10 класс XXVIII МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ
(сайт олимпиады www.cryptolymp.ru) 25.11.2018

1 вариант

1. Каждому набору $(x_1, x_2, x_3, x_4, x_5)$ (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 1) 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 и 2) если в произвольном наборе $(x_1, x_2, x_3, x_4, x_5)$ изменить *одновременно* значения x_2, x_3 и x_4 на противоположные, то 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_{12}, если известны первые 11 членов этой последовательности: 00000100111. Ответ обоснуйте.

Решение: По условию, $x_{12} = f(0,0,1,1,1)$. Изменим второй, третий и четвертый аргумент на противоположные, тогда значение функции изменится на противоположное, т.е. значения x_{12} и $f(0,1,0,0,1)$ противоположны. Но в условии после набора 01001 идет 1. Значит $x_{12} = 0$.

Ответ: 0.

2. Для зашифрования слова из пяти букв каждая его буква заменяется на число согласно таблице. 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 $\overline{y_0}, \overline{y_1}, \overline{y_2}, \overline{y_3}, \overline{y_4}$ по формулам

$$\overline{y_0} = 2^0 \cdot x_0 + 2^4 \cdot x_1 + 2^3 \cdot x_2 + 2^2 \cdot x_3 + 2^1 \cdot x_4,$$

$$\overline{y_k} = \left(2^k \cdot x_0 + 2^{k-1} \cdot x_1 + \cdots + 2^0 \cdot x_k\right) + \left(2^4 \cdot x_{k+1} + 2^3 \cdot x_{k+2} + \cdots + 2^{k+1} \cdot x_4\right),\ k = 1,2,3.$$

$$\overline{y_4} = 2^4 \cdot x_0 + 2^3 \cdot x_1 + 2^2 \cdot x_2 + 2^1 \cdot x_3 + 2^0 \cdot x_4.$$

А затем полагают y_k равным остатку от деления числа $\overline{y_k}$ на 32. Расшифруйте исходное слово, если $(y_0, y_1, y_2, y_3, y_4) = (7,22,25,5,27)$.

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	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Решение: Заметим, что для $k = 0,1,2,3$ справедливо равенство $2\overline{y_k} - \overline{y_{k+1}} = 31x_{k+1}$. Кроме того $2\overline{y_4} - \overline{y_0} = 31x_0$. 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:

$r_{32}(2\overline{y_k} - \overline{y_{k+1}}) = r_{32}(31x_{k+1}) = r_{32}(-x_{k+1}) \Rightarrow x_{k+1} = r_{32}(\overline{y_{k+1}} - 2\overline{y_k}) = r_{32}(y_{k+1} - 2y_k), k = 0,1,2,3.$

Аналогично, $x_0 = r_{32}(\overline{y_0} - 2\overline{y_4}) = r_{32}(y_0 - 2y_4)$.

Отсюда находим $(x_0, x_1, x_2, x_3, x_4) = (17,8,13,19,17)$. Зашифрованное слово – СИНУС.

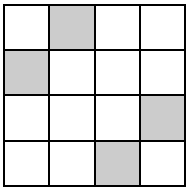
Ответ: СИНУС.

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?

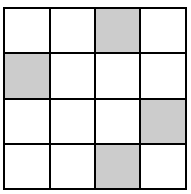
Доска с зернами

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

Пример (серые клетки образуют трансверсаль)



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



Решение: 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 7 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 зерна за 5 ходов (серым отмечены трансверсали, с которых сняли зерна):

1	5	5	0
2	0	4	5
5	1	0	5
3	5	2	1

1	5	0	0
2	0	4	0
0	1	0	5
3	0	2	1

1	3	0	0
0	0	4	0
0	1	0	3
3	0	0	1

0	3	0	0
0	0	3	0
0	0	0	3
3	0	0	0

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Ответ: За **5** ходов.

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

4. 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. Двухзначное 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: **49 97 32 20 52 77 20 37 85 72**. Восстановите исходное слово.

Решение: 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

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

(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

$$A = A_2 \cdot (1 + K_1 K_2) - K_1 . B_2, \qquad (2)$$

$$B = B_2 - K_2 \cdot A_2 \qquad (3)$$

Поскольку $A \in \{0,1,2,3\}$, цифры каждого из чисел **49 97 32 20 52 77 20 37 85 72** удовлетворяют (согласно (2)) одному из следующих четырех равенств:

$$\begin{cases} 0 = A_2 \cdot (1 + K_1 K_2) - K_1 . B_2, \\ \vdots \\ 3 = A_2 \cdot (1 + K_1 K_2) - K_1 . B_2. \end{cases} \qquad (4)$$

a) Подставим в эти равенства цифры числа **20** из шифртекста: $A_2 = 2, B_2 = 0 \Rightarrow 7(1 + K_1 K_2) \in \{0,2\} \Rightarrow 1 + K_1 K_2 \in \{0,1,5,6\}$.

b) Подставив в соотношения (4) цифры числа **77**: $7(1 + K_1 K_2 - K_1) \in \{0,1,2,3\} \Rightarrow$

$$1 + K_1 K_2 - K_1 \in \{0,3,6,9\}. \qquad (5)$$

c) Аналогично для **52**:

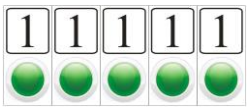
$$5(1 + K_1 K_2) - 2K_1 \in \{0,1,2,3\}. \qquad (6)$$

Теперь для каждого значения суммы $1 + K_1 K_2$, указанного в пункте а), найдем с помощью (5) соответствующее значение K_1, а потом для пары $1 + K_1 K_2$ и K_1 проверим справедливость (6).

- $1 + K_1 K_2 = 0$. Из (5) $\Rightarrow K_1 \in \{0,1,4,7\}$. Значения 0 и 4 не годятся, так как произведение $K_1 K_2$ сейчас нечетно. Значение 7 не удовлетворяет (6). В итоге нашли одну возможную пару ключей $(K_1, K_2) = (1,9) \in \{(1,9), (7,3), (6,8)\}$.
- $1 + K_1 K_2 = 1$. Из (5) $\Rightarrow K_1 \in \{1,2,5,8\}$. Значения 1 и 5 очевидно не годятся (не выполнится равенство $1 + K_1 K_2 = 1$). Возможные пары ключей $(K_1, K_2) \in \{(2,5), (8,5)\}$. Пара (8,5) не удовлетворяет (6).
- $1 + K_1 K_2 = 5$. Из (5) $\Rightarrow K_1 \in \{2,5,6,9\}$. Значение 5 очевидно не годится (не выполнится равенство $1 + K_1 K_2 = 5$). Возможные пары ключей $(K_1, K_2) \in \{(2,2), (2,7), (9,6), (6,4), (6,9)\}$. Условию (6) удовлетворяют только пары (2,2) и (2,7).
- $1 + K_1 K_2 = 6$. Из (5) $\Rightarrow K_1 \in \{0,3,6,7\}$. Значение 0 и 6 очевидно не годятся (не выполнится равенство $1 + K_1 K_2 = 6$). Оставшиеся возможные пары ключей $(K_1, K_2) \in \{(3,5), (7,5)\}$ обе не удовлетворяют (6).

Таким образом предстоит рассмотреть следующие три пары ключей (K_1, K_2): (1,9), (2,5), (2,2) и (2,7). Для них по формулам (2), (3) восстановим исходный текст. Осмысленное слово ХОЛЕСТЕРИН получится для пары (2,7).

Ответ: ХОЛЕСТЕРИН.

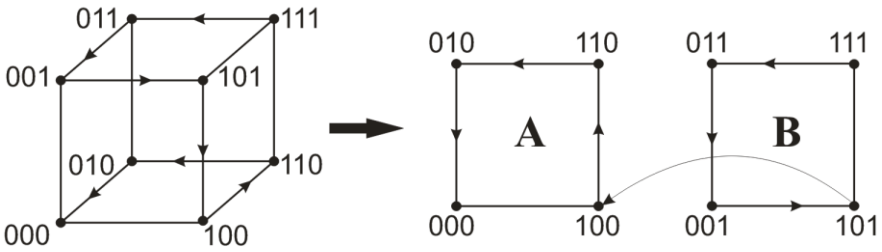
5. 

При входе в личный кабинет на терминале требуется ввести пятизначный пароль из 0 и 1. Для этого на терминале имеются 5 кнопок и 5 окошек. 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?

Решение: Всего имеется $32 = 2^5$ пятизначных паролей из 0 и 1. Один такой пароль 11111 уже набран, значит нам остается перебрать еще 31 вариант, для чего потребуется по крайней мере 31 нажатие кнопок. Покажем, что 31 нажатия действительно хватит. Для этого все пятизначные 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 31 нажатие.

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** (рис.). 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 пятизначных паролей (пятимерный куб равен сумме двух четырехмерных кубов, а четырехмерный куб равен сумме двух трехмерных): 1) сначала обходим двухмерный куб, т.е. меняются первые две цифры, а три последние так и остаются равными 1:



11111 01111 00111 10111. Переходим на вторую грань: теперь третья цифра 0, а последние две по-прежнему 1: **10011 11011 01011 00011**. Обход одного трехмерного куба закончили. Переходим на второй трехмерный куб (предпоследняя цифра стала 0): **00001 01001 11001 10001 10101 00101 01101 11101**. Один четырехмерный куб обошли. Переходим на второй четырехмерный куб, то есть, наконец, последняя цифра становится 0: **11100 01100 00100 10100 10000 11000 01000 00000 00010 01010 11010 10010 10110 00110 01110 11110.**

Ответ: 31 нажатие. Пароли можно перебирать, например, в таком порядке:
11111 01111 00111 10111 10011 11011 01011 00011 00001 01001 11001 10001 10101 00101 01101 11101
11100 01100 00100 10100 10000 11000 01000 00000 00010 01010 11010 10010 10110 00110 01110 11110.

6. Про числа A и B известно следующее: 1) $A = p_1^2 \cdot p_2^2$, где p_1 и p_2 – различные простые числа, 2) $B = q^2, q \in \mathbb{N}$, 3) $B - A = 36^2$. Найдите все такие A и B.

Решение: Пусть $p_1 < p_2$. По условию $B - A = 36^2 \Leftrightarrow q^2 - p_1^2 p_2^2 = 36^2 \Leftrightarrow (q - 36)(q + 36) = p_1^2 p_2^2$. Значит, разложения на простые множители чисел $q - 36$ и $q + 36$ содержат только степени чисел p_1 и p_2. Кроме того, число $q - 36$ меньше, чем $q + 36$. Следовательно, возможны только три случая:

1) $q - 36 = 1,\ q + 36 = p_1^2 p_2^2$. Тогда $q = 37$ и $p_1^2 p_2^2 = 73$, что невозможно.
2) $q - 36 = p_1,\ q + 36 = p_1 p_2^2$. Следовательно, $p_1(p_2^2 - 1) = 72$. Или $p_1 = 2$ и $p_2^2 = 37$, что неверно, или $p_1 = 3$ и $p_2 = 5$.
3) $q - 36 = p_1^2,\ q + 36 = p_2^2$. Отсюда $(p_2 - p_1)(p_2 + p_1) = 72$. Представить число 72 в виде произведения двух множителей, первый из которых меньше второго, можно так: $72 = 1 \cdot 72 = 2 \cdot 36 = 3 \cdot 24 = 4 \cdot 18 = 6 \cdot 12 = 8 \cdot 9$. Рассмотрим эти варианты:

$\begin{cases} p_2 - p_1 = 1 \\ p_2 + p_1 = 72 \end{cases} \Rightarrow 2p_2 = 73 \Rightarrow$ нет решений в целых числах,

$\begin{cases} p_2 - p_1 = 2 \\ p_2 + p_1 = 36 \end{cases} \Rightarrow p_2 = 19,\ p_1 = 17,$

$\begin{cases} p_2 - p_1 = 3 \\ p_2 + p_1 = 24 \end{cases} \Rightarrow 2p_2 = 27 \Rightarrow$ нет решений в целых числах,

$\begin{cases} p_2 - p_1 = 4 \\ p_2 + p_1 = 18 \end{cases} \Rightarrow p_2 = 11,\ p_1 = 7,$

$\begin{cases} p_2 - p_1 = 6 \\ p_2 + p_1 = 12 \end{cases} \Rightarrow p_2 = 9$ – составное число,

$\begin{cases} p_2 - p_1 = 8 \\ p_2 + p_1 = 9 \end{cases} \Rightarrow 2p_2 = 17 \Rightarrow$ нет решений в целых числах.

Для полученных значений p_1 и p_2 найдем им соответствующие q, A и B:

- $p_2 = 5,\ p_1 = 3 \Rightarrow q = 39,\ A = 225,\ B = 1521,$
- $p_2 = 11,\ p_1 = 7 \Rightarrow q = 85,\ A = 5929,\ B = 7225,$
- $p_2 = 19,\ p_1 = 17 \Rightarrow q = 325,\ A = 104329,\ B = 105625.$

Ответ: $\begin{cases} A_1 = 225 \\ B_1 = 1521, \end{cases} \begin{cases} A_2 = 5929 \\ B_2 = 7225, \end{cases} \begin{cases} A_3 = 104329 \\ B_3 = 105625. \end{cases}$