Деление многочленов в полях $\mathbb{Z}_p$

1 Деление многочленов с вещественными коэффициентами (напоминание)

Деление многочленов с остатком — это операция, аналогичная делению чисел с остатком. Чтобы поделить многочлен $a(x)$ на $b(x)$, нужно найти многочлены $q(x)$ (неполное частное) и $r(x)$ (остаток), чтобы выполнялось соотношение:

$$a(x) = b(x)q(x) + r(x),$$

при этом степень остатка должна быть меньше степени делителя: $\deg r(x) < \deg b(x)$.

Многочлены, как и числа, можно делить в столбик. Традиционную запись деления можно посмотреть, например, в википедии в статье «деление многочленов столбиком». В этом тексте нам будет проще оформлять деление иначе, но в своих работах рекомендуется использовать традиционную запись.

Поделим, например, x^4 на $x^2 + 1$:

$$\begin{array}{ll}
x^4 & \\
x^4 + x^2 & = \mathbf{x^2}(x^2+1) \\
\hline
-x^2 & \\
-x^2 - 1 & = -\mathbf{1}(x^2+1) \\
\hline
1 &
\end{array}$$

На первом шаге делитель домножен на x^2, результат умножения вычитается из делимого, остается многочлен $-x^2$. Чтобы сократить с ним, делитель домножается на -1, и после вычитания остается единица. Это значит, что остаток от деления равен единице, а неполное частное составлено из множителей для делителя, оно равно $x^2 - 1$. Это можно записать так:

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

Другой пример, поделим $6x^4 - 7x^3 + 5x^2 + 3x - 1$ на $3x^2 - 2x + 3$:

$$
\begin{array}{llllll}
6x^4 & -7x^3 & +5x^2 & +3x & -1 & \\
6x^4 & -4x^3 & +6x^2 & & & =\mathbf{2x^2}(3x^2-2x+3) \\
\hline
 & -3x^3 & -x^2 & +3x & -1 & \\
 & -3x^3 & +2x^2 & -3x & & =-\mathbf{x}(3x^2-2x+3) \\
\hline
 & & -3x^2 & +6x & -1 & \\
 & & -3x^2 & +2x & -3 & =-\mathbf{1}(3x^2-2x+3) \\
\hline
 & & & 4x & +2 &
\end{array}
$$

Итого, $6x^4 - 7x^3 + 5x^2 + 3x - 1 = (3x^2 - 2x + 3)(2x^2 - x - 1) + (4x + 2)$.

2 Деление в поле $\mathbb{Z}_p$

В предыдущем разделе многочлены имели в качестве коэффициентов вещественные числа. Теперь множество коэффициентов многочлена — это поле $\mathbb{Z}_p$. Фактически, это целые числа по модулю p. Другими словами, в качестве коэффициентов многочлена можно использовать только целые числа, причем числа, сравнимые по модулю p, считаются одинаковыми. Например, по модулю 7, многочлены $x^2 + 2x + 3$ и $-6x^2 + 16x + 24$ — это одинаковые многочлены.

Поделим $3x^4 + 5x^3 + x + 3$ на $5x^2 + 2x + 1$ в $\mathbb{Z}_7$, т.е. по модулю 7. Первым шагом нужно подобрать множитель для делителя, чтобы совпали первые одночлены. Другими словами, нужно умножить что-то на $5x^2$, чтобы получить $3x^4$. В случае вещественных чисел домножать нужно на $\frac{3}{5}x^2$, но числа $\frac{3}{5}$ просто нет в поле $\mathbb{Z}_7$. Вспомним, что мы выполняем вычисления по модулю 7, и тогда домножить можно на 2, действительно, $2 \times 5x^2 = 10x^2$, а это то же самое, что $3x^2$ по модулю 7.

Теперь можем написать весь процесс деления.

$$
\begin{array}{l}
3x^4+5x^3 \qquad\quad +x+3 \\
3x^4+4x^3+2x^2 \qquad\quad =\mathbf{2x^2}(5x^2+2x+1) \\
\hline
\qquad x^3+5x^2\ +x+3 \\
\qquad x^3+6x^2+3x \quad = \mathbf{3x}(5x^2+2x+1) \\
\hline
\qquad\quad 6x^2+5x+3 \\
\qquad\quad 6x^2\ +x+4 = \quad \mathbf{4}(5x^2+2x+1) \\
\hline
\qquad\qquad 4x+6
\end{array}
$$

Обратите внимание, что в вычислениях используются коэффициенты многочлена только из диапазона от 0 до 6 (в общем случае от 0 до $p-1$). Все числа приводятся в этот диапазон. Например, при первом же вычитании из $0x^2$ вычитается $2x^2$, и здесь можно было бы написать ответ $-2x^2$, но он сразу превращен в $5x^2$ по модулю 7. Причина в том, что поле $\mathbb{Z}_p$, как принято считать, состоит только из возможных остатков по модулю p, поэтому числа -2 в поле не существеует. Мы только понимаем, что -2 это другая форма записи числа 5.

Ответ получился следующий: остаток $4x+6$, неполное частное — $2x^2+3x+4$. Его можно проверить следующим равенством:

$$3x^4+5x^3+x+3=(5x^2+2x+1)(2x^2+3x+4)+(4x+6).$$

Равенство верное, потому что после раскрытия скобок в правой части получается $10x^4+19x^3+28x^2+15x+3$, а это то же самое по модулю 7, что и левая часть.