

XXXII

**Межрегиональная олимпиада
школьников имени И.Я. Верченко
по математике и криптографии**

УСЛОВИЯ И РЕШЕНИЯ

Москва 2023

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП.....	3
8,9 КЛАСС	3
10 КЛАСС	7
11 КЛАСС	11
ОТВЕТЫ НА ЗАДАНИЯ ЗАКЛЮЧИТЕЛЬНОГО ЭТАПА.....	14
ОТБОРОЧНЫЙ ЭТАП.....	15
8,9 КЛАСС	15
10 КЛАСС	16
11 КЛАСС	18

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 групп часовых поясов (ЗАПАД, СИБИРЬ, ВОСТОК) для участников 11 класса. Тематика отдельных задач в разных классах пересекается, при этом младшим классам предлагались более легкие варианты заданий.

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

8,9 КЛАСС

1. Найдите все шестизначные числа $A = \overline{a_1 a_2 \dots a_6}$, $a_i \in \{1, 2, \dots, 9\}$ такие, что $8 \cdot A + a_6 = B$,

где $B = \overline{b_1 b_2 \dots b_6}$, $b_i = 10 - a_i$. Решение обоснуйте.

Решение.

Заметим, что $A + B = \underbrace{11 \dots 1}_6 0 = \frac{10^6 - 1}{9} \cdot 10$. Тогда из условия $8 \cdot A + a_6 = B$ получим

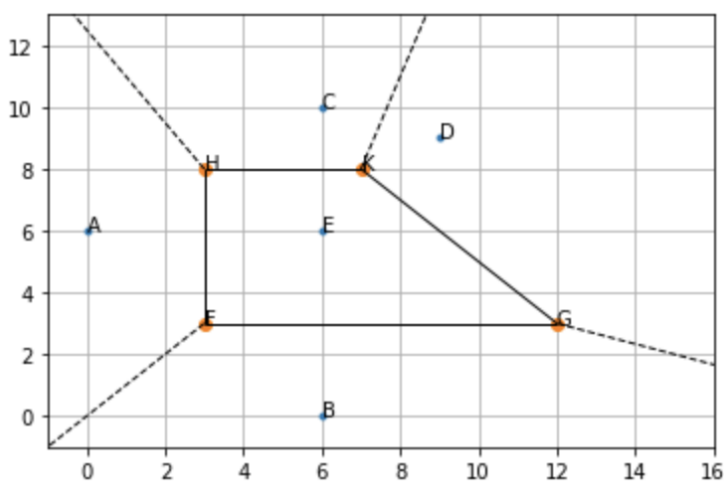
$9 \cdot A + a_6 = \underbrace{11 \dots 1}_6 0$. Остаток от деления на 9 правой части равен 6.

Следовательно, $a_6 = 6$. Разделим число $(\underbrace{11 \dots 1}_6 0 - 6)$ на 9. Получим число 123456.

Ответ: 123456.

2. На координатной плоскости в точках $A(0, 6)$, $B(6, 0)$, $C(6, 10)$, $D(9, 9)$ и $E(6, 6)$ расположены вышки сотовой связи. Будем говорить, что абонент находится в зоне действия данной вышки, если расстояния до неё меньше, чем до любой другой вышки. Найдите площадь зоны действия вышки E .

Решение. Для начала требуется отобразить точки на координатной плоскости. Так как, по условию задачи, требуется найти площадь зоны действия вышки E , то соединим отрезками точку E с точками A, B, C, D . Далее проведем через полученные отрезки серединные перпендикуляры и выделим область, полученную пересечением таких перпендикуляров (отмечены на рис. оранжевым цветом). Таким образом получаем трапецию (см. рисунок ниже), которая демонстрирует область зоны действия вышки E :



Осталось посчитать площадь полученной трапеции. Пересечение серединных перпендикуляров дало нам 4 точки с координатами $F(3, 3)$, $H(3, 8)$, $K(7, 8)$ и $G(12, 3)$. Площадь данной трапеции:

$$S = \frac{1}{2} * (HK + FG) * HF = \frac{1}{2} * (4 + 9) * 5 = 32,5$$

Ответ: 32,5.

3. Пароли в системе состояются из букв английского алфавита (26 букв) и цифр. При этом требуется, чтобы в пароле содержались цифра и заглавная буква. Пользователь допускается в систему, если предъявленный им пароль отличается от установленного не более чем в одном символе. Сколько паролей, соответствующих требованиям составления, позволят войти в систему, если для пользователя был установлен пароль **1wR8dttf** (не совпадающих с установленным паролем)?

Решение. Раскладываем пароль «по слоям»: цифра+заглавная+строчная и смотрим, какие ограничения есть по замене в каждой позиции. Цифр две, поэтому одну из них можно заменить произвольно на любой знак из $26 + 26 + 10 - 1 = 61$. Итого $2 \cdot 61 = 122$ варианта. Если менять заглавную R, то только на заглавную – 25 вариантов. Строчные можно на любые, это еще $5 \cdot 61 = 305$ вариантов.

Ответ: 452.

4. Пусть $\mathbf{x} = (x_1, \dots, x_4)$ – двоичный вектор длины 4. Обозначим \mathbf{x}^d – циклический сдвиг вектора \mathbf{x} на d позиций вправо. Например, если $\mathbf{x} = (1, 0, 0, 0)$, то $\mathbf{x}^2 = (0, 0, 1, 0)$.

При этом считаем, что $\mathbf{x}^0 = \mathbf{x}$. Под суммой векторов $\mathbf{x} = (x_1, \dots, x_4)$ и $\mathbf{y} = (y_1, \dots, y_4)$ будем понимать вектор $\mathbf{x} + \mathbf{y} = (x_1 \oplus y_1, x_2 \oplus y_2, x_3 \oplus y_3, x_4 \oplus y_4)$.

Здесь \oplus – стандартная операция сложения битов: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Пусть $\mathbf{x} = \mathbf{v} + \mathbf{v}^1 + \mathbf{v}^2$. Найдите d_1, \dots, d_n такие, что при любом исходном векторе \mathbf{v} выполняется равенство $\mathbf{v} = \mathbf{x}^{d_1} + \dots + \mathbf{x}^{d_n}$.

Решение. Заметим, что $\mathbf{x}^{d+4n} = \mathbf{x}^d$ для любого натурального числа n . Вектору $\mathbf{x} = (x_1, \dots, x_4)$ взаимно-однозначно соответствует многочлен $x(t) = x_1 + x_2 t + x_3 t^2 + x_4 t^3$. Тогда циклический сдвиг вектора \mathbf{x} на d позиций вправо равносильно умножению многочлена $x(t)$ на t^d и приведению степеней мономов по модулю 4. Вектору $\mathbf{x} = \mathbf{v} + \mathbf{v}^1 + \mathbf{v}^2$ соответствует многочлен $x(t) = 1 + t + t^2$. Таким образом, нахождение d_1, \dots, d_n таких, что $\mathbf{v} = \mathbf{x}^{d_1} + \dots + \mathbf{x}^{d_n}$ равносильно нахождению многочлена $v(t) = t^{d_1} + \dots + t^{d_n}$ со свойством $x(t)v(t) = 1$ (с учётом приведения степеней мономов по модулю 4). Найти многочлен $v(t)$ можно методом неопределённых коэффициентов, но быстрее из следующего алгоритма: $x(t)^2 = 1 + t^2 + t^4 = t^2$, $x(t)^4 = t^4 = 1$. Следовательно, $v(t) = x(t)^3 = 1 + t^2 + t^3$.

Ответ: $\mathbf{v} = \mathbf{x} + \mathbf{x}^2 + \mathbf{x}^3$.

5. Имеется устройство, которое строит последовательность чисел x_0, x_1, x_2, \dots следующим образом: первые два члена x_0 и x_1 мы задаем самостоятельно, а последующие члены устройство вычисляет так: $x_2 = x_0 + 14 \cdot (x_1 + k_1), x_3 = x_1 + 14 \cdot (x_2 + k_2), \dots$ Здесь k_1, k_2, \dots – некоторая фиксированная ключевая последовательность. При этом все числа x_0, x_1, x_2, \dots и k_1, k_2, \dots являются целыми, лежащими в пределах от 0 до 30 включительно. (Если в процессе вычислений получится число, превосходящее 30, то результат будет заменен его остатком от деления на 31; например, $16 + 14 \cdot 5 = 24$.) С помощью этого устройства построили две последовательности a_0, a_1, a_2, \dots и b_0, b_1, b_2, \dots , по первым членам $a_0 = 2, a_1 = 4$ и $b_0 = 8, b_1 = 26$. Верно ли, что найдётся ключевая последовательность k_1, k_2, \dots и некоторое целое t такие, что выполняются условия:

а) $b_t = a_t, b_{t+1} = a_{t+1}$;

б) $b_t = a_t, b_{t+1} = a_{t+1} + 6$?

В случае положительного ответа укажите t и набор k_1, k_2, \dots, k_{t-1} .

Решение.

а) Для всех $t \geq 1$ $a_{t+1} = a_{t-1} + 14(a_t + k_t), a_{t-1} = a_{t+1} - 14(a_t + k_t)$.

Поэтому, если $b_t = a_t, b_{t+1} = a_{t+1}$, то $b_{t-1} = a_{t-1}, b_{t-2} = a_{t-2}, \dots, b_1 = a_1, b_0 = a_0$, что противоречит условию.

б) Удобно перейти к разностям полублоков $z_t = b_t - a_t$ (везде далее действия с полублоками (умножение, сложение и вычитание) производятся по модулю М) и выяснить, может ли появиться биграмма (0,6) в $\{z_t\}$. Из (1) получаем, что:

$$z_{t+1} = b_{t-1} + 14(b_t + k_t) - (a_{t-1} + 14(a_t + k_t)) = z_{t-1} + 14 \cdot z_t, t \geq 1,$$

Последовательность разностей не зависит от ключа. По условию $(z_0, z_1) = (6, 22)$, выработанный на этом заполнении цикл:

$$\{z_t\} = \{6, 22, 4, 16, 11, 15, 4, 9, 6, 0\}$$

Имеет период $T = 10$, ноль – последний элемент цикла, после него следует 6.

Ответ: да, верно, при $t = 10$ и любом ключе.

6. Для входа в университет Криптоландии у каждого студента есть карточка, на которой записана уникальная (у каждого студента своя) последовательность $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ из целых чисел от 0 до 6. При входе в университет студент прикладывает карточку к устройству, которое подсчитывает величины A и B по формулам:

$$A = ((x_1 * x_2) * x_3) * x_4,$$

$$B = (x_5 \circ x_6) \circ x_7.$$

Операции $*$ и \circ задаются таблицами (представляющими собой латинские квадраты: у них в каждой строке и каждом столбце числа не повторяются). Например, $3 * 5 = 4, 2 \circ 4 = 3$. Студенту разрешат войти, если $A = B$. Сколько самое большое может быть студентов в таком университете?

*	0	1	2	3	4	5	6
0	5	6	1	2	4	0	3
1	1	3	6	0	2	5	4
2	4	5	3	1	0	2	6
3	6	0	5	3	1	4	2
4	0	4	2	6	5	3	1
5	2	1	0	4	3	6	5
6	3	2	4	5	6	1	0

o	0	1	2	3	4	5	6
0	4	5	6	3	0	1	2
1	2	0	3	4	5	6	1
2	1	2	4	5	3	0	6
3	6	1	0	2	4	5	3
4	5	3	2	1	6	4	0
5	3	6	5	0	1	2	4
6	0	4	1	6	2	3	5

Решение. Если код составлен из чисел от 0 до $m - 1$, то для каждого числа $k \in \{0, \dots, m - 1\}$

число последовательностей x_1, x_2, x_3, x_4 , для которых $A = k$, равно m^3 , так как при любых заданных x_1, x_2, x_3 значение x_4 определяется в этом случае однозначно. Аналогично, число последовательностей x_5, x_6, x_7 , для которых $B = k$, равно m^2 . Тогда общее число последовательностей $x_1, x_2, x_3, x_4, x_5, x_6, x_7$, для которых $A = B = k$, равно $m^3 m^2 = m^5$. Суммируя по k от 0 до $m - 1$, получаем ответ: m^6 .

Ответ: 7^6 .

10 КЛАСС

1. Найдите все шестизначные числа $A = \overline{a_1 a_2 \dots a_6}$, $a_i \in \{1, 2, \dots, 9\}$ такие, что $8 \cdot A + a_6 = B$, где $B = \overline{b_1 b_2 \dots b_6}$, $b_i = 10 - a_i$. Решение обоснуйте.

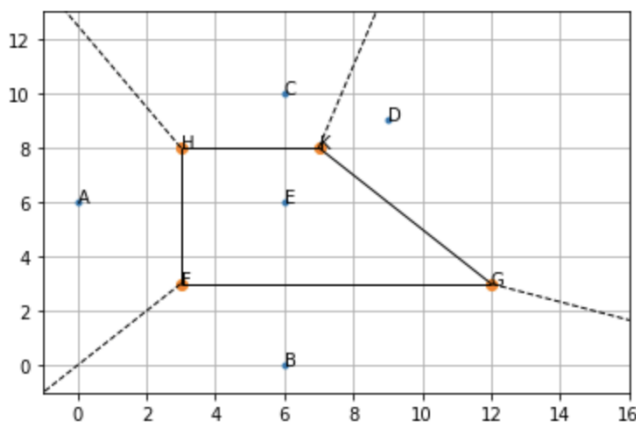
Решение. Заметим, что $A + B = \underbrace{11 \dots 10}_6 = \frac{10^6 - 1}{9} \cdot 10$. Тогда из условия. $8 \cdot A + a_6 = B$ получим $9 \cdot A + a_6 = \underbrace{11 \dots 10}_6$.

Остаток от деления на 9 правой части равен 6. Следовательно, $a_6 = 6$. Разделим число $(\underbrace{11 \dots 10}_6 - 6)$ на 9. Получим число 123456.

Ответ: 123456.

2. На координатной плоскости в точках $A(0, 6)$, $B(6, 0)$, $C(6, 10)$, $D(9, 9)$ и $E(6, 6)$ расположены вышки сотовой связи. Будем говорить, что абонент находится в зоне действия данной вышки, если расстоянию до неё меньше, чем до любой другой вышки. Найдите площадь зоны действия вышки E .

Решение. Для начала требуется отобразить точки на координатной плоскости. Так как, по условию задачи, требуется найти площадь зоны действия вышки E , то соединим отрезками точку E с точками A, B, C, D . Далее проведем через полученные отрезки серединные перпендикуляры и выделим область, полученную пересечением таких перпендикуляров (отмечены на рис. оранжевым цветом). Таким образом получаем трапецию (см. рисунок ниже), которая демонстрирует область зоны действия вышки E :



Осталось посчитать площадь полученной трапеции. Пересечение серединных перпендикуляров дало нам 4 точки с координатами $F(3, 3)$, $H(3, 8)$, $K(7, 8)$ и $G(12, 3)$. Площадь данной трапеции:

$$S = \frac{1}{2} * (HK + FG) * HF = \frac{1}{2} * (4 + 9) * 5 = 32,5$$

Ответ: 32,5.

3. Пароли в системе состояются из букв английского алфавита (26 букв) и цифр. При этом требуется, чтобы в пароле содержались цифра и заглавная буква. Пользователь допускается в систему, если предъявленный им пароль отличается от установленного не более чем в одном символе. Сколько паролей, соответствующих требованиям составления, позволят войти в систему, если для пользователя был установлен пароль **1wR8dttf** (не совпадающих с установленным паролем)?

Решение. Раскладываем пароль «по слоям»: цифра+заглавная+строчная и смотрим, какие ограничения есть по замене в каждой позиции. Цифр две, поэтому одну их них можно заменить произвольно на любой знак из $26 + 26 + 10 - 1 = 61$. Итого $2 \cdot 61 = 122$ варианта. Если менять заглавную R, то только на заглавную – 25 вариантов. Строчные можно на любые, это еще $5 \cdot 61 = 305$ вариантов.

Ответ: 452.

4. Пусть $\mathbf{x} = (x_1, \dots, x_4)$ – двоичный вектор длины 4. Обозначим \mathbf{x}^d – циклический сдвиг вектора \mathbf{x} на d позиций вправо. Например, если $\mathbf{x} = (1, 0, 0, 0)$, то $\mathbf{x}^2 = (0, 0, 1, 0)$.

При этом считаем, что $\mathbf{x}^0 = \mathbf{x}$. Под суммой векторов $\mathbf{x} = (x_1, \dots, x_4)$ и $\mathbf{y} = (y_1, \dots, y_4)$ будем понимать вектор $\mathbf{x} + \mathbf{y} = (x_1 \oplus y_1, x_2 \oplus y_2, x_3 \oplus y_3, x_4 \oplus y_4)$.

Здесь \oplus – стандартная операция сложения битов: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Пусть $\mathbf{x} = \mathbf{v} + \mathbf{v}^1 + \mathbf{v}^2$. Найдите d_1, \dots, d_n такие, что при любом исходном векторе \mathbf{v} выполняется равенство $\mathbf{v} = \mathbf{x}^{d_1} + \dots + \mathbf{x}^{d_n}$.

Решение. Заметим, что $\mathbf{x}^{d+4n} = \mathbf{x}^d$ для любого натурального числа n . Вектору $\mathbf{x} = (x_1, \dots, x_4)$ взаимно-однозначно соответствует многочлен $x(t) = x_1 + x_2 t + x_3 t^2 + x_4 t^3$. Тогда циклический сдвиг вектора \mathbf{x} на d позиций вправо равносильно умножению многочлена $x(t)$ на t^d и приведению степеней мономов по модулю 4. Вектору $\mathbf{x} = \mathbf{v} + \mathbf{v}^1 + \mathbf{v}^2$ соответствует многочлен $x(t) = 1 + t + t^2$. Таким образом, нахождение d_1, \dots, d_n таких, что $\mathbf{v} = \mathbf{x}^{d_1} + \dots + \mathbf{x}^{d_n}$ равносильно нахождению многочлена $v(t) = t^{d_1} + \dots + t^{d_n}$ со свойством $x(t)v(t) = 1$ (с учётом приведения степеней мономов по модулю 4). Найти многочлен $v(t)$ можно методом неопределённых коэффициентов, но быстрее из следующего алгоритма: $x(t)^2 = 1 + t^2 + t^4 = t^2$, $x(t)^4 = t^4 = 1$. Следовательно, $v(t) = x(t)^3 = 1 + t^2 + t^3$.

Ответ: $\mathbf{v} = \mathbf{x} + \mathbf{x}^2 + \mathbf{x}^3$.

5. Имеется устройство, которое строит последовательность чисел x_0, x_1, x_2, \dots следующим образом: первые два члена x_0 и x_1 мы задаем самостоятельно, а последующие члены устройство вычисляет так:

$$x_2 = x_0 + 14 \cdot (x_1 + k_1), x_3 = x_1 + 14 \cdot (x_2 + k_2), \dots$$

Здесь k_1, k_2, \dots – некоторая фиксированная ключевая последовательность. При этом все числа x_0, x_1, x_2, \dots и k_1, k_2, \dots являются целыми, лежащими в пределах от 0 до 30 включительно. (Если в процессе вычислений получится число, превосходящее 30, то результат будет заменен его остатком от деления на 31; например, $16 + 14 \cdot 5 = 24$.) С помощью этого устройства построили две последовательности a_0, a_1, a_2, \dots и b_0, b_1, b_2, \dots , по первым членам $a_0 = 2, a_1 = 4$ и $b_0 = 8, b_1 = 26$. Верно ли, что найдётся ключевая последовательность k_1, k_2, \dots и некоторое целое t такие, что выполняются условия: а) $b_t = a_t, b_{t+1} = a_{t+1}$; б) $b_t = a_t, b_{t+1} = a_{t+1} + 6$? В случае положительного ответа укажите t и набор k_1, k_2, \dots, k_{t-1} .

Решение.

а) Для всех $t \geq 1$

$$a_{t+1} = a_{t-1} + 14(a_t + k_t), a_{t-1} = a_{t+1} - 14(a_t + k_t).$$

Поэтому, если $b_t = a_t, b_{t+1} = a_{t+1}$, то $b_{t-1} = a_{t-1}, b_{t-2} = a_{t-2}, \dots, b_1 = a_1, b_0 = a_0$, что противоречит условию.

б) Удобно перейти к разностям полублоков $z_t = b_t - a_t$ (везде далее действия с полублоками (умножение, сложение и вычитание) производятся по модулю M) и выяснить, может ли появиться биграмма $(0,6)$ в $\{z_t\}$. Из (1) получаем, что:

$$z_{t+1} = b_{t-1} + 14(b_t + k_t) - (a_{t-1} + 14(a_t + k_t)) = z_{t-1} + 14 \cdot z_t, t \geq 1,$$

Последовательность разностей не зависит от ключа. По условию $(z_0, z_1) = (6, 22)$, выработанный на этом заполнении цикл:

$$\{z_t\} = \{6, 22, 4, 16, 11, 15, 4, 9, 6, 0\}$$

Имеет период $T = 10$, ноль – последний элемент цикла, после него следует 6.

Ответ: да, верно, при $t = 10$ и любом ключе.

6. Для входа в университет Криптоландии у каждого студента есть карточка, на которой записана уникальная (у каждого студента своя) последовательность $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ из целых чисел от 0 до 6. При входе в университет студент прикладывает карточку к устройству, которое подсчитывает величины A и B по формулам:

$$A = ((x_1 * x_2) * x_3) * x_4,$$

$$B = (x_5 \circ x_6) \circ x_7.$$

Операции $*$ и \circ задаются таблицами (представляющими собой латинские квадраты: у них в каждой строке и каждом столбце числа не повторяются).

Например, $3 * 5 = 4$, $2 \circ 4 = 3$. Студенту разрешат войти, если $A = B$. Сколько самое большое может быть студентов в таком университете?

*	0	1	2	3	4	5	6
0	5	6	1	2	4	0	3
1	1	3	6	0	2	5	4
2	4	5	3	1	0	2	6
3	6	0	5	3	1	4	2
4	0	4	2	6	5	3	1
5	2	1	0	4	3	6	5
6	3	2	4	5	6	1	0

\circ	0	1	2	3	4	5	6
0	4	5	6	3	0	1	2
1	2	0	3	4	5	6	1
2	1	2	4	5	3	0	6
3	6	1	0	2	4	5	3
4	5	3	2	1	6	4	0
5	3	6	5	0	1	2	4
6	0	4	1	6	2	3	5

Решение. Если код составлен из чисел от 0 до $m - 1$, то для каждого числа

$$k \in \{0, \dots, m - 1\}$$

число последовательностей x_1, x_2, x_3, x_4 , для которых $A = k$, равно m^3 , так как при любых заданных x_1, x_2, x_3 значение x_4 определяется в этом случае однозначно. Аналогично, число последовательностей x_5, x_6, x_7 , для которых $B = k$, равно m^2 . Тогда общее число последовательностей $x_1, x_2, x_3, x_4, x_5, x_6, x_7$, для которых $A = B = k$, равно $m^3 m^2 = m^5$. Суммируя по k от 0 до $m - 1$, получаем ответ: m^6 .

Ответ: 7^6 .

11 КЛАСС

1. Найдите все восьмизначные числа $A = \overline{a_1 a_2 \dots a_8}$, $a_i \in \{1, 2, \dots, 9\}$ такие, что $8 \cdot A + a_8 = B$, где $B = \overline{b_1 b_2 \dots b_8}$, $b_i = 10 - a_i$. Решение обоснуйте.

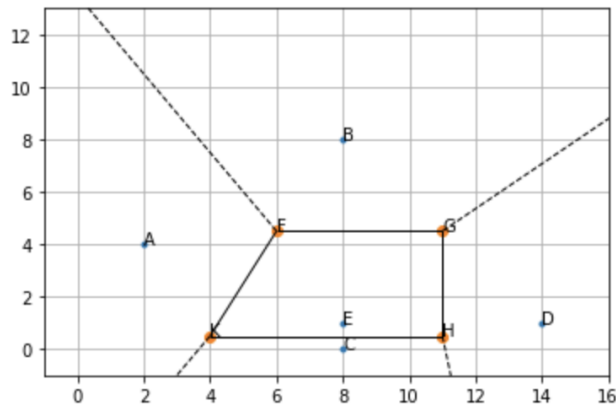
Решение.

Заметим, что $A + B = \underbrace{11 \dots 1}_8 0 = \frac{10^8 - 1}{9} \cdot 10$. Тогда из условия $8 \cdot A + a_8 = B$ получим $9 \cdot A + a_8 = \underbrace{11 \dots 1}_8 0$. Остаток от деления на 9 правой части равен 8. Следовательно, $a_8 = 8$. Разделим число $(\underbrace{11 \dots 1}_8 0 - 8)$ на 9. Получим число 12345678.

Ответ: 12345678.

2. На координатной плоскости в точках $A(2, 4)$, $B(8, 8)$, $C(8, 0)$, $D(14, 1)$ и $E(8, 1)$ расположены вышки сотовой связи. Будем говорить, что абонент находится в *зоне действия* данной вышки, если расстояния до неё меньше, чем до любой другой вышки. Найдите площадь зоны действия вышки E.

Решение. Для начала требуется отобразить точки на координатной плоскости. Так как, по условию задачи, требуется найти площадь зоны действия вышки E, то соединим отрезками точку E с точками A, B, C, D. Далее проведем через полученные отрезки срединные перпендикуляры и выделим область, полученную пересечением таких перпендикуляров (отмечены на рис. оранжевым цветом). Таким образом получаем трапецию (см. рисунок ниже), которая демонстрирует область зоны действия вышки E:



Осталось посчитать площадь полученной трапеции. Пересечение срединных перпендикуляров дало нам 4 точки с координатами $F(6, 4.5)$, $H(11, 0.5)$, $K(4, 0.5)$ и $G(11, 4.5)$. Площадь данной трапеции:

$$S = \frac{1}{2} * (HK + FG) * HG = \frac{1}{2} * (5 + 7) * 4 = 24$$

Ответ: 24.

3. Пароли в системе составляются из букв английского алфавита (26 букв) и цифр. При этом требуется, чтобы в пароле содержались цифра и заглавная буква. Пользователь допускается в систему, если предъявленный им пароль отличается от установленного не более чем в одном символе. Сколько паролей, соответствующих требованиям составления, позволят войти в систему, если для пользователя был установлен пароль **Tw38dttf** (не совпадающих с установленным паролем)?

Решение. Раскладываем пароль «по слоям»: цифра+заглавная+строчная и смотрим, какие ограничения есть по замене в каждой позиции. Цифр две, поэтому одну их них можно заменить произвольно на любой знак из $26 + 26 + 10 - 1 = 61$. Итого $2 \cdot 61 = 122$ варианта. Если менять заглавную T, то только на заглавную – 25 вариантов. Строчные можно на любые, это еще $5 \cdot 61 = 305$ вариантов.

Ответ: 452.

4. Пусть $\mathbf{x} = (x_1, \dots, x_8)$ – двоичный вектор длины 8. Обозначим \mathbf{x}^d – циклический сдвиг вектора

\mathbf{x} на d позиций вправо. Например, если $\mathbf{x} = (1,0,0,0,0,0,0,0)$, то $\mathbf{x}^2 = (0,0,1,0,0,0,0,0)$. При этом считаем, что $\mathbf{x}^0 = \mathbf{x}$. Под суммой векторов $\mathbf{x} = (x_1, \dots, x_4)$ и $\mathbf{y} = (y_1, \dots, y_4)$ будем понимать вектор $\mathbf{x} + \mathbf{y} = (x_1 \oplus y_1, x_2 \oplus y_2, x_3 \oplus y_3, x_4 \oplus y_4)$. Здесь \oplus – стандартная операция сложения битов: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Пусть $\mathbf{x} = \mathbf{v} + \mathbf{v}^1 + \mathbf{v}^4$. Найдите d_1, \dots, d_n такие, что при любом исходном векторе \mathbf{v} выполняется равенство $\mathbf{v} = \mathbf{x}^{d_1} + \dots + \mathbf{x}^{d_n}$.

Решение. Заметим, что $\mathbf{x}^{d+8n} = \mathbf{x}^d$ для любого натурального числа n . Вектору $\mathbf{x} = (x_1, \dots, x_8)$ взаимно-однозначно соответствует многочлен $x(t) = x_1 + x_2 t + \dots + x_7 t^7 + x_8 t^8$. Тогда циклический сдвиг вектора \mathbf{x} на d позиций вправо равносильно умножению многочлена $x(t)$ на t^d и приведению степеней мономов по модулю 8. Вектору $\mathbf{x} = \mathbf{v} + \mathbf{v}^1 + \mathbf{v}^4$ соответствует многочлен $x(t) = 1 + t + t^4$. Таким образом, нахождение d_1, \dots, d_n таких, что $\mathbf{v} = \mathbf{x}^{d_1} + \dots + \mathbf{x}^{d_n}$ равносильно нахождению многочлена $v(t) = t^{d_1} + \dots + t^{d_n}$ со свойством $x(t)v(t) = 1$ (с учётом приведения степеней мономов по модулю 8). Найти многочлен $v(t)$ можно методом неопределённых коэффициентов, но быстрее из следующего алгоритма:

$$x(t)^2 = 1 + t + t^8 = t^2, \quad x(t)^4 = t^4, \quad x(t)^8 = t^8 = 1.$$

Следовательно, $v(t) = x(t)^7 = x(t)^3 x(t)^4 = (1 + t + t^4)t^2 t^4 = t^2 + t^6 + t^7$.

Ответ: $\mathbf{v} = \mathbf{x}^2 + \mathbf{x}^6 + \mathbf{x}^7$.

5. Имеется устройство, которое строит последовательность чисел x_0, x_1, x_2, \dots следующим образом: первые два члена x_0 и x_1 мы задаем самостоятельно, а последующие члены устройство вычисляет так: $x_2 = x_0 + 13 \cdot (x_1 + k_1), x_3 = x_1 + 13 \cdot (x_2 + k_2), \dots$ Здесь k_1, k_2, \dots – некоторая фиксированная ключевая последовательность. При этом все числа x_0, x_1, x_2, \dots и k_1, k_2, \dots являются целыми, лежащими в пределах от 0 до 32 включительно. (Если в процессе вычислений получится число, превосходящее 32, то результат будет заменен его остатком от деления на 33; например, $16 + 13 \cdot 2 = 9$.) С помощью этого устройства построили две последовательности a_0, a_1, a_2, \dots и b_0, b_1, b_2, \dots , по первым членам $a_0 = 1, a_1 = 3$ и $b_0 = 1, b_1 = 12$. Верно ли, что найдётся ключевая последовательность k_1, k_2, \dots и некоторое целое t , большее 0, такие, что выполняются условия: а) $b_t = a_t, b_{t+1} = a_{t+1}$; б) $b_t = a_t + 1$? Решение обоснуйте.

Решение.

а) Для всех $t \geq 1$

$$a_{t+1} = a_{t-1} + 13(a_t + k_t), \quad a_{t-1} = a_{t+1} - 13(a_t + k_t).$$

Поэтому, если $b_t = a_t, b_{t+1} = a_{t+1}$, то $b_{t-1} = a_{t-1}, b_{t-2} = a_{t-2}, \dots, b_1 = a_1, b_0 = a_0$, что противоречит условию.

б) Удобно перейти к разностям полублоков $z_t = b - a_t$ (везде далее действия с полублоками (умножение, сложение и вычитание) производятся по модулю M) и выяснить, может ли 1 появиться в $\{z_t\}$. Из уравнения шифрования $x_{t+1} = x_{t-1} + 13(x_t + k_t)$ получаем, что последовательность разностей:

$$z_{t+1} = b_{t-1} + 13(b_t + k_t) - (a_t + 13(a_t + k_t)) = z_{t-1} + 13z_t, \quad t \geq 1,$$

не зависит от ключа. По условию $(z_0, z_1) = (0, 9), (z_0, z_1, M) = 3$, поэтому все члены последовательности будут делиться на 3, и единицы там не будет.

Ответ: нет.

6. Для входа в университет Криптоландии у каждого студента есть карточка, на которой записана уникальная (у каждого студента своя) последовательность $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ из целых чисел от 0 до 5. При входе в университет студент прикладывает карточку к устройству, которое подсчитывает величины A и B по формулам:

$$A = ((x_1 * x_2) * x_3) * x_4,$$

$$B = (x_5 \circ x_6) \circ x_7.$$

Операции $*$ и \circ задаются таблицами (представляющими собой латинские квадраты: у них в каждой строке и каждом столбце числа не повторяются).

Например, $3 * 2 = 3$, $2 \circ 4 = 2$. Студенту разрешат войти, если $A = B$. Сколько самое большое может быть студентов в таком университете?

*	0	1	2	3	4	5
0	2	3	4	1	0	5
1	4	5	1	0	2	3
2	3	4	5	2	1	0
3	0	2	3	4	5	1
4	1	0	2	5	3	4
5	5	1	0	3	4	2

o	0	1	2	3	4	5
0	4	2	0	1	5	3
1	5	0	3	2	4	1
2	3	5	1	0	2	4
3	1	3	2	4	0	5
4	2	4	5	3	1	0
5	0	1	4	5	3	2

Решение. Если код составлен из чисел от 0 до $m - 1$, то для каждого числа

$$k \in \{0, \dots, m - 1\}$$

число последовательностей x_1, x_2, x_3, x_4 , для которых $A = k$, равно m^3 , так как при любых заданных x_1, x_2, x_3 значение x_4 определяется в этом случае однозначно.

Аналогично, число последовательностей x_5, x_6, x_7 , для которых $B = k$, равно m^2 .

Тогда общее число последовательностей $x_1, x_2, x_3, x_4, x_5, x_6, x_7$, для которых $A = B = k$, равно $m^3 m^2 = m^5$. Суммируя по k от 0 до $m - 1$, получаем ответ: m^6 .

Ответ: 6^6 .

ОТВЕТЫ НА ЗАДАНИЯ ЗАКЛЮЧИТЕЛЬНОГО ЭТАПА

8, 9 КЛАСС

1. 123456.
2. 32,5.
3. 452.
4. $v = x + x^2 + x^3$.
5. да, верно, при $t = 10$ и любом ключе.
6. 7^6 .

10 КЛАСС

1. 123456.
2. 32,5.
3. 452.
4. $v = x + x^2 + x^3$.
5. да, верно, при $t = 10$ и любом ключе.
6. 7^6 .

11 КЛАСС

1. 12345678.
2. 24.
3. 452.
4. $v = x^2 + x^6 + x^7$.
5. нет.
6. 6^6 .

ОТБОРОЧНЫЙ ЭТАП

8,9 КЛАСС

1. Установите, можно ли создать телефонную сеть связи, состоящую из 991 абонента, каждый из которых был бы связан ровно с 93 другими.

2. Дана криптограмма:

ПШ	*	Ь	=	ПЕП
+		*		-
ИИ	+	И	=	ШБ
=		=		=
ЫТЕ	+	ДО	=	ЫДШ

Восстановите цифровые значения букв, при которых справедливы все указанные равенства, если разным буквам соответствуют различные цифры. Расставьте буквы в порядке возрастания их цифровых значений и получите искомый текст. В ответе запишите полученный текст заглавными буквами без пробелов между словами, если их в тексте несколько. Пример: ОТБОРОЧНЫЙЭТАП или ОЛИМПИАДА.

3. Знаками открытого и шифрованного текстов являются пары целых от 0 до 31. Для зашифрования используется секретный ключ k (целое число от 0 до 31), заданная таблично функция h , а также функция $g(c, d)$, которая паре целых чисел (c, d) ставит в соответствие пару $(d, c + h(d + k))$ (причем если число $d + k$ или $d + h(d + k)$ превышает 31, то их заменяют остатком от деления на 32). Знак шифрованного текста (b_1, b_2) получается из знака открытого текста (a_1, a_2) путем 128-кратного применения функции g :

$$(b_1, b_2) = g^{128}(a_1, a_2) = g(\dots g(g(a_1, a_2))).$$

Известно, что знак открытого текста $(21,0)$ преобразовался в знак зашифрованного текста $(15,25)$, знак $(7,3)$ преобразовался в $(29,5)$, $(0,17)$ – в $(25,4)$ и, наконец, $(5,21)$ – в $(22,9)$.

Найдите ключ k .

i	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
$h(i)$	9	1	30	4	24	12	8	23	18	7	16	15	21	26	10	17	19	22	13	28	14	11	2	29	3	6	27	0	5	25	31	20

4. На вход устройства подается лента с записанными на ней нулями и единицами:

Лента	1 0 0 1 0 0 0 1 1 0 1 1 1 1 0 0 0 1 1 0 0 0 0 1 1 0 1 0 1 1 0 1 0 0 1 1 0 1 1 0 ...																														
Позиции	μ_1	μ_2	μ_3																												

За один такт устройство считывает с ленты с позиций μ_1, μ_2, μ_3 (на первом такте $\mu_1 = 1$) три значения x, y, z . Если $x + y + z \geq 2$, то устройство на новой ленте печатает

1, иначе – 0. Затем устройство сдвигается на одну позицию вправо, и процедура повторяется. Найдите разности

$d_1 = \mu_2 - \mu_1$ и $d_2 = \mu_3 - \mu_2$, если известно, что $d_1 + d_2 \leq 10$, а на новой ленте было напечатано следующее: 1 0 0 1 0 0 0 1 1 0 0 0 0 1 1 0 0 0 1 1 0 0 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 0 1... (для примера на рисунке изображен случай $d_1 = 3, d_2 = 5$).

5. Решите уравнение $p^4 + q^2 = n^2$, где p и q - простые числа, а n - натуральное число. В ответе запишите числом значение произведения $p \cdot q \cdot n$.

6. В Криптоландии используется алфавит, состоящий из четырёх латинских букв a, b, c, d . Любая последовательность букв алфавита будет словом криптоландского языка при выполнении единственного ограничения: если в последовательности есть хоть одна буква "a", то тогда в ней обязательно должны встретиться две буквы "a" подряд.

Например, последовательности $baacda, aabb, ddd$ являются словами, а последовательности $bcadda, abba$ – не являются. Найдите число слов длины 8 в криптоландском языке.

10 КЛАСС

1. Установите, можно ли создать телефонную сеть связи, состоящую из 991 абонента, каждый из которых был бы связан ровно с 93 другими.

2. Дана криптограмма:

ПШ	*	Ь	=	ПЕП
+		*		-
ИИ	+	И	=	ШБ
=		=		=
ЫТЕ	+	ДО	=	ЫДШ

Восстановите цифровые значения букв, при которых справедливы все указанные равенства, если разным буквам соответствуют различные цифры. Расставьте буквы в порядке возрастания их цифровых значений и получите искомый текст. В ответе запишите полученный текст заглавными буквами без пробелов между словами, если их в тексте несколько. Пример: ОТБОРОЧНЫЙЭТАП или ОЛИМПИАДА.

3. Знаками открытого и шифрованного текстов являются пары целых от 0 до 31. Для зашифрования используется секретный ключ k (целое число от 0 до 31), заданная таблично функция h , а также функция $g(c, d)$, которая паре целых чисел (c, d) ставит в соответствие пару $(d, c + h(d + k))$ (причем если число $d + k$ или

$d + h(d + k)$ превышает 31, то их заменяют остатком от деления на 32). Знак шифрованного текста (b_1, b_2) получается из знака открытого текста (a_1, a_2) путем 128-кратного применения функции g :

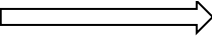
$$(b_1, b_2) = g^{128}(a_1, a_2) = g(\dots g(g(a_1, a_2))).$$

Известно, что знак открытого текста $(21,0)$ преобразовался в знак зашифрованного текста $(15,25)$, знак $(7,3)$ преобразовался в $(29,5)$, $(0,17)$ – в $(25,4)$ и, наконец, $(5,21)$ – в $(22,9)$.

Найдите ключ k .

i	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
$h(i)$	9	1	30	4	24	12	8	23	18	7	16	15	21	26	10	17	19	22	13	28	14	11	2	29	3	6	27	0	5	25	31	20

4. На вход устройства подается лента с записанными на ней нулями и единицами:

Лента	1 0 0 1 0 0 0 1 1 0 1 1 1 1 0 0 0 1 1 0 0 0 0 1 1 0 1 0 1 1 0 1 0 0 1 1 0 1 1 0...																														
Позиции	μ_1	μ_2	μ_3																												

За один такт устройство считывает с ленты с позиций μ_1, μ_2, μ_3 (на первом такте $\mu_1 = 1$) три значения x, y, z . Если $x + y + z \geq 2$, то устройство на новой ленте печатает 1, иначе – 0. Затем устройство сдвигается на одну позицию вправо, и процедура повторяется. Найдите разности

$d_1 = \mu_2 - \mu_1$ и $d_2 = \mu_3 - \mu_2$, если известно, что $d_1 + d_2 \leq 10$, а на новой ленте было напечатано следующее:

1 0 0 1 0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 0 1...

(для примера на рисунке изображен случай $d_1 = 3, d_2 = 5$).

5. Решите уравнение $\mathbf{p}^4 + \mathbf{q}^2 = \mathbf{n}^2$, где \mathbf{p} и \mathbf{q} - простые числа, а \mathbf{n} - натуральное число. В ответе запишите числом значение произведения $\mathbf{p} \cdot \mathbf{q} \cdot \mathbf{n}$.

6. В Криптоландии используется алфавит, состоящий из четырёх латинских букв a, b, c, d . Любая последовательность букв алфавита будет словом криптоландского языка при выполнении единственного ограничения: если в последовательности есть хоть одна буква "a", то тогда в ней обязательно должны встретиться две буквы "a" подряд.

Например, последовательности $baacda, aabb, ddd$ являются словами, а последовательности $bcadda, abba$ – не являются. Найдите число слов длины 8 в криптоландском языке.

11 КЛАСС

1. Установите, можно ли создать телефонную сеть связи, состоящую из 991 абонента, каждый из которых был бы связан ровно с 93 другими.
2. Дана криптограмма:

ПШ	*	Ь	=	ПЕП
+		*		-
ИИ	+	И	=	ШБ
=		=		=
ЫТЕ	+	ДО	=	ЫДШ

Восстановите цифровые значения букв, при которых справедливы все указанные равенства, если разным буквам соответствуют различные цифры. Расставьте буквы в порядке возрастания их цифровых значений и получите искомый текст. В ответе запишите полученный текст заглавными буквами без пробелов между словами, если их в тексте несколько. Пример: ОТБОРОЧНЫЙЭТАП или ОЛИМПИАДА.

3. Знаками открытого и шифрованного текстов являются пары целых от 0 до 31. Для зашифрования используется секретный ключ k (целое число от 0 до 31), заданная таблично функция h , а также функция $g(c, d)$, которая паре целых чисел (c, d) ставит в соответствие пару $(d, c + h(d + k))$ (причем если число $d + k$ или $d + h(d + k)$ превышает 31, то их заменяют остатком от деления на 32). Знак шифрованного текста (b_1, b_2) получается из знака открытого текста (a_1, a_2) путем 128-кратного применения функции g :

$$(b_1, b_2) = g^{128}(a_1, a_2) = g(\dots g(g(a_1, a_2))).$$

Известно, что знак открытого текста $(21,0)$ преобразовался в знак зашифрованного текста $(15,25)$, знак $(7,3)$ преобразовался в $(29,5)$, $(0,17)$ – в $(25,4)$ и, наконец, $(5,21)$ – в $(22,9)$.

Найдите ключ k .

i	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
$h(i)$	9	1	30	4	24	12	8	23	18	7	16	15	21	26	10	17	19	22	13	28	14	11	2	29	3	6	27	0	5	25	31	20

4. На вход устройства подается лента с записанными на ней нулями и единицами:

Лента	1 0 0 1 0 0 0 1 1 0 1 1 1 1 0 0 0 1 1 0 0 0 0 1 1 0 1 0 1 1 0 1 0 0 1 1 0 1 1 0...																														
Позиции	μ_1	μ_2	μ_3	→																											

За один такт устройство считывает с ленты с позиций μ_1, μ_2, μ_3 (на первом такте $\mu_1 = 1$) три значения x, y, z . Если $x + y + z \geq 2$, то устройство на новой ленте печатает

1, иначе – 0. Затем устройство сдвигается на одну позицию вправо, и процедура повторяется. Найдите разности

$d_1 = \mu_2 - \mu_1$ и $d_2 = \mu_3 - \mu_2$, если известно, что $d_1 + d_2 \leq 10$, а на новой ленте было напечатано следующее:

1 0 0 1 0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 0 1...

(для примера на рисунке изображен случай $d_1 = 3$, $d_2 = 5$).

5. Решите уравнение $p^4 + q^2 = n^2$, где p и q - простые числа, а n - натуральное число. В ответе запишите числом значение произведения $p \cdot q \cdot n$.

6. В Криптоландии используется алфавит, состоящий из четырёх латинских букв a , b , c , d . Любая последовательность букв алфавита будет *словом* криптоландского языка при выполнении единственного ограничения: если в последовательности есть хоть одна буква "a", то тогда в ней обязательно должны встретиться две буквы "a" подряд.

Например, последовательности $baacda$, $aabb$, ddd являются словами, а последовательности $bcadda$, $abba$ – не являются. Найдите число слов длины 8 в криптоландском языке.