Math-Net.Ru

Общероссийский математический портал

Н. Г. Мощевитин, О множествах вида $\mathcal{A} + \mathcal{B}$ и конечных цепных дробях, *Матем. сб.*, 2007, том 198, номер 4, 95–116

DOI: <https://doi.org/10.4213/sm3772>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.85.5.30

26 апреля 2023 г., 09:57:27

УДК 511

Н. Г. Мошечитин

О множествах вида $\mathcal{A} + \mathcal{B}$ и конечных цепных дробях

Доказываются оценки на количество правильных несократимых дробей со знаменателем p , начальный и конечный отрезки разложения в регулярную непрерывную дробь которых имеют ограниченные неполные частные. Результаты связаны с применением оценок неполных сумм Клоостермана по множествам вида $\mathcal{A} + \mathcal{B} \subset \mathbb{Z}_p$. Получены результаты о распределении в $\mathbb{Z}_p$ элементов множеств вида $(\mathcal{A} + \mathcal{B})^k$ и $k \cdot (\mathcal{A} + \mathcal{B})^{-1}$.

Библиография: 21 название.

Введение

Пусть $q \geq 2$ — натуральное число, $(a, q) = 1$. Через $b_\nu(a)$ мы будем обозначать неполные частные разложения числа a/q в цепную дробь:

$$\frac{a}{q} = [b_0(a); b_1(a), \dots, b_s(a)] = b_0(a) + \frac{1}{b_1(a) + \frac{1}{b_2(a) + \frac{1}{b_3(a) + \dots + \frac{1}{b_s(a)}}}}.$$

Хорошо известно, что для простого q всегда найдется целое a , $(a, q) = 1$, для которого

$$\max_{\nu} b_\nu(a) \ll \log q.$$

Это утверждение весьма просто доказывается методом усреднения (см. [1]–[3]). Аналогичная оценка (с дополнительным множителем $q/\varphi(q)$ в правой части) справедлива и для составного q (см., например, [4] и более слабое неравенство в [5]). Н. М. Коробовым, а также другими математиками неоднократно высказывалось предположение, что для некоторой абсолютной константы K для любого натурального q найдется a , $(a, q) = 1$, такое, что для всех ν выполнено $b_\nu \leq K$. Эта предположение широко известно под названием гипотезы Зарембы и до сих пор не доказано. Известно, что предположение верно с $K = 5$ в некоторых частных случаях [6], например если $q = 2^\alpha$ или $q = 3^\alpha$. Компьютерные вычисления подтверждают гипотезу. Более того, похоже, что для всех достаточно больших значений q константа K может быть взята равной 3.

В настоящей работе мы получим некоторые результаты о количестве рациональных чисел с простым знаменателем, у которых начальный и конечный

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 06-01-00518), Программы поддержки ведущих научных школ РФ (грант № НШ-1312.2006.1), Программы поддержки молодых докторов РФ (грант № МД-3003.2006.1) и фонда INTAS (грант № 03-51-5070).

отрезки разложения в цепную дробь имеют ограниченные элементы (теоремы 2 и 3). Также мы докажем оценку сверху для количества чисел с заданным знаменателем и ограниченными неполными частными (теорема 1). В заключение для простого p мы покажем, что в достаточно большой мультипликативной подгруппе по модулю p большинство элементов a таковы, что в разложении в цепную дробь a/p неполные частные ограничены величиной $O(\log p)$ (теорема 5). Точные формулировки новых результатов о цепных дробях будут даны в §§ 3 и 9.

Некоторые из доказанных нами теорем будут использовать оценки тригонометрических сумм, которые являются следствием теорем А. Вейля [7], [8]. Возможно, что полученные нами следствия могут иметь самостоятельный интерес. Так в § 5 мы формулируем одно из подобных следствий в виде теоремы об оценке тригонометрических сумм (теорема 4), а в §§ 6–8 обсуждаем ее применение. В частности, мы получим и будем использовать результаты об аддитивных и мультипликативных свойствах по простому модулю p множеств вида $\mathcal{A} + \mathcal{B}$, где $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_p$ суть некоторые множества вычетов, причем множество $\mathcal{A}$ – “большое”, а именно, его мощность больше $p^{1/2}$.

§ 1. Некоторые обозначения

Для целого числа $A_0 \in \mathbb{Z}$ и конечного набора натуральных чисел $A_1, A_2, \dots, A_l \in \mathbb{N}$ через $[A_0; A_1, \dots, A_l]$ будем обозначать регулярную цепную дробь с неполными частными $A_1, \dots, A_l$; через $K(A_1, \dots, A_l)$ – континуант чисел $A_1, \dots, A_l$, т.е. знаменатель несократимой дроби $[A_0; A_1, \dots, A_l]$.

Обозначим через $N(r, q)$ количество натуральных чисел a из отрезка $[1, q]$ таких, что $(a, q) = 1$ и в разложении в регулярную цепную дробь $a/q = [0; A_1(a), \dots, A_{l(a)}(a)]$ все неполные частные $A_j(a)$ ограничены величиной r .

Пусть $R(q)$ обозначает множество всех (возможно, сократимых) рациональных дробей из отрезка $[0, 1]$, знаменатель которых равен q .

Через $F_r(q)$ будем обозначать множество всех рациональных чисел $a/q \in [0, 1]$ со знаменателем равным q , при разложении в цепную дробь которых все неполные частные не превосходят величины r . Через $Q_r(q)$ будем обозначать множество рациональных чисел a/b из отрезка $[0, 1]$ таких, что $b < q$ и все неполные частные разложения a/b в цепную дробь не превосходят r . Ясно, что $Q_r(q) = \bigcup_{1 \leq t < q} F_r(t)$. Через F_r будем обозначать множество иррациональных чисел, все неполные частные которых, кроме нулевого, ограничены сверху величиной r .

§ 2. О результатах Д. Хенсли

Обозначим через κ_r хаусдорфову размерность множества F_r . Для этой размерности известно асимптотическое равенство

$$\kappa_r = 1 - \frac{6}{\pi^2} \frac{1}{r} - \frac{72}{\pi^4} \frac{\log r}{r^2} + O\left(\frac{1}{r^2}\right), \quad r \rightarrow \infty, \quad (1)$$

принадлежащее Д. Хенсли [9]. Отметим, что в более ранней работе Д. Хенсли [10] имеется более простое неравенство

$$1 - \frac{5}{2r} < \kappa_r < 1 - \frac{1}{10(r+1)}. \quad (2)$$

Нам понадобится оценка сверху для мощности множества $Q_r(q)$

$$\#Q_r(q) \leq 32q^{2\kappa_r}, \quad (3)$$

которая следует из формулы (23) работы [10]. В этой же работе Д. Хенсли получил нижнюю оценку вида

$$\#Q_r(q) \geq \varepsilon q^{2\kappa_r}, \quad (4)$$

где ε есть некоторая абсолютная положительная постоянная, которая в указанной работе не вычислена. Доказательство этих оценок элементарно и связано с рассмотрением ζ -функции Гуда. Отметим, что в последующей работе [11] Д. Хенсли дает более точные (и гораздо более сложные) результаты о мощности множества $Q_r(q)$. Там доказано, что

$$\#Q_r(q) \sim K(r)q^{2\kappa_r}, \quad q \rightarrow \infty, \quad (5)$$

где величина $K(r)$ ограничена сверху и снизу не зависящими от r постоянными.

§ 3. Множества $B_r^\pm(t, q)$

Если $u/v \in Q_r(t)$, то, разлагая u/v в цепную дробь, имеем

$$\frac{u}{v} = [0; A_1, \dots, A_l], \quad K(A_1, \dots, A_l) < t.$$

Выберем из множества $Q_r(t)$ те числа $u/v = [0; A_1, \dots, A_l]$, для которых будет выполнено

$$K(A_1, \dots, A_l, 1) \geq t.$$

Обозначим получившееся множество чисел через $\overline{Q_r(t)}$.

ЛЕММА 1. Пусть натуральное $t \geq 1$. Если $\xi \in F_r(q)$ и $q > t$ или если $\xi \in F_r$, то любая подходящая или промежуточная дробь u/v для ξ со знаменателем $v < t$ будет лежать в множестве $Q_r(t)$. Кроме того, существует единственная дробь $u/v \in \overline{Q_r(t)}$ такая, что u/v есть подходящая или промежуточная дробь к числу ξ .

Лемма является очевидным следствием определения множества $\overline{Q_r(t)}$.

Рассмотрим какое-нибудь рациональное число

$$\frac{u}{v} = [0; A_1, \dots, A_{l-1}, A_l] \in Q_r(t), \quad A_l \geq 2.$$

Вместе с ним рассмотрим числа u'/v' , u''/v'' , определяемые равенствами

$$\begin{aligned} \frac{u'}{v'} &= [0; A_1, \dots, A_{l-1}, r+1], \\ \frac{u''}{v''} &= [0; A_1, \dots, A_{l-1}, A_l-1, r+1], \end{aligned}$$

и отрезок $J_{u/v}$ с концами u'/v' , u''/v'' . Понятно, что если $\xi \in J_{u/v}$, то дробь u/v будет подходящей или промежуточной для числа ξ . Верно и обратное: если u/v есть подходящая или промежуточная дробь для ξ и $\xi \in F_r$ или $\xi \in F_r(q)$, то $\xi \in J_{u/v}$. Отметим также, что если число $\xi \in F_r$ (или $\xi \in F_r(q)$) принадлежит двум различным отрезкам J_{u_1/v_1} , J_{u_2/v_2} , то одна из дробей u_j/v_j , $j = 1, 2$, будет подходящей или промежуточной для другой и, поскольку все неполные частные у ξ ограничены величиной r , один из отрезков J_{u_1/v_1} , J_{u_2/v_2} лежит внутри другого.

Из сказанного выше следует, что для двух различных дробей $u_1/v_1, u_2/v_2 \in \overline{Q_r(t)}$ выполнено

$$J_{u_1/v_1} \cap J_{u_2/v_2} = \emptyset. \quad (6)$$

С использованием отрезка $J_{u/v}$ мы переформулируем лемму 1.

СЛЕДСТВИЕ ЛЕММЫ 1. Пусть натуральное $t \geq 1$. Если $\xi \in F_r(q)$ и $q > t$ или если $\xi \in F_r$, то существует единственное рациональное число $u/v \in \overline{Q_r(t)}$ такое, что $\xi \in J_{u/v}$.

Поскольку u/v будет промежуточной дробью для u'/v' и u''/v'' , а $v < v', v'' < (r+1)v$, то отрезок $J_{u/v}$ имеет длину

$$\frac{1}{v^2} < |J_{u/v}| = \left| \frac{u'}{v'} - \frac{u''}{v''} \right| < \frac{2(r+1)}{v^2}. \quad (7)$$

Нам понадобится следующая

ЛЕММА 2. Для количества элементов в множестве $\overline{Q_r(t)}$ с некоторыми абсолютными постоянными c_1, c_2 при достаточно большом t выполнены оценки

$$\frac{c_1 t^{2\kappa_r}}{r} \leq \#\overline{Q_r(t)} \leq c_2 t^{2\kappa_r}.$$

ДОКАЗАТЕЛЬСТВО. Верхняя оценка сразу следует из вложения $\overline{Q_r(t)} \subset Q_r(t)$ и оценки (3). Докажем нижнюю оценку. Поскольку

$$K(A_1, \dots, A_j, 1) = K(A_1, \dots, A_j) + K(A_1, \dots, A_{j-1}) \leq 2K(A_1, \dots, A_j),$$

то

$$\overline{Q_r(t)} \subset Q_r(t) \setminus Q_r(t/2).$$

Если $u_1/v_1 \in Q_r(t) \setminus Q_r(t/2)$, то u_1/v_1 будет промежуточной или подходящей дробью для некоторого $u/v \in \overline{Q_r(t)}$. Но если все A_ν ограничены величиной r , то

$$K(A_1, \dots, A_j, 1) \geq \left(1 + \frac{1}{r+1}\right) K(A_1, \dots, A_j).$$

Стало быть, для каждого $u/v \in \overline{Q_r(t)}$ будет не более $2/(1 + (r+1)^{-1})$ чисел $u_1/v_1 \in Q_r(t) \setminus Q_r(t/2)$, являющихся промежуточными или подходящими дробями. Следовательно,

$$\#\overline{Q_r(t)} \geq \frac{2}{1 + (r+1)^{-1}} (\#Q_r(t) - \#Q_r(t/2)).$$

Теперь оценка леммы 2 вытекает из асимптотической формулы Хенсли (5).

Лемма 2 доказана.

ЗАМЕЧАНИЕ 1. Нижнюю оценку леммы 2 можно было бы доказать с использованием только простых оценок (3), (4), а не (достаточно сложного) асимптотического равенства (5). При этом ухудшатся только значения констант c_1, c_2 .

Теперь мы определим основные объекты, которые оказываются нужными в настоящей работе.

Во-первых, это множество

$$B_r^-(t, q) = R(q) \cap \left(\bigcup_{u/v \in \overline{Q_r(t)}} J_{u/v} \right) = \bigcup_{u/v \in \overline{Q_r(t)}} (R(q) \cap J_{u/v}).$$

Отметим, что если $a/q \in B_r^-(t, q)$ и p_ν/q_ν есть подходящая дробь к a/q , удовлетворяющая условию $q_\nu < t$, то в силу леммы 1 выполняется $p_\nu/q_\nu \in Q_r(t)$. Следовательно, первые ν штук неполных частных для числа a/q будут ограничены величиной r . В этом смысле мы будем говорить, что множество $B_r^-(t, q)$ состоит из тех и только тех правильных несократимых дробей со знаменателем d (здесь $d \mid q, d \geq t$), у которых *начальный отрезок* разложения в цепную дробь имеет ограниченные неполные частные.

Во-вторых, определим множество

$$B_r^+(t, q) = \left\{ a \in R(q) \mid \frac{(a/(a, q))^*}{q/(a, q)} \in B_r^-(t, q) \right\},$$

где $(a/(a, q))^*$ означает элемент кольца вычетов по модулю $d = q/(a, q)$, обратный по умножению к $a/(a, q)$.

Рассмотрим две последние подходящие дроби, возникающие при разложении несократимой дроби a/d в цепную дробь. Пусть это дроби $p_{\nu-1}/q_{\nu-1}$ и $p_\nu/q_\nu = a/d$. Хорошо известно, что

$$aq_{\nu-1} \equiv \pm 1 \pmod{d}$$

и, следовательно, $a^* \equiv \pm q_{\nu-1} \pmod{d}$. Но, с одной стороны, числа

$$\frac{b}{d} = [0; B_1, B_2, \dots, B_s], \quad B_1 \geq 2, \quad \frac{d-b}{d} = [0; 1, B_1-1, B_2, \dots, B_s]$$

принадлежат множеству $B_r^-(t, q)$ одновременно, а с другой стороны, если

$$\frac{a}{d} = [0; A_1, \dots, A_s],$$

то

$$\frac{q_{\nu-1}}{d} = [0; A_s, \dots, A_1].$$

Таким образом, можно считать, что множество $B_r^+(t, q)$ состоит из тех и только тех правильных несократимых дробей со знаменателем $d \mid q, d \geq t$, *конечный отрезок* разложения в цепную дробь которых имеет ограниченные неполные частные.

ЛЕММА 3. Пусть $t \leq \sqrt{q}$. Тогда множество $B_r^-(t, q)$ распадается в дизъюнктное объединение

$$B_r^-(t, q) = \mathcal{B}_1 \sqcup \dots \sqcup \mathcal{B}_T,$$

причем

$$\frac{c_1 t^{2\kappa_r}}{r} \leq T = \# \overline{Q_r(t)} \leq c_2 t^{2\kappa_r},$$

$$\left[\frac{q}{t^2} \right] \leq \# \mathcal{B}_j \leq \left(\frac{8q(r+1)}{t^2} + 1 \right), \quad 1 \leq j \leq T.$$

СЛЕДСТВИЕ 1. В множестве $B_r^-(t, q)$ содержится сумма множеств $\mathcal{A} + \mathcal{B}$, причем

$$A = \# \mathcal{A} = \# \overline{Q_r(t)},$$

$$\mathcal{B} = \left\{ 0, 1, 2, \dots, \left[\frac{q}{t^2} \right] - 1 \right\}.$$

СЛЕДСТВИЕ 2. При $t \leq q/2$ для количества элементов в $B_r^-(t, q)$ справедлива оценка

$$\left[\frac{q}{t^2} \right] \cdot \# \overline{Q_r(t)} \leq \# B_r^-(t, q) \leq \left(\frac{8q(r+1)}{t^2} + 1 \right) \cdot \# \overline{Q_r(t)}.$$

В частности, если $t = q^\beta$, $0 < \beta \leq 1/2$, то

$$\# B_r^-(q^\beta, q) \asymp_r q^{1+2(\kappa_r-1)\beta}.$$

ДОКАЗАТЕЛЬСТВО ЛЕММЫ 3. Упорядочим конечное множество $\overline{Q_r(t)}$ в порядке возрастания его элементов, и пусть u_ν/v_ν — ν -й его элемент. Определим $\mathcal{B}_\nu = J_{u_\nu/v_\nu} \cap R(q)$. В силу (6) имеем дизъюнктное объединение. Оценка величины T вытекает из леммы 2.

Пусть $a \in \mathcal{B}_\nu$. Тогда согласно определению отрезка $J_{u/v}$ дробь $u_\nu/v_\nu = [0; A_1(a), \dots, A_w(a)]$ есть подходящая или промежуточная к числу a/q , причем $t/2 \leq v_\nu < t$. Оценку на мощность $\mathcal{B}_\nu$ теперь сразу получаем из (6). Лемма 3 доказана.

§ 4. Основные результаты

Сначала сформулируем и докажем самый простой результат.

ТЕОРЕМА 1. Величина $N(r, q)$ допускает оценку сверху

$$N(r, q) \leq crq^{\kappa_r} \leq c_1 r q^{1-c_2/r}$$

с некоторыми абсолютными постоянными $c, c_1, c_2 > 0$.

ДОКАЗАТЕЛЬСТВО. Теорема 1 сразу вытекает из следствия леммы 1, верхней оценки из леммы 2, следствия 2 леммы 3 и верхнего неравенства из (2), если взять $t = \sqrt{q}$.

ЗАМЕЧАНИЕ 2. Оценка теоремы 1 несколько точнее неравенства

$$N(r, q) \ll \varphi(q) q^{-c_1/(r \log r)},$$

которое представляет собой теорему 1 из [12]. Отметим также, что теорема 2 из [12] дает результат слабее, чем упомянутая теорема 1 этой работы в силу неравенств из [13].

Теперь мы перейдем к описанию основных результатов настоящей работы. Они касаются асимптотических оценок на количество элементов в пересечении $B_r^-(t_1, p) \cap B_r^+(t_2, p)$ при определенных значениях параметров $t_1, t_2 < p^{1/2}$.

Прежде чем формулировать новые результаты, мы отметим, что при простом p отклонение D двумерной последовательности

$$\left(\frac{a}{p}, \frac{a^*}{p}\right) \in [0, 1)^2, \quad a = 1, \dots, p-1, \quad aa^* \equiv 1 \pmod{p}, \quad (8)$$

удовлетворяет соотношению

$$D \ll \sum_{\substack{1 \leq m_1, m_2 \leq p \\ m_1 + m_2 \neq 0}} \frac{1}{m_1 m_2} \sum_{1 \leq a \leq p-1} \exp\left(\frac{2\pi i(m_1 a + m_2 a^*)}{p}\right) \ll p^{1/2} \log^2 p$$

(см. [14; гл. 2]), здесь последнее неравенство представляет собой оценку полной суммы Клоостермана (см. [15; гл. 5] или [16; гл. 1]). Следовательно, для любых двух отрезков $\mathcal{I}_1, \mathcal{I}_2$, состоящих из последовательных натуральных чисел, с длинами I_1, I_2 такими, что

$$I_1 I_2 \gg p^{3/2+\varepsilon}, \quad \varepsilon > 0,$$

будет иметь место асимптотическая формула для числа P попаданий точек последовательности (8) в прямоугольник $\mathcal{I}_1 \times \mathcal{I}_2$:

$$P = \frac{I_1 I_2}{p} (1 + O(p^{-\varepsilon'})), \quad \varepsilon' > 0.$$

Если теперь положить $t_j = \beta_j$, $\beta_j \in (0, 1/2)$, $j = 1, 2$, и рассмотреть множества $B_r^-(t_j, p)$, то согласно лемме 3 они будут состоять из объединения отрезков натуральных чисел длины $\asymp_r p^{1-2\beta_j}$ соответственно. Теперь если

$$\beta_1 + \beta_2 < \frac{1}{4}, \quad (9)$$

то из сказанного выше сразу получается асимптотическая формула

$$\#(B_r^-(t_1, p) \cap B_r^+(t_2, p)) = \frac{\#B_r^-(t_1, p) \cdot \#B_r^+(t_2, p)}{p} (1 + O(p^\delta)), \quad \delta > 0.$$

Основными результатами настоящей работы являются асимптотические оценки для количества элементов в пересечении $B_r^-(t_1, p) \cap B_r^+(t_2, p)$ при условиях более слабых, чем (9). В частности, нам удалось получить асимптотики даже тогда, когда одно из чисел β_j близко к $1/2$.

Переходим к точным формулировкам. Определим

$$\omega_1 = \omega_1(\beta_1) = \frac{(4\kappa_r \beta_1 - 1)(1 - 2\beta_1)}{8}.$$

ТЕОРЕМА 2. Пусть $q = p$ – простое число и

$$\frac{1}{4\kappa_r} < \beta_1 < \frac{1}{2}, \quad 0 < \beta_2 < \omega_1.$$

Тогда если положить $t_j = p^{\beta_j}$, $j = 1, 2$, то для количества элементов в пересечении множеств $B_r^-(t_1, p)$ и $B_r^+(t_2, p)$ выполнена оценка снизу

$$\#(B_r^-(t_1, p) \cap B_r^+(t_2, p)) \gg_r \frac{\#B_r^-(t_1, p) \cdot \#B_r^+(t_2, p)}{p} > 0.$$

Рассмотрим функцию

$$f(\xi) = \frac{\xi(\lambda + \sigma - \xi)}{2}.$$

При $\lambda, \sigma \in (0, 1/2)$ определим величину

$$\varepsilon_0 = \frac{2 + \lambda + \sigma - \sqrt{(2 + \lambda + \sigma)^2 - 8\sigma}}{2} \in (0, \sigma),$$

являющуюся меньшим корнем уравнения

$$f(\xi) = \sigma - \xi,$$

и положим

$$\omega_2(\lambda, \sigma) = \frac{1}{2} f\left(\min\left\{\frac{\lambda + \sigma}{2}; \varepsilon_0\right\}\right) \in \left(0, \frac{\sigma}{2}\right). \quad (10)$$

ТЕОРЕМА 3. Пусть $q = p$ – простое число и

$$\frac{1}{4\kappa_r} < \beta_1 < \frac{1}{2}, \quad 0 < \beta_2 < \omega_2 = \omega_2\left(\frac{4\kappa_r\beta_1 - 1}{2}, 1 - 2\beta_1\right).$$

Тогда если положить $t_j = p^{\beta_j}$, $j = 1, 2$, то для количества элементов в пересечении множеств $B_r^-(t_1, p)$ и $B_r^+(t_2, p)$ имеет место асимптотическая формула

$$\#(B_r^-(t_1, p) \cap B_r^+(t_2, p)) = \frac{\#B_r^-(t_1, p) \cdot \#B_r^+(t_2, p)}{p} (1 + O(p^{2(\beta_2 - \omega_2)} \log p)).$$

Теоремы 2, 3 утверждают, что существуют рациональные числа со знаменателем p такие, что начальный и конечный отрезки разложения a/p в цепную дробь имеют неполные частные, ограниченные величиной r , причем, в отличие от подхода, связанного с оценкой отклонения двумерной последовательности $(a/p, a^*/p)$, применение теорем 2, 3 позволяет получать результаты в случае, когда величина β_1 может принимать значения сколь угодно близкие к $1/2$ (правда, если $\beta_1 \rightarrow 1/2$, то $\beta_2 \rightarrow 0$).

Для примера рассмотрим ситуацию, когда $\beta_1 = 1/2 - \varepsilon$ и ε мало. Тогда

$$\omega_1 \sim \frac{2\kappa_r - 1}{4} \varepsilon, \quad \omega_2 \sim \frac{2\kappa_r - 1}{2\kappa_r + 3} \varepsilon, \quad \varepsilon \rightarrow 0, \quad \omega_2 < \omega_1.$$

Таким образом, при $\omega_2 \leq \beta_2 < \omega_1$ мы можем применить только теорему 2 и получить лишь оценку снизу на количество элементов в пересечении $B_r^-(t_1, p) \cap B_r^+(t_2, p)$, а при $\beta_2 < \omega_2$ теорема 3 уже обеспечивает асимптотическую формулу.

К сожалению, нам не удастся с помощью предложенного метода доказать какие-либо оценки на мощность рассматриваемого пересечения при $\beta_1 + \beta_2 > 1/2$, и поэтому мы не в состоянии получить усиление оценки теоремы 1.

§ 5. О тригонометрических суммах

Ниже множество $\mathcal{A} \subset \mathbb{Z}_p$ будет играть роль “большого” множества, а множество $\mathcal{B} \subset \mathbb{Z}_p$ будет “маленьким” множеством. Всюду в дальнейшем мощность множеств $\mathcal{A}, \mathcal{B}$ будет обозначаться A, B соответственно. Для множества $\mathcal{A} \subset \mathbb{Z}_p$ определим величину

$$D(\mathcal{A}) = \min \left\{ h \in \mathbb{N} \mid \exists a_0 \exists g \not\equiv 0 \pmod{p} \forall a \in \mathcal{A} \right. \\ \left. \exists a' \in [a_0, a_0 + 1, a_0 + 2, \dots, a_0 + h - 1] : a \equiv a'g \pmod{p} \right\}.$$

Рассмотрим тригонометрическую сумму

$$S_m(\mathcal{A}, \mathcal{B}) = \sum_{\substack{a \in \mathcal{A}, b \in \mathcal{B} \\ a+b \not\equiv 0 \pmod{p}}} \exp \left(2\pi i \frac{m(a+b)^*}{p} \right). \quad (11)$$

ТЕОРЕМА 4. Для произвольного натурального $\nu < p$ и для произвольных множеств $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_p$ при $m \not\equiv 0 \pmod{p}$ выполняется следующая оценка тригонометрической суммы:

$$|S_m(\mathcal{A}, \mathcal{B})| \leq AB\Delta, \quad (12)$$

где

$$\Delta = \min \left\{ \left(\frac{\nu^\nu p}{AB^\nu} + \frac{4\nu\sqrt{p}}{A} \right)^{1/(2\nu)} ; \left(\frac{\nu^\nu D(\mathcal{A})}{AB^\nu} + \frac{8\nu\sqrt{p} \log p}{A} \right)^{1/(2\nu)} \right\}. \quad (13)$$

ДОКАЗАТЕЛЬСТВО. Пусть $P(x)$ и $Q(x)$ – многочлены из кольца $\mathbb{Z}_p[x]$, являющиеся взаимно простыми по модулю p и имеющие различные степени. Тогда выполнена оценка тригонометрической суммы

$$\left| \sum_{\substack{1 \leq x \leq p \\ Q(x) \not\equiv 0 \pmod{p}}} \exp \left(2\pi i \frac{P(x)(Q(x))^*}{p} \right) \right| \leq \left(r - 2 + \sum_{j=1}^r d_j \right) \sqrt{p}, \quad (14)$$

где r – число различных полюсов функции $f(x) = P(x)/Q(x)$ и d_j – кратность j -го полюса (считается, что функция $f(x)$ редуцирована по модулю p , бесконечно удаленный полюс в формуле (14) тоже учитывается). Эта оценка была доказана А. Вейлем [7], [8] с помощью методов алгебраической геометрии, элементарное доказательство можно найти в работе С. А. Степанова [17].

Если применить оценку А. Вейля (14) к функции

$$\frac{P(x)}{Q(x)} = m \left(\frac{1}{x+b_1} + \dots + \frac{1}{x+b_\nu} - \frac{1}{x+b'_1} - \dots - \frac{1}{x+b'_\nu} \right), \quad m \not\equiv 0 \pmod{p},$$

то при условии, что хотя бы для одного μ элементы b_μ и b'_μ будут различными по модулю p (внутри каждого из наборов $b_1, \dots, b_\nu$ и $b'_1, \dots, b'_\nu$ числам совпадать разрешается), получится неравенство

$$\left| \sum_{\substack{1 \leq x \leq p \\ x \not\equiv -b_j, -b'_j \pmod{p}}} \exp \left(2\pi i \frac{m((x+b_1)^* + \dots + (x+b_\nu)^* - (x+b'_1)^* - \dots - (x+b'_\nu)^*)}{p} \right) \right| \\ \leq (4\nu - 2)\sqrt{p}. \quad (15)$$

Точно так же в результате применения оценки А. Вейля (14) к функции

$$f(x) = \frac{P(x)}{Q(x)} = zx + m \left(\frac{1}{x+b_1} + \cdots + \frac{1}{x+b_\nu} - \frac{1}{x+b'_1} - \cdots - \frac{1}{x+b'_\nu} \right)$$

при аналогичных условиях на b_j, b'_j (естественно, считается, что хотя бы одно из чисел m, z не сравнимо с нулем по модулю p) получится неравенство

$$\left| \sum_{\substack{1 \leq x \leq p \\ x \not\equiv -b_j, -b'_j \pmod{p}}} \exp \left(2\pi i \frac{zx + m((x+b_1)^* + \cdots + (x+b_\nu)^* - (x+b'_1)^* - \cdots - (x+b'_\nu)^*)}{p} \right) \right| \leq 4\nu\sqrt{p}. \quad (16)$$

Из оценки (16) стандартным сведением к полной сумме (см. [18; гл. 1, § 2]) выводится неравенство для соответствующей неполной суммы: при всяком натуральном $D < p$ и всяком a_0 получается неравенство

$$\left| \sum_{\substack{a_0 \leq x \leq a_0+D-1 \\ x \not\equiv -b_j, -b'_j \pmod{p}}} \exp \left(2\pi i \frac{m((x+b_1)^* + \cdots + (x+b_\nu)^* - (x+b'_1)^* - \cdots - (x+b'_\nu)^*)}{p} \right) \right| \leq 8\nu\sqrt{p} \log p. \quad (17)$$

Прокомментируем доказательство неравенства (17). Будем обозначать тригонометрическую сумму в левой части неравенства (17) через σ_m , а тригонометрическую сумму в правой части неравенства (16) – через $\sigma_{m,z}$. Используя разрывный множитель

$$\delta_p(\xi) = \frac{1}{p} \sum_{z=0}^{p-1} \exp \left(2\pi i \frac{z\xi}{p} \right),$$

получаем

$$\begin{aligned} \sigma_m &= \sum_{l=a_0}^{a_0+D-1} \sum_{\substack{0 \leq x \leq p-1 \\ x \not\equiv -b_j, -b'_j \pmod{p}}} \delta_p(x-l) \exp \left(2\pi i \frac{m((x+b_1)^* + \cdots - (x+b'_\nu)^*)}{p} \right) \\ &= \frac{1}{p} \sum_{z=0}^{p-1} \sigma_{m,z} \left(\sum_{l=a_0}^{a_0+D-1} \exp \left(-2\pi i \frac{zl}{p} \right) \right). \end{aligned}$$

В последней сумме по переменной l область суммирования представляет собой отрезок натурального ряда от a_0 до $a_0 + D - 1$. Если $z \neq 0$, то

$$\left| \sum_l \exp \left(-2\pi i \frac{zl}{p} \right) \right| \leq \frac{1}{2\|z/p\|},$$

а если $z = 0$, то

$$\left| \sum_l \exp \left(2\pi i \frac{zl}{p} \right) \right| = D \quad \text{и} \quad \sum_{z=0}^{p-1} \left| \sum_l \exp \left(-2\pi i \frac{zl}{p} \right) \right| \leq p(1 + \log p).$$

Таким образом,

$$|\sigma_m| \leq (1 + \log p) \max_{0 \leq z \leq p-1} |\sigma_{m,z}|,$$

и применение оценки (16) сразу дает неравенство (17).

Далее стандартное сведение оценки кратной суммы с помощью неравенства Гёльдера к оценке полной суммы (16) дает желаемый результат:

$$\begin{aligned} |S_m(\mathcal{A}, \mathcal{B})|^{2\nu} &\leq A^{2\nu-1} \sum_{1 \leq a \leq p} \left| \sum_{\substack{b \in \mathcal{B} \\ b \not\equiv -a \pmod{p}}} \exp\left(2\pi i \frac{m(a+b)^*}{p}\right) \right|^{2\nu} \\ &\leq A^{2\nu-1} \sum_{\substack{b_1, \dots, b_\nu \in \mathcal{B} \\ b'_1, \dots, b'_\nu \in \mathcal{B}}} \left| \sum_{\substack{0 \leq a \leq p-1 \\ a \not\equiv -b_j, -b'_j \pmod{p}}} \exp\left(2\pi i \frac{m((a+b_1)^* + \dots + (a+b'_\nu)^*)}{p}\right) \right|^{2\nu} \\ &\leq A^{2\nu-1} (\nu^\nu B^\nu p + 4\nu B^{2\nu} \sqrt{p}). \end{aligned}$$

Точно так же (далее a_0 и g – из определения величины $D(\mathcal{A})$) можно осуществить сведение оценки рассматриваемой суммы к оценке неполной суммы (17) (в нижеследующей выкладке считается, что $a \equiv a'g \pmod{p}$, и применение оценки (17) основано на использовании сравнений $(a+b)^* \equiv g^*(a'+bg^*)^* \pmod{p}$):

$$\begin{aligned} |S_m(\mathcal{A}, \mathcal{B})|^{2\nu} &\leq A^{2\nu-1} \sum_{a_0 \leq a' \leq a_0 + D(\mathcal{A}) - 1} \left| \sum_{\substack{b \in \mathcal{B} \\ b \not\equiv -a \pmod{p}}} \exp\left(2\pi i \frac{m(a+b)^*}{p}\right) \right|^{2\nu} \\ &\leq A^{2\nu-1} \sum_{\substack{b_1, \dots, b_\nu \in \mathcal{B} \\ b'_1, \dots, b'_\nu \in \mathcal{B}}} \left| \sum_{\substack{a_0 \leq a' \leq a_0 + D(\mathcal{A}) - 1 \\ a \not\equiv -b_j, -b'_j \pmod{p}}} \exp\left(2\pi i \frac{m((a+b_1)^* + \dots + (a+b'_\nu)^*)}{p}\right) \right|^{2\nu} \\ &\leq A^{2\nu-1} (\nu^\nu D(\mathcal{A}) B^\nu + 8\nu B^{2\nu} \sqrt{p} \log p). \end{aligned}$$

В последних двух выкладках используется то, что при фиксированном наборе $b_1, \dots, b_\nu$ количество упорядоченных наборов $b'_1, \dots, b'_\nu$, совпадающих (как множества) с набором $b_1, \dots, b_\nu$, не превосходит ν^ν .

Теорема 4 доказана.

§ 6. Примеры применения теоремы 4

Теорема 4 дает нетривиальные оценки только в случае, когда $A > p^{1/2}$.

Рассмотрим случай, когда

$$A = p^{1/2+\varepsilon_1}, \quad B = p^{\varepsilon_2}, \quad 0 < \varepsilon_1 < \frac{1}{2}, \quad 0 < \varepsilon_2 < \frac{1}{2}. \quad (18)$$

Если про величину $D(\mathcal{A})$ ничего не известно, то мы должны использовать первую из величин в равенстве (13). Тогда надо положить $\nu = [1/(2\varepsilon_2)] + 1$ и мы получим оценку

$$|S_m(\mathcal{A}, \mathcal{B})| \ll ABp^{-\varepsilon_1\varepsilon_2/2-\delta}, \quad \delta = (\varepsilon_1\varepsilon_2) \frac{1-2\varepsilon_2}{2(1+2\varepsilon_2)} > 0. \quad (19)$$

Если же дополнительно известно, что

$$D(\mathcal{A}) = Ap^{\varepsilon_3}, \quad 0 < \varepsilon_3 < \frac{1}{2}, \quad (20)$$

то, положив $\nu = [(\varepsilon_3 + \varepsilon_1)/\varepsilon_2] + 1$, получаем оценку

$$|S_m(\mathcal{A}, \mathcal{B})| \ll ABp^{-\varepsilon_1\varepsilon_2/(2(\varepsilon_1+\varepsilon_2+\varepsilon_3))}(\log p)^{\varepsilon_2/(2(\varepsilon_1+\varepsilon_2+\varepsilon_3))}. \quad (21)$$

В качестве приложения этих оценок можно рассмотреть следующую задачу (ср. с вопросами, затронутыми в [19]). Рассмотрим множество

$$\mathcal{C} = \{x \in \mathbb{Z}_p \mid \exists a \in \mathcal{A}, b \in \mathcal{B}: x \equiv (a+b)^* \pmod{p}\}$$

и рассмотрим для него число Варинга

$$g(\mathcal{C}) = \min\{t \in \mathbb{N} \mid \forall \lambda \in \mathbb{Z}_p \exists x_1, \dots, x_t \in \mathcal{C}: x_1 + \dots + x_t \equiv \lambda \pmod{p}\}.$$

Применение сформулированных выше оценок тригонометрической суммы приводит к такому результату.

СЛЕДСТВИЕ. Если выполнено условие (18), то при достаточно большом p для числа Варинга справедлива оценка

$$g_p(\mathcal{C}) \leq \left\lfloor \frac{2}{\varepsilon_1\varepsilon_2} \right\rfloor + 1.$$

Если же кроме (18) выполнено еще (20), то

$$g_p(\mathcal{C}) \leq \left\lfloor \frac{2(\varepsilon_1 + \varepsilon_2 + \varepsilon_3)}{\varepsilon_1\varepsilon_2} \right\rfloor + 1.$$

ДОКАЗАТЕЛЬСТВО. Выясним, при каких значениях t неравенства из теоремы 4 позволяют устанавливать разрешимость сравнений

$$(a_1 + b_1)^* + \dots + (a_t + b_t)^* \equiv \lambda \pmod{p}, \quad a_j \in \mathcal{A}, \quad b_j \in \mathcal{B}.$$

Пусть $N_t(\lambda)$ есть число решений указанного сравнения и $N_t = \max_{\lambda} N_t(\lambda)$. Если мы убедимся, что при некотором t_0 выполнено $N_{t_0} > 0$, то, очевидно, имеет место оценка $g_p(\mathcal{C}) \leq t_0$. Обозначим через Γ количество пар (a, b) , $a \in \mathcal{A}$, $b \in \mathcal{B}$, таких, что $a + b \not\equiv 0 \pmod{p}$, и выразим число решений $N_t(\lambda)$ через разрывный множитель:

$$\begin{aligned} N_t(\lambda) &= \sum_{\substack{a_1, \dots, a_t \in \mathcal{A} \\ b_1, \dots, b_t \in \mathcal{B} \\ a_j + b_j \not\equiv 0 \pmod{p}}} \delta_p((a_1 + b_1)^* + \dots + (a_t + b_t)^* - \lambda) \\ &= \frac{\Gamma^t}{p} + \frac{1}{p} \sum_{m=1}^{p-1} (S_m(\mathcal{A}, \mathcal{B}))^t \exp\left(\frac{-2\pi im\lambda}{p}\right) \\ &= \frac{\Gamma^t}{p} + O\left(\max_{1 \leq m \leq p-1} |S_m(\mathcal{A}, \mathcal{B})|^t\right). \end{aligned}$$

Ясно, что для Γ имеет место оценка снизу: $\Gamma \geq AB - B \gg AB$. Применяя оценки для тригонометрической суммы (19) или (21), получаем, что главный член по порядку больше остаточного при

$$t = \left\lfloor \frac{2}{\varepsilon_1 \varepsilon_2} \right\rfloor + 1 \quad \text{или} \quad t = \left\lfloor \frac{2(\varepsilon_1 + \varepsilon_2 + \varepsilon_3)}{\varepsilon_1 \varepsilon_2} \right\rfloor + 1$$

соответственно, и следствие доказано.

Другое применение связано с подсчетом количества попаданий чисел $(a+b)^*$, $a \in \mathcal{A}$, $b \in \mathcal{B}$, в заданный отрезок $\mathcal{I} \pmod{p}$.

ЛЕММА 4. Пусть $\mathcal{I} = [v, v + I - 1]$ есть отрезок $\pmod{p}$ и величина $M = M(\mathcal{A}, \mathcal{B})$ определена следующим образом:

$$M = M(\mathcal{A}, \mathcal{B}) = \max_{x \pmod{p}} \#\{(a, b) \in (\mathcal{A}, \mathcal{B}) : a + b = x\}.$$

Тогда для числа попаданий

$$T(\mathcal{A}, \mathcal{B}; \mathcal{I}) = \#\{(a, b) \in (\mathcal{A}, \mathcal{B}) : (a + b)^* \in \mathcal{I}\}$$

при любом натуральном $1 \leq H \leq I$ справедлива формула

$$\left| T(\mathcal{A}, \mathcal{B}; \mathcal{I}) - \frac{ABI}{p} \right| \leq AB \left(2 + \log \frac{I}{H} \right) \Delta + HM,$$

где Δ допускает оценку вида (13).

ДОКАЗАТЕЛЬСТВО. Лемма 4 доказывается стандартной процедурой сглаживания. Поскольку

$$T(\mathcal{A}, \mathcal{B}; \mathcal{I}) = \sum_{z \in \mathcal{I}} \sum_{\substack{a \in \mathcal{A}, b \in \mathcal{B} \\ a+b \not\equiv 0 \pmod{p}}} \delta_p((a+b)^* - z),$$

то при каждом $l \leq H - 1$ имеем

$$T(\mathcal{A}, \mathcal{B}; \mathcal{I}) = \sum_{z \in \mathcal{I}} \sum_{\substack{a \in \mathcal{A}, b \in \mathcal{B} \\ a+b \not\equiv 0 \pmod{p}}} \delta_p((a+b)^* - z - l) + 2\Theta_l l M, \quad |\Theta_l| \leq 1.$$

Суммируя по l в пределах $0 \leq l \leq H - 1$, получаем

$$T(\mathcal{A}, \mathcal{B}; \mathcal{I}) = \frac{1}{H} \sum_{0 \leq l \leq H-1} \sum_{z \in \mathcal{I}} \sum_{\substack{a \in \mathcal{A}, b \in \mathcal{B} \\ a+b \not\equiv 0 \pmod{p}}} \delta_p((a+b)^* - z - l) + \Theta H M, \quad |\Theta| \leq 1.$$

Далее, разлагаем разрывный множитель $\delta_p(\cdot)$ в конечный ряд Фурье:

$$\begin{aligned} T(\mathcal{A}, \mathcal{B}; \mathcal{I}) &= \frac{ABI}{p} + \Theta H M \\ &+ \frac{1}{pH} \sum_{m=1}^{p-1} \sum_{l=0}^{H-1} \sum_{z \in \mathcal{I}} \sum_{\substack{a \in \mathcal{A}, b \in \mathcal{B} \\ a+b \not\equiv 0 \pmod{p}}} \exp\left(2\pi i \frac{m(a+b)^* - ml - mz}{p}\right). \end{aligned}$$

В последнем выражении при каждом фиксированном m слагаемое распадается в произведение трех тригонометрических сумм. Одна из них как раз представляет собой тригонометрическую сумму из теоремы 4, и для нее мы применяем оценку (12), равномерную по m . Для двух других множителей имеем

$$\left| \sum_{l=0}^{H-1} \exp\left(2\pi i \frac{-ml}{p}\right) \right| \leq \max\left(H, \frac{p}{m}\right), \quad \left| \sum_{z=v}^{v+I-1} \exp\left(2\pi i \frac{-mz}{p}\right) \right| \leq \max\left(I, \frac{p}{m}\right).$$

Теперь получим:

$$\begin{aligned} \left| T(\mathcal{A}, \mathcal{B}; \mathcal{J}) - \frac{ABI}{p} \right| &\leq \frac{AB\Delta}{pH} \sum_{m=1}^{p-1} \max\left(H, \frac{p}{m}\right) \max\left(I, \frac{p}{m}\right) + HM \\ &\leq AB\Delta \left(2 + \log \frac{I}{H}\right) + HM. \end{aligned}$$

Лемма 4 доказана.

Отметим, что всегда $M(\mathcal{A}, \mathcal{B}) \leq B$, и если выполнены условия (18), то можно взять $H = p^{1/2}$. Тогда второе слагаемое в оценке леммы по порядку меньше первого.

СЛЕДСТВИЕ. Если выполнено условие (18), то при произвольном $\delta_1 < \delta$ (здесь δ определено в (19)) справедливо равенство

$$T(\mathcal{A}, \mathcal{B}; \mathcal{J}) = \frac{ABI}{p} + O(ABp^{-\varepsilon_1 \varepsilon_2 / 2 - \delta_1}),$$

в котором главный член больше остаточного при

$$I \geq p^{1 - \varepsilon_1 \varepsilon_2 / 2}.$$

Если же кроме (18) выполнено еще (20), то

$$T(\mathcal{A}, \mathcal{B}; \mathcal{J}) = \frac{ABI}{p} + O(ABp^{-\varepsilon_1 \varepsilon_2 / (2(\varepsilon_1 + \varepsilon_2 + \varepsilon_3))} (\log p)^{1 + \varepsilon_2 / (2(\varepsilon_1 + \varepsilon_2 + \varepsilon_3))}),$$

причем в этой формуле главный член больше остаточного при I по порядку большему, чем

$$p^{1 - \varepsilon_1 \varepsilon_2 / (2(\varepsilon_1 + \varepsilon_2 + \varepsilon_3))} (\log p)^{1 + \varepsilon_2 / (2(\varepsilon_1 + \varepsilon_2 + \varepsilon_3))}.$$

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2. Согласно следствию 1 леммы 3 в множестве $B_r^-(t_1, q)$ содержится сумма множеств $\mathcal{A} + \mathcal{B} \subset B_r^-(t, q)$, а при рассматриваемом в теореме 2 выборе параметров с учетом леммы 2 выполнено

$$A = \#\mathcal{A} \asymp_r p^{1/2 + (4\kappa_r \beta_1 - 1)/2}, \quad B = \#\mathcal{B} \asymp_r p^{1 - 2\beta_1}.$$

Таким образом, для тригонометрической суммы вида (11) по множеству $\mathcal{A} + \mathcal{B} \subseteq B_r^-(t_1, p)$ (напомним, что $(\mathcal{A} + \mathcal{B})^* \subseteq B_r^+(t_1, p)$) выполнена оценка (19) с

$$\varepsilon_1 = \frac{4\kappa_r \beta_1 - 1}{2}, \quad \varepsilon_2 = 1 - 2\beta_1.$$

С другой стороны, согласно лемме 3 множество $B_r^-(t_2, q)$ представляется в виде объединения отрезков

$$B_r^-(t_2, q) = \mathcal{B}_1^2 \sqcup \cdots \sqcup \mathcal{B}_{T_2}^2, \quad (22)$$

причем, применяя лемму 2, можем утверждать, что

$$T_2 \asymp_r p^{(4\kappa_r\beta_2-1)/2}, \quad \#\mathcal{B}_j^2 \asymp_r p^{1-2\beta_2}. \quad (23)$$

Теперь первая часть следствия леммы 4 обеспечивает асимптотическую формулу для числа попаданий элементов множества $(\mathcal{A} + \mathcal{B})^*$ в каждый из отрезков $\mathcal{B}_j$. Суммируя эти числа по всем отрезкам, получаем заключение теоремы 2.

§ 7. Тригонометрические суммы по множеству $\mathcal{B}_1 \sqcup \cdots \sqcup \mathcal{B}_T$

Пусть натуральные числа $d_1, \dots, d_T$ таковы, что

$$c_1 p^\sigma \leq d_j \leq c_2 p^\sigma, \quad j = 1, \dots, T,$$

с некоторыми положительными постоянными $c_1, c_2, \sigma > 0$. В настоящем параграфе константы в символах “ $\ll$ ”, “ $\asymp$ ” могут зависеть от этих величин c_1, c_2 .

Рассмотрим *непересекающиеся* множества натуральных чисел

$$\mathcal{B}_j = [a_j, a_j+1, a_j+2, \dots, a_j+d_j], \quad j = 1, \dots, T, \quad 0 \leq a_1 < a_2 < \cdots < a_T \leq p-1,$$

и пусть

$$\mathcal{E} = \mathcal{B}_1 \sqcup \cdots \sqcup \mathcal{B}_T \subseteq [a_1, a_1+1, \dots, a_1+D-1].$$

Возьмем также произвольное $\varepsilon \in (0, \sigma)$.

ЛЕММА 5. Пусть $m \not\equiv 0 \pmod{p}$ и $\nu \in \mathbb{N}$. Тогда для тригонометрической суммы S по множеству $\mathcal{E}$ выполнена оценка

$$|S| = \left| \sum_{x \in \mathcal{E}} \exp\left(2\pi i \frac{mx^*}{p}\right) \right| \leq E\Delta_1,$$

где E есть мощность множества $\mathcal{E}$ и

$$\Delta_1 \leq C(c_1, c_2, \nu) \left(\left(\min \left\{ \frac{p^{1-\sigma-\varepsilon(\nu-1)}}{T} + \frac{\sqrt{p}}{Tp^{\sigma-\varepsilon}}; \frac{D}{Tp^{\sigma+\varepsilon(\nu-1)}} + \frac{\sqrt{p} \log p}{p^{\sigma-\varepsilon}T} \right\} \right)^{1/(2\nu)} + \frac{1}{p^{\sigma-\varepsilon}} \right).$$

ДОКАЗАТЕЛЬСТВО. Представим каждое $\mathcal{B}_j$ в виде объединения

$$\mathcal{B}_j = \bigsqcup_{1 \leq i \leq h_j} E_{j,i} \sqcup H_j$$

так, чтобы каждое $E_{j,i}$ состояло ровно из $[p^\varepsilon]$ последовательных натуральных чисел, а множество H_j состояло из не более p^ε элементов. Тогда

$$\mathcal{E} = \bigsqcup_{1 \leq j \leq T} \bigsqcup_{1 \leq i \leq h_j} E_{j,i} \bigsqcup_{1 \leq j \leq T} H_j.$$

Оценим сумму по множеству $\bigsqcup H_j$ тривиально:

$$\left| \sum_{x \in \bigsqcup H_j} \exp\left(2\pi i \frac{mx^*}{p}\right) \right| \leq \sum_{1 \leq j \leq T} \#H_j \leq Tp^\varepsilon.$$

Далее, положим $a_{j,i} = \min E_{j,i}$ и определим множество

$$\mathcal{A} = \{a_{j,i} \mid j = 1, \dots, T, i = 1, \dots, h_j\}.$$

Ясно, что

$$A = \sum_{1 \leq j \leq T} h_j \asymp Tp^{\sigma-\varepsilon}, \quad D(\mathcal{A}) \leq D.$$

Рассмотрим также множество

$$\mathcal{B} = \{0, 1, \dots, [p^\varepsilon] - 1\}.$$

Тогда

$$\bigsqcup_{1 \leq j \leq T} \bigsqcup_{1 \leq i \leq h_j} E_{j,i} = \mathcal{A} + \mathcal{B}$$

и применение теоремы дает оценку

$$\left| \sum_{x \in \bigsqcup_{1 \leq j \leq T} \bigsqcup_{1 \leq i \leq h_j} E_{j,i}} \exp\left(2\pi i \frac{mx^*}{p}\right) \right| \ll Tp^\sigma \left(\min \left\{ \frac{p^{1-\sigma-\varepsilon(\nu-1)}}{T} + \frac{\sqrt{p}}{Tp^{\sigma-\varepsilon}}; \frac{D}{Tp^{\sigma+\varepsilon(\nu-1)}} + \frac{\sqrt{p} \log p}{p^{\sigma-\varepsilon}T} \right\} \right)^{1/(2\nu)},$$

откуда сразу вытекает утверждение леммы. Лемма 5 доказана.

Посмотрим, какую оценку для тригонометрической суммы дает лемма 5 в типичной ситуации, аналогичной (18). Пусть

$$T = p^{1/2+\varepsilon_1}, \quad \sigma = \varepsilon_2, \quad 0 < \varepsilon_j < \frac{1}{2}.$$

Тогда выбор $\nu = [1/(2\varepsilon)] + 1 < 1/\varepsilon$ и оптимизация по параметру ε как раз дает оценку

$$\Delta_1 \ll p^{-2\omega_2(\varepsilon_1, \varepsilon_2)},$$

где величина $\omega_2(\lambda, \sigma)$ определена в (10). Если $(1 + (\varepsilon_1 + \varepsilon_2)/2)^2 \leq 2\varepsilon_2$, то минимум в формуле (10) достигается на первой величине и для понижающего множителя в оценке тригонометрической суммы получается неравенство

$$\Delta_1 \ll p^{-(\varepsilon_1 + \varepsilon_2)^2/8}. \quad (24)$$

Напомним, что в рассмотренном ранее примере применения теоремы 4 понижающий множитель оценивается величиной $p^{-\varepsilon_1 \varepsilon_2/2-\delta}$. Если, например, $\varepsilon_2 > \varepsilon_1/(3 - \sqrt{8})$ и оба ε_j малы, то

$$\frac{\varepsilon_1 \varepsilon_2}{2} + \delta < \varepsilon_1 \varepsilon_2 < \frac{(\varepsilon_1 + \varepsilon_2)^2}{8}$$

и новый понижающий множитель из (24) лучше.

По аналогии с леммой 4 получаем

СЛЕДСТВИЕ ЛЕММЫ 5. Для числа попаданий

$$T(\mathcal{E}; \mathcal{I}) = \#\{a \in \mathcal{E} : a^* \in \mathcal{I}\}$$

в отрезок $\mathcal{I}$, состоящий из I подряд идущих целых чисел, выполнено

$$T(\mathcal{E}; \mathcal{I}) = \frac{EI}{p} + O(Ep^{-2\omega_2(\lambda, \sigma)} \log p).$$

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 3. Согласно лемме 3

$$B_r^-(t_1, q) = \mathcal{B}_1^1 \sqcup \dots \sqcup \mathcal{B}_{T_1}^1,$$

причем при нашем выборе параметров

$$T_1 \asymp_r p^{2\kappa_r \beta_1}, \quad \#\mathcal{B}_j \asymp_r p^{1-2\beta_1}.$$

В то же время для $B_r^-(t_2, p)$ справедливо представление (22) с параметрами (23). Таким образом, каждый отрезок $\mathcal{B}_j^2$ имеет длину $\gg p^{1-2\beta_2}$ и следствие леммы 5 дает асимптотическую формулу, в которой главный член по порядку больше остаточного. Если теперь просуммировать число попаданий точек вида $a^*, a \in B_r^-(t_1, p)$ в отрезок $\mathcal{B}_j^2$ по всем j от 1 до T_2 , то получится именно та асимптотическая формула, которая имеется в заключении теоремы 3. Теорема 3 доказана.

§ 8. О суммах значений характеров по множествам вида $\mathcal{A} + \mathcal{B}$

По аналогии с теоремой могут быть доказаны результаты об оценке сумм значений числовых характеров по простому модулю p .

Здесь мы приведем только формулировки, поскольку, во-первых, доказательства (основанные на сведениях к оценкам А. Вейля [7], [8]) следуют стандартной схеме и мало отличаются от доказательства теоремы 4 и, во-вторых, подробно рассмотренный в работе [20] частный случай множеств, состоящих из чисел с пропущенными цифрами, мало отличается от общего случая (все имеющиеся в [20] рассуждения переносятся на общий случай практически дословно).

ПРЕДЛОЖЕНИЕ. Для простого p и произвольного натурального $\nu < p$, для произвольных множеств $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_p$ и для неглавного характера χ по модулю p выполняется следующая оценка суммы значений характеров:

$$|\sigma(\mathcal{A}, \mathcal{B})| = \left| \sum_{a \in \mathcal{A}, b \in \mathcal{B}} \chi(a+b) \right| \leq AB\Delta,$$

где

$$\Delta \ll_{\nu} \min \left\{ \left(\frac{p}{AB^{\nu}} + \frac{\sqrt{p}}{A} \right)^{1/(2\nu)} ; \left(\frac{D(\mathcal{A})}{AB^{\nu}} + \frac{\sqrt{p} \log p}{A} \right)^{1/(2\nu)} \right\},$$

а величина $D(\mathcal{A})$ определена в § 5.

Точно так же, как и в § 6, сразу получаем аналогичные следствия.

СЛЕДСТВИЕ. Рассмотрим случай, когда выполнено (18). Если про величину $D(\mathcal{A})$ ничего не известно, то имеет место оценка

$$|\sigma_m(\mathcal{A}, \mathcal{B})| \ll ABp^{-\varepsilon_1\varepsilon_2/2-\delta}, \quad \delta > 0.$$

Если же дополнительно имеется оценка (20), то

$$|\sigma(\mathcal{A}, \mathcal{B})| \ll ABp^{-\varepsilon_1\varepsilon_2/(2(\varepsilon_1+\varepsilon_2+\varepsilon_3))}(\log p)^{\varepsilon_2/(2(\varepsilon_1+\varepsilon_2+\varepsilon_3))}.$$

Если теперь рассмотреть множества

$$\mathcal{S} = \{x \in \mathbb{Z}_p \mid \exists a \in \mathcal{A}, b \in \mathcal{B}: x \equiv (a+b) \pmod{p}\}$$

и для него мультипликативное число Варинга

$$g(\mathcal{S}) = \min\{t \in \mathbb{N} \mid \forall \lambda \in \mathbb{Z}_p \exists x_1, \dots, x_t \in \mathcal{S}: x_1 \cdots x_t \equiv \lambda \pmod{p}\},$$

то применение оценок сумм значений характеров дает

СЛЕДСТВИЕ. Если выполнено условие (18), то при достаточно большом p выполнено $g_p(\mathcal{S}) \ll 1/(\varepsilon_1\varepsilon_2)$. Если же кроме (18) выполнено еще и (20), то $g_p(\mathcal{S}) \ll (\varepsilon_1 + \varepsilon_2 + \varepsilon_3)/(\varepsilon_1\varepsilon_2)$.

§ 9. О числах с неполными частными, ограниченными величиной $O(\log p)$, в мультипликативных подгруппах по модулю p

Хорошо известно, что для фиксированного p большинство чисел $1 \leq a \leq p$ таковы, что неполные частные в разложении $a/p = [0; A_1, \dots, A_l]$ ограничены величиной $O(\log p)$. Ниже мы показываем, что подобное утверждение будет справедливо и для больших подгрупп мультипликативной группы $\mathbb{Z}_p^*$.

ТЕОРЕМА 5. Пусть p – простое число, R – мультипликативная подгруппа группы $\mathbb{Z}_p^*$ и с некоторым положительным η выполнено

$$\#R \geq p^{31/32+\eta}. \quad (25)$$

Тогда по крайней мере для половины элементов $a \in R$ в разложении в цепную дробь $a/p = [0; A_1, \dots, A_l]$ все неполные частные A_j ограничены величиной $32 \log p$.

Отметим, что в этой теореме мы не стремились получить наилучшее значение константы и постоянную 32, несомненно, можно уменьшить.

ДОКАЗАТЕЛЬСТВО. Положим $t = 32 \log p$ и рассмотрим величину

$$S(a) = \sum \delta_p(axy^* - 1),$$

где суммирование ведется по тем парам (x, y) , для которых

$$1 \leq x < p, \quad 1 \leq |y| < p, \quad x|y| \leq p/t,$$

$\delta_p(\cdot)$ – характеристическая функция делимости на p .

Во-первых, покажем, что если $S(a) = 0$, то в разложении в цепную дробь числа a/p все неполные частные ограничены величиной t . Действительно, равенство $S(a) = 0$ означает, что при всех $1 \leq x < p$, $1 \leq |y| < p$, $x|y| \leq p/t$, выполняется $ax - y \not\equiv 0 \pmod{p}$. Это означает, что если одновременно выполнены соотношения

$$\begin{cases} ax - y \equiv 0 \pmod{p}, \\ 1 \leq x < p, \\ 1 \leq |y| < p, \end{cases}$$

то

$$x|y| > \frac{p}{t}. \quad (26)$$

В частности, (26) выполнено и для $y = \left\| \frac{ax}{p} \right\| p$. Таким образом, для каждого x из интервала $1 \leq x \leq p-1$ будет иметь место неравенство

$$\left\| \frac{ax}{p} \right\| > \frac{1}{xt}. \quad (27)$$

Но если в разложении в цепную дробь числа a/p встретилось неполное частное $A_\nu = A$, то для знаменателя $x_{\nu-1}$ ($\nu-1$)-й подходящей дроби $y_{\nu-1}/x_{\nu-1}$ будет выполняться оценка

$$\left\| \frac{ax_{\nu-1}}{p} \right\| < \frac{1}{x_{\nu-1}A_\nu}. \quad (28)$$

Из (27), (28) сразу следует, что $A = A_\nu < t$.

Во-вторых, имеет место равенство

$$S(a) = \frac{1}{p-1} \sum_{\chi \pmod{p}} \sum_{1 \leq x \leq p-1} \sum_{1 \leq |y| \leq p/(tx)} \chi(a) \chi(x) \overline{\chi(y)},$$

где суммирование ведется по всем характерам по модулю p . Если теперь усреднить эту величину по подгруппе R и рассмотреть сумму $S = \sum_{a \in R} S(a)$, то получим

$$S = \frac{\#R}{p-1} \sum_{\chi; R} \sum_{1 \leq x \leq p-1} \sum_{1 \leq |y| \leq p/(tx)} \chi(x) \overline{\chi(y)},$$

где $\sum_{\chi; R}$ означает суммирование по всем характерам по модулю p , которые тривиальны на подгруппе R . Таких характеров в точности $(p-1)/\#R$ штук, причем один из них – это главный характер по модулю p . Теперь очевидна оценка

$$|S| \leq \#R \frac{4p \log p}{(p-1)t} + 2 \max_{\chi} \left| \sum_{1 \leq x \leq p-1} \sum_{1 \leq y \leq p/(tx)} \chi(x) \overline{\chi(y)} \right|, \quad (29)$$

где максимум берется по всем неглавным характерам по модулю p . Но

$$\left| \sum_{1 \leq x \leq p-1} \sum_{1 \leq y \leq p/(tx)} \chi(x) \overline{\chi(y)} \right| \leq \left| \sum_{1 \leq x \leq \sqrt{p/t}} \chi(x) \right|^2 + 2 \sum_{1 \leq x \leq \sqrt{p/t}} \left| \sum_{1 \leq y \leq p/(tx)} \chi(y) \right|. \quad (30)$$

Далее нам понадобится количественный вариант неравенства Берджесса (см., например, [16]), принадлежащий Карацубе (см. [21; лемма 6]). Именно, мы

будем пользоваться тем, что для каждого положительного δ при всяком положительном ε с некоторой положительной постоянной $C(\varepsilon)$ при условии, что

$$H \geq p^{1/4+\delta},$$

для любого неглавного характера χ выполняется оценка

$$\left| \sum_{1 \leq x \leq H} \chi(x) \right| \leq C(\varepsilon) H p^{-\delta^2/2+\varepsilon}.$$

Полагая в упомянутом неравенстве $\delta = 1/4 - o(1)$, получаем

$$\left| \sum_{1 \leq x \leq \sqrt{p/t}} \chi(x) \right| \ll_{\varepsilon} \sqrt{\frac{p}{t}} p^{-1/32+\varepsilon}, \quad \left| \sum_{1 \leq y \leq p/(tx)} \chi(y) \right| \ll_{\varepsilon} \frac{p}{tx} p^{-1/32+\varepsilon}.$$

Последние неравенства вместе с формулами (29), (30) и определением величины t приводят к оценке

$$|S| \leq \frac{\#R}{4} + C_1(\varepsilon) p^{15/16+\varepsilon/2} + C_2(\varepsilon) \sum_{1 \leq x \leq \sqrt{p/t}} \frac{p}{tx} p^{-1/32+\varepsilon/2} \leq \frac{\#R}{4} + C_3(\varepsilon) p^{31/32+\varepsilon}.$$

Теперь условие (25) при большом p обеспечивает неравенство для среднего значения

$$\frac{1}{\#R} \left| \sum_{a \in R} S(a) \right| = \frac{|S|}{\#R} < \frac{1}{2}.$$

Напомним, что величина $S(a)$ принимает только неотрицательные целые значения. Если теперь предположить, что она отлична от нуля для не менее чем половины элементов $a \in R$, то получаем неравенство

$$\frac{1}{2} \leq \frac{1}{\#R} \sum_{a \in R} S(a) < \frac{1}{2},$$

которое содержит противоречие. Стало быть, равенство нулю $S(a) = 0$ будет выполнено для не менее чем половины элементов подгруппы R . Теорема 5 доказана.

В заключение автор выражает глубокую признательность рецензенту за ряд ценных замечаний и за исправление многочисленных неточностей в первоначальном варианте статьи.

Список литературы

- [1] Н. М. Коробов, *Теоретико-числовые методы в приближенном анализе*, Физматгиз, М., 1963.
- [2] Н. М. Коробов, “О некоторых вопросах теории диофантовых приближений”, *УМН*, **22:3** (1967), 83–118; англ. пер.: N. M. Korobov, “Some problems in the theory of diophantine approximation”, *Russian Math. Surveys*, **22:3** (1967), 80–118.

- [3] S. K. Zaremba, “La méthode des “bons treillis” pour le calcul des intégrales multiples”, *Applications of number theory to numerical analysis*, Proc. Sympos. Univ. Montreal (Montreal, QC, 1971), Academic Press, New York, 1972, 39–119.
- [4] T. W. Cusick, “Zaremba’s conjecture and sums of the divisor function”, *Math. Comp.*, **61**:203 (1993), 171–176.
- [5] T. W. Cusick, “Products of simultaneous approximations of rational numbers”, *Arch. Math. (Basel)*, **53**:2 (1989), 154–158.
- [6] H. Niederreiter, “Dyadic fractions with small partial quotients”, *Monatsh. Math.*, **101**:4 (1986), 309–315.
- [7] A. Weil, *Sur les courbes algébriques et les variétés qui s’en déduisent*, Hermann & Cie, Paris, 1948.
- [8] A. Weil, “On some exponential sums”, *Proc. Natl. Acad. Sci. USA*, **34**:5 (1948), 204–207.
- [9] D. Hensley, “Continued fraction Cantor sets, Hausdorff dimension, and functional analysis”, *J. Number Theory*, **40**:3 (1992), 336–358.
- [10] D. Hensley, “The distribution of badly approximable numbers and continuants with bounded digits”, *Théorie des nombres* (Québec, PQ, 1987), de Gruyter, Berlin, 1989, 371–385.
- [11] D. Hensley, “The distribution of badly approximable rationals and continuants with bounded digits, II”, *J. Number Theory*, **34**:3 (1990), 293–334.
- [12] С. В. Конягин, Н. Г. Мощевитин, “Представление рациональных чисел конечными цепными дробями”, *УМН*, **51**:4 (1996), 159–160; англ. пер.: S. V. Konyagin, N. G. Moshchevitin, “The representation of rational numbers by terminating continued fractions”, *Russian Math. Surveys*, **51**:4 (1996), 736–738.
- [13] Н. Г. Мощевитин, “О цепных дробях и почти арифметических прогрессиях”, *УМН*, **55**:1 (2000), 189–190; англ. пер.: N. G. Moshchevitin, “On continued fractions and almost arithmetic progressions”, *Russian Math. Surveys*, **55**:1 (2000), 182–183.
- [14] Л. Кейперс, Г. Нидеррайтер, *Равномерное распределение последовательностей*, Наука, М., 1985; пер. с англ.: L. Kuipers, H. Niederreiter, *Uniform distribution of sequences*, Pure Appl. Math., Wiley-Intersci., New York–London–Sydney, 1974.
- [15] Р. Лидл, Г. Нидеррайтер, *Конечные поля*, т. 1, Мир, М., 1988; пер. с англ.: R. Lidl, H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl., **20**, Addison-Wesley, Reading, MA, 1983.
- [16] С. А. Степанов, *Арифметика алгебраических кривых*, Наука, М., 1991; англ. пер.: S. A. Stepanov, *Arithmetic of algebraic curves*, Monogr. Contemp. Math., Consultants Bureau, New York, 1994.
- [17] С. А. Степанов, “Об оценке рациональных тригонометрических сумм с простым знаменателем”, *Сборник статей. Посвящается академику И. М. Виноградову к его 80-летию*. I, Тр. МИАН, **112**, Наука, М., 1971, 346–371; англ. пер.: S. A. Stepanov, “On estimating rational trigonometric sums with prime denominator”, *Proc. Steklov Inst. Math.*, **112** (1973), 358–385.
- [18] Н. М. Коробов, *Тригонометрические суммы и их приложения*, Наука, М., 1989; англ. пер.: N. M. Korobov, *Exponential sums and their applications*, Math. Appl. (Soviet Ser.), **80**, Kluwer Acad. Publ., Dordrecht, 1992.
- [19] С. В. Конягин, “Оценки тригонометрических сумм по подгруппам и сумм Гаусса”, IV Международная конференция “Современные проблемы теории чисел и ее приложения”, посвященная 180-летию П. Л. Чебышева и 110-летию И. М. Виноградова: Актуальные проблемы, ч. III (Тула, 2001), М., 2002, 86–114.

- [20] W. D. Banks, A. Conflitti, I. E. Shparlinski, “Character sums over integers with restricted g -ary digits”, *Illinois J. Math*, **46**:3 (2002), 819–836.
- [21] А. А. Карацуба, “Суммы характеров с простыми числами”, *Изв. АН СССР. Сер. матем.*, **34**:2 (1970), 299–321; англ. пер.: A. A. Karacuba, “Sums of characters over prime numbers”, *Math. USSR-Izv.*, **4**:2 (1970), 303–326.

Н. Г. Мощевитин (N. G. Moshchevitin)

Московский государственный университет

им. М. В. Ломоносова

E-mail: moshchevitin@rambler.ru

Поступила в редакцию

19.04.2005 и 17.11.2006