

Показатели

1. Пусть a, n — взаимно простые числа. Рассмотрим последовательность остатков по модулю n следующих чисел: $1, a, a^2, \dots$. Докажите, что эта последовательность периодическая и не содержит предпериода.

Определение. Минимальный период последовательности остатков из предыдущей задачи называется показателем a по модулю n . Далее будем обозначать его буквой d .

2. Зафиксируем взаимно простые числа a и n .

(a) Докажите, что d — показатель a по модулю n тогда и только тогда, когда d — наименьшее такое натуральное число, что $(a^d - 1)$ делится на n .

(b) Пусть d — показатель a по модулю n . Пусть $a^l \equiv 1 \pmod{n}$. Докажите, что $d|l$.

(c) Докажите, что $a^s \equiv a^r \pmod{n}$ тогда и только тогда, когда $s \equiv r \pmod{d}$.

(d) Докажите, что показатель любого взаимно простого с n числа по модулю n делит $\varphi(n)$ (функция Эйлера).

3. Найдите все простые p и q такие, что $q|(2^p - 1)$ и $p|(2^q - 1)$.

4. Докажите, что если $a > 1$, то n делит $\varphi(a^n - 1)$.

5. (a) Пусть $p > 2$ — простое число. Докажите, что любой простой делитель числа $(a^p - 1)$ или делит $(a - 1)$, или имеет вид $2px + 1$.

(b) Выведите отсюда, что простых чисел вида $2pk + 1$ бесконечно много.

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