

Первообразные корни

Группа 11-2

21.09.17

*...ибо честь, воздаваемая
образу, переходит к
первообразному...*

Догмат о иконопочитании

Все числа натуральны, а p простое.

1. Докажите, что если $a^n \equiv a^k \equiv 1 \pmod{m}$ и $(a, m) = 1$, то $a^d \equiv 1 \pmod{m}$, где $d = (n, k)$.

Определение. Показателем целого a по модулю натурального n (при условии, что a и n взаимно просты) называется наименьшее такое натуральное t , что $a^t \equiv 1 \pmod{n}$.

2. (а) Пусть a и n взаимно просты. Докажите, что $a^d \equiv 1 \pmod{n}$ тогда и только тогда, когда d делится на t .
(б) Пусть a и n взаимно просты. Докажите, что $a^d \equiv a^s \pmod{n}$ тогда и только тогда, когда $d - s$ делится на t .
(с) Докажите, что если $(n, m) = 1$ и показатель n по модулю m равен t , то $\varphi(m)$ делится на t .
3. Пусть n – чётное число. Докажите, что любой делитель $n^4 + 1$ даёт остаток 1 при делении на 8.
4. Пусть p – простое число, d – один из делителей числа $p - 1$. Выберем из остатков $1, 2, \dots, p - 1$ те, чей показатель по модулю p равен d . Чему равен остаток произведения выбранных чисел по модулю p ?
5. (а) Докажите, что показателю k по модулю p может принадлежать не более k остатков.
(б) Докажите, что если a принадлежит по модулю p показателю d , а b – показателю k , при этом $(d, k) = 1$, то число ab принадлежит по модулю p показателю dk .
(с) Пусть d_i – показатель числа i по модулю p . Докажите, что

$$[d_1, d_2, \dots, d_{p-1}] = p - 1.$$

- (д) Из предыдущих пунктов выведите, что по простому модулю p существует *первообразный корень*, то есть число, показатель которого по этому модулю равен $p - 1$.
6. Докажите, что по простому модулю p существует не один первообразный корень, а ровно $\varphi(p - 1)$ штук.

Разные задачи

Группа 11-2

21.09.17

1. Пусть p – простое число. Докажите, что все простые делители числа $p^p - 1$ и большие p дают остаток 1 при делении на p .
2. Найдите наименьшее n , такое, что $2^{2017} | 17^n - 1$.
3. Найдите все натуральные n , для которых $n^n + 1$ и $(2n)^{2n} + 1$ являются простыми.
4. Найдите все натуральные n , такие, что

$$n | 1^n + 2^n + \dots + (n-1)^n$$

5. Найдите все простые p и q для которых $5^p + 5^q$ делится на pq .

ЯГубов.РФ