ВВЕДЕНИЕ В МНОГОЧЛЕНЫ

МНОГОЧЛЕНЫ НАД $\mathbb{Z}/m\mathbb{Z}$

Ближайшие несколько уроков мы посвятим изучению многочленов.

Многочленом называется выражение вида

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$,

где a_i — коэффициенты, причем $a_n \neq 0$.

С одной стороны, многочлены — формальные выражения, которые можно складывать, умножать и т.д., приводя подобные слагаемые при одинаковых степенях и получая новые многочлены.

С другой стороны, многочлены можно рассматривать как функции и находить их значения при разных значениях переменной x.

Например, подставив $x = 1$, мы получим сумму всех коэффициентов многочлена:

$f(1) = a_n + a_{n-1} + \ldots + a_1 + a_0$.

Подставив $x = 0$, получим свободный член a_0:

$f(0) = a_0$.

В школе рассматривают многочлены над полем вещественных чисел. А мы будем рассматривать многочлены над $\mathbb{Z}/m\mathbb{Z}$ — конечной арифметикой остатков по модулю m.

Нас будет интересовать:

- степень многочлена $\deg f = n$, где $a_n \neq 0$ — коэффициент при старшем члене многочлена;
- корень многочлена — это любое такое число $\bar{x}$, что $f(\bar{x}) = 0$.

ЗАМЕЧАНИЕ

Рассматривая многочлены над $\mathbb{Z}/m\mathbb{Z}$, мы под корнем понимаем любое такое число $\bar{x}$, что значение многочлена $f(\bar{x})$ делится на m (сравнимо с нулем в этой конечной арифметике). При этом корни, отличающиеся на число, кратное m (сравнимые между собой по модулю m), мы считаем одинаковыми.

УПРАЖНЕНИЕ

Доказать, что если $\bar{x} \equiv \bar{y} \bmod m$, то $f(\bar{x}) \equiv f(\bar{y}) \bmod m$.

СТЕПЕНЬ ПРОИЗВЕДЕНИЯ НАД $\mathbb{Z}/m\mathbb{Z}$

Вопрос: что изменится по сравнению с привычным нам случаем, когда мы рассматривали многочлены над полем вещественных чисел?

Вспомним, что мы знаем о многочленах над $\mathbb{R}$.

Умножение многочленов:

$f(x)g(x) = (a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0)$.
$(b_r x^r + b_{r-1} x^{r-1} + \ldots + b_1 x + b_0) = a_n b_r x^{n+r} +$
$+ (a_{n-1} b_r + a_n b_{r-1}) x^{n+r-1} + \ldots + (a_0 b_1 + a_1 b_0) x + a_0 b_0$.

Если $a_n, b_r \in \mathbb{R}$, $a_n, b_r \neq 0$, то $a_n, b_r \neq 0$.
А значит, $\deg(fg) = \deg f + \deg g$.

Что же будет в конечной арифметике?

ПРИМЕР:

Рассмотрим над $\mathbb{Z}/6\mathbb{Z}$ произведение многочленов

$f(x) = 3x - 1$ и $g(x) = 2x + 1$.
$f(x)g(x) = (3x - 1)(2x + 1) = 6x^2 + x - 1$.
$6x^2 \equiv 0 \bmod 6 \Rightarrow f(x)g(x) = x - 1$.

Во-первых, мы получили, что степень произведения многочленов не равна сумме степеней множителей.

Во-вторых, для многочлена первой степени $x - 1$ мы получили нетривиальное разложение на множители, что также невозможно для многочленов над $\mathbb{R}$.

Над $\mathbb{R}$ многочлены образуют кольцо (можно убедиться, что все аксиомы выполнены). В этом кольце все линейные многочлены неразложимы, они выполняют роль простых чисел в обычной арифметике.

Далее мы увидим еще целый ряд парадоксов, связанных с переходом к конечным системам остатков.

Вопрос состоит в том, какие условия должны быть выполнены, чтобы подобные парадоксы не возникали.

КОЛИЧЕСТВО КОРНЕЙ НАД $\mathbb{Z}/m\mathbb{Z}$

Итак, нам хотелось бы, чтобы над $\mathbb{Z}/m\mathbb{Z}$ выполнялось $deg(fg) = deg\, f + deg\, g$.

Для этого должно гарантированно выполняться $a_n b_r \neq 0$ при $a_n, b_r \neq 0$ в $\mathbb{Z}/m\mathbb{Z}$. Это возможно только если $m = p$ — простой модуль. Отсюда также будет следовать неразложимость всех многочленов первой степени над $\mathbb{Z}/p\mathbb{Z}$.

Еще один парадокс связан с количеством корней многочлена. Мы знаем, что над $\mathbb{R}$ число корней многочлена f не превосходит $deg\, f$.

ПРИМЕР:

Рассмотрим над $\mathbb{Z}/8\mathbb{Z}$ многочлен $f(x) = x^2 - 1$.
Вспомним таблицу умножения ненулевых остатков по модулю 8:

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Корнями многочлена $f(x) = x^2 - 1$ будут все остатки, дающие на диагонали таблицы 1. Таким образом, имеем для многочлена 2-й степени 4 различных корня: $x_1 = 1$, $x_2 = 3$, $x_3 = 5$, $x_4 = 7$.

Нам нужно исключить подобные ситуации, поэтому в дальнейшем мы перейдем к рассмотрению многочленов над $\mathbb{Z}/p\mathbb{Z}$, где p — простое. В этом случае конечная арифметика остатков является полем.

Но сначала мы докажем теорему Безу, которая верна в конечной арифметике по любому модулю, то есть не только над полем, но и над кольцом. Этим мы займемся на следующем уроке.