

Обратные остатки

Общая интуиция.

В этом листочке речь идет о **простом модуле p** !

Вы умеете складывать, вычитать и умножать остатки на друг друга, получая другие остатки. Единственное, чего не хватает для схожести с "обычными" числами — это умение делить любой остаток на любой ненулевой.

Оказывается, можно и дробям довольно естественным образом сопоставить остатки! Причем при любых арифметических действиях с дробями остатки будут вести себя так же (при сложении складываться, при умножении умножаться и т.д.).

- Дано простое число p и его ненулевой остаток a .
 - Докажите, что в последовательности $a \cdot 1, a \cdot 2, \dots, a \cdot (p - 1)$ все остатки разные.
 - Докажите, что существует единственный остаток b , такой что $ab \equiv 1 \pmod{p}$.

Такой остаток называется обратным остатком для a .

Мораль

Можно ввести понятие остатка или сравнений по модулю для дробей, у которых знаменатель не кратен p :

$$\frac{m}{a} \equiv m \cdot b \pmod{p}, \quad \text{где } b \text{ — обратный остаток } a.$$

П(р)оверьте, что определение действительно корректное:

- остаток дроби не меняется с выбором другой записи той же дроби;
- сумма дробей дает такой же остаток, что и сумма остатков этих дробей (и так со всеми арифм. действиями).

- Какие остатки совпадают со своими обратными остатками?
 - (Теорема Вильсона)** Докажите, что для простого p выполнено $(p - 1)! \equiv -1 \pmod{p}$.
- Найдите остаток $(100!)^{50}$ при делении на 101.
- Докажите, используя обратные остатки, что $m \div 101$, если: $\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{100} = \frac{m}{n}$.
- На доске написаны числа $\frac{100}{1}, \frac{99}{2}, \dots, \frac{1}{100}$. Можно ли выбрать какие-то пять из них, произведение которых равняется единице?
- Докажите, что для простого q выражение $(2q - 1)! - q$ делится на q^2 .