11 класс XXV МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

(сайт олимпиады www.cryptolymp.ru) 29.11.2015

1 вариант

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*:

$A = x_1 + x_2 + x_3 + x_4 + x_6 + x_7 + x_8 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + x_{15} + x_{16}$,

$B = x_1 + x_3 + x_4 + 3x_5 + x_6 + x_7 + 7x_9 + x_{11} + x_{12} + x_{13} + x_{15}$,

$C = x_1 + x_2 + x_4 + 7x_5 + x_8 + 3x_9 + x_{10} + x_{14} + x_{16}$.

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:

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

(по модулю 10).

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

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

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

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

Но тогда первая строка есть сумма третьей и второй по модулю 10. Вычитая из первой строки вторую и третью, а затем из торой строки третью, получим, что система (*) равносильна системе

$$\begin{cases} x_{15} = 4x_5 - x_6 - x_7 + x_8 - 4x_9 + x_{10} - x_{11} - x_{12} - x_{13} + x_{14} \\ x_{16} = -7x_5 - x_8 - 3x_9 - x_{10} - x_{14} \end{cases}$$

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_3	x_4		x_6	x_7	x_8		x_{10}	x_{11}	x_{12}
x_1		x_3	x_4	$3x_5$	x_6	x_7		$7x_9$		x_{11}	x_{12}
x_1	x_2		x_4	$7x_5$			x_8	$3x_9$	x_{10}		

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 $10^{10} - 9^{10}$.

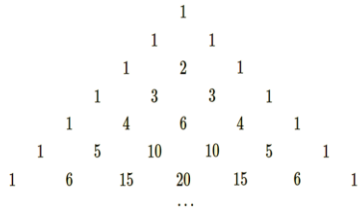
2. Докажите, что существует натуральное число, кратное 2015, десятичная запись которого имеет вид 12351235…1235 (т.е. образована последовательным повторением фрагмента 1235).

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 12351235…1235:

$$x_1 = 1235,\ x_2 = 12351235,\ x_3 = 123512351235,\ \ldots \qquad (1)$$

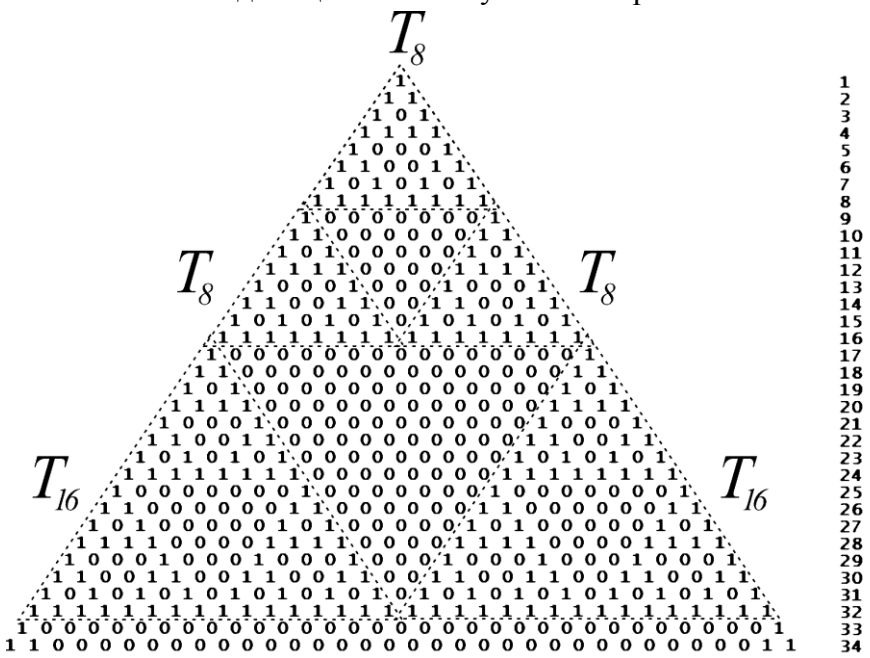
Среди них найдутся два числа, x_m и x_n $(m > n)$, которые имеют одинаковые остатки при делении на 403. (Действительно, чисел вида (1) бесконечно много, а различных остатков от деления на 403 всего 403 штуки.) Тогда их разность $x_m - x_n$ делится на 403. Теперь отбросим все нули на конце десятичной 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 1024? б) в строке с номером 1050?



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 1024 четных чисел нет.



Обратимся теперь к строке 1050. Уже понятно, что, после строки 1024, идет формирование "с нуля" двух одинаковых треугольников. Строки с номером 26 в этих новых треугольниках как раз и содержатся в строке 1050 исходного (большого) треугольника, т.к. 1050=1024+16. Значит единиц в строке 1050 вдвое больше, чем единиц в строке с номером 26. Количество же 1 в строке 26 можно подсчитать непосредственно, или, рассуждая аналогично, заметить, что их вдвое больше, чем в строке 10. То есть всего в строке 26 восемь 1. Значит в строке 1050 их 16. Остальные 1034 – нули.

Ответ: а) 0, б) 1034.

4. Рассмотрим множество всех точек плоскости, координаты которых имеют вид $(m+2n, 3m-n)$, 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 $(m+2n, 3m-n), m, n \in \mathbb{Z}$, 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 $(m_1+2n_1, 3m_1-n_1), m_1, n_1 \in \mathbb{Z}$ существует перпендикуляр вида $(m_2+2n_2, 3m_2-n_2), m_2, n_2 \in \mathbb{Z}$. Другими словами надо решить относительно $k, m_2, n_2 \in \mathbb{Z}$ уравнение

$$k(n_1-3m_1, m_1+2n_1) = (m_2+2n_2, 3m_2-n_2).$$

   Перепишем полученное уравнение в виде системы

$$\begin{cases} k(n_1-3m_1)=m_2+2n_2, \\ k(m_1+2n_1)=3m_2-n_2, \end{cases}$$

которую несложно преобразовать в эквивалентную систему

$$\begin{cases} m_2+2n_2=k(n_1-3m_1), \\ -7n_2=k((m_1+2n_1)-3(n_1-3m_1)), \end{cases}$$

разрешимость которой очевидна – последовательно выбираем подходящие целые числа k, n_2 и m_2.

Таким образом, для всякого вектора $(m_1+2n_1, 3m_1-n_1), m_1, n_1 \in \mathbb{Z}$ существует перпендикулярный ему вектор $k(n_1-3m_1, m_1+2n_1)$ вида $(m_2+2n_2, 3m_2-n_2)$. Нетрудно понять, что вектора $k(m_1+2n_1, 3m_1-n_1)$ и $k(n_1-3m_1, m_1+2n_1)$ являются сторонами искомого квадрата.

2. Методом пристального взгляда, в графическом представлении множества точек $(m+2n, 3m-n), m, n \in Z$, 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 4^4. В качестве названий города имеют различные цифровые комбинации вида (a,b,c,d), где a,b,c и d – целые числа из множества $\{0,1,2,3\}$. Два города, названия которых отличаются одной цифрой, называются *соседними*. Например, города (3201) и (3001) соседние, а (1111) и (3311) – 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 (0000), (1000), (2000) и (3000) любые два являются соседними. Значит, цветов надо минимум четыре. Покажем, что четырех цветов достаточно. Имеющиеся у нас цвета будем называть цвет-0, цвет-1,цвет-2, цвет-3. Флаг города будет окрашен в цвет, номер которого равен остатку от деления на 4 суммы цифр в названии этого города. (Например, для города (3201) 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, 4-х цветов достаточно.

Ответ: 4.

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: $y_1 = f\left(r_{16}(x_1 + 3 \cdot y_0)\right), y_2 = f\left(r_{16}(x_2 + 3 \cdot y_1)\right), y_3 = f\left(r_{16}(x_3 + 3 \cdot y_2)\right)$

a \ b	1	2	3	11	12	13
1	-	+	-	-	-	+
2	-	+	+	-	-	-
3	+	-	+	-	+	-
4	+	-	-	-	+	-
5	-	-	-	+	-	+
6	-	-	-	+	-	+
7	-	+	+	-	-	-
8	-	+	+	-	+	-
9	+	-	-	-	+	-
10	+	-	-	+	-	+

, $y_4 = f\left(r_{16}(x_4 + 3\cdot y_3)\right), y_5 = f\left(r_{16}(x_5 + 3\cdot y_4)\right)$, где $y_0 = 2$, $r_{16}(x)$ – 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: 13,13,1,11,7. 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?

Решение

1. Типовые рассуждения для каждого варианта.

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}

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

Вариант рассуждений а).

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 варианта 1 (зашифрованный пароль: 13,13,1,11,7).

Рассмотрим столбец из данной в условии таблицы с $b = 11$. Из-за закономерностей в образовании “+” не трудно догадаться, что подходящей под критерий структурой будет

+	+	-	-	-	-
15	0	1	2	3	4

Поэтому $a_1 = 15$ и $\pi^{-1}(11) = r_{16}(3 \cdot 15 - 1) = 12$, что позволяет найти x_4:

$x_4 = r_{16}(\pi^{-1}(11) - 3 \cdot 1) = r_{16}(12 - 3) = 9$.

Рассмотрим столбец из данной в условии таблицы с $b = 1$. Не трудно заметить, что подходящей под критерий структурой будет

+	+	-	-	-	-
3	4	5	6	7	8

Поэтому $a_1 = 3$ и $\pi^{-1}(1) = r_{16}(3 \cdot 3 - 1) = 8$, что позволяет найти x_3:

$x_3 = r_{16}(\pi^{-1}(1) - 3 \cdot 13) = r_{16}(8 - 7) = 1$.

Рассмотрим столбец из данной в условии таблицы с $b = 13$. Из-за закономерностей в образовании “-” не трудно догадаться, что подходящей структурой будет

+	+	-	-	-	-
10	11	12	13	14	15

Поэтому $a_1 = 10$ и $\pi^{-1}(13) = r_{16}(3 \cdot 10 - 1) = 13$, что позволяет найти x_1, x_2:

$x_1 = r_{16}(\pi^{-1}(13) - 3 \cdot 2) = r_{16}(13 - 6) = 7$;

$x_2 = r_{16}(\pi^{-1}(13) - 3 \cdot 13) = r_{16}(13 - 7) = 6$.

Ответ: пароль Алисы 7,6,1,9.