УДК 511.3

Комбинаторные свойства множеств вычетов по простому модулю и задача Эрдеша-Грэхэма.[1]

А.А. Глибичук

Аннотация

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

$$a \equiv x_1^{-1} + \ldots + x_N^{-1} (mod p),$$

где x_i^{-1} - наименьшее положительное целое такое, что $x_i^{-1} x_i \equiv \equiv 1 (mod p)$. Это улучшает результат [1].

Библиография: 9 наименований.

1. Введение. Эрдеш и Грэхэм [2] поставили такую задачу.

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 $1 \leq x_i \leq p^{\varepsilon}, i = 1, 2, \ldots, k$, и

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

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

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

Следующим результатом в этом направлении была работа И.Е. Шпарлинского [1]. Он использует оценки тригонометрических сумм А.А. Карацубы (см. [4], [5], [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 $x_i, i = 1, \ldots, k$ таких, что $1 \leq x_i \leq p^{\varepsilon}$ и выполняется (1).

[1]Эта работа поддержана грантом РФФИ 05-01-00066 и грантом поддержки научной школы РФ N НШ-304.2003.1.

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 $a(modp)$ существует положительные целые $x_1, \ldots, x_N \leq p^{\varepsilon}$, удовлетворяющие сравнению:

$$a \equiv \left(x_1^k\right)^{-1} + \cdots + \left(x_N^k\right)^{-1} (modp).$$

Мы докажем следующий результат, усиливающий [1].

Теорема 3. *Для любого $\varepsilon > 0$, для любого достаточно большого простого p и для любого класса вычетов $a(modp)$ существует положительные попарно различные целые $x_1, \ldots, x_N \leq p^{\varepsilon}$, где $N = 8 \cdot \left(\left[\frac{1}{\varepsilon} + \frac{1}{2}\right] + 1\right)^2$, такие, что*

$$a \equiv x_1^{-1} + \cdots + x_N^{-1} (modp).$$

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 $* : X \times X \to X$. 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 $k \in \mathbb{N}$

$$kA = \underbrace{A + A \ldots + A}_{k}.$$

Возьмем в качестве кольца поле вычетов по модулю некоторого простого числа p. Обзначим 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 $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\}$.

Определение 2. Назовем число k *мультипликативным порядком* элемента $g \in \mathbb{Z}_p^*$, если $k = \min\{i : g^i = 1(mod p)\}$. Будем обозначать $k = ord_p g$.

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 $|A||B| > p$, то $8AB = \mathbb{Z}_p$.*

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 $A = \{g^x : 0 \le x \le 2[\sqrt{p}]\}$, где $ord_p g > 2\sqrt{p}$, 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 $N \le \frac{c}{\varepsilon}$, где c - константа, то была бы доказана гипотеза А.А. Карацубы, сформулированная в [10] на стр. 83 (смотри также [11], стр. 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 $G \ne \emptyset$. Тогда найдется $\xi \in G$ такой, что*

$$|A + \xi B| \ge \frac{|A||B||G|}{|A||B| + |G|} \tag{2}$$

и

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

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

$$\sum_{s\in\mathbb{Z}_p}(f_\xi^+(s))^2 = |\{(a_1,b_1,a_2,b_2) : a_1,a_2 \in A, b_1,b_2 \in B, a_1+b_1\xi = a_2+b_2\xi\}|$$

$$= |A||B|+|\{(a_1,b_1,a_2,b_2) : a_1,a_2 \in A, b_1,b_2 \in B, a_1 \neq a_2, a_1+b_1\xi = a_2+b_2\xi\}|,$$

$$\sum_{s\in\mathbb{Z}_p}(f_\xi^-(s))^2 = |\{(a_1,b_1,a_2,b_2) : a_1,a_2 \in A, b_1,b_2 \in B, a_1-b_1\xi = a_2-b_2\xi\}|$$

$$= |A||B|+|\{(a_1,b_1,a_2,b_2) : a_1,a_2 \in A, b_1,b_2 \in B, a_1 \neq a_2, a_1-b_1\xi = a_2-b_2\xi\}|.$$

Таким образом,

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

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:

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

Из неравенства Коши-Буняковского получим:

$$\left(\sum_{s\in\mathbb{Z}_p} f_\xi^+(s)\right)^2 \le |A+\xi B|\sum_{s\in\mathbb{Z}_p}(f_\xi^+(s))^2$$

и

$$\left(\sum_{s\in\mathbb{Z}_p} f_\xi^-(s)\right)^2 \le |A-\xi B|\sum_{s\in\mathbb{Z}_p}(f_\xi^-(s))^2.$$

Кроме того,

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

и

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

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

$$|A+\xi B| \ge \frac{|A|^2|B|^2}{|A||B|+\frac{|A|^2|B|^2}{|G|}} = \frac{|A||B||G|}{|A||B|+|G|}$$

и

$$|A-\xi B| \ge \frac{|A||B||G|}{|A||B|+|G|}.$$

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*

$$|A+\xi B| > \frac{p}{2} \tag{6}$$

и

$$|A-\xi B| > \frac{p}{2}. \tag{7}$$

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:

$$|A + \xi B| > \frac{p}{2}$$

и

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

Лемма 2 доказана. $\square$

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

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

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:

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

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. $\square$

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: $(A+\xi B)\bigcap(-A-\xi B) \neq \emptyset$. 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) получим:

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

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

Таким образом, $|4AB| > \frac{p}{2}$. 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 $|A + \xi B| > \frac{p}{2}$. 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 $|4AB| > \frac{p}{2}$, 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

$$A = A_s \cup (-A_s) \cup A_a, \tag{9}$$

где

$$A_s \cup (-A_s) = \{a \in A | a \in A \Rightarrow -a \in A, a \neq 0\},$$
$$-A_s = \{-a \in A | a \in A_s\},$$
$$A_a = \{a \in A | a \in A \Rightarrow -a \notin A\}.$$

Множество A_s можно построить, используя следующий алгоритм: в начале работы алгоритма $A_s = \emptyset$, затем перебираем все пары $(a; -a)$ со свойством $(a \in A \Rightarrow -a \in A)$ 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. По построению подмножества 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 $A_{sym} \subset A$ и $A_{as} \subset A$, которые определим следующим образом:

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

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

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

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

Доказательство. Представим A в виде (9). Тогда $|A_{sym}| = 2|A_s|$ и $|A_{as}| = |A_s| + |A_a|$. 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

$$|A_s| < \frac{\sqrt{p}}{2} \tag{10}$$

$$|A_s| + |A_a| < \sqrt{p}. \tag{11}$$

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

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

Применяя теорему 1 для множеств A и A_{as}, получим $8AA_{as} = \mathbb{Z}_p$. 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 $|A| > 1, |A||B| > \alpha p, \alpha > 0, m \in \mathbb{N}, m \geq 8(\left[\frac{4}{\alpha}\right] + 1)$ - произвольное число. Тогда $m(AB) = \mathbb{Z}_p$.*

Доказательство. Очевидно, выполняется следующая оценка:

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

Тогда:

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

Последовательно применяя теорему Коши-Давенпорта получим:

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

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

$$|kA||B_{as}| \geq k(|A| - 1)|B_{as}| + |B_{as}| >$$

$$> k\frac{1}{2}|A||B_{as}| > \frac{k\alpha p}{4} > p.$$

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

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* $m \leq \frac{2}{\alpha} - 1$.

Доказательство. Рассмотрим множества

$$A = \left\{ a : |a| \leq \left[\frac{\sqrt{p}}{2} \right] + 1 \right\},$$

$$B = \left\{ b : |b| \leq \left[\frac{\alpha\sqrt{p}}{2} \right] + 1 \right\} \setminus \{0\}.$$

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

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

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

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. $\square$

Следствие 5. *Пусть* $A = \{g^x : 0 \leq x \leq 2[\sqrt{p}]\}$, *где* $ord_p g > \sqrt{p}$. *Тогда* $8A = \mathbb{Z}_p$.

Доказательство.Рассмотим два случая.

Случай 1. Он заключается в том, что $ord_p g > 2\sqrt{p}$. Рассмотрим подмножество $A^0 \subset A, A^0 := \{g^x : 0 \leq x \leq [\sqrt{p}]\}$. Докажем, что A^0 –

антисимметричное. Пусть существует такие i, j, что $0 \le i < j \le [\sqrt{p}]$ такие, что $g^i = -g^j$. Тогда $2(i-j) \le 2[\sqrt{p}]$ и $g^{2(i-j)} = 1$ - получаем противоречие с предположением, что $ord_p g > 2\sqrt{p}$. По следствию 1 получаем, что $8A^0A^0 = \mathbb{Z}_p$. Но $A^0A^0 \subseteq A$, то есть $8A = \mathbb{Z}_p$.

Случай 2. Пусть теперь $\sqrt{p} < ord_p g \le 2\sqrt{p}$. 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 $\frac{1}{x}$.

Лемма 4. *Пусть*

$$A := \left\{ \frac{1}{x} (mod p) : 1 \le x \le p^{\varepsilon} \right\},$$

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

Доказательство. А.А. Карацуба в своей работах [4], [6] рассмотрел суммы вида

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} (mod p) : k+1 \le x_i \le \left(\frac{p-1}{k} \right)^{\frac{1}{2k-1}}, i = 1, \ldots, k,$$

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

$$B_k := \{ \frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} (mod p) : k+1 \le x_i \le \left(\frac{p-1}{2k} \right)^{\frac{1}{2k-1}}, i = 1, \ldots, k \},$$

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 $x_1, x_2, \ldots, x_k$, $y_1, y_2, \ldots, y_k$, что все x_i, y_i-простые и

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} - \frac{1}{y_1} - \frac{1}{y_2} - \cdots - \frac{1}{y_k} \equiv 0 (mod p).$$

Умножив обе части выражения на общий знаменатель этих дробей мы получим

$$s(x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_k) :=$$

$$= x_2 \cdot \ldots \cdot x_k \cdot y_1 \cdot \ldots \cdot y_k + \ldots + x_1 \cdot \ldots \cdot x_{k-1} \cdot y_1 \cdot \ldots \cdot y_k -$$

$$-x_1 \cdot \ldots \cdot x_k \cdot y_2 \cdot \ldots \cdot y_k - \ldots - x_1 \cdot \ldots \cdot x_k \cdot y_1 \cdot \ldots \cdot y_{k-1} = 0(mod p).$$

Поскольку $k+1 \leq x_i \leq \left(\frac{p-1}{2k}\right)^{\frac{1}{2k-1}}, i = 1, \ldots, k$, то

$$|s(x_1, \ldots, x_k, y_1, \ldots, y_k)| \leq |x_2 \cdot \ldots \cdot x_k \cdot y_1 \cdot \ldots \cdot y_k| + \ldots + |x_1 \cdot \ldots \cdot x_{k-1} \cdot y_1 \cdot \ldots \cdot y_k| \leq$$

$$\leq \underbrace{\frac{p-1}{k} + \ldots + \frac{p-1}{k}}_{k} = p - 1.$$

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 $(x_1, x_2, \ldots, x_k)$ и $(y_1, y_2, \ldots, y_k)$ совпадают с точностью до перестановки.

Если B_k не антисимметричное, то найдутся такие $x_1', x_2', \ldots, x_k'$, $y_1', y_2', \ldots, y_k'$, что все x_i', y_i' — простые и

$$\frac{1}{x_1'} + \frac{1}{x_2'} + \cdots + \frac{1}{x_k'} \equiv -\frac{1}{y_1'} - \frac{1}{y_2'} - \cdots - \frac{1}{y_k'}(mod p).$$

Рассуждая аналогично и учитывая, что $k+1 \leq x_i' \leq \left(\frac{p-1}{2k}\right)^{\frac{1}{2k-1}}, k+1 \leq y_i' \leq \left(\frac{p-1}{2k}\right)^{\frac{1}{2k-1}}, i = 1, \ldots, k$ и все x_i' и y_i' — простые можно установить, что сравнение по модулю p можно заменить на равенство

$$\frac{1}{x_1'} + \frac{1}{x_2'} + \cdots + \frac{1}{x_k'} = -\frac{1}{y_1'} - \frac{1}{y_2'} - \cdots - \frac{1}{y_k'}.$$

Но последнее равенство при указаных ограничениях невозможно.

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

$$k = [\frac{1}{2} + \frac{1}{2\varepsilon'}] + 1. \tag{12}$$

Тогда лего понять, что

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

Заметим, что множество B_k по доказаному содержит по крайней мере

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

элементов. Оценим $|B_k|$(используя неравенство Чебышева $\pi(x) \geq C\frac{x}{\ln x}$):

$$|B_k| \geq \frac{\left(\pi\left(\left(\frac{p-1}{2k}\right)^{\frac{1}{2k-1}}\right) - \pi(k+1)\right)^k}{k!} \geq \frac{\left(C_1 \frac{p^{\frac{1}{2k-1}}}{\ln p} - \pi(k+1)\right)^k}{k!}.$$

Далее:

$$\frac{\left(C_1 \frac{p^{\frac{1}{2k-1}}}{\ln p} - \pi(k+1)\right)^k}{k!} \geq \frac{\left(\frac{C_1}{2} \cdot \frac{p^{\frac{1}{2k-1}}}{\ln p}\right)^k}{k!} = \frac{(C_1)^k}{2^k k!} \cdot \frac{p^{\frac{k}{2k-1}}}{(\ln p)^k}.$$

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

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

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

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

для достаточно большого p. Если

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

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

Замечание. Поскольку в работе [6] были рассмотрены сравнения по произвольному модулю (простому или составному), то часть доказательства леммы 4, относящуюся 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 $a(modp)$ существует положительные попарно различные целые $x_1, \ldots, x_N \leq p^{\varepsilon}$, где $N = 8 \cdot \left(\left[\frac{1}{\varepsilon} + \frac{1}{2}\right] + 1\right)^2$ такие, что*

$$a \equiv \frac{1}{x_1} + \cdots + \frac{1}{x_N}(modp).$$

Доказательство. По лемме 4 для любого достаточно большого p и для любого класса вычетов $a(modp)$ существует положительные целые $x_1^{'}, \ldots, x_N^{'} \leq p^{\varepsilon}$, где $N = 8 \cdot \left(\left[\frac{1}{\varepsilon} + \frac{1}{2}\right] + 1\right)^2$, такие, что

$$a \equiv \frac{1}{x_1^{'}} + \cdots + \frac{1}{x_N^{'}}(modp). \tag{14}$$

Нужно получить аналогичное представление,где все $x_i^{'}, i = 1, \ldots, N$— 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 $x_i^{'}$:

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

где $K = \left[\frac{1}{\varepsilon} + \frac{1}{2}\right] + 1$. Тогда при достаточно больших p мы получим, что существует такое $0 < \varepsilon_1 < \varepsilon$, что

$$x_i^{'} < p^{\varepsilon_1}$$

Обозначим

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

Тогда для достаточно большого p выполняется неравенство:

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

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

$$a \equiv \frac{1}{Mx_1^{'}} + \cdots + \frac{1}{Mx_N^{'}}(modp). \tag{15}$$

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

$$a \equiv \frac{2}{Mx_1^{'}} + \frac{1}{Mx_3^{'}} + \cdots + \frac{1}{Mx_N^{'}}(modp).$$

Заметим, что $\frac{2}{Mx_1^{'}} = \frac{1}{\frac{N}{j}Mx_1^{'}} + \frac{1}{\frac{N}{2N-j}Mx_1^{'}}, j = 1, \ldots, N-1$. По определению M все $\frac{N}{j}Mx_1^{'}$ и $\frac{N}{2N-j}Mx_1^{'}$ для любого $j = 1, \ldots, N-1$—различные целые числа. Так как слагаемых в сумме (15) со знаменателем $Mx_i, i = 3, \ldots, N$ всего $N-2$, то можно найти такое j, что $\frac{N}{j}Mx_1^{'}$ и $\frac{N}{2N-j}Mx_1^{'}$ отличаются от всех чисел $Mx_i^{'}, i = 3, \ldots, N$. Повторяя эту процедуру получим представлние a в виде:

$$a \equiv \frac{1}{x_1} + \cdots + \frac{1}{x_N}(modp),$$

где все $x_i, i = 1, \ldots, N$–различны и все x_i меньше $p^{\varepsilon}, i = 1, \ldots, N$. Теорема 3 доказана. □

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ.

[1] Sparlinski I.E. On a question of Erdős and Graham // Arch. Math. V. 78. Basel. 2002. P. 445-448.

[2] Erdős P., Graham R.L. Old and new problems and results in combinational number theory // Monograph. Enseign. Math.1980.V.28.

[3] Croot E.S. On some questions of Erdős and Graham about Egyptian fractions // Mathematika. 1999. V. 46. P. 359-372.

[4] Карацуба А.А. Распределение обратных величин в кольце вычетов по заданному модулю // Докл. РАН. 1993. Т. 333. N 2. стр. 138-139.

[5] Карацуба А.А. Дробные доли специального вида функций // Изв. РАН. Серия математическая. 1995. Т. 59. N 4. стр. 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 Modulio a Prime // arXiv:math. NT/0403360.2004. V. 1. 22.03.2004.

[8] Bourgain J., Katz N., Tao T. A sum-product estimate in finite fields and their applications // ArXiv:math.CO/0301343.2003. V. 1. 29.01.2003.

[9] Шкредов И.Д. О некоторых аддитивных задачах, связанных с показательной функцией // Успехи мат. наук. 2003. Т. 58. Вып. 4. стр. 165 - 166.

[10] Карацуба А.А. Аддитивные сравнения // Изв. РАН. Серия математическая. 1997. Т. 61. N 2. стр. 81-94.

[11] Карацуба А.А. О правильных множествах в остаточных классах // Математические заметки. 1998. Т. 64. В. 2. стр. 224-228.