Лекция 5. Многочлены из $\mathbb{F}_n[x]$

1. Деление с остатком

Множество многочленов с коэффициентами в поле $\mathbb{F}_n$ будет обозначаться $\mathbb{F}_n[x]$. Обычный способ деления в столбик здесь работает. Значит, есть деление с остатком, и, следовательно, имеет место единственность разложения на простые.

Пусть $p = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ — приведенный многочлен с целыми коэффициентами, причем старший коэффициент a_n и младший коэффициент a_0 оба не делятся на простое число k. Если p разложим $p = r \cdot s$, то, заменяя в этом разложении все коэффициенты их остатками от деления на k, получаем разложение многочлена в $\mathbb{F}_k[x]$. Если многочлен неприводим в некотором $\mathbb{F}_k[x]$, то, значит, он неприводим в $\mathbb{Z}[x]$.

Пример. Рассмотрим многочлен $p = 3x^7 - x^6 + x^5 + 5x^4 + x^3 + 4x^2 - 3x - 7 \in \mathbb{Z}[x]$. По модулю 2 p разложим: $x^7+x^6+x^5+x^4+x^3+x+1 = (x^5+x^2+1)(x^2+x+1)$. Это означает, что если p разложим в $\mathbb{Z}[x]$, то он разлагается на множитель степени 5 и на множитель степени 2. В действительности p неприводим по модулю 5, так что он неприводим и в $\mathbb{Z}[x]$.

2. Неприводимые многочлены над конечными полями

Есть формула для числа неприводимых многочленов из $\mathbb{F}_n[x]$. Сначала дадим определение функции Мебиуса.

Определение. Функцией Мебиуса называется функция μ на множестве натуральных чисел $\mathbb{N}$, заданная следующим образом:

$$\mu(n) = \begin{cases} 1, \text{ если } n = 1, \\ (-1)^k, \text{ если } n \text{ есть произведение } k \text{ различных простых чисел}, \\ 0, \text{ если } n \text{ делится на квадрат простого числа.} \end{cases}$$

Теорема. *Число $N_n(k)$ нормированных (т.е. со старшим коэффициентом 1) неприводимых многочленов степени k в $\mathbb{F}_n[x]$ равно*

$$N_n(k) = \frac{1}{k} \sum_{d|k} \mu\left(\frac{k}{d}\right) n^d.$$

Замечание. Обозначение $d|k$ означает, что d делит k.

Пример. Число неприводимых многочленов степени 4 в $\mathbb{F}_2[x]$ равно

$$N_2(4) = \frac{1}{4}(\mu(4) \cdot 2 + \mu(2) \cdot 2^2 + \mu(1) \cdot 2^4) = \frac{1}{4}(-4 + 16) = 3.$$

Вот эти многочлены $x^4 + x + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1$.

3. Поле $\mathbb{F}_4$

Конечные поля не исчерпываются полями $\mathbb{F}_n$, n — простое. Если m — степень простого числа, то существует поле $\mathbb{F}_m$ с m элементами. Простейшее такое поле — это поле $\mathbb{F}_4$. Это поле содержит 0, содержит единицу и еще два элемента a и b. Таблицы сложения и умножения выглядят так:

	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Нетрудно проверить, что так определенный объект действительно поле. Это поле играет важную роль в теории кодирования.

4. Упражнения

- Найдите все неприводимые многочлены степеней 3, 4 и 5 в $\mathbb{F}_2[x]$.
- Найдите все неприводимые нормированные мноночлены степеней 2 и 3 в $\mathbb{F}_3[x]$.
- Используя разложение в $\mathbb{F}_2[x]$, показать, что многочлен $x^6 + x + 1$ неприводим в $\mathbb{Z}[x]$.
- Используя разложение многочлена $x^5+x^4+4x^3+4x^2+3x+4$ в $\mathbb{F}_2[x]$ и $\mathbb{F}_3[x]$, показать, что он неразложим в $\mathbb{Z}[x]$.
- Покажите, что не существует поле с шестью элементами.