Московский государственный университет имени М. В. Ломоносова

Механико-математический факультет

на правах рукописи

УДК 511.35

Копьев Дмитрий Викторович

Квадратичные вычеты и невычеты и их приложения

01.01.06 — математическая логика, алгебра и теория чисел

диссертация на соискание ученой степени

кандидата физико-математических наук

Научный руководитель:

доктор физико-математических наук,

профессор В. Н. Чубариков

Москва — 2013

Содержание

Используемые обозначения

В диссертации используются следующие обозначения:

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

— символ Лежандра;

$\left(\frac{a}{Q}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_n}\right)$ — символ Якоби, где $Q = p_1 p_2 \dots p_n$, а $p_1, p_2, \dots, p_n$ — простые числа;

$e(\alpha) = e^{2\pi i\alpha}$;

$[x]$ — целая часть вещественного числа x;

$\{x\} = x - [x]$ — дробная часть числа x;

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1; \\ (-1)^r, & \text{если } n = p_1 p_2 \dots p_r,\ p_i \text{ — простые числа;} \\ 0, & \text{если } p^2 \mid n \text{ для некоторого простого числа } p \end{cases}$$

— функция Мёбиуса;

$$\mu^2(n) = \begin{cases} 1, & \text{если } n \text{ бесквадратное;} \\ 0, & \text{в противном случае} \end{cases}$$

— характеристическая функция множества бесквадратных чисел (чисел, не делящихся на квадрат простого числа).

Записи $f(x) = O(g(x))$ (символ Э. Ландау) и $f(x) \ll g(x)$ (символ И.М. Виноградова) при $x \to \infty$ означают, что существуют положительные числа C и x_0, такие, что $|f(x)| \leqslant Cg(x)$ при $x \geqslant x_0$.

Введение

Настоящая 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 [2] было опубликовано первое полное доказательство квадратичного закона взаимности, сформулированного в 1783 г. Л. Эйлером [1]: 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 сомножители 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 [8], что $n_p < p^{\frac{1}{2\sqrt{e}}} \ln^2 p$. В 1952 г. Г. Дэвенпорт, П. Эрдеш [34] 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 [30] 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 [22] была получена следующая оценка наименьшего квадратичного невычета $n_p = O(p^{\varepsilon})$. В 1952 г. Н.К. Анкени [29] 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 [7] и Г. Полиа [38] 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 [30] улучшил результат И.М.Виноградова, он пока-

зал, что квадратичных вычетов и невычетов будет асимптотически поровну на промежутке длины превосходящей $p^{\frac{1}{4}+\varepsilon}$.

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 [12], его результат по точности отвечал результату Виноградова — Полиа. Он также получил закон распределения квадратичных вычетов и невычетов на очень коротком промежутке.

В главе 1 «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.

Обозначим символом $V(X)$ количество значений $x \leq X$, удовлетворяющих соотношениям

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

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

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

В 1987 г. А.А. Карацуба [17], 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 [24] 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

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

В настоящей диссертации рассматривается следующее обобщение этой задачи. Пусть $Q = m_1 m_2 \dots m_n$, где $m_1, m_2, \dots, m_n$ — попарно взаимно простые

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

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

Теорема 1.7 *Пусть* $Q = m_1 m_2 \ldots m_n$, *где* $m_1, m_2, \ldots, m_n$ — *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* $Q = m_1 m_2 \ldots m_n$, *где* $m_1, m_2, \ldots, m_n$ — *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 $|W(X)| \ll_\varepsilon XQ^{-\frac{3\varepsilon}{8}}$.

Теоретико-числовые методы играют также важную роль в криптографии с открытым ключом. Ее основы были заложены в работах У. Диффи и

М.Е. Хеллмана [36] и Р. Ривеста, А. Шамира и Л. Адельмана [39], 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 [40]. Он состоит в следующем.

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 сообщение, 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.

Вторая глава диссертации «Уязвимость протокола „Ментальный покер”» посвящена возможности атаки на этот протокол, существенно использующей

свойства квадратичных вычетов и невычетов. Показано, что при неудачном выборе чисел, кодирующих карты, можно 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.

Важнейшим свойством символов Лежандра и Якоби является квадратичный закон взаимности. Одно из возможных доказательств этого факта использует свойства сумм Гаусса (см., например, книгу [11]).

Проблема вычисления одномерных сумм Гаусса хорошо известна и неоднократно рассматривалась в литературе. Так, в книге [4] рассмотрено применение формулы суммирования Пуассона применительно к простому случаю, когда коэффициент при квадратичном члене равен единице. В монографии [20] рассмотрена та же ситуация, и предложена другая процедура их вычисления, основанная на общих свойствах полных сумм и символов Якоби.

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 мат-*

рицы квадратичной формы $T(x_1, \ldots, x_n)$, *и*

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

тогда

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

Многомерный случай вычисления бесконечных экспоненциальных сумм рассматривался в [37], однако используемая в этой работе процедура не может быть напрямую применена к рассматриваемой в диссертации задаче для конечной суммы Гаусса.

Одним из направлений теории чисел являются 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 [12, 13, 14], а также В.Н. Чубарикова и Р.Н. Бояринова [5], И.С. Тимергалиева и Р.Н. Бояринова [26].

В третьей главе настоящей диссертации доказана 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* $\lambda = \frac{3}{2}$*.*

Основные результаты, полученные в настоящей диссертации, опубликованы в работах автора [41, 42, 43, 44, 45].

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

Глава 1

Распределении значений символов Якоби в последовательностях по системе различных модулей

1.1 Вспомогательные леммы и утверждения

Для доказательства основной теоремы этой главы нам потребуется ряд вспомогательных утверждений, которые мы будем использовать также и в других главах диссертации.

Лемма 1.1 (Китайская теорема об остатках) *Пусть целые числа* $m_1, m_2, \ldots, m_r$ *попарно взаимно просты и* $M = m_1 m_2 \ldots m_r$. *Тогда система сравнений*

$$\begin{cases} a \equiv a_1 \pmod{m_1} \\ \vdots \\ a \equiv a_r \pmod{m_r} \end{cases}$$

имеет единственное решение $a \pmod{M}$, *т.е. можно указать ровно один класс вычетов* $x \equiv a \pmod{M}$, *удовлетворяющий этой системе сравнений.*

Лемма 1.2 (теорема Берджесса) *Пусть* $Q \in \mathbb{N}$ *и* χ *— неглавный характер Дирихле по модулю* Q. *Пусть* ε *— фиксированное положительное число и* $r \in \mathbb{N}$. *Далее пусть* Q *— бескубическое число или* $r = 2$, *для любых целых* N *и* H $(H > 0)$

$$S_X(N) = \sum_{x=N+1}^{N+X} \chi(x) \ll_{\varepsilon,r} X^{1-1/r} Q^{(r+1)/4r^2+\varepsilon}.$$

Лемма 1.3 *Для количества бесквадратных чисел, не превосходящих* N *имеет место асимптотическая формула*

$$Q(N) = \sum_{n \le N} \mu^2(n) = \frac{6}{\pi^2} N + O(\sqrt{N}).$$

1.2 Оценки вспомогательных сумм

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 $|S| \ll_\varepsilon XQ^{-\varepsilon}$.

Доказательство. Рассмотрим следующую систему сравнений:

$$\begin{cases} a \equiv a_1 \pmod{m_1}; \\ \vdots \\ a \equiv a_k \pmod{m_k}. \end{cases}$$

По китайской теореме об остатках эта система разрешима и $\left(\frac{x+a_1}{m_1}\right) = \left(\frac{x+a}{m_1}\right), \dots, \left(\frac{x+a_k}{m_k}\right) = \left(\frac{x+a}{m_k}\right)$, а значит наша сумма S может быть представлена в следующем виде:

$$S = \sum_{x \leq X} \left(\frac{x + a}{m_1}\right) \left(\frac{x + a}{m_2}\right) \dots \left(\frac{x + a}{m_k}\right) = \sum_{x \leq X} \left(\frac{x + a}{Q}\right).$$

Поскольку Q — произведение k попарно взаимно простых бескубических чисел, следовательно, Q — число бескубическое, а значит к S можно применить

утверждение леммы 1.2.

$$S \ll_{\varepsilon,r} X^{1-1/r} Q^{(r+1)/4r^2+\varepsilon}.$$

Для получения нетривиальной оценки потребуем $X^{1-1/r} Q^{(r+1)/4r^2+\varepsilon} < X$. Тогда получим

$$X > Q^{(r+1)/4+\varepsilon r} = Q^{1/4+\frac{\sqrt{\varepsilon}}{2}\left(\frac{1}{2\sqrt{\varepsilon}r}+2\sqrt{\varepsilon}r\right)} \geq Q^{1/4+\sqrt{\varepsilon}},$$

причем, по неравенству Коши, значение $Q^{1/4+\sqrt{\varepsilon}}$ будет приниматься только при $r = \frac{1}{2\sqrt{\varepsilon}}$.

Поскольку в лемме 1.2 допустимы только натуральные значения r положим $r = \left[\frac{1}{2\sqrt{\varepsilon}}\right]$, где $[x]$ — целая часть числа x.

Тогда

$$S \ll_{\varepsilon} X^{\left(1-\frac{1}{\left[\frac{1}{2\sqrt{\varepsilon}}\right]}\right)} Q^{\frac{\left(\left[\frac{1}{2\sqrt{\varepsilon}}\right]+1\right)}{4\left[\frac{1}{2\sqrt{\varepsilon}}\right]^2}+\varepsilon} = XQ^{-\frac{1}{\left[\frac{1}{2\sqrt{\varepsilon}}\right]}\frac{\ln X}{\ln Q}+\frac{\left(\left[\frac{1}{2\sqrt{\varepsilon}}\right]+1\right)}{4\left[\frac{1}{2\sqrt{\varepsilon}}\right]^2}+\varepsilon}.$$

Положив $X = Q^{\frac{1}{4}+\omega}$ и потребовав, чтобы правая часть последнего равенства была меньше $XQ^{-\varepsilon}$, получим

$$-\frac{1}{\left[\frac{1}{2\sqrt{\varepsilon}}\right]}\left(\frac{1}{4}+\omega\right)+\frac{\left(\left[\frac{1}{2\sqrt{\varepsilon}}\right]+1\right)}{4\left[\frac{1}{2\sqrt{\varepsilon}}\right]^2}+\varepsilon < -\varepsilon.$$

Отсюда имеем

$$\omega > \frac{1}{4\left[\frac{1}{2\sqrt{\varepsilon}}\right]} + 2\varepsilon\left[\frac{1}{2\sqrt{\varepsilon}}\right] = \frac{1}{4\left(\frac{1}{2\sqrt{\varepsilon}} + \left\{\frac{1}{2\sqrt{\varepsilon}}\right\}\right)} + 2\varepsilon\left(\frac{1}{2\sqrt{\varepsilon}} + \left\{\frac{1}{2\sqrt{\varepsilon}}\right\}\right) =$$

$$= \frac{\sqrt{\varepsilon}}{2 - 4\sqrt{\varepsilon}\left\{\frac{1}{2\sqrt{\varepsilon}}\right\}} + \sqrt{\varepsilon} + 2\varepsilon\left\{\frac{1}{2\sqrt{\varepsilon}}\right\},$$

где $\{x\}$ — дробная часть числа x.

Поскольку $\{x\} < 1$, при $\varepsilon < \frac{1}{4}$ имеем, $2 - 4\sqrt{\varepsilon}\left\{\frac{1}{2\sqrt{\varepsilon}}\right\} > 2 - 4\sqrt{\varepsilon}$. Следовательно

$$\frac{\sqrt{\varepsilon}}{2 - 4\sqrt{\varepsilon}\left\{\frac{1}{2\sqrt{\varepsilon}}\right\}} + \sqrt{\varepsilon} + 2\varepsilon\left\{\frac{1}{2\sqrt{\varepsilon}}\right\} < \frac{\sqrt{\varepsilon}}{2 - 4\sqrt{\varepsilon}} + \sqrt{\varepsilon} + 2\varepsilon =$$

$$= \frac{3\sqrt{\varepsilon} - 8\varepsilon\sqrt{\varepsilon}}{2 - 4\sqrt{\varepsilon}} < \frac{3\sqrt{\varepsilon}}{2 - 4\sqrt{\varepsilon}}.$$

Тогда, если $\omega > \frac{3\sqrt{\varepsilon}}{2-4\sqrt{\varepsilon}}$, $|S| < XQ^{-\varepsilon}$.

Так как по условию $Q^{\frac{1}{4}+\omega} < Q$, поэтому $\omega < \frac{3}{4}$, следовательно для получения допустимых значений ω должно быть выполнено следующее неравенство

$$\frac{3\sqrt{\varepsilon}}{2 - 4\sqrt{\varepsilon}} < \frac{3}{4}.$$

Оно выполняется при $0 < \varepsilon < 0,0625$.

Теорема доказана.

Теорема 1.2 *Пусть $m_1, m_2, \ldots, m_k$ — попарно взаимно простые числа,*

$Q = m_1 m_2 \dots m_k$, $X \leq Q$, причем по крайней мере для одного из чисел m_i найдется такое простое p, что $p^3 | m_i$. 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 $0 < \varepsilon < 0,15625$, при $Q^{\frac{3}{8}+\omega} < X \leqslant Q$, где $\omega = 4\varepsilon$, величина $|S| \ll_\varepsilon XQ^{-\varepsilon}$.

Доказательство. Рассмотрим следующую систему сравнений:

$$\begin{cases} a \equiv a_1 \pmod{m_1}; \\ \vdots \\ a \equiv a_k \pmod{m_k}. \end{cases}$$

По китайской теореме об остатках эта система разрешима (см. например [10]) и $\left(\frac{x+a_1}{m_1}\right) = \left(\frac{x+a}{m_1}\right), \dots, \left(\frac{x+a_k}{m_k}\right) = \left(\frac{x+a}{m_k}\right)$, а значит наша сумма S может быть представлена в следующем виде:

$$S = \sum_{x \leq X} \left(\frac{x + a}{m_1} \right) \left(\frac{x + a}{m_2} \right) \dots \left(\frac{x + a}{m_k} \right) = \sum_{x \leq X} \left(\frac{x + a}{Q} \right).$$

Применим к S утверждение леммы 1.2.

$$S \ll_\varepsilon X^{\frac{1}{2}} Q^{\frac{3}{16}+\varepsilon}.$$

Для получения нетривиальной оценки потребуем $X^{\frac{1}{2}}Q^{\frac{3}{16}+\varepsilon} < X$. Тогда получим

$$X > Q^{\frac{3}{8}+\varepsilon}.$$

Положим $\omega = 4\varepsilon$, тогда при $X > Q^{\frac{3}{8}+\omega}$ получим

$$S \ll_\varepsilon XQ^{\frac{3}{16}+\varepsilon} = XX^{-\frac{1}{2}}Q^{\frac{3}{16}+\varepsilon} < XQ^{-\frac{3}{16}-\frac{\omega}{2}}Q^{\frac{3}{16}+\varepsilon} = XQ^{-\varepsilon}.$$

Теорема доказана.

Теорема 1.3 *Пусть $m_1, m_2, \ldots, m_k$ — попарно взаимно простые бескубические числа, $Q = m_1 m_2 \ldots m_k$. Далее пусть*

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

где штрих в сумме означает, что суммирование ведется только по бесквадратным числам, 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 $|S| \ll_\varepsilon XQ^{-\varepsilon}$.

Доказательство. Поскольку

$$\mu^2(x) = \begin{cases} 1, & \text{если } x \text{ бесквадратное;} \\ 0, & \text{в противном случае,} \end{cases}$$

имеем

$$S = \sum_{x \le X} \mu^2(x) \left(\frac{x+a_1}{m_1}\right) \left(\frac{x+a_2}{m_2}\right) \dots \left(\frac{x+a_k}{m_k}\right).$$

Рассмотрим следующую систему сравнений:

$$\begin{cases} a \equiv a_1 \pmod{m_1}; \\ \vdots \\ a \equiv a_k \pmod{m_k}. \end{cases}$$

По китайской теореме об остатках эта система разрешима и

$$\left(\frac{x+a_1}{m_1}\right) = \left(\frac{x+a}{m_1}\right), \dots, \left(\frac{x+a_k}{m_k}\right) = \left(\frac{x+a}{m_k}\right),$$

а значит наша сумма S может быть представлена в следующем виде:

$$S = \sum_{x \le X} \mu^2(x) \left(\frac{x+a}{m_1}\right) \left(\frac{x+a}{m_2}\right) \dots \left(\frac{x+a}{m_k}\right) = \sum_{x \le X} \mu^2(x) \left(\frac{x+a}{Q}\right) =$$

$$= \sum_{x \le X} \sum_{d^2 \mid x} \mu(d) \left(\frac{x+a}{Q}\right) = \sum_{d \le \sqrt{X}} \mu(d) \sum_{\substack{d^2 \mid x \\ x \le X}} \left(\frac{x+a}{Q}\right) =$$

$$= \sum_{d \le \sqrt{X}} \mu(d) \sum_{k \le \frac{X}{d^2}} \left(\frac{kd^2+a}{Q}\right) = \sum_{d \le P} \mu(d) \sum_{k \le \frac{X}{d^2}} \left(\frac{kd^2+a}{Q}\right) +$$

$$+ \sum_{P < d < \sqrt{X}} \mu(d) \sum_{k \le \frac{X}{d^2}} \left(\frac{kd^2+a}{Q}\right) = W_1 + W_2,$$

где $P = \frac{X^{0,5}}{Q^{0,125+\omega/2}}$.

Сначала оценим вторую сумму, для этого внутреннюю сумму оценим тривиально, а для внешней суммы применим хорошо известную оценку для остатка ряда обратных квадратов:

$$|W_2| \ll \sum_{P<d<\sqrt{X}} \frac{X}{d^2} = O\left(\frac{X}{P}\right) = O(X^{0,5}Q^{0,125+\omega/2}).$$

Для оценки W_1 разобьем сумму на две: U_1 — сумма по d, взаимнопростым с Q, U_2 — сумма по d таким, что $(d^2, Q) = l \neq 1$.

Сначала оценим U_1, применим к внутренней сумме оценку теоремы 1.1.

$$U_1 = \sum_{\substack{d<P \\ (d,Q)=1}} \mu(d) \sum_{k \leq \frac{X}{d^2}} \left(\frac{kd^2+a}{Q}\right) = \sum_{\substack{d<P \\ (d,Q)=1}} \mu(d)\frac{X}{d^2}Q^{-\varepsilon} =$$

$$= XQ^{-\varepsilon} \sum_{\substack{d<P \\ (d,Q)=1}} \frac{\mu(d)}{d^2} \ll XQ^{-\varepsilon}.$$

Для оценки суммы U_2 заметим, что, при $(d^2, Q) = l \neq 1$, $Q = ld_1$

$$\left(\frac{kd^2+a}{Q}\right) = \left(\frac{kd^2+a}{l}\right)\left(\frac{kd^2+a}{d_1}\right) =$$

$$= \left(\frac{kd^2+a}{l}\right)\left(\frac{kd^2+a}{d_1}\right) = \left(\frac{a}{l}\right)\left(\frac{k+a(d')^2}{d_1}\right),$$

где d' — такое, что $d'd \equiv 1 \pmod{d_1}$. Тогда

$$U_2 = \sum_{l|Q} \sum_{\substack{d<P \\ (d^2,Q)=l}} \mu(d) \sum_{k \le \frac{X}{d^2}} \left(\frac{kd^2 + a}{Q} \right) = \sum_{l|Q} \left(\frac{a}{l} \right) \sum_{\substack{d<P \\ (d^2,Q)=l}} \mu(d) \sum_{k \le \frac{X}{d^2}} \left(\frac{k + a(d')^2}{d_1} \right) =$$

$$= \sum_{l|Q} \left(\frac{a}{l} \right) \sum_{\substack{d<P \\ (d^2,Q)=l}} \mu(d) \frac{X}{d^2} \frac{Q^{-\varepsilon}}{l^{-\varepsilon}} \ll XQ^{-\varepsilon} \sum_{l|Q} l^{\varepsilon} \sum_{\substack{d<P \\ (d^2,Q)=l}} \frac{1}{d^2} =$$

$$= XQ^{-\varepsilon} \sum_{d<P} \frac{1}{d^2} (d^2, Q)^{\varepsilon} = XQ^{-\varepsilon} \sum_{d<P} \frac{1}{d^{2-2\varepsilon}} \ll XQ^{-\varepsilon}.$$

Найдем значения X, при которых выполнено неравенство $X^{0,5}Q^{0,125+\omega/2} \leqslant XQ^{-\varepsilon}$: $Q^{0,125+\omega/2+\varepsilon} \leqslant \sqrt{X}$, $X \geqslant Q^{\frac{1}{4}+\omega+2\varepsilon}$. Тогда $|W_1| \ll XQ^{-\varepsilon}$, $|W_2| \ll XQ^{-\varepsilon}$, а следовательно, и $|S| \ll XQ^{-\varepsilon}$.

Так как по условию $Q^{\frac{1}{4}+\omega+2\varepsilon} < Q$, поэтому $\omega + 2\varepsilon < \frac{3}{4}$, следовательно для получения допустимых значений ω должно быть выполнено следующее неравенство

$$2\varepsilon + \frac{3\sqrt{\varepsilon}}{2 - 4\sqrt{\varepsilon}} < \frac{3}{4}.$$

Оно выполняется при $0 < \varepsilon < 0,0533$. Теорема доказана.

Теорема 1.4 *Пусть $m_1, m_2, \ldots, m_k$ — попарно взаимно простые числа, $Q = m_1 m_2 \ldots m_k$, $X \le Q$, причем по крайней мере для одного из чисел*

m_i найдется такое простое p, что $p^3|m_i$. Далее пусть

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

где штрих в сумме означает, что суммирование ведется только по бесквадратным числам, 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 $|S| \ll_\varepsilon XQ^{-\varepsilon}$.

Доказательство. Как и в теореме 1.3, имеем

$$S = \sum_{x \leq X} \mu^2(x)\left(\frac{x+a_1}{m_1}\right)\left(\frac{x+a_2}{m_2}\right)\dots\left(\frac{x+a_k}{m_k}\right).$$

Рассмотрим следующую систему сравнений:

$$\begin{cases} a \equiv a_1 \pmod{m_1}; \\ \vdots \\ a \equiv a_k \pmod{m_k}. \end{cases}$$

По китайской теореме об остатках эта система разрешима и $\left(\frac{x+a_1}{m_1}\right) = \left(\frac{x+a}{m_1}\right), \dots, \left(\frac{x+a_k}{m_k}\right) = \left(\frac{x+a}{m_k}\right)$, а значит наша сумма S может быть представлена в следующем виде:

$$S = \sum_{x \leq X} \mu^2(x)\left(\frac{x+a}{m_1}\right)\left(\frac{x+a}{m_2}\right)\dots\left(\frac{x+a}{m_k}\right) = \sum_{x \leq X} \mu^2(x)\left(\frac{x+a}{Q}\right) =$$

$$= \sum_{x \le X} \sum_{d^2 | x} \mu(d) \left(\frac{x+a}{Q} \right) = \sum_{d \le \sqrt{X}} \mu(d) \sum_{\substack{d^2 | x \\ x \le X}} \left(\frac{x+a}{Q} \right) =$$

$$= \sum_{d \le \sqrt{X}} \mu(d) \sum_{k \le \frac{X}{d^2}} \left(\frac{kd^2+a}{Q} \right) = \sum_{d \le P} \mu(d) \sum_{k \le \frac{X}{d^2}} \left(\frac{kd^2+a}{Q} \right) +$$

$$+ \sum_{P < d < \sqrt{X}} \mu(d) \sum_{k \le \frac{X}{d^2}} \left(\frac{kd^2+a}{Q} \right) = W_1 + W_2,$$

где $P = \frac{X^{1/2}}{Q^{3/16+\omega/2}}$.

Сначала оценим вторую сумму, для этого внутреннюю сумму оценим тривиально, а для внешней суммы применим хорошо известную оценку для остатка ряда обратных квадратов:

$$|W_2| \ll \sum_{P < d < \sqrt{X}} \frac{X}{d^2} = O\left(\frac{X}{P} \right) = O(X^{1/2} Q^{3/16+\omega}).$$

Для оценки W_1 разобьем сумму на две: U_1 — сумма по d, взаимнопростым с Q, U_2 — сумма по d таким, что $(d^2, Q) = l \neq 1$.

Сначала оценим U_1, применим к внутренней сумме оценку теоремы 1.2.

$$U_1 = \sum_{\substack{d < P \\ (d,Q)=1}} \mu(d) \sum_{k \le \frac{X}{d^2}} \left(\frac{kd^2+a}{Q} \right) = \sum_{\substack{d < P \\ (d,Q)=1}} \mu(d) \frac{X}{d^2} Q^{-\varepsilon} =$$

$$= XQ^{-\varepsilon} \sum_{\substack{d < P \\ (d,Q)=1}} \frac{\mu(d)}{d^2} \ll XQ^{-\varepsilon}.$$

Для оценки суммы U_2 заметим, что, при $(d^2, Q) = l \neq 1$, $Q = ld_1$

$$\left(\frac{kd^2+a}{Q}\right) = \left(\frac{kd^2+a}{l}\right)\left(\frac{kd^2+a}{d_1}\right) =$$

$$= \left(\frac{kd^2+a}{l}\right)\left(\frac{kd^2+a}{d_1}\right) = \left(\frac{a}{l}\right)\left(\frac{k+a(d')^2}{d_1}\right),$$

где d' — такое, что $d'd \equiv 1 \pmod{d_1}$. Тогда

$$U_2 = \sum_{l|Q} \sum_{\substack{d<P \\ (d^2,Q)=l}} \mu(d) \sum_{k \leq \frac{X}{d^2}} \left(\frac{kd^2+a}{Q}\right) = \sum_{l|Q} \left(\frac{a}{l}\right) \sum_{\substack{d<P \\ (d^2,Q)=l}} \mu(d) \sum_{k \leq \frac{X}{d^2}} \left(\frac{k+a(d')^2}{d_1}\right) =$$

$$= \sum_{l|Q} \left(\frac{a}{l}\right) \sum_{\substack{d<P \\ (d^2,Q)=l}} \mu(d) \frac{X}{d^2} \frac{Q^{-\varepsilon}}{l^{-\varepsilon}} \ll XQ^{-\varepsilon} \sum_{l|Q} l^{\varepsilon} \sum_{\substack{d<P \\ (d^2,Q)=l}} \frac{1}{d^2} =$$

$$= XQ^{-\varepsilon} \sum_{d<P} \frac{1}{d^2} (d^2, Q)^{\varepsilon} = XQ^{-\varepsilon} \sum_{d<P} \frac{1}{d^{2-2\varepsilon}} \ll XQ^{-\varepsilon}.$$

Найдем значения X, при которых выполнено неравенство $X^{1/2}Q^{3/16+\omega/2} \leqslant XQ^{-\varepsilon}$: $Q^{3/16+\omega/2+\varepsilon} \leqslant \sqrt{X}$, $X \geqslant Q^{\frac{3}{8}+\omega+2\varepsilon}$. Тогда $|W_1| \ll XQ^{-\varepsilon}$, $|W_2| \ll XQ^{-\varepsilon}$, а следовательно, и $|S| \ll XQ^{-\varepsilon}$.

Так как по условию $Q^{\frac{3}{8}+\omega+2\varepsilon} < Q$, поэтому $\rho = \omega + 2\varepsilon = 6\varepsilon < \frac{5}{8}$, следовательно для получения допустимых значений ρ должно быть выполнено неравенство $\rho < \frac{5}{8}$. Оно выполняется при $0 < \varepsilon < \rho/6 = \frac{5}{48}$. Теорема 1.4 доказана.

1.3 Доказательство теоремы для случая бескубических модулей

Обозначим символом $V(X)$ количество значений $x \leq X$, удовлетворяющих соотношениям

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

Теорема 1.5 *Пусть* $Q = m_1 m_2 \ldots m_n$, *где* $m_1, m_2, \ldots, m_n$ — *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. Представим $V(X)$ в следующем виде:

$$V(X) = \frac{1}{2^n} \sum_{x \leq X} 1 + \frac{1}{2^n} \sum{}' (-1)^k \varepsilon_{i_1} \varepsilon_{i_2} \ldots \varepsilon_{i_k} \times$$

$$\times \sum_{x \leq X} \left(\frac{x+a_{i_1}}{m_{i_1}}\right) \left(\frac{x+a_{i_2}}{m_{i_2}}\right) \ldots \left(\frac{x+a_{i_k}}{m_{i_k}}\right)$$

где штрих во второй сумме означает суммирование по всем наборам $1 \leq i_1 < i_2 < \ldots < i_k \leq n$, $1 \leq k \leq n$. Обозначим вторую сумму за $W(x)$, а

$S_{i_1,i_2,\ldots,i_k} = \sum\limits_{x\le X} \left(\frac{x+a_{i_1}}{m_1}\right)\left(\frac{x+a_{i_2}}{m_2}\right)\ldots\left(\frac{x+a_{i_k}}{m_k}\right)$, тогда $V(X) = \frac{X}{2^n} + W(X)$, а

$$|W(X)| \le \frac{1}{2^n}\sum{}' |S_{i_1,i_2,\ldots,i_k}|\,.$$

По теореме 1 имеем следующую оценку:

$$|S_{i_1,i_2,\ldots,i_k}| \ll \min\left(X\left(m_{i_1}m_{i_2}\ldots m_{i_k}\right)^{-\varepsilon}, m_{i_1}m_{i_2}\ldots m_{i_k}\right).$$

Разобьем сумму со штрихом на две $\sum' = \sum'_1 + \sum'_2$, где суммирование в первой сумме идет по всем наборам $m_{i_1}, m_{i_2}, \ldots, m_{i_k}$, для которых $m_{i_1}m_{i_2}\ldots m_{i_k} \le Q^{\frac{1}{4}}$, а во второй — по всем оставшимся. Количество наборов и в первой, и во второй сумме не превосходит 2^n. Тогда оценивая первую сумму тривиально, а вторую — с помощью теоремы 1.1, получим

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

Тем самым теорема доказана.

1.4 Доказательство теоремы в общем случае

Теорема 1.6 *Пусть $Q = m_1m_2\ldots m_n$, где $m_1, m_2, \ldots, m_n$ — 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 $|W(X)| \ll_\varepsilon XQ^{-\frac{3\varepsilon}{8}}$.

Доказательство. Представим $V(X)$ в следующем виде:

$$V(X) = \frac{1}{2^n} \sum_{x \leq X} 1 + \frac{1}{2^n} \sum\nolimits' (-1)^k \varepsilon_{i_1} \varepsilon_{i_2} \dots \varepsilon_{i_k} \times$$

$$\times \sum_{x \leq X} \left(\frac{x + a_{i_1}}{m_{i_1}} \right) \left(\frac{x + a_{i_2}}{m_{i_2}} \right) \dots \left(\frac{x + a_{i_k}}{m_{i_k}} \right)$$

где штрих во второй сумме означает суммирование по всем наборам $1 \leq i_1 < i_2 < \ldots < i_k \leq n$, $1 \leq k \leq n$. Обозначим вторую сумму за $W(x)$, а $S_{i_1,i_2,\ldots,i_k} = \sum\limits_{x \leq X} \left(\frac{x+a_{i_1}}{m_1} \right) \left(\frac{x+a_{i_2}}{m_2} \right) \dots \left(\frac{x+a_{i_k}}{m_k} \right)$, тогда $V(X) = \frac{X}{2^n} + W(X)$, а

$$|W(X)| \leq \frac{1}{2^n} \sum\nolimits' |S_{i_1,i_2,\ldots,i_k}| .$$

По теореме 2 имеем следующую оценку

$$|S_{i_1,i_2,\ldots,i_k}| \ll \min \left(X \left(m_{i_1} m_{i_2} \dots m_{i_k} \right)^{-\varepsilon}, m_{i_1} m_{i_2} \dots m_{i_k} \right).$$

Разобьем сумму со штрихом на две $\sum' = \sum'_1 + \sum'_2$, где суммирование в первой сумме идет по всем наборам $m_{i_1}, m_{i_2}, \dots, m_{i_k}$, для которых

$m_{i_1}m_{i_2}\dots m_{i_k} \le Q^{\frac{3}{8}}$, а во второй — по всем оставшимся. Количество наборов и в первой, и во второй сумме не превосходит 2^n. Тогда оценивая первую сумму тривиально, а вторую — с помощью теоремы 1.2, получим

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

Тем самым теорема доказана.

1.5 Распределение квадратичных вычетов и невычетов в последовательностях бесквадратных чисел

Обозначим символом $F(X)$ количество бесквадратных 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 1.7 *Пусть $Q = m_1m_2\dots m_n$, 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 $|W(X)| \ll_\varepsilon XQ^{-\frac{\varepsilon}{4}}$.

Доказательство. Представим $F(X)$ в следующем виде:

$$F(X) = \frac{1}{2^n}\sum_{x\le X}\mu^2(x) + \frac{1}{2^n}\sum{}'(-1)^k\varepsilon_{i_1}\varepsilon_{i_2}\dots\varepsilon_{i_k}\times$$

$$\times\sum_{x\le X}\mu^2(x)\left(\frac{x+a_{i_1}}{m_{i_1}}\right)\left(\frac{x+a_{i_2}}{m_{i_2}}\right)\dots\left(\frac{x+a_{i_k}}{m_{i_k}}\right)$$

где штрих во второй сумме означает суммирование по всем наборам $1 \le i_1 < i_2 < \dots < i_k \le n$, $1 \le k \le n$.

Введем обозначения

$$S_{i_1,i_2,\dots,i_k} = \sum_{x\le X}\mu^2(x)\left(\frac{x+a_{i_1}}{m_1}\right)\left(\frac{x+a_{i_2}}{m_2}\right)\dots\left(\frac{x+a_{i_k}}{m_k}\right),$$

$$W(x) = \frac{1}{2^n}\sum{}'(-1)^k\varepsilon_{i_1}\varepsilon_{i_2}\dots\varepsilon_{i_k}S_{i_1,i_2,\dots,i_k}.$$

Тогда, применяя лемму 1.3, получим следующее равенство

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

где

$$|W(X)| \le \frac{1}{2^n}\sum{}'\left|S_{i_1,i_2,\dots,i_k}\right|.$$

По теореме 1.3 имеем следующую оценку, для $S_{i_1,i_2,\dots,i_k}$:

$$|S_{i_1,i_2,\dots,i_k}| \ll \min\left(X\left(m_{i_1}m_{i_2}\dots m_{i_k}\right)^{-\varepsilon}, m_{i_1}m_{i_2}\dots m_{i_k}\right).$$

Разобьем сумму со штрихом на две $\sum' = \sum'_1 + \sum'_2$, где суммирование в первой сумме идет по всем наборам $m_{i_1}, m_{i_2}, \ldots, m_{i_k}$, для которых $m_{i_1} m_{i_2} \ldots m_{i_k} \leq Q^{\frac{1}{4}}$, а во второй — по всем оставшимся. Количество наборов и в первой, и во второй сумме не превосходит 2^n. Тогда оценивая первую сумму тривиально, а вторую — с помощью теоремы 1.1, получим

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

Тем самым теорема доказана.

Теорема 1.8 *Пусть $Q = m_1 m_2 \ldots m_n$, где $m_1, m_2, \ldots, m_n$ — 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 $|W(X)| \ll_\varepsilon XQ^{-\frac{3\varepsilon}{8}}$.

Доказательство. Представим $F(X)$ в следующем виде:

$$F(X) = \frac{1}{2^n}\sum_{x \leq X} \mu^2(x) + \frac{1}{2^n}\sum{}'(-1)^k \varepsilon_{i_1}\varepsilon_{i_2}\ldots\varepsilon_{i_k} \times$$

$$\times \sum_{x \le X} \mu^2(x) \left(\frac{x+a_{i_1}}{m_{i_1}}\right)\left(\frac{x+a_{i_2}}{m_{i_2}}\right)\ldots\left(\frac{x+a_{i_k}}{m_{i_k}}\right)$$

где штрих во второй сумме означает суммирование по всем наборам $1 \le i_1 < i_2 < \ldots < i_k \le n$, $1 \le k \le n$.

Введем обозначения

$$S_{i_1,i_2,\ldots,i_k} = \sum_{x \le X} \mu^2(x) \left(\frac{x+a_{i_1}}{m_1}\right)\left(\frac{x+a_{i_2}}{m_2}\right)\ldots\left(\frac{x+a_{i_k}}{m_k}\right),$$

$$W(x) = \frac{1}{2^n} \sum{}' (-1)^k \varepsilon_{i_1}\varepsilon_{i_2}\ldots\varepsilon_{i_k} S_{i_1,i_2,\ldots,i_k}.$$

Тогда, применяя лемму 1.3, получим следующее равенство

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

где

$$|W(X)| \le \frac{1}{2^n} \sum{}' \left|S_{i_1,i_2,\ldots,i_k}\right|.$$

По теореме 1.4 имеем следующую оценку для $S_{i_1,i_2,\ldots,i_k}$:

$$|S_{i_1,i_2,\ldots,i_k}| \ll \min\left(X\left(m_{i_1}m_{i_2}\ldots m_{i_k}\right)^{-\varepsilon}, m_{i_1}m_{i_2}\ldots m_{i_k}\right).$$

Разобьем сумму со штрихом на две $\sum{}' = \sum{}'_1 + \sum{}'_2$, где суммирование в первой сумме идет по всем наборам $m_{i_1}, m_{i_2}, \ldots, m_{i_k}$, для которых $m_{i_1}m_{i_2}\ldots m_{i_k} \le Q^{\frac{3}{8}}$, а во второй — по всем оставшимся. Количество наборов

и в первой, и во второй сумме не превосходит 2^n. Тогда оценивая первую сумму тривиально, а вторую — с помощью теоремы 1.2, получим

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

Тем самым теорема доказана.

Глава 2

Уязвимость протокола „Ментальный покер”

В данной главе изучаются возможности атаки и обмана для игрока начинающего игру в известном криптографическом протоколе, называемом "Ментальный покер"[40].

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).

Перейдем к описанию атакуемого протокола. 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 сообщение, 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.

Перейдем к атакам криптолога на данный протокол. Помимо очевидных предосторожностей при выборе простого p (оно должно быть достаточно большим, чтобы задачу дискретного логарифмирования нельзя было решить быстро) следует соблюдать аккуратность и при выборе чисел α_1, β_1 и γ_1. Ясно, что $\varphi(p) = p - 1$ может довольно легко разлагаться на множители, по крайней мере $2|\varphi(p)$. Предположим, что среди α_1, β_1 и γ_1 первые два числа являются квадратичными вычетами по модулю p, а последнее — квадратичным невычетом. Так как c_A, c_B , d_A и d_B взаимно просты с $\varphi(p)$, то они нечетны, а возведение в нечетную степень оставляет квадратичный вычет квадратичным вычетом, а квадратичный невычет — квадратичным невычетом. Следовательно, γ_1 будет единственным числом, которое при возведении в степень $\frac{p-1}{2}$ выдаст в качестве результата -1 , следовательно, $\mathcal{E}$ легко отслеживает перемещения карты γ.

Пусть теперь $\varphi(p) = p_1^{\delta_1} p_1^{\delta_1} ... p_n^{\delta_n}$. Наблюдатель $\mathcal{E}$ проверяет, сколько будет вычетов степени p_i среди α_1, β_1 и γ_1; если такой вычет единственный или их

два, то точно такие же рассуждения пройдут и для этого случая. Так как c_A, c_B , d_A и d_B взаимно просты с $\varphi(p)$, то возведения в эти степени оставят вычеты вычетами, а невычеты невычетами, и с помощью формулы Эйлера $\mathcal{E}$ отслеживает перемещения карт. Более того, подобрав подходящим образом пару p_i p_j, $\mathcal{E}$ может в точности определить распределение карт по игрокам. Следовательно, для надежности этого протокола следует брать в качестве α_1, β_1 и γ_1 первообразные корни по модулю p.

Исследуем возможности обмана для абонента $\mathcal{A}$, начинающего игру. Пусть даже нам удалось найти первообразные корни и закодировать ими наши карты, тем не менее у $\mathcal{A}$ есть возможность попытаться обмануть $\mathcal{B}$. Абонент $\mathcal{A}$ подменяет один из первообразных корней α_1, β_1, γ_1 квадратичным вычетом a, например, это будет α_1. $\mathcal{A}$ вычисляет числа $u_1 \equiv a^{c_A} \pmod p$, $u_2 \equiv \beta_1^{c_A} \pmod p$, $u_3 \equiv \gamma_1^{c_A} \pmod p$ и высылает их $\mathcal{B}$. Аккуратно посчитаем с какой вероятностью $\mathcal{B}$ выберет и отправит $\mathcal{A}$ испорченную карту. Пусть T_a — это элементарное событие «Испорчена карта α», T_b — «Испорчена карта β», T_c — «Испорчена карта γ» и T — элементарное событие «Абонент $\mathcal{B}$ отправил абоненту $\mathcal{A}$ испорченную карту». Тогда $P(T) = P(T_a|A)P(A) + P(T_b|B)P(B) + P(T_c|C)P(C) = \frac{1}{9} + \frac{1}{9} + \frac{1}{9} = \frac{1}{3}$. Значит, с вероятностью $\frac{2}{3}$ абонент $\mathcal{B}$ вышлет $\mathcal{A}$ неиспорченную карту.

$\mathcal{B}$ вычисляет для оставшихся двух чисел $v_1 \equiv u_1^{c_B} \pmod p$, $v_3 \equiv u_3^{c_B}$

$(\mathrm{mod}\ p)$ и отправляет их $\mathcal{A}$. Абонент $\mathcal{A}$ определяет карту α с помощью формулы Эйлера и отправляет ее в прикуп, $\mathcal{B}$ получает $w_3 \equiv v_3^{d_A} \pmod{p}$, далее, он определяет свою карту и при этом не знает, что отправилось в прикуп. Абонент $\mathcal{A}$ полностью знает распределение карт в раздаче с вероятностью $\frac{2}{3}$.

Абонент $\mathcal{B}$ может устранить возможность подобного обмана, для этого ему необходимо проверить, являются ли α_1, β_1 и γ_1 первообразными корнями. Если одно из чисел окажется не первообразным корнем, то он отправляет его $\mathcal{A}$ и абонент $\mathcal{A}$ уже не сможет определить оставшиеся карты.

Глава 3

О вычислении суммы Гаусса специального вида.

3.1 Вспомогательные леммы и утверждения

Введем следующие обозначения для полных сумм Гаусса:

$$G(N) = G\left(N\right) = \sum_{n=1}^{N} e^{2\pi i \frac{x^2}{N}} = \sum_{n=1}^{N} e\left(\frac{x^2}{N}\right)$$

$$G_a(N) = \sum_{n=1}^{N} e^{2\pi i \frac{ax^2}{N}} = \sum_{n=1}^{N} e\left(\frac{ax^2}{N}\right)$$

Лемма 3.1 *Пусть $G(N)$ — полная сумма Гаусса, N — нечетное число, тогда:*

$$G\left(N\right) = \frac{1 + i^{-N}}{1 + i^{-1}}\sqrt{N}.$$

Доказательство. Запишем формулу суммирования Пуассона в комплексной форме. Тогда при $k \to \infty$

$$G(N) = \sum_{m=-2k}^{2k} I(m) + R$$

где

$$I(m) = \int\limits_{0,5}^{N+0,5} e^{2\pi i\left(\frac{x^2}{N}+mx\right)} dx, R = O\left(\frac{N \ln k}{k}\right)$$

Преобразуем интеграл $I(m)$. Имеем:

$$I(m) = \int\limits_{0,5}^{N+0,5} e^{2\pi i\left((x+0,5mN)^2/N - m^2N/4\right)} dx = e^{-2\pi i\frac{Nm^2}{4}} \int\limits_{0,5mN+0,5}^{N(0,5m+1)+0,5} e^{2\pi i\frac{y^2}{N}} dy$$

Суммируя величины $I(m)$ отдельно по четным числам m $(m = 2l)$ и отдельно по нечетным числам m $(m = 2l - 1)$, получаем:

$$G(N) = \sum_{l=-k}^{k} \int\limits_{Nl+0,5}^{N(l+1)+0,5} e^{2\pi i\frac{y^2}{N}} dy + \sum_{l=-k}^{k} e^{-\frac{\pi iN}{2}} \int\limits_{N(l-0,5)+0,5}^{N(l+0,5)+0,5} e^{2\pi i\frac{y^2}{N}} dy + R =$$

$$= \int\limits_{-Nk+0,5}^{N(k+1)+0,5} e^{2\pi i\frac{y^2}{N}} dy + i^{-N} \int\limits_{N(k-0,5)+0,5}^{N(k+0,5)+0,5} e^{2\pi i\frac{y^2}{N}} dy + R =$$

$$= \sqrt{N}\left(1 + i^{-N}\right) \int\limits_{-\infty}^{\infty} e^{2\pi iz^2} dz + O\left(N^{-1/2}k^{-1}\right)$$

так как при $|\alpha| \leq \sqrt{N}$ имеет место неравенство:

$$\left| \int\limits_{k\sqrt{N}+\alpha}^{\infty} e^{2\pi i z^2} dz \right| \leq k^{-1} N^{-1/2}$$

Переходя к пределу при $k \to \infty$ в последней формуле для $G(N)$, получаем:

$$G(N) = \sqrt{N} \left(1 + i^{-N}\right) \int\limits_{-\infty}^{\infty} e^{2\pi i z^2} dz.$$

В частности, при $N = 1$

$$1 = G(1) = (1 + i^{-1}) \int\limits_{-\infty}^{\infty} e^{2\pi i z^2} dz.$$

Следовательно,

$$G(N) = \frac{1 + i^{-N}}{1 + i^{-1}} \sqrt{N}.$$

Лемма доказана.

Пускай у суммы в знаменателе стоит нечетное простое число. Найдем связь между обычной суммой и суммой, у которой в числителе есть множитель a.

Лемма 3.2 *Пусть p — нечетное простое число, a и p взаимнопросты, тогда*

$$G_a(p) = \sum_{x=1}^{p} e\left(\frac{ax^2}{p}\right) = \left(\frac{a}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}.$$

Доказательство.

$$G_a(p) = \sum_{x=1}^{p} e\left(\frac{ax^2}{p}\right) = 1 + \sum_{x=1}^{p-1} e\left(\frac{ax^2}{p}\right) = 1 + \sum_{x=1}^{p-1} e\left(\frac{ax}{p}\right) +$$

$$+ \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e\left(\frac{ax}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e\left(\frac{ax}{p}\right),$$

поскольку $1 + \sum_{x=1}^{p-1} e\left(\frac{ax}{p}\right) = 0$. Тогда

$$\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e\left(\frac{ax}{p}\right) = \left(\frac{a^2}{p}\right) \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e\left(\frac{ax}{p}\right) = \left(\frac{a}{p}\right) \sum_{x=1}^{p-1} \left(\frac{ax}{p}\right) e\left(\frac{ax}{p}\right) =$$

Поскольку, когда x пробегает приведенную систему вычетов $(\mathrm{mod}\ p)$, ax также пробегает полную систему вычетов $(\mathrm{mod}\ p)$, получаем:

$$\left(\frac{a}{p}\right) \sum_{x=1}^{p-1} \left(\frac{ax}{p}\right) e\left(\frac{ax}{p}\right) = \left(\frac{a}{p}\right) \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e\left(\frac{x}{p}\right) =$$

$$\left(\frac{a}{p}\right) \left(\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e\left(\frac{x}{p}\right) + \sum_{x=1}^{p-1} e\left(\frac{x}{p}\right) + 1 \right) = \left(\frac{a}{p}\right) \sum_{x=1}^{p} e\left(\frac{x^2}{p}\right)$$

Применяя лемму 3.1, окончательно получаем:

$$G_a(p) = \left(\frac{a}{p}\right) \sum_{x=1}^{p-1} e\left(\frac{x^2}{p}\right) = \left(\frac{a}{p}\right) \frac{1 + i^{-p}}{1 + i^{-1}} = \left(\frac{a}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}.$$

Тем самым лемма доказана.

Теперь вычислим сумму Гаусса, если в знаменателе стоит степень простого числа

Лемма 3.3 *Пусть p — нечетное простое число, $\alpha \in \mathbb{N}$ и a и p взаимно-просты, тогда*

$$G_a(p^\alpha) = \left(\frac{a}{p}\right)^\alpha i^{\left(\frac{p^\alpha-1}{2}\right)^2} p^{\frac{\alpha}{2}}$$

Доказательство. Докажем это утверждение с помощью индукции по α.

База при $\alpha = 1$ установлена в лемме 3.2.

Предположим утверждение теоремы верно для всех $\alpha \leqslant n$, покажем, что тогда оно верно и при $\alpha = n+1$

$$G_a\left(p^{n+1}\right) = \sum_{x=1}^{p^{n+1}} e\left(\frac{ax^2}{p^{n+1}}\right) = \sum_{y=1}^{p^n}\sum_{z=0}^{p-1} e\left(\frac{a(y+p^n z)^2}{p^{n+1}}\right) =$$

$$= \sum_{y=1}^{p^n} e\left(\frac{ay^2}{p^{n+1}}\right)\sum_{z=0}^{p-1} e\left(\frac{2ayz}{p}\right) = \sum_{y=1}^{p^n} e\left(\frac{ay^2}{p^{n+1}}\right)\delta_p(2ay),$$

где

$$\delta_p(2ay) = \begin{cases} p, & \text{если } p|2ay; \\ 0, & \text{иначе.} \end{cases}$$

Так как НОД$(2a, p) = 1$, то в сумме останутся только те слагаемые в которых y кратно p. Поэтому

$$G_a\left(p^{n+1}\right) = p\sum_{y=1}^{p^{n-1}} e\left(\frac{ay^2}{p^{n-1}}\right) = pG_a\left(p^{n-1}\right) = \left(\frac{a}{p}\right)^{n-1} i^{\left(\frac{p^{n-1}-1}{2}\right)^2} p^{\frac{n-1}{2}+1}.$$

Поскольку $p^2 \equiv 1 \pmod 8$, следовательно $\left(\frac{p^{n-1}-1}{2}\right)^2 \equiv \left(\frac{p^{n-1}-1}{2}\right)^2 \pmod 4$, поэтому $i^{\left(\frac{p^{n-1}-1}{2}\right)^2} = i^{\left(\frac{p^{n+1}-1}{2}\right)^2}$. Тем самым, имеем

$$G_a\left(p^{n+1}\right) = \left(\frac{a}{p}\right)^{n+1} i^{\left(\frac{p^{n+1}-1}{2}\right)^2} p^{\frac{n+1}{2}}$$

Лемма доказана.

Лемма 3.4 *Пусть* $Q = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, *тогда*

$$\sum_{x=1}^{Q} e\left(\frac{ax^2}{Q}\right) = \prod_{i=1}^{s} \sum_{x_i=1}^{p_i^{\alpha_i}} e\left(\frac{b_i a x^2}{p_i^{\alpha_i}}\right)$$

где b_i *такие, что* $b_1 p_2^{\alpha_2} \dots p_s^{\alpha_s} + \dots + p_1^{\alpha_1} \dots p_{s-1}^{\alpha_{s-1}} b_s \equiv 1 \pmod Q$

$$\left\{\frac{ax^2}{Q}\right\} = \left\{\frac{b_1 a x^2}{p_1^{\alpha_1}} + \dots + \frac{b_s a x^2}{p_s^{\alpha_s}}\right\}$$

Доказательство. Если каждое x_i пробегает полную систему вычетов по $(\mathrm{mod}\ p_i^{\alpha_i})$, то $x_1 p_2^{\alpha_2} \dots p_s^{\alpha_s} + \dots + p_1^{\alpha_1} \dots p_{s-1}^{\alpha_{s-1}} x_s$ пробегает полную систему вычетов по $(\mathrm{mod}\ Q)$. Поэтому

$$\sum_{x=1}^{Q} e\left(\frac{ax^2}{Q}\right) = \sum_{x=1}^{{p_1}^{\alpha_1}} \dots \sum_{x=1}^{{p_s}^{\alpha_s}} e\left(\frac{a\left(x_1 p_2^{\alpha_2} \dots p_s^{\alpha_s} + \dots + p_1^{\alpha_1} \dots p_{s-1}^{\alpha_{s-1}} x_s\right)^2}{Q}\right) =$$

$$= \sum_{x=1}^{{p_1}^{\alpha_1}} \dots \sum_{x=1}^{{p_s}^{\alpha_s}} e\left(a\left(\frac{x_1^2 p_2^{\alpha_2} \dots p_s^{\alpha_s}}{{p_1}^{\alpha_1}} + \dots + \frac{x_s^2 p_1^{\alpha_1} \dots p_{s-1}^{\alpha_{s-1}}}{{p_s}^{\alpha_s}}\right)\right) =$$

$$= \prod_{i=1}^{s} \sum_{x_i=1}^{{p_i}^{\alpha_i}} e\left(\frac{a x_i^2 p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} p_s^{\alpha_s}}{{p_i}^{\alpha_i}}\right)$$

По лемме 1.1 найдется такое b_i, $i = \overline{1,n}$, что:

$$\begin{cases} b_i p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} p_s^{\alpha_s} \equiv 1 \pmod{{p_i}^{\alpha_i}}; \\ b_i \equiv 0 \pmod{p_k^{\alpha_k}}, \text{ при } k \neq i. \end{cases}$$

Тогда, поскольку $(b_i, {p_i}^{\alpha_i}) = 1$, если x_i пробегает полную систему вычетов по модулю ${p_i}^{\alpha_i}$, то и $x_i b_i$ также будет пробегать полную систему по этому модулю, имеем

$$\prod_{i=1}^{s} \sum_{x_i=1}^{{p_i}^{\alpha_i}} e\left(\frac{a x_i^2 p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} p_s^{\alpha_s}}{{p_i}^{\alpha_i}}\right) = \prod_{i=1}^{s} \sum_{x_i=1}^{{p_i}^{\alpha_i}} e\left(\frac{a (x_i b_i)^2 p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} p_s^{\alpha_s}}{{p_i}^{\alpha_i}}\right) =$$

$$= \prod_{i=1}^{s} \sum_{x_i=1}^{{p_i}^{\alpha_i}} e\left(\frac{b_i a x^2}{p_i^{\alpha_i}}\right)$$

Причем, поскольку $b_1 p_2^{\alpha_2} \dots p_s^{\alpha_s} + \dots + b_s p_1^{\alpha_1} \dots p_{s-1}^{\alpha_{s-1}} \equiv 1 \pmod{{p_i}^{\alpha_i}}$, $i = \overline{1,n}$, получаем:

$$b_1 p_2^{\alpha_2} \dots p_s^{\alpha_s} + \dots + b_s p_1^{\alpha_1} \dots p_{s-1}^{\alpha_{s-1}} \equiv 1 \pmod{Q}$$

Лемма доказана.

Лемма 3.5 *Пусть Q — нечетное число, a и Q взаимнопросты, тогда*

$$\sum_{x=1}^{Q} e\left(\frac{ax^2}{Q}\right) = \sqrt{Q} i^{\left(\frac{Q-1}{2}\right)^2} \left(\frac{a}{Q}\right).$$

Доказательство.

Пусть $Q = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, причем $a_1, \dots, a_s$ такие, что

$$a_1 p_2^{\alpha_2} \dots p_s^{\alpha_s} + \dots + p_1^{\alpha_1} \dots p_{s-1}^{\alpha_{s-1}} a_s \equiv 1 \pmod{Q},$$

тогда

$$p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} a_i p_{i+1}^{\alpha_{i+1}} \dots p_s^{\alpha_s} \equiv 1 \pmod{p_i}.$$

Без нарушения общности можно считать

$$\alpha_i = \begin{cases} 1(mod 2) & 1 \le i \le r; \\ 0(mod 2) & r \le i \le s. \end{cases}$$

По лемме 3.3

$$G_a(p^\alpha) = \begin{cases} \left(\frac{a}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} p^{\alpha/2}, & \alpha \equiv 1 \pmod 2; \\ p^{\alpha/2}, & \alpha \equiv 0 \pmod 2, \end{cases}$$

поэтому, применяя лемму 3.4, получаем:

$$\sum_{x=1}^{Q} e\left(\frac{ax^2}{Q}\right) = \prod_{i=1}^{s} \sum_{x_i=1}^{p_i^{\alpha_i}} e\left(\frac{a_i a x^2}{p_i^{\alpha_i}}\right) =$$

$$= \sqrt{Q}\left(\frac{a}{p_1}\right)\ldots\left(\frac{a}{p_r}\right)\left(\frac{a_1}{p_1}\right)\ldots\left(\frac{a_r}{p_r}\right) i^{\left(\frac{p_1-1}{2}\right)^2}\ldots i^{\left(\frac{p_1-1}{2}\right)^2}.$$

Поскольку

$$\left(\frac{p_1^{\alpha_1}\ldots a_i\ldots p_s^{\alpha_s}}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1,$$

отсюда следует

$$\left(\frac{a_i}{p_i}\right) = \left(\frac{p_1\ldots p_{i-1}p_{i+1}\ldots p_r}{p_i}\right) = \prod_{j=1, j\neq i}^{r}\left(\frac{p_j}{p_i}\right).$$

Отсюда имеем:

$$\left(\frac{a_1}{p_1}\right)\ldots\left(\frac{a_r}{p_r}\right) = \prod_{i,j=1; i\neq j}^{r}\left(\frac{p_j}{p_i}\right) = \prod_{i,j=1; i<j}^{r}\left(\frac{p_j}{p_i}\right)\left(\frac{p_i}{p_j}\right).$$

Введем следующие обозначения $\beta_j = \frac{p_j-1}{2}$; $\gamma_r = \sum_{j,i=1,i<j}^{r} \beta_i\beta_j$, тогда, применяя квадратичный закон взаимности, получим:

$$\left(\frac{p_j}{p_i}\right)\left(\frac{p_i}{p_j}\right) = (-1)^{\beta_i\beta_j} = i^{2\beta_i\beta_j} = i^{2\gamma_r},$$

отсюда

$$\left(\frac{a_1}{p_1}\right)\ldots\left(\frac{a_r}{p_r}\right) i^{\left(\frac{p_1-1}{2}\right)^2}\ldots i^{\left(\frac{p_1-1}{2}\right)^2} = i^{\beta_1^2+\ldots\beta_r^2+2\gamma_r} = i^{(\beta_1+\ldots+\beta_r)^2}.$$

$$(\beta_1 + \ldots + \beta_r)^2 \equiv \left(\frac{p_1 - 1}{2} + \ldots + \frac{p_r - 1}{2}\right) \equiv \left(\frac{p_1 \ldots p_r - 1}{2}\right)^2 \equiv$$

$$\equiv \left(\frac{p_1^{\alpha_1} \ldots p_r^{\alpha_r} - 1}{2}\right)^2 \equiv \left(\frac{p_1^{\alpha_1} \ldots p_r^{\alpha_r} p_{r+1}^{\alpha_{r+1}} \ldots p_s^{\alpha_s} - 1}{2}\right)^2 \equiv \left(\frac{Q-1}{2}\right)^2 \pmod 4.$$

Теперь разберемся с $\left(\frac{a}{p_1}\right) \ldots \left(\frac{a}{p_r}\right)$. Сначала мы рассмотрим случай, когда a нечетно, в этом случае можно воспользоваться квадратичным законом взаимности для символов Якоби:

$$\left(\frac{a}{p_1}\right) \ldots \left(\frac{a}{p_r}\right) = (-1)^{\frac{a-1}{2}\left(\frac{p_1-1}{2} + \ldots + \frac{p_r-1}{2}\right)} \left(\frac{p_1}{a}\right) \ldots \left(\frac{p_r}{a}\right) =$$

$$= (-1)^{\frac{a-1}{2}\left(\frac{p_1-1}{2} + \ldots + \frac{p_r-1}{2}\right)} \left(\frac{{p_1}^{\alpha_1}}{a}\right) \ldots \left(\frac{{p_r}^{\alpha_r}}{a}\right) \left(\frac{{p_{r+1}}^{\alpha_{r+1}}}{a}\right) \ldots \left(\frac{{p_s}^{\alpha_s}}{a}\right) =$$

$$= (-1)^{\frac{a-1}{2}\left(\frac{p_1-1}{2} + \ldots + \frac{p_r-1}{2}\right)} \left(\frac{Q}{a}\right) = (-1)^{\frac{a-1}{2}\left(\frac{p_1-1}{2} + \ldots + \frac{p_r-1}{2} + \frac{Q-1}{2}\right)} \left(\frac{a}{Q}\right).$$

Поскольку

$$\frac{p_1 - 1}{2} + \ldots + \frac{p_r - 1}{2} \equiv \frac{Q-1}{2} \pmod 4,$$

следовательно

$$\frac{p_1 - 1}{2} + \ldots + \frac{p_r - 1}{2} + \frac{Q-1}{2} \equiv 0 \pmod 2,$$

поэтому

$$(-1)^{\frac{a-1}{2}\left(\frac{p_1-1}{2}+\ldots+\frac{p_r-1}{2}+\frac{Q-1}{2}\right)}\left(\frac{a}{Q}\right)=\left(\frac{a}{Q}\right).$$

Теперь рассмотрим случай, когда в разложение a входит 2^α. То есть $a=2^\alpha a_1$, где a_1 уже нечетное. Если α-четное, то $\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)$. Тогда

$$\left(\frac{a}{p_1}\right)\ldots\left(\frac{a}{p_r}\right)=\left(\frac{a_1}{p_1}\right)\ldots\left(\frac{a_1}{p_r}\right)=\left(\frac{a_1}{Q}\right)=\left(\frac{a}{Q}\right).$$

Если же α-нечетное, $\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{2^\alpha}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{2}{p}\right)$. Тогда

$$\left(\frac{a}{p_1}\right)\ldots\left(\frac{a}{p_r}\right)=\left(\frac{a_1}{p_1}\right)\ldots\left(\frac{a_1}{p_r}\right)\left(\frac{2}{p_1}\right)\ldots\left(\frac{2}{p_r}\right)=\left(\frac{a_1}{Q}\right)\left(\frac{2}{p_1}\right)\ldots\left(\frac{2}{p_r}\right)$$

$$\left(\frac{2}{p_1}\right)\ldots\left(\frac{2}{p_r}\right)=(-1)^{\frac{{p_1}^2-1}{8}+\ldots+\frac{{p_1}^2-1}{8}}.$$

Поскольку

$$p_1^2-1+\ldots+p_r^2-1\equiv p_1^2\ldots p_r^2-1\equiv p_1^{2\alpha_1}\ldots p_r^{2\alpha_{r+1}}-1\equiv Q^2-1(mod16),$$

следовательно

$$\left(\frac{2}{p_1}\right)\ldots\left(\frac{2}{p_r}\right)=(-1)^{\frac{Q^2-1}{8}}=\left(\frac{2}{Q}\right).$$

А это значит, что

$$\left(\frac{a}{p_1}\right)\ldots\left(\frac{a}{p_r}\right)=\left(\frac{2}{Q}\right)\left(\frac{a_1}{Q}\right)=\left(\frac{a}{Q}\right)$$

Тем самым лемма доказана.

Далее, рассмотрим следующую сумму

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

где $T(x_1,\ldots,x_n)$ — квадратичная форма такая, что ее коэффициенты — целые числа, попарно взаимнопростые с Q.

3.2 Вычисление суммы Гаусса с квадратичной формой в показателе степени

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*

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

тогда

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

Докажем по индукции по порядку квадратичной формы $T(x_1,\ldots,x_n)$. Базис при $n = 1$ установлен в лемме 3.5. Предположим, что утверждение выполнено для любой квадратичной формы порядка $n-1$, удовлетворяющей

условию теоремы, покажем, что тогда оно выполнено и для любой квадратичной формы порядка n. Пусть

$$T(x_1, \ldots, x_n) = \sum_{k=1}^{n} \sum_{l=1}^{n} a_{kl} x_k x_l,$$

где $a_{kl} \in \mathbb{Z}_Q, a_{kl} = a_{lk}$.

Представим квадратичную форму $T(x_1, \ldots, x_n)$ в следующем виде:

$$T(x_1, \ldots, x_n) \equiv a'_{11}(a_{11}x_1 + \ldots + a_{1n}x_n)^2 + R(x_2, \ldots, x_n) \pmod{Q},$$

где a'_{11} такое что $a'_{11}a_{11} \equiv 1 \pmod{Q}$, а $R(x_2, \ldots, x_n)$ также квадратичная форма порядка $n-1$.

$$R(x_2, \ldots, x_n) = \sum_{k=1}^{n} \sum_{l=1}^{n} b_{kl} x_k x_l,$$

где $b_{kl} \in \mathbb{Z}_Q, b_{kl} = b_{lk}$, причем $b_{kl} = a_{kl}a_{1l}a'_{11}$. Поскольку по условию ($a_{kl}$ и Q взаимнопросты для $k = \overline{1,n}$ и $l = \overline{1,n}$, b_{kl} также взаимнопросты с Q. Отсюда имеем:

$$G_T(Q) = \sum_{x_1,\ldots,x_n=1}^{Q} e\left(\frac{a'_{11}(a_{11}x_1 + \ldots + a_{1n}x_n)^2 + R(x_2, \ldots, x_n)}{Q}\right) =$$

$$= \sum_{x_2,\ldots,x_n=1}^{Q} e\left(\frac{R(x_2, \ldots, x_n)}{Q}\right) \sum_{x_1=1+a_{12}x_2+\ldots+a_{1n}x_n}^{Q+a_{12}x_2+\ldots+a_{1n}x_n} e\left(\frac{{x_1}^2 a'_{11}}{Q}\right) =$$

$$= \sum_{x_2,\ldots,x_n=1}^{Q} e\left(\frac{R(x_2,\ldots,x_n)}{Q}\right) \sum_{x_1=1}^{Q} e\left(\frac{{x_1}^2 a'_{11}}{Q}\right).$$

Применяя к внутренней сумме лемму 3.5, получим

$$G_T(Q) = \sqrt{Q}\left(\frac{a'_{11}}{Q}\right) i^{\left(\frac{Q-1}{2}\right)^2} \sum_{x_2,\ldots,x_n=1}^{Q} e\left(\frac{R(x_2,\ldots,x_n)}{Q}\right).$$

По предположению индукции утверждение теоремы выполнено для всех квадратичных форм порядка $n-1$, значит в том числе и для $R(x_2,\ldots,x_n)$, поэтому имеем:

$$G_T(Q) = \sqrt{Q}\left(\frac{a'_{11}}{Q}\right)\left(\frac{a_{11}^2}{Q}\right) i^{\left(\frac{Q-1}{2}\right)^2} \sqrt{Q^{n-1}}\left(\frac{D_1}{Q}\right) i^{(n-1)\left(\frac{Q-1}{2}\right)^2},$$

где D_1 — определитель формы $R(x_2,\ldots,x_n)$.

Матрица перехода S от квадратичной формы $T(x_1,\ldots,x_n)$ к форме $T'(y_1,x_2,\ldots,x_n) = a'_{11}y_1^2 + R(x_2,\ldots,x_n)$ имеет следующий вид:

$$S = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix},$$

поэтому $D = a_{11}|T'|a_{11} = a_{11}D_1$. Отсюда получаем требуемое утверждение:

$$G_T(Q) = i^{n\left(\frac{Q-1}{2}\right)^2}\sqrt{Q^n}\left(\frac{a_{11}D_1}{Q}\right) = i^{n\left(\frac{Q-1}{2}\right)^2}\sqrt{Q^n}\left(\frac{D}{Q}\right).$$

Тем самым теорема доказана.

3.3 Распределение значений очень коротких усредненных сумм Гаусса

Далее рассмотрим усредненную сумму Гаусса вида

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

и найдем распределение ее значений, в случае, если промежуток суммирования очень мал.

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* $\lambda = \frac{3}{2}$.

Доказательство. Найдем моменты порядка $r \geqslant 1$ величины ξ.

$$M\xi^r = \frac{1}{p}\sum_{x=0}^{p-1}\left|\frac{S_h(x)}{h^{\frac{3}{2}}}\right|^{2r} = \frac{1}{ph^{3r}}\sum_{x=0}^{p-1}\left|\sum_{n=x+1}^{x+h}\sum_{m=x+1}^{x+h}\chi(n+m)e\left(\frac{a(n+m)}{p}\right)\right| =$$

$$= \frac{1}{ph^{3r}}\sum_{\substack{n_1,\ldots,n_{2r}=1\\ m_1,\ldots,m_{2r}=1}}^{h} e^{2\pi i\frac{a\left((n_1+m_1)+\ldots+(n_r+m_r)-(n_{r+1}+m_{r+1})-\ldots-(n_{2r}+m_{2r})\right)}{p}}\times$$

$$\times\sum_{x=0}^{p-1}\chi\left(\frac{(x+n_1+m_1)\ldots(x+n_r+m_r)}{(x+n_{r+1}+m_{r+1})\ldots(x+n_{2r}+m_{2r})}\right) =$$

$$= \frac{1}{ph^{3r}}\sum_{l_1,\ldots,l_{2r}=2}^{2h} e^{2\pi i\frac{a\left(l_1+\ldots+l_r-l_{r+1}-\ldots-l_{2r}\right)}{p}} J(l_1)\ldots J(l_{2r})\times$$

$$\times\sum_{x=0}^{p-1}\chi\left(\frac{(x+l_1)\ldots(x+l_r)}{(x+l_{r+1})\ldots(x+l_{2r})}\right) = \frac{1}{ph^{3r}}(M_1+M_2+M_3),$$

где в суммы M_1, M_2 и M_3 входят наборы $(l_1,\ldots,l_{2r})$ из разных непересекающихся классов K_1, K_2 и K_3 соответственно, а $J(l_i)$ — количество решений уравнения $m_i + n_i = l_i$ в целых числах, при условии $1 \leqslant m_i \leqslant h$, $1 \leqslant n_i \leqslant h$. Легко видеть, что $J(l_i) = \min(l_i - 1, 2h - l_i + 1)$.

Класс K_1 состоит только из тех наборов, для которых $(l_{r+1},\dots,l_{2r}$ — есть перестановка набора $(l_1,\dots,l_r)$, тогда

$$M_1=\sum_{(l_1,\dots,l_{2r})\in K_1}(p-\theta r)J(l_1)\dots J(l_{2r})=\left(r!+O\left(\frac{1}{p}\right)\right)\sum_{l_1,\dots,l_r=2}^{2h}J^2(l_1)\dots J^2(l_r)=$$

$$=(r!p+O(1))\,2^r\sum_{l_1,\dots,l_r=2}^{h+1}(l_1-1)^2\dots(l_r-1)^2=$$

$$=(r!p+O(1))\,2^r\prod_{i=1}^{r}\sum_{l_i=1}^{h}l_i^2=(r!p+O(1))\,2^r\prod_{i=1}^{r}\frac{h(h+1)(2h+1)}{6}=$$

$$=\left(\frac{2}{3}\right)^r h^{3r}r!p+O\left(h^{3r}\right).$$

В класс K_2 входят те наборы, не относящиеся K_1, для которых рациональная функция, стоящая под знаком характера, является m-ой степенью, где m — минимальное натуральное число, для которого $\chi^m=\chi_0$. Для комплексного характера χ, можно по крайней мере утверждать, что $m\geqslant 3$. Пусть $f(x)=(x+l_1)\dots(x+l_r)=d(x)f_0^m(x)$ и $g(x)=(x+n_1)\dots(x+n_r)=d(x)g_0^m(x)$, причем $\deg f_0=\deg g_0\geqslant 1$. Отсюда имеем $m=\deg g=\deg f=\deg d+m\deg f_0$, поэтому количество наборов в классе K_2 не превосходит

$$r!h^{\deg d}h^{2\deg f_0}=r!h^{r-m\deg f_0+2\deg f_0}=O\left(h^{r-m+2}\right).$$

Кроме того, на любом допустимом наборе $(l_1, \ldots, l_{2r})$ величина $J(l_1) \ldots J(l_{2r})$ не превосходит h^{2r}, поэтому

$$M_2 = O\left(ph^{3r-m+2}\right).$$

К классу K_3 отнесем все оставшиеся наборы $(l_1, \ldots, l_{2r})$, на них к внутренней сумме может быть применена оценка А. Вейля:

$$\sum_{x=0}^{p-1} \chi\left(\frac{(x+l_1)\ldots(x+l_r)}{(x+l_{r+1})\ldots(x+l_{2r})}\right) \leqslant 2r\sqrt{p}.$$

Отсюда имеем:

$$M_3 = O(h^{4r}\sqrt{p}).$$

Поэтому

$$M\xi^r = \left(\frac{2}{3}\right)^r r! + O\left(\frac{1}{p}\right) + O\left(h^{-m+2}\right) + O\left(\frac{h}{\sqrt{p}}\right).$$

Таким образом, при $p \to +\infty$, поскольку $h(p) \to +\infty$ и $\frac{\log h}{\log p} \to 0$, имеем:

$$M\xi^r \to \left(\frac{2}{3}\right)^r r!.$$

Для нахождения плотности распределения величины ξ мы будем использовать метод характеристических функций (см. например [28]):

$$Me^{i\xi u} = \sum_{k=0}^{+\infty} p\{\xi = k\}e^{iuk}.$$

Характеристическую функцию величины ξ выразим через ее моменты:

$$Me^{i\xi u} = M\sum_{k=0}^{+\infty} \frac{(iu\xi)^k}{k!} = \sum_{k=0}^{+\infty} \frac{(iu)^k}{k!} M\xi^k.$$

Поэтому главный член асимптотики характеристической функции равен:

$$f(u) = \sum_{k=0}^{+\infty} \frac{(iu)^k}{k!} M\xi^k = \sum_{k=0}^{+\infty} \frac{(iu)^k}{k!} \left(\frac{2}{3}\right)^k k! = \sum_{k=0}^{+\infty} \left(\frac{2iu}{3}\right)^k = \frac{1}{1-\frac{2iu}{3}}.$$

Плотность распределения $p(x)$ в таком случае имеет вид:

$$p(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} f(u)e^{-iux}du = \frac{1}{2\pi}\int_{-\infty}^{\infty} \frac{e^{-iux}}{1-\frac{2iu}{3}}du.$$

Для вычисления этого интеграла можно воспользоваться следующей

Лемма 3.6 (Интегральная формула Коши) *Пусть $f(z)$ — функция, однозначная и аналитическая в области G и на ее границе Γ, состоящей из одного или нескольких спрямляемых контуров, ориентированных положительно относительно области G. Тогда для всякой точки $z_0 \in G$ справед-*

лива интегральная формула Коши:

$$f(z_0) = \frac{1}{2\pi i}\int_\Gamma \frac{f(u)}{u - z_0}du.$$

Доказательство. см. [21]

В нашем случае в качестве контура Γ возьмем замкнутую кривую, проходимую против часовой стрелки, состоящую из отрезка $[-R, R]$ и нижней полуокружности γ с центром в точке $(0; 0)$ и радиусом R, тогда:

$$\int_\Gamma \frac{e^{-iux}}{1 - \frac{2iu}{3}}du = \int_{-R}^{R} \frac{e^{-iux}}{1 - \frac{2iu}{3}}du + \int_\gamma \frac{e^{-iux}}{1 - \frac{2iu}{3}}du.$$

Для вычисления интеграла в левой части применим лемму 3.6:

$$\int_\Gamma \frac{e^{-iux}}{1 - \frac{2iu}{3}}du = \frac{3}{2i}\int_\Gamma \frac{e^{-iux}}{u + \frac{3i}{2}}du = \frac{3}{2i}2\pi i e^{-\frac{3}{2}x} = 3\pi e^{-\frac{3}{2}x}.$$

Для оценки интеграла по нижней полуокружности γ представим $u \in \gamma$ в виде $u = Re^i\phi$, где $\pi \leqslant \phi \leqslant 2\pi$. Получим следующую оценку:

$$\left|\int_\gamma \frac{e^{-iux}}{1 - \frac{2iu}{3}}du\right| = \left|\int_\pi^{2\pi} \frac{e^{-ixRe^{i\phi}}}{1 - \frac{2iRe^i\phi}{3}}iRe^{i\phi}d\phi\right| \leqslant \frac{R}{\frac{2R}{3} - 1}\int_\pi^{2\pi} e^{xR\sin\phi}d\phi \leqslant$$

$$\leqslant \frac{2R}{\frac{2R}{3} - 1}\int_0^{\pi/2} e^{-xR\sin\phi}d\phi \leqslant \frac{2R}{\frac{2R}{3} - 1}\int_0^{\pi/2} e^{-xR\frac{2\phi}{\pi}}d\phi = \frac{-2R}{\frac{2R}{3} - 1}e^{-xR\frac{2\phi}{\pi}}\frac{1}{xR\frac{2}{\pi}}\Bigg|_0^{\pi/2} \leqslant$$

$$\leqslant \frac{2R}{\frac{2R}{3} - 1}\frac{\pi}{2}\frac{1}{xR} = \frac{\pi}{x\left(\frac{2R}{3} - 1\right)}.$$

Переходя в равенстве

$$\int_{\Gamma} \frac{e^{-iux}}{1-\frac{2iu}{3}}du = \int_{-R}^{R} \frac{e^{-iux}}{1-\frac{2iu}{3}}du + \int_{\gamma} \frac{e^{-iux}}{1-\frac{2iu}{3}}du$$

к пределу при $R \to \infty$ получим:

$$\int_{-R}^{R} \frac{e^{-iux}}{1-\frac{2iu}{3}}du = 3\pi e^{-\frac{3}{2}x}.$$

Отсюда для плотности распределения величины ξ получаем:

$$p(x) = \frac{1}{2\pi} 3\pi e^{-\frac{3}{2}x} = \frac{2}{3} e^{-\frac{3}{2}x}, x \geqslant 0.$$

Рассмотренная величина ξ асимптотически имеет экспоненциальное распределение $p(x) = \lambda e^{-\lambda x}$, с параметром $\lambda = \frac{3}{2}$.

Теорема доказана.

Список литературы

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

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

[3] *П.Г.Л Дирихле* Лекции по теории чисел: В обработке и с добавлениями Р Дедекинда. Пер. с нем./Под ред. Б.И. Сегала. Изд. 3-е —М.: Книжный дом «Либроком». — 2009. — 368 с.

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

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

[6] *А.А. Бухштаб* Теория чисел. Изд. 2-е, испр. —М.: Просвещение. — 1966. — 384 с.

[7] *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.

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

[9] *И.М. Виноградов* Основы теории чисел. М.: Наука, 1972.

[10] *И.М. Виноградов* Метод тригонометрических сумм в теории чисел. М.: Наука, 1971.

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

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

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

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

[15] *А.А. Карацуба* Основы аналитической теории чисел. Изд. 2-е, испр. — М.: Едиториал УРСС. — 2004. — 184 с.

[16] *А.А. Карацуба* Суммы характеров и первообразные корни в конечных полях // Докл. АН СССР. 1968. Т.180. №6. С.1287–1289.

[17] *А.А. Карацуба* О суммах характеров с простыми числами // Докл. АН СССР. 1970. Т.190. №3. С.517–518.

[18] *А.А. Карацуба* Об оценках сумм характеров // Изв. АН СССР. 1970. Т.34. №1. С.20-30.

[19] *А.А. Карацуба* Распределение степенных вычетов и невычетов в аддитивных последовательностях // Докл. АН СССР. 1971. Т.196. №4.

[20] *Н.М. Коробов* Тригонометрические суммы и их приложения. — М.: Наука. Гл. ред. физ.-мат. пит.— 1989 —240 с. С.759–760.

[21] *М.А. Лаврентьев, Б.В. Шабат* Методы теории функций комплексного переменного:Учеб. пособие для ун-тов.— 5-е изд., испр.— М.: Наука. Гл. ред.физ.-мат. лит., 1987.— 688с.

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

[23] *Х.Л. Монтгомери* Мультипликативная теория чисел. — М.: Мир, 1974.

[24] *О.В. Попов* О квадратичных вычетах и невычетах в последовательности бесквадратных чисел // Вестник Моск. ун-та. Серия 1. Математика. Механика. 1989. №5. С. 81–83.

[25] *А.Г. Постников* Введение в аналитическую теорию чисел. — М.: Наука. Гл. ред. физ.-мат. лит. — 1971. — 416 с.

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

[27] *К. Хооли* Применение методов решета в теории чисел / Пер. с англ. В.Н. Чубарикова. — М.: Наука. Гл. ред. физ.-мат. лит. — 1987. — 136 с.

[28] *А.Н. Ширяев* Вероятность. В 2-х кн.— 3-е изд., перераб. и доп.— М.:МЦНМО, 2004.— 928 с.

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

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

[31] *D.A. Burgess* On character sums and primitive roots, // Proc. London Math. Soc. (3) 1962. **12,** P. 179–192.

[32] *D.A. Burgess* On character sums and L-series. // Proc. London Math. Soc. (3) 1962. **12,** P. 193–206.

[33] *D.A. Burgess* On character sums and L-series, II. // Proc. London Math. Soc. (3) 1963. **13,** P. 524–536.

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

[35] *G.H. Hardy, E.M. Wright* An Introduction to the Theory of Numbers // Oxford University Press. 1975. 421 p.

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

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

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

[39] *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.

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

Работы автора по теме диссертации

[41] *Д.В. Копьев* О вычетах и невычетах по системе модулей. Доклады академии наук. Т. 453, є 2, 2013. С. 136–137.

[42] *Д.В. Копьев, М.П. Минеев, В.Н. Чубариков* 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. - 369с. С. 55–64.

[43] *Д.В. Копьев* Об уязвимости одного криптографического протокола. Вестник Моск. ун-та. Серия 1. Математика. Механика. №1. 2009. С. 55–54.

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

[45] *Д.В. Копьев* 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.