Решение задач третьей олимпиады

Задача 2008–1

Преобразуем сумму $\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{1200}$ в дробь $\frac{m}{n}$. Докажите, что m делится на 1201. (*Предложил Ю. Г. Прохоров.*)

Решение. Достаточно доказать утверждение для несократимой дроби $\frac{m}{n}$. Заметим, что число 1201 простое. Поэтому кольцо $\mathbb{Z}_{1201}$ — поле. В этом поле имеем равенство $\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{1200}=\frac{m}{n}$ (знаменатель n не делится на 1201). В сумме слева знаменатели пробегают все ненулевые элементы поля. Таким образом, все члены этой суммы различны и также пробегают все ненулевые элементы поля. Следовательно, эта сумма равна нулю в $\mathbb{Z}_{1201}$.

Упражнение 1. Покажите, что m делится даже на 1201^2.

Задача 2008–2

По комнате, имеющей форму параллелепипеда, ползают тараканы. В полночь каждый таракан переползает на одну из четырех граней, соседних с той, на которой он находился (например, все тараканы, находившиеся на полу, заползают на стены); причем в результате число тараканов на каждой грани остается постоянным. В этой задаче 24 неизвестных: количество тараканов, переползших с каждой грани на каждую из соседних с ней граней. А сколько у этой задачи линейно независимых решений? Найдите фундаментальную систему решений. (*Предложил А. А. Клячко.*)

Решение. В задаче шесть однородных линейных уравнений, выражающих постоянство числа тараканов на каждой грани. Одно из этих уравнений является следствием остальных. Действительно, если известно, что число тараканов на каждой грани, кроме потолка, остается постоянным, то число тараканов на потолке также постоянно, поскольку общее число тараканов не изменяется при переползании. (Более точно, сумма всех шести уравнений равна нулевому уравнению.) Это единственная зависимость между уравнениями, то есть любые 5 из шести уравнений независимы. Чтобы это доказать, достаточно предъявить ситуации, удовлетворяющие всем уравнениям, кроме двух (произвольных). Другими словами, нужно построить примеры, когда число тараканов на каждой грани, кроме ровно двух, остается постоянным. Если речь идет о двух соседних гранях, например, о поле и одной из стен, то можно рассмотреть такую ситуацию: *в комнате всего один таракан, он находится на полу, а потом заползает на стену.* При этом не меняется число тараканов на каждой грани, кроме пола и этой стены. Если же речь идет о двух противоположных гранях, например, о поле и потолке, то нам подойдет такая ситуация: *в комнате всего два таракана, один на полу, другой на стене; в полночь таракан с пола заползает на эту стену, а таракан со стены заползает на потолок.* При этом не меняется число тараканов на каждой грани, кроме пола и потолка.

Таким образом, размерность пространства решений равна девятнадцати $(24-5)$. Построим теперь 19 линейно независимых решений. Для каждого из двенадцати ребер e параллелепипеда рассмотрим следующее простейшее решение:

D_e: *в комнате находятся всего два таракана на гранях, разделенных ребром e; в полночь эти тараканы меняются местами.* Одно из таких решений изображено на рисунке 1 (в центре).

Кроме того, для каждой из восьми вершин v параллелепипеда рассмотрим следующее, чуть более сложное, решение:

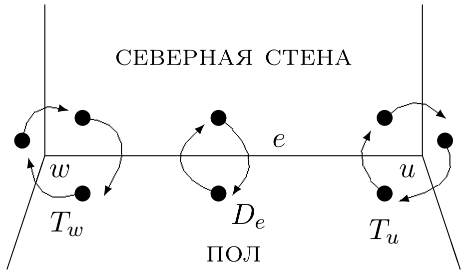
T_v: *в комнате находятся всего три таракана на гранях, смежных с вершиной v; в полночь эти тараканы меняются местами по циклу, по часовой стрелке (если смотреть изнутри комнаты).* Два таких решения также изображены на рисунке 1.

Эти 20 решений, разумеется, линейно зависимы: $\sum\limits_e D_e=\sum\limits_v T_v$. Мы покажем, что это единственная зависимость, то есть если

$$\sum_e \lambda_e D_e+\sum_v \mu_v T_v=0 \quad \text{для некоторых 20-ти чисел } \lambda_e \text{ и } \mu_v, \tag{$*$}$$

то все λ_e равны между собой, все μ_v равны между собой и $\lambda_e=-\mu_v$. Отсюда очевидным образом будет вытекать, что любые 19 из наших 20-ти решений линейно независимы и, следовательно, образуют фундаментальную систему решений.

Сосредоточим свое внимание на некотором ребре e. Без ограничения общности будем считать, что это ребро отделяет пол от северной стены. Западный конец этого ребра обозначим буквой w, а восточный конец — буквой u (рис.1). Всякому решению s сопоставим число $y_e(s)$ — число тараканов, забравшихся на стену через ребро e. (Эта величина представляет собой один из наших исходных 24-х неизвестных.) Тогда $y_e(D_e) = 1$ и $y_e(T_u) = 1$, а для остальных 18-ти наших решений величина y_e равна нулю.



Применяя теперь функцию $y_e(\cdot)$ к обеим частям равенства $(*)$, мы получаем, что $\mu_u = -\lambda_e$. По аналогичным причинам $\mu_w = -\lambda_e$ (в частности, $\mu_u = \mu_w$). В силу произвольности ребра e и связности графа, составленного из ребер параллелепипеда, это означает, что $\mu_v = -\lambda_e$ для всех вершин v и всех ребер e, что и требовалось.

Упражнение. Решите аналогичную задачу для произвольного выпуклого многогранника. Какие новые эффекты появляются на невыпуклых многогранниках?

Задача 2008–3

Матрица называется *магической*, если суммы ее элементов в каждой строке, каждом столбце, на главной диагонали и на побочной диагонали одинаковы. Какова размерность пространства магических матриц? (*Предложил А. Э. Гутерман*[1].)

Ответ.
При $n = 1$ и $n = 2$ размерность равна 1.
При $n \geqslant 3$ в общем случае размерность равна $n^2 - 2n$.
Есть одно исключение: $n = 4$, $\operatorname{char}\mathbb{F} = 2$. Тогда размерность равна 9, то есть, $n^2 - 2n + 1$.

Решение 1. Введем следующие обозначения. Пусть

– $\mathbb{F}$ — основное поле,
– $\mathbb{F}^n$ — линейное пространство размерности n над $\mathbb{F}$,
– $M_n(\mathbb{F})$ — множество $n \times n$-матриц с коэффициентами из $\mathbb{F}$;
– E — единичная матрица;
– J — матрица, у которой на побочной диагонали 1, а все остальные элементы 0;
– C_i — матрица, у которой i-й столбец состоит из 1, а все остальные элементы равны 0;
– R_i — матрица, у которой i-я строка состоит из 1, а все остальные элементы равны 0;
– $\langle A, B\rangle = \operatorname{tr}(AB^\top)$ для $A, B \in M_n(\mathbb{F})$, где $B^\top$ — транспонированная матрица;
– $\mathcal{M}_n \subset M_n(\mathbb{F})$ — пространство магических $n \times n$ матриц.

Во введенных выше обозначениях условие магичности переписывается следующим образом: *матрица $A \in M_n(\mathbb{F})$ является магической тогда и только тогда, когда для всех $i, j = 1, \ldots, n$ справедливо*

$$\langle C_i, A\rangle = \langle R_j, A\rangle = \langle E, A\rangle = \langle J, A\rangle.$$

Легко видеть, что для любой константы $c \in \mathbb{F}$ условие $\langle R_n, A\rangle = c$ следует из условий

$$\langle C_i, A\rangle = \langle R_j, A\rangle = \langle E, A\rangle = \langle J,\ A\rangle = c,$$

где $i = 1, \ldots, n$; $j = 1, \ldots, n-1$.

Таким образом, матрица $A \in M_n(\mathbb{F})$ является магической тогда и только тогда, когда для всех $i = 1, \ldots, n$; $j = 1, \ldots, n-1$ справедливо

$$\langle C_i, A\rangle = \langle R_j, A\rangle = \langle E, A\rangle = \langle J, A\rangle. \tag{1}$$

В теореме 1 мы сведем эту систему к однородной и вычислим размерность пространства ее решений, как разность числа неизвестных и ранга матрицы коэффициентов.

Для начала докажем, что за исключением двух случаев, которые будут рассмотрены отдельно в лемме 2, матрица, строки которой — векторы C_i, R_j, E, J, имеет максимальный ранг, т. е. ее строки линейно независимы в $\mathbb{F}^{n^2}$.

[1]См. также статью Arno Van Den Essen, “Magic Squares and Linear Algebra”, American Mathematical Monthly, vol. 97, No. 1 (1990) 60–62.

Лемма 1. *Пусть $n \geqslant 3$. Тогда векторы $C_1, \ldots, C_n, R_1, \ldots, R_{n-1}, E, J$ линейно независимы в пространстве $\mathbb{F}^{n^2}$ за исключением случаев*

А) *$n = 3$ и $\operatorname{char} \mathbb{F} = 3$, или*

Б) *$n = 4$ и $\operatorname{char} \mathbb{F} = 2$.*

Доказательство. Предположим, что существуют такие константы $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_{n-1}, \gamma, \delta$, что

$$\alpha_1 C_1 + \ldots + \alpha_n C_n + \beta_1 R_1 + \ldots + \beta_{n-1} R_{n-1} + \gamma E + \delta J = 0.$$

Для удобства обозначений будем рассматривать эти векторы в виде матриц. Обозначим

$$X = (x_{i,j}) = \alpha_1 C_1 + \ldots + \alpha_n C_n + \beta_1 R_1 + \ldots + \beta_{n-1} R_{n-1} + \gamma E + \delta J = 0 \in M_n(\mathbb{F}).$$

1. Рассмотрим элементы $x_{n,2}, \ldots, x_{n,n-1}$. Равенство $x_{n,2} = \ldots = x_{n,n-1} = 0$ влечет равенство $\alpha_2 = \ldots = \alpha_{n-1} = 0$.
2. Тогда из $x_{1,2} = 0$ следует $\beta_1 = 0$.
3. Тогда из $x_{1,1} = x_{n,1} = x_{n,n} = 0$ следует $\alpha_1 + \gamma = \alpha_1 + \delta = \alpha_n + \gamma$, откуда $\alpha_1 = \alpha_n = -\gamma = -\delta$. Рассмотрим подслучаи.
   а) Если $\alpha_1 = 0$, то $\alpha_n = -\gamma = -\delta = 0$, следовательно $\beta_2 = \ldots = \beta_{n-1} = 0$, т.к. векторы $R_2, \ldots, R_{n-1}$ линейно независимы.
   б) Если $\alpha_1 \neq 0$, то, деля на ненулевое число, можно без ограничения общности предположить, что $\alpha_1 = 1$, откуда по п. 2 $\alpha_n = 1$, $\gamma = \delta = -1$.
      б.1). Теперь если $n > 4$, то, рассматривая элементы $x_{2,2}$ и $x_{2,3}$, получим, что
         (i) из $x_{2,2} = 0$ следует $\beta_2 - 1 = 0$, т. е. $\beta_2 = 1$, и
         (ii) из $x_{2,3} = 0$ следует $\beta_2 = 0$, что противоречит (i).
      Таким образом, при $n > 4$ случай б) не реализуется.
      б.2). Если $n = 4$, то из $x_{2,1} = 0$ следует, что $\beta_1 = -1$, а из $x_{2,2} = 0$ следует, что $\beta_2 = 1$ — противоречие, т. к. по условию $\operatorname{char} \mathbb{F} \neq 2$, значит случай б) опять не реализуется.
      б.3). Если $n = 3$, то вторая строка матрицы X имеет вид
      $$(\beta_2 + 1, \beta_2 - 2, \beta_2 + 1).$$
      Так как $X = 0$, это опять противоречит тому, что $\operatorname{char} \mathbb{F} \neq 3$.
   Таким образом, случай б) никогда не реализуется, т. е. векторы линейно независимы.

□

Рассмотрим матрицу коэффициентов системы (1) в двух оставшихся случаях.

Лемма 2.

1. *Пусть $n = 3$ и $\operatorname{char} \mathbb{F} = 3$. Тогда C_1, C_2, C_3, R_1, R_2, E линейно независимы над $\mathbb{F}$ и*
$$J = C_1 + C_3 - E - R_2.$$
2. *Пусть $n = 4$ и $\operatorname{char} \mathbb{F} = 2$. Тогда C_1, C_2, C_3, C_4, R_1, R_2, R_3, E линейно независимы над $\mathbb{F}$ и*
$$J = C_1 + C_4 + E + R_2 + R_3.$$

Доказательство мы оставляем читателю в качестве несложного упражнения. □

Теорема 1. *Пусть $n \geqslant 3$. Тогда $\dim \mathcal{M}_n = n^2 - 2n$ за исключением случая $n = 4$, $\operatorname{char} \mathbb{F} = 2$. В случае $\operatorname{char} \mathbb{F} = 2$ размерность $\dim \mathcal{M}_4 = 9$ $(= n^2 - 2n + 1)$.*

Доказательство. Случай 1. Рассмотрим сначала случаи $n > 4$ или $n = 4$ и $\operatorname{char} \mathbb{F} \neq 2$ или $n = 3$ и $\operatorname{char} \mathbb{F} \neq 3$.

Обозначим $B_i = C_i$, $i = 1, \ldots, n$, $B_{j+n} = R_j$, $j = 1, \ldots, n-1$, $B_{2n} = E$, $B_{2n+1} = J$. Обозначим $D_k = B_k - B_{k+1}$ $(k = 1, \ldots, 2n)$.

Легко видеть, что система уравнений (1) эквивалентна системе уравнений

$$\langle D_i, A \rangle = 0 \qquad (i = 1, \ldots, 2n).$$

По лемме 1 векторы $D_1, \ldots, D_{2n}$ линейно независимы над $\mathbb{F}$. Тогда по теореме о размерности пространства решений системы однородных линейных уравнений размерность пространства магических матриц есть разность числа неизвестных (n^2 коэффициентов матриц) и ранга матрицы коэффициентов, т.е. $n^2 - 2n$.

Случай 2. Рассмотрим случай $n = 3$ и $\operatorname{char} \mathbb{F} = 3$. Подставляя $J = C_1 + C_3 - E - R_2$ в систему (1), получаем, что $\langle J, A \rangle = 0$. Тогда система (1) преобразуется к виду:

$$\langle C_1, A \rangle = \langle C_2, A \rangle = \langle C_3, A \rangle = \langle R_1, A \rangle = \langle R_2, A \rangle = \langle E, A \rangle = 0.$$

Здесь 6 уравнений и они линейно независимы по лемме 2.1. Отсюда $\dim \mathcal{M}_n = 9 - 6 = 3 = n^2 - 2n$.

Случай 3. Рассмотрим случай $n = 4$ и $\operatorname{char}\mathbb{F} = 2$. Так как $J = C_1 + C_4 + E + R_2 + R_3$ по лемме 2.2, непосредственная проверка показывает, что величина $\langle J, A\rangle$ может быть произвольной в $\mathbb{F}$. Как и в случае 1, введем $B_i = C_i$, $i = 1, \ldots, 4$, $B_{j+4} = C_j$, $j = 1, 2, 3$, $B_8 = E$ и $D_i = B_{i+1} - B_i$, $i = 1, \ldots, 7$. Векторы D_i линейно независимы по лемме 2.2. Отсюда $\dim \mathcal{M}_4 = 16 - 7 = 9$. $\square$

Решение 2. Назовем магическую матрицу *c-магической*, если эти суммы равны c.

Лемма 3. *Над полем $\mathbb{F}$ все магические матрицы $n \times n$ являются 0-магическими тогда и только тогда, когда либо $n = \operatorname{char}\mathbb{F} = 2$, либо $n = \operatorname{char}\mathbb{F} = 3$.*

Доказательство. Вот примеры 1-магических матриц:

$$\begin{pmatrix}
\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}\\
0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}, \quad
\begin{pmatrix}
0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0\\
\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}\\
0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0
\end{pmatrix}, \quad
\frac{1}{3}\begin{pmatrix}1&1&1\\1&1&1\\1&1&1\end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix}1&1\\1&1\end{pmatrix}.$$

Первый пример[2] годится для любого поля и любого четного $n > 3$, второй пример — для любого поля и любого нечетного $n > 3$, третий пример подходит при $n = 3 \neq \operatorname{char}\mathbb{F}$, а четвертый пример — при $n = 2 \neq \operatorname{char}\mathbb{F}$.

В двух оставшихся исключительных случаях все магические матрицы являются 0-магическими, в силу следующих тождеств, справедливых для любой матрицы X:

$$\begin{aligned}
&\text{если } n = 2, \text{ то } J = R_1 + C_1 - 2x_{11},\\
&\text{если } n = 3, \text{ то } 2J = R_1 + R_3 + 2C_2 + 2E - 3(x_{12} + x_{32}).
\end{aligned} \tag{2}$$

Здесь и далее символы R_i, C_i, E и J обозначают сумму элементов i-й строки, i-го столбца, главной и побочной диагонали, соответственно. $\square$

Эта лемма показывает, что размерность пространства магических матриц на единицу больше размерности пространства 0-магических матриц, кроме случаев $n = \operatorname{char}\mathbb{F} = 2$ и $n = \operatorname{char}\mathbb{F} = 3$ (в которых эти размерности равны). В дальнейшем мы будем предполагать, что $n > 2$, одномерный и двумерный случаи тривиальны и мы оставляем их читателям.

Условия 0-магичности $R_i = 0$, $C_i = 0$, $E = 0$ и $J = 0$ представляют собой систему, состоящую из $2n+2$ линейных однородных уравнений. Между этими уравнениями есть очевидная линейная зависимость: $\sum R_i = \sum C_i$. Чтобы показать, что других зависимостей нет, достаточно построить матрицы $\mathbf{E}$, $\mathbf{J}$ и $\mathbf{S}_{ij}$, такие, что

– $\mathbf{E}$ удовлетворяет всем уравнениям, кроме $E = 0$;
– $\mathbf{J}$ удовлетворяет всем уравнениям, кроме $J = 0$;
– $\mathbf{S}_{ij}$ удовлетворяет всем уравнениям, кроме $R_i = 0$ и $C_j = 0$.

Построив матрицу $\mathbf{E}$, мы покажем, что уравнение $E = 0$ не следует из остальных, то есть никакая зависимость между уравнениями не включает в себя это уравнение. Матрица $\mathbf{J}$ имеет аналогичный смысл. А если нам удастся построить матрицы $\mathbf{S}_{ij}$, мы покажем, что каждая зависимость, включающая R_i, включает и C_j; комбинируя это с равенством $\sum R_i = \sum C_i$, мы получим, что R_i и C_j входят в каждую зависимость с противоположными коэффициентами. Отсюда будет вытекать, что $\sum R_i = \sum C_i$ — единственная зависимость (с точностью до пропорциональности).

[2]Можно ли расставить на шахматной доске шашки так, чтобы в каждом горизонтальном ряду, в каждом вертикальном ряду и на каждой из двух больших диагоналей стояло ровно по одной шашке?

Вот примеры матриц $\mathbf{E}$:

$$\begin{pmatrix}
\mathbf{1} & 0 & \mathbf{-1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\mathbf{-1} & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}, \quad \frac{1}{4}\begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}, \quad \frac{1}{3}\begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}.$$

Первый пример годится для любого поля при $n > 4$, второй — при $n = 4$ и $\operatorname{char}\mathbb{F} \neq 2$, третий — при $n = 3 \neq \operatorname{char}\mathbb{F}$. В случае $n = 3 = \operatorname{char} F$ такие примеры невозможны в силу тождества (2). В случае $n = 4$ и $\operatorname{char}\mathbb{F} = 2$ подобный пример также построить не удастся в силу следующего тождества, справедливого для любой матрицы X:

$$\text{если } n = 4, \text{ то } E = R_2 + R_3 + C_1 + C_4 + J - 2(x_{14} + x_{21} + x_{23} + x_{24} + x_{31} + x_{32} + x_{34} + x_{41}).$$

Матрицы $\mathbf{J}$ строятся аналогично (вы их увидите, если повернете эту книжку на $\frac{\pi}{2}$), а примеры матриц $\mathbf{S}_{ij}$ можно получить теперь совсем бесплатно:

$$\mathbf{S}_{ij} = \begin{cases} E_{ij} \text{ (матричная единица)}, & \text{если } i \neq j \neq n - i + 1; \\ E_{ij} - \mathbf{E}, & \text{если } i = j \neq n - i + 1; \\ E_{ij} - \mathbf{J}, & \text{если } i \neq j = n - i + 1; \\ E_{ij} - \mathbf{E} - \mathbf{J}, & \text{если } i = j = n - i + 1. \end{cases}$$

Таким образом, во всех случаях, кроме $n = 3 = \operatorname{char}\mathbb{F}$ и $n = 4 = 2\operatorname{char}\mathbb{F}$, пространство 0-магических матриц задается системой из $2n+1$ независимых однородных линейных уравнений от n^2 неизвестных и поэтому размерность этого пространства равна $n^2 - 2n - 1$. Размерность пространства всех магических матриц в этих ситуациях, как отмечалось, на единицу больше. Разобрать два исключительных случая мы предоставляем читателю.

Упражнение. Матрица называется *полумагической*, если суммы ее элементов в каждой строке и каждом столбце одинаковы. Найдите размерность пространства полумагических матриц. Докажите, что полумагические матрицы, в отличие от магических, образуют алгебру. Найдите минимальную систему порождающих этой алгебры.

Упражнение. Покажите, что в любой квадратной матрице A порядка большего двух над полем нулевой характеристики можно изменить (причем единственным образом) последнюю строку, последний столбец и элемент a_{11} и получить магическую матрицу.

Задача 2008–4

Покажите, что неравенство

$$\operatorname{rk}(MEX - MAT) > \operatorname{rk}(BMK),$$

где A, B, E, K, M, T, X — неизвестные матрицы 3×3 над полем из ста одного элемента, имеет больше решений, чем противоположное строгое неравенство. (*Предложил А. А. Клячко.*)

Решение. Идея доказательства состоит в том, что матрица $EX - AT$ бывает вырожденной реже, чем матрица BK. Под словом «матрица» здесь и далее понимается матрица 3×3 над полем из ста одного элемента.

Мы будем использовать вероятностную терминологию, но никаких знаний по теории вероятностей от читателей не требуется. Вероятности можно себе представлять просто как доли. Например, вероятность того, что произведение двух матриц вырождено, следует понимать как отношение числа таких пар матриц (A, B), что $|AB| = 0$, к общему числу пар матриц (то есть к 101^{18}).

Какова вероятность того, что случайная матрица вырождена? Эта вероятность a очень мала. Действительно, число невырожденных матриц задается формулой

$$|\mathbf{GL}_3(\mathbb{Z}_{101})| = (101^3 - 1)(101^3 - 101)(101^3 - 101^2),$$

так как первая строка невырожденной матрицы может быть любой ненулевой ($101^3 - 1$ возможностей); если первая строка уже выбрана, то вторая строка может быть любой непропорциональной первой ($101^3 - 101$ возможностей); если первые две строки выбраны, то третья строка может быть любой, не являющейся линейной комбинацией первых двух строк ($101^3 - 101^2$ возможностей). Поэтому вероятность того, что случайная матрица невырождена, очень велика:

$$1 - a = \frac{|\mathbf{GL}_3(\mathbb{Z}_{101})|}{101^9} = \frac{(101^3 - 1)(101^3 - 101)(101^3 - 101^2)}{101^9} =$$
$$= \left(1 - \frac{1}{101^3}\right)\left(1 - \frac{1}{101^2}\right)\left(1 - \frac{1}{101}\right) > \left(\frac{99}{100}\right)^3 \gg \frac{5}{6}.$$

Калькуляторный эксперимент показывает, что на самом деле $a < 0{,}01$, но нам достаточно ручной оценки $a < \frac{1}{6}$.

Какова вероятность того, что произведение двух случайных матриц вырождено? Произведение двух матриц невырождено тогда и только тогда, когда каждый из сомножителей невырожден. Следовательно, интересующая нас вероятность b может быть вычислена по формуле

$$b = 1 - (1 - a)^2 = 2a - a^2.$$

Какова вероятность того, что матрица $AB - CD$ вырождена? Для этой вероятности c нетрудно получить оценку

$$c < a + a^2.$$

Действительно, разобьем c в сумму трех слагаемых: $c = c_1 + c_2 + c_3$, где

- c_1 — вероятность того, что $|AB - CD| = 0$ и $|A| \neq 0$;
- c_2 — вероятность того, что $|AB - CD| = 0$, $\quad |A| = 0$ и $|C| \neq 0$;
- c_3 — вероятность того, что $|AB - CD| = 0$, $\quad |A| = 0$ и $|C| = 0$.

Найдем c_1. Домножая на невырожденную матрицу A^{-1}, мы получаем, что c_1 совпадает с вероятностью того, что $|B - A^{-1}CD| = 0$ и $|A| \neq 0$. Следовательно,

$$c_1 = a(1 - a).$$

Понимаете, почему?[3]

Аналогичным образом найдем c_2. Домножая на невырожденную матрицу C^{-1}, мы получаем, что c_2 совпадает с вероятностью того, что $|C^{-1}AB - D| = 0$, $|A| = 0$ и $|C| \neq 0$. Следовательно,

$$c_2 = a^2(1 - a)$$

по тем же причинам.

Что касается вероятности c_3, мы не будем крохоборствовать и скажем, что c_3 не превосходит вероятности одновременного вырождения матриц A и C, то есть $c_3 \leqslant a^2$.

Итого, общая вероятность вырождения матрицы $AB - CD$ оценивается так:

$$c = c_1 + c_2 + c_3 \leqslant a(1 - a) + a^2(1 - a) + a^2 = a + a^2 - a^3 < a + a^2.$$

Вооружившись этими знаниями, приступим теперь собственно к решению задачи. Для выполнения неравенства $\mathrm{rk}(MEX{-}MAT) > \mathrm{rk}(BMK)$ достаточно, чтобы матрицы M и $EX - AT$ были невырожденными, а матрица BK — вырожденной. Поэтому вероятность выполнения этого неравенства не меньше, чем

$$(1 - a)(1 - c)b > (1 - a)(1 - a - a^2)(2a - a^2) = a(1 - a - a^2)(1 - a)(2 - a).$$

Для выполнения противоположного строгого неравенства для рангов необходимо, чтобы матрица $EX - AT$ была вырожденной (поскольку иначе $\mathrm{rk}(MEX{-}MAT) = \mathrm{rk}(M) \geqslant \mathrm{rk}(BMK)$). Следовательно, вероятность выполнения нежелательного для нас строгого неравенства меньше c, то есть меньше, чем

$$a + a^2 = a(1 + a).$$

---

[3]Потому что между множествами четверок матриц

$$\{(A, B, C, D)\ ;\ |B - A^{-1}CD| = 0,\ |A| \neq 0\} \quad \text{и} \quad \{(A, B, C, D)\ ;\ |B| = 0,\ |A| \neq 0\}$$

есть взаимно однозначное соответствие $(A, B, C, D) \mapsto (A,\ B - A^{-1}CD,\ C,\ D)$, а вероятность попасть во второе множество, очевидно, равна $a(1 - a)$.

Осталось заметить, что

$$1 + a < (1 - a - a^2)(1 - a)(2 - a) = 2 - 5a + 2a^2 + 2a^3 - a^4$$

или, что то же самое,

$$1 - 6 + 2a^2 + 2a^3 - a^4 > 0.$$

Левая часть здесь больше, чем $1 - 6a$, поэтому все хорошо при $a < \frac{1}{6}$.

Упражнение. Исследуйте аналогичную задачу над произвольным конечным полем. Быть может, на очень маленьких полях наши друзья смогут нас победить?

Задача 2008–5

Пусть $f_1, \ldots, f_n$ и $g_1, \ldots, g_n$ — вещественные многочлены от одной переменной, такие, что $\sum\limits_{i=1}^{n} f_i g_i = 0$. Докажите, что найдутся такие многочлены $h_2, \ldots, h_n$, что

$$g_1 \;=\; h_2 \frac{f_2}{(f_1, f_2)} \;+\; \ldots \;+\; h_n \frac{f_n}{(f_1, f_n)}.$$

Верно ли аналогичное утверждение для многочленов от двух переменных? (*Предложил Е. С. Голод.*)

Решение 1. Сначала покажем, что g_1 делится на $d = \left(\frac{f_i}{(f_1, f_i)},\ i = 2, \ldots, n\right)$, а для этого докажем делимость g_1 на p^k — максимальную степень неприводимого многочлена p, входящего в упомянутый НОД. Если $k = 0$, то доказывать нечего. Пусть $k > 0$ и p входит в f_i с кратностью k_i. Тогда $k_i > k_1$ при $i \geqslant 2$ и

$$k = \min\{k_i - k_1,\ i = 2, \ldots, n\}.$$

Итак,

$$f_1 g_1 = -\sum_{i=2}^{n} f_i g_i \implies \left(\frac{f_1}{p^{k_1}}\right) g_1 = -\sum_{i=2}^{n} \left(\frac{f_i}{p^{k_1}}\right) g_i = -\sum_{i=2}^{n} \left(\frac{f_i}{p^{k_i}}\right) p^{k_i - k_1} g_i \implies p^k \mid g_1.$$

Так как d представляется в виде

$$d = \sum_{i=2}^{n} u_i \frac{f_i}{(f_1, f_i)}$$

для некоторых многочленов u_i, то и g_1 представляется в требуемом виде.

Для многочленов от двух переменных это утверждение неверно: пусть

$$f_1 = x + y,\ f_2 = x,\ f_3 = y.$$

Тогда $f_1 - f_2 - f_3 = 0$ и $(f_1, f_2) = (f_1, f_3) = 1$, но $1 \neq h_2 x + h_3 y$.

Решение 2. Приведем еще одно решение задачи, основанное на манипуляциях с идеалами в кольце многочленов. Пусть F — поле, I — идеал в $F[x]$ и f — некоторый многочлен. *Дробным идеалом* $I : f$ называется идеал $\{g \in F[x] \mid fg \in I\}$. Задачу можно сформулировать так: *доказать, что дробный идеал* $(f_2, \ldots, f_n) : f_1$ *содержится в идеале* $\left(\frac{f_2}{(f_1, f_2)}, \ldots, \frac{f_n}{(f_1, f_n)}\right)$.

Упражнение 1. Докажите, что $(g) : f = \left(\frac{g}{(f, g)}\right)$.

Пусть h — наибольший общий делитель многочленов $f_2, \ldots, f_n$. Тогда

$$(f_2, \ldots, f_n) : f_1 = (h) : f_1 = \left(\frac{h}{(f_1, h)}\right) = \left(\frac{f_2}{(f_1, h)}, \ldots, \frac{f_n}{(f_1, h)}\right) \subset \left(\frac{f_2}{(f_1, f_2)}, \ldots, \frac{f_n}{(f_1, f_n)}\right),$$

поскольку $(f_1, h) \mid (f_1, f_k)$.

Упражнение 2. Докажите, что последнее включение идеалов на самом деле является равенством.

Упражнение 3. Пусть идеал $I \cap (g)$ порождается многочленами $p_1, \ldots, p_s$. Найдите систему образующих идеала $I : g$.

Упражнение 4. Пусть I, J — идеалы в $F[x_1,\ldots,x_m]$. *Частным* идеалов $I:J$ называется идеал

$$\{g\in F[x_1,\ldots,x_m]\mid fg\in I\;\forall\, f\in J\}.$$

Докажите следующие равенства:

$$\left(\bigcap_{i=1}^{r} I_i\right):J=\bigcap_{i=1}^{r}(I_i:J),$$

$$I:\left(\sum_{i=1}^{r} J_i\right)=\bigcap_{i=1}^{r}(I:J_i),$$

$$(I:J):K=I:JK.$$

Задача 2008–6

Назовем конечную абелеву группу *уравновешенной*, если сумма всех ее элементов равна нулю. Каких абелевых групп порядка $\leqslant 2008$ больше: уравновешенных или неуравновешенных? (*Предложил А. А. Клячко.*)

Решение. Конечные абелевы группы при решении этой задачи мы будем для краткости называть просто группами. Уравновешенных групп гораздо больше. Действительно,

$$\sum_{g\in G} g=\sum_{g\in G}(-g)=-\sum_{g\in G} g,\quad \text{значит,}\quad 2\sum_{g\in G} g=0.$$

Следовательно, *все группы нечетного порядка уравновешены, а группы четного порядка становятся уравновешенными после прибавления группы порядка два*:

$$\sum_{x\in\mathbb{Z}_2\oplus G} x\;=\sum_{a\in\mathbb{Z}_2,\,g\in G}(a,g)=\left(|G|,\;2\sum_{g\in G} g\right)=(0,0).$$

Стало быть, каждой неуравновешенной группе G порядка $\leqslant 2008$ мы можем сопоставить уравновешенную группу $f(G)$ порядка $\leqslant 2008$ по правилу

$$f(G)=\begin{cases}2G, & \text{если } |2G| \text{ нечетный;}\\ 2G\oplus\mathbb{Z}_2, & \text{если } |2G| \text{ четный.}\end{cases}\qquad \text{Здесь } 2G:=\{2g\mid g\in G\}.$$

Из однозначности разложения в прямую сумму примарных циклических следует, что неуравновешенная группа G однозначно восстанавливается по группе $2G$: если $2G\simeq H$ и $|G|\geqslant|H|$, то $G\simeq H\oplus\mathbb{Z}_2\oplus\cdots\oplus\mathbb{Z}_2$, но тогда неуравновешенной может быть только одна из этих групп (если $G\not\simeq H$). Значит, соответствие f инъективно и неуравновешенных групп не больше, чем уравновешенных. Осталось заметить, что группы порядка 2008 (которые все уравновешены) не лежат в образе отображения f, поскольку если $|2G|=2008$, то $|G|$ либо равен 2008 (и тогда G уравновешена), либо слишком велик.

Упражнение 1. Сформулируйте и докажите критерий уравновешенности на языке разложения в прямую сумму примарных циклических.

Упражнение 2. Покажите, что $\mathbb{Z}_2\times G\simeq\mathbb{Z}_2\times H\implies G\simeq H$ для любых конечных групп G и H, не обязательно абелевых. Более того, $\mathbb{Z}_2$ здесь также можно заменить на любую конечную группу (теорема Ремака–Шмидта).

Задача 2008–7

Помогите доценту Н. Е. Нормальному доказать следующий важный результат.

Теорема 3. *Если группа содержит ровно 3 ненормальные подгруппы, то ее порядок делится на 3.*

Можно ли тройки в этом утверждении заменить на двойки? А на четверки? (*Предложил А. А. Клячко.*)

Решение. Рассмотрим действие группы на множестве всех своих подгрупп сопряжениями. Орбита ненормальной подгруппы не может состоять из одной точки. Следовательно, в условиях теоремы 3 все три ненормальные подгруппы сопряжены. Значит, нормализатор (то есть стабилизатор при этом действии) каждой из этих подгрупп имеет индекс 3 и, стало быть, тройка делит порядок группы. В случае, когда имеется ровно две ненормальные подгруппы, ситуация полностью аналогичная.

С четверками дело обстоит немного сложнее. Может случиться, что множество из четырех ненормальных подгрупп разбивается на две орбиты длины два. Допустим, что порядок группы не делится на четыре. Нормализатор каждой из четырех ненормальных подгрупп имеет индекс 2; следовательно, все четыре нормализатора совпадают, поскольку пересечение двух различных подгрупп индекса 2 имеет индекс 4. (Докажите!) Порядок этого общего нормализатора N нечетный (иначе порядок группы делился бы на 4). Порядок каждого элемента y, не лежащего в N, четный (понимаете, почему?). Следовательно, некоторая степень $y^k = x \notin N$ имеет порядок 2. Значит, $G = N \cup xN$. Но подгруппа N нормализует все и, в частности, циклическую подгруппу $\langle x \rangle_2$, а это означает, что x — центральный элемент и, значит, тоже нормализует все, то есть содержится в N. Это противоречие показывает, что гипотетическая теорема 4 доцента Н. Е. Нормального тоже верна.

Упражнение 1. Существуют ли группы, о которых идет речь в этой задаче, то есть группы, содержащие ровно 2, 3 или 4 ненормальные подгруппы?

Упражнение 2. Что вы думаете о будущей теореме 5 доцента Н. Е. Нормального?

Задача 2008–8

Покажите, что для вещественных матриц A справедлива импликация $A^{2008} = A^\top \Longrightarrow A^{2010} = A$. (*Предложил А. А. Клячко.*)

Решение. Допустим, что вещественная матрица A удовлетворяет уравнению $A^{2008} = A^\top$. Транспонируя это равенство, мы получаем, что $\left(A^\top\right)^{2008} = A$ и, следовательно, $A^{2008^2} = A$. Таким образом, аннулирующий многочлен $x^{2008^2} - x$, соответствующего оператора $\mathcal{A}$ не имеет кратных корней и, следовательно, этот оператор диагонализируем (над $\mathbb{C}$).

Умножая исходное равенство $A^{2008} = A^\top$ на A, мы приходим к выводу, что $A^{2009} = A^\top A$. В правой части здесь стоит матрица неотрицательно определенного симметрического оператора. Значит, 2009-е степени собственных значений оператора $\mathcal{A}$ вещественны и неотрицательны. Поскольку эти собственные значения λ_k являются корнями аннулирующего многочлена $x^{2008^2} - x$, мы видим, что $\lambda_k^{2009} \in \{0, 1\}$. Следовательно, $\lambda_k^{2010} = \lambda_k$ и $A^{2010} = A$ (поскольку $\mathcal{A}$ диагонализируем).

Упражнение. Покажите, что пространство, на котором действует оператор из этой задачи, раскладывается в прямую сумму двух взаимно ортогональных $\mathcal{A}$-инвариантных подпространств, на одном из которых $\mathcal{A}$ действует как ортогональный оператор, а на другом — как нулевой.