главы - получение новой верхней оценки для задачи 3). Соответствующий результат формулируется так.

Теорема 15. *Для каждого $\varepsilon > 0$ существует такое $\delta > 0$, что при достаточно больших Q неравенство:*

$$l_p \leq (\log p)^{\frac{3}{2}+\varepsilon}$$

выполнено для всех простых $p < Q$, за исключением $O(Q^{1-\delta})$ простых.

При доказательстве этой теоремы используются идеи доказательства теоремы 13 и результат второй главы – теорема 8.

В последней части четвертой главы будет доказана оценка о делимости частных Ферма на квадрат простого числа. Точнее, будет интересовать наименьшее a, для которого не выполнено сравнение

$$q_p(a) \equiv 0 \pmod{p^2}.$$

Для простого p обозначим это число l_p'.

В работе[12] для задачи 1) была получена верхняя оценка на l_p для всех простых p. Было доказано следующее утверждение.

Теорема 16. *Имеет место неравенство:*

$$l_p \leq (\log p)^{\frac{463}{252}+o(1)}, p \to \infty$$

С помощью более сильных результатов об энергии подгрупп, И.Д. Шкредов улучшил этот результат в работе[6]. Ниже мы приводим этот результат.

Теорема 17. *Имеет место неравенство:*

$$l_p \leq (\log p)^{\frac{7829}{4284}+o(1)}, p \to \infty$$

Новые оценки энергии подгрупп и тригонометрических сумм, полученные И.Д. Шкредовым, позволяют доказать следующую теорему о делимости частных Ферма на квадрат простого числа. Эта теорема приведена в конце четвертой главы.

Теорема 18. *Имеет место неравенство:*

$$l_p' \leq (\log p)^{\frac{2077}{1404}+o(1).}$$

При доказательстве теоремы 18 используются метод Ю.В. Малыхина[17] получения верхних оценок величин $|S(a,G)|$, $G \in \mathbb{Z}_{p^r}$, где r – произвольное. Также используются современные оценки тригонометрических сумм по модулю p^2 и величины $T_2(G)$, полученные И.Д. Шкредовым[6 8].

Заключение

В диссертации исследованы современные методы получения нетривиальных оценок тригонометрических сумм по подгруппам. В некоторых случаях получены новые верхние оценки модуля таких сумм и связанных с ними величин. Получены правильные по порядку оценки о количестве чисел, не превосходящих заданного, вычеты по двум модулям которых принадлежат двум фиксированным множествам. Этот результат использовался для вывода новой оценки первого числа, частное Ферма которого не обладает свойством делимости на простое число, за исключением множества простых относительной нулевой плотности. В диссертации установлена взаимосвязь количества элементов мультипликативных полугрупп на коротких интервалах с числом элементов на длинных интервалах.

Полученные в диссертации результаты относятся к вопросам о распределении элементов подгрупп и других множеств. Примененные методы могут быть использованы и в других подобных задачах.

Благодарности.

Соискатель считает своим приятным долгом в первую очередь поблагодарить своего научного руководителя, доктора физико–математических наук, профессора С. В. Конягина.

Работы автора по теме диссертации

[1] Штейников Ю. Н. Делимость частных Ферма. Математические заметки, 92:1 (2012), 116 –122.

[2] Штейников Ю. Н. О распределении элементов полугрупп натуральных чисел, Чебышевский сборник, 13:3 (2012), 91 –99.

[3] Штейников Ю. Н. О множестве совместных представителей вычетов по двум модулям, Труды МИАН, том 290, (2015), 202 –210.

[4] Штейников Ю. Н. Тригонометрические суммы по подгруппам и некоторые их приложения, Математические заметки, 98:4 (2015), 606 –625.

[5] Штейников Ю. Н. О распределении элементов полугрупп натуральных чисел, Материалы конференции – Компьютерная алгебра и информационные технологии, 89–90.

[17] Малыхин Ю.В. Оценки тригонометрических сумм по модулю p^r, Матем. заметки, 80:5 (2006), 793–796.

[6] Штейников Ю. Н. Оценки тригонометрических сумм по подгруппам, Материалы тринадцатой молодежной школы-конференции – Лобачевские чтения - 2014 , с. 181–183.

[7] Штейников Ю. Н. О произведениях множеств с малым мультипликативным удвоением и интервалов , Материалы конференции – Воронежская зимняя математическая школа - 2015 , с. 151.

[8] Штейников Ю. Н. О множестве совместных представителей вычетов по двум модулям, Материалы конференции – XIII Международная конференция Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения - 2015 , с. 254–255.

[9] Штейников Ю. Н. О плотности распределения полугрупп натуральных чисел , Материалы конференции – XII Международная Казанская летняя школа-конференция – Теория функций, ее приложения и смежные вопросы - 2015 , с. 491–492.

Научное издание

Штейников Юрий Николаевич

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата физико-математических наук на тему:

Тригонометрические суммы по подгруппам и

задачи делимости частных Ферма

Подписано в печать 22.10.2015
Тираж 100 экз.

Отпечатано в Математическом институте им. В.А. Стеклова РАН
Москва, 119991, ул. Губкина, 8