

Конечные арифметики

Пусть p — простое число, $a \in \mathbb{Z}_p$ — какой-то ненулевой остаток. Рассмотрим все его степени: $a, a^2, \dots, a^k, \dots$

Задача 1. Докажите, что найдется такое d , для которого $a^d = 1$.

Определение. Минимальное натуральное число d , для которого $a^d = 1$, называется *порядком* элемента a по модулю p и обозначается $d_p(a)$.

Задача 2. Докажите следующие свойства порядков:

- а) Если $d_p(a) = d$ и $a^m = 1$, то m делится на d ;
- б) Если $d_p(a) = m$, $m = kl$, то $d_p(a^k) = l$;
- в) $d_p(a) = d_p(a^{-1})$;
- г) Если $d_p(a) = m$, $d_p(b) = n$, то $d_p(ab)$ является делителем наименьшего общего кратного чисел m и n . Верно ли, что оно всегда равняется этому наименьшему общему кратному?
- д) Если $d_p(a) = m$, $d_p(b) = n$ и числа m и n взаимно просты, то $d_p(ab) = mn$.

Задача 3. Найдите порядок остатка 2 в \mathbb{Z}_7 , \mathbb{Z}_{11} , \mathbb{Z}_{13} .

Задача 4. Докажите, что:

- а) Если $A = a^4 + b^4 + c^4 + d^4$ делится на 5, то A делится и на 625;
- б) Если $a^3 + b^3 + c^3$ делится на 7, то abc делится на 7;
- в) Если $a^2 + b^2$ делится на 7, то и a , и b делятся на 7.