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

10 КЛАСС

1. Найдите пять простых чисел, образующих арифметическую прогрессию с разностью 12. Ответ обоснуйте.

Ответ: 5,17,29,41,53.

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 $1 \le t \le 99$ 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.

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 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.

3. а) 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	…	$2n$	$2n$
$f(x)$	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. а) 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:

а) 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 $N=44814101$ и $x^{22400353}=x(mod\ N)$ 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 $\frac{\varphi(N)}{2} + 1 = 22400353$. Тогда получим систему уравнений

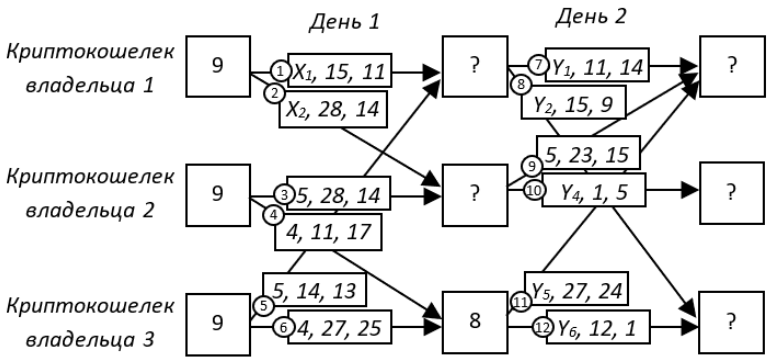
$p \cdot q = 44814101, \quad (p-1) \cdot (q-1) = 44800704.$

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

Ответ: $p = 6949, q = 6449$.

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?



Решение.

Сначала по рисунку выпишем очевидные соотношения:

$$X_1 + X_2 = 9 \qquad (1)$$
$$Y_1 + Y_2 = X_1 + 5 \qquad (2)$$
$$5 + Y_4 = X_2 + 5 \qquad (3)$$
$$Y_5 + Y_6 = 8 \qquad (4)$$

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).

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 $a_i^{(1)} = (b_i + 1)(mod\ 17), i = 1,2,3,4$, 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?

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: 0,6,10,16.