Lagrange-interpoláció

Tétel

Legyen R test, $c_0, c_1, \ldots, c_n \in R$ különbözőek, továbbá $d_0, d_1, \ldots, d_n \in R$ tetszőlegesek. Ekkor létezik egy olyan legfeljebb n-ed fokú polinom, amelyre $f(c_j) = d_j$, ha $j = 0, 1, \ldots, n$.

Bizonyítás

Legyen

$$\ell_j(x) = \frac{\prod_{i \neq j}(x - c_i)}{\prod_{i \neq j}(c_j - c_i)},$$

a j-edik Lagrange-interpolációs alappolinom, és legyen

$$f(x) = \sum_{j=0}^{n} d_j \ell_j(x).$$

$\ell_j(c_i) = 0$, ha $i \neq j$, és $\ell_j(c_j) = 1$-ből következik az állítás.

Lagrange-interpoláció

Példa

Adjunk meg olyan $f \in \mathbb{R}[x]$ polinomot, amelyre $f(0) = 3$, $f(1) = 3$, $f(4) = 7$ és $f(-1) = 0$!

A feladat szövege alapján $c_0 = 0$, $c_1 = 1$, $c_2 = 4$, $c_3 = -1$, $d_0 = 3$, $d_1 = 3$, $d_2 = 7$ és $d_3 = 0$ értékekkel alkalmazzuk a Lagrange-interpolációt.

$\ell_0(x) = \frac{(x-1)(x-4)(x+1)}{(0-1)(0-4)(0+1)} = \frac{1}{4}x^3 - x^2 - \frac{1}{4}x + 1$

$\ell_1(x) = \frac{(x-0)(x-4)(x+1)}{(1-0)(1-4)(1+1)} = -\frac{1}{6}x^3 + \frac{1}{2}x^2 + \frac{2}{3}x$

$\ell_2(x) = \frac{(x-0)(x-1)(x+1)}{(4-0)(4-1)(4+1)} = \frac{1}{60}x^3 - \frac{1}{60}x$

$\ell_3(x) = \frac{(x-0)(x-1)(x-4)}{(-1-0)(-1-1)(-1-4)} = -\frac{1}{10}x^3 + \frac{1}{2}x^2 - \frac{2}{5}x$

$f(x) = 3\ell_0(x) + 3\ell_1(x) + 7\ell_2(x) + 0\ell_3(x) = \frac{22}{60}x^3 - \frac{3}{2}x^2 + \frac{68}{60}x + 3$

	$\frac{22}{60}$	$-\frac{3}{2}$	$\frac{68}{60}$	3	
1	$\times$	$\frac{22}{60}$	$-\frac{68}{60}$	0	3
4	$\times$	$\frac{22}{60}$	$-\frac{2}{60}$	1	7
-1	$\times$	$\frac{22}{60}$	$-\frac{112}{60}$	3	0

Lagrange-interpoláció

Alkalmazás

A Lagrange-interpoláció használható titokmegosztásra a következő módon:
legyenek $1 \leq m < n$ egészek, továbbá $s \in \mathbb{N}$ a titok, amit n ember között akarunk szétosztani úgy, hogy bármely m részből a titok rekonstruálható legyen, de kevesebből nem. Válasszunk a titok maximális lehetséges értékénél és n-nél is nagyobb p prímet, továbbá $a_1, a_2, \ldots, a_{m-1} \in \mathbb{Z}_p$ véletlen együtthatókat, majd határozzuk meg az $f(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_1x + s$ polinomra az $f(i)$ értékeket, és adjuk ezt meg az i. embernek $(i = 1, 2, \ldots, n)$.
Bármely m helyettesítési értékből a Lagrange-interpolációval megkapható a polinom, így annak konstans tagja is, a titok.
Ha m-nél kevesebb helyettesítési értékünk van, akkor nem tudjuk meghatározni a titkot, mert tetszőleges t esetén az $f(0) = t$ értéket hozzávéve a többihez létezik olyan legfeljebb m-ed fokú polinom, aminek a konstans tagja t, és az adott helyeken megfelelő a helyettesítési értéke.

Titokmegosztás

Példa

Legyen $m = 3$, $n = 4$, $s = 5$, $p = 7$, továbbá $a_1 = 3$ és $a_2 = 4$. Ekkor $f(x) = 4x^2 + 3x + 5 \in \mathbb{Z}_7[x]$, a titokrészletek pedig $f(1) = 5$, $f(2) = 6$, $f(3) = 1$ és $f(4) = 4$. Ha rendelkezünk például az $f(1) = 5$, $f(3) = 1$ és $f(4) = 4$ információkkal, akkor $c_0 = 1$, $c_1 = 3$, $c_2 = 4$, $d_0 = 5$, $d_1 = 1$, és $d_2 = 4$ értékekkel alkalmazzuk a Lagrange-interpolációt.

$$\ell_0(x) = \frac{(x-3)(x-4)}{(1-3)(1-4)} = \frac{1}{6}(x^2 - 7x + 12) = \frac{1}{-1}(-6x^2 - 2) = 6x^2 + 2$$

$$\ell_1(x) = \frac{(x-1)(x-4)}{(3-1)(3-4)} = -\frac{1}{2}(x^2 - 5x + 4) = -4(x^2 + 2x + 4) = 3x^2 + 6x + 5$$

$$\ell_2(x) = \frac{(x-1)(x-3)}{(4-1)(4-3)} = \frac{1}{3}(x^2 - 4x + 3) = 5(x^2 + 3x + 3) = 5x^2 + x + 1$$

$$f(x) = 5\ell_0(x) + \ell_1(x) + 4\ell_2(x) = 30x^2 + 10 + 3x^2 + 6x + 5 + 20x^2 + 4x + 4 =$$
$$= 53x^2 + 10x + 19 = 4x^2 + 3x + 5$$