ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

10 КЛАСС

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

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 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

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

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

Что доказывает невозможность указанного представления.

Задача 4

a) 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.

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

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

ОТВЕТ: $p = 6949, q = 6449$.

Задача 5

Сначала по рисунку выпишем очевидные соотношения:

$X_1 + X_2 = 9$ (1)

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

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

$Y_5 + Y_6 = 8$ (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:
$11 = (15X_1 + S_1k)(mod\,28)$,
$9 = (15Y_2 + S_1k)(mod\,28)$.
Отсюда получим: $2 = 30 = (15(X_1 - Y_2))(mod\,28)$.
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:
$25 = (27 \cdot 4 + S_3k)(mod\,28)$,
$24 = (27Y_5 + S_3k)(mod\,28)$.
Отсюда получим: $1 = -27 = (27(4 - Y_5))(mod\,28)$. Следовательно, $Y_5 = 5$ и уже находится $\Sigma_1 = 7 + 5 + 5 = 17$.

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