

18. Работа с системами вычетов

12 июля

Определение. Множество всех вычетов по модулю n называют *полной системой вычетов* по модулю n .

Определение. Обозначим через $\varphi(n)$ количество чисел, не больших n , взаимно простых с n . Говорят, что набор из $\varphi(n)$ различных вычетов, взаимно простых с n (если выбрать из каждого класса вычетов по представителю), образует *приведенную систему вычетов* по модулю n .

Упражнение. Пусть a — произвольное целое число. Тогда при сдвиге полной системы вычетов на a мы снова получим полную систему вычетов.

Упражнение. Пусть $(a, n) = 1$. Тогда при домножении полной/приведенной системы вычетов на a мы снова получим полную/приведенную систему вычетов.

Следствие. Пусть $(a, n) = 1$. Докажите, что существует *обратный* к a вычет по модулю n , то есть такой вычет b , что $a \cdot b \equiv 1 \pmod{n}$.

Следствие. Пусть $(a, n) = 1$. Докажите, что $a^{\varphi(n)} \equiv 1 \pmod{n}$.

1. Дано простое число $p > 100$. Докажите, что существуют различные целые неотрицательные числа a, b, c, d, e , каждое из которых меньше p , и такие, что $a + 2b + 3c + 4d + 5e$ делится на p .

Подсказка. Зафиксируйте произвольные различные a, b, c, d, e и попробуйте сдвигать их на одно и то же число по модулю p .

2. Пусть n — нечетное натуральное число. Докажите, что наборов из k различных натуральных чисел, меньших n , сумма чисел в котором дает остаток 1 по модулю n столько же, сколько наборов из k различных натуральных чисел, меньших n , сумма которых дает остаток 2 по модулю n .

3. Пусть p — простое число. Сколькими способами можно выбрать несколько натуральных чисел из набора $\{1, 2, 3, \dots, p-1, p\}$ так, чтобы их сумма делилась на p ?

4. Дано нечётное простое число p . Для каждого натурального $k \leq p-1$ обозначим через a_k количество натуральных делителей числа $kp+1$, больших k и меньших p . Найдите $a_1 + a_2 + \dots + a_{p-1}$.

5. Дано простое p и p натуральных чисел a_1, \dots, a_p . Докажите, что при некотором целом k

(а) среди чисел $a_1 + k, a_2 + 2k, \dots, a_p + pk$ есть не более $\frac{p-1}{2}$ пар, дающих одинаковые остатки при делении на p ;

(б) числа $a_1 + k, a_2 + 2k, \dots, a_p + pk$ дают не менее $p/2$ разных остатков при делении на p .

6. Дано простое число $p > 2$. Докажите, что среди любых $p+1$ целых чисел можно выбрать $p-1$ число a_1, a_2, \dots, a_{p-1} так, чтобы $a_1 + 2a_2 + 3a_3 + \dots + (p-1)a_{p-1}$ делилось на p .

7. Для каких натуральных n существует такая перестановка p_1, p_2, \dots, p_n чисел $1, 2, \dots, n$, что в каждом из наборов чисел $p_1 + 1, p_2 + 2, \dots, p_n + n$ и $p_1 - 1, p_2 - 2, \dots, p_n - n$ все числа дают разные остатки при делении на n ?

8. Дано нечётное простое число p . Последовательность целых неотрицательных чисел a_1, a_2, \dots, a_p , каждое из которых меньше p , назовём *прекрасной*, если

(1) $a_1 + a_2 + \dots + a_p$ не делится на p ;

(2) $a_1a_2 + a_2a_3 + \dots + a_{p-1}a_p + a_pa_1$ делится на p .

Найдите количество прекрасных последовательностей.

9. Дано нечётное натуральное число n . На доске выписаны в порядке возрастания все остатки, которые могут давать степени 2 при делении на n . (Например, при $n = 9$ на доске были бы написаны числа 1, 2, 4, 5, 7, 8.) Всегда ли по этим числам можно определить n ?

10. Дано простое число $p \geq 5$. Для каждой перестановки (x_1, x_2, \dots, x_p) чисел $1, 2, \dots, p$, в которой $x_i \neq i$ для каждого $i \leq p$, посчитали остаток от деления числа $x_1 + 2x_2 + \dots + px_p$ на p . Докажите, что перестановок, у которых этот остаток равен 1, столько же, сколько перестановок, у которых он равен 4.