# Дополнение к семинару 19-20.

## Многочлены над полями вычетов.

При работе с многочленами над полями вычетов действуют те же правила, что и в полях $\mathbb{R}$ и $\mathbb{C}$, за исключением того, что операции над коэффициентами многочлена проводятся в соответствующем поле вычетов.

**Задача 1.** Разложить многочлен
$$f(x) = x^4 + 4x^3 + 4x + 1$$
на неприводимые над полем вычетов $\mathbb{Z}_5$.

**Решение:** Заметим, что 4 в $\mathbb{Z}_5$ обратна самой себе, а потому слагаемые в многочлене можно сгруппировать:
$$f(x) = x^4 + 4x^3 + 4x + 1 = x^3(x+4) + 4(x+4) = (x^3+4)(x+4).$$
Задача сводится к разложению на неприводимые множители многочлена
$$g(x) = x^3 + 4.$$
Это многочлен третьей степени. Если он приводим, он раскладывается на произведение линейного двучлена и квадратного трёхчлена (возможно, приводимого). Значит, многочлен $g(x)$ должен иметь корни над $\mathbb{Z}_5$. Подбором получаем, что $x=1$ является корнем $g(x)$:
$$g(1) = 1 + 4 = 5 = 0.$$
Значит, многочлен $g(x)$ должен делиться на $x-1 = x+4$. Поделим $g(x)$ на $x+4$ столбиком:

$$\begin{array}{r|l} x^3 + 0x^2 + 0x + 4 & x+4 \\ \hline -\,x^3 + 4x & x^2 + x + 1 \\ \hline x^2 + 0x & \\ -\,x^2 + 4x & \\ \hline x + 4 & \\ -\,x + 4 & \\ \hline 0 & \end{array}$$

Обратите внимание, что операции производятся в $\mathbb{Z}_5$, а потому $-1 = 4$.

Осталось выяснить, является ли многочлен
$$h(x) = x^2 + x + 1$$
неприводимым над $\mathbb{Z}_5$. Если он приводим, он раскладывается на произведение линейных двучленов, а значит, имеет 2 корня в поле $\mathbb{Z}_5$. В поле $\mathbb{Z}_5$ всего 5 чисел: 0, 1, 2, 3, 4, а потому корни многочлена в этом поле можно найти перебором всех:
$$h(0) = 1 \neq 0$$
$$h(1) = 1 + 1 + 1 = 3 \neq 0$$
$$h(2) = 4 + 2 + 1 = 2 \neq 0$$
$$h(3) = 4 + 3 + 1 = 3 \neq 0$$
$$h(4) = 1 + 4 + 1 = 1 \neq 0$$
Многочлен $h(x)$ не имеет корней в $\mathbb{Z}_5$, а значит, он неприводим. В итоге имеем:
$$f(x) = (x+4)(x+4)(x^2 + x + 1). \blacksquare$$

**Задача 2.** Найти все неприводимые многочлены степени $\leq 4$ в поле вычетов $\mathbb{Z}_2$.

**Решение:** В поле $\mathbb{Z}_2$ есть 2 неприводимых многочлена степени 1:

$$f_1 = x \quad ; \quad f_2 = x+1.$$

Кроме того, заметим, что

$$(x+1)^2 = x^2+2x+1 = x^2+1 \pmod 2$$
$$(x+1)^4 = ((x^2+1)^2)^2 = (x^2+1)^2 = x^4+1 \pmod 2$$

Это пригодится далее.

Существует 4 многочлена степени 2 в $\mathbb{Z}_2$:

$$x^2 \; ; \; x^2+1 \; ; \; x^2+x \; ; \; x^2+x+1$$

Из них первые 3 являются приводимыми, поскольку имеют корни в $\mathbb{Z}_2$ (в $\mathbb{Z}_2$ всего 2 элемента, поэтому найти корни можно непосредственной перебором). Многочлен $x^2+x+1$ корней в $\mathbb{Z}_2$ не имеет, а потому неприводим:

$$f_3 = x^2+x+1$$

Заметим также, что если многочлен в $\mathbb{Z}_2$ имеет чётное число слагаемых, то он приводим, поскольку 1 является корнем такого многочлена. Поэтому далее ограничимся рассмотрением многочленов с нечётным числом слагаемых (кроме $x^n$ — такой многочлен приводим). Таким образом, рассмотрим 3 многочлена степени 3 в $\mathbb{Z}_2$:

$$f_4 = x^3+x^2+1, \quad f_5 = x^3+x^2+x, \quad f_6 = x^3+x+1$$

Из них $f_5$ приводим:

$$f_5 = x^3+x^2+x = x(x^2+x+1),$$

а два других — нет (в противном случае они бы раскладывались на произведение линейного двучлена и квадратного трёхчлена, а значит, имели бы корни в $\mathbb{Z}_2$).

Рассмотрим многочлены с нечётным числом слагаемых степени $\leq 4$ в $\mathbb{Z}_2$:

$$f_7 = x^4+x^3+1, \quad f_8 = x^4+x^3+x^2, \quad f_9 = x^4+x^3+x \; ;$$
$$f_{10} = x^4+x^2+x, \quad f_{11} = x^4+x^2+1; \quad f_{12} = x^4+x+1 \; ; \; f_{13} = x^4+x^3+x^2+x+1.$$

Очевидно, что $f_8, f_9, f_{10}$ приводимы, поскольку делятся на $x$. Остальные многочлены ($f_7, f_{11}, f_{12}, f_{13}$) не имеют корней в $\mathbb{Z}_2$. Но какой-нибудь из них может оказаться приводимым, если раскладывается на произведение неприводимых многочленов степени 2. Такой многочлен в $\mathbb{Z}_2$ всего один: $f_3 = x^2+x+1$. А значит, приводимым среди многочленов $f_7, f_{11}, f_{12}, f_{13}$ является тот, который равен $f_3^2$, таковым:

$$f_3^2 = (x^2+x+1)^2 = x^4+(x+1)^2 = x^4+x^2+1 = f_{11}.$$

Многочлены $f_7, f_{12}, f_{13}$ неприводимы.

**Ответ:**
Степени 1: $x, x+1$
Степени 2: $x^2+x+1$
Степени 3: $x^3+x^2+1, \; x^3+x+1$
Степени 4: $x^4+x^3+1, \; x^4+x+1, \; x^4+x^3+x^2+x+1.$ ■

**Задача 3.** Является ли многочлен
$$f(x) = x^5 + x^4 + 1$$
неприводимым над полем вычетов $\mathbb{Z}_2$? Если нет, разложить его на неприводимые сомножители.

**Решение:** Если $f(x)$ приводим, то есть 2 возможности:
1) в разложении есть линейные двучлены $\Leftrightarrow$ многочлен $f(x)$ имеет корни в $\mathbb{Z}_2$
2) $f(x)$ раскладывается на произведение многочленов второй и третьей степени (неприводимых).

Первое проверим, поскольку $f(0) = 1 \neq 0$; $f(1) = 1 \neq 0$.
Проверим, делится ли $f(x)$ на единственный неприводимый многочлен степени 2 над $\mathbb{Z}_2$, т.е. на $x^2 + x + 1$,

$$\begin{array}{r|l} x^5 + x^4 + 0x^3 + 0x^2 + 0x + 1 & x^2 + x + 1 \\ \hline x^5 + x^4 + x^3 & x^3 + x + 1 \\ \hline x^3 + 0x^2 + 0x & \\ x^3 + x^2 + x & \\ \hline x^2 + x + 1 & \\ x^2 + x + 1 & \\ \hline 0 & \end{array}$$

Получили, что $f(x)$ делится на $x^2 + x + 1$. Значит, $f(x)$ приводим и раскладывается на неприводимые множители следующим образом:
$$f(x) = (x^3 + x + 1)(x^2 + x + 1).$$ ■

**Задача 4.** Является ли многочлен
$$f(x) = x^3 + x + 2$$
неприводимым над полем вычетов $\mathbb{Z}_3$? Если нет, разложить его на неприводимые множители.

**Решение:** Если $f(x)$ приводим, то он раскладывается на произведение линейного двучлена и квадратного трехчлена. Значит, в этом случае $f(x)$ имеет корень в $\mathbb{Z}_3$. Найдем корни перебором:
$$f(0) = 2 \neq 0$$
$$f(1) = 1 + 1 + 2 \neq 0$$
$$f(2) = 2 + 2 + 2 = 0 \Rightarrow x = 2 \text{ является корнем } f(x).$$
Таким образом, $f(x)$ делится на $x - 2 = x + 1$. Поделим $f(x)$ на $x + 1$:

$$\begin{array}{r|l} x^3 + 0x^2 + x + 2 & x + 1 \\ \hline x^3 + x^2 & x^2 + 2x + 2 \\ \hline 2x^2 + x & \\ 2x^2 + 2x & \\ \hline 2x + 2 & \\ 2x + 2 & \\ \hline 0 & \end{array}$$

Значит, $f(x) = (x+1)(x^2 + 2x + 2)$. Выясним, является ли многочлен $h(x) = x^2 + 2x + 2$ неприводимым над $\mathbb{Z}_3$. Если он приводим, то он раскладывается на произведение линейных множителей, а значит, имеет корни в $\mathbb{Z}_3$. Числа 0 и 1 не могут быть корнями $h(x)$, поскольку в этом случае они являлись бы и корнями $f(x)$.
$$h(2) = 1 + 1 + 2 = 1 \neq 0 \Rightarrow$$
$\Rightarrow$ многочлен $h(x)$ неприводим.

**Ответ:** $f(x) = (x+1)(x^2 + 2x + 2)$. ■

# Алгоритм Евклида

Поскольку для многочленов определено деление с остатком, для них можно применить алгоритм Евклида нахождения наибольшего делителя.

**Задача 5.** Найти НОД $(x^5 + 4x^4 + 4x^3 + 2x^2 + 4x + 3,\ x^4 + 2x^3 + 2x^2 + 2x + 1)$ в поле вычетов $\mathbb{Z}_5$.

**Решение:** Сначала делим многочлен большей степени на многочлен меньшей степени:

$$\begin{array}{r|l} x^5 + 4x^4 + 4x^3 + 2x^2 + 4x + 3 & x^4 + 2x^3 + 2x^2 + 2x + 1 \\ \hline x^5 + 2x^4 + 2x^3 + 2x^2 + 2x & x + 2 \\ \hline 2x^4 + 2x^3 + 0x^2 + 3x + 3 & \\ 2x^4 + 4x^3 + 4x^2 + 4x + 2 & \\ \hline 3x^3 + x^2 + 4x + 1 & \end{array}$$

$$\Rightarrow x^5 + 4x^4 + 4x^3 + 2x^2 + 4x + 3 = (x+2)(x^4 + 2x^3 + 2x^2 + 2x + 1) + (3x^3 + x^2 + 4x + 1$$

Далее для удобства умножим остаток от деления на $3^{-1} = 2$:

$$2 \cdot (3x^3 + x^2 + 4x + 1) = x^3 + 2x^2 + 3x + 2$$

Теперь делим $x^4 + 2x^3 + 2x^2 + 2x + 1$ на приведенный остаток от деления:

$$\begin{array}{r|l} x^4 + 2x^3 + 2x^2 + 2x + 1 & x^3 + 2x^2 + 3x + 2 \\ \hline x^4 + 2x^3 + 3x^2 + 2x & x \\ \hline 4x^2 + 1 & \end{array}$$

$$\Rightarrow x^4 + 2x^3 + 2x^2 + 2x + 1 = x(x^3 + 2x^2 + 3x + 2) + (4x^2 + 1).$$

Умножим на $4^{-1} = 4$:

$$4 \cdot (4x^2 + 1) = x^2 + 4.$$

Делим $x^3 + 2x^2 + 3x + 2$ на $x^2 + 4$:

$$\begin{array}{r|l} x^3 + 2x^2 + 3x + 2 & x^2 + 4 \\ \hline x^3 + 0x^2 + 4x & x + 2 \\ \hline 2x^2 + 4x + 2 & \\ 2x^2 + 0x + 3 & \\ \hline 4x + 4 & \end{array}$$

$$\Rightarrow x^3 + 2x^2 + 3x + 2 = (x^4 + 2)(x + 2) + (4x + 4).$$

Умножим на $4^{-1} = 4$: $4 \cdot (4x + 4) = x + 1$. Делим $x^2 + 4$ на $x + 1$:

$$\begin{array}{r|l} x^2 + 0x + 4 & x + 1 \\ \hline x^2 + x & x + 4 \\ \hline 4x + 4 & \\ 4x + 4 & \\ \hline 0. & \end{array}$$

$$\Rightarrow x^2 + 4 = (x+1)(x+4) + 0.$$

Последний ненулевой остаток равен $x + 1 \Rightarrow$

$\Rightarrow$ НОД $(x^4 + 2x^3 + 2x^2 + 2x + 1,\ x^5 + 4x^4 + 4x^3 + 2x^2 + 4x + 3) = x + 1.$ ■

**Замечание.** Конечно, последнее деление можно не делать, если заметить, что

$$x^2 + 4 = x^2 - 1 = (x-1)(x+1) = (x+4)(x+1).$$