ФГБОУ ВПО «Московский государственный университет
имени М. В. Ломоносова»

На правах рукописи

Копьев Дмитрий Викторович

Квадратичные вычеты и невычеты и их приложения

Специальность 01.01.06 — математическая логика, алгебра и теория чисел

Автореферат

диссертации на соискание учёной степени
кандидата физико-математических наук

Москва — 2014

Работа выполнена на кафедре математического анализа механико-математического факультета ФГБОУ ВПО «Московский государственный университет имени М. В. Ломоносова».

Научный руководитель: **Чубариков Владимир Николаевич**, доктор физико-математических наук, профессор

Официальные оппоненты: **Рахмонов Зарулло Хусенович**, доктор физико-математических наук, профессор (Институт математики имени А. Джураева Академии наук Республики Таджикистан

Авдеев Иван Федорович, кандидат физико-математических наук, доцент (ГОУ ВПО «Орловский государственный университет», факультет экономики и управления)

Ведущая организация: **ФГБОУ ВПО «Московский педагогический государственный университет»**

Защита диссертации состоится 25 апреля 2014 г. в 16 ч. 45 мин. на заседании диссертационного совета Д 501.001.84, созданного на базе ФГБОУ ВПО «Московский государственный университет имени М. В. Ломоносова», по адресу: Российская Федерация, 119991, г. Москва, ГСП-1, Ленинские горы, д. 1, ФГБОУ ВПО МГУ имени М. В. Ломоносова, механико-математический факультет, аудитория 14–08.

С диссертацией можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВПО «Московский государственный университет имени М. В. Ломоносова» (г. Москва, Ломоносовский проспект, д. 27, сектор А).

Автореферат разослан 25 марта 2014 года.

Учёный секретарь диссертационного
совета Д 501.001.84, созданного на базе
ФГБОУ ВПО МГУ имени М. В. Ломоносова
доктор физико-математических наук,
профессор Александр Олегович Иванов

Общая характеристика работы

Актуальность темы

Диссертация относится к аналитической теории чисел. Одними из важнейших объектов исследования этой области математики являются квадратичные вычеты и невычеты. Если число a взаимно просто с числом m и сравнение $x^2 \equiv a \pmod{m}$ разрешимо, то a называется квадратичным вычетом по модулю m, если данное сравнение неразрешимо, то a называется квадратичным невычетом по модулю m. А. Лежандр ввел специальный символ для обозначения квадратичных вычетов и невычетов по простому модулю p, принимающий значения ± 1.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{если } a \text{ — квадратичный вычет по модулю } p; \\ -1 & \text{если } a \text{ — квадратичный невычет по модулю } p; \\ 0 & \text{если } p|a. \end{cases}$$

Само понятие квадратичного вычета было введено Л. Эйлером, хотя первые результаты для сравнений второй степени были получены еще П. Ферма. П. Ферма показал, при каких условиях на модуль p сравнение $x^2 \equiv -1 \pmod{p}$ имеет решение, т.е. при каких условиях -1 будет квадратичным вычетом. С помощью символа Лежандра его результат можно сформулировать следующим образом:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{если } p \equiv 1 \pmod 4; \\ -1 & \text{если если } p \equiv 3 \pmod 4. \end{cases}$$

а Л. Эйлер нашел критерий разрешимости сравнения $x^2 \equiv 2 \pmod{p}$. В 1801 г. К.Ф. Гауссом[1] было опубликовано первое полное доказательство квадратичного закона взаимности, сформулированного в 1783 г. Л. Эйлером[2]: если p и q — простые нечетные числа, то

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

В 1837 г. К. Якоби обобщил символ Лежандра на случай нечетного составного модуля: пусть $P = p_1 p_2 \dots p_n$ — разложение нечетного числа P на простые сомно-

[1] *C.F. Gauss* Disquisitiones Arithmeticae, Göttingen: Königlichen Gesellschaft der Wissenchaften. 1863 (original: 1801).

[2] *L. Euler* Disquisitio accuratior circa residua ex divisione quadratorum altiorumque potestatum per numeros primos relicta, Opera Omnia, I, 3, pp. 513–543 (original: 1783).

жители и a — взаимно просто с P, тогда

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_n}\right).$$

Одной из важнейших задач теории чисел является задача об оценке наименьшего квадратичного невычета n_p по модулю p. И.М.Виноградов первым получил результаты в этом направлении. Он доказал[3], что $n_p < p^{\frac{1}{2\sqrt{e}}} \ln^2 p$. В 1952 г. Г. Дэвенпорт, П. Эрдеш[4] улучшили оценку Виноградова для наименьшего квадратичного невычета, показав, что $n_p < p^{\frac{1}{2\sqrt{e}}} \ln^{\frac{1}{2\sqrt{e}}} p$. В 1957 г. Д. Берджесс[5] также улучшил результат И.М.Виноградова. Он показал, что $n_p < p^{\frac{1}{4\sqrt{e}}+\varepsilon}$.

В предположении справедливости гипотезы Римана Ю.В. Линником[6] была получена следующая оценка наименьшего квадратичного невычета $n_p = O(p^{\varepsilon})$. В 1952 г. Н.К. Анкени[7] улучшил результат Ю.В. Линника и показал, что в предположении справедливости гипотезы Римана $n_p = O(\log^2 p)$.

Принципиальным шагом в нахождении порядка наименьшего квадратичного невычета, представляющим самостоятельный интерес, является решение задачи о распределении квадратичных вычетов и невычетов на коротком промежутке. Обратим внимание, что согласно теореме Гаусса, в полной системе вычетов половина из них будет квадратичными вычетами, а другая половина — квадратичными невычетами. Задачу о распределении квадратичных вычетов и невычетов на коротком промежутке возможно меньшей длины поставил в 1914 г. И.М. Виноградов. И.М. Виноградов[8] и Г. Полиа[9] независимо друг от друга доказали, что на промежутке длины порядка $\sqrt{p} \ln p$ асимптотически поровну квадратичных вычетов и невычетов.

В 1957 г. Д. Берджесс[10] улучшил результат И.М. Виноградова, он показал, что квадратичных вычетов и невычетов будет асимптотически поровну на промежутке длины превосходящей $p^{\frac{1}{4}+\varepsilon}$.

---

[3] *И.М. Виноградов* О распределении квадратичных вычетов и невычетов // Журн. физ.-матем. об-ва при Пермском ун-те. 1919. **2,** С. 1–16.

[4] *H. Davenport, P. Erdös* The destribution of quadratic and higher residues // Publ. Math., Debrecen. 1952. **2,** №3–4, P. 252–265.

[5] *D.A. Burgess* The destribution of quadratic residues and nonresidues. // Math. 1957. **4,** №8, P. 106–112.

[6] *Ю.В. Линник* Замечание о наименьшем квадратичном невычете. Докл. АН СССР, 1942. Т. 36. №4-5, С.119–120

[7] *N.C. Ankeny* The least quadratic non-residue. // Ann. of Math. 1952. **55,** P. 65–72.

[8] *И.М. Виноградов* Sur la distribution des residues et des non residues des puissances // Журн. физ.-матем. об-ва при Пермском ун-те. 1918. **1,** С. 94–98.

[9] *G. Pólya* Über die Verteelung der quadratischen Reste und Nichtreste // Gött. Nachr. 1918. P.21–29.

[10] *D.A. Burgess* The destribution of quadratic residues and nonresidues. // Math. 1957. **4,** №8, P. 106–112.

В.Н. Чубариков сформулировал многомерный аналог задачи Виноградова на коротком промежутке о количестве вычетов $x \leq X$ таких, что

$$\left(\frac{x+a_1}{p_1}\right) = \varepsilon_1, \ldots, \left(\frac{x+a_n}{p_n}\right) = \varepsilon_n, \quad \varepsilon_i = \pm 1, i = \overline{1,n},$$

а $p_1, \ldots p_n$ — простые числа. Первые результаты принадлежат Э.К. Жимбо[11], его результат по точности отвечал результату Виноградова — Полиа. Он также получил закон распределения квадратичных вычетов и невычетов на очень коротком промежутке.

Многими авторами рассматривались задачи о распределении квадратичных вычетов и невычетов в различных числовых последовательностях.

В 1987 г. А.А. Карацуба[12], получил результат о совместном распределении вычетов и невычетов в арифметических последовательностях $p+a, p+b$, где p пробегает последовательность простых чисел таких, что $p \equiv a \pmod{q}$, где q также простое число.

В 1988 г. О.В. Попов рассмотрел задачу о распределении квадратичных вычетов и невычетов в последовательности бесквадратных чисел. Он получил следующий результат. Пусть $0 < \varepsilon \leqslant \frac{1}{2}$, $\delta = \varepsilon^2/32$, p — простое число. Тогда для $x > p^{\frac{1}{4}+2\delta+\varepsilon}$ число квадратичных вычетов по модулю p в последовательности бесквадратных чисел, не превосходящих X, равно

$$\frac{3}{\pi^2}X + O(Xp^{-\delta}).$$

Теоретико-числовые методы играют также важную роль в криптографии с открытым ключом. Ее основы были заложены в работах У. Диффи и М.Е. Хеллмана[13] и Р. Ривеста, А. Шамира и Л. Адельмана[14], последняя из которых посвящена известному протоколу RSA.

Одним из протоколов с открытым ключом является протокол «Ментальный покер», разработанный в 1976 г. также Р. Ривестом, А. Шамиром и Л. Адельманом[15].

Важнейшим свойством символов Лежандра и Якоби является квадратичный за-

[11] *Э.К. Жимбо* О распределении значений модулей неполных сумм Гаусса // Вестник Моск. ун-та. Сер. 1, Математика. Механика. 2001. №2. С.66–67.

[12] *А.А. Карацуба* О суммах характеров с простыми числами // Докл. АН СССР. 1970. Т.190. №3.

[13] *M.E. Hellman, W.Diffie* New directions in cryptography // IEEE Transaction on Information Theory, vol. 22, 1976, p. 644–654.

[14] *R.L. Rivest, A. Shamir, L. Adleman.* A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. New York, NY, USA: ACM, 1978. V. 21. №2. 1978. P. 120–126.

[15] *R.L. Rivest, A. Shamir, L. Adleman.* Mental poker // Mathematical Gardner. 1981. P. 37–43.

кон взаимности. Одно из возможных доказательств этого факта использует свойства сумм Гаусса (см., например, книгу[16]).

Проблема вычисления одномерных сумм Гаусса хорошо известна и неоднократно рассматривалась в литературе. Так, даже в учебной литературе[17] рассмотрено применение формулы суммирования Пуассона к простому случаю, когда коэффициент при квадратичном члене равен единице. В других монографиях[18] рассмотрена та же ситуация, и предложена другая процедура их вычисления, основанная на общих свойствах полных сумм и символов Якоби. Многомерный случай вычисления бесконечных экспоненциальных сумм рассматривался у Э. Ландау[19], однако используемая в этой работе процедура не может быть напрямую применена к рассматриваемой задаче для конечной суммы Гаусса.

Одним из направлений теории чисел являются также исследования по теории моментов арифметических функций и нахождение законов распределения сумм Гаусса, Клоостермана, сумм характеров и т. д. В этом направлении стоит отметить результаты В.Н. Чубарикова и Э.К. Жимбо[20,21], а также В.Н. Чубарикова и Р.Н. Бояринова[22], И.С. Тимергалиева и Р.Н. Бояринова [23].

Цель и задачи исследования

Получение новых оценок для задач о распределении квадратичных вычетов и невычетов в различных совместно распределенных последовательностях (арифметических прогрессиях и последовательности бесквадратных чисел). Получение арифметических подходов к атаке на один криптографический протокол. Вычисление точного значения многомерной суммы Гаусса в особом случае. Получение закона распределения значений очень коротких усредненных сумм Гаусса.

---

[16] *Г. Девенпорт* Высшая арифметика. Введение в теорию чисел. — М.: Наука. Гл. ред. физ.-мат. лит. — 1965. — 176 с.

[17] *Г.И. Архипов, В.А. Садовничий, В.Н. Чубариков* Лекции по математическому анализу. — М.: Дрофа. — 2003. — 640 с.

[18] *Н.М. Коробов* Тригонометрические суммы и их приложения. — М.: Наука. Гл. ред. физ.-мат. пит.— 1989 —240 с.

[19] *E. Landau* Handbuch der Lehre von der Verteilung der Primzahlen. Teubner. 1909. 961 p.

[20] *Э.К. Жимбо, В.Н. Чубариков* Об распределении арифметических функций по простому модулю// Дискр. матем. 2001. №2. С.47–58.

[21] *Э.К. Жимбо, В.Н. Чубариков* Об асимптотических распределениях значений арифметических функций // Доклады академии наук. Т. 377, №2, 2001. С. 156–157.

[22] *Р.Н. Бояринов, В.Н. Чубариков* О распределении значений функций на последовательности Фибоначчи // Доклады академии наук. Т. 379, №1, 2001. С. 9–11.

[23] *И.С. Тимергалиев, Р.Н. Бояринов* О распределении значений неполных сумм Гаусса // Чебышевский сб. 2013. **14**:3. С. 127–133.

Методы исследования

В работе применяются методы аналитической теории чисел, комплексного анализа и теории вероятностей.

Научная новизна

Результаты диссертации являются новыми и получены автором самостоятельно. Они состоят в следующем:

1. Получены законы распределения символов Якоби в последовательностях по системе различных попарно взаимно простых модулей по непрерывному промежутку и по последовательности бесквадратных чисел. Получена оценка суммы Гаусса специального вида.

2. Арифметическим методом обнаружены уязвимости одного криптографического протокола.

3. Вычислено точное значение многомерной суммы Гаусса. Найден закон распределения очень коротких усреднённых сумм Гаусса.

Теоретическая и практическая ценность

Диссертация имеет теоретический характер. Результаты диссертации представляют интерес для специалистов в области аналитической теории чисел и могут найти применение в теории чисел.

Апробация работы

Результаты диссертации докладывались на следующих научно-исследовательских семинарах:

1. Научно-исследовательский семинар «Аналитическая теория чисел» под руководством проф. Г. И. Архипова и проф. В. Н. Чубарикова в 2012—2013 гг.

2. Семинар «Арифметические функции» под руководством проф. В. Н. Чубарикова и доц. Р. Н. Бояринова в 2011—2012 гг.

3. Семинар «Арифметические методы в криптографии» под руководством проф. В. Н. Чубарикова и проф. М. П. Минеева в 2010—2011 гг.

Результаты диссертации докладывались также на следующих международных научных конференциях:

1. VII Международная научная конференция «Алгебра и теория чисел: современные проблемы и приложения», посвященная памяти профессора Анатолия Алексеевича Карацубы (г. Тула, 11—16 мая 2010 г.).

2. Международная научная конференция «Современные проблемы теории функций и дифференциальных уравнений», посвященная 85-летию академика Михайлова Л. Г. (г. Душанбе, 17—18 июня 2013 г.)

Публикации

Основные результаты диссертации опубликованы в 5 работах автора (список приведён в конце автореферата), из них 2 работы — в журналах, включённых Высшей аттестационной комиссией России в список изданий, рекомендуемых для опубликования основных научных результатов диссертаций на соискание ученой степени кандидата и доктора наук.

Структура и объем диссертации

Диссертация состоит из введения, трёх глав и списка литературы, насчитывающего 45 наименований. Объём диссертации составляет 71 страницу.

Краткое содержание работы

Введение содержит исторический обзор результатов по теме диссертации и формулировки основных теорем, доказанных в диссертации.

В **первой главе** «Распределении значений символов Якоби в последовательностях по системе различных модулей» рассмотрена задача о распределении квадратичных вычетов и невычетов в совместно распределенных последовательностях по различным модулям. Получено улучшение результата Э.К. Жимбо. Результат по точности отвечает результату Д. Берджесса.

Пусть $Q = m_1 m_2 \dots m_n$, где $m_1, m_2, \dots, m_n$ — попарно взаимно простые числа. Обозначим символом $V(X)$ количество значений $x \le X$, удовлетворяющих соотношениям

$$\left(\frac{x+a_1}{m_1}\right) = \varepsilon_1, \dots, \left(\frac{x+a_n}{m_n}\right) = \varepsilon_n.$$

Теорема 1.5. *Пусть* $Q = m_1 m_2 \dots m_n$, *где* $m_1, m_2, \dots, m_n$ — *попарно взаимно простые бескубические числа. Тогда для любого фиксированного* ε *такого, что* $0 < \varepsilon < 0,0625$, *при* $Q^{\frac{1}{4}+\omega} < X \leqslant Q$, *где* $\omega = \frac{3\sqrt{\varepsilon}}{2-4\sqrt{\varepsilon}}$, *величина*

$$V(X) = \frac{X}{2^n} + W(X),$$

где $|W(X)| \ll_\varepsilon XQ^{-\frac{\varepsilon}{4}}$.

Доказательство этой теоремы существенно опирается на следующую оценку произведений символов Якоби.

Теорема 1.1. *Пусть* $m_1, m_2, \dots, m_k$ — *попарно взаимно простые бескубические числа,* $Q = m_1 m_2 \dots m_k$. *Далее пусть*

$$S = \sum_{x \leq X} \left(\frac{x+a_1}{m_1}\right)\left(\frac{x+a_2}{m_2}\right)\dots\left(\frac{x+a_k}{m_k}\right),$$

тогда для любого фиксированного ε *такого, что* $0 < \varepsilon < 0,0625$, *при* $Q^{\frac{1}{4}+\omega} < X \leqslant Q$, *где* $\omega = \frac{3\sqrt{\varepsilon}}{2-4\sqrt{\varepsilon}}$, *величина* $|S| \ll_\varepsilon XQ^{-\varepsilon}$.

Также получен более общий результат для произвольных взаимно простых модулей, но для промежутка большей длины, чем в теореме 1.1.

Теорема 1.6. *Пусть* $Q = m_1 m_2 \dots m_n$, *где* $m_1, m_2, \dots, m_n$ — *попарно взаимно простые числа, причем по крайней мере для одного из чисел* m_i *найдется такое простое* p, *что* $p^3 | m_i$. *Тогда для любого фиксированного* ε *такого, что* $0 < \varepsilon < 0,15625$, *при* $Q^{\frac{1}{4}+\omega} < X \leqslant Q$, *где* $\omega = 4\varepsilon$, *величина*

$$V(X) = \frac{X}{2^n} + W(X),$$

где $|W(X)| \ll_\varepsilon XQ^{-\frac{3\varepsilon}{8}}$.

Пусть $F(X)$ — количество бесквадратных значений $x \leq X$, удовлетворяющих соотношениям

$$\left(\frac{x+a_1}{m_1}\right) = \varepsilon_1, \dots, \left(\frac{x+a_n}{m_n}\right) = \varepsilon_n.$$

Теорема 1.7. *Пусть* $Q = m_1 m_2 \dots m_n$, *где* $m_1, m_2, \dots, m_n$ — *попарно взаимно простые бескубические числа. Тогда для любого фиксированного* ε *такого, что* $0 < \varepsilon < 0,0533$, *при* $Q^{\frac{1}{4}+\omega+2\varepsilon} < X \leqslant Q$, *где* $\omega = \frac{3\sqrt{\varepsilon}}{2-4\sqrt{\varepsilon}}$, *величина*

$$F(X) = \frac{6}{\pi^2}\frac{X}{2^n} + W(X),$$

где $|W(X)| \ll_\varepsilon XQ^{-\frac{\varepsilon}{4}}$.

Теорема 1.8. *Пусть* $Q = m_1 m_2 \dots m_n$, *где* $m_1, m_2, \dots, m_n$ — *попарно взаимно простые числа, причем по крайней мере для одного из чисел* m_i *найдется такое простое* p, *что* $p^3 | m_i$. *Тогда для любого фиксированного* ε *такого, что* $0 < \varepsilon < \frac{5}{48}$, *при* $Q^{\frac{3}{8}+\rho} < X \leqslant Q$, *где* $\rho = 6\varepsilon$, *величина*

$$F(X) = \frac{6}{\pi^2}\frac{X}{2^n} + W(X),$$

где $|W(X)| \ll_\varepsilon XQ^{-\frac{3\varepsilon}{8}}$.

Вторая глава диссертации «Уязвимость протокола „Ментальный покер”» посвящена возможности атаки этого протокола, существенно использующей свойства квадратичных вычетов и невычетов.

Приведем краткое описание атакуемого протокола.

Два абонента $\mathcal{A}$ и $\mathcal{B}$ раздают карты α, β и γ следующим образом: $\mathcal{A}$ и $\mathcal{B}$ получают по одной карте, и одна карта отправляется в прикуп. При этом должны соблюдаться следующие условия:

1) каждый игрок может получить любую из трех карт α, β и γ с равными вероятностями;

2) каждый игрок знает только свою карту;

3) в случае спора можно пригласить судью и выяснить кто прав, а кто виноват;

4) при раздаче карт никто не знает, кому какая карта досталась (хотя раздача происходит по открытой линии связи и наблюдатель $\mathcal{E}$ может записать все передаваемые сообщения).

Участники выбирают некоторое большое простое число p и три различных случайных числа α_1, β_1 и γ_1, которыми кодируются карты α, β и γ соответственно, причем эта информация известна всем. Затем $\mathcal{A}$ выбирает случайным образом число c_A, взаимно простое с $p-1$, и строит такое число d_A, что $c_A d_A \equiv 1 \pmod{p-1}$. Игрок $\mathcal{B}$ также аналогичным образом строит пару чисел c_B и d_B, такую, что $c_B d_B \equiv 1 \pmod{p-1}$. Эти числа каждый игрок держит в секрете.

1-й шаг. Абонент $\mathcal{A}$ вычисляет числа $u_1 \equiv \alpha_1^{c_A} \pmod{p}$; $u_2 \equiv \beta_1^{c_A} \pmod{p}$; $u_3 \equiv \gamma_1^{c_A} \pmod{p}$ и высылает их игроку $\mathcal{B}$, предварительно перемешав их случайным образом.

2-й шаг. Абонент $\mathcal{B}$ получает три числа, выбирает случайно одно из полученных чисел, например u_2, и отправляет его абоненту $\mathcal{A}$ по линии связи. Это и будет та карта, которая достанется $\mathcal{A}$ в процессе раздачи. Абонент $\mathcal{A}$, получив это сообще-

ние, может вычислить $u_2 \equiv u_1^{d_A} \equiv \beta_1^{c_A d_A} \equiv \beta_1 \pmod p$, то есть он узнает, что ему досталась карта β.

3-й шаг. Абонент $\mathcal{B}$ вычисляет для оставшихся двух чисел $v_1 \equiv u_1^{c_B} \pmod p$, $v_3 \equiv u_3^{c_B} \pmod p$ и отправляет их абоненту $\mathcal{A}$.

4-й шаг. Абонент $\mathcal{A}$ выбирает случайно одно из полученных чисел, например v_1, вычисляет число $w_1 \equiv v_1^{d_A} \pmod p$ и отправляет это число обратно $\mathcal{B}$. Абонент $\mathcal{B}$ вычисляет число $z_1 \equiv w_1^{d_B} \pmod p$ и узнает свою карту $z \equiv w_1^{d_B} \equiv v_1^{d_A d_B} \equiv u_1^{c_B d_B d_A} \equiv \alpha_1^{c_A c_B d_A d_B} \equiv \alpha_1 \pmod p$. Карта, соответствующая v_3, отправляется в прикуп.

Во второй главе диссертации показано, что при неудачном выборе чисел, кодирующих карты, возможно отследить перемещение карт по столу. Также показано, что даже в случае правильного выбора кодирующих чисел абонент $\mathcal{A}$ может попытаться обмануть абонента $\mathcal{B}$, и в случае успеха он с вероятностью $\frac{2}{3}$ будет знать распределение карт на игровом столе.

Третья глава диссертации «О вычислении суммы Гаусса специального вида» посвящена вычислению полной суммы Гаусса с квадратичной формой в показателе степени, у которой коэффициенты взаимно просты со знаменателем. Доказана следующая теорема.

Теорема 3.1. *Пусть Q — нечетное число, коэффициенты квадратичной формы $T(x_1, \ldots, x_n)$ попарно взаимно просты с Q, D — определитель матрицы квадратичной формы $T(x_1, \ldots, x_n)$, и*

$$G_T(Q) = \sum_{x_1=1}^{Q} \cdots \sum_{x_n=1}^{Q} e\left(\frac{T(x_1, \ldots, x_n)}{Q}\right),$$

тогда

$$G_T(Q) = i^{n\left(\frac{Q-1}{2}\right)^2} \sqrt{Q^n} \left(\frac{D}{Q}\right).$$

Доказана также следующая теорема о распределении значений коротких усредненных сумм Гаусса.

Теорема 3.2. *Пусть*

$$S_h(x) = \sum_{n=x+1}^{x+h} \sum_{m=x+1}^{x+h} \chi(n+m) e\left(\frac{a(n+m)}{p}\right),$$

где p — простое, $(a,p)=1$, числа x, h — целые в пределах $0 \leqslant x < p$ и $0 < h < p$, а χ — комплексный характер по модулю p.

Тогда при $p \to +\infty$, поскольку $h(p) \to +\infty$ и $\frac{\log h}{\log p} \to 0$ величина $\xi = \xi(h,p) = \left|\frac{S_h(x)}{h^{\frac{3}{2}}}\right|^2$ асимптотически имеет экспоненциальное распределение с параметром $\lambda = \frac{3}{2}$.

Благодарности

Автор приносит благодарность научному руководителю профессору В. Н. Чубарикову за постановку задач и внимание к работе.

Публикации автора по теме диссертации

[1] Копьев Д. В. *О вычетах и невычетах по системе модулей* // Докл. АН. Т. 453, № 2, 2013. С. 136—137.

[2] Копьев Д. В., Минеев М. П., Чубариков В. Н. *О некоторых арифметических подходах к задачам криптографии* // Современные проблемы математики и механики. Том 3. Математика. Выпуск 1. Под редакцией Т. П. Лукашенко и В. Н. Чубарикова. М.: Изд-во МГУ, 2009. 369 с. С. 55—64.

[3] Копьев Д. В. *Об уязвимости одного криптографического протокола.* Вестник Моск. ун-та. Серия 1. Математика. Механика. № 1. 2009. С. 55—56.

[4] Копьев Д. В. *О «Ментальном покере»* // Материалы VII Международной научной конференции «Алгебра и теория чисел: современные проблемы и приложения», посвящённая памяти профессора Анатолия Алексеевича Карацубы. Тула: Изд-во ТГПУ имени Л. Н. Толстого. С. 104.

[5] Копьев Д. В. *О распределении значений символов Якоби в последовательностях по системе различных модулей* // Материалы международной научной конференции «Современные проблемы теории функций и дифференциальных уравнений», посвященной 85-летию академика АН Республики Таджикистан Михайлова Л. Г. (Душанбе, 17—18 июня 2013 г.). С. 75—78.

В работе [2] Д. В. Копьеву принадлежит параграф «Взлом одного криптопротокола с помощью арифметических функций».