

Китайская теорема об остатках

1. **Китайская теорема об остатках.** Пусть имеется два набора чисел a_1, a_2, \dots, a_n и m_1, m_2, \dots, m_n , причем числа во втором наборе попарно взаимно просты. Тогда система сравнений

$$\begin{cases} x \equiv a_1 \pmod{m_1}; \\ x \equiv a_2 \pmod{m_2}; \\ \dots \\ x \equiv a_n \pmod{m_n}; \end{cases}$$

имеет единственное решение по модулю $m_1 \cdot m_2 \cdot \dots \cdot m_n$.

Подсказка для комбинаторного доказательства. Сколько существует различных остатков по модулю m_1 ? А сколько существует пар остатков таких, что первый из них $\pmod{m_1}$, а второй $\pmod{m_2}$? А сколько существует различных наборов остатков таких, что первый из них $\pmod{m_1}$, второй $\pmod{m_2}$, \dots , n -й — $\pmod{m_n}$?

Подсказка для конструктивного доказательства. Попробуйте придумать решение для системы, в которой один остаток a_i равен 1, а все остальные $a_j, j \neq i$, равны 0. При помощи таких решений (для разных i) выписывается решение для произвольной системы.

2. При каких целых n число $a_n = n^2 + 3n + 1$ делится на 55?
3. При каких целых x выполняется данная система сравнений?

$$\begin{cases} x \equiv 3 \pmod{5}; \\ x \equiv 7 \pmod{17}. \end{cases}$$

4. (а) Трехзначное число 625 обладает своеобразным свойством самовоспроизводимости, как то: $625^2 = 390625$. Сколько четырехзначных чисел удовлетворяют уравнению $x^2 \equiv x \pmod{10000}$?
(б) Докажите, что при любом k существует ровно 4 набора из k цифр — $00 \dots 00$, $00 \dots 01$ и еще два, оканчивающиеся пятеркой и шестеркой, — обладающие таким свойством: если натуральное число оканчивается одним из этих наборов цифр, то его квадрат оканчивается тем же набором цифр.
5. **Большое войско.** Генерал хочет построить для парада своих солдат в одинаковые квадратные каре, но он не знает, сколько солдат (от 1 до 37) находится в лазарете. Докажите, что у генерала может быть такое количество солдат, что он, независимо от заполнения лазарета, сумеет выполнить свое намерение. Например, войско из 9 человек можно поставить в виде квадрата 3×3 , а если один человек болен, то в виде двух квадратов 2×2 . (Каре 1×1 , естественно, не допускается.)