Домашнее задание на 15.05 (Алгебра)

Емельянов Владимир, ПМИ гр №247

№1 (a) Пусть

$$f(x) = x^5 + x^4 + x^2 - 4x - 2, \qquad g(x) = 2x^4 - x^3 - 2x^2 - 2x - 12.$$

Применим алгоритм Евклида.

$$\begin{aligned}
f(x) &= \left(\tfrac{1}{2}x + \tfrac{3}{2}\right) g(x) + r_1(x), && deg(r_1) = 3,\\
r_1(x) &= f(x) - (\tfrac{1}{2}x + \tfrac{3}{2})g(x) = \cdots = \frac{5}{2}x^3 + \frac{7}{2}x^2 + x + 16, &&\\
g(x) &= q_2(x)\, r_1(x) + r_2(x), && deg(r_2) = 2,\\
r_2(x) &= g(x) - q_2(x)r_1(x) = \cdots = x^2 + 2, &&\\
r_1(x) &= q_3(x)\, r_2(x) + r_3(x), && deg(r_3) < 2,\\
r_3(x) &= r_1(x) - q_3(x)r_2(x) = 0. &&
\end{aligned}$$

Вычисления дают

$$\gcd\bigl(f, g\bigr) = x^2 + 2,$$

Теперь восстанавливаем коэффициенты.

$$\begin{aligned}
r_2(x) &= g(x) - q_2(x)r_1(x)\\
r_1(x) &= f(x) - \left(\tfrac{1}{2}x + \tfrac{3}{2}\right)g(x)
\end{aligned}$$

Подставляя, получаем

$$x^2 + 2 = s(x)f(x) + t(x)g(x),$$

где

$$s(x) = \frac{5-2x}{7}, \quad t(x) = \frac{x^2-x-2}{7}$$

такие, что

$$s(x)\,f(x) + t(x)\,g(x) \;=\; x^2+2$$

(b) $K = \mathbb{Z}_7$

Рассмотрим

$$f(x) = x^5 + x^3 + 3x^2 + 5x + 3, \quad g(x) = 3x^4 + 3x^3 + 6x + 1$$

применим алгоритм Евклида в $\mathbb{Z}_7[x]$:

$$\begin{aligned}
f(x) &= 5x\,g(x) + r_1(x), & r_1(x) &= f - 5xg = 6x^4 + x^3 + x^2 + 3,\\
g(x) &= 4\,r_1(x) + r_2(x), & r_2(x) &= g - 4r_1 = 6x^3 + 3x^2 + 6x + 3,\\
r_1(x) &= x\,r_2(x) + r_3(x), & r_3(x) &= r_1 - xr_2 = x^2 + 4x + 5,\\
r_2(x) &= (6x+1)\,r_3(x) + r_4(x), & r_4(x) &= r_2 - (6x+1)r_3 = x - 3,\\
r_3(x) &= 3x + 6\,r_4(x) + 0.
\end{aligned}$$

Отсюда

$$\gcd(f,g) = r_4(x) = x-3$$

Восстановим коэффициенты:

$$\begin{aligned}
r_4(x) &= r_2(x) - (6x+1)r_3(x),\\
r_3(x) &= r_1(x) - xr_2(x),\\
r_2(x) &= g(x) - 4r_1(x),\\
r_1(x) &= f(x) - 5xg(x).
\end{aligned}$$

В итоге

$$x-3 = u(x)f(x) + v(x)g(x), \quad u(x) = 3x^2+4x+1,\ v(x) = 6x^3+2x^2+6x+1$$

№2 (a) $f(x) = x^5 + 3x^3 - 4x^2 - 12$

Заметим, что

$$x^5 + 3x^3 - 4x^2 - 12 \; = \; (x^3 - 4)(x^2 + 3),$$

получаем следующие разложения:

- При $K = \mathbb{R}$ многочлен $x^3 - 4$ даёт единственный действительный корень $\sqrt[3]{4}$, а $x^2 + 3$ неприводим.

$$f(x) \; = \; (x^3 - 4)(x^2 + 3)$$

- При $K = \mathbb{C}$ раскладываем оба множителя на линейные:

$$x^3 - 4 \; = \; \prod_{k=0}^{2}\Big(x - \sqrt[3]{4}\, e^{2\pi i k/3}\Big), \qquad x^2 + 3 = (x - i\sqrt{3})(x + i\sqrt{3})$$

Значит,

$$f(x) \; = \; \big(x - \sqrt[3]{4}\big)\, \big(x - \sqrt[3]{4}\, e^{2\pi i/3}\big)\, \big(x - \sqrt[3]{4}\, e^{4\pi i/3}\big)\, (x - i\sqrt{3})(x + i\sqrt{3})$$

(b) $K = \mathbb{Z}_5$, $f(x) = x^5 + x^4 + 3x^2 + x + 3 \in \mathbb{Z}_5[x]$ Проверкой всех возможных корней и факторизацией по модулю 5 получаем

$$f(x) \; = \; (x - 2)^2\, (x + 1)\, (x^2 - x + 2) \pmod 5,$$

где квадратный трёхчлен $x^2 - x + 2$ неприводим над $\mathbb{Z}_5$

№3 Пусть $\mathbb{Z}_3 = \{0, 1, 2\}$ — поле вычетов по модулю 3. Перечислим все неприводимые многочлены со старшим коэфицентом 1, степеней $1, 2, 3$ и укажем число таких степени 4.

(a) $\deg = 1$. линейные многочлены:

$$x, \quad x+1, \quad x+2.$$

(b) $\deg = 2$. квадратичные многочлены без корней в $\mathbb{Z}_3$:

$$x^2+1, \quad x^2+x+2, \quad x^2+2x+2.$$

(c) $\deg = 3$. кубические многочлены без корней в $\mathbb{Z}_3$:

$$x^3+2x+1, \quad x^3+2x+2,$$
$$x^3+x^2+2, \quad x^3+x^2+x+2, \quad x^3+x^2+2x+1,$$
$$x^3+2x^2+1, \quad x^3+2x^2+x+1, \quad x^3+2x^2+2x+2.$$

(d) $\deg = 4$.

Рассмотрим все многочлены вида

$$f(x) = x^4 + ax^3 + bx^2 + cx + d, \quad a, b, c, d \in \mathbb{Z}_3$$

Всего таких многочленов $|\mathbb{Z}_3|^4 = 3^4 = 81$.

- **Многочлены, имеющие линейный множитель (корень) в $\mathbb{Z}_3$.**

  Для каждого $\alpha \in \{0, 1, 2\}$ число многочленов с корнем α равно 3^3. По принципу включений–исключений получаем

  $$N \ = \ 3 \cdot 3^3 \ - \ \binom{3}{2} 3^2 \ + \ \binom{3}{3} 3 \ = \ 81 - 27 + 3 \ = \ 57$$

- **Многочлены, раскладывающиеся в произведение двух неприводимых квадратичных (но не имеющие линейных множителей).**

  Из предыдущего пункта известно, что неприводимых квадратичных над $\mathbb{Z}_3$ ровно 3. Число их попарных произведений (с повторениями) равно

$$\binom{3}{2} + 3 = 3 + 3 = 6$$

Следовательно, число оставшихся (неприводимых) многочленов степени 4:

$$81 \;-\; 57 \;-\; 6 \;=\; 18$$

№4 Пусть $f(x), g(x) \in \mathbb{Q}[x]$ — два неприводимых многочлена, и пусть они имеют общий корень $r \in \mathbb{C}$. Тогда в кольце $\mathbb{Q}[x]$ их наибольший общий делитель $\gcd(f, g)$ — не константа, а значит его степень ≥ 1.

Но неприводимость каждого из них означает, что единственные делители (с ненулевой степенью) — это они сами (с точностью до константы). Поэтому

$$\gcd(f, g) \sim f \quad \text{и} \quad \gcd(f, g) \sim g.$$

Отсюда $f \mid g$ и $g \mid f$, что возможно только если

$$g(x) = c\, f(x) \quad \text{для некоторого } c \in \mathbb{Q}^{\times}.$$

Иными словами, f и g отличаются лишь константой, то есть пропорциональны.