8-9 класс XXIV МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

(сайт олимпиады www.cryptolymp.ru) 30.11.2014

1 вариант

1. Женя решила поделиться забавным палиндромом с Ксюшей. Но, чтобы никто о нем больше не узнал, Женя удалила пробелы между словами, перемешала буквы и получила вот что: **алжбанкнаабанжалкаан**. Помогите Ксюше прочитать палиндром (палиндром – текст, читающийся одинаково в обоих направлениях. Например: «А роза упала на лапу Азора»).
Ответ: нажал кабан на баклажан

2. Линия связи состоит из 4-х каналов, пронумерованных числами 1,2,3,4. Для передачи по линии сигнала на каждый канал подается свой импульс, величина которого может быть 7, 9 или 11 единиц. В каждом канале есть усилитель, который увеличивает поданный импульс в 3^{i-1} раз, где i - номер канала. На выходе линии формируется сигнал, который равен остатку от деления на 81 суммы полученных по каналам импульсов. Какие импульсы необходимо подать на каналы, чтобы получить сигнал, величиной 6 единиц?
Решение:
Заметим, что числа 7, 9, 11, равные импульсам, которые передаются по каналам, дают разные и в точности все возможные остатки при делении на 3.
Пусть $a \in \mathbb{Z}$ - значение, равное сумме импульсов, переданных по четырем каналам. Тогда по условию $r_{81}(a) = 6$, где $r_{81}(a)$ – остаток от деления a на 81. Справедливо представление

$$a = a_1 + 3a_2 + 9a_3 + 27a_4,$$

где $a_i \in \{7, 9, 11\},\ i \in \{1, 2, 3, 4\}$. В то же время из условия задачи

$$a = 6 + 81q, \qquad q \in \mathbb{Z}.$$

Но тогда, нетрудно понять, что

$$r_3(a_1) = r_3(a) = r_3(6 + 81q) = r_3(6) = 0.$$

Откуда следует, что число a_1 может равняться только 9, поскольку только оно дает остаток 0 при делении на число 3. Получим

$$a - 9 = 3a_2 + 9a_3 + 27a_4 = -3 + 81q,$$
$$a_2 + 3a_3 + 9a_4 = -1 + 27q.$$

Аналогично предыдущим рассуждениям имеем:

$$r_3(a_2) = r_3(a_2 + 3a_3 + 9a_4) = r_3(-1 + 27q) = r_3(-1) = 2.$$

Отсюда находим, что $a_2 = 11$. Далее получим равенства:

$$3a_3 + 9a_4 = -1 + 27q - 11 = -12 + 27q,$$
$$a_3 + 3a_4 = -4 + 9q.$$

Также аналогично найдем

$$r_3(a_3) = r_3(a_3 + 3a_4) = r_3(-4 + 9q) = 2.$$

Следовательно, $a_3 = 11$. И, наконец, вычислим:

$$3a_4 = -4 + 9q - 11 = -15 + 9q,$$
$$a_4 = -5 + 3q.$$

Придем к равенствами

$$r_3(a_4) = r_3(-5 + 3q) = r_3(-5) = 1$$

и $a_4 = 7$. Таким образом, искомый набор импульсов на входе физической линии есть (9, 11, 11, 7).
Ответ: 9, 11, 11, 7.

3. Дана последовательность из 11 чисел $x_1, x_2, \ldots, x_{11}$. В ней каждое число x_i равно либо 0, либо 1. Из этой последовательности получили последовательность из 10 чисел $y_1, y_2, \ldots, y_{10}$ по формулам: $y_1 = x_1 \cdot x_2,\ y_2 = x_2 \cdot x_3, \ldots, y_{10} = x_{10} \cdot x_{11}$. Определите, какие из четырёх приведённых ниже последовательностей $y_1, y_2, \ldots, y_{10}$ могли быть получены указанным способом, а какие нет.
(I): 0011001100; (II): 0001111101; (III): 1000111000; (IV): 1100110110.
Ответ обоснуйте.

Решение: Для всевозможных последовательностей из четырех символов x_1, x_2, x_3, x_4 найдем им соответствующие последовательности y_1, y_2, y_3. Результаты приведены в таблице. Видим, что выходная последовательность y_i не может содержать фрагмент 101 (назовем его *запретом*).

x_1, x_2, x_3, x_4	y_1, y_2, y_3
0, 0, 0, 0	0, 0, 0
0, 0, 0, 1	0, 0, 0
0, 0, 1, 0	0, 0, 0
0, 0, 1, 1	0, 0, 1
0, 1, 0, 0	0, 0, 0
0, 1, 0, 1	0, 0, 0
0, 1, 1, 0	0, 1, 0
0, 1, 1, 1	0, 1, 1
1, 0, 0, 0	0, 0, 0
1, 0, 0, 1	0, 0, 0
1, 0, 1, 0	0, 0, 0
1, 0, 1, 1	0, 0, 1
1, 1, 0, 0	1, 0, 0
1, 1, 0, 1	1, 0, 0
1, 1, 1, 0	1, 1, 0
1, 1, 1, 1	1, 1, 1

Покажем теперь, что любая последовательность, не содержащая 101, может быть получена при некоторой входной последовательности x_i. Предположим, что последовательность $y_1,\ldots,y_k$ нами уже получена с помощью некоторой последовательности $x_1,\ldots,x_{k+1}, k>2.$ Покажем, что мы сможем тогда получить и последовательность $y_1,\ldots,y_{k+1}$ (конечно, если она не содержит 101).

Если $y_{k+1}=0,$ то последовательность $y_1,\ldots,y_k,0$ можно получить, добавив 0 к входной последовательности, из которой получена последовательность $y_1,\ldots,y_k$. Если $y_{k+1}=1,$ то возможны три случая:

(1) последовательность $y_1,\ldots,y_{k-2},0,0,1$

(2) последовательность $y_1,\ldots,y_{k-2},0,1,1$

(3) последовательность $y_1,\ldots,y_{k-2},1,1,1$

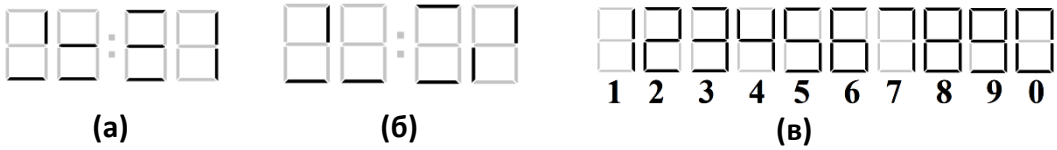
Случай (1). Если последовательность $y_1,\ldots,y_{k-2},0,0$ получена с помощью входа $x_1,\ldots,x_{k+1}$, то она же может быть получена и с помощью входа $x_1,\ldots,x_{k-1},0,1$. Тогда требуемая последовательность $y_1,\ldots,y_{k-2},0,0,1$ получается с помощью входа $x_1,\ldots,x_{k-1},0,1,1$

Случай (2) Если последовательность $y_1,\ldots,y_{k-2},0,1$ получена с помощью входа $x_1,\ldots,x_{k+1}$, то $x_k=x_{k+1}=1$. Тогда требуемая последовательность $y_1,\ldots,y_{k-2},0,1,1$ получается с помощью входа $x_1,\ldots,x_{k-1},1,1,1$

Случай (3) рассматривается аналогично случаю (2).

Ответ: запрет 101, не содержат запрета последовательности (I) и (III).

4. Имеются сломанные электронные часы (они идут точно, но некоторые элементы табло перегорели). Показания часов в некоторый момент времени приведены на рисунке (а), а спустя ровно 1 час 8 минут – на рисунке (б). Определите время, которое на рисунке (а) показывали бы исправные часы. Отображение цифр на исправном табло показано на рисунке (в).



(а) **(б)** **(в)**

Решение: Так как на табло часы, то получаем ограничения на цифры на первой и третьейпозиции слева. Первая цифра это 0, 1 или 2. Третья цифра это 0, 1, 2, 3, 4, 5.

Рассмотрим третью слева позицию на часах. На рисунке а) подходят цифры 2,3,5. На рисунке б) подходят цифры 2,3,5,0. Получаем возможные пары:

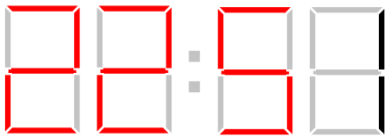
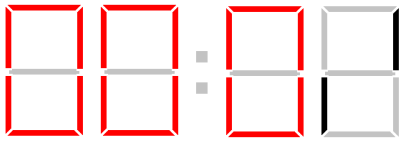
(2,2) , (2,3) , (3,3) , (5,5) ,(5,0). Так как на рисунке а) горит средний горизонтальный элемент, а на рисунке б) не горит, то остается только пара (5,0).

а) б)

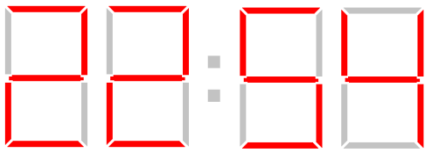
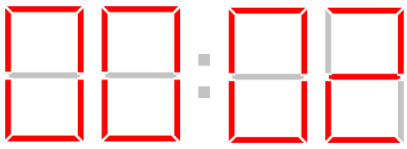
Теперь рассмотрим вторую слева позицию на часах. На рисунке а) подходят цифры: 2,3,5,6,8,9. На рисунке б) подходят цифры: 2,3,5,6,8,9,0. По условию сказано, что прошло ровно 1 час и 8 минут. Т.е, вторая позиция слева могла измениться либо на 1 либо на 2. Тогда подходят пары: (2,0) , (3,0) , (8,0) , (9,0). Так как в третьей слева цифре произошел переход через десяток, значит, во второй позиции цифры отличаются на 2. Тогда остаются пары: (2,0), (8,0).

Теперь рассмотрим первую слева позицию на часах, отвечающую за десятки часов.Нарисунках обоих рисунках подходят цифры 0, 2. Возможные пары получаются: (0,0) , (2,2) , (2,0). Ни под одну эту пару не походит пара (8,0) из второй слева позиции часов.

Таким образом, получаем:

а)  б) 

Осталось определить последнюю пару цифр. На рисунке а) подходят: 0,1,3,4,7,8,9. На рисунке б): 2,8,0. С учетом разницы в 8 минут остаются пары: (0,8), (4,2). Пара (0,8) не подходит, так как должен бы гореть правый нижний элемент на рисунке б). Остается только пара (4,2).

а)  б) 

Ответ: 22:54

5. Для доступа на сайт Алиса вводит в строке браузера его имя. Затем это имя по сети отправляется на специальный DNS-сервер, который по имени сайта определяет его IP-адрес – набор из четырех целых чисел $x_1.x_2.x_3.x_4$, причем $0 < x_i < 255,\ i = 1,2,3,4.$ Этот IP-адрес сервер отправляет Алисе. Чтобы защитить передаваемый адрес от подделки, сервер вместе с адресом передает число s, которое он вычисляет так: $s = r_{141}((h_4)^d)$, где d – секретное натуральное число, известное только Алисе и серверу, а $r_{141}(x)$ – остаток от деления числа *x* на 141; число h_4 находится последовательным применением правила $h_i = r_{141}(h_{i-1} \cdot x_i)$, где i принимает значения $1,2,3,4,$ а $h_0 = 1$. Получив IP-адрес, Алиса также вычисляет *s* и, если оно совпадает с присланным сервером значением, Алиса признает этот IP-адрес подлинным. Злоумышленник узнал, что на запрос Алисы сервер ответил: 10.10.1.1 при $s = 115$. Он хочет от имени сервера отправить Алисе ложный (отличающийся от исходного) адрес вида 10.10.*a.b* и такое число *s′*, чтобы этот адрес Алиса признала подлинным. Найдите хотя бы одну такую тройку *a,b, s′* с условием $s' \geq 1$.

Решение:

Заметим, что факторизовывать число $N = 141$ и находить значение d нет необходимости – достаточно найти пару x_3', x_4' такую, что $x_3' \neq x_3,\ x_4' \neq x_4$ и описанное преобразование сжатия (в основе которого лежит итеративная функция h) от значений x_1, x_2, x_3', x_4' дает тоже значение h_4. То есть, попробуем найти коллизию сжимающего преобразования, тогда и значение s отIP-адресов $x_1.x_2.x_3.x_4$ и $x_1.x_2.x_3'.x_4'$ будет одинаковым.

Замечаем, что так как $x_3 = 1,\ x_4 = 1$, то $h_4 = r_N(h_2)$. Тогда при условии сохранения прежних компонент $x_1.x_2$, для искомого IP-адреса получаем, что необходимо найти такие x_3', x_4' и параметр h_3', которые удовлетворяют системе:

$$\begin{cases} h_3' = r_N(h_2 \cdot x_3') \\ h_4 = r_N(h_3' \cdot x_4') \end{cases},$$

из которой с учетом того, что $h_4 = r_N(h_2),$ следует, что $r_N(x_3' \cdot x_4') = 1$, то есть $x_3' \cdot x_4' = 1 + t \cdot N$, t - натуральное. Тогда при $t = 1$ имеем: $x_3' \cdot x_4' = 142 = 2 \cdot 5 \cdot 17$, откуда получаем следующий возможный вариант для пары (x_3', x_4'): (2, 71).

Ответ, возможный вариант: 10.10.2.71 с исходным значением s.

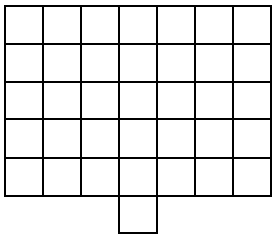
Замечание

Это не единственные ответы, так как могут быть получены ответы и при $t = 2$ и т.д.

Дополнительная информация для проверки

p	q	$\varphi(N)$	d	h_1	h_2	h_3	h_4
3	47	$92 = 2^2 \cdot 23$	5	10	100	100	100

6. Докажите, что *нельзя обойти* все клетки изображенной на рисунке фигуры, побывав в каждой ровно один раз. Начинать движение можно из любой клетки. Разрешается двигаться на *одну клетку* только вправо, влево, вверх или вниз. Движение по диагонали запрещено.



Решение: Раскрасим клетки как на рисунке. Делая один шаг, мы из черной клетки попадаем в белую и наоборот. Значит, если бы искомый обход был возможен, то клеток одного цвета было бы от силы на единицу больше, чем клеток другого цвета. Но черных клеток на две больше, чем белых. Поэтому обход невозможен.