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

(сайт олимпиады www.cryptolymp.ru) 29.11.2015

1. На кодовом замке имеется круглый диск с нанесенными на равноотстоящих интервалах по его периметру числами от 1 до 12. Изначально диск установлен как на Рис.1. Замок откроется, если диск окажется повернутым на 30^0 относительно своего первоначального положения (Рис. 2). Для изменения положения диска имеется специальный стержень, который можно продеть через два любых диаметрально противоположных числа (например, через 1 и 7 как на Рис.3), а затем повернуть диск вокруг стержня на 180^0 (в результате диск окажется в положении, изображенном на Рис.4). Каким образом и за какое наименьшее число таких поворотов можно открыть замок?

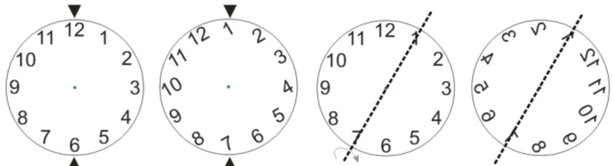


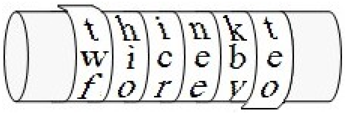
Рис. 1 Рис. 2 Рис. 3 Рис. 4

Решение: При повороте диска на месте четных чисел вновь оказываются четные, а на месте нечетных – нечетные. Поэтому открыть замок нельзя.

Ответ: Такими поворотами открыть замок нельзя.

Замечание. *Здесь возможны и более "математизированные" рассуждения. Поворот диска вокруг стержня на 180^0 – это осевая симметрия диска относительно прямой, содержащей стержень. Будем эти осевые симметрии обозначать буквой S. В задаче требуется найти симметрии, композиция которых – поворот на 30^0. Композиция двух осевых симметрий S_1 и S_2 относительно прямых, угол между которыми α, – это поворот на угол 2α. Обозначая поворот буквой R, можем, таким образом, записать $S_2 \circ$ Композицией симметрии и поворота будет вновь симметрия ($S \circ$), а двух поворотов, очевидно, снова поворот ($R \circ$). Видим также, что симметрия меняет начертание цифр на "зеркальное" (см. переход от Рис.3 к Рис.4). Значит, чтобы диск оказался в положении, изображенном на Рис.2, симметрий должно быть четное число. Но каждая пара симметрий – это поворот, а композиция поворотов – это опять же поворот. Следовательно, композиция четного числа симметрий – поворот, причем на угол, кратный 60^0 (т.к. минимальный угол между прямыми – 30^0). Поэтому повернуть диск на 30^0 не получится.*

2. Для шифрования сообщений Катя и Антон использовали шифр Сцитала: на круглую палочку виток к витку без просветов и нахлёстов наматывалась лента. При горизонтальном положении палочки на ленту по всей длине стержня построчно записывался текст сообщения без знаков препинания и пробелов. После этого лента с записанным на ней текстом посылалась адресату. Антон передал Кате ленту, на которой было написано вот что:



н м и о с с а в т з о л п ы с д к е р с я р с д а о з и ы и с т а п п т н а м ы у о о м н

л ч л я г о ь и е б р ю н й н е е п ы г я г х о е о б у а п у л е к л я т о г с ч т к д п

и н а н н а о ы м у ы х н й т в й у с г а в л ч к о к п е и и н н е в й

К сожалению, Катя свою палочку потеряла, но она видит, что лента исписана полностью, и знает, что при намотке ленты было сделано целое число оборотов. Помогите ей восстановить сообщение.

Решение: Лента исписана полностью, а при ее намотке было сделано целое число оборотов. Это означает, что текст был по сути вписан в ячейки прямоугольной таблицы. Причем таблица оказалась заполненной полностью. В тексте 126 букв, и $126=2\cdot3^2\cdot7$. Значит, стоит попробовать вписать зашифрованный текст (по столбцам сверху вниз) в таблицы размеров типа 2×63, 9×14 и 6×21. Осмысленный текст (при чтении по строкам) получается в последнем случае.

н	а	п	р	а	с	н	о	я	б	е	г	у	к	с	и	о	н	с	к	и
м	в	ы	с	о	т	а	м	г	р	е	х	а	л	ч	н	ы	й	г	о	н
и	т	с	я	з	а	м	н	о	ю	п	о	п	я	т	а	м	т	а	к	н
о	з	д	р	и	п	ы	л	ь	н	ы	е	у	т	к	н	у	в	в	п	е
с	о	к	с	ы	п	у	ч	и	й	г	о	л	о	д	н	ы	й	л	е	в
с	л	е	д	и	т	о	л	е	н	я	б	е	г	п	а	х	у	ч	и	й

Ответ:

Напрасно я бегу к сионским высотам,

Грех алчный гонится за мною по пятам...

Так, ноздри пыльные уткнув в песок сыпучий,

Голодный лев следит оленя бег пахучий

3. Докажите, что для каждого натурального $n \geq 5$ квадрат можно разрезать на n прямоугольников (не обязательно одинаковых), у каждого из которых одна сторона вдвое больше другой. Резать разрешается по линиям, параллельным сторонам исходного квадрата.

Рис.I

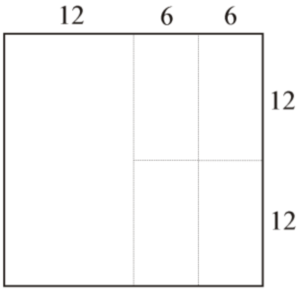


Рис.II. $n = 5$.

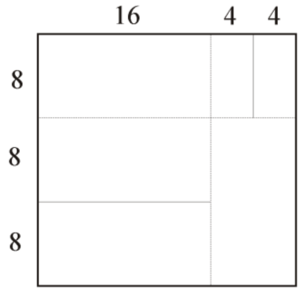


Рис.III. $n = 6$.

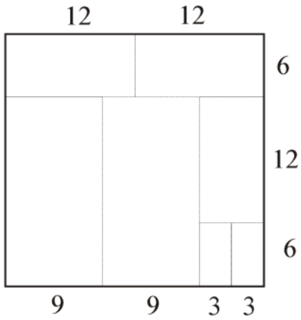


Рис.IV. $n = 7$.

Решение: Если квадрат уже разрезан на k прямоугольников с отношением сторон 2:1, то его можно разрезать и на k+3 таких прямоугольников. Действительно, для этого достаточно один из этих k прямоугольников, разрезать на четыре прямоугольника, у каждого из которых стороны также относятся как 2:1 (Рис.I). Таким образом, для завершения доказательства остается показать, что квадрат можно разрезать на n=5,6 и 7 прямоугольников указанного вида. Соответствующие линия разреза приведены на Рис.II–IV. Для удобства сторона квадрата принята равной 24.

4. Для зашифрования осмысленного русского слова используется последовательность натуральных чисел $y_1, y_2, \ldots$ которая формируется так: y_1 выбирается произвольно, а остальные члены последовательности вычисляются по формуле $y_{n+1} = 4y_n + 23, n = 1, 2, \ldots$. Зашифрование производилось следующим образом. Первая буква слова заменялась числом согласно таблице и умножалась на y_1. Потом также заменялась вторая буква и умножалась на y_2 и т.д. Затем все произведения были замены остатками от деления на 32. В результате получилось вот что:

26, 26, 1, 10, 19, 19, 0, 1, 20, 7, 17, 27.

Какое слово было зашифровано?

А	Б	В	Г	Д	ЕЁ	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: Обозначим через $r_{32}(a)$ остаток от деления числа a на 32. Вычислим несколько первых членов последовательности $y_1, y_2, \ldots$

$$y_2 = 4y_1 + 23,\ y_3 = 4\left(4y_1 + 23\right) + 23 = 16y_1 + 5 \cdot 23,\ y_4 = 64y_1 + 21 \cdot 23.$$

Далее $r_{32}(y_4) = r_{32}(21 \cdot 23) = 3,$ а значит $r_{32}(y_5) = r_{32}\left(4y_4 + 23\right) = r_{32}\left(4 \cdot 3 + 23\right) = 3.$ То есть, начиная с четвертого номера, все члены последовательности $r_{32}(y_n)$ равны 3. Пусть $x_1, x_2, \ldots$ – числовые значения букв искомого слова. Чтобы найти x_4 надо решить уравнение $r_{32}(y_4 x_4) = 10.$ Заметим, что

$r_{32}(y_4x_4)=10 \Leftrightarrow r_{32}(3x_4)=10 \Leftrightarrow r_{32}(11\cdot 3x_4)=r_{32}(11\cdot 10) \Leftrightarrow r_{32}(x_4)=14 \Rightarrow x_4=14.$ Следовательно, четвертая буква слова – О. Аналогично находятся числовые значения букв $x_5,\dots$ В итоге, искомое слово принимает вид ***ОССАЛЬНЫЙ. Ответ легко угадывается.

Ответ: КОЛОССАЛЬНЫЙ.

5. На столе выложены 12 карточек в порядке возрастания их номеров (Рис.а). Карточки разрешается перекладывать *тройками*, а именно: выбираем три любые карточки, например, с номерами 2, 3 и 5. Затем крайняя левая карточка перемещается на место средней, средняя на место крайней правой, а крайняя правая на место крайней левой. Результат изображен на Рис.б. Можно ли, перекладывая карточки указанным способом, уложить их как на Рис.а, но в порядке убывания номеров (карточка с номером 12 – первая, с номером 1 – последняя)?

Решение: Покажем, что у любых четырех карточек *A,B,C,D* можно изменить порядок их следования на противоположный (точками сверху будем отмечать те карточки, которые собираемся перекладывать): $\dot{A},\dot{B},C,\dot{D} \to D,\dot{A},\dot{C},\dot{B} \to D,\dot{B},\dot{A},\dot{C} \to D,C,B,A.$ Теперь, перекладывая карточки сразу *четверками*, покажем как переложить 12 карточек в обратном порядке:

$$\dot{1},\dot{2},3,4,5,6,7,8,9,10,\dot{11},\dot{12} \to 12,11,\dot{3},\dot{4},5,6,7,8,\dot{9},\dot{10},2,1 \to$$

$$\to 12,11,10,9,\dot{5},\dot{6},\dot{7},\dot{8},4,3,2,1 \to 12,11,10,9,8,7,6,5,4,3,2,1.$$

Ответ: Можно.

6. *Треугольником Паскаля* называют бесконечную треугольную таблицу чисел, у которой на вершине и по бокам стоят единицы, а каждое число внутри равно сумме двух стоящих над ним чисел. Так, например, третья строка треугольника (1,2,1) содержит два нечетных числа и одно четное. Сколько четных чисел содержится в строке с номером 140?

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
…

Решение: Будем заменять в треугольнике нечетные числа единицами, а четные нулями. При этом каждое число внутри по-прежнему остается равным сумме стоящих над ним чисел, если принять, что 0+0=1+1=0, 1+0=0+1=1. Рассмотрим структуру треугольника подробнее. Треугольник, сформированный первыми восемью строками, обозначим T_8. В строке 9 всего две единицы (по бокам), остальные – нули. С этой строки и вниз далее идет формирование двух треугольников T_8, которые "встречаются друг с другом" в строке 16. Начиная со строки 17 и ниже, образовываются два треугольника T_{16}, которые, в свою очередь, "встречаются" в строке 32. Со строки 33 и ниже формируются два треугольника T_{32} и т.д. Таким образом, строки, чей номер представляет собой степень двойки, состоят только из единиц.

Понятно, что, после строки 128, идет формирование "с нуля" двух одинаковых треугольников. Строки с номером 12 в этих новых треугольниках как раз и содержатся в строке 140 исходного (большого) треугольника, т.к. 140=12+128. Значит единиц в строке 140 вдвое больше, чем единиц в строке с номером 12. Количество же 1 в строке 12 можно подсчитать непосредственно – их 8 штук. Значит в строке 140 их 16. Остальные 124 – нули.

Ответ: 124.

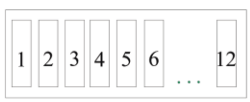


Рис. а

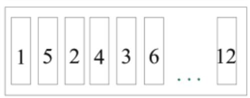
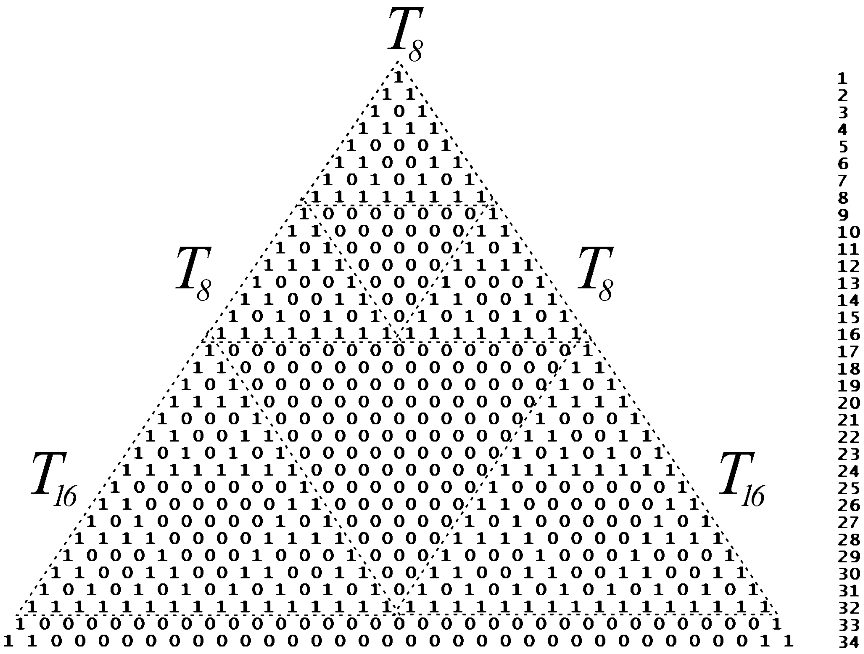


Рис. б



T_8
T_8
T_8
T_{16}
T_{16}
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 32 33 34

1. На кодовом замке имеется круглый диск с нанесенными на равноотстоящих интервалах по его периметру числами от 1 до 12. Изначально диск установлен как на Рис.1. Замок откроется, если диск окажется повернутым на 30^0 относительно своего первоначального положения (Рис. 2). Для изменения положения диска имеется специальный стержень, который можно продеть через два любых диаметрально противоположных числа (например, через 1 и 7 как на Рис.3), а затем повернуть диск вокруг стержня на 180^0 (в результате диск окажется в положении, изображенном на Рис.4). Каким образом и за какое наименьшее число таких поворотов можно открыть замок?

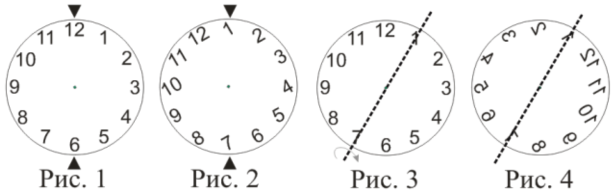


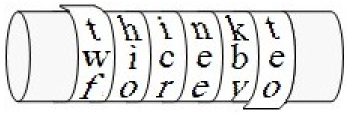
Рис. 1 Рис. 2 Рис. 3 Рис. 4

Решение: При повороте диска на месте четных чисел вновь оказываются четные, а на месте нечетных – нечетные. Поэтому открыть замок нельзя.

Ответ: Такими поворотами открыть замок нельзя.

Замечание. *Здесь возможны и более "математизированные" рассуждения. Поворот диска вокруг стержня на 180^0 – это осевая симметрия диска относительно прямой, содержащей стержень. Будем эти осевые симметрии обозначать буквой S. В задаче требуется найти симметрии, композиция которых – поворот на 30^0. Композиция двух осевых симметрий S_1 и S_2 относительно прямых, угол между которыми α, – это поворот на угол 2α. Обозначая поворот буквой R, можем, таким образом, записать $S_2 \circ$ Композицией симметрии и поворота будет вновь симметрия ($S \circ$), а двух поворотов, очевидно, снова поворот ($R \circ$). Видим также, что симметрия меняет начертание цифр на "зеркальное" (см. переход от Рис.3 к Рис.4). Значит, чтобы диск оказался в положении, изображенном на Рис.2, симметрий должно быть четное число. Но каждая пара симметрий – это поворот, а композиция поворотов – это опять же поворот. Следовательно, композиция четного числа симметрий – поворот, причем на угол, кратный 60^0 (т.к. минимальный угол между прямыми – 30^0). Поэтому повернуть диск на 30^0 не получится.*

2. Для шифрования сообщений Катя и Антон использовали шифр Сцитала: на круглую палочку виток к витку без просветов и нахлёстов наматывалась лента. При горизонтальном положении палочки на ленту по всей длине стержня построчно записывался текст сообщения без знаков препинания и пробелов. После этого лента с записанным на ней текстом посылалась адресату. Антон передал Кате ленту, на которой было написано вот что:



н м и о с с а в т з о л п ы с д к е р с я р с д а о з и ы и с т а п п т н а м ы у о о м н
л ч л я г о ь и е б р ю н й н е е п ы г я г х о е о б у а п у л е к л я т о г с ч т к д п
и н а н н а о ы м у ы х н й т в й у с г а в л ч к о к п е и и н н е в й

К сожалению, Катя свою палочку потеряла, но она видит, что лента исписана полностью и знает, что при намотке ленты было сделано целое число оборотов. Помогите ей восстановить сообщение.

Решение: Лента исписана полностью, а при ее намотке было сделано целое число оборотов. Это означает, что текст был по сути вписан в ячейки прямоугольной таблицы. Причем таблица оказалась заполненной полностью. В тексте 126 букв, и $126=2\cdot3^2\cdot7$. Значит, стоит попробовать вписать зашифрованный текст (по столбцам сверху вниз) в таблицы размеров типа 2×63, 9×14 и 6×21. Осмысленный текст (при чтении по строкам) получается в последнем случае.

н	а	п	р	а	с	н	о	я	б	е	г	у	к	с	и	о	н	с	к	и

м	в	ы	с	о	т	а	м	г	р	е	х	а	л	ч	н	ы	й	г	о	н
и	т	с	я	з	а	м	н	о	ю	п	о	п	я	т	а	м	т	а	к	н
о	з	д	р	и	п	ы	л	ь	н	ы	е	у	т	к	н	у	в	в	п	е
с	о	к	с	ы	п	у	ч	и	й	г	о	л	о	д	н	ы	й	л	е	в
с	л	е	д	и	т	о	л	е	н	я	б	е	г	п	а	х	у	ч	и	й

Ответ:

Напрасно я бегу к сионским высотам,

Грех алчный гонится за мною по пятам...

Так, ноздри пыльные уткнув в песок сыпучий,

Голодный лев следит оленя бег пахучий

3. Для проверки корректности номера пластиковой карты, представляющего собой набор из 16 цифр $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16})$, вычисляются контрольные суммы *A*, *B* и *C*:

$A = x_1 + x_2 + x_5 + 3x_7 + x_8 + 7x_{10} + x_{12} + x_{13} + x_{15}$,

$B = x_1 + x_3 + x_6 + 7x_7 + x_9 + 3x_{10} + x_{11} + x_{14} + x_{16}$, $C = x_1 + x_4 + x_5 + x_6 + x_8 + x_9 + x_{11} + x_{12} + x_{13} + x_{14} + x_{15} + x_{16}$.

Если все три суммы *A*, *B* и *C* делятся нацело на 10, то номер признаётся корректным. Каких корректных номеров больше и насколько: у которых первые 4 цифры 0 0 0 0 или тех, у которых последние 4 цифры 0 0 0 0?

Решение: количество корректных номеров есть число решений системы линейных уравнений:

$$\begin{cases} A = 0 \\ B = 0 \\ C = 0 \end{cases} \qquad (*)$$

(по модулю 10).

Для удобства расположим слагаемые (из вида A, B и C) в таблице:

x_1	x_2			x_5		$3x_7$	x_8		$7x_{10}$		x_{12}	x_{13}		x_{15}	
x_1		x_3			x_6	$7x_7$		x_9	$3x_{10}$	x_{11}			x_{14}		x_{16}
x_1			x_4	x_5	x_6		x_8	x_9		x_{11}	x_{12}		x_{14}	x_{15}	x_{16}

Если первые 4 цифры 0 0 0 0, то таблица примет вид:

x_5		$3x_7$	x_8		$7x_{10}$		x_{12}	x_{13}		x_{15}	
	x_6	$7x_7$		x_9	$3x_{10}$	x_{11}			x_{14}		x_{16}
x_5	x_6		x_8	x_9		x_{11}	x_{12}		x_{14}	x_{15}	x_{16}

Но тогда третья строка есть сумма первой и второй по модулю 10. Вычитая из третьей строки первую и вторую, получим, что x_{15}, x_{16} линейно выражаются через $x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}$. Количество решений есть количество способов поставить всеми возможными способами на места переменных $x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}$ числа 0,1,2,…,9. Таким образом, число корректных номеров равно 10^{10}.

Если последние 4 цифры 0 0 0 0, то таблица примет вид:

x_1	x_2			x_5		$3x_7$	x_8		$7x_{10}$		x_{12}
x_1		x_3			x_6	$7x_7$		x_9	$3x_{10}$	x_{11}	
x_1			x_4	x_5	x_6		x_8	x_9		x_{11}	x_{12}

В отличии от первой части, в этом случае переменные x_1, x_2, x_3 будут линейно выражаться через $x_4, x_6, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}$. Тогда число решений системы равно 9^{10}

Ответ: в первом случае корректных номеров больше, чем во втором на $10^{10} - 9^{10}$.

4. Для зашифрования осмысленного русского слова используется последовательность натуральных чисел $y_1, y_2, \dots$ которая формируется так: y_1 выбирается произвольно, а остальные члены последовательности вычисляются по формуле $y_{n+1} = 4y_n + 25, n = 1, 2, \dots$. Зашифрование производилось следующим образом. Первая буква слова заменялась числом согласно таблице и умножалась на y_1. Потом также заменялась вторая буква и умножалась на y_2 и т.д. Затем все произведения были замены остатками от деления на 32. В результате получилось вот что: **7, 8, 28, 28, 1, 10, 16, 8, 11, 9, 31, 21.** Какое слово было зашифровано?

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: Обозначим через $r_{32}(a)$ остаток от деления числа a на 32. Вычислим несколько первых членов последовательности $y_1, y_2, \dots$

$$y_2 = 4y_1 + 25,\ y_3 = 4(4y_1 + 25) + 25 = 16y_1 + 5 \cdot 25,\ y_4 = 64y_1 + 21 \cdot 25.$$

Далее $r_{32}(y_4) = r_{32}(21 \cdot 25) = 13$, а значит $r_{32}(y_5) = r_{32}(4y_4 + 25) = r_{32}(4 \cdot 13 + 25) = 13$. То есть, начиная с четвертого номера, все члены последовательности $r_{32}(y_n)$ равны 13. Пусть $x_1, x_2, \dots$ – числовые значения букв искомого слова. Чтобы найти x_4 надо решить уравнение $r_{32}(y_4 x_4) = 28$. Заметим, что $r_{32}(y_4 x_4) = 28 \Leftrightarrow r_{32}(13x_4) = 28 \Leftrightarrow r_{32}(5 \cdot 13x_4) = r_{32}(5 \cdot 28) \Leftrightarrow r_{32}(x_4) = 12 \Rightarrow x_4 = 12$. Следовательно, четвертая буква слова – М. Аналогично находятся числовые значения букв $x_5, \dots$ В итоге, искомое слово принимает вид ***МЕТРИЧНЫЙ. Ответ легко угадывается.

Ответ: СИММЕТРИЧНЫЙ.

5. На столе выложены 14 карточек в порядке возрастания их номеров (Рис.а). Карточки разрешается перекладывать *тройками*, а именно: выбираем три любые карточки, например, с номерами 2, 3 и 5. Затем крайняя левая карточка перемещается на место средней, средняя на место крайней правой, а крайняя правая на место крайней левой. Результат изображен на Рис.б. Можно ли, перекладывая карточки указанным способом, уложить их как на Рис.а, но в порядке убывания номеров (карточка с номером 14 – первая, с номером 1 – последняя)?

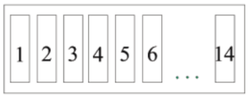


Рис. а

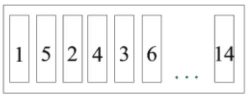


Рис. б

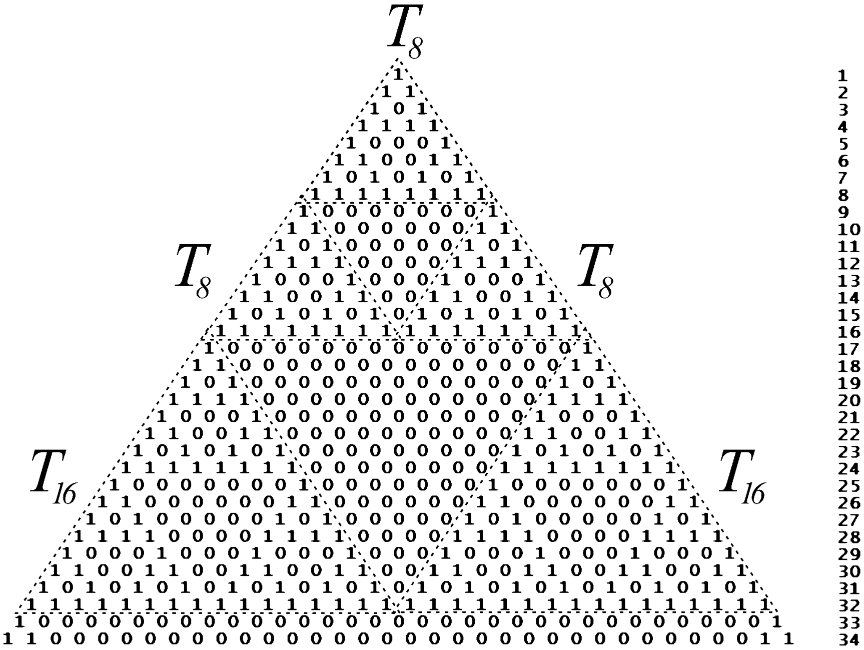
Решение: Пусть сейчас карточки выложены в каком-то порядке. Пару карточек будем называть *беспорядком*, если у левой карточка номер больше, чем у правой. Например, для пяти карточек 1,2,5,4,3 имеется три беспорядка: (5,4), (5,3), (4,3). В исходном расположении карточек на столе число беспорядков равно нулю. Перекладывая тройку карточек указанным в условии способом, мы число беспорядков изменяем на некоторое четное число. Значит количевсо беспорядков всегда должно оставаться четным. Но, если карточки выложены в обратном порядке, то число беспорядков равно 13+12+…+1, то есть нечетно.

Ответ: Нельзя.

6. *Треугольником Паскаля* называют бесконечную треугольную таблицу чисел, у которой на вершине и по бокам стоят единицы, а каждое число внутри равно сумме двух стоящих над ним чисел. Так, например, третья строка треугольника (1,2,1) содержит два нечетных числа и одно четное. Сколько четных чисел содержится: а) в строке с номером 257? б) в строке с номером 300?

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
…

Решение: Будем заменять в треугольнике нечетные числа единицами, а четные нулями. При этом каждое число внутри по-прежнему остается равным сумме стоящих над ним чисел, если принять, что $0+0=1+1=0$, $1+0=0+1=1$. Рассмотрим структуру треугольника подробнее. Треугольник, сформированный первыми восемью строками, обозначим T_8. В строке 9 всего две единицы (по бокам), остальные – нули. С этой строки и вниз далее идет формирование двух треугольников T_8, которые "встречаются друг с другом" в строке 16. Начиная со строки 17 и ниже, образовываются два треугольника T_{16}, которые, в свою очередь, "встречаются" в строке 32. Со строки 33 и ниже формируются два треугольника T_{32} и т.д. Таким образом, строки, чей номер представляет собой степень двойки, состоят только из единиц. Поэтому в строке 256 одни единицы, и, следовательно, в строке 257 все числа равны нулю кроме двух единиц по краям.



Обратимся теперь к строке 300. Понятно, что, после строки 256 (степень двойки), идет формирование "с нуля" двух одинаковых треугольников. Строки с номером 44 в этих новых треугольниках как раз и содержатся в строке 300 исходного (большого) треугольника, т.к. $300=256+44$. Значит единиц в строке 300 вдвое больше, чем единиц в строке с номером 44. В свою очередь единиц в строке 44 вдвое больше, чем в строке 12 (рассмотреть треугольники, формирующиеся после строки 32). Количество же 1 в строке 12 можно подсчитать непосредственно – их 8 штук. Значит в строке 300 их 32, остальные 268 – нули.

Ответ: а) 255, б) 268.

11 класс XXV МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

(сайт олимпиады www.cryptolymp.ru) 29.11.2015

1. Для проверки корректности номера пластиковой карты, представляющего собой набор из 16 цифр $(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_{10},x_{11},x_{12},x_{13},x_{14},x_{15},x_{16})$, вычисляются контрольные суммы A, B и C: $A = x_1 + x_2 + x_5 + 3x_7 + x_8 + 7x_{10} + x_{12} + x_{13} + x_{15}$,

$B = x_1 + x_3 + x_6 + 7x_7 + x_9 + 3x_{10} + x_{11} + x_{14} + x_{16}$, $C = x_1 + x_4 + x_5 + x_6 + x_8 + x_9 + x_{11} + x_{12} + x_{13} + x_{14} + x_{15} + x_{16}$.

Если все три суммы A, B и C делятся нацело на 10, то номер признаётся корректным. Каких корректных номеров больше и насколько: у которых первые 4 цифры 0 0 0 0 или тех, у которых последние 4 цифры 0 0 0 0?

Решение: количество корректных номеров есть число решений системы линейных уравнений:

$$\begin{cases} A = 0 \\ B = 0 \\ C = 0 \end{cases} \qquad (*)$$

(по модулю 10).

Для удобства расположим слагаемые (из вида A, B и C) в таблице:

x_1	x_2			x_5		$3x_7$	x_8		$7x_{10}$		x_{12}	x_{13}		x_{15}	
x_1		x_3			x_6	$7x_7$		x_9	$3x_{10}$	x_{11}			x_{14}		x_{16}
x_1			x_4	x_5	x_6		x_8	x_9		x_{11}	x_{12}		x_{14}	x_{15}	x_{16}

Если первые 4 цифры 0 0 0 0, то таблица примет вид:

x_5		$3x_7$	x_8		$7x_{10}$		x_{12}	x_{13}		x_{15}	
	x_6	$7x_7$		x_9	$3x_{10}$	x_{11}			x_{14}		x_{16}
x_5	x_6		x_8	x_9		x_{11}	x_{12}		x_{14}	x_{15}	x_{16}

Но тогда третья строка есть сумма первой и второй по модулю 10. Вычитая из третьей строки первую и вторую, получим, что x_{15}, x_{16} линейно выражаются через $x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}$. Количество решений есть количество способов поставить всеми возможными способами на места переменных $x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}$ числа 0,1,2,…,9. Таким образом, число корректных номеров равно 10^{10}.

Если последние 4 цифры 0 0 0 0, то таблица примет вид:

x_1	x_2			x_5		$3x_7$	x_8		$7x_{10}$		x_{12}
x_1		x_3			x_6	$7x_7$		x_9	$3x_{10}$	x_{11}	
x_1			x_4	x_5	x_6		x_8	x_9		x_{11}	x_{12}

В отличии от первой части, в этом случае переменные x_1, x_2, x_3 будут линейно выражаться через $x_4, x_6, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}$. Тогда число решений системы равно 9^{10}

Ответ: в первом случае корректных номеров больше, чем во втором на $10^{10} - 9^{10}$.

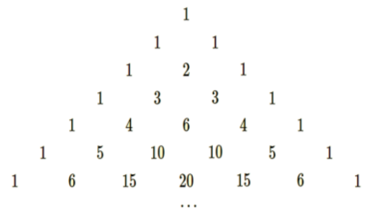
2. Докажите, что существует натуральное число, кратное 2015, десятичная запись которого имеет вид 23152315…2315 (т.е. образована последовательным повторением фрагмента 2315).

Решение: Натуральное число делится на 2015 нацело в том и только том случае, когда оно делится на 5 и на 403. Рассмотрим теперь все числа, десятичная запись которых имеет вид 23152315…2315:

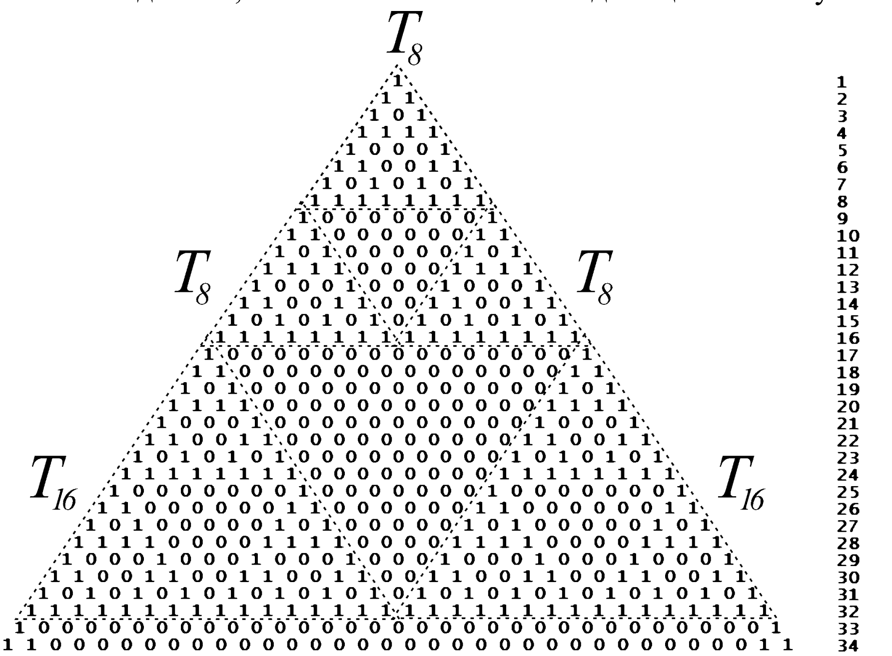
$$x_1 = 2315,\ x_2 = 23152315,\ x_3 = 231523152315,\ \ldots \qquad (1)$$

Среди них найдутся два числа, x_m и x_n $(m > n)$, которые имеют одинаковые остатки при делении на 403. (Действительно, чисел вида (1) бесконечно много, а различных остатков от деления на 403 всего 403 штуки.) Тогда их разность $x_m - x_n$ делится на 403. Теперь отбросим все нули на конце десятичной записи этой разности. В результате получим число вида (1). И это число, очевидно, по-прежнему делится на 403. Оно делится также и на 5, так как на 5 оканчивается, а значит делится на 2015.

3. *Треугольником Паскаля* называют бесконечную треугольную таблицу чисел, у которой на вершине и по бокам стоят единицы, а каждое число внутри равно сумме двух стоящих над ним чисел. Так, например, третья строка треугольника (1,2,1) содержит два нечетных числа и одно четное. Сколько четных чисел содержится: а) в строке с номером 2048? б) в строке с номером 2015?



Решение: Будем заменять в треугольнике нечетные числа единицами, а четные нулями. При этом каждое число внутри по-прежнему остается равным сумме стоящих над ним чисел, если принять, что 0+0=1+1=0, 1+0=0+1=1. Рассмотрим структуру треугольника подробнее. Треугольник, сформированный первыми восемью строками, обозначим T_8. В строке 9 всего две единицы (по бокам), остальные – нули. С этой строки и вниз далее идет формирование двух треугольников T_8, которые "встречаются друг с другом" в строке 16. Начиная со строки 17 и ниже, образовываются два треугольника T_{16}, которые, в свою очередь, "встречаются" в строке 32. Со строки 33 и ниже формируются два треугольника T_{32} и т.д. Таким образом, строки, чей номер представляет собой степень двойки, состоят только из единиц. Поэтому в строке 2048 четных чисел нет.



Обратимся теперь к строке 2015. Уже понятно, что, после строки 1024 (степень двойки), идет формирование "с нуля" двух одинаковых треугольников. Строки с номером 991 в этих новых треугольниках как раз и содержатся в строке 2015 исходного (большого) треугольника, т.к. 2015=1024+991. Значит, единиц в строке 2015 вдвое больше, чем единиц в строке с номером 991. В свою очередь, единиц в строке 991 вдвое больше, чем в строке 479 (рассмотреть треугольники, формирующиеся после строки 512). В строке 479 их вдвое больше, чем в строке 223, в строке 223 вдвое больше, чем в строке 95. И, наконец, в строке 95 их вдвое больше, чем в строке 31. И, поскольку строка 32 состоит из одних 1, в строке 31 единицы и нули чередуются, то есть единиц всего 16. Значит в строке 2015 их $32 \cdot 16 = 512$ штук, остальные 1503 – нули.

Ответ: а) 0, б) 1503.

4. Рассмотрим множество всех точек плоскости, координаты которых имеют вид $(m+n, 4m-3n)$, где $m, n-$ целые числа. Докажите, что на прямой, проходящей через любые две точки указанного множества, лежит сторона некоторого квадрата, все четыре вершины которого принадлежат этому множеству. Укажите минимальную площадь такого квадрата.

Решение

1. Для решения поставленной задачи достаточно доказать, что на любой прямой, проходящей через $(0,0)$ и точку вида $(m+n, 4m-3n), m, n \in \mathbb{Z}$, лежит сторона некоторого квадрата, все вершины которого принадлежат указанному множеству.
Известно, что перпендикулярными к вектору (a,b) являются все вектора вида $k(-b,a), k \in \mathbb{R}$ и только они. Применительно к нашей задаче, требуется проверить, что для каждого вектора $(m_1+n_1, 4m_1-3n_1), m_1, n_1 \in \mathbb{Z}$ существует перпендикуляр вида $(m_2+n_2, 4m_2-3n_2), m_2, n_2 \in \mathbb{Z}$. Другими словами надо решить относительно $k, m_2, n_2 \in \mathbb{Z}$ уравнение
$$k(3n_1-4m_1, m_1+n_1) = (m_2+n_2, 4m_2-3n_2).$$
Перепишем полученное уравнение в виде системы
$$\begin{cases} k(3n_1-4m_1) = m_2+n_2, \\ k(m_1+n_1) = 4m_2-3n_2, \end{cases}$$
которую несложно преобразовать в эквивалентную систему
$$\begin{cases} m_2+n_2 = k(3m_1-4n_1), \\ -7n_2 = k((m_1+n_1)-4(3n_1-4m_1)), \end{cases}$$
разрешимость которой очевидна – последовательно выбираем подходящие целые числа k, n_2 и m_2.
Таким образом, для всякого вектора $(m_1+n_1, 4m_1-3n_1), m_1, n_1 \in \mathbb{Z}$ существует перпендикулярный ему вектор $k(3n_1-4m_1, m_1+n_1)$ вида $(m_2+n_2, 4m_2-3n_2)$. Нетрудно понять, что вектора $k(m_1+n_1, 4m_1-3n_1)$ и $k(3n_1-4m_1, m_1+n_1)$ являются сторонами искомого квадрата.
2. Методом пристального взгляда, в графическом представлении множества точек $(m+n, 4m-3n), m, n \in \mathbb{Z}$, легко обнаружить квадрат со сторонами $(7,0)$ и $(0,7)$. При этом несложно убедиться (опять-таки из графического представления), что не существует пары ортогональных векторов, с длинами менее 7.

5. Число городов в Криптоландии равно 3^6. В качестве названий города имеют различные цифровые комбинации вида (a,b,c,d,e,f), где a,b,c,d,e и f – целые числа из множества {0,1,2}. Два города, названия которых отличаются одной цифрой, называются *соседними*. Например, города (210100) и (210120) соседние, а (000000) и (220000) – нет. У каждого города есть флаг определенного цвета, причем флаги соседних городов всегда имеют несовпадающие цвета. Власти объявили конкурс на создание системы флагов для городов, имеющей наименьшее возможное число различных цветов. Найдите это наименьшее число. Ответ обоснуйте.

Решение: Заметим, что среди городов (000000), (100000) и (200000) любые два являются соседними. Значит, надо минимум три цвета. Покажем, что трех цветов достаточно. Имеющиеся у нас цвета будем называть цвет-0, цвет-1,цвет-2. Флаг города будет окрашен в цвет, номер которого равен остатку от деления на 3 суммы цифр в названии этого города. (Например, для города (310100) этот остаток равен 2, значит его флаг будет окрашен в цвет-2.) У соседних городов эти остатки всегда различны, так как их названия отличаются *одной* цифрой. Следовательно, 3-х цветов достаточно.

Ответ: 3.

6. Чтобы снять деньги с карточки, Алиса в банкомате вводит пин-код (ПК) x_1, x_2, x_3, x_4 – набор из 4-х целых чисел ($0 \le x_i \le 9, i = 1,2,3,4$). Банкомат зашифровывает введенный ПК по следующему правилу: он случайным образом выбирает целое число x_5 такое, что $10 \le x_5 \le 15$, а затем формирует зашифрованный пин-код (ЗПК) y_1, y_2, y_3, y_4, y_5 по формулам: $y_1 = f\left(r_{16}(x_1 + 3\cdot y_0)\right)$, $y_2 = f\left(r_{16}(x_2 + 3\cdot y_1)\right)$, $y_3 = f\left(r_{16}(x_3 + 3\cdot y_2)\right)$, $y_4 = f\left(r_{16}(x_4 + 3\cdot y_3)\right)$, $y_5 = f\left(r_{16}(x_5 + 3\cdot y_4)\right)$, где $y_0 = 3$, $r_{16}(x)$ – остаток от деления числа x на 16, а f – некоторое правило, по которому одно целое число от 0 до 15 заменяется на другое (возможно, то же самое) целое число от 0 до 15, причем разные числа заменяются разными. После этого ЗПК отправляется на сервер, где он расшифровывается (т.е. по присланным числам y_1, y_2, y_3, y_4, y_5 вычисляются x_1, x_2, x_3, x_4 и x_5), и, если x_5 не удовлетворяет неравенству $10 \le x_5 \le 15$, то сервер выдает сообщение об ошибке. Известно, что для ПК Алисы был сформирован следующий ЗПК: 10,2,0,0,11. Известно также, что хакеры пытались отсылать на сервер (напрямую, минуя банкомат) в качестве y_1, y_2, y_3, y_4, y_5 комбинации чисел вида $0,0,0,a,b$. Результаты их попыток приведены в таблице (знак “+” – сервер не выдал сообщение об ошибке, знак “-” – выдал). Какой ПК у Алисы?

$a \backslash b$	0	1	2	9	10	11
0	-	-	-	+	+	+
1	-	-	+	+	-	+
2	-	+	+	-	-	-
3	-	+	-	-	-	-
4	+	-	-	-	+	-
5	+	-	-	+	+	-
6	-	-	-	+	-	+
7	-	+	+	-	-	+
8	-	+	+	-	-	-
9	+	-	-	-	+	-

Решение

<u>1. Типовые рассуждения для каждого варианта.</u>

Для формирования величины паддинга, который будет проверяться на предмет того, принадлежит ли он множеству $\{10,11,12,13,14,15\}$, будут задействованы только последние два числа, пусть a, b и процедура проверки будет выглядеть следующим образом:

$$x_5 = r_{16}(\pi^{-1}(b) - 3a) \overset{?}{\in} \{10,11,12,13,14,15\} = \Omega .$$

Тогда структура каждого столбца с номером b таблицы с точки зрения возникающих ошибок паддинга будет следующей (до этого можно догадаться по закономерностям в данной в задании таблице):

+	+	-	-	-	-	+	+	-	-	-	+	+	-	-	-
a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}

$a_j = r_{16}(a_1 + j), j = \overline{1,16}$.

<u>Вариант рассуждений а).</u>

Выделяем случаи, когда паддинг верный (помечены в таблице темным, далее по тексту условно обозначим $\Omega + c$ - множество элементов Ω, к каждому из которых прибавлено число c и от получившихся значений взят остаток от деления на 16):

- при a_1 имеем $r_{16}(\pi^{-1}(b) - 3a_1) \in \Omega_1 = \{10,11,12,13,14,15\}$;

- при $a_2 = a_1 + 1$ имеем $r_{16}(\pi^{-1}(b) - 3a_1) \in \Omega_1 + 3 = \Omega_2 = \{13,14,15,0,1,2\}$;

- при $a_7 = a_1 + 6$ имеем $r_{16}(\pi^{-1}(b) - 3a_1) \in \Omega_1 + 2 = \Omega_7 = \{12,13,14,15,0,1\}$;

- при $a_8 = a_1 + 7$ имеем $r_{16}(\pi^{-1}(b) - 3a_1) \in \Omega_1 + 5 = \Omega_8 = \{15,0,1,2,3,4\}$;

- при $a_{12} = a_1 + 11$ имеем $r_{16}(\pi^{-1}(b) - 3a_1) \in \Omega_1 + 1 = \Omega_{12} = \{11,12,13,14,15,0\}$;

- при $a_{13} = a_1 + 12$ имеем $r_{16}(\pi^{-1}(b) - 3a_1) \in \Omega_1 + 4 = \Omega_{13} = \{14,15,0,1,2,3\}$.

Нетрудно заметить, что $\Omega_1 \cap \Omega_8 = \{15\}$, то есть $r_{16}(\pi^{-1}(b) - 3a_1) = 15$.

Вариант рассуждений б).

Ответим на вопрос, при каких значениях паддинга $x_5 = r_{16}(\pi^{-1}(b) - 3 \cdot a)$ возможна ситуация, что при его проверке при a_1 будет "+", при $a_2 = a_1 + 1$ будет "+", а при $a_3 = a_2 + 1$, $a_4 = a_3 + 1$, $a_5 = a_4 + 1$, $a_6 = a_5 + 1$ будет "-". Исходя из приведенной ниже таблицы, нетрудно заметить, что только при $x_5 = r_{16}(\pi^{-1}(b) - 3a_1) = 15$.

$-3 \cdot a =$	-15	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0
	-	-	-	-	-	-	-	-	-	-	+	+	+	+	+	+
$x_5 =$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	a_6			a_5			a_4			a_3			a_2			a_1

Общий вывод из рассуждений а) или б):

Если в таблице ошибок паддинга при заданном b есть структура вида

+	+	-	-	-	-
a_1	a_2	a_3	a_4	a_5	a_6

то $r_{16}(\pi^{-1}(b) - 3a_1) = 15$, то есть $\pi^{-1}(b) = r_{16}(3a_1 - 1)$. Это является удобным критерием для определения обратных значений подстановки.

Решение (зашифрованный пароль: 10,2,0,0,11).

Рассмотрим столбец из данной в условии таблицы с $b = 2$. Не трудно заметить, что подходящей под критерий структурой будет

+	+	-	-	-	-
1	2	3	4	5	6

Поэтому $a_1 = 1$ и $\pi^{-1}(2) = r_{16}(3 \cdot 1 - 1) = 2$, что позволяет найти x_2:

$x_2 = r_{16}(\pi^{-1}(2) - 3 \cdot 10) = r_{16}(2 - 14) = 4$.

Рассмотрим столбец из данной в условии таблицы с $b = 0$. Из-за закономерностей в образовании "+" не трудно догадаться, что подходящей под критерий структурой будет

+	+	-	-	-	-
14	15	0	1	2	3

Поэтому $a_1 = 14$ и $\pi^{-1}(0) = r_{16}(3 \cdot 14 - 1) = 9$, что позволяет найти x_3, x_4:

$x_3 = r_{16}(\pi^{-1}(0) - 3 \cdot 2) = r_{16}(9 - 6) = 3$;

$x_4 = r_{16}(\pi^{-1}(0) - 3 \cdot 0) = r_{16}(9 - 0) = 9$.

Рассмотрим столбец из данной в условии таблицы с $b = 10$. Из-за закономерностей в образовании "-" не трудно догадаться, что подходящей структурой будет

+	+	-	-	-	-
9	10	11	12	13	14

Поэтому $a_1 = 9$ и $\pi^{-1}(10) = r_{16}(3 \cdot 9 - 1) = 10$, что позволяет найти x_1:

$x_1 = r_{16}(\pi^{-1}(10) - 3 \cdot 3) = r_{16}(10 - 9) = 1$.

Ответ: пароль Алисы 1,4,3,9