Арифметика остатков

Задача 1. Решите в целых числах уравнение $x^2 + 7y^3 = 12$.

Соглашение. Через p обозначается простое число, большее 2.

Определение. *Делителем нуля* называется такой ненулевой элемент кольца, который при умножении на некоторый ненулевой элемент дает нуль.

Задача 2. Докажите эквивалентность условий:

а) элемент $a \in \mathbb{Z}/m\mathbb{Z}$ не является обратимым;

б) a является делителем нуля;

в) a и m не взаимно просты.

Задача 3. а) Докажите, что в $\mathbb{Z}/p\mathbb{Z}$ уравнение $x^2 = a$, где $a \neq 0$, имеет либо два решения, либо ни одного.

б) Придумайте такие m и a, что уравнение $x^2 = a$ имеет в $\mathbb{Z}/m\mathbb{Z}$ более двух решений.

в) При $p \leq 11$ выясните, при каких $a \neq 0$ уравнение $x^2 = a$ разрешимо в $\mathbb{Z}/p\mathbb{Z}$ (такие a называются *квадратичными вычетами*).

Задача 4. Верно ли, что для всякого $k \in \mathbb{N}$ найдутся такие $m \in \mathbb{N}$, $a \in \mathbb{Z}/m\mathbb{Z}$, что уравнение $x^2 = a$ имеет в $\mathbb{Z}/m\mathbb{Z}$ ровно k решений?

Задача 5 (ленивый бином Ньютона). а) Докажите, что в $\mathbb{Z}/p\mathbb{Z}$ имеет место равенство

$$(a + b)^p = a^p + b^p.$$

б) Верно ли аналогичное утверждение в $\mathbb{Z}/m\mathbb{Z}$ без предположения простоты m?

в) Выведите из пункта а) малую теорему Ферма.

Задача 6 (теорема Безу). Пусть $\mathbb{K}$ — поле (например, $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ или $\mathbb{K} = \mathbb{R}$). Пусть $p(x) \in \mathbb{K}[x]$ — многочлен, коэффициенты которого являются элементами поля $\mathbb{K}$.

а) Пусть $a \in \mathbb{K}$ — корень многочлена $p(x)$. Докажите, что $p(x)$ делится на двучлен $x - a$.

б) Докажите, что многочлен степени d имеет не более d корней в $\mathbb{K}[x]$.

Задача 7. Бывает ли ненулевой многочлен над $\mathbb{Z}/p\mathbb{Z}$, имеющий корни во *всех* точках $\mathbb{Z}/p\mathbb{Z}$? (Как известно, над $\mathbb{R}$ такого не бывает: если вещественный многочлен равен нулю во всех точках, то он тождественно равен нулю).

Задача 8*. Придумайте комбинаторное доказательство теоремы Вильсона в духе доказательства малой теоремы Ферма через подсчет каруселей.

Евгений Юрьевич Смирнов, esmirnov@hse.ru