УДК 512.643.8+511.217

ТРЕУГОЛЬНИК ПАСКАЛЯ И p-ЛАТИНСКИЕ МАТРИЦЫ

В.В. Карачик[1]

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

Ключевые слова: треугольник Паскаля, латинские матрицы, биномиальные коэффициенты.

1. Введение

Одним из эффективных методов вычисления строк треугольника Паскаля по модулю простого числа p является сведение этой задачи к решению определенной системы линейных рекуррентных уравнений. Этот подход был успешно применен Б.А. Бондаренко [1] при исследовании распределения биномиальных коэффициентов $\bmod p$ для некоторых значений p и только для определенных строк треугольника Паскаля. Однако некоторые характерные свойства матриц полученных систем рекуррентных уравнений были отмечены и они привели к идее введения понятия p-латинской матрицы. Б.А. Бондаренко применял p-латинские матрицы и при исследовании других арифметических треугольников, отличных от треугольника Паскаля [2]. В данной статье 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 (13) получено распределение элементов треугольника Паскаля $\bmod p$ для произвольной строки (15). Подробно исследован случай $p=7$. Некоторые результаты по свойствам p-латинских матриц были получены автором в [3] и [4].

2. p- латинские матрицы

Приведем определение p-латинской матрицы, как оно дано в [1] и [5].

Определение 1. Квадратная матрица порядка n называется латинским квадратом порядка n [5], если ее элементы принимают значения $1,\ldots,n$ 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 $(1,2,\ldots,n)$ и главная диагональ записана в форме $(1,1,\ldots,1)$.

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

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

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

[1] Карачик Валерий Валентинович – доктор физико-математических наук, заведующий кафедрой дифференциальных уравнений и динамических систем, Южно-Уральский государственный университет.
E-mail: karachik@susu.ru

Теорема 1. Если p простое, то матрица P является нормализованным p-латинским квадратом 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 является латинским квадратом. 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 $js=is$ и значит $j=i$ и рассматриваемый элемент должен находиться на главной диагонали. Аналогичная ситуация обстоит и с побочной диагональю: $j/i=(j+s)/(i-s)\Rightarrow -j=i\Rightarrow j+i=p$ и значит элемент j/i лежит на побочной диагонали. В соответствии с определением 2 матрица P является p-латинским квадратом. Поскольку первая строка P имеет вид $(1,2,\ldots,n)$, главная диагональ записана в форме $(1,1,\ldots,1)$, то P – нормализованный p-латинский квадрат.

Определение 4. Матрицы вида

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

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

Пример 2. Пусть $p=7$. В соответствии с примером 1 следующая матрица принадлежит $\mathbb{N}_7$

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

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 верны равенства

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

где все операции над индексами производятся в $\mathbb{Z}_p$. Поэтому если обозначить $a_k=\sum_{s=1}^{p-1}c_s b_{k/s}$, тогда будем иметь $CB=\left(a_{j/i}\right)_{i,j=\overline{1,p-1}}$ и, следовательно, $CB\in\mathbb{N}_p$. Более того, аналогичные рассуждения дают

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

где использовалось равенство $a_k=\sum_{s=1}^{p-1}c_{k/s}b_s$. Следовательно, $CB=BC$. Лемма доказана.

Ниже мы докажем и 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 также 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 $C_k(n,m)=kC(n,m)(\mathrm{mod}\,p)$, и обозначим через $\Delta_s^{(k)}$ конечный треугольник, содержащий только первые s строк треугольника $\Delta^{(k)}$. Очевидно, что $\Delta_s^{(k)}=k\Delta_s^{(1)}$.

Определение 5. Конечный треугольник с sm 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

$$\Delta_4^{(1)} = \begin{array}{c} 1 \\ 1\ \ 1 \\ 1\ \ 2\ \ 1 \\ 1\ \ 3\ \ 3\ \ 1 \end{array}, \quad \Delta_3^{(1)} = \begin{array}{c} 1 \\ 1\ \ 1 \\ 1\ \ 2\ \ 1 \end{array}, \quad \Delta_3^{(2)} = \begin{array}{c} 2 \\ 2\ \ 2 \\ 2\ \ 4\ \ 2 \end{array}, \quad \Delta_3^{(3)} = \begin{array}{c} 3 \\ 3\ \ 3 \\ 3\ \ 1\ \ 3 \end{array}.$$

Поэтому мы получаем

$$\Delta_4^{(1)} * \Delta_3 = \Delta_4^{(1)} \equiv \begin{array}{c} \Delta_3^{(1)} \\ \Delta_3^{(1)}\ \ \Delta_3^{(1)} \\ \Delta_3^{(1)}\ \ \Delta_3^{(2)}\ \ \Delta_3^{(1)} \\ \Delta_3^{(1)}\ \ \Delta_3^{(3)}\ \ \Delta_3^{(3)}\ \ \Delta_3^{(1)} \end{array} = \begin{array}{c} 1 \\ 1\ \ 1 \\ 1\ \ 2\ \ 1 \\ 1\ \ 0\ \ 0\ \ 1 \\ 1\ \ 1\ \ 0\ \ 1\ \ 1 \\ 1\ \ 2\ \ 1\ \ 1\ \ 2\ \ 1 \\ 1\ \ 0\ \ 0\ \ 2\ \ 0\ \ 0\ \ 1 \\ 1\ \ 1\ \ 0\ \ 2\ \ 2\ \ 0\ \ 1\ \ 1 \\ 1\ \ 2\ \ 1\ \ 2\ \ 4\ \ 2\ \ 1\ \ 2\ \ 1 \\ 1\ \ 0\ \ 0\ \ 3\ \ 0\ \ 0\ \ 3\ \ 0\ \ 0\ \ 1 \\ 1\ \ 1\ \ 0\ \ 3\ \ 3\ \ 0\ \ 3\ \ 3\ \ 0\ \ 1\ \ 1 \\ 1\ \ 2\ \ 1\ \ 3\ \ 1\ \ 3\ \ 3\ \ 1\ \ 3\ \ 1\ \ 2\ \ 1 \end{array}$$

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 $\Delta_3^{(k)}$ на количество чисел равных k в треугольнике $\Delta_4^{(1)}$, т.е. на число 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 $C_{i+1}^{j+1} = C_i^j + C_i^{j+1} (\mathrm{mod}\, p)$, где j – номер элемента в строке (этот номер начинается с нуля и совпадает с номером луча, параллельного левой стороне треугольника и начинающегося с числа на правой стороне треугольника), $C_i^j = 0$ 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 $j=p^n$ и они равны k, так как $C_{p^n}^j = 0(\mathrm{mod}\, p)$ 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 внут-

ренних сторон станут соседними только в строке $i = 2p^n - 1$ и 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 $i = 2p^n$ будут 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, исходя из правила построения строк в $\Delta_{mp^n}^{(k)}$. Воспользуемся методом индукции. Пусть в строке с номером $i = sp^n$, $s = 2,\ldots,m$ 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 $r_1 + r_2 (\mathrm{mod}\, p)$, 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 $r_1 + r_2 (\mathrm{mod}\, p)$ «породит» треугольник $\Delta_{p^n}^{(r_1 + r_2 (\mathrm{mod}\, p))}$, т.е. из треугольников $\Delta_{p^n}^{(r_1)}$ и $\Delta_{p^n}^{(r_2)}$ возникает треугольник $\Delta_{p^n}^{(r_1 + r_2 (\mathrm{mod}\, p))}$

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

Кроме этого, 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 $t = 0,1,\ldots,s-1$. Итак, строка $i = sp^n$ порождает строку $i = (s+1)p^n$ в соответствии с правилом построения строк в треугольнике Паскаля. Если теперь в строке $i = sp^n$ отбросить элементы, стоящие на местах, номера которых не кратны p^n (они нулевые), то мы получим строку треугольника $\Delta_m^{(k)}$ с номером $i = s$. Поскольку s произвольно и при $s = 1,2$ утверждение теоремы справедливо, то оно справедливо и при любом s. Утверждаемое доказано.

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

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

Определение 6. Матрицей B_k при $0 \le k \le p-1$ назовем такую квадратную матрицу порядка $p-1$, элемент $b_{i,j}$ которой является числом элементов, равных j в k-й строке треугольника $\Delta_p^{(i)}$. Очевидно, что $B_0 = \mathrm{diag}(1,\ldots,1) \equiv E$.

Обозначим через $g_s^{(k)}(n,p)$ число элементов, равных s $(1 \le s \le p-1)$ по модулю p в n-й строке треугольника $\Delta^{(k)}$.

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

$$g_s^{(k)}(n,p)=\left(B_{a_r}\cdots B_{a_0}\right)_{k,s}. \tag{1}$$

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 $\Delta_{p^r}^{(k)}$, $k=\overline{1,p-1}$ (см. пример 3). Если ввести обозначение $n_{(k)}\equiv(a_{r-k},\ldots,a_0)_p$, 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, получаем равенство

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

Так как $n_{(r)}=a_0$ и $g_s^{(k)}(a_0,p)=\left(B_{a_0}\right)_{k,s}$, то мы получаем

$$\begin{pmatrix} g_s^{(1)}(n,p)\\ \vdots \\ g_s^{(p-1)}(n,p)\end{pmatrix}=B_{a_r}B_{a_r}\cdots B_{a_1}\left(B_{a_0}\right)_s=\left(B_{a_r}B_{a_r}\cdots B_{a_1}B_{a_0}\right)_s,$$

откуда сразу следует равенство (1). Здесь $\left(B_k\right)_s$ обозначает s-й столбец матрицы B_k.

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

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

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

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

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

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

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

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

для $s=\overline{1,p-1}$. Если обозначить элементы матрицы B_k через $b_{i,j}^{(k)}$, то, используя (3) и определение 6 матрицы B_k, можем записать $b_{1,j}^{(k)}=b_{s,js}^{(k)}$ 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 (2).

Пусть n_i обозначает число элементов, равных i в p-арном представлении числа $n=(a_r,\ldots,a_0)_p$. В силу (1) с помощью следствия 1 можем записать

$$g_s^{(k)}(n,p)=\left(\prod_{i=1}^{p-1}B_i^{n_i}\right)_{k,s}. \qquad (4)$$

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

3. Свойства матриц из $\mathbb{N}_p$

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

Лемма 2. $\dim\mathbb{N}_p=p-1$ и

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

где $I_k\in\mathbb{N}_p$ и $I_k=\left(\delta_{ki,j}\right)_{i,j=\overline{1,p-1}}$. Здесь $\delta_{i,j}$ – символ Кронеккера 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 $k=j/i\ (\mathrm{mod}\ p)\Rightarrow j=ki\ (\mathrm{mod}\ p)$. Поэтому

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

Нетрудно видеть, что $I_1=E$.

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

Доказательство. В самом деле,

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

и, следовательно, элемент матрицы I_kI_m с индексами i и j не равен нулю, если существует такое $s\in\mathbb{Z}_p$, что $ki=s\ (\mathrm{mod}\ p)$ и $ms=j\ (\mathrm{mod}\ p)$. Значит $j=kmi\ (\mathrm{mod}\ p)$ и поэтому $I_kI_m=\left(\delta_{kmi,j}\right)_{i,j=\overline{1,p-1}}=I_{km}$.

Определение 7. Пусть ν – корень уравнения $x^{p-1}=1$ в поле $\mathbb{Z}_p$ такой, что для каждого $k=\overline{1,p-2}$ верно неравенство $\nu^k\neq1$ (примитивный корень). Тогда обозначим $J_k=\left(I_\nu\right)^k$. Ясно, что $J_{p-1}=\left(I_\nu\right)^{p-1}=E$.

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

$$B=\sum_{k=1}^{p-1}c_kJ_k\ . \qquad (6)$$

Лемма 4. Пусть μ – собственное число матрицы $B \in \mathbb{N}_p$. Тогда существует λ – корень уравнения $z^{p-1}=1$ в $\mathbb{C}$ такой, что верно равенство

$$\mu = \sum_{k=1}^{p-1} c_k \lambda^k , \tag{7}$$

где коэффициенты c_k определяются из (6). Кроме того, числа вида (7) где λ – произвольный корень уравнения $z^{p-1}=1$ являются собственными числами матрицы B.

Доказательство. Пусть a – некоторый вектор из $\mathbb{C}^{p-1}$ и

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

Тогда верно равенство

$$J_s b = \sum_{k=1}^{p-1} \lambda^{-k} J_s J_k a = \sum_{k=1}^{p-1} \lambda^{-k} J_{s+k(\mathrm{mod}(p-1))} a = \lambda^s b$$

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 – собственный вектор матрицы B. Остается доказать, что формула (7) задает все собственные значения матрицы B. Мы завершим это доказательство после леммы 9.

Следствие. Матрицы J_k, а значит и матрицы I_k являются невырожденными матрицами и $\det I_k = \det J_k = 1$ для $k = \overline{1, p-1}$.

Доказательство. В силу леммы 4 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 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 $\mu = \lambda_1 \cdots \lambda_{p-1}$. Используя равенство $\sum_{k=1}^{p-1} k = 0 \,(\mathrm{mod}\, p)$ мы получаем $\mu = 1$ и значит $\det J_k = 1$ для $k = \overline{1, p-1}$. Это означает, что и $\det I_k = 1$.

Лемма 5. Матрицы I_k, а значит и матрицы J_k ортогональны и J_k обладают свойством $J_k J_m = J_{k+m}$, где сумма $k+m$ приведена по $\mathrm{mod}(p-1)$.

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

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

поскольку по лемме 3 $I_k I_{1/k} = I_1 = E$. Далее $J_k J_m = \left(I_\nu\right)^k \left(I_\nu\right)^m = \left(I_\nu\right)^{k+m} = J_{k+m(\mathrm{mod}(p-1))}$ и значит поскольку $J_{p-1} = E$, то $J_k J_m = E \Rightarrow k+m = p-1 \Rightarrow m = p-k-1$ и значит для $k = \overline{1, p-2}$

$$J_k^{-1} = J_k^* = J_{p-k-1} . \tag{8}$$

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

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

Доказательство. Используя (8) и равенство $J_{p-1}^* = E^* = E = J_{p-1}$, мы немедленно получаем

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

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

$$S_i = \frac{1}{p-1} \sum_{k=1}^{p-1} \lambda_i^{-k} J_k \ . \tag{9}$$

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 λ - примитивный корень уравнения $z^{p-1} = 1$ в $\mathbb{C}$, т.е. при $k = \overline{1, p-2}$ имеем $\lambda^k \neq 1$. Поэтому в формуле (9) можно считать, что $\lambda_i = \lambda^i$. Поскольку $\lambda_i^{-k} = \overline{\lambda}_k^i$, то (9) можно переписать в виде

$$S_i = \frac{1}{p-1} \sum_{k=1}^{p-1} \overline{\lambda}_i^k J_k = \frac{1}{p-1} \sum_{k=1}^{p-1} \overline{\lambda}_k^i J_k \ . \tag{9'}$$

Теорема 5. Следующие равенства

$$S_i S_j = \delta_{i,j} S_i \tag{10}$$

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

Доказательство. Рассмотрим левую часть (10). Если положить $J_0 = \left(I_\nu\right)^0 = E$, то $S_i = \frac{1}{p-1} \sum_{k=0}^{p-2} \lambda_i^{-k} J_k$ и с учетом $\lambda_i^{-k} \lambda_j^k = \lambda_{i-j}^{-k}$, после некоторых преобразований будем иметь

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

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

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

и значит, после объединения внутренних сумм будем иметь

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

Исследуем полученное равенство. Используя равенство $\lambda_{i-j} = \lambda_i / \lambda_j$, где $\lambda_i \neq \lambda_j$, т.е. $i \neq j$, получаем

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

Следовательно (10) верно при $i \neq j$. Далее, при $i = j$ имеем $\lambda_{i-j} = \lambda^0 = 1$ и значит

$$\sum_{k=0}^{p-2} \lambda_{i-j}^{-k} = \begin{cases} 0, & i \neq j \\ p-1, & i = j \end{cases}, \tag{11}$$

откуда получим $S_i^2 = S_i$. Доказательство завершено.

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

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

Доказательство. Действительно, для $i = \overline{1, p-1}$ с учетом того, что $\overline{\lambda}_i = \lambda_{p-i-1} = \lambda_i^{-1}$, и равенства (8) 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

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

Теорема 6. Для $k=\overline{1,p-1}$ справедливы равенства

$$J_k = \sum_{i=1}^{p-1}\lambda_i^k S_i, \tag{12}$$

обратные к (9).

Доказательство. Используя определение (9) матриц S_i, равенства (11) и делая некоторые преобразования, получим

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

Что и утверждалось.

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

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

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

Лемма 8. Пусть $B\in\mathbb{N}_p$, тогда верно равенство

$$B = \sum_{i=1}^{p-1}\mu_i S_i, \tag{13}$$

где μ_i – некоторые собственные числа матрицы B.

Доказательство. Действительно из формул (6) и (7) 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

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

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 $S_1,\ldots,S_{p-1}$ линейно независимы поскольку из равенства $\alpha_1 S_1+\ldots+\alpha_{p-1}S_{p-1}=0$ после умножения на S_i по теореме 5 вытекает, что $\alpha_i S_i = 0 \Rightarrow \alpha_i = 0$. Значит, по лемме 2 $S_1,\ldots S_{p-1}$ базис в $\mathbb{N}_p$. Используя этот базис, мы можем легко выписать произведение матриц из $\mathbb{N}_p$.

Теорема 7. Пусть $\mu_1^{(i)},\ldots,\mu_{p-1}^{(i)}$ – собственные числа матриц B_i из теоремы 3. Если положим

$$\sigma_j = \prod_{i=1}^{p-1}\left(\mu_j^{(i)}\right)^{n_i}, \tag{14}$$

то справедливы равенства

$$g_s^{(k)}(n,p)=\left(\sum_{i=1}^{p-1}\sigma_i S_i\right)_{k,s}. \qquad (15)$$

Доказательство. Нетрудно видеть, что, используя (13) и теорему 5, мы можем получить

$$B_i^2=\left(\mu_1^{(i)}S_1+\cdots+\mu_{p-1}^{(i)}S_{p-1}\right)^2=\left(\mu_1^{(i)}\right)^2 S_1+\cdots+\left(\mu_{p-1}^{(i)}\right)^2 S_{p-1}\Rightarrow B_i^{n_i}=\sum_{j=1}^{p-1}\left(\mu_j^{(i)}\right)^{n_i} S_j\ .$$

Поэтому, равенство (4) преобразуется в (15) и доказательство завершено.

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

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

$$b_i=\sum_{(j),\,\mu_j=\mu_i} S_j c_j\ , \qquad (16)$$

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

Доказательство. Пусть b_i – собственный вектор матрицы $B\in\mathbb{N}_p$, отвечающий собственному значению μ_i. Действуя матрицей S_s на равенство $Bb_i=\mu_i b_i$, используя (13) из леммы 8 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, используя равенство $E=S_1+\cdots+S_{p-1}$, которое следует из леммы 8, при $B=E$ ($\mu_i=1$) получаем представление (16): $b_i=Eb_i=(S_1+\cdots+S_{p-1})b_i=\sum_{(j)}S_j b_i$.

Далее рассмотрим некоторый вектор $c\in\mathbb{C}^{p-1}$. В силу представления (13) имеем $BS_i c=\mu_i S_i c$ и значит вектор $S_i c$ – 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.

Продолжение доказательства леммы 4. Возьмем $c\in\mathbb{C}^{p-1}$ такое, что $\forall k, S_k c\neq 0$. Это возможно, например, для $c=(1,0,\ldots,0)$. Выше мы видели, что вектор $c_k=S_k c$ – собственный вектор матрицы $B\in\mathbb{N}_p$, отвечающий собственному числу μ_k, определяемому из (7) при $\lambda=\lambda_k$. По выбору c он ненулевой. Докажем, что вектора $c_k\neq 0$ при $k=\overline{1,p-1}$ линейно независимы. Действительно, если числа $\delta_1,\ldots\delta_{p-1}\in\mathbb{C}$ не все равные нулю и такие, что $\delta_1 c_1+\cdots+\delta_{p-1}c_{p-1}=0$, то действуя на это равенство матрицей S_k, получаем $\delta_k c_k=0$ и значит $\delta_k=0$. Противоречие. Значит вектора $c_k\neq 0$ 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

$$c=\delta_1 c_1+\cdots+\delta_{p-1}c_{p-1}\Rightarrow \mu c=\delta_1\mu_1 c_1+\cdots+\delta_{p-1}\mu_{p-1}c_{p-1}\Rightarrow c=\delta_1\frac{\mu_1}{\mu}c_1+\cdots+\delta_{p-1}\frac{\mu_{p-1}}{\mu}c_{p-1}$$

и в силу единственности разложения c по базису при $\delta_k\neq 0$ имеем $\mu=\mu_k$. Наконец, если $\forall k,\mu_k\neq 0$, 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 10. Если $\mu_i\neq 0$ для $i=\overline{1,p-1}$ (см. (7)), то матрица $B\in\mathbb{N}_p$ имеет обратную, записываемую в виде

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

Доказательство. Согласно лемме 8, теореме 5 и равенству $E=S_1+\cdots+S_{p-1}$, имеем

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

Лемма доказана.

Теперь мы можем применить полученные свойства матриц из $\mathbb{N}_p$ к вычислению $g_s^{(k)}(n,p)$ для $p=7$. Следует отметить, что в [6] эта проблема была рассмотрена для $p=3$ и $p=5$. Прежде чем сделать это докажем еще одно интересное свойство биномиальных коэффициентов, вытекающее из теоремы 2.

Теорема 8. [Люка] Пусть $n \ge m \ge 0$ целые. Если $n=(a_r,\ldots,a_0)_p$ и $m=(b_r,\ldots,b_0)_p$ являются p-арным представлением чисел n и m, то верно равенство

$$C_n^m = C_{a_r}^{b_r} \cdots C_{a_0}^{b_0} (\mathrm{mod}\, p),$$

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 в n-й строке, на m-м месте треугольника $\Delta_{p^{r+1}}^{(1)}$, обозначим его (n,m), должен быть в треугольнике вида $C_{a_r}^{b_r}(\mathrm{mod}\, p)\cdot\Delta_{p^r}^{(1)}$ и находиться там в строке с номером $n_{(1)}=(a_{r-1},\ldots,a_0)_p$ на месте с номером $m_{(1)}=(b_{r-1},\ldots,b_0)_p$. Если окажется, что $a_{r-1} < b_{r-1}$, то элемент (n,m) попадет в пространство между соседними треугольниками вида $\Delta_{p^r}^{(k)}$, составляющими $\Delta_p^{(1)}$, которое заполнено нулями. Таким образом получим, $(n,m) \in C_{a_r}^{b_r} \cdots C_{a_{r-k+1}}^{b_{r-k+1}} (\mathrm{mod}\, p)\cdot\Delta_{p^{r-k+1}}^{(1)}$ и находится там в $n_{(k)}$-й строке на $m_{(k)}$-м месте, где $n_{(k)} \equiv (a_{r-k},\ldots,a_0)_p$ (это будет при $a_{r-i} \ge b_{r-i}$), либо (n,m) попадет в пространство, заполненное нулями, и значит $C_n^m = 0 (\mathrm{mod}\, p)$. Отсюда при $k=r$ с учетом того, что элемент треугольника $\Delta_p^{(1)}$ в a_0-й строке на b_0-м месте равен $C_{a_0}^{b_0}(\mathrm{mod}\, p)$, получим доказываемую формулу.

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

4. Вычисление $g_s^{(k)}(n,7)$

Чтобы вычислить $g_s^{(k)}(n,7)$, в соответствии с теоремой 7, необходимо исследовать треугольники $\Delta_7^{(k)}$ для $k=\overline{1,6}$. Треугольник $\Delta_7^{(1)}$ имеет вид

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

Если мы умножим каждый элемент треугольника $\Delta_7^{(1)}$ на k в $\mathbb{Z}_7$, то мы получим $\Delta_7^{(k)}$. Например треугольник $\Delta_7^{(3)}$ имеет вид

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

Теперь нам необходимо найти матрицы B_k для $k=\overline{0,6}$. Возьмем, например, 4-ю строку треугольников $\Delta_7^{(k)}$, которая дает нам матрицу B_4 (нумерация начинается с нуля). 4-я 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, то 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 дает нам желаемый результат $(0,0,2,1,2,0)$. Таким образом, мы можем подсчитать все матрицы B_k при $k=\overline{0,6}$. Чтобы записать наши вычисления воспользуемся матрицами J_k, $k=\overline{1,6}$. Найдем матрицу J_1. В нашем случае $\nu=3$ потому, что для всякого $k=\overline{1,5}$ верно неравенство $3^k\neq 1(\mathrm{mod}\,7)$ (см. определение 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 мы можем записать:

$$
\begin{gathered}
B_0=J_6,\quad B_1=2J_6,\quad B_2=J_2+2J_6,\quad B_3=2J_1+2J_6, \\
B_4=J_3+2J_4+2J_6,\quad B_5=2J_1+2J_5+2J_6,\quad B_6=3J_3+4J_6
\end{gathered}. \tag{17}
$$

Используя обозначения теоремы 7, формулы (7) и (17), для каждого $k=\overline{1,6}$ найдем:

$$
\begin{gathered}
\mu_k^{(1)}=2,\quad \mu_k^{(2)}=\lambda_k^2+2,\quad \mu_k^{(3)}=2\lambda_k+2,\quad \mu_k^{(4)}=\lambda_k^3+2\lambda_k^4+2, \\
\mu_k^{(5)}=2\left(\lambda_k+\lambda_k^5+1\right),\qquad \mu_k^{(6)}=3\lambda_k^3+4.
\end{gathered}
$$

Предположим, что число $k=\overline{1,6}$ содержится в записи числа $(n)_7$ всего n_k раз. Тогда, согласно (14) имеем $\sigma_k=\left(\mu_k^{(1)}\right)^{n_1}\cdots\left(\mu_k^{(6)}\right)^{n_6}$ и значит, учитывая что $\lambda_k=\exp(ik\pi/3)$ (здесь $i^2=-1$), будем иметь (σ_1 вычислено подробно):

$$
\begin{gathered}
\sigma_1=2^{n_1}\left(2-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^{n_2}\left(2+1+i\sqrt{3}\right)^{n_3}\left(2-1-1-i\sqrt{3}\right)^{n_4}\left(1+i\sqrt{3}+1-i\sqrt{3}+2\right)^{n_5}\times \\
\left(-3+4\right)^{n_6}=2^{n_1-n_2}\left(3+i\sqrt{3}\right)^{n_2+n_3}\left(-i\sqrt{3}\right)^{n_4}4^{n_5}, \\
\sigma_2=2^{n_1-n_2}\left(3-i\sqrt{3}\right)^{n_2}\left(1+i\sqrt{3}\right)^{n_3}\left(2+i\sqrt{3}\right)^{n_4}\left(2\lambda_2+2\lambda_4+2\right)^{n_5}7^{n_6}, \\
\sigma_3=(-1)^{n_5}2^{n_1+n_5}3^{n_2+n_4}\left(2\lambda_3+2\right)^{n_3},\quad \sigma_4=\overline{\sigma_2},\quad \sigma_5=\overline{\sigma_1},\quad \sigma_6=2^{n_1}3^{n_2}4^{n_3}5^{n_4}6^{n_5}7^{n_6},
\end{gathered} \tag{18}
$$

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 пятерка, то $\sigma_2=0$.

Чтобы воспользоваться формулой (15) из теоремы 7 нам нужны матрицы S_k ($k=\overline{1,6}$). В соответствии с (9') матрицы S_1 и S_2 имеют вид:

$$S_1=\frac{1}{6}\begin{pmatrix} 1 & \overline{\lambda_2} & \overline{\lambda_1} & \lambda_2 & \lambda_1 & -1 \\ \lambda_2 & 1 & \lambda_1 & \overline{\lambda_2} & -1 & \overline{\lambda_1} \\ \lambda_1 & \overline{\lambda_1} & 1 & -1 & \lambda_2 & \overline{\lambda_2} \\ \overline{\lambda_2} & \lambda_2 & -1 & 1 & \overline{\lambda_1} & \lambda_1 \\ \overline{\lambda_1} & -1 & \overline{\lambda_2} & \lambda_1 & 1 & \lambda_2 \\ -1 & \lambda_1 & \lambda_2 & \overline{\lambda_1} & \overline{\lambda_2} & 1 \end{pmatrix},\quad S_2=\frac{1}{6}\begin{pmatrix} 1 & \lambda_2 & \overline{\lambda_2} & \overline{\lambda_2} & \lambda_2 & 1 \\ \overline{\lambda_2} & 1 & \lambda_2 & \lambda_2 & 1 & \overline{\lambda_2} \\ \lambda_2 & \overline{\lambda_2} & 1 & 1 & \overline{\lambda_2} & \lambda_2 \\ \lambda_2 & \overline{\lambda_2} & 1 & 1 & \overline{\lambda_2} & \lambda_2 \\ \overline{\lambda_2} & 1 & \lambda_2 & \lambda_2 & 1 & \overline{\lambda_2} \\ 1 & \lambda_2 & \overline{\lambda_2} & \overline{\lambda_2} & \lambda_2 & 1 \end{pmatrix}.$$

Далее, если обозначить k -ю строку матрицы S_3 через $(S_3)_k$, тогда будем иметь

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

Кроме этого из леммы 7 вытекает, что $S_4=S_2^t$, $S_5=S_1^t$, $S_6=1/6(1)_{i,j=\overline{1,6}}$. Теперь из (15), учитывая (18), легко получаем:

$$\begin{aligned} g_1^{(1)}(n,7)&=1/6\big(2\,\mathrm{Re}(\sigma_1+\sigma_2)+\sigma_3+\sigma_6\big),\\ g_2^{(1)}(n,7)&=1/6\big(2\,\mathrm{Re}(\lambda_4\sigma_1+\lambda_2\sigma_2)+\sigma_3+\sigma_6\big),\\ g_3^{(1)}(n,7)&=1/6\big(2\,\mathrm{Re}(\lambda_5\sigma_1+\lambda_4\sigma_2)-\sigma_3+\sigma_6\big),\\ g_4^{(1)}(n,7)&=1/6\big(2\,\mathrm{Re}(\lambda_2\sigma_1+\lambda_4\sigma_2)+\sigma_3+\sigma_6\big),\\ g_5^{(1)}(n,7)&=1/6\big(2\,\mathrm{Re}(\lambda_1\sigma_1+\lambda_2\sigma_2)-\sigma_3+\sigma_6\big),\\ g_6^{(1)}(n,7)&=1/6\big(2\,\mathrm{Re}(-\sigma_1+\sigma_2)-\sigma_3+\sigma_6\big), \end{aligned} \tag{19}$$

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 (19) надо считать $\sigma_3=0$. Если $n_3=0$ и $n_5\neq 0$, то в (19) 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 (18).

5. Заключение

Отметим три простых свойства чисел $g_s^{(k)}(n,p)$. Рассмотрим две строки треугольника Паскаля с номерами $(n)_p$ и $(m)_p$. Первое, если числа $(n)_p$ и $(m)_p$ содержат в их записи одно и то же число цифр $1,2,\ldots,p-1$ исключая 0, то $g_s^{(k)}(n,p)=g_s^{(k)}(m,p)$ для всех s и k. Это так, поскольку в (4) $B_0=E$. Второе, если число $(n)_p$ содержит цифру 1 на l штук больше, чем число $(m)_p$, то $g_s^{(k)}(n,p)=2^l g_s^{(k)}(m,p)$ для всех s и k. Это так, поскольку в (4) $B_1=2E$ для любого p. Третье, 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 $2,\ldots,p-2$, т.е. $g_s^{(1)}(n,p)=0$ при $s=2,\ldots,p-2$. Это так, поскольку в формуле (4) будет присутствовать только степень матрицы B_{p-1}, которая является суммой диагональной матрицы и кососиагональной матрицы:

$$B_{p-1}=\frac{p+1}{2}E+\frac{p-1}{2}\widetilde{E}. \tag{20}$$

Поскольку $\widetilde{E}^2=E$, то степень матрицы B_{p-1} обладает такой же структурой, а значит $\left(B_{p-1}^k\right)_{1,s}=0$ при $s=2,\ldots,p-2$. Для доказательства (20) 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 $(k+1)\left(C_{p-1}^{k+1}+C_{p-1}^{k}\right)=0(\mathrm{mod}\,p)\Rightarrow C_{p-1}^{k+1}+C_{p-1}^{k}=0(\mathrm{mod}\,p)$. Так как $C_{p-1}^{0}=1$, то $C_{p-1}^{1}=p-1$ и значит $C_{p-1}^{2}=1$ и т.д. В последней строке треугольника $\Delta_{p-1}^{(1)}$ идет чередование чисел 1 и $p-1$, причем единиц на одну больше. В последней строке треугольника $\Delta_{p-1}^{(2)}$ будут только числа $2\cdot 1=2$ и $2\cdot(p-1)=p-2$ и значит на втором месте во второй строке B_{p-1} будет $\frac{p+1}{2}$, а в предпоследней строке $\frac{p-1}{2}$ и т.д. Формула (20) доказана.

Литература

1. Bondarenko, B.A. Generalized Pascal Triangles and Pyramids: Their Fractals, Graphs and Applications / B.A. Bondarenko; пер. с рус.; под ред. R.C. Bollinger. – Santa Clara, Calif: The Fibonacci Association, 1993.

2. Karachik, V.V. Distribution of Eulerian and Stirling numbers mod m in arithmetical triangles / V.V. Karachik, B.A. Bondarenko // Вопросы вычислительной и прикладной математики. – 1996. – Issue 102. – P. 133–140.

3. Karachik, V.V. P-latin matrices and Pascal's triangle modulo a prime / V.V. Karachik // The Fibonacci Quarterly. – 1996. – Vol. 34, № 4. – P. 362–372.

4. Карачик, В.В. Свойства нормализованных p-латинских матриц / В.В. Карачик // Узбекский журнал «Проблемы информатики и энергетики». – 1992. – № 5–6. – С. 9–14.

5. Denes, J. Latin Squares and Their Applications / J. Denes, A.D. Keedwell. – Budapest: Akad. Kiado, 1974. – 547 p.

6. Hexel, E. Counting Residues Modulo a Prime in Pascal's Triangle / E. Hexel, H. Sachs // Indian J. Math. – 1978. – Vol. 20, № 2. – P. 91–105.

Поступила в редакцию 17 апреля 2012 г.

PASCAL'S TRIANGLE AND p-LATIN MATRICES

***V.V. Karachik*[1]**

Properties of a special class of matrices arising in the analysis of binominal coefficients distribution in terms of a prime number modulus are considered. Formulae of elements distribution in the row of Pascal's triangle in terms of a prime number modulus are obtained.

Keywords: Pascal's triangle, latin matrices, binominal coefficient.

References

1. Bondarenko B.A. *Generalized Pascal Triangles and Pyramids: Their Fractals, Graphs and Applications*. Santa Clara, Calif: The Fibonacci Association, 1993.

2. Karachik V.V., Bondarenko B.A. Distribution of Eulerian and Stirling numbers mod m in arithmetical triangles. *Vopposy vychislitel'noi i ppikladnoi matematiki*. 1996. Issue 102. pp. 133–140. (in Russ.).

3. Karachik V.V. P-latin matrices and Pascal's triangle modulo a prime. *The Fibonacci Quarterly*. 1996. Vol. 34, no. 4. pp. 362–372.

4. Karachik V.V. Svoistva nopmalizovannykh p-latinskikh matpits (Properties of Standardized p-Latin Matrices). *Uzbekskii zhurnal «Problemy informatiki i energetiki»*. 1992. no. 5–6. pp. 9–14. (in Russ.).

5. Denes J., Keedwell A.D. *Latin Squares and Their Applications*. Budapest: Akad. Kiado, 1974. 547 p.

6. Hexel E., Sachs H. Counting Residues Modulo a Prime in Pascal's Triangle. *Indian J. Math.* 1978. Vol. 20, no. 2. pp. 91–105.

[1] Karachik Valeriy Valentinovich is Dr. Sc. (Physics and Mathematics), Head of Differential equations and Dynamical Systems Department, South Ural State University.
E-mail: karachik@susu.ru