Лекция по дискретной математике

29 апреля 2019

Задача интерполяции

Найти многочлен $p = F[x], p(x_i) = y_i$, где $x_i, y_i \in F, x_i \neq x_j \forall i, j$

К примеру, p(0) = 1, p(1) = 1, p(2) = 3

Теорема

Для задачи интерполяции

$p(x_i) = y_i$, где i = от 1 до n

$\exists$ единственный многочлен p, решение, причем $deg(p) <= n - 1$

Доказательство:

Единственность.

Пусть p и q оба подходят

$p(x) - q(x)$ имеет корни x_i (n штук)

$p(x) = q(x) = y_i$

$deg(p(x) - q(x)) <= n - 1 \Leftrightarrow p(x) - q(x) = 0$

Существование.

1. Метод Лагранжа

$\sum_{i=1}^{n} y_i = \frac{\prod_{j=1}^{n}(x-j)}{\prod_{j=1}^{n}(x_i - x_j)}$

Пример

p(0) = 1, p(1) = 1, p(2) = 3

$1 * \frac{(x-1)(x-2)}{(0-1)(0-2)} + 1 * \frac{(x-0)(x-2)}{(1-0)(1-2)} + 3 * \frac{(x-0)(x-1)}{(2-0)(2-1)}$

2. Метод Ньютона

Начинать с многочлена $p_1(x_1) = y_1$. Он подходит под одно уравнение - $p_1(x_1) = y_1$.

$p_2(x_2)$ должен подходить под два уравнения. $p_2(x_2) = y_2, p_2(x) = p_1(x) + (x - x_1)\alpha$

$p_{k+1}(x) = p_k(x) + (x - x_1)...(x - x_k)\alpha$

НОД многочленов

Определение

НОД p(x) и q(x) - многочлен d(x): 1) $p(x) \vdots d(x)$

$q(x) \vdots d(x)$

2) d(x) - наибольшая степень

Также, например, $d(x) \vdots \overline{\text{d(x)}}$, если $\overline{\text{d(x)}}$ - общий делитель p(x) и q(x).

Если $d_1(x)$ и $d_2(x)$ - НОДы p(x) и q(x), то $d_1(x) \vdots d_2(x)$ и $d_2(x) \vdots d_1(x)$

$\Rightarrow d_1(x) = d_2(x) * u(x)$, где deg(u(x)) = 0 (число)

Все НОД отличаются домножением на константу.

Можно рассматривать только d(x) со старшим коэффициентом, равном единице

Пример

$5x^2 - 6x + 1, 3x^2 + 2x - 5$

$\frac{5x^2-6x+1}{3x^2+2x-5} = \frac{5}{3} - \frac{28}{3}x + \frac{28}{3}$

$5x^2 - 6x + 1(1, 0)3x^2 + 2x - 5(0, 1)$

$-\frac{28}{3}x + \frac{28}{3}(1, -\frac{5}{3})3x^2 + 2x - 5(0, 1)$

НОД (p(x), q(x)) = НОД (α p(x), $\beta q(x)$)

Ответ: $-x + 1 = \frac{3}{28}5x^2 - 6x + 1 - \frac{5}{28}(3x^2 + 2x - 5)$

Аналогично числам, есть простые многочлены, или неприводные, их нельзя представить в виде произведения меньших степеней

Неприводимость

Приводимость зависит от поля

$x^2 + 1$ над $\mathbb{R}$ неприводим

$x^2 + 1$ над C приводим: $x^2 + 1 = (x + i)(x - i)$

$x^2 + 1$ над $\mathbb{Z}_2$ приводим: $x^2 + 1 = (x + 1)(x + 1)$

Утверждение

Над C неприводимы многочлены только первой степени $\alpha x + \beta, \alpha \neq 0$

Утверждение

Над $\mathbb{R}$ неприводимы только $\alpha x + \beta, \alpha x^2 + \beta x + \gamma$, где $\beta^2 - 4\alpha\gamma < 0$

Утверждение

Приводимость над $\mathbb{Q} \Leftrightarrow$ над $\mathbb{Z}$

Доказательство:

$p(x) = q(x) * r(x)$ p(x) имеет целые коэффициенты $q(x), r(x)$ имеют вещественные коэффициенты

Утверждение

f(x) с целыми коэф. проводим в $\mathbb{Q} \Rightarrow$ f(x) приводим в $\mathbb{Z}_p$, где старший коэффициент $f \not\vdots p$

Доказательство

f(x) = g(x)h(x). Рассмотрим по модулю p

$f(x) \equiv g(x)h(x) \pmod{p}$

f(x) той же степени, что и над Q[x]

Критерий Эйзенштейна

приводимость над $\mathbb{Z}(Q)$

$a_n x^n + ... + a_1 x + a_0, p \in \mathbb{P}$

Если $a_n \not\vdots p, a_i \vdots p, a_0 \not\vdots p^2$

$\Rightarrow$ многочлен неприводим

Пример:

$x^3 + 2x^2 + 4x - 2$ неприводим (при p = 2)

$x^n \pm 2$ неприводим

Доказательство:

$a_n x^n + ... + a_0 = (b_m x^m + ... + b_0) * (c_k x^k + ... + c_0)$

$b_0 c_0 = a_0 \vdots p \Rightarrow b_0$ или $c_0 \vdots p (a_0 \not\vdots p^2)$

$b_0c_1 + b_1c_0 = a_1 \vdots p$

$b_0c_1 \vdots p \Rightarrow b_1c_0 \vdots p \Rightarrow b_1 \vdots p$

$\Rightarrow b_i \vdots p \forall i \Rightarrow a_n \vdots p$

Над $\mathbb{Z}_2$ неприводимы x+1, x