XXVIII
Межрегиональная олимпиада школьников им. И.Я.Верченко по математике и криптографии

УСЛОВИЯ И РЕШЕНИЯ

Москва 2019

9 КЛАСС

УСЛОВИЯ ЗАДАЧ

1. Каждому набору $(x_1,x_2,x_3,x_4,x_5)(\text{где } x_i\in\{0,1\})$ функция $f(x_1,x_2,x_3,x_4,x_5)$ ставит в соответствие либо 0, либо 1. Условимся значения 0 и 1 называть *противоположными*. Известно, что если в произвольном наборе (x_1,x_2,x_3,x_4,x_5) изменить значение x_1 или x_5 на противоположное, то и соответствующее значение функции $f(x_1,x_2,x_3,x_4,x_5)$ изменится на противоположное. Последовательность $x_1,x_2,\ldots$ получена по правилу:

$$x_1=x_2=x_3=x_4=x_5=0,$$
$$x_{k+5}=f(x_k,x_{k+1},x_{k+2},x_{k+3},x_{k+4}),k=1,2,\ldots$$

Найдите x_{14}, если известны первые 13 членов этой последовательности: 0000010110011. Ответ обоснуйте.

2. Для зашифрования слова из пяти букв каждая его буква заменяется на число согласно таблице.

					Е Ё																							
					5				0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0

Полученный набор чисел (x_0,x_1,x_2,x_3,x_4) затем преобразуется в набор (y_0,y_1,y_2,y_3,y_4) по следующему правилу. Сначала вычисляют вспомогательные числа $\acute{y}_0,\acute{y}_1,\acute{y}_2,\acute{y}_3,\acute{y}_4$ по формулам

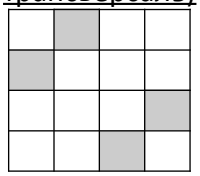
$$\acute{y}_0=2^0\cdot x_0+2^4\cdot x_1+2^3\cdot x_2+2^2\cdot x_3+2^1\cdot x_4,$$
$$\acute{y}_k=\left(2^k\cdot x_0+2^{k-1}\cdot x_1+\ldots+2^0\cdot x_k\right)+\left(2^4\cdot x_{k+1}+2^3\cdot x_{k+2}+\ldots+2^{k+1}\cdot x_4\right),k=1,2,3.$$
$$\acute{y}_4=2^4\cdot x_0+2^3\cdot x_1+2^2\cdot x_2+2^1\cdot x_3+2^0\cdot x_4.$$

А затем полагают y_k равным остатку от деления числа $\acute{y}_k$ на 32. Расшифруйте исходное слово, если $(y_0,y_1,y_2,y_3,y_4)=(11,27,2,16,0)$.

Доска с зернами

1	7	2	5
4	5	4	2
2	1	5	7
8	2	4	1

Пример (серые клетки образуют трансверсаль)



Пример (серые клетки **не** образуют трансверсаль)

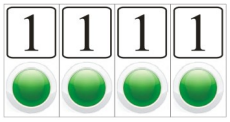
3. В каждую клетку доски 4×4 Аня положила по нескольку зерен и передала доску Боре (см. рис.). *Трансверсалью* доски называется набор из 4 клеток, любые две из которых расположены в разных строках и разных столбцах (см. примеры). Боря за один ход может снять одинаковое количество зерен с каждой клетки какой-либо одной трансверсали. За какое минимальное число ходов Боря может снять все зерна с доски?

4. Ваня покрасил n точек числовой прямой с координатами $a_1=1,a_2=a_1+2=3,\ldots,a_n=a_{n-1}+n$ в белый цвет, а остальные точки из отрезка $[a_1,a_n]$ с целыми координатами – в синий. Какое максимальное количество отрезков разной длины, один из концов которого белый, а другой – синий, он сможет построить?

А	Б	В	Г	Д	Е,Ё	Ж	З	И, Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь, Ъ	Э	Ю	Я
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

5. Для зашифрования слова каждая его буква заменяется на двухзначное число согласно таблице. Затем выбираются секретные ключи K_1,K_2 – натуральные числа от 1 до 9. С их помощью каждое двузначное число преобразуется так. Пусть A – первая цифра двузначного числа, B – его вторая цифра. Двузначное число (A,B) преобразуется в число (A_1,B_1) по формулам $A_1=B,B_1=r_{10}(A+K_1\cdot B)$. Здесь $r_{10}(x)$ – остаток от деления числа x на 10. Затем

число (A_1, B_1) преобразуется в число (A_2, B_2) по аналогичным формулам, но только вместо ключа K_1 используется ключ K_2. Далее каждое исходное двузначное число (A, B) было заменено числом (A_2, B_2). В результате получилось вот что: **59 28 77 64 95 64 90 41 64**. Восстановите исходное слово.



6. При входе в личный кабинет на терминале требуется ввести четырехзначный пароль из 0 и 1. Для этого на терминале имеются 4 кнопки и 4 окошка. При нажатии на кнопку в ей соответствующем окошке текущий символ заменяется на противоположный (то есть если в окошке сейчас горит цифра 1, то после нажатия на кнопку там будет 0, и наоборот). Сейчас во всех окошках выставлена 1. Какое наименьшее количество нажатий кнопок потребуется, чтобы перебрать все возможные варианты пароля?

РЕШЕНИЯ ЗАДАЧ

Задача 1

По условию, $x_{14}=f(1,0,0,1,1)$. Изменим первый и пятый аргумент на противоположные, в результате значение функции останется прежним, т.е. $x_{14}=f(0,0,0,1,0)$. Но в условии после набора 00010 идет 1. Значит $x_{14}=1$.

Ответ: 1.

Задача 2

Заметим, что для $k=0,1,2,3$ справедливо равенство $2\acute{y}_k - y'_{k+1} = 31x_{k+1}$. Кроме того $2\acute{y}_4 - \acute{y}_0 = 31x_0$. Числа 31 и (-1) при делении на 32 дают один и тот же остаток 31, то есть $31 = r_{32}(31) = r_{32}(-1)$. (Здесь традиционно $r_{32}(x)$ – остаток от деления числа x на 32.) Значит $r_{32}(31x_{k+1}) = r_{32}(-x_{k+1})$ и $r_{32}(31x_0) = r_{32}(-x_0)$. В результате получаем формулы, непосредственно выражающие искомые числа x_0, x_1, x_2, x_3, x_4 через данные в условии y_0, y_1, y_2, y_3, y_4:

$$r_{32}(2\acute{y}_k - y'_{k+1}) = r_{32}(31x_{k+1}) = r_{32}(-x_{k+1}) \Rightarrow x_{k+1} = r_{32}(y'_{k+1} - 2\acute{y}_k) = r_{32}(y_{k+1} - 2y_k),$$
$$x_0 = r_{32}(\acute{y}_0 - 2\acute{y}_4) = r_{32}(y_0 - 2y_4).$$

Отсюда находим $(x_0, x_1, x_2, x_3, x_4) = (11,5,12,12,0)$. Зашифрованное слово – ЛЕММА.

Ответ: ЛЕММА.

Задача 3

За один ход Боря может освободить не более 4 клеток. Следовательно, ему придется сделать *минимум* 4 хода (так как изначально среди 16 клеток нет ни одной пустой). Заметим, что есть клетка с 8 зернами, а в остальных клетках зерен меньше. Значит с этой клетки зерна придется снимать минимум дважды. Поэтому за 4 хода Боря не справится.

Покажем как снять все зерна за 5 ходов (серым отмечены трансверсали, с которых сняли зерна):

Ответ: За **5** ходов.

Задача 4

Пусть N – искомое количество отрезков. Вначале найдем N для $n=2,3,4$.

n	Целые числа отрезка $[a_1,a_n]$. (Числа a_k выделены жирным.)	Отрезки с разноцветными концами различной длины	Искомое количество отрезков N
2	**1** 2 **3**	[**1**,2]	1
3	**1** 2 **3** 4 5 **6**	[**1**,2], [**3**,5], [**1**,4], [**1**,5]	4
4	**1** 2 **3** 4 5 **6** 7 8 9 **10**	[**1**,2], [**3**,5], [**1**,4], [**1**,5],[**3**,8], [**1**,7], [**1**,8], [**1**,9]	8

Сделанные наблюдения позволяют предположить, что $N=a_n-2$. То есть при фиксированном n имеются отрезки с разноцветными концами любой длины от 1 до a_n-2 включительно. Докажем это, предполагая $n>2$. Заметим, что отрезок длины a_n-1 построить невозможно, так как точки a_1 и a_n одного цвета. Значит $N\le a_n-2$. Отрезки длины 1 и a_n-2, очевидно, построить можно – это отрезки $[1,2]$ и $[1,a_n-1]$. Покажем, что для любого натурального m такого, что $1<m<a_n-2$, существует отрезок с разноцветными концами длины m. Действительно, рассмотрим отрезки длины m вида $[a_1,a_1+m]$ и $[a¿¿2,a_2+m]¿$. Их левые концы окрашены в белый цвет. При этом их правые концы a_1+m и a_2+m находятся друг от друга на расстоянии 2, а значит оба окрашенными в белый цвет они быть не могут, так как, по условию, расстояние между соседними белыми точками увеличивается с ростом n, и на расстоянии 2 друг от друга лежат только две белые точки $a_1=1$ и $a_2=3$. Значит, хотя бы один из отрезков $[a_1,a_1+m]$, $[a¿¿2,a_2+m]¿$ имеет концы разных цветов. Таким образом, формула $N=a_n-2$ доказана. Осталось получить явную зависимость a_n от n. Для этого данные в условии равенства $a_1=1,a_2=a_1+2=3,\ldots,a_n=a_{n-1}+n$ сложим между собой. В результате получим

$$a_1+\ldots a_{n-1}+a_n=a_1+\ldots a_{n-1}+1+\ldots+n \Leftrightarrow a_n=1+\ldots+n=\frac{n(n+1)}{2}.$$

Ответ: $\frac{n(n+1)}{2}-2$.

Задача 5

Если решать задачу перебором, то придется проверить 81 пару ключей (K_1,K_2). Чтобы перебор уменьшить, воспользуемся тем, что цифра A может принимать только значения 0, 1, 2, 3. Для этого выразим A (а заодно и B) через A_2,B_2,K_1,K_2. По условию

$$\begin{cases} A_1=B \\ B_1=A+K_1\cdot B \end{cases} и \begin{cases} A_2=B_1 \\ B_2=A_1+K_2\cdot B_1. \end{cases} (1)$$

(Здесь и далее условимся для краткости вместо $r_{10}(x)=y$ писать просто $x=y$, то есть равными для нас будут числа, дающие одинаковый остаток при делении на 10; например, $8=-2$). Отсюда

$$\begin{matrix} A=A_2\cdot(1+K_1K_2)-K_1.B_2,(2) \\ B=B_2-K_2\cdot A_2(3) \end{matrix}$$

Заметим сразу, что $A\ne 3$. Так как, если $A=3$, то $B=0$ (с цифры 3 начинается только буква Я). Тогда, согласно (1), $A_2=B_1=A=3$, но среди цифр A_2 троек нет.

Итак, $A\in\{0,1,2\}$. Следовательно, цифры каждого из чисел **59 28 77 64 95 64 90 41 64** удовлетворяют (согласно (2)) одному из следующих равенств:

$$\begin{cases} 0 = A_2 \cdot (1 + K_1 K_2) - K_1 . B_2, \\ 1 = A_2 \cdot (1 + K_1 K_2) - K_1 . B_2, \\ 2 = A_2 \cdot (1 + K_1 K_2) - K_1 . B_2. \end{cases} \quad (4)$$

Подставим в эти равенства цифры числа **90** из шифртекста: $A_2 = 9, B_2 = 0 \Rightarrow 9(1 + K_1 K_2) \in \{0,1,2\}$. Равенство $9(1 + K_1 K_2) = 0$ невозможно, так как в этом случае $1 + K_1 K_2 = 0$. Следовательно, K_1 нечетно, но тогда для $B_2 = 5$(число **95** из шифртекста) произведение $K_1 . B_2 = 5$, а в левых частях (4) пятерки нет. Поэтому возможны только два случая 1) $9(1 + K_1 K_2) = 1$ или 2) $9(1 + K_1 K_2) = 1$. Рассмотрим их подробнее:

1 случай) $9(1 + K_1 K_2) = 1 \Rightarrow 1 + K_1 K_2 = 9 \Rightarrow K_1 K_2 = 8$. Соотношения (4) принимают вид:

$$\begin{cases} 0 = 9 A_2 - K_1 . B_2, \\ 1 = 9 A_2 - K_1 . B_2, \\ 2 = 9 A_2 - K_1 . B_2. \end{cases} \quad (5)$$ Подставив в эти соотношения цифры числа **64**, получим, что

$4 - 4 K_1 = 0$ *либо* $4 - 4 K_1 = 2$ (6) Для числа **59** из (5) найдем, что $K_1 \in \{5,6,7\}$. Значения 5 и 7 не годятся, так как они не удовлетворяют ни одному из равенств (6). Таким образом, $K_1 = 6$ и, так как $K_1 K_2 = 8$, то $K_2 = 3$ *или* 8.

2 случай) $9(1 + K_1 K_2) = 2 \Rightarrow 1 + K_1 K_2 = 8 \Rightarrow K_1 K_2 = 7$. Соотношения (4) принимают вид:

$$\begin{cases} 0 = 8 A_2 - K_1 . B_2, \\ 1 = 8 A_2 - K_1 . B_2, \\ 2 = 8 A_2 - K_1 . B_2. \end{cases}$$

Для числа **59** получаем, что $9 K_1 \in \{0,8,9\}$. Значит $K_1 \in \{1,2\}$. Вариант $K_1 = 2$ не годится, так как K_1 нечетно (из-за того, что $K_1 K_2 = 7$). Окончательно $K_1 = 1, K_1 = 7$.

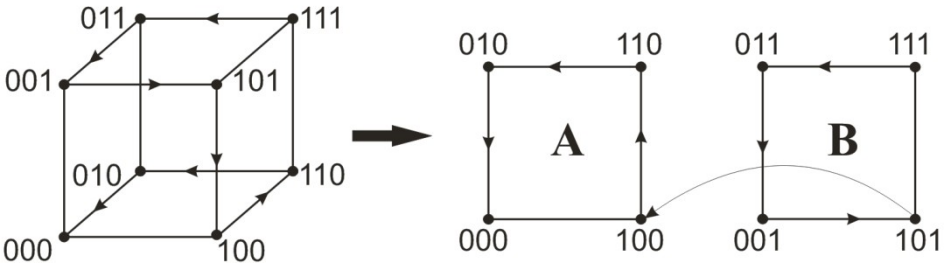
Для каждой из найденных пар ключей $(K_1, K_2) \in \{(1,7),(6,3),(6,8)\}$ по формулам (2), (3) восстановим исходный текст. Осмысленное слово ОБРЕТЕНИЕ получится для пары (6,3).

Ответ: ОБРЕТЕНИЕ.

Задача 6

Всего имеется $16 = 2^4$ четырехзначных паролей из 0 и 1. Один такой пароль 1111 уже набран, значит нам остается перебрать оставшиеся 15 вариантов, для чего потребуется по крайней мере 15 нажатий кнопок. Покажем, что 15 нажатий действительно хватит. Для этого все четырехзначные наборы упорядочим так, чтобы соседние наборы отличались только в одном символе (классический *код Грея*). Тогда переход от одного набора к соседнему будет осуществляться нажатием одной кнопки, и всего потребуется как раз 15 нажатий.

Упорядочить так наборы можно многими способами. Одну из возможных идей проиллюстрируем на примере трехзначных паролей, которые будем интерпретировать как координаты вершин трехмерного куба со стороной 1. Координаты вершин, лежащих на одном ребре, как раз отличаются только в одном символе. Значит, если, двигаясь вдоль ребер, мы обойдем все вершины куба, то тем самым получим требуемое упорядочение. Отметим, что все вершины лежат или на верхней **A**, или на нижней грани **B**. То есть, можно сказать, что наш трехмерный куб представляет собой сумму двух граней (или *двухмерных кубов*) **A** и **B**. Начнем обход, например, с вершины 111. Сначала обойдем вершины двумерного куба **B** (при этом последняя цифра пароля (координата z) равна 1), затем переместимся на куб **A** и обойдем его вершины. Получим искомую последовательность паролей: **111 011 001 101 100 110 010 000**.



Несложно теперь проделать тоже самое и для четырехзначных паролей (четырехмерный куб равен сумме двух трехмерных): 1) сначала обходим двухмерный куб, т.е. меняются первые две цифры, а две последние так и остаются равными 1: **1111 0111 0011 1011**. Переходим на вторую грань: теперь третья цифра 0, а последняя по-прежнему 1: **1001 1101 0101 0001**. Обход одного трехмерного куба закончили. Переходим на второй трехмерный куб: **0000 0100 1100 1000 1010 0010 0110 1110**.

Ответ: 15 нажатий. Пароли можно перебирать, например, в таком порядке:
1111 0111 0011 1011 1001 1101 0101 0001 0000 0100 1100 1000 1010 0010 0110 1110.