Math-Net.Ru

Общероссийский математический портал

А. В. Устинов, О точках модулярной гиперболы под графиком линейной функции, *Матем. заметки*, 2015, том 97, выпуск 2, 296–301

DOI: <https://doi.org/10.4213/mzm10314>

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: 54.162.127.20

26 апреля 2023 г., 12:48:03

О точках модулярной гиперболы под графиком линейной функции

А. В. Устинов

Для числа решений сравнения $xy \equiv 1 \pmod{p}$ под графиком линейной функции доказывается асимптотическая формула с корневым понижением в остаточном члене.

Библиография: 9 названий.

DOI: 10.4213/mzm10314

Ряд теоретико-числовых задач сводится к исследованию точек модулярной гиперболы (см. обзор [1])

$$\mathcal{H}_p = \{(x, y) : xy \equiv 1 \pmod{p}, 1 \leq x, y < p\}.$$

В данной работе мы ограничимся рассмотрением простого модуля p и точками внутри квадрата $[1, p]^2$, хотя в приложениях возникают и более общие ситуации. Случай составного модуля и произвольной области может быть проанализирован аналогично (см. [2]).

Распределение точек модулярной гиперболы можно изучать, рассматривая суммы вида

$$T_p[F] = \sum_{(x, y) \in \mathcal{H}_p} F\left(\frac{x}{p}, \frac{y}{p}\right),$$

где $F: [0, 1]^2 \rightarrow \mathbb{C}$ – произвольная функция. В частности, если

$$A(x, y) = \begin{cases} 1, & \text{если } (x, y) \in A, \\ 0, & \text{если } (x, y) \notin A, \end{cases}$$

характеристическая функция множества A , то $T_p[A]$ есть число решений сравнения $xy \equiv 1 \pmod{p}$, для которых $(x/p, y/p) \in A$. Величина $T_p[F]$ асимптотически ведет себя как

$$p \cdot I[F] = p \int_0^1 \int_0^1 F(x, y) dx dy.$$

Работа выполнена при поддержке фонда “Династия” и Российского фонда фундаментальных исследований (грант № 14-01-90002).

Остаточный член $R_p[F]$ в асимптотической формуле

$$T_p[F] = p \cdot I[F] + R_p[F]$$

обычно оценивается с помощью сумм Клостермана

$$K_p(m, n) = \sum_{(x, y) \in \mathcal{H}_p} e\left(\frac{mx + ny}{p}\right),$$

где $e(z) = e^{2\pi iz}$. Из оценки Вейля (см. [3]), которая утверждает, что при $(m, n) \not\equiv (0, 0) \pmod{p}$

$$|K_p(m, n)| \leq 2\sqrt{p}, \quad (1)$$

следует, что для прямоугольника $\Pi = [a_1, b_1] \times [a_2, b_2] \subset [0, 1]^2$ (см., например, [2])

$$R_p[\Pi] \ll \sqrt{p} \log^2 p. \quad (2)$$

В общем случае остаток $R_p[A]$ можно оценивать, аппроксимируя данную область A прямоугольниками, что приводит к оценке $R_p[A] \ll p^{3/4} \log p$. Если A — это область под графиком дважды непрерывно дифференцируемой функции, то можно использовать метод ван дер Корпута (см. [4], [2]), который обычно приводит к оценкам вида $R_p[A] \ll p^{2/3+\varepsilon}$ (см. [5], [6]).

В некоторых задачах возникает необходимость в рассмотрении ситуации, когда A есть область под графиком линейной функции (см. [7]–[9]). Целью данной работы является распространение оценки (2) на этот случай. В частности, из предлагаемого результата следует, что для произвольного n -угольника $M \subset [0, 1]^2$

$$T_p[M] = p \cdot I[M] + O(n\sqrt{p} \log^2 p).$$

ТЕОРЕМА. Пусть p — простое число, и пусть $f(x) = \alpha x + \beta$, $0 < a \leq b < 1$, $0 \leq f(a), f(b) < 1$, и

$$A = \{(x, y) : a \leq x \leq b, 0 < y \leq f(x)\}.$$

Тогда

$$T_p[A] = p \cdot I[A] + O(\sqrt{p} \log^2 p).$$

ДОКАЗАТЕЛЬСТВО. Если $c = f(a)$, $d = f(b)$ и $\alpha \geq 0$, то область $A \cup A'$, где

$$A' = \{(x, y) : c \leq y \leq d, 0 < x \leq f^{-1}(y)\}$$

можно представить как объединение двух прямоугольников, для каждого из которых выполняется оценка (2) (при $\alpha < 0$ аналогичным свойством обладает симметрическая разность A и A'). Поскольку из двух функций f и f^{-1} всегда можно выбрать ту, для которой коэффициент углового наклона по модулю не превосходит единицы, доказательство теоремы достаточно провести при условии, что $|\alpha| \leq 1$.

Кроме того, доказательство теоремы всегда можно свести к случаю, когда значения функции f на отрезке $[a, b]$ находятся в интервале от $1/p$ до $1 - 1/p$. Действительно, пусть, например, $\alpha \geq 0$ и $f(b) > 1 - 1/p$. Тогда, определяя b' равенством $f(b') = 1 - 1/p$ и применяя к прямоугольнику $\Pi = \{(x, y) : a \leq x \leq b', 0 < y \leq 1 - 1/p\}$

формулу (2), получаем, что задача сводится к рассмотрению функции f на отрезке $[a, b']$. Аналогично, если $f(a) < 1/p$, то можно перейти к отрезку $[a', b]$, где a' выбирается из условия $f(a') = 1/p$.

Заметим также, что сравнение $xy \equiv 1 \pmod{p}$ не имеет решений при $y = 0$. Поэтому $T[A] = T[A_0]$, где

$$A_0 = \left\{ (x, y) : a \leq x \leq b, \frac{1}{p} \leq y \leq f(x) \right\}.$$

Выберем $\Delta = 1/(2p)$ и определим множества $A_{\pm}$ равенствами

$$A_{\pm} = \{(x, y) \in [0, 1]^2 : a \mp \Delta \leq x < b \pm \Delta, 2\Delta \mp \Delta \leq y \leq g(x) \pm \Delta\}.$$

Сглаженные характеристические функции множеств $A_{\pm}$

$$F_{\pm}(x, y) = \frac{1}{4\Delta^2} \int_{-\Delta}^{\Delta} \int_{-\Delta}^{\Delta} A_{\pm}(x+u, y+v) du dv$$

удовлетворяют неравенствам

$$F_{-}(x, y) \leq A_0(x, y) \leq F_{+}(x, y).$$

Следовательно,

$$T_p[F_{-}] \leq T_p[A] \leq T_p[F_{+}].$$

Кроме того,

$$I[F_{\pm}] = I[A] + O\left(\frac{1}{p}\right).$$

Поэтому для доказательства теоремы достаточно проверить, что

$$R_p[F_{\pm}] = T_p[F_{\pm}] - p \cdot I[F_{\pm}] \ll \sqrt{p} \log^2 p. \quad (3)$$

Подставим в определение $T_p[F_{\pm}]$ разложение функций $F_{\pm}(x, y)$ в ряды Фурье

$$F_{\pm}(x, y) = \sum_{m, n=-\infty}^{\infty} \widehat{F}_{\pm}(m, n) e(mx + ny)$$

с коэффициентами

$$\widehat{F}_{\pm}(m, n) = \int_0^1 \int_0^1 F_{\pm}(x, y) e(-mx - ny) dx dy.$$

Учитывая равенство $K_p(0, 0) = p - 1$, приходим к оценке

$$R_p[F_{\pm}] \ll \sum_{\substack{m, n=-\infty \\ (m, n) \neq (0, 0)}}^{\infty} |\widehat{F}_{\pm}(m, n)| |K_p(m, n)| + 1. \quad (4)$$

Коэффициенты Фурье функций $F_{\pm}$ выражаются через коэффициенты Фурье характеристических функций множеств $A_{\pm}$:

$$\begin{aligned}\widehat{F}_{\pm}(m, n) &= \frac{1}{4\Delta^2} \int_{-\Delta}^{\Delta} \int_{-\Delta}^{\Delta} du dv \int_0^1 \int_0^1 A_{\pm}(x+u, y+v) e(-mx - ny) dx dy \\ &= \frac{1}{4\Delta^2} \int_{-\Delta}^{\Delta} \int_{-\Delta}^{\Delta} e(mu + nv) du dv \int_0^1 \int_0^1 A_{\pm}(x, y) e(-mx - ny) dx dy \\ &= \frac{1}{4\Delta^2} \int_{-\Delta}^{\Delta} \int_{-\Delta}^{\Delta} e(mu + nv) du dv \widehat{A}_{\pm}(m, n).\end{aligned}$$

Поскольку

$$\left| \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} e(kt) dt \right| \leq h_p(k), \quad (5)$$

где $h_p(k) = \min\{1, p/|k|\}$, то

$$|\widehat{F}_{\pm}(m, n)| \leq h_p(m) h_p(n) |\widehat{A}_{\pm}(m, n)|.$$

Оценим коэффициенты Фурье функций $A_{\pm}$. Если $n = 0$ и $m \neq 0$, то

$$\begin{aligned}\widehat{A}_{\pm}(m, 0) &= \int_{a \mp \Delta}^{b \pm \Delta} e(-mx)(\alpha x + \beta \pm 2\Delta) dx \\ &= \frac{e(-mx)(\alpha x + \beta \pm 2\Delta)}{-2\pi i m} \Big|_{x=a \mp \Delta}^{b \pm \Delta} + \frac{\alpha}{2\pi i m} \int_{a \mp \Delta}^{b \pm \Delta} e(-mx) dx \ll \frac{1}{|m|}.\end{aligned}$$

Если же $n \neq 0$, то

$$\begin{aligned}\widehat{A}_{\pm}(m, n) &= -\frac{1}{2\pi i n} \int_{a \mp \Delta}^{b \pm \Delta} dx e(-mx) \int_{2\Delta \mp \Delta}^{g(x) \pm \Delta} de(-ny) \\ &= \frac{1}{2\pi i n} \int_{a \mp \Delta}^{b \pm \Delta} e(-mx)(e(-n(2\Delta \mp \Delta)) - e(-n(g(x) \pm \Delta))) dx \\ &\ll \frac{1}{|n|} \left(\min\left\{1, \frac{1}{|m|}\right\} + \min\left\{1, \frac{1}{|m + \alpha n|}\right\} \right).\end{aligned}$$

Из (4), (5) и последней оценки следует, что

$$\begin{aligned}R[F_{\pm}] &\ll \sum_{\substack{m=-\infty \\ m \neq 0}}^{\infty} \frac{h_p(m)}{|m|} |K_p(m, 0)| \\ &\quad + \sum_{\substack{m, n=-\infty \\ n \neq 0}}^{\infty} \frac{h_p(m) h_p(n)}{|n|} \left(\min\left\{1, \frac{1}{|m|}\right\} + \min\left\{1, \frac{1}{|m + \alpha n|}\right\} \right) |K_p(m, n)| + 1.\end{aligned}$$

Выделяя слагаемые, для которых $m \equiv n \equiv 0 \pmod{p}$, и используя для остальных слагаемых неравенство (1), приходим к оценке

$$R[F_{\pm}] \ll R_1 + R_2 + R_3(\alpha) + R_4(\alpha), \quad (6)$$

где

$$R_1 = \sqrt{p} \sum_{m=1}^{\infty} \frac{h_p(m)}{m}, \quad R_2 = p \sum_{\substack{m=1 \\ p|m}}^{\infty} \frac{h_p(m)}{m},$$

$$R_3(\alpha) = \sqrt{p} \sum_{\substack{n=-\infty \\ n \neq 0}}^{\infty} \sum_{m=-\infty}^{\infty} \frac{h_p(m)h_p(n)}{|n|} \left(\min \left\{ 1, \frac{1}{|m|} \right\} + \min \left\{ 1, \frac{1}{|m + \alpha n|} \right\} \right),$$

$$R_4(\alpha) = p \sum_{\substack{n=-\infty \\ n \neq 0, p|n}}^{\infty} \sum_{\substack{m=-\infty \\ p|m}}^{\infty} \frac{h_p(m)h_p(n)}{|n|} \left(\min \left\{ 1, \frac{1}{|m|} \right\} + \min \left\{ 1, \frac{1}{|m + \alpha n|} \right\} \right).$$

Оценим каждый из возникших рядов. Заметим сначала, что

$$R_1 \leq \sqrt{p} \left(\sum_{m=1}^p \frac{1}{m} + \sum_{m>p} \frac{p}{m^2} \right) \ll \sqrt{p} \log p, \quad (7)$$

$$R_2 = p \sum_{m=1}^{\infty} \frac{h_p(pm)}{pm} = \sum_{m=1}^{\infty} \frac{1}{m^2} \ll 1. \quad (8)$$

Поскольку $R_3(\alpha)$ и $R_4(\alpha)$ являются четными функциями от α , то

$$R_3(\alpha) \ll \sqrt{p} \sum_{\substack{n=-\infty \\ n \neq 0}}^{\infty} \frac{h_p(n)}{|n|} \sum_{m=0}^{\infty} h_p(m) \left(\min \left\{ 1, \frac{1}{|m|} \right\} + \min \left\{ 1, \frac{1}{|m + \alpha n|} \right\} \right),$$

$$R_4(\alpha) = p \sum_{\substack{n=-\infty \\ n \neq 0, p|n}}^{\infty} \frac{h_p(n)}{|n|} \sum_{m=0}^{\infty} h_p(m) \left(\min \left\{ 1, \frac{1}{|m|} \right\} + \min \left\{ 1, \frac{1}{|m + \alpha n|} \right\} \right).$$

Проверим, что при любом действительном a сумма

$$S(a) = \sum_{m=0}^{\infty} h_p(m) \min \left\{ 1, \frac{1}{|m - a|} \right\}$$

допускает равномерную по a оценку

$$S(a) \ll \log p. \quad (9)$$

Если $a \geq 0$, то $|m - a|^{-1} \geq |m + a|^{-1}$. Значит, оценку (9) достаточно проверить для неотрицательных a . Заметим, что при $m \geq 2a$ выполняется неравенство $|m - a|^{-1} \leq 2m^{-1}$. Поэтому при $a \leq p$

$$S(a) \ll \sum_{m=0}^{2p-1} \min \left\{ 1, \frac{1}{|m - a|} \right\} + \sum_{m \geq 2p} \frac{p}{m^2} \ll \log p.$$

Если же $a > p$, то

$$\begin{aligned} S(a) &\ll \sum_{1 \leq m < 2a} \frac{p}{m} \min \left\{ 1, \frac{1}{|m - a|} \right\} + \sum_{m \geq 2a} \frac{p}{m^2} + 1 \ll \sum_{1 \leq m \leq a-1} \frac{p}{m(a-m)} + 1 \\ &= \frac{p}{a} \sum_{1 \leq m \leq a-1} \left(\frac{1}{m} + \frac{1}{a-m} \right) + 1 \ll \frac{p}{a} \log a + 1 \ll \log p. \end{aligned}$$

Применяя формулу (9) к рядам $R_3(\alpha)$ и $R_4(\alpha)$, приходим к оценкам

$$R_3(\alpha) \ll \sqrt{p} \log p \sum_{n=1}^{\infty} \frac{h_p(n)}{n} \leq \sqrt{p} \log p \left(\sum_{n=1}^p \frac{1}{n} + \sum_{n>p} \frac{p}{n^2} \right) \ll \sqrt{p} \log^2 p, \quad (10)$$

$$R_4(\alpha) \ll p \log p \sum_{\substack{n=1 \\ p|n}}^{\infty} \frac{h_p(n)}{n} = \log p \sum_{n=1}^{\infty} \frac{1}{n^2} \ll \log p. \quad (11)$$

Подставляя (7), (8) и (10), (11) в формулу (6), получаем нужную требуемую оценку (3).

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] I. E. Shparlinski, “Modular hyperbolas”, *Japan. J. Math.*, **7**:2 (2012), 235–294.
- [2] А. В. Устинов, “О числе решений сравнения $xy \equiv l \pmod{q}$ под графиком дважды непрерывно дифференцируемой функции”, *Алгебра и анализ*, **20**:5 (2008), 186–216.
- [3] A. Weil, “On some exponential sums”, *Proc. Natl. Acad. Sci. USA*, **34** (1948), 204–207.
- [4] В. А. Быковский, “Асимптотические свойства целых точек (a_1, a_2) , удовлетворяющих сравнению $a_1 a_2 \equiv l(q)$ ”, *Аналитическая теория чисел и теория функций*. 4, Зап. научн. сем. ЛОМИ, **112**, Изд-во «Наука», Ленинград. отд., Л., 1981, 5–25.
- [5] О. А. Горкуша, “О конечных цепных дробях специального вида”, *Чебышевский сб.*, **9**:1 (2008), 80–107.
- [6] А. В. Устинов, “О распределении чисел Фробениуса с тремя аргументами”, *Изв. РАН. Сер. матем.*, **74**:5 (2010), 145–170.
- [7] I. E. Shparlinski, A. Winterhof, “On the number of distances between the coordinates of points on modular hyperbolas”, *J. Number Theory*, **128**:5 (2008), 1224–1230.
- [8] А. В. Устинов, “Спиновые цепочки и задача Арнольда о статистиках Гаусса–Кузьмина для квадратичных иррациональностей”, *Матем. сб.*, **204**:5 (2013), 143–160.
- [9] C. Cobeli, Y. Gallot, P. Moree, A. Zaharescu, “Sister Beiter and Kloosterman: a tale of cyclotomic coefficients and modular inverses”, *Indag. Math. (N.S.)*, **24**:4 (2013), 915–929.

А. В. Устинов

Хабаровское отделение

Института прикладной математики ДВО РАН

E-mail: ustinov@iam.khv.ru

Поступило

23.05.2013