

XXXIII

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

УСЛОВИЯ И РЕШЕНИЯ



Москва 2024

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП	2
9 КЛАСС	2
УСЛОВИЯ ЗАДАЧ	2
РЕШЕНИЯ ЗАДАЧ.....	4
10 КЛАСС	5
УСЛОВИЯ ЗАДАЧ	5
РЕШЕНИЯ ЗАДАЧ.....	6
11 КЛАСС	8
УСЛОВИЯ ЗАДАЧ	8
РЕШЕНИЯ ЗАДАЧ.....	9
ОТБОРОЧНЫЙ ЭТАП	12
9 КЛАСС	12
10 КЛАСС	13
11 КЛАСС	14
ОТВЕТЫ.....	16

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

9 КЛАСС

УСЛОВИЯ ЗАДАЧ

1. Найдите пять простых чисел, образующих арифметическую прогрессию с разностью 12. Ответ обоснуйте.
2. Катя и Юра играют в следующую игру. Имеется пустая таблица из одной строки, состоящая из $k = 100$ пустых ячеек: (a_1, \dots, a_k) , которые игроки заполняют числами от 0 до 6. Первым ходит Юра, который выбирает число t такое, что $1 \leq t \leq 99$ и заполняет t ячеек.

Второй ходит Катя, которая заполняет оставшиеся ячейки. Победитель определяется по следующему правилу: если в результате получается «счастливая» комбинация чисел – полностью заполненная таблица, в которой числа можно разбить на две непересекающиеся группы, суммы чисел в которых одинаковы, то выигрывает Катя, в противном случае выигрывает Юра. Например, комбинация (1,5,3,4,6) не является «счастливой», так как в ней присутствует нечетное число нечетных чисел. С другой стороны, комбинация (6,5,3,6,4) является «счастливой», так как $6 + 6 = 5 + 3 + 4$. У кого из игроков имеется выигрышная стратегия? Ответ обоснуйте.

3. а) перестановка f чисел $\{0, 1, \dots, 6\}$ задана таблицей:

Например, $f(2) = 0$. Найдите две перестановки g и h такие, что для всех $x \in \{0, 1, \dots, 6\}$ выполняется

x	0	1	2	3	4	5	6
$f(x)$	2	3	0	4	6	5	1

$$f(x) = (g(x) + h(x)) \pmod{7}.$$

б) перестановка f задана на чётном количестве чисел $\{0, 1, \dots, 2n - 1\}$ таблицей:

x	0	1	2	..	$2n - 2$	$2n - 1$
$f(x)$	i_0	i_1	i_2	..	i_{2n-2}	i_{2n-1}

Здесь $(i_0, i_1, \dots, i_{2n-1})$ – перестановка чисел $\{0, 1, \dots, 2n - 1\}$.

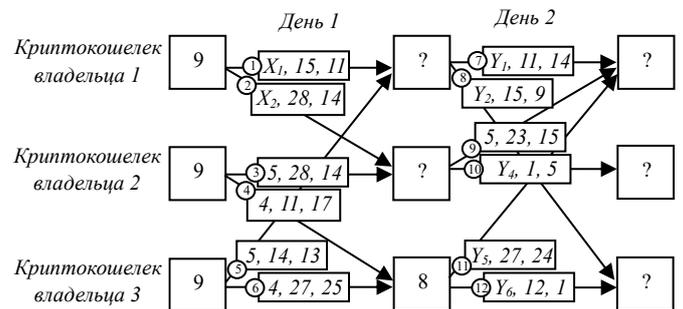
Докажите, что не существует перестановок g и h таких, что для всех $x \in \{0, 1, \dots, 2n - 1\}$ выполняется $f(x) = (g(x) + h(x)) \pmod{2n}$.

4. В криптосистеме RSA (знания алгоритма шифрования не требуется для решения задачи) элементы надёжности определяются несколькими параметрами. В частности, выбором числа $N = p \cdot q$, где p, q – различные нечётные простые числа, и значением $\varphi(N) = (p - 1) \cdot (q - 1)$. Известна следующая теорема (малая теорема Ферма): если p – простое число, a – целое число, не делящееся на p , то $a^{p-1} = 1 \pmod{p}$. Используя это:

а) докажите, что $x^{\frac{\varphi(N)+1}{2}} = x \pmod{N}$ для всех $x \in \{1, 2, \dots, N - 1\}$.

б) найдите p и q , если известно, что $N = 44814101$ и $x^{22400353} = x \pmod{N}$ для всех $x \in \{1, 2, \dots, N - 1\}$.

5. Каждый из трех владельцев криптокошельков имеет на своем счету по 9 криптокойнов. Каждый из двух дней ими совершаются по две транзакции: по переводу части криптокойнов со своего криптокошелька на криптокошелек другого владельца и по возврату оставшихся криптокойнов обратно на свой кошелек. У каждого имеется свой секретный ключ $S \in \{1, 2, \dots, 28\}$. При совершении транзакции указываются три числа (X, a, b) , где X – число переводимых криптокойнов, (a, b) – электронная подпись перевода. Электронная подпись находится по правилу: выбираем произвольное $k \in \{1, 2, \dots, 28\}$, затем находим $a = r_{29}(2^k)$, $b = r_{28}(Xa + Sk)$, где $r_N(M)$ – остаток от деления числа M на N .



На рисунке указаны совершенные транзакции (пронумерованы числами в кружках) за два дня. Сколько будет криптокойнов у каждого владельца криптокошелька по окончании двух дней?

6. Вася хочет заполнить квадратную таблицу (криптографическую мозаику) размера 4×4 целыми числами от 0 до 16 по следующему правилу. Сначала он выбирает четыре целых числа $b_1, b_2, b_3, b_4 \in \{0, 1, \dots, 16\}$. Затем первую строку Вася заполняет числами $a_i^{(1)} = (b_i + 1) \pmod{17}, i = 1, 2, 3, 4$, вторую строку – числами $a_i^{(2)} = (b_i + 4) \pmod{17}, i = 1, 2, 3, 4$,

XXXIII Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии третью $a_i^{(3)} = (b_i + 13)(\text{mod } 17), i = 1, 2, 3, 4$ и, аналогично, четвертую $a_i^{(4)} = (b_i + 16)(\text{mod } 17), i = 1, 2, 3, 4$. При этом числа b_1, b_2, b_3, b_4 Вася выбрать должен так, чтобы все числа в таблице оказались различными и не было числа 8. Сумеет ли Вася это сделать? Если да, то чему равны b_1, b_2, b_3, b_4

РЕШЕНИЯ ЗАДАЧ

Задача 1

ОТВЕТ: 5,17,29,41,53.

Задача 2

Очевидно, что достаточно рассмотреть случай, когда игрок, делающий первый ход, заполняет максимально возможное число ячеек, равное $k - 1$. Расположим эти $k - 1$ число в порядке не убывания: $a_{i_1} \leq a_{i_2} \leq \dots \leq a_{i_{k-1}}$.

Здесь в индексах указаны номера позиций, на которых стоят эти числа в таблице. Образует два множества позиций, которые заполнены: $\{i_1, i_3, \dots\}$ и $\{i_2, i_4, \dots\}$, беря указанные числа через одно. Тогда суммы чисел на этих позициях могут отличаться друг от друга не более, чем на 6. Поэтому оставшуюся незаполненной позицию можно заполнить числом от 0 до 6 так, чтобы получилась «счастливая» комбинация

ОТВЕТ: Если первым ходит Юра, то Катя всегда может выиграть.

Задача 3

а) Так как $\text{НОД}(2,7)=\text{НОД}(6,7)=1$, то $g(x) = 2f(x)(\text{mod } 7)$ и $h(x) = 6f(x)(\text{mod } 7)$ являются перестановками. Но тогда, например, $g(x) = 2f(x), h(x) = 6f(x)$ и выполняется $g(x) + h(x) = 2f(x) + 6f(x) = f(x)(\text{mod } 7)$.

б) $\sum_{i=0}^{2n-1} f(x) = \sum_{i=0}^{2n-1} x = (2n + 1)n = n(\text{mod } (2n))$.

С другой стороны, если указанное условия пункта б) представление существует, то

$$\sum_{i=0}^{2n-1} f(x) = \sum_{i=0}^{2n-1} g(x) + \sum_{i=0}^{2n-1} h(x) = 2(2n + 1)n = 0(\text{mod } (2n)).$$

Что доказывает невозможность указанного представления.

Задача 4

а) из условия задачи и равенства $a^{p-1} = 1(\text{mod } p)$ следует $a^{k(p-1)+1} = a(\text{mod } p)$ для любого натурального k . Тогда при $k = \frac{q-1}{2}$ получим $a^{\frac{\varphi(N)}{2}+1} = a(\text{mod } p)$.

Аналогично $a^{\frac{\varphi(N)}{2}+1} = a(\text{mod } q)$. Так как p, q – простые числа, то из этих полученных выше равенств следует $a^{\frac{\varphi(N)}{2}+1} = a(\text{mod } N)$. Пункт а) доказан.

б) предположим, что $\frac{\varphi(N)}{2} + 1 = 22400353$. Тогда получим систему уравнений $p \cdot q = 44814101, (p - 1) \cdot (q - 1) = 44800704$.

Решая полученную систему, находим $p = 6949, q = 6449$.

ОТВЕТ: $p = 6949, q = 6449$.

Задача 5

Сначала по рисунку выпишем очевидные соотношения:

$$X_1 + X_2 = 9 \quad (1)$$

$$Y_1 + Y_2 = X_1 + 5 \quad (2)$$

$$5 + Y_4 = X_2 + 5 \quad (3)$$

$$Y_5 + Y_6 = 8 \quad (4)$$

Необходимо найти: $\Sigma_1 = Y_1 + 5 + Y_5, \Sigma_2 = Y_4, \Sigma_3 = Y_2 + Y_6$.

Далее, заметим, что транзакции №1 и №8 осуществлены одним и тем же владельцем – владельцем 1. То есть использовался один и тот же секретный ключ S_1 , при этом использовалось одно и то же значение k в подписи, поэтому:

$$11 = (15X_1 + S_1k)(\text{mod } 28),$$

$$9 = (15Y_2 + S_1k)(\text{mod } 28).$$

$$\text{Отсюда получим: } 2 = 30 = (15(X_1 - Y_2))(\text{mod } 28).$$

$$\text{Следовательно, } X_1 - Y_2 = 2.$$

$$\text{С учетом (2) имеем: } Y_1 = X_1 - Y_2 + 5 = 7.$$

Аналогичное свойство замечаем у транзакций №6 и №11:

$$25 = (27 \cdot 4 + S_3k)(\text{mod } 28),$$

$$24 = (27Y_5 + S_3k)(\text{mod } 28).$$

Отсюда получим: $1 = -27 = (27(4 - Y_5))(\text{mod } 28)$. Следовательно, $Y_5 = 5$ и уже находится $\Sigma_1 = 7 + 5 + 5 = 17$.

Теперь обратим внимание на транзакцию №10, у которой $a = 1 = 2^0(\text{mod } 29)$, т.е. $k = 0(\text{mod } 28) = 28$. Значит $5 = (Y_4 + S_2 \cdot 28)(\text{mod } 28) = Y_4$ и $\Sigma_2 = 5$.

Т.к. исходная сумма криптокойнов была равна 27, то $\Sigma_3 = 27 - \Sigma_1 - \Sigma_2 = 5$.

ОТВЕТ: (17,5,5).

Задача 6

Задачу можно решить древовидным перебором всех вариантов. Существование подобных мозаик для других простых чисел является открытой проблемой. Гипотеза утверждает, что такие мозаики существуют только для простых чисел Ферма: 3,5,17,257.

ОТВЕТ: 0,6,10,16.

10 КЛАСС

УСЛОВИЯ ЗАДАЧ

1. Найдите пять простых чисел, образующих арифметическую прогрессию с разностью 12. Ответ обоснуйте.
2. Катя и Юра играют в следующую игру. Имеется пустая таблица из одной строки, состоящая из $k = 100$ пустых ячеек: (a_1, \dots, a_k) , которые игроки заполняют числами от 0 до 6. Первым ходит Юра, который выбирает число t такое, что $1 \leq t \leq 99$ и заполняет t ячеек. Второй ходит Катя, которая заполняет оставшиеся ячейки. Победитель определяется по следующему правилу: если в результате получается «счастливая» комбинация чисел – полностью заполненная таблица, в которой числа можно разбить на две непересекающиеся группы, суммы чисел в которых одинаковы, то выигрывает Катя, в противном случае выигрывает Юра. Например, комбинация (1,5,3,4,6) не является «счастливой», так как в ней присутствует нечетное число нечетных чисел. С другой стороны, комбинация (6,5,3,6,4) является «счастливой», так как $6 + 6 = 5 + 3 + 4$. У кого из игроков имеется выигрышная стратегия? Ответ обоснуйте.
3. а) перестановка f чисел $\{0,1, \dots, 6\}$ задана таблицей:
Например, $f(2) = 0$. Найдите две перестановки g и h такие, что для всех $x \in \{0,1, \dots, 6\}$ выполняется
выполняется
 $f(x) = (g(x) + h(x))(\text{mod } 7)$.

x	0	1	2	3	4	5	6
$f(x)$	2	3	0	4	6	5	1

b) перестановка f задана на чётном количестве чисел $\{0, 1, \dots, 2n - 1\}$ таблицей:

x	0	1	2	...	$2n - 2$	$2n - 1$
$f(x)$	i_0	i_1	i_2	...	i_{2n-2}	i_{2n-1}

Здесь $(i_0, i_1, \dots, i_{2n-1})$ – перестановка чисел $\{0, 1, \dots, 2n - 1\}$.

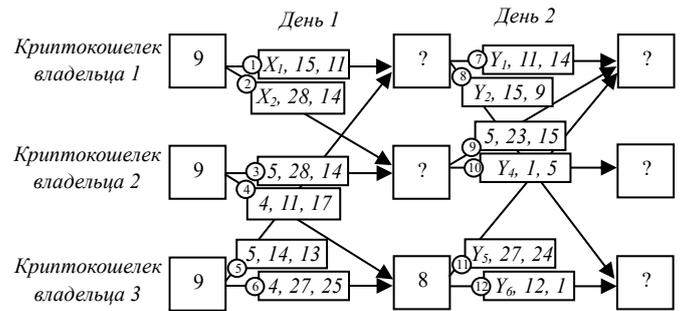
Докажите, что не существует перестановок g и h таких, что для всех $x \in \{0, 1, \dots, 2n - 1\}$ выполняется $f(x) = (g(x) + h(x)) \pmod{2n}$.

4. В криптосистеме RSA (знания алгоритма шифрования не требуется для решения задачи) элементы надёжности определяются несколькими параметрами. В частности, выбором числа $N = p \cdot q$, где p, q – различные нечётные простые числа, и значением $\varphi(N) = (p - 1) \cdot (q - 1)$. Известна следующая теорема (малая теорема Ферма): если p – простое число, a – целое число, не делящееся на p , то $a^{p-1} = 1 \pmod{p}$. Используя это:

с) докажите, что $x^{\frac{\varphi(N)}{2}+1} = x \pmod{N}$ для всех $x \in \{1, 2, \dots, N - 1\}$.

d) найдите p и q , если известно, что $N = 44814101$ и $x^{22400353} = x \pmod{N}$ для всех $x \in \{1, 2, \dots, N - 1\}$.

6. Каждый из трех владельцев криптокошельков имеет на своем счету по 9 криптокойнов. Каждый из двух дней ими совершаются по две транзакции: по переводу части криптокойнов со своего криптокошелька на криптокошелек другого владельца и по возврату оставшихся криптокойнов обратно на свой кошелек. У каждого имеется свой секретный ключ $S \in \{1, 2, \dots, 28\}$. При совершении транзакции указываются три числа (X, a, b) , где X – число переводимых криптокойнов, (a, b) – электронная подпись перевода. Электронная подпись находится по правилу: выбираем произвольное $k \in \{1, 2, \dots, 28\}$, затем находим $a = r_{29}(2^k)$, $b = r_{28}(Xa + Sk)$, где $r_N(M)$ – остаток от деления числа M на N .



На рисунке указаны совершенные транзакции (пронумерованы числами в кружках) за два дня. Сколько будет криптокойнов у каждого владельца криптокошелька по окончании двух дней?

7. Вася хочет заполнить квадратную таблицу (криптографическую мозаику) размера 4×4 целыми числами от 0 до 16 по следующему правилу. Сначала он выбирает четыре целых числа $b_1, b_2, b_3, b_4 \in \{0, 1, \dots, 16\}$. Затем первую строку Вася заполняет числами $a_i^{(1)} = (b_i + 1) \pmod{17}, i = 1, 2, 3, 4$, вторую строку – числами $a_i^{(2)} = (b_i + 4) \pmod{17}, i = 1, 2, 3, 4$, третью $a_i^{(3)} = (b_i + 13) \pmod{17}, i = 1, 2, 3, 4$ и, аналогично, четвертую $a_i^{(4)} = (b_i + 16) \pmod{17}, i = 1, 2, 3, 4$. При этом числа b_1, b_2, b_3, b_4 Вася выбрать должен так, чтобы все числа в таблице оказались различными и не было числа 8. Сумеет ли Вася это сделать? Если да, то чему равны b_1, b_2, b_3, b_4

РЕШЕНИЯ ЗАДАЧ

Задача 1

ОТВЕТ: 5,17,29,41,53.

Задача 2

Очевидно, что достаточно рассмотреть случай, когда игрок, делающий первый ход, заполняет максимально возможное число ячеек, равное $k - 1$. Расположим эти $k - 1$ число в порядке не убывания: $a_{i_1} \leq a_{i_2} \leq \dots \leq a_{i_{k-1}}$.

XXXIII Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии
Здесь в индексах указаны номера позиций, на которых стоят эти числа в таблице. Образуются два множества позиций, которые заполнены: $\{i_1, i_3, \dots\}$ и $\{i_2, i_4, \dots\}$, беря указанные числа через одно. Тогда суммы чисел на этих позициях могут отличаться друг от друга не более, чем на 6. Поэтому оставшуюся незаполненной позицию можно заполнить числом от 0 до 6 так, чтобы получилась «счастливая» комбинация

ОТВЕТ: Если первым ходит Юра, то Катя всегда может выиграть.

Задача 3

а) Так как $\text{НОД}(2,7)=\text{НОД}(6,7)=1$, то $g(x) = 2f(x)(\text{mod } 7)$ и $h(x) = 6f(x)(\text{mod } 7)$ являются перестановками. Но тогда, например, $g(x) = 2f(x)$, $h(x) = 6f(x)$ и выполняется

$$g(x) + h(x) = 2f(x) + 6f(x) = f(x)(\text{mod } 7).$$

б) $\sum_{i=0}^{2n-1} f(x) = \sum_{i=0}^{2n-1} x = (2n+1)n = n(\text{mod } (2n)).$

С другой стороны, если указанное условие пункта б) представление существует, то

$$\sum_{i=0}^{2n-1} f(x) = \sum_{i=0}^{2n-1} g(x) + \sum_{i=0}^{2n-1} h(x) = 2(2n+1)n = 0(\text{mod } (2n)).$$

Что доказывает невозможность указанного представления.

Задача 4

а) из условия задачи и равенства $a^{p-1} = 1(\text{mod } p)$ следует $a^{k(p-1)+1} = a(\text{mod } p)$ для любого натурального k . Тогда при $k = \frac{q-1}{2}$ получим $a^{\frac{\varphi(N)}{2}+1} = a(\text{mod } p)$.

Аналогично $a^{\frac{\varphi(N)}{2}+1} = a(\text{mod } q)$. Так как p, q – простые числа, то из этих полученных выше равенств следует $a^{\frac{\varphi(N)}{2}+1} = a(\text{mod } N)$. Пункт а) доказан.

с) предположим, что $\frac{\varphi(N)}{2} + 1 = 22400353$. Тогда получим систему уравнений $p \cdot q = 44814101$, $(p-1) \cdot (q-1) = 44800704$.

Решая полученную систему, находим $p = 6949, q = 6449$.

ОТВЕТ: $p = 6949, q = 6449$.

Задача 5

Сначала по рисунку выпишем очевидные соотношения:

$$X_1 + X_2 = 9 \quad (1)$$

$$Y_1 + Y_2 = X_1 + 5 \quad (2)$$

$$5 + Y_4 = X_2 + 5 \quad (3)$$

$$Y_5 + Y_6 = 8 \quad (4)$$

Необходимо найти: $\Sigma_1 = Y_1 + 5 + Y_5$, $\Sigma_2 = Y_4$, $\Sigma_3 = Y_2 + Y_6$.

Далее, заметим, что транзакции №1 и №8 осуществлены одним и тем же владельцем – владельцем 1. То есть использовался один и тот же секретный ключ S_1 , при этом использовалось одно и то же значение k в подписи, поэтому:

$$11 = (15X_1 + S_1k)(\text{mod } 28),$$

$$9 = (15Y_2 + S_1k)(\text{mod } 28).$$

Отсюда получим: $2 = 30 = (15(X_1 - Y_2))(\text{mod } 28)$.

Следовательно, $X_1 - Y_2 = 2$.

С учетом (2) имеем: $Y_1 = X_1 - Y_2 + 5 = 7$.

Аналогичное свойство замечаем у транзакций №6 и №11:

$$25 = (27 \cdot 4 + S_3k)(\text{mod } 28),$$

$$24 = (27Y_5 + S_3k)(\text{mod } 28).$$

Отсюда получим: $1 = -27 = (27(4 - Y_5))(\text{mod } 28)$. Следовательно, $Y_5 = 5$ и уже находится $\Sigma_1 = 7 + 5 + 5 = 17$.

XXXIII Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии
 Теперь обратим внимание на транзакцию №10, у которой $a = 1 = 2^0 \pmod{29}$, т.е. $k = 0 \pmod{28} = 28$. Значит $5 = (Y_4 + S_2 \cdot 28) \pmod{28} = Y_4$ и $\Sigma_2 = 5$.

Т.к. исходная сумма криптокойнов была равна 27, то $\Sigma_3 = 27 - \Sigma_1 - \Sigma_2 = 5$.

ОТВЕТ: (17,5,5).

Задача 6

Задачу можно решить древовидным перебором всех вариантов. Существование подобных мозаик для других простых чисел является открытой проблемой. Гипотеза утверждает, что такие мозаики существуют только для простых чисел Ферма: 3,5,17,257.

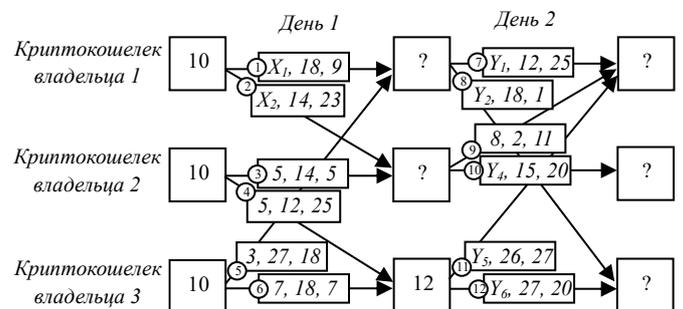
ОТВЕТ: 0,6,10,16.

11 КЛАСС

УСЛОВИЯ ЗАДАЧ

1. Катя и Юра играют в следующую игру. Имеется пустая таблица из одной строки, состоящая из $k = 2023^2$ пустых ячеек: (a_1, \dots, a_k) , которые игроки заполняют числами от 0 до 2022. Первым ходит Юра, который выбирает число t такое, что $1 \leq t \leq k - 1$ и заполняет t ячеек. Второй ходит Катя, которая заполняет оставшиеся ячейки. Победитель определяется по следующему правилу: если в результате получается «счастливая» комбинация чисел – полностью заполненная таблица, в которой числа можно разбить на две непересекающиеся группы, суммы чисел в которых одинаковы, то выигрывает Катя, в противном случае выигрывает Юра. Например, комбинация (7,5,3,4,6) не является «счастливой», так как в ней присутствует нечетное число нечетных чисел. С другой стороны, комбинация (4,5,1,6,8) является «счастливой», так как $4 + 8 = 5 + 1 + 6$. У кого из игроков имеется выигрышная стратегия? Ответ обосновать.

2. Каждый из трех владельцев криптокошельков имеет на своем счету по 10 криптокойнов. Каждый из двух дней ими совершаются по две транзакции: по переводу части криптокойнов со своего криптокошелька на криптокошелек другого владельца и по возврату оставшихся криптокойнов обратно на свой кошелек. У каждого имеется свой секретный ключ $S \in \{1, 2, \dots, 28\}$. При совершении транзакции указываются три числа (X, a, b) , где X - число переводимых криптокойнов, (a, b) - электронная подпись перевода. Электронная подпись находится по правилу: выбираем произвольное $k \in \{1, 2, \dots, 28\}$, затем находим $a = r_{29}(2^k)$, $b = r_{28}(Xa + Sk)$, где $r_N(M)$ – остаток от деления числа M на N . На рисунке указаны совершенные транзакции (пронумерованы числами в кружках) за два дня. Сколько будет криптокойнов у каждого владельца криптокошелька по окончании двух дней?



3. а) перестановка f чисел $\{0, 1, \dots, 6\}$ задана таблицей:
 Например, $f(2) = 4$. Найдите две различные перестановки g и h такие, что для всех $x \in \{0, 1, \dots, 6\}$ выполняется

x	0	1	2	3	4	5	6
$f(x)$	3	2	4	0	5	6	1

$$f(x) = (g(x) + h(x)) \pmod{7}.$$

b) перестановка f задана на чётном количестве чисел $\{0, 1, \dots, 2n - 1\}$ таблицей:

x	0	1	2	..	$2n - 2$	$2n - 1$
$f(x)$	i_0	i_1	i_2	..	i_{2n-2}	i_{2n-1}

Здесь $(i_0, i_1, \dots, i_{2n-1})$ – перестановка чисел $\{0, 1, \dots, 2n - 1\}$.

Докажите, что не существует перестановок g и h таких, что для всех $x \in \{0, 1, \dots, 2n - 1\}$ выполняется $f(x) = (g(x) + h(x)) \pmod{(2n)}$?

4. В криптосистеме RSA (знания алгоритма шифрования не требуется для решения задачи) элементы надёжности определяются несколькими параметрами. В частности, выбором числа $N = p \cdot q$, где p, q – различные нечётные простые числа, и значением $\varphi(N) = (p - 1) \cdot (q - 1)$. Известна следующая теорема (малая теорема Ферма): если p – простое число, a – целое число, не делящееся на p , то $a^{p-1} = 1 \pmod{p}$. Используя это:

a) докажите, что $x^{\frac{\varphi(N)}{2}+1} = x \pmod{N}$ для всех $x \in \{1, 2, \dots, N - 1\}$.

b) найдите p и q , если известно, что $N = 42494861$ и $x^{2^{1240913}} = x \pmod{N}$ для всех $x \in \{1, 2, \dots, N - 1\}$.

5. Четыре компьютера, расположенные в вершинах квадрата $ABCD$, соединены прямолинейными отрезками проводов с сервером, который находится в точке O пересечения диагоналей. Сторона квадрата равна 2 м. Несложно заметить, что для такого подключения потребуется $4\sqrt{2}$ метров провода. Чтобы уменьшить длину проводов, вам разрешается передвинуть сервер из точки O в любую другую точку O_1 , а также компьютер из точки A в любую другую точку A_1 так, чтобы новая суммарная длина проводов $S = O_1A_1 + O_1B + O_1C + O_1D$ была как можно меньше. Разрешается компьютеры и сервер размещать в одной точке (например, точка A_1 может совпасть с точкой B). Компьютеры в вершинах B, C, D двигать нельзя. Чему равно минимальное значение S .
6. Вася хочет заполнить квадратную таблицу (криптографическую мозаику) размера 4×4 целыми числами от 1 до 16 по следующему правилу. Сначала он выбирает четыре целых числа $b_1, b_2, b_3, b_4 \in \{0, 1, \dots, 16\}$. Затем первую строку Вася заполняет числами $a_i^{(1)} = (b_i + 1) \pmod{17}, i = 1, 2, 3, 4$, вторую строку – числами $a_i^{(2)} = (b_i + 4) \pmod{17}, i = 1, 2, 3, 4$, третью $a_i^{(3)} = (b_i + 13) \pmod{17}, i = 1, 2, 3, 4$ и, аналогично, четвертую $a_i^{(4)} = (b_i + 16) \pmod{17}, i = 1, 2, 3, 4$. При этом числа b_1, b_2, b_3, b_4 Вася выбрать должен так, чтобы все числа в таблице оказались различными. Сумеет ли Вася это сделать? Если да, то чему равны b_1, b_2, b_3, b_4 ?

РЕШЕНИЯ ЗАДАЧ

Задача 1

Очевидно, что достаточно рассмотреть случай, когда игрок, делающий первый ход, заполняет максимально возможное число ячеек, равное $k - 1$. Расположим эти $k - 1$ число в порядке не убывания: $a_{i_1} \leq a_{i_2} \leq \dots \leq a_{i_{k-1}}$.

Здесь в индексах указаны номера позиций, на которых стоят эти числа в таблице. образуем два множества позиций, которые заполнены: $\{i_1, i_3, \dots\}$ и $\{i_2, i_4, \dots\}$, беря указанные числа через одно. Тогда суммы чисел на этих позициях могут отличаться друг от друга не более, чем на 2023. Поэтому оставшуюся незаполненной позицию можно заполнить числом от 0 до 2023 так, чтобы получилась «счастливая» комбинация.

ОТВЕТ: Если первым ходит Юра, то Катя всегда может выиграть.

XXXIII Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии
Задача 2

Сначала по рисунку выпишем очевидные соотношения:

$$X_1 + X_2 = 10 \quad (1)$$

$$Y_1 + Y_2 = X_1 + 3 \quad (2)$$

$$8 + Y_4 = X_2 + 5 \quad (3)$$

$$Y_5 + Y_6 = 12 \quad (4)$$

Необходимо найти: $\Sigma_1 = Y_1 + 8 + Y_5$, $\Sigma_2 = Y_4$, $\Sigma_3 = Y_2 + Y_6$.

Далее, заметим, что транзакции №1 и №8 осуществлены одним и тем же владельцем – владельцем 1. То есть использовался один и тот же секретный ключ S_1 , при этом использовалось одно и то же значение k в подписи, поэтому:

$$9 = (18X_1 + S_1k)(\text{mod } 28),$$

$$1 = (18Y_2 + S_1k)(\text{mod } 28). \quad \text{Отсюда получим } 8 = 36 = (18(X_1 - Y_2))(\text{mod } 28).$$

Следовательно, $X_1 - Y_2 = 2$. С учетом (2) имеем: $Y_1 = X_1 - Y_2 + 3 = 5$.

Аналогичное свойство замечаем у транзакций №5 и №12:

$$18 = (27 \cdot 3 + S_3k)(\text{mod } 28),$$

$$20 = (27Y_6 + S_3k)(\text{mod } 28). \quad \text{Отсюда получим } -2 = 54 = (27(3 - Y_6))(\text{mod } 28).$$

Следовательно, $3 - Y_6 = 2$, $Y_6 = 1$.

С учетом (4) имеем: $Y_5 = 11$ и уже находится $\Sigma_1 = 5 + 8 + 11 = 24$.

Теперь обратим внимание на транзакции №9 и №10, осуществленные владельцем 2, для которых, как нетрудно заметить, использовались одинаковые k , но с разными знаками, т.к. $(2 \cdot 15) = 1(\text{mod } 29)$.

Поэтому:

$$11 = (2 \cdot 8 + S_2k)(\text{mod } 28),$$

$$20 = (15Y_4 - S_2k)(\text{mod } 28).$$

Отсюда получим: $15Y_4 = 31 - 16 = 15(\text{mod } 28)$, $Y_4 = 1 = \Sigma_2$.

Т.к. исходная сумма криптокойнов была равна 30, то $\Sigma_3 = 30 - \Sigma_1 - \Sigma_2 = 5$

ОТВЕТ: (24,1,5).

Задача 3

а) Так как $\text{НОД}(2,7)=\text{НОД}(6,7)=1$, то $g(x) = 2f(x)(\text{mod } 7)$ и $h(x) = 6f(x)(\text{mod } 7)$ являются перестановками. Но тогда, например, $g(x) = 2f(x)$, $h(x) = 6f(x)$ и выполняется $g(x) + h(x) = 2f(x) + 6f(x) = f(x)(\text{mod } 7)$.

$$\text{б) } \sum_{i=0}^{2n-1} f(x) = \sum_{i=0}^{2n-1} x = (2n+1)n = n(\text{mod } (2n)).$$

С другой стороны, если указанное условие пункта б) представление существует, то

$$\sum_{i=0}^{2n-1} f(x) = \sum_{i=0}^{2n-1} g(x) + \sum_{i=0}^{2n-1} h(x) = 2(2n+1)n = 0(\text{mod } (2n)).$$

Что доказывает невозможность указанного представления.

Задача 4

а) из условия задачи и равенства $a^{p-1} = 1(\text{mod } p)$ следует $a^{k(p-1)+1} = a(\text{mod } p)$ для любого натурального k . Тогда при $k = \frac{q-1}{2}$ получим $a^{\frac{\varphi(N)}{2}+1} = a(\text{mod } p)$.

Аналогично $a^{\frac{\varphi(N)}{2}+1} = a(\text{mod } q)$. Так как p, q – простые числа, то из этих полученных выше равенств следует $a^{\frac{\varphi(N)}{2}+1} = a(\text{mod } N)$. Пункт а) доказан.

д) предположим, что $\frac{\varphi(N)}{2} + 1 = 21240913$. Тогда получим систему уравнений $p \cdot q = 42494861$, $(p-1) \cdot (q-1) = 21240913$.

Решая полученную систему, находим $p = 6547, q = 7057$

ОТВЕТ: $p = 6547, q = 7057$.

XXXIII Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии
Задача 5

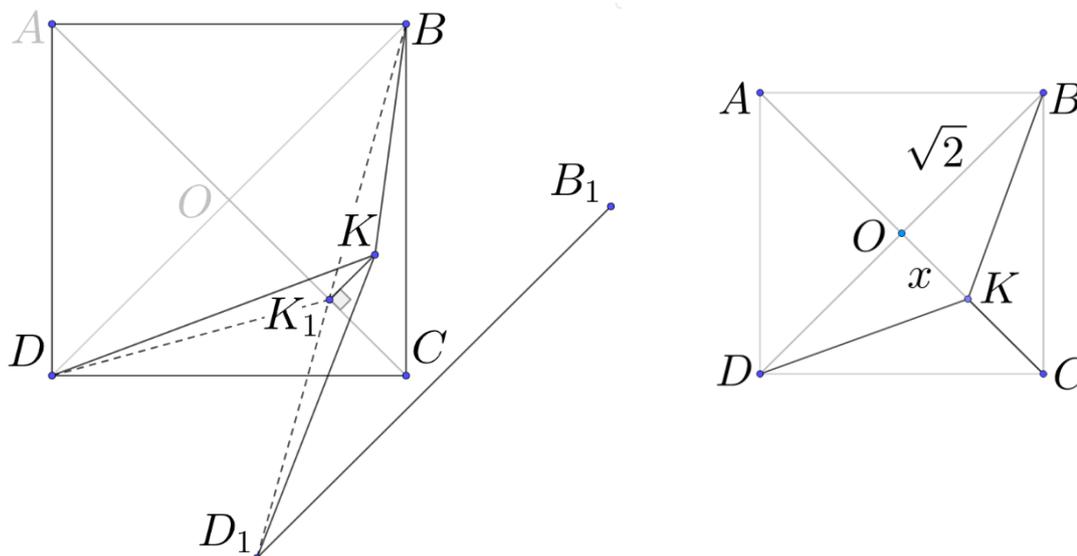
Заметим, что точки A_1 и O_1 совпадают. Действительно, пусть минимум достигается на конфигурации, где это не так. Но тогда, сдвинув точку A_1 в точку O_1 , мы длину проводов уменьшим. Таким образом, компьютер A_1 и сервер O_1 должны оказаться в некоторой точке K ($K = A_1 = O_1$).

Покажем, что K лежит на диагонали AC . Предположим обратное. Пусть K_1 – основание перпендикуляра, опущенного из точки K на прямую AC . Покажем, что сумма расстояний от точки K_1 до вершин B, C, D , которую обозначим $S_{K_1} = K_1B + K_1C + K_1D$, меньше аналогичной суммы $S_K = KB + KC + KD$. Длина проекции меньше длины наклонной, поэтому $K_1C < KC$. Чтобы доказать, что

$$K_1D + K_1B < KD + KB, \quad (1)$$

отразим отрезок BD относительно прямой KK_1 (при этом точка B перейдет в точку B_1 , точка D – в точку D_1). Точки B, K_1, D_1 окажутся на одной прямой. Тогда $K_1D + K_1B = K_1D_1 + K_1B = D_1B$, и при этом $KD + KB = KD_1 + KB > D_1B$. Неравенство (1) доказано. Следовательно, $S_{K_1} < S_K$, а значит искомая точка K должна лежать на диагонали.

Пусть $OK = x$. Тогда $S(x) = KC + KB + KD = 2\sqrt{x^2 + 2} + \sqrt{2} - x$. На отрезке $[0, \sqrt{2}]$



функция $S(x)$ имеет (единственный) минимум в точке $x_0 = \sqrt{2/3}$ (x_0 – корень уравнения $S'(x) = 2x/\sqrt{x^2 + 2} - 1 = 0$), и $S(x_0) = 2\sqrt{2/3 + 2} + \sqrt{2} - \sqrt{2/3} = \sqrt{6} + \sqrt{2}$.

ОТВЕТ: $\sqrt{6} + \sqrt{2}$.

Задача 6

Задачу можно решить древовидным перебором всех вариантов. Существование подобных мозаик для других простых чисел является открытой проблемой. Гипотеза утверждает, что такие мозаики существуют только для простых чисел Ферма: 3, 5, 17, 257.

ОТВЕТ: 2, 8, 9, 15.

ОТБОРОЧНЫЙ ЭТАП

9 КЛАСС

1. Найдите шестизначное число $A = \overline{a_1 a_2 \dots a_6}$, $a_i \in \{1, 2, \dots, 9\}$ такие, что $8A + a_6 = B$, где $B = \overline{b_1 b_2 \dots b_6}$, $b_i = 10 - a_i$. В ответе запишите это число, например, 987654.
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 Е. В ответе запишите число без единиц измерения, при необходимости дробное число запишите через точку, например, 12 или 13.5.
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)?
4. На уроке Истории математики Лена узнала необычный факт и придумала как с помощью него можно шифровать сообщение. Российский шахматный мастер и теоретик Карл Яниш нашёл замкнутый маршрут обхода всех клеток шахматной доски ходом коня ровно по одному разу. Прочтите текст, вписанный Леной в клетки шахматной доски по такому маршруту, если начало текста в g3.

8	о	о	л	а	з	а	т	з
7	а	я	с	м	с	я	г	к
6	т	в	э	р	м	о	н	а
5	с	н	ч	п	с	н	о	у
4	е	н	т	т	е	ы	н	о
3	е	н	у	т	р	т	м	м
2	ч	ш	о	м	л	т	в	н
1	з	а	а	ч	н	н	н	а
	а	б	с	д	е	ф	г	h

В ответе запишите полученный текст слитно (без пробелов и знаков препинания), с маленькой буквы. Например, это пример полученного текста

5. Юный криптограф изучает свойства паролей в учебном варианте парольного словаря. В нем 60 паролей содержат букву "Ф", 40 - букву "С", 100 - букву "Б". Буквы "Б" и "С" вместе содержатся в 20 паролях. Буквы "Б" и "Ф" вместе содержатся в 30 паролях. Ни один пароль не содержит вместе букв "Ф" и "С". Сколько паролей содержат хотя бы одну из этих трех букв?
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

XXXIII Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии 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? Ответ напишите в виде целого числа. Например, 12345678.

*	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

10 КЛАСС

7. Найдите шестизначное число $A = \overline{a_1 a_2 \dots a_6}$, $a_i \in \{1, 2, \dots, 9\}$ такие, что $8A + a_6 = B$, где $B = \overline{b_1 b_2 \dots b_6}$, $b_i = 10 - a_i$. В ответе запишите это число, например, 987654.
8. 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 расстояние до неё меньше, чем до любой другой вышки. Найдите площадь зоны действия вышки E. В ответе запишите число без единиц измерения, при необходимости дробное число запишите через точку, например, 12 или 13.5.
9. 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)?
10. На уроке Истории математики Лена узнала необычный факт и придумала как с помощью него можно шифровать сообщение. Российский шахматный мастер и теоретик Карл Яниш нашёл замкнутый маршрут обхода всех клеток шахматной доски ходом коня ровно по одному разу. Прочтите текст, вписанный Леной в клетки шахматной доски по такому маршруту, если начало текста в g3.

8	о	о	л	а	з	а	т	з
7	а	я	с	м	с	я	г	к
6	т	в	э	р	м	о	н	а
5	с	н	ч	п	с	н	о	у
4	е	н	т	т	е	ы	н	о
3	е	н	у	т	р	т	м	м
2	ч	ш	о	м	л	т	в	н
1	з	а	а	ч	н	н	н	а
	а	б	с	д	е	ф	г	h

В ответе запишите полученный текст слитно (без пробелов и знаков препинания), с маленькой буквы. Например, это пример полученного текста

11. Юный криптограф изучает свойства паролей в учебном варианте парольного словаря. В нем 60 паролей содержат букву "Ф", 40 - букву "С", 100 - букву "Б". Буквы "Б" и "С" вместе содержатся в 20 паролях. Буквы "Б" и "Ф" вместе содержатся в 30 паролях. Ни один пароль не содержит вместе букв "Ф" и "С". Сколько паролей содержат хотя бы одну из этих трех букв?

12. 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? Ответ напишите в виде целого числа. Например, 12345678.

*	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

11 КЛАСС

1. Найдите восьмизначное число $A = \overline{a_1 a_2 \dots a_8}$, $a_i \in \{1, 2, \dots, 9\}$ такие, что $8A + a_8 = B$, где $B = \overline{b_1 b_2 \dots b_8}$, $b_i = 10 - a_i$. В ответе запишите это число, например, 98765432.

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

XXXIII Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии
вышки Е. В ответе запишите число без единиц измерения, при необходимости дробное число
запишите через точку, например, 12 или 13.5.

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 Tw38dttf (не совпадающих с
установленным паролем)?

4. На уроке Истории математики Лена узнала необычный факт и придумала как с помощью
него можно шифровать сообщение. Российский шахматный мастер и теоретик Карл Яниш
нашёл замкнутый маршрут обхода всех клеток шахматной доски ходом коня ровно по одному
разу. Прочтите текст, вписанный Леной в клетки шахматной доски по такому маршруту, если
начало текста в g3.

8	р	л	с	о	и	р	о	я
7	р	я	ы	а	к	и	п	о
6	л	к	т	т	в	м	п	й
5	а	о	а	л	н	с	д	о
4	а	и	т	л	к	и	я	т
3	с	н	с	б	ь	е	к	г
2	м	н	и	л	л	о	е	х
1	ч	и	ы	я	п	б	а	д
	а	б	с	д	е	ф	г	h

В ответе запишите полученный текст слитно (без пробелов и знаков препинания), с маленькой
буквы. Например, это пример полученного текста

5. Юный криптограф изучает свойства паролей в учебном варианте парольного словаря. В
нем 100 паролей содержат букву "А", 120 - букву "Ф", 140 - букву "С" и 160 букву "Б". Буквы
"А" и "Ф" вместе содержатся в 50 паролях, буквы "А" и "С" вместе содержатся в 70 паролях,
буквы "А" и "Б" вместе содержатся в 60 паролях, буквы "Ф" и "С" вместе содержатся в 70
паролях, буквы "Ф" и "Б" вместе содержатся в 80 паролях, а буквы "С" и "Б" вместе содержатся
в 50 паролях. Буквы "А", "Ф" и "С" вместе содержатся в 30 паролях, буквы "А", "Ф" и "Б"
вместе содержатся в 40 паролях, буквы "А", "С" и "Б" вместе содержатся в 40 паролях, а буквы
"Ф", "С" и "Б" вместе содержатся в 30 паролях. Буквы "А", "Ф", "С" и "Б" вместе содержатся в
20 паролях. Сколько паролей содержат хотя бы одну из этих четырех букв?

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? Ответ напишите в виде целого числа. Например, 12345678.

*	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

ОТВЕТЫ

9 КЛАСС

- 1) 123456.
- 2) 32.5.
- 3) 452.
- 4) материал становится знакомым и лучше воспринимается, это значит, что мозгу.
- 5) 150.
- 6) 7^6 .

10 КЛАСС

- 1) 123456.
- 2) 32.5.
- 3) 452.
- 4) материал становится знакомым и лучше воспринимается, это значит, что мозгу.
- 5) 150.
- 6) 7^6 .

11 КЛАСС

- 1) 12345678.
- 2) 24.
- 3) 452.
- 4) кандидатской степени продвигался на крыльях блистая отличными баллами.
- 5) 260.
- 6) 7^6 .