

Системы вычетов и обратные остатки.

Определение. Остаток b называется обратным остатку a по модулю m , если $ab \equiv 1 \pmod{m}$. Можно обозначать $b \equiv a^{-1} \pmod{m}$.

В случае если $(a; m) = 1$, то у остатка a существует обратный по модулю m . Если $(a; m) \neq 1$, то обратного остатка a по модулю m нет.

Определение. Будем говорить, что несократимая дробь $\frac{a}{b}$ имеет остаток x при делении на простое число p , если $a \equiv bx \pmod{p}$.

Свойства дробных остатков.

(а) $\frac{a}{b} \cdot \frac{c}{d} \equiv \frac{ac}{bd} \pmod{p}$;

(б) $\frac{a}{b} + \frac{c}{d} \equiv \frac{ad+bc}{bd} \pmod{p}$.

0.1. Предположим, что $p > 3$. Преобразуем сумму

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{(p-1)^2}$$

в несократимую дробь $\frac{m}{n}$. Докажите, что m делится на p .

0.2. Вася выписывает в ряд 400 натуральных чисел. Первое число он пишет любое, а каждое следующее — либо в 9 раз больше предыдущего, либо в 2 раза меньше предыдущего (при условии, что получается целое число). Может ли сумма всех его чисел оказаться равной 24^{2000} ?

1. Докажите, что у числа $100! + 52$ есть натуральный делитель, больший 100, но меньший 110.
2. На доске написаны числа $\frac{100}{1}, \frac{99}{2}, \dots, \frac{1}{100}$. Можно ли выбрать какие-то 29 из них, произведение которых равно 1?
3. Даны натуральные числа a, b, c такие, что $ab + 9b + 81$ и $bc + 9c + 81$ делятся на p для простого $p > 3$. Докажите, что $ca + 9a + 81$ тоже делится на p .
4. Дано простое число p . Для каждого натурального $x \in \{1, 2, \dots, p-1\}$ рассмотрим выражение $x^2 + 3x + 1$. Оказалось, что ровно 1 из них делится на p . Найдите все возможные значения p .
5. Пусть $p = 4k + 3$ — простое число, а $\frac{m}{n}$ — такая несократимая дробь, что

$$\frac{1}{0^2 + 1} + \frac{1}{1^2 + 1} + \dots + \frac{1}{(p-1)^2 + 1} = \frac{m}{n}$$

Докажите, что $2m - n$ делится на p .

6. Докажите, что для каждого простого p числа от 1 до $p-1$ можно выписать в ряд $a_1, a_2, \dots, a_{p-1}$ так, что все произведения $a_1 a_2 \dots a_k$ различны по модулю p .

7. Пусть p — простое число, большее 2. Докажите, что существует такая перестановка $(x_1, x_2, \dots, x_{p-1})$ чисел $(1, 2, \dots, p-1)$, что

$$x_1x_2 + x_2x_3 + \dots + x_{p-2}x_{p-1} \equiv 2 \pmod{p}$$