Серия 6. Многочлены над полями

Определение. Многочленом над полем $\mathbb{F}$ называется последовательность $(a_0, a_1, a_2, \ldots, a_n, \ldots)$ из элементов поля $\mathbb{F}$, в которой все члены, кроме конечного числа, равны нулю. Суммой многочлена $(a_0, a_1, a_2, \ldots, a_n, \ldots)$ и многочлена $(b_0, b_1, b_2, \ldots, b_n, \ldots)$ называется многочлен $(a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n, \ldots)$, а произведением – многочлен $(c_0, c_1, c_2, \ldots, c_n, \ldots)$, где $c_k = \sum_{s+t=k} a_s b_t$. Степенью многочлена называется наибольшее целое неотрицательное d, для которого a_d не равно нулю.[1] Множество всех многочленов над $\mathbb{F}$ обозначается через $\mathbb{F}[x]$.

Многочлен $(a_0, a_1, a_2, \ldots, a_n, \ldots) \in \mathbb{F}[x]$ мы будем записывать более привычным образом как $a_d x^d + \ldots + a_1 x + a_0$. Здесь эта запись – это формальное обозначение, x – это формальный символ.

Определение. Значением многочлена $f = a_d x^d + \ldots + a_1 x + a_0 \in \mathbb{F}[x]$ в точке $x_0 \in \mathbb{F}$ называется элемент $f(x_0) := a_d x_0^d + a_{d-1} x_0^{d-1} + \ldots + a_1 x_0 + a_0$ поля $\mathbb{F}$. Из аксиом поля следует, что для любых $f, g \in \mathbb{F}[x], x_0 \in \mathbb{F}$ верно $f(x_0) + g(x_0) = (f+g)(x_0); f(x_0)g(x_0) = (fg)(x_0)$.

Далее по умолчанию все многочлены – это элементы $\mathbb{F}[x]$, где $\mathbb{F}$ – произвольное поле.

Упражнение. Докажите, что для любых многочленов f, g имеет место $\deg(fg) = \deg(f) + \deg(g)$ и $\deg(f+g) \leqslant \max(\deg(f), \deg(g))$. В частности, произведение двух ненулевых многочленов – ненулевой многочлен.

Аналогично случаю многочленов с вещественными коэффициентами, для элементов $\mathbb{F}[x]$ определяются понятия корня и кратности корня. Также аналогично формулируются и доказываются теорема Виета, теорема Безу и теорема о том, что любой ненулевой многочлен f над полем имеет не более $\deg(f)$ корней с учётом кратности.

Определение. Говорят, что многочлен f делится на многочлен g, если существует такой многочлен h, что $f = gh$. Многочлен f называется неприводимым над $\mathbb{F}$, если f имеет степень не меньше 1 и f нельзя разложить в произведение двух многочленов над $\mathbb{F}$ степени не меньше 1. Иными словами, многочлен степени $\geqslant 1$ неприводим тогда и только тогда, когда он делится лишь на ненулевые константы [2] и на многочлены, получаемые из него умножением на ненулевые константы. Многочлен h называется наибольшим общим делителем многочленов f и g, если f и g делятся на h и h делится на любой общий делитель f и g.

Факт. Над $\mathbb{C}$ неприводимы только линейные многочлены. Многочлен над $\mathbb{R}$ неприводим тогда и только тогда, когда он линейный или квадратный с отрицательным дискриминантом. Над $\mathbb{Q}$ найдётся неприводимый многочлен любой степени; для

[1] Договоримся считать степень нулевого многочлена равной $-\infty$.
[2] Константами называются нулевой многочлен и многочлены степени нуль.

любого простого p над $\mathbb{F}_p$ также найдётся неприводимый многочлен любой степени.[3]

Упражнение. Кубический многочлен над полем неприводим тогда и только тогда, когда он не имеет корней.

Теорема. а) Для любых многочленов $g \neq 0, f$ найдутся такие многочлены q, r, что $f = gq + r$ и $\deg(r) < \deg(g)$.
б) Для любых двух ненулевых многочленов f, g существует НОД. Если h является НОДом f и g, то найдутся такие u, v, что $fu + gv = h$.
в) Любой многочлен раскладывается в произведение неприводимых, причём это разложение однозначно с точностью до порядка сомножителей и умножения на ненулевую константу.

План доказательства. Возможность деления с остатком (пункт а)) доказывается стандартной процедурой деления уголком – она работает над любым полем. Далее с помощью деления с остатком вводим алгоритм Евклида. Тогда результат h применения алгоритма Евклида к многочленам f, g является общим делителем f и g, причём h делится на любой другой общий делитель f и g, откуда получаем, что $h = \text{НОД}(f, g)$. Алгоритм Евклида также даёт нам и линейное разложение НОДа (пункт б)). Доказательство пункта в) использует линейное разложение НОДа и по сути повторяет доказательство обычной основной теоремы арифметики о разложении натурального числа на простые множители.

Упражнение. $\text{НОД}(f, g)$ определён с точностью до умножения на ненулевую константу (т. е. любые два многочлена, являющиеся НОДом, отличаются умножением на ненулевую константу).

В этом листке нас в первую очередь будет интересовать случай многочленов над полем $\mathbb{F}_p$.

Определение. Редукцией многочлена с целыми коэффициентами по модулю простого числа p называется многочлен с коэффициентами в $\mathbb{F}_p$, полученный заменой всех коэффициентов исходного многочлена на их остатки по модулю p. Будем обозначать редукцию многочлена f по модулю p через $[f]_p$.
Два свойства редукции:
1) $\deg(f) \geqslant \deg[f]_p$.
2) $[f + g]_p = [f]_p + [g]_p$; $[fg]_p = [f]_p[g]_p$.

Упражнения.
1) Найти все неприводимые многочлены степени 2 над $\mathbb{F}_2$ и над $\mathbb{F}_3$.
2) Разложить на неприводимые множители многочлен $f(x) = x^3 + x + 1$ с коэффициентами в $\mathbb{F}_3$
3) Разложить на неприводимые множители многочлен $f(x) = x^4 + x^2 + 1$ с коэффициентами в $\mathbb{F}_2$.

[3]Здесь $\mathbb{F}_p$ – это обозначение поля остатков по модулю p.

1. **(a)** Рассмотрим многочлен из $\mathbb{F}_p[x]$. Докажите, что его значения во всех точках равны нулю тогда и только тогда, когда этот многочлен делится на $x^p - x$.
(b) Разложите на неприводимые множители многочлен $x^p - 1 \in \mathbb{F}_p[x]$.

2. Для какого-нибудь натурального составного m приведите пример ненулевого многочлена над $\mathbb{Z}_m$, число различных корней которого больше его степени.

3. Пусть $a \in \mathbb{F}_p$. Запишите в замкнутом виде какой-нибудь многочлен $h \in \mathbb{F}_p[x]$, значение которого в точке a равно 1, а в остальных точках – нулю.

4. **(a)** Пусть p – простое число, $e_k(x_1, x_2, \ldots, x_p)$ – k-й стандартный симметрический многочлен от p переменных (сумма всевозможных произведений по k различных множителей; $1 \leqslant k \leqslant p$). Докажите, что при всех $k \neq p-1$ $e_k(1, 2, \ldots, p)$ делится на p.
(b) Докажите, что если $h(x)$ – многочлен с целыми коэффициентами степени не больше $p-2$, то $h(1) + h(2) + \ldots + h(p) \equiv 0 \pmod{p}$.

5. Назовём многочлен с целыми коэффициентами *перестановочным* по модулю p, если его значения дают все возможные остатки при делении на p. Существует ли перестановочный по модулю 101 многочлен степени
(a) 17; **(b)** 100; **(c)** 10?

6. Напомним, что ненулевой элемент a поля $\mathbb{F}_p$ называется квадратичным вычетом по модулю нечётного простого p, если многочлен $x^2 - a \in \mathbb{F}_p[x]$ имеет корень. Докажите, что $a \in \mathbb{F}_p$ является квадратичным вычетом тогда и только тогда, когда $a^{(p-1)/2} = 1$.

7. Можно ли разбить числа от 1 до 2016 на группы по 7 так, чтобы сумма чисел в каждой семёрке делилась на 2017?

8. Дано простое число p и натуральное число $n \geqslant p$. Пусть $a_1, a_2, \ldots, a_n$ – произвольный набор натуральных чисел, а f_k – количество k-элементных подмножеств этого набора, сумма чисел в которых делится на p. Докажите, что $\sum_{k=0}^{n} (-1)^k f_k \vdots p$. (Мы считаем, что $f_0 = 1$.)

9. Пусть p – нечётное простое. Про целые числа $a_1, a_2, \ldots, a_p$ известно, что $a_1^k + a_2^k + \ldots + a_p^k$ делится на p при любом натуральном k. Докажите, что все a_i числа попарно сравнимы по модулю p.

10. Вооружившись теорией про многочлены над полями, дорешайте задачу 10 из листочка про поля.