От «переводчика»

Предлагаемый перевод знаменитой работы по дьявольским квадратам осуществлен человеком, который, мягко говоря, плохо знает английский язык. Поэтому я буду благодарен за замечания по тексту. Направляйте эти замечания на мой адрес: svb@ninodom.ru , можете также заглянуть на мою страничку http://svb.hut.ru/mag.htm , которая посвящена магическим квадратам. Материала там пока мало (май 2010), но, возможно, со временем станет больше.

Несколько слов о второй возможной проблеме. В тексте очень много формул с индексами, поэтому вполне возможны ошибки. Надеюсь, что с помощью читателей их удастся исправить.

24.05.2010.
Беляев С.В.

20.10.2010 Исправлено выражение в доказательстве теоремы 2.5

АЛГЕБРАИЧЕСКАЯ ТЕОРИЯ ДЬЯВОЛЬСКИХ МАГИЧЕСКИХ КВАДРАТОВ

Barkley Rosser, R.J. Walker

1. Введение. Много столетий магические квадраты привлекали внимание людей, интересующихся математикой. Однако общая теория магических квадратов не была разработана, отчасти потому, что такая теория предназначена для решения частных задач неожиданно сложного характера. Если предположить, что элементами квадрата должны быть первые n^2 положительных целых чисел, то изучение магических квадратов становится обычной алгебраической задачей решения линейных уравнений с n^2 переменными. Для дьявольских магических квадратов, в которых все диагонали имеют одинаковую сумму, совокупность алгебраических условий намного больше, чем для обычных магических квадратов, в которых только две главных диагонали имеют эту сумму, и результирующая теория более интересна. Поэтому мы ограничили наше внимание дьявольскими квадратами и их обобщениям.

В первой части статьи рассматривается общая алгебраическая теория дьявольских квадратов. Построена группа преобразований дьявольских квадратов порядка n; для простых $n \geq 7$ показано, что это самая большая группа, переводящая общий дьявольский квадрат в дьявольский квадрат. Последний результат доказан в предположении простоты порядка квадрата, это общее решение $4n$ линейных уравнений, которым элементы квадрата должны удовлетворять.

В последней части статьи изложены приложения этих результатов к квадратам из целых чисел $1,...,n^2$. Показано, что имеется точно 28,800 дьявольских квадратов порядка 5, имеющих простую конструкцию и которые мы назвали регулярными. Существование или не существование регулярных и нерегулярных дьявольских квадратов демонстрируется для квадратов всех порядков.

2. Некоторые определения. Квадратом S_n порядка n мы будем обозначать квадратную матрицу порядка n, элементы которой принадлежат любому полю K с характеристикой взаимно простой с n. Элементы S_n будем обозначать A_{ij} или $A(i,j)$, где i обозначает строку, а j столбец, и всякий раз, когда i или j оказываются не в диапазоне от 1 до n, мы подразумеваем, что они должны быть взяты по модулю n. Квадрат с элементами A_{ij}, будем обозначать A.

Конфигурация в S_n это любая линейная комбинация элементов

$$\sum_{x=1}^{r} \alpha_x A(i_x, j_x),$$

где α_x являются элементами K. Говорим, что S_n допускает конфигурацию, если

$$\sum_{x=1}^{r} \alpha_x A(i+i_x, j+j_x) = N \sum \alpha_x$$

N не зависит от i и j для всех i и j. Суммируя это уравнение по i и j, мы получим

$$N = \frac{1}{n^2} \sum_{i,j=1}^{n} A_{ij}$$

для $\sum \alpha_x \neq 0$. Если $\sum \alpha_x = 0$, то N не определено и ему можно дать вышеупомянутое значение. Если S_n допускает некоторый набор конфигураций, то можно получить квадрат с элементами

$$A'_{ij} = A_{ij} - \frac{1}{n^2}\sum_{i,j=1}^{n} A_{ij}$$

и для этого квадрата $N = 0$. Поэтому, когда мы имеем дело с квадратом, для которого имеется некоторый набор допустимых конфигураций, то без ограничения общности можно считать $N = 0$.

Конфигурации, которые нас будут интересовать – это суммы n элементов

$$\sum_{x=1}^{n} A(i + ax, j + bx),$$

где $(a,b,n) = 1$. (Мы используем стандартную запись $(x,y,...,z)$ для наибольшего общего делителя $x,y,...,z$). Будем их обозначать $P(i,j;a,b)$ и называть путями. Нас не часто будут интересовать частные пути $P(i,j;a,b)$, а прежде всего весь набор из n путей с заданными a,b. В этом случае мы будем говорить "путь $P(a,b)$", обозначая таким образом любой из этого набора путей.

Если $(c,n) = 1$, то пути $P(i,j;a,b)$ и $P(i,j;ca,cb)$ содержат одни и те же элементы, поэтому $P(ca,cb) = P(a,b)$.

Наиболее важные пути – $P(0,1)$, $P(1,0)$, $P(1,1)$ и $P(1,-1)$. Они являются соответственно строками, столбцами, и двумя наборами диагоналей S_n. Если S_n допускает эти четыре пути, то говорят, что это дьявольский квадрат (d.s.).

Интересный набор конфигураций

$$A_{ij} + A_{kl} - A_{il} - A_{kj}.$$

Квадрат, который допускает все эти конфигурации, будем называть примитивным квадратом (p.s.).

Если d – делитель n, то конфигурация

$$\sum_{x,y=1}^{n/d} A(i + dx, j + dy)$$

называется решеткой порядка n/d, и обозначается $L(i,j;d)$. В частности, когда i и j не имеют значения, решетка обозначается $L(d)$. Мы также используем слово "решетка" и символ $L(i,j;d)$ для ссылки на квадрат порядка n/d с элементами $B(x,y) = A(i + dx, j + dy)$.

Теорема 2.1. *p.s. порядка n допускает все пути $P(a,b)$, если $(ab,n) = 1$.*

Это легко следует из определения p.s.

Теорема 2.2. *Каждая решетка в p.s. является p.s.*

Доказательство.

$A(i + dx, j + dy) + A(i + ds, j + dt) - A(i + dx, j + dt) - A(i + ds, j + dy) = 0$.

Теорема 2.3. *Пусть в квадрате порядка mn допустимы пути*

$$P(a_i, b_i) \qquad (i = 1, 2, ..., s).$$

Если для квадрата порядка n допустимы те же самые пути, то из требования допустимости для него конфигурации

$$\sum_{x=1}^{t} \alpha_x A(i_x, j_x)$$

следует, что квадрат порядка mn допускает конфигурацию

$$\sum_{x=1}^{t} \alpha_x L(i_x, j_x; n).$$

Доказательство. Пусть квадрат A порядка mn допускает пути

$$P(a_i, b_i) \qquad (i = 1, 2, ..., s).$$

Предположим, что $N = 0$. Определим квадрат B, порядка n,

$$B(i, j) = L(i, j; n).$$

Для доказательства нашей теоремы, очевидно, достаточно доказать, что B допускает пути $P(a_i, b_i)$. Пусть $P_i(u, v)$ обозначает путь $P(u, v; a_i, b_i)$ взятый из B

$$P_i(u, v) = \sum_{z=1}^{n} \sum_{x,y=1}^{m} A(u + a_i z + nx, v + b_i z + ny).$$

$P(a_i, b_i)$ это путь в A, $(a_i, b_i, mn) = 1$. Выберем α_i и β_i так, чтобы $a_i\beta_i - \alpha_i b_i = 1 \pmod{mn}$. Пусть $Q_i(u, v)$ обозначает

$$\sum_{k=1}^{m} P(u + k\alpha_i n, v + k\beta_i n; a_i, b_i)$$

взятый из A. Легко показать, что имеется точно $m^2 n$ элементов в $Q_i(u, v)$, и что каждый элемент $Q_i(u, v)$ является элементом $P_i(u, v)$. Имеется всего $m^2 n$ элементов $P_i(u, v)$, т.е. $P_i(u, v)$ и $Q_i(u, v)$ будут одинаковыми и $P_i(u, v) = 0$.

Теорема 2.4. *d.s. четного порядка допускает* $L(2)$.

Доказательство. В d.s. порядка 2 при $N = 0$

$$2A_{11} = P(1,1;1,1) + P(1,1;0,1) - P(1,2;1,0) = 0.$$

Или d.s. порядка 2 допускает A_{ij}. Тогда, согласно теореме 2.3, d.s. порядка $2m$ допускает $L(i, j; 2)$.

Теорема 2.5. *d.s. порядка* $3m$ *допускает* $L(3)$.

Доказательство. В d.s. порядка 3 при $N = 0$

$$3A_{11} = P(1,1;1,1) + P(1,1;1,-1) + P(1,1;0,1) - P(1,2;1,0) - P(1,3;1,0) = 0.$$

Т.е. d.s. порядка 3 допускает A_{ij}. Теорема следует из теоремы 2.3.

Теорема 2.6. *d.s. порядка* $4m$ *допускает* $L(i,j;4)+L(i+2,j+2;4)$.

Доказательство. d.s. порядка 4 допускает $A(i,j)+A(i+2,j+2)$.[1] Теорема следует из теоремы 2.3.

Теорема 2.7. *Допустим, что для данного* d*, каждая решетка* $L(i,j;d)$ *квадрата* A *является дьявольским квадратом и значениями путей в* $L(i,j;d)$ *являются* N_{ij}*. Тогда, если квадрат порядка* d *с элементами* N_{ij} *в* i*-ой строке и* j*-ом столбце дьявольский, то* A *дьявольский.*

Доказательство. Рассмотрим, например, $P(1,-1)$.

$$\begin{aligned} P(i,j;1,-1) &= \sum_{x=1}^{n} A(i+x, j-x) \\ &= \sum_{y=1}^{d}\sum_{z=1}^{n/d} A(i+y+dz, j-y-dz) \\ &= \sum_{y=1}^{d} N_{i+y,j-y} \end{aligned}$$

Следовательно $P(i,j;1,-1)$ независим от i и j.

3. Преобразования. Пусть

$$T = \begin{Vmatrix} a & c \\ b & d \end{Vmatrix}$$

матрица целых чисел с $|T|$ взаимно простым с n. Определим преобразование квадрата A с помощью $T: A \to B$, где $B(ai+cj, bi+dj) = A(i,j)$. Ясно, что это преобразование каждого вектора (i,j) в вектор $(ai+cj, bi+dj)$ с помощью T имеет обычные свойства линейного преобразования векторов, задаваемого матрицами, в частности

(a) результат преобразования сначала T и затем S дает тот же самый результат, что и преобразование с помощью результата матричного произведения ST;

(b) т.к. $|T|$ взаимно просто с n, то можно найти такое e, что $e(ad - bc) = 1 \pmod{n}$ и

$$T^{-1} = \begin{Vmatrix} de & -ce \\ -be & ae \end{Vmatrix};$$

(c) $B(ai+cj+(ae+cf)x,\ bi+dj+(be+df)x) = A(i+ex, j+fx)$, т.е. T преобразует путь $P(e,f)$ в путь $P(ae+cf, be+df)$;

(d) $B(ai+cj+(ax+cy)f, bi+dj+(bx+dy)f) = A(i+fx, j+fy)$, т.е. T преобразует решетку $L(f)$ в решетку $L(f)$.

[1] Barkley Rosser and R. J. Walker, On the transformation group for diabolic magic squares of order four, Bull. Am. Math. Sot., vol. 44(1938), pp. 416-420. See Theorem 2.

Теорема 3.1. *Результат преобразование p.s. порядка* n *с помощью*

$$T = \begin{Vmatrix} a & c \\ b & d \end{Vmatrix}$$

будет дьявольским квадратом, если $abcd\left(a^2-b^2\right)\left(c^2-d^2\right)$ *взаимно просто с* n.

Доказательство. Пути, которые преобразуются в $P(0,1)$, $P(1,0)$, $P(1,1)$, $P(1,-1)$ получаются с помощью преобразования T^{-1}. Удалив коэффициент e с помощью $(e,n)=1$, мы увидим, что они равны $P(-c,a)$, $P(d,-b)$, $P(-c+d,a-b)$, $P(c+d,-a-b)$. Теорема следует из теоремы 2.1.

Преобразование, удовлетворяющее условиям теоремы 3.1, называется *регулярным.*

Из определения p.s. следует, что он остается примитивным при любой перестановке строк и столбцов. Два p.s. получаемые друг из друга такой перестановкой считаются одного типа. Следовательно имеется $(n!)^2$ квадратов p.s. порядка n любого заданного типа, если все элементы квадрата различны.

Мы желаем определить число d.s. получаемых регулярными преобразованиями из p.s. данного типа, чьи элементы все различны. Сначала заметим, что два различных p.s. одинакового типа могут давать тот же самый d.s. под воздействием двух различных регулярных преобразований. Если A p.s., T – регулярное преобразование и

$$S = \begin{Vmatrix} \alpha & 0 \\ 0 & \beta \end{Vmatrix} \qquad ((\alpha\beta, n) = 1),$$

тогда SA примитивный и того же самого типа, что и A; TS регулярно и $(TS)A = T(SA)$. Наоборот, если A и B – p.s. одного типа и $T_1A = T_2B$, т.е. $A = T_1^{-1}T_2B$, следовательно $T_1^{-1}T_2$ преобразует строки в строки и столбцы в столбцы. Но единственные матрицы, которые так делают это вида S. Следовательно $T_1^{-1}T_2 = S$ или $T_2 = T_1S$. Теперь, если T регулярно, то можно найти β, δ такие, что $b\beta = d\delta = 1 \pmod{n}$, и следовательно

$$T' = T\begin{Vmatrix} \beta & 0 \\ 0 & \delta \end{Vmatrix} = \begin{Vmatrix} a\beta & c\delta \\ 1 & 1 \end{Vmatrix}$$

Регулярное преобразование, для которого $b = d = 1 \pmod{n}$ будем называть нормальным. Очевидно, что никакие два нормальных преобразования не могут быть связаны соотношением $T_1 = T_2S$, если S не матрица тождества, число d.s. которые получаются регулярными преобразованиями p.s. данного типа с различными элементами равно $(n!)^2\,\theta(n)$, где $\theta(n)$ - число нормальных преобразований порядка n. Мы желаем определить функцию $\theta(n)$.

Следующая лемма легко доказывается.

Лемма 3.1. *Пусть* $F(x_1,...,x_r)$ *любая целочисленная функция от целых чисел такая, что для всех* n

$$F(x_1,...,x_r) = F(y_1,...,y_r) \pmod{n},$$

если $x_i = y_i \pmod{n}$. *Если* $\theta(n)$ *обозначает число наборов* $(a_1,...,a_r)$ $(0 \le a_i \le n-1)$ *таких, что* $F(a_1,...,a_r)$ *взаимно просты с* n, *тогда*

(a) $\theta(mn) = \theta(m)\theta(n)$, *если* $(m,n) = 1$;

(b) $\theta(p^s) = p^{r(s-1)}\theta(n)$, *если* p *простое.*

Теорема 3.2. *Имеется* $(n!)^2\,\theta(n)$ *d.s., которые получаются после регулярных преобразований p.s. данного типа, элементы которого различны, где*

(a) $\theta(mn) = \theta(m)\theta(n)$, *если* $(m,n) = 1$;

(b) $\theta(p^s) = p^{2s-2}(p-3)(p-4)$, *если* p *нечетное простое;*

(c) $\theta(2^s) = 0$.

Доказательство. Используя определение регулярного преобразования и то, что детерминант преобразования должен быть взаимно прост с n, мы получаем, что матрица

$$\begin{Vmatrix} a & c \\ 1 & 1 \end{Vmatrix}$$

задает регулярное преобразование тогда и только тогда, когда

$$F(a,c) = ac(a^2-1)(c^2-1)(a-c)$$

взаимно просто с n. Любой полином с целочисленными коэффициентами удовлетворяет условию леммы 3.1, мы должны только определить значение $\theta(p)$ для функции $F(a,c)$. Аргумент a может иметь любое из значений $2,3,...,p-2$, c может иметь любое из этих значений за исключением значения a. Следовательно $\theta(2) = 0$ и $\theta(p) = (p-3)(p-4)$ при $p > 2$ и теорема доказана.

Известно что любой d.s. преобразуется в d.s. при повороте на 90°, при отражении относительно диагонали и при циклических перестановках строк и столбцов. Следующая теорема дает более полное представление о ситуации.

Теорема 3.3. *Перестановки элементов квадрата порядка* $n \ge 4$ *которые переводят строки, столбцы, и два набора диагоналей* (r,c,d,d') *в* r,c,d,d', *не обязательно в том же самом порядке, формируют группу* G, *которая генерируется перестановками*

$$L = \begin{cases} i' = i-1 \\ j' = j \end{cases},\ M = \begin{cases} i' = i \\ j' = j-1 \end{cases},\ S_\alpha = \begin{Vmatrix} \alpha & 0 \\ 0 & \alpha \end{Vmatrix} \quad ((\alpha,n) = 1),$$

$$O = \begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix},\quad P = \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix},\quad Q = \begin{Vmatrix} 1 & 1 \\ 1 & -1 \end{Vmatrix}$$

если n *нечетно, и* L, M, S_α, O, P *при четном* n.

Доказательство. Каждая из этих перестановок, как легко видеть, преобразует r,c,d,d' в r,c,d,d'. Мы должны показать, что и обратно, если перестановка T имеет это свойство, то она принадлежит G.

Прежде всего, если T преобразует одну строку в строку, то и другие строки преобразуются аналогично; если две строки имеют различные наборы элементов, то они не могут быть преобразованы друг в друга. То же самое справедливо для столбцов и диагоналей. Сначала рассмотрим случай, где T преобразует r,c,d в r,c,d соответственно, ничего не говоря о том, куда переходит d'. Пусть

$$T=\begin{cases} i'=f(i,j) \\ j'=g(i,j) \end{cases}.$$

Из $Tr=r$ следует, что i' должен быть независим от j, а из $Tc=c$ следует, что j' должен быть независим от i. Следовательно

$$T=\begin{cases} i'=f(i) \\ j'=g(j) \end{cases}.$$

Если $f(0)=a$, $g(0)=b$ и не оба равны 0, то рассмотрим преобразование $T'=L^aM^bT$, которое также переводит r,c,d в r,c,d соответственно. Очевидно

$$T'=\begin{cases} i'=f'(i) \\ j'=g'(j) \end{cases}$$

И $f'(0)=g'(0)=0$. Из $T'd=d$ следует, что T' преобразует d

$$A(i,0),A(i+1,1),...,A(i+j,j),...$$

в d. Из этого следует, что

$$f'(i+j)-g'(j)=f'(i)-g'(0)=f'(i).$$

Положим $i=0$, тогда $f'(j)=g'(j)$ и мы получим

$$f'(i+j)=f'(i)+f'(j),$$

откуда следует, что $f'(i)=\alpha i$ и, таким образом, $L^aM^bT=S_\alpha$ или $T=M^{-b}L^{-a}S_\alpha$. А так как T' является перестановкой, то инвертируется, а для этого, очевидно, требуется $(\alpha,n)=1$.

Теперь пусть T переводит r,c,d,d' в r,c,d,d' в любом порядке. Если $Tr=c$, то $(PT)r=r$. При четном n $Tr\neq d$ или d', d и d' имеют два или ни одного общего элемента, в то время как r имеет только один общий элемент с любым c,d или d'. Если n нечетно и $Tr=d'$, то $(QT)r=r$; если $Tr=d$, то $(PQT)r=r$. Следовательно, в любом случае имеется элемент H из G такой, что если $T''=HT$, $T''r=r$. Если $T''c=c$ и $T''d=d'$, то $(OT'')r=r$, $(OT'')c=c$, и $(OT'')d=d$, и таким образом OT'' и, следовательно, T принадлежат G в соответствии с предыдущим параграфом. Если $T''c=d$, $T''d=d'$, то n нечетно и WT'', где

$$W=\begin{Vmatrix} 2 & 0 \\ 1 & -1 \end{Vmatrix},$$

переводит r,c,d в r,c,d, соответственно, и, следовательно, является элементом G; это невозможно, так как из $T''d'=c$ мы имели бы $(WT'')d'=Wc=P(2,1)$. Если $T''c=d$, $T''d=c$, то мы получим тот же самый результат, используя $WT''O$. Если $T''c=d'$ мы обработаем OT'' тем же способом. Это истощает все возможности, и в каждом случае T - член G.

Теорема 3.4. *Группа G имеет порядок $4n^2\varphi(n)$, если n четно и $8n^2\varphi(n)$, если n нечетно, $\varphi(n)$ - это число целых чисел меньше чем n и взаимно простых с n.*

Доказательство. Предположим, что n нечетно. Мы покажем, что каждый элемент G может быть выражен в уникальной форме

$$L^a M^b S_\alpha O^e P^f Q^g,$$

где $0 \le a \le n-1$; $0 \le b \le n-1$; $0 \le \alpha \le n$; $e = 0,1$; $f = 0,1$; $g = 0,1$.

Следующие соотношения легко проверяются:

(a) $ML = LM$,

(b) $$\begin{Vmatrix} a & c \\ b & d \end{Vmatrix} L = L^a M^b \begin{Vmatrix} a & c \\ b & d \end{Vmatrix},$$

$$\begin{Vmatrix} a & c \\ b & d \end{Vmatrix} L = L^c M^d \begin{Vmatrix} a & c \\ b & d \end{Vmatrix},$$

(c) $S_\alpha S_\beta = S_{\alpha\beta}$,

(d) $$\begin{Vmatrix} a & c \\ b & d \end{Vmatrix} S_\alpha = S_\alpha \begin{Vmatrix} a & c \\ b & d \end{Vmatrix},$$

(e) $PO = S_{n-1} OP$,

(f) $L^n = M^n = O^2 = P^2 = S_1$,

(g) $Q^2 = S_2$,

(h) $QO = PQ$, $QP = OQ$.

Теперь в любом данном произведении степеней генераторов мы можем передвинуть все Q к правому концу с использованием (b), (d), и (h), и с использованием (g) уменьшить степень Q до 0 или 1. Затем мы используем (b), (d), и (e) для переноса P следующим за Q и (f) для уменьшения степени P до 0 или 1. Затем O перенесем рядом с P и снова уменьшим степень до 0 или 1. В заключение присоединим S, и L, M поместим в соответствующем порядке. L и M – оба порядка n и имеется $\varphi(n)$ возможностей для α, таким образом общее количество таких нормальных форм - $8n^2\varphi(n)$. Мы должны теперь только доказать, что никакие две такие нормальные формы не могут представлять один и тот же элемент группы. Предположим

$$L^a M^b S_\alpha O^e P^f Q^g = L^{a'} M^{b'} S_{\alpha'} O^{e'} P^{f'} Q^{g'}.$$

Если $g \ne g'$, Q может быть выражен через L, M, S_α, O, P. Но это преобразование r в r или c, в то время как Q переводит r в d. Следовательно $g = g'$, и Q может быть опущен из уравнения. Если $f \ne f'$, P выражается через L, M, S_α, O, все из которых переводят r в r, в то время как P переводит r в c. Следовательно $f = f'$ и P может быть опущен. Если $e \ne e$, то O выражается через L, M, S_α, каждый из которых переводит d в d, в то время как O переводит d в d'. Следовательно $e = e$ и O может быть опущен. $S_{\alpha\beta}$, где $\beta\alpha' = 1 \pmod n$, выражается через L, M, каждое из которых сохраняет циклический порядок строк; что требует $\alpha\beta = 1 \pmod n$, или $\alpha' = \alpha$. L и M очевидно независимы.

Если n четно, то применяются те же аргументы, с вычеркиванием всех упоминаний о Q.

Теорема 3.5. *Набор* $(n!)^2\,\theta(n)$ *d.s. теоремы 3.2 инвариантен относительно* G.

Доказательство. Пусть A p.s. и R регулярное преобразование; тогда RA дьявольский квадрат. Мы желаем показать, что, если T является любым членом G, то существует регулярное преобразование R' и p.s. A' того же типа как и A, так что $TRA = R'A'$. Для этого достаточно показать, что если T - любой генератор G, то имеется регулярное преобразование R' такое, что $TR = R'T'$, где T' является перестановкой строк и столбцов. Пусть

$$R = \begin{Vmatrix} a & c \\ b & d \end{Vmatrix}.$$

Из (a) и (b) теоремы 3.4 мы получаем

$$RL^{\alpha}M^{\beta} = L^{a\alpha+\beta c}M^{\alpha b+\beta d}R.$$

Решая $\alpha a+\beta c=1$, $\alpha b+\beta d=1 \pmod n$, мы получим $\alpha = ed$, $\beta = -eb$, $e(ad-bc)=1 \pmod n$, так, что

$$LR = RL^{ed}M^{-eb}.$$

Точно так же

$$MR = RL^{-ec}M^{ea}.$$

Умножением матриц мы получаем

$$S_{\alpha}R = RS_{\alpha},\ OR = \begin{Vmatrix} a & c \\ -b & -d \end{Vmatrix},\ PR = \begin{Vmatrix} b & d \\ a & c \end{Vmatrix},\ QR = \begin{Vmatrix} a+b & c+d \\ a-b & c-d \end{Vmatrix}.$$

Каждая из новых матриц регулярна (последняя потому, что n нечетно) и поэтому L, M и S_{α} являются простым перемешиванием строк и столбцов между собой, теорема доказана.

4. Квадраты простых порядков. В этом разделе мы рассмотрим некоторые специальные свойства квадратов с простыми порядками p.

Соглашение, что квадрат S допускает данный набор конфигураций, подразумевает, что элементы S удовлетворяют некоторому набору линейных уравнений. Общее решение этих уравнений с элементами, являющимися линейными функциями некоторого числа определяющих, независимых параметров, назовем обобщенным квадратом порядка n допускающим данные конфигурации.

Лемма 4.1. *Обобщенный квадрат простого порядка* p*, допускающий все пути имеет вид* $A_{ij} = N$.[2]

Доказательство.

$$\begin{aligned} pN &= \sum_{b=1}^{p} P(i,j;1,b) - \sum_{x=1}^{p-1} P(i+x,0;0,1) \\ &= \sum_{b=1}^{p}\left(\sum_{x=1}^{p} A(i+x,j+bx)\right) - \sum_{x=1}^{p-1}\left(\sum_{y=1}^{p} A(i+x,y)\right) \\ &= \sum_{b=1}^{p} A(i,j) + \sum_{x=1}^{p-1}\left(\sum_{b=1}^{p} A(i+x,j+bx)\right) - \sum_{x=1}^{p-1}\left(\sum_{y=1}^{p} A(i+x,y)\right) \end{aligned}$$

[2] This theorem is true for squares of any order. The proof is very complicated, so it is not included here. A typewritten copy of the proof has been deposited in the Cornell University library as part of a monograph bearing the title Magic Squares, Supplement, by J. B. Rosser and R. J. Walker. This monograph will be referred to as "the supplement".

$$= pA(i,j) + \sum_{x=1}^{p-1}\left(\sum_{k=1}^{p} A(i+x,k)\right) - \sum_{x=1}^{p-1}\left(\sum_{y=1}^{p} A(i+x,y)\right)$$
$$= pA(i,j).$$

Лемма 4.2. *Число определяющих, независимых параметров в обобщенном квадрате S_p простого порядка, допускающих r наборов путей равно $p^2-(p-1)r$.*

Доказательство. Пусть s число независимых уравнений среди pr уравнений, выражающих факт, что S_p допускает r наборов рассматриваемых путей. Следовательно, число определяющих, независимых параметров в общем решении p^2-s. Допустимость для S_p пути $P(a,b)$ обозначает, что для каждого i и j выполняется

$$\sum_{x=1}^{p} A(i+ax, j+bx) = \frac{1}{p}\sum_{u,v} A(u,v)$$

Следовательно мы видим, что, если S_p допускает все, кроме одного из набора путей $P(a,b)$, то это автоматически позволяет его удалить. Следовательно, по крайней мере, r из pr уравнений зависимы и $s \le (p-1)r$. Предположим $s < (p-1)r$. Если мы подсоединим уравнения для остающихся путей, то число независимых уравнений в возникающем в результате наборе будет равно p^2-1 (лемма 4.1.) Следовательно, если t – число независимых добавленных уравнений, то $s+t \ge p^2-1$, и таким образом $t > (p-1)(p+1-r)$. Однако, имеется точно $p+1$ наборов путей, а именно, $P(0,1)$, $P(1,0)$, $P(1,1)$, ..., $P(1,p-1)$. Следовательно среди $p(p+1-r)$ добавленных уравнений, по крайней мере, $p+1-r$ являются зависимыми, поэтому $t \le (p-1)(p+1-r)$. Из этого противоречия следует $s=(p-1)r$ и лемма доказана.

Лемма 4.3. *В квадрате с простым порядком p, два пути различных наборов имеют точно один общий элемент.*

Доказательство. Если $P(i,j;a,b)$ и $P(k,l;c,d)$ находятся в различных наборах, то $ad-bc \not\equiv 0 \pmod p$. Следовательно верны соотношения

$$\begin{aligned} xa - yc &= k - i \\ xb - yd &= l - j \end{aligned} \pmod p,$$

имеющие единственное решение. Из это следует, что два пути имеют один общий элемент

$$A(i+ax, j+bx) = A(k+cy, l+dy).$$

Пусть $P(a_1,b_1)$, $P(a_2,b_2)$,..., $P(a_{p+1},b_{p+1})$ упорядоченный набор путей S_p. Для каждого s выберем α_s и β_s так, чтобы $\alpha_s b_s - a_s\beta_s \not\equiv 0 \pmod p$. Затем определим A^s для $s=1,2,...,p+1$, чтобы для всех значений z

$$A^s(za_s + y\alpha_s, zb_s + y\beta_s) = x_{(p-1)(s-1)+y} \qquad (y=1,2,...,p-1)$$

$$A^s(za_s, zb_s) = -\sum_{y=1}^{p-1} x_{(p-1)(s-1)+y}.$$

То есть каждый путь набора $P(a_s,b_s)$ для A^s имеет все элементы, заполненные либо

$$x_{(p-1)(s-1)+1}, x_{(p-1)(s-1)+2}, ..., x_{(p-1)s} \text{ или } -\sum_{y=1}^{p-1} x_{(p-1)(s-1)+y} .$$

Также определим A^0

$$. \ A_{ij}^0 = x_0 .$$

Ясно, что A^0 допускает все пути и по лемме 4.3, если $s = 1, 2, ..., p+1$, то A^s допускает все пути за исключением $P(a_s, b_s)$.

Теорема 4.1. *Если A определен как*

$$A_{ij} = \sum_{s=0}^{k} A^s(i, j), \ (0 \le k \le p+1),$$

тогда A - обобщенный квадрат простого порядка p, допускающий все пути $P(a_t, b_t)$ для $k+1 \le t \le p+1$

Доказательство. Очевидно A допускает рассматриваемые пути. Также A включает переменные $x_0, x_1, ..., x_{(p-1)k}$ и поэтому имеет правильное число параметров, согласно лемме 4.2. Теперь остается показать, что эти параметры являются независимыми. Для этого необходимо показать, что соответствующие значения могут быть произвольно назначены x и получившийся квадрат A будет допускать данные пути. Пусть B допускает пути $P(a_t, b_t)$ для $k+1 \le t \le p+1$. Выберем

$$x_0 = \frac{1}{p^2} \sum_{i,j} B_{ij}$$

Затем определим C и D

$$C_{ij} = B_{ij} - x_0, \ D_{ij} = A_{ij} - x_0 .$$

То есть

$$D_{ij} = \sum_{s=1}^{k} A^s(i, j).$$

Ясно, что C допускает те же самые пути, что и B, и $N = 0$ для C. Также этого достаточно для показа того, что $x_1, x_2, ..., x_{(p-1)k}$ можно выбрать так, чтобы D и C были одинаковыми.

Для $1 \le y \le p-1$, $1 \le s \le k$ выберем $x_{(p-1)(s-1)+y}$ следующим образом. Наложим A^s на C; затем выберем только те элементы A^s, которые состоят из $x_{(p-1)(s-1)+y}$ и покрываются путем $P(i_y, j_y; a_s, b_s)$ из C. Возьмем

$$x_{(p-1)(s-1)+y} = \frac{1}{p} P(i_y, j_y; a_s, b_s).$$

При таком выборе, ясно, что для всех x

$$-\sum_{y=1}^{p-1} x_{(p-1)(s-1)+y} = \frac{1}{p} P(0, 0; a_s, b_s).$$

Это значит, что выбрав x таким способом при $1 \le s \le k$ каждый элемент пути $P(i_y, j_y; a_s, b_s)$ в A^s будет равен

$$\frac{1}{p} (\text{путь } P(i, j; a_s, b_s) \text{ в C}).$$

Ясно, что

$$D_{ij} = \frac{1}{p}\sum_{s=1}^{k} P(i, j; a_s, b_s),$$

является $P(i_y, j_y; a_s, b_s)$ взятым из C. Однако, для C $P(a_t, b_t) = 0$, если $k+1 \le t \le p+1$. Итак

$$D_{ij} = \frac{1}{p}\sum_{s=1}^{p+1} P(i, j; a_s, b_s).$$

То есть pD_{ij} является суммой всех путей C через C_{ij}. Каждая пара этих путей уже имеет общий C_{ij} и согласно лемме 4.3 никаких других общих элементов иметь не может. Следовательно, сумма всех путей через C_{ij} содержит C_{ij} $(p+1)$ раза и каждый другой элемент C_{ij} точно один раз, и поэтому

$$pC_{ij} + \sum_{i,j} C_{ij} = pC_{ij}$$

Это доказывает теорему.

Теорема 4.2. *Квадрат простого порядка, допускающий все пути кроме строк и столбцов является примитивным.*[3]

Доказательство. Положим $a_1 = 0$, $b_1 = 1$, $a_2 = 1$, $b_2 = 0$, $\alpha_1 = 1$, $\beta_1 = 0$, $\alpha_2 = 0$, $\beta_2 = 1$. Тогда A, определяемый следующим образом

$$A_{ij} = \sum_{s=0}^{2} A^s(i, j),$$

очевидно, является примитивным.

Любую трансформацию p.s. будем называть *регулярным квадратом*.

Следствие 4.1. *Квадрат простого порядка, допускающий все, кроме двух путей, регулярен.*

Доказательство. Правильным преобразованием два пути можно перевести в строки и столбцы, и возникающий в результате квадрат должен быть примитивным согласно теореме 4.2. Применение обратного преобразования доказывает следствие.

Следствие 4.2. *Каждый d.s. порядка 5 регулярен.*

Для d.s. 5 порядка допускаются все пути кроме двух.

Теорема 4.3. *Общий d.s. 5 порядка допускает строки, столбцы, диагонали, конфигурацию* $A(1,1) + A(1,2) + A(1,5) + A(2,1) + A(5,1)$ *и трансформации последних под действием группы* G *теоремы 3.3. Он не допускает никаких иных конфигураций, которые являются суммой пяти элементов. Общий d.s.* S_p *простого порядка* ≥ 7 *не допускает никаких других конфигураций* C*, состоящих из суммы* p *элементов, за исключением строк, столбцов, и диагоналей.*[4]

---

[3] Эта теорема истинна для квадратов любого порядка. Доказательство дано в добавлении.

[4] d.s. порядка 5 допускает названную конфигурацию, d.s. порядка 4 допускает L(2) и $A_{00}+A_{01}+A_{10}+A_{11}$, d.s. порядка 8 допускает L(0,0;4)+L(2,2;4) и d.s. порядка 9 допускает L(3). Насколько мы знаем, это единственные значения n, для которых общий d.s. порядка n допускает конфигурацию n элементов, отличную от строки, столбца или диагонали.

Доказательство. Возьмем простое $p \geq 5$, пусть S_p обобщенный d.s. порядка p, и пусть C конфигурация, состоящая из суммы p элементов. Так как элементы A^s и A^t $(s \neq t)$ независимы, A^s должен допускать C, если S_p допускает и $P(a_s, b_s)$ не строка, столбец, или диагональ. Т.к. C - сумма p элементов, то A^s должен допускать C тогда и только тогда, когда C содержит ровно один элемент из каждого пути набора $P(a_s, b_s)$. Известно, что единственные пути S_p, которые могут содержать два элемента C это строки, столбцы, или диагонали. Теперь предположим, что C не строка, столбец, или диагональ и предположим, что S_p допускает C. Возьмем три элемента C, которые не одной строке, столбце, или диагонали. Мы только что видели, что каждая пара элементов из C должна лежать в строке, столбце, или диагонали. Следовательно, три пары из трех элементов, которые мы выбрали, должны лежать соответственно в любой строке, столбце, и диагонали, или в строке и в каждом из двух видов диагоналей, или в столбца и и в каждом виде диагоналей. В двух последних случаях мы можем применить преобразование Q теоремы 3.3 и говорить, что пары находятся в строке, столбце, и диагонали. Дальнейшими преобразованиями из G, мы можем выбрать пару, которая находится в строке с $A(1,1)$ и $A(1,2)$, а с третья в столбце с $A(1,1)$ и в диагонали с $A(1,2)$. Следовательно третья является или $A(2,1)$ или $A(p,1)$. Заключительным преобразованием из G, мы переведем третью в $A(2,1)$. Теперь пусть $A(i,j)$ любой элемент C. Тогда $A(i,j)$ должен быть в строке, столбце или диагонали с каждым из $A(1,1)$, $A(1,2)$ и $A(2,1)$. То есть $P(i-1, j-1)$, $P(i-1, j-2)$ и $P(i-2, j-1)$ должен каждый быть строкой, столбцом или диагональю. Проверив все эти возможности, мы получим, что либо $i=1$, $j=p$ или $i=p$, $j=1$, или $i=j=2$, или $i=j=\frac{1}{2}(p+3)$. Однако, ни $A(2,2)$, ни $A\left(\frac{1}{2}(p+3), \frac{1}{2}(p+3)\right)$ не находятся в одной строке или столбце с $A(1,p)$ или $A(p,1)$. Поэтому C должен состоять из $A(1,1)+A(1,2)+A(2,1)+A(1,p)+A(p,1)$ или из $A(1,1)+A(1,2)+A(2,1)+A(2,2)+A\left(\frac{1}{2}(p+3), \frac{1}{2}(p+3)\right)$. Применив $L^2M^{-1}Q$ теоремы 3.3 к результату, мы получим шаблон. Следовательно, результат это трансформация шаблона под воздействием преобразований группы G. Следовательно, первая названная конфигурация допускается S_5, что может быть проверкой обобщенного квадрата порядка 5.

Следствие 4.3. *Единственные перестановки элементов общего d.s. простого порядка* ≥ 7*, которые сохраняют дьявольский квадрат это преобразования набора строк, столбцов и диагоналей в набор строк, столбцов и диагоналей.*

Следствие 4.4. *Группа перестановок общего d.s. простого порядок* ≥ 7 *в d.s. является группой* G *теоремы 3.3, порядка* $8p^2(p-1)$.

Теорема 4.4. *Если H - группа, сгенерированная преобразованиями P теоремы 3.3 и перестановками строк между собой и, если*

$$T = \begin{Vmatrix} 3 & 2 \\ 1 & 1 \end{Vmatrix},$$

то любое преобразование вида TUT^{-1}, где U входит в H, будет преобразовывать d.s. порядка 5 в d.s. порядка 5.

Доказательство. Если S_5 - d.s., то $T^{-1}S_5$ будет p.s., $UT^{-1}S_5$ будет p.s. и $TUT^{-1}S_5$ также будет d.s.

Мы покажем в следствии 5.2, что любое преобразование, которое переводит обобщенный d.s. порядка 5 в d.s. должен иметь вид TUT^{-1}, где U принадлежит H.

5. Числовые квадраты. Любой квадрат S_n с элементы из целых чисел $1,2,...,n$ называется числовым квадратом (n.s.). Таким образом, мы можем говорить о дьявольском числовом квадрате (n.d.s.) и о примитивном числовом квадрате (n.p.s.). В n.s. мы имеем

$$N = \frac{1}{n^2}\sum_{i,j=1}^{n} A_{ij} = \frac{1}{n^2}\sum_{k=1}^{n^2} k = \frac{1}{n^2}\frac{n^2\left(n^2+1\right)}{2} = \frac{n^2+1}{2}.$$

Теорема 5.1. *Не существует квадратов n.d.s. порядка 3.*
Это следует из леммы 4.1.

Теорема 5.2. *Не существует n.d.s. порядка n при $n = 2 \pmod 4$.*

Доказательство. Пусть $n = 4m+2$, и предположим, что S_n - n.d.s. Следовательно S_n допускает решетку $L(2)$ по теореме 2.4. Так как элементы квадрата целые числа, то и элементы $L(2)$ целые числа. Однако, $L(2)$ имеет $(2m+1)^2$ элементов со средним значением N равным $\frac{1}{2}\left(n^2+1\right)$. Но

$$L(2) = (2m+1)^2\,\frac{1}{2}\left(n^2+1\right)$$

не является целым.

В дальнейшем будет показано, что существуют n.d.s. всех порядков, кроме случаев предшествующих двух теоремам, поэтому хотелось бы узнать возможную структуру n.p.s. Этим мы сейчас займемся.

Как и в теореме 5.3, мы полагаем, что индексы (i,j) в $A(i,j)$ всегда лежат в диапазоне $1,2,...,n$.

По определению свойство примитивности является инвариантом относительно преобразования H теоремы 4.4. Следовательно мы можем нормализовать наш n.p.s. так, чтобы

$$A(1,1)=1,\quad A(1,2)<A(2,1),\quad A(1,i)<A(1,i+j),\quad A(i,1)<A(i+j,1) \tag{1}$$

если $1 \le j$. Пусть $\Phi(n)$ число нормализованных n.p.s. порядка n. Тогда общее число n.p.s. будет $2(n!)^2\,\Phi(n)$. Из

$$A_{ij} + A_{kl} = A_{il} + A_{kj} \tag{2}$$

из (1) следует

(3) $$A(i,j) < A(i+k, j+l)$$

если $0 \le k$, $0 \le l$, $1 \le k+l$. Из (3) мы видим, что $A(1,2) = 2$. Пусть m самое большое значение j, такое, что для $i \le j$ $A(1,i) = i$. Т.е. $2 \le m \le n$; также из (3) мы имеем $A(2,1) = m+1$. Покажем сначала, что элементы в строках наборы m последовательных целых чисел. Если это верно для первой строки, то это верно и для других согласно (2). Допустим, что это неправильно для первой строки. Пусть первые rm элементов первой строки лежат в таком наборе, но

$$A(1, mr+1), A(1, mr+2), ..., A(1, m(r+1))$$

не являются последовательными целыми числами. Пусть k самое большое целое число, что для всех j, $1 \le j \le k$, выполнено

$$A(1, mr+j) = A(1, mr+1) - 1 + j.$$

Тогда $1 \le k \le m-1$ и $A(1, mr+1) + k$ не встречается в первой строке. Пусть оно встречается i-ой строке.

Случай 1. Имеется $l \ge 1$ такое, что

$$A(1, mr+j) + k = A(i, mr+l)$$

Т.к. $i \ge 2$, то мы имеем

$$A(1, mr+1) + k = A(i, mr+l) \ge A(i, mr+1)$$
$$= A(1, mr+1) + A(i,1) - A(1,1) \ge A(1, mr+1) + A(2,1) - A(1,1)$$
$$\ge A(1, mr+1) + m + l - 1 \ge A(1, mr+1) + m.$$

Это противоречит условию 1≤k≤m-1.

Случай 2. Имеются j $(0 \le j \le r-1)$ и l $(1 \le l \le m)$ такие, что

$$A(1, mr+1) + k = A(i, mj+l)$$

Поэтому элементы первых rm столбцов встречаются в строках в наборе m последовательных целых чисел,

$$A(1, mr+1) + k + w - l = A(i, mj+w)$$

для $1 \le w \le m$. Если $l \ge 2$, тогда $A(1, mr+1) + k - 1$ должно встретиться в обеих и первой и в i-ой строках. Т.е. $i = 1$. Следовательно

$$A(1, mr+1) + m = A(i, mj+m+1-k).$$

Однако,

$$A(1,1) + A(2, mr+1) = A(1, mr+1) + A(2,1),$$

и $A(1,1) = 1$, $A(2,1) = m+1$, т.е.

$$A(2, mr+1) = A(1, mr+1) + m = A(i, mj+m+1-k),$$

и условия $k \ge 1$, $j \le r-1$ приводят к противоречию.

Мы можем заключить, что элементы, встречающиеся в строках наборы m последовательных целых чисел. Также ясно, что элементы $A(i, mj)$ должны быть множителями m. Если мы определим B как

$$B(i,j) = \frac{1}{m} A(i, mj),$$

то, очевидно, что прямоугольник B примитивный и

$$B(1,1) = 1, \quad B(2,1) = 2, \quad B(i,j) \le B(i+k, j+l)$$

если $0 \le k$, $0 \le l$, $1 \le k+l$. Так как предшествующие аргументы сохраняются одинаково хорошо для прямоугольников, мы можем поменять строки со столбцами B и повторить

аргументацию. Этот процесс, очевидно, завершается после конечного числа шагов. Так, нормализованный n.p.s. порядка четыре может иметь структуры

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

1	2	9	10
3	4	11	12
5	6	13	14
7	8	15	16

1	2	5	6
3	4	7	8
9	10	13	14
11	12	15	16

и никаких других.

Важным свойством n.p.s. является факт, что элементы 1 и 2 всегда встречаются в одной и той же строке или столбце. Это свойство можно использовать при создании неправильных квадратов. Точное число $\Phi(n)$ нормализованных n.p.s. порядка n равно числу путей выбираемых из $d_1, d_2, ..., d_s$ и $f_1, f_2, ..., f_t$, так, чтобы $s = t$ или $t+1$; $d_1 = 1$, $d_s = n$; $f_1 \neq 1$, $f_t = n$; $d_i \neq d_{i+1}$, $f_i \neq f_{i+1}$; d_i делит d_{i+1}; и f_i делит f_{i+1}. Это, конечно, меньше или равно $(n!)^2$, т.к. d_1 не может быть выбрано более чем n способами, d_2 не может быть выбрано более чем $n-1$ способами, и т.д., и то же самое применимо к f.

Ясно, что для простых порядков имеется точно один нормализованный n.p.s. Следовательно имеются ровно два типа n.p.s. простого порядка (см. обсуждение после доказательства теоремы 3.1), а именно, того же самого типа как A, где

$$A_{ij} = (i-1)p + j,$$

и того же самого типа как PA (P как в теореме 3.3). Если B получен из PA регулярным преобразованием T, то B получен из A регулярным преобразованием TP. n.d.s. не может быть получен из A или PA не регулярным преобразованием. Такое преобразование любого n.p.s. простого порядка должно переводить строки или столбцы в строки, столбцы, или диагонали, и поэтому нет двух строк или столбцов n.p.s, имеющих ту же самую сумму, преобразованный квадрат не может быть дьявольским. Следовательно, n.d.s. простого порядка будет регулярным тогда и только тогда, когда он может быть получен из n.p.s. A регулярным преобразованием, и согласно теореме 3.2, мы имеем

Теорема 5.3. *При нечетном простом p имеется ровно $(p!)^2 (p-3)(p-4)$ регулярных n.d.s. порядка p.*

Регулярный n.d.s. нечетного простого порядка, полученный из нормализованного n.p.s. это так называемые "step squares". Регулярный n.d.s. является естественным обобщением

"step squares". Например, обобщенные "step squares", рассмотренные A.H.Frost[5], все являются регулярными n.d.s.

Следствие 5.1. *Имеется точно 28,800 n.d.s, порядка 5.*
Используем вышеупомянутую теорему и следствие 4.2.

Следствие 5.2. *Любое преобразование, которое переводит общий дьявольский квадрат порядка 5 в дьявольский квадрат, должно иметь форму TUT^{-1}, где T и U - как в теореме 4.4.*

Доказательство. Любое преобразование V, которые переводит обобщенный d.s. порядка 5 в d.s. должно переводить n.d.s. в n.d.s. Следовательно имеется по крайней мере так много n.d.s., сколько имеется преобразований V. Имеется всего 28,800 преобразований V. Однако, TUT^{-1}, очевидно, является V. Также H имеет порядок 28,800 (=2(5!)^2) так как имеется 5! перестановок строк и 5! перестановок столбцов, а также две ориентации квадрата. Т.е. имеется ровно 28,800 V и TUT^{-1}.

Так как n.p.s. всех порядков существуют, то существование регулярных n.d.s. любого простого порядка >6, следует из теоремы 3.2. Мы можем создавать регулярные n.d.s. всех порядков, кроме исключений теорем 5.1 и 5.2. Мы также можем создавать неправильные n.d.s. всех порядков, кроме исключений теорем 5.1, 5.2, и 5.4.

Теорема 5.4. *Любой d.s. порядка 1, 4 или 5 должен быть регулярным.*

Доказательство. Теорема очевидна для $n=1$. Для $n=5$ используем следствие 4.2. Для квадрата порядка 4 можно найти обобщенный квадрат просто решая уравнения, чтобы квадрат допускал строки, столбцы, и диагонали. Обобщенный квадрат, как можно затем увидеть, получается с помощью преобразования

$$\begin{Vmatrix} 1 & 2 \\ 2 & 1 \end{Vmatrix}$$

из p.s.

Лемма 5.1. *Если m и n - оба нечетные целые числа большие или равные 3, то возможно упорядочить целых числа $0,1,2,\ldots,mn-1$ в прямоугольном массиве из n строк и m столбцов таким способом, чтобы суммы n элементов в каждом столбце были одинаковыми.*

Доказательство. Пусть первая строка начинается с 0 в первом столбце и увеличивается $m-1$ раза на 1 до m-ого столбца. Пусть вторая строка начинается с $\frac{1}{2}(3m+1)$ в первом столбце и увеличивается на 1 до $2m-1$ в $\frac{1}{2}(m-1)$-ом столбце, затем стартуем с m в $\frac{1}{2}(m+1)$-ом столбце и увеличиваем на 1 до $\frac{1}{2}(3m-1)$ в m-ом столбце. Пусть третья строка начинается с $3m-2$ в первом столбце и уменьшается на 2 до $2m+1$ в $\frac{1}{2}(m-1)$ столбце и затем стартует с $3m-1$ в $\frac{1}{2}(m+1)$-ом столбце и уменьшается на 2 до $2m$ в m-

[5] A. H. Frost, On the general properties of Nasik squares, Quart. Jour. Mth., vol. 15(1877), pp. 34-49.

ом столбце. Ясно, что сумма из первых трех элементов в каждом столбце равна $\frac{1}{2}(9m-3)$.

Если $n \geq 5$, то массив может быть создан, стартуя по четным строкам с множителями m в первом столбце и увеличением на 1 направо, и, стартуя по нечетным строкам с множителя m в m-ом столбце и увеличением на 1 налево.

Теорема 5.5. *Имеются регулярные n.d.s. всех порядков, кроме случаев теорем 5.1 и 5.2.*

Доказательство.
Случай 1. Если n – простое больше 6, то используем теорему 3.2.
Случай 2. Пусть $n = 4m$, и пусть

$$T = \begin{Vmatrix} 2 & -1 \\ -3 & 2 \end{Vmatrix}.$$

Положим $a(i) = i$, $a(i+2m) = 4m+1-i$ для $1 \leq i \leq 2m$, и положим $a(i \pm 4m) = a(i)$ и определим A

$$A_{ij} = na(i) + a(j) - n.$$

Ясно, что A - n.p.s. Покажем, что TA является n.d.s., который, следовательно, является регулярным. T переводит пути $P(1,2)$, $P(2,3)$, $P(3,5)$, $P(1,1)$ в пути $P(0,1)$, $P(1,0)$, $P(1,1)$ и $P(1,-1)$. Так что мы просто должны показать, что A допускает первый набор из названных путей. Доказательства подобны для каждого пути, и мы иллюстрируем их, давая доказательство для $P(2,3)$.

$$\begin{aligned} P(i,j;2,3) &= \sum_{x=1}^{n} \left(na(i+2x) + a(j+3x) - n \right) \\ &= n\sum_{x=1}^{n} a(i+2x) + \sum_{x=1}^{n} a(j+3x) - n^2 \end{aligned}$$

Теперь

$$\begin{aligned} \sum_{x=1}^{n} a(i+2x) &= 2\sum_{x=1}^{2m} a(i+2x) = 2\sum_{x=1}^{m} \left[a(i+2x) + a(i+2x+2m) \right] \\ &= 2\sum_{x=1}^{m} (4m+1) = 2m(4m+1) = \frac{1}{2} n(n+1). \end{aligned}$$

Если $m \neq 0 \pmod{n}$,

$$\sum_{x=1}^{n} a(j+3x) = \sum_{x=1}^{n} a(x) = \frac{1}{2} n(n+1).$$

Если $m = 3s$,

$$\begin{aligned} \sum_{x=1}^{n} a(j+3x) &= 3\sum_{x=1}^{4s} a(j+3x) = 3\sum_{x=1}^{2s} \left[a(j+3x) + a(j+3x+2m) \right] \\ &= 3 \cdot 2s(n+1) = \frac{1}{2} n(n+1). \end{aligned}$$

В любом случае,

$$P(i,j;2,3) = n\frac{1}{2}\left(n^2+1\right) = nN.$$

Случай 3. $n = 3m$, m нечетно, $m \geq 3$. Пусть

$$T = \begin{Vmatrix} 1 & 1 \\ 2 & 3 \end{Vmatrix}.$$

Упорядочив числа $0,1,2,\ ...,\ 3m$-1 в массив как в лемме 5.1, получим 3 столбца и m строк. Положим $a(3x+y)$ равным элементу в $(x+1)$-ой строке и у столбце массива, и положим $a(i \pm n) = a(i)$. Затем

$$\sum_{x=1}^{m} a(3x+y) = \frac{1}{6} n(n-1).$$

Определим A

$$A_{ij} = na(i) + a(j) + 1.$$

A - n.p.s. T переводит пути P (1,-1), $P(3,-2), P(2,-1), P(4,-3)$ в $P(0,1), P(1,0), P(1,1), P(1,-1)$. A допускает $P(1,-1)$ и $P(2,-1)$ по теореме 2.1. Мы докажем, что A допускает $P(4,-3)$, и доказательство того, A допускает что $P(3,-2)$ такое же.

$$P(i, j; 4, -3) = \sum_{x=1}^{n} (na(i+4x) + a(j-3x) + 1)$$

$$= n\sum_{x=1}^{n} a(i+4x) + \sum_{x=1}^{n} a(j-3x) + n.$$

Теперь

$$\sum_{x=1}^{n} a(i+4x) = \sum_{x=1}^{n} a(x) = \frac{1}{2} n(n-1),$$

и

$$\sum_{x=1}^{n} a(j-3x) = 3\sum_{x=1}^{m} a(j+3x) = \frac{1}{2} n(n-1).$$

Следовательно $P(i, j; 4, -3) = nN$.

Теорема 5.6. *Имеются нерегулярные n.d.s. любых порядков, кроме исключенных теоремами 5.1, 5.2, и 5.4.*

Случай 1. n нечетно и $(n, 6) = 1$.

2	47	38	35	24	20	9
26	16	8	6	46	42	31
49	39	33	23	15	12	4
19	11	7	45	41	30	22
37	29	27	17	14	3	48
10	5	44	36	34	25	21
32	28	18	13	1	43	40

Является нерегулярным n.d.s. Это можно видеть из обсуждения, предшествующего теореме 5.3, если бы это был регулярный квадрат, то он должен трансформироваться из n.p.s., в котором столбец содержал бы 1,8,15,22,29,36,43. Но они не составляют путь в данном квадрате, и, следовательно, такое преобразование невозможно.

Возьмем теперь $n \geq 11$. Пусть A задан, как

$$A_{ij} = (i-1)n + a_j,$$

где $a_1,\ a_2,\ ..., a_{11} = 2,7,4,9,6,11,1,8,3,10,5$ соответственно и $a_j = j$ для $12 \leq j \leq n$.

Определим B как квадрат с B(1,4), B(4,4), B(4,2), B(3,4), B(3,9), B(2,11), B(2,9), B(5,9), B((n+7)/2,2), B((n+5)/2,4), B((n+5), 2), B((n+11)/2,2), B((n+3)/2,9), B((n+9)/2,9), B((n+9)/2,7) и B((n+7)/2,9) равными +1; B(3,3), B(2,5), B(2,3), B(5,3), B(1,10), B(4,10), B(4,8), B(3,10), B((n+3)/2,3), B((n+9)/2,3), B((n+9)/2,1), B((n+7)/2,3), B((n+7)/2,8), B((n+5)/2,10), B((n + 5)/2,8) и B((n+11)/2,8) равными -1; все остальные элементы равны 0. Положим

$$T = \begin{Vmatrix} 2 & 1 \\ 1 & 2 \end{Vmatrix}.$$

Т.к. TA - n.d.s., то T регулярное, и A - n.p.s. Также может быть легко замечено, что каждая строка, столбец, или диагональ TB содержит так много +1 как -1, т.е. TB дьявольский. Следовательно, $TA+TB$ дьявольский. Следовательно, он - n.d.s., если содержит все элементы $1,2,...,n^2$. Однако, $TA+TB=T(A+B)$ и $(A+B)$, как легко видеть, есть результат обмена парами элементов $A_{i,j}$ и $A_{i,j+6}$ в A. Т.е. $TA+TB$ - n.d.s. Если $T(A+B)$ регулярный, то $A+B$ будет также регулярным. Мы имеем $A_{17}+B_{17}=1$, $A_{11}+B_{11}=2$; эти элементы находятся на уникальном пути $P(1,1;0,6)=P(1,1;0,1)$ т.к. $7\text{-}1=6$ взаимно просто с n и следовательно преобразует $A+B$ в p.s., переводя всю первую строку $A+B$ в строку. Так как эта строка состоит из чисел $1,...,n$ число $n+1$ должно найтись в том же самом столбце преобразованного квадрата как 1. Т.к. $n+1=A_{27}+B_7$ принадлежит тому столбцу $A+B$ что и 1, то преобразование переводит строки в строки и столбцы в столбцы и преобразованный квадрат будет примитивным, $A+B$ будет примитивным. Но это, очевидно, не так.

Случай 2. $n=4m$, $m\geq 2$. Рассмотрим $2m^2$ пары $(0,16m^2\text{-}4)$, $(4,16m^2\text{-}8)$, $(8,16m^2\text{-}12)$, ..., $(8m^2\text{-}4,8m^2)$. Если (A,C) и (B,D) - две пары, тогда

(4)

A+1	B+4	C+1	D+4
C+2	D+3	A+2	B+3
A+4	B+1	C+4	D+1
C+3	D+2	A+3	B+2

является дьявольским с $N=\frac{1}{2}\left(16m^2+1\right)$. Заполним $L(m)$ S_{4m} квадратами подобно (4), используя различные наборы пар для каждого квадрата. Получим результат - n.d.s. согласно теореме 2.7. Число путей назначения пары к парам каждой $L(m)$ равно

$$\frac{\left(2m^2\right)!}{2^{m^2}}.$$

Квадрат, составляющий любую $L(m)$ может быть размещен 384 способами.[6] Т.е. имеется по крайней мере

(5) $$(192)^{m^2}\left(2m^2\right)!$$

n.d.s. порядка $4m$.[7] Мы теперь покажем, что это превышает число регулярных n.d.s, порядка $4m$. Пусть $\psi(4m)$ число нормализованных n.p.s. порядка $4m$. Тогда имеются $2\left((4m)!\right)^2\psi(4m)$ n.p.s. порядка $4m$. Однако, с помощью аргументов, предшествующих теореме 5.3, мы можем увидеть, что регулярных n.d.s., получаемых после преобразований n.p.s. только $\left((4m)!\right)^2\psi(4m)$. Пусть

$$T = \begin{Vmatrix} a & c \\ b & d \end{Vmatrix}.$$

С помощью рассуждений, аналогичных предшествующим лемме 3.1, мы видим, что, если b или d взаимно просто с $4m$, то может получиться единство. Так для $m=2$, мы можем

[6]Barkley Rosser and R. J. Walker, loc. cit., Theorem 4.

[7]The squares of order 4m constructed by this method satisfy the conditions that each L(m) is a d.s. of order 4. This gives $12m^2$ independent linear conditions on the elements. As the general square of order 4m satisfies only 16m-4 independent linear conditions, the number of such squares must be immense.

рассмотреть следующие случаи: $b=d=1$; $b=1$, d четное; b четное, $d=1$; b и d оба четные. Для каждого случая a и c могут выбираться 8 способами. Т.е. всего имеются $64+4\cdot 64+4\cdot 64+16\cdot 64=1600$ преобразований, которые могут выдавать различные n.d.s. порядка 8. Из того, что $\psi(8)=10$, мы видим, что число регулярных n.d.s. порядка 8 меньше чем число n.d.s, порядка 8 полученных по формуле (5). Для $m\geq 3$ мы можем просто получить число преобразований как меньше чем $(4m)^4$. Следовательно имеется всего

(6) $$(4m)^4\left((4m)!\right)^2\psi(4m)$$

регулярных n.d.s. порядка $4m$. $\psi(12)=42$, т.е. для $m=3$ (6) дает меньше чем (5). Мы показали что $\psi(n)\leq(n!)^2$. Используя это в (6) и используя аппроксимацию $n!$, мы видим, что для $m\geq 4$ (5) превышает (6).

Случай 3. $n=9$.

(7)

1	65	48	41	24	58	81	34	17
57	76	33	13	8	70	53	39	20
68	49	44	27	62	75	28	12	4
80	36	16	3	64	47	40	23	60
52	38	19	56	78	32	15	7	72
30	11	6	67	51	43	26	61	74
42	22	59	79	35	18	2	66	46
14	9	71	54	37	21	55	77	31
25	63	73	29	10	5	69	50	45

Не является регулярным n.d.s. Для того, чтобы он был регулярным один из путей, содержащих 1 и 2, должен трансформироваться из строки n.p.s. Но единственные пути, содержащие 1 и 2, это P(1,1), P(1,4) и P(1,7). Т.к. (7) допускает P(1,1), эти пути не могут быть строками n.p.s. Элементы P(1,1;1,4) 1, 2, 3, 4, 5, 6, 7, 8, 9. Если это была строка n.p.s., то числа 1, 10, 19, 28, 37, 46, 55, 64, 73 были бы должны формировать столбец. Однако, они не составляют путь в (7). Элементы P(1,1;1,7) 1, 2, 3, 37, 38, 39, 73, 74, 75. Они не могут составлять строку n.p.s.

Случай 4. n=3m, (m,6)=1, m≥5. Если $a(x,1)$, $a(x,2)$, ..., $a(x,m)$ - набор m различных целых чисел, находящихся между 0 и $9m-1$, и если A_x определен

$$A_{ij}=9mi+a(x,j)-9m+1,$$

и по теореме 3.2 имеется регулярное преобразование T, такое, что TA является d.s. Упорядочим числа 0,1,2, ..., $9m$-1 в массиве леммы 5.1, принимая m строк и 9 столбцов. Возьмем $a(x,y)$ чтобы он был элементом в y-ой строке и x-ом столбце. Тогда TA_1, TA_2, ..., TA_9 - каждый d.s., и вместе используют целые числа 1,2, ..., n^2. Т.е., если мы возьмем TA_x как решетки $L(3)$ квадрата порядка n, то это будет n.d.s. по теореме 2.7. Решетки могут быть вставлены таким способом, что 1,2 и 3 будут первыми тремя элементами первой строки n.d.s. порядка n. Затем проверкой массива леммы 5.1, заметим, что остающиеся элементы первой строки это $9m\alpha+15$, $9m\alpha+16$, $9m\alpha+17$, $9m\beta+22$, $9m\beta+24$, $9m\beta+26$, $9m\gamma+28$, $9m\gamma+29$, $9m\gamma+30$, ... Любое преобразование, переводящее квадрат в p.s. будет переводить первую строку в строку, так как она - единственный путь, содержащий 1 и 2. Но строка состоит из $m-1$ триплетов последовательных целых чисел и одного триплета непоследовательных целых чисел, и она не может быть строкой n.p.s. Следовательно, рассматриваемый квадрат не регулярный.

Случай 5. $n=9m$, m нечетно, $m\geq 3$. Возьмем T как в случае 2 теоремы 5.5. Упорядочим числа $0,1,2,\ ...,\ 27m$-1 в массиве леммы 5.1, принимая 27 столбцов и m строк. Примем $a(x,3y+z)$ равным элементу в $(y+1)$-ой строке и $(x+9z-9)$-ом столбце $(x=1,2,\ ...,9)$. Определим A_x

$$A_{ij}=27mi+a(x,j)-27m+1,$$

С помощью аргументов, аналогичных случаю 2 теоремы 5.5, получаем, что TA_x - d.s. Затем мы можем использовать TA_x как решетки $L(3)$ из n.d.s. порядка n. Рассуждения, как в предшествующем случае, покажут, что это может быть выполнено при нерегулярном n.d.s. порядка n. Это завершает доказательство теоремы.

Если A и B - n.d.s. порядков m и n, и мы определяем решетку $L(i,j;m)$ квадрата D порядка mn так, чтобы

$$C_{xy}=B_{xy}+n(A_{ij}-1),$$

то D - n.d.s. по теореме 2.7. Если B не регулярный, то D не регулярный по теореме 2.2 и факта, что решетки преобразуются в решетки. Если B регулярный, то можно трансформировать некоторые, но не все решетки D преобразованиями группы G теоремы 3.3 и результаты обычно будут не регулярными.

В добавлении описаны средства построения n.d.s. B порядка $3m$ из n.d.s. A порядка m. Этим доказывается, что, если A не регулярный, то и B не регулярный.

6. Заключение. Методы, используемые при получении свойств дьявольских квадратов могут применяться к другим подобным проблемам. Очевидно, что дьявольские кубы (или hypercubes) могут быть определены и изучаться аналогичным способом. В добавлении установлено существование или не существование числового дьявольского куба любого данного порядка.

Другое приложение к теории латинских квадратов. Латинский квадрат наиболее просто определяется как квадрат, чьи элементы - n независимых переменных, которые встречаются n раз каждое. Таким образом, дьявольский латинский квадрат (d.l.s) должен содержать каждую переменную один раз в каждой строке, столбце и диагонали. Принципиальные результаты относительно d.l.s. доказанные в добавлении следующие:

(a) нет d.l.s. порядка, делящегося на 2, но не делящегося на 8, или на 3, но не на 9.

(b) имеются регулярные d.l.s. порядка n тогда и только тогда, когда $(n,6)=1$.

(c) имеются нерегулярные d.l.s. простого порядка p только при $p>11$.