

7 июля

## Китайская теорема об остатках

**Формулировка КТО.** Пусть натуральные числа  $a_1, \dots, a_k$  попарно взаимно просты. Тогда для любого набора целых чисел  $r_1, \dots, r_k$  существует единственное число  $x$  по модулю  $a_1 \cdot a_2 \cdot \dots \cdot a_k$ , удовлетворяющее системе:

$$\begin{cases} x \equiv r_1 \pmod{a_1} \\ x \equiv r_2 \pmod{a_2} \\ \dots \\ x \equiv r_k \pmod{a_k} \end{cases}$$

1. а) Пусть  $a$  и  $b$  взаимно просты. Докажите, что  $\{0, a, 2 \cdot a, \dots, (b-1) \cdot a\}$  - полная система вычетов по модулю  $b$ .

б) Существует ли решение системы:

$$\begin{cases} x \equiv r_1 \pmod{a_1} \\ x \equiv r_2 \pmod{a_2} \end{cases}$$

в) Докажите КТО по индукции.

### 2. Другое доказательство КТО.

а) Докажите, что у каждого остатка  $r$  по модулю  $a$  такого, что  $(a, r) = 1$ , существует обратный.

*Указание:* остатки  $r_1$  и  $r_2$  обратные по модулю  $a$ , если  $r_1 \cdot r_2 \equiv 1 \pmod{a}$

б) Найдите решение системы:

$$\begin{cases} x \equiv r_1 \pmod{a_1} \\ x \equiv 0 \pmod{a_2} \\ \dots \\ x \equiv 0 \pmod{a_k} \end{cases}$$

в) Найдите явное решение для КТО.

### 3. Решите систему сравнений:

а)  $a \equiv 2 \pmod{5}$  и  $a \equiv 4 \pmod{6}$ ;

б)  $a \equiv 2 \pmod{5}$ ,  $a \equiv 4 \pmod{6}$  и  $a \equiv 3 \pmod{7}$ ;

4. Из натуральных чисел, меньших 1000000, Маша выписала все, дающие остаток 17 при делении на 23 и остаток 5 при делении на 11. Саша из натуральных чисел, меньших 1000000, выписала все, дающие остаток 11 при делении на 21 и остаток 3 при делении на 13.

а) У кого чисел больше?

б) Повторяются ли числа в списках Маши и Саши?

5. Найдите остаток от деления **(а)**  $19^{14}$  на 70; **(б)**  $17^9$  на 48; **(с)**  $14^{14^{14}}$  на 100.

6. При каких целых  $n$  число  $n^2 + 3n + 1$  делится на 55?

7. Докажите, что для любого  $n$  найдутся  $n$  подряд идущих натуральных чисел, делителем каждого из которых является точный куб, больший 1.

8. Докажите, что можно переставить все числа натурального ряда так, чтобы сумма первых  $n$  чисел делилась на  $n$ .