Math-Net.Ru

Общероссийский математический портал

А. А. Глибичук, Комбинаторные свойства множеств вычетов по простому модулю и задача Эрдёша–Грэхэма, *Матем. заметки*, 2006, том 79, выпуск 3, 384–395

DOI: <https://doi.org/10.4213/mzm2708>

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: 54.237.59.107

26 апреля 2023 г., 18:37:18

КОМБИНАТОРНЫЕ СВОЙСТВА МНОЖЕСТВ ВЫЧЕТОВ ПО ПРОСТОМУ МОДУЛЮ И ЗАДАЧА ЭРДЁША–ГРЭХЭМА

А. А. Глибичук

Рассмотрим произвольное $\varepsilon > 0$ и достаточно большое простое число $p > 2$. Доказано, что для любого целого числа a существуют попарно различные целые $x_1, x_2, \dots, x_N$, где $N = 8([1/\varepsilon + 1/2] + 1)^2$, такие, что $1 \leq x_i \leq p^\varepsilon$, $i = 1, \dots, N$, и

$$a \equiv x_1^{-1} + \dots + x_N^{-1} \pmod{p},$$

где x_i^{-1} – наименьшее положительное целое такое, что $x_i^{-1}x_i \equiv 1 \pmod{p}$. Это улучшает результат Шпарлинского.

Библиография: 11 названий.

1. Введение. Эрдёш и Грэхэм [1] поставили такую задачу.

ЗАДАЧА. Существует ли для любого $\varepsilon > 0$ такое $k(\varepsilon) \in \mathbb{N}$, что для любого достаточно большого простого p и для любого целого c существует $k \leq k(\varepsilon)$ попарно различных целых чисел x_i таких, что $1 \leq x_i \leq p^\varepsilon$, $i = 1, 2, \dots, k$, и

$$\sum_{i=1}^k x_i^{-1} \equiv c \pmod{p}, \quad (1)$$

где здесь и в дальнейшем x_i^{-1} – наименьшее положительное целое такое, что $x_i^{-1}x_i \equiv 1 \pmod{p}$.

Крут [2] показал, что можно выбрать $k \leq \log^{3+o(1)} p$ попарно различных чисел на интервале $[1, p^\varepsilon]$, чтобы выполнялось (1).

Следующим результатом в этом направлении была работа И. Е. Шпарлинского [3]. Он использует оценки тригонометрических сумм А. А. Карацубы (см. [4]–[6]) и устанавливает, что для любого $\varepsilon > 0$ и для достаточно большого p можно выбрать $k = 4\varepsilon^{-3} + O(\varepsilon^{-2})$ попарно различных чисел x_i , $i = 1, \dots, k$, таких, что $1 \leq x_i \leq p^\varepsilon$ и выполняется (1).

Далее Крут [7] доказал, что для любого $\varepsilon \in (0, 1]$ и для любой степени $k \geq 1$ существует $N = N(k, \varepsilon)$ такое, что для любого достаточно большого простого p и для любого класса вычетов $a \pmod{p}$ существуют положительные целые $x_1, \dots, x_N \leq p^\varepsilon$, удовлетворяющие сравнению

$$a \equiv (x_1^k)^{-1} + \dots + (x_N^k)^{-1} \pmod{p}.$$

Мы докажем следующую теорему, усиливающую результат работы [3].

Работа выполнена при поддержке Российского фонда фундаментальных исследований, грант № 05-01-00066, и программы “Ведущие научные школы”, грант № НШ-304.2003.1.

ТЕОРЕМА 3. Для любого $\varepsilon > 0$, для любого достаточно большого простого p и для любого класса вычетов $a \pmod{p}$ существуют положительные попарно различные целые $x_1, \dots, x_N \leq p^\varepsilon$, где $N = 8 \cdot ([1/\varepsilon + 1/2] + 1)^2$, такие, что

$$a \equiv x_1^{-1} + \dots + x_N^{-1} \pmod{p}.$$

В доказательстве будет использована техника работ [4], [6], а также комбинаторные свойства множеств вычетов по простому модулю. Для того, чтобы сформулировать эти свойства, нам потребуется несколько определений и обозначений.

Пусть на X задана некоторая бинарная операция $*$: $X \times X \rightarrow X$. Рассмотрим A и B – произвольные подмножества X . Обозначим

$$A * B = \{a * b : a \in A, b \in B\}.$$

В частности, для подмножеств A и B некоторого кольца мы определим две операции: сумма множеств

$$A + B = \{a + b : a \in A, b \in B\}$$

и произведение множеств

$$A \cdot B = AB = \{ab : a \in A, b \in B\}.$$

В дальнейшем будем обозначать для некоторого $k \in \mathbb{N}$

$$kA = \underbrace{A + A + \dots + A}_k.$$

Возьмем в качестве кольца поле вычетов по модулю некоторого простого числа p . Обозначим его $\mathbb{Z}_p$. Здесь и ниже будем полагать, что p – простое число.

ОПРЕДЕЛЕНИЕ 1. Назовем подмножество $A \subset \mathbb{Z}_p$ *симметричным*, если $A = -A$, где $-A = \{-a : a \in A\}$ и *антисимметричным*, если $A \cap (-A) = \emptyset$.

Множество обратимых элементов $\mathbb{Z}_p$ будем обозначать $\mathbb{Z}_p^*$. Очевидно, что $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

ОПРЕДЕЛЕНИЕ 2. Назовем число k *мультипликативным порядком* элемента $g \in \mathbb{Z}_p^*$, если $k = \min\{i : g^i = 1 \pmod{p}\}$. Будем обозначать $k = \text{ord}_p g$.

ТЕОРЕМА 1. Если $A \subset \mathbb{Z}_p$ и $B \subset \mathbb{Z}_p$ такие, что B антисимметричное и $|A||B| > p$, то $8AB = \mathbb{Z}_p$.

ТЕОРЕМА 2. Пусть $A \subset \mathbb{Z}_p$ и $B \subset \mathbb{Z}_p$ такие, что B симметричное и $|A||B| > p$; тогда $8AB = \mathbb{Z}_p$.

Доказательство теорем 1 и 2 использует технику работы [8]. Из теорем 1 и 2 мы выведем ряд следствий и теорему 3. Здесь мы приведем формулировку одного из полученных следствий.

СЛЕДСТВИЕ 5. Пусть $A = \{g^x : 0 \leq x \leq 2[\sqrt{p}]\}$, где $\text{ord}_p g > \sqrt{p}$, тогда $8A = \mathbb{Z}_p$.

Это следствие является улучшением теоремы 2 из [9] для случая, когда $|A|$ не намного больше $2[\sqrt{p}]$.

Если бы аналог теоремы 3 удалось доказать при $N \leq c/\varepsilon$, где c — константа, то была бы доказана гипотеза Карацубы, сформулированная в [10] на стр. 83 (смотри также [11, с. 225]).

2. Доказательство теорем 1, 2 и следствий. Докажем следующий аналог леммы 4.2 из [8].

ЛЕММА 1. Пусть $A \subset \mathbb{Z}_p$, $B \subset \mathbb{Z}_p$, $G \subset \mathbb{Z}_p^*$ и $G \neq \emptyset$. Тогда найдется $\xi \in G$ такой, что

$$|A + \xi B| \geq \frac{|A| |B| |G|}{|A| |B| + |G|}, \quad (2)$$

$$|A - \xi B| \geq \frac{|A| |B| |G|}{|A| |B| + |G|}. \quad (3)$$

ДОКАЗАТЕЛЬСТВО. Возьмем произвольные элементы $\xi \in G$ и $s \in \mathbb{Z}_p$. Введем обозначения

$$f_\xi^+(s) := |\{(a, b) : a \in A, b \in B, a + b\xi = s\}|,$$

$$f_\xi^-(s) := |\{(a, b) : a \in A, b \in B, a - b\xi = s\}|.$$

Тогда

$$\begin{aligned} \sum_{s \in \mathbb{Z}_p} (f_\xi^+(s))^2 &= |\{(a_1, b_1, a_2, b_2) : a_1, a_2 \in A, b_1, b_2 \in B, a_1 + b_1\xi = a_2 + b_2\xi\}| \\ &= |A| |B| + |\{(a_1, b_1, a_2, b_2) : a_1, a_2 \in A, b_1, b_2 \in B, a_1 \neq a_2, a_1 + b_1\xi = a_2 + b_2\xi\}|, \\ \sum_{s \in \mathbb{Z}_p} (f_\xi^-(s))^2 &= |\{(a_1, b_1, a_2, b_2) : a_1, a_2 \in A, b_1, b_2 \in B, a_1 - b_1\xi = a_2 - b_2\xi\}| \\ &= |A| |B| + |\{(a_1, b_1, a_2, b_2) : a_1, a_2 \in A, b_1, b_2 \in B, a_1 \neq a_2, a_1 - b_1\xi = a_2 - b_2\xi\}|. \end{aligned}$$

Таким образом,

$$\sum_{s \in \mathbb{Z}_p} (f_\xi^-(s))^2 = \sum_{s \in \mathbb{Z}_p} (f_\xi^+(s))^2. \quad (4)$$

В дальнейшем, учитывая (4), мы будем работать лишь со второй суммой квадратов. Заметим, что для любых $a_1, a_2 \in A, b_1, b_2 \in B$ таких, что $a_1 \neq a_2$, существует не более одного η такого, что $a_1 + b_1\eta = a_2 + b_2\eta$. Тогда

$$\sum_{\xi \in G} \sum_{s \in \mathbb{Z}_p} (f_\xi^+(s))^2 \leq |A| |B| |G| + |A|^2 |B|^2.$$

Тогда найдется такое $\xi \in G$, что выполнено следующее неравенство:

$$\sum_{s \in \mathbb{Z}_p} (f_\xi^+(s))^2 \leq |A| |B| + \frac{|A|^2 |B|^2}{|G|}. \quad (5)$$

Из неравенства Коши–Буняковского получим

$$\begin{aligned} \left(\sum_{s \in \mathbb{Z}_p} f_\xi^+(s) \right)^2 &\leq |A + \xi B| \sum_{s \in \mathbb{Z}_p} (f_\xi^+(s))^2, \\ \left(\sum_{s \in \mathbb{Z}_p} f_\xi^-(s) \right)^2 &\leq |A - \xi B| \sum_{s \in \mathbb{Z}_p} (f_\xi^-(s))^2. \end{aligned}$$

Кроме того,

$$\sum_{s \in \mathbb{Z}_p} f_\xi^+(s) = |A| |B|, \quad \sum_{s \in \mathbb{Z}_p} f_\xi^-(s) = |A| |B|.$$

Таким образом, из последних неравенств, учитывая (5), получим

$$|A + \xi B| \geq \frac{|A|^2 |B|^2}{|A| |B| + |A|^2 |B|^2 / |G|} = \frac{|A| |B| |G|}{|A| |B| + |G|}, \quad |A - \xi B| \geq \frac{|A| |B| |G|}{|A| |B| + |G|}.$$

Лемма 1 доказана.

ЛЕММА 2. Пусть $A \subset \mathbb{Z}_p$, $B \subset \mathbb{Z}_p$ и $|A| |B| > p$. Тогда существует $\xi \in \mathbb{Z}_p^*$ такое, что

$$|A + \xi B| > \frac{p}{2}, \quad (6)$$

$$|A - \xi B| > \frac{p}{2}. \quad (7)$$

ДОКАЗАТЕЛЬСТВО. Применим лемму 1 с $G = \mathbb{Z}_p^*$. Она гарантирует нам существование $\xi \in G$ такого, что выполняются (2) и (3). Из условий на A и B получим

$$\frac{|A| |B| |G|}{|A| |B| + |G|} > \frac{|A| |B| |G|}{2|A| |B|} = \frac{p-1}{2}.$$

Тогда

$$|A + \xi B| > \frac{p}{2}, \quad |A - \xi B| > \frac{p}{2}.$$

Лемма 2 доказана.

Для двух подмножеств $A \subset \mathbb{Z}_p$, $B \subset \mathbb{Z}_p$ обозначим

$$I(A; B) := \{(b_1 - b_2) \cdot a_1 + (a_2 - a_3) \cdot b_3 : a_1, a_2, a_3 \in A, b_1, b_2, b_3 \in B\}.$$

Теперь нам понадобится следующее обобщение леммы 2.1 из [8].

ЛЕММА 3. Пусть $A \subset \mathbb{Z}_p$, $B \subset \mathbb{Z}_p$. Если для некоторого $\xi \in \mathbb{Z}_p$

$$|A + \xi B| < |A| |B|,$$

то

$$|I(A; B)| \geq |A + \xi B|.$$

ДОКАЗАТЕЛЬСТВО. Из условия $|A + \xi B| < |A| |B|$ следует, что существуют такие $a_1, a_2 \in A$, $b_1, b_2 \in B$, что $(a_1, b_1) \neq (a_2, b_2)$ и

$$(a_1 - a_2) + (b_1 - b_2) \cdot \xi = 0. \quad (8)$$

Очевидно, что $b_1 \neq b_2$. Рассмотрим множество

$$S := (b_1 - b_2)(A + \xi B) = \{(b_1 - b_2) \cdot s : s \in A + \xi B\}.$$

Ясно, что $|S| = |A + \xi B|$. Каждый элемент $s \in S$ можно записать в виде

$$s = (b_1 - b_2) \cdot a + (b_1 - b_2) \cdot b\xi, \quad a \in A, \quad b \in B.$$

Используя (8), получаем

$$s = (b_1 - b_2) \cdot a + (a_2 - a_1) \cdot b.$$

Поэтому $S \subset I(A; B)$ и лемма 3 доказана.

ТЕОРЕМА 1. Если $A \subset \mathbb{Z}_p$ и $B \subset \mathbb{Z}_p$ такие, что B – антисимметричное множество и $|A| |B| > p$, то $8AB = \mathbb{Z}_p$.

ДОКАЗАТЕЛЬСТВО. По лемме 2 для множеств A и B существует $\xi \in G$ такой, что выполняются (6) и (7). Из (6) получим $(A + \xi B) \cap (-A - \xi B) \neq \emptyset$. Тогда существуют $a_1, a_2 \in A$, $b_1, b_2 \in B$ такие, что $a_1 + b_1\xi = -(a_2 + b_2\xi)$. Таким образом,

$$\xi = -\frac{a_1 + a_2}{b_1 + b_2}.$$

Так как B – антисимметричное множество, то $b_1 + b_2 \neq 0$ для любых $b_1, b_2 \in B$ и элемент ξ определен корректно.

Из (7) получаем

$$\left| \left\{ a_3 + \frac{a_1 + a_2}{b_1 + b_2} b_3 : a_3 \in A, b_3 \in B \right\} \right| > \frac{p}{2}$$

или, что то же самое,

$$|\{a_3(b_1 + b_2) + b_3(a_1 + a_2) : a_3 \in A, b_3 \in B\}| > \frac{p}{2}.$$

Таким образом, $|4AB| > p/2$. По теореме Коши–Давенпорта $8AB = \mathbb{Z}_p$ и теорема 1 доказана.

ТЕОРЕМА 2. Пусть $A \subset \mathbb{Z}_p$ и $B \subset \mathbb{Z}_p$ такие, что B – симметричное множество и $|A||B| > p$. Тогда $8AB = \mathbb{Z}_p$.

ДОКАЗАТЕЛЬСТВО. По лемме 2 для множеств A и B из формулировки теоремы существует такой $\xi \in \mathbb{Z}_p$, что $|A + \xi B| > p/2$. Из условий теоремы мы получаем, что $|A + \xi B| \leq p < |A||B|$. Теперь, используя лемму 3, получим

$$|I(A; B)| \geq |A + \xi B| > \frac{p}{2}.$$

Так как множество B симметричное, то $I(A; B) \subset 4AB$. Отсюда получаем, что $|4AB| > p/2$; тогда по теореме Коши–Давенпорта $8AB = \mathbb{Z}_p$ и теорема 2 доказана.

Отсюда можно вывести очевидное

СЛЕДСТВИЕ 1. Если $A \subset \mathbb{Z}_p$ – произвольное симметричное или антисимметричное подмножество, то $8AA = \mathbb{Z}_p$.

Пусть $A \subset \mathbb{Z}_p$ – произвольное подмножество. Запишем A в виде

$$A = A_s \cup (-A_s) \cup A_a, \quad (9)$$

где

$$A_s \cup (-A_s) = \{a \in A \mid a \in A \implies -a \in A\}, \\ -A_s = \{-a \in A \mid a \in A_s\}, \quad A_a = \{a \in A \mid a \in A \implies -a \notin A\}.$$

Множество A_s можно построить, используя следующий алгоритм: в начале работы алгоритма $A_s = \emptyset$, затем перебираем все пары $(a; -a)$ со свойством $(a \in A \implies -a \in A)$ и добавляем в A_s произвольный элемент пары. Если алгоритм уже прошел пару $(a; -a)$, то он не берет в рассмотрение пару $(-a; a)$. Ясно, что при этом будет построено нужное множество. Из построения подмножеств A_s и A_a ясно, что $A_s \cap A_a = \emptyset$. Очевидно также, что $0 \in A_s$, $0 \notin A_a$ и $A_s \cap (-A_s) = \{0\}$, если $0 \in A$.

Рассмотрим подмножества $A_{\text{sym}} \subset A$ и $A_{\text{as}} \subset A$, которые определим следующим образом:

$$A_{\text{as}} = A_s \cup A_a \setminus \{0\}, \quad A_{\text{sym}} = A_s \cup (-A_s).$$

По определению ясно, что A_{sym} – максимальное симметрическое подмножество A , а A_{as} – максимальное антисимметрическое подмножество A . Из определения также можно получить следующие соотношения:

$$|A_{\text{sym}}| = 2 \cdot |A_s| - 1, \quad 0 \in A, \quad |A_{\text{sym}}| = 2 \cdot |A_s|, \quad 0 \notin A, \\ |A_{\text{as}}| = |A_s| + |A_a| - 1, \quad 0 \in A, \quad |A_{\text{as}}| = |A_s| + |A_a|, \quad 0 \notin A.$$

СЛЕДСТВИЕ 2. Если $A \subset \mathbb{Z}_p^*$ – произвольное подмножество такое, что $|A| > (1/4 + \sqrt{17}/4)\sqrt{p}$, то $8AA = \mathbb{Z}_p$.

ДОКАЗАТЕЛЬСТВО. Представим A в виде (9). Тогда $|A_{\text{sym}}| = 2|A_s|$ и $|A_{\text{as}}| = |A_s| + |A_a|$. По следствию 1 если A такое, что $2|A_s| > \sqrt{p}$ или $|A_s| + |A_a| > \sqrt{p}$, то $8AA = \mathbb{Z}_p$ и следствие доказано. Теперь рассмотрим случай, когда

$$|A_s| < \frac{\sqrt{p}}{2}, \quad (10)$$

$$|A_s| + |A_a| < \sqrt{p}. \quad (11)$$

Из (10) и (11) получим $|A| - \sqrt{p}/2 < 2|A_s| + |A_a| - |A_s| = |A_s| + |A_a| = |A_{\text{as}}|$. По условию $|A| > (1/4 + \sqrt{17}/4)\sqrt{p}$, откуда следует, что

$$\left(|A| - \frac{\sqrt{p}}{2}\right)|A| > p.$$

Применяя теорему 1 для множеств A и A_{as} , получим $8AA_{\text{as}} = \mathbb{Z}_p$. Отсюда следует, что $8AA = \mathbb{Z}_p$ и следствие доказано.

СЛЕДСТВИЕ 3. Пусть $A \subset \mathbb{Z}_p$, $B \subset \mathbb{Z}_p^*$ – произвольные подмножества такие, что $|A| > 1$, $|A||B| > \alpha p$, $\alpha > 0$, $m \in \mathbb{N}$, $m \geq 8([4/\alpha] + 1)$ – произвольное число. Тогда $m(AB) = \mathbb{Z}_p$.

ДОКАЗАТЕЛЬСТВО. Очевидно, выполняется следующая оценка:

$$\frac{1}{2}|B| \leq |B_{\text{as}}| \leq |B|.$$

Тогда

$$|A||B_{\text{as}}| \geq \frac{1}{2}|A||B| > \frac{\alpha p}{2}.$$

Последовательно применяя теорему Коши–Давенпорта, получим

$$|kA| \geq \min(k(|A| - 1) + 1; p).$$

Положим $k = [4/\alpha] + 1$. Если $|kA| = p$, то $kA = \mathbb{Z}_p$ и тогда $8k(AB) = \mathbb{Z}_p$. Если же $|kA| \geq k(|A| - 1) + 1$, то

$$|kA||B_{\text{as}}| \geq k(|A| - 1)|B_{\text{as}}| + |B_{\text{as}}| > k\frac{1}{2}|A||B_{\text{as}}| > \frac{k\alpha p}{4} > p.$$

Видим, что выполнены условия теоремы 1 для множеств kA и B_{as} ; следовательно, $8(kA)B_{\text{as}} = 8(kA)B = \mathbb{Z}_p$. Таким образом, $(8k)AB = \mathbb{Z}_p$, что доказывает следствие.

ПРИМЕР 1. Если $0 < \alpha < 1$, то при условии, что $p > p(\alpha)$, существуют множества $A \subset \mathbb{Z}_p$ и $B \subset \mathbb{Z}_p^*$ такие, что $|A| > 1$, $|A||B| > \alpha p$, но $m(AB) \neq \mathbb{Z}_p$ при $m \leq 2/\alpha - 1$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим множества

$$A = \left\{ a : |a| \leq \left\lfloor \frac{\sqrt{p}}{2} \right\rfloor + 1 \right\}, \quad B = \left\{ b : |b| \leq \left\lfloor \frac{\alpha\sqrt{p}}{2} \right\rfloor + 1 \right\} \setminus \{0\}.$$

Из определения A и B видно, что $|A||B| > \alpha p$. Ясно, что $AB \subset [-M; M]$, где $M = (\lfloor \sqrt{p}/2 \rfloor + 1)(\lfloor \alpha\sqrt{p}/2 \rfloor + 1)$. Легко понять также, что $mAB \subset [-mM; mM]$. Заметим, если взять $m = \lfloor 2/\alpha \rfloor - 1$, то при $p > p(\alpha)$ справедливо неравенство

$$mM = \left(\left\lfloor \frac{2}{\alpha} \right\rfloor - 1 \right) \left(\left\lfloor \frac{\sqrt{p}}{2} \right\rfloor + 1 \right) \left(\left\lfloor \frac{\alpha\sqrt{p}}{2} \right\rfloor + 1 \right) < \frac{p-1}{2}.$$

Поэтому $m(AB) \neq \mathbb{Z}_p$ и пример 1 построен.

СЛЕДСТВИЕ 4. Если H – подгруппа $\mathbb{Z}_p^*$, $|H| > \sqrt{p}$, то $8H = \mathbb{Z}_p$.

ДОКАЗАТЕЛЬСТВО. Пусть $-1 \in H$; тогда H – симметрическое подмножество $\mathbb{Z}_p$. Если же $-1 \notin H$, то H антисимметрична. Тогда по теоремам 1 и 2 для $A = B = H$ получим, что $8HH = 8H = \mathbb{Z}_p$. Следствие доказано.

СЛЕДСТВИЕ 5. Пусть $A = \{g^x : 0 \leq x \leq 2\lfloor \sqrt{p} \rfloor\}$, где $\text{ord}_p g > \sqrt{p}$. Тогда $8A = \mathbb{Z}_p$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим два случая.

Случай 1. Он заключается в том, что $\text{ord}_p g > 2\sqrt{p}$. Рассмотрим подмножество $A^0 \subset A$, $A^0 := \{g^x : 0 \leq x \leq \lfloor \sqrt{p} \rfloor\}$. Докажем, что A^0 антисимметричное. Пусть существуют i, j , $0 \leq i < j \leq \lfloor \sqrt{p} \rfloor$, такие, что $g^i = -g^j$. Тогда $2(i-j) \leq 2\lfloor \sqrt{p} \rfloor$ и $g^{2(i-j)} = 1$; получаем противоречие с предположением, что $\text{ord}_p g > 2\sqrt{p}$. По следствию 1 получаем, что $8A^0A^0 = \mathbb{Z}_p$. Но $A^0A^0 \subseteq A$, т.е. $8A = \mathbb{Z}_p$.

Случай 2. Пусть теперь $\sqrt{p} < \text{ord}_p g \leq 2\sqrt{p}$. Тогда A совпадает с подгруппой, порожденной элементом g , и утверждение вытекает из следствия 4. Следствие доказано.

3. Доказательство теоремы 3. В данном пункте мы будем вместо x^{-1} писать $1/x$.

ЛЕММА 4. Пусть

$$A := \left\{ \frac{1}{x} \pmod{p} : 1 \leq x \leq p^\varepsilon \right\},$$

где $\varepsilon > 0$ – произвольное действительное число. Если $m \in \mathbb{N}$, $m > 8 \cdot ([1/\varepsilon + 1/2] + 1)^2$, и p – достаточно большое простое число, то $mA = \mathbb{Z}_p$.

ДОКАЗАТЕЛЬСТВО. Карацуба в своих работах [4], [6] рассмотрел суммы вида

$$\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_k} \pmod{p} : k+1 \leq x_i \leq \left(\frac{p-1}{k} \right)^{1/(2k-1)}, \quad i = 1, \dots, k,$$

где все x_i – простые целые, а p – простой модуль. Рассмотрим множество

$$B_k := \left\{ \frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_k} \pmod{p} : k+1 \leq x_i \leq \left(\frac{p-1}{2k} \right)^{1/(2k-1)}, \quad i = 1, \dots, k \right\},$$

где все x_i простые. Используя технику работ [4], [6] докажем, что все суммы из B_k попарно различны, и B_k – антисимметричное множество для любого k .

Если в B_k есть одинаковые суммы, то найдутся такие $x_1, x_2, \dots, x_k, y_1, y_2, \dots, y_k$, что все x_i, y_i простые и

$$\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_k} - \frac{1}{y_1} - \frac{1}{y_2} - \dots - \frac{1}{y_k} \equiv 0 \pmod{p}.$$

Умножив обе части выражения на общий знаменатель этих дробей, получим

$$\begin{aligned} s(x_1, x_2, \dots, x_k, y_1, y_2, \dots, y_k) \\ := x_2 \cdots x_k \cdot y_1 \cdots y_k + \dots + x_1 \cdots x_{k-1} \cdot y_1 \cdots y_k \\ - x_1 \cdots x_k \cdot y_2 \cdots y_k - \dots - x_1 \cdots x_k \cdot y_1 \cdots y_{k-1} \equiv 0 \pmod{p}. \end{aligned}$$

Поскольку $k+1 \leq x_i \leq ((p-1)/2k)^{1/(2k-1)}$, $i = 1, \dots, k$, то

$$\begin{aligned} |s(x_1, \dots, x_k, y_1, \dots, y_k)| &\leq |x_2 \cdots x_k \cdot y_1 \cdots y_k| + \dots + |x_1 \cdots x_{k-1} \cdot y_1 \cdots y_k| \\ &\leq \underbrace{\frac{p-1}{2k} + \dots + \frac{p-1}{2k}}_k = \frac{p-1}{2}. \end{aligned}$$

Таким образом, сравнение дробей по модулю p влечет равенство в поле действительных чисел. Так как все x_i и y_i простые и $x_i \geq k+1$, $y_i \geq k+1$, то при группировке одинаковых слагаемых мы получим сумму дробей, меньших единицы. Поэтому равенство может быть тогда и только тогда, когда наборы $(x_1, x_2, \dots, x_k)$ и $(y_1, y_2, \dots, y_k)$ совпадают с точностью до перестановки.

Если B_k не антисимметричное, то найдутся такие $x'_1, x'_2, \dots, x'_k, y'_1, y'_2, \dots, y'_k$, что все x'_i, y'_i простые и

$$\frac{1}{x'_1} + \frac{1}{x'_2} + \dots + \frac{1}{x'_k} \equiv -\frac{1}{y'_1} - \frac{1}{y'_2} - \dots - \frac{1}{y'_k} \pmod{p}.$$

Рассуждая аналогично и учитывая, что $k+1 \leq x'_i \leq ((p-1)/2k)^{1/(2k-1)}$, $k+1 \leq y'_i \leq ((p-1)/2k)^{1/(2k-1)}$, $i = 1, \dots, k$, и все x'_i и y'_i простые, можно установить, что сравнение по модулю p можно заменить на следующее равенство в поле действительных чисел:

$$\frac{1}{x'_1} + \frac{1}{x'_2} + \dots + \frac{1}{x'_k} = -\frac{1}{y'_1} - \frac{1}{y'_2} - \dots - \frac{1}{y'_k}.$$

Но последнее равенство при указанных ограничениях невозможно.

Найдем такое k , что $B_k \subset kA_{\varepsilon'}$, где $\varepsilon' = \varepsilon/2$. Выберем

$$k = \left\lceil \frac{1}{2} + \frac{1}{2\varepsilon'} \right\rceil + 1. \quad (12)$$

Тогда легко понять, что

$$\left(\frac{p-1}{2k} \right)^{1/(2k-1)} < p^{\varepsilon'}.$$

Заметим, что множество B_k по доказанному содержит по крайней мере

$$\frac{1}{k!} \left(\pi \left(\left(\frac{p-1}{2k} \right)^{1/(2k-1)} \right) - \pi(k+1) \right)^k$$

элементов. Используя неравенство Чебышева $\pi(x) \geq Cx/\ln x$, оценим $|B_k|$:

$$\begin{aligned} |B_k| &\geq \frac{1}{k!} \left(\pi \left(\left(\frac{p-1}{2k} \right)^{1/(2k-1)} \right) - \pi(k+1) \right)^k \\ &\geq \frac{1}{k!} \left(C_1 \frac{p^{1/(2k-1)}}{\ln p} - \pi(k+1) \right)^k \\ &\geq \frac{1}{k!} \left(\frac{C_1}{2} \cdot \frac{p^{1/(2k-1)}}{\ln p} \right)^k = \frac{(C_1)^k}{2^k k!} \cdot \frac{p^{k/(2k-1)}}{(\ln p)^k}. \end{aligned}$$

Последнее неравенство верно лишь для достаточно большого p . Из (12) получим

$$\frac{(C_1)^k}{2^k k!} \cdot \frac{p^{k/(2k-1)}}{(\ln p)^k} \geq C(\varepsilon) \cdot \frac{p^{1/2+\varepsilon'/2}}{(\ln p)^k},$$

где $C(\varepsilon)$ – некоторая положительная константа, зависящая лишь от ε . То есть

$$|B_k| \geq C(\varepsilon) \cdot \frac{p^{1/2+\varepsilon'/2}}{(\ln p)^k}$$

для достаточно большого p . Если

$$C(\varepsilon) \cdot \frac{p^{1/2+\varepsilon'/2}}{(\ln p)^k} > \sqrt{p}, \quad (13)$$

то $|B_k| > \sqrt{p}$. Но (13) выполнено при достаточно большом p . Таким образом, для выбранного k и достаточно большого p $B_k \subset kA$, $|B_k| > \sqrt{p}$ и B_k антисимметричное.

Используем теорему 1 для $A = B = B_k$, получим

$$8B_k \cdot B_k = \mathbb{Z}_p.$$

Так как $B_k \cdot B_k \subset k^2 A$, то $8k^2 A = \mathbb{Z}_p$ и лемма 4 доказана.

ЗАМЕЧАНИЕ. Поскольку в работе [6] были рассмотрены сравнения по произвольному модулю (простому или составному), то часть доказательства леммы 4, относящаяся к построению и исследованию свойств множества B_k , можно с небольшими изменениями обобщить на случай не обязательно простого модуля. Для переноса леммы 4 на составной модуль требуется обобщение теоремы 1. Однако очевидно, что в приведенной выше формулировке теорема для составного модуля не верна и требуются дальнейшие исследования для доказательства аналога теоремы 1, верной для произвольного модуля.

ТЕОРЕМА 3. Для любого $\varepsilon > 0$, для любого достаточно большого простого p и для любого класса вычетов $a \pmod{p}$ существуют положительные попарно различные целые $x_1, \dots, x_N \leq p^\varepsilon$, где $N = 8 \cdot ([1/\varepsilon + 1/2] + 1)^2$, такие, что

$$a \equiv \frac{1}{x_1} + \dots + \frac{1}{x_N} \pmod{p}.$$

ДОКАЗАТЕЛЬСТВО. По лемме 4 для любого достаточно большого p и для любого класса вычетов $a \pmod{p}$ существуют положительные целые $x'_1, \dots, x'_N \leq p^\varepsilon$, где $N = 8 \cdot ([1/\varepsilon + 1/2] + 1)^2$, такие, что

$$a \equiv \frac{1}{x'_1} + \dots + \frac{1}{x'_N} \pmod{p}. \quad (14)$$

Нужно получить аналогичное представление, где все $x'_i, i = 1, \dots, N$, различны. Его мы построим с помощью (14). Заметим, что при построении суммы (14) в доказательстве леммы 4 мы, на самом деле, имеем другое ограничение на x'_i :

$$x'_i < \left(\frac{p-1}{2K} \right)^{2/(2K-1)},$$

где $K = [1/\varepsilon + 1/2] + 1$. Тогда при достаточно больших p получим, что существует такое $0 < \varepsilon_1 < \varepsilon$, что $x'_i < p^{\varepsilon_1}$.

Обозначим

$$M = \prod_{\substack{i=1 \\ i \neq N}}^{2N-1} (2N-i).$$

Тогда для достаточно большого p выполняется неравенство

$$NM < p^{\varepsilon - \varepsilon_1}.$$

Рассмотрим вычет $a' \equiv a \cdot M \pmod{p}$. Найдутся такие $x'_i < p^{\varepsilon_1}, i = 1, \dots, N$, что выполняется (14). Отсюда следует, что

$$a \equiv \frac{1}{Mx'_1} + \dots + \frac{1}{Mx'_N} \pmod{p}. \quad (15)$$

Пусть в записи (15) есть два одинаковых слагаемых. Тогда без ограничения общности можно записать

$$a \equiv \frac{2}{Mx'_1} + \frac{1}{Mx'_3} + \dots + \frac{1}{Mx'_N} \pmod{p}.$$

Заметим, что

$$\frac{2}{Mx'_1} = \frac{1}{(N/j)Mx'_1} + \frac{1}{(N/(2N-j))Mx'_1}, \quad j = 1, \dots, N-1.$$

По определению M все $(N/j)Mx'_1$ и $(N/(2N-j))Mx'_1$ для любого $j = 1, \dots, N-1$ — различные целые числа. Так как слагаемых в сумме (15) со знаменателем $Mx'_i, i = 3, \dots, N$, всего $N-2$, можно найти такое j , что $(N/j)Mx'_1$ и $(N/(2N-j))Mx'_1$ отличаются от всех чисел $Mx'_i, i = 3, \dots, N$. Повторяя эту процедуру, получим представление a в виде

$$a \equiv \frac{1}{x_1} + \dots + \frac{1}{x_N} \pmod{p},$$

где все $x_i, i = 1, \dots, N$, различны и меньше $p^\varepsilon, i = 1, \dots, N$. Теорема 3 доказана.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Erdős P., Graham R. L. Old and New Problems and Results In Combinational Number Theory. Monograph. Enseign. Math. V. 28, 1980.
- [2] Croot E. S. On some questions of Erdős and Graham about Egyptian fractions // *Mathematika*. 1999. V. 46. P. 359–372.
- [3] Sparlinski I. E. On a question of Erdős and Graham // *Arch. Math.* 2002. V. 78. P. 445–448.
- [4] Карацуба А. А. Распределение обратных величин в кольце вычетов по заданному модулю // *Докл. РАН*. 1993. Т. 333. №2. С. 138–139.
- [5] Карацуба А. А. Дробные доли специального вида функций // *Изв. РАН. Серия матем.* 1995. Т. 59. №4. С. 61–80.
- [6] Карацуба А. А. Аналоги неполных сумм Клоостермана и их приложения // *Tatra Mountain Math. Publ.* 1997. V. 11. P. 89–120.
- [7] Croot E. S. Reciprocal power sums modulo a prime // E-print `math.NT/0403360`, 2004.
- [8] Bourgain J., Katz N., Tao T. A sum-product estimate in finite fields and their applications // E-print `math.CO/0301343`, 2003.
- [9] Шкредов И. Д. О некоторых аддитивных задачах, связанных с показательной функцией // *УМН*. 2003. Т. 58. №4. С. 165–166.
- [10] Карацуба А. А. Аддитивные сравнения // *Изв. РАН. Серия матем.* 1997. Т. 61. №2. С. 81–94.
- [11] Карацуба А. А. О правильных множествах в остаточных классах // *Матем. заметки*. 1998. Т. 64. №2. С. 224–228.

Московский государственный университет им. М. В. Ломоносова
E-mail: `aanatol@mail.ru`

Поступило
03.05.2005
Исправленный вариант
26.09.2005