

УДК 512.643.8+511.217

СТРОКИ ТРЕУГОЛЬНИКА ПАСКАЛЯ ПО МОДУЛЮ ПРОСТОГО ЧИСЛА

В. В. Карачик

Аннотация. Исследуются свойства специального класса матриц, возникающих при изучении распределения биномиальных коэффициентов по модулю простого числа. Получены формулы распределения элементов в строках треугольника Паскаля по модулю простого числа.

Ключевые слова: треугольник Паскаля, латинская матрица, биномиальные коэффициенты, модуль простого числа.

Введение

Одним из эффективных методов вычисления строк треугольника Паскаля по модулю простого числа p является сведение этой задачи к решению определённой системы линейных рекуррентных уравнений. Этот подход успешно применён в [2] при исследовании распределения биномиальных коэффициентов $\bmod p$ для некоторых значений p и только для определённых строк треугольника Паскаля. Отмечены некоторые характерные свойства матриц полученных систем рекуррентных уравнений, что привело к идее введения понятия p -латинской матрицы. p -Латинские матрицы применяются и при исследовании других арифметических треугольников, отличных от треугольника Паскаля [5]. Нами в разд. 1 и 2 получены новые свойства p -латинских матриц и на их основе исследован треугольник Паскаля по модулю простого числа p . Используя представление p -латинских матриц в удобном базисе (15), получено распределение элементов в треугольнике Паскаля $\bmod p$ для произвольной строки (17). В разд. 3 подробно исследован случай $p = 7$. Некоторые результаты по свойствам p -латинских матриц получены в [1, 6].

1. p -Латинские матрицы

Приведём определение p -латинской матрицы [2, 3].

Определение 1. Квадратная матрица порядка n называется *латинским квадратом порядка n* [3], если её элементы принимают значения $1, \dots, n$ таким образом, что каждое число встречается только один раз в каждом столбце и каждой строке.

Определение 2. Латинский квадрат порядка n называется *p -латинским квадратом порядка n* , если ни одна диагональ матрицы за исключением главной и побочной диагоналей ($i + j = n + 1$) не имеет равных элементов.

Определение 3. p -Латинский квадрат порядка n называется *нормализованным p -латинским квадратом порядка n* , если его первая строка имеет вид $(1, 2, \dots, n)$ и главная диагональ записана в форме $(1, 1, \dots, 1)$.

Построим такие квадраты для любого простого p . Введём матрицу вида $P = (j/i)_{i,j=\overline{1,p-1}}$ порядка $p - 1$, элементы которой принадлежат полю \mathbb{Z}_p .

ПРИМЕР 1. Для $p = 7$ матрица P имеет вид

$$\begin{pmatrix} 1/1 & 2/1 & 3/1 & 4/1 & 5/1 & 6/1 \\ 1/2 & 2/2 & 3/2 & 4/2 & 5/2 & 6/2 \\ 1/3 & 2/3 & 3/3 & 4/3 & 5/3 & 6/3 \\ 1/4 & 2/4 & 3/4 & 4/4 & 5/4 & 6/4 \\ 1/5 & 2/5 & 3/5 & 4/5 & 5/5 & 6/5 \\ 1/6 & 2/6 & 3/6 & 4/6 & 5/6 & 6/6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \\ 5 & 3 & 1 & 6 & 4 & 2 \\ 2 & 4 & 6 & 1 & 3 & 5 \\ 3 & 6 & 2 & 5 & 1 & 4 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

Теорема 1. Если p простое, то матрица P — нормализованный p -латинский квадрат порядка $p - 1$.

ДОКАЗАТЕЛЬСТВО. Очевидно, что элементы матрицы P , находящиеся в одном столбце или в одной строке, различны и принадлежат мультипликативной группе поля \mathbb{Z}_p . Значит, матрица P — латинский квадрат. Пусть j/i — элемент некоторой диагонали, параллельной главной, тогда любой другой элемент этой диагонали имеет вид $(j + s)/(i + s)$. Предположим, что один из этих элементов равен данному. Тогда $js = is$, тем самым $j = i$ и рассматриваемый элемент должен находиться на главной диагонали. Аналогично для побочной диагонали: $j/i = (j + s)/(i - s) \Rightarrow -j = i \Rightarrow j + i = p$, значит, элемент j/i лежит на побочной диагонали. В соответствии с определением 2 матрица P — p -латинский квадрат. Поскольку первая строка P имеет вид $(1, 2, \dots, n)$ и главная диагональ записана в форме $(1, 1, \dots, 1)$, P — нормализованный p -латинский квадрат. Теорема 1 доказана.

Определение 4. Матрицы вида

$$\mathbb{N}_p = \{(c_{p_{i,j}})_{i,j=\overline{1,p-1}} : c_1, \dots, c_{p-1} \in \mathbb{C}, (p_{i,j}) = P\}$$

называются *p-латинскими матрицами порядка p - 1*.

ПРИМЕР 2. Пусть $p = 7$. В соответствии с примером 1 следующая матрица C при $c_k \in \mathbb{C}$ принадлежит \mathbb{N}_7 :

$$C = \begin{pmatrix} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 \\ c_4 & c_1 & c_5 & c_2 & c_6 & c_3 \\ c_5 & c_3 & c_1 & c_6 & c_4 & c_2 \\ c_2 & c_4 & c_6 & c_1 & c_3 & c_5 \\ c_3 & c_6 & c_2 & c_5 & c_1 & c_4 \\ c_6 & c_5 & c_4 & c_3 & c_2 & c_1 \end{pmatrix}.$$

Лемма 1. Если $C, B \in \mathbb{N}_p$, то $CB \in \mathbb{N}_p$ и $CB = BC$.

ДОКАЗАТЕЛЬСТВО. Действительно, если $C = (c_{i,j})$ и $B = (b_{i,j})$, то

$$CB = \left(\sum_{k=1}^{p-1} c_{k/i} b_{j/k} \right)_{i,j=\overline{1,p-1}} = \left(\sum_{s=1}^{p-1} c_s b_{(j/i)/s} \right)_{i,j=\overline{1,p-1}},$$

где все операции над индексами производятся в \mathbb{Z}_p . Поэтому, если ввести обозначение $a_k = \sum_{s=1}^{p-1} c_s b_{k/s}$, то $CB = (a_{j/i})_{i,j=\overline{1,p-1}}$ и, следовательно, $CB \in \mathbb{N}_p$. Более того, рассуждая аналогично, с использованием равенства $a_k = \sum_{s=1}^{p-1} c_{k/s} b_s$ получаем

$$BC = \left(\sum_{s=1}^{p-1} b_s c_{(j/i)/s} \right)_{i,j=\overline{1,p-1}} = (a_{j/i})_{i,j=\overline{1,p-1}}.$$

Таким образом, $CB = BC$. Лемма 1 доказана.

Ниже докажем другие свойства матриц из \mathbb{N}_p . Обозначим через $\Delta^{(1)}$ треугольник Паскаля по модулю простого p , и пусть $C(n, m)$ — его произвольный элемент. Обозначим через $\Delta_s^{(1)}$ конечный треугольник, содержащий только первые s строк треугольника $\Delta^{(1)}$. Рассмотрим другой бесконечный треугольник $\Delta^{(k)} = k\Delta^{(1)}$, элементы которого $C_k(n, m)$ определяются равенствами $C_k(n, m) = kC(n, m) \pmod{p}$, и обозначим через $\Delta_s^{(k)}$

конечный треугольник, содержащий только первые s строк треугольника $\Delta^{(k)}$. Очевидно, что $\Delta_s^{(k)} = k\Delta_s^{(1)}$.

Конечный треугольник с st строками, возникающий из треугольника $\Delta_s^{(k)}$ заменой его элементов $C_k(n, l)$ треугольниками $\Delta_m^{(C_k(n, l))}$ и заполнением пустых мест нулями, обозначим через $\Delta_s^{(k)} * \Delta_m$.

ПРИМЕР 3. Для $p = 5$ треугольники $\Delta_4^{(1)}$ и $\Delta_3^{(k)}$ имеют вид

$$\Delta_4^{(1)} = \begin{array}{cccc} & & 1 & \\ & 1 & 1 & \\ 1 & 2 & 1 & \\ 1 & 3 & 3 & 1 \end{array}, \quad \Delta_3^{(1)} = \begin{array}{ccc} & & 1 \\ & 1 & 1 \\ 1 & 2 & 1 \end{array}, \quad \Delta_3^{(2)} = \begin{array}{ccc} & & 2 \\ & 2 & 2 \\ 2 & 4 & 2 \end{array}, \quad \Delta_3^{(3)} = \begin{array}{ccc} & & 3 \\ & 3 & 3 \\ 3 & 1 & 3 \end{array},$$

и тогда

$$\Delta_4^{(1)} * \Delta_3 = \Delta_4^{(1)} \equiv \begin{array}{ccccccc} & & & \Delta_3^{(1)} & & & \\ & & \Delta_3^{(1)} & & \Delta_3^{(1)} & & \\ & \Delta_3^{(1)} & & \Delta_3^{(2)} & & \Delta_3^{(1)} & \\ \Delta_3^{(1)} & & \Delta_3^{(3)} & & \Delta_3^{(3)} & & \Delta_3^{(1)} \end{array}$$

$$= \begin{array}{cccccccccccc} & & & & & & & & & & & & \\ & & & & & & & & & & & 1 & \\ & & & & & & & & & & 1 & 1 & \\ & & & & & & & & & 1 & 2 & 1 & \\ & & & & & & & & 1 & 0 & 0 & 1 & \\ & & & & & & & 1 & 1 & 0 & 1 & 1 & \\ & & & & & & 1 & 2 & 1 & 1 & 2 & 1 & \\ & & & & 1 & 0 & 0 & 2 & 0 & 0 & 1 & & \\ & & & 1 & 1 & 0 & 2 & 2 & 0 & 1 & 1 & & \\ & & 1 & 2 & 1 & 2 & 4 & 2 & 1 & 2 & 1 & & \\ & 1 & 0 & 0 & 3 & 0 & 0 & 3 & 0 & 0 & 1 & & \\ 1 & 1 & 0 & 3 & 3 & 0 & 3 & 3 & 0 & 1 & 1 & & \\ 1 & 2 & 1 & 3 & 1 & 3 & 3 & 1 & 3 & 1 & 2 & 1 & \end{array}.$$

Для того чтобы подсчитать число единиц, например, в 11-й строке треугольника $\Delta_4^{(1)} * \Delta_3$, надо найти строку треугольника $\Delta_4^{(1)}$, состоящего из треугольников $\Delta_3^{(k)}$, в которую входит 11-я строка, т.е. вычислить число $[(11-1)/3] + 1 = 4$. В 4-ю строку треугольника $\Delta_4^{(1)}$ входят только треугольники $\Delta_3^{(1)}$ и $\Delta_3^{(3)}$ по два раза. Затем надо взять строку треугольников $\Delta_3^{(k)}$, в которую входит 11-я строка, т.е. строку с номером $11 - 3((11-1)/3) = 2$, и вычислить число единиц в каждом из треугольников вида $\Delta_3^{(k)}$, входящих во 2-ю строку. Сложить произведение числа

единиц в $\Delta_3^{(k)}$ и количества чисел, равных k , в 4-й строке треугольника $\Delta_4^{(1)}$, т. е. числа треугольников $\Delta_3^{(k)}$ в $\Delta_4^{(1)}$. Имеем $2 \cdot 2 + 2 \cdot 0 = 4$.

Докажем важное фрактальное свойство треугольника Паскаля.

Теорема 2. Для любых $n, m \in \mathbb{N}$ и любого $k = \overline{1, p-1}$ верно равенство $\Delta_m^{(k)} * \Delta_{p^n} = \Delta_{mp^n}^{(k)}$.

ДОКАЗАТЕЛЬСТВО. Пусть $m > 1$, поскольку при $m = 1$ теорема очевидна. Рассмотрим треугольник $\Delta_{mp^n}^{(k)}$, каждая строка которого с номером $i + 1$ строится по строке с номером i по правилу $C(i + 1, j + 1) = C(i, j) + C(i, j + 1) \pmod{p}$, где j — номер элемента в строке, $C(i, j) = 0$ при $j > i$ или $j < 0$ и $C(0, 0) = k$. У него в строке с номером $i = p^n$ отличны от нуля только элементы с номерами $j = 0$ и $j = p^n$, они равны k , так как $C(p^n, j) = C_{p^n}^j = 0 \pmod{p}$ при $j \neq 0$ и $j \neq p^n$. Эти элементы будут вершинами двух треугольников $\Delta_{p^n}^{(k)}$ (они строятся по тому же правилу), у которых левая сторона левого и правая сторона правого треугольников совпадают с соответствующими сторонами треугольника $\Delta_{mp^n}^{(k)}$, а элементы внутренних сторон станут соседними только в строке $i = 2p^n - 1$, поэтому в строке $i = 2p^n$ элемент с номером $j = p^n$ будет равен $2k$. Кроме этого, элементы, стоящие на местах с номерами $j = 0$ и $j = 2p^n$ в строке $i = 2p^n$, равны k , остальные же элементы этой строки нулевые как элементы последних строк треугольников $\Delta_{p^n}^{(k)}$. Далее, элементы, находящиеся в строках с номерами $p^n < i < 2p^n$ между правой стороной левого треугольника $\Delta_{p^n}^{(k)}$ и левой стороной правого треугольника, нулевые в силу правила построения строк в $\Delta_{mp^n}^{(k)}$. Воспользуемся методом индукции. Пусть в строке с номером $i = sp^n$, $s = 2, \dots, m$, элементы с номерами мест, не кратными p^n , нулевые. Рассмотрим элементы, стоящие в этой строке на местах $j = tp^n$ и $j = (t + 1)p^n$. Пусть они равны r_1 и r_2 . Очевидно, что элементы правой стороны треугольника $\Delta_{p^n}^{(r_1)}$ с вершиной в элементе с координатами $i = sp^n$, $j = tp^n$ и левой стороны треугольника $\Delta_{p^n}^{(r_2)}$ с вершиной в элементе с координатами $i = sp^n$ и $j = (t + 1)p^n$ будут соседними в строке $i = (s + 1)p^n - 1$ и поэтому дадут в строке $i = (s + 1)p^n$ элемент $r_1 + r_2 \pmod{p}$, стоящий на месте $j = (t + 1)p^n$. Элементы же строки $i = (s + 1)p^n$, стоящие на местах $tp^n < j < (t + 1)p^n$ и $(t + 1)p^n < j < (t + 2)p^n$, будут нулевыми как элементы последних строк треугольников $\Delta_{p^n}^{(r_1)}$ и $\Delta_{p^n}^{(r_2)}$. Поэтому элемент $r_1 + r_2 \pmod{p}$ породит треугольник $\Delta_{p^n}^{(r_1 + r_2 \pmod{p})}$, т. е.

$$\begin{array}{ccc} \Delta_{p^n}^{(r_1)} & \Delta_{p^n}^{(r_2)} & r_1 \quad r_2 \\ \downarrow & & \downarrow \\ \Delta_{p^n}^{(r_1+r_2 \pmod{p})} & \sim & r_1 + r_2 \pmod{p} \end{array}.$$

Кроме того, элементы треугольника $\Delta_{mp^n}^{(k)}$, находящиеся между соседними сторонами треугольников $\Delta_{p^n}^{(r_1)}$ и $\Delta_{p^n}^{(r_2)}$, будут также нулевыми в соответствии с правилом построения строк в $\Delta_{mp^n}^{(k)}$. Аналогичные рассуждения верны для всех $t = 0, 1, \dots, s-1$. Итак, строка $i = sp^n$ порождает строку $i = (s+1)p^n$ в соответствии с правилом построения строк в треугольнике Паскаля. Если в строке $i = sp^n$ отбросить элементы, стоящие на местах, номера которых не кратны p^n (они нулевые), то получим строку треугольника $\Delta_m^{(k)}$ с номером $i = s$. Поскольку s произвольно и при $s = 1, 2$ утверждение теоремы справедливо, оно справедливо и при любом s . Теорема 2 доказана.

Теорема 2 позволяет свести исследование треугольника $\Delta^{(1)}$ к исследованию треугольников $\Delta_p^{(k)}$ для $k = \overline{1, p-1}$. Детали даны в теореме 3.

Пусть для простоты изложения $n \in \mathbb{N}_0 \equiv \mathbb{N} \cup \{0\}$, т. е. первую строку треугольника $\Delta^{(k)}$ будем считать нулевой строкой, то же верно для треугольников $\Delta_p^{(k)}$.

Определение 5. Матрицей B_k при $0 \leq k \leq p-1$ назовём такую квадратную матрицу порядка $p-1$, элемент $b_{i,s}$ которой является числом элементов, равных s , в k -й строке треугольника $\Delta_p^{(i)}$. Очевидно, что $B_0 = \text{diag}(1, \dots, 1) \equiv E$.

Обозначим через $g_s^{(i)}(k, p)$ число элементов, равных s ($1 \leq s \leq p-1$) по модулю p , в k -й строке треугольника $\Delta^{(i)}$. Ясно, что $(B_k)_{i,s} = g_s^{(i)}(k, p)$.

Теорема 3. Если $n = (a_r, \dots, a_0)_p$ является p -арным представлением числа n , то

$$g_s^{(i)}(n, p) = (B_{a_r} \dots B_{a_0})_{i,s}. \quad (1)$$

Доказательство. Используя теорему 2, запишем равенство

$$\Delta_{p^{r+1}}^{(1)} = \Delta_p^{(1)} * \Delta_{p^r},$$

которое означает, что n -я строка треугольника $\Delta_{p^{r+1}}^{(1)}$ находится в a_r -й строке треугольника $\Delta_p^{(1)}$, состоящего из треугольников $\Delta_{p^r}^{(i)}$, $i = \overline{1, p-1}$

(см. пример 3). Если ввести обозначение $n_{(k)} \equiv (a_{r-k}, \dots, a_0)_p$, то из определения матриц B_k вытекает следующее векторное равенство:

$$\begin{pmatrix} g_s^{(1)}(n, p) \\ \vdots \\ g_s^{(p-1)}(n, p) \end{pmatrix} = B_{a_r} \begin{pmatrix} g_s^{(1)}(n_{(1)}, p) \\ \vdots \\ g_s^{(p-1)}(n_{(1)}, p) \end{pmatrix}.$$

Продолжая этот процесс, получим равенство

$$\begin{pmatrix} g_s^{(1)}(n, p) \\ \vdots \\ g_s^{(p-1)}(n, p) \end{pmatrix} = B_{a_r} B_{a_{r-1}} \dots B_{a_1} \begin{pmatrix} g_s^{(1)}(n_{(r)}, p) \\ \vdots \\ g_s^{(p-1)}(n_{(r)}, p) \end{pmatrix}.$$

Так как $n_{(r)} = a_0$ и $g_s^{(i)}(a_0, p) = (B_{a_0})_{i,s}$, имеем

$$\begin{pmatrix} g_s^{(1)}(n, p) \\ \vdots \\ g_s^{(p-1)}(n, p) \end{pmatrix} = B_{a_r} B_{a_{r-1}} \dots B_{a_1} (B_{a_0})_s = (B_{a_r} B_{a_{r-1}} \dots B_{a_1} B_{a_0})_s,$$

откуда следует равенство (1). Здесь $(B_k)_s$ обозначает s -й столбец матрицы B_k . Теорема 3 доказана.

Используя терему 3, можно свести вычисление $g_s^{(1)}(n, p)$, $s = \overline{1, p-1}$, к нахождению произведения матриц B_k .

Теорема 4. Для $k = \overline{0, p-1}$ верно включение $B_k \in \mathbb{N}_p$, т. е. B_k — p -латинские матрицы.

ДОКАЗАТЕЛЬСТВО. Пусть $b_1^{(k)}, \dots, b_{p-1}^{(k)}$ — элементы первой строки матрицы B_k . Докажем равенство

$$B_k = (b_{p_{i,j}}^{(k)})_{i,j=\overline{1,p-1}}, \quad (2)$$

где матрица $(p_{i,j})_{i,j=\overline{1,p-1}} = P$ определена выше. Можем определить операцию сложения треугольников $\Delta_p^{(k)}$ как операцию сложения между элементами этих треугольников, стоящих на одинаковых местах по модулю p , т. е.

$$\Delta_p^{(k_1)} + \Delta_p^{(k_2)} = k_1 \Delta_p^{(1)} + k_2 \Delta_p^{(1)} = (k_1 + k_2)(\text{mod } p) \Delta_p^{(1)} = \Delta_p^{(k_1+k_2)},$$

где сложение в верхнем индексе треугольника производится в \mathbb{Z}_p . Например, верно равенство

$$\sum_{k=1}^s \Delta_p^{(1)} = \Delta_p^{(s)} \quad (3)$$

для $s = \overline{1, p-1}$. Если обозначить элементы матрицы B_k через $b_{i,j}^{(k)}$, то, используя (3) и определение 5 матрицы B_k , можем записать $b_{1,j}^{(k)} = b_{s,j_s}^{(k)}$ для каждого $s = \overline{1, p-1}$. Таким образом, $b_{i,j}^{(k)} = b_{1,j/i}^{(k)}$ и, значит, вспоминая определение матрицы P , убеждаемся в верности формулы (2). Теорема 4 доказана.

Пусть n_k обозначает число элементов, равных k , в p -арном представлении числа $n = (a_r, \dots, a_0)_p$. В силу (1) с помощью леммы 1 можем записать

$$g_s^{(i)}(n, p) = \left(\prod_{k=1}^{p-1} B_k^{n_k} \right)_{i,s}. \quad (4)$$

Матрица $B_0 = E$ здесь опущена. Чтобы вычислить значение $g_s^{(k)}(n, p)$, нужно исследовать дополнительные свойства матриц из \mathbb{N}_p .

2. Свойства матриц из \mathbb{N}_p

Ясно, что \mathbb{N}_p является подпространством в пространстве квадратных матриц порядка $p-1$. Кроме этого справедлива

Лемма 2. $\dim \mathbb{N}_p = p-1$ и

$$B \in \mathbb{N}_p \Rightarrow B = \sum_{k=1}^{p-1} b_k I_k, \quad (5)$$

где $I_k \in \mathbb{N}_p$ и $I_k = (\delta_{ki,j})_{i,j=\overline{1,p-1}}$. Здесь $\delta_{i,j}$ — символ Кронекера и все операции над индексами производятся в \mathbb{Z}_p .

ДОКАЗАТЕЛЬСТВО. Действительно, в силу определения 4 элемент b_k матрицы B , стоящий в первой строке на k -м месте, будет стоять в i -й строке на месте с номером j , определяемом из равенства

$$k = j/i \pmod{p} \Rightarrow j = ki \pmod{p}.$$

Поэтому

$$B \in \mathbb{N}_p \Rightarrow B = \sum_{k=1}^{p-1} b_k (\delta_{ki,j})_{i,j=\overline{1,p-1}} = \sum_{k=1}^{p-1} b_k I_k.$$

Нетрудно видеть, что $I_1 = E$. Лемма 2 доказана.

Лемма 3. Матрицы I_k обладают свойством $I_k I_m = I_{km}$, $k = \overline{1, p-1}$, где число km приведено по mod p .

ДОКАЗАТЕЛЬСТВО. В самом деле,

$$I_k I_m = \left(\sum_{s=1}^{p-1} \delta_{ki,s} \delta_{ms,j} \right)_{i,j=\overline{1,p-1}},$$

следовательно, элемент матрицы $I_k I_m$ с индексами i и j не равен нулю, если существует такое $s \in \mathbb{Z}_p$, что $ki = s \pmod{p}$ и $ms = j \pmod{p}$. Значит, $j = kmi \pmod{p}$, поэтому

$$I_k I_m = (\delta_{kmi,j})_{i,j=\overline{1,p-1}} = I_{km}.$$

Лемма 3 доказана.

Пусть ν — корень уравнения $x^{p-1} = 1$ в поле \mathbb{Z}_p такой, что для каждого $k = \overline{1, p-2}$ верно неравенство $\nu^k \neq 1$ (примитивный корень). Тогда обозначим $J_k = (I_\nu)^k$. Ясно, что $J_{p-1} = (I_\nu)^{p-1} = E$.

Пусть $B \in \mathbb{N}_p$. Если обозначить $c_k = b_{\nu^k}$, то равенство (5) перепишется в виде

$$B = \sum_{k=1}^{p-1} c_k J_k. \quad (6)$$

Лемма 4. Матрицы I_k , а значит, и J_k ортогональны, и J_k обладают свойством $J_k J_m = J_{k+m}$, где сумма $k+m$ приведена по mod $(p-1)$.

ДОКАЗАТЕЛЬСТВО. Докажем, что $I_k I_k^* = E$, где $(a_{i,j})^* = (\bar{a}_{j,i})$ и черта означает комплексное сопряжение. Это следует из равенства

$$I_k^* = (\delta_{kj,i})_{i,j=\overline{1,p-1}} = (\delta_{i,kj})_{i,j=\overline{1,p-1}} = (\delta_{i/k,j})_{i,j=\overline{1,p-1}} = I_{1/k},$$

поскольку $I_k I_{1/k} = I_1 = E$ по лемме 3. Тем самым

$$J_k J_k^* = (I_\nu)^k (I_\nu^k)^* = (I_\nu I_\nu^*)^k = E.$$

Далее

$$J_k J_m = (I_\nu)^k (I_\nu)^m = (I_\nu)^{k+m} = J_{k+m \pmod{p-1}},$$

значит, $J_k J_m = E \Rightarrow k+m = p-1 \Rightarrow m = p-k-1$, поскольку $J_{p-1} = E$, и, стало быть, для $k = \overline{1, p-2}$

$$J_k^{-1} = J_k^* = J_{p-k-1}. \quad (7)$$

Лемма 4 доказана.

Лемма 5. Пусть μ — собственное число матрицы $B \in \mathbb{N}_p$. Тогда уравнение $z^{p-1} = 1$ имеет корень λ в \mathbb{C} такой, что

$$\mu = \sum_{k=1}^{p-1} c_k \lambda^k, \quad (8)$$

где коэффициенты c_k определяются из (6). Кроме того, числа вида (8), где λ — произвольный корень уравнения $z^{p-1} = 1$, являются собственными числами матрицы B .

ДОКАЗАТЕЛЬСТВО. Пусть a — некоторый вектор из \mathbb{C}^{p-1} , λ — корень уравнения $z^{p-1} = 1$ и

$$b = \sum_{k=1}^{p-1} \lambda^{-k} J_k a. \quad (9)$$

Тогда

$$J_s b = \sum_{k=1}^{p-1} \lambda^{-k} J_s J_k a = \sum_{k=1}^{p-1} \lambda^{-k} J_{s+k \pmod{p-1}} a = \lambda^s \sum_{k+s=1}^{p-1} \lambda^{-k-s} J_{s+k} a = \lambda^s b$$

для любого $s = \overline{1, p-1}$. Поэтому, используя (6), запишем

$$Bb = \sum_{k=1}^{p-1} c_k J_k b = \sum_{k=1}^{p-1} c_k \lambda^k b = \mu b,$$

т. е. μ — собственное число матрицы B . Остаётся доказать, что формула (8) задаёт все собственные числа матрицы B . Завершим доказательство после леммы 9.

Следствие 1. Матрицы J_k и I_k таковы, что $\det I_k = \det J_k = 1$, $k = \overline{1, p-1}$.

ДОКАЗАТЕЛЬСТВО. В силу леммы 5 числа $\mu_i = \lambda_i^k$, где λ_i — некоторый корень уравнения $z^{p-1} = 1$ в \mathbb{C} , и только они являются собственными числами матрицы J_k , $k = \overline{1, p-1}$. Если $\mu_i = \mu_j$, то собственные векторы вида (9) при некотором a различны. Если λ_i , $i = \overline{1, p-1}$, — все корни уравнения $z^{p-1} = 1$, то $\det J_k = \prod_{i=1}^{p-1} \lambda_i^k = \mu^k$, где $\mu = \lambda_1 \dots \lambda_{p-1}$. Испол-

зуя равенство $\sum_{k=1}^{p-1} k = 0 \pmod{p}$, получаем $\mu = 1$ и, значит, $\det J_k = 1$ для $k = \overline{1, p-1}$. Это означает, что и $\det I_k = 1$. Следствие 1 доказано.

Лемма 6. Пусть матрица B принадлежит \mathbb{N}_p и записана в виде (6). Тогда

$$B^* = \sum_{k=1}^{p-2} \bar{c}_{p-k-1} J_k + \bar{c}_{p-1} J_{p-1}.$$

ДОКАЗАТЕЛЬСТВО. Используя (7) и равенство $J_{p-1}^* = E^* = E = J_{p-1}$, получаем

$$\begin{aligned} B^* &= \sum_{k=1}^{p-2} \bar{c}_k J_k^* + \bar{c}_{p-1} J_{p-1}^* = \sum_{k=1}^{p-2} \bar{c}_k J_{p-k-1} + \bar{c}_{p-1} J_{p-1} \\ &= \sum_{k=1}^{p-2} \bar{c}_{p-k-1} J_k + \bar{c}_{p-1} J_{p-1}. \end{aligned}$$

Лемма 6 доказана.

Введём класс матриц S_i при $i = \overline{1, p-1}$ в виде

$$S_i = \frac{1}{p-1} \sum_{k=1}^{p-1} \lambda_i^{-k} J_k. \quad (10)$$

Здесь, как и раньше, λ_i — один из корней уравнения $z^{p-1} = 1$ в \mathbb{C} . Ясно, что матрицы S_i принадлежат \mathbb{N}_p как линейные комбинации матриц из \mathbb{N}_p и $S_i \neq 0$. Пусть ν — примитивный корень уравнения $z^{p-1} = 1$ в \mathbb{C} , т. е. при $k = \overline{1, p-2}$ имеем $\nu^k \neq 1$. Поэтому в (10) можно считать, что корни λ_i для удобства записи занумерованы в соответствии со степенями примитивного корня ν так, что $\lambda_i = \nu^i$. Поскольку $\lambda_i^{-k} = (\bar{\lambda}_k)^i$, равенство (10) можно переписать в виде

$$S_i = \frac{1}{p-1} \sum_{k=1}^{p-1} \bar{\lambda}_i^k J_k = \frac{1}{p-1} \sum_{k=1}^{p-1} \bar{\lambda}_k^i J_k. \quad (11)$$

Теорема 5. Равенства

$$S_i S_j = \delta_{i,j} S_i \quad (12)$$

справедливы при $i, j = \overline{1, p-1}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим левую часть (12). Если положить $J_0 = (I_\nu)^0 = E$, то

$$S_i = \frac{1}{p-1} \sum_{k=0}^{p-2} \lambda_i^{-k} J_k$$

и с учётом $\lambda_i^{-k} \lambda_j^k = \lambda_{i-j}^{-k}$ после некоторых преобразований имеем

$$S_i S_j = \frac{1}{(p-1)^2} \left(\sum_{l=0}^{p-2} \lambda_j^{-l} J_l \sum_{k=0}^l \lambda_{i-j}^{-k} + \sum_{l=p-1}^{2(p-2)} \lambda_j^{-l} J_l \sum_{k=l-p+2}^{p-2} \lambda_{i-j}^{-k} \right),$$

откуда, заменяя $l-p+1 \rightarrow l$ во второй внешней сумме, с учётом равенства $J_k = J_{k+p-1}$ получим

$$S_i S_j = \frac{1}{(p-1)^2} \left(\sum_{l=0}^{p-2} \lambda_j^{-l} J_l \sum_{k=0}^l \lambda_{i-j}^{-k} + \sum_{l=0}^{p-3} \lambda_j^{-l} J_l \sum_{k=l+1}^{p-2} \lambda_{i-j}^{-k} \right),$$

значит, после объединения внутренних сумм имеем

$$S_i S_j = \frac{1}{(p-1)^2} \sum_{l=0}^{p-2} \lambda_j^{-l} J_l \sum_{k=0}^{p-2} \lambda_{i-j}^{-k}.$$

Исследуем полученное равенство. С учётом того, что $\lambda_{i-j} = \lambda_i / \lambda_j$, где $\lambda_i \neq \lambda_j$, при $i \neq j$, получаем

$$\sum_{k=0}^{p-2} \lambda_{i-j}^{-k} = \frac{\lambda_{i-j}^{1-p} - 1}{\lambda_{i-j}^{-1} - 1} = 0.$$

Следовательно, (12) верно при $i \neq j$. Далее, при $i = j$ имеем $\lambda_{i-j} = \lambda^0 = 1$ и, значит,

$$\sum_{k=0}^{p-2} \lambda_{i-j}^{-k} = \begin{cases} 0, & i \neq j, \\ p-1, & i = j, \end{cases} \quad (13)$$

откуда $S_i^2 = S_i$. Теорема 5 доказана.

Обозначим через $A^t = (a_{j,i})_{i,j=\overline{1,p-1}}$ матрицу, транспонированную к A .

Лемма 7. Матрицы S_i при $i = \overline{1, p-1}$ эрмитовы, т. е. $S_i^* = S_i$, и при $i = \overline{1, p-2}$ верны равенства $S_i^t = S_{p-i-1}$.

ДОКАЗАТЕЛЬСТВО. Действительно, для $i = \overline{1, p-1}$ с учётом того, что $\bar{\lambda}_i = \lambda_{p-i-1} = \lambda_i^{-1}$, ввиду равенства (7) запишем

$$S_i^* = \frac{1}{p-1} \sum_{k=1}^{p-1} \lambda_i^k J_k^* = \frac{1}{p-1} \sum_{k=1}^{p-1} \lambda_i^{k-p+1} J_{p-k-1} = S_i.$$

Аналогично можно получить

$$\begin{aligned} S_i^t &= \frac{1}{p-1} \sum_{k=1}^{p-1} \lambda_i^{-k} J_k^* = \frac{1}{p-1} \sum_{k=1}^{p-1} \lambda_i^{p-k-1} J_{p-k-1} = \frac{1}{p-1} \sum_{k=1}^{p-1} \lambda_i^k J_k \\ &= \frac{1}{p-1} \sum_{k=1}^{p-1} \lambda_{p-i-1}^{-k} J_k = S_{p-i-1}. \end{aligned}$$

Лемма 7 доказана.

Теорема 6. Для $k = \overline{1, p-1}$ справедливы равенства, обратные к (10):

$$J_k = \sum_{i=1}^{p-1} \lambda_i^k S_i. \quad (14)$$

ДОКАЗАТЕЛЬСТВО. Используя определение (10) матриц S_i и равенства (13), в результате преобразований получим

$$\begin{aligned} \sum_{i=1}^{p-1} \lambda_i^k S_i &= \sum_{j=1}^{p-1} \left(\frac{1}{p-1} \sum_{i=1}^{p-1} \lambda_i^{k-j} \right) J_j = \sum_{j=1}^{p-1} \left(\frac{1}{p-1} \sum_{i=0}^{p-2} \lambda_{j-k}^{-i} \right) J_j \\ &= \sum_{j=1}^{p-1} \delta_{j,k} J_j = J_k. \end{aligned}$$

Теорема 6 доказана.

В дополнение к лемме 7 следует отметить, что матрица S_{p-1} состоит из одних чисел $\frac{1}{p-1}$ на всех местах, значит, $S_{p-1}^t = S_{p-1}$. Это следует из равенств

$$\begin{aligned} S_{p-1} &= \frac{1}{p-1} \sum_{k=1}^{p-1} J_k = \frac{1}{p-1} \sum_{k=1}^{p-1} I_k = \frac{1}{p-1} \left(\sum_{k=1}^{p-1} \delta_{ki,j} \right)_{i,j=\overline{1,p-1}} \\ &= \frac{1}{p-1} (1)_{i,j=\overline{1,p-1}}, \end{aligned}$$

если учесть, что $\sum_{k=1}^{p-1} \delta_{ki(\bmod p),j} = 1$ для всех $i, j = \overline{1, p-1}$.

Лемма 8. Пусть $B \in \mathbb{N}_p$. Тогда

$$B = \sum_{i=1}^{p-1} \mu_i S_i, \quad (15)$$

где μ_i — некоторые собственные числа матрицы B .

ДОКАЗАТЕЛЬСТВО. Действительно, из формул (6) и (8) и теоремы 6 следует представление

$$B = \sum_{k=1}^{p-1} c_k J_k = \sum_{i=1}^{p-1} S_i \sum_{k=1}^{p-1} c_k \lambda_i^k = \sum_{i=1}^{p-1} \mu_i S_i,$$

где $\mu_i = \sum_{k=1}^{p-1} c_k \lambda_i^k$. Рассмотрим вектор вида $b_i = S_i a$. Для него по теореме 5 выводим

$$S_i b_i = S_i S_i a = S_i a = b_i, \quad S_j b_i = S_j S_i a = 0 \quad (i \neq j).$$

Поэтому $Bb_i = \sum_{j=1}^{p-1} \mu_j S_j b_i = \mu_i b_i$, т.е. μ_i — собственное число матрицы B , а b_i — собственный вектор, отвечающий ему. Ясно, что матрицы S_1, \dots, S_{p-1} линейно независимы, поскольку из равенства $\alpha_1 S_1 + \dots + \alpha_{p-1} S_{p-1} = 0$ после умножения на S_i по теореме 5 вытекает, что $\alpha_i S_i = 0 \Rightarrow \alpha_i = 0$. Значит, по лемме 2 S_1, \dots, S_{p-1} — базис в \mathbb{N}_p . Используя этот базис, можем легко выписать произведение матриц из \mathbb{N}_p . Лемма 8 доказана.

Теорема 7. Пусть $\mu_1^{(i)}, \dots, \mu_{p-1}^{(i)}$ — собственные числа матриц B_i из теоремы 3 и

$$\sigma_j = \prod_{i=1}^{p-1} (\mu_j^{(i)})^{n_i}. \quad (16)$$

Тогда

$$g_s^{(i)}(n, p) = \left(\sum_{j=1}^{p-1} \sigma_j S_j \right)_{i,s}. \quad (17)$$

ДОКАЗАТЕЛЬСТВО. Нетрудно видеть, что, используя (15) и теорему 5, можем получить

$$\begin{aligned} B_i^2 &= (\mu_1^{(i)} S_1 + \dots + \mu_{p-1}^{(i)} S_{p-1})^2 = (\mu_1^{(i)})^2 S_1 + \dots + (\mu_{p-1}^{(i)})^2 S_{p-1} \\ &\Rightarrow B_i^{n_i} = \sum_{j=1}^{p-1} (\mu_j^{(i)})^{n_i} S_j. \end{aligned}$$

Поэтому равенство (4) преобразуется в (17). Теорема 7 доказана.

Заметим, что из (1) следует, что $\sigma_j = \mu_j^{(a_r)} \dots \mu_j^{(a_0)}$.

Лемма 9. Любой собственный вектор b_i матрицы $B \in \mathbb{N}_p$, отвечающий собственному значению μ_i , может быть записан в виде

$$b_i = \sum_{(j), \mu_j = \mu_i} S_j c_j, \quad (18)$$

где $c_j \in \mathbb{C}^{p-1}$ и суммирование ведётся по таким j , что $\mu_j = \mu_i$.

ДОКАЗАТЕЛЬСТВО. Пусть b_i — собственный вектор $B \in \mathbb{N}_p$, отвечающий собственному значению μ_i . Действуя матрицей S_s на равенство $Bb_i = \mu_i b_i$ и используя (15) и теорему 5, получим $\mu_s S_s b_i = \mu_i S_s b_i$. Если здесь $\mu_s \neq \mu_i$, то $S_s b_i = 0$. Теперь с помощью равенства $E = S_1 + \dots + S_{p-1}$, которое следует из леммы 8 при $B = E$ ($\mu_i = 1$), получаем представление (18):

$$b_i = Eb_i = (S_1 + \dots + S_{p-1})b_i = \sum_{(j)} S_j b_i.$$

Рассмотрим некоторый вектор $c \in \mathbb{C}^{p-1}$. В силу представления (15) $BS_i c = \mu_i S_i c$, значит, $S_i c$ — собственный вектор B , отвечающий собственному числу μ_i , т. е. правая часть (16) при любых $c_j \in \mathbb{C}^{p-1}$ — собственный вектор, отвечающий μ_i . Лемма 9 доказана.

ПРОДОЛЖЕНИЕ ДОКАЗАТЕЛЬСТВА ЛЕММЫ 5. Возьмём $c \in \mathbb{C}^{p-1}$ такое, что $S_k c \neq 0$ для любого k . Это возможно, например, для $c = (1, 0, \dots, 0)$. Выше показано, что $c_k = S_k c$ — собственный вектор матрицы $B \in \mathbb{N}_p$, отвечающий собственному числу μ_k , определяемому из (8) при $\lambda = \lambda_k$. По выбору c он ненулевой. Докажем, что векторы $c_k \neq 0$ при $k = \overline{1, p-1}$ линейно независимы. Действительно, если не все равные нулю числа $\delta_1, \dots, \delta_{p-1} \in \mathbb{C}$ таковы, что $\delta_1 c_1 + \dots + \delta_{p-1} c_{p-1} = 0$, то, действуя на это равенство матрицей S_k , получим $\delta_k c_k = 0$ и, значит, $\delta_k = 0$; противоречие. Тем самым векторы $c_k \neq 0$ при $k = \overline{1, p-1}$ образуют базис в \mathbb{C}^{p-1} . Если $\mu \neq 0$ — некоторое собственное число матрицы $B \in \mathbb{N}_p$, а c — собственный вектор, то $c = \delta_1 c_1 + \dots + \delta_{p-1} c_{p-1} \Rightarrow \mu c = \delta_1 \mu_1 c_1 + \dots + \delta_{p-1} \mu_{p-1} c_{p-1} \Rightarrow c = \delta_1 \frac{\mu_1}{\mu} c_1 + \dots + \delta_{p-1} \frac{\mu_{p-1}}{\mu} c_{p-1}$, и в силу единственности разложения c по базису при $\delta_k \neq 0$ имеем $\mu = \mu_k$. Наконец, если $\mu_k \neq 0$ для любого k , то матрица $B \in \mathbb{N}_p$ не может иметь собственное число $\mu = 0$, поскольку из формулы выше в этом случае следует, что $Bc = 0 \Rightarrow c = 0$. Лемма 5 доказана.

Лемма 10. Если $\mu_i \neq 0$ для $i = \overline{1, p-1}$, то матрица $B \in \mathbb{N}_p$ имеет обратную вида $B^{-1} = \sum_{i=1}^{p-1} \mu_i^{-1} S_i$.

ДОКАЗАТЕЛЬСТВО. Согласно лемме 8 и теореме 5 имеем

$$B \sum_{i=1}^{p-1} \mu_i^{-1} S_i = \sum_{i=1}^{p-1} \mu_i S_i \sum_{i=1}^{p-1} \mu_i^{-1} S_i = \sum_{i=1}^{p-1} S_i = E,$$

так как $E = S_1 + \dots + S_{p-1}$. Лемма 10 доказана.

Теперь можно применить полученные свойства матриц из \mathbb{N}_p к вычислению $g_s^{(i)}(n, p)$ для $p = 7$. Следует отметить, что в [4] эта проблема рассмотрена для $p = 3$ и $p = 5$. Упомянем интересное свойство биномиальных коэффициентов, вытекающее из теоремы 2.

Теорема 8 (Люка [7]). Пусть числа $n \geq m \geq 0$ целые. Если $n = (a_r, \dots, a_0)_p$ и $m = (b_r, \dots, b_0)_p$ являются p -арными представлениями чисел n и m , то

$$C_n^m = C_{a_r}^{b_r} \dots C_{a_0}^{b_0} (\bmod p),$$

где следует считать, что $C_i^j = 0$ при $j > i$.

ДОКАЗАТЕЛЬСТВО. Используя теорему 2, запишем равенство

$$\Delta_{p^{r+1}}^{(1)} = \Delta_p^{(1)} \equiv \Delta_p^{(1)} * \Delta_{p^r},$$

которое означает, что n -я строка треугольника $\Delta_{p^{r+1}}^{(1)}$ находится в a_r -й строке треугольника $\Delta_p^{(1)}$, состоящего из треугольников $\Delta_{p^r}^{(k)}$, $k = \overline{1, p-1}$, а элемент с номером m в этой строке находится на b_r -м месте в строке с номером a_r треугольника $\Delta_p^{(1)}$ (см. пример 3). Нумерация строк начинается тоже с нуля. Таким образом, элемент на m -м месте в n -й строке треугольника $\Delta_{p^{r+1}}^{(1)}$ (обозначим его через $C(n, m)$) должен быть в треугольнике вида $C_{a_r}^{b_r} (\bmod p) \cdot \Delta_{p^r}^{(1)}$ в строке с номером $n_{(1)} = (a_{r-1}, \dots, a_0)_p$ на месте с номером $m_{(1)} = (b_{r-1}, \dots, b_0)_p$. Если окажется, что $a_{r-1} < b_{r-1}$, то элемент $C(n, m)$ попадёт в пространство между соседними треугольниками вида $\Delta_{p^r}^{(k)}$, составляющими $\Delta_p^{(1)}$, которое заполнено нулями. Тем самым получим

$$C(n, m) \in C_{a_r}^{b_r} \dots C_{a_{r-k+1}}^{b_{r-k+1}} (\bmod p) \cdot \Delta_{p^{r-k+1}}^{(1)}$$

и либо $C(n, m)$ находится в $n_{(k)}$ -й строке на $m_{(k)}$ -м месте в $\Delta_{p^{r-k+1}}^{(1)}$, где $n_{(k)} \equiv (a_{r-k}, \dots, a_0)_p$ (это будет при $a_{r-i} \geq b_{r-i}$), либо $C(n, m)$ попадёт в пространство, заполненное нулями, и, значит, $C_n^m = 0 (\bmod p)$. Отсюда при $k = r$ с учётом того, что элемент треугольника $\Delta_p^{(1)}$ в a_0 -й строке и на

b_0 -м месте, равен $C_{a_0}^{b_0}(\bmod p)$, получим доказываемую формулу. Теорема 8 доказана.

ПРИМЕР 4. Вычислим $C_{68}^3(\bmod 7)$. Нетрудно подсчитать, что $68 = 7^2 + 2 \cdot 7 + 5 = (125)_7$. Значит, по теореме 8 имеем $C_{68}^3 = C_1^0 C_2^0 C_5^3 = 10 = 3(\bmod 7)$.

3. Вычисление $g_s^{(i)}(n, 7)$

Чтобы вычислить $g_s^{(i)}(n, 7)$ в соответствии с теоремой 7, необходимо исследовать треугольники $\Delta_7^{(k)}$ для $i = \overline{1, 6}$. Треугольник $\Delta_7^{(1)}$ имеет вид, изображённый на рис. 1 слева. Если умножим каждый элемент треугольника $\Delta_7^{(1)}$ на k в \mathbb{Z}_7 , то получим $\Delta_7^{(k)}$. Например, треугольник $\Delta_7^{(3)}$ имеет вид, изображённый на рис. 1 справа.

$$\begin{array}{cccccc}
 & & 1 & & & & & & 3 & & & \\
 & & 1 & 1 & & & & & 3 & 3 & & \\
 & & 1 & 2 & 1 & & & & 3 & 6 & 3 & \\
 & & 1 & 3 & 3 & 1 & & & 3 & 2 & 2 & 3 \\
 & & 1 & 4 & 6 & 4 & 1 & & 3 & 5 & 4 & 5 & 3 \\
 & & 1 & 5 & 3 & 3 & 5 & 1 & 3 & 1 & 2 & 2 & 1 & 3 \\
 & & 1 & 6 & 1 & 6 & 1 & 6 & 1 & 3 & 4 & 3 & 4 & 3 & 4 & 3
 \end{array}$$

Рис. 1

Теперь необходимо найти матрицы B_k для $k = \overline{0, 6}$. Возьмём, например, 4-ю строку треугольников $\Delta_7^{(k)}$, которая даёт нам матрицу B_4 (нумерация начинается с нуля). Четвёртая строка треугольника $\Delta_7^{(1)}$ имеет вид $(1, 4, 6, 4, 1)$. Поскольку числа 1 и 4 встречаются дважды, а число 6 встречается один раз, первая строка матрицы B_4 имеет вид $(2, 0, 0, 2, 0, 1)$. Если мы хотим подсчитать 3-ю строку матрицы B_4 , то надо взять 4-ю строку треугольника $\Delta_7^{(3)}$, которая даёт нам желаемый результат $(0, 0, 2, 1, 2, 0)$. Таким образом можем подсчитать все матрицы B_k при $k = \overline{0, 6}$. Чтобы записать наши вычисления, воспользуемся матрицами J_k , $k = \overline{1, 6}$. Найдём матрицу J_1 . В нашем случае $\nu = 3$, потому что для всякого $k = \overline{1, 5}$ верно неравенство $3^k \neq 1(\bmod 7)$. Поэтому

$$J_1 = I_3 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Теперь можем записать

$$\begin{aligned} B_0 &= J_6, & B_1 &= 2J_6, & B_2 &= J_2 + 2J_6, & B_3 &= 2J_1 + 2J_6, \\ B_4 &= J_3 + 2J_4 + 2J_6, & B_5 &= 2J_1 + 2J_5 + 2J_6, & B_6 &= 3J_3 + 4J_6. \end{aligned} \quad (19)$$

Используя обозначения теоремы 7 и формулы (8) и (19), для каждого $k = \overline{1, 6}$ найдём

$$\mu_k^{(1)} = 2, \quad \mu_k^{(2)} = \lambda_k^2 + 2, \quad \mu_k^{(3)} = 2\lambda_k + 2, \quad \mu_k^{(4)} = \lambda_k^3 + 2\lambda_k^4 + 2,$$

$$\mu_k^{(5)} = 2(\lambda_k + \lambda_k^5 + 1), \quad \mu_k^{(6)} = 3\lambda_k^3 + 4.$$

Предположим, что число $k = \overline{1, 6}$ содержится в записи числа $(n)_7$ всего n_k раз. Тогда согласно (16) имеем $\sigma_k = (\mu_k^{(1)})^{n_1} \dots (\mu_k^{(6)})^{n_6}$, значит, учитывая, что $\lambda_k = \exp(ik\pi/3)$ (здесь $i^2 = -1$), имеем (σ_1 вычислено подробно)

$$\begin{aligned} \sigma_1 &= 2^{n_1} \left(2 - \frac{1}{2} + i\frac{\sqrt{3}}{2} \right)^{n_2} (2 + 1 + i\sqrt{3})^{n_3} (2 - 1 - 1 - i\sqrt{3})^{n_4} \\ &\quad \times (1 + i\sqrt{3} + 1 - i\sqrt{3} + 2)^{n_5} (-3 + 4)^{n_6} \\ &= 2^{n_1 - n_2} (3 + i\sqrt{3})^{n_2 + n_3} (-i\sqrt{3})^{n_4} 4^{n_5}, \\ \sigma_2 &= 2^{n_1 - n_2} (3 - i\sqrt{3})^{n_2} (1 + i\sqrt{3})^{n_3} (2 + i\sqrt{3})^{n_4} (2\lambda_2 + 2\lambda_4 + 2)^{n_5} 7^{n_6}, \\ \sigma_3 &= (-1)^{n_5} 2^{n_1 + n_5} 3^{n_2 + n_4} (2\lambda_3 + 2)^{n_3}, \\ \sigma_4 &= \overline{\sigma_2}, \quad \sigma_5 = \overline{\sigma_1}, \quad \sigma_6 = 2^{n_1} 3^{n_2} 4^{n_3} 5^{n_4} 6^{n_5} 7^{n_6}, \end{aligned} \quad (20)$$

где черта означает комплексное сопряжение. Здесь, как нетрудно видеть, $2\lambda_2 + 2\lambda_4 + 2 = 0$ и $2\lambda_3 + 2 = 0$. Если, например, $n_5 \neq 0$, т. е. в записи числа $(n)_7$ есть хотя бы одна пятёрка, то $\sigma_2 = 0$. Чтобы воспользоваться формулой (17), нужны матрицы S_k ($k = \overline{1, 6}$). В соответствии с (11) матрицы S_1 и S_2 имеют вид

$$S_1 = \frac{1}{6} \begin{pmatrix} 1 & \overline{\lambda_2} & \overline{\lambda_1} & \lambda_2 & \lambda_1 & -1 \\ \lambda_2 & 1 & \lambda_1 & \overline{\lambda_2} & -1 & \overline{\lambda_1} \\ \lambda_1 & \overline{\lambda_1} & 1 & -1 & \lambda_2 & \overline{\lambda_2} \\ \overline{\lambda_2} & \lambda_2 & -1 & 1 & \overline{\lambda_1} & \lambda_1 \\ \overline{\lambda_1} & -1 & \overline{\lambda_2} & \lambda_1 & 1 & \lambda_2 \\ -1 & \lambda_1 & \lambda_2 & \overline{\lambda_1} & \overline{\lambda_2} & 1 \end{pmatrix},$$

$$S_2 = \frac{1}{6} \begin{pmatrix} 1 & \lambda_2 & \overline{\lambda_2} & \overline{\lambda_2} & \lambda_2 & 1 \\ \overline{\lambda_2} & 1 & \lambda_2 & \lambda_2 & 1 & \overline{\lambda_2} \\ \lambda_2 & \overline{\lambda_2} & 1 & 1 & \overline{\lambda_2} & \lambda_2 \\ \lambda_2 & \overline{\lambda_2} & 1 & 1 & \overline{\lambda_2} & \lambda_2 \\ \overline{\lambda_2} & 1 & \lambda_2 & \lambda_2 & 1 & \overline{\lambda_2} \\ 1 & \lambda_2 & \overline{\lambda_2} & \overline{\lambda_2} & \lambda_2 & 1 \end{pmatrix}.$$

Далее, если обозначить k -ю строку матрицы S_3 через $(S_3)_k$, то

$$(S_3)_1 = (S_3)_2 = -(S_3)_3 = (S_3)_4 = -(S_3)_5 = -(S_3)_6 = \frac{1}{6}(1, 1, -1, 1, -1, -1).$$

Кроме того, из леммы 7 вытекает, что $S_4 = S_2^t$, $S_5 = S_1^t$, $S_6 = \frac{1}{6}(1)_{i,j=\overline{1,6}}$. Теперь из (17), учитывая (20), получаем

$$\begin{aligned} g_1^{(1)}(n, 7) &= 1/6 (2 \operatorname{Re}(\sigma_1 + \sigma_2) + \sigma_3 + \sigma_6), \\ g_2^{(1)}(n, 7) &= 1/6 (2 \operatorname{Re}(\lambda_4 \sigma_1 + \lambda_2 \sigma_2) + \sigma_3 + \sigma_6), \\ g_3^{(1)}(n, 7) &= 1/6 (2 \operatorname{Re}(\lambda_5 \sigma_1 + \lambda_4 \sigma_2) - \sigma_3 + \sigma_6), \\ g_4^{(1)}(n, 7) &= 1/6 (2 \operatorname{Re}(\lambda_2 \sigma_1 + \lambda_4 \sigma_2) + \sigma_3 + \sigma_6), \\ g_5^{(1)}(n, 7) &= 1/6 (2 \operatorname{Re}(\lambda_1 \sigma_1 + \lambda_2 \sigma_2) - \sigma_3 + \sigma_6), \\ g_6^{(1)}(n, 7) &= 1/6 (2 \operatorname{Re}(-\sigma_1 + \sigma_2) - \sigma_3 + \sigma_6). \end{aligned} \tag{21}$$

Полученные равенства справедливы, только если $n_3 = n_5 = 0$, поскольку $2\lambda_2 + 2\lambda_4 + 2 = 0$ и $2\lambda_3 + 2 = 0$. Если $n_3 \neq 0$ и $n_5 = 0$, то в (21) $\sigma_3 = 0$. Если $n_3 = 0$ и $n_5 \neq 0$, то в (21) надо считать, что $\sigma_2 = 0$. Наконец, если $n_3 \neq 0$ и $n_5 \neq 0$, то $\sigma_2 = \sigma_3 = 0$. Во всех других случаях, кроме указанных выше, надо пользоваться формулами (20).

4. Заключение

Отметим три простых свойства чисел $g_s^{(i)}(n, p)$. Рассмотрим две строки треугольника Паскаля с номерами $(n)_p$ и $(m)_p$. Если числа $(n)_p$ и $(m)_p$ содержат в своей записи одно и то же число цифр $1, 2, \dots, p-1$ (за исключением 0), то $g_s^{(i)}(n, p) = g_s^{(i)}(m, p)$ для всех s и i . Это верно, поскольку в (4) $B_0 = E$. Если в записи числа $(n)_p$ цифр 1 на l больше, чем в записи числа $(m)_p$, то $g_s^{(i)}(n, p) = 2^l g_s^{(i)}(m, p)$ для всех s и i . Это верно, поскольку в (4) $B_1 = 2E$ для любого p . Если число $(n)_p$ в своей записи содержит только цифры 0 и $p-1$, то строка треугольника Паскаля с номером $(n)_p$ не содержит чисел $2, \dots, p-2$, т. е. $g_s^{(1)}(n, p) = 0$ при $s = 2, \dots, p-2$. Это

так, поскольку в формуле (4) будет присутствовать только степень матрицы B_{p-1} , которая является суммой диагональной и косодиагональной матриц:

$$B_{p-1} = \frac{p+1}{2}E + \frac{p-1}{2}\tilde{E}. \quad (22)$$

Так как $\tilde{E}^2 = E$, степень матрицы B_{p-1} обладает такой же структурой, а значит, $(B_{p-1}^k)_{1,s} = 0$ при $s = 2, \dots, p-2$. Для доказательства (22) рассмотрим последнюю строку треугольника $\Delta_{p-1}^{(1)}$. Нетрудно получить равенство $(k+1)C_{p-1}^{k+1} = (p-k-1)C_{p-1}^k$, из которого следует, что

$$(k+1)(C_{p-1}^{k+1} + C_{p-1}^k) = 0 \pmod{p} \Rightarrow C_{p-1}^{k+1} + C_{p-1}^k = 0 \pmod{p}.$$

Поскольку $C_{p-1}^0 = 1$, имеем $C_{p-1}^1 = p-1$, значит, $C_{p-1}^2 = 1$, и т. д. В последней строке треугольника $\Delta_{p-1}^{(1)}$ чередуются числа 1 и $p-1$, причём единиц на одну больше. Тем самым в первой строке матрицы B_{p-1} будут все нули, кроме первого элемента, равного $\frac{p+1}{2}$, и последнего, равного $\frac{p-1}{2}$. В последней строке треугольника $\Delta_{p-1}^{(2)}$ будут только числа $2 \cdot 1 = 2$ и $2 \cdot (p-1) = p-2$, стало быть, во второй строке матрицы B_{p-1} все нули, кроме элемента на втором месте, равного $\frac{p+1}{2}$, и элемента на предпоследнем месте, равного $\frac{p-1}{2}$, и т. д. Формула (22) доказана.

ЛИТЕРАТУРА

1. **Карачик В. В.** Свойства нормализованных p -латинских матриц // Пробл. информатики и энергетики. — 1992. — № 5–6. — С. 9–14.
2. **Bondarenko B. A.** Generalized Pascal triangles and pyramids: their fractals, graphs and applications. — Santa Clara: The Fibonacci Association, 1993. — 253 p.
3. **Denes J., Keedwell A. D.** Latin squares and their applications. — Budapest: Akad. Kiado, 1974. — 547 p.
4. **Hexel E., Sachs H.** Counting residues modulo a prime in Pascal's triangle // Indian J. Math. — 1978. — Vol. 20, N 2. — P. 91–105.
5. **Karachik V. V., Bondarenko B. A.** Distribution of Eulerian and Stirling numbers mod m in arithmetical triangles // Вопросы вычисл. и прикл. математики. — 1996. — Вып. 102. — P. 133–140.
6. **Karachik V. V.** p -Latin matrices and Pascal's triangle modulo a prime // Fibonacci Quarterly. — 1996. — Vol. 34, N 4. — P. 362–372.

7. **Lucas E.** Théorie des fonctions numériques simplement périodiques // Amer. J. Math. — 1878. — Vol. 1, N 2. — P. 184–196.

Карачик Валерий Валентинович,
e-mail: karachik@susu.ru

Статья поступила
7 июня 2012 г.

Переработанный вариант —
10 октября 2012 г.