10 класс XXIX Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии

1 вариант

1. На билетах в кинотеатры Криптоландии проставляется шестизначный номер от (0,0,0,0,0,0) до (8,8,8,8,8,8). При этом используются только цифры 0,1,2,3,4,5,6,7,8. Билет считается «счастливым», если остатки от деления на 9 суммы первых трех цифр и суммы последних трех цифр отличаются на фиксированное число $k = 2$. Например, билеты с номерами 123026 и 123661 – счастливые, а с номерами 123000 и 876111 – нет. Найдите число счастливых билетов.

Решение: Количество трёхзначных чисел $x_1x_2x_3$, у которых остаток от деления на 9 суммы цифр равен фиксированному значению $t \in \{0,1, \dots ,8\}$, равно $9^2 = 81$, поскольку любые две цифры однозначно определяют третью из соотношения $r_9(x_1 + x_2 + x_3) = t$. Приведём возможные варианты для значений остатков для первой и последней тройки цифр:

(0,2), (1,3), … , (6,8), (2,0), (3,1), … , (8,6)

их число равно $2 \times 7 = 14$, и тогда общее число счастливых билетов равно $2 \times 7 \times 9^2 \times 9^2 = 2 \times 7 \times 9^4 = 91854$.

Ответ: 91854.

2. Известно, что p_1, p_2, p_3 – различные простые числа и $p_3^2 = p_1 \cdot p_2 + 4$. Найдите все такие числа p_1, p_2, p_3. Ответ обоснуйте.

Решение: Поскольку p_1, p_2 – простые числа и

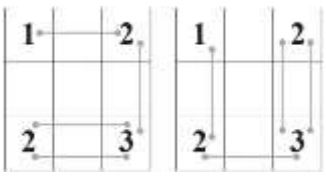
$$(p_3 - 2)(p_3 + 2) = p_1 \cdot p_2,$$

постольку возможны варианты:

1. $p_3 - 2 = 1$. Тогда $p_3 = 3$ и $p_1p_2 = 5$, чего быть не может.
2. $p_1 = p_3 - 2$, $p_2 = p_3 + 2$ (с точностью до переобозначений). И т.к. $p_3 \neq 3$, из чисел $p_3 - 2$ и $p_3 + 2$ одно делится на 3. А в силу простоты чисел p_1 и p_2 одно равно 3. Непосредственно проверяется, что p_2 не может равняться 3. Отсюда $p_1 = 3$, $p_3 = 5$, $p_2 = 7$.

Ответ: $p_1 = 3$, $p_3 = 5$, $p_2 = 7$ либо $p_1 = 7$, $p_3 = 5$, $p_2 = 3$.

3. Сообщение передается в виде таблицы 7 × 7 клеток. В каждой клетке записана либо буква, либо цифра. Чтобы прочитать сообщение, необходимо зачеркнуть отрезками лишние символы. Отрезки проводят по следующим правилам (см. примеры): 1) концы отрезков лежат только в клетках с цифрами, причем цифра показывает сколько концов в этой клетке лежит, 2) отрезки могут проходить только горизонтально или вертикально, 3) две цифры могут быть



3	с	з	**4**	е	м	**3**
ю	с	е	р	д	е	у
ш	в	в	н	**2**	ь	**5**
о	г	д	р	б	о	ф
а	а	о	к	д	х	л
я	ж	н	т	ц	и	у
1	я	к	**2**	т	е	**2**

соединены не более, чем двумя отрезками. Прочитайте сообщение, которое получается выписыванием каждой третьей не зачёркнутой буквы.

Решение: Для решения задачи следует для каждого числа рассматривать количество соседей – чисел, с которыми оно может соединяться отрезками.

3	**=**	**=**	**4**	**–**	**–**	**3**
|	**с**	е	**|**	д	**е**	**‖**
|	в	в	**|**	**2**	**=**	**5**
|	**г**	д	**|**	б	**о**	**|**
|	а	о	**|**	**д**	х	**|**
|	ж	**н**	**|**	ц	и	**|**
1	**я**	к	**2**	**–**	**–**	**2**

Если число соответствует удвоенному количеству своих соседей, то с каждым соседом его соединяет по два отрезка. Если число равно удвоенному количеству своих соседей, то с каждым из них оно соединяется как минимум одним отрезком.

Начинать можно с рассмотрения угловых клеток таблицы, это позволяет провести первые отрезки. Затем возможно рассмотреть клетки вдоль краёв таблицы. По мере проведения отрезков между числами, начинает уменьшаться количество возможных вариантов построения новых отрезков. Если к числу приходит необходимое количество отрезков, значит, оно уже не может соединяться с другими своими соседями.

В условии написано, что сообщение составляет каждая третья буква, но не указано, с какой буквы следует начинать чтение. Выписывая три возможных варианта, получаем, что читаемый будет лишь в случае чтения каждой третьей незачёркнутой буквы, начиная с первой.

Ответ: сегодня.

4. Для зашифрования сообщении каждая его буква заменяется числом по таблице (внизу страницы). В результате получается числовая последовательность $x_1, \dots, x_n$. Затем вырабатывают последовательность $\gamma_1, \gamma_2, \dots$ по следующему правилу: γ_1 – некоторое натуральное число, γ_2 – сумма цифр квадрата γ_1, увеличенная на 1, и т.д. Например, если $\gamma_1 = 7$, то $\gamma_2 = 14$, $\gamma_3 = 17$ и т.д. После этого выбирается некоторое натуральное t и формируется зашифрованное сообщение по правилу: $r_{32}(x_1 + \gamma_t), \dots, r_{32}(x_n + \gamma_{t+n-1})$, где $r_{32}(a)$ – остаток от деления числа a на 32. Известно, что для $\gamma_1 = 2019$ и некоторого t получился следующий шифртекст: 10, 6, 26, 22, 15, 13, 20, 13, 29, 13, 28, 23, 4. Восстановите исходное сообщение.

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: Будем перебирать возможные значения t, а затем, «раскрутив» последовательность $\gamma_t, \ldots, \gamma_{t+n-1}$, попробуем расшифровать на ней текст. Занесем в таблицу последовательность $\gamma_1, \gamma_2, \ldots$ и соответствующий открытый текст (ОТ), который получается если расшифровать шифртекст с помощью последовательности $\gamma_t, \ldots, \gamma_t+n-1$.

t	γ_i	ОТ		ОТ		ОТ		ОТ		ОТ	
1	2019	7	З								
2	28	10	К	14	О						
3	20	6	Ж	18	Т	22	Ц				
4	5	17	С	21	Х	1	Б	5	Е		
5	8	7	З	14	О	18	Т	30	Ю	2	В
6	11	2	В	4	Д	11	Л	15	П	27	Ы
7	5	15	П	8	И	10	К	17	С	21	Х
8	8	5	Е	12	М	5	Е	7	З	14	О
9	11	18	Т	2	В	9	Й	2	В	4	Д
10	5	8	И	24	Ш	8	И	15	П	8	И
11	8	20	Ф	5	Е	21	Х	5	Е	12	М
12	11	12	М	17	С	2	В	18	Т	2	В
13	5	31	Я	18	Т	23	Ч	8	И	24	Ш
14	8			28	Ь	15	П	20	Ф	5	Е
15	11					25	Щ	12	М	17	С
16	5							31	Я	18	Т
17	8									28	Ь

Нетрудно из таблицы заметить, что последовательность $\{\gamma_i\}$ периодическая с периодом (5, 8, 11) и подходом (2019, 28, 20), поэтому для расшифрования сообщения достаточно начинать расшифровывать при t = 1, … 6. . Осмысленный текст получается при t = 5.

Ответ: выходим в шесть.

5. Для зашифрования осмысленного слова его буквы переводят в числа $x_1, x_2, \ldots, x_n$ по таблице (внизу страницы). Затем выбирают натуральные числа x_0 и k. Далее число x_0 приписывают в начало последовательности $x_1, x_2, \ldots, x_n$, а число $x_{n+1} = x_0 + 11^n$ (где n – длина слова) – в ее конец. Получившаяся в результате последовательность $x_0, x_1, \ldots, x_n, x_{n+1}$ (где $x_{n+1} = x_0 + 11^n$) затем преобразуется в последовательность $y_0, y_1, \ldots, y_n, y_{n+1}$ по формуле

$$y_i = r_{32}(x_i + 2x_i \cdot k + k), \qquad i = 0, \ldots, n + 1,$$

где $r_{32}(a)$ – остаток от деления числа a на 32. Затем числа $y_0, y_1, \ldots, y_{n+1}$ заменяют буквами согласно таблице. В результате получилось вот что: **ЩБНХБМЩХЪ**. 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: Нетрудно понять, что длина слова $n = 7$, а также несложно найти остаток $r_{32}(11^n) = 3$. Преобразуем зашифрованный текст в последовательность чисел: $y_0 = 25$, $y_1 = 1$, $y_2 = 13$, $y_3 = 21$, $y_4 = 1$, $y_5 = 12$, $y_6 = 25$, $y_7 = 21$, $y_8 = 26$.

Из условия следует, что $x_8 - x_0 = 3$. Рассмотрим разность $r_{32}(y_8 - y_0) = r_{32}(x_8 + 2x_8 \cdot k + k - x_0 - 2x_0 \cdot k - k) = = r_{32}((1 + 2k) \cdot (x_8 - x_0)) = r_{32}(3 \cdot (1 + 2k))$.

Имеем: $r_{32}(3 \cdot (1 + 2k)) = 1$.

Заметим, что $r_{32}(3 \cdot 11) = 1$. Откуда находим $r_{32}(1 + 2k) = 11$. Значит,

$1 + 2k = 11 + 32t \Leftrightarrow k = 5 + 16t$

Значит, $r_{32}(k) = 5$ или $r_{32}(k) = 21$. Рассмотрим первый случай. Согласно правилу зашифрования

$y_1 = 1 = r_{32}(x_1 + 2x_1 \cdot 5 + 5) = r_{32}(x_1 \cdot 11 + 5)$,

$\Leftrightarrow 11x_1 + 5 = 1 + 32t \Leftrightarrow 11x_1 = -4 + 32t$

Т.е. $r_{32}(11x_1) = 28 \Longrightarrow r_{32}(33x_1) = r_{32}(28 \cdot 3) = 20 \Longrightarrow r_{32}(x_1) = 20$.

Аналогично продолжая, получим последовательность 20, 24, 16, 20, 21, 28, 16.

Что соответствует неосмысленному слову ФШРФХЬР.

Рассмотрим второй случай $r_{32}(k) = 21$. Имеем $y_1 = 1 = r_{32}(x_1 + 2x_1 \cdot 21 + 21) = r_{32}(x_1 \cdot 43 + 21)$, $\Leftrightarrow 11x_1 + 21 = 1 + 32t \Leftrightarrow 11x_1 = -20 + 32t \Longrightarrow r_{32}(11x_1) = 12 \Longrightarrow r_{32}(33x_1) = r_{32}(12 \cdot 3) = 4 \Longrightarrow r_{32}(x_1) = 4$.

$y_2 = 13 = r_{32}(x_2 + 2x_2 \cdot 21 + 21) = r_{32}(x_2 \cdot 43 + 21), \Leftrightarrow 11x_2 + 21 = 13 + 32t \Leftrightarrow 11x_2 = -8 + 32t$ $\Longrightarrow r_{32}(11x_2) = 24 \Longrightarrow r_{32}(33x_1) = r_{32}(24 \cdot 3) = 8 \Longrightarrow r_{32}(x_2) = 8$. И т.д.

Окончательно получим, исходную последовательность чисел 4, 8, 0, 4, 5, 12, 0.

Согласно табл. ей соответствует слово ДИАДЕМА.

Ответ: ДИАДЕМА.

6. Каждому из четырех абонентов A_1, A_2, A_3, A_4 надо выдать по два уравнения вида $ax + by + cz = d$, где $a, b, c, d, x, y, z \in \{0,1\}$. Значения секретных битов w, x, y, z одинаковы для всех абонентов и им заранее неизвестны. Пусть, например, A_1 получит уравнения $\{x + y + z = 1, x + y + 0 \cdot z = 1\}$, а A_2 – $\{0 \cdot x + y + 0 \cdot z = 1, 0 \cdot x + 0 \cdot y + 0 \cdot z = 0\}$. Здесь традиционно полагается, что $1 + 1 = 0$. Тогда, объединившись, из имеющихся в их распоряжении четырех уравнений они однозначно найдут, что $x = 0$, $y = 1$, $z = 0$. При этом будем говорить, что пара абонентов $\{A_1, A_2\}$ может *достоверно вычислить* секретные биты x, y, z. Приведите хотя бы один пример уравнений, которые надо выдать этим четырем абонентам, чтобы каждая пара $\{A_1, A_2\}$, $\{A_1, A_3\}$, $\{A_1, A_4\}$ могла достоверно вычислить x, y, z, но чтобы при этом ни одна другая пара абонентов это сделать не смогла и ни один абонент в одиночку не смог бы найти даже один секретный бит.

Решение: "Спрятать" один бит, пусть z, от всех абонентов, но сделать его доступным для пары $\{A_i, A_j\}$ можно следующим общим способом: выбрать некоторый бит a, пусть $a = p$, выдать это уравнение A_i, а абоненту A_j – уравнение $a + z = q$ ($p, q \in \{0,1\}$ – произвольные, но зафиксированные значения). Ни A_i, ни A_j не могут достоверно получить значение бита z из имеющихся у них уравнений, но вместе они смогут его вычислить: $a + a + z = z = p + q$.

Применительно к задаче, в качестве бита a можно использовать сумму других двух секретных бит. Выдадим абоненту A_2 уравнение $x + y = p_1$, а A_1 – уравнение $x + y + z = q_1$, тогда сложив эти уравнения вместе, пара абонентов $\{A_1, A_2\}$ найдет $z = p_1 + q_1$. Выдадим абоненту A_2 также

уравнение $x + z = p_2$, тогда они найдут бит $y = p_2 + q_1$. Очевидно, что при таком способе, если пара абонентов находит 2 бита, то она найдет и третий, так как он будет присутствовать хотя бы у одного абонента в линейной комбинации: $x = p_1 + p_2 + q_1$.

Этот способ можно распространить и на пары абонентов $\{A_1, A_3\}$, $\{A_1, A_4\}$, проверяя при этом, что пары абонентов $\{A_2, A_3\}$, $\{A_2, A_4\}$, $\{A_3, A_4\}$ не смогут найти ни одного бита.

Ответ: A_1: $x + y + z = q_1$; A_2, A_3, A_4: $x + y = p_1$, $x + z = p_2$.