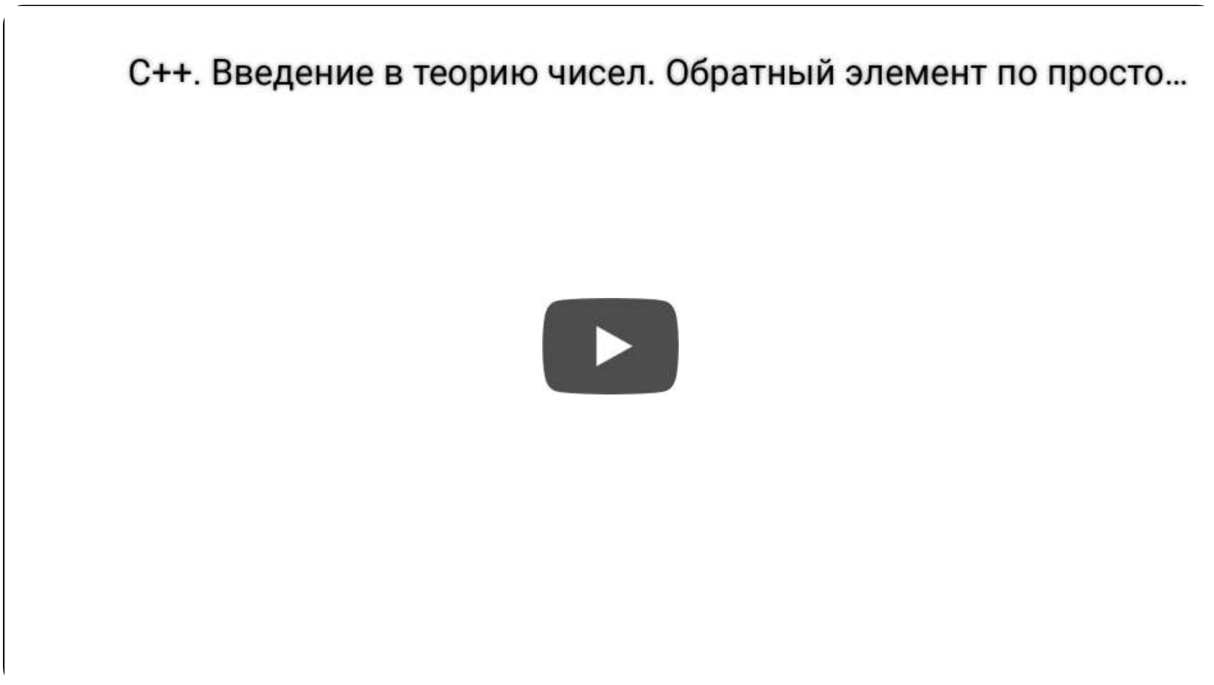
Обратный элемент по простому модулю



Малая теорема Ферма

Пусть дано простое число p и целое число a, не делящееся на p, тогда $a^{p-1} \equiv 1 \pmod{p}$.

Например, при $p = 5$:

- $1^4 \equiv 1 \pmod{5}$
- $2^4 \equiv 1 \pmod{5}$
- $3^4 \equiv 1 \pmod{5}$
- $4^4 \equiv 1 \pmod{5}$

Докажем, что из теоремы следует утверждение

$$a^{-1} \equiv a^{p-2} \pmod{p}.$$

Для этого умножим обе части выражения на a:

$$a^{-1} \cdot a \equiv a^{p-2} \cdot a \pmod{p},$$

что равносильно

$$1 \equiv a^{p-1} \pmod{p}.$$

А это верно по малой теореме Ферма.

Заметим, что теперь мы можем легко найти обратное число к a в $\mathbb{Z}_p$ для простого модуля p. Для этого достаточно возвести a в степень $p-2$ по модулю p.

Так как число p может быть весьма большим, то для ускорения поиска обратного числа рекомендуется использовать алгоритм быстрого возведения в степень, что позволит искать обратный элемент по простому модулю за $O(\log p)$ операций.