МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В.ЛОМОНОСОВА

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи
УДК 511.235.1

Глибичук Алексей Анатольевич

СВОЙСТВА СУММ И ПРОИЗВЕДЕНИЙ ПОДМНОЖЕСТВ ПРОИЗВОЛЬНОГО КОНЕЧНОГО ПОЛЯ

01.01.06 - математическая логика, высшая алгебра и теория чисел

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва 2009

Работа выполнена на кафедре общих проблем управления Механико-Математического факультета Московского государственного университета имени М. В. Ломоносова.

Научный руководитель:	доктор физико–математических наук, профессор Сергей Владимирович Конягин
Официальные оппоненты:	доктор физико–математических наук, профессор Сергей Александрович Степанов
	кандидат физико–математических наук, старший научный сотрудник Максим Александрович Королёв
Ведущая организация:	Хабаровское отделение института прикладной математики Дальневосточного отделения Российской Академии Наук

Защита диссертации состоится 17 апреля 2009 г. в 16 ч. 45 м. на заседании диссертационного совета Д.501.001.84 при Московском государственном университете имени М. В. Ломоносова по адресу: Российская Федерация, 119991, Москва, ГСП-1, Ленинские горы, д. 1, МГУ, Механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в библиотеке механико-математического факультета МГУ (Главное здание, 14 этаж).

Автореферат разослан 30 марта 2009 г.

Ученый секретарь
диссертационного совета
Д.501.001.84 при МГУ
доктор физико-математических наук,
профессор А. О. Иванов

Общая характеристика работы

Актуальность темы.

Задачи, рассматриваемые в диссертации, относятся к быстро развивающемуся в настоящее время разделу математики — аддитивной комбинаторике. Большое количество результатов, полученных в этой области, обусловлено разнообразием методов, используемых при их изучении. Вопросы, исследуемые в работе, так или иначе связаны с обобщением проблемы Варинга для конечных полей и с задачами изучения роста суммы и произведения подмножеств в этих полях.

Гипотеза, называемая сейчас проблемой Варинга, была высказана им в 1770 г. Она формулируется так: доказать, что для любого натурального $n \geqslant 2$ существует число $s(n)$ с тем свойством, что всякое натуральное число представимо в виде суммы n-х степеней натуральных чисел, причем количество слагаемых не превосходит $s(n)$. Многие математики занимались этой проблемой и задачами, с нею связанными. Среди обширной литературы, посвященной проблеме Варинга и ее обобщениям, следует упомянуть работы Д.Гильберта[1], Ю.В. Линника[2], Л. Диксона[3], С. Пиллаи[4],Г. Харди и Д. Литтлвуда[5], И.М. Виноградова[6], А.А. Карацубы[7], Р. Вона[8] и Т. Вули[9]. Методы, предложенные в этих работах, зачастую использовались в других задачах и легли в основание новых математических теорий.

Определение 1. Рассмотрим произвольное полукольцо R. Множество $A \subseteq R$ является базисом R порядка $k \in \mathbb{N}$, если каждый элемент $x \in R$ представим в виде $x_1 + x_2 + \ldots + x_k = x$, где $x_1, x_2, \ldots, x_k \in A$, но существует такой элемент $x_0 \in R$, что $x_1 + x_2 + \ldots + x_{k-1} \neq x_0$ для любых $x_1, x_2, \ldots, x_{k-1} \in A$.

Таким образом, проблема Варинга может быть переформулирована следующим образом: для любого натурального n найдется такое число $s(n)$, что множество n-х степеней целых неотрицательных чисел образует базис порядка, не превосходящего $s(n)$, в полукольце целых неотрицательных чисел.

---

[1] Д. Гильберт, *Избранные труды в двух томах*, 1998, Москва, Факториал, с. 312 — 328.

[2] Ю.В. Линник, *Элементарное решение проблемы Waring'а по методу Шнирельмана*, Матем. сб., т. 12(54), 1943, вып. 2, стр. 225 — 230

[3] L.E. Dickson, *Researches on Waring's problem*, Carnegie Inst. of Washington Publications, vol. 464, 1936.

[4] S. Pillai , *On Waring's problem*, Journal of Indian Math. Soc., ser. 2, vol. 2, 1937, pp. 213 — 214.

[5] G.H. Hardy, J.E. Littlewood, *A new solution of Waring's problem*, Q.J. Math., vol. 48, 1919, pp. 272 — 293.

[6] И.М. Виноградов, *К вопросу о верхней границе для $G(n)$*, Изв. РАН СССР, сер. матем., т. 23, 1959, вып. 5, стр. 637—642.

[7] А.А. Карацуба, *О функции $G(n)$ в проблеме Варинга*, Изв. АН СССР. Сер. матем., т. 49, 1985, вып. 5, стр. 935—-947.

[8] Р. Вон, *Метод Харди-Литтлвуда*, Москва, Мир, 1985.

[9] T. D. Wooley, *Large improvements in Waring's problem*, Ann. of Math., vol. 135, 1992, no. 1, pp. 131—164.

Если $\mathbb{F}_q$ — поле порядка q, то множество n-х степеней ненулевых элементов $\mathbb{F}_q$ образует подгруппу порядка $\frac{q-1}{(q-1,n)}$ мультипликативной группы $\mathbb{F}_q^*$ поля. Поэтому для оценки числа слагаемых в проблеме Варинга достаточно оценить порядок базисности подгруппы $H \subseteq \mathbb{F}_q^*$. Такие оценки хорошо известны, если $|H|$ существенно больше $\sqrt{q}$. Используя метод С. А. Степанова[10] можно получить нетривиальные оценки тригонометрических сумм[11] по подгруппам $\mathbb{F}_p^*$ для простого p и вывести из них нетривиальные оценки порядка базисности этой подгруппы, если ее мощность существенно больше $p^{\frac{1}{4}}$. Известна также задача исследования базисных свойств подмножеств конечных полей, более общих, чем подгруппы, а именно, множеств последовательных степеней фиксированного элемента поля.[12]

Известно, что в поле $\mathbb{F}_p$ для фиксированных $k \in \mathbb{N}$ и $\varepsilon > 0$ случайно сгенерированное множество мощности $> p^{\frac{1}{k}+\varepsilon}$ является базисом порядка k с большой вероятностью (стремящейся к 1 при $p \to \infty$). А.А. Карацуба[13] строит конструктивные примеры базисов мощности, близкой к оптимальной, в кольце вычетов по модулю степени простого числа.

Недавний прогресс в исследовании базисных свойств относительно небольших специфических подмножеств конечных полей связан с появлением оценок сумм и произведений подмножеств таких полей. Вначале аналогичные оценки рассматривались для конечных подмножеств множества натуральных и действительных чисел.

Если A и B — подмножества конечного поля, то можно рассмотреть две операции: сложение $A + B := \{a + b : a \in A, b \in B\}$ и умножение $A \cdot B = A \cdot B := \{ab : a \in A, b \in B\}$. Определим для некоторого $k \in \mathbb{N}$ и множества A его кратную сумму $kA = \underbrace{A + A \ldots + A}_{k}$ и k-ю степень этого подмножества $A^k = \underbrace{A \cdot A \cdot \ldots \cdot A}_{k}$. Гипотеза П. Эрдеша и Э. Семереди[14] утверждает, что для любого конечного непустого подмножества $A \subset \mathbb{N}$ и

[10] С. А. Степанов, *О числе точек гиперэллиптической кривой над простым конечным полем*, Известия РАН СССР.Серия математическая, т. 33, 1969, стр. 1171 — 1181.

[11] С. В. Конягин, *Оценки тригонометрических сумм по подгруппам и суммы Гаусса*, IV международная конференция «Современные проблемы теории чисел их приложения».Актуальные проблемы.Часть III, стр. 86 — 114.

[12] И.Д. Шкредов, *О некоторых аддитивных задачах, связанных с показательной функцией*, Успехи мат. наук., т. 58., вып. 4, 2003, стр. 165 — 166.

Z. Rudnick, A. Zaharescu, *The distribution of spaces between small powers of a primitive root*, Israel Journal of Math., vol. 120, 2000, pp. 271 — 287.

M. Vâjâitu, A. Zaharescu, *Differences between powers of a primitive root*, International Journal of Mathematical Sciences, vol. 29, 2002, pp. 325 — 331.

[13] А.А. Карацуба, *Правильные множества по заданному модулю*, Acta Matem. Et. Informat., Univ. Ostraviensis, 1998, v. 6, p. 129—-134.

[14] P. Erdős, E. Szemerédi, *On sums and products of integers*, Studies in Pure Mathematics, Birkhauser, Basel, 1983, pp. 213 — 218.

произвольного действительного числа $\varepsilon > 0$ верно неравенство:

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

В той же работе доказано, что $\max\{|A \cdot A|, |A + A|\} \geqslant c|A|^{1+\delta}, c > 0$ для некоторого $\delta > 0$. Позже была получена версия последнего неравенства с точными константами, которые в ряде работ последовательно улучшались. Наилучшая в настоящий момент оценка доказана И. Шолумоши[15]. Она имеет вид: $\max\{|A \cdot A|, |A + A|\} \geqslant |A|^{\frac{4}{3}-\varepsilon}$, где $\varepsilon > 0$ — произвольное действительное число, и верна также для конечных подмножеств множества комплексных чисел. Аналогичных теорем для конечных колец не было до работы Ж. Бургена, Н. Катца и Т. Тао[16], которые показали, что, если A — подмножество поля порядка p для некоторого простого p, удовлетворяющее условию $p^\delta < |A| < p^{1-\delta}$, где $\delta > 0$ — произвольное действительное число, то $\max\{|A \cdot A|, |A + A|\} > c|A|^{1+\alpha}$, причем константы c и α зависят только от δ. Затем Ж. Бурген и С. В. Конягин[17] (вторая работа выполнена в соавторстве с диссертантом) получили аналогичную оценку, предполагая, что A удовлетворяет более слабому условию: $|A| < p^{1-\delta}$ для некоторого действительного $\delta > 0$. Из результата этих статей вытекает, что порядок базисности мультипликативной подгруппы $H \subseteq \mathbb{F}_p^*, |H| > p^\delta$, ограничена сверху величиной, зависящей только от δ. Аналогичные вопросы для подгрупп произвольных конечных полей оставались открытыми.

В ряде работ Ж. Бургена[18] получены обобщения теоремы о суммах и произведениях подмножеств и найдены многочисленные приложения этих результатов к задачам оценивания модулей различных тригонометрических сумм, проблемам p - адической теории, алгебраической теории чисел, криптографии и другим разделам математики. Х. Хельфготт[19] использует неравенства на суммы и произведения подмножеств для получения оценок на диаметр графа Кэли. Оценки на α в неравенстве для сумм и произведений

[15] J. Solymosi, *Bounding multiplicative energy by the sumset*, arXiv:0806. 1040v3, math.CO.

[16] J. Bourgain, N. Katz, T. Tao, *A sum-product estimate in finite fields and their applications*, Geom and Funct. Anal., vol. 14, 2004, pp. 27—57.

[17] J. Bourgain, S.V. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, C. R. Math. Acad. Sci. Paris, vol. 337, 2003, no. 2, pp. 75–80.

J. Bourgain, A. Glibichuk, S. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, Journal of London Math. Society, vol. 73, N.2, 2006, pp. 380 — 398.

[18] J. Bourgain, *Multilinear exponential sums in prime fields under optimal entropy conditions on the sources*, to appear in Geom and Funct. Anal.

J. Bourgain, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc., vol. 18, 2005, pp. 477 — 499.

J. Bourgain, *More on the sum-product phenomenon in prime fields and its applications, International Journal of Number Theory*, vol. 1, no. 1, 2005, pp. 1 — 32.

J. Bourgain, *Estimates on exponential sums related to the Diffie-Hellman distributions*, GAFA, vol. 15, 2005, pp. 1 — 34.

[19] H.A. Helfgott, *Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$*, Annals of Mathematics, ser. 2, vol. 167, no. 2, 2008, pp. 601 —- 623.

были улучшены в работах Гараева[20], Катца и Шена[21].

Методы, разработанные в статье Ж. Бургена, Н. Катца и Т. Тао, выявляют взаимосвязь проблемы Эрдеша-Семереди для конечных полей с задачей о базисных свойствах множества произведений ограниченного количества элементов подмножества A конечного поля. Последняя задача является основным объектом исследования настоящей работы. 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[22] нетрудно получить, что множество попарных произведений элементов множества A образует базис, порядок которого не превосходит некоторого числа, зависящего только от ε. Если же множество A имеет меньшую мощность, то для исследования базисных свойств множеств $A \cdot A, A \cdot A \cdot A, \ldots$ приходится использовать методы и результаты работ, связанных с суммами и произведениями подмножеств конечных полей. Данная работа продолжает упомянутые исследования.

Цель работы.

Цель настоящей работы — исследовать базисные свойства множества произведений ограниченного количества элементов из подмножества конечного поля при минимальных ограничениях на его мощность и структуру, и в частности, множества последовательных степеней фиксированного элемента.

Научная новизна.

В диссертации решены следующие новые задачи:

1. Доказано, что любой элемент конечного поля представим в виде суммы не более 16 слагаемых из произведения двух больших подмножеств этого поля.

2. Доказано, что в поле $\mathbb{F}_p$, где p — простое число, произведение произвольного количества множеств при минимальном ограничении на их мощность является базисом ограниченного порядка.

---

[20] M. Z. Garaev, *The sum-product estimate for large subsets of prime fields*, Proc. Amer. Math. Soc., vol. 136, no. 8, 2008, pp. 2735–2739.

M. Z. Garaev, *An explicit sum-product estimate in $\mathbb{F}_p$ for subsets of incomparable sizes*, The Electronic Journal of Combinatorics, vol. 15, 2008, $\#R$ 58.

M. Z. Garaev, *An explicit sum-product estimate in $\mathbb{F}_p$,* Int. Math. Res. Not. IMRN, no. 11, Art. ID rnm035, 2007, 11 pp.

[21] N. H. Katz, Ch.-Y. Shen, *A slight improvement to Garaev's sum product estimate*, Proc. Amer. Math. Soc., vol. 136 , no. 7, 2008, pp. 2499–2504.

N. H. Katz, Ch.-Y. Shen, *Garaev's inequality in finite fields not of prime order*, Online J. Anal. Comb., No. 3, Art. 3, 2008, 6 pp.

[22] Виноградов И. М., *Основы теории чисел*, Москва-Ижевск, НИЦ "Регулярная и хаотическая динамика", 2005, стр. 103, упражнение 8α.

3. Доказано, что произвольная степень подмножества конечного поля при минимальных ограничениях на его мощность и структуру является базисом, порядок которого может быть оценен числом, не зависящим от характеристики этого поля.

Основные методы исследования.

В работе используются методы арифметической комбинаторики, теории полей и линейной алгебры.

Теоретическая и практическая ценность работы.

Диссертация носит теоретический характер. Изложенные в диссертации методы и доказанные результаты представляют интерес для специалистов по теории чисел, комбинаторики и алгебры, о чем свидетельствует уже появившиеся приложения идей работы.

Апробация работы.

Результаты диссертации докладывались на следующих научно - исследовательских семинарах и конференциях:

1. Кафедральный семинар кафедры теории чисел под руководством д.ф.-м.н., чл.-корр. РАН Ю.В. Нестеренко и д.ф.-м.н., профессора Н. Г. Мощевитина.

2. Семинар «Аналитическая теория чисел» под руководством д.ф.-м.н., проф. А.А. Карацубы.

3. Научно-исследовательский семинар по алгебре, проводимый кафедрой высшей алгебры МГУ им. Ломоносова.

4. Семинаре по теории функций под руководством к.ф.-м.н., доц. В.Б. Демидовича, д.ф.-м.н., проф. С.В.Конягина и к.ф.-м.н., доц. А.С. Кочурова — неоднократно, по мере получения результатов.

5. Международная конференция по аддитивной комбинаторике (Монреаль, Канада, 6 — 12 апреля 2006 г.).

6. Международная конференция «Clay-Fields Conference on Additive Combinatorics, Number Theory, and Harmonic Analysis» (Торонто, Канада, 5 — 13 апреля 2008г.).

7. Специальная программа по арифметической комбинаторике, проходившей в Институте Высших Исследований(Принстон, США, 23 сентября — 23 декабря 2007г.).

Публикации.

Основное содержание диссертации было опубликовано в четырех работах, список которых приведен в конце автореферата [1] — [4].

Структура и объем диссертации.

Диссертация состоит из введения и 5 глав и списка литературы. Полный объем диссертации — 84 страницы, библиография включает 68 наименований.

Краткое содержание работы

Во введении обсуждаются предварительные сведения и формулируются основные определения. Через $|X|$ обозначается мощность множества X. Если $q = p^r$ является степенью простого числа p, то $\mathbb{F}_q$ обозначает поле из q элементов. Для множеств $X, Y \subset \mathbb{F}_q$ и натурального k вводятся обозначения

$$XY = \{xy : x \in X,\, y \in Y\},$$

$$X^k = \{x_1 \dots x_k : x_1, \dots, x_k \in X\},$$
$$kX = \{x_1 + \dots + x_k : x_1, \dots, x_k \in X\}.$$

Множество $A \subset \mathbb{F}_q$ названо особым, если оно покрывается каким-либо множеством вида $\{ds : s \in S\}$, где $d \in \mathbb{F}_q$, S — собственное подполе поля $\mathbb{F}_q$, и неособым в противном случае. *Мультипликативный порядок* $\mathrm{ord}_q x$ произвольного элемента $x \in \mathbb{F}_q \setminus \{0\}$ определяется как наименьшее натуральное l такое, что $x^l = 1$.

Содержание главы 1.

В первой главе мы обсуждаем предварительные сведения и формулируем основные определения. В параграфе 1.1 определяется размерность произвольного подмножества конечного поля и доказывается нижняя оценка на размерность степени неособого подмножества. Также устанавливаются структура подмножеств $X, Y \subset \mathbb{F}_q$, удовлетворяющих условию $|X+Y| = |X|$, где символ $|X|$ обозначает мощность подмножества X. В параграфе 1.2 доказываются основные оценки сумм-произведений, которые можно вывести, используя свойства множества отношений разностей. Здесь также доказано, что для данного неособого подмножества $X \subseteq \mathbb{F}_q, q = p^r$, его степень X^r является базисом порядка, не превышающего $q - 1$. Легко понять, что любая степень особого подмножества не может быть базисом. В параграфе 1.3 формулируются классические оценки на сумму произвольных подмножеств: неравенство Коши-Давенпорта, неравенство треугольника Ружи и неравенство Кнессера. Кроме того, доказывается две оценки на сумму подмножеств, использующиеся в доказательстве ряда результатов работы.

Содержание главы 2.

Назовем множество X симметричным, если оно вместе с каждым своим элементом x содержит элемент $-x$, и антисимметричным, если из включения $x \in X$ следует, что $-x \notin X$. Во параграфе 2.1 доказываются такие утверждения.

Теорема 1. *Если $X \subseteq \mathbb{F}_q$ и $Y \subseteq \mathbb{F}_q$ таковы, что Y антисимметрично и $|X||Y| > q$, то $8(XY) = \mathbb{F}_q$.*

Теорема 2. *Рассмотрим подмножества $X \subseteq \mathbb{F}_q$ и $Y \subseteq \mathbb{F}_q$ такие, что Y симметрично. Если выполнено неравенство $|X||Y| > q$, то $8(XY) = \mathbb{F}_q$.*

Из теорем 1 и 2 выводятся такие следствия.

Следствие 1. *Если H - мультипликативная подгруппа $\mathbb{F}_q \setminus \{0\}$, $|H| > \sqrt{q}$, то $8H = \mathbb{F}_q$.*

Следствие 2. *Пусть $A = \left\{g^x : x \in \mathbb{N}, 0 \leq x \leq 2[\sqrt{q}]\right\}$, где $g \in \mathbb{F}_q \setminus \{0\}$ — некоторый элемент такой, что $\mathrm{ord}_q g > \sqrt{q}$. Тогда $8A = \mathbb{F}_q$.*

Кроме того, в этом параграфе устанавливается, что условие $|X||Y| > q$ в теоремах 1 и 2 является неулучшаемым. В параграфе 2.2 из этих теорем выводятся такие результаты.

Теорема 3. *Если $X \subseteq \mathbb{F}_q \setminus \{0\}$ — произвольное подмножество такое, что $|X| > \left(\frac{1}{4} + \frac{\sqrt{17}}{4}\right)\sqrt{q}$, то $8(X^2) = \mathbb{F}_q$.*

Теорема 4. *Рассмотрим произвольные подмножества $X, Y \subseteq \mathbb{F}_q$ такие, что $|X||Y| > q$. Тогда выполнено равенство $16(XY) = \mathbb{F}_q$.*

Теорема 4 была улучшена М. Рудневым[23]. Он показал, что при тех же ограничениях на множества X и Y выполнено равенство $10(XY) = \mathbb{F}_q$. Следует отметить, что Д. Коверт[24], Д. Харт[25], А. Иосевич[26], Д. Кох, М. Руднев[27], И. Шолумоши, М. Гараев, В. Гарсиа и С.В. Конягин[28] в своих работах находят различные приложения теоремы 4 к ряду вопросов, в частности к задаче

[23]M. Rudnev, *An improved estimate on sums of product sets*, arXiv:0805. 2696v1, math.CO.

[24]D. Covert, D. Hart, A. Iosevich, D. Koh, M. Rudnev, *Generalized incidence theorems, homogeneous forms, and sum-product estimates in finite fields*, arXiv: 0801.0728v2, math.CO.

[25]D. Hart, A. Iosevich, J. Solymosi, *Sum-product estimates in finite fields via Kloosterman sums*, IMRN, vol. 2007, 2007, article ID: rmn007.

[26]D. Hart, A. Iosevich, D. Koh, M. Rudnev, *Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture*, arXiv: 0707.3473v2, math.CA.

D. Hart, A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*, arXiv: 0705.4256v4, math.NT.

[27]M. Rudnev, *An improved estimate on sums of product sets*, arXiv:0805. 2696v1, math.CO.

[28]М. Гараев, В. Гарсиа, С.В. Конягин, *Проблема Варинга с τ–функцией Рамануджана*, Известия РАН. Серия математическая, т. 72, 2008, №1, стр. 39–50.

Эрдеша о расстояниях, задаче Эрдеша-Фалконера и проблеме Варинга с τ–функцией Рамануджана.

В параграфе 2.3 получается приложение теорем 1-4 к задаче Эрдеша-Грэхэма[29], который формулируется так: существует ли для любого $\varepsilon > 0$ такое $k(\varepsilon) \in \mathbb{N}$, что для любого достаточно большого простого p и для любого целого c существует $k \leq k(\varepsilon)$ попарно различных целых чисел x_i таких, что $1 \leqslant x_i \leqslant p^{\varepsilon}, i = 1, 2, \ldots, k$, и

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

где запись x_i^{-1} обозначает наименьшее положительное целое такое, что $x_i^{-1} x_i \equiv 1(mod\ \ p)$? Доказан такой результат.

Теорема 5. *Для любого $\varepsilon > 0$, для любого достаточно большого простого p и для любого класса вычетов $a(mod\ \ p)$ существует положительные попарно различные натуральные числа $x_1, \ldots, x_N \leqslant p^{\varepsilon}$, где $N = 8\left(\left[\frac{1}{\varepsilon} + \frac{1}{2}\right] + 1\right)^2$, такие, что*

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

Содержание главы 3.

В параграфе 3.1 доказываются оценки сумм-произведений, необходимые для доказательства основного результата главы 3. В параграфе 3.2 выводится основной результат, который формулируется следующим образом.

Теорема 6. *Для любых подмножеств $A_1, A_2, \ldots, A_n \subseteq \mathbb{F}_p, n \geqslant 2$, таких, что $|A_i| \geqslant 2, 1 \leqslant i \leqslant n$, и*

$$|A_1| \cdot |A_2| \cdot \ldots \cdot |A_n| > p^{1+\varepsilon}$$

для некоторого $\varepsilon > 0$, мы имеем

$$N(A_1 \cdot A_2 \cdot \ldots \cdot A_n) = \mathbb{F}_p,$$

где

$$N = \begin{cases} 10, & \text{если } n = 2; \\ 10 \cdot \max\left\{1, 24\left(\left[\log_2\left(\frac{1}{\varepsilon}\right)\right] + 1\right)\right\}, & \text{если } n = 3; \\ 16^{n-2} \cdot \max\{1120, 320(-11 - [\log_2(\varepsilon(n-2))])\}, & \text{если } n > 3. \end{cases}$$

Теорема 6 обобщает теорему 4 для поля $\mathbb{F}_p$.

[29]P. Erdős, R.L. Graham, *Old and new problems and results in combinational number theory*, Monograph. Enseign. Math., vol. 28, 1980.

Содержание главы 4.

В параграфе 4.1 выводится такой результат о базисных свойствах произвольной степени достаточно большого неособого подмножества конечного поля.

Теорема 7. *Для любого целого числа $n \geqslant 2$, для любых чисел $\varepsilon \in (0;1)$, любого простого p и любого неособого множества A такого, что $A \subseteq \mathbb{F}_{p^2}$, $|A| > p^{\frac{2}{n-\varepsilon}}$, мы имеем $N(A^n) = \mathbb{F}_{p^2}$, где*

$$N = \begin{cases} 10, & \text{если } n = 2; \\ \frac{5}{6}\left(5 \cdot 4^n - 32\right)\left(3 + \left[\log_2\left(\frac{1}{\varepsilon}\right)\right]\right), & \text{если } n \geqslant 3. \end{cases}$$

В параграфе 4.2 доказывается нижняя оценка на мощность множества $3(X^2) - 3(X^2)$ для любого неособого подмножества $X \subseteq \mathbb{F}_q$. В параграфе 4.3 получается нижняя граница на мощность множества $N_k X^k - N_k X^k$, где $X \subseteq \mathbb{F}_q, q = p^r$ и $N_k = \frac{5}{24}4^k - \frac{1}{3}, k \geqslant 3$. Основные результаты параграфов 4.2 и 4.3 используются в доказательствах всех последующих теорем. В параграфе 4.4 устанавливается такая теорема.

Теорема 8. *Рассмотрим произвольное неособое подмножество $A \subset \mathbb{F}_{p^3}$, такое, что $|A| \geqslant p^{\frac{3}{n-\varepsilon}}$ для некоторого натурального $n \geqslant 2$ и действительного $\varepsilon \in (0,1)$. Тогда имеет место соотношение:*

$$N(A^n) = \mathbb{F}_{p^3},$$

где

$$N = \begin{cases} 10, & \text{если } n = 2; \\ 120(2 + \left[\log_2\left(\frac{1}{\varepsilon}\right)\right]), & \text{если } n = 3; \\ \frac{5}{3}(5 \cdot 4^n - 32)\left(3 + \left[\log_2\left(\frac{1}{\varepsilon}\right)\right]\right), & \text{если } n \geqslant 4. \end{cases}$$

Из теорем 7 и 8 выводятся следствия, аналогичные следствиям 1 и 2.

Содержание главы 5.

В параграфе 5.1 доказывается, что произвольное неособое подмножество конечного поля в некоторой степени, зависящей только от его мощности, является базисом ограниченного порядка. А именно, установлен такой результат.

Теорема 9. *Дано произвольное неособое подмножество $A \subset \mathbb{F}_q$ такое, что $|A| > q^{\frac{1}{n-\varepsilon}}$ для некоторого $\varepsilon \in (0,1)$. Тогда выполнено равенство*

$$N(A^{2n-2}) = \mathbb{F}_q,$$

где

$$N = \begin{cases} 10, & \text{если } n = 2; \\ 6^{n-3}\max\left\{30 \cdot \left(3 + \left[\log_2\left(\frac{1}{\varepsilon}\right)\right]\right), 160 \cdot (1 + [\log_2 n])\right\}, & \text{если } n \geqslant 3. \end{cases}$$

Отметим, что показатель степени $2n-2$, вообще говоря, неулучшаем.

Из теоремы 9 выводятся такие следствия для множеств специального вида.

Следствие 3. *Для любой подгруппы по умножению $H \subseteq \mathbb{F}_q$, не лежащей ни в каком нетривиальном подполе $\mathbb{F}_q$ и удовлетворяющей условию $|H| > q^{\frac{1}{n-\varepsilon}}$ для некоторого натурального $n \geqslant 2$ и действительного $\varepsilon > 0$, имеет место равенство $NH = \mathbb{F}_q$, где N — число, определенное в формулировке теоремы 9.*

Следствие 4. *Рассмотрим произвольное натуральное число $n \geqslant 2$ и любое действительное $\varepsilon > 0$. Тогда для любого натурального $k \geqslant \left[q^{\frac{1}{n-\varepsilon}}\right] + 1$, произвольного элемента g, не лежащего ни в каком нетривиальном подполе $\mathbb{F}_q$, такого, что $\mathrm{ord}_q g \geqslant k$, и множества $A = \{g^x : 0 \leqslant x \leqslant k(2n-2)\}$ выполнено равенство $NA = \mathbb{F}_q$, где N — число, определенное в формулировке теоремы 9.*

Из следствия 3 вытекает, что если $H \subset \mathbb{F}_q$ — подгруппа, не лежащая ни в каком нетривиальном подполе $\mathbb{F}_q$ и удовлетворяющая условию $|H| > q^{\delta}$, то $NH = \mathbb{F}_q, N = N(r,\delta)$. Аналогичное утверждение при более сильных ограничениях на подгруппу H вытекает из результата Ж. Бургена и М. Ч. Чанг.[30]

В параграфе 5.2 доказываются необходимые следствия из оценок параграфов 4.2 и 4.3, которые используются в параграфе 5.3 для доказательства теоремы 10.

Теорема 10. *Для произвольного неособого подмножества $A \subset \mathbb{F}_q, r \geqslant 3$, такого, что $|A| > q^{\frac{1}{n-\varepsilon}}$ для некоторого натурального $n \geqslant r$ и действительного $\varepsilon \in (0,1)$, имеет место соотношение:*

$$N(A^n) = \mathbb{F}_q, \tag{1}$$

где

$$N = \begin{cases} 10 \cdot 2^{\left[\frac{r-1}{\log_2 3-1}\right]+1} \left(3 + \left[\log_2\left(\frac{r}{\varepsilon}\right)\right]\right)\left(\frac{5}{24}4^{r-1} - \frac{1}{3}\right), & \text{если } n = r; \\ 10 \cdot 2^{\left[\frac{r+2}{\log_2 3-1}\right]+1} \left(3 + \left[\log_2\left(\frac{1}{\varepsilon}\right)\right]\right)\left(\frac{5}{24}4^{n-1} - \frac{1}{3}\right), & \text{если } n \geqslant r+1. \end{cases}$$

Из теорем 4 и 10 вытекает, что равенство (1), где $N = N(n,\varepsilon)$ справедливо для любого неособого подмножества $A \subset \mathbb{F}_{p^4}$ такого, что $|A| > p^{\frac{4}{n-\varepsilon}}$, в случаях $n = 2$ и $n \geqslant 4$. Однако, аналогичное утверждение верно и в случае $n = 3$, что доказано в параграфе 5.3. Таким образом, равенство (1), где $N = N(n,r,\varepsilon)$, справедливо при $r \leqslant 4$ и, вообще говоря, несправедливо при $r > 4$.

[30] J. Bourgain, M.C. Chang, *A Gauss sum estimate in arbitrary finite field*, C.R. Acad. Sci. Paris, Ser. 1, vol. 342, 2006, pp. 643 — 646.

В параграфе 5.4 доказывается, что степень n у множества A^n в теоремах 7, 8 и 10 неулучшаема, а именно, устанавливается справедливость такой теоремы.

Теорема 11. *Для любых натуральных чисел $n \geqslant 2, r \geqslant 1$, действительного числа $0 < \varepsilon < 1$ и любого натурального N существуют простое число p и подмножество $A \subseteq \mathbb{F}_q, q = p^r$, такое, что $|A| > q^{\frac{1}{n-\varepsilon}}$ и $N(A^{n-1}) \neq \mathbb{F}_q$.*

Благодарности.

Автор выражает глубокую благодарность своему научному руководителю доктору физико–математических наук, профессору С.В. Конягину за постановки задач и постоянное внимание. Автор также благодарен профессору Ж. Бургену (Университет Высших Исследований, Принстон, США) и профессору М. Рудневу (Университет Бристоля, Бристоль, Великобритания) за плодотворные обсуждения поставленных задач и постоянную поддержку. Автор выражает благодарность коллективу кафедры общих проблем управления механико–математического факультета МГУ, и в особенности доктору физико–математических наук, профессору В. Ю. Протасову, а также члену–корреспонденту РАН Ю. В. Нестеренко и доктору физико–математических наук, профессору Н. Г. Мощевитину за поддержку и внимание.

Список публикаций по теме диссертации.

[1] А.А. Глибичук, *Комбинаторные свойства множеств вычетов по простому модулю и задача Эрдеша-Грэхэма*, Мат. заметки, т. 79, 2006, стр. 384—395.

[2] А.А. Глибичук, *Свойства сумм и произведений подмножеств конечного поля простого порядка*, Чебышевский сборник, том 8, вып. 2, 2007, стр. 30 — 43.

[3] А.А. Глибичук, *Аддитивные свойства произведений подмножеств поля $\mathbb{F}_{p^2}$*, Вестник Московского Государственного Университета.Серия 1.Математика.Механика, №1, 2009, стр. 3 — 8.

[4] А.А. Глибичук, *Свойства степеней больших подмножеств в поле из p^3 элементов*, Депонировано в ВИНИТИ РАН, 30.09.2008г., №769-В2008, 32 с.