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

11 КЛАСС

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 $1 \le t \le k-1$ 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.

Решение. 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:

$$a_{i_1} \le a_{i_2} \le \dots \le a_{i_{k-1}}.$$

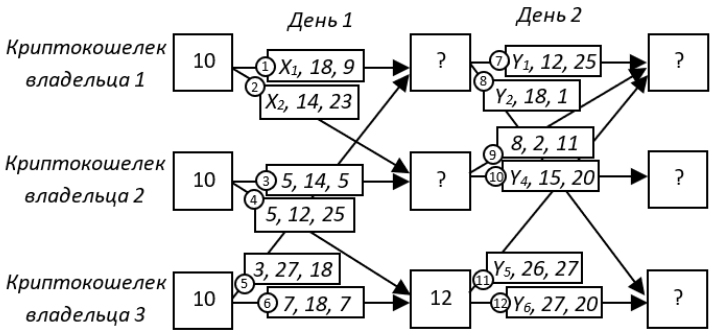
Здесь в индексах указаны номера позиций, на которых стоят эти числа в таблице. Образуем два множества позиций, которые заполнены: $\{i_1, i_3, \dots\}$ и $\{i_2, i_4, \dots\}$, беря указанные числа через одно. Тогда суммы чисел на этих позициях могут отличаться друг от друга не более, чем на 2023. Поэтому 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.

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?



Решение. Сначала по рисунку выпишем очевидные соотношения:

$$X_1 + X_2 = 10 \qquad (1)$$
$$Y_1 + Y_2 = X_1 + 3 \qquad (2)$$
$$8 + Y_4 = X_2 + 5 \qquad (3)$$
$$Y_5 + Y_6 = 12 \qquad (4)$$

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:

$$9 = (18X_1 + S_1k)(mod\ 28),$$
$$1 = (18Y_2 + S_1k)(mod\ 28).$$

Отсюда получим $8 = 36 = (18(X_1 - Y_2))(mod\ 28)$. 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:

$$18 = (27 \cdot 3 + S_3k)(mod\ 28),$$
$$20 = (27Y_6 + S_3k)(mod\ 28).$$

Отсюда получим $-2 = 54 = (27(3 - Y_6))(mod\ 28)$.
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. $(2 \cdot 15) = 1(mod\ 29)$.
Поэтому:

$$11 = (2 \cdot 8 + S_2k)(mod\ 28),$$
$$20 = (15Y_4 - S_2k)(mod\ 28).$$

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

Т.к. исходная сумма криптокойнов была равна 30, то $\Sigma_3 = 30 - \Sigma_1 - \Sigma_2 = 5$.
Ответ: (24,1,5).

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

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

Например, $f(2) = 4$. Найдите две перестановки g и h такие, что для всех $x \in \{0,1,\dots,6\}$ выполняется $f(x) = \big(g(x) + h(x)\big)(mod\ 7)$.

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

x	0	1	2	…	$2n$	$2n$
$f(x)$	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 $f(x) = \big(g(x) + h(x)\big)(mod\ (2n))$.

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

$$g(x) + h(x) = 2f(x) + 6f(x) = f(x)(mod\ 7)$$

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

С другой стороны, если указанное условии пункта b) представление существует, то

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

Что доказывает невозможность указанного представления.

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 $a^{p-1} = 1(mod\ p)$. Используя это:

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

b) найдите p и q, если известно, что $N = 42494861$ и $x^{21240913} = x(mod\ N)$ для всех $x \in \{1,2,\dots,N-1\}$..

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

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

b) предположим, что $\frac{\varphi(N)}{2} + 1 = 21240913$. Тогда получим систему уравнений

$$p \cdot q = 42494861, \qquad (p-1) \cdot (q-1) = 21240913.$$

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

Ответ: $p = 6547, q = 7057$.

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?

Решение.

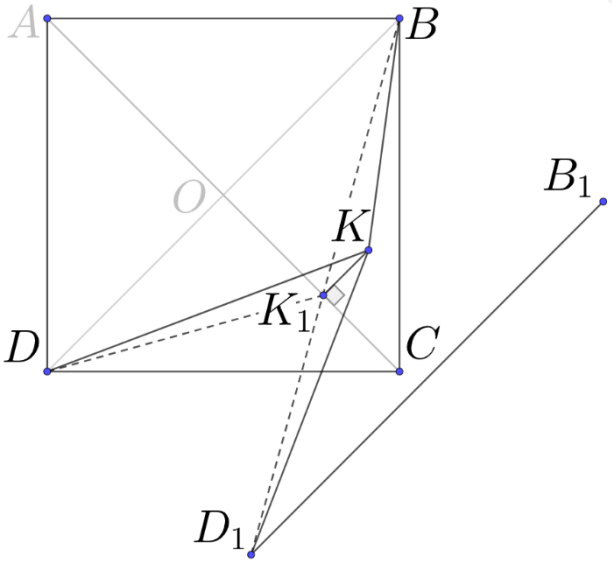
Заметим, что точки A_1 и O_1 совпадают. Действительно, пусть минимум достигается на конфигурации, где это не так. Но тогда, сдвинув точку A_1 в точку O_1, мы длину проводов уменьшим. Таким образом, компьютер A_1 и сервер O_1 должны оказаться в некоторой точке K ($K = A_1 = O_1$).

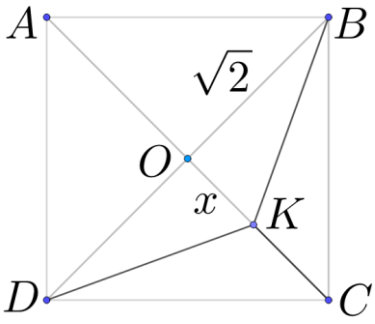
Покажем, что K лежит на диагонали AC. Предположим обратное. Пусть K_1 – основание перпендикуляра, опущенного из точки K на прямую AC. Покажем, что сумма расстояний от точки K_1 до вершин B, C, D, которую обозначим $S_{K_1} = K_1B + K_1C + K_1D$, меньше аналогичной суммы $S_K = KB + KC + KD$. Длина проекции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

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

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: $\sqrt{6} + \sqrt{2}$.

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 $b_1, b_2, b_3, b_4 \in \{0, 1, \ldots, 16\}$. Затем первую строку Вася заполняет числами $a_i^{(1)} = (b_i + 1)(mod\ 17), i = 1,2,3,4$, вторую строку – числами $a_i^{(2)} = (b_i + 4)(mod\ 17), i = 1,2,3,4$, третью $a_i^{(3)} = (b_i + 13)(mod\ 17), i = 1,2,3,4$ и, аналогично, четвертую $a_i^{(4)} = (b_i + 16)(mod\ 17), i = 1,2,3,4$. При этом числа b_1, b_2, b_3, b_4 Вася выбрать должен так, чтобы все числа в таблице оказались различными. Сумеет ли Вася это сделать? Если да, то чему равны b_1, b_2, b_3, b_4?

Решение. 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.