Math-Net.Ru

Общероссийский математический портал

А. А. Карацуба, Аддитивные сравнения, *Изв. РАН. Сер. матем.*, 1997, том 61, выпуск 2, 81–94

DOI: <https://doi.org/10.4213/im116>

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: 54.197.217.227

26 апреля 2023 г., 18:20:30

УДК 511

А. А. Карацуба

Аддитивные сравнения

Введено понятие s -правильного множества по модулю m и доказано существование таких множеств, если m есть степень фиксированного нечетного простого числа.

Библиография: 6 наименований.

§ 1. Основные понятия. Формулировка теоремы

Пусть m – натуральное число, $m \geq m_0 > 0$ (m – растущий параметр), E_m – полная система вычетов по модулю m , A – некоторое подмножество E_m , т.е. $A \subseteq E_m$.

ОПРЕДЕЛЕНИЕ 1. Будем говорить, что A является базисом E_m порядка k , если каждое число l из E_m представимо в виде

$$x_1 + \dots + x_k \equiv l \pmod{m}, \quad (1)$$

где $x_1, \dots, x_k$ принадлежат A , и существует такое $l_0 \in E_m$, что

$$x_1 + \dots + x_{k-1} \not\equiv l_0 \pmod{m}$$

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

Везде ниже буквой A будем обозначать базис E_m конечного порядка. Можно считать, что число элементов A не меньше двух, так как в противном случае $k = m$. Далее, очевидно, что A является базисом первого порядка тогда и только тогда, когда $A = E_m$.

Порядок k множества A будем обозначать символом $k(A)$, число элементов A – символом $\|A\|$. Таким образом, исключая тривиальные случаи, считаем, что

$$2 \leq \|A\| < \|E_m\| = m.$$

Легко доказать неравенство

$$k(A) > \frac{\log m}{\log \|A\|}. \quad (2)$$

Действительно, так как $k \geq 2$ в (1), то число всех возможных различных сумм вида $x_1 + \dots + x_k$ с условием $x_j \in A$, $j = 1, \dots, k$, не более чем

$$\frac{1}{k!} \|A\|^k \leq \frac{1}{2} \|A\|^k.$$

Число всех различных вычетов l из E_m равно m . Поэтому, чтобы (1) имело решение при любом l , необходимо выполнение неравенства

$$\|A\|^k > \frac{1}{2} \|A\|^k \geq m. \quad (3)$$

Из (3) следует неравенство (2).

ОПРЕДЕЛЕНИЕ 2. Множество A назовем *правильным* (*c-правильным по модулю m*), если существует абсолютная постоянная $c \geq 1$ такая, что

$$k(A) \leq c \frac{\log m}{\log \|A\|}. \quad (4)$$

Таким образом, в определении 2 постоянная c не зависит от m , которое может быть большим.

Пусть теперь ε – сколь угодно малое положительное число (ε – убывающий параметр). Спрашивается, существуют ли правильные множества A с условием

$$\|A\| \leq m^\varepsilon, \quad m \geq m_0(\varepsilon). \quad (5)$$

Всегда можно считать $\varepsilon < 0,1$ или $\varepsilon \leq \varepsilon_1 < 1$, ε_1 – фиксированное число, так как если доказано, что при $\varepsilon \leq \varepsilon_1 < 1$ множество A является c -правильным по модулю m , то оно, очевидно, будет c_1 -правильным, $c_1 = c\varepsilon_1^{-1}$.

Заметим также, что если справедлива гипотеза Харди–Литтлвуда о том, что $G(n) \leq 4n$ ($G(n)$ – известная в проблеме Варинга функция Харди–Литтлвуда), или несколько более слабое, но еще не доказанное предположение, что $G(n) = O(n)$, то легко доказать существование c -правильных множеств A по модулю m при любом m . Действительно, пусть $0 < \varepsilon < 0,1$. Определим натуральное число n неравенствами

$$\frac{1}{n} \leq \varepsilon < \frac{1}{n-1}.$$

Предположим, далее, что $m \geq m_1(n) = m_2(\varepsilon) > 0$, m – целое число. Тогда при любом целом числе l из промежутка $1 \leq l \leq m$ разрешимо уравнение Варинга следующего вида:

$$x_1^n + \dots + x_k^n = l + m.$$

В этом уравнении $1 \leq x_j \leq (2m)^{1/n} \leq (2m)^\varepsilon$, $j = 1, \dots, k$, и $k \leq G(n) \leq c_1 n$, где по предположению $c_1 \geq 1$ – абсолютная постоянная (в случае справедливости гипотезы Харди–Литтлвуда $c_1 = 4$). Таким образом, определяя множество A как

множество вычетов по модулю m чисел вида x^n , $x = 1, 2, \dots, [(2m)^\varepsilon]$, получаем, что каждое целое число l представимо в виде

$$x_1^n + \dots + x_k^n \equiv l \pmod{m}, \quad 1 \leq x_1, \dots, x_k \leq (2m)^\varepsilon,$$

причем

$$k(A) \leq c_1 n < c_1 \left(\frac{1}{\varepsilon} + 1 \right) < 2c_1 \frac{\log m}{\log \|A\|}.$$

Можно предполагать, что s -правильными множествами по модулю m будут множества вычетов чисел вида g^x , где g – фиксированное натуральное число, большее 1 и взаимно простое с m , $x = 1, 2, \dots, [m^\varepsilon]$, а также множества вычетов чисел вида x^* , где $x^* x \equiv 1 \pmod{m}$, $(x, m) = 1$, $x = 1, \dots, [m^\varepsilon]$.

Цель настоящей работы – доказать существование правильных множеств A для модулей m , являющихся степенью фиксированного нечетного простого числа. Тем же самым методом можно доказать существование правильных множеств A и для более широкого класса модулей m , но все они в какой-то мере похожи на $m = p^N$. Заметим также, что в теореме ε может стремиться к нулю при $m \rightarrow +\infty$, но не очень быстро, именно, не быстрее, чем $8(\log m)^{-1/3}$.

ТЕОРЕМА. Пусть $p \geq 3$, p – простое число, N – натуральное число с условием

$$N \geq \max(512000, 512p^{3/2}), \quad (6)$$

$m = p^N$, ε – произвольное число из промежутка

$$8 \sqrt[3]{\frac{\log p}{\log m}} \leq \varepsilon \leq \min \left(\frac{1}{10}, \frac{1}{\sqrt{p}} \right). \quad (7)$$

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

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

При доказательстве теоремы мы следуем рассуждениям статьи [1], где рассмотрен аналог проблемы Варинга для сравнений. Замечу, что метод статьи [1] послужил источником нового p -адического метода доказательства теоремы Виноградова о среднем [2] и ее обобщений на многомерный случай, что, в свою очередь, дало возможность построить теорию кратных тригонометрических сумм (подробную историю вопроса и результаты см. в [3]). К проблеме Варинга p -адический метод был применен автором в [4]. Это не только упростило доказательство И. М. Виноградова его известной (последней) оценки величины $G(n)$ (см. [5]), но также позволило несколько уточнить оценку. В [4, с. 935] указывалось также, что при конкретных небольших значениях n можно оптимальным образом подбирать параметры предлагаемого метода и получать улучшение результатов о величине $G(n)$.

(“... этот метод дает возможность улучшить прежние результаты при малых значениях n ”), при каждом конкретном n следует оптимально выбрать параметры в леммах 1 и 2 из [5]. В последние годы английские математики Р. Вон и Т. Вули опубликовали большое количество работ, в которых на основе метода статьи [4] получили много новых интересных результатов относительно $G(n)$ при малых n . Однако при больших n классическая оценка И. М. Виноградова

$$G(n) = O(n \log n),$$

полученная им в 1934 г. (см. [6]), до сих пор не улучшена.

ОБОЗНАЧЕНИЯ. Применяются стандартные теоретико-числовые обозначения, в частности $\varphi(a)$ – функция Эйлера.

§ 2. Доказательство теоремы

Множество A построим конструктивно. Возьмем произвольное простое число из промежутка $(32\varepsilon^{-2}, 64\varepsilon^{-2}]$ и обозначим его буквой n . Такое простое число найдется в силу известной теоремы П. Л. Чебышёва (постулат Бертрана). Так как $\varepsilon \leq p^{-1/2}$, то $n > 32p$ и, следовательно, $(n, p(p-1)) = 1$. Множество A определим как множество вычетов по модулю m чисел вида x^n , $x = 1, 2, \dots, [m^\varepsilon]$. Мы докажем, что при любом целом числе l разрешимо сравнение

$$x_1^n + x_2^n + \dots + x_k^n \equiv l \pmod{m}, \quad 1 \leq x_1, x_2, \dots, x_k \leq m^\varepsilon, \quad (8)$$

причем $k < 9(\log m)/\log \|A\|$. Это и означает правильность множества A по модулю m .

Введем два новых параметра s и μ . Целое число s определим неравенствами

$$p^{2sn} \leq m^\varepsilon < p^{2(s+1)n}.$$

Из этих неравенств следует, что

$$s \leq \frac{\varepsilon \log m}{2n \log p} < s + 1. \quad (9)$$

Так как $n \in (32\varepsilon^{-2}, 64\varepsilon^{-2}]$, то

$$s + 1 > \frac{\varepsilon^3 \log m}{128 \log p}, \quad s \leq \frac{\varepsilon^3 \log m}{64 \log p}.$$

Далее, ввиду того, что $\varepsilon \geq 8(\log m)^{-1/3}(\log p)^{1/3}$, получаем $s + 1 > 4$, $s \geq 4$. Таким образом, s – натуральное число, не меньшее, чем 4, причем

$$\frac{\varepsilon^3 \log m}{256 \log p} < s \leq \frac{\varepsilon^3 \log m}{64 \log p}. \quad (10)$$

Целое число μ определим неравенствами

$$p^{2sn(\mu-1)} < m = p^N \leq p^{2sn\mu}.$$

Из этих неравенств следует, что

$$2sn(\mu-1) < N \leq 2sn\mu = N_1, \quad (11)$$

$$\mu-1 < \frac{\log m}{2sn \log p} \leq \mu. \quad (12)$$

Далее, из (9) находим

$$\frac{\varepsilon \log m}{2 \log p} < 2sn \leq \frac{\varepsilon \log m}{\log p},$$

следовательно,

$$\frac{1}{\varepsilon} \leq \mu < \frac{2}{\varepsilon} + 1. \quad (13)$$

Наконец, из (7) и последнего неравенства следует, что μ – натуральное число, причем $\mu \geq 10$.

Пусть теперь $m_1 = p^{2sn\mu} = p^{N_1}$. Из (11) следует, что $m = p^N$ делит m_1 . Пусть l – произвольное целое число. Докажем разрешимость следующего сравнения:

$$x_1^n + x_2^n + \dots + x_k^n \equiv l \pmod{m_1}, \quad 1 \leq x_1, x_2, \dots, x_k \leq p^{2sn} = p^r, \quad (14)$$

причем $k = 2 + 4\mu < 9(\log m)/\log \|A\|$. Так как m делит m_1 , $p^{2sn} \leq m^\varepsilon$, то из разрешимости (14) следует разрешимость (8), т.е. следует утверждение теоремы.

Обозначим символом $I_k(l)$ количество решений сравнения (14). Докажем, что при $k = 2 + 4\mu$ справедлива оценка

$$I_k(l) > 0. \quad (15)$$

Доказательство неравенства (15) разобьем на ряд пунктов.

1. При натуральном числе k_1 с условием $2 \leq k_1 \leq n$ и при целом числе l_1 рассмотрим сравнение

$$x_1^n + x_2^n + \dots + x_{k_1}^n \equiv l_1 \pmod{m_1}, \quad 1 \leq x_1, x_2, \dots, x_{k_1} \leq p^{2sn} = p^r = P. \quad (16)$$

Пусть $W(l_1)$ – количество решений (16). Применяя известную формулу, находим

$$W(l_1) = m_1^{-1} \sum_{a=0}^{m_1-1} S^{k_1} \left(\frac{a}{m_1} \right) \exp \left(-2\pi i \frac{al_1}{m_1} \right), \quad (17)$$

где

$$S \left(\frac{a}{m_1} \right) = \sum_{x=1}^P \exp \left(2\pi i \frac{ax^n}{m_1} \right). \quad (18)$$

Каждое целое a , $0 < a < m_1$, представим в виде $a = p^{N_1-\nu}a_1$, $(a_1, p) = 1$, $\nu = 1, 2, \dots, N_1$. Для a_1 выполняются неравенства $0 < a_1 < p^\nu$. Поэтому, выделяя в (17) слагаемое с $a = 0$, получаем

$$W(l_1) = m_1^{-1}P^{k_1} + m_1^{-1} \sum_{\nu=1}^{N_1} \sum_{\substack{a_1=1 \\ (a_1, p)=1}}^{p^\nu} S^{k_1} \left(\frac{a_1}{p^\nu} \right) \exp \left(-2\pi i \frac{a_1 l_1}{p^\nu} \right). \quad (19)$$

Сумму по ν в (19) разобьем на две: в первую отнесем те слагаемые, для которых $\nu \leq r = 2sn$, во вторую – оставшиеся слагаемые. Приходим к новому равенству

$$W(l_1) = m_1^{-1}P^{k_1} + W_1(l_1) + W_2(l_1), \quad (20)$$

где

$$W_1(l_1) = m_1^{-1} \sum_{\nu=1}^r \sum_{\substack{a_1=1 \\ (a_1, p)=1}}^{p^\nu} S^{k_1} \left(\frac{a_1}{p^\nu} \right) \exp \left(-2\pi i \frac{a_1 l_1}{p^\nu} \right),$$

$$W_2(l_1) = m_1^{-1} \sum_{\nu=r+1}^{N_1} \sum_{\substack{a_1=1 \\ (a_1, p)=1}}^{p^\nu} S^{k_1} \left(\frac{a_1}{p^\nu} \right) \exp \left(-2\pi i \frac{a_1 l_1}{p^\nu} \right).$$

Цель настоящего пункта – доказать неравенство

$$m_1^{-1}P^{k_1} + W_1(l_1) \geq 0,5m_1^{-1}P^{k_1}. \quad (21)$$

Мы докажем, что

$$W_1(l_1) \geq -m_1^{-1}P^{k_1}p^{-k_1+1}.$$

Отсюда неравенство (21) следует тривиально.

Воспользуемся хорошо известными формулами о величине сумм Гаусса (см., например, [2, с. 270]):

$$\sum_{x=1}^{p^\nu} \exp \left(2\pi i \frac{a_1 x^n}{p^\nu} \right) = \begin{cases} p^{\nu - [\frac{\nu}{n}] - 1}, & \text{если } \nu \not\equiv 0, 1 \pmod{n}, \\ p^{\nu - \frac{\nu}{n}}, & \text{если } \nu \equiv 0 \pmod{n}, \\ 0, & \text{если } \nu \equiv 1 \pmod{n}. \end{cases}$$

Отсюда при $\nu = 1, 2, \dots, r$ находим

$$S \left(\frac{a_1}{p^\nu} \right) = \sum_{x=1}^P \exp \left(2\pi i \frac{a_1 x^n}{p^\nu} \right) = F(\nu) = \begin{cases} p^{r - [\frac{\nu}{n}] - 1}, & \text{если } \nu \not\equiv 0, 1 \pmod{n}, \\ p^{r - \frac{\nu}{n}}, & \text{если } \nu \equiv 0 \pmod{n}, \\ 0, & \text{если } \nu \equiv 1 \pmod{n}. \end{cases} \quad (22)$$

Из (22) и определения $W_1(l_1)$ находим

$$\begin{aligned} m_1 W_1(l_1) &= \sum_{\nu=1}^r F^{k_1}(\nu) \sum_{\substack{a_1=1 \\ (a_1, p)=1}}^{p^\nu} \exp\left(-2\pi i \frac{a_1 l_1}{p^\nu}\right) \\ &= \sum_{\nu=2}^r F^{k_1}(\nu) \left\{ \sum_{a_1=1}^{p^\nu} \exp\left(-2\pi i \frac{a_1 l_1}{p^\nu}\right) - \sum_{a_1=1}^{p^{\nu-1}} \exp\left(-2\pi i \frac{a_1 l_1}{p^{\nu-1}}\right) \right\}. \end{aligned}$$

Если $(l_1, p) = 1$, то обе суммы в фигурной скобке равны нулю и, следовательно,

$$W_1(l_1) = 0.$$

Пусть $l_1 = p^{\mu_0} l_2$, $(l_2, p) = 1$, $1 \leq \mu_0$. Если $\mu_0 \geq r$, то выражение в фигурной скобке равно

$$p^\nu - p^{\nu-1} > 0,$$

и так как $F(\nu) \geq 0$, $F(2) > 0$, то $W_1(l_1) > 0$.

Пусть $1 \leq \mu_0 \leq r-1$,

$$\begin{aligned} \Delta(\nu) &= \sum_{a_1=1}^{p^\nu} \exp\left(-2\pi i \frac{a_1 l_2}{p^{\nu-\mu_0}}\right) - \sum_{a_1=1}^{p^{\nu-1}} \exp\left(-2\pi i \frac{a_1 l_2}{p^{\nu-\mu_0-1}}\right), \\ m_1 W_1(l_1) &= \sum_{\nu=2}^r F^{k_1}(\nu) \Delta(\nu). \end{aligned}$$

Если $\nu \geq \mu_0 + 2$, то $\Delta(\nu) = 0$, т.е.

$$m_1 W_1(l_1) = \sum_{\nu=2}^{\mu_0+1} F^{k_1}(\nu) \Delta(\nu).$$

Если $\mu_0 = 1$, то

$$m_1 W_1(l_1) = F^{k_1}(2) \Delta(2), \quad F(2) = p^{r-1}, \quad \Delta(2) = -p,$$

т.е.

$$m_1 W_1(l_1) = -p^{k_1 r - (k_1 - 1)} = -P^{k_1} p^{-k_1 + 1}.$$

Пусть $2 \leq \mu_0 \leq r-1$. Если $\nu = \mu_0 + 1$, то

$$\Delta(\nu) = -p^{\mu_0}.$$

Если $\nu \leq \mu_0$, то

$$\Delta(\nu) = p^\nu - p^{\nu-1}.$$

Поэтому получаем такое равенство:

$$m_1 W_1(l_1) = \sum_{\nu=2}^{\mu_0} F^{k_1}(\nu)(p^\nu - p^{\nu-1}) - F^{k_1}(\mu_0 + 1)p^{\mu_0}.$$

Представим μ_0 в виде $\mu_0 = \mu_1 n + \mu_2$, $\mu_1 \geq 0$, $1 \leq \mu_2 \leq n$. Если $\mu_2 = n$, то $F(\mu_0 + 1) = 0$ и, следовательно, $W_1(l_1) \geq 0$. Пусть $1 \leq \mu_2 \leq n - 1$. Если $\mu_1 = 0$, то $\mu_2 \geq 2$,

$$m_1 W_1(l_1) = \sum_{\nu=2}^{\mu_2} F^{k_1}(\nu)(p^\nu - p^{\nu-1}) - F^{k_1}(\mu_2 + 1)p^{\mu_2},$$

причем

$$F(\nu) = p^{r-1}, \quad 2 \leq \nu \leq \mu_2 \leq n - 1,$$

$$F(\mu_2 + 1) = \begin{cases} p^{r-1}, & \text{если } \mu_2 + 1 < n, \\ p^{r-1} = p^{r-\frac{\mu_2+1}{n}}, & \text{если } \mu_2 + 1 = n. \end{cases}$$

Поэтому имеем

$$m_1 W_1(l_1) = \sum_{\nu=2}^{\mu_2} p^{k_1(r-1)}(p^\nu - p^{\nu-1}) - p^{k_1(r-1)+\mu_2} = -p^{k_1 r - k_1 + 1} = -P^{k_1} p^{-k_1 + 1}.$$

Пусть $\mu_1 \geq 1$, $1 \leq \mu_2 \leq n - 1$. Тогда имеем равенство

$$\begin{aligned} m_1 W_1(l_1) &= \sum_{j=1}^{\mu_2} F^{k_1}(\mu_1 n + j)(p^{\mu_1 n + j} - p^{\mu_1 n + j - 1}) \\ &\quad + \sum_{j=0}^{\mu_1 - 1} \sum_{i=1}^n F^{k_1}(nj + i)(p^{nj+i} - p^{nj+i-1}) \\ &\quad - F^{k_1}(\mu_1 n + \mu_2 + 1)p^{\mu_1 n + \mu_2}. \end{aligned} \quad (23)$$

Если $\mu_2 = 1$, то первое слагаемое правой части (23) равно нулю и, следовательно,

$$\begin{aligned} m_1 W_1(l_1) &= \sum_{j=0}^{\mu_1 - 1} \sum_{i=2}^n F^{k_1}(nj + i)(p^{nj+i} - p^{nj+i-1}) - F^{k_1}(\mu_1 n + 2)p^{\mu_1 n + 1} \\ &= \sum_{j=0}^{\mu_1 - 1} p^{k_1(r-j-1)}(p^{nj+n} - p^{nj+1}) - p^{k_1(r-\mu_1-1)+\mu_1 n + 1} \\ &= (1 - p^{-n+1}) \sum_{j=0}^{\mu_1 - 1} p^{k_1(r-1)+(n-k_1)j+n} - p^{k_1(r-1)+(n-k_1)\mu_1 + 1} \\ &\geq (1 - p^{-n+1})p^{k_1(r-1)+(n-k_1)\mu_1 + k_1} - p^{k_1(r-1)+(n-k_1)\mu_1 + 1} > 0. \end{aligned}$$

Пусть $2 \leq \mu_2 \leq n-1$. Отметим, что при $2 \leq i \leq n$ в силу формул (22) справедливо равенство

$$F(nj+i) = p^{r-j-1}.$$

Поэтому из (23) получаем

$$\begin{aligned} m_1 W_1(l_1) &= \sum_{j=2}^{\mu_2} p^{(r-\mu_1-1)k_1} (p^{\mu_1 n+j} - p^{\mu_1 n+j-1}) \\ &\quad + \sum_{j=0}^{\mu_1-1} p^{k_1(r-j-1)} \sum_{i=2}^n (p^{nj+i} - p^{nj+i-1}) \\ &\quad - p^{k_1(r-\mu_1-1)+\mu_1 n+\mu_2} = p^{k_1(r-\mu_1-1)} (p^{\mu_1 n+\mu_2} - p^{\mu_1 n+1}) \\ &\quad + \sum_{j=0}^{\mu_1-1} p^{k_1(r-j-1)} (p^{nj+n} - p^{nj+1}) - p^{k_1(r-\mu_1-1)+\mu_1 n+\mu_2} \\ &= -p^{k_1(r-1)+(n-k_1)\mu_1+1} + (1-p^{-n+1}) \sum_{j=0}^{\mu_1-1} p^{k_1(r-1)+(n-k_1)j+n} \\ &\geq -p^{k_1(r-1)+(n-k_1)\mu_1+1} + (1-p^{-n+1}) p^{k_1(r-1)+(n-k_1)\mu_1+k_1} > 0. \end{aligned}$$

Таким образом, при всех возможных значениях μ_0 выполняется неравенство

$$W_1(l_1) \geq -m_1^{-1} P^{k_1} p^{-k_1+1},$$

откуда следует (21).

2. Введем p -адические аналоги u -чисел Виноградова (см. [2, с. 169, 170, или с. 174, 175, или с. 279, 280]), которые также назовем u -числами. По определению u -числами будем называть числа вида

$$u = y_1^n + (p^{2s} y_2)^n + (p^{2s \cdot 2} y_3)^n + \dots + (p^{2s(\mu-1)} y_\mu)^n,$$

где $y_1, y_2, \dots, y_\mu$ принимают значения натуральных чисел, взаимно простых с p и таких, что

$$y_1 \leq p^{2sn}, \quad y_2 \leq p^{2sn-2s}, \quad y_3 \leq p^{2sn-2s \cdot 2}, \quad \dots, \quad y_\mu \leq p^{2sn-2s(\mu-1)}.$$

Из (13) и определения n следует

$$n > 32\varepsilon^{-2} > 2\varepsilon^{-1} > \mu - 1.$$

Поэтому если буквой U обозначить множество u -чисел, а символом $\|U\|$ — количество элементов U , то имеем следующие соотношения:

$$2^{-\mu} p^{2sn\mu(1-\frac{\mu-1}{2n})} \leq \|U\| = \prod_{j=0}^{\mu-1} \varphi(p^{2sn-2sj}) < p^{2sn\mu(1-\frac{\mu-1}{2n})}.$$

Отметим, что числа $u \in U$ попарно несравнимы по модулю $p^{2sn\mu} = m_1$. Действительно, пусть u, u' – два разных u -числа из U , т.е.

$$\begin{aligned} u &= (y_1)^n + (p^{2s}y_2)^n + \dots + (p^{2s(\mu-1)}y_\mu)^n, \\ u' &= (y'_1)^n + (p^{2s}y'_2)^n + \dots + (p^{2s(\mu-1)}y'_\mu)^n, \end{aligned}$$

причем $\bar{y} = (y_1, y_2, \dots, y_\mu) \neq \bar{y}' = (y'_1, y'_2, \dots, y'_\mu)$, и пусть $u \equiv u' \pmod{m_1}$. Из последнего сравнения следует

$$\begin{aligned} (y_1)^n &\equiv (y'_1)^n \pmod{p^{2sn}}, & n \operatorname{ind} y_1 &\equiv n \operatorname{ind} y'_1 \pmod{\varphi(p^{2sn})}, \\ \operatorname{ind} y_1 &\equiv \operatorname{ind} y'_1 \pmod{\varphi(p^{2sn})}, & y_1 &\equiv y'_1 \pmod{p^{2sn}} \end{aligned}$$

(мы воспользовались тем, что $(y_1, p) = (y'_1, p) = 1$, $(n, \varphi(p^{2sn})) = 1$). Следовательно, $y_1 = y'_1$, так как $1 \leq y_1, y'_1 < p^{2sn}$. После очевидных преобразований приходим к сравнению

$$(y_2)^n \equiv (y'_2)^n \pmod{p^{2sn}},$$

из которого получим $y_2 = y'_2$, и так далее. После μ -го шага указанного процесса получим $y_\mu = y'_\mu$, т.е. $u = u'$, что противоречит предположению $u \neq u'$. Итак, числа $u \in U$ попарно несравнимы по модулю m_1 . Определим далее множество чисел U_1 , подобное множеству U . По определению u_1 -числами будем называть числа вида

$$u_1 = z_1^n + (p^s z_2)^n + (p^{s \cdot 2} z_3)^n + \dots + (p^{s(2\mu-1)} z_{2\mu})^n,$$

где $z_1, z_2, \dots, z_{2\mu}$ принимают значения натуральных чисел, взаимно простых с p и таких, что

$$z_1 \leq p^{sn}, \quad z_2 \leq p^{sn-s}, \quad z_3 \leq p^{sn-s \cdot 2}, \quad \dots, \quad z_{2\mu} \leq p^{sn-s(2\mu-1)}.$$

Из (13) и определения n следует, что $n > 2\mu - 1$. Буквой U_1 обозначим множество так определенных чисел u_1 , а символом $\|U_1\|$ – количество элементов U_1 . Тогда имеем следующие соотношения:

$$2^{-2\mu} p^{2sn\mu(1-\frac{2\mu-1}{2n})} \leq \|U_1\| = \prod_{j=0}^{2\mu-1} \varphi(p^{ns-j}) < p^{2sn\mu(1-\frac{2\mu-1}{2n})}.$$

Числа $u_1 \in U_1$ попарно несравнимы по модулю m_1 .

Наконец, буквой T обозначим множество натуральных чисел t , не превосходящих p^{sn} и взаимно простых с p , т.е. если $t \in T$, то $1 \leq t < p^{sn}$, $(t, p) = 1$. Очевидно, что

$$2^{-1} p^{sn} \leq \|T\| = \varphi(p^{sn}) < p^{sn}.$$

Отметим, что число $t^n u_1$, $t \in T$, $u_1 \in U_1$, равняется сумме 2μ слагаемых, каждое из которых есть n -я степень натурального числа, не превосходящего $p^{2sn} = P$.

3. Рассмотрим тригонометрическую сумму S вида

$$S = \sum_{t \in T} \sum_{u_1 \in U_1} \exp \left(2\pi i \frac{a_1 t^n u_1}{p^\nu} \right), \quad (a_1, p) = 1,$$

и оценим сверху $|S|$ при условии, что $r = 2sn < \nu \leq 2sn\mu$.

ЛЕММА. Для $|S|$ при $2sn < \nu \leq 2sn\mu$ справедлива следующая оценка:

$$|S| \leq \|T\| \|U_1\| \Delta_1,$$

где

$$\Delta_1 = 2^{\mu+1} p^{-sn/3} = 2^{\mu+1} P^{-1/6}.$$

ДОКАЗАТЕЛЬСТВО. Оценку проведем методом сглаживания Виноградова (см. [6]). Определим целое число λ неравенствами

$$s\lambda n < \nu \leq s(\lambda + 1)n.$$

Так как по условию леммы $\nu > 2sn$, то $2sn < s(\lambda + 1)n$, $\lambda > 1$. Так как $\nu \leq 2sn\mu$, то $s\lambda n < 2sn\mu$, $\lambda < 2\mu$. Таким образом, для λ выполняются неравенства $2 \leq \lambda \leq 2\mu - 1$.

По определению положим

$$v_\lambda = z_1^n + (p^s z_2)^n + \dots + (p^{s\lambda} z_{\lambda+1})^n.$$

Тогда очевидно сравнение

$$u_1 \equiv v_\lambda \pmod{p^\nu}.$$

Кроме того очевидно также, что если v_λ и v'_λ разные, т.е. если

$$\bar{z} = (z_1, z_2, \dots, z_{\lambda+1}) \neq \bar{z}' = (z'_1, z'_2, \dots, z'_{\lambda+1}),$$

то $v_\lambda \not\equiv v'_\lambda \pmod{p^\nu}$. Учитывая сделанные замечания, последовательно находим

$$\begin{aligned} S &= S_1 \prod_{j=\lambda+1}^{2\mu-1} \varphi(p^{ns-j s}), \quad S_1 = \sum_{t \in T} \sum_{v_\lambda} \exp \left(2\pi i \frac{a_1 v_\lambda t^n}{p^\nu} \right); \\ |S_1|^2 &\leq \prod_{j=0}^{\lambda} \varphi(p^{ns-j s}) \sum_{z=1}^{p^\nu} \left| \sum_{t \in T} \exp \left(2\pi i \frac{a_1 z t^n}{p^\nu} \right) \right|^2 \\ &\leq p^\nu \varphi(p^{sn}) \left(\prod_{j=0}^{\lambda} \varphi(p^{ns-j s}) \right)^2 \left(\prod_{j=0}^{\lambda} \varphi(p^{ns-j s}) \right)^{-1}, \\ |S| &\leq \varphi(p^{sn}) \prod_{j=0}^{2\mu-1} \varphi(p^{ns-j s}) \Delta = \|T\| \|U_1\| \Delta, \end{aligned}$$

где

$$\begin{aligned}\Delta^2 &\leq p^\nu (\varphi(p^{sn}))^{-1} \left(\prod_{j=0}^{\lambda} \varphi(p^{ns-j}) \right)^{-1} \\ &\leq 2^{\lambda+2} p^{\nu-sn-(\lambda+1)ns+s\frac{\lambda(\lambda+1)}{2}} \leq 2^{\lambda+2} p^{-sn(1-\frac{\lambda(\lambda+1)}{2n})}.\end{aligned}$$

Далее, так как $n > 32\varepsilon^{-2}$, $\mu < 2\varepsilon^{-1} + 1 < 3\varepsilon^{-1}$, $\lambda \leq 2\mu - 1$, то получаем

$$\begin{aligned}\frac{\lambda(\lambda+1)}{2n} &< \frac{(2\mu-1)\mu}{n} < \frac{(4\varepsilon^{-1}+1)(2\varepsilon^{-1}+1)}{32\varepsilon^{-2}} < \frac{9}{32}, \\ \Delta^2 &\leq 2^{\lambda+2} p^{-\frac{23}{32}sn}, \\ \Delta &\leq 2^{\mu+1} p^{-2sn\frac{23}{128}} < 2^{\mu+1} p^{-2sn\frac{1}{6}} = 2^{\mu+1} P^{-\frac{1}{6}}.\end{aligned}$$

Лемма доказана.

4. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ. Пусть l – любое целое число. Рассмотрим следующее сравнение:

$$x_1^n + x_2^n + u + u' + t^n u_1 \equiv l \pmod{p^{2sn\mu}}, \quad (24)$$

где $1 \leq x_1, x_2 \leq p^{2sn}$, $u, u' \in U$, $t \in T$, $u_1 \in U_1$. Обозначим символом I количество решений (24). Сравнение (24) можно записать еще так:

$$x_1^n + x_2^n \equiv l_1 \pmod{p^{2sn\mu}},$$

где $l_1 = l - u - u' - t^n u_1$.

При фиксированных u, u', t, u_1 по формуле (20) имеем равенство

$$W(l_1) = m_1^{-1} p^{4sn} + W_1(l_1) + W_2(l_1). \quad (25)$$

По (21), где следует взять $k_1 = 2$, получаем

$$m_1^{-1} p^{4sn} + W_1(l_1) \geq 0,5 m_1^{-1} p^{4sn}. \quad (26)$$

Суммируя обе части равенства (25) по $u, u' \in U$, $t \in T$, $u_1 \in U_1$ и пользуясь (26), найдем

$$\begin{aligned}I &= \sum_{u, u' \in U} \sum_{t \in T} \sum_{u_1 \in U_1} (m_1^{-1} p^{4sn} + W_1(l_1)) \\ &\quad + m_1^{-1} \sum_{\nu=r+1}^{N_1} \sum_{\substack{a_1=1 \\ (a_1, p)=1}}^{p^\nu} S^2\left(\frac{a_1}{p^\nu}\right) \sum_{u, u' \in U} \exp\left(2\pi i \frac{a_1(u+u')}{p^\nu}\right) \\ &\quad \times \sum_{t \in T} \sum_{u_1 \in U_1} \exp\left(2\pi i \frac{a_1 t^n u_1}{p^\nu}\right) \exp\left(-2\pi i \frac{a_1 l}{p^\nu}\right) \\ &\geq 0,5 m_1^{-1} p^{4sn} \|U\|^2 \|T\| \|U_1\| - m_1^{-1} \sum_{\nu=r+1}^{N_1} \sum_{\substack{a_1=1 \\ (a_1, p)=1}}^{p^\nu} \left| S\left(\frac{a_1}{p^\nu}\right) \right|^2 \\ &\quad \times \left| \sum_{u \in U} \exp\left(2\pi i \frac{a_1 u}{p^\nu}\right) \right|^2 \left| \sum_{t \in T} \sum_{u_1 \in U_1} \exp\left(2\pi i \frac{a_1 t^n u_1}{p^\nu}\right) \right|. \quad (27)\end{aligned}$$

Оценим сверху второе слагаемое в (27), которое обозначим символом I_2 . Для этого модуль суммы $S(a_1/p^\nu)$ оценим тривиально количеством слагаемых, т.е. p^{2sn} ; модуль кратной суммы по t, u_1 оценим, пользуясь леммой:

$$\left| \sum_{t \in T} \sum_{u_1 \in U_1} \exp \left(2\pi i \frac{a_1 t^n u_1}{p^\nu} \right) \right| < 2^{\mu+1} p^{-\frac{1}{3}sn} \|T\| \|U_1\|.$$

Тем самым получаем

$$\begin{aligned} I_2 &\leq p^{4sn} \cdot 2^{\mu+1} p^{-\frac{1}{3}sn} \|T\| \|U_1\| m_1^{-1} \sum_{\nu=r+1}^{N_1} \sum_{\substack{a_1=1 \\ (a_1, p)=1}}^{p^\nu} \left| \sum_{u \in U} \exp \left(2\pi i \frac{a_1 u}{p^\nu} \right) \right|^2 \\ &\leq p^{4sn} 2^{\mu+1} p^{-\frac{1}{3}sn} \|T\| \|U_1\| m_1^{-1} \sum_{\nu=1}^{N_1} \sum_{\substack{a_1=1 \\ (a_1, p)=1}}^{p^\nu} \left| \sum_{u \in U} \exp \left(2\pi i \frac{a_1 u}{p^\nu} \right) \right|^2 \\ &\leq 2^{\mu+1} p^{4sn - \frac{1}{3}sn} \|T\| \|U_1\| m_1^{-1} \sum_{a=0}^{m_1-1} \left| \sum_{u \in U} \exp \left(2\pi i \frac{au}{m_1} \right) \right|^2 \\ &= 2^{\mu+1} p^{4sn - \frac{1}{3}sn} \|T\| \|U_1\| \|U\|. \end{aligned} \quad (28)$$

Из (27) и (28) находим

$$I \geq 0,5 m_1^{-1} p^{4sn} \|U\|^2 \|T\| \|U_1\| \Delta_1, \quad (29)$$

где

$$\Delta_1 = 1 - 2^{\mu+2} m_1 p^{-\frac{1}{3}sn} \|U\|^{-1}.$$

Для количества элементов множества U мы имели нижнюю оценку:

$$\|U\| \geq 2^{-\mu} p^{2sn\mu(1-\frac{\mu-1}{2n})}.$$

Поэтому

$$2^{\mu+2} m_1 p^{-\frac{1}{3}sn} \|U\|^{-1} \leq 2^{2\mu+2} p^{-\frac{1}{3}sn + s\mu(\mu-1)} = 2^{2\mu+2} p^{-\frac{sn}{3} \left(1 - \frac{3\mu(\mu-1)}{n}\right)}.$$

Так как $\mu < 2\varepsilon^{-1} + 1$, $n > 32\varepsilon^{-2}$, $\varepsilon \leq 0,1$, то

$$\begin{aligned} \frac{3\mu(\mu-1)}{n} &\leq \frac{(6\varepsilon^{-1} + 3)2\varepsilon^{-1}}{32\varepsilon^{-2}} < \frac{16\varepsilon^{-2}}{32\varepsilon^{-2}} = \frac{1}{2}, \\ 2^{2\mu+2} p^{-\frac{sn}{3} \left(1 - \frac{3\mu(\mu-1)}{n}\right)} &< 2^{2\mu+2} p^{-\frac{sn}{6}} < 2^{2\mu+2 - \frac{sn}{6}} < 2^{-1}, \quad \Delta_1 > 2^{-1}, \\ I &> 0,25 m_1^{-1} p^{4sn} \|U\|^2 \|T\| \|U_1\| > 0. \end{aligned}$$

Отсюда следует разрешимость сравнения (24), а следовательно, и сравнения (14). Число слагаемых в левой части (24), которые являются n -ми степенями натуральных чисел, не превосходящих $p^{2sn} \leq m^\varepsilon$, равно k ,

$$k = 2 + 2\mu + 2\mu = 2 + 4\mu < 9(\log m)/(\log \|A\|).$$

Теорема доказана.

ЗАМЕЧАНИЕ 1. Определенные и построенные правильные множества A являются достаточно “густыми”, так как количество элементов в них не меньше чем

$$\exp(c_1 \log^{2/3} m), \quad c_1 = c_1(p) > 0.$$

Если рассматривать “редкие” множества A , то при определении их “правильности” следует учитывать k в неравенстве $m \leq (k!)^{-1} \|A\|$.

ЗАМЕЧАНИЕ 2. Можно прямо воспользоваться результатом статьи [1] для доказательства существования правильных множеств. Но тогда получится только теорема существования. Эффективные соотношения между m , p и ε , которые даются неравенствами (7), будут значительно более слабыми из-за больших констант, зависящих от n . Такое же явление имеет место и в том случае, если пользоваться гипотезой Харди–Литтлвуда о величине $G(n)$ или гипотезой $G(n) = O(n)$.

ЗАМЕЧАНИЕ 3. В теореме вместе с N может расти также p . Порядок роста p определяется неравенствами (6) и (7).

Список литературы

1. Карацуба А. А. Проблема Варинга для сравнения по модулю, равному степени простого числа // Вестн. Московского ун-та. Сер. 1. Математика, механика. 1962. Т. 4. С. 28–38.
2. Виноградов И. М. Избранные труды. М.: Изд-во АН СССР, 1952.
3. Артипов Г. И., Карацуба А. А., Чубариков В. Н. Теория кратных тригонометрических сумм. М.: Наука, 1987.
4. Карацуба А. А. О функции $G(n)$ в проблеме Варинга // Изв. АН СССР. Сер. матем. 1985. Т. 49. № 5. С. 935–947.
5. Виноградов И. М. К вопросу о верхней границе для $G(n)$ // Изв. АН СССР. Сер. матем. 1959. Т. 23. № 5. С. 637–642.
6. Виноградов И. М. Новая оценка $G(n)$ в проблеме Варинга // Докл. АН СССР. 1934. Т. 4. № 5–6. С. 249–253.

МИАН

Поступило в редакцию
15.X.1996