



ИНДЕКС

ИНДЕКС в теории чисел, число, играющее при решении сравнений роль, аналогичную роли логарифмов при решении показательных уравнений; обозначается ind . Если p – нечётное простое число, g – [первообразный корень](#) по модулю p , то И. числа a называется такое число $k = \text{inda}$, что $a \equiv g^k \pmod{p}$. И. обладает свойствами

$$\text{ind}(ab) = \text{inda} + \text{ind}b \pmod{p-1},$$

$$\text{ind} \frac{a}{b} = \text{inda} - \text{ind}b \pmod{p-1},$$

где a/b понимается как корень сравнения $bx \equiv a \pmod{p}$. При решении двучленных уравнений $ax^n \equiv b \pmod{p}$ И. используют для перехода к линейным сравнениям $\text{inda} + n\text{ind}x \equiv \text{ind}b \pmod{p-1}$. Ввиду практич. пользы И., для каждого простого модуля p (не слишком большого) имеются спец. таблицы. Понятие «И.» утвердилось в теории чисел после работ К. [Гаусса](#) в нач. 19 в.

Литература

Лит.: Виноградов И. М. Основы теории чисел. 11-е изд. М., 2006.

Processing math: 100%