РЕШЕНИЯ ЗАДАЧ

Задача 1

Количество трёхзначных чисел $x_1x_2x_3$, у которых остаток от деления на 7 суммы цифр равен фиксированному значению $t \in \{0,1,\dots,6\}$, 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:

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

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

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