ЧЕБЫШЕВСКИЙ СБОРНИК
Том 24. Выпуск 4.

УДК 511.512 DOI 10.22405/2226-8383-2023-24-4-252-263

О некоторых арифметических применениях к теории симметрических групп

У. М. Пачев, Р. А. Дохов, А. Х. Кодзоков, М. С. Нирова

Пачев Урусби Мухамедович — доктор физико-математических наук, профессор, Кабардино-Балкарский государственный университет им. Х. М. Бербекова (г. Нальчик); Северо-Кавказский центр математических исследований (г. Ставрополь).
e-mail: urusbi@rambler.ru

Дохов Резуан Ауесович — кандидат физико-математических наук, Северо-Кавказский центр математических исследований (г. Ставрополь).
e-mail: rezuan.dokhov@yandex.ru

Кодзоков Азамат Хасанович — Кабардино-Балкарский государственный университет им. Х. М. Бербекова (г. Нальчик).
e-mail: Kodzoko@mail.ru

Нирова Марина Сефовна — кандидат физико-математических наук, доцент, Кабардино-Балкарский государственный университет им. Х. М. Бербекова (г. Нальчик).
e-mail: nirova_m@mail.ru

Аннотация

Работа посвящена некоторым арифметическим применениям к теории симметрических групп. С помощью свойств сравнений и классов вычетов из теории чисел установлено существование в симметрической группе S_n степени n циклических, абелевых и неабелевых подгрупп соответственно порядков k, $\varphi(k)$ и $k\varphi(k)$, где $k \leq n$, φ – функция Эйлера, т.е. получены представления групп $(\mathbb{Z}/k\mathbb{Z}, +)$, $(\mathbb{Z}/k\mathbb{Z})^*$ и их произведения через подстановки степени k. При этом изоморфные вложения этих групп строятся, следуя доказательству теоремы Кэли, но наряду с этим используется понятие линейного перестановочного двучлена $\overline{a}x + \overline{b}$ кольца вычетов $\mathbb{Z}/k\mathbb{Z}$, где НОД $(a, k) = 1$.

Кроме того, результат, относящийся к изоморфному вложению группы $(\mathbb{Z}/k\mathbb{Z})^*$ в группу S_k распространяется на знакопеременную группу A_k при нечётных k.

Во второй части работы рассматриваются некоторые применения теории простых чисел к циклическим подгруппам симметрической группы S_n. В частности, применяя формулу суммирования Эйлера-Маклорена и оценки для k-го простого числа, получена нижняя оценка для максимального числа простых делителей порядков циклических подгрупп в симметрической группе S_n.

Ключевые слова: симметрическая группа, порядок подгруппы, сравнение по модулю, функция Эйлера, знак подстановки, квадратичные вычеты, перестановочный многочлен, простой делитель порядка циклической подгруппы.

Библиография: 22 названия.

Для цитирования:
У. М. Пачев, Р. А. Дохов, А. Х. Кодзоков, М. С. Нирова. О некоторых арифметических применениях к теории симметрических групп // Чебышевский сборник, 2023, т. 24, вып. 4, с. 252–263.

CHEBYSHEVSKII SBORNIK

Vol. 24. No. 4.

UDC 511.512 DOI 10.22405/2226-8383-2023-24-4-252-263

On Some arithmetic applications to the theory of symmetric groups

U. M. Pachev, R. A. Dokhov, A. Kh. Kodzokov, M. S. Nirova

Pachev Urusbi Mukhamedovich — doctor of physical and mathematical sciences, professor, Berbekov Kabardino–Balkarian State University (Nalchik); North–Caucasus Federal University (Stavropol).

e-mail: urusbi@rambler.ru

Rezuan Auesovich Dokhov — candidate of physical and mathematical sciences, assistant professor, North–Caucasus Federal University (Stavropol).

e-mail: rezuan.dokhov@yandex.ru

Azamat Khasanovich Kodzokov — Berbekov Kabardino–Balkarian State University (Nalchik).

e-mail: Kodzoko@mail.ru

Marina Sefovna Nirova — candidate of physical and mathematical sciences, assistant professor, Berbekov Kabardino–Balkarian State University (Nalchik).

e-mail: nirova_m@mail.ru

Abstract

The work is devoted to some arithmetic applications to the theory of symmetric groups. Using the properties of congruences and classes of residues from number theory, the existence in the symmetric group S_n of degree n of cyclic, Abelian and non-Abelian subgroups respectively, of orders is establisned k, $\varphi(k)$, and $k\varphi(k)$, where $k \leq n$, φ – Euler function, those representations jf grups $(\mathbb{Z}/k\mathbb{Z}, +)$, $(\mathbb{Z}/k\mathbb{Z})^*$ and theorem product in the form of degree substitutions k. In this case isomorphic embeddings of these groups are constructed following the proof of Cayley's theorem, but along with this, a linear binomial is used $\mathbb{Z}/k\mathbb{Z}$ residue class rings, where $\gcd(a, k) = 1$.

In addition, the result concerning the isomorphic embedding of a group $(\mathbb{Z}/k\mathbb{Z})^*$ in to a group $(\mathbb{Z}/k\mathbb{Z})^*$ in to a group S_k extends to an alternating group A_k for odd k.

The second part of the work examines some applications of prime number theory to cyclic subgroups of the symmetric group S_n. In particular, applying the Euler-Maclaurin summation formula and bounds for the k in prime, a lower bound for maximum number of prime divisors of cyclic orders in the summetric group S_n.

Keywords: symmetric group, subgroup order, modulo congruence, Euler function, substitution sign, quadratic residnes, permutation polynomial, prime divisor of cyclic subgroup order.

Bibliography: 22 titles.

For citation:

U. M. Pachev, R. A. Dokhov, A. Kh. Kodzokov, M. S. Nirova, 2023, "On Some arithmetic applications to the theory of symmetric groups" , *Chebyshevskii sbornik*, vol. 24, no. 4, pp. 252–263.

1. Введение

Хорошо известны применения теоретико-групповых методов в теории чисел (см. [1]). В свою очередь и теория чисел, также имеет полезные применения к группам подстановок. Одним из первых применений теоретико-числовых результатов к теории симметрических групп является постулат Бертрана [2] о простых числах (между натуральными числами n и $2n$ при $n > 1$ содержится хотя бы одно простое число), из которого следует, что симметрическая группа S_n не имеет подгрупп, индекс i которых удовлетворяет неравенствам $2 < i < n$ при $n > 4$. Постулат Бертрана был доказан Чебышевым в 1852 г.

Дальнейшие применения теории чисел к вопросу нахождения максимального порядка подстановки заданной степени даны Э. Ландау [3], доказавшему асимптотику

$$\log g(n) \sim \sqrt{n \log n},$$

где $g(n)$ — максимальный порядок элемента симметрической группы S_n. Спустя 36 лет С. Шах [4] уточнил асимптотику Ландау, представив оценку сверху для $\left|\log G(n) - \sqrt{n \log n}\right|$ (в дальнейших публикациях функцию Ландау $g(n)$ стали обозначать $G(n)$).

Продолжая эти исследования по оценке функции Ландау $G(n)$ Дж. Массиас [5], получил явную верхнюю границу для $G(n)$ и определил значение n, при котором $\log G(n) - \sqrt{n \log n}$ достигает своего максимума. М. Салаи [6] несколько усилил результат С. Шаха, а также дал оценку максимального порядка элемента симметрической полугруппы с единицей.

Дальнейшие проведённые исследования связаны со свойствами функции $G(n)$.
Так Дж. Николя [7] установлено одно свойство делимости $G(n)$ на простые числа. Сравнивая $G(n)$ с n, М. Натансон [8] доказал, что $G(n)$ растёт быстрее, чем любая степень числа n с ограниченным показателем. Особенно интересный результат получен Дж. Николя [7], согласно которому существуют длинные цепочки последовательных целых чисел, для которых $G(n)$ является стационарной.

Все результаты исследований, приведённых до 1987 г. относительно функции $G(n)$ описаны В. Миллер [9] с полным обзором используемых методов.

С несколько другой точки зрения проводились также исследования по арифметическим применениям к теории симметрических групп У. М. Пачевым и В. Н. Шокуевым [10], основанные на свойствах сравнений и классов вычетов по модулю и арифметических функций.

В последнее время проводилось также исследование и по применениям теоретико-числовых функций к вопросу о максимальном значении числа простых делителей порядков циклических подгрупп симметрической группы S_n (см. предварительное сообщение [11]).

2. О подгруппах симметрических групп, получаемых с помощью классов вычетов по данному модулю

В этой части рассматривается один арифметический способ построения подгрупп в симметрической группе S_m степени m, основанный на свойствах сравнений или классов вычетов по заданному модулю (см. [10]). Однако, изложение результатов в указанной работе далеко не полно и обычно не содержит доказательств (или они лишь намечены). В связи с этим, даём более совершенное изложение, делая его более разработанным в деталях.

Наше изложение основано на следующем свойстве полных систем вычетов по модулю m.

Лемма 1. *Если $(a, m) = 1$ и x пробегает полную систему вычетов по модулю m, то $ax + b$, где b – целое число, тоже пробегает полную систему вычетов по модулю m.*

Доказательство даётся в [12].

Иногда при обсуждении арифметических и алгебраических проблем бывает удобнее работать с кольцом классов вычетов $\mathbb{Z}/m\mathbb{Z}$ по модулю m. В виду этого, лемму 1 можно переформулировать в следующем виде.

Лемма 2. *Если* $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^*$, *т.е.* $(a, m) = 1$, *то* $\left\{\overline{a}\,\overline{x} + \overline{b} \mid \overline{x} \in \mathbb{Z}/m\mathbb{Z}\right\} = \mathbb{Z}/m\mathbb{Z}$.

Доказательство непосредственно следует из леммы 1 и определений классов вычетов вместе с операциями над ними.

Поставим теперь во взаимно однозначное соответствие каждому линейному двучлену $\overline{a}\,\overline{x} + \overline{b}$, где НОД$(a, m) = 1$ подстановку из симметрической группы S_m степени m по следующему правилу

$$\overline{a}\,\overline{x} + \overline{b} \leftrightarrow \begin{pmatrix} \overline{1} & \overline{2} & \cdots & \overline{m} \\ \overline{a}\cdot\overline{1} + \overline{b} & \overline{a}\cdot\overline{2} + \overline{b} & \cdots & \overline{a}\cdot\overline{m} + \overline{b} \end{pmatrix}. \tag{1}$$

Ввиду леммы 2, нижняя строка в подстановке (1) представляет собой некоторую перестановку элементов верхней строки.

Соответствие вида (1) имеет место и в симметрической группе S_k ввиду её изоморфной вложенности в S_m, где $2 \le k \le m$, при этом используется кольцо классов вычетов $\mathbb{Z}/k\mathbb{Z}$.

Обозначим подстановку вида (1) через $\tau_{\overline{a},\overline{b}}(m)$, т.е.

$$\tau_{\overline{a},\overline{b}}(m) = \begin{pmatrix} \overline{1} & \overline{2} & \cdots & \overline{m} \\ \overline{a}\cdot\overline{1} + \overline{b} & \overline{a}\cdot\overline{2} + \overline{b} & \cdots & \overline{a}\cdot\overline{m} + \overline{b} \end{pmatrix}.$$

Рассмотрим также подстановки вида

$$\tau_{\overline{a},\overline{b}}(k) = \begin{pmatrix} \overline{1} & \overline{2} & \cdots & \overline{k} \\ \overline{a}\cdot\overline{1} + \overline{b} & \overline{a}\cdot\overline{2} + \overline{b} & \cdots & \overline{a}\cdot\overline{k} + \overline{b} \end{pmatrix}, \tag{2}$$

где $2 \le k \le m$; $\overline{a} \in (\mathbb{Z}/k\mathbb{Z})^*$, $\overline{b} \in \mathbb{Z}/k\mathbb{Z}$.

Обозначим множество всех подстановок вида (2) через $H_{k\varphi(k)}$, т. е.

$$H_{k\varphi(k)} = \left\{\tau_{\overline{a},\overline{b}}(k) \mid \overline{a} \in (\mathbb{Z}/k\mathbb{Z})^*, \quad \overline{b} \in \mathbb{Z}/k\mathbb{Z}\right\},$$

где φ — функция Эйлера.

Теорема 1. *Множество подстановок* $H_{\varphi(k)} = \left\{\tau_{\overline{a},\overline{0}}(k) \mid \overline{a} \in (\mathbb{Z}/k\mathbb{Z})^*\right\}$ *степени* $2 \le k \le m$ *образует абелеву подгруппу порядка* $\varphi(k)$ *группы* S_k, *изоморфную группе* $(\mathbb{Z}/k\mathbb{Z})^*$, *где* φ – *функция Эйлера.*

Доказательство. Покажем замкнутость $H_{\varphi(k)}$ относительно умножения подстановок. Пусть $\tau_{\overline{a},\overline{0}}(k),\ \tau_{\overline{c},\overline{0}}(k) \in H_{\varphi(k)}$, где $\overline{a},\ \overline{c} \in (\mathbb{Z}/k\mathbb{Z})^*$. Тогда

$$\tau_{\overline{a},\overline{0}}(k) \cdot \tau_{\overline{c},\overline{0}}(k) = \tau_{\overline{a}\,\overline{c},\overline{0}}(k) \in H_{\varphi(k)},$$

так как $\overline{a}, \overline{c} \in (\mathbb{Z}/k\mathbb{Z})^*$. Кроме того, $\tau^{-1}_{\overline{a},\overline{0}}(k) = \tau_{\overline{a}^{-1},\,\overline{0}}(k) \in H_{\varphi(k)}$.

Значит, $H_{\varphi(k)} < S_k$. Пользуясь теперь взаимно однозначным соответствием $\tau_{\overline{a},\,\overline{0}}(k) \leftrightarrow \overline{a}$, получаем, что $H_{\varphi(k)} \cong (\mathbb{Z}/k\mathbb{Z})^*$. Из этого изоморфизма следует, что $H_{\varphi(k)}$ — абелева подгруппа в S_k, так как $(\mathbb{Z}/k\mathbb{Z})^*$ — абелева группа, и значит,

$$\left|H_{\varphi(k)}\right| = |(\mathbb{Z}/k\mathbb{Z})^*| = \varphi(k), \quad \text{ч.т.д.}$$

□

Теорема 2. *Множество подстановок вида* $H_k = \left\{\tau_{\overline{1},\,\overline{b}}(k) | \overline{b} \in \mathbb{Z}/k\mathbb{Z}\right\}$ *образует циклическую подгруппу в группе* S_k*, изоморфную аддитивной группе классов вычетов* $\mathbb{Z}/k\mathbb{Z}$.

Доказательство проводится по той же схеме, что и в случае теоремы 1, но учитывая при этом следующее соответствие $\tau_{\overline{1},\,\overline{b}}(k) \leftrightarrow \overline{b} \in \mathbb{Z}/k\mathbb{Z}$.

Результат теоремы 1 можно перенести на соответствующие абелевы подгруппы знакопеременной группы A_k нечётной степени k. Для этого рассмотрим нужное нам обобщение одной леммы Золотарёва [14] о знаке подстановки из симметрической группы S_p, где p — простое число. Сформулируем её в наших обозначениях.

Лемма 3 (Золотарёв).

Знак подстановки $\tau_{\overline{a},\,\overline{0}}(p)$, где $\overline{a} \in (\mathbb{Z}/k\mathbb{Z})^*$, p — нечётное простое число, равен символу Лежандра $\left(\frac{a}{p}\right)$, т.е. $\operatorname{sgn}\tau_{\overline{a},\,\overline{0}}(p) = \left(\frac{a}{p}\right)$.

Обобщение леммы Золотарёва даём в следующем виде.

Лемма 4.

Если k — нечётное число и число a взаимно просто с k, то знак подстановки $\tau_{\overline{a},\,\overline{0}}(k) \in S_k$ при $\overline{a} \in (\mathbb{Z}/k\mathbb{Z})^*$ определяется соотношением $\operatorname{sgn}\tau_{\overline{a},\,\overline{0}}(k) = \left(\frac{a}{k}\right)$, где $\left(\frac{a}{k}\right)$ — символ Якоби.

Доказательство представлено в [15] в виде решения ряда взаимосвязанных задач, снабжённых указаниями.

Нам понадобится ещё один результат о квадратичных вычетах.

Лемма 5.

Число квадратичных вычетов в приведённой системе по нечётному модулю n равно $\frac{\varphi(n)}{2^{\upsilon(n)}}$, где φ — функция Эйлера, $\upsilon(n)$ — число простых делителей числа n.

Доказательство. (См. [16]). □

Теорема 3. *Множество подстановок* $H_{k\varphi(k)}$ *образует неабелеву подгруппу порядка* $k\varphi(k)$ *симметрической группы* S_m *при* $3 \le k \le m$*, где* φ *— функция Эйлера.*

Доказательство. Проверяем замкнутость множества $H_{k\varphi(k)}$ относительно операции умножения подстановок.

Имеем

$$\tau_{\overline{a},\overline{b}}(k) \cdot \tau_{\overline{c},\overline{d}}(k) =$$

$$= \begin{pmatrix} \overline{1} & \overline{2} & \cdots & \overline{k} \\ \overline{a}\cdot\overline{1}+\overline{b} & \overline{a}\cdot\overline{2}+\overline{b} & \cdots & \overline{a}\cdot\overline{k}+\overline{b} \end{pmatrix} \cdot$$

$$\begin{pmatrix} \overline{a}\cdot\overline{1}+\overline{b} & \overline{a}\cdot\overline{2}+\overline{b} & \cdots & \overline{a}\cdot\overline{k}+\overline{b} \\ \overline{c}\left(\overline{a}\cdot\overline{1}+\overline{b}\right)+\overline{d} & \overline{c}\left(\overline{a}\cdot\overline{2}+\overline{b}\right)+\overline{d} & \cdots & \overline{c}\left(\overline{a}\cdot\overline{k}+\overline{b}\right)+\overline{d} \end{pmatrix} =$$

$$= \begin{pmatrix} \overline{1} & \overline{2} & \cdots & \overline{k} \\ \overline{c}\cdot\overline{a}\cdot\overline{1}+\overline{b}\cdot\overline{c}+\overline{d} & \overline{c}\cdot\overline{a}\cdot\overline{2}+\overline{b}\cdot\overline{c}+\overline{d} & \cdots & \overline{c}\cdot\overline{a}\cdot\overline{k}+\overline{b}\cdot\overline{c}+\overline{d} \end{pmatrix} =$$

$$\tau_{\overline{a}\cdot\overline{c},\;\overline{b}\cdot\overline{c}+\overline{d}}(k), \tag{3}$$

где

$$\overline{a}\cdot\overline{c} \in (\mathbb{Z}/k\mathbb{Z})^*, \quad \overline{b}\cdot\overline{c}+\overline{d} \in (\mathbb{Z}/k\mathbb{Z}).$$

Из (3) также следует, что

$$\tau_{\overline{a},\overline{b}}(k) = \tau_{\overline{a},\overline{0}}(k) \cdot \tau_{\overline{1},\overline{b}}(k) \tag{4}$$

Следовательно,

$$\tau_{\overline{a},\overline{b}}(k) \cdot \tau_{\overline{c},\overline{d}}(k) = \tau_{\overline{a}\cdot\overline{c},\;\overline{b}\cdot\overline{c}+\overline{d}}(k) \in H_{k\varphi(k)},$$

при этом $\overline{a}\,\overline{c} \in (\mathbb{Z}/k\mathbb{Z})^*$, $\overline{b}\,\overline{c}+\overline{d} \in \mathbb{Z}/k\mathbb{Z}$.

Значит, множество $H_{k\varphi(k)}$ замкнуто относительно операции умножения подстановок.

Покажем теперь существование обратного элемента в $H_{k\varphi(k)}$. Ясно, что $\tau_{\overline{1},\overline{0}}(k) = E$ есть единичная подстановка в симметрической группе S_k. Обозначая через $\tau_{\overline{x},\overline{y}}(k)$ подстановку, обратную к $\tau_{\overline{a},\overline{b}}(k)$ (она существует во всей группе S_k), будем иметь

$$\tau_{\overline{a},\overline{b}}(k) \cdot \tau_{\overline{x},\overline{y}}(k) = \tau_{\overline{1},\overline{0}}(k).$$

Но тогда в силу соотношения (3) имеем

$$\tau_{\overline{a}\cdot\overline{x},\ \overline{b}\cdot\overline{x}+\overline{y}}(k) = \tau_{\overline{1},\overline{0}}(k).$$

Отсюда получаем $\overline{a} \cdot \overline{x} = \overline{1}$, откуда $\overline{x} = \overline{a}^{-1}$ и тогда $\overline{y} = -\overline{b}\overline{a}^{-1}$.

Значит,

$$\tau^{-1}_{\overline{a},\overline{b}}(k) = \tau_{\overline{a}^{-1},\ \overline{b}\overline{a}^{-1}}(k),$$

т.е. $\tau^{-1}_{\overline{a},\overline{b}}(k) \in H_{k\varphi(k)}$.

Следовательно, $H_{k\varphi(k)}$ подгруппа симметрической группы S_m ввиду изоморфной вложенности S_k в S_m при $2 \le k \le m$.

Наконец, докажем, что $\left|H_{k\varphi(k)}\right| = k\varphi(k)$.

Во-первых, ясно, что $H_{k\varphi(k)} = H_k \cdot H_{\varphi(k)} = H_{\varphi(k)} \cdot H_k$, но поэлементной перестановочности нет, и во-вторых, $H_k \cap H_{\varphi(k)} = E$, где E — единичная подстановка. Но тогда (см. [13]) имеем

$$\left|H_{k\varphi(k)}\right| = \frac{|H_k| \cdot \left|H_{\varphi(k)}\right|}{\left|H_k \cap H_{\varphi(k)}\right|} = |H_k| \cdot \left|H_{\varphi(k)}\right| = k\varphi(k), \quad \text{ч.т.д.}$$

Опираясь соответственно на абелевость и цикличность групп $(\mathbb{Z}/k\mathbb{Z})^*$ и $\mathbb{Z}/k\mathbb{Z}$, получаем ещё следующий результат. □

Теорема 4. *В знакопеременной группе A_k нечётной степени k множество подстановок вида $\tau_{\overline{a},\ \overline{0}}(k)$, где $\overline{a} \in (\mathbb{Z}/k\mathbb{Z})^{*2}$, образует абелеву подгруппу порядка $\frac{\varphi(k)}{2^{\upsilon(k)}}$, при этом $(\mathbb{Z}/k\mathbb{Z})^{*2}$ — группа классов квадратичных вычетов по модулю k; φ — функция Эйлера, $\upsilon(k)$ — число простых делителей k.*

Доказательство. 1^0. Сначала покажем, что множество подстановок вида $\tau_{\overline{a},\ \overline{0}}(k)$, при $\overline{a} \in (\mathbb{Z}/k\mathbb{Z})^{*2}$ есть подмножество знакопеременной группы A_k. Для удобства рассуждений обозначим множество таких подстановок через $H_k^{(2)}$. Тогда покажем, что $H_k^{(2)} \subset A_k$. Пусть $\tau_{\overline{a},\ \overline{0}}(k) \in H_k^{(2)}$. Тогда по лемме 4 имеем $\operatorname{sgn}\left(\tau_{\overline{a},\ \overline{0}}(k)\right) = \left(\frac{a}{k}\right) = 1$ ввиду условия $\overline{a} \in (\mathbb{Z}/k\mathbb{Z})^{*2}$. Из этого следует, что $\tau_{\overline{a},\ \overline{0}}(k) \in A_k$ и значит, $H_k^{(2)} \subset A_k$.

2^0. Теперь покажем, что множество $H_k^{(2)}$ образует абелеву подгруппу группы A_k. Пусть $\tau_{\overline{a},\ \overline{0}}(k),\ \tau_{\overline{c},\ \overline{0}}(k) \in H_k^{(2)}$, т.е. $\overline{a},\ \overline{c} \in (\mathbb{Z}/k\mathbb{Z})^{*2}$. Тогда имеем $\tau_{\overline{a},\ \overline{0}}(k) \cdot\ \tau_{\overline{c},\ \overline{0}}(k) = \tau_{\overline{a}\cdot\overline{c},\ \overline{0}}(k) \in H_k^{(2)}$ ввиду того, что $\overline{a}\cdot\overline{c} \in (\mathbb{Z}/k\mathbb{Z})^{*2}$. Учитывая, что рассматриваемые группы являются конечными, можно считать выполненной аксиома об обратном элементе в множестве $H_k^{(2)}$.

Значит, $H_k^{(2)}$ — подгруппа группы A_k, т.е. $H_k^{(2)} < A_k$. Учитывая ещё теорему 1, получаем, что $H_k^{(2)}$ является абелевой подгруппой группы A_k.

3^0. Наконец, в силу леммы 5 получаем, что

$$\left|H_k^{(2)}\right| = \frac{\varphi(k)}{2^{\upsilon(k)}}, \quad \text{ч.т.д.}$$

□

3. Соотношения, связанные с некоторыми циклическими подгруппами симметрической группы

Эта часть нашей работы имеет некоторое отношение к исследованиям относительно функции Ландау, описанным во введении (см. [3]–[9]).

Но в отличие от этих работ, связанных с вопросом о максимальном порядке элементов симметрической группы S_n, мы рассматриваем оценку снизу максимального числа простых делителей порядков циклических подгрупп в S_n. Следующий вспомогательный результат даёт формулу для наименьшего общего кратного первых m натуральных чисел.

Лемма 6.

$$\text{НОК}(1,2,\ldots,m)=\prod_{p\le m}p^{\left[\frac{\log m}{\log p}\right]},$$

где произведение берётся по всем простым числам, не превосходящим m, $[\,]$ — знак целой части действительного числа.

Доказательство. (См. [17]).

□

Теорема 5. *В симметрической группе S_n существует циклическая подгруппа $<\tau>$, порядок которой определяется формулой*

$$|<\tau>|=\prod_{p\le m}p^{\left[\frac{\log m}{\log p}\right]},$$

где $m=\left[\frac{\sqrt{8n+1}-1}{2}\right]$, произведение берётся по всем простым числам, не превосходящим числа m.

Доказательство. Рассмотрим подстановку $\tau\in S_n$, представленную в виде произведения циклов

$$\tau=(a_1)\,(a_2a_3)\cdot\ldots\cdot(a_ma_{m+1}\cdot\ldots\cdot a_{2m-1}),$$

длины которых соответственно равны 1, 2, ..., m. Но, как известно, порядок подстановки, разложенной в циклы, равен наименьшему общему кратному длин циклов, т.е.

$$|<\tau>|=\text{НОК}(1,2,\ldots,m).$$

Но тогда в силу леммы 6, имеем

$$|<\tau>|=\prod_{p\le m}p^{\left[\frac{\log m}{\log p}\right]}.$$

Наконец, так как общее количество элементов в рассматриваемых циклах для подстановки τ не должно превосходить числа n, то

$$1+2+\ldots+m\le n,$$

откуда

$$m=\left[\frac{\sqrt{8n+1}-1}{2}\right],\quad \text{ч.т.д.}$$

□

Результат теоремы 5 позволяет получить нижнюю оценку для максимального числа простых делителей порядков циклических подгрупп группы S_n.

Следствие 1. *Для максимального числа* $\max_{\tau\in S_n}\upsilon\left(|<\tau>|\right)$ *простых делителей порядков циклических подгрупп симметрической группы* S_n *справедливо неравенство*

$$\max_{\tau\in S_n}\upsilon\left(|<\tau>|\right)>0{,}84\frac{\sqrt{n}}{\log(8n+1)}\ .$$

Доказательство. В силу теоремы 5 имеем $\upsilon\left(|<\tau>|\right)=\pi(m)$, где $\pi(m)$ – функция распределения простых чисел, при этом $m=\left[\frac{\sqrt{8n+1}-1}{2}\right]$.

Применяя теорему Чебышева (см. [18]), будем иметь

$$\pi(m)>\frac{\log 2}{2}\cdot\frac{m}{\log m}=\frac{\log 2}{2}\cdot\frac{\left[\frac{\sqrt{8n+1}-1}{2}\right]}{\log\left[\frac{\sqrt{8n+1}-1}{2}\right]}>$$

$$>\frac{\log 2}{2}\cdot\left(\frac{\sqrt{8m+1}-3}{2}\right)/\log\left(\frac{\sqrt{8n+1}-1}{2}\right)>$$

$$>\frac{\log 2}{4}\cdot\left(\sqrt{8m+1}-3\right)/\log\left(\frac{\sqrt{8n+1}-1}{2}\right)>$$

$$>\frac{\log 2}{4}\cdot\frac{\sqrt{8n+1}-3}{\log\sqrt{8n+1}}=\frac{\log 2}{2}\cdot\frac{\sqrt{8}\left(\sqrt{n+\frac{1}{8}}-\frac{3}{\sqrt{8}}\right)}{\log(8n+1)}=$$

$$=\left(\sqrt{2}\log 2\right)\cdot\frac{\sqrt{n}}{\log(8n+1)}>0{,}84\frac{\sqrt{n}}{\log(8n+1)},\quad \text{ч.т.д.}$$

□

Рассмотрим ещё вопрос об уточнении полученной оценки снизу максимального числа простых делителей порядков циклических подгрупп симметрической группы S_n. Но сначала приведём два вспомогательных факта.

Лемма 7.

Для любого натурального числа n справедливы неравенства

$$n\log n<p_n<n\left(\log n+[1+o(1)]\log\log n\right),$$

где p_n — есть n-ое простое число; $o(1)$ — величина, стремящаяся к нулю при $n\to\infty$.

Доказательство. (См. [19]). □

Лемма 8 (формула суммирования Эйлера—Маклорена).

Если $f(t)$ непрерывна на $[a,b]$ и однократно непрерывно дифференцируема на (a,b) и $\psi(t)=t-[t]-\frac{1}{2}$, то

$$\sum_{a<n\le b}f(n)=\int_a^b f(t)\,dt-\psi(b)f(b)+$$

$$+\psi(a)f(a)+\int_a^b f'(t)\psi(t)\,dt.$$

Доказательство. |(См. [20]). □

Пусть теперь подстановка $\tau\in S_n$ представлена в виде произведения циклов, длины которых соответственно равны подряд идущим простым числам $p_1,p_2,\ldots,p_s$, при этом

$$p_1+p_2+\ldots+p_s\le n \tag{5}$$

и

$$p_1 + p_2 + \ldots + p_s + p_{s+1} > n. \tag{6}$$

По свойству порядков циклов имеем

$$| < \tau > | = \text{НОК}\,(p_1, p_2, \ldots, p_s) = p_1 \cdot p_2 \cdot \ldots \cdot p_s, \tag{7}$$

и значит, количество простых делителей числа $| < \tau > |$ равно s, т. е.

$$\upsilon(< \tau >) = s, \tag{8}$$

где υ — функция числа простых делителей. Оценим теперь число s снизу в зависимости от n. В силу леммы 7 при $k > 2$ получаем

$$p_k < 2k \log k. \tag{9}$$

Тогда из (6) и (9) следует, что

$$n + 1 < p_1 + p_2 + \ldots + p_s + p_{s+1} < 2 \sum_{1 \le k \le s+1} k \log k. \tag{10}$$

Теперь оценим сверху сумму в правой части неравенства (10). Для этого воспользуемся леммой 8, в которой положим $f(k) = k \ln k$, $a = 1$, $b = s + 1$.

Тогда имеем

$$\begin{aligned}
\sum_{1 \le k \le s+1} k \log k &= \int_1^{s+1} t \log t \, dt - \psi(s+1) \cdot (s+1) \log(s+1) + \\
&+ \psi(1) \ln 1 + \int_1^{s+1} (t \ln t)' \psi(t) \, dt = \\
&= \left(\frac{t^2}{2} \ln t - \frac{t^2}{4} \right) \Big|_1^{s+1} + \frac{1}{2}(s+1) \ln(s+1) + \\
&+ \int_1^{s+1} (\ln t + 1) \psi(t) \, dt = \frac{(s+1)^2 \ln(s+1)}{2} - \frac{(s+1)^2}{4} + \frac{1}{4} + \\
&+ \frac{1}{2}(s+1) \ln(s+1) + \int_1^{s+1} (\ln t + 1) \cdot \left(t - [t] - \frac{1}{2} \right) dt < \\
&< \frac{(s+1)^2 \ln(s+1)}{2} - \frac{(s+1)^2}{4} + \frac{1}{4} + \frac{1}{2}(s+1) \ln(s+1) + \\
&+ \int_1^{s+1} (\ln t + 1) \, dt - \frac{1}{2} \int_1^{s+1} (\ln t + 1) \, dt = \\
&= \frac{(s+1)^2 \ln(s+1)}{2} - \frac{(s+1)^2}{4} + \frac{1}{4} + \frac{1}{2}(s+1) \ln(s+1) + \frac{1}{2} \int_1^{s+1} (\ln t + 1) \, dt = \\
&= \frac{(s+1)^2 \ln(s+1)}{2} + (s+1) \ln(s+1) = \\
&= \{(s+1) \ln(s+1)\} \cdot \frac{s+3}{2} < \frac{(s+1)(s+3)}{2} \log(s+1) < \\
&< \frac{(s+1)^2}{2} \log(s+1) < \frac{(s+2)^2}{2} \log(s+1).
\end{aligned}$$

Итак

$$\sum_{1 \le k \le s+1} k \log k < \frac{(s+2)^2 \ln(s+1)}{2}. \tag{11}$$

Подставляя (11) в (10), получаем

$$(s+2)^2 \ln(s+1) > n,$$

откуда

$$s+2 > \sqrt{\frac{2n}{\ln(s+1)}}. \tag{12}$$

Но из неравенства (5) следует, что $s < n-1$, т. е. $s+1 < n$. В таком случае из (12) получаем

$$\upsilon\left(|<\tau>|\right) > \sqrt{\frac{2n}{\log n}} - 2,$$

откуда

$$\max_{\tau \in S_n} \upsilon\left(|<\tau>|\right) > \sqrt{\frac{2n}{\log n}} - 2.$$

Таким образом, доказана следующая

Теорема 6. *Для максимального числа* $\max_{\tau \in S_n} \upsilon\left(|<\tau>|\right)$ *простых делителей порядков циклических подгрупп симметрической группы* S_n *справедливо неравенство*

$$\max_{\tau \in S_n} \upsilon\left(|<\tau>|\right) > \sqrt{\frac{2n}{\log n}} - 2,$$

где υ *— функция числа простых делителей.*

Замечание 1. *Теорема 6 представляет собой уточнение результата из [11].*

4. Заключение

Использованное нами соответствие (5) между линейным двучленами вида $\overline{a}\,\overline{x}+\overline{b}$ над кольцом классов вычетов $\mathbb{Z}/m\mathbb{Z}$ и соответствующими подстановками из симметрической группы S_m имеет некоторое отношение к понятию перестановочного многочлена над конечным полем F_q, осуществляющего перестановку элементов конечного поля F_q (см. [21] том 2). Представляет интерес вопрос о том, какие ещё многочлены являются перестановочными для кольца $\mathbb{Z}/m\mathbb{Z}$.

Условие перестановочности линейного двучлена конечного поля в неявной форме даётся и в [22]. Интересно также получить верхнюю оценку для максимального числа простых делителей циклических подгрупп в S_n.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Боревич З. И., Шафаревич И. Р. Теория чисел. М.: Наука. 1985. 504 с.

2. Bertran, Journ. de l'Ecole Polyt, (1845).

3. Landau E. Über die Maximalordnung der Permutation gegeben Grads // Archiv der Math. Und Phus., Ser. 3,5 (1903). S. 92–103.

4. Shah S. An Ineguality for the Arithmetical Function $g(x)$. I. Indian Math. Soc., 3 (1939), pp. 316–318.

5. Massian I. Majoration explite de l'ordre maximum d'un element du group symetrique, Ann, Fac. Shi. Toulouse Math. 5(6) (1984) no. 3–4 (1985), 269–281.

6. Szalay M. On the Maximal Order in S_n and S_n^*. Acta Arith. 37 (1980), pp. 321–331.

7. Nicolas I. L. Ordre maximal d'un element du group des permutations et highly composite numbers, Bull. Soc. Math. Franke, 97 (1969), pp. 129–191.

8. Nathanson M. B. On the Greatest Order of an Element of the Symmetric Group, this Monthly, 79 (1972), pp. 500–501.

9. Miller W. The Maximum Order of an Element of a Finite Symmetric Group. The American Mathematical Montly, vol. 94, №6, 1987, pp. 497–506.

10. Пачев У. М., Шокуев В. Н. О применении теории сравнений к изучению подгрупп в симметрических группах // Изв. КБНЦ РАН, 2001, №1(6). С. 68–69.

11. Дохов Р. А., Пачев У. М. О максимальном числе простых делителей порядков циклических подгрупп в симметрической группе // Материалы XXII Международной конференции «Алгебра, теория чисел, дискретная геометрия и многомасштабная моделирование: современные проблемы, приложения и проблемы истории». Тула 26–29 сентября 2023 г. С. 173–174.

12. Виноградов И. М. Основы теории чисел. М.: Изд. «Наука». 1981. 168 с.

13. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. М.: Наука. 1982, 288 с.

14. Zolotareff G. Nouvelle demonstration de la loi de reciprocite de Legendre // Nouv. Ann. Math. (2), 1872. Vol. 11. P. 354–362.

15. Гашков С. Б. Современная элементарная алгебра в задачах и упражнениях. М. Из-во МЦНМО, 2006, 328 с.

16. Гекке Э. Лекции по теории алгебраических чисел. М-Л. 1940, 260 с.

17. Трост Э. Простые числа. М.: ГИФМЛ. 1959, 136 с.

18. Бухштаб А. А. Теория чисел. М., 1966.

19. Rosser B. The n-th Prime is greater than $n \log n$. Proc. London. Math. Soc. 45 (1938), pp. 21–44.

20. Krätzel E. Zahlentheorie. VEB Deutscher Verlag der Wissenschaften. Berlin, 1981.

21. Лидл Р., Нидеррайтер Г. Конечные поля. Том. 2. М.: «Мир». 1988, с. 438–820.

22. Пачев У. М. Избранные главы теории чисел. Нальчик. 2016, 186 с.

REFERENCES

1. Borevich Z. I., Zhafarevich I. R. 1985, "Number theory", *Nauka, Moscow*, 510 p. (Russia).

2. Bertrand. 1845, Journ. de l'Ecole Polyt.

3. Landau E. 1903, "On the maximum substitution order of a given degree"", *Archives of Mathematics and Physics*. Ser. 3,5. pp. 92–103.

4. Shah S. 1939, "An Inequality for the Arithmetical Function $g(x)$", *J. Indian Math. Soc.*, 3, pp. 316–318.

5. Massias I. 1984, (1985), "Majoration explete de l'ordre maximum d'un element du group symetrique", *Ann, Fac. Shi. Toulouse Math.*, 5(6), no. 3–4, pp. 269–281.

6. Szalay M. 1980, "On the Maximal Order in S_n and S_n^*", *Acta Arith.*, 37, pp. 321–331.

7. Nicolas I. L. 1969, "Ordre maximal d'un element du group des permutation et highly composite numbers", *Bull. Soc. Math. Franke*, 97, pp. 129–191.

8. Nathanson M. B. 1972, "On the Greatest Order of an Element of the Symmetric Group", *this Monthly*, 79, pp. 500–501.

9. Miller W. 1987, "The Maximum Order of *a* Finite Symmetric Group", *The American Mathematical Monthly*, vol. 94, № 6, pp. 497–506.

10. Pachev U. M., Shokuev V. N. 2001, "On thr application of the theory of congruence to the study of subgroups in symmetric groups", *Jzw. KBNTs RAS*, № 1 (6), pp. 68–69.

11. Dokhov R. A., Pachev U. M., 2023, "On the maximum number of primedivisors of orders of cyclic subgroups in *a* symmetris group", *Procceedings of the XXII International Conference "Algebra, number theory, discrete geometry and multiscale modeling: modern problems, applications and prolems of history". Tula*, pp. 173–174.

12. Vinogradov I. M. 1981, "Fundavental of Number Theoury", *M.: Nauka*, 186 p.

13. Kargapolov M. I., Merzlyakov Yu. I. 1982, "Fundamentals of group theory", *M.: Nauka*. 288 p.

14. Zolotareff G. 1972, "Nouvelle de'monstration de la loi de reciprocite de Legendre", Nouv. Ann. Math. (2). Vol. 11, pp. 354–362.

15. Gashkov S. B. 2006, "Modern Elementary Algebra in Problems and Exercises", *M.: MCNMO*, 328 p.

16. Gecke E. 1940, "Lectures on the theory of algebraic numbers",*M.-L.* 260 p.

17. Trost E. 1959, "Prime numbers", *M.: GIFML*, 136 p.

18. Buhshtab A. A. 1966, "Number theory".

19. Rosser B. 1938, "The n-th Prime is greater than $n \log n$". Proc. London. Math. Soc. 45, pp. 21–44.

20. Krätzel E. 1981, "Zahlentheorie. VEB Dentscher Verlag der Wissenschaften". Berlin.

21. Lidl R., Niederreiter G. 1988, "Finite Fields", *M.: Mir*, vol. 2, pp. 437–820.

22. Pachev U. M. 2016, "Selected chapter of number theory", *Nalchik*, 186 p.

Получено: 21.08.2023
Принято в печать: 11.12.2023