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

УСЛОВИЯ И РЕШЕНИЯ

Москва 2020

Оглавление

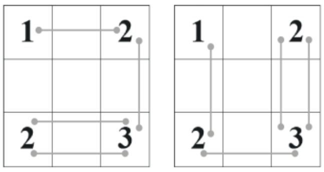
Приводимые задания предлагались в трех возрастных категориях (9, 10, 11 классы) по два равноценных по сложности варианта в 9 и 10 классах и по два равноценных по сложности варианта в каждом из трех регионов (ЗАПАД, СИБИРЬ, ВОСТОК) для участников 11 класса. Тематика отдельных задач в разных классах пересекается, при этом младшим классам предлагались более легкие варианты заданий.

9 КЛАСС

УСЛОВИЯ ЗАДАЧ

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

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**



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

5. Для зашифрования осмысленного слова его буквы переводят в числа $x_1, x_2, \dots, x_n$ по таблице (внизу страницы). Затем выбирают натуральные числа x_0 и k. Далее число x_0 приписывают в начало последовательности $x_1, x_2, \dots, x_n$, а число $x_{n+1} = x_0 + 11^n$ (где n – длина слова) – в ее конец. Получившаяся в результате последовательность $x_0, x_1, \dots, x_n, x_{n+1}$ (где $x_{n+1} = x_0 + 11^n$) затем преобразуется в последовательность $y_0, y_1, \dots, y_n, y_{n+1}$ по формуле
$$y_i = r_{32}(x_i + 2x_i \cdot k + k), \qquad i = 0, \dots, n+1,$$
где $r_{32}(a)$ – остаток от деления числа a на 32. Затем числа $y_0, y_1, \dots, y_{n+1}$ заменяют буквами согласно таблице. В результате получилось вот что: **ЩБНХБМЩХЪ**. 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

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.

РЕШЕНИЯ ЗАДАЧ

Задача 1

Количество трёхзначных чисел $x_1x_2x_3$, у которых остаток от деления на 9 суммы цифр равен фиксированному значению $t \in \{0,1,\ldots,8\}$, 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:

$$(0,2), (1,3), \ldots, (6,8),$$
$$(2,0), (3,1), \ldots, (8,6)$$

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.

Задача 2

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 $p_1 = 7,\ p_3 = 5,\ p_2 = 3$.

Задача 3

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.

Задача 4

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

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 $t = 1, \dots 6.$. Осмысленный текст получается при $t = 5$.

Ответ: выходим в шесть.

Задача 5

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

$$r_{32}(y_8 - y_0) = r_{32}(x_8 + 2x_8 \cdot k + k - x_0 - 2x_0 \cdot k - k) =$$
$$= r_{32}\big((1 + 2k) \cdot (x_8 - x_0)\big) = r_{32}\big(3 \cdot (1 + 2k)\big).$$

Имеем:

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

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

Аналогично продолжая, получим последовательность 20, 24, 16, 20, 21, 28, 16. Что соответствует неосмысленному слову ФШРФХЬР.

Рассмотрим второй случай $r_{32}(k) = 21$. Имеем

$$y_1 = 1 = r_{32}(x_1 + 2x_1 \cdot 21 + 21) = r_{32}(x_1 \cdot 43 + 21),$$
$$\Leftrightarrow 11x_1 + 21 = 1 + 32t \Leftrightarrow 11x_1 = -20 + 32t$$
$$\Rightarrow r_{32}(11x_1) = 12 \Rightarrow r_{32}(33x_1) = r_{32}(12 \cdot 3) = 4 \Rightarrow r_{32}(x_1) = 4.$$
$$y_2 = 13 = r_{32}(x_2 + 2x_2 \cdot 21 + 21) = r_{32}(x_2 \cdot 43 + 21),$$
$$\Leftrightarrow 11x_2 + 21 = 13 + 32t \Leftrightarrow 11x_2 = -8 + 32t$$
$$\Rightarrow r_{32}(11x_2) = 24 \Rightarrow r_{32}(33x_1) = r_{32}(24 \cdot 3) = 8 \Rightarrow r_{32}(x_2) = 8. \text{ И т.д.}$$

Окончательно получим, исходную последовательность чисел

$$4, 8, 0, 4, 5, 12, 0.$$

Согласно табл. ей соответствует слово ДИАДЕМА.

Ответ: ДИАДЕМА.

Задача 6

“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.

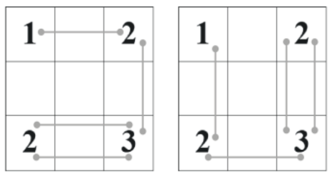
Ответ: A_1: $x + y + z = q_1$; A_2, A_3, A_4: $x + y = p_1$, $x + z = p_2$.

10 КЛАСС

УСЛОВИЯ ЗАДАЧ

1. На билетах в кинотеатры Криптоландии проставляется шестизначный номер от (0,0,0,0,0,0) до (6,6,6,6,6,6). При этом используются только цифры 0,1,2,3,4,5,6. Билет считается «счастливым», если остатки от деления на 7 суммы первых трех цифр и суммы последних трех цифр отличаются на фиксированное число $k = 3$. Например, билеты с номерами 123226 и 111661 – счастливые, а с номерами 123000 и 666111 – нет. Найдите число счастливых билетов.
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.
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 соединены не более, чем двумя отрезками. Прочитайте сообщение, которое получается выписыванием каждой третьей незачеркнутой буквы.

1	н	**2**	б	а	**1**	о
е	у	с	р	с	п	д
2	о	**6**	с	е	**3**	у
щ	е	е	т	т	д	н
а	м	**5**	к	в	ф	**2**
р	к	т	л	ц	а	л
1	и	**2**	к	**1**	м	**2**



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: $r_{32}(x_1 +$

$\gamma_t), \ldots, r_{32}(x_n + \gamma_{t+n-1})$, где $r_{32}(a)$ – остаток от деления числа a на 32. Известно, что для $\gamma_1 = 1407$ и некоторого t получился следующий шифртекст: 15, 11, 18, 7, 29, 13, 7, 25, 23, 20, 16, 18, 7, 9, 23, 25, 10. 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

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 $x_{n+1} = x_0 + 3^n$ (где n – длина слова) – в ее конец. Получившаяся в результате последовательность $x_0, x_1, \ldots, x_n, x_{n+1}$ (где $x_{n+1} = x_0 + 3^n$) затем преобразуется в последовательность $y_0, y_1, \ldots, y_n, y_{n+1}$ по формуле

$$y_i = r_{32}(x_i + 10x_i \cdot k + k), \quad i = 0,1,\ldots,n+1,$$

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 получили вот что: **ЩВМЫЭДЫЭЪ**. 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

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.

РЕШЕНИЯ ЗАДАЧ

Задача 1

Количество трёхзначных чисел $x_1x_2x_3$, у которых остаток от деления на 7 суммы цифр равен фиксированному значению $t \in \{0,1,\ldots,6\}$, равно $7^2 = 49$, 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:

$$(0,3), (1,4), \ldots, (3,6),$$
$$(3,0), (4,1), \ldots, (6,3)$$

их число равно $2 \times 4 = 8$, и тогда общее число счастливых билетов равно $2 \times 4 \times 7^2 \times 7^2 = 2 \times 4 \times 7^4 = 19208$.

Ответ: 19208.

Задача 2

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 $p_1 p_2 = 5$, 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 $p_1 = 7,\ p_3 = 5,\ p_2 = 3$.

Задача 3

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

1	—	**2**	**б**	а	**1**	о
е	у	│	р	**с**	│	д
2	—	**6**	═	═	**3**	у
│	**е**	║	т	т	**д**	н
│	м	**5**	—	—	—	**2**
│	**к**	║	л	ц	**а**	│
1	и	**2**	к	**1**	—	**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: беседка.

Задача 4

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

t	γ_i					

1	1407	16	Р								
2	46	29	Э	1	Б						
3	11	7	З	0	А	4	Д				
4	5	2	В	13	Н	6	Ж	10	К		
5	8	21	Х	31	Я	10	К	3	Г	7	З
6	11	2	В	18	Т	28	Ь	7	З	0	А
7	5	2	В	8	И	24	Ш	2	В	13	Н
8	8	17	С	31	Я	5	Е	21	Х	31	Я
9	11	12	М	14	О	28	Ь	2	В	18	Т
10	5	15	П	18	Т	20	Ф	2	В	8	И
11	8	8	И	12	М	15	П	17	С	31	Я
12	11	7	З	5	Е	9	Й	12	М	14	О
13	5	2	В	13	Н	11	Л	15	П	18	Т
14	8	1	Б	31	Я	10	К	8	И	12	М
15	11	12	М	30	Ю	28	Ь	7	З	5	Е
16	5	20	Ф	18	Т	4	Д	2	В	13	Н
17	8	2	В	17	С	15	П	1	Б	31	Я
18	11			31	Я	14	О	12	М	30	Ю
19	5					5	Е	20	Ф	18	Т
20	8							2	В	17	С
21	11									31	Я

Нетрудно из таблицы заметить, что последовательность $\{\gamma_i\}$ периодическая с периодом (11, 5, 8) и подходом (1407, 46), поэтому для расшифрования сообщения достаточно начинать расшифровывать при $t = 1, \dots 6$. Осмысленный текст получается при $t = 5$.

Ответ: занятия отменяются.

Задача 5

Нетрудно понять, что длина слова $n = 7$, а также несложно найти остаток $r_{32}(3^n) = 11$.

Преобразуем зашифрованный текст в последовательность чисел:

$$y_0 = 25, y_1 = 2, y_2 = 12, y_3 = 27, y_4 = 29, y_5 = 4, y_6 = 27,$$
$$y_7 = 29, y_8 = 26.$$

Из условия следует, что $x_8 - x_0 = 11$. Рассмотрим разность

$$r_{32}(y_8 - y_0) = r_{32}(x_8 + 10x_8 \cdot k + k - x_0 - 10x_0 \cdot k - k) =$$
$$= r_{32}\big((1 + 10k) \cdot (x_8 - x_0)\big) = r_{32}\big(11 \cdot (1 + 10k)\big).$$

Имеем:

$$r_{32}\big(11 \cdot (1 + 10k)\big) = 1.$$

Заметим, что $r_{32}(3 \cdot 11) = 1$. Откуда находим $r_{32}(1 + 10k) = 3$. Значит,

$$1 + 10k = 3 + 32t \Leftrightarrow 5k = 1 + 16t \Leftrightarrow 65k = 13 + 13 \cdot 16t$$

Значит, $r_{16}(65k) = r_{16}(k) = 13$. Поэтому $r_{32}(k) = 13$ или $r_{32}(k) = 29$. Рассмотрим первый случай. Согласно правилу зашифрования

$$y_1 = 2 = r_{32}(x_1 + 10x_1 \cdot 13 + 13) = r_{32}(x_1 \cdot 3 + 13),$$
$$\Leftrightarrow 3x_1 + 13 = 2 + 32t \Leftrightarrow 3x_1 = -11 + 32t$$

Т.е. $r_{32}(3x_1) = 21 \Rightarrow r_{32}(33x_1) = r_{32}(21 \cdot 11) = 7 \Rightarrow r_{32}(x_1) = 7$.

Аналогично продолжая, получим последовательность 7, 21, 26, 16, 29, 26, 16. Что соответствует неосмысленному слову ЗХЪРЭЪР.

Рассмотрев аналогично второй случай $r_{32}(k) = 29$, можно убедиться, что ему соответствует осмысленное слово ЧЕКАНКА

Ответ: ЧЕКАНКА.

Задача 6

“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 $\{\mathrm{A}_1, \mathrm{A}_3\}, \{\mathrm{A}_1, \mathrm{A}_4\}$, проверяя при этом, что пары абонентов $\{\mathrm{A}_2, \mathrm{A}_3\}, \{\mathrm{A}_2, \mathrm{A}_4\}, \{\mathrm{A}_3, \mathrm{A}_4\}$ не смогут найти ни одного бита.

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

11 КЛАСС

УСЛОВИЯ ЗАДАЧ

1. Известно, что p, p_1, p_2, p_3 – различные простые числа, и $p^3 - 2p^2 - 16p = p_1 \cdot p_2 \cdot p_3 - 32$. Найдите все такие числа p, p_1, p_2, p_3. Ответ обоснуйте.
2. Для зашифрования осмысленного слова его буквы переводят в числа $x_1, x_2, \ldots, x_n$ по таблице. 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 $x_{n+1} = x_0 + 19^{n+4}$ (где n – длина слова) – в ее конец. Получившаяся в результате последовательность $x_0, x_1, \ldots, x_n, x_{n+1}$ затем преобразуется в последовательность $y_0, y_1, \ldots, y_n, y_{n+1}$ по формуле $y_i = r_{32}(x_i + 6x_i \cdot k^3 + k)$, $i = 0,1, \ldots, n+1$, 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 получили вот что: **КЙЫЦНБНЦЛ**. Какое слово было зашифровано?

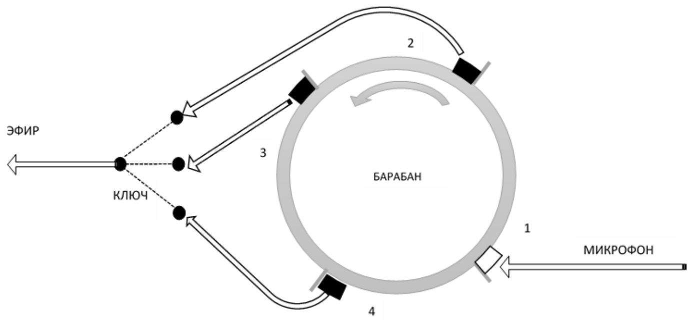
А	Б	В	Г	Д	Е Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

3. Каждому из четырех абонентов A_1, A_2, A_3, A_4 надо выдать по два уравнения вида $aw + bx + cy + +dz = t$, где $a, b, c, d, t, w, x, y, z \in \{0,1\}$. Значения секретных битов w, x, y, z одинаковы для всех абонентов и им заранее неизвестны. Приведите хотя бы один пример уравнений, которые надо выдать этим четырем абонентам, чтобы каждая пара $\{A_1, A_3\}, \{A_1, A_4\}, \{A_2, A_3\}$ могла достоверно вычислить w, x, y, z, но чтобы при этом: 1) ни одна другая пара абонентов не могла бы достоверно вычислить более одного секретного бита; 2) ни один абонент в одиночку не был в состоянии достоверно вычислить даже один секретный бит. Например, если абонент A_1 получит уравнения $\{w + x + y + z = 1;\ w + x + 0 \cdot y + 0 \cdot z = 1\}$, а A_2 – $\{w + 0 \cdot x + y + 0 \cdot z = 0;\ w + x + 0 \cdot y + +z = 0\}$. Тогда, объединившись, из имеющихся в их распоряжении четырех уравнений они однозначно найдут, что $w = 1, x = 0, y = 1, z = 1$. При этом будем говорить, что пара абонентов $\{A_1, A_2\}$ может *достоверно вычислить* секретные биты w, x, y, z. Здесь традиционно полагается, что 1+1=0.

4. Саша решил отправить Маше записку. Для этого каждую букву сообщения он заменил комбинацией из 0 и 1 согласно таблице (А – 00000, Б – 00001, …, Я – 11111). Взяв день "Д" и номер месяца "М" своего рождения Саша вычислил $u_1 = \text{Д}^2 + \text{М}^2, u_2 = \text{Д} \cdot \text{М}, u_3 = \text{Д} - \text{М}$. Далее Саша вычислил четвертое $u_4 = r_{32}(u_1 + u_2 u_3)$, пятое $u_5 = r_{32}(u_2 + u_3 u_4)$, …, n-ое число $u_n = r_{32}(u_{n-3} + u_{n-2} u_{n-1})$, где $r_{32}(a)$ – остаток от деления числа a на 32. К i-му биту символу исходного сообщения (0 или 1) он прибавил число u_i и взял остаток от деления на 2. Полученную последовательность из 0 и 1 он вновь преобразовал в буквы по таблице и получил следующее сообщение: **ЖДУЛЩБШЛТВШЩЧ**. Помогите Маше прочитать его.

А	Б	В	Г	Д	Е	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

5. Звук записывается на магнитный слой барабана, который вращается с постоянной скоростью, совершая один оборот за 4 секунды. Рядом с барабаном по окружности через равные расстояния размещены записывающая (1) и три



читающие головки (2), (3), (4). В каждый момент времени в телефонную линию передается сигнал с одной из читающих головок. Устройство спроектировано так, что каждый участок сигнала будет передан в линию один раз, а сама передача стартует, как только начало записи окажется у 3-й читающей головки. Сколько различных вариантов звука, переданного в линию, может получиться, если сообщение длилось 20 секунд?

6. Рассмотрим девять чисел $k_1, \dots, k_9$, где $k_i \epsilon \{0,1,2\}$. При этом хотя бы одно число k_i отлично от нуля. С помощью этих чисел вырабатывают последовательность $u_1, u_2, \dots, u_{2019}$ по формулам: $u_1 = k_1, u_2 = k_2, \dots, u_9 = k_9,\ u_{i+9} = r_3(u_i + u_{i+1})$, $i = 1,2, \dots, 2010$, где $r_3(a)$ – остаток от деления числа a на 3. Найдите такое наименьшее натуральное число l, что какие бы исходные числа $k_1, \dots, k_9$ мы ни взяли, в последовательности $u_1, u_2, \dots, u_l$ каждое из чисел 0, 1 и 2 гарантированно встретится хотя бы один раз.

РЕШЕНИЯ ЗАДАЧ

Задача 1

Пусть $p_1 < p_2 < p_3$. По условию $p^3 - 2p^2 - 16p + 32 = p_1 \cdot p_2 \cdot p_3$. Разложим левую часть на множители:

$$(p-2)(p-4)(p+4) = p_1 \cdot p_2 \cdot p_3. \qquad (1)$$

Непосредственной проверкой убеждаемся, что $p \neq 2,3,5$. Значит $p > 5$. Следовательно, числа в левой части (1) различны и отличны от 1. Поэтому $p - 4 = p_1$, $p - 2 = p_2$, $p + 4 = p_3$. Поскольку p на 3 не делится, возможны случаи:

- число p при делении на 3 дает остаток 1. Тогда на 3 делится число $p - 4$. Такое возможно только, когда $p - 4 = 3$, так как число $p - 4$ простое. Отсюда $p = 7, p_1 = 3, p_2 = 5, p_3 = 11$.
- число p при делении на 3 дает остаток 2. Тогда на 3 делится $p + 4$. Значит $p + 4 = 3$, что невозможно.

Ответ: $p = 7, p_1 = 3, p_2 = 5, p_3 = 11$ (при условии $p_1 < p_2 < p_3$).

Задача 2

Нетрудно понять, что длина слова $n = 7$, а также несложно найти остаток $r_{32}(19^{11}) = 11$.

Преобразуем зашифрованный текст в последовательность чисел:

$$y_0 = 10, y_1 = 9, y_2 = 27, y_3 = 22, y_4 = 13, y_5 = 1, y_6 = 13,$$
$$y_7 = 22, y_8 = 11.$$

Из условия следует, что $x_8 - x_0 = 11$. Рассмотрим разность

$$r_{32}(y_8 - y_0) = r_{32}(x_8 + 6x_8 \cdot k^3 + k - x_0 - 6x_0 \cdot k^3 - k) =$$
$$= r_{32}\big((1 + 6k^3) \cdot (x_8 - x_0)\big) = r_{32}\big(11 \cdot (1 + 6k^3)\big).$$

Имеем:

$$r_{32}\big(11 \cdot (1 + 6k^3)\big) = 1.$$

Заметим, что $r_{32}(3 \cdot 11) = 1$. Откуда находим $r_{32}(1 + 6k^3) = 3$. Значит,

$$1 + 6k^3 = 3 + 32t \Leftrightarrow 3k^3 = 1 + 16t \Leftrightarrow 33k^3 = 11 + 11 \cdot 16t$$

Значит, $r_{16}(33k^3) = r_{16}(k^3) = 11$. В итоге

$$k^3 = 11 + 16p.$$

При $p = 1$ получим $k^3 = 27$. Отсюда $k = 3$. Опробуем полученное значение. Согласно правилу зашифрования

$$y_1 = 9 = r_{32}(x_1 + 6x_1 \cdot 27 + 3) = r_{32}(x_1 \cdot 3 + 3),$$
$$\Leftrightarrow 3x_1 + 3 = 9 + 32t \Leftrightarrow 3x_1 = 6 + 32t$$

Т.е. $r_{32}(3x_1) = 6 \Rightarrow r_{32}(x_1) = 2$. Продолжая дальше получим:

$$y_2 = 27 = r_{32}(x_2 + 6x_2 \cdot 27 + 3) = r_{32}(x_2 \cdot 3 + 3),$$
$$\Leftrightarrow 3x_2 + 3 = 27 + 32t \Leftrightarrow 3x_2 = 24 + 32t$$

Т.е. $r_{32}(3x_2) = 24 \Rightarrow r_{32}(x_2) = 8$. В итоге получим

Ответ: ВИСОКОС.

Задача 3

Пусть w_0, x_0, y_0, z_0 – значения секретных битов w, x, y, z. Решим прежде задачу, предполагая, что все секретные биты равны нулю: $w_0 = x_0 = y_0 = z_0 = 0$. Затем в уравнениях можно будет сделать замену $w \to w + w_0, \dots, z \to z + z_0$ и тем самым получить решение задачи в общем случае.

Запишем теперь какую-нибудь систему из четырех уравнений, которой удовлетворяют *только* нулевые значения. Например,

$$w + x = 0 \quad (1) \qquad y + z = 0 \quad (3)$$
$$x + y = 0 \quad (2) \qquad w + x + y = 0 \quad (4)$$

Запишем еще одно уравнение, сложив эти четыре:

$$x + y + z = 0 \qquad (5)$$

Система из *любых* четырех уравнений из набора (1) – (5) имеет только нулевое решение.

Далее идея в следующем. Если пара абонентов должна уметь находить все биты, то этой паре выдадим четыре *различные* уравнения из набора (1) – (5), если же нет, то хоть одно уравнение у этой пары должно быть общим.

Замечание. *Здесь нет четких алгоритмов и успех заранее не гарантирован. Возможно, следовало выбрать какие-то другие уравнения (1) – (4). Заметим, например, что абонентам, которые не должны уметь находить секрет, нельзя выдать уравнения (1), (2) и (4), так как значение бита* z *они не найдут, но определят, что* $w = x = y = 0$, *а это по условию недопустимо. Никакому абоненту нельзя выдать уравнения (2) и (5), так как из них следует, что* $z = 0$.

Абонентам раздать уравнения можно так: A_1: (1), (2); A_2: (1), (5); A_3: (3), (4); A_4: (4), (5).
Выполнив замену, запишем ответ в общем случае.
Ответ: Например,

$$A_1: w + x = w_0 + x_0,\ x + y = x_0 + y_0;\ A_2:\ w + x = w_0 + x_0,\ x + y + z = x_0 + y_0 + z_0;$$
$$A_3: y + z = y_0 + z_0,\ w + x + y = w_0 + x_0 + y_0;$$
$$A_4: w + x + y = w_0 + x_0 + y_0,\ x + y + z = x_0 + y_0 + z_0.$$

Задача 4

По условию числа u_k прибавляются к битам открытого текста, а результат заменяется остатком от деления на 2 (то есть на 0 или 1). Поэтому сразу заменим u_k его остатком от деления на 2: считаем, что $u_k = 0$ (если изначально u_k было четным) или $u_k = 1$ (если оно было нечетным). Вычисление остатка от деления на 32 при построении последовательности $u_1, u_2, \dots$ никакой роли не играет (четные числа дают четный остаток, а нечетные – нечетный).

Оказывается, в зависимости от четности чисел Д , М могут быть получены всего три различные последовательности $u_1, u_2, \dots$, а именно:

1. Числа Д , М нечетные. Тогда $u_1 = 0, u_2 = 1, u_3 = 0, \dots$
2. Числа Д , М имеют разную четность. Тогда $u_1 = 1, u_2 = 0, u_3 = 1, \dots$
3. Числа Д , М четные. Тогда $u_1 = u_2 = \dots = u_{32} = 0$. В этом случае текст Машиной записки остался бы без изменения, что, очевидно, не так.

Далее необходимо в первых двух случаях вычислить последовательность $\{u_n\}$ полностью, вычесть ее из зашифрованного текста (**ЗТ**) и убедиться, что читаемый вариант получается во втором случае (см. таблицу).

	Ж	Д	У	Л	Щ	Б	Ш	Л	У	В	Ш	Ц	Ч
	00110	00100	10011	01011	11001	00001	11000	01011	10011	00010	11000	10110	10111
1. Д, М нечетные													
$\{u_n\}$	01001	00100	10010	01001	00100	10010	01001	00100	10000	01001	00100	10010	01001
ЗТ-u_n	01111	00000	00001	00010	11101	10011	10001	01111	00011	01011	11100	00100	11110
	П	А	Б	В	Э	У	С	П	Г	Л	Ь	Д	Ю
2. Д, М разной четности													
$\{u_n\}$	10111	01110	11101	11011	10111	01110	11101	11011	10110	01110	11101	11011	10111
ЗТ-u_n	10001	01010	01110	10000	01110	01111	00101	10000	00101	01100	00101	01101	00000
	С	К	О	Р	О	П	Е	Р	Е	М	Е	Н	А

Ответ: **СКОРОПЕРЕМЕНА**

Задача 5

Решим задачу в общем случае, когда передача длилась n секунд. Так как переключение между читающими головками происходит раз в секунду, весь звук можно разбить на n фрагментов по 1 секунде и тогда звук, переданный в линию, будет перестановкой этих фрагментов. Обозначис количество возможных перестановок $T(n)$.

Представим весь процесс в виде таблицы, элементами которой являются номера фрагментов. Например, на второй секунде, с которой начинается передача, на пишущей головке будет 3-ий фрагмент звука, 2-ой фрагмент будет на (2)-ой читающей головке, а 1-ый фрагмент на (3)-ей читающей головке. Передача закончится на $n+1$ секунде.

Сек.	Пишущая головка	Читающая головка			В линию передан
		(2)	(3)	(4)	
0	1	–	–	–	–
1	2	1	–	–	–
2	3	2	1	–	2 или 1
3	4	3	2	1	3, 2 или 1
4	5	4	3	2	4, 3 или 2
…	…	…	…	…	
$n-1$	n	$n-1$	$n-2$	$n-3$	
n	–	n	$n-1$	$n-2$	
$n+1$	–	–	n	$n-1$	n или $n-1$

На $n+1$ секунде в линию может быть передан n или $n-1$ фрагмент звука. По очереди рассмотрим оба случая.

1. Пусть на $n+1$ секунде в линию был передан n-ый фрагмент (см. таблицу). Тогда n-ый фрагмент не мог быть передан на предыдущей секунде. Если посмотреть на таблицу то видно, что количество перестановок фрагментов в этом случае совпадает с $T(n-1)$, то есть количеством способов переставить звук длины $n-1$.

Читающая головка			В линию
(2)	(3)	(4)	
2	1	–	2 или 1
3	2	1	3, 2 или 1
4	3	2	4, 3 или 2
…	…	…	
$n-1$	$n-2$	$n-3$	
n	$n-1$	$n-2$	$n-1$ или $n-2$
–	$\boldsymbol{n}$	$n-1$	n

2. Пусть на $n+1$ секунде в линию был передан $(n-1)$-ый фрагмент (см. таблицу). Тогда $(n-1)$-ый фрагмент не мог быть передан на предыдущих секундах. Так как n-ый фрагмент должен уйти в линию, то он должен быть передан в момент времени n. Тогда до $(n-1)$-ой должно быть передано $(n-2)$ последовательных фрагментов, что может быть сделано $T(n-2)$ способами.

Читающая головка			В линию
(2)	(3)	(4)	
2	1	–	2 или 1
3	2	1	3, 2 или 1
4	3	2	4, 3 или 2
…	…	…	
$n-1$	$n-2$	$n-3$	$n-2$ или $n-3$
$\boldsymbol{n}$	$n-1$	$n-2$	n
–	n	$\boldsymbol{n-1}$	$n-1$

Таким образом $T(n) = T(n-1) + T(n-2)$. Тогда для нахождения количества перестановок $T(n)$ для любого n, достаточно найти $T(1)$, $T(2)$.

Читающая головка			В линию
(2)	(3)	(4)	
–	1	–	1

$$T(1) = 1$$

Читающая головка			В линию
(2)	(3)	(4)	
2	1	–	2 или 1
–	2	1	2 или 1

$$T(2) = 2$$

Остатется с использованием формулы $T(n) = T(n-1) + T(n-2)$ вычислить нужное значение.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	10946

Ответ. 10946

Задача 6

Для каждого набора $\boldsymbol{k} = (k_1, \dots, k_9)$ укажем такое минимальное l, что в соответствующей последовательности $u_1, u_2, \dots, u_l$ присутствует каждое из чисел 0, 1 и 2. Затем среди всех таких l останется выбрать наибольшее – это и будет ответом в задаче.

1. В наборе $\boldsymbol{k}$ встречается каждое из чисел 0, 1 и 2. Тогда искомое l не превосходит 9;
2. Набор $\boldsymbol{k}$ состоит только из 1. Тогда $u_{10} = \cdots = u_{17} = 2$ и $u_{18} = 0$. Значит $l = 18$;
3. В наборе $\boldsymbol{k}$ присутствуют и 1, и 2, но нет 0. Значит среди чисел $u_1, u_2, \dots, u_9$ есть два соседних (u_s и u_{s+1}), одно из которых равно 1, а другое 2. Тогда $u_{s+9} = 0$ и $l \leq 17$;
4. Набор $\boldsymbol{k}$ состоит из 0 и 1. Число 2 впоследствии дадут только две рядом стоящие 1. Поэтому рассмотрим варианты:
   a) в $\boldsymbol{k}$ есть рядом стоящие 1. Тогда $l < 19$;
   b) в $\boldsymbol{k}$ нет рядом стоящих 1. Здесь возможны следующие случаи:
      - Есть хоть одна 1 «не с краю». То есть найдется номер s такой, что $2 \leq s \leq 8$ и $k_s = 1$. Рядом стоящих 1 нет, поэтому $k_{s-1} = k_{s+1} = 0$. Тогда $u_{s+8} = u_{s+9} = 1$. Следовательно, $u_{s+17} = 2$ и $l \leq 25$;
      - 1 есть только «с краю». Пусть $\boldsymbol{k} = (1,0,\dots,0)$. В этом случае начало последовательности $u_1, u_2, \dots$ можно вычислить непосредственно: $\{u_n\} = \{1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0,$

0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 2, 1, 0,…} и убедиться, что $l = 27$. Пусть $\boldsymbol{k} = (1,0, \dots 0,1)$. Тогда $\{u_n\}$ ={1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 2, 1, 0…} и $l = 18$. И, наконец, для $\boldsymbol{k} = (0, \dots 0,1)$ находим $\{u_n\}$ ={0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 2, 1, 0, …}, $l = 26$.

Отметим, что случаи, «$\boldsymbol{k}$ состоит только из 2» и «$\boldsymbol{k}$ состоит только из 0 и 2» эквивалентны случаям 2 и 4 соответственно. Действительно, если в последовательности $\{u_n\}$, отвечающей набору $2 \cdot \boldsymbol{k}$, заменить все 2 на 1, а 1 на 2, то получится последовательность, соответствующая набору $\boldsymbol{k}$.

Ответ: $l = 27$.

ОБОРОЧНЫЙ ТУР

9 КЛАСС

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 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. Последовательность $x_1, x_2, \ldots$ получена по правилу: $x_1 = x_2 = x_3 = x_4 = x_5 = 1$, $x_{k+5} = f(x_k, x_{k+1}, x_{k+2}, x_{k+3}, x_{k+4})$, $k = 1,2, \ldots$ Найдите x_{14}, если известны первые 13 членов этой последовательности: 1111101001100.

2. Для зашифрования слова из пяти букв каждая его буква заменяется на число

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

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

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

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

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

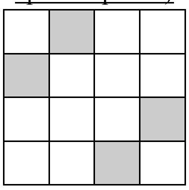
А затем полагают y_k равным остатку от деления числа $\overline{y_k}$ на 32. Расшифруйте исходное слово, если $(y_0, y_1, y_2, y_3, y_4) = (18,18,27,0,0)$ и запишите его буквами в ВЕРХНЕМ регистре , то есть если у Вас получился ответ: **олимпиада**, то его следует записать, как **ОЛИМПИАДА**.

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?

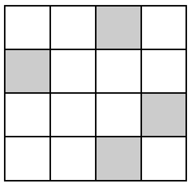
Доска с зернами

5	4	4	2
1	2	8	4
4	5	2	4
5	4	1	5

Пример (серые клетки образуют трансверсаль)



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



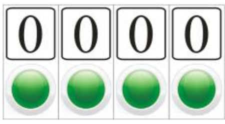
4. Для зашифрования слова каждая его буква заменяется на двухзначное число

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

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: **76 29 52 38 24 05 76 81 66 29**. Восстановите исходное слово и запишите его буквами в ВЕРХНЕМ регистре, то есть если у Вас получился ответ: **олимпиада** , то его следует записать, как **ОЛИМПИАДА**.

5. При входе в личный кабинет на терминале требуется ввести четырехзначный пароль из 0 и 1. Для этого на терминале имеются 4 кнопки и 4 окошка. 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 выставлен 0. Какое наименьшее количество нажатий кнопок потребуется, чтобы перебрать все возможные варианты пароля?



6. Натуралист решил исследовать популяцию кувшинок на озере. Он каждый день записывал количество кувшинок в течение 100 дней и обнаружил следующую закономерность. Каждый день число кувшинок увеличивалось на $2n + 1$ кувшинку по сравнению с предыдущим днем, где n - это номер дня наблюдения. Сколько находилось кувшинок на озере на 100 день наблюдения, если известно, что в первый день на озере была только четыре кувшинки?

10 КЛАСС

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 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. Последовательность $x_1, x_2, \dots$ получена по правилу: $x_1 = x_2 = x_3 = x_4 = x_5 = 1$, $x_{k+5} = f(x_k, x_{k+1}, x_{k+2}, x_{k+3}, x_{k+4})$, $k = 1,2, \dots$ Найдите x_{14}, если известны первые 13 членов этой последовательности: 1111101001100.

2. Для зашифрования слова из пяти букв каждая его буква заменяется на число

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

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

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

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

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

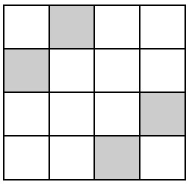
А затем полагают y_k равным остатку от деления числа $\overline{y_k}$ на 32. Расшифруйте исходное слово, если $(y_0, y_1, y_2, y_3, y_4) = (18,18,27,0,0)$ и запишите его буквами в ВЕРХНЕМ регистре , то есть если у Вас получился ответ: **олимпиада**, то его следует записать, как **ОЛИМПИАДА**.

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?

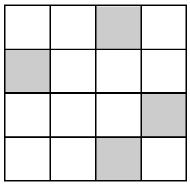
Доска с зернами

5	4	4	2
1	2	8	4
4	5	2	4
5	4	1	5

Пример (серые клетки образуют трансверсаль)



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

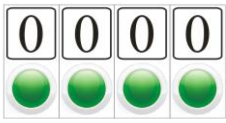


4. Для зашифрования слова каждая его буква заменяется на двухзначное число

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

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: **76 29 52 38 24 05 76 81 66 29**. Восстановите исходное слово и запишите его буквами в ВЕРХНЕМ регистре, то есть если у Вас получился ответ: **олимпиада** , то его следует записать, как **ОЛИМПИАДА**.

5. При входе в личный кабинет на терминале требуется ввести четырехзначный пароль из 0 и 1. Для этого на терминале имеются 4 кнопки и 4 окошка. 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 выставлен 0. Какое наименьшее количество нажатий кнопок потребуется, чтобы перебрать все возможные варианты пароля?



6. Натуралист решил исследовать популяцию кувшинок на озере. Он каждый день записывал количество кувшинок в течение 100 дней и обнаружил следующую закономерность. Каждый день число кувшинок увеличивалось на $2n + 1$ кувшинку по сравнению с предыдущим днем, где n - это номер дня наблюдения. Сколько находилось кувшинок на озере на 100 день наблюдения, если известно, что в первый день на озере была только четыре кувшинки?

11 КЛАСС

1. 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

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

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

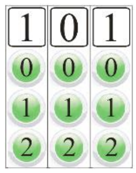
$$\overline{y_4} = 2^4 \cdot x_0 + 2^3 \cdot x_1 + 2^2 \cdot x_2 + 2^1 \cdot x_3 + 2^0 \cdot x_4.$$

А затем полагают y_k равным остатку от деления числа $\overline{y_k}$ на 32. Расшифруйте исходное слово, если $(y_0, y_1, y_2, y_3, y_4) = (18,18,27,0,0)$ и запишите его буквами в

ВЕРХНЕМ регистре , то есть если у Вас получился ответ: **олимпиада**, то его следует записать, как **ОЛИМПИАДА**.

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

2. При входе в личный кабинет на терминале требуется ввести трехзначный пароль x_1, x_2, x_3, где $x_i \in \{0,1,2\}$. Для этого на терминале имеются 3 окошка, а под каждым окошком расположены три кнопки. При нажатии на кнопку в окошке над ней появляется соответствующая цифра. Сейчас в окошках выставлена комбинация 101. Какое наименьшее количество нажатий кнопок потребуется, чтобы перебрать все возможные варианты пароля?



3. В Крипто-Вегасе на табло игрового автомата отображаются два натуральных числа $x_0 = 9$ и $y_0 = 450$. При нажатии кнопки первое из этих чисел заменяется на $x_1 = r_{11}(a \cdot x_0 + b)$, где a и b – некоторые неизвестные натуральные числа, а второе число заменяется на $y_1 = r_{2017}(y_0 + 321)$. Здесь $r_k(m)$ – остаток от деления натурального числа m на k. Определите какая из следующих четырех последовательностей при надлежащем выборе a и b из вышеуказанных фиксированных x_0, y_0 могли бы совпасть с последовательностью $(x_1, \cdots, x_5)$, полученной на этом игровом автомате?

Варианты ответов:

(1): (8, 3, 0, 7, 2),

(2): (8, 9, 7, 5, 4),

(3): (7, 6, 0, 8, 1),

(4): (2, 1, 6, 6, 3)

4. Для подтверждения переводимой в банк суммы братья **A** и **B** используют «кольцевую подпись», которая не позволяет определить, кто именно из них совершил перевод. **A** имеет свой открытый ключ $e_A = 3$ и некий секрет, позволяющий для любого натурального y $(y \leq 90)$ находить x_A такое, что $y = r_{91}(x_A^{e_A})$. Здесь $r_k(m)$ – остаток от деления натурального числа m на k. (У **B** есть свой ключ $e_B = 9$ и свой секрет.) Тогда **A** для подписи суммы M случайно выбирает натуральные числа x_B и v, не превосходящие 100, вычисляет $y_B = r_{91}(x_B^{e_B})$ и находит y_A из уравнения:

$$r_{101}\big(M\big(y_A + M(y_B + v)\big) - v^3\big) = 0. \quad (*)$$

Используя свой секрет, **A** находит x_A такой, что $y_A = r_{91}(x_A^{e_A})$. Тогда тройка чисел (x_A, x_B, v) будет подтверждением факта перевода суммы M. Например, $(1, 90, 46)$ корректное подтверждение суммы 46. Выберите корректное подтверждение суммы $M = 74$.

Варианты ответов:

(1): (3,1,74),

(2): (12,2,74),

(3): (26,1,74),

(4): (6,2,74).

5. В некоторые клетки 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. 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?

1	7	7	0
7	0	1	7
2	6	3	4
5	2	4	4

6. Натуралист решил исследовать популяцию кувшинок на озере. Он каждый день записывал количество кувшинок в течение 100 дней и обнаружил следующую закономерность. Каждый день число кувшинок увеличивалось на $2n + 1$ кувшинку по сравнению с предыдущим днем, где n - это номер дня наблюдения. Сколько находилось кувшинок на озере на 100 день наблюдения, если известно, что в первый день на озере была только четыре кувшинки?

ОТВЕТЫ

9 КЛАСС

1) 0.
2) ТОЧКА.
3) 5.
4) НАСЛЕДНИЦА.
5) 15.
6) 10201.

10 КЛАСС

1) 0.
2) ТОЧКА.
3) 5.
4) НАСЛЕДНИЦА.
5) 15.
6) 10201.

11 КЛАСС

1) ТОЧКА.
2) 26.
3) **(3):** (7, 6, 0, 8, 1).
4) **(1):** (3,1,74).
5) 5.
6) 10201.