

Пересечения сдвигов мультипликативных подгрупп

Вьюгин И. В., Солодкова Е. В., Шкредов И. Д.*

Аннотация.

С помощью метода Степанова найдена оценка сверху на мощность пересечения аддитивных сдвигов нескольких мультипликативных подгрупп конечного поля. Полученное неравенство применяется к одному вопросу об аддитивной разложимости подгрупп.

УДК 511.218

1 Введение

Пусть p — простое число, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ — конечное поле из p элементов, $G \subseteq \mathbb{F}_p^*$ — некоторая мультипликативная подгруппа этого поля. А. Гарсия и Дж. Ф. Волох [4] показали, что для произвольной подгруппы $G \subseteq \mathbb{F}_p^*$, такой что $|G| < (p-1)/((p-1)^{\frac{1}{4}} + 1)$ и произвольного $\mu \in \mathbb{F}_p^*$ справедлива оценка

$$|G \cap (G + \mu)| \leq 4|G|^{\frac{2}{3}}. \quad (1)$$

Д. Р. Хиф-Браун и С. В. Конягин передоказали и обобщили этот результат в работе [5] при помощи известного в теории чисел метода Степанова [12]. Дальнейшее обобщение было получено в [1] и ниже мы приводим основной результат этой работы.

Теорема 1 Пусть $G \subseteq \mathbb{F}_p^*$ — мультипликативная подгруппа, $\mu_1, \dots, \mu_k \in \mathbb{F}_p^*$ — различные ненулевые элементы поля, $k > 1$. Пусть также

$$32k2^{20k \log(k+1)} \leq |G|, \quad p \geq 4k|G|(|G|^{\frac{1}{2k+1}} + 1).$$

Тогда

$$|G \cap (G + \mu_1) \cap \dots \cap (G + \mu_k)| \leq 4(k+1)(|G|^{\frac{1}{2k+1}} + 1)^{k+1}.$$

Проще говоря, вышеуказанная теорема утверждает, что $|G \cap (G + \mu_1) \cap \dots \cap (G + \mu_k)| \ll_k |G|^{\frac{1}{2} + \alpha_k}$, при условии, что $1 \ll_k |G| \ll_k p^{1 - \beta_k}$, где $\{\alpha_k\}, \{\beta_k\}$ — некоторые последовательности целых чисел, стремящиеся к нулю при $k \rightarrow \infty$.

В статье [7] Митькин обобщил неравенство (1) на случай двух различных подгрупп и нашел оценку среднего значения пересечения нескольких различных смежных классов (предыдущие результаты в этом направлении были получены в [6] и [5]).

*Работа выполнена при поддержке гранта РФФИ 14-11-00433.

Лемма 2 (Митькин) Пусть $p > 2$ — простое, Γ, Π — мультипликативные подгруппы поля \mathbb{F}_p , и M_Γ, M_Π — некоторые полные системы представителей смежных классов группы \mathbb{F}_p^* по подгруппам Γ и Π , соответственно. Для произвольного множества $\Theta \subset M_\Gamma \times M_\Pi$, удовлетворяющего условиям $(|\Gamma||\Pi|)^2|\Theta| < p^3$ и $|\Theta| \leq 33^{-3}|\Gamma||\Pi|$, справедливо неравенство

$$\sum_{(u,v) \in \Theta} \left| \{(x, y) \in \Gamma \times \Pi : ux + vy = 1\} \right| \ll (|\Gamma||\Pi||\Theta|^2)^{1/3}. \quad (2)$$

Отсюда можно получить оценку (1) (с точностью до мультипликативной константы), положив в (2) $\Gamma = \Pi$ и взяв в качестве Θ одноэлементное множество.

В настоящей работе мы продвинулись чуть дальше и получили результат, аналогичный теореме 1, но для пересечения нескольких, возможно различных, мультипликативных подгрупп. Наш подход, так же, как и в [6], [1], состоит в применении подходящего обобщения метода Степанова. Новым также является использование результатов работ [9], [3] для доказательства линейной независимости набора многочленов.

Теорема 3 Пусть $G_0, \dots, G_k \subseteq \mathbb{F}_p^*$ — некоторые мультипликативные подгруппы, μ_1, \dots, μ_k — различные ненулевые остатки. Если выполнены условия

$$|G_0| \cdot \dots \cdot |G_s| < (s+2)^{-s-1/2} p^{s+1/2} \quad (3)$$

при всех $s = 1, \dots, k$ и

$$\frac{1}{2} \left(\prod_{i=0}^l |G_i| \right)^{\frac{1}{2l+1}} < |G_m| < \frac{1}{2(l+3)} \left(\prod_{i=0}^l |G_i| \right)^{\frac{2}{2l+1}} \quad (4)$$

при всех $l = 0, \dots, k$ и $m = 0, \dots, l$ и для пары $l = k-1, m = k$, то справедлива оценка

$$|G_0 \cap (G_1 + \mu_1) \cap \dots \cap (G_k + \mu_k)| \leq 16k(k+2)(|G_0||G_1| \dots |G_k|)^{\frac{1}{2k+1}}.$$

Применение данной теоремы в частном случае $k = 1$ (так же, как и леммы 2) позволяет получить новый результат об аддитивной разложимости мультипликативных подгрупп, см. работы [2, 8, 11] и раздел 3.

При $n \in \mathbb{N}$, обозначим через $[n] = \{1, \dots, n\}$, $\overline{0, n} = \{0, 1, \dots, n\}$ — отрезки ряда целых чисел. Далее \mathbb{Z}_N — множество $\mathbb{Z}/N\mathbb{Z}$ остатков по модулю N , а \mathbb{Z}_N^* — подгруппу обратимых элементов \mathbb{Z}_N . Все логарифмы, используемые в работе, берутся по основанию 2. Через $\mathbb{F}_p[[x]]$ мы обозначаем пространство формальных степенных рядов от x с коэффициентами из \mathbb{F}_p . Через \ll и \gg мы обозначаем обычные символы Виноградова.

2 Пересечение аддитивных сдвигов мультипликативных подгрупп

Доказательство теоремы 3. Пусть

$$\Omega = G_0 \cap (G_1 + \mu_1) \cap \dots \cap (G_k + \mu_k)$$

и $|G_0| = t_0, \dots, |G_k| = t_k$.

Будем оценивать $|\Omega|$ при помощи метода Степанова. Нам нужно построить многочлен

$$\Psi(x) = \sum_{\mathbf{a}, d} C_{\mathbf{a}, d} x^d x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_k)^{a_k t_k},$$

где $\mathbf{a} = (a_0, \dots, a_k)$, $a_i < B_i$, $d < D$, $i = \overline{0, k}$, коэффициенты $C_{\mathbf{a}, d}$ которого не равны нулю одновременно, и у которого все производные

$$\left. \frac{d^n}{dx^n} \Psi(x) \right|_{x \in \Omega} = 0, \quad n = \overline{0, M-1} \quad (5)$$

до порядка $M-1$ включительно и сам он обращаются в ноль на элементах $x \in \Omega$.

Для $x \in \Omega$ условие (5) эквивалентно следующему

$$\left[x(x - \mu_1) \dots (x - \mu_k) \right]^n \left. \frac{d^n}{dx^n} \Psi(x) \right|_{x \in \Omega} = 0, \quad n = \overline{0, M-1}.$$

Заметим, что

$$\begin{aligned} [x(x - \mu_1) \dots (x - \mu_k)]^n \frac{d^n}{dx^n} \left(x^d x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_k)^{a_k t_k} \right) = \\ x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_k)^{a_k t_k} P_{n, \mathbf{a}, d}(x), \end{aligned}$$

где многочлен $P_{n, \mathbf{a}, d}(x)$ или равен тождественно нулю, или $\deg P_{n, \mathbf{a}, d}(x) \leq D + kn$. Заметим также, что при $x \in \Omega$

$$x^{t_0} = (x - \mu_1)^{t_1} = \dots = (x - \mu_k)^{t_k} = 1.$$

Следовательно,

$$\left[x(x - \mu_1) \dots (x - \mu_k) \right]^n \left. \frac{d^n}{dx^n} \left(x^d x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_k)^{a_k t_k} \right) \right|_{x \in \Omega} = P_{n, \mathbf{a}, d}(x),$$

и

$$\left[x(x - \mu_1) \dots (x - \mu_k) \right]^n \left. \frac{d^n}{dx^n} \Psi(x) \right|_{x \in \Omega} = \sum_{\mathbf{a}, d} C_{\mathbf{a}, d} P_{n, \mathbf{a}, d}(x) \stackrel{\text{def}}{=} P_n(x).$$

Теперь выберем коэффициенты $C_{\mathbf{a}, d}$ так, чтобы многочлены $P_n(x)$ были тождественно равны нулю при всех $n < M$. Это можно сделать, поскольку коэффициенты многочленов $P_n(x)$ являются однородными линейными формами от коэффициентов $C_{\mathbf{a}, d}$, а условие

$$P_n(x) \equiv 0 \quad \forall n = \overline{0, M-1}$$

равносильно системе линейных однородных уравнений. Известно, что такая система имеет ненулевое решение, если количество неизвестных $C_{\mathbf{a}, d}$ превышает количество уравнений (в данном случае оно равно суммарному количеству коэффициентов многочленов $P_n(x)$, $n < M$). Следовательно, должно выполняться неравенство

$$MD + k \frac{M^2}{2} < DB_0 B_1 \dots B_k. \quad (6)$$

Если многочлен $\Psi(x)$ ненулевой, то

$$|\Omega| \leq \frac{\deg \Psi(x)}{M}. \quad (7)$$

Нижеследующая лемма объясняет, при каких условиях $\Psi(x)$ не равен тождественно нулю.

Лемма 4 Пусть $k \geq 1$, t_0, \dots, t_k — положительные целые числа, такие, что

$$\prod_{i=0}^s t_i < (s+2)^{-s-\frac{1}{2}} p^{s+\frac{1}{2}}, \quad (8)$$

при всех $s = 1, \dots, k$ и

$$\frac{1}{2} \left(\prod_{i=0}^l t_i \right)^{\frac{1}{2l+1}} < t_m < \frac{1}{2(l+3)} \left(\prod_{i=0}^l t_i \right)^{\frac{2}{2l+1}} \quad (9)$$

при всех $l = 0, \dots, k$ и всех $m = 0, \dots, l$ и для пары $l = k-1$, $m = k$. Пусть также

$$\tau = \left(\prod_{i=0}^k t_i \right)^{\frac{2}{2k+1}}, \quad (10)$$

и определим $B_i = \lfloor \tau/t_i \rfloor$ для любого $i = \overline{0, k}$, $D = \lfloor \frac{1}{2} \prod_{i=0}^k B_i \rfloor$.

Тогда многочлены вида

$$x^d x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_k)^{a_k t_k}, \quad (11)$$

где $a_i < B_i$, $d < D$, $i = \overline{0, k}$ линейно независимы над полем \mathbb{F}_p .

Доказательство. Будем доказывать лемму по индукции по k . Базой индукции служит тот факт, что набор мономов x^d при $d = 0, \dots, D-1$ является линейно независимым. Поскольку, как нетрудно заметить, все шаги индукции доказываются аналогично первому, то мы подробно разберем первый шаг. Итак, предположим, что набор произведений вида:

$$x^d x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_k)^{a_{k-1} t_{k-1}},$$

где $a_i < B_i$, $d < D$, $i = \overline{0, k-1}$ линейно независим над полем \mathbb{F}_p .

Доказательство шага индукции проведем от противного, а именно, предположим, что многочлены (11) линейно зависимы. Тогда существует их нетривиальная линейная комбинация, также являющаяся многочленом такая, что

$$\tilde{\Psi}(x) = \sum_{d, \mathbf{a}=(a_0, \dots, a_k)} \tilde{C}_{\mathbf{a}, d} x^d x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_k)^{a_k t_k} \equiv 0. \quad (12)$$

Перепишем его в следующей форме

$$\tilde{\Psi}(x) = (x - \mu_k)^{t_k} \Upsilon(x) + \Phi(x), \quad (13)$$

где

$$\Upsilon(x) = \sum_{d, \mathbf{a}: a_k \neq 0} \tilde{C}_{\mathbf{a}, d} x^d x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_k)^{(a_k - 1) t_k} \quad (14)$$

и

$$\Phi(x) = \sum_{d, \mathbf{a}: a_k = 0} \tilde{C}_{\mathbf{a}, d} x^d x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_{k-1})^{a_{k-1} t_{k-1}}. \quad (15)$$

Из (13) видно, что $\Phi(x)$ делится нацело на $(x - \mu_k)^{t_k}$.

Воспользоваться предположением индукции, которое утверждает, что многочлены (2) линейно независимы и, следовательно, $\Phi(x) \not\equiv 0$. Поэтому далее будем предполагать, что многочлен $\Phi(x)$ ненулевой.

Перепишем $\Phi(x)$ в виде

$$\Phi(x) = \sum_{\mathbf{a}: a_k = 0} H_{\mathbf{a}}(x) x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_{k-1})^{a_{k-1} t_{k-1}},$$

где $H_{\mathbf{a}}(x) = \sum_d \tilde{C}_{\mathbf{a}, d} x^d$, все векторы \mathbf{a} попарно различны и $a_i \in \{0, \dots, B_i - 1\}$, $i = \overline{0, k-1}$. Ясно, что $\deg H_{\mathbf{a}}(x) < D$ при всех \mathbf{a} .

Обозначим

$$Q_{\mathbf{a}}(x) := H_{\mathbf{a}}(x) x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_{k-1})^{a_{k-1} t_{k-1}},$$

а также переобозначим $\mathbf{a} := (a_0, \dots, a_{k-1})$, оставив только первые k компонент.

Рассмотрим вронскиан

$$W(x) = \begin{vmatrix} Q_{(0, \dots, 0)}(x) & \dots & Q_{(B_0 - 1, \dots, B_{k-1} - 1)}(x) \\ Q'_{(0, \dots, 0)}(x) & \dots & Q'_{(B_0 - 1, \dots, B_{k-1} - 1)}(x) \\ \vdots & \ddots & \vdots \\ Q_{(B_0 B_1 \dots B_{k-1} - 1)}(x) & \dots & Q_{(B_0 - 1, \dots, B_{k-1} - 1)}(x) \end{vmatrix}. \quad (16)$$

Нам известно из предположения индукции, что многочлены $Q_{\mathbf{a}}(x)$ линейно независимы. В таком случае вронскиан $W(x)$ не обращается тождественно в нуль. Данный факт следует из результата Ф. К. Шмидта [9] (см. также [3]), который мы сформулируем в удобной для нашего случая форме:

Лемма 5 (Ф. К. Шмидт) Пусть \mathbb{F} — поле характеристики $p > 0$. Рассмотрим многочлены $f_1 = f_1(x), \dots, f_n = f_n(x)$ как элементы поля степенных рядов $\mathbb{F}[[x]]$. Тогда f_1, \dots, f_n линейно независимы над $\mathbb{F}[[x^p]]$ если и только если их вронскиан $W(f_1, \dots, f_n)$ не равен тождественно нулю.

Если мы убедимся, что многочлены $Q_{\mathbf{a}}(x)$ линейно независимы над \mathbb{F}_p , а их степени не превосходят p , то вронскиан $W(x)$, построенный по набору многочленов $Q_{\mathbf{a}}(x)$, не может обращаться в ноль тождественно. Действительно, если бы вронскиан $W(x)$ был бы тождественно нулевым, это повлекло бы существование нетривиальной линейной комбинации:

$$\sum_{\mathbf{a}} \varphi_{\mathbf{a}}(x) Q_{\mathbf{a}}(x) \equiv 0 \quad (17)$$

с коэффициентами $\varphi_{\mathbf{a}}(x) \in \mathbb{F}_p[[x^p]]$. Без ограничения общности можно считать, что хотя бы одно из чисел $\varphi_{\mathbf{a}}(0) \neq 0$, иначе все коэффициенты $\varphi_i(x)$ можно было бы одновременно поделить на подходящую степень x^p . В этом случае, легко видеть, что линейная комбинация

$$\sum_{\mathbf{a}} \varphi_{\mathbf{a}}(0) Q_{\mathbf{a}}(x) \equiv 0 \quad (18)$$

также является тождественно нулевой, так как члены линейной комбинации (17), не входящие в комбинацию (18) заведомо не могут сократиться с членами комбинации (18), так как их степени заведомо больше p , а значит, члены комбинации (18) сокращаются друг с другом. Показав, что (18) является нетривиальной равной нулю линейной комбинацией многочленов $Q_{\mathbf{a}}(x)$, мы пришли к противоречию с предположением, что многочлены $Q_{\mathbf{a}}(x)$ линейно независимы над \mathbb{F}_p .

Убедимся, что степени многочленов $Q_{\mathbf{a}}(x)$ превосходят p . Выполнение данного условия следует из (8). Действительно,

$$Q_{\mathbf{a}}(x) < D + \sum_{i=0}^{k-1} t_i B_i < (k+1)\tau = (k+1) \left(\prod_{i=0}^k t_i \right)^{\frac{2}{2k+1}} < (k+1) \left((k+2)^{-\frac{2k+1}{2}} p^{\frac{2k+1}{2}} \right)^{\frac{2}{2k+1}} = \frac{k+1}{k+2} p$$

и, следовательно, $\deg \Phi(x) < \frac{k+1}{k+2} p$. Таким образом, получаем, что если $Q_{\mathbf{a}}(x)$ линейно независимы, то соответствующий вронскиан (16) – ненулевой многочлен от x .

Как многочлен $W(x)$ делится на

$$R(x) = \prod_{\mathbf{a}} \frac{x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_{k-1})^{a_{k-1} t_{k-1}}}{(x(x - \mu_1) \dots (x - \mu_{k-1}))^{B_0 \dots B_{k-1} - 1}},$$

поскольку (по определению B_j) $t_i > B_0 \dots B_{k-1}$ при любом $i = 0, \dots, k-1$, и при любом \mathbf{a} столбец с индексом \mathbf{a} делится на

$$\frac{x^{a_0 t_0} (x - \mu_1)^{a_1 t_1} \dots (x - \mu_{k-1})^{a_{k-1} t_{k-1}}}{(x(x - \mu_1) \dots (x - \mu_{k-1}))^{B_0 \dots B_{k-1} - 1}}.$$

Докажем неравенство $t_j > B_0 \dots B_{k-1}$. Действительно, из неравенства (9) следует, что

$$t_k < \frac{1}{2} \left(\prod_{i=0}^k t_i \right)^{\frac{2}{2k+1}},$$

отсюда, домножив на $t_k^{-1} \left(\prod_{i=0}^k t_i \right)^{\frac{2k-1}{2k+1}}$, получим

$$\left(\prod_{i=0}^k t_i \right)^{\frac{2k-1}{2k+1}} < \frac{1}{2} t_0 \cdot \dots \cdot t_{k-1},$$

умножим обе части на $\left(\prod_{i=0}^k t_i\right)^{\frac{1}{2k+1}} (t_0 \cdots t_{k-1})^{-1}$, получим

$$\frac{\left(\prod_{i=0}^k t_i\right)^{\frac{2k}{2k+1}}}{t_0 \cdots t_{k-1}} < \frac{1}{2} \left(\prod_{i=0}^k t_i\right)^{\frac{1}{2k+1}}.$$

Из предыдущих неравенств и выражения (10) следует, что

$$t_j > \frac{1}{2} \left(\prod_{i=0}^k t_i\right)^{\frac{1}{2k+1}} > \frac{\left(\prod_{i=0}^k t_i\right)^{\frac{2k}{2k+1}}}{t_0 \cdots t_{k-1}} = \frac{\tau^k}{t_0 \cdots t_{k-1}} \geq B_0 \cdots B_{k-1}.$$

Таким образом неравенство доказано. Заметим, что это неравенство необходимо доказать только на первом шаге индукции.

Из делимости $W(x)$ на $R(x)$ следует, что

$$\deg(W(x)/R(x)) \leq DB_0 B_1 \cdots B_{k-1} + k \frac{(B_0 \cdots B_{k-1})^2}{2}. \quad (19)$$

Действительно, степень многочлена $\deg W(x)/R(x)$ равна $\deg W(x) - \deg R(x)$, а она не превосходит величины, стоящей в правой части неравенства (19). Нам известно, что $(x - \mu_k)^{t_k}$ делит $\Phi(x)$, следовательно $(x - \mu_k)^{t_k - (B_0 \cdots B_{k-1} - 1)}$ делит $W(x)$, поскольку нетривиальная линейная комбинация столбцов вронскиана делится на $(x - \mu_k)^{t_k - (B_0 \cdots B_{k-1} - 1)}$. Кратность корня $x = \mu_k$ не превосходит степени многочлена, поэтому

$$t_k - (B_0 \cdots B_{k-1} - 1) \leq DB_0 B_1 \cdots B_{k-1} + k \frac{(B_0 \cdots B_{k-1})^2}{2},$$

Следовательно, если выполнено неравенство

$$t_k > DB_0 B_1 \cdots B_{k-1} + k \frac{(B_0 \cdots B_{k-1})^2}{2} + B_0 \cdots B_{k-1} - 1 \quad (20)$$

то многочлены (11) линейно независимы.

Рассмотрим величину

$$\gamma = \min_{0 \leq i \leq k} (1 - t_i/\tau). \quad (21)$$

Поскольку $t_i B_i > t_i(\tau/t_i - 1) \geq \gamma\tau$, то

$$t_i > \gamma\tau/B_i, \quad i = 0, \dots, k. \quad (22)$$

Второе неравенство из (9) даёт $\gamma > 1 - \frac{1}{2(k+3)}$ и $B_j \geq 2(k+3)$, $j = 0, \dots, k$. Получаем

$$\begin{aligned} DB_0 B_1 \cdots B_{k-1} + k \frac{(B_0 \cdots B_{k-1})^2}{2} + B_0 \cdots B_{k-1} - 1 &\leq \frac{1}{B_k} \left(\frac{1}{2} \left(\prod_{i=0}^k B_i\right)^2 + \frac{k}{2B_k} \left(\prod_{i=0}^k B_i\right)^2 + \prod_{i=0}^k B_i - B_k \right) \\ &< \frac{1}{B_k} \left(\prod_{i=0}^k B_i\right)^2 \left(\frac{1}{2} + \frac{k}{4(k+3)} + \frac{1}{(2k+6)^{k+1}} \right) < \frac{1}{B_k} \left(\prod_{i=0}^k B_i\right)^2 \left(1 - \frac{1}{2(k+3)} \right) < \gamma \frac{\tau}{B_k} < t_k. \end{aligned}$$

Следовательно, выполнено неравенство (20), а с ним и утверждение леммы.

Вернёмся к доказательству теоремы 3.

Возьмём значения параметров τ , B_i ($i = \overline{0, k}$), D, γ такие же, как в лемме 4. Тогда

$$\gamma \frac{\tau}{t_i} < B_i \leq \frac{\tau}{t_i} \quad (23)$$

и пользуясь указанным выше неравенством $\gamma > 1 - \frac{1}{2(k+3)}$, получаем

$$\gamma^{k+1} > \left(1 - \frac{1}{2(k+3)}\right)^{k+1} > 1/\sqrt{e} > 1/2. \quad (24)$$

Возьмём в качестве минимальной кратности M следующую величину

$$M = \left\lfloor \frac{1}{4k} \prod_{i=0}^k B_i \right\rfloor. \quad (25)$$

Применяя неравенство (22), получаем оценку на M

$$M = \left\lfloor \frac{1}{4k} \prod_{i=0}^k B_i \right\rfloor \geq \left\lfloor \frac{\gamma^{k+1}}{4k} \frac{\tau^{k+1}}{\prod_{i=0}^k t_i} \right\rfloor \geq \frac{\gamma^{k+1}}{8k} \left(\prod_{i=0}^k t_i \right)^{\frac{1}{2k+1}}. \quad (26)$$

Легко показать, что при этом выполняется неравенство (6). В самом деле, из (25) и того, что $k \geq 1$ следует

$$\begin{aligned} MD + k \frac{M^2}{2} &\leq \frac{1}{8k} \left(\prod_{i=0}^k B_i \right)^2 + \frac{1}{32k} \left(\prod_{i=0}^k B_i \right)^2 = \frac{5}{32k} \left(\prod_{i=0}^k B_i \right)^2 \\ &< \frac{1}{4} \left(\prod_{i=0}^k B_i \right)^2 < \left\lfloor \frac{1}{2} \left(\prod_{i=0}^k B_i \right) \right\rfloor \left(\prod_{i=0}^k B_i \right) = D \left(\prod_{i=0}^k B_i \right). \end{aligned} \quad (27)$$

Возвращаясь к (7) и применяя (26), получаем оценку

$$|\Omega| \leq \frac{\deg \Psi(x)}{M} < \frac{(k+2)\tau}{\frac{\gamma^{k+1}}{8k} \left(\prod_{i=0}^k t_i \right)^{\frac{1}{2k+1}}} < \frac{8k(k+2)}{\gamma^{k+1}} \left(\prod_{i=0}^k t_i \right)^{\frac{1}{2k+1}}, \quad (28)$$

а из (24) следует, что

$$|\Omega| < 16k(k+2) \left(\prod_{i=0}^k t_i \right)^{\frac{1}{2k+1}}. \quad (29)$$

Завершено доказательство шага индукции, а следовательно и всей теоремы, так как все остальные шаги проделываются аналогично.

Заметим что результат теоремы 3 можно легко расширить на случай нескольких смежных классов мультипликативных подгрупп G_0, G_1, \dots, G_k , см. подробности в [1].

Доказанную нами теорему можно переписать в следующем виде.

Следствие 6 *Рассмотрим систему уравнений*

$$(x - \mu_i)^{\lambda_i} = 1, \quad i = 0, \dots, k, \quad x \in \mathbb{F}_p, \quad (30)$$

где $\mu_i \in \mathbb{F}_p^*$, $i = \overline{0, k}$ — попарно различные элементы, каждое λ_i делит $(p - 1)$, и $p, t_i = (p - 1)/\lambda_i$ удовлетворяют условиям леммы 4. Тогда число решений системы (30) не превосходит

$$16k(k + 2) \left(\prod_{i=0}^k \frac{p}{\lambda_i} \right)^{\frac{1}{2k+1}}.$$

3 Аддитивное разложение подгрупп малого размера

Пусть \mathbf{G} — произвольная абелева группа и $A, B \subseteq \mathbf{G}$ ее любые подмножества. Сумма $A + B$ определяется как множество

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

попарных сумм элементов A и B .

Пусть S — некоторое подмножество группы \mathbf{G} . Назовём S *приводимым* или *аддитивно разложимым*, (см. [2, 8]), если оно представляется в виде

$$S = A + B,$$

где A, B — произвольные подмножества \mathbf{G} , причем $|A|, |B| \geq 2$.

В данном разделе будут показаны возможности применения теоремы 3 и аналогичных результатов к изучению аддитивной разложимости мультипликативных подгрупп малого размера, лежащих в поле \mathbb{F}_p .

Нам понадобятся обозначения. Пусть $f, g : \mathbb{F}_p \rightarrow \mathbb{C}$ — произвольные функции. Положим

$$(f \circ g)(x) := \sum_{y \in \mathbb{F}_p} f(y)g(y + x),$$

Ясно, что $(f \circ g)(x) = (g \circ f)(-x)$, $x \in \mathbb{F}_p$. Также мы будем использовать одну и ту же букву для обозначения множества $S \subseteq \mathbf{G}$ и его характеристической функции $S : \mathbf{G} \rightarrow \{0, 1\}$.

При $k = 1$ теорема 3 имеет следующий вид

Следствие 7 *Пусть $G_0, G_1 \subseteq \mathbb{F}_p^*$ — мультипликативные подгруппы, $\mu \in \mathbb{F}_p^*$ — некоторый ненулевой элемент. Если*

$$|G_0||G_1| < 3^{-3/2}p^{3/2}, \quad |G_0|^2 > 512|G_1|, \quad |G_1|^2 > 512|G_0|,$$

то

$$(G_1 \circ G_0)(\mu) = |G_0 \cap (G_1 + \mu)| \leq 48(|G_0||G_1|)^{1/3}.$$

Лемма 2 даёт верхнюю оценку среднего значения свёртки двух различных подгрупп Γ и Π . В случае $\Gamma = \Pi$ похожая оценка была получена Конягиным в [6]. При помощи метода из [6] в сочетании с нашим подходом можно найти оценку, аналогичную (2).

Сформулируем основной результат этого раздела.

Теорема 8 Пусть $\varepsilon \in (0, 1]$ — вещественное число, $A, G \subset \mathbb{F}_p^*$, $|A| \geq 2 \cdot 33^3$ и $B \subseteq \mathbb{F}_p$ — произвольное множество. Если $|G \cap A| \leq |A|^{1-\varepsilon}$, $|G|^2|A|^{1+\varepsilon}|B| < 2^{-1}p^3$, $|G|^2|A|^2 < p^3$ и $A + B \subseteq G$, то $|B||A|^{1+\varepsilon} \ll |G|$.

Доказательство. Заметим, что B не может содержать нуль, так как тогда A будет целиком содержаться в G и $|G \cap A| = |A|$, что запрещено условиями теоремы. Обозначим $H = G \cap A$. Очевидно, что H также является мультипликативной подгруппой. Пусть $B_\xi = B \cap \xi H$, $\xi \in \mathbb{F}_p^*/H$, так, что $B = \bigsqcup_\xi B_\xi$. Каждое множество B_ξ содержит не более $|H|$ элементов, следовательно, существует непустое подмножество $\tilde{B} \subseteq B$ из, по крайней мере, $k = \lceil |B||A|^{1-\varepsilon} \rceil$ ненулевых элементов, таких, что $b_i \not\equiv b_j \pmod{H}$ при $b_i, b_j \in \tilde{B}, i \neq j$.

Пусть $U = \{(1/b_i, -1/b_i) : b_i \in \tilde{B}, i = 1, \dots, k\}$. Можно показать, что найдется пара полных систем M_G и M_A представителей различных смежных классов \mathbb{F}_p^* по подгруппам G и A соответственно, так, что $U \subseteq M_G \times M_A$. В самом деле, если $1/b_i \equiv 1/b_j \pmod{G}$ и $-1/b_i \equiv -1/b_j \pmod{A}$ при некоторых $i \neq j$, то $b_j/b_i \in H$, что невозможно по определению U .

Теперь можно воспользоваться леммой 2 при $\Gamma = G, \Pi = A$ и $\Theta = U$. Если G, A и B удовлетворяют условиям нашей теоремы, то легко убедиться, что G, A и U удовлетворяют и обоим условиям леммы: $(|A||G|)^2|U| < p^3$ и $|U| \leq 33^{-3}|A||G|$. Действительно, если $k = 1$, то первое условие эквивалентно неравенству $|G|^2|A|^2 < p^3$, которое справедливо. Второе условие вытекает из того, что $|A| \geq 2 \cdot 33^3 \geq 33^3$. Пусть теперь $k \geq 2$. Тогда $|U| \leq 2|B||A|^{1-\varepsilon}$ и оценка $(|A||G|)^2|U| < p^3$ вытекает из условия $|G|^2|A|^{1+\varepsilon}|B| < 2^{-1}p^3$. Наконец

$$|U| \leq 2|B||A|^{1-\varepsilon} \leq 2|B| \leq 33^{-3}|A||B| \leq 33^{-3}|A||G|,$$

ибо $|A| \geq 2 \cdot 33^3$.

В результате получаем оценку

$$\sum_{(u,v) \in U} |\{(x, y) \in G \times A : ux + vy = 1\}| = \sum_{i=1}^k (A \circ G)(b_i) \ll (|G||A|k^2)^{1/3}. \quad (31)$$

Заметим, что если $A + B \subseteq G$, то $\sum_{i=1}^k (A \circ G)(b_i) = k|A|$, так, что $k \ll |G||A|^2$, из чего следует утверждение теоремы.

В случае $A+B = G$ можно воспользоваться оценками на мощность A и B , полученными в [11].

Лемма 9 (Шпарлинский) Пусть p — простое число. Если подгруппа $G \subset \mathbb{F}_p^*$, не совпадающая со всей группой \mathbb{F}_p^* , аддитивно разложима на некоторые множества A и B , то имеют место оценки

$$|G|^{1/2+o(1)} = \min(|A|, |B|) \leq \max(|A|, |B|) = |G|^{1/2+o(1)} \quad (32)$$

при $|G| \rightarrow \infty$.

Следствие 10 Пусть $\varepsilon \in (0, 1]$ — вещественное, $A, G \subset \mathbb{F}_p^*$ — мультипликативные подгруппы, $|G| \geq C(\varepsilon)$ — достаточно большая и $B \subseteq \mathbb{F}_p$ — произвольное непустое подмножество. Если $|G \cap A| \leq |A|^{1-\varepsilon}$, то у G нет нетривиального представления в виде $G = A + B$.

Доказательство. Предположим противное, то есть, что $G = A + B$. Если G достаточно велико и $|G| \ll p^{1-\varepsilon/6}$, то, применяя оценки (32), видим, что мощности множеств G, A, B удовлетворяют условиям теоремы 8. Кроме того из этих оценок будет вытекать, что и подгруппа A достаточно большая. Следовательно, если $A + B = G$ и $|G \cap A| \leq |A|^{1-\varepsilon}$, $|G| \ll p^{1-\varepsilon/6}$, то по лемме 9 и теореме 8 получаем, что $|G|^{1+\varepsilon/2+o(1)} \ll |B||A|^{1+\varepsilon} \ll |G|$, противоречие.

Если же $|G| \gg p^{1-\varepsilon/6}$, то из теоремы Шпарлинского вытекает, в частности, что $|A| \geq p^{1/3}$ про достаточно больших $|G|$. Кроме того, поскольку A и G подгруппы, то

$$|G \cap A| \geq \frac{|A||G|}{p-1} \gg |A|p^{-\varepsilon/6} > |A|^{1-\varepsilon},$$

что противоречит условию $|G \cap A| \leq |A|^{1-\varepsilon}$. Следствие доказано.

4 Благодарности

Авторы выражают благодарность Сергею Владимировичу Колягину за ряд плодотворных обсуждений. Работа первого автора выполнена при поддержке РФФИ (грант № 14-01-00346).

Список литературы

- [1] Вьюгин И. В., Шкрёдов И. Д., *Об аддитивных сдвигах мультипликативных подгрупп*, Матем. сб. **203:6** (2012), 81–100.
- [2] C. DARTYGE AND A. SÁRKÖZY, *On additive decompositions of the set of primitive roots modulo p* , Monatsh. Math. **169** (2013), 317–328.
- [3] A. GARCIA, J.F. VOLOCH, *Wronskians and linear independence in fields of prime characteristic*, Manuscripta Math. **59** (1987), 457–469.
- [4] A. GARCIA, J.F. VOLOCH, *Fermat curves over finite fields*, J. Number Theory, **30:3** (1988), 345–356.
- [5] D. R. HEATH–BROWN, S. V. KONYAGIN, *New bounds for Gauss sums derived from k th powers, and for Heilbronn’s exponential sum*, Quart. J. Math. **51** (2000), 221–235.
- [6] Колягин С. В., *Оценки для тригонометрических сумм на подгруппы и для гауссовых сумм*, IV интернац. конф. “Современные проблемы теории чисел и ее приложения”, Актуальные проблемы. Часть 3 (Тула, 2001), Изд-во Моск. ун-та, М., 2002, 86–114.
- [7] Митькин Д. А., *Оценка суммарного числа рациональных точек некоторого множества кривых в простом конечном поле*, Чебышёвский сборник, **4:4** (2003), 94–102.
- [8] A. SÁRKÖZY, *On additive decompositions of the set of the quadratic residues modulo p* , Acta Arith. **155** (2012), 41–51.

- [9] F.K. SCHMIDT, *Die Wronskische Determinante in beliebigen differenzierbaren Funktionenkorpern*, Math. Z. **45** (1939), 62–74.
- [10] T. SCHOEN, I. D. SHKREDOV, *Additive properties of multiplicative subgroups of \mathbb{F}_p* , Quart. J. Math. **63**:3 (2012), 713–722.
- [11] I. E. SHPARLINSKI, *Additive Decompositions of Subgroups of Finite Fields*, SIAM J. Discrete Math., **27**:4 (2013), 1870–1879.
- [12] СТЕПАНОВ С. А., *О числе точек гиперэллиптической кривой над простым конечным полем*, ИАН **33** (1969), 1171–1181.
- [13] T. TAO, V. VU, *Additive combinatorics*, Cambridge University Press 2006.

Вьюгин И. В.

Институт проблем передачи информации РАН,
Большой Каретный пер. 19, Москва, Россия, 127994

и

Национальный исследовательский университет Высшая школа экономики,
ул. Вавилова, 7, Москва, Россия, 117312

vyugin@gmail.com.

Солодкова Е.В.

Институт проблем передачи информации РАН,
Большой Каретный пер. 19, Москва, Россия, 127994

hsolodkova@gmail.com

Шкредов И. Д.

Отдел алгебры и теории чисел,
Математический институт им. В.А. Стеклова РАН,
ул. Губкина, 8, Москва, Россия, 119991

и

Лаборатория дискретной и вычислительной геометрии им. Б. Н. Делоне,
Ярославский государственный университет им. П. Г. Демидова,
ул. Советская, 14, Ярославль, Россия, 150000

и

Институт проблем передачи информации РАН,
Большой Каретный пер. 19, Москва, Россия, 127994
ilya.shkredov@gmail.com