Алгебра I, осенний семестр 2013 г.

Решения избранных задач из домашних заданий.

факультет математики, НИУ ВШЭ

Решения нужно сдавать в письменном виде. Пожалуйста, пишите разборчиво или набирайте в TeX.

Задача (3.2). Найдите квадратный многочлен f с рациональными коэффициентами, такой что

$$f(1) = 2, \quad f(2) = 20, \quad f(3) = 200.$$

Решение. Многочлен $f = 2f_1 + 20f_2 + 200f_3$, где

$$f_1 = \frac{1}{2}(x-2)(x-3); \quad f_2 = -(x-1)(x-3); \quad f_3 = \frac{1}{2}(x-1)(x-2)$$

удовлетворяет условию задачи, так как для всех $i, j = 1, 2, 3$ имеем

$$f_i(j) = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}.$$

Осталось раскрыть скобки и привести подобные члены в $f = 2f_1 + 20f_2 + 200f_3$.

Ответ: $f = 81x^2 - 225x + 146$

Задача (4.2). Обозначим через $\mathbb{F}_5$ поле из пяти элементов. Найдите все пары изоморфных колец в следующем списке:

(1) $\mathbb{F}_5$, (2) $\mathbb{F}_5 \oplus \mathbb{F}_5$, (3) $\mathbb{F}_5[x]/(x^2+1)$, (4) $\mathbb{Z}[i]/(5)$, (5) $\mathbb{Z}[i]/(2+i)$, (6) $\mathbb{F}_5[x]/(x^2-1)$.

Решение. Мы будем неоднократно использовать, что кольцо $R[x]/(x-a)$ изоморфно R для любого кольца R и любого элемента $a \in R$. Изоморфизм переводит многочлен $f(x)$ в $f(a)$.

Поскольку $x^2 + 1 = (x+2)(x-2)$ в кольце $\mathbb{F}_5[x]$, и $x+2$ и $x-2$ взаимно просты, то по китайской теореме об остатках

$$\mathbb{F}_5[x]/(x^2+1) \simeq \mathbb{F}_5[x]/(x-2) \oplus \mathbb{F}_5[x]/(x+2),$$

откуда (2) $\simeq$ (3). Аналогично получаем изоморфизм (2) $\simeq$ (6), так как $x^2 - 1 = (x-1)(x+1)$.

Поскольку $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(x^2+1)$ (изоморфизм переводит i в x) и $\mathbb{F}_5[x] \simeq \mathbb{Z}[x]/(5)$ (изоморфизм переводит x в x), то

$$\mathbb{Z}[i]/(5) \simeq \big(\mathbb{Z}[x]/(x^2+1)\big)/(5) = (\mathbb{Z}[x]/(5))/(x^2+1) \simeq \mathbb{F}_5[x]/(x^2+1),$$

то есть (3) $\simeq$ (4).

Изоморфизм (1) $\simeq$ (5) доказывается похожим образом:

$$\mathbb{Z}[i]/(2+i) \simeq \big(\mathbb{Z}[x]/(x^2+1)\big)/(2+x) = (\mathbb{Z}[x]/(2+x))/(x^2+1) \simeq \mathbb{Z}/(2^2+1) = \mathbb{F}_5.$$

Кольца $\mathbb{F}_5$ и $\mathbb{F}_5 \oplus \mathbb{F}_5$ неизоморфны, так как в них разное число элементов.

Ответ: (1) $\simeq$ (5), (2) $\simeq$ (3) $\simeq$ (4) $\simeq$ (6)

Задача (4.3). Для каждого $k \in \mathbb{N}$ найдите число решений уравнения

$$x^2 = 1$$

в кольце $\mathbb{Z}/2^k\mathbb{Z}$.

Решение. Перепишем уравнение в виде

$$(x-1)(x+1) \equiv 0 \pmod{2^k},$$

и будем искать все целые решения x, такие что $0 \leq x < 2^k$. Поскольку $(x-1, x+1) \leq 2$, числа $x+1$ и $x-1$ не могут одновременно делится на 4. Следовательно, одно из них должно делиться на 2^{k-1}, то есть должно быть равно 0 или 2^{k-1}. Отсюда $x = \pm 1$ или $x = 2^{k-1} \pm 1$. Все эти решения различны при $k > 2$.

Ответ: Четыре решения при $k > 2$, и два решения при $k = 1, 2$

Задача (4.4). Найдите неприводимый над $\mathbb{Z}$ многочлен $f \in \mathbb{Z}[x]$ степени 4 со старшим коэффициентом 1, такой что

$$f(\sqrt{2} + \sqrt{3}) = 0.$$

Решение. Многочлен

$$f = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3})$$

имеет корень $\sqrt{2} + \sqrt{3}$. Раскрывая скобки находим, что $f = x^4 - 10x^2 + 1$. Проверим, что f неприводим над $\mathbb{Z}$. Поскольку все корни многочлена f иррациональны, он не может разложиться в произведение кубического и линейного многочлена с целыми коэффициентами. Осталось проверить, не раскладывается ли он в произведение двух квадратных многочленов с целыми коэффициентами. Если

$$f = (x^2 + ax + b)(x^2 + cx + d),$$

то $a + c = 0$, $ac + b + d = -10$, $ad + bc = 0$, $bd = 1$, откуда $b = d = \pm 1$, $a = -c$, $a^2 = 10 \mp 2$. Последнее уравнение не имеет целых решений, поэтому f неприводим над $\mathbb{Z}$.

Ответ: $x^4 - 10x^2 + 1$

Задача (4.5). Пусть $p, q \in \mathbb{N}$ — различные простые числа. Докажите, что сравнение

$$p^x + q^y \equiv 1 \pmod{pq}$$

разрешимо в натуральных числах.

Решение. Так как $(p, q) = 1$ по малой теореме Ферма получаем $q^{p-1} \equiv 1 \pmod{p}$, $p^{q-1} \equiv 1 \pmod{q}$, откуда $q^{p-1} + p^{q-1}$ — решение системы сравнений $x \equiv 1 \pmod{p}$, $x \equiv 1 \pmod{q}$. По китайской теореме об остатках $q^{p-1} + p^{q-1}$ также является решением сравнения $x \equiv 1 \pmod{pq}$.

Задача (5.3). Решите уравнение

$$100x = 999$$

в кольце $\mathbb{Z}/1001\mathbb{Z}$.

Решение. Поскольку $1001 - 10 \cdot 100 = 1$ (это можно найти с помощью алгоритма Евклида), получаем, что $[100] \cdot [-10] = 1$ в $\mathbb{Z}/1001\mathbb{Z}$. Умножая обе части исходного уравнения на обратимый элемент $[-10]$, получаем равносильное уравнение

$$x = [999] \cdot [-10],$$

откуда $x = [999] \cdot [-10] = [-2] \cdot [-10] = [20]$.

Ответ: $x = 20$