Math-Net.Ru

Общероссийский математический портал

А. А. Карацуба, О правильных множествах в остаточных классах, *Матем. заметки*, 1998, том 64, выпуск 2, 224–228

DOI: <https://doi.org/10.4213/mzm1390>

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: 35.173.219.12

26 апреля 2023 г., 13:52:18

УДК 511.3

О ПРАВИЛЬНЫХ МНОЖЕСТВАХ В ОСТАТОЧНЫХ КЛАССАХ

А. А. Карацуба

Конструктивно построены правильные множества по модулю, равному степени фиксированного нечетного простого числа, при условии, что количество элементов этих множеств не превосходит сколь угодно малой положительной степени модуля.

Библиография: 12 названий.

В [1] поставлен вопрос о существовании правильных множеств по заданному модулю m при условии, что количество элементов этих множеств не превосходит m^ε , где $0 < \varepsilon < 1$, $m \geq m_1(\varepsilon)$, и конструктивно построены такие множества для $m = p^N$, p – фиксированное нечетное простое число. Вопрос возник в результате рассмотрения автором проблемы Варинга [2]–[5].

Пусть m – натуральное число, $m \geq m_1 > 0$, E_m – полная система вычетов по модулю m , $A \subseteq E_m$, $\|A\|$ – количество элементов A .

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

$$x_1 + \dots + x_k \equiv l \pmod{m}, \quad x_1, \dots, x_k \in A,$$

и существует $l_1 \in E_m$ такое, что

$$x_1 + \dots + x_{k-1} \not\equiv l_1 \pmod{m}, \quad x_1, \dots, x_{k-1} \in A.$$

ОПРЕДЕЛЕНИЕ 2. Множество A называется *правильным* (*с-правильным*) по модулю m , если оно является базисом E_m порядка $k = k(A)$ и существует абсолютная постоянная $c \geq 1$ такая, что

$$k \leq c \frac{\log m}{\log \|A\|}.$$

Функция $k = k(A)$ является аналогом известной функции $G(n)$ в проблеме Варинга. Если A – правильное множество, то для этого аналога справедлива правильная оценка сверху, которой нет для $G(n)$. Поэтому представляют интерес следующие задачи: будут ли правильными множество $A = \{x^n, 1 \leq x \leq m^\varepsilon, n = n(\varepsilon)\}$; множество $B = \{x^{-1} \pmod{m}, 1 \leq x \leq m^\varepsilon, (x, m) = 1\}$; множество $D = \{2^x, 1 \leq x \leq m^\varepsilon\}$?

В [1] доказана

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, грант № 97-01-00721, и гранта профессора Б. Новака (Карлов Университет, г. Прага).

ТЕОРЕМА 1. Пусть $p \geq 3$, p – простое число, N – натуральное число с условием $N \geq \max(512000, 512p^{1.5})$, $m = p^N$, ε – произвольное число такое, что

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

Тогда существует s -правильное множество A по модулю m с условием $\|A\| \leq m^\varepsilon$ и верхней оценкой порядка $k = k(A)$ вида

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

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

Подобная задача, в более общем виде, рассматривалась М.Б. Натансоном в [6], где изложена история задачи (проблема Рорбаха для конечных групп), а также доказана

ТЕОРЕМА 2 (М.Б. Натансон). Каждая конечная группа G порядка n имеет базис B порядка 2 такой, что

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

Кроме того, для каждого $h \geq 3$ и $\delta > 0$ существует целое число $M = M(h, \delta)$ такое, что каждая конечная группа G порядка $n \geq M$ имеет базис B порядка h такой, что

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

ТЕОРЕМА 3 (Ю. Белый). При заданных $\varepsilon, \delta > 0$ для каждого $m > m_0(\varepsilon, \delta) = (2\varepsilon^{-1} + 2)^{(1+\delta)/\delta}(\varepsilon^{-1} + 1)$ существует множество $A \subseteq \mathbb{Z}$, $\|A\| \leq m^\varepsilon$, такое, что

$$k(A) \leq (1 + \delta) \frac{\log m}{\log \|A\|}.$$

Указанным множеством A являются k -регулярные числа x , $x = 1, 2, \dots, m$, $k = [\varepsilon^{-1}]$ (число x называется k -регулярным, если при записи его в двоичной системе счисления $x = 2^{e_1} + \dots + 2^{e_t}$ выполняются сравнения $e_1 \equiv \dots \equiv e_t \pmod{k}$). Таким образом, теорема 3 дает конструктивный пример правильного множества A с почти точной верхней оценкой величины $k(A)$.

Конструктивное построение правильных множеств по модулю m имеет самостоятельный интерес. В частности, такие множества могут найти применение в прикладных вопросах. Как отмечалось в [1], правильными множествами по модулю m , по-видимому, будут множества вычетов чисел вида g^x , $x = 1, 2, \dots, [m^\varepsilon]$, где g – фиксированное натуральное число взаимно простое с m , показатель которого по модулю m достаточно велик, в частности, если g – первообразный корень по модулю m , m – простое число; а также множества вычетов чисел x^* , $x = 1, 2, \dots, [m^\varepsilon]$, $(x, m) = 1$, где $xx^* \equiv 1 \pmod{m}$.

В связи с теоремами 2 и 3 полезно следующее замечание. Как отмечалось в [7], проблема Варинга изучает базисные свойства (имеется в виду аддитивный базис натурального ряда чисел) последовательности x^n , $x = 0, 1, 2, \dots, n$ – фиксированное натуральное число. Указанная последовательность замечательна тем, что очень просто устроена. Такими же простыми являются приведенные выше последовательности, которые, по-видимому, будут правильными множествами по модулю m . Элементы правильного множества теоремы 3 устроены сложно, они являются суммами растущего количества слагаемых вида g^x . Это в очередной раз подчеркивает разумность постановки проблемы Варинга и родственных ей аддитивных проблем теории чисел.

В настоящей статье построены новые правильные множества для модуля $m = p^N$, p – фиксированное нечетное простое число. Модули такого вида замечательны 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 [8] и применен М. Б. Барбаном, Ю. В. Линником и Н. Г. Чудаковым [9] к проблеме распределения простых чисел в коротких арифметических прогрессиях; автором [10], а затем В. Н. Чубариковым [11] к проблеме границы нулей L -рядов Дирихле; М. М. Петечуком [12] к проблеме делителей Дирихле в коротких арифметических прогрессиях. Отметим также, что если рассматривать задачу о сложности вычисления дискретного логарифма числа x по $\text{mod } m$, 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, $N \geq N_1(p, \varepsilon) > 0$, N – натуральное число, $m = p^N(p-1)$.

ТЕОРЕМА 4. Пусть $m = p^N(p-1)$, $Q = p^{N+1}$, g – некоторый первообразный корень по модулю Q , $\text{ind } x = \text{ind}_g x$. Тогда числа вида $\text{ind } x$, $(x, p) = 1$, $x = 1, 2, \dots, [m^\varepsilon]$, образуют правильное множество A по модулю m , причем

$$k = k(A) \leq 2 \frac{\log m}{\log \|A\|} + 3. \quad (1)$$

ДОКАЗАТЕЛЬСТВО. Определим целое число $t \geq 10$ неравенствами

$$\frac{1}{t} \leq \varepsilon \leq \frac{1}{t-1}.$$

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

$$\text{ind } x_1 + \text{ind } x_2 + \dots + \text{ind } x_r \equiv l \pmod{m}, \quad 1 \leq x_j \leq Y, \quad (x_j, p) = 1, \quad j = 1, 2, \dots, r. \quad (2)$$

Пусть $K = K(Y; m, r)$ – количество решений (2). Пользуясь свойством полной рациональной тригонометрической суммы, находим

$$K = \frac{1}{m} \sum_{a=0}^{m-1} \left(\sum'_{1 \leq x \leq Y} \exp\left(2\pi i \frac{a \text{ind } x}{m}\right) \right)^r \exp\left(-2\pi i \frac{al}{m}\right),$$

где сумма со штрихом означает, что $(x, p) = 1$. Выделяя слагаемое при $a = 0$, получим $K = \frac{1}{m} Y_1^r + R$, где Y_1 – количество $x \leq Y$, $(x, p) = 1$,

$$|R| \leq \max_{0 < a < m} \left| \sum'_{0 < x \leq Y} \exp\left(2\pi i \frac{a \operatorname{ind} x}{m}\right) \right|^s \frac{1}{m} \sum_{a=0}^{m-1} \left| \sum'_{0 < x \leq Y} \exp\left(2\pi i \frac{a \operatorname{ind} x}{m}\right) \right|^{2t}. \quad (3)$$

Обозначим

$$S = \sum'_{0 < x \leq Y} \exp\left(2\pi i \frac{a \operatorname{ind} x}{m}\right) = \sum_{0 < n \leq Y} \chi(n),$$

где $\chi(n)$ – неглавный характер Дирихле по модулю Q . К $|S|$ применима оценка тригонометрической суммы из [10]

$$|S| \leq c_1 Y \exp\left(-c \frac{\log^3 Y}{\log^2 Q}\right), \quad (4)$$

где $c_1, c > 0$ – абсолютные постоянные. Далее, обозначим

$$W = \frac{1}{m} \sum_{a=0}^{m-1} \left| \sum'_{0 < x \leq Y} \exp\left(2\pi i \frac{a \operatorname{ind} x}{m}\right) \right|^{2t}; \quad (5)$$

W равна количеству решений сравнения

$$\begin{aligned} \operatorname{ind} x_1 + \dots + \operatorname{ind} x_t &\equiv \operatorname{ind} y_1 + \dots + \operatorname{ind} y_t \pmod{m}, \\ 1 \leq x_j, y_j &\leq Y, \quad (x_j, p) = (y_j, p) = 1, \quad j = 1, 2, \dots, t. \end{aligned} \quad (6)$$

Из (6) находим

$$x_1 \dots x_t \equiv y_1 \dots y_t \pmod{Q}. \quad (7)$$

Так как $Y^t = m < Q$, то из (7) следует, что $x_1 \dots x_t = y_1 \dots y_t$. Поэтому для W выполнена оценка

$$W \leq \sum_{n \leq Y^t} \tau_t^2(n) \leq t^2 (t!)^{-t-1} Y^t (t \log Y + t^t - 1)^{t^2-1}. \quad (8)$$

Из (3)–(8) находим

$$|R| \leq c_1^s Y^s \exp\left(-\frac{cs \log^3 Y}{\log^2 Q}\right) t^2 (t!)^{-t-1} Y^t (t \log Y + t^t - 1)^{t^2-1}. \quad (9)$$

При $s = 1$ из (9) получаем

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

где постоянная в знаке “ $\ll$ ” зависит только от ε . Следовательно,

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

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

$$K \geq m^{-1} Y_1^{2t+1} - c_2(\varepsilon) Y^{t+1} m^{-c\varepsilon_1^3 (\log m)^{\varepsilon_1^{-2}}} \geq 0.5 m^{-1} Y_1^{2t+1} \geq 0.25 (1 - p^{-1})^{2t+1} m Y.$$

Отсюда следует, что каждое l представимо в виде (2) и число слагаемых в левой части (2) равно

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

т.е. выполнено (1). Теорема 4 доказана.

ЗАМЕЧАНИЕ 1. В доказанной теореме ε может стремиться к 0 при $m \rightarrow +\infty$ не быстрее, чем

$$\sqrt[5]{\frac{\log \log m}{\log m}}.$$

ЗАМЕЧАНИЕ 2. Если в (9) взять $s = \varepsilon_1^{-1}$, то оценка для $k = k(A)$ примет вид

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

в этом случае ε может стремиться к 0 при $m \rightarrow +\infty$ не быстрее, чем

$$\sqrt[4]{\frac{\log \log m}{\log m}}.$$

Автор глубоко признателен профессору Т. Лучаку и профессору Т. Шoenу (13-я Чешская и Словацкая Международная конференция по теории чисел, Остравица, 1–6 сентября 1997 года), указавшим на работу М.Б. Натансона [6]; а также выражает искреннюю благодарность профессору Ю. Белому, который любезно сообщил в письме от 1 декабря 1997 года (Y. Bilu, Institut für Mathematik Technische Universität Graz), что справедлива теорема 3, приведенная выше в данной работе.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Карацуба А. А. Аддитивные сравнения // Изв. РАН. Сер. матем. 1997. Т. 61. № 2. С. 81–94.
- [2] Карацуба А. А. Аналог проблемы Варинга // Вестн. МГУ. Сер. 1. Матем., мех. 1962. № 1. С. 38–46.
- [3] Карацуба А. А. Проблема Варинга для сравнений по модулю, равному степени простого числа // Вестн. МГУ. Сер. 1. Матем., мех. 1962. № 4. С. 28–38.
- [4] Карацуба А. А. Системы сравнений и уравнения варинговского типа // Докл. АН СССР. 1965. Т. 165. № 2. С. 274–276.
- [5] Карацуба А. А. О функции $G(n)$ в проблеме Варинга // Изв. АН СССР. Сер. матем. 1985. Т. 49. № 5. С. 935–947.
- [6] Nathanson M. B. On a problem of Rohrbach for finite groups // J. Number Theory. 1992. V. 41. P. 69–76.
- [7] Карацуба А. А. Проблема Гильберта–Камке в аналитической теории чисел // Матем. заметки. 1987. Т. 41. № 2. С. 272–284.
- [8] Постников А. Г. О сумме характеров по модулю, равному степени простого числа // Изв. АН СССР. Сер. матем. 1955. Т. 19. № 1. С. 11–16.
- [9] Барбан М. В., Линник Ю. В., Чудаков Н. Г. On prime numbers in an arithmetic progression with a prime-power difference // Acta Arith. 1964. V. 9. № 4. P. 375–390.
- [10] Карацуба А. А. Тригонометрические суммы специального вида и их применения // Изв. АН СССР. Сер. матем. 1964. Т. 28. № 2. С. 237–248.
- [11] Чубариков В. Н. Уточнение границы нулей L -рядов Дирихле по модулю, равному степени простого числа // Вестн. МГУ. Сер. 1. Матем., мех. 1973. № 2. С. 46–52.
- [12] Петечук М. М. Сумма значений функций делителей в арифметических прогрессиях с разностью, равной степени нечетного простого числа // Изв. АН СССР. Сер. матем. 1979. Т. 43. № 4. С. 892–908.