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.

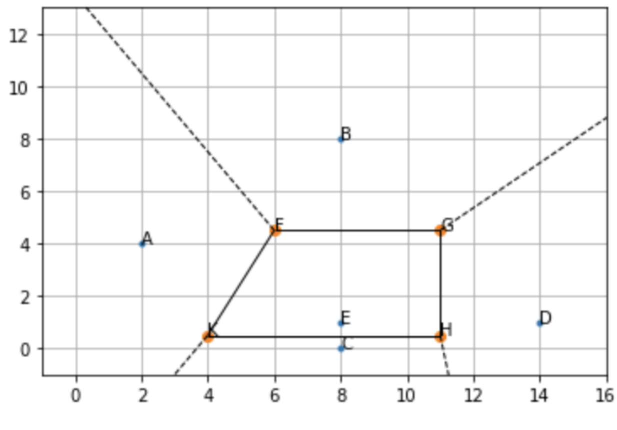
Решение.

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

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

Решение. Заметим, что $\boldsymbol{x}^{d+8n}=\boldsymbol{x}^d$ для любого натурального числа n. Вектору $\boldsymbol{x}=(x_1,\dots,x_8)$ взаимно-однозначно соответствует многочлен $x(t)=x_1+x_2t+\dots+x_7t^7+x_8t^8$. Тогда циклический сдвиг вектора $\boldsymbol{x}$ на d позиций вправо равносилен умножению многочлена $\boldsymbol{x(t)}$ на $\boldsymbol{t^d}$ и приведению степеней мономов по модулю 8. Вектору $\boldsymbol{x}=\boldsymbol{v}+\boldsymbol{v}^1+\boldsymbol{v}^4$ соответствует многочлен $x(t)=1+t+t^4$. Таким образом, нахождение $d_1,\dots,d_n$ таких, что $\boldsymbol{v}=\boldsymbol{x}^{d_1}+\dots+\boldsymbol{x}^{d_n}$ 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:

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

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

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

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 $t \geq 1$

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

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:

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

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:

$$A = \big((x_1 * x_2) * x_3\big) * x_4,$$
$$B = (x_5 \circ x_6) \circ x_7.$$

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

∘	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.