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

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

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: $(a_1 \quad ,\dots, \quad a_k)$, которые игроки заполняют числами от 0 до 6. Первым ходит Юра, который выбирает число t такое, что $1 \le t \le 99$ 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. a) перестановка f чисел $\{0,1,\dots,6\}$ задана таблицей:

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

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

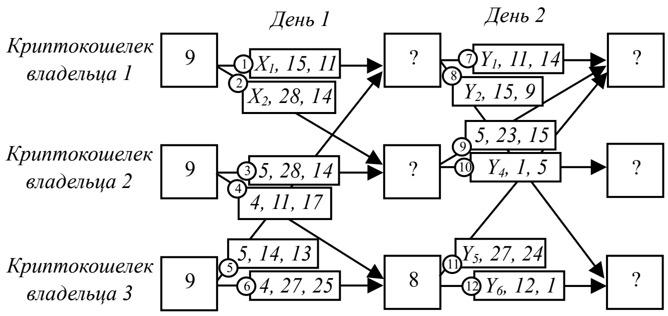
Здесь $(i_0, i_1, \dots, i_{2n-1})$ – перестановка чисел $\{0,1,\dots,2n-1\}$.
Докажите, что не существует перестановок g и h таких, что для всех $x \in \{0,1,\dots,2n-1\}$ выполняется $f(x) = \big(g(x) + h(x)\big)(mod\ (2n))$.

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

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

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

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 $S \in \{1,2,\ldots,28\}$. 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 $k \in \{1,2,\ldots,28\}$, 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 $b_1, b_2, b_3, b_4 \in \{0, 1, \ldots, 16\}$. 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 и не было числа 8. Сумеет ли Вася это сделать? Если да, то чему равны b_1, b_2, b_3, b_4