

Практика №9 (19.11.20)

6. Примитивные корни и индексы.

6.1. Порядок целого числа по модулю n .

1. Найти порядок целых чисел 2, 3, 5:

- по модулю 17;
- по модулю 19;
- по модулю 23.

2. Доказать, что $\phi(2^n - 1)$ кратно n для любого $n > 1$.

3. Пусть h – порядок a по модулю n , k – порядок b по модулю n . Доказать, что порядок ab по модулю n делит hk . В частности, если $\text{НОД}(h, k) = 1$, тогда ab будет являться порядком hk .

6.2. Примитивные корни по простому модулю.

5. Убедиться, что каждое сравнение $x^2 \equiv 1 \pmod{15}$ и $x^2 \equiv -1 \pmod{65}$ имеет четыре решения.

6. Найти все примитивные корни по модулю $p = 17$ и выразить каждый из них как степень одного из корней.

7. Для простого числа $p > 3$ доказать, что примитивные корни по модулю p встречаются в парах r, r' где $rr' \equiv 1 \pmod{p}$.