ЧЕБЫШЕВСКИЙ СБОРНИК
Том 26. Выпуск 4.

УДК: 511.17 DOI: 10.22405/2226-8383-2025-26-4-174-182

О сравнениях Гаусса и Якобшталя

К. И. Пименов, И. Н. Фаизов, И. Б. Жуков

Пименов Константин Игоревич — кандидат физико-математических наук, Санкт-Петербургский государственный университет (г. Санкт-Петербург).
e-mail: k.pimenov@spbu.ru
Фаизов Ильдар Николаевич — ООО «Яндекс-Технологии» (г. Санкт-Петербург).
e-mail: ildar_faizov@mail.ru
Жуков Игорь Борисович — доктор физико-математических наук, Санкт-Петербургский государственный университет (г. Санкт-Петербург).
e-mail: i.zhukov@spbu.ru

Аннотация

Данная статья посвящена распространеннию классического сравнения Вольстенхольма для центрального биномиального коэффициента $\binom{2p}{p}$ на случай составного числа. Переносом малой теоремы Ферма на составной случай является сравнение Гаусса, которое имеет простую комбинаторно-динамическую интерпретацию. Для распространения сравнения Вольстенхольма на составной случай необходимо использовать сравнение Якобшталя. Приводится комбинаторное доказательство его ослабленной версии, основанное на исследовании длин орбит некоторого действия силовской p-подгруппы симметрической группы.

Ключевые слова: малая теорема Ферма, элементарная теория чисел, силовская подгруппа, арифметическая динамика, сравнения Гаусса, последовательность Дольда, теорема Вольстенхольма

Библиография: 16 названий.

Для цитирования:
Пименов К. И., Фаизов И. Н., Жуков И. Б. О сравнениях Гаусса и Якобшталя // Чебышевский сборник, 2025, т.26, вып.4, с. 174–182.

CHEBYSHEVSKII SBORNIK
Vol. 26. No. 4.

UDC: 511.17 DOI: 10.22405/2226-8383-2025-26-4-174-182

On Gauss and Jacobsthal congruences

K. I. Pimenov, I. N. Faizov, I. B. Zhukov

Pimenov Konstantin Igorevich — candidate of physical and mathematical sciences, Saint Petersburg State University (St. Petersburg).
e-mail: k.pimenov@spbu.ru
Faizov Ildar Nikolaevich — LLC “Yandex Technologies” (St. Petersburg).
e-mail: ildar_faizov@mail.ru
Zhukov Igor Borisovich — doctor of physical and mathematical sciences, Saint Petersburg State University (St. Petersburg).
e-mail: i.zhukov@spbu.ru

Abstract

This paper is devoted to extending the classical Wolstenholme congruence for the central binomial coefficient $\binom{2p}{p}$ to the case of a composite number. An extension of Fermat's little theorem to the composite case is the Gauss congruence, which has a simple combinatorial-dynamic interpretation. To extend Wolstenholme's congruence to the composite case, it is necessary to use the Jacobsthal congruence. A combinatorial proof of its weakened version is given based on investigation of the orbit lenghts for a suitable action of Sylow p-subgroups of the symmetric group.

Keywords: Fermat little theorem, elementary number theory, arithmetical dynamics, Sylow subgroup, Gauss congruence, Dold Sequence,Wolstenholme's theorem

Bibliography: 16 titles.

For citation:
Pimenov, K. I., Faizov, I. N., Zhukov, I. B. 2025, "On Gauss and Jacobsthal congruences" , *Chebyshevskii sbornik*, vol.26, no.4, pp. 174–182.

Статья посвящена светлой памяти незабвенного Учителя, коллеги и старшего друга Сергея Владимировича Востокова

1. Введение

Пусть $\mu : \mathbb{N} \to \{0, 1, -1\}$ —обычная арифметическая функция Мёбиуса:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ (-1)^r, & \text{если } n = p_1 p_2 \cdots p_r \text{ для различных простых } p_1, p_2, \ldots, p_r, \\ 0, & \text{если } p^2 \mid n \text{ для некоторого простого } p. \end{cases}$$

Сравнение Гаусса $\sum\limits_{d|n} \mu\left(\frac{n}{d}\right) a^d \equiv 0 \pmod{n}$, справедливое для любого натурального n и целого a, можно рассматривать как обобщение малой теоремы Ферма на случай составного модуля. Комбинаторное доказательство малой теоремы Ферма подсчетом числа раскрасок элементов циклической группы дословно переносится на случай составного модуля. На языке динамических систем оно может быть переизложено следующим образом.

Пусть $T : X \to X$ — преобразование множества X такое, что число неподвижных точек $F_T(n) = |\{x \in X \,|\, T^n(x) = x\}|$ преобразования T^n конечно для любого $n \in \mathbb{N}$. Обозначим через $L_T(m)$ число орбит длины m преобразования T. Тогда $F_T(n) = \sum\limits_{d|n} dL_T(d)$ и по формуле обращения Мёбиуса $nL_T(n) = \sum\limits_{d|n} \mu\left(\frac{n}{d}\right) F_T(n)$, следовательно,

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) F_T(d) \equiv 0 \pmod{n}. \tag{1}$$

Возьмём в качестве X множество раскрасок $\mathbb{Z}^A = \{\theta : \mathbb{Z} \to A\}$ целых точек на прямой в $|A| = a$ цветов, и в качестве T возьмем сдвиг на 1, то есть $(T(\theta))(k) = \theta(k-1)$. Доказательство сравнения Гаусса для натурального a отсюда немедленно вытекает, поскольку число раскрасок, переходящих в себя при сдвиге на n, равно a^n: для того, чтобы задать такую раскраску необходимо и достаточно раскрасить точки из полной системы вычетов по модулю n. Таким образом, сравнение (1) превращается в сравнение Гаусса.

Настоящая заметка возникла при попытке рассматривать иные раскраски в приведенном выше рассуждении. Например, если в качестве X рассмотреть множество периодических раскрасок целых точек на прямой в два цвета таких, что в каждом периоде имеется одинаковое число точек каждого цвета, то мы получим сравнение

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \binom{2d}{d} \equiv 0 \pmod{n}. \tag{2}$$

В действительности, последнее сравнение справедливо по модулю n^2, а если n не делится ни на 2, ни на 3, то даже и по модулю n^3. За доказательство этого результат второй автор еще в бытность его школьником был удостоен первой премии на научной конференции для школьников «VI Колмогоровские чтения», проходившей 4–6 мая 2006 г. при СУНЦ МГУ. Настоящая публикация подготовлена на основе этой неопубликованной работы второго автора, включает в себя обзор смежных результатов и комбинаторное доказательство усиления сравнения (2) по модулю n^2. К сожалению, мы не знаем комбинаторного доказательства усиления сравнения (2) по модулю n^3.

2. Последовательности Дольда

Последовательность a_n целых чисел, для любого натурального n, удовлетворяющую сравнению $\sum_{d|n} \mu\left(\frac{n}{d}\right) a_d \equiv 0 \pmod{n}$, мы будем называть *последовательностью Дольда*, следуя работе [6]. Нам также удобно будет определить последовательности Дольда r-го порядка как последовательности $\{a_k\}_{k\in\mathbb{N}}$, удовлетворяющие сравнениям $\sum_{d|n} \mu\left(\frac{n}{d}\right) a_d \equiv 0 \pmod{n^r}$. Кроме того, мы рассматриваем обобщенные последовательности Дольда как 1-го, так и r-го порядка со значениями в коммутативном кольце R таком, что для любого $n \in \mathbb{N}$ отображение $R \to R$, переводящее x в nx, инъективно. Обобщённая последовательность Дольда порядка 0 со значениями в кольце R — это произвольная последовательность со значениями в R. Постоянная последовательность $a_k = 1$ является последовательностью Дольда r-го порядка для любого r.

Как уже было показано во введении, основным примером последовательностей Дольда являются так называемые *реализуемые* последовательности, т. е. последовательности вида $a_n = F_T(n)$ для подходящей динамической системы $T : X \to X$. Имеет место следующая характеризация обычных последовательностей Дольда 1-го порядка:

Предложение 2.1.([6, Prop. 4.2]) Для последовательности $\{a_k\}_{k\in\mathbb{N}}$ следующие условия равносильны:

(a) $\{a_k\}_{k\in\mathbb{N}}$ — это последовательность Дольда;

(b) $\{a_k\}_{k\in\mathbb{N}}$ — это разность двух реализуемых последовательностей;

(c) для любого простого p и натуральных m и k имеет место сравнение $a_{mp^k} \equiv a_{mp^{k-1}} \pmod{p^k}$.

Равносильность $(a) \Leftrightarrow (b)$ почти сразу же следует из сказанного выше. Для последовательности a_n, реализуемой как $a_n = F_T(n)$, соответствующая последовательность $b_n = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) a_d$ будет состоят из неотрицательных целых чисел, так как $b_n = L_T(n)$. В обратную сторону, нетрудно построить преобразование счётного множества $T : X \to X$, имеющее b_n орбит длины n при всех натуральных n для произвольной последовательности $\{b_k\}$ неотрицательных

целых чисел. Поскольку любую последовательность целых чисел можно выразить как разность двух последовательностей неотрицательных целых чисел, мы получаем равносильность $(a) \Leftrightarrow (b)$.

Равносильность $(a) \Leftrightarrow (c)$ последнего предложения дословно переносится на случай обобщённых последовательностей Дольда r-го порядка:

Предложение 2.2. Последовательность $\{a_k\}_{k\in\mathbb{N}} \subset R$ тогда и только тогда является обобщённой последовательностью Дольда порядка r, когда для любого простого p и натуральных m и k имеет место сравнение $a_{mp^k} \equiv a_{mp^{k-1}} \pmod{p^k R}$.

Доказательство. Возьмем последовательность Дольда r-го порядка a_n и выберем p, k и m. Будем считать, что m не делится на p, и проведём доказательство индукцией по m. В случае $m = 1$ требуемое следует непосредственно из определения последовательности Дольда. Для $m > 1$

$$p^{kr} \mid \sum_{d\mid mp^k} \mu\left(\frac{mp^k}{d}\right) a_d = \sum_{d\mid m} \left(\mu\left(\frac{mp^k}{dp^k}\right) a_{dp^k} + \mu\left(\frac{mp^k}{dp^{k-1}}\right) a_{dp^{k-1}}\right) =$$

$$= \left(a_{mp^k} - a_{mp^{k-1}}\right) + \sum_{(d\mid m)\wedge(d\neq m)} \mu\left(\frac{m}{d}\right)\left(a_{dp^k} - a_{dp^{k-1}}\right),$$

где слагаемые в последней сумме делятся на p^{kr} по индукционному предположению.

Обратно, для проверки делимости суммы из определения последовательности Дольда на n^r достачно проверить делимость на p^{kr} для всех простых $p \mid n$ и $k = v_p(n)$, которая вытекает сразу же из приведённой выше выкладки.

□

Следствие 2.3. Последовательности Дольда r-го порядка со значениями в кольце R образуют подкольцо в кольце всех последовательностей со значениями в R с поточечными операциями сложения и умножения.

Доказательство. При сложении и умножении последовательностей сравнения $a_{mp^k} \equiv a_{mp^{k-1}} \pmod{p^k R}$ складываются и умножаются для операндов. □

Ключевой пример целочисленных последовательностей Дольда 1-го порядка доставляется последовательностями вида $a_k = \mathrm{Tr}(A^k)$, где $A \in M_r(\mathbb{Z})$.

Доказательство сравнения $\mathrm{Tr}(A^p) = \mathrm{Tr}(A) \pmod{p}$ для простого p опубликовано еще в 1846 [14]. То же сравнение в примарном случае $\mathrm{Tr}\left(A^{p^k}\right) \equiv \mathrm{Tr}\left(A^{p^{k-1}}\right) \pmod{p^k}$, которое по Предложению 2.1 равносильно сравнению

$$\sum_{d\mid n} \mu\left(\frac{n}{d}\right) \mathrm{Tr}\left(A^d\right) \equiv 0 \pmod{n}, \tag{3}$$

было доказано в 1921 г. [10]. Исайя Шур передоказал последнее утверждение в 1937 г. [13], используя большие вектора Витта, в тот момент еще не изобретённые. Комбинаторное доказательство предложил C. J. Smyth [15]. Г. Олмквист переоткрыл соотношение (3) в 1983 г., см. его препринт [1]. В XXI веке интерес к этому соотношению оживил В. И. Арнольд [2], свой вариант доказательства опубликовали Э. Б. Винберг [3] и даже П. Делинь [8]. Детальный исторический обзор на 2008 год имеется в работе [4].

Комбинаторное доказательство сравнения (3) для фиксированного n достаточно провести для квадратной матрицы с неотрицательными целыми компонентами, а такую матрицу можно проинтерпретировать как матрицу смежности $A = A(G)$ для некоторого ориентированного графа G с петлями и кратными ребрами. Мы считаем, что вершины графа пронумерованы от 1 до r и компоненты a_{ij} равна числу стрелок, направленных их i-й вершины в j-ю. Тогда $\mathrm{Tr}\left(A^k\right)$ вычисляет количество различных траекторий длины k в графе, с совпадающими началом и концом. Так как число апериодических траекторий длины d с совпадающими началом и концом равно $db_d(G)$, где $b_d(G)$ — число апериодических замкнутых

траекторий без выбора начала, то $\operatorname{Tr}(A(G)^n) = \sum\limits_{d|n} db_d(G)$ и, по формуле обращения Мёбиуса, $b_n(G) = \frac{1}{n}\sum\limits_{d|n} \mu\left(\frac{n}{d}\right) \operatorname{Tr}\left(A(G)^d\right)$, что доказывает (3).

Последовательность $\operatorname{Tr}(A^k)$, где $A \in M_r(\mathbb{Q})$ — это линейная рекуррентная последовательность рациональных чисел. На вопрос, исчерпываются ли последовательностями указанного вида с целочисленной матрицей A все линейные рекуррентные целочисленные последовательности Дольда 1-го порядка, утвердительный ответ даётся в препринте [1] и работе [12].

К сожалению, похожая разумная характеризация последовательностей Дольда старших порядков, по-видимому, невозможна. Мы предполагаем, что нет нетривиальных линейных рекуррентных последовательностей Дольда 2-го порядка. Имеется серия последовательностей Дольда 2-го порядка и выше, удовлетворяющих линейному рекуррентному соотношению с непостоянными коэффициентами, изучение которых началось с открытия чисел Апери в 1980-ые. Этому направлению посвящено множество работ, ссылки на которые мы не приводим.

3. Сравнение Якобшталя

Классическое сравнение Вольстенхольма $\binom{2p}{p} \equiv 2 \pmod{p^3}$ для простого $p \geqslant 5$ было в 1940-ые распространено на примарный случай немецким математиком еврейского происхождения Е. Якобшталем, который был вынужден бежать в 30-ые годы в Тронхейм, и его норвежскими коллегами [9], [7]. Согласно [7], ещё в 1934 г. Вигго Брун заметил, что $v_2\left(\binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}}\right) \geqslant 2n$. Фьельдстад установил в 1942 г., отвечая на вопрос, поставленный Якобшталем, что $v_2\left(\binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}}\right) \geqslant 3n$ при $n \geqslant 2$, и сразу же за ним Льюнгрен [11] показал, что $v_p\left(\binom{p^{n+1}}{p^n} - \binom{p^n}{p^{n-1}}\right) \geqslant 3n + \epsilon$, где $\epsilon = 2$ для простого $p \geqslant 5$ и $\epsilon = 1$ для $p = 3$. В работе [7] доказательства Фьелдстада и Льюнгрена опубликованы на английском языке и Якобшталь точно определяет $v_p\left(\binom{ap^n}{bp^m} - \binom{ap^{n-1}}{bp^{m-1}}\right)$ в терминах чисел Бернулли. Впоследствии результат Якобшталя переоткрывался рядом авторов, включая работу [5]. Из теоремы Якобшталя следует, что $v_p\left(\binom{2p^n}{p^n} - \binom{2p^{n-1}}{p^{n-1}}\right) \geqslant 3n - \epsilon$, где $\epsilon = -1$ при $p = 3$, а также в случае, когда $p = 2$ и $n = 1$. В остальных случаях $\epsilon = 0$.

Учитывая предложение 2.2 мы заключаем, что справедлива теорема:

Теорема 3.1. Имеет место сравнение

$$\sum_{d|n} \mu\left(\frac{n}{d}\right)\binom{2d}{d} \equiv 0 \pmod{n^2}. \tag{4}$$

При этом для n, не делящегося на 2 и на 3, справедливо сравнение

$$\sum_{d|n} \mu\left(\frac{n}{d}\right)\binom{2d}{d} \equiv 0 \pmod{n^3}. \tag{5}$$

Мы рассмотрим в этом разделе комбинаторное доказательство ослабленной формы сравнения Якобшталя. Начнём с комбинаторного доказательства сравнения Вольстенхольма в его ослабленной версии $\binom{2p}{p} \equiv 2 \pmod{p^2}$. Обозначим через $C_p \times C_p$ нециклическую группу порядка p^2. Рассмотрим её как подгруппу, порожденную двумя независимыми циклами длины p в S_{2p}, и соответствующее действие $C_p \times C_p$ на $2p$ точках, которое индуцирует действие той же группы на множестве из $\binom{2p}{p}$ двуцветных раскрасок $2p$ точек таких, что количество точек первого и второго цвета одинаково и равно p. Ясно, что раскраска неподвижна относительно действия нашей группы в том и только в том случае, когда все точки каждого из двух p-блоков

покрашены в одинаковый цвет. Таких раскрасок две. Если же в одном из p-блоков встречаются точки обоих цветов, то и во втором p-блоке встречаются точки обоих цветов, поскольку количество точек каждого цвета равно p. Таким образом, оставшиеся $\binom{2p}{p} - 2$ раскрасок разбиваются на орбиты длины p^2, откуда следует ослабленное сравнение Вольстенхольма.

Автор работы [15] предложил вместо элементарных абелевых p-групп изучать действия на раскрасках силовских p-подгрупп симметрической группы. Хорошо известно, что силовская p-подгруппа P_k в S_{p^k} представляет собой итерированное сплетение, то есть строится следующим образом: полагаем $P_1 = C_p \subset S_p$ — циклическая группа, порождённая циклом длины p; $P_2 = C_p \wr C_p \subset S_{p^2}$ — группа порядка p^{p+1} и $P_{i+1} = P_i \wr C_p = (P_i \times \cdots \times P_i) \leftthreetimes C_p$, где прямое произведение действует на p блоках размера p^i, а правый сомножитель полупрямого произведения переставляет блоки.

Из конструкции ясно, что P_k можно описать также как сплетение $C_p \wr P_{k-1} = (C_p)^{p^{k-1}} \leftthreetimes \leftthreetimes P_{k-1}$, в котором сомножители прямого произведения $(C_p)^{p^{k-1}}$ действуют независимо на p^{k-1} блоках размера p, а P_{k-1} переставляет p-блоки. Аналогично, мы для каждого i можем описать P_k как сплетение $P_i \wr P_{k-i} = (P_i)^{p^{k-i}} \leftthreetimes P_{k-i}$, в котором сомножители прямого произведения, изоморфные P_i, действуют по отдельности на p^{k-i} штук блоков размера p^i, а группа P_{k-i} переставляет блоки.

Для действия группы $P_k \subset S_{p^k}$ на раскрасках p^k точек в несколько цветов заметим, что раскраски, стабилизатор которых содержит подгруппу $(P_i)^{p^{k-i}} \lhd P_k$ — это те раскраски, в которых точки каждого p^i-блока имеют одинаковый цвет, и они отождествляются с раскрасками множества из p^{k-i} точек вместе с действием P_{k-i}. Раскраску будем называть *неприводимой* относительно действия P_k, если её стабилизатор не содержит подгруппу $(C_p)^{p^{k-1}}$. Очевидно, что количество неприводимых раскрасок p^k -элементного множества в два цвета, в которых в первый цвет раскрашено bp точек, равно $\binom{p^k}{bp} - \binom{p^{k-1}}{b}$. Если для данной раскраски i — максимальное такое, что стабилизатор раскраски содержит $P_i^{p^{k-i}}$, то данная раскраска отвечает неприводимой раскраске множества, состоящего из p^{k-i} блоков размера p^i.

Предложение 3.2. Для действия группы P_k на множестве неприводимых двуцветных раскрасок множества из p^k точек, в которых в первый цвет раскрашено b точек, все орбиты имеют длину, делящуюся на $k + v_p(b) + \epsilon$, где $\epsilon = -1$ при $p = 2$ и чётном b и $\epsilon = 0$ в остальных случаях.

Доказательство. Проведем доказательство индукцией по k, используя разложение $P_k = P_{k-1} \wr C_p$, которому отвечает разбиение p^k-элементного множества на p блоков размера p^{k-1}. Ограничивая данную неприводимую раскраску на каждый блок мы получаем p раскрасок, из которых по крайней мере одна будет неприводимой по отношению к действию P_{k-1}.

I случай. Предположим, что некоторый элемент группы P^k, переставляющий p блоков размера p^{k-1} по циклу, переводит данную раскраску в себя. Тогда все p блоков раскрашены по существу одинаково, в каждом из блоков в первый цвет раскрашено b' точек, где $b = pb'$. Все раскраски неприводимы и имеют одинаковую длину орбиты действия P_{k-1}, эта длина делится на $p^{k-1+v_p(b')+\epsilon}$ по индукционному предположению. Тогда длина орбиты P_k для исходной раскраски делится на $p^{p(k-1+v_p(b')+\epsilon)}$. Легко проверяется, что $p(k-1+v_p(b')+\epsilon) \geqslant k+(1+v_p(b'))+\epsilon$.

II случай. Если не все блоки раскрашены одинаково, то длина орбиты данной раскраски будет равна произведению длин орбит для раскрасок каждого блока, дополнительно домноженному на p, поскольку циклическая перестановка блоков меняет раскраску. Пусть b' — количество точек, покрашенных в первый цвет, в выбранном нами блоке с неприводимой относительно P_{k-1} раскраской. Если $v_p(b') \geqslant v_p(b) + 1$, то требуемое сразу же следует по индукционному предположению, примененному к выбранному блоку. Далее разбираем случай, когда $v_p(b') \leqslant v_p(b)$. Может случиться так, что некоторые из оставшихся p блоков раскрашены монохромно. Но заведомо можно утверждать, что найдется другой блок, в котором в первый цвет раскрашено b'' точек, где $i = v_p(b'') \leqslant v_p(b')$. Пускай для раскраски второго блока

j —- максимальное такое, что все подблоки размера p^j раскрашены мнохромно. Тогда $j \leqslant i$ и раскраске второго блока отвечает неприводимая по отношению к P_{k-j} раскраска множества из p^{k-j} блоков размера p^j. По индукционному предположению, длина P_{k-j} -орбиты этой раскраски делится на $p^{k-j+(v_p(b'')-j)+\epsilon}$, следовательно, на $p^{k-j+\epsilon}$.

Тогда искомая длина P_k -орбиты исходной раскраски делится на

$$p^{k-1+v_p(b')+\epsilon} \cdot p^{k-j+\epsilon} \cdot p = p^{2k+(v_p(b')-j)+2\epsilon}.$$

Осталось заметить, что $v_p(b') \geqslant v_p(b'') \geqslant j$ и $k + 2\epsilon \geqslant v_p(b) + \epsilon$ поскольку $v_p(b) \leqslant k-1$. □

Для $p = 2$ предложение 3.2 при $k = n+1$ и $b = 2^n$ является комбинаторным доказательством сравнения $\binom{2^{n+1}}{2^n} \equiv \binom{2^n}{2^{n-1}} \pmod{2^{2n}}$.

Следствие 3.3. Рассмотрим естественное действие группы $P_k \times P_k$ на множестве M из $p^k + p^k$ элементов и индуцированное действие на подмножестве из $\binom{2p^k}{p^k}$ двухцветных раскрасках. Тогда неприводимые раскраски имеют длину орбиты, делящуюся на p^{2k}.

Доказательство. Если две группы G_1, G_2 действуют на множествах M_1 и M_2, то возникает естественное действие $G = G_1 \times G_2$ на множестве раскрасок $A^{M_1 \sqcup M_2} = A^{M_1} \times A^{\times M_2}$ дизъюнктного объединения $M = M_1 \sqcup M_2$ в цвета из множества A. Орбита раскраски $\theta = (\theta_1, \theta_2)$, где $\theta_i : M_i \to A$ — раскраски частей M, равна прямому произведению орбит $G_1\theta_1 \times G_2\theta_2 \subset A^{M_1} \times A^{M_2}$. В рассматриваемой ситуации $G_i = P_k$, а M_1, M_2 — это p^k-элементные множества. Если для раскраски θ каждая из двух раскрасок p^k-элементных частей θ_i будет неприводима, то $p^k \mid |G_i\theta_i|$ и $p^{2k} \mid |G_1\theta_1| \cdot |G_2\theta_2| = |G\theta|$.

Если же неприводима только одна из раскрасок, скажем, θ_1, и число точек из M_1, покрашенных в первый цвет, равно b, то число точек в M_2, покрашенных в первый цвет, равно $p^k - b$ и $v_p(b) = v_p\left(p^k - b\right) = i$. Так что даже в том случае, когда вторая раскраска приводима, она отвечает неприводимой относительно P_{k-j} раскраске p^{k-j}-элементного множества для некоторого $j \leqslant i$ и по предложению 3.2 $|G_2\theta_2|$ делится на p^{k-j}. Так как $|G_1\theta_1|$ делится на p^{k+i}, перемножая, получаем требуемое.

□

Два замечания в заключение. Во-первых, отметим, что сумму $\sum\limits_{d|n} \mu\left(\frac{n}{d}\right)\binom{2d}{d}$ можно интерпретировать как подсчет числа раскрасок $2n$ точек в два цвета таких, что в каждый цвет раскрашено по n точек и раскраска является неприводимой по отношению к действию силовской подгруппы $P \subset S_{2n}$ для каждого простого $p \mid n$. Так что сравнение (4) следует также из анализа длин орбит неприводимых раскрасок по отношению к действию прямого произведения всех силовских подгрупп в S_{2n}. Действуя по указанной схеме, можно было бы избежать ссылки на утверждение 2.2, носящее некомбинаторный характер.

Во-вторых, задача определения минимальной длины орбиты неприводимой раскраски представляется интересной сама по себе и остается открытой.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Almkvist G. Integrity of ghosts // Preprint. — 1983. — URL: https://arxiv.org/abs/math/0612443 (дата обращения: 01.01.2024).

2. Арнольд В. И. Матричная теорема Эйлера–Ферма // Известия Российской академии наук. Серия математическая. — 2004. — Т. 68, № 6. — С. 3–24.

3. Винберг Э. Б. Малая теорема Ферма и ее обобщения // Математическое просвещение. Серия 3. — 2008. — Вып. 12. — С. 7–17.

4. Зарелуа А. В. О сравнениях для следов степеней некоторых матриц // Труды Математического института имени В. А. Стеклова. — 2008. — Т. 263. — С. 85–105.

5. Трахтман Ю. А. О делимости некоторых разностей, составленных из биномиальных коэффициентов // Доклады Академии наук Армянской ССР. — 1974. — Т. 59. — С. 10–16.

6. Byszewski J., Graff G., Ward T. Dold sequences, periodic points, and dynamics // Bulletin of the London Mathematical Society. — 2021. — Vol. 53. — P. 1263–1298.

7. Brun V., Stubban J. O., Fjeldstad J. E., Tambs-Lyche R., Aubert K. E., Ljunggren W., Jacobsthal E. On the divisibility of the difference between two binomial coefficients // Den 11te Skandinaviske Matematikerkongress, Trondheim 1949. — 1952. — P. 42–54.

8. Deligne P. Extended Euler congruence // Functional Analysis and Other Mathematics. — 2009. — Vol. 2. — P. 249–250.

9. Jacobsthal E. Tallteoretiske egenskaper ved binominalkoeffisientene // Norske Videnskabers Selskabs Skrifter (Trondheim). — 1945. — No. 4. — P. 1–28.

10. Jänichen W. Über die Verallgemeinerung einer Gaussschen Formel aus der Theorie der höheren Kongruenzen // Sitzungsberichte der Berliner Mathematischen Gesellschaft. — 1921. — Vol. 20. — P. 23–29.

11. Ljunggren W. Eine Eigenschaft der mittleren Binomialkoeffizienten // Norsk Matematisk Tidsskrift. — 1942. — Vol. 24. — P. 18–22.

12. Minton G. T. Linear recurrence sequences satisfying congruence conditions // Proceedings of the American Mathematical Society. — 2014. — Vol. 142, No. 7. — P. 2337–2352.

13. Schur I. Arithmetische Eigenschaften der Potenzsummen einer algebraischen Gleichung // Compositio Mathematica. — 1937. — Vol. 272. — P. 432–444.

14. Schönemann T. Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist // Journal für die reine und angewandte Mathematik. — 1846. — Vol. 31. — P. 269–325.

15. Smith J. H. Combinatorial Congruences from p-subgroups of the Symmetric Group // Graphs and Combinatorics. — 1993. — Vol. 9. — P. 293–304.

16. Smyth C. J. A coloring proof of a generalization of Fermat's little theorem // The American Mathematical Monthly. — 1986. — Vol. 93. — P. 469–471.

REFERENCES

1. Almkvist, G. 1983, "Integrity of ghosts", *Preprint*, Available at: https://arxiv.org/abs/math/0612443.

2. Arnold, V.I. 2004, "The Matrix Euler-Fermat theorem", *Izvestiya: Mathematics*, 68(6), pp. 1119–1128.

3. Vinberg, E.B. 2008, "Fermat's little theorem and generalizations", *Matematicheskoe Prosveshchenie*, 12, pp. 43–54.

4. Zarelua, A.V. 2008, "On congruences for the traces of powers of some matrices", *Proceedings of the Steklov Institute of Mathematics*, 263, pp. 78–98.

5. Trachtman, Yu.A. 1974, "On the divisibility of certain differences, formed from binomial coefficients", *Doklady Akademii Nauk Armyanskoi SSR*, 59, pp. 10–16.

6. Byszewski, J., Graff, G., and Ward, T. 2021, "Dold sequences, periodic points, and dynamics", *Bulletin of the London Mathematical Society*, 53, pp. 1263–1298.

7. Brun, V., Stubban, J.O., Fjeldstad, J.E., Tambs-Lyche, R., Aubert, K.E., Ljunggren, W., and Jacobsthal, E. 1952, "On the divisibility of the difference between two binomial coefficients", in *Den 11te Skandinaviske Matematikerkongress, Trondheim 1949*, pp. 42–54.

8. Deligne, P. 2009, "Extended Euler congruence", *Functional Analysis and Other Mathematics*, 2, pp. 249–250.

9. Jacobsthal, E. 1945, "Tallteoretiske egenskaper ved binominalkoeffisientene", *Norske Videnskabers Selskabs Skrifter (Trondheim)*, 4, pp. 1–28.

10. Jänichen, W. 1921, "Über die Verallgemeinerung einer Gaussschen Formel aus der Theorie der höheren Kongruenzen", *Sitzungsberichte der Berliner Mathematischen Gesellschaft*, 20, pp. 23–29.

11. Ljunggren, W. 1942, "Eine Eigenschaft der mittleren Binomialkoeffizienten", *Norsk Matematisk Tidsskrift*, 24, pp. 18–22.

12. Minton, G.T. 2014, "Linear recurrence sequences satisfying congruence conditions", *Proceedings of the American Mathematical Society*, 142(7), pp. 2337–2352.

13. Schur, I. 1937, "Arithmetische Eigenschaften der Potenzsummen einer algebraischen Gleichung", *Compositio Mathematica*, 272, pp. 432–444.

14. Schönemann, T. 1846, "Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist", *Journal für die reine und angewandte Mathematik*, 31, pp. 269–325.

15. Smith, J.H. 1993, "Combinatorial Congruences from p-subgroups of the Symmetric Group", *Graphs and Combinatorics*, 9, pp. 293–304.

16. Smyth, C.J. 1986, "A coloring proof of a generalization of Fermat's little theorem", *The American Mathematical Monthly*, 93, pp. 469–471.

Получено: 13.06.2025
Принято в печать: 17.10.2025