Math-Net.Ru

Общероссийский математический портал

А. А. Глибичук, Суммы степеней подмножеств произвольного конечного поля, *Изв. РАН. Сер. матем.*, 2011, том 75, выпуск 2, 35–68

DOI: <https://doi.org/10.4213/im4067>

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: 54.162.27.143

26 апреля 2023 г., 15:28:41

УДК 511.235.1

А. А. Глибичук

Суммы степеней подмножеств произвольного конечного поля

Обсуждается следующая задача: даны натуральное число $n \geq 2$, действительное число $\varepsilon \in (0, 1)$ и произвольное подмножество $A \subseteq \mathbb{F}_q$, не лежащее ни в каком нетривиальном мультипликативном сдвиге никакого собственного подполя $\mathbb{F}_q$ и удовлетворяющее условию $|A| > q^{\frac{1}{n-\varepsilon}}$, где $\mathbb{F}_q$ – конечное поле из $q = p^r$ элементов; для каких натуральных N и m выполнено множественное равенство $NA^m = \mathbb{F}_q$? В частности, показано, что последнее равенство справедливо при $m = 2n - 2$ и $N = N(n, r, \varepsilon)$.

Библиография: 42 наименования.

Ключевые слова: суммы-произведения множеств, конечное поле.

§ 1. Введение

Рассмотрим некоторое непустое множество X с определенной на нем бинарной операцией $*$: $X \times X \rightarrow X$. Тогда можно определить операцию $*$ на парах подмножеств $A, B \subseteq X$ следующей формулой: $A * B = \{a * b : a \in A, b \in B\}$. В частности, если A и B – подмножества кольца, то можно рассмотреть две операции на подмножествах: сложение $A + B := \{a + b : a \in A, b \in B\}$ и умножение $AB = A \cdot B := \{ab : a \in A, b \in B\}$. Определим для некоторого $k \in \mathbb{N}$ и множества A его кратную сумму $kA = \underbrace{A + A + \dots + A}_k$, k -ю степень

$A^k = \underbrace{A \cdot A \cdot \dots \cdot A}_k$ этого множества и операцию умножения $b * A = \{b\} \cdot A$ произвольного элемента кольца b на множество A . Иногда, если это не приводит к путанице в обозначениях, знак $*$ записывать не будем.

Далее через $|A|$ будем обозначать мощность множества A . В качестве кольца будем рассматривать конечное поле $\mathbb{F}_q$ из $q = p^r$ элементов для произвольного простого p . Все множества будут предполагаться подмножествами поля $\mathbb{F}_q$. Для некоторого множества $Y \subseteq \mathbb{F}_q$ определим множество его обратимых элементов $Y^* := Y \setminus \{0\}$. Далее всегда будет предполагаться, что p – некоторое простое число и что $\mathbb{F}_p \subset \mathbb{F}_q$, поскольку произвольное конечное поле характеристики p содержит подполе, изоморфное $\mathbb{F}_p$. Рассматривая произвольный элемент $x \in \mathbb{F}_q^*$, мы можем определить его мультипликативный порядок $\text{ord}_q x$ как наименьшее натуральное l такое, что $x^l = 1$. Для любого действительного y через $[y]$ обозначается его целая часть, т.е. наибольшее целое число, не превосходящее y , а дробная часть y обозначается через $\{y\}$.

Определим также операцию сложения $h + A = \{h\} + A$ произвольного элемента $h \in \mathbb{F}_q$ с множеством A . Операция умножения множеств всегда имеет

Работа выполнена при финансовой поддержке РФФИ (грант № 08-01-00208-а) и Программы Президента РФ “Поддержка ведущих научных школ”(грант НШ-3233.2008.1).

Г.Б. Манна [23]. Аналогичный результат для порядка базиса подмножества в $\mathbb{F}_p$ выводится из теоремы Коши–Дэвенпорта (см. теорему 10).

Известно, что в поле $\mathbb{F}_p$ для фиксированных $k \in \mathbb{N}$ и $\varepsilon > 0$ случайно сгенерированное множество мощности больше $p^{\frac{1}{k} + \varepsilon}$ является базисом порядка k с большой вероятностью (стремящейся к 1 при $p \rightarrow \infty$). В работе [24] построены конструктивные примеры базисов мощности, близкой к оптимальной, в кольце вычетов по модулю степени простого числа.

ОПРЕДЕЛЕНИЕ 2. Подмножество $X \subset \mathbb{F}_q$ называется *особым*, если существуют элемент $d \in \mathbb{F}_q$ и нетривиальное подполе $S \subset \mathbb{F}_q$ такие, что $X \subset dS$. В частности, любое подмножество Y , $|Y| = 1$, является особым.

ОПРЕДЕЛЕНИЕ 3. *Размерностью* подмножества $X \subset \mathbb{F}_q$ называется размерность его линейной оболочки $\text{Span}(X)$ над полем $\mathbb{F}_p$. Мы будем обозначать размерность подмножества X через $\dim(X)$.

В настоящей работе будет изучаться следующая

ЗАДАЧА 1. Для любого натурального $n \geq 2$, действительного числа $0 < \varepsilon < 1$ и неособого подмножества $A \subset \mathbb{F}_q$, $q = p^r$, удовлетворяющего условию $|A| > q^{\frac{1}{n-\varepsilon}}$, найти такое натуральное число m , что для некоторого натурального $N = N(n, r, \varepsilon)$ выполнено равенство $NA^m = \mathbb{F}_q$.

Если подмножество $A \subseteq \mathbb{F}_q$ особо, то для любых натуральных N и m верно неравенство $|NA^m| \leq |S| < q$, а это означает, что для особого подмножества A не существует натуральное число m , удовлетворяющее условиям задачи 1. В настоящей статье доказано существование m и получена оценка сверху этого числа для неособых подмножеств. Согласно теореме 8 число m можно оценить снизу следующим образом: $m \geq n$.

Согласно лемме 9 равенство $NA^m = \mathbb{F}_q$ верно для любого неособого множества, если положить $N = q - 1$ и $m = r$. Нас интересуют значения N и m , не зависящие от p .

Первые оценки мощности кратных сумм и степеней в конечных полях были получены в известной работе [25]. Идеи из этой статьи используются в настоящей работе.

Напомним следующий результат, полученный автором настоящей статьи и М. Рудневым [26], [27].

ЛЕММА 1. Если $A, B \subset \mathbb{F}_q$ – произвольные подмножества такие, что $|A||B| > q$, то $10AB = \mathbb{F}_q$.

Из леммы 1 следует равенство $m = 2$ в задаче 1, если предположить, что $n = 2$.

ОПРЕДЕЛЕНИЕ 4. Произвольное непустое подмножество $X \subset \mathbb{F}_q$ назовем *симметричным*, если выполнено равенство $X = -X$, и *антисимметричным*, если имеет место соотношение $X \cap (-X) = \emptyset$.

Для симметричных и антисимметричных подмножеств верно следующее утверждение, более сильное, чем лемма 1.

ЛЕММА 2 [27]. Рассмотрим пару подмножеств $X, Y \subset \mathbb{F}_q$ таких, что одно из этих подмножеств либо симметрично, либо антисимметрично и выполнено неравенство $|X||Y| > q$. Тогда $8XY = \mathbb{F}_q$.

Леммы 1, 2 будут использованы при доказательстве многих результатов настоящей работы.

ТЕОРЕМА 1 [28, теорема 1.2]. *Для любого целого $n > 1$ и действительных $\delta > 0$, $\varepsilon > 0$ таких, что $\delta \geq 1/(n - \varepsilon)$ и $0 < \varepsilon < n$, существует целое*

$$N \leq 15 \cdot 4^n \ln \left(2 + \frac{1}{\varepsilon} \right)$$

такое, что для произвольного подмножества $A \subseteq \mathbb{F}_p$, удовлетворяющего условию $|A| > p^\delta$, имеет место соотношение

$$NA^n = \mathbb{F}_p.$$

Аналогичный результат для поля $\mathbb{F}_{p^2}$ был доказан автором в [29, теорема 4.1].

ТЕОРЕМА 2. *Существует константа C такая, что для любого целого числа $n \geq 2$, для любых чисел $\varepsilon \in (0, n]$, $\delta \geq \frac{1}{n-\varepsilon}$, любого простого p и любого неособого подмножества $A \subset \mathbb{F}_{p^2}$, удовлетворяющего условию $|A| > q^\delta$, выполнено*

$$NA^n = \mathbb{F}_{p^2},$$

где $N \leq C \cdot 4^n \ln(2 + \frac{1}{\varepsilon})$.

В доказательствах теорем 2, 1 использовались одни и те же идеи. Усложняющим фактором в поле $\mathbb{F}_{p^2}$ является наличие нетривиальных аддитивных подгрупп. Используя в качестве основы метод доказательства теоремы 2, автор получил следующую теорему.

ТЕОРЕМА 3 [30]. *Для произвольного неособого подмножества $A \subset \mathbb{F}_{p^3}$ такого, что $|A| \geq p^{\frac{3}{n-\varepsilon}}$, для некоторого натурального $n \geq 2$ и действительного $\varepsilon \in (0, 1)$ имеет место соотношение*

$$NA^n = \mathbb{F}_{p^3},$$

где

$$N = \begin{cases} 10, & \text{если } n = 2, \\ 120 \left(2 + \left\lceil \log_2 \frac{1}{\varepsilon} \right\rceil \right), & \text{если } n = 3, \\ \max \left\{ \frac{5}{3} (5 \cdot 4^n - 32) \left(3 + \left\lceil \log_2 \frac{1}{\varepsilon} \right\rceil \right), 16384 \right\}, & \text{если } n \geq 4. \end{cases}$$

В настоящей работе будут доказаны обобщения теорем 2, 3 в случае произвольного поля.

ТЕОРЕМА 4. *Для произвольного неособого подмножества $A \subseteq \mathbb{F}_q$, $q = p^r$, $r \geq 3$, такого, что $|A| > q^{\frac{1}{n-\varepsilon}}$ для некоторого натурального $n \geq r$ и действительного $\varepsilon \in (0, 1)$, имеет место соотношение*

$$M_n A^n = \mathbb{F}_q,$$

где

$$M_n = \begin{cases} 10 \cdot 2^{\left\lceil \frac{r-1}{\log_2 3-1} \right\rceil + 1} \left(3 + \left\lceil \log_2 \frac{r}{\varepsilon} \right\rceil \right) \left(\frac{5}{24} 4^{r-1} - \frac{1}{3} \right), & \text{если } n = r, \\ 10 \cdot 2^{\left\lceil \frac{r+2}{\log_2 3-1} \right\rceil + 1} \left(3 + \left\lceil \log_2 \frac{1}{\varepsilon} \right\rceil \right) \left(\frac{5}{24} 4^{n-1} - \frac{1}{3} \right), & \text{если } n \geq r + 1. \end{cases}$$

ТЕОРЕМА 5. Для любого неособого подмножества $A \subset \mathbb{F}_{p^4}$ такого, что $|A| > p^{\frac{4}{n-\varepsilon}}$ для некоторого натурального $n \geq 2$ и действительного $\varepsilon \in (0, 1)$, выполнено равенство

$$M_n A^n = \mathbb{F}_{p^4},$$

где

$$M_n = \begin{cases} 10, & \text{если } n = 2, \\ \max \left\{ 120 \left(2 + \left\lceil \log_2 \frac{1}{\varepsilon} \right\rceil \right), 2400 \right\}, & \text{если } n = 3, \\ 8320 \left(3 + \left\lceil \log_2 \frac{4}{\varepsilon} \right\rceil \right), & \text{если } n = 4, \\ 20480 \left(3 + \left\lceil \log_2 \frac{1}{\varepsilon} \right\rceil \right) \left(\frac{5}{24} 4^{n-1} - \frac{1}{3} \right), & \text{если } n \geq 5. \end{cases}$$

Для поля $\mathbb{F}_q$, $q = p^r$, $r \geq 5$, равенство $m = n$ в задаче 1 верно не всегда. Возьмем произвольный примитивный элемент $\xi \in \mathbb{F}_q^*$ и рассмотрим подмножество $A = \mathbb{F}_p + \xi \mathbb{F}_p$. В доказательстве теоремы 8 показано, что элементы $\{1, \xi, \dots, \xi^{r-1}\}$ линейно независимы. Тогда $A^l \subset \mathbb{F}_p + \xi \mathbb{F}_p + \dots + \xi^l \mathbb{F}_p$ для любого натурального $1 \leq l \leq r-2$, и поэтому $\dim(A^l) \leq l+1$. Если рассмотреть произвольное натуральное число $\frac{r}{2} + \varepsilon \leq n \leq r-2$, то выполнено неравенство $|A| = p^2 > q^{\frac{1}{n-\varepsilon}}$, но $\dim(A^n) \leq n+1 < r$, а значит, $NA \neq \mathbb{F}_q$ для любого натурального N . В частности, если $r = 2k+1$ для некоторого натурального k и $n = k+1$, то $\dim(A^{2n-3}) = \dim(A^{r-2}) \leq r-1$, и поэтому также $NA \neq \mathbb{F}_q$ для любого натурального N . Мы докажем следующую теорему.

ТЕОРЕМА 6. Пусть $A \subset \mathbb{F}_q$ – произвольное неособое подмножество такое, что $|A| > q^{\frac{1}{n-\varepsilon}}$ для некоторого $\varepsilon \in (0, 1)$. Тогда выполнено равенство

$$NA^{2n-2} = \mathbb{F}_q,$$

где

$$N = \begin{cases} 10, & \text{если } n = 2, \\ 6^{n-3} \max \left\{ 30 \cdot \left(3 + \left\lceil \log_2 \frac{1}{\varepsilon} \right\rceil \right), 160 \cdot (1 + \lfloor \log_2 n \rfloor) \right\}, & \text{если } n \geq 3. \end{cases}$$

Из теоремы 6 получаем

СЛЕДСТВИЕ 1. Если $H \subset \mathbb{F}_q \setminus \{0\}$ – произвольная неособая мультипликативная подгруппа такая, что $|H| > q^{\frac{1}{n-\varepsilon}}$ для некоторого $\varepsilon \in (0, 1)$, то выполнено равенство

$$NH = \mathbb{F}_q,$$

где N – число, определенное в формулировке теоремы 6.

Применяя теоремы 1–5, мы можем улучшить величину N из следствия 1 в ряде частных случаев. Если использовать оценки тригонометрических сумм по мультипликативным подгруппам конечных полей (скажем, теорему Бургена–Чанг из [31]), то получается аналогичный результат для подгрупп, которые пересекаются с любым нетривиальным подполем поля $\mathbb{F}_q$ по небольшому числу элементов. Следствие 1, выведенное при помощи комбинаторных аргументов,

более общо и дает лучшую границу для числа слагаемых, поэтому оно не вытекает из упомянутого результата Бургена–Чанг.

Гипотеза П. Эрдеши и Э. Семереди [32] утверждает, что для любого конечного непустого подмножества $A \subset \mathbb{N}$ и произвольного действительного числа $\varepsilon > 0$ верно неравенство

$$\max\{|AA|, |A + A|\} \geq c(\varepsilon)|A|^{2-\varepsilon}, \quad c(\varepsilon) > 0.$$

В [32] также доказано, что $\max\{|AA|, |A + A|\} \geq c|A|^{1+\delta}$, $c > 0$, для некоторого $\delta > 0$. Позже для константы δ в последнем неравенстве была получена оценка снизу, причем эта оценка в ряде работ улучшалась. В настоящий момент наилучшая оценка доказана Дж. Шолумоши [33]. Она имеет вид $\max\{|AA|, |A + A|\} \geq |A|^{\frac{4}{3}-\varepsilon}$, где $\varepsilon > 0$ – произвольное действительное число, и верна также для конечных подмножеств множества комплексных чисел.

Методы, разработанные в [25], выявляют взаимосвязь проблемы Эрдеши–Семереди для конечных полей с задачей о базисных свойствах множества произведений ограниченного количества элементов подмножества A конечного поля. Последняя задача является основным объектом исследования в настоящей работе. Если $\mathbb{F}_p$ – поле простого порядка p и A – его подмножество, удовлетворяющее условию $|A| > p^{\frac{1}{2}+\varepsilon}$, $\varepsilon > 0$, то из классических оценок тригонометрических сумм (см., например, [34, с. 103, упражнение 8α]) нетрудно получить, что множество попарных произведений элементов неособого множества A образует базис, порядок которого не превосходит некоторого числа, зависящего только от ε . Если множество A имеет меньшую мощность или является подгруппой по сложению, то для исследования базисных свойств множеств $AA, AAA, \dots$ приходится использовать методы и результаты работ, связанных с суммами и произведениями подмножеств конечных полей (см., например, [35], [36]). Настоящая работа продолжает такие исследования.

В § 2 приведены предварительные утверждения, необходимые для доказательства теорем 4–6. Теорема 6 будет доказана в § 3. В § 4, 5 описан индукционный процесс, который используется в § 6 для вывода нескольких вспомогательных утверждений, необходимых для доказательства теорем 4, 5. Эти теоремы получены в § 7. В § 4–7 предполагается, что простое число p удовлетворяет неравенству $p > 2$. Случай малых p рассматривается в § 7 отдельно. Далее везде считается, что $r \geq 3$, так как случаи $r = 1, 2$ уже рассмотрены в теоремах 1, 2 соответственно.

§ 2. Предварительные результаты

ОПРЕДЕЛЕНИЕ 5. Для произвольных подмножеств $X, Y \subset \mathbb{F}_q$ определим два множества следующими равенствами:

$$Q[X, Y] = \frac{X - X}{(Y - Y) \setminus \{0\}},$$

$$I(X, Y) = \{x_1(y_1 - y_2) + y_3(x_2 - x_3) : x_1, x_2, x_3 \in X, y_1, y_2, y_3 \in Y\}.$$

ОПРЕДЕЛЕНИЕ 6. Для любого подмножества $X \subset \mathbb{F}_q$ его *группа симметрии* (обозначаемая через $\text{Sym}_1(X)$) задается равенством

$$\text{Sym}_1(X) = \{h : h + X = X\}.$$

ЗАМЕЧАНИЕ 1. Ясно, что $\text{Sym}_1(X)$ – аддитивная подгруппа поля $\mathbb{F}_q$. Более того, $\text{Sym}_1(X)$ – линейное подпространство над полем $\mathbb{F}_p \subset \mathbb{F}_q$.

ЗАМЕЧАНИЕ 2. Если X – неособое множество, то оно содержит элементы по меньшей мере двух мультипликативных смежных классов по подгруппе $\mathbb{F}_p^* \subset \mathbb{F}_q^*$, т. е. в нем лежат как минимум два линейно независимых над $\mathbb{F}_p$ элемента.

ЗАМЕЧАНИЕ 3. Если подмножества X и Y поля $\mathbb{F}_q$ таковы, что $Y + X = X$, то $\text{Span}(Y) \subseteq \text{Sym}_1(X)$. В частности, если $1 + X = X$, то $\mathbb{F}_p \subseteq \text{Sym}_1(X)$.

Нам понадобится следующая

ТЕОРЕМА 7 [37]. Пусть $g(p)$ – наименьшее натуральное число, которое по модулю простого нечетного p является первообразным корнем. Тогда для любого действительного $x \geq 3$ верно равенство

$$\frac{1}{\pi(x)} \sum_{p \leq x} g(p) = O((\log x)^2 (\log \log x)^4),$$

где $\pi(x)$ – количество простых чисел, не превосходящих x .

ЛЕММА 3. Для заданного натурального числа r существует бесконечно много нечетных простых чисел p таких, что $p \equiv 1 \pmod{r}$ и выполнено неравенство $g(p) \leq (\ln p)^3$.

ДОКАЗАТЕЛЬСТВО. Обозначим множество всех простых чисел через $\mathcal{P}$. Предположим, что множество $\mathcal{C} = \{p \in \mathcal{P} : g(p) \leq (\ln p)^3, p \equiv 1 \pmod{r}\}$ конечно. Тогда для достаточно большого x мы получим

$$\begin{aligned} \frac{1}{\pi(x)} \sum_{p \leq x} g(p) &\geq \frac{1}{\pi(x)} \sum_{\frac{x}{2} < p \leq x, p \equiv 1 \pmod{r}} g(p) \geq \frac{1}{\pi(x)} \sum_{\frac{x}{2} < p \leq x, p \equiv 1 \pmod{r}} (\ln p)^3 \\ &\geq \frac{1}{\pi(x)} \left(\ln \frac{x}{2} \right)^3 \left(\pi(x, r, 1) - \pi\left(\frac{x}{2}, r, 1\right) \right), \end{aligned} \quad (1)$$

где $\pi(y, r, 1) = |\{p \in \mathcal{P} : p \leq y, p \equiv 1 \pmod{r}\}|$. Для произвольной константы $\frac{2}{3} < C < 1$ можно подобрать такое x_0 , что для любого $x \geq x_0$ одновременно выполнены следующие неравенства (здесь использована теорема об асимптотике количества простых чисел в арифметической прогрессии, доказательство которой можно найти, например, в [38, гл. 9]):

$$\begin{aligned} \pi(x, r, 1) &\geq C \frac{x}{\varphi(r) \ln x}, & \pi\left(\frac{x}{2}, r, 1\right) &\leq \frac{3}{2} C \frac{x}{2\varphi(r) \ln \frac{x}{2}}, \\ \pi(x) &\leq \frac{3}{2} C \frac{x}{\ln x}, & \ln \frac{x}{16} &\geq \frac{1}{2} \ln x. \end{aligned}$$

Тогда цепочку неравенств (1) можно продолжить:

$$\begin{aligned} \frac{1}{\pi(x)} \sum_{p \leq x} g(p) &\geq \frac{1}{\pi(x)} \left(\ln \frac{x}{2} \right)^3 \left(\pi(x, r, 1) - \pi\left(\frac{x}{2}, r, 1\right) \right) \\ &\geq \frac{2}{3C} \frac{\ln x}{x} \left(\ln \frac{x}{2} \right)^3 \left(C \frac{x}{\varphi(r) \ln x} - \frac{3}{4} C \frac{x}{\varphi(r) \ln \frac{x}{2}} \right) \\ &= \frac{1}{6\varphi(r)} \left(\ln \frac{x}{2} \right)^2 \ln \frac{x}{16} \geq \frac{1}{48\varphi(r)} (\ln x)^3. \end{aligned} \quad (2)$$

Согласно теореме 7 выполнено неравенство

$$\frac{1}{\pi(x)} \sum_{p \leq x} g(p) = O((\ln x)^2 (\ln \ln x)^4),$$

которое противоречит соотношению (2), если x достаточно велико. Лемма доказана.

ТЕОРЕМА 8. *Для любых натуральных чисел $n \geq 2$, $r \geq 1$, действительного числа $0 < \varepsilon < 1$ и любого натурального N существуют простое число p и подмножество $A \subset \mathbb{F}_q$, $q = p^r$, такие, что $|A| > q^{\frac{1}{n-\varepsilon}}$ и $NA^{n-1} \neq \mathbb{F}_q$.*

ДОКАЗАТЕЛЬСТВО. Рассмотрим некоторое достаточно большое простое p , значение которого будет выбрано позже, и произвольный элемент $\xi \in \mathbb{F}_q^*$, не лежащий ни в одном собственном подполе $\mathbb{F}_q$. Определим множество

$$A = \left\{ \sum_{i=0}^{r-1} x_i \xi^i : x_i \in \mathbb{N}, 0 \leq x_i \leq [p^{\frac{1}{n-\varepsilon}}], 0 \leq i \leq r-1 \right\}.$$

Заметим, что все элементы вида $\{1, \xi, \dots, \xi^{r-1}\}$ линейно независимы в совокупности над полем $\mathbb{F}_p$. Действительно, в противном случае существуют элементы $a_0, a_1, \dots, a_{r-1} \in \mathbb{F}_p$, одновременно не равные нулю, такие, что $a_0 + a_1 \xi + \dots + a_{r-1} \xi^{r-1} = 0$. В этом случае минимальное поле, содержащее $\mathbb{F}_p$ и элемент ξ , является собственным подполем в $\mathbb{F}_q$, а это противоречит выбору элемента ξ . Из этого следует, что $|A| = ([p^{\frac{1}{n-\varepsilon}}] + 1)^r > p^{\frac{r}{n-\varepsilon}}$. Легко видеть, что $A^{n-1} \subseteq C$, где

$$C = \left\{ \sum_{i=0}^{(r-1)(n-1)} y_i \xi^i : y_i \in \mathbb{N}, 0 \leq y_i \leq K, 0 \leq i \leq (r-1)(n-1) \right\};$$

здесь $K = (r-1)^{n-2} [p^{\frac{1}{n-\varepsilon}}]^{n-1}$. Согласно лемме 3 можно выбрать достаточно большое простое p такое, что $p \equiv 1 \pmod{r}$ и выполнено неравенство $g(p) \leq (\ln p)^3$, т.е. существует натуральное число a такое, что $a \leq (\ln p)^3$ и $a \pmod{p}$ является первообразным корнем. Выбрав такое простое p и натуральное число a , покажем, что если многочлен $f(x) = x^r - a$ неприводим над полем $\mathbb{F}_p$, то можно найти корень $f(x)$ в поле $\mathbb{F}_q$, который не будет лежать ни в каком собственном подполе $\mathbb{F}_q$. Действительно, рассмотрим поле $\mathbb{F}_p[x]/(f(x))$, где $(f(x))$ – идеал кольца $\mathbb{F}_p[x]$, содержащий многочлен $f(x)$; мы получим поле из p^r элементов, изоморфное полю $\mathbb{F}_q$, в котором элемент $\xi_1 = x + (f(x))$ будет корнем многочлена $f(x)$. Более того, если элемент ξ_1 лежит в некотором нетривиальном подполе, то его степени $\{1, \xi_1, \dots, \xi_1^{r-1}\}$ линейно зависимы, а значит, существуют элементы $b_0, b_1, \dots, b_{r-1} \in \mathbb{F}_p$, одновременно не равные нулю, такие, что $b_0 + b_1 \xi_1 + \dots + b_{r-1} \xi_1^{r-1} = 0$. Последнее означает, что многочлен $x^r - a$ приводим над полем $\mathbb{F}_p$, его делителем является наибольший общий делитель многочленов $x^r - a$ и $b_0 + b_1 x + \dots + b_{r-1} x^{r-1}$, которые не взаимно просты, так как имеют общий корень ξ_1 . Это противоречие доказывает, что элемент ξ_1 не лежит ни в одном собственном подполе поля $\mathbb{F}_q$.

Покажем теперь, что многочлен $x^r - a$ является неприводимым в поле $\mathbb{F}_p$. Действительно, если он приводим, то, рассмотрев его поле разложения F , возьмем корни этого многочлена $x_1, x_2, \dots, x_r \in F$. Поскольку $x^r - a =$

$\prod_{i=1}^r (x - x_i) \in \mathbb{F}_p[x]$, существуют натуральное число $1 \leq l < r$ и элементы $x_{i_1}, x_{i_2}, \dots, x_{i_l}$ такие, что $\prod_{j=1}^l (x - x_{i_j}) \in \mathbb{F}_p[x]$, а значит, $\zeta = \prod_{j=1}^l x_{i_j} \in \mathbb{F}_p$. Отметим, что $\zeta^r = a^l$. Так как p выбрано таким, что верно сравнение $p \equiv 1 \pmod{r}$, то $a^{l(\frac{p-1}{r})} \equiv 1 \pmod{p}$. Поскольку a является первообразным корнем, последнее сравнение эквивалентно соотношению $\frac{l(p-1)}{r} \equiv 0 \pmod{p-1}$, из которого легко вывести, что $\frac{l}{r} \in \mathbb{Z}$. В силу того, что $l < r$, мы получаем противоречие, которое доказывает неприводимость многочлена $x^r - a$.

Рассуждения, приведенные в начале доказательства, не зависят от выбора элемента ξ , поэтому можно без ограничения общности предполагать, что выполнено равенство $\xi^r = a$. Тогда легко видеть, что

$$C \subseteq \left\{ \sum_{i=0}^{r-1} z_i \xi^i : z_i \in \mathbb{N}, 0 \leq z_i \leq L, 0 \leq i \leq r-1 \right\},$$

где $L = K \frac{a^{d+1}-1}{a-1} \leq K \frac{(\ln p)^{3(d+1)}-1}{(\ln p)^3-1}$ и $d = \lfloor \frac{(n-1)(r-1)}{r} \rfloor$. Если выбрать p , удовлетворяющее ограничениям, указанным выше, настолько большим, чтобы выполнялись неравенства

$$NK \frac{a^{d+1}-1}{a-1} \leq N(r-1)^{n-2} \left[p^{\frac{1}{n-\varepsilon}} \right]^{n-1} \frac{(\ln p)^{3(d+1)}-1}{(\ln p)^3-1} < p-1,$$

получим

$$|NA^{n-1}| \leq |NC| \leq \left(NK \frac{a^{d+1}-1}{a-1} \right)^r < (p-1)^r < q.$$

Теорема доказана.

ЛЕММА 4. Пусть X и Y – подмножества в $\mathbb{F}_q$ такие, что $|X+Y| = |X|$. Тогда Y – подмножество некоторого аддитивного сдвига $\text{Sym}_1(X)$, а X является объединением (аддитивных) смежных классов по подгруппе $\text{Sym}_1(X)$. В частности, если $X+Y = X$, то $Y \subset \text{Sym}_1(X)$ и X имеет ту же аддитивную структуру.

ДОКАЗАТЕЛЬСТВО. Рассмотрим произвольный элемент $y \in Y$ и соответствующее ему множество $Y' = -y + Y$. Тогда $0 \in Y'$ и $|X+Y'| = |X|$. Поскольку $X \subset X+Y'$, то $X = X+Y'$, и поэтому $Y \subset y + \text{Sym}_1(X)$. Осталось доказать вторую часть леммы. Для этого достаточно показать, что произвольный смежный класс $a + \text{Sym}_1(X)$ либо не пересекается с множеством X , либо в нем содержится. Действительно, пусть существует элемент b такой, что $b \in X \cap (a + \text{Sym}_1(X))$. Тогда $b + \text{Sym}_1(X) \subset X$, но, с другой стороны, $b + \text{Sym}_1(X) = a + \text{Sym}_1(X)$, откуда вытекает утверждение леммы. Лемма доказана.

ЛЕММА 5. Если X – любое подмножество в $\mathbb{F}_q$ и G – произвольная подгруппа группы $\text{Sym}_1(X)$, то X является объединением аддитивных смежных классов по группе G .

ДОКАЗАТЕЛЬСТВО. Согласно замечанию 1 группа $\text{Sym}_1(X)$ – аддитивная подгруппа в $\mathbb{F}_q$. Достаточно показать, что произвольный смежный класс по подгруппе G либо содержится во множестве X , либо не пересекается с X . Пусть $x + G$ имеет непустое пересечение с множеством X . Выберем произвольный элемент $y \in X \cap (x + G)$. Теперь мы видим, что смежный класс $y + G$ совпадает со смежным классом $x + G$. С другой стороны, из условия $G \subseteq \text{Sym}_1(X)$ следует, что $y + G \subset X$. Лемма доказана.

ЛЕММА 6. Для любого $X \subset \mathbb{F}_q$, удовлетворяющего условию $|X| > \frac{q}{2}$, выполнено равенство $X + X = \mathbb{F}_q$.

ДОКАЗАТЕЛЬСТВО. Возьмем произвольный элемент $x \in \mathbb{F}_q$ и рассмотрим множество $x - X$. Из неравенства $|x - X| = |X| > \frac{q}{2}$ следует, что множества $x - X$ и X имеют непустое пересечение, а это означает, что существуют элементы $x_1, x_2 \in X$ такие, что $x - x_1 = x_2$, т. е. $x = x_1 + x_2$. Последнее равенство завершает доказательство леммы.

ЛЕММА 7. Для произвольного неособого подмножества $X \subset \mathbb{F}_q$ и любого натурального n , удовлетворяющих условию $\dim(X^n) < r$, где $\dim(X^n)$ – размерность множества X^n согласно определению 3, выполнено неравенство $\dim(X^{n+1}) \geq \dim(X^n) + 1$.

ДОКАЗАТЕЛЬСТВО. Предположим, что $\dim(X^n) = \dim(X^{n+1})$. Поскольку умножение множества на любой элемент не изменяет размерность этого множества, то, заменяя X на $\frac{1}{x} * X$, $x \in X$, $x \neq 0$, можно считать, что $1 \in X$. Определим аддитивные подгруппы $G' = \text{Span}(X^n)$, $G = \text{Span}(X)$. Включение $1 \in X$ гарантирует выполнение соотношений $G \subset G'$ и $\text{Span}(X^n) = \text{Span}(X^{n+1})$. Легко понять, что

$$G' = \bigcup_{m=1}^{\infty} mX^n = \bigcup_{m=1}^{\infty} mX^{n+1}, \quad G \subseteq G' = \bigcup_{m=1}^{\infty} mX.$$

Из последних равенств получаем

$$\begin{aligned} GG' &= \bigcup_{m_1=1}^{\infty} \bigcup_{m_2=1}^{\infty} ((m_1X)(m_2X^n)) \subseteq \bigcup_{m_1=1}^{\infty} \bigcup_{m_2=1}^{\infty} (m_1m_2X^{n+1}) \\ &= \bigcup_{m=1}^{\infty} (mX^{n+1}) = G' \Rightarrow GG' = G'. \end{aligned}$$

Поскольку $X^{n+2} \subseteq GG' = G'$, то $\dim(X^n) = \dim(X^{n+2})$, и поэтому $G' = \text{Span}(X^{n+2}) = \bigcup_{m=1}^{\infty} mX^{n+2}$. Используя аналогичные аргументы, по индукции получим равенство $G' = \text{Span}(X^k) = \bigcup_{m=1}^{\infty} mX^k$ для любого $k \geq n$. Заметим, что

$$G'G' = \bigcup_{m_1=1}^{\infty} \bigcup_{m_2=1}^{\infty} ((m_1X^n)(m_2X^n)) \subseteq \bigcup_{m=1}^{\infty} mX^{2n} = G',$$

а это означает, что G' – подполе. Поскольку $X \subset G'$, получено противоречие с тем, что множество X неособо. Лемма доказана.

ЛЕММА 8. Для любого неособого подмножества $X \subset \mathbb{F}_q$ и произвольных натуральных чисел i и t таких, что $\dim(mX^i - mX^i) < r$, выполнено $\dim(mX^{i+1} - mX^{i+1}) \geq \dim(mX^i - mX^i) + 1$.

ДОКАЗАТЕЛЬСТВО. Будем рассуждать от противного. Предположим, что $\dim(mX^{i+1} - mX^{i+1}) = \dim(mX^i - mX^i)$. Поскольку умножение множества на любой элемент не изменяет размерности любой степени и кратной суммы этого множества, то, заменяя X на $\frac{1}{x} * X$, $x \in X$, $x \neq 0$, можно считать, что $1 \in X$. Значит, можно без ограничения общности считать, что $mX^i - mX^i \subseteq mX^{i+1} - mX^{i+1}$.

Обозначим $G = \text{Span}(mX^i - mX^i) = \text{Span}(mX^{i+1} - mX^{i+1})$. Поскольку $0 \in mX^i - mX^i$, для любого натурального $l \geq 1$ имеет место включение $mX^i - mX^i \subseteq l(mX^i - mX^i)$, а значит, можно найти такое натуральное число $N \geq 1$, что $G = N(mX^i - mX^i)$ и одновременно $G = N(mX^{i+1} - mX^{i+1})$. Нетрудно видеть, что

$$XG = X(N(mX^i - mX^i)) \subseteq N(X(mX^i - mX^i)) \subseteq N(mX^{i+1} - mX^{i+1}) = G,$$

поэтому

$$GG = (N(mX^i - mX^i))G \subseteq N((mX^i - mX^i)G) \subseteq N(m(X^iG) - m(X^iG)) = G.$$

Мы установили, что $GG = G$, откуда следует, что G – подполе. Поскольку $1 \in X$, то $X - X \subseteq mX^i - mX^i \subseteq G$, откуда следует, что $X \subseteq 1 + G = G$, а из последнего включения вытекает, что X – особое множество. Противоречие. Лемма доказана.

ЛЕММА 9. *Рассмотрим произвольное неособое подмножество $X \subset \mathbb{F}_q$. Тогда существует натуральное число $N \leq q - 1$ такое, что $NX^r = \mathbb{F}_q$. Более того, если $Q[X, X] = \frac{X-X}{(X-X) \setminus \{0\}} \not\subseteq \mathbb{F}_p$, то существует натуральное число $N_1 \leq q - 1$ такое, что $N_1X^{r-1} = \mathbb{F}_q$.*

ДОКАЗАТЕЛЬСТВО. Если для любого $k \leq q - 1$ верны соотношения $|kX^r| \geq |(k - 1)X^r| + 1$, то $(q - 1)X^r = \mathbb{F}_q$ и лемма доказана. Если же существует натуральное число $N \leq q - 1$ такое, что $|NX^r| = |(N + 1)X^r|$, то для любого $k \geq N$ будет иметь место равенство $|kX^r| = |(k + 1)X^r|$. В этом случае легко понять, что существуют элемент $b \in \mathbb{F}_q$ и аддитивная подгруппа $G \subset \mathbb{F}_q$ такие, что $NX^r = b + G$. Если $G = \mathbb{F}_q$, то $NX^r = \mathbb{F}_q$ и лемма доказана. Если же $G \neq \mathbb{F}_q$, то из леммы 8 следует, что $\dim(NX^r - NX^r) = r$. С другой стороны, выполнено равенство $NX^r - NX^r = G$, из которого вытекает, что $\dim(NX^r - NX^r) = \dim(G) \leq r - 1$. Полученное противоречие завершает доказательство первого утверждения леммы.

Если $Q[X, X] \not\subseteq \mathbb{F}_p$, то $\dim(X - X) \geq 2$ (в противном случае $Q[X, X] \subseteq \mathbb{F}_p$), а значит, согласно лемме 8 имеем $\dim(lX^{r-1} - lX^{r-1}) = r$ для любого натурального $l \geq 1$. Теперь, повторяя те же рассуждения, мы находим натуральное число $N_1 \leq q - 1$ такое, что $N_1X^{r-1} = \mathbb{F}_q$. Лемма доказана полностью.

Следующая лемма является простым обобщением леммы 2.50 из [39].

ЛЕММА 10. *Рассмотрим $\xi \in \mathbb{F}_q$. Тогда $\xi \in Q[X, Y]$, если и только если $|X + \xi * Y| < |X||Y|$.*

ДОКАЗАТЕЛЬСТВО. Рассмотрим отображение $F: X \times Y \rightarrow X + \xi * Y$, определенное равенством $F(x, y) = x + \xi y$. Отображение F не инъективно тогда и только тогда, когда $|X + \xi * Y| < |X||Y|$. С другой стороны, условие того, что F не инъективно, означает, что существуют элементы $x_1, x_2 \in X$, $y_1, y_2 \in Y$ такие, что $(x_1, y_1) \neq (x_2, y_2)$ и $F(x_1, y_1) = F(x_2, y_2)$. Отметим, что $y_1 \neq y_2$, так как иначе мы выводим равенство $x_1 = x_2$ и получаем противоречие с условием $(x_1, y_1) \neq (x_2, y_2)$. Таким образом, $\xi = (x_1 - x_2)/(y_2 - y_1) \in (X - X)/((Y - Y) \setminus \{0\})$. Лемма доказана.

Доказательства следующих двух лемм аналогичны доказательствам леммы 1 и леммы 3 из работы [40].

ЛЕММА 11. Пусть $X, Y \subset \mathbb{F}_q$, $G \subset \mathbb{F}_q^*$ и $G \neq \emptyset$. Тогда найдется элемент $\xi \in G$ такой, что

$$|X + \xi Y| \geq \frac{|X||Y||G|}{|X||Y| + |G|}.$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим произвольные элементы $\xi \in G$ и $s \in \mathbb{F}_q$. Введем следующее обозначение:

$$f_\xi^+(s) := |\{(x, y) \in X \times Y : x + y\xi = s\}|.$$

Тогда

$$\begin{aligned} \sum_{s \in \mathbb{F}_q} (f_\xi^+(s))^2 &= |\{(x_1, y_1, x_2, y_2) \in X \times X \times Y \times Y : x_1 + y_1\xi = x_2 + y_2\xi\}| \\ &= |X||Y| + |\{(x_1, y_1, x_2, y_2) \in X \times X \times Y \times Y : x_1 \neq x_2, x_1 + y_1\xi = x_2 + y_2\xi\}|. \end{aligned}$$

Заметим, что для любых $x_1, x_2 \in X$, $y_1, y_2 \in Y$ таких, что $x_1 \neq x_2$, существует не более одного η такого, что $x_1 + y_1\eta = x_2 + y_2\eta$. Тогда

$$\sum_{\xi \in G} \sum_{s \in \mathbb{F}_q} (f_\xi^+(s))^2 \leq |X||Y||G| + |X|^2|Y|^2. \quad (3)$$

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

$$\sum_{s \in \mathbb{F}_q} (f_\xi^+(s))^2 \leq |X||Y| + \frac{|X|^2|Y|^2}{|G|}. \quad (4)$$

Из неравенства Коши–Буняковского–Шварца получим

$$\left(\sum_{s \in \mathbb{F}_q} f_\xi^+(s) \right)^2 \leq |X + \xi Y| \sum_{s \in \mathbb{F}_q} (f_\xi^+(s))^2. \quad (5)$$

Кроме того,

$$\sum_{s \in \mathbb{F}_q} f_\xi^+(s) = |X||Y|.$$

Таким образом, из неравенств (3), (5), учитывая (4), получим

$$|X + \xi Y| \geq \frac{|X|^2|Y|^2}{|X||Y| + \frac{|X|^2|Y|^2}{|G|}} = \frac{|X||Y||G|}{|X||Y| + |G|}.$$

Лемма доказана.

ЛЕММА 12. Пусть $X, Y \subset \mathbb{F}_q$. Если для некоторого $\xi \in \mathbb{F}_q$ выполнено

$$|X + \xi Y| < |X||Y|,$$

то имеем

$$|2XY - 2XY| \geq |I(X, Y)| \geq |X + \xi Y|.$$

ДОКАЗАТЕЛЬСТВО. Неравенство $|2XY - 2XY| \geq |I(X, Y)|$ вытекает непосредственно из определения 5 множества $|I(X, Y)|$. Из условия $|X + \xi Y| < |X||Y|$ следует, что существуют такие $x_1, x_2 \in X$, $y_1, y_2 \in Y$, что $(x_1, y_1) \neq (x_2, y_2)$ и

$$(x_1 - x_2) + (y_1 - y_2)\xi = 0. \quad (6)$$

Очевидно, что $y_1 \neq y_2$. Рассмотрим множество

$$S := (y_1 - y_2)(X + \xi Y) = \{(y_1 - y_2)s : s \in X + \xi Y\}.$$

Ясно, что $|S| = |X + \xi Y|$. Каждый элемент $s \in S$ можно записать в следующем виде:

$$s = (y_1 - y_2)a + (y_1 - y_2)b\xi, \quad a \in X, \quad b \in Y.$$

Используя (6), получаем

$$s = (y_1 - y_2)a + (x_2 - x_1)b.$$

Поэтому $S \subset I(X, Y)$ и лемма доказана.

Следующая лемма доказана в работе [28]. Она является простым следствием неравенства треугольника Ружа [39, лемма 2.6].

ЛЕММА 13. *Если $Y \subset \mathbb{F}_q$ – некоторое подмножество и k – произвольное натуральное число, то*

$$|kY| \geq |Y|^{2^{1-k}} |Y - Y|^{1-2^{1-k}}.$$

Мы используем результат, верный для подмножеств произвольной коммутативной аддитивной группы (см. [39, теорема 5.5] или [41]).

ТЕОРЕМА 9 (М. Кнезер). *Для произвольных подмножеств $X, Y \subset \mathbb{F}_q$ верно неравенство*

$$\begin{aligned} |X + Y| &\geq |X + \text{Sym}_1(X + Y)| + |Y + \text{Sym}_1(X + Y)| - |\text{Sym}_1(X + Y)| \\ &\geq |X| + |Y| - |\text{Sym}_1(X + Y)|. \end{aligned}$$

Частным случаем теоремы 9 является, очевидно, следующее утверждение.

ТЕОРЕМА 10 (О. Коши, Г. Дэвенпорт). *Для произвольных подмножеств $X, Y \subset \mathbb{F}_p$ верно неравенство*

$$|X + Y| \geq \min\{|X| + |Y| - 1, p\}.$$

Из теоремы 9 также следует

ЛЕММА 14. *Рассмотрим произвольное подмножество $B \subset \mathbb{F}_q$ такое, что $|B| \geq 2$. Тогда либо верно неравенство $|B + B| \geq \frac{3}{2}|B|$, либо существует аддитивная подгруппа $G \subset \mathbb{F}_q$ такая, что $B \subseteq b + G$ для некоторого элемента $b \in B$ и выполнено ограничение $|B| > \frac{2}{3}|G|$. Более того, во втором случае можно утверждать, что $B + B = 2b + G$.*

ДОКАЗАТЕЛЬСТВО. Применяя теорему 9, получаем

$$|B + B| \geq 2|B + \text{Sym}_1(B + B)| - |\text{Sym}_1(B + B)| \geq 2|B| - |\text{Sym}_1(B + B)|. \quad (7)$$

Поскольку $\text{Sym}_1(B + B)$ является аддитивной подгруппой в $\mathbb{F}_q$, существует натуральное число $0 \leq l \leq r$ такое, что $|\text{Sym}_1(B + B)| = p^l$. Заметим, что $\text{Sym}_1(B + B) \subset \text{Sym}_1(B + \text{Sym}_1(B + B))$. Из леммы 5 легко вывести равенство $|B + \text{Sym}_1(B + B)| = mp^l$ для некоторого натурального m . Из неравенства (7) вытекает оценка

$$|B + B| \geq (2m - 1)p^l. \quad (8)$$

Предположим, что выполнено соотношение $|B + B| < \frac{3}{2}|B|$. Тогда из неравенства (7) мы получим

$$\frac{3}{2}|B| > 2|B| - |\text{Sym}_1(B + B)| \Leftrightarrow |B| < 2p^l,$$

откуда следует, что $|B + B| < \frac{3}{2} \cdot 2p^l = 3p^l$. Последнее соотношение вместе с неравенством (8) дает нам условие $2m - 1 < 3$, из которого следует, что m может принимать только одно значение: $m = 1$. Если $m = 1$, то

$$|B + \text{Sym}_1(B + B)| = |\text{Sym}_1(B + B)| = p^l.$$

Рассмотрим произвольный элемент $b \in B$ и множество $B' = B - b$. Учитывая условия $0 \in B - b = B'$ и $|B + \text{Sym}_1(B + B)| = |\text{Sym}_1(B + B)|$, мы выводим равенство $B' + \text{Sym}_1(B + B) = \text{Sym}_1(B + B)$, из которого следует, что $B' \subset \text{Sym}_1(B + B)$. Согласно определению B' мы выводим соотношение $B \subset b + \text{Sym}_1(B + B)$. Из (8) можно получить неравенство $|B + B| \geq p^l$. Согласно включению $B + B \subset 2b + \text{Sym}_1(B + B)$ имеем $|B + B| = |\text{Sym}_1(B + B)| = p^l$. Теперь легко понять, что если $|B| \leq \frac{2}{3}p^l$, то верно неравенство $|B + B| \geq \frac{3}{2}|B|$, а в противном случае для подгруппы по сложению $G = \text{Sym}_1(B + B)$ мы получаем включение $B \subseteq b + G$ и условие $|B| > \frac{2}{3}|G|$. Для завершения доказательства осталось заметить, что при выполнении последних двух соотношений из леммы 6 легко вывести равенство $B + B = 2b + G$. Лемма доказана полностью.

Следующие две леммы применяются при проведении индукционного процесса.

ЛЕММА 15. *Рассмотрим подмножества $X, Y \subset \mathbb{F}_q$ такие, что $|X| \geq 1$, $|Y| > 1$. Если элемент $a \in \mathbb{F}_q^*$ таков, что $a + Q[X, Y] \not\subseteq Q[X, Y]$, то*

$$|2XY - 2XY + a * Y^2 - a * Y^2| \geq |X| |Y|.$$

ДОКАЗАТЕЛЬСТВО. Здесь используются идеи из [28, доказательство леммы 3.2]. Из условия леммы вытекает существование элемента $\xi \in Q[X, Y]$, удовлетворяющего условию $a + \xi \notin Q[X, Y]$. Поскольку $\xi \in Q[X, Y]$, найдутся элементы $x_1, x_2 \in X$, $y_1, y_2 \in Y$, $y_1 \neq y_2$, для которых можно записать $\xi = (x_1 - x_2)/(y_1 - y_2)$. Более того, поскольку $(x_1 - x_2)/(y_1 - y_2) + a = \xi + a \notin Q[X, Y]$, из леммы 10 следует равенство

$$\left| \left\{ x + \left(\frac{x_1 - x_2}{y_1 - y_2} + a \right) y : x \in X, y \in Y \right\} \right| = |X| |Y|.$$

Умножая все элементы множества в левой части равенства на $y_1 - y_2$, получаем

$$|\{x(y_1 - y_2) + (x_1 - x_2)y + (y_1 - y_2)ay : x \in X, y \in Y\}| = |X| |Y|. \quad (9)$$

Заметим, что

$$x(y_1 - y_2) + (x_1 - x_2)y + (y_1 - y_2)ay \in 2XY - 2XY + a * Y^2 - a * Y^2. \quad (10)$$

Теперь утверждение леммы вытекает из соотношений (9), (10).

ЛЕММА 16. *Для любого непустого подмножества $X \subset \mathbb{F}_q$ и любого подмножества $Y \subset \mathbb{F}_q$, удовлетворяющего условию $|Y| \geq 2$, выполнено неравенство*

$$|2XY - 2XY| \geq \frac{|X| |Y| |Q[X, Y] \setminus \{0\}|}{|X| |Y| + |Q[X, Y] \setminus \{0\}|}.$$

ДОКАЗАТЕЛЬСТВО. Пусть $G = Q[X, Y] \setminus \{0\}$. Используя лемму 11 для множества G , мы выведем существование элемента $\xi \in Q[X, Y] \setminus \{0\}$ такого, что

$$|X + \xi Y| \geq \frac{|X||Y||Q[X, Y] \setminus \{0\}|}{|X||Y| + |Q[X, Y] \setminus \{0\}|}.$$

Из леммы 10 вытекает, что для любого элемента $\eta \in Q[X, Y]$ выполнено неравенство $|X + \eta * Y| < |X||Y|$. Теперь утверждение леммы следует из леммы 12. Лемма доказана.

§ 3. Доказательство теоремы 6

В доказательстве следующей леммы используются идеи Ж. Бургена, изложенные им в личной переписке с автором.

ЛЕММА 17. Для любых подмножеств $X, Y \subset \mathbb{F}_q$ таких, что $|X| > 1$, $|Y| > 1$, Y – неособое и $Q[X, Y] \neq \mathbb{F}_q$, выполнено неравенство

$$|3XY^2 - 3XY^2| \geq |X||Y|.$$

ДОКАЗАТЕЛЬСТВО. Заменяя множества X и Y на множества $\frac{1}{x} * X$, $x \in X$, и $\frac{1}{y} * Y$, $y \in Y$, соответственно, мы не изменим мощности множеств, участвующих в формулировке леммы. Поэтому можно без ограничения общности считать, что $1 \in X$ и $1 \in Y$.

Если $1 + Q[X, Y] \neq Q[X, Y]$, то существуют элементы $x_1, x_2 \in X$, $y_1, y_2 \in Y$, $y_1 \neq y_2$, такие, что $1 + \frac{x_1 - x_2}{y_1 - y_2} \notin Q[X, Y]$. Применяя лемму 10 и тот факт, что $1 \in X$ и $1 \in Y$, получим

$$\begin{aligned} \left| X + \left(1 + \frac{x_1 - x_2}{y_1 - y_2} \right) Y \right| &= |X||Y| \Rightarrow |(y_1 - y_2)X + (y_1 - y_2 + x_1 - x_2)Y| = |X||Y| \\ &\Rightarrow |2XY - 2XY + Y^2 - Y^2| \geq |X||Y| \\ &\Rightarrow |3XY^2 - 3XY^2| \geq |X||Y|. \end{aligned}$$

Последнее неравенство завершает доказательство леммы для этого случая.

Пусть выполнено равенство

$$1 + Q[X, Y] = Q[X, Y]. \quad (11)$$

Рассмотрим три множества:

$$G = \{g \in \mathbb{F}_q : g + Q[X, Y] = Q[X, Y]\}, \\ F = \{r \in \mathbb{F}_q : rQ[X, Y] \subseteq Q[X, Y]\}, \quad F_0 = \{f \in \mathbb{F}_q : fG \subseteq G\}.$$

Для любого ненулевого элемента $r \in F$ имеют место очевидные соотношения $rQ[X, Y] \subseteq Q[X, Y]$ и $|rQ[X, Y]| = |Q[X, Y]|$, из которых следует выполнение равенства $rQ[X, Y] = Q[X, Y]$. Далее, для любых двух элементов $g_1, g_2 \in G$ верны включения $g_1 + g_2 + Q[X, Y] \subseteq g_1 + Q[X, Y] \subseteq Q[X, Y]$, и поэтому $g_1 + g_2 \in G$, а это означает, что G – аддитивная подгруппа. Аналогично, для любых двух элементов $f_1, f_2 \in F_0$ выводим свойства $(f_1 + f_2)G \subseteq f_1G + f_2G \subseteq G + G = G$ и $f_1f_2G \subseteq f_1G \subseteq G$, из которых вытекают условия $f_1 + f_2 \in F_0$ и $f_1f_2 \in F_0$. Из последних включений следует, что F_0 – подполе. Рассмотрим произвольные элементы $g \in G$, $r \in F$, $r \neq 0$, и выведем:

$$rg + Q[X, Y] \subseteq rg + rQ[X, Y] = r(g + Q[X, Y]) = rQ[X, Y] \subseteq Q[X, Y],$$

а значит, $rg + Q[X, Y] = Q[X, Y]$ и $rg \in G$. Отметим, что если $0 \in F$ и $r = 0$, то также $rg = 0 \in G$. Из последнего соотношения следует, что $r \in F_0$, и поэтому $F \subseteq F_0$.

Если $Y \not\subseteq F$, то существуют элемент $y \in Y$ и элементы $x_1, x_2 \in X$, $y_1, y_2 \in Y$ такие, что $y \frac{x_1 - x_2}{y_1 - y_2} \notin Q[X, Y]$. Далее, используя лемму 10, мы видим, что

$$\begin{aligned} \left| X + y \frac{x_1 - x_2}{y_1 - y_2} Y \right| &= |X| |Y| \Leftrightarrow |(y_1 - y_2)X + y(x_1 - x_2)Y| = |X| |Y| \\ &\Rightarrow |2XY^2 - 2XY^2| \geq |X| |Y|. \end{aligned}$$

Последнее неравенство доказывает лемму в этом случае.

Пусть теперь справедливо включение $Y \subseteq F$ и выполнено равенство (11). Заметим, что $F \subseteq F_0$, а значит, $Y \subseteq F_0$. Если $F_0 \neq \mathbb{F}_q$, то последнее соотношение противоречит тому, что Y – неособое множество. Если $F_0 = \mathbb{F}_q$, то $G = \mathbb{F}_q$, а следовательно, $Q[X, Y] = \mathbb{F}_q$. Последнее равенство противоречит условиям леммы. Лемма доказана полностью.

В доказательстве следующего предложения используются идеи работы [42, лемма 6.2].

ПРЕДЛОЖЕНИЕ 1. Пусть $X, Y \subset \mathbb{F}_q$ – произвольные подмножества такие, что $|X| > 1$, $|Y| > 1$ и Y – неособое множество. Если $|X - X| |Y - Y| \leq q$, то

$$|3XY^2 - 3XY^2| \geq |X| |Y|.$$

Если же $|X - X| |Y - Y| > q$, то

$$16XY - 16XY = \mathbb{F}_q.$$

ДОКАЗАТЕЛЬСТВО. Предположим сначала, что $|X - X| |Y - Y| \leq q$. Ясно, что $|Q[X, Y]| \leq |X - X| (|Y - Y| - 1) < q$, и поэтому мы можем применить лемму 17, из которой выводим неравенство

$$|3XY^2 - 3XY^2| \geq |X| |Y|,$$

что завершает рассмотрение данного случая.

Если имеет место соотношение $|X - X| |Y - Y| > q$, то мы, учитывая симметричность множества $X - X$, можем использовать лемму 2 и вывести равенство

$$8(X - X)(Y - Y) = \mathbb{F}_q \Rightarrow 16XY - 16XY = \mathbb{F}_q,$$

которое завершает доказательство предложения.

ЛЕММА 18. Пусть $X \subset \mathbb{F}_q$ – произвольное неособое подмножество такое, что $|X| > 1$. Если натуральное число $k \geq 2$ удовлетворяет условию

$$|X - X| |6^{k-2} X^{2k-3} - 6^{k-2} X^{2k-3}| \leq q, \quad (12)$$

то выполнены следующие неравенства:

$$|6^{k-2} \cdot 3X^{2k-1} - 6^{k-2} \cdot 3X^{2k-1}| \geq |X|^k, \quad |6^{k-1} \cdot 3X^{2k-1}| \geq |X|^{k-\Sigma_{k-1}},$$

где $\Sigma_{k-1} = \frac{1}{2^5} + \frac{1}{2^{2 \cdot 5}} + \dots + \frac{1}{2^{(k-1) \cdot 5}} < \frac{1}{31}$.

ДОКАЗАТЕЛЬСТВО. Применим метод математической индукции. Если $|X - X|^2 \leq q$, то, используя предложение 1, мы получаем неравенство

$$|3X^3 - 3X^3| \geq |X|^2.$$

Согласно полученному соотношению из леммы 13 при $k = 6$ получим

$$|6 \cdot 3X^3| \geq |3X^3|^{\frac{1}{25}} |3X^3 - 3X^3|^{1-\frac{1}{25}} \geq |X|^{\frac{1}{25}} |X|^{2(1-\frac{1}{25})} = |X|^{2-\frac{1}{25}}.$$

База индукции доказана.

Пусть натуральное число $k \geq 3$ удовлетворяет условию (12) и для $k-1$ лемма выполнена. Используя предложение 1, в котором в качестве множества X взято множество $6^{k-2} \cdot 3X^{2k-3}$, а вместо множества Y – множество X , получим

$$|6^{k-2} \cdot 3X^{2k-1} - 6^{k-2} \cdot 3X^{2k-1}| \geq |X|^k.$$

Теперь из леммы 13, применяя последнее неравенство и предположение индукции, имеем

$$\begin{aligned} |6^{k-1} \cdot 3X^{2k-1}| &\geq |6^{k-2} \cdot 3X^{2k-1}|^{\frac{1}{25}} |6^{k-2} \cdot 3X^{2k-1} - 6^{k-2} \cdot 3X^{2k-1}|^{1-\frac{1}{25}} \\ &\geq |6^{k-2} \cdot 3X^{2k-3}|^{\frac{1}{25}} |X|^{k(1-\frac{1}{25})} \geq |X|^{\frac{1}{25}(k-1-\Sigma_{k-2})+k(1-\frac{1}{25})} \\ &= |X|^{k-\Sigma_{k-1}}. \end{aligned}$$

Лемма доказана полностью.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 6. Если $n = 2$, то утверждение теоремы следует из леммы 1. Предположим, что $n \geq 3$. В случае, когда верно неравенство $|A - A| |6^{n-3} A^{2n-5} - 6^{n-3} A^{2n-5}| > q$, из леммы 1 следует, что

$$16 \cdot 6^{n-3} A^{2n-4} - 16 \cdot 6^{n-3} A^{2n-4} = \mathbb{F}_q.$$

Используя принцип Дирихле, легко показать, что $|16 \cdot 6^{n-3} A^{2n-4}| \geq \sqrt{q}$. Применим лемму 13 с параметром $k = k_1 = 1 + \lfloor \log_2 n \rfloor$, получим

$$|16k_1 \cdot 6^{n-3} A^{2n-4}| \geq q^{\frac{1}{2k_1} + (1-\frac{1}{2k_1-1})} = q^{1-\frac{1}{2k_1}}.$$

Теперь ясно, что $|16k_1 \cdot 6^{n-3} A^{2n-4}| |A| > q^{1+\frac{1}{n-\varepsilon} + \frac{1}{2k_1}} > q$, и поэтому, применяя лемму 1, имеем равенство

$$160 \cdot 6^{n-3} k_1 A^{2n-3} = \mathbb{F}_q,$$

которое завершает доказательство теоремы в этом случае.

Если n удовлетворяет условию $|A - A| |6^{n-3} A^{2n-5} - 6^{n-3} A^{2n-5}| \leq q$, то из леммы 18 получаем

$$\begin{aligned} |6^{n-3} \cdot 3A^{2n-3} - 6^{n-3} \cdot 3A^{2n-3}| &\geq |A|^{n-1}, \\ |6^{n-3} \cdot 3A^{2n-3}| &\geq |6^{n-3} \cdot 3A^{2n-5}| \geq |A|^{n-1-\frac{32}{31}}. \end{aligned}$$

Вводя новый параметр $k_2 = 3 + \lfloor \log_2 \frac{1}{\varepsilon} \rfloor$, применяя два последних неравенства и используя лемму 13, докажем, что

$$|6^{n-3} k_2 \cdot 3A^{2n-3}| \geq |A|^{\frac{1}{2k_2-1}(n-1-\frac{32}{31})+(n-1)(1-\frac{1}{2k_2-1})} = |A|^{n-1-\frac{32}{31} \frac{1}{2k_2-1}}.$$

Из полученного соотношения мы легко выводим неравенство $|3 \cdot 6^{n-3} k_2 A^{2n-3}| \geq |A|^{n-1-\varepsilon}$, поэтому имеем $|6^{n-3} k_2 \cdot 3A^{2n-3}| |A| \geq |A|^{n-\varepsilon} > q$. Теперь из леммы 1 получаем нужное равенство

$$30 \cdot 6^{n-3} k_2 A^{2n-2} = \mathbb{F}_q.$$

Теорема доказана полностью.

§ 4. Первый шаг индукционного процесса

Доказательство следующей леммы практически совпадает с доказательством леммы 3 из работы [29].

ЛЕММА 19. *Если X – произвольное подмножество $\mathbb{F}_q$, удовлетворяющее условиям $Q[X, X] \subset \mathbb{F}_{p^2} \subset \mathbb{F}_q$, $1 + Q[X, X] = Q[X, X]$, то либо $Q[X, X] = \mathbb{F}_p \subset \mathbb{F}_{p^2}$, либо $Q[X, X] = \mathbb{F}_{p^2}$.*

ДОКАЗАТЕЛЬСТВО. В силу замечания 3 имеем $\mathbb{F}_p + Q[X, X] = Q[X, X]$. Из этого факта и леммы 4 получаем, что $Q[X, X]$ является объединением аддитивных смежных классов по $\mathbb{F}_p$. Более того, верно соотношение $(Q[X, X] \setminus \{0\})^{-1} = Q[X, X] \setminus \{0\}$.

Пусть

$$\mathbb{F}_p \subsetneq Q[X, X]. \quad (13)$$

Рассмотрим произвольный смежный класс $b_0 + \mathbb{F}_p \subset Q[X, X] \setminus \{0\}$, $b_0 \notin \mathbb{F}_p$. В этом случае все элементы вида $\frac{1}{b_0+h}$, $h \in \mathbb{F}_p$, содержатся в множестве $Q[X, X] \setminus \{0\}$. Если пара элементов $\frac{1}{b_0+h_1}$, $\frac{1}{b_0+h_2}$, где $h_1 \in \mathbb{F}_p$, $h_2 \in \mathbb{F}_p$, лежит в одном классе смежности по $\mathbb{F}_p$, то их разность $\frac{1}{b_0+h_1} - \frac{1}{b_0+h_2}$ тоже принадлежит $\mathbb{F}_p$. Отсюда вытекает включение $\frac{h_1-h_2}{(b_0+h_1)(b_0+h_2)} \in \mathbb{F}_p$, из которого выводим условие

$$(b_0 + h_1)(b_0 + h_2) \in \mathbb{F}_p. \quad (14)$$

Однако для любого $h_1 \in \mathbb{F}_p$ существует не более одного элемента $h_2 \in \mathbb{F}_p$, обладающего свойством (14). Действительно, если для h_1 найдется другой элемент $h'_2 \in \mathbb{F}_p$, $h'_2 \neq h_2$, удовлетворяющий соотношению (14), то $(b_0 + h_1)(h_2 - h'_2) \in \mathbb{F}_p \Rightarrow b_0 + h_1 \in \mathbb{F}_p$. Последнее включение противоречит выбору элемента b_0 . Поэтому $Q[X, X]$ содержит как минимум $\lfloor \frac{p}{2} \rfloor + 1$ смежных классов по $\mathbb{F}_p$. Предположим, что $Q[X, X] \subsetneq \mathbb{F}_{p^2}$. Рассуждая аналогичным образом и используя равенство $(\mathbb{F}_{p^2} \setminus Q[X, X])^{-1} = \mathbb{F}_{p^2} \setminus Q[X, X]$, установим следующее утверждение: $\mathbb{F}_{p^2} \setminus Q[X, X]$ содержит также как минимум $\lfloor \frac{p}{2} \rfloor + 1$ смежных классов по $\mathbb{F}_p$. Поскольку в $\mathbb{F}_{p^2}$ содержатся только p смежных классов по $\mathbb{F}_p$, мы получаем противоречие. Таким образом, из (13) следует соотношение $Q[X, X] = \mathbb{F}_{p^2}$. Лемма доказана.

В доказательстве следующей леммы частично используются идеи из доказательства леммы 3.1 работы [30].

ЛЕММА 20. *Рассмотрим произвольное неособое подмножество $X \subset \mathbb{F}_q$ такое, что $1 + Q[X, X] = Q[X, X]$, $Q[X, X] \neq \mathbb{F}_p$ и $Q[X, X] \neq \mathbb{F}_{p^2}$. Тогда*

$$|Q[X, X] \setminus \{0\}| \geq \frac{p^2(p-1)}{2} + p.$$

ДОКАЗАТЕЛЬСТВО. Поскольку $Q[X, X] \neq \mathbb{F}_p$, можно найти элемент $\xi \notin \mathbb{F}_p$, удовлетворяющий ограничению $\xi \in Q[X, X]$. Более того, если $Q[X, X] \subseteq \mathbb{F}_{p^2}$, то из леммы 19 следует равенство $Q[X, X] = \mathbb{F}_{p^2}$. Последнее соотношение противоречит условиям леммы, поэтому без ограничения общности можно считать, что $\xi \notin \mathbb{F}_{p^2}$, $\xi \in Q[X, X]$. Из ограничения $1 + Q[X, X] = Q[X, X]$ легко вывести следующее свойство множества $Q[X, X]$: для любого $x \in Q[X, X]$ и для любого $b \in \mathbb{F}_p$ элементы $x + b$ и $\frac{1}{x}$ принадлежат $Q[X, X]$, если $x \neq 0$. Обозначим

множество квадратных матриц с двумя строками и элементами из поля $\mathbb{F}_p$ через $\mathbb{M}_2(\mathbb{F}_p)$. Для удобства сопоставим каждой матрице из $\mathbb{M}_2(\mathbb{F}_p)$ с ненулевой второй строкой элемент из множества $\frac{\mathbb{F}_p\xi + \mathbb{F}_p}{\mathbb{F}_p\xi + \mathbb{F}_p}$ по следующему правилу:

$$\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \rightarrow \frac{x_1\xi + x_2}{x_3\xi + x_4}.$$

Данное соответствие не является взаимно однозначным.

Назовем матрицу *требуемой*, если соответствующий ей элемент лежит в $Q[X, X]$. Описанное выше свойство множества $Q[X, X]$ можно переформулировать следующим образом: перестановка строк требуемой матрицы оставляет ее требуемой, таким же свойством обладает прибавление к верхней строке нижней строки, умноженной на произвольный элемент поля $\mathbb{F}_p$. Первое преобразование умножает определитель матрицы на -1 , второе сохраняет его без изменения. Из определения элемента ξ мы выводим, что матрица $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ требуемая. Теперь преобразуем ее для элементов $y_1, y_2, y_3 \in \mathbb{F}_p$ следующим образом:

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &\rightarrow \begin{pmatrix} 1 & y_1 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & y_1 \end{pmatrix} \rightarrow \begin{pmatrix} y_2 & 1 + y_1y_2 \\ 1 & y_1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & y_1 \\ y_2 & 1 + y_1y_2 \end{pmatrix} \\ &\rightarrow \begin{pmatrix} 1 + y_2y_3 & y_1 + y_3 + y_1y_2y_3 \\ y_2 & 1 + y_1y_2 \end{pmatrix}. \end{aligned} \quad (15)$$

Легко понять, что все матрицы трехпараметрического семейства (15) требуемые и имеют определитель 1. Теперь нужно выяснить, сколько различных матриц в этом семействе.

Рассмотрим произвольную матрицу $X \in \mathbb{M}_2(\mathbb{F}_p)$, $X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$, с определителем 1. Предположим сначала, что $x_3 \neq 0$. Докажем, что существует только один набор значений параметров $(y_1, y_2, y_3) \in \mathbb{F}_p \times \mathbb{F}_p^* \times \mathbb{F}_p$, для которых матрица (15) совпадает с матрицей X . Действительно, из равенства этих матриц вытекает, что параметры y_1, y_2, y_3 однозначно выражаются через элементы матрицы X следующим образом: $y_1 = \frac{x_4 - 1}{y_2}$, $y_2 = x_3$, $y_3 = \frac{x_1 - 1}{y_2}$, а значит, различным значениям параметров y_1, y_2, y_3 , где $y_2 \neq 0$, соответствуют различные матрицы семейства (15). Мы нашли $p^2(p-1)$ различных требуемых матриц.

Если матрица X такова, что $x_3 = 0$, то, выражая аналогично параметры y_1, y_2, y_3 через элементы матрицы X , выводим: $y_2 = x_3 = 0$, $y_1 + y_3 = x_2$. Кроме того, если матрица X , удовлетворяющая условию $x_3 = 0$, принадлежит множеству матриц (15), то $x_1 = x_4 = 1$, и поэтому в данном случае мы получаем p различных требуемых матриц.

Осталось понять, каким матрицам семейства (15) соответствует один и тот же элемент.

Поскольку матрице вида $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ соответствует элемент $\xi + c$, при условии $y_2 = 0$ мы получаем p различных элементов, которым соответствуют матрицы семейства. Рассмотрим случай $x_3 \neq 0$. Пусть двум разным матрицам $X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$ и $X' = \begin{pmatrix} x'_1 & x'_2 \\ x'_3 & x'_4 \end{pmatrix}$ с определителями, равными 1, соответствует один элемент. Это условие эквивалентно равенству

$$\frac{x_1\xi + x_2}{x_3\xi + x_4} = \frac{x'_1\xi + x'_2}{x'_3\xi + x'_4} \Leftrightarrow (x_1\xi + x_2)(x'_3\xi + x'_4) = (x'_1\xi + x'_2)(x_3\xi + x_4). \quad (16)$$

Представив поле $\mathbb{F}_q$ как алгебраическое расширение поля $\mathbb{F}_p$, полученное присоединением к нему элемента ξ , равенство из (16) можно рассматривать как

равенство многочленов (заметим, что $\xi \notin \mathbb{F}_{p^2}$, и поэтому ξ является алгебраическим элементом порядка, большего, чем 2). Поскольку многочлен не может иметь два различных неприводимых разложения, то равенство в (16) может иметь место только в том случае, когда $x_1\xi + x_2$ делит один из многочленов $x'_1\xi + x'_2$, $x_3\xi + x_4$ и то же выполнено для многочлена $x'_3\xi + x'_4$, причем оба они делят различные многочлены. Поскольку равенство $x_1\xi + x_2 = K(x_3\xi + x_4)$ невозможно ни для какой константы $K \in \mathbb{F}_p$ (иначе определитель матрицы X был бы равен нулю), для некоторого $c \in \mathbb{F}_p^*$ выполнено соотношение $x_1\xi + x_2 = c(x'_1\xi + x'_2)$ и одновременно $x_3\xi + x_4 = c(x'_3\xi + x'_4)$ для той же константы. Из последних равенств легко вывести, что матрица X равна матрице $cX' = \begin{pmatrix} cx'_1 & cx'_2 \\ cx'_3 & cx'_4 \end{pmatrix}$. Поскольку определитель матрицы X равен 1, то $c^2 = 1$ и, следовательно, $c \in \{-1, 1\}$. Поэтому трехпараметрическому семейству матриц (15) при условии $y_2 \neq 0$ соответствует не менее $\frac{p^2(p-1)}{2}$ различных элементов.

Осталось доказать, что матрицам $X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$ и $X' = \begin{pmatrix} x'_1 & x'_2 \\ x'_3 & x'_4 \end{pmatrix}$, удовлетворяющим условиям $x_3 \neq 0$ и $x'_3 = 0$ и имеющим определитель, равный 1, не соответствует один и тот же элемент. Действительно, из обратного предположения следует, что

$$\frac{x_1\xi + x_2}{x_3\xi + x_4} = \frac{x'_1(x'_1\xi + x'_2)}{x'_3(x'_3\xi + x'_4)} \Leftrightarrow x_1\xi + x_2 = x'_1(x'_1\xi + x'_2)(x_3\xi + x_4).$$

Поскольку $\xi \notin \mathbb{F}_{p^2}$, то ξ не является алгебраическим элементом второго порядка и последнее равенство невозможно, что приводит нас к противоречию. Из требуемости матриц семейства (15) вытекает принадлежность всех полученных элементов множеству $Q[X, X]$. Очевидно, что все эти элементы не равны нулю (только вырожденная матрица может соответствовать нулю). Лемма доказана.

ПРЕДЛОЖЕНИЕ 2. Для любого неособого подмножества $X \subset \mathbb{F}_q$, удовлетворяющего условию $|X| > 1$, выполнено соотношение

$$|3X^2 - 3X^2| \geq \frac{|X|^2 \left(\frac{p^2(p-1)}{2} + p \right)}{|X|^2 + \frac{p^2(p-1)}{2} + p}. \quad (17)$$

ДОКАЗАТЕЛЬСТВО. Заменяя множество X на множество $\frac{1}{x} * X$, $x \in X$, мы не изменим мощности множеств, участвующих в формулировке предложения. Поэтому можно без ограничения общности считать, что $1 \in X$. Рассмотрим три случая.

Случай 1. Множество $Q[X, X]$ удовлетворяет условию $1 + Q[X, X] \not\subseteq Q[X, X]$. Тогда, применив лемму 15, где в качестве множеств X и Y мы возьмем множество X , а вместо элемента a подставим 1, получим

$$|3X^2 - 3X^2| \geq |X|^2 \geq \frac{|X|^2 \left(\frac{p^2(p-1)}{2} + p \right)}{|X|^2 + \frac{p^2(p-1)}{2} + p}. \quad (18)$$

Случай 2. Верны соотношения $1 + Q[X, X] = Q[X, X]$ и $Q[X, X] \subseteq \mathbb{F}_{p^2}$. Тогда согласно лемме 19 либо $Q[X, X] = \mathbb{F}_p$, либо $Q[X, X] = \mathbb{F}_{p^2}$. Поскольку множество X неособое, существует элемент, удовлетворяющий условиям $\xi \notin Q[X, X]$, $\xi \in X$. Используя лемму 10, получаем

$$|X + \xi * X| = |X|^2 \Rightarrow |2X^2| \geq |X|^2 \geq \frac{|X|^2 \left(\frac{p^2(p-1)}{2} + p \right)}{|X|^2 + \frac{p^2(p-1)}{2} + p}. \quad (19)$$

Случай 3. Верны ограничения $1 + Q[X, X] = Q[X, X]$ и $Q[X, X] \not\subseteq \mathbb{F}_{p^2}$. Применим леммы 16, 20 и получим оценку

$$|2X^2 - 2X^2| \geq \frac{|X|^2(\frac{p^2(p-1)}{2} + p)}{|X|^2 + \frac{p^2(p-1)}{2} + p}. \quad (20)$$

Неравенство (17) теперь очевидным образом следует из соотношений (18)–(20). Предложение доказано.

§ 5. Следующие шаги индукционного процесса

ЛЕММА 21. Для любого натурального числа $3 \leq k \leq r$, любого неособого подмножества $X \subset \mathbb{F}_q$ такого, что $\dim(X) = 2$ и $Q[X, X] \subseteq \mathbb{F}_p$, выполнено неравенство

$$|kX^k| \geq |X|^k.$$

ДОКАЗАТЕЛЬСТВО. Из условия $Q[X, X] = \frac{X-X}{(X-X) \setminus \{0\}} \subseteq \mathbb{F}_p$ вытекает ограничение $X - X \subseteq dY$ для некоторого элемента $d \in \mathbb{F}_q$ и подмножества $Y \subseteq \mathbb{F}_p$, а значит, существуют $x_0 \in \mathbb{F}_q$ и подмножество $Y' \subseteq Y$ такие, что $X = x_0 + dY'$. Элементы x_0 и d можно выбрать так, чтобы были выполнены включения $x_0 \in X$ и $x_0 + d \in X$, которые равносильны условиям $0 \in Y$ и $1 \in Y$. Легко понять, что для любого нетривиального подполя S_1 имеет место соотношение $\frac{x_0}{d} \notin S_1$, так как в противном случае $X \subset dS_1$ и множество X особое. Имеем

$$kX^k = \left\{ kx_0^k + x_0^{k-1}d \sum_{i=1}^k \sum_{j=1}^k x_j^{(i)} + x_0^{k-2}d^2 \sum_{i=1}^k \sum_{1 \leq j_1 < j_2 \leq k} x_{j_1}^{(i)} x_{j_2}^{(i)} + \dots \right. \\ \left. \dots + d^k \sum_{i=1}^k x_1^{(i)} x_2^{(i)} \dots x_k^{(i)} : x_j^{(i)} \in Y, 1 \leq i, j \leq k \right\}.$$

Элементы $\{x_0^{k-1}d, x_0^{k-2}d^2, \dots, d^k\}$ линейно независимы, иначе существовали бы элементы $a_1, \dots, a_{k-1} \in \mathbb{F}_p$, не равные одновременно нулю и удовлетворяющие равенству $a_1 x_0^{k-1}d + \dots + a_{k-1}d^k = 0$. Записывая это уравнение в виде $a_1(\frac{x_0}{d})^{k-1} + \dots + a_k = 0$, находим, что $\frac{x_0}{d}$ лежит в собственном подполе $\mathbb{F}_q$, так как является корнем уравнения степени, меньшей r . Однако, как мы показали, последнее невозможно, и мы приходим к противоречию. Определим значения параметров следующим образом:

$$\begin{aligned} x_j^{(i)} &= 1, & 1 \leq i \leq k-1, & \quad i \leq j \leq k-1, \\ x_{j_1}^{(i_1)} &= 0, & 2 \leq i_1 \leq k, & \quad 1 \leq j_1 \leq i_1-1, \\ x_k^{(i_2)} &= x_{i_2}, & 1 \leq i_2 \leq k, & \end{aligned} \quad (21)$$

где $x_m \in Y$, $1 \leq m \leq k$, – произвольные элементы. Равенства (21) выделяют во множестве kX^k некоторое подмножество $K \subseteq kX^k$. Если элемент подмножества K равен элементу $kx_0^k + x_0^{k-1}dy_1 + x_0^{k-2}d^2y_2 + \dots + d^ky_k$ для некоторых $y_1, y_2, \dots, y_k \in \mathbb{F}_p$, то, выписывая равенства коэффициентов при элементах $x^{k-i}d^i$, можно составить систему линейных уравнений, имеющую верхнетреугольную матрицу с определителем, равным 1. Это означает, что данная

система имеет единственное решение для любых значений $y_1, y_2, \dots, y_k$, т. е. различным значениям параметров $x_1, x_2, \dots, x_k \in Y$ соответствуют различные элементы множества K . Отсюда следует, что K содержит ровно $|Y|^k = |X|^k$ элементов. Лемма доказана полностью.

Рассмотрим произвольное неособое множество X и определим последовательность подмножеств следующим образом: $X_1 = X$, $X_k = N_k X^k - N_k X^k$, где $N_k = \frac{5}{24}4^k - \frac{1}{3}$ и $k \geq 2$ – любое натуральное число. Таким образом,

$$X_2 = 3X^2 - 3X^2, \quad X_3 = 13X^3 - 13X^3, \quad X_4 = 53X^4 - 53X^4, \quad \dots$$

Легко доказать, что числа N_k удовлетворяют рекуррентному соотношению $N_{k+1} = 4N_k + 1$.

ЛЕММА 22. *Для любого неособого подмножества $X \subset \mathbb{F}_q$ такого, что $\dim(X) \geq 3$, выполнено неравенство*

$$|N_k X^k - N_k X^k| \geq \frac{|X_{k-1}| |X| (p^k - 1)}{|X_{k-1}| |X| + (p^k - 1)},$$

где $3 \leq k \leq r$ – произвольное натуральное число.

ДОКАЗАТЕЛЬСТВО. Если существует элемент $x \in X^{k-2}$ такой, что $x + Q[X_{k-1}, X] \notin Q[X_{k-1}, X]$, то, взяв в лемме 15 в качестве элемента a найденный элемент x , получаем

$$|N_k X^k - N_k X^k| \geq |X| |X_{k-1}|.$$

В случае, когда такого элемента x не существует, легко понять, что $X^{k-2} + Q[X_{k-1}, X] = Q[X_{k-1}, X]$. Применяв лемму 7, мы увидим, что выполнено неравенство $\dim(X^{k-2}) \geq k$. Более того, согласно замечанию 3 верно равенство $\text{Span}(X^{k-2}) + Q[X_{k-1}, X] = Q[X_{k-1}, X]$, поэтому из леммы 4 следует, что $|Q[X_{k-1}, X]| \geq p^{\dim(X^{k-2})} \geq p^k$. Используя лемму 16, где вместо множеств X и Y подставлены множества X и X_{k-1} соответственно, мы получим

$$|4N_{k-1} X^k - 4N_{k-1} X^k| \geq \frac{|X| |X_{k-1}| (p^k - 1)}{|X| |X_{k-1}| + (p^k - 1)}.$$

Лемма доказана.

В доказательстве следующей леммы используются идеи из доказательства леммы 4.1 работы [30].

ЛЕММА 23. *Пусть $X \subset \mathbb{F}_q$ – произвольное неособое подмножество такое, что $\dim(X) = 2$, $Q[X, X] \not\subseteq \mathbb{F}_p$ и $X^{k-2} + Q[Y, X] = Q[Y, X]$, где $Y = N_{k-1} X^{k-1} - N_{k-1} X^{k-1}$ и $3 \leq k \leq r$ – произвольное натуральное число. Тогда*

$$|Q[Y, X]| \geq p^{k-1} \frac{|X| (p - 1)}{|X| + (p - 1)}. \quad (22)$$

ДОКАЗАТЕЛЬСТВО. Из условия $Q[X, X] \not\subseteq \mathbb{F}_p$ вытекает существование четырех элементов $x_1, x_2, x_3, x_4 \in X$, удовлетворяющих условию

$$\frac{x_1 - x_2}{x_3 - x_4} \notin \mathbb{F}_p. \quad (23)$$

Рассмотрим отображение $\Phi: \mathbb{F}_q \rightarrow \mathbb{F}_q/\mathbb{F}_p$, проецирующее произвольный элемент поля $x \in \mathbb{F}_q$ в элемент $x \bmod \mathbb{F}_p$ (через $\mathbb{F}_q/\mathbb{F}_p$ обозначена факторгруппа аддитивной группы $\mathbb{F}_q$ по подгруппе $\mathbb{F}_p$). Все пары вида $(\Phi(\frac{x}{x_1-x_2}), \Phi(\frac{x}{x_3-x_4}))$, $x \in X$, попарно различны, так как из равенства $(\Phi(\frac{x}{x_1-x_2}), \Phi(\frac{x}{x_3-x_4})) = (\Phi(\frac{x'}{x_1-x_2}), \Phi(\frac{x'}{x_3-x_4}))$ следует, что $\frac{x-x'}{x_1-x_2} \in \mathbb{F}_p$ и $\frac{x-x'}{x_3-x_4} \in \mathbb{F}_p$. Последние два включения могут быть выполнены одновременно, только когда $x = x'$, так как имеет место соотношение (23). Из попарной различности определенных выше пар следует неравенство

$$\max \left\{ \left| \Phi \left(\frac{X}{x_1 - x_2} \right) \right|, \left| \Phi \left(\frac{X}{x_3 - x_4} \right) \right| \right\} \geq \sqrt{|X|}. \quad (24)$$

Переход от множества X к его произвольному мультипликативному сдвигу не влияет на мощность $Q[Y, X]$. Воспользовавшись условием (24) и обозначив мультипликативный сдвиг множества X той же буквой, мы можем считать, что $|\Phi(X)| \geq \sqrt{|X|}$ и $1 \in X - X$.

Поскольку $1 \in X - X$ и $\dim(X) = 2$, то, выбрав произвольный элемент $\xi \notin \mathbb{F}_p$, $\xi \in X - X$ (так как $X - X$ неособое), мы видим, что $\text{Span}(X) = \mathbb{F}_p + \xi \mathbb{F}_p$. Очевидно, что $X \subset \text{Span}(X)$, и, значит, для любого нетривиального подполя S имеет место соотношение $\xi \notin S$, так как иначе $\text{Span}(X) \subset S$ и X оказывается особым. Из этого следует, что система $\{1, \xi, \dots, \xi^{k-1}\}$ линейно независима. Действительно, в противном случае нашлись бы элементы $a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_p$, удовлетворяющие условию $a_0 + \xi a_1 + \dots + a_{k-1} \xi^{k-1} = 0$, и, следовательно, ξ лежит в некотором нетривиальном подполе порядка, меньшего либо равного p^k . Из условия леммы мы выводим $\text{Span}(X^{k-2}) = \mathbb{F}_p + \xi \mathbb{F}_p + \dots + \xi^{k-2} \mathbb{F}_p$, а значит, выполнено соотношение $\mathbb{F}_p + \xi \mathbb{F}_p + \dots + \xi^{k-2} \mathbb{F}_p + Q[Y, X] = Q[Y, X]$. Любой элемент $x \in X$ представим в виде $x = \xi y_1 + y_2$, $y_1, y_2 \in \mathbb{F}_p$, единственным образом, поэтому можно определить новое отображение $\tilde{\Phi}: \mathbb{F}_p + \xi \mathbb{F}_p \rightarrow \mathbb{F}_p$ следующим равенством: $\tilde{\Phi}(\xi y_1 + y_2) = y_1$. Поскольку $1 \in X - X$, имеет место включение

$$\begin{aligned} & N_{k-1} X^{k-1} - N_{k-1} X^{k-1} + \mathbb{F}_p + \xi \mathbb{F}_p + \dots + \xi^{k-2} \mathbb{F}_p \\ &= \mathbb{F}_p + \xi \mathbb{F}_p + \dots + \xi^{k-2} \mathbb{F}_p + \frac{N_{k-1} X^{k-1} - N_{k-1} X^{k-1}}{1} \\ &\subseteq \mathbb{F}_p + \xi \mathbb{F}_p + \dots + \xi^{k-2} \mathbb{F}_p + \frac{Y - Y}{(X - X) \setminus \{0\}} \subseteq Q[Y, X]. \end{aligned} \quad (25)$$

Из определения преобразований Φ и $\tilde{\Phi}$ непосредственно вытекает, что $|\tilde{\Phi}(X)| = |\Phi(X)| \geq \sqrt{|X|}$. Возьмем $2(k-1)N_{k-1}$ произвольных, возможно, совпадающих элементов $x_i^j \in X$, $1 \leq i \leq k-1$, $1 \leq j \leq 2N_{k-1}$, и рассмотрим их представления в базисе $(1, \xi)$: $x_i^j = z_i^j \xi + w_i^j$, $z_i^j, w_i^j \in \mathbb{F}_p$, $1 \leq i \leq k-1$, $1 \leq j \leq 2N_{k-1}$. Ясно, что сумма

$$s = \sum_{j=1}^{N_{k-1}} \prod_{i=1}^{k-1} x_i^j - \sum_{j=N_{k-1}+1}^{2N_{k-1}} \prod_{i=1}^{k-1} x_i^j$$

принадлежит множеству $N_{k-1} X^{k-1} - N_{k-1} X^{k-1}$ и ее можно записать в виде $s = s_0 + \xi s_1 + \dots + \xi^{k-1} s_{k-1}$, где $s_0, s_1, \dots, s_{k-1} \in \mathbb{F}_p$, причем

$$s_{k-1} = \sum_{j=1}^{N_{k-1}} \prod_{i=1}^{k-1} z_i^j - \sum_{j=N_{k-1}+1}^{2N_{k-1}} \prod_{i=1}^{k-1} z_i^j \in N_{k-1} \tilde{\Phi}(X)^{k-1} - N_{k-1} \tilde{\Phi}(X)^{k-1}.$$

Применив включение (25), мы выводим, что

$$\xi^{k-1}(N_{k-1}\tilde{\Phi}(X)^{k-1} - N_{k-1}\tilde{\Phi}(X)^{k-1}) + \xi^{k-2}\mathbb{F}_p + \xi^{k-3}\mathbb{F}_p + \dots + \mathbb{F}_p \subset Q[Y, X].$$

Таким образом,

$$|Q[Y, X]| \geq |N_{k-1}\tilde{\Phi}(X)^{k-1} - N_{k-1}\tilde{\Phi}(X)^{k-1}| p^{k-1}. \quad (26)$$

Отметим соотношение $\tilde{\Phi}(X) \subseteq \mathbb{F}_p$. Используя очевидное неравенство

$$|N_{k-1}\tilde{\Phi}(X)^{k-1} - N_{k-1}\tilde{\Phi}(X)^{k-1}| \geq |3\tilde{\Phi}(X)^2 - 3\tilde{\Phi}(X)^2|, \quad (27)$$

мы завершим доказательство леммы, получив оценку мощности множества $|3\tilde{\Phi}(X)^2 - 3\tilde{\Phi}(X)^2|$. Если $Q[\tilde{\Phi}(X), \tilde{\Phi}(X)] \neq \mathbb{F}_p$, то, применяя лемму 15, где в качестве множеств X и Y мы возьмем множество $\tilde{\Phi}(X)$, а вместо элемента a подставим 1, легко вывести, что

$$|3\tilde{\Phi}(X)^2 - 3\tilde{\Phi}(X)^2| \geq |\tilde{\Phi}(X)|^2 \geq |X|. \quad (28)$$

Последнее неравенство завершает доказательство леммы для этого случая.

Если $Q[\tilde{\Phi}(X), \tilde{\Phi}(X)] = \mathbb{F}_p$, то из леммы 16 имеем

$$|2\tilde{\Phi}(X)^2 - 2\tilde{\Phi}(X)^2| \geq \frac{|\tilde{\Phi}(X)|^2(p-1)}{(p-1) + |\tilde{\Phi}(X)|^2} \geq \frac{|X|(p-1)}{|X| + (p-1)}. \quad (29)$$

Объединяя оценки (27)–(29), получаем

$$|N_{k-1}\tilde{\Phi}(X)^{k-1} - N_{k-1}\tilde{\Phi}(X)^{k-1}| \geq |3\tilde{\Phi}(X)^2 - 3\tilde{\Phi}(X)^2| \geq \frac{|X|(p-1)}{|X| + (p-1)}. \quad (30)$$

Теперь соотношение (22) легко выводится из неравенств (26) и (30). Лемма доказана.

ПРЕДЛОЖЕНИЕ 3. Рассмотрим такое произвольное неособое подмножество $X \subset \mathbb{F}_q$, что $Q[X, X] \not\subseteq \mathbb{F}_p$. Тогда

$$|X_k| = |N_k X^k - N_k X^k| \geq \frac{|X_{k-1}| |X| (p^{k-1} \frac{|X|(p-1)}{|X| + (p-1)} - 1)}{|X_{k-1}| |X| + (p^{k-1} \frac{|X|(p-1)}{|X| + (p-1)} - 1)},$$

где $3 \leq k \leq r$ – произвольное натуральное число.

ДОКАЗАТЕЛЬСТВО. Если существует элемент $x \in X^{k-2}$ такой, что $x + Q[X_{k-1}, X] \not\subseteq Q[X_{k-1}, X]$, то, взяв в лемме 15 в качестве элемента a найденный элемент x , получим

$$|N_k X^k - N_k X^k| \geq |X| |X_{k-1}|.$$

В случае, когда такого элемента x не существует, легко понять, что $X^{k-2} + Q[X_{k-1}, X] = Q[X_{k-1}, X]$. Согласно условиям леммы имеем $Q[X, X] \not\subseteq \mathbb{F}_p$. Если $\dim(X) \geq 3$, то из леммы 22 получаем неравенство

$$|N_k X^k - N_k X^k| \geq \frac{|X_{k-1}| |X| (p^k - 1)}{|X_{k-1}| |X| + (p^k - 1)}.$$

Если $\dim(X) = 2$, то нужное соотношение является следствием лемм 23, 16:

$$|4N_{k-1}X^k - 4N_{k-1}X^k| \geq \frac{|X_{k-1}| |X| (p^{k-1} \frac{|X|(p-1)}{|X|+(p-1)} - 1)}{|X_{k-1}| |X| + (p^{k-1} \frac{|X|(p-1)}{|X|+(p-1)} - 1)}.$$

Учитывая то, что $p^k - 1 \geq p^{k-1} \frac{|X|(p-1)}{|X|+(p-1)} - 1$, и возрастание функции $\frac{xy}{x+y}$ по переменным x и y , мы можем объединить все неравенства и получить утверждение предложения. Предложение доказано.

ПРЕДЛОЖЕНИЕ 4. *Рассмотрим произвольное неособое подмножество $X \subset \mathbb{F}_q$. Тогда для любого натурального $k \geq r + 1$ выполнено неравенство*

$$|X_k| = |N_k X^k - N_k X^k| \geq \frac{|X_{k-1}| |X| (q - 1)}{|X_{k-1}| |X| + (q - 1)}.$$

ДОКАЗАТЕЛЬСТВО. Если существует элемент $x \in X^{k-2}$ такой, что $x + Q[X_{k-1}, X] \notin Q[X_{k-1}, X]$, то, взяв в лемме 15 в качестве элемента a найденный элемент x , получим

$$|N_k X^k - N_k X^k| \geq |X| |X_{k-1}|. \quad (31)$$

В случае, когда такого элемента x не существует, легко понять, что $X^{k-2} + Q[X_{k-1}, X] = Q[X_{k-1}, X]$. Учитывая неравенство $\dim(X) \geq 2$, из леммы 7 легко получить равенство $\dim(X^{k-2}) = r$. Поэтому в данном случае $Q[X_{k-1}, X] = \mathbb{F}_q$, и из леммы 16 имеем соотношение

$$|4N_{k-1}X^k - 4N_{k-1}X^k| \geq \frac{|X_{k-1}| |X| (q - 1)}{|X_{k-1}| |X| + (q - 1)}. \quad (32)$$

Объединяя неравенства (31), (32), мы получим утверждение предложения. Предложение доказано.

§ 6. Описание индукционного процесса

ЛЕММА 24. *Для любого неособого множества $X \subset \mathbb{F}_q$, $p \geq 5$ и произвольного натурального числа $2 \leq k \leq r$ выполнено неравенство*

$$|N_k X^k - N_k X^k| \geq \frac{(\min\{|X|, p\})^k}{2^k}. \quad (33)$$

ДОКАЗАТЕЛЬСТВО. Пусть $k = 2$. Если $|X| \geq p$, то, применяя предложение 2 и учитывая условие $p \geq 5$, мы получим

$$|3X^2 - 3X^2| \geq \frac{|X|^2 (\frac{p^2(p-1)}{2} + p)}{|X|^2 + \frac{p^2(p-1)}{2} + p} \geq \frac{|X|^2 p^2}{p^2 + |X|^2} \geq \frac{p^2}{2}. \quad (34)$$

Если $|X| \leq p - 1$, то

$$|3X^2 - 3X^2| \geq \frac{|X|^2 (\frac{p^2(p-1)}{2} + p)}{|X|^2 + \frac{p^2(p-1)}{2} + p} \geq \frac{|X|^2}{2}. \quad (35)$$

Соотношения (34), (35) доказывают неравенство (33) для $k = 2$.

Рассмотрим теперь случай $k = 3$. Если $|X| \geq p$ и $Q[X, X] \not\subseteq \mathbb{F}_p$, то из предложения 3 и оценки (34) находим

$$\begin{aligned} |13X^3 - 13X^3| &\geq \frac{|X_2| |X| (p^2 \frac{|X|(p-1)}{|X|+(p-1)} - 1)}{|X_2| |X| + (p^2 \frac{|X|(p-1)}{|X|+(p-1)} - 1)} \\ &\geq \frac{\frac{p^3}{2} (p^2 \frac{p-1}{2} - 1)}{\frac{p^3}{2} + (p^2 \frac{p-1}{2} - 1)} \geq p^2 \frac{p-1}{4} - \frac{1}{2} > \frac{p^3}{6}. \end{aligned} \quad (36)$$

Последнее неравенство выполнено при $p \geq 5$. В случае, когда $|X| \leq p-1$ и $Q[X, X] \not\subseteq \mathbb{F}_p$, учитывая соотношение (35), получаем

$$|13X^3 - 13X^3| \geq \frac{|X_2| |X| (p^2 \frac{|X|(p-1)}{|X|+(p-1)} - 1)}{|X_2| |X| + (p^2 \frac{|X|(p-1)}{|X|+(p-1)} - 1)} \geq \frac{\frac{|X|^3}{2} (p^2 \frac{|X|}{2} - 1)}{\frac{|X|^3}{2} + (p^2 \frac{|X|}{2} - 1)} \geq \frac{|X|^3}{4}. \quad (37)$$

Если $Q[X, X] \subseteq \mathbb{F}_p$, то согласно лемме 21 выполнено неравенство $|3X^3| \geq |X|^3$. Полученные оценки (36), (37) завершают доказательство леммы в этом случае.

Предположим, что для некоторого $3 \leq k \leq r-1$ справедливость соотношения (33) установлена. Если $|X| \geq p$ и $Q[X, X] \not\subseteq \mathbb{F}_p$, то из предложения 3 следует неравенство

$$\begin{aligned} |N_{k+1}X^{k+1} - N_{k+1}X^{k+1}| &\geq \frac{|X_k| |X| (p^k \frac{|X|(p-1)}{|X|+(p-1)} - 1)}{|X_k| |X| + (p^k \frac{|X|(p-1)}{|X|+(p-1)} - 1)} \\ &\geq \frac{\frac{p^{k+1}}{2^k} (p^k \frac{p-1}{2} - 1)}{\frac{p^{k+1}}{2^k} + (p^k \frac{p-1}{2} - 1)} > \frac{p^{k+1}}{2^{k+1}}, \end{aligned} \quad (38)$$

которое верно при $p \geq 5$. Если $|X| \leq p-1$ и $Q[X, X] \not\subseteq \mathbb{F}_p$, то

$$\begin{aligned} |N_{k+1}X^{k+1} - N_{k+1}X^{k+1}| &\geq \frac{|X_k| |X| (p^k \frac{|X|(p-1)}{|X|+(p-1)} - 1)}{|X_k| |X| + (p^k \frac{|X|(p-1)}{|X|+(p-1)} - 1)} \\ &\geq \frac{\frac{|X|^{k+1}}{2^k} (p^k \frac{|X|}{2} - 1)}{\frac{|X|^{k+1}}{2^k} + (p^k \frac{|X|}{2} - 1)} \geq \frac{|X|^{k+1}}{2^{k+1}}. \end{aligned} \quad (39)$$

В случае, когда $Q[X, X] \subseteq \mathbb{F}_p$, из леммы 21 вытекает, что $|(k+1)X^{k+1}| \geq |X|^{k+1}$. Объединяя оценки (38), (39), мы завершаем доказательство соотношения (33) по индукции. Лемма доказана полностью.

ЛЕММА 25. Для любого неособого множества $X \subset \mathbb{F}_q$, удовлетворяющего условию $|X| \geq p$, $p \geq 5$, и для любого натурального числа $2 \leq k \leq r-1$ выполнено неравенство

$$|4N_kX^k| \geq \frac{1}{2^{r-1}} p^{k-\frac{1}{8}-\frac{1}{8^2}-\dots-\frac{1}{8^{k-1}}} > \frac{1}{2^{r-1}} p^{k-\frac{1}{7}}. \quad (40)$$

ДОКАЗАТЕЛЬСТВО. Установим справедливость неравенства (40) при $k = 2$. Для этого применим леммы 13, 24, из которых выведем неравенства

$$|12X^2| \geq |3X^2|^{\frac{1}{8}} |3X^2 - 3X^2|^{1-\frac{1}{8}} \geq p^{\frac{1}{8}} \left(\frac{p^2}{2} \right)^{1-\frac{1}{8}} \geq \frac{1}{2} p^{2-\frac{1}{8}}.$$

Из последнего неравенства вытекает утверждение леммы для $k = 2$.

Пусть для некоторого $2 \leq k \leq r-2$ соотношение (40) доказано. Тогда из лемм 13, 24 следует нужное неравенство, поскольку

$$\begin{aligned} |4N_{k+1}X^{k+1}| &\geq |N_{k+1}X^{k+1}|^{\frac{1}{8}} |N_{k+1}X^{k+1} - N_{k+1}X^{k+1}|^{1-\frac{1}{8}} \\ &\geq \frac{1}{2^{r-1}} p^{k+1-\frac{1}{8}-\frac{1}{8^2}-\dots-\frac{1}{8^k}}. \end{aligned}$$

Лемма доказана полностью.

ЛЕММА 26. *Если множество $X \subset \mathbb{F}_q$ неособое, $k \geq r$, то для любого натурального $l \geq 1$ верно неравенство*

$$|2^l X^k| \geq \min \left\{ \left(\frac{3}{2} \right)^l |X^k|, q \right\}.$$

Более того, если $Q[X, X] \not\subseteq \mathbb{F}_p$, то последнее соотношение верно для любых $l \geq 1$ и $k \geq r-1$.

ДОКАЗАТЕЛЬСТВО. Из леммы 14 вытекает, что либо верна оценка $|2^l X^k| \geq (\frac{3}{2})^l |X^k|$, либо существуют элемент $b \in \mathbb{F}_q$ и аддитивная подгруппа $G \subseteq \mathbb{F}_q$ такие, что $2^l X^k = b + G$. Во втором случае выполнено соотношение $2^l X^k - 2^l X^k = G$. Если $G = \mathbb{F}_q$, то лемма доказана. Если подгруппа G нетривиальна, то $\dim(2^l X^k - 2^l X^k) \leq r-1$. С другой стороны, из леммы 8 находим $\dim(2^l X^k - 2^l X^k) = r$. Полученное противоречие завершает доказательство первого утверждения леммы.

Если $Q[X, X] \not\subseteq \mathbb{F}_p$, то $\dim(2^l X - 2^l X) \geq 2$. Поэтому согласно лемме 8 верно соотношение $\dim(2^l X^{r-1} - 2^l X^{r-1}) = r$. Повторив рассуждения из первой части доказательства, легко убедимся в том, что неравенство $|2^l X^{r-1}| \geq \min\{(\frac{3}{2})^l |X^{r-1}|, q\}$ верно. Лемма доказана полностью.

ПРЕДЛОЖЕНИЕ 5. *Рассмотрим произвольное неособое подмножество $X \subset \mathbb{F}_q$, $r \geq 3$, такое, что $|X| \geq p$, $p \geq 5$. Тогда*

$$NX^{r+1} = \mathbb{F}_q,$$

где $N = 20 \cdot \left(\frac{5}{24} 4^r - \frac{1}{3}\right) \cdot 2^{\lceil \frac{r}{\log_2 3-1} \rceil + 1}$.

ДОКАЗАТЕЛЬСТВО. Используя леммы 13, 24, 25, получаем неравенства

$$|2N_r X^r| \geq (|4N_{r-1} X^{r-1}| |N_r X^r - N_r X^r|)^{\frac{1}{2}} \geq \frac{1}{2^r} p^{r-\frac{4}{7}}.$$

Пусть $r_0 = \lceil \frac{r}{\log_2 3-1} \rceil + 1$. Применяя лемму 26, находим

$$|2^{r_0+1} N_r X^r| \geq \min \left\{ \left(\frac{3}{2} \right)^{r_0} |2N_r X^r|, q \right\}.$$

Если $(\frac{3}{2})^{r_0} |2N_r X^r| \geq q$, то $2^{r_0+1} N_r X^r = \mathbb{F}_q$, и предложение доказано. Если $(\frac{3}{2})^{r_0} |2N_r X^r| < q$, то

$$|2^{r_0+1} N_r X^r| \geq \left(\frac{3}{2} \right)^{r_0} \cdot \frac{1}{2^r} p^{r-\frac{4}{7}} > p^{r-\frac{4}{7}}.$$

Замечаем, что имеет место неравенство $|2^{r_0+1} N_r X^r| |X| > q$, из леммы 1 выводим, что $20 \cdot 2^{r_0} N_r X^{r+1} = \mathbb{F}_q$. Предложение доказано полностью.

ПРЕДЛОЖЕНИЕ 6. Для любого неособого подмножества $X \subset \mathbb{F}_q$, $r \geq 3$, удовлетворяющего условию $|X| > q^{\frac{1}{r-\varepsilon}}$ для некоторого действительного $\varepsilon \in (0, 1)$, выполнено равенство

$$M_r X^r = \mathbb{F}_q,$$

где $M_r = 10 \cdot 2^{\lceil \frac{r-1}{\log_2 3-1} \rceil + 1} (3 + \lceil \log_2(\frac{r}{\varepsilon}) \rceil) (\frac{5}{24} 4^{r-1} - \frac{1}{3})$.

ДОКАЗАТЕЛЬСТВО. Заметим, что ограничение $Q[X, X] \subseteq \mathbb{F}_p$ равносильно вложению $X - X \subseteq d\mathbb{F}_p$ для некоторого элемента $d \in \mathbb{F}_q$, поэтому в данном случае $|X| \leq |X - X| \leq p$. Последнее неравенство противоречит условиям предложения 6, а значит, верно соотношение $Q[X, X] \not\subseteq \mathbb{F}_p$. Если $p < 5$, то из леммы 9 следует равенство $(3^r - 1)X^r = \mathbb{F}_q$, которое завершает доказательство предложения в данном случае. Поэтому мы можем считать, что $p \geq 5$. Применяя леммы 24, 25, получаем

$$\begin{aligned} |N_{r-1}X^{r-1} - N_{r-1}X^{r-1}| &\geq \frac{p^{r-1}}{2^{r-1}}, \\ |N_{r-1}X^{r-1}| &\geq |4N_{r-2}X^{r-2}| \geq \frac{p^{r-\frac{15}{7}}}{2^{r-1}}. \end{aligned}$$

Пусть $r_0 = \lceil \frac{r-1}{\log_2 3-1} \rceil + 1$ и $l_0 = 3 + \lceil \log_2(\frac{r}{\varepsilon}) \rceil$. Применив лемму 13, получим

$$\begin{aligned} |l_0 N_{r-1}X^{r-1}| &\geq |N_{r-1}X^{r-1}|^{\frac{1}{2^{l_0-1}}} |N_{r-1}X^{r-1} - N_{r-1}X^{r-1}|^{1-\frac{1}{2^{l_0-1}}} \\ &\geq \frac{1}{2^{r-1}} p^{r-1-\frac{8}{7 \cdot 2^{l_0-1}}}. \end{aligned}$$

Теперь из леммы 26 следует, что

$$|2^{r_0} l_0 N_{r-1}X^{r-1}| \geq \min \left\{ \left(\frac{3}{2} \right)^{r_0} \frac{1}{2^{r-1}} |l_0 N_{r-1}X^{r-1}|, q \right\}.$$

Если $(\frac{3}{2})^{r_0} \frac{1}{2^{r-1}} |l_0 N_{r-1}X^{r-1}| \geq q$, то $2^{r_0} l_0 N_{r-1}X^{r-1} = \mathbb{F}_q$, и предложение доказано. Если $(\frac{3}{2})^{r_0} \frac{1}{2^{r-1}} |l_0 N_{r-1}X^{r-1}| < q$, то

$$|2^{r_0} l_0 N_{r-1}X^{r-1}| \geq \left(\frac{3}{2} \right)^{r_0} \frac{1}{2^{r-1}} p^{r-1-\frac{8}{7 \cdot 2^{l_0-1}}} \geq p^{r-1-\frac{8}{7 \cdot 2^{l_0-1}}}.$$

Заметим, что $|2^{r_0} l_0 N_{r-1}X^{r-1}| |X| > p^{r-1-\frac{8}{7 \cdot 2^{l_0-1}} + \frac{r}{r-\varepsilon}} \geq p^{r-1-\frac{\varepsilon}{r} + \frac{r}{r-\varepsilon}} \geq q$. Теперь из леммы 1 вытекает равенство $10 \cdot 2^{r_0} l_0 N_{r-1}X^r = \mathbb{F}_q$, которое завершает доказательство предложения.

В доказательствах следующих трех лемм используются идеи из работы [28, леммы 5.1–5.3].

ЛЕММА 27. Для произвольного неособого подмножества $X \subset \mathbb{F}_q$, удовлетворяющего условию $5 \leq |X| \leq p-1$, и любого действительного $0 \leq u \leq |X|^k$ выполнено неравенство

$$|N_k X^k - N_k X^k| \geq \frac{1}{2^r} u - \frac{5}{4} \frac{u^2}{2^{2r}(q-1)}, \quad (41)$$

где $k \geq 2$ – произвольный натуральный параметр.

ДОКАЗАТЕЛЬСТВО. Если $2 \leq k \leq r$, то согласно лемме 24 имеем

$$|N_k X^k - N_k X^k| \geq \frac{|X|^k}{2^k} \geq \frac{|X|^k}{2^r} \geq \frac{1}{2^r} u - \frac{5}{4} \frac{u^2}{2^{2r}(q-1)}$$

для любого $0 \leq u \leq |X|^k$, чем завершается доказательство леммы для этих значений k .

Предположим теперь, что неравенство (41) доказано для некоторого $k \geq r$. Обозначим $V = \frac{1}{2^r} u - \frac{5}{4} \frac{u^2}{2^{2r}(q-1)}$, где $0 \leq u \leq |X|^k$ – произвольное действительное число. Заметим, что если $V < 0$, то верна оценка $\frac{1}{2^r} |X| u - \frac{5}{4} \frac{|X|^2 u^2}{2^{2r}(q-1)} < 0$, и поэтому $|X_{k+1}| > \frac{1}{2^r} |X| u - \frac{5}{4} \frac{|X|^2 u^2}{2^{2r}(q-1)}$. Если $V \geq 0$, то, используя предложение 4 и учитывая, что $|X| \geq 5$, мы получим

$$\begin{aligned} |X_{k+1}| &\geq \frac{|X| |X_k| (q-1)}{|X| |X_k| + (q-1)} \geq \frac{|X| V (q-1)}{|X| V + (q-1)} \geq |X| V \left(1 - \frac{|X| V}{q-1}\right) \\ &\geq \frac{1}{2^r} |X| u - \frac{5}{4} \frac{|X| u^2}{2^{2r}(q-1)} - \frac{|X|^2 (\frac{1}{2^r} u)^2}{q-1} \\ &\geq \frac{|X| u}{2^r} - \frac{u^2 |X|^2}{2^{2r}(q-1)} \left(1 + \frac{5}{4|X|}\right) \geq \frac{1}{2^r} |X| u - \frac{5}{4} \frac{|X|^2 u^2}{2^{2r}(q-1)}. \end{aligned}$$

Определяя новый параметр $v = |X| u$, мы завершаем доказательство леммы.

ЛЕММА 28. Для любого неособого $X \subset \mathbb{F}_q$, удовлетворяющего условиям $5 \leq |X| \leq p-1$, и любого натурального $k \geq 2$ выполнено неравенство

$$|N_k X^k - N_k X^k| \geq \frac{1}{2^{r+1}} \min \left\{ |X|^k, \frac{q-1}{2} \right\}.$$

ДОКАЗАТЕЛЬСТВО. Применяя лемму 27, где в неравенство (41) в качестве параметра u подставлено число $U = \min \left\{ |X|^k, \frac{q-1}{2} \right\}$, мы получаем

$$|N_k X^k - N_k X^k| \geq \frac{1}{2^r} U - \frac{5}{4} \frac{U^2}{2^{2r}(q-1)} \geq \left(\frac{1}{2^r} - \frac{5}{8 \cdot 2^{2r}} \right) U \geq \frac{1}{2^{r+1}} U.$$

Лемма доказана.

ЛЕММА 29. Для любого неособого $X \subset \mathbb{F}_q$, удовлетворяющего условиям $5 \leq |X| \leq p-1$, и любого натурального k такого, что $2 \leq k \leq 1 + \frac{\log_2(\frac{q-1}{2})}{\log_2 |X|}$, выполнено неравенство

$$|N_k X^k| \geq \frac{1}{2^{r+1}} |X|^{k-\frac{8}{7}}. \quad (42)$$

ДОКАЗАТЕЛЬСТВО. Докажем лемму индукцией по k . При $k = 2$ утверждение леммы очевидно. Предположим, что неравенство (42) верно для некоторого k и число $k+1$ удовлетворяет условию $k+1 \leq 1 + \frac{\log_2(\frac{q-1}{2})}{\log_2 |X|}$. Последняя оценка эквивалентна соотношению $|X|^k \leq \frac{q-1}{2}$. Используя лемму 28, получаем

$$|N_k X^k - N_k X^k| \geq \frac{1}{2^{r+1}} |X|^k.$$

Из леммы 13 следует

$$\begin{aligned} |4N_k X^k| &\geq |N_k X^k|^{\frac{1}{8}} |N_k X^k - N_k X^k|^{\frac{7}{8}} \geq |N_k X^k|^{\frac{1}{8}} \left(\frac{1}{2^{r+1}} |X|^k \right)^{\frac{7}{8}} \\ &\geq \left(\frac{1}{2^{r+1}} |X|^{k-\frac{8}{7}} \right)^{\frac{1}{8}} \left(\frac{1}{2^{r+1}} |X|^k \right)^{\frac{7}{8}} = \frac{1}{2^{r+1}} |X|^{k-\frac{1}{7}}. \end{aligned}$$

Осталось отметить, что $|N_{k+1} X^{k+1}| \geq |4N_k X^{k+1}| \geq |4N_k X^k|$. Лемма доказана.

§ 7. Доказательство теорем 4, 5

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 4. Если $n = r$, то из предложения 6 следует равенство

$$10 \cdot 2^{\lfloor \frac{r-1}{\log_2 3-1} \rfloor + 1} \left(3 + \left\lceil \log_2 \left(\frac{r}{\varepsilon} \right) \right\rceil \right) \left(\frac{5}{24} 4^{r-1} - \frac{1}{3} \right) X^r = \mathbb{F}_q,$$

которое завершает доказательство теоремы в данном случае.

Если $p < 7$ и $n \geq r+1$, то из леммы 9 мы выводим соотношение $(5^r - 1)A^r = \mathbb{F}_q$, поэтому мы полагаем, что

$$p \geq 7. \quad (43)$$

Аналогично, если $|A| \leq 4$ и $n \geq r+1$, то $q \leq |A|^n \leq 4^n$, откуда из леммы 9 получим $(4^n - 1)A^r = \mathbb{F}_q$, а значит, мы считаем, что

$$|A| \geq 5. \quad (44)$$

Если $|A| \geq p$, $n \geq r+1$ и верно неравенство (43), то из предложения 5 следует равенство $N_1 A^{r+1} = \mathbb{F}_q$, где $N_1 = 20 \left(\frac{5}{24} 4^r - \frac{1}{3} \right) \cdot 2^{\lfloor \frac{r}{\log_2 3-1} \rfloor + 1}$. Теорема при данных ограничениях доказана.

Осталось доказать теорему в случае, когда $|A| \leq p-1$ и выполнены неравенства $n \geq r+1$, (43) и (44). Определим параметр $n_0 = \lfloor \frac{\log_2(\frac{q-1}{2})}{\log_2 |A|} \rfloor$. Легко видеть, что $n_0 \leq n-1$, так как $|A|^n > q > \frac{q-1}{2} \geq |A|^{n_0}$. Рассмотрим два случая.

Случай 1. Имеет место равенство $n_0 = n-1$. В этом случае из лемм 28, 29 мы выводим неравенства

$$|N_{n-1} A^{n-1} - N_{n-1} A^{n-1}| \geq \frac{1}{2^{r+1}} |A|^{n-1}, \quad |N_{n-1} A^{n-1}| \geq \frac{1}{2^{r+1}} |A|^{n-\frac{15}{7}}.$$

Рассмотрим параметр $k = 3 + \lfloor \log_2(\frac{1}{\varepsilon}) \rfloor$. Применяя лемму 13, мы получаем цепочку неравенств

$$\begin{aligned} |k N_{n-1} A^{n-1}| &\geq |N_{n-1} A^{n-1}|^{2^{1-k}} |N_{n-1} A^{n-1} - N_{n-1} A^{n-1}|^{1-2^{1-k}} \\ &\geq \frac{1}{2^{r+1}} |A|^{n-1-\frac{8}{7} \cdot 2^{1-k}} \geq \frac{1}{2^{r+1}} |A|^{n-1-\varepsilon}. \end{aligned}$$

Вводя новый параметр $r_1 = \lfloor \frac{r+1}{\log_2 3-1} \rfloor + 1$ и используя лемму 26, имеем

$$|2^{r_1} k N_{n-1} A^{n-1}| \geq \min \left\{ \left(\frac{3}{2} \right)^{r_1} |k N_{n-1} A^{n-1}|, q \right\}.$$

Если $(\frac{3}{2})^{r_1} |kN_{n-1}A^{n-1}| \geq q$, то $2^{r_1} kN_{n-1}A^{n-1} = \mathbb{F}_q$, и теорема доказана. Если $(\frac{3}{2})^{r_1} |kN_{n-1}A^{n-1}| < q$, то $|2^{r_1} kN_{n-1}A^{n-1}| |A|^{n-\varepsilon} > q$ и из леммы 1 получаем

$$10 \cdot 2^{r_1} kN_{n-1}A^n = \mathbb{F}_q.$$

Случай 2. Имеем $n_0 < n - 1$. Используя леммы 28, 29, получаем

$$\begin{aligned} |N_{n-1}A^{n-1} - N_{n-1}A^{n-1}| &\geq \frac{1}{2^{r+2}}(q-1), \\ |N_{n-1}A^{n-1}| &\geq |N_{n_0}A^{n_0}| \geq \frac{1}{2^{r+1}}|A|^{n_0-\frac{8}{7}} \geq \frac{1}{2^{r+2}}(q-1)|A|^{-\frac{15}{7}}. \end{aligned}$$

Применяя лемму 13, находим:

$$|3N_{n-1}A^{n-1}| \geq \frac{1}{2^{r+2}}(q-1)|A|^{-\frac{15}{28}}.$$

Введем новый параметр $r_2 = [\frac{r+2}{\log_2 3-1}] + 1$. Используя лемму 26, мы видим, что

$$|3 \cdot 2^{r_2} N_{n-1} A^{n-1}| \geq \min \left\{ \left(\frac{3}{2} \right)^{r_2} |3N_{n-1}A^{n-1}|, q \right\}.$$

Если $(\frac{3}{2})^{r_2} |3N_{n-1}A^{n-1}| \geq q$, то $3 \cdot 2^{r_2} N_{n-1}A^{n-1} = \mathbb{F}_q$, и теорема доказана. Если $(\frac{3}{2})^{r_2} |3N_{n-1}A^{n-1}| < q$, то $|3 \cdot 2^{r_2} N_{n-1}A^{n-1}| |A| > (q-1)|A|^{\frac{13}{28}}$. Из соотношений (43) и (44) следуют неравенства $q-1 > \frac{1}{2}q$ и $|A|^{\frac{13}{28}} > 2$, из которых мы выводим, что $|3 \cdot 2^{r_2} N_{n-1}A^{n-1}| |A| > q$. Применяя лемму 1, получаем равенство

$$30 \cdot 2^{r_2} N_{n-1}A^n = \mathbb{F}_q.$$

Теорема доказана полностью.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 5. Утверждение теоремы для случая $n = 2$ следует из леммы 1, а если $n \geq 4$ – из теоремы 4. Осталось доказать теорему при $n = 3$.

Заметим сначала, что $\dim(A - A) \geq 2$, так как в противном случае имеем $|A| \leq |A - A| \leq p$, но это противоречит условию $|A| > p^{\frac{4}{3-\varepsilon}}$. Из соотношения $\dim(A - A) \geq 2$ следует, что $Q[A, A] \not\subseteq \mathbb{F}_p$, и согласно леммам 7, 8 неравенства $\dim(lA^2) \geq 3$ и $\dim(lA^2 - lA^2) \geq 3$ верны для любого натурального $l \geq 2$.

Если $|A|^2 \geq \frac{p^3}{3}$, то из предложения 2 вытекает соотношение

$$|3A^2 - 3A^2| \geq \frac{|A|^2(\frac{p^2(p-1)}{2} + p)}{|A|^2 + \frac{p^2(p-1)}{2} + p} \geq \frac{|A|^2 \frac{p^3}{3}}{|A|^2 + \frac{p^3}{3}} \geq \frac{p^3}{6}.$$

Используя лемму 13, мы видим, что

$$|12A^2| \geq |3A^2|^{\frac{1}{8}} |3A^2 - 3A^2|^{\frac{7}{8}} \geq \frac{1}{6^{\frac{7}{8}}} p^{3-\frac{1}{4}}.$$

Согласно лемме 14 либо имеет место оценка $|16 \cdot 12A^2| > 5|12A^2| > p^{3-\frac{1}{4}}$, либо существуют элемент $b \in \mathbb{F}_{p^4}$ и аддитивная подгруппа $G \subseteq \mathbb{F}_{p^4}$ такие, что $16 \cdot 12A^2 = 16b + G$. В первом случае при $p \geq 11$ выполнено неравенство $|192A^2| |A| > \frac{1}{\sqrt{3}} p^{3-\frac{1}{4}+\frac{3}{2}} > p^4$. Теперь, используя лемму 1, мы получим соотношение $1920A^3 = \mathbb{F}_{p^4}$. Во втором случае если $G = \mathbb{F}_{p^4}$, то верно

равенство $192A^2 = \mathbb{F}_{p^4}$, а если $G \subsetneq \mathbb{F}_{p^4}$, то, используя доказанную оценку $\dim(192A^2 - 192A^2) = \dim(G) \geq 3$, мы видим, что $|192A^2| = p^3$ и при $p \geq 11$ верно неравенство $|192A^2||A| > \frac{1}{\sqrt{3}}p^{4+\frac{1}{2}} > p^4$. Применяя лемму 2 (множество $192A^2$ симметрично, если $16b \in G$, и антисимметрично иначе), мы получим соотношение $1536A^3 = \mathbb{F}_{p^4}$. Если $p < 11$, то согласно лемме 9 выполнено равенство $2400A^3 = \mathbb{F}_{p^4}$. Объединив полученные тождества, мы завершаем рассмотрение случая $|A|^2 \geq \frac{p^3}{3}$.

Если $|A|^2 < \frac{p^3}{3}$, то из предложения 2 вытекает соотношение

$$|3A^2 - 3A^2| \geq \frac{|A|^2(\frac{p^2(p-1)}{2} + p)}{|A|^2 + \frac{p^2(p-1)}{2} + p} \geq \frac{|A|^2 \frac{p^3}{3}}{|A|^2 + \frac{p^3}{3}} \geq \frac{|A|^2}{2}.$$

Определим параметр $l_0 = 2 + [\log_2 \frac{1}{\varepsilon}]$. Используя лемму 13, мы видим, что

$$|3l_0A^2| \geq |3A^2|^{\frac{1}{2^{l_0-1}}} |3A^2 - 3A^2|^{\frac{1}{2^{l_0-1}}} \geq \frac{1}{2} |A|^{2-\frac{1}{2^{l_0-1}}} \geq \frac{1}{2} |A|^{2-\varepsilon}.$$

Согласно лемме 14 либо имеет место оценка $|12l_0A^2| > 2|3l_0A^2|$, либо существуют элемент $b \in \mathbb{F}_{p^4}$ и аддитивная подгруппа $G \subseteq \mathbb{F}_{p^4}$ такие, что $12l_0A^2 = 4b + G$. В первом случае выполнено неравенство $|12l_0A^2||A| > |A|^{3-\varepsilon} > p^4$. Теперь, используя лемму 1, мы получим соотношение $120l_0A^3 = \mathbb{F}_{p^4}$.

Пусть существуют элемент $b \in \mathbb{F}_{p^4}$ и аддитивная подгруппа $G \subseteq \mathbb{F}_{p^4}$ такие, что $12l_0A^2 = 4b + G$. Если $G = \mathbb{F}_{p^4}$, то верно равенство $12l_0A^2 = \mathbb{F}_{p^4}$. Если $G \subsetneq \mathbb{F}_{p^4}$, то, используя доказанную оценку $\dim(12l_0A^2 - 12l_0A^2) = \dim(G) \geq 3$, мы видим, что $|12l_0A^2| = p^3$ и верно неравенство $|12l_0A^2||A| > p^{3+\frac{4}{3-\varepsilon}} > p^4$. Применяя лемму 2 (множество $12l_0A^2$ симметрично, если $4b \in G$, и антисимметрично иначе), мы получим тождество $96l_0A^3 = \mathbb{F}_{p^4}$. Объединяя последние равенства, мы завершаем доказательство теоремы.

Список литературы

1. Г. Дэвенпорт, *Высшая арифметика. Введение в теорию чисел*, Наука, М., 1965; пер. с англ.: H. Davenport, *The higher arithmetic. An introduction to the theory of numbers*, Hutchinson's Univ. Library, London; Longmans, New York, 1952.
2. Д. Гильберт, *Избранные труды*, в 2-х т., Факториал, М., 1998; пер. с нем.: D. Hilbert, *Gesammelte Abhandlungen*, Springer-Verlag, Berlin-Heidelberg-New York, 1970.
3. Ю. В. Линник, "Элементарное решение проблемы Waring'a по методу Шнирельмана", *Матем. сб.*, **12(54)**:2 (1943), 225–230.
4. L. E. Dickson, *Researches on Waring's problem*, Carnegie Inst. of Washington Publ., Washington, 1935.
5. S. Pillai, "Waring's problem. V. On $g(6)$.", *J. Indian Math. Soc. (N.S.)*, **2** (1937), 213–214.
6. G. H. Hardy, J. E. Littlewood, "Some problems of "Partitio Numerorum". VI. Further researches in Waring's problem", *Math. Z.*, **23**:1 (1925), 1–37.
7. И. М. Виноградов, *Избранные труды*, Изд-во АН СССР, М., 1952; англ. пер.: I. M. Vinogradov, *Selected works*, Springer-Verlag, Berlin, 1985.
8. И. М. Виноградов, "К вопросу о верхней границе для $G(n)$ ", *Изв. АН СССР. Сер. матем.*, **23**:5 (1959), 637–642.

9. А. А. Карацуба, “О функции $G(n)$ в проблеме Варинга”, *Изв. АН СССР. Сер. матем.*, **49**:5 (1985), 935–947; англ. пер.: А. А. Karatsuba, “On the function $G(n)$ in Waring’s problem”, *Math. USSR-Izv.*, **27**:2 (1986), 239–249.
10. R. C. Vaughan, T. D. Wooley, “On Waring’s problem: some refinements”, *Proc. London Math. Soc.* (3), **63**:1 (1991), 35–68.
11. Р. Вон, *Метод Харди–Литтлвуда*, Мир, М., 1985; пер. с англ.: R. C. Vaughan, *The Hardy–Littlewood method*, Cambridge Tracts in Math., **80**, Cambridge Univ. Press, Cambridge–New York, 1981.
12. T. D. Wooley, “Large improvements in Waring’s problem”, *Ann. of Math.* (2), **135**:1 (1992), 131–164.
13. D. Hilbert, “Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n^{ter} Potenzen (Waringsches Problem)”, *Math. Ann.*, **67**:3 (1909), 281–300.
14. E. Kamke, “Verallgemeinerungen des Waring–Hilbertschen Satzes”, *Math. Ann.*, **83**:1–2 (1921), 85–112.
15. К. К. Марджанишвили, “Об одновременном представлении n чисел суммами полных первых, вторых, ..., n -х степеней”, *Изв. АН СССР. Сер. матем.*, **1**:4 (1937), 609–631.
16. К. К. Марджанишвили, “О некоторых нелинейных системах уравнений в целых числах”, *Матем. сб.*, **33(75)**:3 (1953), 639–675.
17. И. М. Виноградов, “Некоторые проблемы аналитической теории чисел”, *Тр. третьего Всесоюзного матем. съезда* (Москва, 1956), М., 1958, 3–13.
18. А. А. Карацуба, “Об одной системе сравнений”, *Матем. заметки*, **19**:3 (1976), 389–392; англ. пер.: А. А. Karatsuba, “A system of congruences”, *Math. Notes*, **19**:3 (1976), 237–239.
19. Г. И. Архипов, “О значении особого ряда в проблеме Гильберта–Камке”, *Докл. АН СССР*, **259**:2 (1981), 265–267; англ. пер.: G. I. Arkhipov, “On the value of the singular series in the Hilbert–Kamke problem”, *Soviet Math. Dokl.*, **24** (1981), 49–51.
20. Г. И. Архипов, “О проблеме Гильберта–Камке”, *Изв. АН СССР. Сер. матем.*, **48**:1 (1984), 3–52; англ. пер.: G. I. Arkhipov, “On the Hilbert–Kamke problem”, *Math. USSR-Izv.*, **24**:1 (1985), 1–47.
21. В. Н. Чубариков, “Об асимптотических формулах для интеграла И. М. Виноградова и его обобщений”, *Теория чисел, математический анализ и их приложения*, Тр. МИАН СССР, **157**, Наука, М., 1981, 214–232; англ. пер.: V. N. Chubarikov, “On asymptotic formulas for an integral of I. M. Vinogradov and its generalizations”, *Proc. Steklov Inst. Math.*, **157** (1983), 229–248.
22. Л. Г. Шнирельман, “Об аддитивных свойствах чисел”, *УМН*, 1940, № 7, 7–46.
23. H. B. Mann, “A proof of the fundamental theorem on the density of sums of set of positive integers”, *Ann. of Math.* (2), **43**:3 (1942), 523–527.
24. А. А. Карацуба, “Правильные множества по заданному модулю”, *Acta Math. Inform. Univ. Ostraviensis*, **6**:1 (1998), 129–134.
25. J. Bourgain, N. Katz, T. Tao, “A sum-product estimate in finite fields, and applications”, *Geom. Funct. Anal.*, **14**:1 (2004), 27–57.
26. M. Rudnev, *An improved estimate on sums of product sets*, arXiv:abs/0805.2696.
27. A. Glibichuk, *Additive properties of product sets in an arbitrary finite field*, arXiv:abs/0801.2021.
28. А. А. Глибичук, S. V. Konyagin, “Additive properties of product sets in fields of prime order”, *Additive combinatorics* (Montreal, 2006), CRM Proc. Lecture Notes, **43**, Amer. Math. Soc., Providence, RI, 2007, 279–286; arXiv:math/0702729.
29. А. А. Глибичук, “Аддитивные свойства произведений подмножеств поля $\mathbb{F}_{p^2}$ ”, *Вестн. Моск. ун-та. Сер. 1. Матем., мех.*, **64**:1 (2009), 3–8; англ. пер.: А. А. Glibichuk, “Additive properties of product sets in the field $\mathbb{F}_{p^2}$ ”, *Moscow Univ. Math. Bull.*, **64**:1 (2009), 1–6.

30. А. А. Глибичук, *Свойства степеней больших подмножеств в поле из p^3 элементов*, деп. в ВИНТИ 769-B2008.
31. J. Bourgain, M.-Ch. Chang, “A Gauss sum estimate in arbitrary finite fields”, *C. R. Math. Acad. Sci. Paris*, **342**:9 (2006), 643–646.
32. P. Erdős, E. Szemerédi, “On sums and products of integers”, *Studies in pure mathematics*, Birkhäuser, Basel, 1983, 213–218.
33. J. Solymosi, “Bounding multiplicative energy by the sumset”, *Adv. Math.*, **222**:2 (2009), 402–408.
34. И. М. Виноградов, *Основы теории чисел*, РХД, М.–Ижевск, 2005.
35. N. H. Katz, Ch.-Y. Shen, “Garaev’s inequality in finite fields not of prime order”, *Online J. Anal. Comb.*, 2008, № 3, Art. 3.
36. J. Bourgain, A. A. Glibichuk, S. V. Konyagin, “Estimates for the number of sums and products and for exponential sums in fields of prime order”, *J. London Math. Soc.* (2), **73**:2 (2006), 380–398.
37. D. A. Burgess, P. D. T. A. Elliott, “The average of the least primitive root”, *Mathematika*, **15** (1968), 39–50.
38. А. А. Карацуба, *Основы аналитической теории чисел*, 2-е изд., Наука, М., 2004.
39. T. Tao, V. H. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., **105**, Cambridge Univ. Press, Cambridge, 2006.
40. А. А. Глибичук, “Комбинаторные свойства множеств вычетов по простому модулю и задача Эрдеша–Грэхэма”, *Матем. заметки*, **79**:3 (2006), 384–395; англ. пер.: А. А. Glibichuk, “Combinatorial properties of sets of residues modulo a prime and the Erdős–Graham problem”, *Math. Notes*, **79**:3–4 (2006), 356–365.
41. M. Kneser, “Abschätzung der asymptotischen Dichte von Summenmengen”, *Math. Z.*, **58**:1 (1953), 459–484.
42. T. Cochrane, C. Pinner, “Sum-product estimates applied to Waring’s problem mod p ”, *Integers*, **8**:1 (2008), A46.

А. А. Глибичук (А. А. GLIBICHUK)
Московский государственный университет
им. М. В. Ломоносова
E-mail: aanatol@mail.ru

Поступило в редакцию
18.12.2008
31.10.2009