2014 Теоретические основы прикладной дискретной математики № 4(26)

DOI 10.17223/20710410/26/2

УДК 519.1:511.2

СРАВНЕНИЯ ДЛЯ ЧИСЕЛ ПОЛНЫХ ОТОБРАЖЕНИЙ[1]

Л. Н. Бондаренко*, М. Л. Шарапова**

*Пензенский государственный университет, г. Пенза, Россия

**Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

E-mail: leobond5@mail.ru

Для чисел стандартных полных отображений и для чисел стандартных сильных полных отображений получены сравнения по модулю простого числа. Доказательства основаны на рассмотрении свойств некоторых статистик и чисел Эйлера на соответствующих множествах перестановок. Получены аналогичные результаты для этих множеств с учётом знака их элементов.

Ключевые слова: *полные отображения, перестановка, статистика, числа Эйлера, смещение перестановки.*

Введение

Все перестановки симметрической группы S_{n-1} над алфавитом $\{1,\dots,n-1\}$, вычитание из которых единичной перестановки $\varepsilon \in S_{n-1}$ приводит к перестановке из S_{n-1}, определяют множество $CM(\mathbb{Z}_n)$ стандартных полных отображений. Если сложение $\varepsilon \in S_{n-1}$ с перестановкой из $CM(\mathbb{Z}_n)$ также приводит к перестановке из S_{n-1}, то все такие перестановки задают множество $SCM(\mathbb{Z}_n)$ стандартных сильных полных отображений [1]. Рассматриваемое сложение (вычитание) перестановок выполняется посимвольно по $\bmod n$, т. е. на аддитивной группе $\mathbb{Z}_n$, отождествляемой с множеством $\{0,1,\dots,n-1\}$; такие операции с перестановками находят применение, в частности, в криптографии.

В работе [1] показано, что задачи вычисления чисел $\#CM(\mathbb{Z}_n)$ и $\#SCM(\mathbb{Z}_n)$ не являются #P-полными, но являются трудными вычислительными проблемами.

В [2] доказан ряд утверждений о делимости перманента $P_n = \operatorname{per}(\omega^{km})_{k,m=0}^{n-1}$, где $\omega = \exp(2\pi i/n)$ — корень n-й степени из единицы, а $(n \times n)$-матрица Шура $(\omega^{km})_{k,m=0}^{n-1}$ встречается в теории чисел, теории кодирования, комбинаторном анализе и т. п. В [3] вычисление чисел P_n сведено к нахождению мощности множества $CM(\mathbb{Z}_n)$ с учётом знака его элементов.

В настоящей работе получены некоторые сравнения для $\#CM(\mathbb{Z}_n)$ и $\#SCM(\mathbb{Z}_n)$, а также для мощностей множеств $CM(\mathbb{Z}_n)$ и $SCM(\mathbb{Z}_n)$ с учётом знака их элементов. Эти результаты связаны с нахождением сравнений по простым модулям для чисел Эйлера на соответствующих множествах перестановок.

1. Свойства некоторых статистик и отображений

При делении с остатком мощности некоторого множества на заданное число можно разбить это множество на части, для которых этот вопрос решается проще, а затем использовать полученные результаты. Этот подход удобно применять для достаточно сложных по структуре множеств перестановок, определяя понятие статистики как неотрицательной целочисленной функции, заданной для каждой перестановки рассматриваемого множества.

[1]Работа поддержана грантом РФФИ № 14-01-00273.

Например, статистика $\mathrm{des}(\sigma) = \#\{i : 1 \leqslant i \leqslant n-1,\ \sigma_i > \sigma_{i+1},\ \sigma_n = 0\}$ при фиксированном $n \geqslant 2$ описывает число спусков перестановки $\sigma = \sigma_1 \dots \sigma_{n-1} \in S_{n-1}$, т. е. спуск учитывается также на последнем символе перестановки, и индуцирует производящий многочлен Эйлера

$$A_{n-1}(t) = \sum_{\sigma \in S_{n-1}} t^{\mathrm{des}(\sigma)} = \sum_{k=1}^{n-1} A_{n-1,k}\, t^k, \tag{1}$$

коэффициенты которого $A_{n-1,k} = \#\{\sigma : \sigma \in S_{n-1},\ \mathrm{des}(\sigma) = k\}$ называются числами Эйлера [4]. Так как $\#S_{n-1} = A_{n-1}(1)$, остаток от деления $\#S_{n-1}$ на n можно найти, используя остатки от деления чисел $A_{n-1,k}$, $k = 1, \dots, n-1$, на n.

При исследовании делимости мощностей некоторых множеств перестановок полезно ввести некоторые отображения.

Зададим биекцию $\mathbf{c} : S_{n-1} \to S_{n-1}$, определяющую дополнение $\overline{\sigma} = \mathbf{c}\sigma$ к перестановке $\sigma = \sigma_1\sigma_2 \dots \sigma_{n-1} \in S_{n-1}$, с помощью равенств $\mathbf{c}\sigma_i = n - \sigma_i$, $1 \leqslant i \leqslant n-1$.

Непосредственно из этого определения следует, что отображение $\mathbf{c}$ есть инволюция, а $\sigma + \overline{\sigma} = 0$, причём элементарное равенство $\mathrm{des}(\sigma) + \mathrm{des}(\overline{\sigma}) = n$ влечёт соотношение $t^n A_{n-1}(t^{-1}) = A_{n-1}(t)$, т. е. $A_{n-1,k} = A_{n-1,n-k}$, $k = 1, \dots, n-1$.

Статистика $\mathrm{des}(\sigma^*)$ для расширения $\sigma^* = \sigma_1 \dots \sigma_{n-1}0 \in S_n$ перестановки $\sigma \in S_{n-1}$ обладает свойством $\mathrm{des}(\sigma^*) = \mathrm{des}(\sigma) + 1$, и справедливо простое равенство

$$\mathrm{des}(\sigma) = \frac{1}{n} \sum_{i=0}^{n-1} (\sigma_{i+1} - \sigma_i),\ \sigma_0 = \sigma_n = 0, \tag{2}$$

где разности под знаком суммы вычисляются по модулю n.

На симметрической группе S_n в [5] применяются биекции $\mathbf{t} : S_n \to S_n$ и $\mathbf{u} : S_n \to S_n$, задаваемые для перестановки $\pi = \pi_1 \dots \pi_n \in S_n$ над алфавитом $\{0, 1, \dots n-1\}$ соотношениями $\mathbf{t}\,\pi{=}\pi_2 \dots \pi_n\pi_1$ и $\mathbf{u}\,\pi_i = \pi_i + 1 \bmod n$, $1 \leqslant i \leqslant n$.

Преобразования переноса $\mathbf{t}$ и единичного сдвига $\mathbf{u}$ позволяют ввести отношение эквивалентности на S_n: перестановки $\sigma, \tau \in S_n$ называются эквивалентными, если найдутся такие целые числа k и m, что $\mathbf{t}^k\mathbf{u}^m\sigma = \tau$. Мощность фактор-множества по этому отношению эквивалентности вычисляется по формуле

$$\frac{1}{n^2} \sum_{d|n} \varphi^2\,(n/d)\,(n/d)^d\,d!, \tag{3}$$

где $\varphi(n)$ — функция Эйлера [5].

Определение 1. Биекцию $\mathbf{d} : S_{n-1} \to S_{n-1}$, задающую смещение перестановки $\sigma = \sigma_1 \dots \sigma_{n-1} \in S_{n-1}$, опишем выражениями

$$(\mathbf{d}\,\sigma)^* = \mathbf{t}\,\mathbf{u}^{-\sigma_1}\sigma^*,$$

а порядком $d(\sigma)$ перестановки $\sigma \in S_{n-1}$ (относительно операции $\mathbf{d}$) назовём наименьшее положительное целое k, для которого $\mathbf{d}^k\sigma = \sigma$.

Определение 1 позволяет аналогично работе [5] ввести отношение эквивалентности на S_{n-1}: перестановки $\sigma, \tau \in S_{n-1}$ назовём эквивалентными, если найдётся такое целое число k, что $\mathbf{d}^k\sigma = \tau$; мощность соответствующего фактор-множества по этому отношению эквивалентности вычисляется также по формуле (3). Поэтому $d(\sigma)|n$, а мощность каждого класса эквивалентности, содержащего перестановку $\sigma \in S_{n-1}$, совпадает с порядком $d(\sigma)$.

Лемма 1. Для $\sigma \in S_{n-1}$ справедливо равенство $\mathrm{des}(\mathbf{d}\,\sigma) = \mathrm{des}(\sigma)$.

Доказательство. Записывая, согласно определению 1, смещение $\mathbf{d}$ перестановки $\sigma = \sigma_1 \dots \sigma_{n-1} \in S_{n-1}$ в виде $\mathbf{d}\,\sigma = (\sigma_2 - \sigma_1) \dots (\sigma_{n-1} - \sigma_1)(n - \sigma_1)$, где разности вычисляются по модулю n, и применяя соотношение (2), получаем требуемое. ■

Статистика $\operatorname{inv}(\pi) = \#\{(i,j) : 1 \leqslant i < j \leqslant n, \pi_i > \pi_j\}$ задаёт число инверсий перестановки $\pi \in S_n$ [4], причём $\operatorname{inv}(\sigma^*) = \operatorname{inv}(\sigma) + n - 1$. С помощью этой статистики определяется знак $\operatorname{sgn}(\sigma) = (-1)^{\operatorname{inv}(\sigma)}$ перестановки $\sigma \in S_{n-1}$.

Лемма 2. Если n нечётно, то $\operatorname{sgn}(\mathbf{d}\,\sigma) = \operatorname{sgn}(\sigma)$, $\sigma \in S_{n-1}$.

Доказательство. Для перестановки $\pi \in S_n$ с $\pi_i = 0$, где $1 \leqslant i \leqslant n$, легко устанавливается равенство $\operatorname{inv}(\mathbf{u}^{-1}\pi) = \operatorname{inv}(\pi) + n - 2i + 1$, применение которого совместно с определением 1 даёт требуемый результат. ■

Леммы 1 и 2 показывают, что по введённому отношению эквивалентности перестановки каждого класса эквивалентности на S_{n-1} характеризуются одинаковым числом спусков и при нечётном n имеют одинаковый знак.

Использование знака перестановок на S_{n-1} позволяет определить производящий многочлен

$$B_{n-1}(t) = \sum_{\sigma \in S_{n-1}} \operatorname{sgn}(\sigma)\, t^{\operatorname{des}(\sigma)} = \sum_{k=1}^{n-1} B_{n-1,k}\, t^k, \tag{4}$$

коэффициенты которого $B_{n-1,k}$, $k = 1, \dots, n-1$, также назовём числами Эйлера, но с учётом знака элементов множества S_{n-1}.

Пусть множество $R_n = \{r\varepsilon : r \in \{1, \dots, n-1\}, (r,n) = 1, \varepsilon \in S_{n-1}\}$ образовано умножением чисел r из приведённой системы вычетов по модулю n на единичную перестановку $\varepsilon \in S_{n-1}$ (умножение выполняется посимвольно по модулю n и $\#R_n = \varphi(n)$). Тогда имеет место следующее утверждение.

Лемма 3. Если $r\varepsilon \in R_n$, то $\operatorname{des}(r\varepsilon) = r$, а для простого нечётного числа $n = p$ справедливо равенство $\operatorname{sgn}(r\varepsilon) = \left(\dfrac{r}{p}\right)$, где $\left(\dfrac{r}{p}\right)$ — символ Лежандра.

Доказательство. Соотношение $\operatorname{des}(r\varepsilon) = r$ устанавливается с помощью формулы (2), а равенство $\operatorname{sgn}(r\varepsilon) = \left(\dfrac{r}{p}\right)$ получено И. И. Золотаревым (см. [6]). ■

Отметим, что применение операции композиции перестановок позволяет найти выражение для знака $r\varepsilon \in R_n$ и при составном n.

2. Сравнения для чисел Эйлера на S_{n-1}

Известная теорема Вильсона [7] утверждает, что $(p-1)! \equiv -1 \pmod p$, где p — простое число. Так как $A_{p-1}(1) = \#S_{p-1} = (p-1)!$, новое доказательство этой теоремы может быть получено с помощью явного выражения для чисел Эйлера $A_{p-1,k}$, $k = 1, \dots, p-1$.

Для чисел $A_{n,k}$, $k = 1, \dots, n$, методом математической индукции нетрудно доказать следующее известное рекуррентное соотношение [8]:

$$A_{0,k} = \delta_{0k},\ A_{n,k} = kA_{n-1,k} + (n-k+1)A_{n-1,k-1},\ k \in \mathbb{Z},\ n \geqslant 1, \tag{5}$$

в котором δ_{ij} — символ Кронекера.

Действительно, если (5) верно для $\sigma \in S_{n-1}$ над алфавитом $\{1, \dots, n-1\}$, то для получения $\pi \in S_n$ с $\operatorname{des}(\pi) = k$ из $\sigma \in S_{n-1}$ с $\operatorname{des}(\sigma) = k$ символ 0 можно вставить k способами, а из $\sigma \in S_{n-1}$ с $\operatorname{des}(\sigma) = k-1$ — $(n-k+1)$ способами.

С помощью формулы (5) находится рекуррентное соотношение

$$A_0(t) = 1,\ A_n(t) = ntA_{n-1}(t) + t(1-t)A'_{n-1}(t),\ n \geqslant 1, \tag{6}$$

и известная формула Ворпицкого [8]

$$t^n = \sum_{k=1}^{n} A_{n,k} \binom{t+k-1}{n},$$

а её обращение в смысле Мебиуса приводит к выражению для чисел Эйлера

$$A_{n,k} = \sum_{i=0}^{k-1} (-1)^i \binom{n+1}{i} (k-i)^n. \tag{7}$$

В частности, имеем $A_{n,1} = A_{n,n} = 1$.

Малая теорема Ферма [7] и формула (7) сразу дают следующее утверждение, из которого легко выводится теорема Вильсона.

Теорема 1. Для простого p имеем $A_{p-1,k} \equiv 1 \pmod{p},\ k = 1, \ldots, p-1$.

Доказательство. Приведём косвенное получение сравнений теоремы 1 без использования выражения (7) для чисел Эйлера. При $n = p$ приведённая система вычетов состоит из чисел $r = 1, \ldots, p-1$, порядок $d(r\varepsilon) = 1$, а для перестановок $\sigma \in S_{p-1} \setminus R_p$ порядок $d(\sigma) = p$. Поэтому применение лемм 1 и 3 дает требуемый результат. ■

Отметим, что из равенства $\#S_{n-1} = (n-1)!$ при составном n непосредственно находим $\#S_{n-1} \equiv 0 \pmod{n}$. Мощность множества S_{n-1} с учётом знака его элементов равна нулю, т. е. $B_{n-1}(1) = 0$, $n > 2$. Покажем, что и для множества S_n с учётом знака его элементов существуют аналоги выражений (5) и (6).

Теорема 2. Числа Эйлера $B_{n,k}$, $k = 1, \ldots, n$, с учётом знака элементов множества S_n удовлетворяют следующему рекуррентному соотношению:

$$\begin{gathered} B_{0,k} = \delta_{0k},\ B_{1,k} = \delta_{1k}, \\ B_{n,k} = kB_{n-2,k} + (n-2k+1)B_{n-2,k-1} - (n-k+1)B_{n-2,k-2},\ k \in \mathbb{Z},\ n \geqslant 2, \end{gathered} \tag{8}$$

справедливы также рекуррентная формула

$$B_0(t) = 1,\ B_1(t) = t,\ B_n(t) = t(1-t)((n-1)B_{n-2}(t) + (1-t)B'_{n-2}(t)),\ n \geqslant 2 \tag{9}$$

и следующее выражение:

$$B_n(t) = A_{[(n+1)/2]}(t)(1-t)^{[n/2]},\ n \geqslant 0, \tag{10}$$

где $[\cdot]$ — целая часть числа, а $A_{[(n+1)/2]}(t)$ — многочлены Эйлера. В частности, имеем $|B_{n,1}| = |B_{n,n}| = 1$.

Доказательство. При установлении справедливости (8) методом математической индукции базис тривиален. Пусть (8) верно для S_{n-2} над алфавитом $\{2, \ldots, n-1\}$. Тогда для получения $\pi \in S_n$ с $\operatorname{des}(\pi) = k$ из $\sigma \in S_{n-2}$ с $\operatorname{des}(\sigma) = k$ пара символов 01 вставляется k способами без изменения знака перестановок, так как число транспозиций чётно. Для получения $\pi \in S_n$ с $\operatorname{des}(\pi) = k$ из $\sigma \in S_{n-2}$ с $\operatorname{des}(\sigma) = k-1$ пара символов 01 вставляется $(n-k)$ способами без изменения знака перестановок, а пара символов 10 вставляется $(k-1)$ раз с изменением знака перестановок. Для получения $\pi \in S_n$ с $\operatorname{des}(\pi) = k$ из $\sigma \in S_{n-2}$ с $\operatorname{des}(\sigma) = k-2$ пара символов 10 вставляется

$(n-k+1)$ способами с изменением знака перестановок. Остальные вставки символов 0 и 1 разбиваются на пары, имеющие противоположные знаки.

Формула (9) проверяется с помощью (4) и (8), а из неё раздельно для чётных и нечётных n получается и соотношение (10). ■

Таким образом, явные выражения для чисел $B_{n,k}$, $k=1,\dots,n$, можно получить, например, с помощью соотношений (7) и (10).

Значительно легче аналог теоремы 1 для чисел Эйлера $B_{p-1,k}$, $k=1,\dots,p-1$, с учётом знака элементов множества S_{p-1} получить косвенно.

Теорема 3. Для простого p имеем $B_{p-1,k} \equiv \left(\dfrac{k}{p}\right) \pmod p$, $k=1,\dots,p-1$.

Доказательство. Как и при доказательстве теоремы 1 для $n=p$, заметим, что приведённая система вычетов состоит из чисел $r=1,\dots,p-1$, порядок $d(r\varepsilon)=1$, а для перестановок $\sigma \in S_{p-1} \setminus R_p$ порядок $d(\sigma)=p$. Поэтому применение лемм 1, 2 и 3 даёт требуемый результат. ■

Так как $\sum\limits_{k=1}^{p-1}\left(\dfrac{k}{p}\right)=0$ [7], тривиальным следствием теоремы 3 является сравнение $B_{p-1}(1)\equiv 0 \pmod p$, перекрываемое равенством $B_{n-1}(1)=0$.

3. Сравнения для чисел Эйлера на $\overline{CM}(\mathbb{Z}_n)$

Введём множество перестановок $\overline{CM}(\mathbb{Z}_n)$.

Определение 2. Перестановки $\sigma, \widetilde{\sigma} \in S_{n-1}$ назовём сопряжёнными относительно $\overline{\varepsilon} \in S_{n-1}$, если $\sigma + \widetilde{\sigma} = \overline{\varepsilon}$, а ε — единичная перестановка.

Все перестановки, удовлетворяющие определению 2, образуют множество $\overline{CM}(\mathbb{Z}_n)$. Следуя определению 2, можно задать перестановки, сопряжённые относительно любой $\tau \in S_{n-1}$, в частности, множество $CM(\mathbb{Z}_n)$ всех стандартных полных отображений [1] является множеством всех перестановок, сопряжённых относительно $\varepsilon \in S_{n-1}$, причём справедливость равенства $\#CM(\mathbb{Z}_n) = \#\overline{CM}(\mathbb{Z}_n)$ очевидна.

Числа Эйлера $\widetilde{A}_{n-1,k}$, $k=1,\dots,n-1$, на множестве $\overline{CM}(\mathbb{Z}_n)$ определим как коэффициенты многочлена $\widetilde{A}_{n-1}(t)$ вида (1), построенного на множестве перестановок $\overline{CM}(\mathbb{Z}_n)$. Аналогично числами Эйлера $\{\widetilde{B}_{n-1,k}\}_{k=1}^{n-1}$ на множестве $\overline{CM}(\mathbb{Z}_n)$ с учётом знака его элементов будем называть коэффициенты многочлена $\widetilde{B}_{n-1}(t)$ вида (4), но построенного на множестве перестановок $\overline{CM}(\mathbb{Z}_n)$ с учётом знака его элементов.

При чётном n не существует сопряжённых перестановок $\sigma, \widetilde{\sigma} \in S_{n-1}$ относительно $\overline{\varepsilon} \in S_{n-1}$. Действительно, предполагая противное и суммируя все символы перестановок левой части равенства $\sigma + \widetilde{\sigma} = \overline{\varepsilon}$, а также все символы правой части, легко получить противоречие. Поэтому в этом случае $\#CM(\mathbb{Z}_n)=0$ и $\widetilde{A}_{n-1}(t)=\widetilde{B}_{n-1}(t)=0$.

При нечётном n находим $\#CM(\mathbb{Z}_n) \equiv 1 \pmod 2$, так как в этом случае существует только одна самосопряжённая относительно $\overline{\varepsilon} \in S_{n-1}$ перестановка σ, определяемая равенством $2\sigma = \overline{\varepsilon}$.

Лемма 4. Если $\sigma \in \overline{CM}(\mathbb{Z}_n)$, n — нечётное, то $\operatorname{des}(\sigma) + \operatorname{des}(\widetilde{\sigma}) = n-1$.

Доказательство. Применение формулы (2) к сопряжённым относительно $\overline{\varepsilon} \in S_{n-1}$ перестановкам $\sigma, \widetilde{\sigma} \in S_{n-1}$ сразу дает требуемое. ■

Отметим, что множество $\widetilde{R}_n = R_n \cap \overline{CM}(\mathbb{Z}_n)$ не содержит $\overline{\varepsilon} \in S_{n-1}$. Поэтому по первой части леммы 3 имеем $\widetilde{A}_{n-1,n-1} = \widetilde{B}_{n-1,n-1} = 0$, а по лемме 4 получаем равенство

$t^{n-1}\widetilde{A}_{n-1}(t^{-1}) = \widetilde{A}_{n-1}(t)$, т. е. $\widetilde{A}_{n-1,k} = \widetilde{A}_{n-1,n-k-1}$, $k = 1, \ldots, n-2$, и имеют место равенства $\deg\widetilde{A}_{n-1}(t) = \deg\widetilde{B}_{n-1}(t) = n-2$.

Если $n > 1$ имеет разложение $n = \prod\limits_{p|n} p^{\mathrm{ord}_p(n)}$ на простые множители, то аналогично формуле для функции Эйлера $\varphi(n)$ находится выражение

$$\#\widetilde{R}_n = n\prod_{p|n}\left(1 - \frac{2}{p}\right), \tag{11}$$

которое также показывает, что $\#\widetilde{R}_n = 0$ при чётном n. Формула (11) базируется на подсчёте количества представлений числа $n-1$ суммой двух натуральных слагаемых r и s, взаимно простых с n.

Из предыдущих рассмотрений следует, что основные свойства чисел $A_{p-1,k}$ наследуются числами $\widetilde{A}_{p-1,k}$. Поэтому аналогично теореме 1 доказывается

Теорема 4. Если простое $p > 2$, то $\widetilde{A}_{p-1,k} \equiv 1 \pmod p$ для $k = 1, \ldots, p-2$; $\widetilde{A}_{p-1,p-1} = 0$.

Следствие 1. Если простое $p > 2$, то $\#CM(\mathbb{Z}_p) \equiv -2 \pmod p$.

Числа $\#CM(\mathbb{Z}_n)$ при нечётных $n = 1, 3, \ldots, 25$ приведены в [9]. Вычисления при составном n показывают, что $n|\#CM(\mathbb{Z}_n)$, но рассматриваемый подход даёт только следующее частное утверждение.

Теорема 5. $p|\#CM(\mathbb{Z}_{p^s})$ при простом $p > 2$ и $s > 1$.

Доказательство. По формуле (11) имеем $p|\#\widetilde{R}_{p^s}$, а для перестановок $\sigma \in \overline{CM}(\mathbb{Z}_{p^s}) \setminus \widetilde{R}_{p^s}$ имеем $p|d(\sigma)$. ■

Если на множестве $\overline{CM}(\mathbb{Z}_n)$ наряду с сопряжением относительно $\overline{\varepsilon} \in S_{n-1}$ рассматривать и обращение перестановки, то $\left(\widetilde{\sigma^{-1}}\right)^{-1} = \widetilde{(\widetilde{\sigma})^{-1}}$ [3], а $\overline{CM}(\mathbb{Z}_n)$ разбивается на шестёрки перестановок вида $\left\{\sigma, \widetilde{\sigma}, \sigma^{-1}, \widetilde{\sigma^{-1}}, (\widetilde{\sigma})^{-1}, \left(\widetilde{\sigma^{-1}}\right)^{-1}\right\}$, причём в некоторых шестёрках могут встречаться и одинаковые члены. Можно показать, что при $n = 6m+5$ имеются только шестёрки различных перестановок и одна тройка, содержащая самосопряжённую перестановку, т. е. $\#CM(\mathbb{Z}_{6m+5}) \equiv 3 \pmod 6$.

В работе [2] для перманентов матрицы Шура P_n получены следующие результаты:

а) $P_p \equiv p! \pmod{p^3}$ для простого $p > 3$;

б) $P_p \equiv 0 \pmod q$ для нечётных простых чисел p и q, связанных равенством $p = 2q^s + 1$ при $s \geqslant 1$;

в) если $p^s|n$ при простом p и $s \geqslant 1$, то $p^{\frac{(p^s-1)n}{(p-1)p^s}}\Big|P_n$.

Числа P_n при нечётных $n = 1, 3, \ldots, 33$ приведены в [10], причём имеет место равенство $\widetilde{B}_{n-1}(1) = (-1)^{(n-1)/2}n^{-1}P_n$ [3]. Так как основные свойства чисел $B_{p-1,k}$ наследуются числами $\widetilde{B}_{p-1,k}$, с помощью теоремы 3 получаем следующее утверждение.

Теорема 6. Если простое $p > 2$, то $\widetilde{B}_{p-1,k} \equiv \left(\frac{k}{p}\right) \pmod p$ для $k = 1, \ldots, p-2$; $\widetilde{B}_{p-1,p-1} = 0$.

Следствие 2. Если простое $p > 2$, то $\widetilde{B}_{p-1}(1) \equiv (-1)^{(p+1)/2} \pmod p$.

Доказательство. Так как $\sum\limits_{k=1}^{p-1}\left(\frac{k}{p}\right) = 0$ и $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ [7], легко находим требуемый результат. ■

Таким образом, для перманента матрицы Шура при простом $p > 2$ также имеет место сравнение $p^{-1}P_p \equiv -1 \pmod p$.

4. Сравнения для чисел Эйлера на $SCM(\mathbb{Z}_n)$

Множество всех стандартных сильных полных отображений $SCM(\mathbb{Z}_n)$ [1] задаётся равенством $SCM(\mathbb{Z}_n) = CM(\mathbb{Z}_n) \cap \overline{CM}(\mathbb{Z}_n)$.

Числа Эйлера $\widehat{A}_{n-1,k}$, $k = 1, \ldots, n-1$, на множестве перестановок $SCM(\mathbb{Z}_n)$ определим как коэффициенты многочлена $\widehat{A}_{n-1}(t)$ вида (1), построенного на множестве $SCM(\mathbb{Z}_n)$, а числами Эйлера $\widehat{B}_{n-1,k}$, $k = 1, \ldots, n-1$, на множестве перестановок $SCM(\mathbb{Z}_n)$ с учётом знака его элементов будем называть коэффициенты многочлена $\widehat{B}_{n-1}(t)$ вида (4), но построенного на множестве $SCM(\mathbb{Z}_n)$ с учётом знака его элементов.

Так как множество $\widehat{R}_n = R_n \cap SCM(\mathbb{Z}_n)$ не содержит как $\overline{\varepsilon} \in S_{n-1}$, так и $\varepsilon \in S_{n-1}$, по лемме 3 находим $\widehat{A}_{n-1,1} = \widehat{A}_{n-1,n-1} = 0$ и $\widehat{B}_{n-1,1} = \widehat{B}_{n-1,n-1} = 0$. Очевидно, что при чётном n выполняются равенства $\#SCM(\mathbb{Z}_n) = 0$ и $\widehat{A}_{n-1}(t) = \widehat{B}_{n-1}(t) = 0$; можно показать их выполнение и при n, кратном трём.

Из определения множества перестановок $SCM(\mathbb{Z}_n)$ следует, что при $\sigma \in SCM(\mathbb{Z}_n)$ также и $\overline{\sigma} \in SCM(\mathbb{Z}_n)$. Поэтому в силу равенства $\mathrm{des}(\sigma) + \mathrm{des}(\overline{\sigma}) = n$ получаем соотношение $t^n \widehat{A}_{n-1}(t^{-1}) = \widehat{A}_{n-1}(t)$, т. е. $\widehat{A}_{n-1,k} = \widehat{A}_{n-1,n-k}$, $k = 2, \ldots, n-2$, и имеют место равенства $\deg \widehat{A}_{n-1}(t) = \deg \widehat{B}_{n-1}(t) = n-2$.

Аналогично формуле (11) при нечётном $n > 1$ находится выражение

$$\#\widehat{R}_n = n \prod_{p|n} \left(1 - \frac{3}{p}\right), \tag{12}$$

которое также показывает, что $\#\widehat{R}_n = 0$ при n, кратном трём.

На множестве $SCM(\mathbb{Z}_n)$ аналогично теореме 4 доказывается

Теорема 7. Если простое число $p > 3$, то справедливы следующие соотношения: $\widehat{A}_{p-1,1} = 0$; $\widehat{A}_{p-1,k} \equiv 1 \pmod p$, $k = 2, \ldots, p-2$; $\widehat{A}_{p-1,p-1} = 0$.

Следствие 3. Если простое $p > 3$, то $\#SCM(\mathbb{Z}_p) \equiv -3 \pmod p$.

Вычисления при составном n показывают, что $n|\#SCM(\mathbb{Z}_p)$, но рассматриваемый подход даёт только следующее частное утверждение, аналогичное теореме 5 (в доказательстве вместо формулы (11) применяется (12)).

Теорема 8. $p|\#SCM(\mathbb{Z}_{p^s})$ при простом $p > 3$ и $s > 1$.

В качестве аналога теоремы 6 отметим также следующий результат.

Теорема 9. Если простое число $p > 3$, то справедливы следующие соотношения: $\widehat{B}_{p-1,1} = 0$; $\widehat{B}_{p-1,k} \equiv \left(\dfrac{k}{p}\right) \pmod p$, $k = 2, \ldots, p-2$; $\widehat{B}_{p-1,p-1} = 0$.

Следствие 4. Если простое $p > 3$, то $\widehat{B}_{p-1}(1) \equiv (-1)^{(p+1)/2} - 1 \pmod p$.

Доказательство. Так как $\sum\limits_{k=1}^{p-1} \left(\dfrac{k}{p}\right) = 0$ и $\left(\dfrac{1}{p}\right) = 1$, $\left(\dfrac{-1}{p}\right) = (-1)^{(p-1)/2}$ [7], легко находим требуемый результат. ■

Следствия 1 и 3 можно рассматривать как аналоги теоремы Вильсона для чисел стандартных полных отображений $\#CM(\mathbb{Z}_p)$ и чисел стандартных сильных полных отображений $\#SCM(\mathbb{Z}_p)$, но многие вопросы делимости этих чисел при составном n остаются открытыми.

Авторы благодарны рецензенту за внимательное прочтение статьи и ценные замечания.

ЛИТЕРАТУРА

1. *Hsiang J., Hsu D. F., and Shieh Y. P.* On the hardness of counting problems of complete mappings // Discrete Mathematics. 2004. V. 277. P. 87–100.
2. *Graham R. L.and Lehmer D. H.* On the permanent of Schur's matrix // J. Australian Math. Soc. 1976. V. 21 (Series A). Part 4. P. 487–497.
3. *Бондаренко Л. Н.* Перманенты и «аддитивные» задачи перечисления перестановок // Материалы VII Междунар. семинара «Дискретная математика и ее приложения» (29 января–2 февраля 2001 г.). Ч. III. М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2001. С. 335–338.
4. *Стенли Р.* Перечислительная комбинаторика. Т. 1. М.: Мир, 1990. 440 с.
5. *Moser W. O. J.* A (modest) generalization of theorems of Wilson and Fermat // Canadian Math. Bul. 1990. V. 33 (2). P. 253–256.
6. *Мельников И. Г., Славутский И. Ш.* О двух забытых доказательствах закона взаимности // Труды института истории естествознания и техники. Т. 28. История физико-математических наук. М., 1959. С. 201–218.
7. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987. 416 с.
8. *Бондаренко Л. Н., Шарапова М. Л.* Применение обобщенной формулы Родрига в комбинаторном анализе // Изв. вузов. Поволжский регион. Физ.-мат. науки. 2011. № 4 (20). С. 44–58.
9. `http://oeis.org/A003111` — Sloane N. J. A. The on-line encyclopedia of integer sequences.
10. `http://oeis.org/A003112` — Sloane N. J. A. The on-line encyclopedia of integer sequences.