

Сравнение по модулю

Определение. Целое число a делится на число b с остатком r ($r < b$), если существует целое число c такое, что $a = b \cdot c + r$.

Обозначение. Если a и b имеют одинаковые остатки при делении на n , то говорят, что они сравнимы по модулю

$$a \equiv b \pmod{n}$$

Разминка. Докажите, что

- (a) $a \equiv b \pmod{n}$ тогда и только тогда, когда $a - b : n$
- (b) Если $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$, то $a + c \equiv b + d \pmod{n}$
- (c) Если $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$, то $a \cdot c \equiv b \cdot d \pmod{n}$
- (d) Если $a \equiv b \pmod{n}$, то $a^k \equiv b^k \pmod{n}$

1. Найдите остаток

- (a) 11^7 при делении на 8
- (b) 9^{512} при делении на 239
- (c) 13^{2024} при делении на 7

2. Найдите всевозможные a и n при которых $a \equiv a + 1 \pmod{n}$

- 3. (a) Докажите, что если $a \equiv b \pmod{n}$, то $a \cdot m \equiv b \cdot m \pmod{n \cdot m}$
- (b) Докажите, что если $a \cdot m \equiv b \cdot m \pmod{n \cdot m}$, то $a \equiv b \pmod{n}$

4. Пусть m и n взаимно просты ($\text{НОД}(m, n) = 1$).

- (a) Докажите, что если $a \equiv b \pmod{n}$, то $a \cdot m \equiv b \cdot m \pmod{n}$
- (b) Докажите, что если $a \cdot m \equiv b \cdot m \pmod{n}$, то $a \equiv b \pmod{n}$

Определение. Будем говорить, что числа a_1, a_2, \dots, a_n образуют полную систему остатков по модулю n , если никакие два числа не сравнимы по модулю n . Чаще всего в качестве полной системы остатков выбирается множество $\{0, 1, 2, \dots, n - 1\}$ или множество $\{1, 2, \dots, n\}$.

5. Докажите, что числа a_1, a_2, \dots, a_n образуют полную систему остатков по модулю n . тогда и только тогда, когда для любого натурального числа k найдётся ровно одно число a_i такое, что $k \equiv a_i \pmod{n}$

6. (a) Придумайте полную систему остатков по модулю 9 состоящую из трёх-значных чисел палиндромов.

(b) Является ли 1, 2, 4, 8, 16, 32, 64 полной системой остатков по модулю 7?

(c) Докажите, что $3, 6, \dots, 3n$ образует полную систему остатков по модулю n тогда и только тогда когда n не делится на 3.

(d) Пусть n взаимно просто с a ($\text{НОД}(n, a) = 1$). Докажите, что $a, 2a, 3a, \dots, na$ образует полную систему остатков по модулю n .

7. Докажите, что среди чисел, записываемых одними единицами, есть число, которое делится на 533239, причём для записи этого числа понадобится не более 533240 единиц.

8. Вася посчитал сумму нескольких целых чисел, а Петя посчитал сумму их кубов. Мог ли результат Пети быть на 72704 больше?

9. Докажите, что ни при каком натуральном n число $3^n + 5^n$ не является полным квадратом.

10. Найдите наименьшее число, дающее следующие остатки: 1 - при делении на 3, 2 - при делении на 5, 3 - при делении на 7.

11. Последовательность a_1, a_2, \dots, a_n определена следующим образом $a_1 = 2$, а число a_i равно наибольшему простому делителю числа $a_1 \cdot a_2 \cdot \dots \cdot a_{i-1} + 1$. Докажите, что эта последовательность не содержит числа 5.