ДЕЛЕНИЕ МНОГОЧЛЕНА НА $x - b$

Научимся делить произвольный многочлен
$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$,
на многочлен вида $x - b$.

Будем делить в столбик, точно так же, как с числами:

$$
\begin{array}{r|l}
-\; a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 & x - b \\
\underline{a_n x^n + a_n b x^{n-1}} \qquad\qquad\qquad & \overline{a_n x^{n-1} + \ldots} \\
-\; (a_{n-1} + a_n b) x^{n-1} + \ldots & \\
\ldots \qquad\qquad &
\end{array}
$$

ВОПРОС: до какого момента продолжается деление?

ОТВЕТ: до появления в остатке некоторого числа A.

(Если $A = 0$, то $f(x)$ делится на $x - b$ без остатка).

В результате мы получим, что $f(x) = g(x)(x - b) + A$,
где $g(x)$ — многочлен степени $n - 1$ со старшим коэффициентом a_n.

ТЕОРЕМА БЕЗУ

Остаток от деления многочлена $f(x)$ на $x - b$ равен значению $f(x)$ при $x = b$: $f(x) = g(x)(x - b) + f(b)$.

ДОКАЗАТЕЛЬСТВО

Подставим $x = b$ в равенство $f(x) = g(x)(x - b) + A$:
$f(b) = g(b)(b - b) + A$.
Т.к. $b - b = 0$, получаем $A = f(b)$.

Что и требовалось доказать.

$x^2 - 1$ НАД $\mathbb{Z}/8\mathbb{Z}$ И ТЕОРЕМА БЕЗУ

Рассмотрим наш пример из предыдущего урока:
многочлен $x^2 - 1$ над кольцом $\mathbb{Z}/8\mathbb{Z}$. Разделим его на $x - 1$.

$$
\begin{array}{r|l}
-\; x^2 - 1 & x - 1 \\
\underline{x^2 - x} & \overline{x + 1} \\
-\; x - 1 & \\
\underline{x - 1} & \\
0 &
\end{array}
$$

Мы получили в частном $x + 1$ и в остатке 0, а значит,
$x^2 - 1 = (x - 1)(x + 1)$.

А теперь вспоминаем, что у $x^2 - 1$ есть и другие корни.

Например, $x = 3$. Тогда многочлен $x^2 - 1$ должен поделиться нацело на $x - 3$. Поделим:

Действительно, т.к. $8 \equiv 0 \bmod 8$, мы получили деление без остатка:
$x^2 - 1 = (x - 3)(x + 3)$.

Мы получили два разных разложения на простые множители в кольце многочленов над $\mathbb{Z}/8\mathbb{Z}$, что было бы невозможно над $\mathbb{R}$, где выполнена основная теорема арифметики для многочленов. К тому же здесь нельзя гарантировать неразложимость («простоту») многочленов вида $x - b$.

Изучим далее деление любого многочлена на любой и посмотрим, когда выполнена основная теорема арифметики.

2 СЛЕДСТВИЕ ТЕОРЕМЫ БЕЗУ ДЛЯ $\mathbb{Z}/p\mathbb{Z}$

Просуммируем, что мы знаем.

В кольце многочленов над $\mathbb{Z}/m\mathbb{Z}$ для любого модуля m верны следующие утверждения:

ТЕОРЕМА БЕЗУ

Остаток от деления $f(x)$ на $x - b$ равен $f(b)$;

СЛЕДСТВИЕ

b — корень $f(x) \Leftrightarrow f(x) = g(x)(x - b)$.

Если p — простое, то над $\mathbb{Z}/p\mathbb{Z}$ верно также:

СЛЕДСТВИЕ ($\mathbb{Z}/p\mathbb{Z}$)

Если c — другой корень многочлена $f(x)$, то c является корнем многочлена $g(x)$.

Тем самым, выполнено: $f(x) = h(x)(x - c)(x - b)$ для некоторого многочлена $h(x)$.

ДОКАЗАТЕЛЬСТВО

Действительно, подставим $x = c$ в равенство $f(x) = g(x)(x - b)$.

Получим: $0 = f(c) = g(c)(c - b)$.

Т.к. $c - b \neq 0$ по модулю p, в силу простоты p должно быть выполнено $g(c) = 0$. А значит, c — корень многочлена $g(x)$. Доказано.

Данное следствие будет работать в любом поле.

Вспомним наш пример:
многочлен $x^2 - 1$ над кольцом $\mathbb{Z}/8\mathbb{Z}$.

В результате деления на $x - 1$ мы получили следующее представление:
$x^2 - 1 = (x - 1)(x + 1)$.

Подставим в него $x = 3$. Получим:
$0 = 3^2 - 1 = (3 - 1)(3 + 1) = 2 \cdot 4$.

В арифметике $\mathbb{Z}/8\mathbb{Z}$ остатки 2 и 4 являются делителями 0, т.е. будучи сами отличными от 0, в произведении они дают 0. Поэтому в такой ситуации нельзя сделать вывод, что многочлен, который получается при делении на $x - 1$, наследует другой корень многочлена $x^2 - 1$.

Далее мы будем рассматривать многочлены только над $\mathbb{Z}/p\mathbb{Z}$.

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

Заметим, что все выводы, которые мы получим для многочленов над полем остатков по простому модулю p, справедливы для любого другого поля.

ТЕОРЕМА О КОРНЯХ МНОГОЧЛЕНА

Для любого многочлена $f(x)$ над полем $\mathbb{Z}/p\mathbb{Z}$ число корней $f(x)$ не превосходит $\deg f$.

Если $b_1, b_2, \dots b_l$ — различные корни $f(x)$, то
$f(x) = h(x)(x - b_1)(x - b_2) \cdot \ldots \cdot (x - b_l)$.

ДОКАЗАТЕЛЬСТВО

Мы уже знаем, что если b_1 и b_2 — корни $f(x)$, то $f(x) = \alpha(x)(x - b_1)(x - b_2)$ для некоторого многочлена $\alpha(x)$. Подставим в это равенство $x = b_3$:
$0 = f(b_3) = \alpha(b_3)(b_3 - b_1)(b_3 - b_2)$.

По простому модулю это равенство возможно только если $\alpha(b_3) = 0$. Но тогда по следствию из теоремы Безу многочлен $\alpha(x)$ делится нацело на $x - b_3$:
$\alpha(x) = \bar{\alpha}(x)(x - b_3)$.

Значит, и $f(x)$ делится нацело на $x - b_3$.
По индукции можно заключить, что утверждение верно для всех остальных корней многочлена $f(x)$.

Итак, мы доказали,
что $f(x) = h(x)(x - b_1)(x - b_2) \cdot \ldots \cdot (x - b_l)$.

Тогда $deg\ h = deg\ f - l$, т.к. при каждом делении степень падает на 1.

То есть, если есть $deg\ f$ различных корней, то степень оставшегося многочлена $h(x)$ будет равна 0, и мы получим полное разложение $f(x)$ на линейные множители:
$f(x) = (x - b_1)(x - b_2) \cdot \ldots \cdot (x - b_{deg\ f})$.

Теорема доказана.

На следующем уроке мы перейдем к долгому изучению малой теоремы Ферма. Но прежде поговорим об основной теореме арифметики для многочленов, рассматриваемых над полями, в частности, $\mathbb{Z}/p\mathbb{Z}$.