ЧЕБЫШЕВСКИЙ СБОРНИК
Том 17. Выпуск 3.

УДК 511.31

О РАСПРЕДЕЛЕНИИ ЭЛЕМЕНТОВ ПОЛУГРУПП НАТУРАЛЬНЫХ ЧИСЕЛ II.[1]

Ю. Н. Штейников (г. Москва)

Аннотация

Пусть имеется подмножество A натуральных чисел из отрезка $[1, q]$ со следующим условием. Если элементы a, b из A и ab не превосходит q, то ab принадлежит A. Пусть также известно, что $|A| < q^{\nu}$, ν- некоторое фиксированное число не превосходящее 1. В данной работе ставится вопрос о числе элементов A на отрезке длины существенно меньше чем q, — на отрезке $[1, x]$, где x существенно меньше чем произвольная степень q.

В этой задаче в случае, когда A — множество специального вида и при некоторых ограничениях на $|A|$ и x, уже получены определенные результаты. Так, из работы Ж. Бургейна, С. Конягина и И. Шпарлинского вытекают нетривиальные оценки в случае когда A — некоторая мультипликативная подгруппа группы обратимых элементов системы вычетов по простому модулю.

Исходная задача обобщает ее на случай полугрупп вместо мультипликативных подгрупп. Отметим, что имеются вполне определенные результаты по этой задаче. Основной результат данной работы — выведена новая оценка на число элементов полугруппы натуральных чисел заданном коротком интервале от 1 до x. Полученные оценки содержательны, когда x существенно меньше чем любая степень q. Более точно, пусть A — наша полугруппа, $g := \frac{\log\log x}{\log\log q}, x = q^{o(1)}$, при q стремящемся к бесконечности. Тогда число элементов A в интервале $(1, x)$ не превосходит $x^{1-C(g,\nu)+o(1)}$, где $C(g, \nu)$ — некоторая явно выписываемая положительная функция. Предыдущие результаты относились к оценке функции $C(g, \nu)$, найденная новая оценка для $C(g, \nu)$ улучшает предыдущий результат для некоторой области параметров (g, ν).

При доказательстве существенно используются свойства распределения гладких чисел, чисел с большой гладкой частью, оценки на число делителей фиксированно числа в заданном диапазоне. В работе используются некоторые результаты Ж. Бургейна, С. Конягина и И. Шпарлинского.

Ключевые слова: полугруппа, распределение, гладкие числа, делимость, делители.
Библиография: 15 названий.

ON THE DISTRIBUTION OF ELEMENTS SEMIGROUPS OF NATURAL NUMBERS II.

Yu. N. Shteinikov (Moscow)

Abstract

Suppose there is subset A of positive integers from the interval $[1, q]$ with the following condition. If the elements a, b of A and ab is at most q, then ab belongs to A. In addition let also know that $|A| < q^{\nu}$, ν - is some fixed number, not exceeding 1. In this paper we consider the question of the number of elements belonging to A on the interval with length substantially less than q, - on the interval $[1, x]$, where x is much smaller than an arbitrary power of q.

In this task, in the case when A - is a special set and with certain restrictions on $|A|$ and x, there exists some results. So, from the work of J. Bourgain, S. Konyagin and I. Shparlinskii there

[1]Работа выполнена при поддержке гранта РФФИ № 14-01-00332

are nontrivial estimates in the case when A - a multiplicative subgroup of invertible elements of the residue ring modulo prime.

The initial problem generalize it to the case of semigroups instead of multiplicative subgroups. It should be noted that there are quite definite results on this task. The main result of this work is to derived a new estimate on the number of elements of the semigroup of natural numbers given short interval from 1 to x. These estimates are meaningful when x is much smaller than any power of q. More precisely, let A - our semigroup, $g := \frac{\log\log x}{\log\log q}, x = q^{o(1)}$ for q tends to infinity. Then the number of elements of A in the interval $(1, x)$ does not exceed $x^{1-C(g,\nu)+o(1)}$, where $C(g,\nu)$ - some clearly written positive function. Previous result relates to the estimation of function $C(g,\nu)$, a new estimate for the $C(g,\nu)$ improves the previous result for a certain range of parameters (g,ν).

We essentially use in the proof the distribution of smooth numbers, the numbers with a large part of the smooth part, estimates on the number of divisors of a fixed number in a given interval. We use some results of J. Bourgain, S. Konyagin and I. Shparlinski.

Keywords: semigroup, distribution, smooth numbers, divisibility, divisors.
Bibliography: 15 titles.

1. Введение

Пусть $A \subset \mathbb{N}$ — множество, замкнутое относительно операции умножения, то есть если $a_1, a_2 \in A$, то $a_1 a_2 \in A$. Такие множества A называют полугруппами. В частности, можно взять множество $A = \{n \in \mathbb{N} : n \in G \pmod m\}$, где $m \in \mathbb{N}$, а G — мультипликативная подгруппа группы $\mathbb{Z}_m^*$.

Нас будет интересовать случай, когда для некоторого натурального q и $0 < \nu < 1$ справедливо неравенство:

$$|\{n \in A; n \le q\}| < q^{\nu}. \tag{1}$$

Пусть для $x > 0$ определим :

$$f(x) = |A \cap [1, x]|.$$

В работе [3] получены оценки на количество чисел не превосходящих n, которые принадлежат подгруппе порядка t группы $\mathbb{Z}_p^*$. Эти оценки содержательны, когда t мало по сравнению с p. Из нашей работы вытекают оценки в случае, когда t растет как степень p, а n мало. В работе [6] были уже получены нетривиальные верхние оценки на $f(n)$, когда n растет медленнее, чем произвольная степень q. Целью данной работы является доказать более сильный вариант теоремы, доказанной в [6].

Приведем утверждение, доказанное в [6].

Теорема 1. *Пусть A — множество, замкнутое относительно операции умножения и удовлетворяет условию (1) для некоторого фиксированного $\nu \in (0,1)$ и задано x. Если $\gamma := \frac{\log\log x}{\log\log q}$ и $\log x = o(\log q)$, то*

$$f(x) \le x^{1-max\{L_\gamma, M_\gamma\}+o(1)}, q \to \infty, \tag{2}$$

где

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

Основной результат этой статьи — доказать следующий более сильный вариант теоремы 1.

Теорема 2. *Пусть A — множество, замкнутое относительно операции умножения и удовлетворяет условию (1) для некоторого фиксированного $\nu \in (0,1)$ и задано x. Если $\gamma := \frac{\log\log x}{\log\log q}$ и $\log x = o(\log q)$, то*

$$f(x) \le x^{1-C_\gamma+o(1)}, q \to \infty, \tag{3}$$

где

$C_\gamma = \gamma(\frac{\gamma-1+\sqrt{\gamma^2+\nu-2\gamma\nu}}{2\gamma-1})^2$ *если* $\gamma \neq \frac{1}{2}$ *и* $C_{\frac{1}{2}} := \lim_{\gamma\to\frac{1}{2}} C_\gamma = \frac{1}{2}(1-\nu)^2$.

Схема доказательства теоремы 2 совпадает со схемой доказательства теоремы 1. Но при этом в доказательстве будем пользоваться одной более точной оценкой, которая и приводит к результату теоремы 2.

2. Вспомогательные утверждения

Введем некоторые определения и обозначения аналогичные в статье [6]. Нам потребуются оценки для множеств чисел, у которых все простые делители малы. Для натурального n пусть $P^+(n)$ обозначает наибольший простой делитель числа n, $P^+(1) = 1$. Для $x \geqslant y \geqslant 2$ полагаем:

$$\psi(x,y) = |\{n \leqslant x : P^+(n) \leqslant y\}| \tag{4}$$

Известна следующая теорема. Ее формулировку можно найти в работе [1].

Теорема A [1]. *Пусть* $x \geq y \geq 2, v = \frac{\log x}{\log y}$ *Тогда для любого* $\varepsilon > 0$ *на множестве* $v \leq y^{1-\varepsilon}$ *имеет место неравенство:*

$$\psi(x,y) = xv^{-v(1+o(1))},$$

если $v \to \infty$.

Предположим, что задано целое y. Каждое натуральное n представим в виде $n = n_1 n_2$, так что если простое p делит n_1, то $p \leq y$, а если делит n_2, то $p > y$. Пусть также даны x, z. Определим множество:

$$N(x,y,z) = \{n \leq x : n_1 > z\}.$$

Мы хотим оценить сверху количество элементов множества $N(x,y,z)$. На довольно большой области изменения x, y, z была получена ассимптотика $N(x,y,z)$ в работе [4]. Следуя схеме, предложенной в [4] в работе [6] был получен более грубый результат, но при еще слабых ограничениях на параметры x, y, z. Ниже приводится его формулировка.

Лемма 1. *Пусть* $\varepsilon > 0$ *фиксировано,* q, x *— достаточно большие. Пусть положительные вещественные* $\alpha, \beta, \gamma := \frac{\log\log x}{\log\log q}$ *удовлетворяют условиям*

$$\beta < 1, \gamma \leq \alpha(1-\varepsilon), \varepsilon \leq \frac{\beta}{\alpha} \leq \frac{1}{\varepsilon}$$

и также

$$y := (\log q)^\alpha \geq 2, z := x^\beta.$$

Если $\frac{\log x}{\log\log q} \to \infty$ *при* $q \to \infty$, *то*

$$|N(x,y,z)| \leq x^{1-\frac{\beta\gamma}{\alpha}+o(1)}. \tag{5}$$

Нам также понадобится утверждение, доказанное в [6]. Оно приводится ниже.

Лемма 2. *Количество делителей числа* $n < Q$, *не превосходящих* z, *не превосходит* $\psi(z, (1+o(1))\log Q), Q \to \infty$..

Теперь все готово для доказательства теоремы 2.

3. Доказательство теоремы 2

Пусть $\gamma := \frac{\log\log x}{\log\log q}$ Введем положительные вещественные параметры $\alpha > 1, \beta$; удовлетворяющие условию леммы 1 для некоторого фиксированного $\varepsilon > 0$ и соответственно $y = (\log q)^\alpha, z = x^\beta$. Каждое натуральное n представим в виде $n = n_1 n_2$, так что если простое p делит n_1, то $p \le y$, а если p делит n_2, то $p > y$. Разделим элементы множества $A \cap [1, x]$ на два подмножества A' и A'', $A \cap [1, x] = A' \cup A''$. По определению полагаем $A'' := \{n \in A \cap [1, x] : n_1 > z\}$, $A' := \{A \cap [1, x]\} \setminus A''$. Совершенно ясно, что $f(x) = |A'| + |A''|$.

I)Оценим размер множества A''. По лемме 1 получаем

$$|A''| \le N(x, y, z) \le x^{1-\frac{\beta\gamma}{\alpha}+o(1)}, q \to \infty. \tag{6}$$

II)Теперь перейдем к оценке $|A'|$. Для этого рассмотрим множество $B =: \{m_1 \dots m_r\}$, где $r = [\frac{\log q}{\log x}] = [(\log q)^{1-\gamma}]$ и $m_1, \dots, m_r \in A'$. Из определения r следует, что если $m \in B$, то $m \le q$. Так как произведение чисел из A' является числом из A то легко видеть, что $|B| \le |A \cap [1, q]| \le q^\nu$. Теперь оценим снизу $|B|$. Пусть каждый $m_i \in A'$ по аналогии представим в виде $m_i = m_{1,i} m_{2,i}$, так что если простое p делит $m_{1,i}$, то $p \le y$, а если p делит $m_{2,i}$, то $p > y$. Определим из равенства $N_1, N_2 : m = m_1 \dots m_r = m_{1,1} \dots m_{1,r} m_{2,1} \dots m_{2,r} = N_1 N_2$, где $N_1 = m_{1,1} \dots m_{1,r}$ и $N_2 = m_{2,1} \dots m_{2,r}$.

Возьмем конкретный представитель, например элемент $m \in B$ и оценим сверху число представлений его в виде произведения r множителей, где каждый принадлежит A'.

Пусть $m = N_1 N_2$, оценим количество представлений для N_2 в виде произведения r чисел $m_{2,1} \dots m_{2,r}$, $N_2 = m_{2,1} \dots m_{2,r} = p_1 \dots p_s$,где все $p_i > y$ и являются простыми числами. Видим, что $s \le [\frac{\log N_2}{\log y}] \le \frac{\log N_2}{\alpha \log\log q}$.

Каждый делитель $p_i, i = 1, \dots, s$ может входить в разложение некоторого $m_{2,j}, j = 1, \dots, r$. Значит количество представлений числа N_2 не превосходит $r^s \le N_2^{\frac{1-\gamma}{\alpha}}$.

Теперь оценим количество представлений для фиксированного N_1 в виде $N_1 = m_{1,1} \dots m_{1,r}$, когда $m_{1,i} \in A'$ Покажем, что число таких представлений числа N_1 не превосходит $N_1^{1-\gamma} q^{o(1)}, q \to \infty$. Возьмем и зафиксируем достаточно большое натуральное число J. Введем по определению интервалы $\triangle_j := [z^{\frac{j-1}{J}}, z^{\frac{j}{J}}), j \in [1, J]$. Каждый из множителей $m_{1,i}, i = 1, \dots, r$ попадает в один из интервалов $\triangle_j, j = 1, \dots, J$. Число способов распределения r чисел $m_{1,i}, i = 1, \dots, r$ по интервалам $\triangle_j$ не превосходит $J^r = q^{o(1)}, q \to \infty$. Пусть теперь каждый $m_{1,i}, i = 1, \dots, r$ относится к какому-то из $\triangle_j, j = 1, \dots, J$. Если, например $m_{1,1} \in \triangle_j$, то $m_{1,1} \le z^{\frac{j}{J}}$ и $m_{1,1}$ является делителем числа $N_1 < q$. По лемме 2 количество таких $m_{1,1}$ не превосходит $\psi(z^{\frac{j}{J}}, (1 + o(1)) \log q)$. Пользуясь теоремой A, получаем $\psi(z^{\frac{j}{J}}, (1 + o(1)) \log q) = z^{\frac{j}{J}(1-\gamma+o(1))}, q \to \infty$. Таким образом, если $m_{1,i} \in \triangle_j$ то число число возможностей для числа $m_{1,i}$ не превосходит $z^{\frac{j}{J}(1-\gamma+o(1))}$ и

$$z^{\frac{j}{J}(1-\gamma+o(1))} \le z^{(\frac{j-1}{J}+\frac{1}{J})(1-\gamma+o(1))} \le m_{1,i}^{1-\gamma+o(1)} z^{\frac{1}{J}(1-\gamma+o(1))}. \tag{7}$$

Поэтому если фиксировано, что каждый из $m_{1,i}, i = 1, \dots, r$ принадлежит какому-то из $\triangle_j$, то число представлений числа N_1 в виде произведения чисел $m_{1,i}$ не превосходит $N_1^{1-\gamma+o(1)} q^{\frac{\beta}{J}(1-\gamma+o(1))}$. Умножив эту величину на число способов распределения чисел $m_{1,i}$ по интервалам $\triangle_j$, которое равно $q^{o(1)}$ получим верхнюю оценку на искомое число представлений N_1 в виде произведения $m_{1,1} \dots m_{1,r}$. Оно не превосходит $N_1^{1-\gamma+o(1)} q^{\frac{\beta}{J}(1-\gamma)+o(1)}$. В силу произвольности J эта величина есть $N_1^{1-\gamma+o(1)} q^{o(1)}, q \to \infty$.

Итак, мы оценили количество представлений чисел N_1 и N_2 в виде произведения $m_{1,1} \dots m_{1,r}$ и соответственно $m_{2,1} \dots m_{2,r}$. Число же представлений элемента $m \in B$ в виде произведения $m_1 \dots m_r$, где $m_i \in A'$ не превосходит произведения числа представлений для

N_1 и N_2, то есть $N_1^{1-\gamma}N_2^{\frac{1-\gamma}{\alpha}}$. При $\alpha > 1$ наибольшее значение, которое эта величина может принимать равно $q^{(1-\gamma)(\beta+\frac{1-\beta}{\alpha})+o(1)}$.

Отсюда получается и нижняя оценка для B :

$$\frac{|A'|^r}{q^{(1-\gamma)(\beta+\frac{1-\beta}{\alpha})+o(1)}} \le |B| \le q^{\nu}. \tag{8}$$

Отсюда следует оценка для $|A'|$:

$$|A'| \le x^{\nu+(1-\gamma)(\beta+\frac{1-\beta}{\alpha})+o(1)}.$$

Вспоминаем, что

$$|A''| \le x^{1-\frac{\beta\gamma}{\alpha}+o(1)}.$$

Оценка для $f(x)$ складывается из оценок для $|A'|$ и $|A''|$. Теперь осталось выбрать параметры $\alpha > 1, \beta$ для оптимизации финальной оценки. Если $\gamma \neq \frac{1}{2}$ то возьмем следующие параметры $\beta := \frac{\gamma-1+\sqrt{\gamma^2-2\gamma\nu+\nu}}{2\gamma-1}, \alpha := \frac{1}{\beta}$. Если $\gamma = \frac{1}{2}$ то $\beta = \frac{1}{\alpha} = 1-\nu$. Подставляя такие параметры, мы завершаем доказательство теоремы 2.

4. Заключение

Получим нижние оценки на величину $f(x)$, когда $x = exp\{(\log q)^{\gamma}\}$.

Возьмем любое число $0 < \nu < 1$ и положим A_q- полугруппа y — гладких чисел, где

$$y = (\log q)^{\lambda},$$

где $\lambda = \frac{1}{1-\nu+\varepsilon}$, где ε — малое число.

Пользуясь теоремой [A] о количестве гладких чисел при при $q \ge q(\nu, \varepsilon)$ получаем,

$$|A_q \bigcap [1, q]| < q^{\nu}.$$

Тогда выполнено неравенство (1).

Пользуясь вновь теоремой [A], получаем

$$|A_q \bigcap [1, e^{(\log q)^{\gamma}}]| = x^{1-\gamma+\gamma\nu-\varepsilon'\gamma+o(1)}, q \to \infty,$$

где $\varepsilon' > 0$ — некоторое малое число.

Поэтому верхняя оценка для функции C_γ с точностью до слагаемых малых порядков такая $\gamma-\gamma\nu$. Оценка, которая получена в теореме 2 для функции C_γ хуже чем эта. Возможно именно она и является правильной.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Hildebrand A., Tenenbaum G. Integers without large prime factors // J Theorie des Nombres de Bordeaux. 1993. Vol 5, № 2. P. 411-484.

2. Прахар К. Распределение простых чисел. М.: Мир, 1967, 512 с.

3. Bourgain J., Konyagin S., Shparlinski I. Distribution of elements of cosets of small subgroups and applications // International Math Research Notices. 2012. Vol 201, №9. P. 1968–2009.

4. Banks W., Shparlinski I. Integers with a large smooth divisor // Electronic journal of combinatorial number theory. 2007 Vol. 7.

5. Tenenbaum G. Introduction to analytic and probabilistic number theory. Cambridge Universit Press, Cambridge, UK, 1995.

6. Штейников Ю.Н. О распределении элементов полугрупп натуральных чисел // Чебышевский сборник. 2012. Т. 13, № 3. С. 91–99.

7. Малыхин Ю. В. Оценки тригонометрических сумм по модулю p^2 // Фундаментальная и прикладная математика. 2005. Т. 11, № 6. С. 81–94.

8. Малыхин Ю. В. Оценки тригонометрических сумм по модулю p^r // Математические заметки. 2006. Т. 80, № 5, С. 793–796.

9. Bourgain J., Konyagin S., Shparlinski I. Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm // Int. Math Research Notices. 2008. rnn 090, P. 1–29.

10. Bourgain J., Ford K. , Konyagin S., Shparlinski I. On the divisibility of Fermat Quotients // Michigan J. Math. 2010. Vol.59, № 2, P. 313–328.

11. Bourgain J., Konyagin S. Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order // C. R. Math. Acad. Sci. Paris, 2003. Vol. Vol.337, № 2, P. 75–80.

12. Heath-Brown D. R., Konyagin S. New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum // Q. J. Math., 2000. Vol. 51, №2, P. 221–235.

13. Konyagin S., Shparlinski I. Character sums with exponential functions. Cambridge University Press, Cambridge, 1999.

14. Shkredov I. On Heilbronn's exponential sum // Q. J. Math., 2013. Vol. 64, № 4, P. 1221–1230.

15. Zhou B. A note on exponential sums over subgroups of $\mathbb{Z}_{p^2}^*$ and their applications // J. Number Theory, 2010. Vol. 130, № 11, P. 2467–2479.

REFERENCES

1. Hildebrand, A., & Tenenbaum, G. 1993, "Integers without large prime factors J Theorie des Nombres de Bordeaux, 5, 2. pp. 411–484.

2. Prachar, K. 1967, "Raspredelenie prostich chisel (Russian) [Distribution of prime numbers] Mir, Moscow, pp. 1–512.

3. Bourgain, J., Konyagin. S., & Shparlinski. I. 2012, "Distribution of elements of cosets of small subgroups and applications"Int. Math Research Notices, 201, 9. pp. 1968–2009.

4. Banks, W., & Shparlinski, I. 2007, "Integers with a large smooth divisor Electronic journal of combinatorial number theory, 7.

5. Tenenbaum, G. 1995, "Introduction to analytic and probabilistic number theory Cambridge Universit Press, Cambridge, pp. 1–466.

6. Shteinikov, Y.N. 2012, "On the distribution of semigroups of natural numbers Chebishev's sbornik, 13, 3, pp. 91–99.

7. Malykhin, Y. V. 2005, "Estimates of exponential sums modulo p^2 Fundamentalnaya i prikladnaya matematika, 11, 6, pp. 81–94.

8. Malykhin, Y. V. 2006, "Estimates of exponential sums modulo p^r Mathematical Notes, 80, 5, pp. 793–796.

9. Bourgain, J. Konyagin, S. & Shparlinski I. 2008, "Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm Int. Math Research Notices, rnn 090, pp. 1–29.

10. Bourgain, J. Ford, K. Konyagin, S. & Shparlinski, I. 2010, "On the divisibility of Fermat Quotients Michigan J. Math., 59, 2, pp. 313–328.

11. Bourgain, J. & Konyagin, S. 2003, "Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order C. R. Math. Acad. Sci. Paris, 337, 2, pp. 75–80.

12. Heath-Brown, D. R. & Konyagin, S. 2000, "New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum Q. J. Math., 51, 2, pp. 221–235.

13. Konyagin, S., & Shparlinski, I. 1999, "Character sums with exponential functions Cambridge University Press, Cambridge, pp. 1–163.

14. Shkredov, I.D. 2013, "On Heilbronn's exponential sum Q. J. Math., 64, 4, pp. 1221–1230.

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

ФГУ ФНЦ Научно-исследовательский институт системных исследований Российской академии наук
Получено 9.03.2016 г.
Принято в печать 13.09.2016 г.