Acta Mathematica et Informatica Universitatis Ostraviensis

Anatolii Alekseevich Karatsuba

Правильные множества по заданному модулю

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 6 (1998), No. 1, 129--134

Persistent URL: http://dml.cz/dmlcz/120524

Правильные множества по заданному модулю

Анатолий А. Карацуба

Abstract: Конструктивно построены правильные множества по модулю, равному степени фиксированного нечетного простого числа. Число элементов этих множеств не превосходит сколь-угодно малой положительной степени модуля.

Key Words: Additive congruences, character sums, trigonometric sums

Mathematics Subject Classification: Primary 11L05; Secondary 11K06

В [1] поставлен вопрос о существовании правильных множеств по заданному модулю m при условии, что количество элементов этих множеств не превосходит m^{ε}, и конструктивно построены правильные множества для $m = p^N$, $p^{\smile}$-фиксированное нечетное простое число. Напомню определения из [1]. Пусть $m^{\smile}$-натуральное число, $m = m_1 > 0$, $E_m{}^{\smile}$-полная система вычетов по модулю m, $A \leqslant E_m$, $\|A\|$-количество элементов A.

Определение 1. Множество A называется базисом E_m порядка $k = k(A)$, если каждое $l \in E_m$ представляется в виде

$$x_1 + \cdots + x_k \equiv l \pmod{m},$$

$x_1, \ldots, x_k \in A$, и существует такое $l_1 \in E_m$, что

$$x_1 + \cdots + x_{k-1} \not\equiv l_1 \pmod{m}$$

при любых $x_1, \ldots, x_{k-1} \in A$.

Определение 2. Множество A называется правильным ($c^{\smile}$-правильным по модулю m), если оно является базисом E_m порядка $k = k(A)$, и существует абсолютная постоянная $c \geqslant 1$ такая, что

$$k = k(A) \leqslant c\frac{\log m}{\log \|A\|}.$$

В [1] поставлен вопрос о существовании правильных множеств A с условием $\|A\| \leqslant m^{\varepsilon}$, $1 > \varepsilon > 0$, $m > m_1(\varepsilon) > 0$. Вопрос возник в результате занятий автора проблемой Варинта ([2]–[4] , [11]). В [1] доказана следующая теорема.

This paper was partly supported by grant N^o F 1247/1997 Ministry of Education of the Czech Republic (MŠMT).

Теорема 1. *(А. А. Карацуба [1]). Пусть $p \geqslant 3$, $p^{\smile}$-простое число, $N^{\smile}$-натуральное число с условием*

$$N \geqslant \max(512000, 512p^{1.5}),$$

$m = p^N$, $\varepsilon^{\smile}$-произвольное число из промежутка

$$8\sqrt[3]{\frac{\log p}{\log m}} \leqslant \varepsilon \leqslant \min\left(\frac{1}{10}, \frac{1}{\sqrt{p}}\right).$$

Тогда существуют $c^{\smile}$-правильные множества A по модулю m с условием $\|A\| \leqslant m^{\varepsilon}$ и с верхней оценкой порядка $k = k(A)$ вида

$$k < 9\frac{\log m}{\log \|A\|}.$$

Правильными множествами A сформулированной теоремы будут вычеты по модулю m чисел вида x^n, $x = 1, 2, \ldots, [m^{\varepsilon}]$, $[x, m) = 1$ где $n^{\smile}$-произвольное простое число из промежутка $(32\varepsilon^{-2}, 64\varepsilon^{-2}]$.

Подобная проблема, но в более общем виде, рассматривалась M. B. Nathanson'ом в [5].

Теорема 2. (M. B. Nathanson [5]). *Every finite group G of order n has a basis B of order 2 such that*

$$|B| < 2(n \log n)^{1/2} + 2,$$

and, for every $h \geqslant 3$ and $\delta > 0$, there exists an integer $M = M(h, \delta)$ such that every finite group G of order $n \geqslant M$ has a basis B of h such that

$$|B| < (h + \delta)(n \log n)^{1/h}.$$

В [5] также изложена история рассматриваемой проблемы (проблема Rohrbach'a для конечных групп).

На работу M. B. Nathanson'a [5] мне указали профессор T. Luchak и профессор T. Schoen (13^{th} Czech and Slovak International Conference on Number Theory, Ostravice, September, 1–6, 1997), которым я глубоко благодарен.

Конструктивное построение правильных множеств по модулю m имеет самостоятельный интерес. В частности, такие множества могут найти применения в прикладных вопросах.

Как отмечалось в [1], правильными множествами по модулю m, по-видимомы, будут множества вычетов чисел вида g^x, $x = 1, 2, \ldots, [m^{\varepsilon}]$, где $g^{\smile}$-фиксированное натуральное число, взаимно-простое с m, показатель которого по модулю m, достаточно велик, в частности, если $g^{\smile}$-первообразный корень по модулю m, $m^{\smile}$-простое число, множества вычетов чисел x^*, $x = 1, 2, \ldots [m^{\varepsilon}]$, $(x, m) = 1$, где $xx^* \equiv 1 \pmod m$.

В настоящей статье построены новые правильные множества для модуля $m = p^N$, $p^{\smile}$-фиксированное нечетное простое число.

Модули такого вида интересны тем, что для них решены некоторые проблемы теории чисел, к которым, в общем случае, пока нет никаких подходов. Этот феномен был обнаружен А. Г. Постниковым [6], и применен затем М. Б. Барбаном, Ю. В. Линником, Н. Г. Чудаковым [7] к проблеме распределения простых чисел в коротких арифметических прогрессиях, автором [8] а затем – В. Н. Чубариковым [9] к проблеме границы нулей L-рядов Дирихле, М. М. Петеч уком [10] – к проблеме делителей Дирихле в коротких арифметических прогрессиях. Отмечу также, что если рассматривать задачу о сложности вычисления дискретного логарифма числа x по $\bmod m$, то в этом случае легко получить верхнюю оценку сложности вида $O(\log^c m)$, $c > 0$, c˘-абсолютная постоянная.

Ниже считаем, что $0 < \varepsilon < 0.1$; p˘-нечетное простое число. $N \geqslant N_1$ $(p;\varepsilon) > 0$, N-натуральное число с $m = p^N\ (p-1)$.

Теорема 3. *Пусть* $m = p^N\,(p-1)$, $Q = p^{N+1}$, g˘*-некоторый первообразный корень по модулю* Q, $\operatorname{ind} x = \operatorname{ind}_g x$. *Тогда числа вида* $\operatorname{ind} x$, $(x,p) = 1$, $x = 1,2,\ldots,[m^\varepsilon]$, *образую правильное множество* A *по модулю* m, *причем*

$$k = k(A) \leqslant 2\frac{\log m}{\log \|A\|} + 3\,.$$

Доказательство. Определим целое число $t \geqslant 10$ неравенствами:

$$\frac{1}{t} \leqslant \varepsilon < \frac{1}{t-1}\,.$$

Пусть $t\varepsilon_1 = 1$, $Y = m^{\varepsilon_1}$, l˘-произвольное целое число, s˘-натуральное число, $r = s + 2t$.

Рассмотрим сравнение:

$$\begin{aligned} &\operatorname{ind} x_1 + \operatorname{ind} x_2 + \cdots + \operatorname{ind} x_r \equiv l \pmod m\,,\\ &1 \leqslant x_j \leqslant Y, \quad (x_j,p) = 1\,, \quad j = 1,2,\ldots,r\,. \end{aligned} \tag{1}$$

Пусть $K = K(Y\,m;r)$˘-количество решений (1). Пользуясь свойством полной рациональной тригонометрической суммы, находим:

$$K = \frac{1}{m}\sum_{a=0}^{m-1}\Bigg(\sum_{1\leqslant x\leqslant Y}{}' e^{2\pi i\frac{a\operatorname{ind} x}{m}}\Bigg)^r e^{-2\pi i\frac{al}{m}}\,, \tag{2}$$

где штрих в сумме означает, что $(x,p) = 1$.

Выделяя слагаемое при $a = 0$, найдем:

$$K = \frac{1}{m}\,Y_1^r + R\,, \tag{3}$$

где Y_1˘-количество $x \leqslant Y$, $(x,p) = 1$,

$$\begin{aligned} |R| \leqslant \max_{0<a<m}\Bigg|\sum_{0<x\leqslant Y}{}' e^{2\pi i\frac{a\operatorname{ind} x}{m}}\Bigg|^s \times\\ \times\frac{1}{m}\sum_{a=0}^{m-1}\Bigg|\sum_{0<x\leqslant Y}{}' e^{2\pi i\frac{a\operatorname{ind} x}{m}}\Bigg|^{2t}\,. \end{aligned} \tag{4}$$

Сумма в первом множителе правой части (4) равняется S,

$$S = \sum_{0<n\leqslant Y} \chi(n)\,,$$

где $\chi(n)^{\smile}$-неглавный характер Дирихле по модулю Q. К $|S|$ применима оценка тригонометрической суммы из [8]:

$$|S| \leqslant c_1 Y \exp\Big(-c\frac{\log^3 Y}{\log^2 Q}\Big)\,, \tag{5}$$

где $c_1 > 0$, $c > 0^{\smile}$-абсолютные постоянные.

Далее, сумма W,

$$W = \frac{1}{m}\sum_{a=0}^{m-1}\Big|\sum_{0<x\leqslant Y}{}' e^{2\pi i\frac{a\,\mathrm{ind}\,x}{m}}\Big|^{2t}\,, \tag{6}$$

равняется количеству решений сравнения

$$\begin{aligned}&\mathrm{ind}\,x_1 + \cdots + \mathrm{ind}\,x_t \equiv \mathrm{ind}\,y_1 + \cdots + \mathrm{ind}\,y_t \pmod m\\ &1 \leqslant x_j,\, y_j \leqslant Y, \quad (x_j, p) = (y;, p) = 1, \quad j = 1,\ldots,t\,.\end{aligned} \tag{7}$$

Из (7) находим:

$$x_1 \ldots x_t \equiv y_1 \ldots y_t \pmod Q\,. \tag{8}$$

Так как $Y^t = m < Q$, то из (8) следует, что

$$x_1 \ldots x_t = y_1 \ldots y_t\,.$$

Поэтому, для W выполняется оценка:

$$\begin{aligned}W = \sum_{n\leqslant Y^t}\tau_t^2(n) \leqslant\\ \leqslant t^2(t!)^{-t-1}Y^t(t\log Y + t^t - 1)^{t^2-1}\,.\end{aligned} \tag{9}$$

Из (4) – (9) находим:

$$\begin{aligned}|R| \leqslant c_1^s Y^s \exp\Big(-\frac{cs\log^3 Y}{\log^2 Q}\Big)t^2(t!)^{-t-1}Y^t\times\\ \times\,(t\log Y + t^t - 1)^{t^2-1}\,.\end{aligned} \tag{10}$$

При $s = 1$ из (10) находим:

$$|R| \ll Y^{t+1}m^{-c\varepsilon_1^3}(\log m)^{\varepsilon_1^{-2}}\,,$$

где постоянная в знаке $\ll$ зависит только от ε.

Следовательно

$$K = \frac{1}{m} Y_1^{2t+1} + O\big(Y^{t+1} m^{-c\varepsilon_1^3} (\log m)^{\varepsilon_1^{-2}}\big)$$

и при $m \geqslant m_1(\varepsilon) > 0$ получаем:

$$K \geqslant \frac{1}{m} Y_1^{2t+1} - c_2(\varepsilon) Y^{t+1} m^{-c\varepsilon_1^3} (\log m)^{\varepsilon_1^{-2}} \geqslant$$
$$\geqslant \frac{1}{2m} Y_1^{2t+1} \geqslant \frac{1}{4}\Big(1 - \frac{1}{p}\Big)^{2t+1} m Y .$$

Отсюда следует, что каждое l представимо в виде (1) и число слагаемых в левой части (1) равно

$$2t + 1 = 2\varepsilon_1^{-1} + 1 \leqslant 2\varepsilon^{-1} + 3 \leqslant 2\frac{\log m}{\log \|A\|} + 3 ,$$

т.е.

$$k = k(A) \leqslant 2\frac{\log m}{\log A\|} + 3 .$$

Теорема 3 доказана.

Замечания. 1. В доказанной теореме ε может стремиться к нулю при $m \to +\infty$, но не быстрее, чем $\sqrt[5]{\frac{\log\log m}{\log m}}$.

2. Если в (10) взять $s = \varepsilon_1^{-1}$, то оценка для $k = k(A)$ примет вид

$$k \leqslant 3\frac{\log m}{\log \|A\|} + 3 ,$$

и ε может стремиться к нулю при $m \to +\infty$, но не быстрее, чем $\sqrt[4]{\frac{\log\log m}{\log m}}$.

Литература

[1] Карацуба, А. А., *Аддитивные сравнения* Izv. AN Rosii, ser. matem. **т. 61** (1997), но. в. 2, 81–94.

[2] Карацуба, А. А., *Аналог проблемы Варинга* Vestnik MGU, ser. I , Матем., мех. **1** (1962), 38–46.

[3] Карацуба, А. А., *Проблема Варинга для сравнений по модулю, равному степени простого числа* Vestnik MGU, ser. I , Матем., мех. **4** (1962), 28–38.

[4] Карацуба, А. А., *Системы сравнений и уравнения варинговского типа* Dokl. AN SSSR **т. 165** (1965), но. в. 2, 274–276.

[5] Nathanson Melvyn, B., *On a Problem of Rohrbach for Finite Groups*, J. Number Theory **41** (1992), 69–76.

[6] Постников, А. Г., *О сумме характеров по модулю, равному степени простого числа* Izv. AN SSSR, ser. matem. **т. 19** (1955), но. в. 1, 11–16.

[7] Барбан, М. Б.; Линник, Ю. Б., Чудаков, Н. Г., *On prime numbers in an arithmetic progression with a prime-power difference*, Acta Arithm. IX (1964), но. в. 4, 375–390.

[8] Карацуба, А. А., *Тригонометрические суммы специального вида и их применения* Izv. AN SSSR, ser. matem. **т. 28** (1964), но. 2, 237–248.

[9] Чубариков, В. Н., *Уточнение границы нулей L-рядов Дирихле по модулю, равному степени простого числа* Vestnik MGU, ser. I , Матем., мех. **2** (1973), 46–52.

[10] Петечук, М. М., *Сумма значений функции делителей в арифметических прогрессиях с разностью, равной степени нечетного простого числа* Izv. AN SSSR, ser. matem. **т. 43** (1979), но. в. 4, 892–908.

[11] Карацуба, А. А., *О функции $G(n)$ в проблеме Варинга* Izv. AN SSSR, ser. matem. **т. 49** (1985), но. в. 5, 935–947.

Author's address: Steklov Mathematical Institute; Vavilov str. 42; 117966 Moscow, GSP–1; RUSSIA

Received: February 12, 1998