Конечные арифметики

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

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 $A = a^4 + b^4 + c^d + d^4$ 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.

Задача 5. а) Какие простые числа встречаются в разложении выражений вида $n^2 + 1$ на простые множители?

б) Докажите, что простых чисел вида $4k + 1$ бесконечно много.

Задача 6. Докажите, что сравнение $ax^2+bx+c \equiv 0 \mod p$ имеет два решения по модулю p, если дискриминант — квадратичный вычет; не имеет решений, если дискриминант — квадратичный невычет; имеет ровно одно решение по модулю p, если дискриминант равен нулю по модулю p.

Задача 7 (теорема Жирара). Пусть $x^2 + y^2$ делится на простое число p вида $4k + 3$. Докажите, что x и y делятся на p.

Задача 8. С помощью квадратичного закона взаимности вычислите символы Лежандра:
а) $\left(\frac{57}{239}\right)$; **б)** $\left(\frac{179}{1543}\right)$; **в)** $\left(\frac{1789}{2017}\right)$.

Задача 9. Разрешимо ли по модулю 239 уравнение $x^2 + 57x + 179 = 0$?